ivanti

Ivanti EPMM 11.4.0.0 - 11.12.0.0 Device Management Guide

for iOS and macOS Devices

Revised: April 2024

Revision history

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

Contents

Managing Devices

This section addresses the management of devices.

Before you begin

Be sure to consider and configure "Enabling Server Name Lookup" below.

Once this has been done, then proceed to:

- "Registering Devices" on page 11
- "General management of devices" on page 53
- "Searching for Devices" on page 55
- "Securing Devices" on page 85

Enabling Server Name Lookup

Administrators must initiate registration or invite the device user to register. To do this, you will need to file a support ticket with Ivanti Customer Support, and provide the email domain and Ivanti EPMM URL. Ivanti then adds this information to the App Gateway. At this point, anyone with some effort can figure out how to query the App Gateway and discover your Ivanti EPMM URL irrespective of whether you enabled Server Name Lookup or not. If you are not comfortable that your Ivanti EPMM URL may be discovered by anyone, then you should not file a support ticket to enable Server Name Lookup.

If you have opted-in Server Name Lookup but now want to opt-out, it is not enough to deselect the Enable Server Lookup check box in Ivanti EPMM. You will need to file a support ticket and request that Server Name Lookup be disabled. See "Disabling Server Name Lookup" on the next page.

If the administrator has not enabled Server Name Lookup, the email the device user gets will ask them to enter the full URL of Ivanti EPMM into Ivanti Mobile@Work . If the administrator enabled Server Name Lookup, the email sent to the device user will ask them to enter the email domain.

Procedure

1. File a [support ticket](#) and provide the email_domain and the Ivanti EPMM URL. Ask that Server Name Lookup be enabled.

2. In the Admin Portal, go to **Settings > System Settings**.

3. Select on **Users & Devices > Device Registration**.

4. Select the **Enable Server Name Lookup** check box.

5. Select **Save**.

Disabling Server Name Lookup

If you have opted-in but now want to opt-out, it is not enough to deselect the Enable Server Lookup check box. You will need to file a support ticket and request that the Server Name Lookup be disabled. Once this is completed, anyone can discover the URL of your Ivanti EPMM.

> **IMPORTANT:** If you are not comfortable that your Ivanti EPMM URL can be discovered by anyone, you should not file a support ticket to disable Server Name Lookup.

Procedure

1. File a [support ticket](#) and provide the email_domain and the Ivanti EPMM URL. Ask that Server Name Lookup be disabled.

2. In the Admin Portal, go to **Settings > System Settings**.

3. Select on **Users & Devices > Device Registration**.

4. Deselect the **Enable Server Name Lookup** check box.

5. Select **Save**.

Registering Devices

A device is available for management by Ivanti EPMM 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 22
- "Visual privacy" on page 27
- " Invite users to register " on page 31
- "In-app registration for iOS " on page 33
- "Registering iOS and macOS devices through the web" on page 34
- "Registering macOS devices with Ivanti EPMM using Ivanti Mobile@Work for macOS" on page 40
- "ActiveSync device registration" on page 41
- "Managing operators and countries" on page 42
- "Specifying eligible platforms for registration" on page 44
- "Setting the registration PIN code length for device user registration" on page 45
- "Customizing registration messages" on page 45
- "Configuring the default ownership for newly registered devices" on page 51
- "Assign a unique attribute as a device's name" on page 52
- "Disabling analytics data collection" on page 53
- "Removing an old or expired MDM profile from an iOS or macOS device" on page 52
- "Disabling analytics data collection" on page 53

Refer to the *Getting Started with Ivanti EPMM* 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 Ivanti EPMM.

> ℹ️ Support for Android 5.0 and 5.1 has ended. Ivanti EPMM 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 45

The following registration methods are available:

- "In-app registration" on the next page

- "Customized registration using a URL or a QR Code" on page 16

- "Customized registration using SAML IdP" on page 19

- "Users register additional devices" on page 20

- "Administrator registers ActiveSync devices" on page 21

- "Registering an Apple TV" on page 21

- "Registration via user portal" on page 22

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

Administrator invites device users to register

For device 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

In-app registration

One way to reduce the load on IT personnel is to instruct iOS, macOS, and Android users to download the Ivanti EPMM app directly from the App Store on iTunes or from Google Play and initiate registration from within the Ivanti Mobile@Work app.

> ℹ️ If the administrator has not enabled Server Name Lookup, the email the device user gets will ask them to enter the full URL of Ivanti EPMM into Ivanti Mobile@Work. If the administrator enabled Server Name Lookup, the email sent to the device user will ask them to enter the email domain.

For iOS devices

1. Go to **Settings > System Settings > iOS > MDM** and select the **Send email to device user and notification to client if MDM profile is not installed** check box.

2. You will need to enable the MDM profile. In the MDM page, select the **Enable MDM Profile** check box.

   > ℹ️ You can enter the Apple ID used to generate or renew the MDM certificate.

3. Select **Save**.

4. Go to **Settings > System Settings > Users & Devices > Device Registration**. In the In-App Registration Requirement field, select one of the following:

   a. **Password** - device user will be required to enter username and password.

   b. **Registration PIN** - device user will be required to enter a registration PIN.

   c. **Password and Registration PIN** - device user will be required to enter a username, password, and registration PIN.

   d. **User and Registration PIN** - prompts device user to enter username and PIN.

   e. **Allow silent in-app registration only** - Selecting the check box will install the app silently. The app is installed when the device checks in with Ivanti EPMM.

5. **Silent in-app registration time limit (minutes) iOS and macOS)** - Keep the default 240 minutes or enter your preferred time limit.

6. Select **Save**.

7. For Apple Web-based Registration Requirement, select one of the following:

   a. **Password** - device user will be required to enter username and password.

   b. **Registration PIN** - device user will be required to enter a registration PIN.

   c. **Password and Registration PIN** - device user will be required to enter a username, password, and registration PIN.

   d. **User and Registration PIN** - prompts device user to enter username and PIN.

8. Select **Save**.

Device users of iOS 12.2 and later will need to download Ivanti Mobile@Work, manually navigate to Settings view and download the MDM profile.

Device users then complete the registration process by responding to registration prompts. If Ivanti EPMM detects that the MDM profile has not yet been installed, upon the next device check-in, Ivanti Mobile@Work will display a notification asking the device user to re-enroll.

> In iOS 13, the option to "Allow Always" was removed from the iOS Settings app. Instead, a dialog box displays requesting device users to enable tracking when the Ivanti Mobile@Work app is running. Ivanti Mobile@Work opens iOS Settings where device users can choose "Ask Next Time" or "Never". Ivanti, Inc recommends device users to enable tracking. This change applies to all versions of iOS 13 or supported newer versions. Ivanti Mobile@Work for iOS does not track device users' location without consent.

For macOS devices

- Applicable to macOS 11.0 or supported newer versions.
- Once completed, the mac device is a supervised device.

Procedure

For macOS device registration in the self-service portal, a device user must perform the following steps:

1. Log in with their credentials.

2. In the Install Management Profile page, the device user grants permission for the download of the profile. The profile is downloaded to the device user's local system.

3. Double-click the downloaded profile (macenroll.mobileconfig) to make it visible in the device user's System Preferences. There is limited time for the device user to install the profile before it becomes invalid.

4. Go to **System Preferences > Profiles**.

5. Select **Install** to install the management profile.

6. Continue and finish the installation procedure. Enter the system password when prompted.

Administrator tasks

- This feature depends on access to the Ivanti EPMM Gateway; therefore, the corresponding port must be properly configured. See the Pre-Deployment Checklist in the *On-Premise Installation Guide* for details. The User Portal role must be assigned to the user.

- To auto-populate the Ivanti EPMM server name during registration, the following setup is required:

    ○ The user associated with the device must be known as an LDAP user or defined as a local user.

    ○ To auto-populate based on the email address, you must register your VSP with Ivanti EPMM

- Set up the registration email template, see "Customizing registration messages" on page 45

- Schedule email reminders, see "Customizing registration messages" on page 45

- Send the email invitation to device users.

Customized registration using a URL or a QR Code

As a convenience, instead of device users entering registration credentials, you can setup an infrastructure to use a QR Code or URL link to automatically enter the registration credentials. This feature is applicable for iOS and macOS devices.

Before you begin

The company administrator must set up an infrastructure to generate a web page containing a QR Code or URL link from the credentials generated by UEM (see "Implementing infrastructure for QR code with device PIN" below.)

- In the case where the web page generated by the company is viewed on a computer, a QR Code would be appropriate to present. When constructing the QR code, it should contain a URL and follow this format:

    ```
    mirp://<server host name>&user=<Username>&pin=<PIN>
    ```

    Example: mirp://your.server.rock.com&user=you@rock.com&pin=4444

    > **i** It is recommended that the web page created by the administrator to provide a QR code also provides the instructions to download the app from the iTunes App Store or Google Play and the instructions to scan the QR code.

- In the case where the web page is viewed on the device where Ivanti Mobile@Work is being registered, a URL link would be appropriate.

Implementing infrastructure for QR code with device PIN

The below procedure works for iOS devices and utilizes the PIN code as part of the registration.

1. Enable the PIN code registration

1. Go to **Settings > Users & Devices > Device Registration**.

2. Select the appropriate field for the type of Android device:

   - For unmanaged Android devices, change the In-App registration requirement to **Registration PIN**.

   - For managed Android devices, change the Zero Touch and Samsung Knox Mobile Enrollment field OR the Managed Devices / Device Owner (afw#, QR code, NFC) field to **Registration PIN**.

2. Enable the QR code integration

1. Go to **Settings > Users & Devices > Device Registration**.

2. Select on Templates tab > Registration Templates.

3. Select your language and then select the **Edit** button.

4. In the Registration Email section, PIN field, replace the default text with this code:

   ```
   <li>Registration PIN: <i>$PASSCODE$</i> (valid for $PASSCODE_TTL$ hours)
   <p>
   Or Scan the QR Code:
   </p>
   <P>
   <img id=&#39;barcode&#39;
   src="https://api.qrserver.com/v1/create-qr-code/?data=mirp%3A%2F%2F$SERVER_
   URL$%26user%3D$USER_ID$%26pin%3D$PASSCODE$"
   width="200"
   height="200" />
   </P>
   ```

5. Select **Save**.

   When this code has been added, administrators can directly register a device from the Device Registration screen in Ivanti EPMM and / or the device user can initiate the registration from the e-mail invitation.

Registering using a web page on a desktop computer

Below is a sample implementation where the web page is viewed on a desktop computer.

Procedure

1. Ivanti EPMM administrator sends device user an email with a link to the company's webpage.

2. In the email, the device user taps on the link.

   The link opens to the company web page displaying a QR code on it.

3. On the user's device, the user goes to the iTunes App Store or Google Play and downloads Ivanti Mobile@Work.

4. User launches the phone's camera.

   > ℹ️ The Scan QR Code page may open. Device users will need to allow access to the device camera for scanning the QR code. Tap on **Open Settings**, slide the camera on, then return to Ivanti Mobile@Work.

5. User scans the QR code that is on the web page.

   The Ivanti Mobile@Work login page opens with the username, server address and PIN/password fields populated.

   > ℹ️ If the PIN field is not automatically populated, the device user will need to manually enter it.

6. User taps **Go** or **Register** and continues the registration process.

Note the following:

- On launching the Ivanti Mobile@Work app, the user can tap on the QR code icon (to the right of the user name field), and launch the in-app camera. This camera can then be used to scan the QR code and continue with the registration process.

- On devices running iOS 11.0 or later, the native camera can be used to scan the QR code. Upon scanning the QR code, the device user is prompted to launch Ivanti Mobile@Work. Tapping on the prompt launches Ivanti Mobile@Work with the device user's credentials filled in. The device user can then tap **Go** or **Register** to continue with the registration process.

- On devices running iOS 10, the native camera lacks the ability to scan QR codes. To work around this, the device user can launch the Ivanti Mobile@Work app, tap on the QR code icon (to the right of the user name field), and launch an in-app camera. This camera can then be used to scan the QR code and continue with the registration process.

Registering using a web page on an iOS device

Below is a sample implementation where the web page is viewed on an iOS device.

Procedure

1. Administrator sends device user an email with a link to the company's web page.

2. In the email, the device user taps on the link.

   The company's web page opens displaying two links.

3. Device user taps on the first link and downloads the Ivanti Mobile@Work app from the iTunes App store or from Google Play.

4. Device user taps on the second link, the Ivanti Mobile@Work login page opens with the username, server address and PIN/password fields populated.

   > ℹ️ If the PIN field is not automatically populated, the device user will need to manually enter it.

5. User taps **Go** or **Register** and continues the registration process.

   > ℹ️ In iOS 13, the option to "Allow Always" was removed from the iOS Settings app. Instead, a dialog box displays requesting device users to enable tracking when the Ivanti Mobile@Work app is running. Ivanti Mobile@Work opens iOS Settings where device users can choose "Ask Next Time" or "Never". Ivanti, Inc recommends device users to enable tracking. This change applies to all versions of iOS 13 or supported newer versions. Ivanti Mobile@Work for iOS does not track device users' location without consent.

Customized registration using SAML IdP

As a part of the registration process, device users log into a third-party identity provider (IdP), such as Ping. Once the authentication is successful, the device user is prompted to download the profile, completing the registration process.

Before you begin

You must have SAML enabled. See "Configuring SAML/IdP support" in the *Ivanti EPMM System Manager Guide*.

Procedure

1. Enable SAML in the System Manager.

2. Configure an identity provider.

3. In the Admin Portal, go to **Settings > Users & Devices > Device Registration** page.

4. In the Apple Web-based Registration Requirement field, select **SAML-based registration**. If this field is not selected, there will be no change in the registration.

   > Once SAML on iReg or DEP is set, SAML configuration from the System Manager can be either disabled or deleted. You must first de-select the "SAML-based registration" check box in the Device Registration page in Ivanti EPMM before you can disable the IdP SAML connection in the System Manager.

5. Select **Save**.

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

Administrator 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 Ivanti EPMM 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

Registering an Apple TV

You can register an Apple TV to Ivanti EPMM only through Apple Configurator.

Before you begin

The Apple TV must be connected to your corporate network. You can do this by configuring Wi-Fi on the Apple TV or connecting the Apple TV to your Ethernet.

Procedure

- Follow the instructions in "Distributing MDM Profiles with Apple Configurator" on page 134.

> ℹ️ Using the Apple TV Assistant to import the MDM profile results in an error message. Cancel out of the Apple TV Assistant.

You can do the following when you manage an Apple TV with Ivanti EPMM:

- View device information.

- Distribute Wi-Fi profiles to the Apple TV.

- Retire the device.

Registration via user portal

The user portal can be used to streamline the registration process. See "Self-service User Portal" on page 945 for more information.

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 EPMM*.

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 943.

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.

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

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

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 860.

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

[Decline] [Accept]

Visual privacy

Ivanti EPMM allows you to display privacy information to device users.

Visual privacy describes to users what device information is collected and why, and what actions administrators can take on the device, based on Ivanti EPMM settings. Additionally, Ivanti EPMM notifies users when changes are made to the privacy policy or MDM profile settings.

Users view the visual privacy information during registration, when they must accept the privacy policy.

> If both custom terms of service and the privacy policy are enabled, users will have to accept the privacy policy first.

Enabling visual privacy for devices

When enabled, end-users will be able to learn more about the privacy of their data. Ivanti Mobile@Work will show what content stays private on the device, what information is collected and why, and what actions the IT administrator can take on the debice, according to the settings on the server. This can help reduce end-user questions and concerns.

Procedure

1. Go to **Settings** > **System Settings > Users & Devices > Registration**.
2. Select **Enable privacy settings in Ivanti Mobile@Work** .
3. Select **Save**.

Viewing visual privacy settings in Ivanti Mobile@Work

Procedure

1. In Ivanti Mobile@Work , tap the **Settings** icon to open the Ivanti Mobile@Work Settings menu.
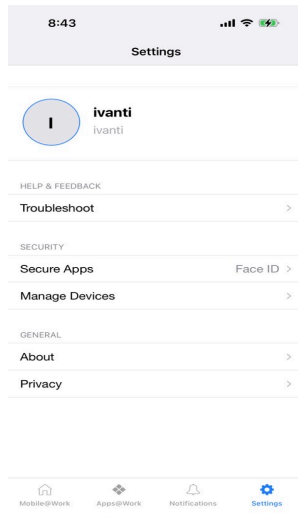
2. Tap **Privacy** to open the main **Privacy** menu.
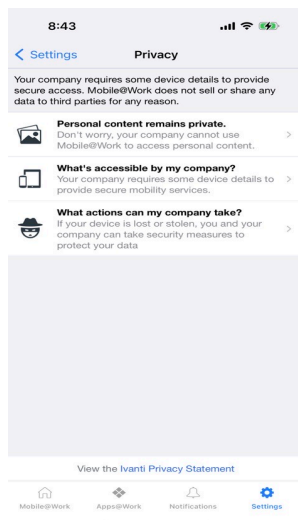
3. Tap each option in the **Privacy** menu to view more details about privacy related to personal content, device details accessible by your company, and actions your company can take if your device is lost or stolen.
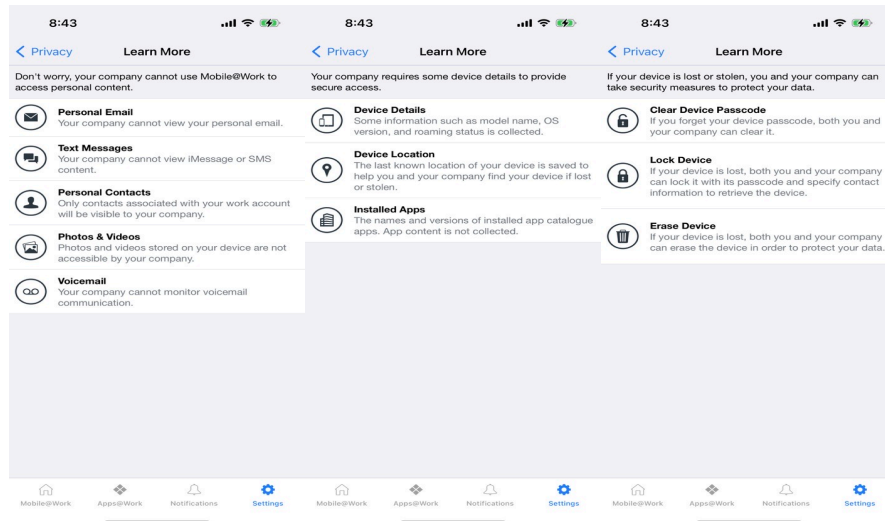
4. Alternatively, tap the **Ivanti Privacy Statement** link to view the privacy policy in its entirety.

Privacy policy for users

Upon registration with Ivanti EPMM, a visual privacy policy is displayed in Ivanti Mobile@Work . Users must tap **Continue** to accept the privacy policy and continue the registration process.

FIGURE 1. PRIVACY POLICY FOR USERS
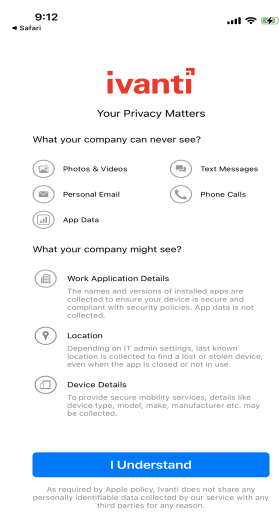
After registration, device users can view the new **Privacy** sub-menu from the **Settings** menu in Ivanti Mobile@Work .

FIGURE 2. PRIVACY SUB-MENU FOR USERS
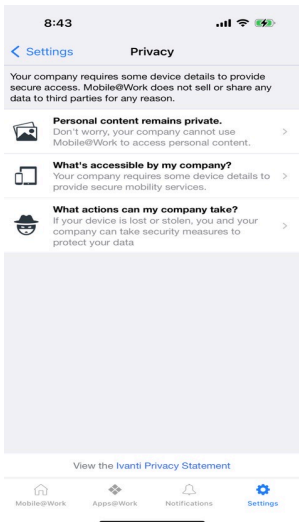
The **Privacy** sub-menu includes visual and text descriptions of the privacy of personal content, the device details accessible by Ivanti EPMM, and the actions that can be taken by Ivanti EPMM in the event that a user's device is lost or stolen.

FIGURE 3. PRIVACY DETAILS FOR USERS
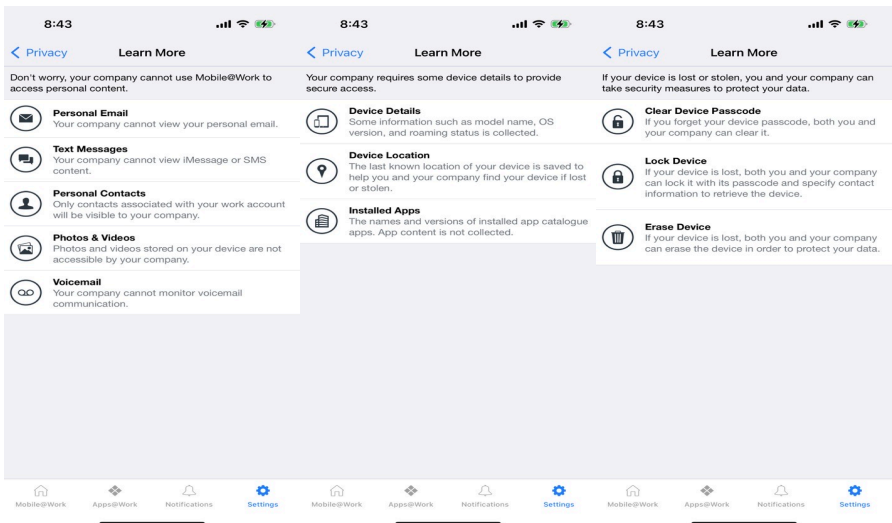
Invite users to register

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 945 for information on this self-service user portal. The administrator sends invitations that provide the instructions necessary to complete the registration process.

> ℹ️ Language-specific templates are not currently available for invitations.

See "Registration methods" on page 12 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**.

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 945 for information on what the user is expected to do to complete the registration process.

In-app registration for iOS

You can ask iOS device users to download Ivanti Mobile@Work from the iOS App Store and register by themselves.

Procedure

1. Make sure that the device user has a user record (local or LDAP) available in Ivanti EPMM. See "Managing Users" in *Getting Started with Ivanti EPMM*.

2. Instruct the device user on downloading the app and registering. The device user will need the following information:

   - user name

   - password and/or Registration PIN

   - server (and the port number, if you did not use the default port number for TLS)

Related topics

- "Registration methods" on page 12 for points to consider before using this registration method.

- iOS Apps@Work AppStore Features in the *Ivanti EPMM Apps@Work Guide*.

What the device user sees

> For iOS 12.2 or supported newer versions, when doing the iReg and in-app registration of the MDM profile, the device user experiences a different registration process.

After downloading and installing Ivanti Mobile@Work , the device user must register with Ivanti EPMM by entering their user name, password, and server details.

> In iOS 13, the option to "Allow Always" was removed from the iOS Settings app. Instead, a dialog box displays requesting device users to enable tracking when the Ivanti Mobile@Work app is running. Ivanti Mobile@Work opens iOS Settings where device users can choose "Ask Next Time" or "Never". Ivanti, Inc recommends device users to enable tracking. This change applies to all versions of iOS 13 or supported newer versions. Ivanti Mobile@Work for iOS does not track device users' location without consent.

If a customized terms of service agreement has been defined on Ivanti EPMM, device users will need to accept the agreement before registering with Ivanti EPMM.

Auto-populating the Ivanti EPMM server name during registration

Auto-populating the Ivanti EPMM server name streamlines the registration process and eliminates the need for the device user to type it. You can auto-populate the Ivanti EPMM server address based on the device phone number (for Android only) or the email address.

Auto-populating the Ivanti EPMM server name based on email address

To auto-populate the server name based on the device user's email address, you only need to register your Ivanti EPMM with Ivanti, Inc. Additional configuration on Ivanti EPMM is not required.

Device users must enter their full email address when prompted to enter their user name in the registration screen. Ivanti, Inc matches the email domain to the appropriate Ivanti EPMM and populates the registration screen with the correct server name.

Registering your Ivanti EPMM with Ivanti, Inc

To register your Ivanti EPMM, open a ticket on the Ivanti, Inc Support portal and provide the following information:

- Your company name (e.g. Ivanti, Inc)

- Your email domain (e.g. ivanti.com)

Registering iOS and macOS devices through the web

Web-based registration is the process of registering iOS and macOS devices in bulk for large deployments. The benefits of this style of registration include:

- iTunes accounts are not required
- No end-user interaction is required

> The MDM profile applied to macOS devices following registration is only applicable to the device user logged in to the device, not to the device itself. In effect, this means that devices running macOS and registered with Ivanti EPMM do not allow multi-user support.

For registering macOS devices using Ivanti Mobile@Work , see "Registering macOS devices with Ivanti EPMM using Ivanti Mobile@Work for macOS" on page 40.

Before you begin

Because users will be informed of the registration via email before they receive the device, consider turning off user notification when you bulk register devices. As an alternative, consider editing the registration template or informing users that they should ignore the email. See "Customizing registration messages" on page 45 for information on editing the template.

> Web-based registration requires a Safari browser on the device.

Procedure

1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Device Registration**.

2. Select the device registration settings that are relevant to your devices:

Item	Description
Enable Server Name Lookup	Select to enable server name lookup during registration. Enabling the Server Name Lookup makes registration easier by automatically filling in the server address for the device user. Administrators will need to follow important, specific instructions for this feature. Please see "Enabling Server Name Lookup" on page 9.
Allow registration when password change is required	When a device user logs in for the first time, he/she will be asked to update the password for the next login. Selecting this field allows Ivanti EPMM to authenticate the device user and completes enrollment. This is limited to device registrations only. Disabled by default.

Item	Description
Restrict device registrations by enrollment type	Select this option to restrict device registrations by enrollment type. Once checked, three additional checkboxes appear. Select all that apply: • Apple devices that are part of the Automated Device Enrollment Program • Android devices that are part of the Google Zero Touch • Android devices that are part of Samsung Knox Mobile Enrollment
Display QR Code and Registration URL	Enabled by default. When enabled, your users have access to a registration URL and QR code in their registration invitation.
In-App Registration Requirement	Select an authentication option for devices registering with Ivanti EPMM through Ivanti Mobile@Work : • **Password**: Select to enable authentication through Ivanti Mobile@Work using a password only. • **Registration PIN**: Select to enable authentication through Ivanti Mobile@Work using only a PIN. • **Password and Registration PIN**: Select to enable authentication through Ivanti Mobile@Work using both a password and a PIN. Note the following: • Registration PINs are valid for four hours. If a device user launches Ivanti Mobile@Work for iOS within four hours of web-based registration, the user does not need to re-enter credentials. • In-app registration does not apply to macOS devices.

Item	Description
Allow silent in-app registration only once. (iOS and macOS)	Consider this extra security option if you are: • including Ivanti Mobile@Work for iOS and macOS in the Ivanti EPMM App Catalog and • sending an installation request to devices after device users complete registration, such as with web-based registration. In this case, device users do not have to reenter their credentials when they launch Ivanti Mobile@Work . However, you can limit this silent registration with Ivanti Mobile@Work to one time only by selecting this option.
Silent in-app registration time limit (minutes) (iOS and macOS)	Allows the administrator to specify the silent registration grace period. The minimum can be 1 minute, the maximum 525600 minutes (365 days). The default value is 240 minutes (4 hours).
Apple Web-Based Registration Requirement	Select an authentication option for devices registering with Ivanti EPMM through the web: • **Password**: Select to enable authentication through the web using a password only. • **Registration PIN**: Select to enable authentication through the web using only a PIN. • **Password and Registration PIN**: Select to enable authentication through the web using both a password and a PIN. • **User and Registration PIN**: Select to enable authentication through the web using both their user name and a PIN. ⓘ These options also apply to macOS devices.

3. Click **Save**.

4. Apply the iOS or macOS label(s).

5. Bulk register the devices on Ivanti EPMM.

See "Bulk device registration" in the *Getting Started with Ivanti EPMM* for information on using bulk registration.

After these devices are registered, they will appear in the **Devices & Users > Devices** page with a status of Pending.

6. "Create a pending device report" on the next page.

7. On each device, point the browser to the following URL:

   https://<fully-qualified domain name for Ivanti EPMM>/go

   The registration screen appears.

8. Enter the requested information for the user who will receive the device.

   The registration screen appears.

9. Instruct the device user to enter the requested information.

10. Instruct the device user to tap or click **Register**.

    If a terms of service agreement has been defined, it is displayed here.
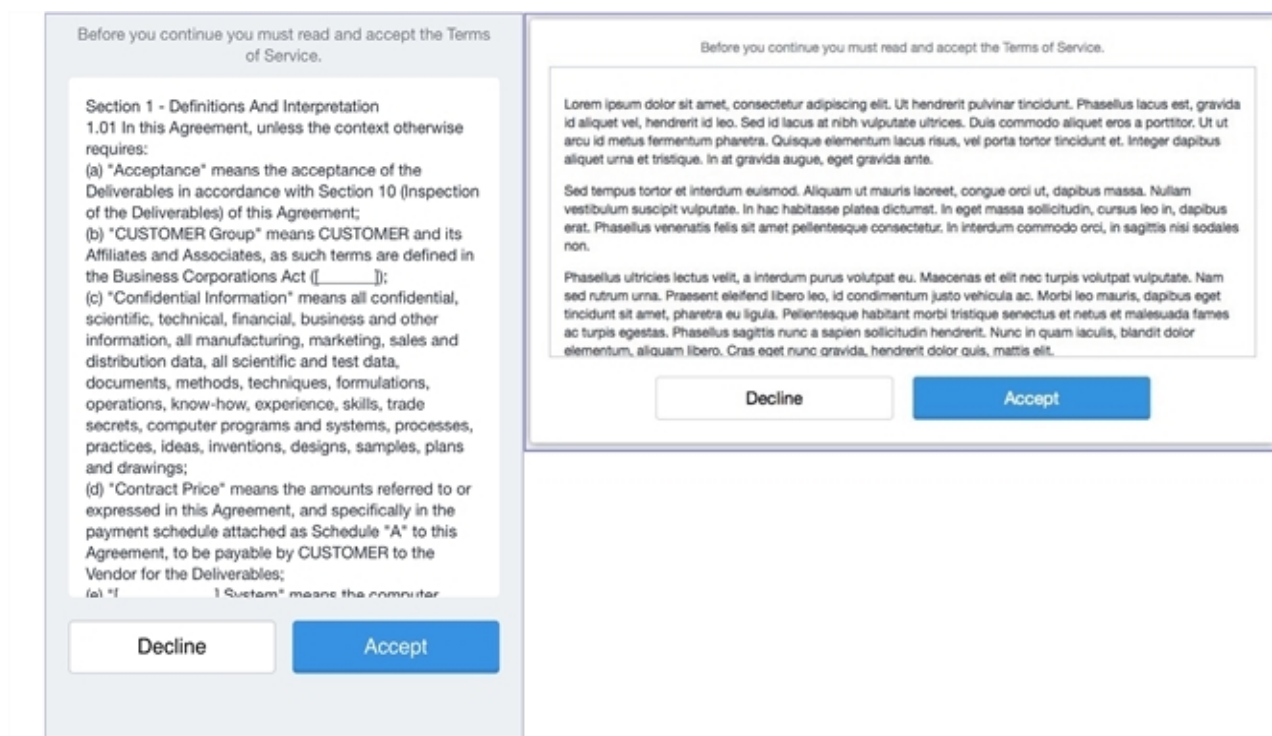
11. Instruct the device user to tap or click **Accept**.

12. Instruct the device user to follow the on-screen instructions for installing the relevant device management profiles.

Next steps

"Create a pending device report" below

Related topics

- "Auto-populating the Ivanti EPMM server name during registration" on page 34
- "Creating a terms of service agreement" on page 23
- "Visual privacy" on page 27
- "Limit for failed attempts to enter a registration password" on page 45

Create a pending device report

This feature is supported on macOS devices.

A pending device report is used to list the username and the PIN and/or password you will need to complete the registration process on each user's behalf.

Procedure

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

2. Open Advanced Search by clicking the advanced search icon.

3. Using the query builder, select the following:

   - Select **Status** for Field
   - Select **Equals** for Operator
   - Select **Pending** for Value

4. Click **Search**. The devices in pending state are shown in the table.

5. To download this report in CSV format, click **Export To CSV**. The report includes the PIN and/or password required to complete registration, as appropriate.

Next steps

For iOS devices, proceed to .

Registering macOS devices with Ivanti EPMM using Ivanti Mobile@Work for macOS

Ivanti Mobile@Work for macOS allows you to:

- register macOS devices with Ivanti EPMM using web-based registration (this automatically installs Ivanti Mobile@Work)
- run shell scripts on macOS devices.

As a convenience, instead of macOS device users manually entering registration credentials, you can set it up so devices are automatically registered with Ivanti EPMM.

What the device user sees:

1. Device user receives an email invitation with a link in it.

2. Device user selects on the link.

3. The device user enters username, password and accepts the terms of service displayed in Ivanti Mobile@Work for macOS.

4. Device user then downloads the enroll.mobileconfig file. When this happens, Ivanti Mobile@Work is automatically downloaded and user registration is automatically completed.

Note the following:

What happens after downloading the enroll.mobileconfig file varies based upon the user's browser and settings:

- If the user uses the default browser (Safari), Settings is launched with the enroll.mobileconfig file and the user will need to go through permissions dialogs to enable MDM on the mac.
- If the user is not using a default browser, the enroll.mobileconfig file is downloaded but Settings is not launched. This means the user will need to double-click on the enroll.mobileconfig file to continue registration.

What the administrator does

As with other types of devices, you can configure whether you want macOS device users to enter a password, PIN, or both during registration, as described in "Setting the registration PIN code length for device user registration" on page 45.

Device users can retire their macOS devices from Ivanti EPMM by uninstalling Ivanti Mobile@Work for macOS from their devices.

Procedure

1. Upload the PKG file for Ivanti Mobile@Work for macOS to a secure server. This server must be accessible to device users. See "Using the wizard to add an in-house macOS bundled app to the App Catalog" in the *Ivanti EPMM Apps@Work Guide*.
2. Set up the email invitation template. See "Customizing registration messages" on page 45
3. Send the email invitation to device users.
4. Monitor devices for status in **Devices & Users > Devices**.

Related topics

"Running shell scripts on macOS devices" on page 808

Customized terms of service

ActiveSync device registration

This feature is not applicable to macOS devices.

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 12 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 Ivanti EPMM* for instructions on completing the registration process.

Managing operators and countries

Ivanti EPMM 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. Ivanti EPMM 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. Select the check box next to each operator you want to enable.

4. Select **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.

> ℹ️ This feature only supports country operators for the US and Canada.

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. Select the arrow button to move them to the **Enabled Countries** list.

5. Select **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. Select the check box next to each operator you want to disable.

4. Select **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. Select the search icon to display the matching operators.

3. Select 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 an Ivanti EPMM-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. Select **Save**.

For iOS and macOS registration authentication, see "Registering iOS and macOS devices through the web" on page 34

Limit for failed attempts to enter a registration password

After the sixth failed attempt to enter a registration password, Ivanti EPMM 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.

Customizing registration messages

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.

Ivanti EPMM 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 Ivanti EPMM discovers device users that have not downloaded the MDM profile, reminder email scheduling capabilities are provided

Viewing registration templates

To view Ivanti EPMM message templates:

1. In Admin Portal, select **Settings > Templates**.

2. Select **Registration Templates**.

3. Select 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 select the **Edit** pencil icon.

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

3. Make changes to the displayed registration messages.

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

4. Select 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" on the next page for additional details.

5. Select **Save**.

Next steps

"Scheduling reminder notifications for completing registration" on page 49

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 select 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, Phone	REG_LINK
Registration Email	
Registration Email, Subject (Phone)	ENT_NAME, $USER, $PHONE$
Registration Email, Subject (PDA)	ENT_NAME, $USER, $PHONE$
Registration Email, Body(Phone)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
Registration Email, Body(PDA)	ENT_NAME, $BRAND_COMPANY_NAME$, REG_LINK, $INAPP_REG_STEPS$
Registration Email, Reminder Subject (Phone)	ENT_NAME, $USER$, $PHONE$
Registration Email, Reminder Subject (PDA)	ENT_NAME, $USER$, $PHONE$
Registration Email, Reminder Body (Phone)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
Registration Email, Reminder Body (PDA)	ENT_NAME, $BRAND_COMPANY_NAME$, REG_LINK, $INAPP_REG_STEPS$
Values for $INAPP_REG_STEPS$	
Server	$SERVER_URL$
Username	$USER_ID$
PIN	$PASSCODE$, $PASSCODE_TTL$
Post-Registration Email	

TABLE 2. VARIABLES USED IN DIFFERENT TYPES OF REGISTRATION MESSAGES (CONT.)

Type	Supported Variables
Post Registration Email, Subject (Phone)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$
Post Registration Email, Subject (PDA)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$
Post Registration Email, Body (Phones)	$PHONES$, $BRAND_COMPANY_NAME$

Variables used inside registration messages

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

TABLE 3. DESCRIPTION OF VARIABLES USED INSIDE REGISTRATION MESSAGES

Variable	Description
$BRAND_COMPANY_NAME$	An internal variable.
ENT_NAME	The name of the organization using Ivanti EPMM to secure the device. See the field **Enterprise Name** 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 Ivanti EPMM.
$PASSCODE_TTL$	The number of hours that the registration PIN remains valid. See the field **Passcode Expiry** in **Settings > System 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/i for iOS).
$SERVER_URL$	The Ivanti EPMM server address used for registration.
$USER$	The name of the user associated with the device, as displayed in Ivanti EPMM.
$USER_ID$	The user ID for the user associated with the device, as defined in the user account on Ivanti EPMM.

Scheduling reminder notifications for completing registration

This feature works on iOS devices only.

Ivanti EPMM detects whether device users have completed registration or not. To ensure that device users complete their registration, set up notifications to remind device users to complete the registration process. It is recommended that a notification is sent to the device user every hour.

Notifications are only possible if the registration is done within the Mobile@Work registration. No reminders are needed for Apple Device Enrollment registrations because the MDM profile is always installed as part of the Apple Device Enrollments.

Procedure

1. In the Admin Portal, select **Settings > System Settings**.

2. Select **iOS > MDM**. The MDM page displays.

3. Select the Send email to user and notification to client if MDM profile is not installed check box.

   The field expands, displaying additional fields.

4. Select how often to send a reminder email in the every hour field. If the device user registers within 8 minutes of the hour, the device user will not get a reminder until the next hour.

5. Select the Maximum Number of Emails / Notifications to be sent. A maximum of 24 emails/notifications can be sent within a 24-hour period.

6. Select **Save**.

Next steps

Send the email invitation to device users. See "Administrator invites device users to register" on page 12

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, Inc:

1. In the **Settings > Registration Templates** page, select the template you want to restore.

2. Select **Restore to Factory Default**.

Configuring the default ownership for newly registered devices

This feature is supported on macOS 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 "What is the self-service user portal?" on page 945

- Selecting **Devices & Users** > **Devices** > **Actions** > **Change Ownership** in Ivanti EPMM.

Procedure

1. In Ivanti EPMM, go to **Settings > System Settings > Users & Devices > Registration**.

2. Under Ownership Settings:

    a. For the **Default ownership for a newly registered device** setting, select the relevant radio button **Company owned** or **Employee owned**.

    b. For the **Default ownership for a device newly registered at the user Self-Serive Portal** setting, select the relevant radio button **Company owned** or **Employee owned**.

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

3. Select **Save**.

Assign a unique attribute as a device's name

You can assign a unique attribute as the device name for a supervised iOS device using "Substitution variables for compliance policy rules" on page 358. By setting the device names using the Device Name policy, the device name is automatically applied to the iOS device when the device registers with Ivanti EPMM.

For more information, see "Device name policies" on page 305

Related topics

- "Configuring a device name policy" on page 306

Removing an old or expired MDM profile from an iOS or macOS device

If a device has an old or expired MDM profile installed, the old or expired MDM profile may prevent the new MDM profile from being installed, which, in turn, may prevent the device from being registered. If a device has an old or expired MDM profile, you must remove it to enable device registration.

> When removing the MDM profile from an iOS device, Ivanti EPMM can no longer track the apps installed to the device. Ivanti EPMM stores the last known state of all installed apps (at the time of MDM profile removal) until retiring the device.

Procedure

1. Tap the **Settings** icon on the iOS device.

2. Tap **General**.

3. Scroll down to the **Profiles** section.

4. Tap **Profiles**.

5. Select the profile.

6. Tap the **Remove** button.

Procedure

1. On the macOS device, select the Apple icon.

2. Go to **System Preferences**.

3. Select **Profiles**.

4. Examine the list of device profiles for any MDM profiles that may be expired or irrelevant.

5. Select the expired profile.

6. Select the minus (-) button to remove the expired profile.

Disabling analytics data collection

Ivanti, Inc collects data to analyze the use of Ivanti EPMM 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.

The data is collected from:

- Ivanti Mobile@Work

- Apps@Work

Procedure

1. In Ivanti EPMM, go to **Settings > System Settings > General > Analytics**.

2. Select the **Disable data collection from Mobile@Work and Apps@Work** check box.

3. Select **Save**. A confirmation dialog opens.

4. Select **Yes** to confirm or **No** to cancel and allow analytics data collection.

General management of devices

This section provides information on the general communication with 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 Ivanti EPMM*.

Sending a message to devices

Procedure

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

2. Select the device(s) you want to message.

3. Select **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 Ivanti Mobile@Work client has an active connection to Ivanti EPMM.
   - 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.
   - To send a push notification, select the **Push Notification** check box and enter text into the **Message (Plain text)** field.

   > ℹ️   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. Select **Send Message**.

Related Topics

- Sending a company-branded email
- Setting wallpapers for devices
- App Updates for Android Enterprise

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 search for devices" below
- "Advanced searching " on page 57
- "Using the query builder" on page 77
- "Using a manually edited search expression" on page 78
- "Using both the query builder and manual editing" on page 78
- "Negative operators with advanced search" on page 80
- "Clearing an advanced search" on page 82
- "Searching for retired devices" on page 83
- "Searching for blocked devices" on page 83
- "Saving a search criterion to a label" on page 83

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

- Using the Dashboard
- Creating custom attributes
- Deleting retired devices

ⓘ   The features described in this section are supported on macOS devices.

Basic search for devices

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

- Label
- iOS MAC Address
- iOS Serial Number

- iOS UDID

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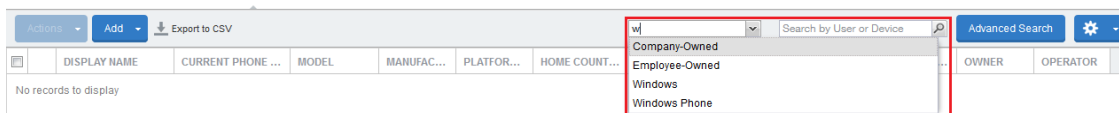
To search by the other criteria, select any label in the **Labels** list then use the following syntax in the **Search by User or Device** field:

- mac:<iOS MAC Address>

- sn:<iOS Serial Number>

- udid:<iOS UDID>

- 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 77 and "Using both the query builder and manual editing" on page 78.) 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 860.

> ℹ️ For information about searching in apps, see Running an advanced search of Installed Apps in the *Ivanti EPMM Apps@Work Guide*.

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	5G Network Slicing	True / false if devices' app traffic is routed through the network 5G slice.
	Admin Activated	True / false if device activated by admin.
	Android Automated Enrollment (This field is valid for Ivanti EPMM 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 Ivanti EPMM 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 Ivanti EPMM version 10.6.0.0 or later.
	Android Battery Charging Status	Docs/Tooltip: Battery health status as reported by Android OS. Field Name: Battery Charging Status property: status possible values: CHARGING, DISCHARGING, FULL, NOT_CHARGING, UNKNOWN
	Android Battery Health Status	Docs/Tooltip: Battery health status as reported by Android OS. Field Name: Android Battery Health Status property: health Possible values: COLD, DEAD, GOOD, OVERHEAT, OVER_VOLTAGE, UNKNOWN, UNSPECIFIED_VALUE

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Bulk Enrollment Profile Name	Can search for active or deleted profiles (and associated devices) using "Starts with" and "Equals."
	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.
	Battery Charge Cycles (OEM)	This field will only populate if the device is a Zebra device; otherwise blank. Docs: Number of charge cycles completed in total for supported device manufacturers such as Zebra devices. Field Name: Battery Charge Cycles property: battery_usage_numb possible values: Integer
	Battery Health Percentage (OEM)	This field will only populate if the device is a Zebra device; otherwise blank. Docs: Battery health in percentage for supported device manufacturers such as Zebra devices. Field Name: Battery Health Percentage property: health_percentag possible values: Integer
	Battery Manufacture Date (OEM)	This field will only populate if the device is a Zebra device; otherwise blank. Docs: Battery manufactured date for supported device manufacturers such as Zebra devices. Field Name: Battery Manufacture Date. property: mfd possible values: String yyyy-mm-dd
	Brand	Brand of the device.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	C2DM Token	C2DM token of the device if present, otherwise blank.
	Code Name	Code name of the Ivanti Mobile@Work client
	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.
	Inventory MAC address	The Android 7+ true physical MAC address for inventory purposes.
	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.
	Non GMS Device	True if Non GMS device is enabled, otherwise false.

TABLE **4.** D**EVICE FIELD DEFINITIONS** (C**ONT.**)

Device Type	Field	Description
	OS API Level	The Android OS API level. See https://developer.android.com/studio/releases/platforms for more details. 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 247.
	Platform Flags	Internal string representing the capabilities of the Ivanti 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

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		• Work Profile on Company Owned device • 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 Firmware E-FOTA has been decommissioned. As of August 2022, Samsung discontinued the Samsung E-FOTA service. For more information, see Activating the Samsung firmware E-FOTA license .
	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.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		• **True** - Indicates the PIN is to expire in 7 days or less. • **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 247.
	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 Ivanti Mobile@Workinstalled on the Wear OS device.
	Wear OS Device is Paired	True if one or more Wear OS device is paired to device via Bluetooth.
	Wi-Fi Security Level	Lists the security level of the Wi-Fi the device is currently connected to: • Personal Network Based Security - blocks personal Wi-Fi networks such as WEP, WPA/WPA2/WPA3, etc. • Enterprise EAP Network Based Security - blocks EAP protocol-based Wi-Fi networks. • Enterprise 192 Network Based Security - blocks EAP corporate-based Wi-Fi networks.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		The security level is also listed under "Required Wi-Fi Security Level" in the **Device Details page > Device tab**. For more information, see Lockdown policies in *Getting Started with Ivanti EPMM*.
	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 • **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.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	APNS Capable	Only true if there is an APNS token for the Ivanti Mobile@Work client, otherwise false.
	AppConnect Terms of Service	True/false for if the AppConnect Terms of Service was accepted.
	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 Last Reported Status	Lists the device's compliance status in Azure. Possible values are:

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		• In-progress • Compliant • Failed
	Azure Device Compliance Last Reported Time	The time Ivanti EPMM reported the device compliance status to Microsoft Intune. A blank field indicates one of the following: • Because that feature is disabled • Ivanti EPMM 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. Ivanti EPMM 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 withIvanti 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 Ivanti Mobile@Work client.
	Client Last Check-in	Date/Time of last check-in.
	Client Migration Status	Status of Ivanti Mobile@Work client migration from Ivanti EPMM to Cloud (true/false).
	Client Name	The name of the client, if registered with Ivanti Mobile@Work client.
	Client Version	The version of the client, if registered with Ivanti Mobile@Work client; otherwise, false.
	Cloud Migration Status	Status of device migration from Ivanti EPMM to Ivanti Neurons for MDM (true/false).
	Comment	A field that the administrator 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 administrator (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.
	Device Owner	Company or Personal.
	Device Space	Name of the space the device belongs to.
	Device UUID	Unique ID of the device generated from Ivanti EPMM.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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	ISI (International Mobile Subscriber Identity) number.
	IP Address	Current IP address of the device. ⓘ If you configured the GDPR, and you want to hide new fields that are added in new Ivanti EPMM releases (such as IP Address and eSIM ID), edit the GDPR profile.
	Language	Language of the device.
	Last Check-in	Last check-in time of the device.
	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.
	Ivanti Threat Defense Status	Mobile Threat Defense Status.
	Ivanti Tunnel App Installed	True / false if the Tunnel app was installed.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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.
	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.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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	The randomized 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	Ivanti Mobile@Work client APNS wakeup token. Applicable to iOS.
	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.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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.
	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 iCloud 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.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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.
	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.
	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.
	Organization Info	Organization for the device. Applicable to iOS.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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.
	Rapid Security Response	Rapid Security Response fields: • SupplementalBuildVersion - Build version associated with the currently installed rapid security response. If there's no installed rapid security response, this value is identical to the value reported through BuildVersion. Requires Device Information permission. • SupplementalOSVersionExtra - OS update rapid security response version letter if a rapid security response update is installed. Requires Device Information permission. To activate these fields, select the Security Responses & System Files option for Software Update **in Settings > General**. The fields are displayed in the Device Details tab. Administrators can use the iOS or macOS policies software updates to update devices to the latest Rapid Security Response updates. Use the **Update to the latest version** option. The **Update to a specific version** option is not supported in iOS for Rapid security response update formats from either the iOS Software update policy or the **Device** actions menu.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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.
	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.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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 *Ivanti EPMM 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 Ivanti EPMM.
	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.
	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.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Trusted Device	True if device is trusted.
	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.
	Last Admin Portal Login Time	Date of admin's last log in into Ivanti EPMM.
	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.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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).
	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.

Related topics

- "Using a manually edited search expression" below

- "Using both the query builder and manual editing" below

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

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).

   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 860.

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 860.

Clearing an advanced search

Use the following:

- 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 *Ivanti Standalone Sentry Guide for EPMM*.

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
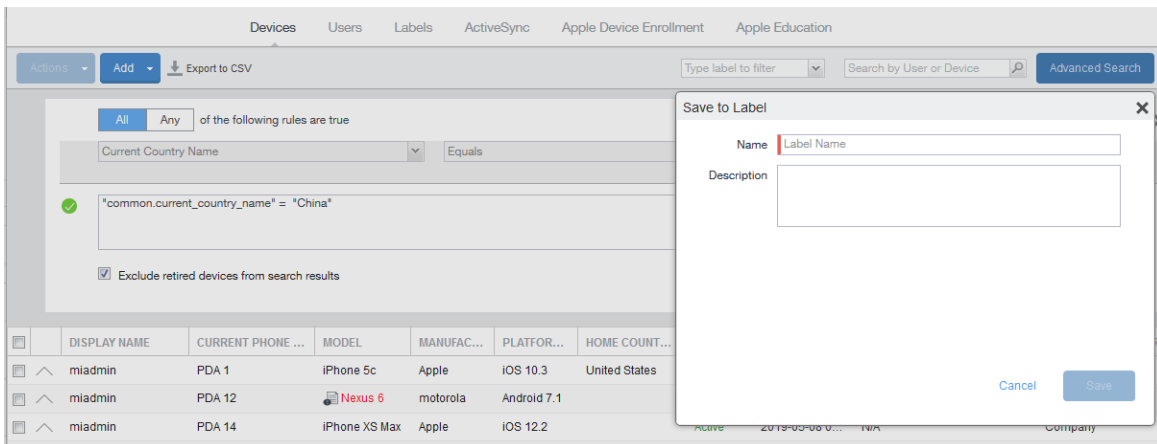
If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see "Best practices: label management" on page 860.

Securing Devices

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

- "Turning Bluetooth on and off on iOS and macOS devices" on page 130
- "Setting the time zone of a device" on page 132

Refer to the *Getting Started with Ivanti EPMM* 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	Restarts the Ivanti EPMM provisioning process for the device	Troubleshooting incomplete registration
Retire	Ends the registration (and Ivanti EPMM management) for a device	Moving devices out of inventory

Reprovisioning a device

This feature is not supported on macOS devices.

Select **Re-provision Device** to restart the Ivanti EPMM provisioning process without repeating the whole registration process. For example, you might want to do this if the initial attempt was interrupted, leaving the registration in the Pending state.

> This action applies only to devices in the Pending or Verified state. To reinstall the client in the Active state, you can either restore from a backup snapshot or retire the device and re-register it. To reinstall the client in the Wiped state, you must re-register the device.

Procedure

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

2. Select the check box for the device.

3. Select **Actions > Re-provision Device**.

4. The same registration settings are used.

Using self service security features

Users can perform lock, unlock, wipe and retire functions on devices on which they are registered from the new **My Devices** page on the device.

Procedure

1. Open the Ivanti Mobile@Work app on the device.
2. Click the menu icon in the upper left corner of the landing page.
3. Click **My Devices.**
4. You are prompted to login. Login is required when accessing the page for the first time.
5. Click **Continue**.
   A list of the devices on which the user is registered is displayed on the **My Devices** page.
6. Select the device. The **Device Details** page is displayed.
7. Choose to **Lock Device** or **Unlock Device**.
   When **Lock Device** or **Unlock Device** is selected the user is prompted to enter their password and confirm the action.
8. Click the menu icon on the upper right to select **Wipe** or **Retire** the device.
   When **Wipe** or **Retire** is selected the user is prompted to enter their password and confirm the action.

Retiring a device

Retiring a device archives the data for that device and removes the configurations and settings applied by Ivanti EPMM (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.) The device 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 *Ivanti Standalone Sentry Guide for EPMM*.

Retiring an iOS device removes AppConnect app data.

This feature is supported on macOS devices.

If you have duplicate devices, see "Managing Duplicate Devices" on page 98.

Procedure

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

   The **Retire** dialog opens.
4. Confirm the device information and enter an optional note. This information will be saved in the Audit Logs.
5. [Optional] Select **Force Retire**. Usually, when you issue a Retire command for a device, it is moved to a Retired state and is considered "Retire Pending." Sometimes the devices remain in the Retire Pending state. Ivanti EPMM offers a Force Retire check box to make sure the device is Retired. For more information, see"Automated Device Cleanup" on page 93.

   ℹ️ From the self-service portal, the retire action is **Force Retire**.

6.
7. Select **Retire**.
8. The device user receives notification of the action.

To see a list of retired devices, see "Searching for retired devices" in the *Getting Started with Ivanti EPMM*.

Deletion of retired devices

As device users leave your enterprise or change to new devices, more and more devices in the Ivanti EPMM database are retired. When you retire a device, Ivanti EPMM un-registers it and no longer manages or secures the device. All the configurations and settings that Ivanti EPMM had applied to the device are removed. The device can no longer access enterprise data or apps.

However, Ivanti EPMM retains retired devices in its database. Deleting these devices from the database improves Ivanti EPMM performance and frees up disk space. Although Ivanti EPMM also provides a web services API and a CLI command to delete retired devices, using the Admin Portal display is easier. It also provides an easy way to automatically delete retired devices every day.

With this Admin Portal display, you can:

- Easily navigate to the list of retired devices.

- Delete devices that have been retired for more than a specified number of days.

- Configure Ivanti EPMM to automatically delete retired devices daily, weekly, or monthly.

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

When Ivanti EPMM 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 Ivanti EPMM during the next LDAP sync.

This feature is supported on macOS devices.

Deleting retired devices by threshold

A common task, although not necessarily a daily task, is deleting retired devices. Deleting these devices from the database improves Ivanti EPMM performance and frees up disk space.

Prerequisites

Make sure you are assigned the required administrator role. To delete retired devices, you must be:

- Assigned to the global space

- Assigned the administrator role **Delete retired device**

Procedure

1. In the Admin Portal, go to **Settings > System Settings**.

2. Select **Users & Devices > Delete Retired Devices**.

3. Optional. Select the number of days after which retired devices should be deleted, or accept the default of 30 days.

4. Optional. Select the maximum retired devices to delete in each session, or accept the default of 100 devices.

5. Optional. Select **Delete Now** to delete the retired devices that meet the new criteria.

6. Select **Save** to save the configuration.

If **Delete Now** is disabled, only an administrator who is a "super administrator" can assign you to the global space and assign the **Delete retired device** administrator 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 the next page.

Deleting retired devices by schedule

You have the option to delete retired devices at daily, weekly, or monthly intervals.

Procedure

1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Delete Retired Devices**.

2. Optional. Select the number of days after which retired devices should be deleted, or accept the default of 30 days.

3. Optional. Select the maximum retired devices to delete in each session, or accept the default of 100 devices.

4. Select **Automatically Delete Retired Devices on a Schedule**. The Delete Schedule Configuration menu displays.

5. Select the **Weekly** or **Monthly** radio button, or accept the **Daily** default. Additional fields display.

   a. **Daily** - Select the hour you want the process to run.

   b. **Weekly** - Select the day and the hour you want the process to run.

   c. **Monthly** - Select the hour you want the process to run on the first day of the month.

6. Select **Save** to keep the configuration. The retired devices that match or exceed the threshold at the scheduled time will be deleted.

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. Select **Save**.

Retiring and deleting unused and retired devices

As device users leave your enterprise or change to new devices, you will need to retire devices. When you retire a device, Ivanti EPMM de-registers it and no longer manages or secures the device. All the configurations and settings that Ivanti EPMM had applied to the device are removed. The device can no longer access enterprise data or apps.

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

Within the 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 Ivanti EPMM to automatically retire or delete devices daily, weekly, or monthly.

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

When Ivanti EPMM 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 Ivanti EPMM during the next LDAP sync.

This feature is supported on macOS devices.

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**.

Automated Device Cleanup

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 Ivanti EPMM performance and frees up disk space.

After saving the settings, to view the logs for the automated device cleanup, use the Filters section on the left side of the Audit Logs page to narrow the search.

Prerequisites

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

- Assigned to the global space

- Assigned the administrator role **Delete retired device**

Retiring devices that have not been checked-in for N days

1. In the Admin Portal, go to **Settings > System Settings**.

2. Select **Users & Devices > Automated Device Cleanup**. The Automated Device Cleanup page opens.

3. Enter the settings as per below:

TABLE 7. RETIRING OF DEVICES

Field	Description
Retire Devices That have Been Not Checked-In More Than (days)	Days: 30 days is default, 365 days is maximum allowed.
Show not checked-in devices list	Selecting the link opens the Advanced searching page in Devices & Users and poplulates the search with the regular expression for the search. Select **Search**.
Maximum Devices to Retire in Each Session	Select 100 (default), 500, or 1000. The cleanup session may have an impact on the overall system performance. Configure the maximum limit for your environment.
Automatically Retire Devices on a Schedule	Selecting this check box expands the Retire Schedule Configuration section. • **Daily**: Select the run time from the **At:** drop-down menu. The default is midnight. • **Weekly**: Select the day and time for the clean up. Default value is Sunday at midnight. • **Monthly**: Select the time for a first-day-of-the-month schedule frequency. Default is first day of the month at midnight.

4. Select **Retire Now**

5. Select **Save** to save the configuration.

> ℹ️ If the **Retire 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 administrator 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 92.

Deleting devices that have been in selected states for N days

1. In the Admin Portal, go to **Settings > System Settings**.

2. Select **Users & Devices > Automated Device Cleanup**. The Automated Device Cleanup page opens.

3. Enter the settings as per below:

TABLE 8. DELETING OF DEVICES IN SELECTED STATES

Field	Description
Select the states to take actions on	Select all or just the desired options: • Retired • Retire Pending • Wiped • Wipe Pending
Delete devices that have been in selected states more than (days)	Days: 30 days is default, 365 days is maximum allowed.
Show devices in selected states	Selecting the link opens the Advanced searching page in Devices & Users and poplulates the search with the regular expression for the search. Select **Search**.
Maximum devices to delete (in selected states) in each session	Select 100 (default), 500, or 1000. The cleanup session may have an impact on the overall system performance. Configure the maximum limit for your environment.
Automatically delete devices in selected states on a schedule	Selecting this check box expands the Delete Schedule Configuration section. • **Daily**: Select the run time from the **At:** drop-down menu. The default is midnight. • **Weekly**: Select the day and time for the clean up. Default value is Sunday at midnight.

TABLE 8. DELETING OF DEVICES IN SELECTED STATES (CONT.)

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

4. Select **Delete Now**

5. Select **Save** to save the configuration.

> If the **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 administrator role to you. The procedure for the super administrator and definition of a super administrator are in .

Retire the Retire Pending devices that have not been checked-in N days

1. In the Admin Portal, go to **Settings > System Settings**.

2. Select **Users & Devices > Automated Device Cleanup**. The Automated Device Cleanup page opens.

3. Enter the settings as per below:

TABLE 9. RETIRE THE RETIRE PENDING DEVICES

Field	Description
Retire the Retire Pending Devices that have not been checked in for more than	• **Days:** 30 days is default, 365 days is maximum allowed. • **Hours:** 1 hour is default, 23 hours is maximum allowed.
Show retire pending devices list	Selecting the link opens the Advanced searching page in Devices & Users and poplulates the search with the regular expression for the search. Select **Search**.
Maximum Retire Pending devices to Retire in Each Session	Select 100 (default), 500, or 1000. The cleanup session may have an impact on the overall system performance. Configure the maximum limit for your environment.
Automatically Retire the Retire Pending Devices on a schedule	Selecting this check box expands the Retire the Retire Pending Devices Schedule Configuration section. • **Daily**: Select the run time from the **At:** drop-down menu. The default is midnight. • **Weekly**: Select the day and time for the clean up. Default value is Sunday at midnight. • **Monthly**: Select the time for a first-day-of-the-month schedule frequency. Default is first day of the month at midnight.

4. Select **Force Retire the Retire Pending Devices Now** OR **Force Retire All the Retire Pending Devices**.

5. Select **Save** to save the configuration.

> **i** If the **Force Retire the Retire Pending Devices Now** OR **Force Retire All the Retire Pending Devices** button is disabled, only an administrator who is a "super administrator" can assign you to the global space and assign the Delete retired device administrator 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 92.

Managing Duplicate Devices

This section is applicable to Android, iOS, macOS, and Windows 8 devices.

By selecting **Enable managing duplicate devices**, administrators can set duplicate active devices to the Retire or Wipe status or to the Unknown status. Administrators can also set a scan schedule for either Daily, Weekly or Monthly.

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

- Android Enterprise devices - When a new Android device is registered, Ivanti EPMM matches its device attributes (MAC, Serial Number, etc.) and its registration status (mode) to any existing entries. If the latest entry is found to duplicate the previous (old) entry, the old entry deleted and an error is entered into the logs.
- 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

Ivanti EPMM matches devices by device type. Ivanti EPMM uses various device information to determine whether a device is a duplicate or not. For information on finding devices by device type for Apple User Enrollment, see Apple documentation.

Procedure

1. In the Admin Portal, go to **Settings > System Settings**.

2. Expand **Users & Devices** and then select **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. Select **Save**.

TABLE 10. MANAGING DUPLICATE DEVICES SETTINGS

Item	Description
Scan Schedule	Select **Change** to make your settings. Once set, the current schedule will display under Scan Schedule.
Enable for following OS	Select the applicable option(s): • Android • iOS - For iOS duplicate supervised devices, the administrator will need to disable the MDM profile of the old device before using the Wipe command. • Windows
Frequency and Time	Enabled by default to run at 12AM in UTC time, daily. 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 Ivanti EPMM server. • **Weekly** - Select the day and time of the of the duplicate device. This is the time on the Ivanti EPMM 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 Ivanti EPMM server.
Device Action > **Retire or Wipe the old device - (default)**	ⓘ Wipe takes precedence on platform where both Retire and Wipe actions are available.

TABLE 10. MANAGING DUPLICATE DEVICES SETTINGS (CONT.)

Item	Description
	When a new Android device is registered, Ivanti EPMM matches its device attributes (MAC, Serial Number, etc.) and its registration status (mode) to any existing entries. If the latest entry is found to duplicate the previous (old) entry, the old entry deleted and an error is entered into the logs. Select an option: • **Retire old devices** - When selecting Retire, Ivanti EPMM is not actually retiring the device; instead, the device is marked as "Retired" in the EPMM database. All the entries with "Retired" status are then removed from the database through the Scheduler. **Note:** Android devices that do not support Retire will not have any action taken on them. • **Wipe old duplicate Android Devices** - for unsupervised devices. Once selected, device moves into "Wipe Pending" state. The administrator will need to go to **System Settings > Users & Devices > Automated Device Cleanup** and select **Wipe Pending**. • **Wipe duplicate old supervised Apple Devices** - Once selected, device moves into "Wipe Pending" state. The administrator will need to go to **System Settings > Users & Devices > Automated Device Cleanup** and select **Wipe Pending**.
Device Action > **Mark the old device as "Unknown"**	The old device is marked as Unknown. Duplicate entries caused by other types of registrations will be dealt with via compliance policy actions.

Related topics

"Automated Device Cleanup" on page 93

"Retiring a device" on page 87

Security-related features and tasks

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

TABLE 11. 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	Reverses the Lock function ⓘ The unlock feature is not supported on macOS devices. You can, however, unlock an macOS device using a different process described in "Unlocking a macOS device" on page 971.	Accessing the device when the passcode has been forgotten or reassigning the device to a different user ⓘ For security reasons, it is inadvisable to execute this command on lost or stolen devices.
Unlock AppConnect Container	This feature is not supported for macOS devices. This feature is not supported for iOS devices.	This feature is not supported for macOS devices. This feature is not supported for iOS 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	Attempts to cancel a wipe action for devices.	Reversing an inadvertent Wipe command. ⓘ Wipe cannot be reversed after it completes.
Block AppTunnels	This feature is not supported on macOS devices. Immediately blocks access to all AppTunnels for all AppConnect apps on a device.	Dealing with lost and stolen devices Immediately removing access to servers behind the firewall
Lost	Flags a device as lost	Dealing with lost and stolen devices

TABLE 11. SECURITY-RELATED FEATURES AND TASKS (CONT.)

Feature	Description	Use Case
Found	Flags a device as found	Dealing with lost and stolen devices
Locate	This feature is not supported on macOS devices. Reports the last known location for a device	Dealing with lost and stolen devices
Reset PIN	This feature is not supported on Android, iOS, or macOS devices.	

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.

This feature is supported on macOS devices.

Procedure

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

2. Select the check box for the device.

3. Select **Lock** from the **Actions** menu.

The **Lock** dialogue for an iOS device displays additional options for you to enter a contact number and a message. The **Lock Message** field allows you enter up to 500 characters. The contact number and the message appear on the screen for the device you locked. The device user can call the number displayed on the locked device.

Unlock

Unlocking the device passcode is supported as follows:

> **IMPORTANT:** The Unlock feature is not supported on macOS devices. You can, however, unlock an macOS device using a different process described in "Unlocking a macOS device" on page 971.

Procedure

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

2. Select the check box(es) for the device.

3. Click **Actions > Unlock Device**.

Encryption

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

This feature is supported on macOS devices.

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

ⓘ   This feature is only supported on macOS devices that have FileVault 2 (FDE) enabled.

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

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. Select **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 Ivanti EPMM 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. Select **Wipe**.

Related topics

- "Cancel Wipe" below

Cancel Wipe

Cancel Wipe attempts to cancel or reverse 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 Ivanti EPMM. Using **Cancel Wipe**, you may be able to stop or reverse the wipe action.

Cancel Wipe is supported for iOS devices with the status of **Wipe pending**, **Wiped.**

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

> This feature is only supported on macOS devices with FileVault 2 enabled.

Procedure

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 Ivanti EPMM is wiping their current, active device. De-select the check box to suppress notification when the Cancel Wipe command is used.

> **i** 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**.

   If an iOS device is wiped before the **Cancel Wipe** action can stop it, you can restore the device contents from the most recent device backup.

   If the device backup includes the MDM profile, the device is able to check in with Ivanti EPMM and receive updates

> **i** If you attempt to restore an iOS device without using **Cancel Wipe,** the device will be wiped again when it checks in with Ivanti EPMM.

Related topics

Selective Wipe

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

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

- Using Sentry and ActiveSync

Block AppTunnels

ⓘ   This feature is not supported on Mac OS devices.

You can manually block the AppTunnel feature (standard and Advanced) in AppConnect apps on a device. The authorized AppConnect apps remain authorized, but the apps will no longer be able to access the web sites configured to use the AppTunnel feature.

To manually block the AppTunnel feature in AppConnect apps on a device:

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

2. Select the check box for the device.

3. Select **Actions > Block App Tunnels** from the **Actions** menu to open the **Block AppTunnels** dialog.

4. Add a note and click **Block AppTunnels**.

Lost

When a user reports a lost device, you can set its status to **Lost**. Setting this status does not have a functional effect on the phone. It just flags the phone as lost for tracking purposes and to ensure that it appears in the Lost Phones screen.

This feature is supported on macOS devices.

Procedure

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

2. Select the check box for the device.

3. Select **Actions > Lost** from the **Actions** menu.

4. In the displayed dialog, confirm the user and device information and enter a note.

5. Click **Lost**.

   The entry for this device will appear with a status of "Lost." Use the Found action to undo this status. See "Found" on the next page

Found

If a user reports that a lost phone has been found, you can use the Found action to remove the Lost indicator from the entry for the phone. Setting this status does not have a functional effect on the phone.

This feature is supported on macOS devices.

Procedure

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

2. Select the check box for the device.

3. Select **Actions > Found** from the **Actions** menu.

4. In the displayed dialog, confirm the user and device information and enter a note.

5. Click Found to return the entry for this device to **Active** status.

Locate

> ℹ️ iOS devices use cell towers to locate the device. This feature is not supported on Mac OS devices.

Most registered phones can be located on a map using cell tower IDs. When locating a device via cell tower IDs, Ivanti Mobile@Work records tower data until the next time data is synchronized between Ivanti Mobile@Work and Ivanti EPMM. See "Sync policies" in *Getting Started with Ivanti EPMM* for information on changing the Sync Interval setting. Using the Force Device Check-in in the Admin Portal or in Ivanti Mobile@Work will result in immediate synchronization.

Required role

The **Privacy Control: Locate device** role is required to use this feature.

Procedure

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

2. Select the check box for the device.

3. Select **Actions > Actions > Locate**.

4. Select the phone icon on the map to display the date and time stamp of the last known location of the phone.
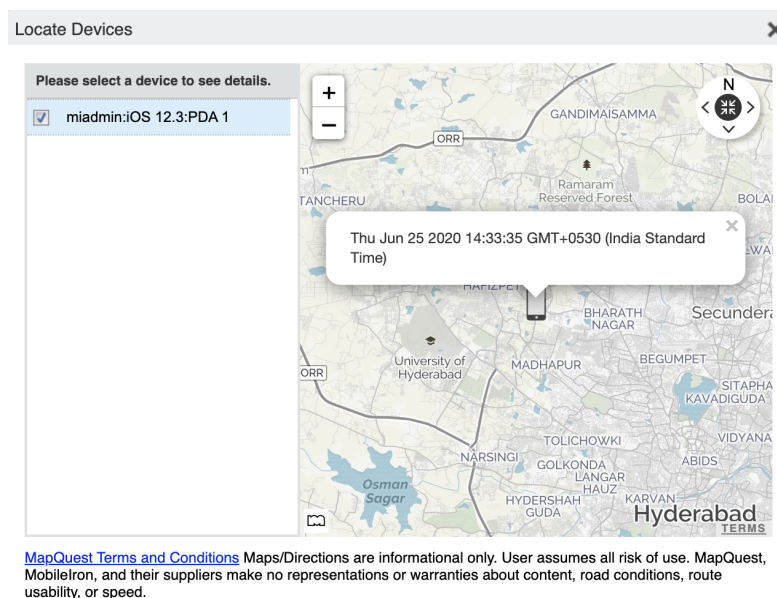
Reset device PIN

ℹ️ This feature is not supported on macOS iOS devices.

Force Device Check-In

You can use the **Force Device Check-in** feature to force the device to connect to the Ivanti EPMM. You might use this feature if Ivanti 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 Ivanti EPMM operations.

ℹ️ The **Force Device Check-in** feature on the Admin Portal does not sync the policies and settings related to AppConnect. The app check-in interval on the AppConnect global policy controls updates to those policies and settings. See the *AppConnect Guide for EPMM*. However, in the Ivanti Mobile@Work for iOS app *on the device*, the **Check for Updates** option *does* sync the policies and settings related to AppConnect.

This feature is supported on macOS devices.

Procedure

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

2. Select the check box for the device.

3. Select **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. Select **Force Device Check-in**.

Managing devices in Apple MDM lost mode

You can place a supervised device in MDM lost mode through Ivanti EPMM. This means you report the device as lost to Apple servers, allowing you to retrieve the last recorded location of the device, as well as disable lost mode if the device is found.

Ivanti EPMM allows you to carry out the following MDM lost mode tasks:

- "Enable MDM lost mode" on the next page
- "Disable MDM lost mode" on page 111
- "Request the MDM server to locate a device" on page 111

Note the following:

- MDM lost mode and all related features are supported on supervised devices **only** running iOS 9.3 or supported newer versions.
- Ivanti, Inc recommends using the MDM lost mode features on devices with working SIM cards and cellular connections. Before enabling MDM lost mode, note for future reference the iCloud login used on the device.
- Ivanti recommends not removing the device from iCloud. As long as the administrator / enterprise has ownership of the device, it will be difficult for the person who took or found the device to re-purpose it. If that lost Apple device does get switched on, the device will ping its location to another Apple device close to it. The device is found through Apple's Find My Device. For more information, see Apple documentation on Using Lost Mode in the iCloud and Mark your device as lost.
- MDM lost mode is different from Ivanti EPMM lost mode, as described in "Lost" on page 106.

Enable MDM lost mode

You can report a lost device to Apple servers by placing the device in MDM lost mode.

After you have placed a device in lost mode:

- If the device is retired, you cannot disable lost mode.

- If the device is wiped, you cannot locate or track the device.

To enable MDM lost mode:

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

2. Select the check box for the device.

3. Select **Actions > iOS Only > Lost Mode**.

4. In the Lost Mode window, enter the following:

Item	Description
Enable Lost Mode	Select to place the iOS device in MDM lost mode.
Message to display on lock screen	Optionally enter a message to be displayed on the locked screen of the lost device.
Contact number to display on lock screen:	Optionally enter a contact number to be displayed on the locked screen of the lost device. If someone finds the device, they can call the number to report it.
Footnote (Message to display in place of "Slide to Unlock"):	Optionally enter the text you would like to appear at the bottom of the locked screen. .
Play Lost Mode Sound	Select this option to play a sound on a device when the device is in lost mode. The sound plays until you disable lost mode or a user disables the sound at the device. This option is available only for supervised devices running iOS 10.3 or supported newer versions.

5. Select **Send Request**.

The lost mode message, contact number, and footnote are shown on the lost device.

Disable MDM lost mode

If a device in MDM lost mode is retrieved, or MDM lost mode was enabled in error, you can disable MDM lost mode.

> ℹ️   If the lost device is retired from Ivanti EPMM, disabling MDM lost mode will not work.

To disable MDM lost mode:

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

2. Select the check box for the device.

3. Select **Actions > iOS Only > Lost Mode**.

Request the MDM server to locate a device

You can determine the last recorded location of a given supervised device using the Request Device Location feature. The device location request is sent to Apple, but Ivanti EPMM shows the last recorded location and time stamp before receiving a response from Apple. It may take some time for Apple servers to respond to Ivanti EPMM. To view the latest device location response from Apple, execute the device location request again.

> ℹ️   If the device is wiped, you will not be able to locate the device.

To request the location of a device:

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

2. Select the check box for the device.

3. Select **Actions > iOS Only > Request Device Location**.

4. In the window that opens, select **Map It** to view the last recorded device location.

Setting up background check-ins with APNs

Background check-ins allow Ivanti EPMM to communicate with devices in the background through Ivanti Mobile@Work . To do this, Ivanti EPMM wakes up Ivanti Mobile@Work by sending a silent Apple Push Notification service (APNs) message to Ivanti Mobile@Work by way of the APNs server. Ivanti EPMM uses background check-ins to provide accurate jailbreak detection or policy updates without relying on device location changes, for example. As opposed to relying on location changes, using APNs for background check-ins uses less device battery power while using more predictable update intervals.

The sync interval defined in the sync policy applied to a device determines how often Ivanti EPMM sends a check-in notification for iOS devices.

Procedure

1. Go to **Policies & Configs > Policies**.

2. Select the sync policy name.

3. Select **Edit**. The Modify Sync Policy dialog box opens.

4. Set the **Sync Interval** to the preferred number of minutes. The default interval is 240 minutes. If you want to make more frequent checks for certain policy changes or jailbreak indicators, decrease the value. More frequent checks will have a greater effect on device battery life.

5. Select **Save**.

Managed iBooks

This feature is not supported on macOS devices.

The iBooks feature allows you to distribute iBooks, Kindle books (ePub), and PDF files to iOS devices managed by Ivanti EPMM. You can also edit and delete managed books, and search for particular managed books.

Benefits

The iBooks feature allows administrators to distribute useful material to device users, such as end-user guides for apps or marketing collateral. Administrators can also edit and delete managed books.

Impacts

Distributing iBooks to iOS devices involves adding the book file to Ivanti EPMM and applying the relevant labels.

Ivanti EPMM distributes managed books to the iOS devices with the relevant labels applied. Managed iBooks are displayed in the iBooks app on iOS devices. The managed device profile includes a list of managed iBooks associated with that profile.

Note the following:

- Removing a device from management also removes the managed books from that device.
- After a book has been opened on a device, the book title reflects the title in the book's metadata, regardless of the title entered for the book in Ivanti EPMM. To avoid confusion, be sure to use the title shown in the metadata of a given book when entering the title in the Admin Portal. This behavior is due to Apple's implementation of iBooks.

Distributing managed books to iOS devices

Distributing managed books to iOS devices is a two step process: add the book to Ivanti EPMM, then apply the relevant labels such that Ivanti EPMM sends the book to the relevant devices. You can add ePub, iBook, and PDF files to the list of managed books.

Procedure

1. In the Admin Portal, go to **Apps > iBooks**.

2. In the **Add Content** window, enter the URL of the iBook, PDF, or ePub file you want to distribute to iOS devices. Alternatively, select **Browse** to select the file from the file system.

3. Use the following table as a guide for filling in the form.

Fields	Description
Document Type	• Select **URL** to obtain the file from the web. Or: • Select **File** to browse for and upload a file.
File/URL	Required. The file extension must match the selected file format. For example, if you are uploading an ePub file, you must select **ePub** as the file format. • If you selected **File** for the document type, select Browse to select the file you want to upload to Ivanti EPMM. • If you selected **URL** for the document type, enter the URL of the file you want to upload to Ivanti EPMM.
Title	Enter the title of the iBook, ePub, or PDF. Required.
Author	Enter the name of the author in the space provided. Optional.
File Format	Select **ePub**, **iBooks**, or **PDF** for the file format. Required.

Fields	Description
	The file extension is automatically selected to match the format of the file. For example, if you are uploading an ePub file, then **ePub** is automatically selected as the file format.

4. Select **Save**.

   The book is added to the managed iBooks on Ivanti EPMM.

5. In the iBooks window, select the managed book you just created.

6. Go to **Actions > Apply to Label**.

7. Select the relevant labels.

8. Select **Apply**.

   Ivanti EPMM distributes the books to the relevant devices during the next sync, as defined by your sync policy.

9. To confirm receipt of the managed book, see "Confirming receipt of managed books" below.

Confirming receipt of managed books

You can confirm that Ivanti EPMM has sent a given book to the relevant iOS devices, as described in "Distributing managed books to iOS devices" on page 113.

To confirm distribution of managed books:

1. In the Admin Portal, go to **Apps > iBooks**.

2. Locate the managed book whose distribution you want to confirm.

3. Examine the **Devices Installed** column for the book.

   A number greater than zero indicates that the book has been distributed, assuming the label you applied includes one or more devices.

4. Select the number in the **Devices Installed** column to see a list of devices to which the book has been sent.

Editing managed books

ℹ️ If you edit the name of a managed book, device users may still see the old book name.

Procedure

1. In the Admin Portal, go to **Apps > iBooks**.

2. Select the managed book you want to edit.

3. Go to **Actions > Edit**.

4. Edit as desired.

   ℹ️ If you clear the existing file and browse for a different file, make sure the new file is of the same type as the old file. For example, you can only replace an ePub file with another ePub file. You cannot change the file type of the managed book.

5. Select **Save**.

   The edited book is updated on devices at the next sync.
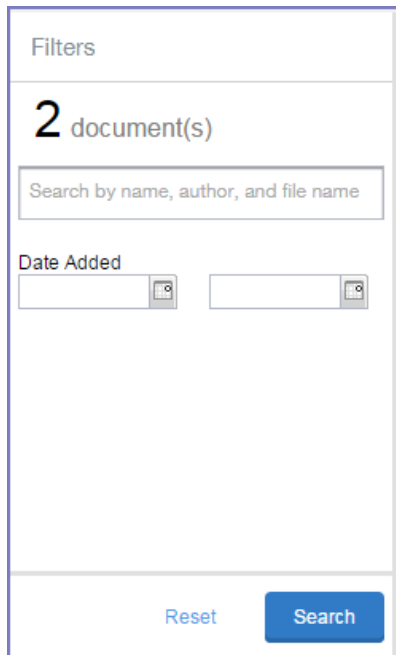
Searching for managed books

You can search for a particular book in the list of managed books.

Procedure

1. In the Admin Portal, go to **Apps > iBooks**.

2. In the **Filters** pane on the left, enter the search criteria you want to use.

Filters

2 document(s)

Search by name, author, and file name

Date Added

Reset   Search

3. Use the following criteria for your search:

- book title

- author

- file name

- date added to Ivanti EPMM (or date range)

4. Select **Search**.

5. After examining the search results, select **Reset** to remove the search filters and show all managed books.

Removing managed books from a subset of devices

You can remove managed books from particular devices while still keeping the books in the catalog of managed books on Ivanti EPMM. This is done by removing the books from the label or labels to which they are applied.

> ℹ️ If you remove a label from a device, all managed books associated with that label are removed from the device.

Procedure

1. In the Admin Portal, go to **Apps > iBooks**.

2. Select the managed book you want to remove from users' devices.

3. Go to **Actions > Remove from label**.

4. Select the labels you want to remove from the book.

5. Select **Remove**.

Deleting managed books

You can delete a managed book from the catalog of managed books on Ivanti EPMM. Doing so deletes the managed book from the relevant devices.

> ℹ️ Device users cannot effectively delete managed books from their devices. If they do, Ivanti EPMM simply sends the deleted books back to the devices.

Procedure

1. In the Admin Portal, go to **Apps > iBooks**.

2. Select the managed book you want to delete from the catalog of managed books on Ivanti EPMM.

3. Go to **Actions > Delete**.

4. When a prompt displays asking if you want to delete the book, select **Yes**.

   The book is deleted from both the catalog of managed books and relevant user devices.

Viewing the list of managed books on the device

For troubleshooting purposes, administrators and technical support can direct users to view the complete list of managed books on the device. This list is separate from the book list in iBooks, as it includes only those managed books associated with the Ivanti EPMM device management profile.

Procedure

1. On the device, go to **Settings > General > Device Management**.

2. Tap the **Ivanti** device management profile.

3. Tap **Books** to view the list of managed book titles.
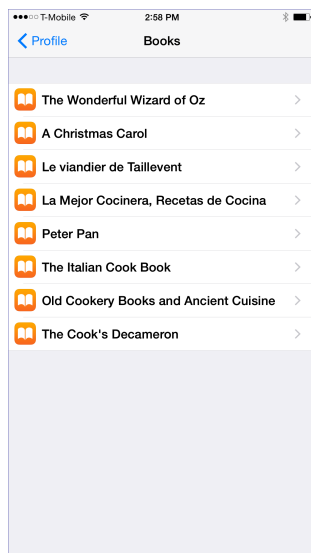
4. Tap a managed book to view the restrictions applied to it.
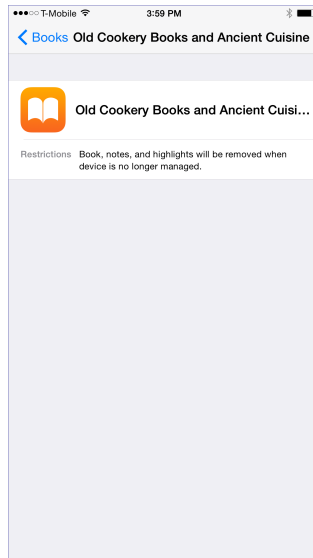
Personal hotspot on/off switch

This feature is not supported on macOS devices.

Ivanti EPMM enables you to turn personal hotspots on or off for iOS devices. While you can turn the personal hotspot on or off, device users can turn their personal hotspots back on or off again.

Overage fees for personal hotspots can be expensive for your organization, particularly when employees use their devices while traveling abroad. Turning off personal hotspots on iOS devices can help your organization reduce the cost of your employees' mobile data plans.

Turning the personal hotspot on or off for iOS devices involves simply changing the hotspot setting in the list of devices under Devices & Users > Devices. This sends an MDM command to devices requesting the personal hotspot to be switched on or off. The command is queued from Ivanti EPMM, and executes on the device at the discretion of iOS. Device users can see if their personal hotspot has been switched on or off by going to **Settings > Personal Hotspot** on their devices.

Before you begin

Make sure you have selected the **View dashboard, device page, device details** line item under the device management role.

Procedure

1. In Ivanti EPMM, go to **Admin > Admins**.

2. Select the administrator who will be managing personal hotspot settings.

3. Go to **Actions > Edit roles**.

4. Select **View dashboard, device page, device details**.
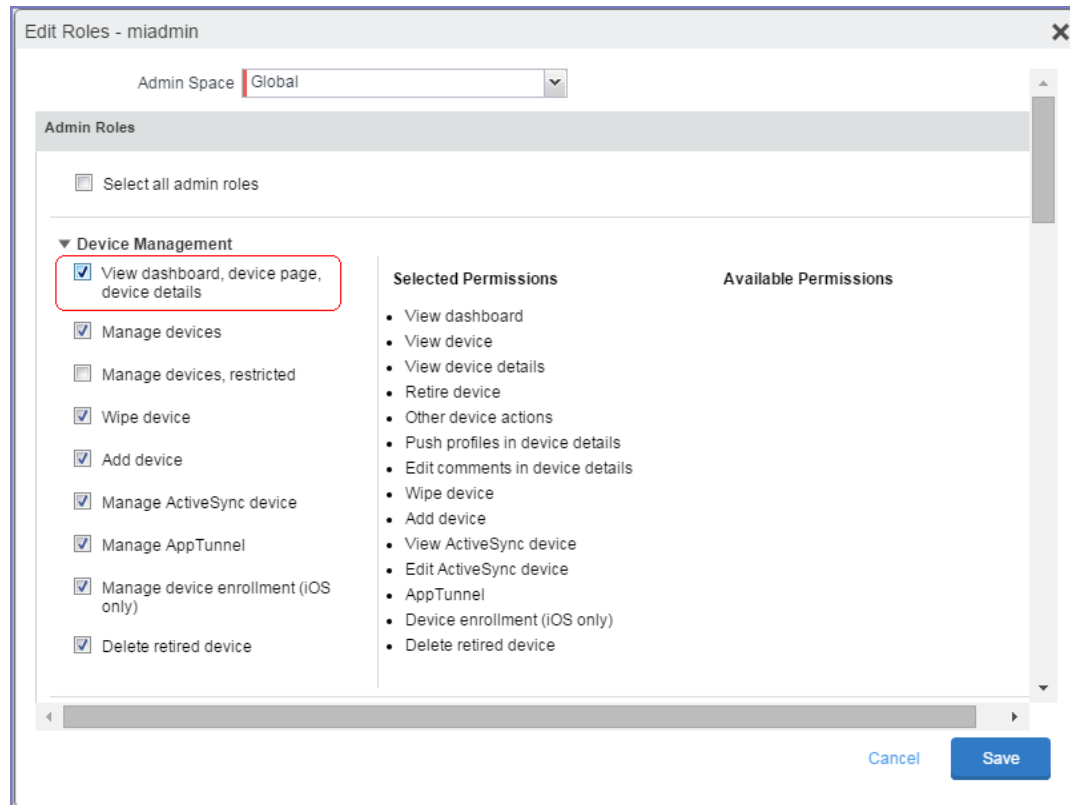
5. Click **Save**.

Turning the personal hotspot on or off on iOS devices

If a device user enables their personal hotspot at the same time that the Ivanti EPMM administrator is disabling their personal hotspot through Ivanti EPMM, then the device user's setting takes precedence over the command sent by the administrator. This is standard iOS behavior.

Procedure

1. In Ivanti EPMM, go to **Devices & Users > Devices**.

2. Select the device or devices whose personal hotspot settings you want to turn on or off.

3. Go to **Actions > iOS Only > Update Personal Hotspot Setting**.

4. Use the following table as a guide for filling in the form:

Item	Description
Enable Personal Hotspot	Select to turn on the personal hotspot feature on the device or devices.
Disable Personal Hotspot	Select to turn off the personal hotspot feature on the device or devices.
Note	Optionally, add a note regarding this setting.

5. Click **Update** to save your changes.

6. On the Devices page, select the device or devices for which you switched on or off the personal hotspot.

7. To verify that the command worked, go to **Actions > Force Device Check-In**.

8. Check if the personal hotspot has been turned on or off for a given device, as described in "Checking if the personal hotspot is turned on or off for a given device" below.

> ℹ️ While you can turn the personal hotspot on or off for a given device or set of devices, device users can still change the setting for the personal hotspot even after you send the command. If you have turned off a device's personal hotspot, it is possible for the device user to turn it back on again immediately after.

Checking if the personal hotspot is turned on or off for a given device

You can check whether the personal hotspot was turned on or off for a given device as of the latest device check-in.

Procedure

1. In Ivanti EPMM, go to **Devices & Users > Devices**.

2. Click the caret symbol (**^**) next to the device whose settings you want to check.

3. The **Device Details** tab is displayed.

4. Scroll down and find **Personal Hotspot Enabled**.

- If the value of **Personal Hotspot Enabled** is false, the hotspot was turned off as of the most recent device check-in.

- If the value of **Personal Hotspot Enabled** is true, the personal hotspot was turned on as of the most recent device check-in.

Reinstalling system apps on iOS devices

You can reinstall system apps on iOS devices when they have been deleted by the user. This action is useful because most system apps are not available in the Apple App Store for users to reinstall themselves.

This feature is supported on iOS 11.3.

When you select a system app to reinstall:

- If the system app is not on the device, the latest version is installed.

- If an older version of the app is on the device, the app is upgraded.

- If the same version of the app is on the device, the app is not reinstalled.

Procedure

1. In Ivanti EPMM, go to **Devices & Users > Devices**.

2. Select the device or devices for which you want to reinstall deleted system apps.

3. Go to **Actions > iOS Only > Reinstall iOS System Apps**.

   The **Reinstall iOS System Apps** window is displayed.

4. Select the system apps that you want to reinstall.

5. If you want to use different images for the home and locked screens:

6. Select **Reinstall Apps**.

   The apps will be reinstalled when each device next checks in.

Manually setting the wallpaper for iOS devices

You can set the wallpaper of the home and locked screens of supervised iOS devices to images of your choice. You can perform this manual action at any time on devices that are already registered. You can choose the same image or different images for the home screen and locked screen.

This feature is useful in a kiosk setting, or shared device environment in a retail setting.

Note the following:

- To set the wallpaper automatically **when a device registers**, use the wallpaper policy.

- Before choosing an image file, browse the Apple website for the latest recommended image resolution by device type and screen size.

- The file must be either a PNG or JPG file.

Procedure

1. In Ivanti EPMM, go to **Devices & Users > Devices**.

2. Select the device or devices whose wallpaper you wish to set.

3. Go to **Actions > iOS Only > Set Wallpaper**.

   The Set Wallpaper window is displayed.

4. If you want to use the same image for both home and locked screens:

   - Select **Use same image for Home Screen and Lock Screen**.

   - Select **Choose File** to select an image file.

5. If you want to use different images for the home and locked screens:

   - Under the Home Screen section, select **Choose File** to select an image file.

   - Under the Lock Screen section, select **Choose File** to select an image file.

6. Select **Send Request**.

   Ivanti EPMM sends the wallpaper request to the selected devices.

Related topics

"Wallpaper policies" on page 300

Adding fonts to iOS devices

You can push a font to managed iOS devices by defining a configuration and applying it to the relevant labels. The font configuration is sent to devices upon the next sync with Ivanti EPMM.

After the new font arrives, device users will be able to select the font if they wish. You can create additional font configurations to push more fonts to devices. Each configuration includes one font.

Note the following:

- Font configurations are not encrypted.

- Large font files can have unpredictable performance impact on Ivanti EPMM. The performance impact is due to Ivanti EPMM requiring multiple device check-ins to apply the font to all devices. The performance impact depends on the size of the font file and on the number of devices impacted. To avoid performance impact, manage your labels to limit the number of devices impacted by a configuration with a large font file.

Procedure

1. In the Admin Portal, select **Policies & Configs** > **Configurations**.

2. Select **Add New > Apple > iOS / tvOS** > **Fonts**. The New Fonts Configuration dialog box opens.

3. Enter your specifications using the table below as guidance.

Item	Description
Name	Enter a name for the font configuration.
Description	Enter a description for the font configuration.
Upload Fonts	Click **Browse** and select your .ttf or .otf font file. The maximum file size for a font file is 40MB.

4. Click **Save**.

5. Select the font configuration.

6. Click **Actions > Apply to Label**, and select the labels to which you want to apply the font.

7. Click **Save**.

Restarting or shutting down supervised iOS devices

iOS onlyYou can use Ivanti EPMM to restart or shut down supervised iOS devices running iOS 10.3 or supported newer versions. If you attempt to restart or shutdown a device running prior iOS versions, Ivanti EPMM displays an error message.

Procedure

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

2. Select the devices which you want to restart or shutdown.

3. Select **Actions > iOS Only > Restart/Shutdown Devices**.

   A confirmation window displays. By default, the device passcode is cleared on restart or shutdown.

4. (Optional) Clear the device passcode on restart or shutdown.

   If the passcode is not cleared, the device will require a passcode and will not be connected to Wi-Fi after it is restarted.

5. Select **Send Request**.

   Ivanti EPMM sends the iOS restart or shutdown command to devices.

6. Select **OK**.

Reporting on managed devices

Ivanti EPMM 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 *Ivanti EPMM V2 API Guide*.

This feature is supported on macOS devices.

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. Select **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. Select **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 12. EXPORT TO CSV FIELD OPTIONS

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, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, $REG_LINK
Body (PDAs)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
Reminder Subject (Phones)	ENT_NAME, $USER$, $PHONE$
Reminder Subject (PDAs)	ENT_NAME, $USER$, $PHONE$
Reminder Body (Phones)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
Reminder Body (PDAs)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $INAPP_REG_STEPS$, REG_LINK
$INAPP_REG_STEPS$	
Server	$SERVER_URL$
Username	$USER_ID$
Password	$PASSCODE$, $PASSCODE_TTL$
Post Registration Email	
Subject (Phones)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$

TABLE 12. EXPORT TO CSV FIELD OPTIONS (CONT.)

Type	Supported Variables
Subject (PDAs)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$
Body (Phones)	$BRAND_COMPANY_NAME$, $PHONE$
Body (PDAs)	$BRAND_COMPANY_NAME$, $PHONE$
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)
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 12. EXPORT TO CSV FIELD OPTIONS (CONT.)

Type	Supported Variables
iOS Attributes	User ID, Device UUID, Activation Lock Bypass Code, Activation Lock is Enabled, APNS Token, Apple Device Mac Address, Apple Device Version, Bluetooth MAC, Build Version, Carrier Settings Version, Current Mobile Country Code, Current Mobile Network Code, Data Protection, Data Roaming Enabled, DEP Device, DEP Enrolled, Device Locator Service Is Enabled, Device Name, Do Not Disturb Is In Effect, Force Encrypted Backup, Full Disk Encryption Enabled, Full Disk Encryption Has Institutional Recovery Key, Full Disk Encryption Has Personal Recovery Key, Hardware Encryption Caps, iCloud Backup Is Enabled, iOS Background Status, iPhone ICCID, iPhone Mac Address, iPhone Product, iPhone UDID, iPhone User ID, iPhone User Long Name, iPhone User Short Name, iPhone Version, IT Policy Result, iTunes Store Account Hash, iTunes Store Account Is Active, Languages, Last Acknowledged Lock PIN, Last Acknowledged Wipe PIN, Last iCloud Backup Date, Locales, MacOS User ID, MacOS User Long Name, MacOS User Short Name, Maximum Resident Users, MDM Lost Mode Enabled, MDM Service Enrolled, Modem Firmware Version, Network Tethered, Organization Info, OS Update Status, Passcode Compliant, Passcode Compliant with Profiles, Passcode Present, Personal Hotspot Enabled, Product Code, Product Name, Security Reason Code, Subscriber Carrier Network, Subscriber MCC, Subscriber MNC, Supervised, UDID, Voice Roaming Enabled, VPN IP Address, Wakeup Status

Turning Bluetooth on and off on iOS and macOS devices

Ivanti EPMM enables you to turn Bluetooth on or off for iOS and macOS devices. As this is a discrete action, rather than a restriction, administrators and users can turn Bluetooth back on or off after taking this action.

Turning Bluetooth on or off for iOS and macOS devices involves simply changing the Bluetooth setting in the list of devices under Devices & Users > Devices. This sends a command to devices, requesting Bluetooth to be switched on or off. The command is queued from Ivanti EPMM, and executes on the device at the discretion of iOS or macOS. Device users can see if their Bluetooth has been switched on or off by going to **Settings > Bluetooth** on their devices.

Before you begin

Make sure you have selected the **View dashboard, device page, device details** line item under the device management role.

---

1. In Ivanti EPMM, go to **Admin > Admins**.

2. Select the administrator who will be managing personal hotspot settings.

3. Go to **Actions > Edit roles**.

4. Select **View dashboard, device page, device details**.

5. Click **Save**.

Procedure

1. In Ivanti EPMM, go to **Devices & Users > Devices**.

2. Select the device or devices whose Bluetooth you want to turn on or off.

3. Select **Actions > iOS and macOS > Update Bluetooth Setting**.

4. Use the following table as a guide for filling in the form:

Item	Description
Enable Bluetooth	Select to turn on Bluetooth for the device or devices.
Disable Bluetooth	Select to turn off Bluetooth for the device or devices.
Note	Optionally, add a note regarding this setting.

5. Click **Update** to save your changes.

6. On the Devices page, select the device or devices for which you switched Bluetooth on or off.

7. To issue the command immediately, select **Actions > Force Device Check-In**.

> While you can turn Bluetooth on or off for a given device or set of devices, device users can still change the Bluetooth setting on their device even after you send the command. If you have turned off a device's Bluetooth, it is possible for the device user to turn it back on again immediately after.

Setting the time zone of a device

For setting time zones in Android devices, see Provisioning an Android Enterprise 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 Ivanti EPMM 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 57.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select one or more devices.
3. Select **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. Select **Set Time Zone**.

Distributing MDM Profiles with Apple Configurator

This section addresses the distribution of iOS MDM profiles using Apple Configurator and bulk registration of devices based on serial number.

- "MDM profile distribution with Apple Configurator" below
- "Automatically matching Apple devices with serial numbers" on the next page
- "Exporting an MDM profile from Ivanti EPMM 7.0.0.0 - 9.0.0.0" on page 136
- "Using Apple Configurator to register an Apple device with Ivanti EPMM" on page 137

MDM profile distribution with Apple Configurator

Ivanti EPMM supports the distribution of iOS MDM profiles by means of Apple Configurator. In addition, you can use bulk registration in the Admin Portal to automatically match users to devices based on serial number.

> Administrators who are experimenting or troubleshooting individual devices can also use the iPhone Configuration Utility to deploy a registration profile to a device.

Note the following:

- **Do not assign user-specific configurations to the iOS label.** Devices registered through the Configurator are initially registered as anonymous users, so pushing user-specific configurations (such as Exchange configurations) introduces unnecessary processing that must be repeated after Ivanti EPMM matches the device to the user.
- **If you are using Apple Configurator to register devices that display the Setup Assistant, then enable supervision of the devices in Apple Configurator.** The Setup Assistant is the wizard-like interface you see when starting the device for the first time. The Setup Assistant prevents display of the registration dialogs, causing deployment of configuration profiles to fail, unless supervision is enabled.

- **Consider installing the WiFi profile in a separate operation prior to installing the MDM profile.** This approach prevents the MDM profile installation from failing if the device does not acquire an IP address (required for Ivanti EPMM connectivity) in a timely manner.

Automatically matching Apple devices with serial numbers

You can automatically match Apple devices with serial numbers by completing the following tasks:

- "Acquiring serial numbers" below

- "Bulk-registering devices" below

Acquiring serial numbers

This step is only necessary if you want to automatically associate devices with their serial numbers in Ivanti EPMM.

To automatically associate users to Configurator-registered devices, you must bulk-register the devices on Ivanti EPMM and specify the device serial numbers in the registration spreadsheet.

Check the following sources for serial numbers:

- The back of the device

- In iOS (**Settings** > **General** > **About**)

- In the retail and bulk device packaging (in both readable and barcode form)

For large roll-outs of devices, we recommend using a barcode scanner and the iPhone Configuration Utility to quickly import serial numbers for tethered devices. This is particularly useful as the serial number can by copied from IPCU and pasted into the spreadsheet. This practice is also useful if you intend to recycle and re-register devices.

Bulk-registering devices

This step is only necessary if you want to automatically associate devices with their serial numbers in Ivanti EPMM.

Before you begin

Before you bulk-register devices with Ivanti EPMM, make sure you have collected the serial number for each device, as described in "Acquiring serial numbers" above.

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

Procedure

1. In the Admin Portal, select **Devices & Users > Devices > Add > Multiple Devices**.

2. Click **Sample CSV File**.

3. Save the sample file to your local drive.

4. Add an entry for each device, including the serial number.

   For more information on completing the bulk registration CSV file, see the "Bulk device registration" section in the "Registering Devices" chapter of *Getting Started with Ivanti EPMM*.

5. In the Adding Multiple Devices dialog, click **Browse** to select the edited CSV file.

6. Click **Import File**.

Next steps

Proceed to "Exporting an MDM profile from Ivanti EPMM 7.0.0.0 - 9.0.0.0" below or "Using Apple Configurator to register an Apple device with Ivanti EPMM" on the next page.

Exporting an MDM profile from Ivanti EPMM 7.0.0.0 - 9.0.0.0

Versions of Ivanti EPMM prior to 9.1.0.0 require exporting an iOS MDM profile prior to importing the profile into Apple Configurator, so that the MDM profile may be applied to devices using Apple Configurator.

Procedure

1. In the Admin Portal, select **Policies & Configs > Configurations**.

2. Select the **System - iOS MDM** setting, and select **Export MDM Profile**.

3. Save the file to your local drive.

   The file will have a .mobileconfig extension.

4. Tether the device.

5. Prepare your devices and import the MDM profile using Apple Configurator, as described in "Preparing devices" on the next page.

6. Follow the steps in "Creating and applying a blueprint" on page 139.

7. For unsupervised devices, respond to the profile installation prompts displayed on the device.

   Prompts do not display on supervised devices.

8. Confirm that the registration has been completed on Ivanti EPMM. The devices should be visible in the Admin Portal after they check in.

   If you did not bulk-register the devices, they will be displayed in the Admin Portal with the "<Anonymous>" user account. When a device user installs and signs in to Ivanti Mobile@Work , Ivanti EPMM switches the device to that user's account.

Using Apple Configurator to register an Apple device with Ivanti EPMM

> ℹ️ This procedure is incompatible with Apple School Manager iOS devices, and can only be done with on-premise installations of Ivanti EPMM.

Apple Configurator allows you to provision devices using mobile device management (MDM) without having to download and manage configuration profiles. This is supported in Ivanti EPMM 9.1.0.0 through the latest release.

Provisioning one or more devices involves the following main steps:

1. "Deleting all content and settings from an iOS device" below
2. "Creating a Wi-Fi profile" on the next page
3. "Preparing devices" on the next page
4. "Creating and applying a blueprint" on page 139

Deleting all content and settings from an iOS device

You may wish to delete all content from the device before you begin. Otherwise, the device will download a new version of iOS from Apple servers, a process that may be very time consuming.

Procedure

To remove all content from the device, select **Settings > General > Reset > Erase All Content and Settings** on the iOS device.

Creating a Wi-Fi profile

Ivanti, Inc recommends creating a Wi-Fi profile so as to configure Wi-Fi for the device immediately. This allows the device to more quickly access Ivanti EPMM and receive the configurations for device enrollment.

Before you begin

Before creating a Wi-Fi profile, you must have completed "Deleting all content and settings from an iOS device" on the previous page.

Procedure

1. Create a Wi-Fi profile.

2. Define Wi-Fi settings.

Preparing devices

Preparing devices is the first step in any iOS device deployment for Apple Business Manager or Apple School Manager. You need to prepare devices before you distribute them to users. To accomplish this task, you use the Prepare Assistant in Apple Configurator.

Procedure

- Prepare your devices for manual enrollment.

- For the host name or URL of the MDM server, either accept the default path populated by Apple Configurator:

  ```
  https://www.example.com/devicemanagement/mdm/dep_mdm_enroll
  ```

  Or enter the full path with the following syntax:

  ```
  https://www.example.com/mifs/c/i/reg/depenroll.mobileconfig
  ```

> Apple Configurator may show a message such as the following: "Unable to verify the server's enrollment URL." If so, disregard this message.

Creating and applying a blueprint

The blueprint is an Apple Configurator feature that allows you to create a sort of template for the device, including the URL of the MDM server (Ivanti EPMM) and the Wi-Fi profile you created in "Creating a Wi-Fi profile" on the previous page. The blueprint allows you to point to a set of configurations during setup, rather than having to specify each configuration repeatedly.

Before you begin

Before creating a blueprint, you must have completed "Creating a Wi-Fi profile" on the previous page.

Procedure

1. Create a blueprint.

2. In the blueprint, specify whether you want to include an MDM profile you exported from Ivanti EPMM, as described in "Exporting an MDM profile from Ivanti EPMM 7.0.0.0 - 9.0.0.0" on page 136. This step is only necessary when using versions of Ivanti EPMM earlier than 9.1.0.0.

3. Select the Wi-Fi profile you created in "Creating a Wi-Fi profile" on the previous page.

4. Tether the device to the computer:

   a. Use a USB cable to connect the iOS device to the computer you are using to create the blueprint in Apple Configurator 2.

   b. Select the tethered device.

   c. Select **Actions > Apply >** *Name of your MDM Server*.

   d. Repeat with any additional devices.

5. Apply the blueprint, as described in the link in step 1.

Managing Devices Enrolled in Apple Device Enrollment

Ivanti EPMM supports the use of the Apple Device Enrollment with iOS, macOS, and tvOS devices.

Apple Device Enrollment with Ivanti EPMM overview

Apple Device Enrollment allows you to quickly and easily deploy a fleet of corporate-owned iOS, macOS, and tvOS devices. With Apple Device Enrollment, organizations such as universities and corporations can purchase, enroll, and manage Apple devices en masse. After purchasing Apple devices, administrators enroll devices and manage the devices using a Mobile Device Management (MDM) server such as Ivanti EPMM. Apple Device Enrollment and Ivanti EPMM are linked so that they can easily communicate and new devices assigned to the Apple Device Enrollment account can be synchronized with Ivanti EPMM.

> Apple Device Enrollment is different from other methods of enrolling / registering devices, see "Registration methods" on page 12. See also iOS Apps@Work AppStore Features in the *Ivanti EPMM Apps@Work Guide*.

Changes in Device Enrollment

The original Apple Device Enrollment portal had three sections that represented device enrollment: MDM Servers, Device Assignments and Assignment History. These three are represented in Ivanti EPMM as "Apple Device Enrollment." There are two types of device enrollment programs that Ivanti EPMM manages: Apple Business Manager and Apple School Manager. Apple no longer allows new customers to sign up for the legacy Device Enrollment Program (DEP) portal at deploy.apple.com. New accounts with Apple Device Enrollment will be provisioned on Apple Business Manager.

Apple Business Manager

Apple Business Manager is a place for IT teams to automate device deployment, purchase and distribute content, and manage roles in their organizations. Working seamlessly with Ivanti EPMM, you can enroll devices, deploy content, and delegate administrative privileges.

The Device Enrollment Program (DEP) and the Volume Purchase Program (VPP) are now integrated into Apple Business Manager, so you can bring together everything needed to deploy iOS devices, Mac computers, and Apple TV into your organization. In Ivanti EPMM, the terms "Device Enrollment Program (DEP) is now renamed to "Apple Device Enrollment" and "Device Enrollment." "Volume Purchase Program" (VPP) has been renamed to "Apple Licenses."

- To enroll in Apple Business Manager, see the Apple Business Manager User Guide on the Apple website. A login is required.

- To enroll in User Enrollment, see "User Enrollment with Apple Business Manager" on page 221.

Apple School Manager

Apple School Manager is a simple, web-based portal for IT administrators to deploy iOS, macOS, and tvOS devices all from one place. When used with Ivanti EPMM, you can configure device settings and buy and distribute apps and books. Apple School Manager integrates with Student Information Systems (SISs) so you can quickly create accounts with school rosters and classes.

To enroll in Apple School Manager, see the Apple School Manager User Guide on the Apple website. A login is required..

Apple Device Enrollment features

Using Apple Device Enrollment for large-scale deployments, you can:

- Deploy devices without having to touch them

- Automate mobile device management (MDM) enrollment

- Enable device supervision, including restrictions

- Skip some Setup Assistant screens, allowing device users to use their devices immediately

Apple Device Enrollment setup

The main steps of setting up Apple Device Enrollment are:

1. Enrolling in the Apple Business Manager or Apple School Manager programs.

2. Linking to your MDM server, in this case, Ivanti EPMM.

3. Assigning devices to Ivanti EPMM. For assigning multi-user devices, see "Configuring devices in bulk for Apple School Manager" on page 178.

4. Applying MDM configurations, as desired.

The MDM server you are linking to is Ivanti EPMM. After setting up Apple Device Enrollment, you use Ivanti EPMM to secure and manage your devices, and apply MDM configurations.

If you configure your devices to be supervised, you can apply additional restrictions through Ivanti EPMM.

Best practices for managing devices in Apple Device Enrollment

Following are some best practices to keep in mind for managing enrolled devices in a Device Enrollment Program:

- You can enroll devices in an Apple Device Enrollment you previously registered in Ivanti EPMM, as long as you wipe and retire these devices first.

- Use Apple Device Enrollment to purchase a large group of devices, which you can more easily manage in Ivanti EPMM.

Related topics

- "iOS and tvOS restrictions settings" on page 726

- "macOS settings" on page 772

Setting up Apple Device Enrollment with Ivanti EPMM

Setting up Apple Device Enrollment with Ivanti EPMM involves the following main steps:

1. "Editing Ivanti EPMM roles for Apple Device Enrollment" on the next page
2. "Linking Ivanti EPMM to Apple Device Enrollment" on page 144
3. "Assigning devices to the Apple Device Enrollment account" on page 146
4. "Creating an Apple Device Enrollment Profile" on page 150
5. "Assigning Apple Device Enrollment devices to an enrollment profile en masse" on page 147

6. "Checking for Apple Device Enrollment account updates" on page 149
7. "Setting up Apple Device Enrollment with Ivanti EPMM" on the previous page

Before you begin

Sign up for Apple Business Manager. Apple's deprecated deployment accounts will continue to be supported by Ivanti EPMM as long as Apple continues support.

For more information, see the Apple documentation for setting up an Apple Device Enrollment account.

> When using the hold feature while registering a device with Apple Device Enrollment, it is possible for the device to get stuck in the hold screen if its Internet connectivity drops, causing the Apple MDM server to be unable to reconnect to the device. Make sure you have a stable Internet connection before registering a Apple School Manager device using the hold feature.

Editing Ivanti EPMM roles for Apple Device Enrollment

Before you can set up and manage Apple Device Enrollment in Ivanti EPMM, you must be sure your user name has the correct permissions for these actions. By default, user names with the administrator role will have the correct permissions.

Procedure

1. In the Admin Portal, select **Admin** > **Admins**.
2. Select the administrators whose permissions you want to edit.
3. Select **Actions** > **Edit Roles**.

4. In the Edit Roles window, select the following:

Item	Description
Admin Space	Select the space over which this administrator has administrative control. For example, select **Global** to allow the administrator to use the permissions selected here throughout Ivanti EPMM.
Manage custom attributes	Select to allow the administrator to create custom attributes for use with Apple Device Enrollment.
Manage device enrollment (iOS only)	Select to enable Apple Device Enrollment. ⓘ You can use Apple Device Enrollment to manage macOS and tvOS devices.

5. Click **Save**.

Linking Ivanti EPMM to Apple Device Enrollment

Linking your Ivanti EPMM server to the Apple School Manager portal allows you to use Ivanti EPMM as the designated MDM server for your Apple School Manager devices. You can then use Ivanti EPMM to manage and secure your enrolled devices.

This process involves:

- downloading a public key from Ivanti EPMM and uploading it to the Apple School Manager
- downloading the Apple School Manager server token file and uploading it to Ivanti EPMM

After you upload it to the Apple School Manager, the public key certificate encrypts the authentication server token file for secure transfer to Ivanti EPMM.

ⓘ If you have multiple Apple School Manager accounts for the same instance of Ivanti EPMM, you can use the same certificate you download from Ivanti EPMM for all your Apple School Manager accounts.

ⓘ The following procedure is applicable for only Apple School Manager. If you try to create a MDM server using Apple Business Manager, you will not be able to connect it to Apple School Manager.

Procedure

1. In Ivanti EPMM, go to **Devices & Users > Apple Device Enrollment**.

2. Click **Add+**. The Add Account dialog box opens.

3. In the **Add Account** window, click **Download Certificate**. A .CRT file is downloaded to the file system.

4. Go to your Apple School Manager portal and sign in using a dedicated Apple ID.

5. Navigate to the Manage Servers page and add an MDM server using the certificate (.CRT file) downloaded in the previous steps.

6. Download the server token (.P7M file) from the Apple School Manager. The file will download to your default download location.

7. Go back to Ivanti EPMM and in the **Add Account** window, click **Browse** next to the **ServerToken** field.

8. Select the server token (.P7M file) you downloaded from the Apple School Manager portal.

9. Click **Open**.

10. Click **Save**.

11. Go back to the Apple School Manager portal.

12. Click **Done**.

13. In Ivanti EPMM, click **Check for Updates**. Ivanti EPMM retrieves the new devices.

Assigning devices to the Apple Device Enrollment account

After linking your Apple School Manager account to Ivanti EPMM, you must add devices to your Apple Device Enrollment account. Devices added to Apple Device Enrollment are assigned to Ivanti EPMM, as this is the MDM server you linked to in "Linking Ivanti EPMM to Apple Device Enrollment" on page 144.

Procedure

1. Go to the Apple School Manager portal and sign in using a dedicated Apple ID.

2. Navigate to the **Manage Devices** page and select the method by which you want to add devices, and take action accordingly.

Choose Devices By...	Description
Serial Number	Enter one or more comma-separated serial numbers for the devices you want to assign.
Order Number Choose an order	• Click the **Order Number** radio button. • Select a specific order number from the **Choose an order** drop-down list. A list of devices purchased with that order number is displayed.
Upload CSV File	• Click the **Upload CSV File** radio button. • Click the **Choose File** link to select a CSV file listing devices by serial number.

3. Select **Assign to Server**.
4. From the **Choose MDM Server** drop-down list, select your instance of Ivanti EPMM.
5. Click **OK**. The devices are assigned.

Creating an Apple Device Enrollment profile for Apple School Manager

There are many options for creating a profile for Apple School Manager. The list can be found here: "Creating an Apple Device Enrollment Profile" on page 150.

Mark this location if you will be returning to this page, or open the above link in a new window.

Example Device Enrollment Profiles for Apple School Manager

- Teacher Profile - create a single profile that meets your teacher requirements.
- Student Profile (1:1) - Create a single profile that meets your student requirements for student 1:1 devices (not multi-user).
- Shared iPad Profile (Multi-User)

a. Create a new Add Enrollment Profile and ensure that it has the following settings selected:
   - **Enable Supervision**
   - **Require MDM Enrollment**
   - **Enable Shared iPad (multi-user) for Apple Education**

b. Click **Save**. The Shared iPad profile displays in the Device Enrollment page. The profile is marked as "Multi--user" and from this point forward, any devices that get this enrollment profile will automatically be set for multi-user.

Next steps

- For Apple Business Manager, continue to "Assigning Apple Device Enrollment devices to an enrollment profile en masse" below.
- For Apple School Manager, continue to .

Assigning Apple Device Enrollment devices to an enrollment profile en masse

After linking Ivanti EPMM to a Apple Device Enrollment account, the devices assigned to this account are displayed in the Ivanti EPMM Admin Portal. The Apple Device Enrollment devices are organized so that clicking the number in the Devices column for an account shows the devices assigned to that account. To manage your devices in Apple Device Enrollment, it can help to assign multiple devices to an enrollment profile. You can do that by:

- selecting the devices and adding them
- creating a CSV file containing the relevant devices and uploading the file to Ivanti EPMM

You can also assign custom attributes to the devices using a CSV file. This happens when you assign these devices to an enrollment profile.

If you have already created an enrollment profile and assigned it as the default for all Apple Device Enrollment devices associated with your Apple School Manager account, then your devices have already been assigned an enrollment profile, and you can skip this step. Continue on to "Checking for Apple Device Enrollment account updates" on the next page.

Note the following:

- The CSV file can contain up to 5,000 devices.
- Assigning devices and profiles with a CSV file containing UTF-8 characters may cause errors due to invalid encoding.
- When adding a custom attribute to a CSV file, the column header must match the name of the custom attribute exactly. For multi-users in shared device carts, be sure the CSV file you upload has a new column for the custom attribute created when you enabled Apple Education and connected to the MDM server. Each of these devices must be pre-assigned to a device cart.
- The value of a custom attribute must match the data type of the custom attribute. For example, a boolean type custom attribute can only have a boolean value. For Apple Education Managed Apple ID and Apple Education Device Cart attributes, string is the only valid data type.

Procedure

1. Go to Apple School Manager and sign in using your Apple ID.
2. Select **Device Enrollment Program** in the sidebar.
3. Select **Manage Servers**, then click the name of the server.
4. In the Server Details window, click **Download Serial Numbers** to download a comma-separated value (CSV) file that contains the serial numbers of all assigned devices.
5. After you download the CSV file, click **OK**.
6. Open the CSV file in an editor.
7. Remove the column next to the serial numbers. This column may be called MODEL.
8. Optionally, you can assign a custom attribute to the devices listed in the CSV file by editing the CSV file. The custom attribute is assigned to devices when the devices are assigned to the enrollment profile.
   a. Add a column to the file and name it.
   b. The name of the column is the name of the custom attribute.
   c. Enter a value for the custom attribute in each device row.
   d. Optionally, add more custom attributes and values.

9. Save your changes.

10. In Ivanti EPMM, select **Devices & Users > Apple Device Enrollment**.

11. Find the Apple School Manager account you want to use, and click the number in the **Enrollment Profiles** cell. Ivanti EPMM displays the available enrollment profiles.

12. Select the device enrollment profile you want to use.

13. Select **Actions** > **Assign Devices to Profile**.The Assign Devices to Profile dialog box opens.

14. Click **Upload**, and browse for the CSV file you downloaded from the Apple School Manager Portal.

15. Click **Assign**.

Checking for Apple Device Enrollment account updates

As devices are added to the Apple Device Enrollment account on the Apple School Manager portal, and not on Ivanti EPMM, it is recommended to occasionally check for Device Enrollment account updates in Ivanti EPMM. Ivanti EPMM will synchronize with the Apple School Manager portal, and any devices that have been added or removed will be reflected in the Ivanti EPMM Admin Portal. If an enrollment profile has been configured as the default for the Apple Device Enrollment account, the default enrollment profile will be applied to all newly assigned Apple School Manager devices.

Procedure

1. In Admin Portal, go to **Devices & Users > Apple Device Enrollment**.
2. Click **Check for Updates**.

Verifying the Apple Device Enrollment status of a device

Two values in the Device Details tab indicate the status of a device:

1. Apple School Manager Device
   - A value of true indicates the device was purchased from Apple as a Apple School Manager device. The device itself may or may not be enrolled via Apple School Manager.
   - A value of false indicates the device is either not a Apple School Manager device, or the device was a Apple School Manager device that was later removed from the Apple School Manager portal.

2. Apple Device Enrolled

- A value of true indicates the device is enrolled in the Apple School Manager. Alternatively, the device is enrolled in the Apple School Manager and registered with Ivanti EPMM, but the device has been removed from the Apple School Manager portal.

- A value of false indicates the device is not currently enrolled via Apple School Manager.

If a Apple School Manager device is not enrolled in Apple Device Enrollment, you can retire and wipe the device so as to re-purpose the device for another user.

Procedure

1. In the Admin Portal, select **Devices & Users** > **Devices**.
2. Find the device whose enrollment details you want to examine, and click the carat (^) next to it.
3. Click the **Device Details** tab.
4. Examine the values for **DEP Device** and **DEP Enrolled**.

Creating an Apple Device Enrollment Profile

Apple Device Enrollment profiles allow you to apply a set of mobile device management (**MDM**) features to the devices assigned to a given Apple deployment program account. There is no limit to the number of Device Enrollment profiles, however, you can assign only one default enrollment profile per Apple School Manager account.

> ℹ️ "Apple deployment program" means either Apple Business Manager or Apple School Manager.

The Apple Device Enrollment profile allows you to specify:

- Account details, such as the department of the organization to which the Apple deployment program account is assigned, and the phone number device users may call for support

- The default profile, indicating whether the enrollment profile is automatically assigned to all devices in the Apple deployment program account

- MDM features, such as enabling supervision, requiring MDM enrollment, shared iPad, and allowing devices to pair with a host

- Setup options, such as whether device users are permitted to skip screens in the Setup Assistant

- Certificates, such as anchor certificates (from which the chain of trust is derived) and pairing

certificates (allowing the bearer of the certificate to pair with the device)

- Enrollment options, such as whether to use anonymous, PIN-based enrollment

> For tvOS, the Apple device enrollment profile does not get downloaded until AFTER the Wi-Fi is
> configured. It is advised you use ethernet for tvOS device enrollment.

Procedure

1. In the Admin Portal, go to **Devices & Users** > **Apple Device Enrollment**.

2. Select a Apple deployment program account, and then go to **Actions** > **Add Enrollment Profile**.
   The Add Enrollment Profile dialog box opens. See descriptions of the settings below.

3. Create or edit an enrollment profile.

4. Click **Save**.
   If you have assigned the enrollment profile as the default for devices in your Apple deployment
   program account, the enrollment profile is tagged with a purple icon that reads **Default**.

Apple device enrollment profile settings

The following is a list of the Apple device enrollment profile setting links in this section.

Profile settings are below.

General

TABLE 13. APPLE DEVICE ENROLLMENT PROFILE SETTINGS

Item	Description
Profile Name (Click on column heading to sort alpha-numerically.)	Enter a name for the device enrollment profile. Required.
Description (Click on column heading to sort alpha-numerically.)	Enter a description of the device enrollment profile.
Department (Click on column heading to sort alpha-numerically.)	Enter the name of the department associated with the account. Required.
Support Phone Number (Click on column heading to sort alpha-numerically.)	Enter the support phone number for the Apple deployment program account. Required.
Default Enrollment Profile	Select to have all devices added to this account be automatically assigned to the default profile. If you change the default profile for your Device Enrollment account, existing devices are not affected. This means devices that were previously assigned to the old default enrollment profile continue to be assigned to the old default enrollment profile.

Authentication Type

TABLE 14. AUTHENTICATION TYPE

Item	Description
Password	Select to enable enrollment with a username and password. Device users enter their username and password when prompted.
PIN	Select to enable PIN-based enrollment. Ivanti EPMM will prompt the device user to enter their username and a PIN.

TABLE 14. AUTHENTICATION TYPE (CONT.)

	To enable PIN-based enrollment for an individual device:
	1. Go to **Devices & Users** > **Devices**.
	2. Select **Add > Single Device**.
	3. Search for the **User**.
	4. Select the **Device Platform**. Choices are Android, iOS, macOS or Windows.
	5. If you select iOS or macOS, the **Include Registration PIN only for Apple Device Enrollment** field activates. Select this check box.
	6. Enter a username, operator, and mobile number (or select This devices has no phone number) for the device, as you normally would.
	7. Enter a username, operator, and mobile number (or select This devices has no phone number) for the device, as you normally would.
	8. Make other selections for **Device Ownership**, **Device Language**, and **User Notification**.
	9. Click **Register**.
	To enable PIN-based enrollment for multiple Apple deployment program devices using bulk registration:
	• Create a CSV file containing the information you need to bulk register a number of devices.
	• Add the field **Include DEP Only Registration Pin (TRUE or FALSE)** to the CSV file, with a value of TRUE for all devices for which you want to enable anonymous Apple Device Enrollment.

TABLE 14. AUTHENTICATION TYPE (CONT.)

	For more information about single or bulk device registration in Ivanti EPMM, see the following sections in *Getting Started with Ivanti EPMM*. • "Single device registration" • "Registering multiple devices" • "Bulk device registration CSV file requirements"
Anonymous	Select to enable device enrollment without assigning a username and password during enrollment. After completing the Device Enrollment, the device will be in a signed-out state (with no user assigned). Usernames will be assigned after devices are distributed, using the Secure Sign In web clip. For more information about the Secure Sign In web clip, see "Multi-User Support" on page 229. ⓘ You cannot use the Anonymous enrollment option on macOS devices.
Enable SAML	As part of DEP profile, the MDM server provides custom enrollment URL along with standard URL to get the MDM profile to Apple server. This URL can be used to enforce your own authentication model or to provide any other information. Select this to support external IdP with DEP enrollment. This feature is applicable for iOS 13.0 and macOS 10.15 devices or supported newer versions. • You must have SAML enabled. (See "Configuring SAML/IdP support" in the *Ivanti EPMM System Manager Guide*.) If the IdP has not been configured properly, and is not reachable, the **Enable SAML** check box will not display.

TABLE 14. AUTHENTICATION TYPE (CONT.)

	• Once set up for SAML on iReg or DEP devices, you will not be able to disable SAML from the System Manager. You must first de-select **Enable SAML** in the Device Registration page before you can disable the IdP SAML connection in the System Manager.

Custom Enrollment

Custom Enrollment URL: (iOS 13.0+ and macOS 10.15+) Create custom enrollment web page(s).

Specify your own custom web page (web view) to authenticate device users during Device Enrollment. Use this page to display custom information such as authentication type, branding, consent text, and privacy policy. See "Adding a custom Automated Device Enrollment web page" on page 169 for more details.

Enter the URL, such as https://mycustomweburl.com. This URL defines the value of the custom URL to present to the device user in a web view.

MDM (Mobile Device Management) Options

Item	Description
Enable supervision	Select to allow Apple School Manager devices to be supervised. Supervision allows the use of additional device restrictions and configurations (For iOS 13+ and macOS 10.15+, Supervised mode will be selected by default). In iOS 13+ and supported later versions, all devices using Apple Device Enrollment will be supervised and the iOS will ignore the is_supervised flag. ℹ️ For more information about applying restrictions to supervised Apple devices, see "iOS and tvOS restrictions settings" on page 726.
Require MDM enrollment	Select to force users to apply the enrollment profile when Setup Assistant runs. In iOS 13+ and supported newer versions, all Apple Device Enrollments are mandatory.

	(For iOS 13+ & macOS 10.15+, selected by default).
Allow MDM profile removal	Select to allow device users to remove the device from device management. Supervision is required to disallow removal.
Allow pairing	Select to allow host pairing functions, such as iTunes synchronization. Pairing is always allowed for hosts that have valid pairing certificates (Not applicable for iOS 13+ & macOS 10.15+).
Enable Shared iPad (multi-user)	• If this field is selected, you MUST also have the **Await device configuration during Apple device enrollment** field selected. • For Apple Business Manager, this is applicable to iOS 14.5 and later. ⓘ Only Apple-licensed apps are sent to Shared iPad devices through registration. This is set up by selecting the **Send Installation Request on device registration or sign in** option in the AppCatalog. For more information, see "Using the wizard to import iOS apps from the Apple App Store" in the *Ivanti EPMM Apps@Work Guide*. ⓘ Be sure to also select the following settings: **Enable supervision** and **Require MDM enrollment**. For Apple Business Manager, when this field is selected, new options display: **Allow Guest / Temporary Sessions Only** - Guest / temporary shared iPad users to use the iPad, but the data in the guest's partition is deleted when the user logs out. The next guest that logs into the same iPad will start afresh.

	When the **Allow Guest / Temporary Sessions Only** field is selected, only the **Guest/Temporary Session Timeout (seconds)** field displays. Enter the number of seconds into the field. If this field is 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.
	
	If **Allow Guest/Temporary Sessions Only** is deselected, the following fields display:
	
	• **Use Device Defaults** - Select to set the session timeouts and let Apple figure out the Quota Size for you.
	
	• **Set Maximum Resident Users** - Set the number of users on the Shared iPad. Apple will then automatically allocate the quota space evenly between the number of users. 32 is the maximum number of users allowed on a shared iPad.
	
	  ⓘ If the maximum resident users is set to five users on a Shared iPad, and a sixth user logs in, the data from the oldest user on the Shared iPad gets deleted.
	
	• **Set Quota Size (MB)** - The size allocated for the user's data on the Shared iPad. For example, on a 100 GB iPad with 10 users, then each user has 10 GB for that iPad.
	
	  ⓘ Administrators need to choose either **Set Max Residence User** or **Set Quota Size**.
	
	• **Guest/Temporary Session Only** - 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. Once the temporary session has ended (user logs out), the data is deleted from the iPad. Label to be used: Allow only Temporary Session.

	• **User Session Timeout (seconds)** - If left blank, the timeout will use the system defaults. If set to zero, there will be no timeout. Maximum limit is 1800 seconds. Label to be used: Set Timeout for User Session - Seconds.
	Be sure to also select the following settings: **Enable supervision** and **Require MDM enrollment**.
	• **Online Authentication Grace Period (Day(s)** - Select the number of days' grace period before the online authentication against Apple's identity server is required. During the grace period, the Shared iPad only verifies the user's passcode locally during login (for users that already exist on the device.) Default value is 0. Applicable to iPadOS 16+. • **Domains** - Click the **Add+** button to add default domains to make it easier for the Shared iPad user to select from a list the domain user wants to sign in to. This list is located just above the keypad on the iPad. Optionally, device user can also type in the domain when signing in. Applicable to iPadOS 16+.
Await device configuration during Apple device enrollment **Wait until policies and configurations are pushed to devices**	Select to set device-based VPP applications to install during the DEP enrollment process and during (supervised) device enrollment. Using VPP apps using device-based licenses, the applications can be installed and available for the device user by the time the device finishes set up. When registering a Apple School Manager device, the device will be held in the Setup Assistant screen until Ivanti EPMM receives confirmation that the profiles and configurations for that device have been pushed to the device. The Apple School Manager device is then released from the Setup Assistant screen.

	If a Apple School Manager device checks in with Ivanti EPMM, and Ivanti EPMM detects this device is still awaiting its profiles and configurations, Ivanti EPMM sends a command to release the Apple School Manager device from the Setup Assistant, if a command has not already been sent. • Applicable to supervised iOS devices - Install in-house apps are also supported during DEP await configuration along with VPP apps. • Applicable to supervised macOS devices - In-house apps are not supported. **Time Limit (Minutes)** - Enter the number of minutes for which you want to hold all iOS and macOS devices in the Setup Assistant. The maximum is 10 minutes. If, after the specified time limit has passed and Ivanti EPMM has not received acknowledgment that the profiles and configurations have been pushed to the device, the device is released from the Setup Assistant. This is helpful in case there are a lot of apps that require more time. The remaining apps will be automatically installed after the device is registered. ⓘ If selecting this field, then you need to also select **Send installation upon device registration** in the specific app. ⓘ For macOS devices, selecting **Await device configuration during Apple device setup** has the effect of allowing account setup during the Apple Device Enrollment process.
Auto Advance Setup	Device will tell Setup Assistant to automatically advance through its screens (Applicable for tvOS and macOS 11.0 and later versions.)

Setup Options

Skip Options

Select the screens to be skipped when Setup Assistant runs on Apple School Manager or Apple Business Manager devices.

Note the following:

- Selecting **Skip signing in to Apple ID and iCloud** auto-selects the **Skip Apple Pay Setup** option.

- Selecting **Skip passcode creation** auto-selects the **Skip Apple Pay Setup** and **Skip Touch ID Setup** options.

- Selecting **Skip Touch ID** Setup auto-selects the **Skip Apple Pay Setup** option.

- **Skip on-boarding informational screens** - The information in this screen is used for user education, for example: Cover Sheet, Multitasking & Control Center.

- You can choose to skip or enable as many screens as you like. Device users will be able to set up skipped features later.

Skip options available

Skip Option	Notes
Skip All Options	Applicable to iOS 13.0, macOS 10.14, and macOS 10.15 or supported newer versions. Default setting is disabled.
Skip Location Services	
Skip Restore from Backup	
Skip Move from Android	
Skip signing in to Apple ID and iCloud	
Skip Terms and Conditions	
Skip passcode creation	
Skip Siri	
Skip automatically sending diagnostic information	

Skip Registration Screen	macOS only
Skip Touch ID Setup	
Skip Apple Pay Setup	
Skip Zoom Setup	
Skip FileVault Setup Assistant Screen (macOS only)	
Skip DisplayTone Setup	
Skip the Home Button screen	
Skip iCloud Storage	
Skip the Tap To Set Up option in AppleTV	tvOS only
Skip the Aerial Screensavers Setup in AppleTV	tvOS only
Skip on-boarding informational screens	
Skip the screen for Apple Watch migration	
Skip iCloud Analytics screen	macOS only
Skip Apple TV home screen layout sync screen	tvOS only
Skip the Apple TV provider sign in screen	tvOS only
Skip the Where is this Apple TV? screen	tvOS only
Skip the Privacy screen	
Skip the iMessage and FaceTime screen	
Skip the Screen Time screen	Applicable to macOS 10.15 or supported newer versions.
Skip the Mandatory software update screen	
Skip the Add cellular plan screen	
Skip the Choose Your Look screen	Applicable to iOS 13.0 and macOS 10.14 or supported newer versions.
Skip Express Language Setup pane	Applicable to iOS 13.0 or supported newer versions.

Skip Preferred Language Order pane	Applicable to iOS 13.or supported newer versions.
Skip Get Started pane	Applicable to iOS 13.0 or supported newer versions.
Skip the Accessibility pane (macOS only)	If the Mac is connected to Ethernet and the Device Enrollment profile is downloaded, skips the Accessibility pane. Applicable to macOS 11.0 or supported newer versions.
Skip the Restore Completed pane	Applicable to iOS 14.0 or supported newer versions.
Skip the Software Update Complete pane	Applicable to iOS 14.0 or supported newer versions.
Skip Unlock With Watch (macOS only)	Skips Unlock Your Mac with your Apple Watch pane. Availability: macOS 12+.
Skips the Terms of Address pane	Skips the Terms of Address pane. Availability: iOS 16+, and macOS 13+.
Skip the Device to Device Migration	Skips Device to Device Migration pane. Availability: iOS 13+.
Skip the iMessage pane when using phone number for Message Activation	Skips the iMessage pane. Availability: iOS 10+.

Other Options

- **Show custom text on the Login page**: Select to show customized text on the login page when users log in to their Apple School Manager devices. In the text field that appears when selecting this option, enter your customized text. You can enter up to 50 characters.

- **Anchor Certificates**: Click **Browse**, to select an anchor certificate. Click Add to add an additional anchor certificate. The anchor certificate allows the device to trust the connection to Ivanti EPMM. This is the certificate from which the chain of trust is derived.

> ℹ️ Certificate files must be in DER or PEM format.

- **Pairing Certificates**: Click **Browse**, to select a pairing certificate. Click **Add** to add an additional pairing certificate. The pairing certificate allows the device to securely pair with a host possessing this certificate when **Allow Pairing** is disabled.

> ℹ️ Certificate files must be in DER or PEM format.

macOS Account Creation

Users must enroll macOS devices in the Apple School Manager with an administrator account. You can prompt users to create an administrator account for themselves, or you can create an administrator account in Ivanti EPMM, which Ivanti EPMM then pushes to macOS Apple School Manager devices.

Prompt primary account setup to users

Select to prompt the device user to set up a primary account for the macOS Apple School Manager device.

You can prompt the user to create a regular account or an administrator account. If you prompt users to create a regular account, you will still need to create an administrator account for enrolling macOS devices in Apple School Manager. This is because device enrollment on macOS devices requires the use of an administrator account.

- **Regular user**: The device user is prompted to create a regular user account. If you select this option, you must still create an administrator account for use on the Apple School Manager device in the **Setup Managed macOS Admin Account** section.

- **Administrator user**: The device user is prompted to create an administrator account to be used when enrolling the device in Device Enrollment. You can create an additional administrator account that Ivanti EPMM synchronizes with Apple School Manager devices by selecting the **Create a new admin user account** option.

  For macOS devices, be sure to select **Await device configuration during DEP setup**, as this option has the effect of allowing account setup during the Apple Device Enrollment process.

Skip primary account setup

Apple School Manager device user will not be prompted to setup an account when enrolling the device in Device Enrollment. You create an administrator account in Ivanti EPMM instead, so that an administrator account exists on the device when the user enrolls in Device Enrollment.

Select to create a new user with administrator privileges for use when configuring the Apple School Manager device.

As there is no primary account that can be used as an administrator user, you must create an administrator user in the next section of this window.

Create a new administrator user account

Select to enable the creation of an administrator account.

ⓘ   Device Enrollment on macOS devices requires the use of an administrator account.

Setup Managed macOS Administrator Account

Fill in the following entries to setup the Administrator account:

- **Username**: Enter the username of the macOS device. This is the name that is displayed when logging on to the device.
  The administrator account you create will be associated with the macOS device bearing this username.

- **Full Name**: Enter the name of the macOS device as defined in macOS under **Settings** > **Sharing** > **Computer Name**.
  The administrator account you create will be associated with the macOS device bearing this name.

- **Password**: Enter a password for the administrator account and confirm it.

- **Hide managed administrator account in Users & Groups**: Select this option to hide the administrator account from device users. When selecting **Settings** > **Users & Groups** on a macOS Apple School Manager device, the administrator account will be hidden from view.

Managing Apple Device Enrollment accounts

After adding one or more Apple Device Enrollment accounts to an Ivanti EPMM instance, several actions are available to help manage the accounts, including:

- "Viewing Apple Device Enrollment accounts in Ivanti EPMM" on the next page
- "Editing Apple Device Enrollment account information" on page 166
- "Removing or Re-assigning Apple Device Enrollment profile assignments" on page 167
- "Deleting Apple Device Enrollment profiles" on page 168
- "Deleting Apple Device Enrollment accounts" on page 168
- "Disowning devices enrolled in Apple Device Enrollment " on page 168

For instructions on how to set up a Device Enrollment profile, see "Setting up Apple Device Enrollment with Ivanti EPMM" on page 142.

Viewing Apple Device Enrollment accounts in Ivanti EPMM

After setting up Apple Device Enrollment accounts in an Ivanti EPMM instance, you can view the status of these accounts.

Procedure

1. In Admin Portal, go to **Devices & Users**.

2. Select **Apple Device Enrollment** to display the list of accounts enrolled on the Ivanti EPMM instance.

   > ℹ️ If you have not added an Apple Device Enrollment account to a particular Ivanti EPMM instance, a message is displayed instead of an Apple Device Enrollment account list. The message explains that no Apple Device Enrollment accounts are associated with this Ivanti EPMM instance yet.

The information available for each Apple Device Enrollment account is listed in the following table:

TABLE 15. APPLE DEVICE ENROLLMENT ACCOUNT INFORMATION

Item	Description
Account Name (Select on column heading to sort alpha-numerically.)	Name assigned to account.
Admin Apple ID (Select on column heading to sort alpha-numerically.)	Administrator ID received from Apple.
Organization Name (Select on column heading to sort alpha-numerically.)	Name that you provide to Apple for the organization associated with the Device Enrollment account. Apple uses this name when displaying messages about the account.
Description	Description that you provide to Apple for the organization associated with the Apple Device Enrollment account.
Status (Select on column heading to sort alpha-numerically.)	Account status can be one of three states: • Active, indicates the Ivanti EPMM instance is associated with one or more active Apple Device Enrollment accounts.

TABLE 15. APPLE DEVICE ENROLLMENT ACCOUNT INFORMATION (CONT.)

Item	Description
	• Invalid Token, indicates the Apple server token is either expired or invalid. • Inactive, indicates the Ivanti EPMM instance is associated with a deleted Apple Device Enrollment account.
Expires (Select on column heading to sort alpha-numerically.)	Date the server token expires.
Devices	Number of devices in the Apple Device Enrollment account. Select the number to view the devices in the Devices page.
Enrollment Profiles	Number of enrollment profiles defined for the Apple Device Enrollment account. Select the number to list the enrollment profiles (see "Creating an Apple Device Enrollment profile for Apple School Manager" on page 146.)

> ⓘ You can also run a search using the **Filter Enrollment Profiles** search bar in the top right corner of the page.

Editing Apple Device Enrollment account information

Most Apple Device Enrollment account information is derived from Apple, and cannot be edited in Ivanti EPMM. To edit the Apple-derived device account information, log in to your Apple School Manager and make the changes.

When the server token associated with the account is expiring, you can then change the server token by editing the Ivanti EPMM Apple Device Enrollment account in Ivanti EPMM.

Procedure

1. In Admin Portal, go to **Devices & Users > Apple Device Enrollment**, and then select an account.

2. Go to **Actions > Edit Account**.

3. (Optional) To change the server token, select **Browse**, locate the file, select it, and then select **Open**.

4. (Optional) To change the account description, edit the text in **Account Description**.

5. Select **Save**.

Removing or Re-assigning Apple Device Enrollment profile assignments

This section addresses the removal or re-assigning of Apple Device Enrollment profiles.

Removing Apple Device Enrollment profiles

Removing Apple Device Enrollment devices from an enrollment profile removes the MDM and setup options from the devices.

> After Apple Device Enrollment profile assignments are pushed to devices and the devices complete setup, removing the Apple Device Enrollment profile assignments or changing the device profiles has no effect on existing devices until the device is wiped or reset.

Procedure

1. In Admin Portal, go to **Devices & Users > Apple Device Enrollment**.

2. In the row of the desired account, select the number in the Enrollment Profiles column.

   Ivanti EPMM lists the defined enrollment profiles for that account.

3. Select the number in the Devices column within the selected enrollment profile.

4. Select the profile and then select **Actions > Remove Enrollment Profile**. Alternately, you can reassign the device to a new profile by selecting **Actions > Assign Enrollment Profile**.

5. When prompted, select **Yes** to remove the devices from the enrollment profile or **No** to cancel the deletion.

Re-assigning Apple Device Enrollment profiles

1. In Admin Portal, go to **Devices & Users > Apple Device Enrollment**.

2. In the row of the desired account, select the number in the Devices column within the selected enrollment profile.

3. Select the profile and then select **Actions > Assign Enrollment Profile**.

Deleting Apple Device Enrollment profiles

Deleting an Apple Device Enrollment profile allows you to remove a set of mobile device management (MDM) features associated with the devices assigned to a given Apple Device Enrollment account. When there is a default device enrollment profile and you try to delete a different enrollment profile, Ivanti EPMM re-assigns the device to the default device enrollment profile instead of deleting it.

Procedure

1. In Admin Portal, go to **Devices & Users > Apple Device Enrollment**.

2. Select an account and select the number in the Enrollment Profiles column for that account.

   Ivanti EPMM lists the defined enrollment profiles for that account.

3. Select the enrollment profile to delete, and then go to **Actions > Delete**.

4. When prompted, select **Yes** to delete the profile or **No** to cancel the deletion.

Deleting Apple Device Enrollment accounts

If you delete an Ivanti EPMM Apple Device Enrollment account, you are deleting the mapping between Ivanti EPMM and the Apple MDM servers. Deleting a Device Enrollment account from Ivanti EPMM does not have any affect on the Apple Device Enrollment account.

Procedure

1. In Admin Portal, go to **Devices & Users > Apple Device Enrollment**, and then select one or more accounts.

2. Go to **Actions > Delete Account**.

3. When prompted, select **Yes** to delete the chosen accounts or **No** to cancel the action.

Disowning devices enrolled in Apple Device Enrollment

If a device enrolled in Apple Device Enrollment is sold, lost or damaged beyond repair, you can remove that device from the Apple Device Enrollment portal through the MDM server. Removing the device is called "release device" or "disown device" depending upon what portal you are looking at.

Once a device enrolled in Apple Device Enrollment is disowned, Ivanti EPMM cannot add it back. The Disown action is disabled by default and is not included in the list of actions for devices in Apple Device Enrollment. To add Disown to Actions into the Apple Device Enrollment page, call Customer Support.

Related topics
"Setting up Apple Device Enrollment with Ivanti EPMM" on page 142

Adding a custom Automated Device Enrollment web page

Applicable to: iOS 13.0 and macOS 10.15 or supported newer versions.

In the Custom Enrollment section, you can specify your own custom web page (web view) to authenticate users during Automated Device Enrollment. Use this page to display custom information such as authentication type, branding, a corporate message, consent text, and privacy policy.

When using LDAP for registration, the device user needs to be authorized in Ivanti EPMM or be bulk enrolled. Device users that are not in Ivanti EPMM will not be recognized and registration will fail.

Procedure

1. In the Admin Portal, go to **Devices & Users > Apple Device Enrollment**.

2. Find and select the name of the server you created on the Apple site.

3. Select **Actions > Add Enrollment Profile**.

4. In the Custom Enrollment URL field, enter the URL, such as https://mycustomweburl.com. This URL defines the value of the custom URL to present to the user in a web view loaded during the initial setup of a new Device Enrollment device or an erased device. Use this field to define your own authentication UI with authentication method. After the user is authenticated, the MDM enrollment profile is downloaded.

Workflow of the custom Automated Device Enrollment web page

This section elaborates the behavior of the custom Automated Device Enrollment web page and the procedure to create the custom web page (web view).

When the custom web page specified in the **Custom Enrollment URL** field loads initially:

- The configuration web URL has an HTTPS scheme and is a POST request. The web page should use a publicly trusted certificate.

- A custom header x-apple-aspen-deviceinfo is appended to the POST request by the Apple device on which enrollment is initiated. It contains a base64 encoding of a CMS (Cryptographic Message Syntax) envelope that contains a plist with device attributes. This is the same information, in the same format, as provided in the initial GET request with token-based device enrollments.

When the custom web page loads subsequently:

- The device user interacts with the web page (web view) until the administrator's host server provides a custom.mobileconfig file to the client. The Ivanti EPMM server returns byte code of the MDM profile. In the administrator's host server, the custom.mobileconfig file should be set with a MIME type of application/x-apple-aspen-config so that the MDM profile for the device is downloaded and installed on the device.

- To get the MDM profile for that device and its related user, the administrator's host web server should make a POST request to the Ivanti EPMM server URL. It should contain basic authentication using an Ivanti EPMM user ID with administrator rights. For example, https://IvantiEPMMDomain.com/api/v2/external/mdm/config/DEPMDMProfile). With parameters as principal, and deviceInfo as the header, where:

    o deviceInfo is the "x-apple-aspen-deviceinfo" data Apple sent

    o principal is the Ivanti EPMM user to associate to the Device Enrollment profile's device

    > ⓘ If the principal user does not exist, the Device Enrollment profile must allow the anonymous authentication type in order to associate the device to an anonymous user. If the Anonymous Authentication type is not set, the POST call will fail. To set the anonymous authentication, select "Anonymous" in the Authentication Type field in the Device Enrollment profile.

- Here are the additional details:

    o When a device hits the custom web URL configured in the Device Enrollment profile, administrator's host web server should capture the header "x-apple-aspen-deviceinfo" presented by the device. Between the initial POST with the x-apple-aspen-deviceinfo and the return response with the x-apple-aspen-config, the third party host has control. After the return response, Apple gets control back. The reason for this is the response has to come from the third party host due to the SSL certificate negotiations, as Apple will only trust the response

     from the third party host.

    ◦ After the administrator's host web server receives the byte code, the third party host should respond by setting response headers, Content-Disposition = attachment;filename="custom.mobileconfig" and Content-Type = application/x-apple-aspen-config.

- The web view closes and the OS attempts to install the profile, which must be an MDM enrollment profile.

ℹ️   Ivanti EPMM does not authenticate the user ID for which the MDM profile is returned. Therefore, administrators should perform the necessary authentication for the user ID before requesting for the MDM profile.

For iOS, this workflow is supported during initial setup of an erased device. For macOS, this workflow is supported both within Setup Assistant and also via the Profiles preference pane, if Automated Device Enrollment was skipped during Setup Assistant.

For developer information related to creating a custom web page, see the following Apple documentation references:

[Web Views](#)

[Authenticating Through Web Views](#)

[Sample code to implement a simple iPad web browser that can view either the desktop or mobile version of a website](#)

Managing Apple School Manager Devices

This section addresses Apple School Manager and Apple Education.

Apple School Manager account management overview

Apple School Manager is a service for schools that allows IT departments at educational institutions to manage school devices and deploy apps to these devices. With Apple School Manager, you create and assign roles to students and staff that define the permissions and restrictions applied to groups of users. Apple School Manager uses mobile device management (MDM) solutions, such as Ivanti EPMM, to manage Apple School Manager devices.

Ivanti EPMM uses the following to manage your Apple School Manager devices:

- An Apple Device Enrollment account, to more easily purchase and enroll devices in bulk

- A Apple License account, to manage and distribute apps to teacher and student devices with a device-based license

In Ivanti EPMM's user interface, the term "Apple Education" is used. "Apple School Manager portal" refers to the Apple portal (school.apple.com.)

Using Apple Device Enrollment, you can purchase and enroll devices in bulk. You then create an Apple School Manager account to which you assign your devices. Apple School Manager synchronizes with supported third-party vendor Student Information Systems (SIS) to retrieve student, teacher, and class data. Finally, you connect Apple School Manager to Ivanti EPMM to manage school devices and use the Apple Licenses to distribute apps to teachers and students alike (such as the Apple Classroom app for teachers only, and other apps you may wish to deploy to student devices).

> ℹ️ You can only use one Apple School Manager account in Ivanti EPMM.

For more information about using Apple School Manager, refer to the following documents from Apple (an Apple login is required):

- [Education Deployment Guide](#)

- [Apple School Manager Help](#)

- [Deployment Resources](#)

Apple School Manager managed entities

The entities you manage in an Apple School Manager account include:

- **Students and teachers** -You can add students to your Apple School Manager account using your Student Information System (SIS). You can also manually add students, teachers, and classes to your Apple School Manager account.

  > ℹ️ Apple School Manager does not synchronize user roles with Ivanti EPMM, meaning students and teachers can only be distinguished by context, such as the name of the user teaching a class.

- **Class** - A class requires students and teachers at minimum.

- **Courses** - A unit of study associated with students and teachers. You can only view courses in Ivanti EPMM after synchronizing with Apple School Manager servers.

- **Locations** - You can add one location and multiple sub-locations to your Apple School Manager account. You can only view locations in Ivanti EPMM after synchronizing with Apple School Manager servers.

- **Devices** - When using Apple School Manager, Ivanti EPMM supports supervised iPad devices running iOS 9.3 through the most recently released version of iOS or supported newer versions.

- **Managed Apple ID**. A managed Apple ID allows users to log in to a device and access services such as Apple School Manager, iCloud courses, and iTunes U courses. The Apple School Manager account controls the Managed Apple IDs associated with that account, enabling account administrators to reset passwords, set roles and permissions, and so on. A Managed Apple ID restricts certain services such as the user's ability to make purchases on the Apps, iBooks, and iTunes stores. When you add users to your Apple School Manager account, a Managed Apple ID is created at the time of account creation.

Related topics

For more information, see "What are Managed Apple IDs?" in the [Apple School Manager User Guide](#). An Apple login is required.

Apple School Manager device requirements

Devices you manage with Apple School Manager must:

- Be supervised

- Run iOS 9.3 through the most recently released version of iOS or supported newer versions

Ivanti recommends using Apple Device Enrollment devices with Apple School Manager for ease of management, and beginning with fresh devices. If you are re-purposing a device, Ivanti recommends you wipe and then retire the device before using it with Apple School Manager.

The Classroom app

Classroom is an iPad app that allows teachers to share documents and learning modules with students, as well as manage student devices. Teachers can use Classroom to launch apps or a textbook on student iPad devices and share or project documents or work.

You can use Ivanti EPMM to distribute the Classroom app to teacher devices and configure whether students can control whether teachers can view their screens.

For more information about Classroom, see the following Apple links (an Apple login is required):

- Getting Started with Classroom

- [Classroom Help](#)

Apple School Manager setup with Ivanti EPMM: main steps

The main steps required to set up Apple School Manager with Ivanti EPMM are as follows:

Best practices for managing devices in Apple School Manager

Following are some best practices to keep in mind for managing enrolled devices in Apple School Manager:

- Distribute the Classroom app to teacher devices using Apple Licenses and a label you create for teacher devices. Distribute any apps you want on student devices using Apple Licenses as well, and a label you create for student devices. Use device-based Apple licenses.

- You can enroll devices in an Apple Device Enrollment you previously registered in Ivanti EPMM, as long as you wipe and retire these devices first.

- Use Apple Device Enrollment to purchase a large group of devices, which you can more easily manage in Ivanti EPMM.

- Ivanti recommends against using anonymous enrollment.

- Using a CSV file automates the process of applying a Managed Apple ID for each device, preparing the devices for use with Apple School Manager. When enrolling devices in bulk with Apple Device Enrollment:

  ○ Use a modified CSV file listing both device serial numbers and the Managed Apple ID as a custom attribute value for each device.

  ○ For multi-users in shared device carts, be sure the CSV file you upload has a new column for the custom attribute created when you enabled Apple Education and connected to the MDM server. Each of these devices must be pre-assigned to a device cart.

- It is best to assign only one role to a given Managed Apple ID, as only one type of profile can be pushed to an Apple School Manager device (either teacher or student). If a Managed Apple ID is associated with both a teacher and a student, then the profile pushed to the device will always be a teacher profile.

- Apple's School Manager program sometimes uses the terms "leader" and "member" to indicate teacher and student, respectively.

Creating an Apple School Manager account

Contact Apple to request an Apple School Manager account. When you contact Apple, give them your current Apple Device Enrollment and Apple License accounts so that Apple can link to your Apple School Manager account. Alternatively, you can request new Apple Device Enrollment and Apple License accounts from Apple.

Note the following:

- At this time, only educational institutions are allowed to enroll.

- Ivanti EPMM continues to support multiple Apple Device Enrollment accounts but only one account can be used with Ivanti EPMM's Apple Education feature.

Next steps

- Optionally, add managers to your Apple School Manager account. Managers are essentially administrators who can add students, teachers, classes, and other information to your Apple

School Manager account. For details, refer to "Add Managers" in the Apple School Manager User Guide on the Apple website. A login is required.

Adding school information to your Apple School Manager account

You can add your school information to your Apple School Manager account using a Student Information System (SIS) supported by Apple.

Before you begin

Contact Apple about creating an Apple School Manager account, as described in "Creating an Apple School Manager account" on the previous page.

Procedure

For detailed information about adding school information to your Apple School Manager account, refer to the following Apple documentation:

- Integrate with your Student Information System (SIS)

- Find people in your Student Information System (SIS)

- View and edit SIS information

- Create Managed Apple IDs in the Apple School Manager Help

- Create Managed Apple IDs Apple documentation

Next steps

You will need to set up your administrators in the Apple School Manager portal. Once you have finished, continue to "Editing Ivanti EPMM roles for Apple Education management" below.

Editing Ivanti EPMM roles for Apple Education management

Before you can set up and manage an Apple School Manager account, you must be sure your user name has the correct permissions for these actions. By default, user names with the administrator role will have the correct permissions.

Before you begin

You should have set up your administrators in the Apple School Manager portal.

Procedure

1. In the Admin Portal, select **Admin** > **Admins**.

2. Select the administrators whose permissions you want to edit.

3. Select **Actions** > **Edit Roles**.

4. In the Edit Roles window, select the options according to the table below.

5. Select **Save**.

TABLE 1. EDIT ROLES OPTIONS

Section	Item	Description
	Admin Space	Select the space over which this administrator has administrative control. For example, select **Global** to allow the administrator to use the permissions selected here throughout Ivanti EPMM.
Apple Education Management	**View Apple Education**	Select to allow the administrator to view the Apple Education page.
	Manage Apple Education	Select to allow the administrator to view the Apple Education page and sync with Apple School Manager servers.
	Setup Apple Education	Select to allow the administrator to view the Apple Education page, sync with Apple School Manager servers, toggle the Apple Education feature on/off, and set up an Apple School Manager account. Select to also create, delete, and apply to Class and remove classes from the Device Cart.
Settings and Services Management	**Manage custom attributes**	Select to allow the administrator to create custom attributes for use with Apple School Manager.
Device Management	**Manage device enrollment (iOS only)**	Select to enable Apple Device Enrollment.

Configuring devices in bulk for Apple School Manager

After you have added your devices to Apple School Manager, you must add them to Ivanti EPMM. Teacher and student iPad devices must use Device Enrollment. In addition, the teacher and student 1:1 iPad devices must have the "Managed Apple ID" custom attribute pre-defined and Shared iPad devices must have the "DeviceCartName" custom attribute predefined. Assigning the devices to the correct Apple Device Enrollment Profile and setting the appropriate custom attributes can be done easily in bulk.

Before you begin

Complete the procedure in "Editing Ivanti EPMM roles for Apple Education management" on page 177.

Bulk-assign devices to a Teacher or Student 1:1 device enrollment profile for use with Apple Education

Procedure

1. From your Apple School Manager account, go to the MDM server configured for Apple Education in Ivanti EPMM and download the list of serial numbers. Only devices assigned to this MDM server can be used with the bulk-assign feature.

2. Create a CSV file to pre-assign the Managed Apple ID to the appropriate serial numbers:

   a. Using the CSV file in step 2, remove serial numbers that are not teacher or student 1:1 devices.

   b. Remove the column "DEVICE_TYPE".

   c. Add a column for the column name of your Managed Apple ID custom attribute. This could be something like "ManagedAppleID" and is based on what you chose when Enabling Apple Education in Ivanti EPMM. You can view this attribute name at the top of your Apple Education page under the label "Managed Apple ID Attribute Name."

   d. (Optional) Add any other custom attribute you want to the CSV file by creating a new column for the attribute and entering a value for that attribute for each device. Any custom attribute you create here must match the custom attribute you have already created in Ivanti EPMM.

   e. For each row, add the appropriate Managed Apple ID for the teacher or student in the column created in step c above. This will be something like "jdoe@school.com," and should match an individual in your **Apple Education > Individuals** tab.

   f. Save the CSV file and close it.

3. Navigate to **Devices & Users > Device Enrollment** and, in the row of your Device Enrollment account, select the number link in the **Enrollment Profiles** column. The list of enrollment profiles for your Apple School Manager account displays.

4. Select an existing profile that is a "multi-user" profile and then select **Actions >Assign Devices to Profile**.

5. In the Assign Devices to Profile dialog box, click **Upload** and choose the CSV file you created above and then click **Assign**. The devices will be assigned to this enrollment profile with the appropriate individuals pre-assigned to the devices.

Bulk-assign devices to a Shared iPad (multi-user) enrollment profile for use with Apple Education

Procedure

1. From your Apple School Manager account, go to the MDM server configured for Apple Education in Ivanti EPMM and download the list of serial numbers. Only devices assigned to this MDM server can be used with the bulk-assign feature.

2. Create a CSV file to pre-assign the Managed Apple ID to the appropriate serial numbers:

    a. Using the CSV file in step 2, remove serial numbers that are not Shared iPad devices.

    b. Remove the column "DEVICE_TYPE".

    c. Add a column for the column name of your Device Cart custom attribute. This could be something like "DeviceCart" and is based on what you chose when Enabling Apple Education in Ivanti EPMM. You can view this attribute name at the top of your Apple Education page under the label "Shared Device Cart Attribute Name."

    d. (Optional) Add any other custom attribute you want to the CSV file by creating a new column for the attribute and entering a value for that attribute for each device. Any custom attribute you create here must match the custom attribute you have already created in Ivanti EPMM.

    e. For each row, add the appropriate device cart name in the column created in step c above. This will be something like "History101Cart," and should match an individual in your **Apple Education > Shared Device Carts** tab.

    f. Save the CSV file and close it.

3. Navigate to **Devices & Users > Device Enrollment** and, in the row of your Device Enrollment account, select the number link in the **Enrollment Profiles** column. The list of enrollment profiles for your Apple School Manager account displays.

4. Select an existing profile that is a "multi-user" profile and then select **Actions >Assign Devices to Profile**.

5. In the Assign Devices to Profile dialog box, click **Upload** and choose the CSV file you created above and then click **Assign**. The devices will be assigned to this enrollment profile with the appropriate individuals pre-assigned to the devices.

When you assign your Apple School Manager devices to your Apple Device Enrollment profile using the modified CSV file, Ivanti EPMM automatically assigns the custom attribute (and its value) to each device upon registration.

The above steps can be done multiple times and can include partial lists of serial numbers. Only serial numbers in the uploaded CSV file will be edited. If you wish to remove a custom attribute for a particular device, upload the file with the column name of the custom attribute and leave the value blank.

Note the following:

- If you assign a device cart to a device that was not registered with a multi-user device enrollment profile, the device will be configured incorrectly and will not function as a Shared iPad.

- Ivanti EPMM will reject a CSV file that has invalid serial numbers, invalid custom attribute column names, or has invalid CSV syntax.

What happens on the device

Ivanti EPMM sends the Apple Device Enrollment profile to the relevant devices. When the device is in setup mode, the device will be prompted to apply the configuration and be given a login to the MDM enrollment.

Related topics

For details about creating the custom attribute, see "Creating a custom attribute to use with Apple School Manager" on page 184.

Connecting Ivanti EPMM to Apple School Manager

Add your Apple School Manager account to Ivanti EPMM on the Apple Device Enrollment page.

You can use a previously created Apple Device Enrollment account for with Apple Education, regardless of whether that Device Enrollment account was originally associated with Apple School Manager. Whatever Apple Device Enrollment account you use must be associated with Apple School Manager so that it successfully retrieves Apple School Manager data. You can associate an Apple Device Enrollment account when you contact Apple to create your Apple School Manager account.

Before you begin

- Make sure you have added your school information to your Apple School Manager account. For details, see "Adding school information to your Apple School Manager account" on page 177.

- "Configuring devices in bulk for Apple School Manager" on page 178

Procedure

1. Log in to your Apple School Manager account.

2. Navigate to the **MDM Servers** page on the Apple School Manager portal.

3. Click **Add MDM server** link on the lower right.

4. In the dialog box that opens, enter a name for your Ivanti EPMM server.

5. Switch to another browser window, and open the Admin Portal.

6. In the Admin Portal, select **Devices & Users > Apple Device Enrollment**

7. Click **Add+**.

8. In the **Add Account** window, click **Download Certificate**.

   A file type called .CRT is downloaded to the file system.

9. Switch back to the Apple School Manager portal.

10. Under **Upload Your Public Key**, click **Upload File**, and browse for the .CRT file you downloaded from Ivanti EPMM.

11. Click **Save MDM Server**.

12. The Apple School Manager portal prompts you to download a server token file. Download the server token file.

13. In Ivanti EPMM, **Devices & Users > Apple Device Enrollment** dialog box, click **Browse** next to the **Server Token** field.

14. Select the .P7M file you downloaded from the Apple School Manager portal.

15. Click **Open**.

16. Click **Save**.

   Ivanti EPMM displays a summary of the MDM server you added.

Next steps

"Creating an Apple Device Enrollment Profile" on page 150. If you plan to return to this page, please mark your location or open this link in a new window.

"Adding your enrolled devices to your MDM server" below.

Adding your enrolled devices to your MDM server

After completing your Device Enrollment, you must add devices to your MDM server.

Before you begin

Complete the procedure in "Creating an Apple Device Enrollment profile for Apple School Manager" on page 146.

Procedure

1. Log in to the Apple School Manager portal.

2. Select **Devices** > **Device Assignments**.

3. On the **Manage Devices** page, select the method by which you want to add devices, and take action accordingly.

Choose Devices By...	Description
Serial Number	Enter one or more comma-separated serial numbers for the devices you want to assign.
Order Number Choose an order	• Click the **Order Number** radio button. • Select a specific order number from the **Choose an order** drop-down list. • A list of devices purchased with that order number displays.
Upload CSV File	• Click the **Upload CSV File** radio button. • Click the **Choose File** link to select a CSV file you created for the devices you want to assign.

4. Select **Assign to Server**.

5. From the **Choose MDM Server** drop-down list, select your instance of Ivanti EPMM.

6. Click **Done**.

   The devices are assigned.

7. Switch to the Ivanti EPMM Admin Portal.

8. Select **Devices & Users** > **Apple Device Enrollment**.

9. Click **Check for Updates**.

   Ivanti EPMM retrieves the new devices.

Related topics

For more information, see the [Apple School Manager User Guide](#) on the Apple website. A login is required.

Next steps

  ["Enabling Apple Education in Ivanti EPMM " on the next page](#)

Creating a custom attribute to use with Apple School Manager

> ℹ️ This step is optional, as you can create the custom attribute when you turn on the Apple Education feature, as described in ["Enabling Apple Education in Ivanti EPMM " on the next page](#). If you prefer to create your own custom attribute when enabling Apple Education, skip this procedure and continue on to ["Enabling Apple Education in Ivanti EPMM " on the next page](#).

Apple Education requires the creation of custom attributes so that devices can be assigned to either an individual (teacher or student) or to a device cart. Each device can be either a teacher device, student device, or multi-user student device (shared iPad.) These education roles are determined by the values entered into the custom attributes on a device.

> ℹ️ You can have a total of 300 custom attributes in Ivanti EPMM.

When using Apple Education, there are two custom attributes used to determine the above education roles. The first custom attribute is used to link a device to an individual. These devices are called 1:1 (one to one) devices and are linked via the Managed Apple ID as shown in Apple School Manager and in the Apple Education "Classes" tab. The second custom attribute is optional and is only used if you want to enable the use of Shared iPad devices. This custom attribute is the device cart name and it is what is used to link the device to the device cart.

You can setup these custom attributes prior to enabling Apple Education in Ivanti EPMM in order to help organize existing teacher / student 1:1 devices. Devices in device carts will need to be wiped and restarted after enabling Apple Education in Ivanti EPMM. Once that is done, you can set up the device carts and Multi-user Device Enrollment Profiles.

It is not advisable to have a custom attribute value that has a Managed Apple ID associated to both a teacher *and* a student. It will result in the device being associated to an Apple Education role of Teacher. If Ivanti EPMM has insufficient data to associate a device with a relevant class, then the Apple Education role for that device is None.

ⓘ Devices with an Apple Education role of None will not receive a valid Apple Education role, which precludes these devices from participating in Classroom app activities.

Before you begin

Complete the procedure in .

Procedure

- Follow the procedure for adding a device custom attribute in .

- Assign your custom attribute the value type string.

Enabling Apple Education in Ivanti EPMM

When you enable Apple Education in Ivanti EPMM, the following occurs:

- Ivanti EPMM creates components required to synchronize with Apple School Manager, such as a certificate enrollment profile. Creating an Apple enrollment device profile makes it easier to manage Apple School Manager devices.

- You select a previously created custom attribute or create a new custom attribute to correlate the devices in Ivanti EPMM with the devices in your Apple School Manager account. The custom attribute matches the Managed Apple ID assigned to each user in Apple School Manager or device cart, and must be of type string.

- Ivanti EPMM checks existing devices for values in the defined custom attribute column, and associates relevant devices with courses from the synchronized Apple School Manager data.

- Ivanti EPMM evaluates devices to determine whether the devices have a value for the custom attribute you created. Values should match either the Managed Apple ID for that device or the device cart name for shared iPad devices.

When enabling Apple Education for the first time, Ivanti EPMM creates the following entities:

- 2 local certificate authorities (CA)

- 2 certificate enrollments

- 1 Apple Education configuration (only one auto-generated Apple Education configuration can exist in Ivanti EPMM)

- 1 label: All Education

> **ⓘ** Ivanti, Inc does not recommend editing the certificate enrollment settings and the local CAs. There is no need to apply labels to these automatically-created settings, as Ivanti EPMM automatically applies the "All Education" label to them.

Before you begin

- Be sure to read "Apple School Manager account management overview" on page 172.

- Create the Apple Device Enrollment account. See "Connecting Ivanti EPMM to Apple School Manager" on page 181.

- Complete the procedure in "Adding your enrolled devices to your MDM server" on page 183.

- (Optional) Complete the procedure in "Creating a custom attribute to use with Apple School Manager" on page 184.

- When using Apple School Manager, Ivanti EPMM supports supervised iPad devices running iOS 9.3 or supported newer versions. See "Apple School Manager device requirements" on page 174.

> **ⓘ** **IMPORTANT:** Before devices are registered with Ivanti EPMM, ensure that the devices are associated either to a Managed AppleID or to a device cart. See <add link to Shared devices cart>

In Apple Education, there are three types of device users. Each device used in Apple School Manager must be mapped to one of these device user types:

- Teacher using 1 device (1:1)

  - Teacher iPad devices are required to be assigned directly to the teacher. This assignment is done through setting the teachers' device's custom attribute for the managed Apple ID to the teachers' Managed Apple ID.

  - Example scenario of Teacher 1:1 device usage: At the beginning of class, the teacher will open the Classroom app and start the class enabling the teacher to see all the students' activity.

- Student using 1 device (1:1)

  - One student gets an iPad device. This iPad device is associated to a Managed Apple ID. After this device has been associated to classes, the device is ready for use.

  - Example scenario of Student 1:1 device usage: At the beginning of the school session, a student is assigned an iPad device for use in classes. This iPad is associated to their Managed Apple ID through the Apple Education's Managed Apple ID custom attribute for that device. This device will stay with the student throughout the school session.

- Students sharing a device (multi-user)

  - Two students share the same iPad and that iPad is associated to a device cart. If a device belongs to a student or a teacher, do not select this field.

  - Example scenarios of shared devices cart usage:One device cart will be associated to Room 32 in a local high school. There are 15 iPad devices associated to that device cart. Throughout the day, Room 32 cycles through a History class and an English class. At the beginning of the History class, one student picks up an iPad, logs in using a Managed Apple ID and uses it during the class time. At the end of History, the student returns the iPad devices to the device cart. When English class starts a student picks up an iPad, logs in using a Managed Apple ID and uses it during class. At the end of class, the student returns it to the device cart.

Procedure

1. Select **Devices & Users** > **Apple Education**.
   A toggle button on the page reads **Off**.

2. Select the toggle button to enable Apple Education. The toggle now reads **On**.

3. Enter the information listed in the table below.

4. Select **Save**.

A sync to the Apple Education data located in the Apple School Manager begins and the data (classes, individuals, shared device carts, etc.) downloads into Apple Education. The "Sync Status" field at the top of the Apple Education page displays the status of the sync. The page automatically refreshes and reloads.

Once the sync is done, you can view your courses in Apple Education and begin managing them.

TABLE 1. APPLE EDUCATION ACCOUNT ENTRIES

Item	Description
Apple Device Enrollment Account	Select the drop-down list and select the Apple Device Enrollment account. ℹ️ Make sure to select only an Apple Device Enrollment account associated with Apple School Manager.
Custom Attributes	Select the custom attribute you created to map devices enrolled in Apple School Manager. You can have a total of 300 custom attributes in Ivanti EPMM. • **Managed Apple ID Attribute Name** - (Required) Use this field for 1:1 devices, which can be teachers or students. Select from the drop-down or enter a name that you have determined use when configuring the custom attribute for the device. This will link the device to the individual user. An example of a Managed Apple ID Attribute Name would be `AppleEduID`. Teachers can only be 1:1 devices whereas students can either be 1:1 or multi-user. One device can belong to only one individual and that connection using custom attributes is associated to the name of the attribute you enter here. • **Shared Device Cart Attribute Name**- (Optional) This custom attribute is used to create a mapping between a device and a cart. Enter a name that you will use to assign devices to specific device cart via custom attributes or select the custom attribute name you created. If a shared device cart name is not entered, the device cart tab and links in Apple Education are not shown. One shared device can belong to only one device cart and that connection using custom attributes is associated to the name of the attribute you enter here. An example of a Shared Device Cart Attribute Name would be `DeviceCart`. The Shared Device Cart Attribute Name must be different from the Managed Apple ID Attribute Name.
Restrictions	**Shared Observation Modification Control**– • Not selecting this check box allows the device user privacy, as per the General Data Protection Regulation (GDPR) in Europe.

Item	Description
	• If you want to allow the teacher to remotely control the students' screens, select this check box. Once selected, this check box cannot be disabled.

Related topics

- For details about assigning a custom attribute to Apple School Manager devices later in bulk, see "Configuring devices in bulk for Apple School Manager" on page 178.

- For more information about Shared Device Cart, see <Configuring Shared Device Cart>.

Creating labels for Apple Education

Labels can be assigned to a class, location, course, or type of device. Use the Apple Education labels to assign apps and configurations, like WiFi and Restrictions. For example, you may decide to have a Label for each location's WiFi. Or you may have the WiFi configuration based on location and type of device, as Teachers may be able to access more hosts than students. In addition, you will want to have a teacher label and assign that label to the Classroom App.

Procedure

1. Select on **Devices & Users > Devices**.

2. Select **Advanced Search**.
   The Advanced Search dialog box expands.

3. Select the drop-down arrow and expand Apple Education.

4. Use these guidelines in the table below to complete your search criteria using the query builder or by manually editing the expression.

5. Select **Save to label**.

6. Type a name and description for the new label.

7. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then select **Confirm**. For more information, see "Best practices: label management" on page 860.

TABLE 2. SEARCH CRITERIA GUIDELINES

Field	Description	Example
Apple Education Enabled	Enter a unique name that clearly identifies the purpose of the label.	"apple_education.apple_education_in_use" = true
Class ID	Enter the unique class ID. An example, class ID could be: `02015a85-2815-4939-b6e0-b29334cad952`	"apple_education.class_id" starts with "02015a"
Course ID	Enter the unique course ID, for example, a history class that runs June 2018.	"apple_education.course_id" starts with "CA12@314"
Location ID	Enter the unique location ID. You are assigned one location for your Apple School Manager account. Through the Apple School Manager portal, you can add additional locations.	"apple_education.location_id" = " [CA12@314]"
Apple Education Role	Enter the unique teacher's ID name / number.	Common uses: "apple_education.role" equals "Teacher" "apple_education.role" equals "Student" "apple_education.role" equals "Student (MultiUser)" "apple_education.role" starts with "Student"

Configuring Shared Device Cart

When Apple Education is enabled, the Shared Device Carts tab is populated with all the potential device carts based on the unique values stored in the custom attributes for the device cart. From this tab, an administrator can select one or more device carts and assign them to a class.

It is very important that before devices are turned on, you have **all Shared iPad devices** associated to a device cart. You want all the profiles to be ready for the device before logging into the device. Once a device is logged into using an Apple ID, all the relevant course information will be downloaded onto the device.

Procedure

1. Select **Shared Device Cart** tab.

2. The tab displays four columns:

Field	Description
Device Cart	Selecting on the name of the Device Cart allows you to re-name the device cart.
Classes	The number of classes associated to the device cart displays. Selecting on the number opens the Class List dialog box. When finished viewing the class information, select **OK**.
Registered Devices	Selecting on **View Devices** opens the Device List dialog box. When finished viewing the device information, select **OK**.
Actions	Selecting on the X in the relevant Action row deletes the Device Cart. You will get a confirmation prompt.

3. Select **Add New Device Cart**.
   The Add New Device Cart dialog box opens.

4. Enter a name into the **Device Cart Name** field and then select **Add**.
   The new name displays in the Shared Device Carts tab.

Be aware of making changes to Shared Device Carts during school hours. Changing device carts, classes and associations will cause profiles to be re-evaluated and pushed to the devices. This can cause the devices to be slow. It is advised that you make chages during after school hours or on weekends.

Next steps

Proceed to "Applying a device cart to a class" below.

Related topics

For multi-users in shared device carts, it is useful to upload a CSV file with all the devices pre-assigned to a device cart into a Apple Device Enrollment profile. For more information, see "Configuring devices in bulk for Apple School Manager" on page 178.

Applying a device cart to a class

Applying a class to a device cart displays a new class dialog list.

- In Shared iPad device mode, the iPad device cannot be reset/erased by the end user. To reset the device, send the Wipe command to the device. Then on the device, login with any Managed Apple ID that is part of that EDU account. When the device is logged in, it will get the Wipe MDM command. DO NOT retire the device until it has been reported as wiped and is no longer in "Wipe Pending" state.
- If you toggle Apple Education to OFF, the students' names, device carts, class information, etc., will be deleted. The custom attributes and device values will remain.

> ⓘ The class list is search-able and sortable. A class requires students and teachers at minimum. Classes without a student or teacher should not be assigned to device carts as that will cause invalid configurations.

Procedure

1. Select the **Shared Device Carts** tab.

2. Select a cart and then select **Apply to Classes**.
   The Apply Cart to Classes dialog box opens.

   > ⓘ **TIP:** To view the classes that are already in the cart, select on the **Selected** tab.

3. In the **All** tab, select the class(es) you want to associate to that device cart and then select **Apply**.

4. To remove a class, select **Remove from Classes**.
   The Remove Cart from Classes dialog box opens.

5. Selecting the box next to the Class Name field selects all classes. Alternately, select the individual classes you want to remove.

6. Select **Remove**.

7. Repeat steps if you want to remove additional classes from a Device Cart.

8. Once you have all your devices mapped, select on the **Sync** button or wait for the automiatic sync. Ivanti EPMM automatically syncs every 24 hours (since the last scheduled sync.)

Synchronizing Ivanti EPMM with Apple Education servers

Synchronizing Ivanti EPMM with Apple Education servers allows you to view the most recent information in your Apple Education account. Ivanti EPMM synchronizes with Apple School Manager daily. This option is available to synchronize on demand as needed.

The Last Sync time stamp indicates the last time and date Ivanti EPMM synchronized Apple Education data. **Sync Status** indicates the synchronization progress, success, or failure.

> ℹ️ Synchronizing with Apple Education servers can take some time.

Before you begin

Complete the procedure in "Enabling Apple Education in Ivanti EPMM " on page 185

Procedure

1. Select **Devices & Users** > **Apple Education**. The Apple Education page displays.

2. Under Apple Education, select the **Sync** button.

   When Ivanti EPMM has completed the synchronization attempt, the Sync Status indicates whether the synchronization was successful.

3. Optionally, select the status to view more information about the status of the synchronization.

   For example, if the synchronization failed, select **Failed**. A pop-up window is displayed, indicating that the synchronization with Apple School Manager failed, the error that caused the failure, and the time stamp of when the synchronization attempt began.

4. If the sync fails, select **Sync** again.

   Alternatively, wait for Ivanti EPMM to automatically sync with Apple School Manager servers. Ivanti EPMM attempts to sync with Apple School Manager every 24 hours.

What happens in Ivanti EPMM

After synchronizing with Apple School Manager, you can see the complete list of individuals, classes, locations, and so on, including the role of the individual, such as teacher or student. Ivanti EPMM extrapolates roles based on class and individual information, which includes course, location, teacher, and students.

To view the number of teachers and students:

- Select **Policies & Configs** > **Configurations** > **System - Apple Education Configuration**.
- Select **Details** to view the number of teachers and students.

What happens on the device

If the device has a value for the Managed Apple ID custom attribute and that ID is not associated to a class (as either a student or teacher), Ivanti EPMM shows a value of none for the Role column in the table of Apple School Manager data. In this case, that device shows an error for the Apple Education configuration.

If a class lacks a teacher or students, then Ivanti EPMM shows an error indicating that the configuration is not set.

Distributing apps to Apple School Manager devices

You can distribute apps to teachers and students. The simplest way to do this is to use Apple Licenses and a label for teachers and students. Typically, you would distribute the Classroom app to teachers, and other apps to students. You will need to apply device-based Apple licenses to the iOS apps you distribute to Apple School Manager devices.

> ℹ️ Using a device-based Apple License allows Apple School Manager users to install and use the iOS apps you distribute to them, regardless of the account they use on the device. By configuring any distributed apps to automatically install to the device after the device is registered to Ivanti EPMM, you ensure your users have the requisite apps.

> ℹ️ Shared iPad logged-in users are not allowed to install apps via the Apple App Store and are required to be installed through MDM.

Before you begin

- You need to set up Apple Licenses on Ivanti EPMM before distributing iOS apps to Apple School Manager devices. For more information, see "Importing licensed apps from Apple Licenses account" in the *Ivanti EPMM Apps@Work Guide*.

- Complete the procedure in "Synchronizing Ivanti EPMM with Apple Education servers" on page 192.

Procedure

> ℹ️ For detailed instructions on adding importing apps for use in Apple Education, see the "Using the wizard to import iOS apps from the Apple App Store" section in the *Ivanti EPMM Apps@Work Guide*.

1. In the Admin Portal, go to **Apps > App Catalog**.

2. Select **Add+**.

3. Select **iTunes.**

4. Search for the app by name, for example enter Classroom to search for the Classroom app.

5. Select the app and then select **Next**.

6. Enter the basic information into the screen. The Application Name and Min. OS Version fields are read-only.

7. Select **Next**.

8. Select **Send convert unmanaged to managed app request on device registration or sign-in (iOS 9 or later)** so that after device registration is complete, the device user is prompted to install this app. If the app is already installed as an unmanaged app, the app will be converted to a managed app.

9. Select **Enforce conversion from unmanaged to managed app (iOS 9 or later)** to allow the app to be converted from an unmanaged app to a managed app in Apps@Work on devices running iOS 9 through the most recently released version supported by Ivanti, Inc. The unmanaged app will not require uninstall, as it will be converted directly to a managed app.

10. Select **Finish**.

   The app displays in the **App Catalog**.

11. Repeat the preceding steps for any student apps you want to distribute to student devices.

12. Create two labels, one for teachers, and one for students.

   a. Go to **Device & Users > Labels** and select **Add Label**.

   b. Enter a unique name for the label, such as `teachers` or `students`.

   c. For the label type, select **Filter**.

   d. In the **Criteria** field, enter a search expression for the label.

      For the teachers label, enter: `"apple_education.role = "teacher"`

      For the students label, enter: `"apple_education.role = "student"`

   e. Select **Save**.

   f. Repeat these steps so that you have one label for teachers and one label for students.

13. Apply a device-based Apple license to the app or apps.

    a. Select **Apps > App Catalog**.

    b. Use the check box to select the app or apps to which to apply Apple License device-based licensing.

    c. Select **Manage Licenses** from the **Actions** menu.

    d. In the License Summary page, select the desired license account.

    e. In the Account Details page, expand **License Type**, select **Device-based License**, and then select **Save**.

    f. Expand **License Label Management** and select the desired labels so that target devices that request the selected app receive device-based Apple licenses. This applies to devices running iOS 9.0 or supported newer versions.

14. Apply the apps to the relevant labels.

    a. Select **Apps** > **Apps Catalog**, and check the box next to the Classroom app.

    b. Select **Actions** > **Apply to Labels**.

    c. Select the teachers label you created and select **Apply**.

    d. Repeat these steps with the students label, and any apps you want to distribute to students.

Disabling Apple Education in Ivanti EPMM

When disabling Apple Education in Ivanti EPMM, Ivanti EPMM deletes all Apple School Manager data from its database, including:

- Apple Education entities, such as courses, classes, teachers, and students

- Certificate policies

Ivanti EPMM does **not** delete:

- Labels associated with Apple School Manager

- Assignments

- Custom attributes

- Local CAs and certificates

Before you begin

Before disabling Apple Education in Ivanti EPMM, you must do the following:

1. Retrieve all Apple School Manager devices.

2. Make sure no devices are in lost mode.

3. Wipe all Apple School Manager devices.

4. Retire all Apple School Manager devices from Ivanti EPMM.

Procedure

1. Select **Devices & Users** > **Apple Education**.

   A toggle button on the page reads **On**.

2. Select the toggle button to disable Apple Education.

   Ivanti EPMM shows a warning message.

3. Select Disable Apple Education.

   The toggle now reads **Off**.

Related topics

- For details about wiping a device, see "Wipe" on page 103.

- For details about retiring devices, see "Retiring Devices" in the *Getting Started with Ivanti EPMM*.

Checking Apple Education logs

You can check the audit logs in Ivanti EPMM for the status of actions related to Apple Education.

You can check the following filters to view the status of actions related to Apple Education:

- Disable iOS Education

- Enable iOS Education

- Sync iOS Education with ASM

Procedure

1. Select **Logs** > **Audit Logs**.

2. From the filters on the left, expand **DEP**.

3. Select any or all of the filters related to Apple Education:

   - Disable iOS Education

   - Enable iOS Education

   - Sync iOS Education with ASM

4. Select **Search**.

   Ivanti EPMM shows any actions related to the filters you select, including the following details:

   - Action

   - State

   - Performed by

   - Action Date

   - Completed At

   - Performed On

   - Details

Shared iPad delete user session

Administrators can select the list of users on the shared iPad and then delete the session for all device users on that shared iPad. The delete user option frees up the allocated space that is no longer required.

Administrators can also select individual device users and end their session by clicking the **Log Out** link.

All delete commands are recorded in the device logs.

Deleting logged-in users' from shared iPad device

You can delete a user or multiple user accounts on the shared iPad devices. In the Users tab, the Active column displays currently logged in users. The delete option is not applicable for currently logged in users on the shared iPad device.

Procedure

1. In the Admin Portal, go to **Devices & Users > Devices**.
2. Select a shared iPad device to display the Device Details and then click on the **Users** tab. A list of managed Apple ID users currently logged into the shared device displays.
3. To end the shared iPad session for all logged-in users, click the **Delete All** button.
4. A confirmation dialog box displays. You can select either or both options:

   - **Require Network Tether -**- If selected, the device will not perform the action unless it is network-tethered.

   - **Force Delete regardless of iCloud data upload** - If selected, any information on the device not yet uploaded to iCloud will be lost.

5. Select **I Accept** to confirm logging out all logged in shared iPad users.
6. Click **Delete**.

Logging out user from shared iPad device

The administrator can select and force log out a user on a shared iPad device. A shared iPad user, must be logged out first; logged out users are indicated with a "-" minus icon in the Actions column.

1. In the Device Details page, click on the **Users** tab.
2. In the Actions column of the user you want to log out, click the **Log Out** link.
3. A confirmation dialog box displays. You can select either or both options:

   - **Require Network Tether** -If selected, the device will not perform the action unless it is network-tethered.

   - **Force Delete regardless of iCloud data upload** - Selecting this means any information on the device not yet uploaded to iCloud will be lost.

4. Click **Logout**.

Retiring Shared iPad devices

Wipe the device prior to retiring the device. Once you retire a device, the MDM profile is removed and the Admin cannot make remote MDM commands or changes. This leaves the Shared iPad without MDM and the device user cannot erase or reset the device since it's Shared iPad. If this happens, The only way to erase or reset the Shared iPad device once is to connect to Apple Configurator and select the **Allow Erase All Content and Settings (supervised devices only)** option.

Managing Apple Business Manager

This section addresses Apple Business Manager.

- "Implementing User Enrollment with Apple Business Manager" below

- "Shared iPad devices with Apple Business Manager" on page 205
- "Connecting Ivanti EPMM to Apple Business Manager " on page 209

Implementing User Enrollment with Apple Business Manager

Apple Business Manager is a place for IT teams to automate device deployment, purchase and distribute content, and manage roles in their organizations. Apple Business Manager implements User Enrollment - a modified version of the MDM protocol with a much greater focus on user privacy, implemented with a level of security that enterprises need.

User Enrollment allows the administrator to:

- Install and remove managed applications

- Install and remove network configurations

- Install a partial VPN scoped to managed apps and accounts

- Require the usage of a password

User Enrollment registration is supported on Mobile@Work. When the administrator assigns the device user to User Enrollment mode, the In-App registration will download the User Enrollment Profile to the device.

User Enrollment applies to unsupervised devices with iOS 13.0 or supported newer versions. Devices lower than iOS 13.0 will be considered "device enrollment" regardless if the device user has been enabled for User Enrollment. User Enrollment utilizes the user's managed Apple ID, which is required and associated with all enterprise apps and data on the device and in Ivanti EPMM.

Difference between standard MDM enrollment and User Enrollment

This section addresses the difference between standard MDM enrollment and User Enrollment with Apple Business Manager.

Standard MDM enrollment

Below is what an Ivanti EPMM server can do in a standard MDM enrollment, but will not be able to do in User Enrollment mode in iOS 13.0.

The MDM server:

- Cannot erase the device.

- Does not see the personal apps the device user has installed on the device.

- Cannot convert user-installed apps into MDM-managed apps.

- Cannot clear the device passcode (i.e. unlock the device).

- Cannot set a long, complex device passcode requirement.

- Cannot configure a device-wide VPN or Wi-Fi proxy, nor can it do any management of the cellular functionality.

- Cannot see device identifiers like the UDID, serial number, or IMEI.

- Cannot apply many device-wide restrictions (such as restricting the app content rating), block iCloud, and apply any the supervised restrictions.

ℹ️ When retiring and re-registering devices from Ivanti EPMM, devices are registered as Standard MDM.

User Enrollment with Apple Business Manager

In User Enrollment, the MDM server can still do everything needed to manage enterprise apps, accounts, and data.

User Enrollment can:

- Install in-house apps or apps via user-based (Apple) Apps & Books licenses

- Enforce passcode payload settings:

  - allowSimple = false

  - forcePIN = true

  - minLength = 6

- Query data related to enterprise-managed apps, certificates, and profiles

- Configure a per-app VPN for apps, mail, contacts, and calendars that have been installed by MDM

- Enforce some restrictions, like managed open in, managed contacts, managed data on the lock screen, and several others

Enterprise data is stored in a separate Apple File System (APFS) volume, which is created at enrollment, and encrypted separately from device user data. This volume contains data stored by managed apps; enterprise Notes; enterprise iCloud Drive docs; enterprise Keychain entries; managed mail attachments and bodies; and calendar attachments. Un-enrolling from MDM destroys the volume and the keys.

The final requirement of User Enrollment is the user's managed Apple ID that must be associated with all enterprise apps and data on the device and in iCloud Drive. Managed Apple IDs were first utilized by Apple School Manager and are now utilized by Apple Business Manager for User Enrollment.

All third-party apps can only be either a personal app or a managed app through Ivanti EPMM. The MDM service cannot start managing apps that the device user has already installed. In this case, the administrator will need to request the device user to delete the personal app before installing the app through MDM. The MDM service cannot start managing apps that the user has already installed. However, some system apps like Notes and Files will support both work and personal accounts.

Difference between User Enrollment vs Device Enrollment

This section covers the difference between User Enrollment and device enrollment. User Enrollment applies to devices iOS 13.0 and macOS 10.15 or supported newer versions.

Devices lower than iOS 13.0 will be considered "device enrollment" regardless if the device user has been enabled for User Enrollment.

> ℹ️ User Enrollment for Apple Business Manager does not allow for wipe or unlock. However, the user portal will still have those options available even though they will not work.

TABLE 16. USER ENROLLMENT VS DEVICE ENROLLMENT

Functionality	User Enrollment	MAM	Device Enrollment	DEP
Erase the device and see user's personal apps	No	No	Yes	Yes
Convert managed to unmanaged or vice versa	No	No	Yes	Yes
Clear device passcode, configure device-wide VPN or Wi-Fi proxy nor manage cellular functionality	No	No	Yes	Yes
See device identifiers like serial number, IMEI	No	No	Yes	Yes
Apply supervised restrictions	No	No	Yes*	Yes
Can install and configure apps and accounts	Yes	Yes	Yes	Yes
Can configure a per-app VPN for apps, mail, contacts, and calendars that have been installed by MDM	Yes	No	Yes	Yes
Can enforce some restrictions, like managed open in, managed contacts, managed data on the lock screen, and several others	Yes	No	Yes	Yes
Can query data related to enterprise-managed apps, certificates, and profiles	Yes	No	Yes	Yes

> The "Apply supervised restrictions option" will work for Device Enrollment if the device is supervised using Apple Configurator, otherwise it is unsupported.

Requirements for enabling User Enrollment

Below are the requirements for enabling User Enrollment:

- An Apple Business Manager account

- Managed Apple ID - Managed Apple ID to be associated with each enrolled device. This Managed Apple ID provides authentication for MDM management and app licensing. When the MDM pushes down apps and media, necessary Apple licenses are assigned to the Managed Apple ID associated with the device.

- Device users who are synced to LDAP are to be assigned to a device management role and associated with a Managed Apple ID.

- For LDAP User / Group enrollment for single or bulk registrations, verify the managed Apple ID was generated correctly.

- If the existing registration process is already using PINs, the registration will still work.

- After registration, check the logs for any managed Apple ID failures.

Shared iPad devices with Apple Business Manager

This section addresses enabling shared iPads with Apple Business Manager.

Overview

If you have an Apple Business Manager account loaded in Ivanti EPMM, you can enable Shared iPad devices between multiple employees. This allows organizations to share devices between multiple employees. Employees can sign in using a Managed Apple ID and access their custom profile with Mail accounts, files, app data, etc. The data is stored in iCloud, allowing the employee to log into any Shared iPad.

A sample case study for using Shared iPad devices for Apple Business Manager is in the healthcare industry, where a doctor and nurses can share one device.

Admins of Shared iPad devices can manually create accounts, Managed Apple IDs and passwords and federate to an identity provider like Azure Active Directory.

If Admins installs an app for Shared iPad devices, all users will have that app. Apps for Shared iPad devices are loaded through registration for Apple-licensed apps. You must have the **Send Installation Request on device registration or sign in** selected in the AppCatalog.

Requirements for Shared iPad devices for Apple Business Manager

Below are the requirements for enabling Shared iPad devices:

- An Apple Business Manager account
- Managed Apple ID - Managed Apple ID to be associated with each enrolled device. This Managed Apple ID provides authentication for MDM management and app licensing. When the MDM pushes down apps and media, necessary Apple licenses are assigned to the Managed Apple ID associated with the device. Admins can manually create these accounts or federate to an identity provider like Azure Active Directory.
- Shared iPad devices must have at least 32 GB of storage and be supervised.

Enabling Shared iPad devices for Apple Business Manager

There is only one step for enabling Shared iPad devices:

1. Add an Enrollment Profile and set the sessions for Shared iPad devices. See "Creating an Apple Enrollment profile for Apple Business Manager" on the next page

Shared iPad supported configurations

1. Below are the supported configurations. If these configurations are to be pushed per Shared iPad device user, then you need to create or edit existing configurations to have $MANAGED_APPLE_ID$. You should have already created Managed Apple ID in Apple Business Manager for each Shared iPad device user and also created a separate account for each of the below configurations.
   - CalDAV
   - CardDAV
   - Google Account
   - Subscribed Calendars
   - Exchange
   - Email
   - Managed App Configuration

   > $MANAGED_APPLE_ID$ is also used in a user enrollment scenario, not to be confused with the Shared iPad device scenario.

For more information, see:

- "CalDAV settings (iOS and macOS)" on page 705
- "Supported variables for CardDAV Settings" on page 708
- "Exchange settings" on page 370
- "Creating an Exchange setting for per message S/MIME encryption" on page 389
- "Supported variables" on page 382
- "Substitution variables for compliance policy rules" on page 358
- "Setting up your Exchange setting for access to Google Apps data" on page 399
- "Google Account " on page 761
- "Subscribed Calendars settings" on page 746

2. If you are creating new configurations, add label support for Shared iPad devices. See Managing Labels in *Getting Started with Ivanti EPMM*.

3. MANAGED_APPLE_ID is the only substitution variable that changes in iPad sharing when a device user logs in. (Other device substitution variables can still be used, but it does not denote a device user) If you updated any configurations with user substitution variable $MANAGED_APPLE_ID$, push the configuration. The user substitution will only push on the user channel for Shared iPad devices.

4. Once the Shared iPad device user logs in, the Shared iPad settings display in the Device Details page. You can also search on specific Shared iPad fields, see "Advanced searching " on page 57 for more information.

Creating an Apple Enrollment profile for Apple Business Manager

See "Creating an Apple Device Enrollment Profile" on page 150. Make sure to mark you place here so you can return for the next step if needed.

Retiring Shared iPad devices

Wipe the device prior to retiring the device. Once you retire a device, the MDM profile is removed and the Admin cannot make remote MDM commands or changes. This leaves the Shared iPad without MDM and the device user cannot erase or reset the device since it's Shared iPad. If this happens, The only way to erase or reset the Shared iPad device once is to connect to Apple Configurator and select the **Allow Erase All Content and Settings (supervised devices only)** option.

Related topics

Shared iPad delete user session

Administrators can select the list of users on the shared iPad and then delete the session for all device users on that shared iPad. The delete user option frees up the allocated space that is no longer required.

Administrators can also select individual device users and end their session by clicking the **Log Out** link.

All delete commands are recorded in the device logs.

Deleting logged-in users' from shared iPad device

You can delete a user or multiple user accounts on the shared iPad devices. In the Users tab, the Active column displays currently logged in users. The delete option is not applicable for currently logged in users on the shared iPad device.

Procedure

1. In the Admin Portal, go to **Devices & Users > Devices**.
2. Select a shared iPad device to display the Device Details and then click on the **Users** tab. A list of managed Apple ID users currently logged into the shared device displays.
3. To end the shared iPad session for all logged-in users, click the **Delete All** button.
4. A confirmation dialog box displays. You can select either or both options:

   - **Require Network Tether -**- If selected, the device will not perform the action unless it is network-tethered.

   - **Force Delete regardless of iCloud data upload** - If selected, any information on the device not yet uploaded to iCloud will be lost.

5. Select **I Accept** to confirm logging out all logged in shared iPad users.
6. Click **Delete**.

Logging out user from shared iPad device

The administrator can select and force log out a user on a shared iPad device. A shared iPad user, must be logged out first; logged out users are indicated with a "-" minus icon in the Actions column.

1. In the Device Details page, click on the **Users** tab.

2. In the Actions column of the user you want to log out, click the **Log Out** link.

3. A confirmation dialog box displays. You can select either or both options:

   - **Require Network Tether** -If selected, the device will not perform the action unless it is network-tethered.

   - **Force Delete regardless of iCloud data upload** - Selecting this means any information on the device not yet uploaded to iCloud will be lost.

4. Click **Logout**.

Best practices for managing devices in Apple Business Manager

Following are some best practices to keep in mind for managing enrolled devices in Apple Business Manager:

- You can enroll devices in an Apple Device Enrollment you previously registered in Ivanti EPMM, as long as you wipe and retire the Shared iPad devices first.

- Use Apple Device Enrollment to purchase a large group of devices, which you can more easily manage in Ivanti EPMM.

- It is recommended to create one or more Locations for each Ivanti EPMM that you have. Additionally, it is recommended to not share the Locations ("Locations" in Apple Business Manager are the Apple Licenses.)

- It is recommended to have no more than 10 Apple License accounts total per Ivanti EPMM. The total includes both Apple School Manager and Apple Business Manager licenses.

- When using the $MANAGED_APPLE_ID$ substitution variable, it is best to update your Labels to only include devices that have a Managed Apple ID::

  - "ios.IsMultiUser" = true OR "ios.apple_user_enrolled_device" = true. This is applicable only for both Shared iPad and User Enrollment.

Connecting Ivanti EPMM to Apple Business Manager

This section covers enabling User Enrollment for Apple Business Manager:

1. "Manage MDM Settings" below

2. "Add the Server Token" on the next page

3. "Create users to enable User Enrollment for local users and LDAP users" on the next page

4. "Configure LDAP group members to inherit Apple User Enrollment Roles" on page 212

5. "Match the Location and the Account" on page 215

6. "Distribute apps to Apple Business Manager devices" on page 215

7. "Configuration settings for Apple Business Manager User Enrollment" on page 217

8. "Wi-Fi Policy for user-enrolled devices" on page 218

Once you have completed the above steps, then you can proceed to:

- "Device user instructions for registering using User Enrollment" on page 218

- "Using Logs for Troubleshooting" on page 219

- Retiring Shared iPad devices

For instructions on using Federated authentication, see the Apple Business Manager User Guide on the Apple website. A login is required.

Before you begin

- You must have an Apple Business Manager account. See business.apple.com.

Manage MDM Settings

You will need to make some settings on the MDM page.

Procedure

1. In the Admin Portal, select **Settings > iOS > MDM**.

2. Select the **Enable User Enrollment** check box and then select **Save**.

3. Check that your certificate is valid. If not valid, on the MDM page, select the **Install MDM Certificate** button.

The MDM Certificate Generation dialog box opens.

4. Select **Download Certificate Signing Request**.

5. Select **Upload MDM Certificate**.

   The Upload MDM Certificate dialog box opens.

6. Browse to the certificate, select it and then select **Upload Certificate**.

Add the Server Token

Download the server token from Apple Business Manager.

Procedure

1. Login to Apple Business Manager.

2. Select **Settings > Apps and Books**.

3. Download the server token for your location.

> ℹ️   The VPP token field accepts tokens of lengths up to 1024 characters.

Create users to enable User Enrollment for local users and LDAP users

This section covers creating local and LDAP users and setting the User Enrollment for unsupervised Apple devices. User Enrollment will not work on supervised devices or devices enrolled in Apple's Device Enrollment Program.

Procedure

1. In the Admin Portal, go to **Devices & Users > Users**.

2. Select **Add > Local New User**.

   Enter the new user information. For more information on how to create a user, see "Add New User window" in the *Getting Started with Ivanti EPMM*.

3. Select a user and select **Actions > Assign Roles**.

   The Assign Roles dialog box opens.

4. Select **Use Apple User Enrollment (For Apple unsupervised device only**).

   A text field displays.

5. Enter the **Managed Apple ID** for the user.

6. Select **Save**.

Configure LDAP group members to inherit Apple User Enrollment Roles

You can configure LDAP group members to inherit Apple User Enrollment roles. This gives all the users in that group the Apple User Enrollment setting.

Before you begin

Create your LDAP groups. For instructions, see "Configuring the set of LDAP groups" in *Getting Started with Ivanti EPMM*.

Procedure

1. In the **Devices & Users > Users** page, set the search criteria in the To field to: **LDAP Entries** and the Category field to: **Authorized LDAP Groups**. You can also choose different categories in your search.
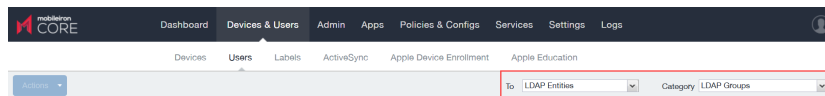
   The search results display in the Users page.

2. Select a group and select **Actions > Assign Role(s)**.

   The Assign Roles dialog box opens.

3. Select **Use Apple User Enrollment (For Apple unsupervised device only)** and add the email address for User Enrollment and Managed Apple ID. You can also use standard substitution variables, for example: $USERID$@ivanti.com. See the table below, Supported Substitution Variables for User Enrollment, for accepted options.

   > ℹ️ Substitution variables are allowed for use with LDAP Groups only and not for LDAP Users.

4. Select **Save**.

TABLE 17. SUPPORTED SUBSTITUTION VARIABLES FOR USER ENROLLMENT

Substitution variable	More information	Sample of substituted value
`$USERID$`	Login ID (email address format)	`jdoe@myCompany.com`
`$EMAIL$`	Email address	`jdoe@myCompany.com`
`$EMAIL_DOMAIN$`	The domain part of the email address (part after the '@')	`myCompany.com`
`$EMAIL_LOCAL$`	The local part of the email address (part before the '@')	`jdoe`
`$FIRST_NAME$`	First name	`Jane`
`$LAST_NAME$`	Last name	`Doe`
`$DISPLAY_NAME$`	Display name	`Jane Doe, CEO`

`$USER_DN$`	Distinguished Name	`CN=Jane Doe,`
		`OU=NA,OU=Users,`
		`OU=XY,`
		`DC=myCompany,`
		`DC=com`

`$USER_UPN$`	The Microsoft userPrincipalName attribute	`jdoe@myCompany.com`
`$USER_LOCALE$`	Locale	`en_US`
`$USER_CUSTOM1$`	Custom field defined for LDAP	The value of the variable as defined in LDAP settings.
`$USER_CUSTOM2$`	Custom field defined for LDAP	The value of the variable as defined in LDAP settings.
`$USER_CUSTOM3$`	Custom field defined for LDAP	The value of the variable as defined in LDAP settings.
`$USER_CUSTOM4$`	Custom field defined for LDAP	The value of the variable as defined in LDAP settings.
`$CN$`	Common Name (CN) attribute extracted from the distinguished name	`Jane Doe`
`$OU$`	Organizational Unit (OU) attribute extracted from the distinquished name	`XY`
`$SAM_ACCOUNT_NAME$`	The Microsoft sAMAccountName attribute	`jdoe`

TABLE 17. SUPPORTED SUBSTITUTION VARIABLES FOR USER ENROLLMENT (CONT.)

Substitution variable	More information	Sample of substituted value
`$REALM$`	The domain component of an LDAP entry	`mycompany.com`

Managing users that belong to multiple groups

If a device user belongs to multiple groups (or nested groups) and is assigned a managed Apple ID substitution variable for various groups, this means there are more than one option available for each user. Ivanti EPMM cannot determine which option to use. This results in Ivanti EPMM creating an audit log entry (Logs > Audit Logs > filter by Managed Apple ID) with the error message: "More than one LDAP Group managed Apple ID option."

To resolve this, assign the concrete Managed Apple ID for the specific LDAP user by using the following instructions.

Procedure

1. Go to **Devices & Users > Users** page, set the following parameters:

   - To: **LDAP Entities**

   - Category: **LDAP users**

   - search for: your LDAP user

2. Select a user, select **Actions > Assign Role(s)**.

   The Assign Roles dialog box opens.

3. Select **Use Apple User Enrollment (For Apple unsupervised device only)** and add a unique email address for User Enrollment and Managed Apple ID.

   > Apple ID substitution variables are not valid for individual users or local users. Use a valid, managed Apple ID, for example, joesmith@ivanti.com.

4. Select **Save**.

Match the Location and the Account

In order for the User Enrollment to work in Ivanti EPMM, the Apple App License Account needs to be part of the same Apple Business Manager account. Within Apple Business Manager, if you have an account listed in Locations, you need to have an Apps and Books matched to the same location. You may need to add a new location (EXAMPLE: West Coast.)

> ℹ️ Apple may change their Apple Business Manager software without notice.

Procedure

If you have an Apple license account (VPP from Apple Business Manager) that is in the same Apple Business Manager account as the Managed Apple IDs that you will be using, you can skip steps 2 and 3.

1. Go to Apple Business Manager and log in.

2. In Apple Business Manager, go to **Settings > Apps and Books**.

3. Add a New Location, enter in the information and then select **Save**.

   > ℹ️ It may take several minutes for the new location to display.

4. Go to **Accounts** and search for the user name.

5. Select the user and select **Edit**.

6. Give the user **Content Manager** permissions for the (new) location, for example, West Coast.)

7. Sign out of Apple Business Manager to allow the permissions to take effect. It is recommended you wait several minutes before going to the next step.

8. Log into Apple Business Manager.

9. Go to **Locations** and confirm the new location is displaying.

Distribute apps to Apple Business Manager devices

You can search for iOS apps on the Apple App Store and add them to the App Catalog for distribution to Apple Business Manager devices. You can also add your own in-house apps for iOS and macOS.

For more information, see "Importing licensed apps from Apple Licenses account" in the *Ivanti EPMM Apps@Work Guide.*

> ℹ️ Apple User Enrolled devices will not report unmanaged apps and are unable to convert an unmanaged app to a managed app. Please adjust compliance actions accordingly.

Before you begin

Purchase your apps in Apple Business Manager.

Procedure

Now you need to import the apps you just purchased into Ivanti EPMM.

1. In the Admin Portal, go to **Apps > Apple Licenses**.

2. Select the account name and then select **Actions > Update licenses**.

   The Update licenses dialog box opens.

3. Select the applications you wish to import into Ivanti EPMM and then select **Import**. It may take a few minutes to import into Ivanti EPMM.

4. Go to **Apps > App Catalog** and import the apps.

5. Select a newly-imported app, for example, Ivanti Mobile@Work , and then select **Actions > Manage Licenses**.

   The License Summary page displays.

6. Select on the link of the license.

   The detailed license page displays.

7. In the License Label management section, select **Apply To labels**.

   The Apply to Labels dialog box opens.

8. Select the desired label and select **Apply**.

   > ℹ️ For License Type, it does not matter which option you select (user-based or device-based), it will always be a user-based license when the device was registered with Apple User Enrollment. If this app is shared with other types of enrollment, device-based would be the suggested setting so that your device user will not need to enter their iTunes/Apple credentials before installing the app.

From here, you can take optional actions:

- Install apps - see "Using the wizard to import iOS apps from the Apple App Store" in the *Ivanti EPMM Apps@Work Guide*.

- Apply labels - see "Managing Labels" in *Getting Started with Ivanti EPMM*.

Configuration settings for Apple Business Manager User Enrollment

This section covers additional configuration settings required for Apple Business Manager User Enrollment: VPN and Wi-Fi.

VPN for User-enrolled devices

User Enrolled devices can only have Per-App VPNs and can no longer have VPNs configured for the whole device. It is recommended that you create one or more VPN configurations specifically for User Enrollment. Now whenever the app is installed, the appropriate VPN configuration will also be installed automatically.

It is recommended that when assigning labels to VPN configurations, the labels should not include devices that are User Enrolled. Using a filter label, you can filter out user enrolled devices by setting in the filter:

```
"ios.apple_user_enrolled_device"= false
```

Procedure

The below steps ensure when the app is installed on the user device, the appropriate VPN configuration will also be automatically installed.

1. Follow the instructions in "Managing VPN Settings" on page 432 to setup a new VPN. Be sure to select **Per App VPN** as part of your configuration.

2. Go to **Apps > App Catalog**.

3. Select the link of an app and then select **Edit**.

4. In the Per-App VPN Settings section, select the newly-created VPN and move it to the panel on the right.

5. Select **Save**.

From here, you can optionally apply a label to your Apple license. See "Applying an Apple license label to an app" in the *Ivanti EPMM Apps@Work Guide*.

> ℹ️ Ivanti, Inc recommends that administrators modify labels for VPN configurations to exclude User Enrolled Devices if the VPN is not supported on User Enrollment. This can be done using the device detail "ios.apple_user_enrolled_device" and including it in the label definition, e.g.: AND "ios.apple_user_enrolled_device" = true

Wi-Fi Policy for user-enrolled devices

You need a Wi-Fi policy specifically for user-enrolled devices.

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

2. Select **Add New > Wi-Fi**.

   The New Wi-Fi Setting dialog box opens.

3. Enter the information. In the Proxy Type field, select **Auto**. This is the only proxy type that can be used for user-enrolled devices.

   For more information about Wi-Fi, see .

Device user instructions for registering using User Enrollment

This section addresses the actions the device user needs to take for registering Apple User Enrollment. The below steps will work with any app your company purchased - the example app used is the client app, Ivanti Mobile@Work .

Procedure

1. On the iOS device, open Safari (never Chrome) and type in the URL for Ivanti Mobile@Work : registrations.company.com/go.

2. The Ivanti Mobile@Work login displays. The device user is to log in using their local user or LDAP credentials.

   The registration page displays with a message saying the profile was downloaded.

   > ℹ️ You must complete registration within 10 minutes or you will have to start registration process over.

3. Tap **Settings**. The Settings page displays.

4. Tap **Enroll in [Your Company Name]**.

5. The User Enrollment page displays.

6. Tap **Enroll My iPhone**.

   If you tap Cancel and Delete Profile, you will have to start the registration process all over again.

7. You will be presented with a login for either Apple or your Federated account. Enter the password for your Managed Apple ID. (The Managed Apple ID will be listed at the top of your login page.)

8. You may be presented with the option to stay signed in, make a selection.

9. A page displays stating the "Enrollment is Successful."

Using Logs for Troubleshooting

To troubleshoot errors or issues for a User Enrolled device, start by reviewing the device MDM logs.

Procedure

1. In the Admin Portal, go to **Devices & Users > Devices**.

2. Select the device to open up the Device Details page.

3. Select the **Logs** tab.

   A list of available logs display.

4. Select the **MDM Activity** link to display the list of MDM actions performed on the device.

5. From the MDM Activity page, you can filter the actions based on a date range, the state of the action (for example, Error) or the action itself (for example, Install Managed Application.)

   If the action is in the Error state, a **View Error** link displays. Select this link to see more details about the error.

View reports on devices

You can see a report on devices by selecting the device , selecting the Log tab and then selecting the **MDM Activity** link.

Activation Error

Errors occur when the device is supervised. Users cannot use a supervised device for User Enrollment. There is no remedy for this as supervised devices cannot be used with User Enrollment.

App fails to install (AppAlreadyInstalled)

The most common Install Managed Application error is `AppAlreadyInstalled`. This error occurs when the device has the app installed in the private space. Since the MDM service is unable to see private apps and is unable to convert the app to managed, an Install Managed Application command sent for an already-installed app will get this error message.

Procedure

1. Instruct the device user to remove the app from the device.

2. Instruct the device user to tap "Install" for the app within Ivanti Mobile@Work .

Procedure(Alternate)

Alternatively, you can send a new installation request to the device for that application.

1. Navigate to **Apps > App Catalog**.

2. Select the check box next to the app.

3. Select **Actions** and select **Send Installation Request**.

4. Select the option to Send request for new installations.

5. Under Actions, choose Select devices to send message and then select **Apply**.

6. Search for the device, select the check box and then select **Send**.

User Enrollment with iREG

When managing user enrollment, there are two options:

- "User Enrollment with Apple Business Manager" below

- "Account-driven Apple User Enrollment" on page 225

User Enrollment with Apple Business Manager

Apple Business Manager is a place for IT teams to automate device deployment, purchase and distribute content, and manage roles in their organizations. Apple Business Manager implements User Enrollment - a modified version of the MDM protocol with a much greater focus on user privacy, implemented with a level of security that enterprises need.

User Enrollment allows the administrator to:

- Install and remove managed applications

- Install and remove network configurations

- Install a partial VPN scoped to managed apps and accounts

- Require the usage of a password

User Enrollment registration is supported on Ivanti Mobile@Work . When the administrator assigns the device user to User Enrollment mode, the In-App registration will download the User Enrollment Profile to the device.

User Enrollment applies to unsupervised devices with iOS 13.0 or supported newer versions. Devices lower than iOS 13.0 will be considered "device enrollment" regardless if the device user has been enabled for User Enrollment. User Enrollment utilizes the user's managed Apple ID, which is required and associated with all enterprise apps and data on the device and in Ivanti EPMM.

Difference between standard MDM enrollment and User Enrollment

This section addresses the difference between standard MDM enrollment and User Enrollment with Apple Business Manager.

Standard MDM enrollment

Below is what a Ivanti EPMM server can do in a standard MDM enrollment, but will not be able to do in User Enrollment mode in iOS 13.0.

The MDM server:

- Cannot erase the device.

- Does not see the personal apps the device user has installed on the device.

- Cannot convert user-installed apps into MDM-managed apps.

- Cannot clear the device passcode (i.e. unlock the device).

- Cannot set a long, complex device passcode requirement.

- Cannot configure a device-wide VPN or Wi-Fi proxy, nor can it do any management of the cellular functionality.

- Cannot see device identifiers like the UDID, serial number, or IMEI.

- Cannot apply many device-wide restrictions (such as restricting the app content rating), block iCloud, and apply any the supervised restrictions.

> When retiring and re-registering devices from Ivanti EPMM, devices are registered as Standard MDM.

User Enrollment with Apple Business Manager

In User Enrollment, the MDM server can still do everything needed to manage enterprise apps, accounts, and data.

User Enrollment can:

- Install in-house apps or apps via user-based (Apple) Apps & Books licenses

- Enforce passcode payload settings:

  - allowSimple = false

  - forcePIN = true

  - minLength = 6

- Query data related to enterprise-managed apps, certificates, and profiles

- Configure a per-app VPN for apps, mail, contacts, and calendars that have been installed by MDM

- Enforce some restrictions, like managed open in, managed contacts, managed data on the lock screen, and several others

Enterprise data is stored in a separate Apple File System (APFS) volume, which is created at enrollment, and encrypted separately from device user data. This volume contains data stored by managed apps; enterprise Notes; enterprise iCloud Drive docs; enterprise Keychain entries; managed mail attachments and bodies; and calendar attachments. Un-enrolling from MDM destroys the volume and the keys.

The final requirement of User Enrollment is the user's managed Apple ID that must be associated with all enterprise apps and data on the device and in iCloud Drive. Managed Apple IDs were first utilized by Apple School Manager and are now utilized by Apple Business Manager for User Enrollment.

All third-party apps can only be either a personal app or a managed app through Ivanti EPMM. The MDM service cannot start managing apps that the device user has already installed. In this case, the administrator will need to request the device user to delete the personal app before installing the app through MDM. The MDM service cannot start managing apps that the user has already installed. However, some system apps like Notes and Files will support both work and personal accounts.

Difference between User Enrollment vs Device Enrollment

This section covers the difference between User Enrollment and device enrollment. User Enrollment applies to devices iOS 13.0 and macOS 10.15 or supported newer versions.

Devices lower than iOS 13.0 will be considered "device enrollment" regardless if the device user has been enabled for User Enrollment.

User Enrollment for Apple Business Manager does not allow for wipe or unlock. However, the user portal will still have those options available even though they will not work.

TABLE 18. USER ENROLLMENT VS DEVICE ENROLLMENT

Functionality	User Enrollment	MAM	Device Enrollment	DEP
Erase the device and see user's personal apps	No	No	Yes	Yes
Convert managed to unmanaged or vice versa	No	No	Yes	Yes
Clear device passcode, configure device-wide VPN or Wi-Fi proxy nor manage cellular functionality	No	No	Yes	Yes
See device identifiers like serial number, IMEI	No	No	Yes	Yes
Apply supervised restrictions	No	No	Yes*	Yes
Can install and configure apps and accounts	Yes	Yes	Yes	Yes
Can configure a per-app VPN for apps, mail, contacts, and calendars that have been installed by MDM	Yes	No	Yes	Yes
Can enforce some restrictions, like managed open in, managed contacts, managed data on the lock screen, and several others	Yes	No	Yes	Yes
Can query data related to enterprise-managed apps, certificates, and profiles	Yes	No	Yes	Yes

> The "Apply supervised restrictions option" will work for Device Enrollment if the device is supervised using Apple Configurator, otherwise it is unsupported.

Requirements for enabling User Enrollment

Below are the requirements for enabling User Enrollment:

- An Apple Business Manager account

- Managed Apple ID - Managed Apple ID to be associated with each enrolled device. This Managed Apple ID provides authentication for MDM management and app licensing. When the MDM pushes down apps and media, necessary Apple licenses are assigned to the Managed Apple ID associated with the device.

- Device users who are synced to LDAP are to be assigned to a device management role and associated with a Managed Apple ID.

- For LDAP User / Group enrollment for single or bulk registrations, verify the managed Apple ID was generated correctly.

- If the existing registration process is already using PINs, the registration will still work.

- After registration, check the logs for any managed Apple ID failures.

Account-driven Apple User Enrollment

User Enrollment can be set up so the device users can self-enroll from the Settings page on their device (usually their personal iphone, iPad, or Mac device.) This feature uses the device user's managed Apple ID, making their devices managed. Account-driven Apple User Enrollment is good for when a device user logs in and out multiple times a day.

Account-driven User Enrollment is not supported in Ivanti EPMMs with SAML enabled for Apple Web-based Registration.

WARNING: Before signing out of iCloud, Ivanti recommends app-based data that is stored on the device to be saved to a server. App-based data in the user-enrolled iCloud account is stored in a separate partition. When signing out of iCloud on the user-enrolled device, Apple removes the management and all data on the device is removed. The device will still show as active on Ivanti EPMM until the administrator retires the device from the console. If the device user would like to sign back in using User Enrollment, device users will need to restart their devices and re-register, creating a new device record in Ivanti EPMM.

To find a managed Apple user-enrolled device:

1. In the Device Details page > Advanced search, select **Apple User Enrolled Device > Equals > true**.

2. Add a second search criteria: **MDM Managed > Equals > false**.

3. Make sure the Exclude retired devices from search results check box is selected.

4. Click **Search**.

If the device user re-registers and the login fails, restart the device and then re-register again.

Enabling device users to enroll in MDM User Enrollment directly

Procedure

Once enrolled, Admins can view information in the Apple User Enrolled Device field in the Device Details page - or search on it in **Advanced Search**.

1. In the Admin Portal, go to **Devices & Users > Users**.

2. Select user check box and then click **Actions > Assign Roles**.

   The Assign Roles dialog box opens.

3. Select **Allow Account Driven Apple User Enrollment**.

4. Enter a valid **Managed Apple ID** that matches the host domain being used in step 2 of Required action by device users.

   For example, joe.smith@ivanti.com is a valid Managed Apple ID for example.URL.ivanti.com, but Joe Smith cannot use joe.smith-abm@ivanti.com on the same Ivanti EPMM.

After configuring, there is "Required action by device users" below.

Required action by device users

When using **Allow Account Driven Apple User Enrollment**, required action must be taken by device users.

Procedure for iOS

1. On their iOS devices, device users navigate to **Settings > General > VPN & Device Management > Sign In to Work or School Account**.On their Mac devices, device users navigate to **Settings > Privacy & Security > Profiles > Sign In to Work or School Account**.

2. In the email address field, device users enter "`[anyusername]@[Ivanti EPMM domain with subdomain]` and then tap **Continue**. For example, any@IvantiEPMM.auto.ivanti.com.

   The Ivanti login page displays. This login accepts either local or LDAP users, as in any other registration. It also supports PINs and passwords.

3. Device users login using a valid local or LDAP account that has **Allow Account Driven Apple User Enrollment** enabled (see "Enabling device users to enroll in MDM User Enrollment directly" on the previous page.)

4. Device user enters the password and then tap **Continue**.

5. Device user acknowledges the privacy policy screen and the Terms of Service screen (if the administrator has configured it to display.)

6. The **iCloud for Work** screen displays. This screen is presented by Apple, not Ivanti EPMM. Device users tap the **Sign in to iCloud** button.

7. Device users enter the password for their **Managed Apple ID** - this is the Apple password, not an Ivanti EPMM password.

8. Device users address the two-factor authentication screen.

9. The Allow Remote Management page displays. Device users tap the **Allow Remote Management** button.

   Apple configures the device for User Enrollment; it will take approximately 30-60 seconds to complete.

10. The device Settings page displays. Device users will see their Managed Apple ID displayed under the local iCloud user in the top left corner of the Settings page. This indicates the device is fully registered with iReg.

WARNING: Before signing out of iCloud, Ivanti recommends app-based data that is stored on the device to be saved to a server. When signing out of the iCloud on the user-enrolled device, Apple removes the management and all data on the device is removed. To return to the iCloud, device users will need to restart their device and then re-register using the steps above.

Procedure for macOS

1. On their macOS devices, device users navigate to **Settings > Privacy & Security > Profiles > Sign In to Work or School Account**.

2. In the email address field, device users enter "`[anyusername]@[Ivanti EPMM domain with subdomain]` and then tap Continue. For example, any@IvantiEPMM.auto.ivanti.com

3. Ivanti recommends device user to select Open Browser, device user's organization requires authentication for using a web browser. The Ivanti login page displays. This login accepts either local or LDAP users, as in any other registration. It also supports PINs and passwords.

4. Enter the username and password, and then tap **Register**.

5. The Ivanti **Your Privacy Matters** page displays. Device users must acknowledge the **Your Privacy Matters** page (If the administrator has configured it to display).

6. The **iCloud for Work** screen displays. This screen is presented by Apple, not Ivanti EPMM. Tap the **Sign In** button to continue with iCloud account.

7. Device users enter the password for their Managed Apple ID - this is the Apple password, not an Ivanti EPMM password. Then tap **Next**.

8. Device users address the two-factor authentication screen. Enter the six-digit verification code, which will be sent to your registered mobile number (if two-factor authentication is enabled).

9. The **Allow Remote Management** page displays. Tap the **Allow** button.

10. The **Profiles** page displays. Enter your password to enroll you in the remote management service.

Multi-User Support

This section addresses multi-user access for devices including secure sign-in and sign-out settings.

- "About multi-user support" below
- "Using Secure Sign-In and Sign-Out" below
- "Setting Secure Sign-In preferences" on the next page
- "Setting unique restrictions for signed-out devices" on page 231
- "Enabling Secure Sign-In" on page 232
- "Customizing the multi-user secure sign-in web clip" on page 232
- "Remote sign-out from a multi-user iOS device" on page 233
- "Setting automatic sign-out for multi-user devices" on page 235

About multi-user support

Ivanti EPMM supports multi-user access for iOS devices. This feature enables multiple employees to use the same device. The Secure Sign-In feature ensures that the profiles and apps are removed when the device user signs out and reinstalled when the next user signs in. Options enable you to specify whether Wi-Fi settings and passcodes are removed. Each app is handled based on how that app is configured for quarantine.

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 Ivanti** options. This allows the user certificate and private key to be delivered each time they log in on the shared device.

Using Secure Sign-In and Sign-Out

Devices configured for multi-user support receive a Secure Sign-In web clip.

Procedure

1. Tap **Secure Sign-In**.

   The Secure Sign-In page displays

2. Enter a valid username and password and then tap **Sign-In**.

   After successfully signing in, Ivanti EPMM sends to the device the profiles configured for the signed-in user.

3. To sign out, tap **Secure Sign Out**.

   Ivanti EPMM removes the profiles assigned to the signed-out device user.

   Optionally, Ivanti EPMM can remove the managed apps assigned to the signed-out device user. The setting for this is in the "Remove app when device is quarantined or signed out" field. For more information, see "Using the wizard to import iOS apps from the Apple App Store" in the *Ivanti EPMM Apps@Work Guide*.

> Web content filters can affect the Secure Sign-in web clip. Ensure your web content filters do not block access to Ivanti EPMM. Blocking access to Ivanti EPMM disables the secure sign-in web clip. For more information, see "Web content filter settings" on page 752.

Setting Secure Sign-In preferences

For multi-user devices, you can determine whether Wi-Fi settings are removed upon user sign out.

> **WARNING:** If you remove Wi-Fi settings on sign out for Wi-Fi only devices, these devices will be unable to connect to any network after the first user signs out.

Procedure

1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Multi-User**.
2. Select one of the following settings to specify how to handle Wi-Fi settings when device users sign out:
   - **Keep Wi-Fi settings**
   - **Remove Wi-Fi settings for cellular-enabled devices**
   - **Remove Wi-Fi settings for cellular-enabled and Wi-Fi-only devices**

3. If you want to clear the passcode on the device when the device user signs out, select the **Clear passcode** option.

4. Click **Save**.

Setting unique restrictions for signed-out devices

The Signed-Out label enables you to specify more stringent restrictions for multi-user devices when a user signs out. This is a dynamic label that applies automatically to any multi-user iOS device that does not have a signed-in user.

Specifying restrictions involves the following main steps:

1. Create the restrictions that you want applied when a user signs out.

   For example, you might want to disable access to YouTube when an authorized user is not signed in.

2. Apply each policy and configuration to the **Signed-Out** label.

Suppose you want iPad devices to be restricted to basic web use when an authorized user is not signed in. You would need to create a Restrictions configuration to lock down the camera, inappropriate content, screen captures, app installation, and so on.

Procedure

1. Go to **Policies & Configs > Configurations**.
2. Select **Add New > Apple > iOS / tvOS > Restrictions**. The New Restrictions Setting dialog box opens.
3. Assign a **Name** to the configuration.
4. Clear the check boxes for the items you want to restrict.
5. Select **Save**.
6. Select the new configuration.
7. Select **Actions > Apply To Label**.
8. Select **Signed-Out**.
9. Select **Apply**.

   Ivanti EPMM sends the new restriction settings to multi-user devices upon sign-out.

Enabling Secure Sign-In

ℹ️ If you intend to distribute certificates to multi-user devices, Ivanti, Inc recommends using user certificates instead of device certificates. This practice ensures that email is configured for the correct user.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select the **System - Multi-User Secure Sign-In** configuration.

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

4. Select the label or labels that represent the devices to be configured for multi-user sign-in.

5. Click **Apply**.

Customizing the multi-user secure sign-in web clip

You can change the look and feel of the multi-user secure sign-in web clip for iOS devices.

Possible changes include:

- A customized touch icon for the web clip

- Removing the icon from iOS screens

- Running the web clip in full-screen mode (except when using Ivanti Tunnel or VPN Safari domain rules)

- Enabling a pre-composed web clip touch icon, so that devices running versions of iOS prior to iOS 7 will display the icon, as designed, without any additional effects imposed on touch icons on versions of iOS prior to 7

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select the **System - Multi-User Secure Sign-In** configuration. The Configuration Details pane displays on the right.

3. Select **Edit**. The Modify Web Clips Setting window displays.

4. Select the **Secure Sign-In** web clip link. The Edit Web Clip dialog box opens.

5. Use the Secure sign-in web clip window to edit the web clip as desired, options are listed in the table below.

6. Select **Save**.

7. In the **Edit Web Clip Setting** window, select **Save**.

TABLE 1. OPTIONS FOR EDITING

Item	Description
Name	Do not modify the name of the web clip.
Address/URL	This URL points to the default multi-user sign-in page that is included with Ivanti EPMM. The page is located at `https://<your host name>/mifs/c/multiuser.html`. Modify the URL if you wish to point to a customized multi-user sign-in page.
Icon	By default, this points to the multi-user sign-in web clip touch icon shown in "Using Secure Sign-In and Sign-Out" on page 229. To upload a customized touch icon: 1. Select **Browse**. 2. Select the customized icon. 3. Select **Open**.
Removable	Select to allow iOS device users to remove the multi-user web clip.
Full Screen	Select to enable the web clip to display in full screen mode on iOS devices. ⓘ Full screen mode will not work for web clips when devices running iOS 8 or supported newer versions use Ivanti Tunnel or Safari domain VPN rules.
Precomposed	Select to use a precomposed icon for the web clip. Precomposed icons will display on iOS 6 through iOS 7 devices as designed, without the imposing of iOS visual effects.

Remote sign-out from a multi-user iOS device

You can use the Admin Portal to remotely sign out users from multi-user devices.

Procedure

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

2. Select the device in the Devices page.

3. Select **Actions > iOS Only > Sign out**.

The following table lists the items removed from a multi-user device when remotely signing out a user.

TABLE 1. ITEMS REMOVED BY IVANTI EPMM ON SIGN OUT FROM A MULTI-USER iOS DEVICE

Item	Remove on sign-out?
Apps@Work access	Yes
Ivanti Docs@Work access	Yes
Passcode	**Optional**
Restrictions	No
Wi-Fi	Optional
VPN, Per-app VPN, VPN on Demand	Yes
Email	Yes
Exchange	Yes
LDAP	Yes
CalDAV	Yes
CardDAV	Yes
Subscribed Calendars	Yes
Web Clips	**No**
Credentials (Certificates)	Yes
SCEP	Yes
Mobile Device Management	No
APN	**No**
Single-App Mode	**Yes**
Global HTTP Proxy	**Yes**
Generic Configuration Profiles	**No**

Item	Remove on sign-out?
Provisioning Profiles (Configurations)	**No**
Provisioning Profiles (App Distribution)	No
General	**No**
AirPlay	No
AirPrint	No
Network Usage Rules	No
Web Content Filter	No
Managed App Config	Yes
Single Sign-on Account	Yes

Setting automatic sign-out for multi-user devices

You can configure Ivanti EPMM so that a user on a multi-user device is automatically signed out of Ivanti EPMM. The user is signed-out after an iOS device is locked *and* a configured time period has elapsed since AppConnect app activity. This feature requires that you are using AppConnect for iOS apps on the device and Ivanti Mobile@Work 11.0 for iOS or supported newer versions.

If you configure automatic sign-out to occur after a configured time period, the following scenario occurs:

1. A user locks a device which is configured for multi-user access or the user switches to a non-AppConnect app.
2. The configured period elapses.
3. A user unlocks the device and opens an AppConnect app, or the user switches back to an AppConnect app from a non-AppConnect app.
4. Control switches to Ivanti Mobile@Work for iOS, which sends a sign-out command to Ivanti EPMM.

The user is signed out of Ivanti EPMM.

Procedure

1. Go to **Policies & Configurations > Policies**.
2. Select the AppConnect Global policy that is applied to the multi-user devices.
3. In the Device Details page, select **Edit**. The Modify AppConnect Global Policy dialog box opens.
4. In the AppConnect field, select **Enable**.

5. In the **iOS** portion of the **AppConnect Security Controls on Device** section, select **Enable multi-user auto sign-out after X minutes of inactivity**.

6. Enter a value between 5 and 120 for the number of minutes of inactivity before the automatic sign-out occurs.

7. Select **Save**.

Related topics

"Configuring the AppConnect global policy" in the *AppConnect Guide for EPMM*.

Managing Custom Attributes

This section addresses all components relating to custom attributes.

- "Custom Attributes" below
- "Assigning a custom attributes role" on the next page
- "Adding custom attributes to users and/or devices" on page 239
- "Viewing custom attributes available for users and/or devices" on page 240
- "Viewing custom attributes assigned to users" on page 241
- "Viewing custom attributes assigned to devices" on page 241
- "Editing custom attributes for users and/or devices" on page 241
- "Searching for custom attributes for users and/or devices" on page 242
- "Exporting a log of the custom attributes for users and/or devices" on page 242
- "Deleting custom attributes from users and/or devices" on page 242
- "Setting custom attribute values for device or users" on page 243
- "Pushing label attribute changes to devices and users" on page 244

ℹ️ The features described in this section are supported on macOS devices.

Custom Attributes

Administrators can assign custom attributes to users or devices to associate additional properties with these objects. These properties can then be used to build groups or distribute configurations.

Set custom attributes manually or update them via API by external systems (any data source external to Ivanti EPMM) to determine what policies, configurations and apps should be applied/available to devices as part of a label filter criteria. Ivanti EPMM specifically integrates with LDAP as one external source of data, so LDAP data can be used in label filter criteria, however, Ivanti EPMM cannot integrate with all external data sources.

The work flow for using custom attributes is:

- Assign custom attributes role

- Create custom attributes for users and/or devices

- Manage custom attributes for users and/or devices, which includes:

  - Viewing custom attributes

  - Editing custom attributes

  - Searching custom attributes

  - Removing custom attributes

  - Exporting a log of custom attributes

- Apply custom attributes to labels

- Set custom attribute values for devices or users

- Pushing label attribute changes to devices and users

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 administrator 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 administrator 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.

Ivanti EPMM supports a maximum of 20 LDAP Custom Attributes as substitution variables. Further Custom Attributes can only be used to define Labels

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. For Apple School Manager, use on the 1:1 (one-to-one) device use case and label it, for example, "ManagedAppleId". This name can be whatever you choose, however, make note of it since you will select this custom attribute name when turning on Apple Education.
Attribute Description	Enter a meaningful description for the custom attribute.
Value Type	Select one of three value types: boolean, integer or string. For Apple School Manager, use the string value type.
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 Ivanti EPMM.

> ⓘ When assigning values to these two custom attributes "ManagedAppleID" and "DeviceCartName", do not assign the device to both values. A device can either be a 1:1 device or it can be a Shared iPad (multi-user). If a device is given both values, Ivanti EPMM will display an error on the Apple Education policy or configuration. If a device is assigned to a device cart that is unknown or to a Managed Apple ID that is unknown, the device details Education Role will display as "None." If the device is given a known Managed Apple ID, but that ID is not assigned to any classes as either a teacher or a student, the device details will display the Apple Education Role as "None". If the device has a valid Managed Apple ID and that Apple ID is assigned to at least one class as a teacher, the Apple Education Role will be "Teacher". If the device has a valid Managed Apple ID and that Apple ID is not assigned to a class as a teacher and is assigned to the class as a student, the Apple Education Role will be "Student". If there is a value entered in the custom attribute for "DeviceCartName", the Apple Education Role will be "Student (multi-user)".

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.

Next steps

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

Use the following procedure to edit custom attributes.

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.

> ℹ️ 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 58.

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

Viewing custom attribute changes

Changes in the modification history for configurations, policies, labels, compliance groups, rules, and actions attributes are displayed in the **Configuration Details** page, which shows before and after content. Logs with before and after values display an icon you can click to see the new information. The new log information is generated for the following actions:

- **Create** - The "Before" column will be empty.

- **Edit** or **change** - Both before and after values display.

- **Delete** - The "After" column will be empty.

In Ivanti EPMM version 11.10.0.0 and later versions, the before and after values can be readily identified from unchanged content because they are highlighted and in blue text in the **Changes - Before & After** panel.

To display the **Changes - Before & After** panel, click on any policy or configuration in the **Policies & Configurations > Configurations** tab to display the **Configuration Details** side panel to the right of the window. Click **Modification History**, and click the box corresponding to the change.

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 108.
- **For users**: force an LDAP sync. See "Synchronizing with the LDAP server" in *Getting Started with Ivanti EPMM*.

Managing Policies

Ivanti EPMM 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 Ivanti EPMM* 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 page 249
- "Viewing policy status and platform support" on page 252
- "Enabling profile encryption" on page 253
- "Enabling or disabling encryption on a macOS device" on page 254
- "Storing and retrieving FileVault personal recovery keys in Ivanti EPMM (macOS)" on page 257
- "Configuring iOS and macOS software updates" on page 263
- "Configuring notification settings" on page 311
- "Configuring a system policy managed setting" on page 258
- "Configuring a system policy control setting" on page 259
- "Configuring a system policy rule" on page 261
- "Configuring iOS and macOS software updates" on page 263
- "Managing the activation lock for iOS devices" on page 270
- "Whitelisting Wi-Fi networks" on page 273
- "Configuring firewall settings for macOS devices" on page 273
- "Sync policies and battery use" on page 275

- "Global App Config Settings policy" on page 275
- "Work Schedule policy" on page 285
- "Country changes and alerts" on page 288
- "iOS location-based wakeups interval and syncing with Ivanti EPMM" on page 288
- "Single-app mode policies" on page 288
- "Configuring a global HTTP proxy policy" on page 291
- "Cellular policies" on page 295
- "Wallpaper policies" on page 300
- Accessibility Settings policy
- "Device name policies" on page 305
- "Customizing a home screen layout" on page 307
- "Customizing a lock screen message" on page 310
- "Configuring notification settings" on page 311
- "tvOS policy settings" on page 315
- "Notifications of changes to the privacy policy" on page 317
- "Exporting the devices in the WatchList" on page 331
- "Impact of changing LDAP server variables" on page 331
- "Configuring encrypted DNS settings" on page 333

ℹ️ For User Enrollment, Ivanti recommends using the label "Apple User Enrolled Device" + "Equals" + "True" or ios.apple_user_enrolled_device = true."

Related topics

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

Working with default policies

ℹ️ The features described in this section are supported on macOS devices.

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. Ivanti EPMM 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.

Ivanti EPMM provides defaults for the following policy types:

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

ⓘ   You cannot delete default policies.

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

Prompting users to change the password

You can configure the default security policy to force users to change their passwords when a device is discovered to be non-compliant.

ⓘ   Consider notifying users of the new specifications before making changes to the policy.

Procedure

This procedure applies to macOS 10.13 or later.

1. In the Admin Portal, go to **Policies & Configs > Policies > Add New > Security** or modify the default security policy.

   The New Security Policy dialog box opens.

2. Enter the Name of the policy.

3. In the Priority field:

   a. For mandatory password changes, select **Lower Than** and choose **Security Policy Omega (1)** from the drop-down.

   b. For optional password changes, select **Lower Than** and choose **Security Policy Sigma (45)** from the drop-down.

4. In the Password field, chose Mandatory or Optional.

    a. Select **Mandatory**.

- Select the **Enforce Password Rule at Next Login** check box.

    b. Select **Optional**

- Select the **Enforce Password Rule at Next Login** check box.

- Select **User Channel** if you want all device users to change their password.

- Select **Device Channel** if you want all users to change their password, including the administrator user.

> For iOS devices, if a security policy is edited and the Password field is set to Optional, then the security policy will not be pushed to devices. This results in an inaccurate count in your WatchList on the Policies & Configurations > Policies page. Ivanti, Inc recommends you have the Password field set to Mandatory.

5. Select **Save**.

6. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then select **Confirm**. For more information, see "Best practices: label management" on page 860.

Upon the next time a macOS device user logs in, the user is prompted to change the password.

> When creating a new security policy and you have either user channel or device channel chosen, you must apply a label to the policy in order for the security policy to be pushed to user devices.

Importing and exporting policies

> The features described in this section are supported on macOS devices.

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

- "Exporting policies or configurations" on the next page

- "Importing policies or configurations" on page 251

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

Exporting policies or configurations

Exporting policies and configurations help reduce errors when you have multiple instances of Ivanti EPMM. 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. Select **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 Ivanti EPMM 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 Ivanti EPMM. 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. select **Import** to locate a saved exported .json file.

3. Enter the name of the file or select **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 select the **I Agree** check box.

7. Select **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), Ivanti EPMM creates them during import. If the child objects already exist, they are overridden.

Viewing policy status and platform support

The features described in this section are supported on macOS devices.

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**: Ivanti EPMM 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

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

Enabling profile encryption

Profile encryption is enabled by default. The administrator has the option to disable this setting. This allows the administrator to control encryption of the backup to iTunes. If profile encryption is enabled, the backup to iTunes is also encrypted. If profile encryption is disabled, the backup to iTunes is not encrypted.

> If you disable profile encryption, backup to iTunes continues to be encrypted for devices that are already registered. The backup to iTunes will be unencrypted for devices that registered after the setting change.

Turning off encrypted backups results in compromised certificates on iOS devices, and disabling SCEP. Ivanti EPMM does not recommend turning off encrypted backups, as this compromises system security.

Procedure

1. Go to **Settings > System Settings > iOS > MDM**.

2. Select or deselect the **Enable Profile Encryption** setting.

3. Deselecting disables profile encryption, and checking the setting enables profile encryption.

4. Select **Save**.

Enabling or disabling encryption on a macOS device

You can encrypt macOS devices using FileVault 2. FileVault 2 can be used to perform full XTS-AES 128 encryption on the contents of a volume. Ivanti EPMM enables you to create FileVault 2 policies that you can use to control the encryption of managed macOS devices. You can apply a single FileValut 2 policy to a device.

The FileVault 2 policy also includes recovery keys. Users can employ recovery keys to unlock the disk, in case they forget the password for that purpose.

There are two types of recovery keys:

- **Personal recovery key**: FileVault 2 automatically generates a personal recovery key at the time of encryption. A personal key is unique to the machine being encrypted. If an encrypted macOS is decrypted and then re-encrypted, the existing personal recovery key is invalid. FileVault 2 would then generate a new personal recovery key during re-encryption.

- **Institutional recovery key**: An institutional recovery key is used for the same purpose as a personal recovery key, but is the same for all macOS devices within an organization. You can use FileVault 2 to generate and install an institutional recovery key to your system before enabling encryption. This common key is used to unlock any managed, encrypted macOS device.

ⓘ   FileVault 2 policies are supported on devices running macOS 10.10 or supported newer versions.

Procedure

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

2. Select **Add New** > **iOS and macOS** > **macOS** > **FileVault 2**.

3. Use the guidelines in the table below to complete this form.

4. Select **Save**.

5. Apply the policy to a macOS label.

TABLE 1. FILEVAULT2 GUIDELINES

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**.

Item	Description
	Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available.
	Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list.
	For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Enable FileVault 2	Select to enable encryption.
FileVault User Settings	
Defer FileVault until the designated user logs out:	
Enable FileVault at SetupAssist	The Enable FileVault at SetupAssist helps to encrypt the device before the user logs in. Note: For FileVault to be enabled at SetupAssist, Await Device Configuration needs to be enabled in the automated Enrollment Profile. For ADE enrolled devices, this option the system also ignores all other keys in this payload, except for Show Recovery Key
Always prompt user to enable FileVault	Select to prompt the user to enable FileVault on the macOS device. The user sees the prompt when logging in to the macOS device. When selecting this option, users cannot bypass enabling the encryption option.
Maximum number of times a user can bypass enabling FileVault	Select to configure a limit to the number of times the user can ignore the prompt to enable FileVault. Select up or down to select the maximum number of times. The user sees the prompt when logging in to the macOS device. When selecting this option, users can choose to skip enabling the encryption option as many times as specified here.
Do not request enabling FileVault at user logout time	Select so that users are not prompted to enable FileVault when they are trying to log out of the device.
Output Path	Enter the path to which the recovery key .plist file will be stored.

Item	Description
	For example:
	/Library/Keychains/recovery.plist
Personal Recovery Key	
Create a personal recovery key	Select to create a personal recovery key. A personal recovery key will be generated when encryption (FileVault) is enabled.
	This private key can be used later to unlock the startup disk of the specific macOS device, in case the device user name and password are not available to unlock the device.
Institutional Recovery Key	
Enable institutional recovery key	Select to enable an institutional recovery key.
	The institutional recovery key can be used to unlock the startup disk of any macOS device that uses the same FileVault 2 master keychain.
	The keychain should be available at the following location before enabling FileVault 2 on the macOS device: `/Library/Keychains/FileVaultMaster.keychain`
Certificate	Enter your certificate information. If you selected **Enable institutional recovery key** without entering a certificate, then the master keychain (/Library/Keychains/FileVaultMaster.keychain) is used when the institutional recovery key is added.

Next Steps

You can verify that encryption is enabled on a given device by checking the device details for that device. Select **Devices & Users** > **Devices**, and select the carat (**^**) next to the relevant macOS device. In the **Device Details** tab, look for the following fields:

- Full Disk Encryption Enabled

- Full Disk Encryption Has Institutional Recovery Key

- Full Disk Encryption Has Personal Recovery Key

Storing and retrieving FileVault personal recovery keys in Ivanti EPMM (macOS)

The FileVault 2 Retrieve Personal Recovery Key setting allows you to store and retrieve personal recovery keys used to encrypt disk volumes with FileVault 2. Ivanti EPMM stores the personal recovery keys for each device in an encrypted form in its database.

When necessary, you can decrypt and display the key on your screen, allowing you to decrypt the associated macOS device.

This feature is supported on macOS 10.12 or supported newer versions.

> When upgrading a macOS device from 10.12 to 10.13, you need to apply this setting to devices again. Do this by creating two policies with two different labels, one for devices running macOS 10.12, and another for devices running macOS 10.13.

Procedure

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

2. Select **Add New** > **iOS and macOS** > **macOS Only** > **FileVault 2 Retrieve Personal Recovery Key**.

3. In the New FileVault 2 Retrieve Personal Recovery Key dialog box, use the guidelines to complete this form.

4. Select **Save**.

5. Apply the policy to a macOS label.

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Store Recovery Key to Ivanti EPMM	Enables the storage of the recovery key to Ivanti EPMM. This option is enabled by default when you create a FileVault 2 policy, and cannot be disabled.

Configuring a system policy managed setting

This setting allows you to disable the contextual menu that macOS users can display in the Finder application. The contextual menu allows macOS users to bypass system policy restrictions, such as rules regarding which applications macOS users can install, execute, or open through a contextual menu

Only one policy is allowed per macOS device. You can define multiple policies and assign a priority level to each, such that Ivanti EPMM can determine which policy it sends to macOS devices.

ℹ️   This policy is supported on devices running macOS 10.10 or supported newer versions.

Procedure

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

2. Select **Add New** > **iOS and macOS** > **macOS** > **System Policy Managed**.

3. Use the guidelines in "System policy managed settings" on the next page to complete this form.

4. Select **Save**.

5. Apply the policy to a macOS label.

TABLE 19. SYSTEM POLICY MANAGED SETTINGS

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Disable override	Select to disable the contextual menu in the Finder application.

Related topics

- System Policy Managed Payload in the Apple Configuration Profile Reference

- "Configuring a system policy control setting" below

- "Configuring a system policy rule" on page 261

Configuring a system policy control setting

The system policy control setting allows you to manage macOS Gatekeeper functionality. Gatekeeper secures the macOS operating system by enforcing code signing and verifying applications downloaded from the web before allowing users to run them. The goal of Gatekeeper is to reduce the likelihood of accidentally running malware.

The system policy control setting you define in Ivanti EPMM is analogous to the options available on macOS under **System Preferences** > **Security & Privacy** > **General**.

Only one policy is allowed per macOS device. You can define multiple policies and assign a priority level to each, such that Ivanti EPMM can determine which policy it sends to macOS devices.

> ℹ️ This policy is supported on devices running macOS 10.10 or supported newer versions.

Procedure

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

2. Select **Add New** > **iOS and macOS** > **macOS** > **System Policy Control**.

3. Use the guidelines in the table below to complete this form.

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Application Assessment	Select to enable the Gatekeeper application assessment functionality. Gatekeeper will assess every application macOS users download from the web.
Allow Identified Developers	Select to allow only those applications with proper code signatures.

4. Select **Save**.

5. Apply the policy to a macOS label.

Related topics

- System Policy Control Payload in the Apple Configuration Profile Reference

- About Gatekeeper

- "Configuring a system policy managed setting" on page 258

- "Configuring a system policy rule" on the next page

Configuring a system policy rule

The system policy rule setting allows you to control Gatekeeper rules. Gatekeeper secures the macOS operating system by enforcing code signing and verifying applications downloaded from the web before allowing users to run them. The goal of Gatekeeper is to reduce the likelihood of accidentally running malware.

The options in this setting are also available in the macOS command-line utility `spctl`. The spctl utility manages the security assessment policy subsystem on macOS. This subsystem evaluates rules you define that determine whether the macOS device allows the installation, execution, and contextual menu opening of applications on the device. The system policy rule setting requires the system policy control in order to work.

For example, if you want to allow applications developed by a company called Salesapps on macOS devices, you would need to do the following:

1. Create a system policy control setting enabling Gatekeeper.

2. Disable the option that allows all applications by identified developers.

3. Create a system policy rule setting with the following syntax:

   ```
   identifier com.salesapps
   ```

The system policy rule and control would allow the execution of all applications developed by the Salesapps company on macOS devices. However, macOS device users would still be able to download other apps.

Only one policy is allowed per macOS device. You can define multiple policies and assign a priority level to each, such that Ivanti EPMM can determine which policy it sends to macOS devices.

ⓘ   This policy is supported on devices running macOS 10.10 or supported newer versions

Procedure

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

2. Select **Add New** > **iOS and macOS** > **macOS** > **System Policy Rule**.

3. Use the guidelines in "System policy rule settings" on the next page to complete this form.

4. Select **Save**.

5. Apply the policy to a macOS label.

TABLE 20. SYSTEM POLICY RULE SETTINGS

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Policy requirement	Enter your desired spctl command. The code you enter here must follow the rules delineated in the Code Signing Requirement Language. (i) You cannot enter the expiration date or operation type in the spctl command you enter here. The expiration date and operation type must be entered or selected in the field and drop-down list below.
Comment	Enter any comments regarding the rule or command.
Expires on	Enter an expiration date for the rule.
Operation type	Select an operation type for the rule. • EXECUTE • INSTALL • LSOPEN

Related topics

- [System Policy Rule Payload in the Apple Configuration Profile Reference](#)

- [Code Signing Requirement Language](#)

- [About Gatekeeper](#)

- "Configuring a system policy managed setting" on page 258

- "Configuring a system policy control setting" on page 259

Configuring iOS and macOS software updates

The software update policy specifies what kind of system updates iOS or macOS devices should receive and when they should receive them. This policy allows you to keep the system software consistent on all your Apple iOS and macOS devices.

Only one software update policy is allowed per device. You can define multiple policies and assign a priority level to each, such that Ivanti EPMM can determine which policy it sends to iOS and macOS devices.

> ℹ️ Once enrolled in the device enrollment program, devices are automatically supervised. Device users would have to use the Apple Configurator to make their devices supervised. If the device is not registered with the device enrollment program, macOS software updates are limited to only checking if a new version is available.

When a device checks in, Ivanti EPMM checks:

- If a software update policy is applied to the device

- The time window of the policy

- If an update is available for that device

- If the available update is applicable for the device's hardware

After MDM sends the update to the device, the device queues the update and the user is prompted to enter their passcode in order to start the software update.

> ℹ️ In order to utilize the iOS Software Update policy, the device users with iOS versions 11.2 and older will be required to upgrade to iOS 11.3 or supported newer versions.

Procedure

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

2. Depending upon the device, select one:

   a. For iOS devices, select **Add New** > **iOS and macOS** > **iOS Only** > **iOS Software Update**.

   b. For macOS devices, select **Add New** > **iOS and macOS** > **macOS Only** > **macOS Software Update**.

3. Use the guidelines in the Software Update settings table below to complete the new Add Updates dialog box.

4. Select **Save**.

5. Apply the policy to a iOS or macOS label.

TABLE 21. SOFTWARE UPDATE SETTINGS

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Set device update to (iOS only)	Select one: **Update to the latest version** - applicable to any iOS device prior to iOS 11.3. **Update to a specific version** - a field displays for you to enter the iOS version you want to update (for iOS 11.3 or supported newer versions.) This field allows you to push the policy for updating a specific version of iOS to supervised devices.

TABLE 21. SOFTWARE UPDATE SETTINGS (CONT.)

Item	Description
Critical Updates (macOS only)	Select **All critical updates** if updates requiring a device restart are acceptable. Otherwise, select **Only critical updates that do not require restart**.
Configuration Data Updates (macOS only)	Select **All configuration data updates** if updates requiring a device restart are acceptable. Otherwise, select **Only configuration data updates that do not require restart**
Firmware Updates (macOS only)	Select **All firmware updates** if updates requiring a device restart are acceptable. Otherwise, select **Only firmware updates that do not require restart**
Scheduling Priority (macOS only)	Sets the priority for installing an operating system update. When set to Low (default), the device end user will have the option to defer the update. When set to High, the update will be pushed to the device and deferrals by the device user will not be allowed. Sending the command with the value `High` is equivalent to the device user requesting the update themselves in **Settings**. This key is supported only for minor operating system updates. Before using this property, you must set **Install Action > InstallLater**.For more information, see
Install Action (macOS only)	Select an option: • **Default** - Download or install the update, depending on the current state. You can check the UpdateResults dictionary to review scheduled updates. This value is available in macOS 10.11+. • **DownloadOnly** - Download the software update without installing it. This value is available in macOS 11+.

TABLE 21. SOFTWARE UPDATE SETTINGS (CONT.)

Item	Description
	• **InstallASAP** - Download the software update and trigger the restart countdown notification. This value is available in macOS 10.11+. • **NotifyOnly** - Download the software update and notify the device user through the App Store. This value is available in macOS 10.11+. • **InstallLater** - Download the software update and install it at a later time. This value is available in macOS 10.11+. When selecte, the Max User Deferrals field displays below. • **InstallForceRestart** - Perform the Default action, and then force a restart if the update requires it. This value is available in macOS 11+. ⓘ **Warning:** InstallForceRestart may result in data loss.
Max User Deferrals (macOS only)	When **Install Action > InstallLater** is selected, the Max User Deferrals field displays. Select to designate the maximum number of times the system allows the device user to postpone an update before installing it. The system prompts the device user once per day. After the maximum number of times, the update occurs automatically. This key is supported only for minor operating system updates. For more information see, "Updates tab" on page 269
Update Hours	Select the timezone for the update times you select in the fields that follow.

TABLE 21. SOFTWARE UPDATE SETTINGS (CONT.)

Item	Description
	For each day of the week, select the time of day and duration to apply the update. The duration indicates the time period in the local time zone specified by the policy. The update is initiated on each device when it checks in during the selected time period.
	If you do not select any days of the week, no updates are initiated for a device, even if updates are available for the device.
	If you select at least one day, but a device has no network access during that time period, no update is initiated for the device.
	If a device does not have a iOS/macOS software update policy applied to it, updates are not initiated for the device.

Related topics

Updating the iOS manually on a single supervised iOS device

Software update recommendation cadence

You can set a user's device to allow all available, the highest available, or the lowest available OS software updates.

Applicable to:

- iOS 14.5 or later

- iPadOS 14.5 or later

Procedure

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

2. Select **Add New > iOS Only > Recommendation Cadence**.

   The Recommendation Cadence Command Policy dialog box opens.

3. Use the guidelines in the Recommendation Cadence Command Policy settings table below to make your settings.

4. Select **Save**.

5. Apply the policy to a iOS or iPadOS label.

TABLE 22. RECOMMENDATION CADENCE COMMAND POLICY SETTINGS

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Show all available OS Software Updates, if available	(Default) Displays all available OS software updates for the device.
Show only the highest available OS Software Update, if available	Displays the highest available OS software update for the device.
Show only the lowest available OS Software Update, if available	Displays the lowest available OS software update for the device.

Disable OS updates

By default, Ivanti EPMM uses the Available OS Updates command to poll Apple devices. You can disable this feature, thus stopping the Available OS Updates commands to iOS devices. To continue to have this feature disabled, for every Ivanti EPMM upgrade, you will need to de-select the Enable Available OS Updates calls field.

Procedure

1. Go to **Settings > System Settings**.

2. Select on **iOS > MDM**. The MDM page opens.

3. De-select the Enable Available OS Updates calls field.

4. Select **Save**.

Updates tab

1. Select Devices & Users > Devices.

2. Click Update. You can view the following details in the Updates tab:
   You can also use the MacOS Update Response Fields filters in the Advanced search, to view all software update relevant details including the MacOS software name.

Label Name	Description
PRODUCT KEY	Displays the current update.
UPDATE NAME	Displays a human readable name of the update.
STATUS	Displays the upgrade status. One of the following status is displayed: • Idle • Downloading • Installing
DOWNLOAD PROGRESS	Displays completion percentage
DEFERRAL TIME REMAINING	Displays the number of remaining number of times the update can be deferred by the user
MAXIMUM DEFERRAL TIME	Displays the maximum number of times the user can defer an update. This is configured by the administrator.
NEXT SCHEDULE INSTALL DATE	Displays when the next software update is available.

These filters are available in:

- Labels

- Spaces

- Compliance Policy Rules

What the device user sees during software upgrade

After a new iOS is released, the iOS device checks and becomes aware that a new version of iOS software is available. If the device is locked with a passcode, the next time the device is unlocked, the device is able to begin to download the new iOS in the background without device user notification. After the download, on the Software Update screen, there is an indication that new version of iOS has been downloaded and the device user has the option to "Install Now". If the device user taps "Later", the Software Update will keep requesting to install the update. After 3-4 attempts to install the new iOS software upgrade, no more deferring of the software update will be allowed. The user is required to input their passcode and that passcode is saved and used to update the device.

Related topics

- ["macOS settings" on page 772](#)

Managing the activation lock for iOS devices

The activation lock feature:

- is designed to prevent anyone from using a lost or stolen device.

- provides administrators with more options for deterring theft of supervised devices.

- enables administrators to reclaim supervised devices and reassign them to other employees.

A security policy option enables the Activation Lock on newly registered phones. Enabling this option prompts Ivanti EPMM to acquire the bypass code for the devices. When you configure an iOS device as supervised, you can generate a device-specific Activation Lock bypass code which you can later use to remove the Activation Lock. The Send Activation Lock Bypass action in the Devices page sends the necessary code to the target devices.

> ⓘ You must have a connection between Ivanti EPMM and Apple's Activation Lock Bypass server to be able to store bypass codes for supervised, managed devices. The server's URL is:

https://deviceservices-external.apple.com/deviceservicesworkers/escrowKeyUnlock

- Per Apple policy, the Activation Lock bypass code works once per device. The device must be reset before another bypass code will work.

- Per Apple policy, Ivanti EPMM can acquire the bypass code only when the device is first registered.

- For supervised devices already registered with Ivanti EPMM, select **Actions > Send Activation Lock Bypass** to acquire the bypass codes for these devices.

Applying an activation lock

As soon as Find My iPhone is turned on, a mapping between this iCloud account and a hardware identifier for this device is saved to Apple's activation servers. From that point, no one can turn off Find My iPhone, erase the device, or reactivate it without entering the existing Apple ID and password. If someone other than you wiped your device and then tried to re-activate and use it, they would be prompted for your Apple ID and password in Setup Assistant.

If you have a corporate-liable deployment, and your devices are supervised, activation lock is disabled for supervised devices by default, and device users cannot turn it on. Most corporate administrators are likely to leave the Activation Lock disabled, as it is primarily a consumer feature. Should you decide to enable the feature:

TABLE 23. ACTIVATION LOCKS

Action	What to Do
Enable Activation Lock	Complete the following steps prior to device registration: 1. Turn on Find My Phone. 2. In the Security policy, select **Enable Activation Lock**. 3. Register the device. Ivanti EPMM acquires the bypass code at this time. Note that it can take some time before the device reports that the activation lock has been enabled.
Send Activation Lock Bypass Code	1. In the Device page, select the iOS device. 2. Select **Actions > Send Activation Lock Bypass Code**.

If you have a corporate-liable deployment, and your devices are unsupervised, activation lock will be enabled as soon as the end-user signs in to iCloud with their Apple ID and turns on Find My Device. MDM servers, including Ivanti EPMM, cannot control activation lock on **unsupervised** devices. Supervision is the flag that says this device is corporate owned. Device users can lock activation with their personal credentials, leaving you no recourse should they leave the company. For this scenario, Ivanti, Inc recommends the following process:

- Add the removal of the Activation Lock to your employee agreement.

  You should not consider the device returned unless the Activation Lock is removed.

- Confirm that the Activation Lock has been removed when the device is returned to you.

- Contact Apple Enterprise Support if the Activation Lock has not been removed.

Removing the Activation Lock

If the device has not been wiped, and the user is willing to enter the Apple ID password:

1. Launch the Settings app on the device.

2. Go to the iCloud screen.

3. Turn off Find My Device.

4. Have the device user enter the Apple ID password.

   Another option is to have the user erase all content and settings.

If the device has already been wiped, and the user is willing to enter the Apple ID password:

1. Follow the steps in Setup Assistant.

2. If the Activation Lock screen is displayed, have the device user enter the Apple ID and password or ask the user to remove the device from their account in iCloud.

If you have an enterprise support contract with Apple, you can contact them to request an activation lock removal.

Whitelisting Wi-Fi networks

You can limit the Wi-Fi networks iOS devices can join only to those Wi-Fi networks installed by profiles. This option enhances security, in that the Wi-Fi networks installed by profiles on iOS devices are secure, trusted networks. You enable this option in the security policy pushed to iOS devices.

This feature applies only to supervised devices running iOS 10.3 or supported newer versions.

Note the following:

- After you push the Wi-Fi whitelist restriction to devices, the restriction will work only if Ivanti EPMM has pushed at least one Wi-Fi network configuration to iOS devices using an MDM profile. The MDM profile with Wi-Fi configuration can only be pushed to devices through Ivanti EPMM (and not through any other means, such as Apple Configurator).

- If Ivanti EPMM removes all Wi-Fi configurations from the device, then the Wi-Fi whitelist restriction is removed as well.

- Enabling and disabling this feature causes Ivanti EPMM to push Wi-Fi configurations to devices. As such, try to minimize enabling and disabling this feature.

Procedure

1. Go to **Policies & Configs** > **Policies**.

2. Select the security policy for which you want to enable this feature.

3. Select **Edit**.

4. Select **Only join Wi-Fi networks installed by profiles (iOS 10.3 and later with supervised devices only)**.

5. Select **Save**.

Configuring firewall settings for macOS devices

You can use Ivanti EPMM to configure a macOS firewall setting for macOS devices. You use the firewall configuration to control connections made to managed macOS devices from other devices on your network on a per-application basis. The firewall configuration prevents managed macOS devices from accepting inbound connections from particular apps or services.

The application firewall is designed to work with TCP and UDP, without having any effect on AppleTalk connections. While you can disable ICMP pings by enabling stealth mode, you can still use earlier ipfw technology from the command line.

Procedure

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

2. Select **Add New** > **Apple** > **macOS only** > **Firewall**.

3. Use the guidelines in the table below to complete this form.

Item	Description
Name	Enter a name for the configuration.
Description	Enter an explanation of the purpose of this configuration.
Enable Firewall	Select to enable the firewall configuration for macOS devices.
Block all incoming connections	Select to prevent all sharing services from receiving incoming connections on macOS devices, such as screen sharing or file sharing. The following system services may still receive incoming connections: • configd, which implements DHCP and other network configuration services • mDNSResponder, which implements Bonjour • racoon, which implements IPSec
Enable stealth mode	Select to prevent macOS devices from responding to probing requests. Managed macOS devices still answer incoming requests for authorized apps, while ignoring unexpected requests, such as ICMP (ping).
Applications	Select specific apps for which you want to receive incoming connections on macOS devices. Select **Add+** to add a row to the list of apps. Select the cell under **Bundle ID** to select the app whose incoming connections you want to explicitly allow. Select the check box in the **Allow Connections** cell to allow incoming connections from the selected app.

4. Select **Save**.

5. Apply the policy to a macOS label.

Sync policies and battery use

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

Global App Config Settings policy

Administrators can create a global policies with different app settings (silent install, auto-update, mandatory, etc.) and can assign it to different labels. By creating a global policy, administrators can avoid editing each app and configuring the settings. When viewing and editing the per-label settings, administrators can set the app to default to the global setting so only the settings that are different for that label need to be changed.

Multiple global App Config Settings policies can be created. The name of the policies should be different; two policies cannot have the same name. Additionally, the exact-same labels should not be applied to them, for example, policy A and policy B cannot have "Android" labels applied to both of them.

- The policy can be prioritized
- The policy will work for both Android and iOS devices
- Applicable to all types of apps

Labels

After setting a basic global policy, administrators can then edit the settings for each label assigned to the app. This is done in the App Catalog, where you can select one or several apps and have the ability to apply this already-created global app configuration to one or more labels.

When viewing and editing the per-label settings, administrators can set the app to default to the global setting so only the settings that are different for that label need to be changed.

If there is an intersection of Policy Labels with App Labels matches, then Ivanti EPMM picks the matching policy as priority. Below are the possible ways to set the appropriate labels to the App Config Settings policy / policies.

TABLE 24. EXAMPLE A – LABEL SETTINGS

Item	Description
Apps:	• Gmail has label_1. • AnyConnect has label_2.
App Config Setting Policies:	• Policy_1 has label_1 with priority 1. • Policy_2 has label_2 with priority 2.
Device:	If device has label_1 and label_2, then the Gmail app will pick Policy_1 and the AnyConnect app will pick Policy_2.

TABLE 25. EXAMPLE B – LABEL SETTINGS

Item	Description
Apps:	• Gmail has label_1. • AnyConnect has label_2.
App Config Setting Policies:	• Policy_1 has label_1 and label_2.
Device:	If device has label_1 and label_2, then both the Gmail and AnyConnect apps will pick Policy_1.

TABLE 26. EXAMPLE C – LABEL SETTINGS

Item	Description
Apps:	• Gmail has label_1. • AnyConnect has label_2.
App Config Setting Policies:	• Policy_1 has label_1.
Device:	If device has label_1 and label_2, then the Gmail app will pick Policy_1 and the AnyConnect app will choose App Catalog settings.

TABLE 27. EXAMPLE D - LABEL SETTINGS

Item	Description
Apps:	• Gmail has label_2.
App Config Setting Policies:	• Policy_1 has label_1.
Device:	If device has label_1 and label_2, then the Gmail app will choose App Catalog settings.

TABLE 28. EXAMPLE E - LABEL SETTINGS

Item	Description
Apps:	• Gmail has label_1 and label_2.
App Config Setting Policies:	• Policy_1 has label_1 with priority 1. • Policy_1 has label_2 with priority 2.
Device:	If device has label_1 and label_2, then the Gmail app will pick Policy_1. The reason is Policy_1 has the highest priority.

Creating a new App Config Settings policy

This section covers how to set a global App Config Settings policy.

Procedure

1. In the Admin Portal, select **Policies & Configs > Policies**.
2. Select **Add New > App Config Settings**. The Add App Config Settings dialog box opens.
3. Enter the policy name in the **Name** field.
4. Select **Active** to enable the policy.
5. Select **Higher than** or **Lower than** in the **Priority** option, then select the other priority.

   This option is available only if you have two or more App Config Setting policies. Use it to select the priority on one policy over the other in cases of conflicts.

6. (Optional) Enter a **Description** of the policy.

7. In the **General**, **iOS Settings**, and/or **Android Settings** tabs, make your app configuration selections. For definitions of the fields, see "App Config Settings" below.

8. Click **Save**.

9. Edit / Update your labels. See Creating Labels in *Getting Started with Ivanti EPMM*.

10. Apply labels to your new App Config Settings policy / policies. See "Applying configurations to labels" on page 330.

11. In the **App Catalog**, edit your apps and select the **Use Global App Config Policy** option so the app will default to the App Config Settings policy.

12. In the **App Catalog**, apply labels to apps.

13. In the **Device Details > Apps** tab, for every app that the global App Config Settings policy is applied to, the name of that policy displays in the **Global Policy Name** column.

    The global policy will not be displayed under **Device Details > Policies tab** or in the Watchlist and Device Count columns under **Policies & Configs > Policies**.

App Config Settings

This section covers the field definitions for the global App Config Settings policy.

General tab > Common App Setting section

The General tab applies to both iOS and Android apps.

TABLE 29. GENERAL TAB - COMMON APP SETTINGS

Field	Description
Disable App Delivery Network for this App	If there is a content delivery network (CDN) enabled in Ivanti EPMM, administrators can choose to disable it for an app. This option displays only if a CDN is enabled.

iOS Settings tab

The iOS settings are only applicable if MDM setting is enabled.

TABLE 30. iOS SETTINGS – MANAGED APP SETTINGS

Field	Description
Prevent backup of the app data	Select to ensure that iTunes will not attempt to back up possibly sensitive data associated with the given app. ⓘ This setting is not displayed for iOS apps when Ivanti EPMM is configured for MAM-only iOS devices.
Remove app when device is quarantined or signed out	Select to enable configured compliance actions to remove the app if a policy violation results in a quarantined device or the device signs out in multi-user mode. To enable this feature, you must also configure a corresponding compliance action, and security policy with that compliance action selected. Once the device is no longer quarantined, the app can be downloaded again. • If you change the setting after the app is added, the changed setting will not be applied to the app. • This setting is not displayed for iOS apps when Ivanti EPMM is configured for MAM-only iOS devices. This option is ignored when "Use Global App Config Policy" and "Send convert unmanaged to managed app request for quarantine devices (iOS 9.0+)" is enabled for a particular app. For more information, see "Using Secure Sign-In and Sign-Out" on page 229.
Send installation request on device registration or sign in	Select to send a installation request upon device registration or sign-in. If the app is already installed on the device, Ivanti EPMM will do nothing. Deselected by default. For User Enrollment and Shared iPad devices for Apple Business Manager, this field will only send installation request on device registration or sign-in. Only Apple-licensed apps are sent to Shared iPad devices through registration. Deselected by default.
Send installation request to quarantine devices	Select to send an installation request to quarantine devices. Deselected by default.
Remove app when MDM profile is removed	Selected by default, this option removes the app from the device when the MDM profile is removed from the device.

TABLE 30. IOS SETTINGS – MANAGED APP SETTINGS (CONT.)

Field	Description
	ℹ️ This setting is not displayed for iOS apps when Ivanti EPMM is configured for MAM-only iOS devices.
Prevent user from removing and offloading app	Select this option to prevent device users from removing and uninstalling the managed app (for example, Ivanti Mobile@Work.) It also prevents the OS from automatically offloading apps that are not being used. When the device user tries to uninstall the app, a pop-up will state: "Uninstall Not Allowed - It is not possible to uninstall this app at this time." De-select to allow the device users to remove and uninstall the app. Applicable to iOS 14.0 or newer versions.

Android Settings tab

- The Android Settings apply to Android and Android Enterprise devices.
- Android Enterprise (all Modes) settings are applicable only if Google JSON is uploaded.
- Delegated Permissions are applicable to Android 8.0 and later.

TABLE 31. ANDROID SETTINGS TAB

Field	Description
Feature this App in the Apps@Work Catalog	Select if you want to highlight this app in the Featured apps list.
Silent install for Mandatory Apps	The app is installed when the device checks in with Ivanti EPMM. Device user action is not required. This feature only applies to devices that support silent installation. This feature is not supported for MAM-only Android devices. De-selecting the check box means the device user will need to manually install the app. If this check box is selected for Android Enterprise apps, the apps will be installed on the device with a higher priority than the "Silent install for work managed devices" option (irrespective of the constraints set for "Silent install for work managed devices.") This is because Ivanti EPMM will send the request to Google and Google then forwards the request to the Android devices.

TABLE 31. ANDROID SETTINGS TAB (CONT.)

Field	Description
	Administrators will need to disable "Silent install for Mandatory Apps" if they want to configure the apps via the "Silent install for work managed devices" option. For more information, see Silent install and uninstall of mandatory apps in the *Ivanti EPMM Apps@Work Guide*. If the Android Enterprise public app is rendered as an AOSP in-house app, then use the **Silent install for work managed devices** option to install the app silently on the AOSP-device owned (DO) device. Applicable to: • Samsung SAFE devices MDM version 1.0+ • Zebra MX 4.4+ • LG devices
Enforce this version for Mandatory Apps	Select to ensure that every version of the same app is installed, including the latest version. The version enforcement feature is supported only with regular (non-AppConnect) in-house apps. It does not apply to AppConnect apps or Google Play apps. Use the version enforcement feature to: • Ensure devices have the in-house app installed, regardless of version number. • Lock users to a particular version of the Ivanti Mobile@Work app. This applies to organizations that install Ivanti Mobile@Work as an in-house app instead of installing it from Google Play. • Ensure users do not upgrade to a new version of an in-house app while the newer version is still undergoing testing. • Downgrade users to a previous version of an in-house app. See Enforcement of specific app versions for mandatory in-house apps in the *Ivanti EPMM Apps@Work Guide*.

TABLE 31. ANDROID SETTINGS TAB (CONT.)

Field	Description
Require the user to install the latest version of the app in order to run it.	Select to ensure the device user installs the latest version of this app. **ⓘ IMPORTANT:** You must select this check box for the entries for each version of this same app in order for this feature to take effect. Clear the check box for all versions of this app to allow users to work with any version of this app. For more information, see Specify latest version required for a secure app in the *Ivanti EPMM Apps@Work Guide.*
Silent install for work managed devices	This feature is specifically for private in-house Android Enterprise apps and applies only to devices that support silent installation. Clearing the check box means the device user will need to manually install the app. If this check box is selected, then the apps will be installed on the device according to the app constraints and time it takes to install. The app is installed when the device checks in with Ivanti EPMM. Device user action is not required. If "Silent install for Mandatory Apps" is enabled along with "Silent install for work managed devices," then "Silent install for Mandatory Apps" will take precedence and the app will be installed on the device irrespective of the constraints set for the "Silent install for work managed devices" option. Administrators will need to disable "Silent install for Mandatory Apps" if they want to configure the apps via the "Silent install for work managed devices" option. **ⓘ** Silent install is not supported for MAM-only Android devices. Additional settings can be made for silent installs of work managed devices. These settings are applicable for public and private apps. Prerequisite apps are pushed before dependent apps. **Auto Install Mode** - Self hosted apps will not be auto installed. • Force Install (default) • Auto Install Once - recommended by Ivanti.

TABLE 31. ANDROID SETTINGS TAB (CONT.)

Field	Description
	App Download Priority - You can prioritize downloading of specific apps before other apps. For example, prioritizing the download of Tunnel and Email apps before other non-critical apps. • Low • Medium (default) • High **Install only when connected to Wi-Fi** - Default is de-selected. **Install only when charging** - Default is de-selected. **Install only when Idle** - Default is de-selected. For more information, see Silent install and uninstall of mandatory apps in the *Ivanti EPMM Apps@Work Guide*. If the Android Enterprise public app is rendered as an AOSP in-house app, then use the **Silent install for work managed devices** option to install the app silently on the AOSP-device owned (DO) device.
Silently install Mandatory Apps	This feature only applies to devices that support silent installation. This feature is not supported for MAM-only Android devices. Selected by default. De-selecting the check box means the device user will need to manually install the app. If this check box is selected for Android Enterprise apps, the apps will be installed on the device with a higher priority than the "Silent install for work managed devices" option (irrespective of the constraints set for "Silent install for work managed devices.") This is because Ivanti EPMM will send the request to Google and Google then forwards the request to the Android devices. ⓘ Administrators will need to disable "Silent install for Mandatory Apps" if they want to configure the apps via the "Silent install for work managed devices" option. For more information, see Silent install and uninstall of mandatory apps in the *Ivanti EPMM Apps@Work Guide*. If the Android Enterprise public app is rendered as an AOSP in-house app, then use the **Silent install for work managed devices** option to install the app silently on the AOSP-device owned (DO) device.

TABLE 31. ANDROID SETTINGS TAB (CONT.)

Field	Description
Block Widget on Home Screen	If selected, the app cannot place widgets on the home screen on work profile devices. For example, calendar apps are not permitted to place calendar widgets on the home screen. Applicable only to apps installed in the Managed profile.
Block Uninstall	Selected by default, this feature prevents the device user from uninstalling the app.
Quarantine app when device is quarantined	Required for Work Profile mode, Work Managed Device mode, and Managed Device with Work Profile mode. Selected by default, this enables configured compliance actions to hide the app if a policy violation results in a quarantined device. This is a required selection for Work Profile mode, Work Managed Device mode and Managed Device with Work Profile mode. A second step is required to enable this feature: configure a corresponding compliance action and security policy with that compliance action selected. Once the device is no longer quarantined, the app can be used again. If this option is deselected, the app is available for usage, even when the device is quarantined. ⓘ If you change the setting after the app is added, the changed setting will be applied to the app.
Auto Launch Application on Install	Selected by default. After installation, the Ivanti Mobile@Work app would be in the foreground when launching apps. Applicable to Android devices in: • Work Profile mode • Work Profile on Company Owned Device mode
Update Priority	Select from the drop-down: Default, High Priority, Postpone for 90 days
Minimum Version Code	Select from the drop-down the version code number.
Configure third-party app runtime permissions	Select this check box to modify runtime permissions for other apps. • Applicable to public / private apps on Work Managed Device mode on Android 8.0 or newer versions

TABLE 31. ANDROID SETTINGS TAB (CONT.)

Field	Description
	- Applicable to in-house apps and public / private apps on Managed Device with Work Profile (COPE) mode on Android devices versions 8-10. - Applicable to only public / private apps on all managed work Profiles, including Work Profiles on Company Owned Devices mode Android versions 11.0 or newer versions.
Hide and suspend third-party apps	Select this check box to delegate third-parties to have permission to hide and suspend the selected app. - Applicable to in-house and public / private apps for Work Managed Device mode and Managed Devices with Work Profile (COPE) mode starting from Android 8. - Applicable to public / private apps on managed profiles. - Applicable to public / private apps on Work Profile on Company Owned Device mode starting from Android 11.
Manage certificates	Select this check box to delegate permission for managing certificates. - Applicable to in-house and public / private apps for managed devices and Managed Devices with Work Profile (COPE) mode starting from Android 8. - Applicable to public / private apps on managed profiles. - Applicable to public / private apps on Work Profile on Company Owned Device mode starting from Android 11.

Work Schedule policy

This policy allows administrators to set work schedules for device users. After the scheduled work time, users are blocked from accessing specified apps and services, which include:

- Exchange Active Sync services
- AppConnect-enabled apps
- Managed apps that use Tunnel on Sentry

After the scheduled work time-period, users are unable to open any of these apps or services. In its place, users see a message indicating that access is not available. Message can vary, depending on the app or service they attempt to use. The policy starts and ends after the next scheduled sync following the specified start time and duration period.

This section contains the following procedures:

- "Adding a Work Schedule policy" below
- "Applying a Work Schedule policy" on the next page
- "Managing a Work Schedule policy" on the next page
- "Setting up Work Schedule policy notifications" on the next page

Adding a Work Schedule policy

Use this procedure to add a policy that sets a work schedule and blocks apps and services outside of the scheduled time.

> **i** Enforcement of this policy requires Standalone Sentry 9.0.0.

Procedure

1. Log into the Admin Portal.
2. Select **Policies & Configs > Policies > Add New > Work Schedule**.
3. Enter the policy name in the **Name** field.
4. Select **Active** to enable the schedule.

   Select **Inactive** to disable the policy.

5. Select **Higher than** or **Lower than** in the **Priority** option, then select the other priority.

   This option is available only if you have two or more Work Schedule policies. Use it to select the priority on one policy over the other in cases of conflicts.

6. Use the drop down to select a **Timezone**, which defines the start and end times for the policy.

7. Set up the weekly work schedule.

   The policy treats unchecked days as a time period outside of the work schedule, blocking affected

apps and services for that 24-hour period.

8. Select **Save** to add the policy to the **Policies** page.

Applying a Work Schedule policy

Ivanti EPMM sends the policy to Sentry and Sentry enforces the policy. When you apply the policy to a label, any device associated with the selected label will receive the policy during the next sync between the Sentry and the device.

Procedure

1. Log into the Admin Portal.

2. Select **Policies & Configs > Policies**.

3. Select the work schedule policy.

4. Select **Actions > Apply to Label**.

5. Select one or more labels and select **Apply**.

Managing a Work Schedule policy

Use this procedure to modify or delete a work schedule policy.

Procedure

1. Log into the Admin Portal.

2. Select **Policies & Configs > Policies**.

3. Select the work schedule policy you want to manage.

   a. Select **Edit** to modify the work schedule, then select **Save**.

   b. Select **Actions > Delete** to delete the policy.

Setting up Work Schedule policy notifications

Use this procedure to modify or delete a work schedule policy.

Procedure

1. Log into the Admin Portal.
2. Select **Logs > Event Settings**.
3. Select **Add New > Device Status Event**.

4. Complete the form and check **Work schedule policy applied**.

   See the "Working with Events" section for details.

5. Select **Save**.

Country changes and alerts

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

iOS location-based wakeups interval and syncing with Ivanti EPMM

Location-based wakeup intervals enable Ivanti EPMM to periodically wake Ivanti Mobile@Work for iOS, which then reports any critical changes to Ivanti EPMM. This feature allows changes to be communicated to Ivanti EPMM without having to manually start Ivanti Mobile@Work .

Independent of the location-based wakeup interval, iOS may wake Ivanti Mobile@Work based on changes in cell tower location. In this case, the app determines whether device details have been sent to Ivanti EPMM within the specified iOS location-based wakeup interval. If device details have not been sent during that interval, then Ivanti Mobile@Work sends device details to Ivanti EPMM. If Ivanti Mobile@Work wakes up and determines that the device has been compromised or the SIM state has changed, this information is immediately sent to Ivanti EPMM.

Single-app mode policies

Single-app mode enables you to configure an iOS device for kiosk use, restricting use of the device to the designated app. For example, you might want to configure an iPad for use as an electronic catalog. The Home button and features such as taking a screenshot or receiving notifications are disabled. The device returns to the specified app automatically when it wakes or is rebooted.

Note the following:

- Single-app mode policy applies only to supervised devices running iOS 6 or supported newer versions.
- AppConnect apps or in-house apps developed with the AppConnect wrapper (including AppConnect apps available on the Apple App Store, such as Ivanti Email+ for iOS and Ivanti Web@Work for iOS) **cannot** run in single-app mode.
- The single-app mode policy is different from the single-app mode restriction, which allows you to whitelist apps capable of autonomously running in single-app mode. For more information about the single-app mode restriction, see "iOS / tvOS settings" on page 719.
- Make sure to install the app you want to use in single-app mode before placing your devices in single-app mode, otherwise, the device will get stuck in single-app mode without an app.

Procedure

1. Select **Policies & Configs > Policies > Add New > iOS and macOS > iOS Only > Single-App Mode**.

2. In the New Single-App Mode Policy dialog box, use the following guidelines to complete this form:

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. It is recommended to use unique names across policy types to allow for clearer log entries.
Status	Select **Active** to enable the policy, or **Inactive** to disable it. Only one active single-app mode policy can be applied to a device. You can define two single-app mode policies and send them to supervised devices, for example, as long as only one of the policies is active. You can easily switch policies by inactivating the policy you want to disable and then forcing a device check-in. Supervised devices can have any number of policies that you can activate at any time, but only one policy is active.

Item	Description
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B". ⓘ Priority will only work when the policies (lower and higher priority) are applied together via label to the device after it's initial registration is done. In this case, higher priority will take precedence; for the rest of the cases, priority will not work.
Description	Enter an explanation of the purpose of this policy.
Identifier	Enter the bundle ID of the app to be used in single-app mode. Example: com.apple.mobilesafari.

Settings (These settings apply only to supervised devices running iOS 7 through iOS 9.3.)

Auto Lock	Select to enable iOS to put the screen to sleep after a set period.
Device Rotation	Select to enable device rotation.
Mono Audio	Select to play all audio through a single mono channel.
Ringer Switch	Select to enable the ringer switch so that device users can use it to mute the sound on the device.
Sleep/Wake Button	Select to enable the Sleep/Wake button so that device users can put to sleep or wake their devices.
Speak Selection	Select to enable speak selection.
Touch Screen	Select to enable basic touch controls, such as tapping and pinching.
Volume Buttons	Select to enable volume adjustments using the volume buttons.
User Enabled Settings	*Enable*

Item	Description	
Assistive Touch	Select to enable Assistive Touch so that device users can modify their screen interactions and use a compatible adaptive accessory.	Aside from activating these settings on supervised devices, you can also enable device users to manage these options for themselves.

Select **Enable** for each setting you want device users to control themselves. |
Invert Colors	Select to enable the use of invert colors. Invert color displays are high contrast, and can be helpful for visually impaired device users.	
Voice Over	Select to enable Voice Over controls used to enter text or perform other tasks using voice, such as the device reading aloud artifacts that a device user taps.	
Zoom	Select to allow device users to magnify the screen.	

3. Click **Save**.

4. Apply the policy to the relevant labels.

Finding the bundle ID

To determine the bundle ID:

1. Sync your device to your iTunes library.
2. On your PC or Mac, open the Mobile Applications folder in the iTunes library.
3. Duplicate the app file and assign a .zip extension.
4. Open the iTunesMetadata.plist file in the zip file.
5. Find the softwareVersionBundleId key in the list.

Configuring a global HTTP proxy policy

By imposing a global HTTP proxy policy on supervised iOS 6 through iOS 9.3 devices, you can ensure that HTTP traffic is redirected to the proxy server you specify. You can manually enter the proxy server URL and port number, or the URL for the relevant PAC (proxy auto-configuration) file, which automatically determines the correct proxy server to use for a given URL. If the policy does not include a URL to the PAC file, then the policy uses WPAD (web proxy auto-discovery) to attempt to locate the PAC file.

The global HTTP proxy policy can include two features that provide solutions on-the-fly for when devices cannot access the proxy server:

- **Direct connection**: For circumstances where the PAC file is unreachable, you can specify that the policy create a direct connection to the requested URL, bypassing the proxy server altogether. This option applies only to automatic proxy connections.

- **Proxy bypass**: You can configure the policy to bypass the proxy server altogether when a device attempts a connection to a captive network such as a wifi hotspot at a coffee shop or a hotel. Selecting this option allows the device to connect directly to the captive network. Device users establish uninterrupted wifi internet access by logging in through the captive portal before the policy redirects them to the proxy server.

If your organization uses a proxy server to provide data leak protection or content filtering, for example, a global HTTP proxy policy allows you to direct HTTP traffic to and from supervised iOS 6 through iOS 9.3 devices to the proxy server of your choice.

The direct connection and proxy bypass features allow supervised iOS 7 through iOS 9.3 devices to continue accessing the internet even if:

- The PAC file referenced in their global HTTP proxy policy is unavailable

  OR

- They must first log in to a captive portal before accessing a wifi hotspot.

> (i) The direct connection and proxy bypass options apply only to supervised iOS 7 through iOS 9.3 devices.

> (i) **IMPORTANT:** Confirm that you have specified the correct proxy information, and the proxy is reachable. An invalid or unreachable proxy server will make the device unreachable by the network. In this case, physical access is required to reset the device.

Procedure

1. Go to **Policies & Configs > Policies**.

2. Select **Add New > iOS and macOS > iOS Only > Global HTTP Proxy**.

3. In the New Global HTTP Proxy Policy dialog box, use the guidelines in "Global HTTP Proxy Policy" on the next page to complete this form.

4. Click **Save**.

5. Apply the policy to the appropriate labels.

Global HTTP Proxy Policy

Below are the setting definitions for the New Global HTTP Proxy Policy dialog box.

TABLE 32. GLOBAL HTTP PROXY POLICY

Items	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.
Status	Select **Active** to turn on this policy. Select **Inactive** to turn off this policy. **Why:** Use the Status feature to turn a policy on or off across all phones affected by it. The policy definition is preserved in case you want to turn it on again.
Priority	Specifies the priority of this custom policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is associated with a specific device. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B". Because this priority applies only to custom policies, this field is not enabled when you create the first custom policy of a given type.
Description	Enter an explanation of the purpose of this policy.
Proxy Type: Manual	
Manual	If you select Manual, specify the proxy server address and port through which all HTTP traffic will be directed. Optionally, enter values for the username and password used for devices to authenticate with the proxy server. If you do enter a value for the password, go to **Settings > System Settings > Users & Devices > Registration > Save User Password Preferences** and select **Save User Password**. If you do not enter values for the proxy server username and password, supervised device users will need to enter a username and password every time they access the proxy server.
Proxy Server	Enter the network address for the proxy server.
Proxy Server Port	Enter the port number for the proxy server.
User Name	Optional. Enter the user name for authenticating with the proxy server.

TABLE 32. GLOBAL HTTP PROXY POLICY (CONT.)

Items	Description
	You can use any of the following variables for the username value: `$USERID$`, `$EMAIL$`, `$USER_CUSTOM1$`, `$USER_CUSTOM2$`, `$USER_CUSTOM3$`, `$USER_CUSTOM4$`. You can also combine text with variables, such as `$USERID$:$USER_CUSTOM1$` or `$USERID$_$USER_CUSTOM1$`. Custom attribute variable substitutions are supported.
Proxy Password	Optional. Enter the password for authenticating with the proxy server. You can use any of the following variables for the password value: `$PASSWORD$`, `$USER_CUSTOM1$`, `$USER_CUSTOM2$`, `$USER_CUSTOM3$`, `$USER_CUSTOM4$`. You can also combine text with variables, such as `$PASSWORD$:$USER_CUSTOM1$` or `$PASSWORD$_$USER_CUSTOM1$`. Custom attribute variable substitutions are supported.
Allow bypassing proxy to access captive networks	Selecting this feature allows the device to display the login page for captive networks (such as a LAN at a coffee shop which customers access through wifi), bypassing the proxy server altogether. Deselected by default. ⓘ This feature applies only to iOS 7 through iOS 9.3 devices.
Proxy Type: Auto	
Auto	If you select Auto, enter the URL of the PAC (proxy auto-configuration) file, which specifies the location of the proxy server. The PAC file enables web browsers and user agents to automatically select the correct proxy server for any requested URL.
Proxy PAC URL	Optional. Enter the URL for the proxy auto-configuration (PAC) file. If you leave this field blank, the device will use the web proxy auto-discovery (WPAD) protocol to guess the location of the PAC file.
Allow direct connection if PAC is unreachable	Selecting this feature allows the supervised device to access the requested URL directly (without the proxy server), if the proxy auto-configuration file cannot be reached. Deselected by default. ⓘ This feature applies only to iOS 7 through iOS 9.3 devices.
Allow bypassing proxy to access captive networks	Selecting this feature allows the device to display the login page for captive networks (such as a LAN at a coffee shop which customers access through wifi), bypassing the proxy server altogether. Deselected by default. ⓘ This feature applies only to iOS 7 through iOS 9.3 devices.

Related topics

- "Impact to tunneling when using a global HTTP proxy" in the *AppConnect Guide for EPMM*.

Cellular policies

ℹ️ Apple disabled APN settings in iOS 9.0, but re-enabled APN settings in iOS 9.0.1. Ivanti strongly recommends creating a cellular policy for new configurations.

Ivanti EPMM provides a cellular policy that defines the network path for cellular data connectivity, or the Access Point Name (APN). It is possible to configure a cellular data policy using an APN setting or a cellular policy, depending on the version of iOS running on a given device.

The cellular policy allows you to define a customized APN for devices without disrupting device users' cellular connectivity. The cellular policy in Ivanti EPMM supports Apple's configuration profile com.apple.cellular payload.

The cellular policy includes the following information:

- A name and description

- Active or inactive status

- A username and password for connecting to the cellular network

- Priority, if more than one cellular policy is defined in Ivanti EPMM

- The preferred method of authenticating with the cellular network

- An Access Point Name (APN), which defines the gateway between the mobile network and your computer network

ℹ️ Cellular policies can be applied to devices running iOS 7 through the most recently released version of iOS or supported newer versions.

Only one cellular policy can be used on a device at any given time. A cellular policy cannot co-exist with an APN setting on the same device. If you upgrade a device from iOS 8 to iOS 9, for example, you must remove the APN setting and apply a cellular policy.

Migrating devices from an APN setting to a cellular policy

If you are managing devices with an APN setting applied, you will need to migrate these devices to a cellular policy.

1. Make sure the devices are connected to a Wi-Fi network.

2. Apply the relevant iOS devices to a label, and remove the APN setting from that label.

3. Ensure the APN setting has been removed from iOS devices in the label.

4. Apply the new cellular policy to the label applied to the iOS devices.

Defining a cellular policy

If you define more than one cellular policy, you can set the priority of each policy in relation to the others. For instance, if you define three policies, you can configure each policy to take precedence over the next, such that policy 1 would take priority over policy 2, which, in turn, would take priority over policy 3. Note that the most recent priority setting overrides the previous. For example, if you edit policy 3 to take higher priority than policy 2, then the order of priority shifts to policy 1, policy 3, policy 2.

All things being equal, this means that policy 1 will be applied to devices. If, however, policy 1 is only applied to label 1, this means that policy 3 will be applied to label 2.

To define a cellular policy:

1. Go to **Policies & Configs > Policies**.

2. Click **Add New**.

3. Select **iOS and macOS > iOS Only > Cellular**.

   The New Cellular Policy dialog box opens.

4. Use the table in as a guideline for filling out the form.

5. Click **Save**.

6. Go to **Actions > Apply To Label**.

7. Select the label or labels to apply from the **Apply To Label** dialog.

8. Click **Apply**.

Cellular policy settings

The following table describes the settings available in the New Cellular Policy window. For more information about creating a cellular policy, see "Defining a cellular policy" on the previous page.

TABLE 33. CELLULAR POLICY SETTINGS

Item	Description
Name	Enter a name for the cellular policy.
Status	Select **Active** to enable the policy, or **Inactive** to disable it.
Priority	Set the priority of cellular policies if there is more than one cellular policy. If you want to place greater priority on this cellular policy than another, select **Higher than**, and then select the cellular policy over which this policy will take priority. If you want to place lesser priority on this cellular policy than another, select **Lower than**, and then select the cellular policy that will be used before the one you are defining.
Description	Enter a description of the cellular policy.
User Name	Enter a user name for authentication.
Password	Enter a password for authentication.
Authentication Type	Select **CHAP** to use Challenge-Handshake Authentication Protocol (CHAP) to authenticate the user with the cellular carrier. Select **PAP** to use Password Authentication Protocol (PAP) to authenticate the user with the cellular carrier.
Protocol Mask	Select the version of Internet Protocol you would like to enable for this cellular policy: **IPv4**, **IPv6**, or **Both**.
APN Configurations	Click **+** to configure the name of the gateway between a mobile network and your computer network. ⓘ Currently, iOS only uses the first APN setting from the list of APN settings. For each APN, enter the following values: • **Name**: Enter a name for the APN. • **Authentication Type**: Enter the authentication type.

TABLE 33. CELLULAR POLICY SETTINGS (CONT.)

Item	Description
	• **User Name**: Enter a username for authenticating with the cellular network. • **Password**: Enter a password for authenticating with the cellular network. • **Proxy server**: Enter the URL of the proxy server on the cellular network. • **Port**: Enter the port number for the proxy server. • **Enable XLAT-464**: Choose whether to enable the XLAT-464 option. • **Roaming Protocol Mask**: Select the IP version to use for roaming in the context of this cellular policy: **IPv4**, **IPv6**, or **Both**. **Note**: Ivanti EPMM now supports the `Cellular.APNsItem EnableXLAT464` Apple property, which enables the XLAT-464 option to provide access service for IPv6 across IPv6 networks. • **Domestic Roaming Protocol Mask**: Select the default IP version to use for domestic roaming in the context of this cellular policy: **IPv4**, **IPv6**, or **Both**. **Note**: Starting with Ivanti EPMM 11.8.0.0, the Apple `Cellular.APNsItem DefaultProtocolMask` deprecated property is no longer supported.

Configuring an eSIM refresh cellular plan policy

An embedded SIM ("eSIM") can digitally store the information that is normally stored on a physical SIM card. Because the encrypted eSIM is not linked to a specific cellular carrier, it is easy to switch from one carrier to another.

In order to activate eSIM cellular plan profiles, configure devices to query and respond to a carrier URL that is provided by your carrier.

Examples of carrier URLs:

- **Verizon:** https://2.vzw.otgeuicc.com

- **AT&T:** https://cust-001-v4-prod-atl2.gdsb.net

- **T-Mobile:** https://t-mobile.gdsb.net

This feature is applicable only to iPad devices with iPadOS 13.0+ and 14.0+ that have a cellular plan.

Activity related to eSIM is tracked in the logs. You can view the eSIM ID in the Device Details page; see .

> To delete a cellular plan, you can wipe the device. However, if you want to keep the data plan on the device, deselect the **Preserve data plan** field in the Wipe dialog box (**Devices > Actions > Wipe**.)

Procedure

1. Go to **Policies & Configs > Policies**.

2. Click **Add New**.

3. Select **iOS and macOS > iOS Only > eSIM Refresh Cellular Plan**.

   The eSIM Refresh Cellular Plan dialog box opens.

4. Use the information in Table 2 below, eSIM Refresh Cellular Plan Policy Settings, as a guideline for filling out the form.

5. Click **Save**.

TABLE 34. eSIM Refresh Cellular Plan policy settings

Item	Description
Name	Enter a name for the eSIM Refresh Cellular Plan policy.
Status	Select **Active** to enable the policy, or **Inactive** to disable it.
Priority	Set the priority of cellular policies if there is more than one cellular policy.
	If you want to place greater priority on this cellular policy than another, select **Higher than**, and then select the cellular policy over which this policy will take priority.
	If you want to place lesser priority on this cellular policy than another, select **Lower than**, and then select the cellular policy that will be used before the one you are defining.

TABLE 34. eSIM REFRESH CELLULAR PLAN POLICY SETTINGS (CONT.)

Item	Description
Description	Enter a description of the eSIM Refresh Cellular Plan policy.
eSIM Cellular Plan URL	Enter the eSIM cellular plan URL that will be used.
	For the correct URL to use, check:
	https://www.apple.com/ipad/cellular/

Wallpaper policies

Use the wallpaper policy to set the wallpaper of the home and locked screens of supervised iOS devices to images of your choice. By setting the wallpaper using the wallpaper policy, the wallpaper is automatically applied to the device when the device registers with Ivanti EPMM.

This feature is useful in a kiosk setting, or shared device environment in a retail setting.

In the wallpaper policy you can choose:

- Images for iPhone and iPod devices

- Images for iPad devices

In both cases, you can choose the same image or different images for the home screen and locked screen.

Note the following:

- You can also set the wallpaper **manually** on a device that is already registered by using the Admin Portal action **Set Wallpaper**.

- You cannot export, import, or make a copy of (save as) a wallpaper policy.

Related topics

- "Configuring a wallpaper policy" on the next page

- "Wallpaper policy settings" on the next page

- "Manually setting the wallpaper for iOS devices" on page 125

Configuring a wallpaper policy

Configure a wallpaper policy so that the home and locked screens of supervised iOS devices use images of your choice. The wallpaper is automatically applied when a device registers with Ivanti EPMM.

Procedure

1. Go to **Policies & Configs > Policies**.

2. Select **Add New**.

3. Select **iOS and macOS > iOS only > Wallpaper**.

   The Wallpaper Policy window is displayed.

4. See "Wallpaper policy settings" below as a guideline for filling out the form.

5. Select **Save**.

6. Go to **Actions > Apply To Label**.

   > ℹ️ Wallpaper policies are supported on supervised devices and should be associated to a "Supervised" label.

7. Select the label or labels to apply from the **Apply To Label** dialog box.

8. Select **Apply**.

> ℹ️ The files that you upload when creating the policy are listed in the **Policy Details** pane that displays when you select the policy's row in **Policies & Configs > Policies**. However, when you edit a wallpaper policy, the files are not listed in the **Wallpaper Policy** screen.

Related topics

- "Wallpaper policies" on the previous page

- "Wallpaper policy settings" below

- "Manually setting the wallpaper for iOS devices" on page 125

Wallpaper policy settings

The following table describes the settings available in the wallpaper policy.

TABLE 1. WALLPAPER POLICY SETTINGS

Item	Description
Name	Enter a name for the wallpaper policy.
Status	Select **Active** to enable the policy, or **Inactive** to disable it.
Priority	Set the priority of wallpaper policies if there is more than one wallpaper policy. If you want to place greater priority on this wallpaper policy than another, select **Higher than**, and then select the wallpaper policy over which this policy will take priority. If you want to place lesser priority on this wallpaper policy than another, select **Lower than**, and then select the wallpaper policy that will be used before the one you are defining.
Description	Enter a description of the wallpaper policy.
iPhone/iPod Wallpaper	
Use same image for Home Screen and Lock Screen	Select this option to use the same image for both the home screen and the lock screen on iPhone and iPod devices. When selected, the display changes to allow you to upload only one file.
Home Screen	Choose the file for the home screen image. File requirements: • either PNG or JPG format • less than 5 MB*
Lock Screen	Choose the file for the lock screen image. File requirements: • either PNG or JPG format • less than 5 MB*
iPad Wallpaper	
Use same image for Home Screen and Lock Screen	Select this option to use the same image for both the home screen and the lock screen on iPad devices. When selected, the display changes to allow you to upload only one file.

Item	Description
Home Screen	Choose the file for the home screen image. File requirements: • either PNG or JPG format • less than 5 MB*
Lock Screen	Choose the file for the lock screen image. File requirements: • either PNG or JPG format • less than 5 MB*

* 5 MB are acceptable and are applied to the devices with the appropriate labels. However, larger files can have unpredictable performance impact on Ivanti EPMM. The performance impact is due to Ivanti EPMM requiring multiple device check-ins to apply the wallpaper to all devices. The performance impact depends on the size of the file and on the number of devices impacted. Note that the wallpaper file size does not impact any other actions that Ivanti EPMM performs on device check-in.

Related topics

- "Wallpaper policies" on page 300

- "Configuring a wallpaper policy" on page 301

- "Manually setting the wallpaper for iOS devices" on page 125

Accessibility Settings Policy

In 11.11.0.0 release, a new Accessibility Settings Policy is added, which will provide the administrator with the ability to configure the following accessibility controls remotely for supervised iOS devices.

Configuring a Accessibility Setting policy

Procedure

1. Go to **Policies & Configs > Policies**.

2. Select **Add New**.

3. Select **iOS and macOS > iOS only > Accessibility Setting**.

   The Accessibility Setting Policy window is displayed.

4. See "Accessibility Setting policy settings" below as a guideline for filling out the form.

5. Select **Save**.

6. Go to **Actions > Apply To Label**.

   > **i** Accessibility Setting policies are supported on supervised devices and should be associated to a "Supervised" label.

7. Select the label or labels to apply from the **Apply To Label** dialog box.

8. Select **Apply**.

Accessibility Setting policy settings

The following table describes the settings available in the accessibility setting policy.

TABLE 1. ACCESSIBILITY SETTING POLICY SETTINGS

Item	Description
Name	Enter a name for the accessibility setting policy.
Status	Select **Active** to enable the policy, or **Inactive** to disable it.
Priority	Set the priority of accessibility setting policy, if there is more than one accessibility setting policy. If you want to place greater priority on this accessibility setting policy than another, select **Higher than**, and then select the accessibility setting policy over which this policy will take priority. If you want to place lesser priority on this accessibility setting policy than another, select **Lower than**, and then select the accessibility setting policy that will be used before the one you are defining.
Description	Enter a description of the accessibility setting policy.
Bold Text Enabled (Boolean)	If true, enables bold text.
Increase Contrast Enabled (Boolean)	If true, enables increase contrast.

Item	Description
Reduced Motion Enabled (Boolean)	If true, enables reduced motion.
Reduce Transparency Enabled (Boolean)	If true, enables reduced transparency.
Text Size	The accessibility text size apps that support dynamic text use. 0 is the smallest value, and 11 is the largest value available. Default value is 4.
Touch Accommodations Enabled (Boolean)	If true, enables touch accommodations.
Voice Over Enabled (Boolean)	If true, enables voice over.
Zoom Enabled (Boolean)	If true, enables zoom.

Device name policies

Use the Device Name policy to set the name of supervised iOS devices of your choice. By setting the device names using this policy, the device name is automatically applied to the iOS device when the device registers with Ivanti EPMM.

This feature is useful in a kiosk setting, or shared device environment in a retail setting.

In the device name policy you can set the name using substitution variables that may be used to dynamically create a device name. Editing this name will result in all iOS supervised device names being updated. For any supervised iOS device with the policy, when the device checks in, Ivanti EPMM will check the current device name and compare it with the resolved desired device name. If the names are different, Ivanti EPMM will send a command to change the device name and queue a check-in at a later time.

Note the following:

- After a device name policy is applied to a device, the device name settings are not removed from the device if you delete the policy or remove the device's label from the policy.

- If the device user changes the device name, at every sync, Ivanti EPMM will check to see if the device name is the expected one for the policy assigned and, if it does not match, enforce / resend the device name command. Ivanti EPMM will continue to do this as long as the policy is assigned.

- You cannot export, import, or make a copy of (save as) a device name policy.

- Advanced search and labels supports iOS device names, i.e., ios.DeviceName, so administrators must be careful how they use the device name as a label since the device user could change the device name themselves, thus making the device fall out of the label until the device name was changed back.

- If the device's attribute is set to NULL, the Device Name policy will remain in a pending state.

- When the device belongs to the device name policy, it displays as Applied in the Device Details page.

Related topics

- "Configuring a device name policy" below

- "Device name policy settings" on the next page

Configuring a device name policy

Configure a device name policy so that the supervised iOS devices use names of your choice. The device name policy is automatically applied when a device registers with Ivanti EPMM.

Procedure

1. Go to **Policies & Configs > Policies**.

2. Select **Add New**.

3. Select **iOS and macOS > iOS only > Create Device Name**.

   The Add Device Name Policy dialog box opens.

4. See "Device name policy settings" on the next page as a guideline for filling out the form.

5. Select **Save**.

6. Go to **Actions > Apply To Label**.

   > ℹ️ Device name policies are supported on supervised devices and should be associated to a "Supervised" label.

7. Select the label or labels to apply from the **Apply To Label** dialog box.

8. Select **Apply**.

Device name policy settings

The following table describes the settings available in the device name policy.

TABLE 1. WALLPAPER POLICY SETTINGS

Item	Description
Name	Enter a name for the device name policy.
Status	Select **Active** to enable the policy, or **Inactive** to disable it.
Priority	Set the priority of device name policies if there is more than one device name policy.
	If you want to place greater priority on this device name policy than another, select **Higher than**, and then select the device name policy over which this policy will take priority.
	If you want to place lesser priority on this device name policy than another, select **Lower than**, and then select the device name policy that will be used before the one you are defining.
Description	Enter a description of the device name policy.
Device Name	Type $ to see list of variables that may be used to dynamically create a device name. Editing this name will result in all iOS supervised device names being updated.
	Examples:
	• Device Name: $EMAIL$'s device resolves to jsmith@invanti.com's device
	• Device Name: $USERID$ - $MODEL$ device resolves to jsmith - iPad device.
	For more information about substitution variables, see "Substitution variables for compliance policy rules" on page 358.

Customizing a home screen layout

You can customize the layout of the home screen on managed devices. You can define multiple home screen layout policies, and prioritize the use of each. This allows for a unified look and feel across devices, or groups of devices.

Customized components of the home screen layout include the dock and additional home page screens, if desired. The dock can include Ivanti EPMM App Catalog apps, whereas customized home pages can include custom folders, as well as apps. There is no option to change menus or control panel options.

This feature is supported on supervised devices running iOS 9.3 or supported newer versions.

> Specifying a web clip in this payload does not create the web clip. Use the WebClip payload to create a web clip on the device.

Procedure

1. Go to **Policies & Configs > Policies**.

2. Select **Add New**.

3. Select **iOS and macOS > iOS Only > Home Screen Layout**.

4. The Add Home Screen Layout Policy dialog box opens.

5. Define a home screen layout policy, using the following table as a guideline.

Item	Description
Name	Enter a name for the home screen layout policy.
Status	Select **Active** to enable the home screen layout policy, or **Inactive** to disable it.
Priority	Set the priority of the home screen layout policies if there is more than one policy.
	If you want to place greater priority on this home screen layout policy than another, select **Higher than**, and then select the home screen layout policy over which this policy will take priority.
	If you want to place lesser priority on this home screen layout policy than another, select **Lower than**, and then select the home screen layout policy that will be used before the one you are defining.
Description	Enter a description for the home screen layout policy.

6. Select the **Add** button below the Dock table to add apps to the dock.

   A new row is added to the Dock table.

7. Use the following table as a guideline for adding an app or webclip to the dock.

Item	Description
Type	Select the drop-down list to select the type of item you want to add to the dock: **Application**.
App Name	If you are adding an app to the dock, select the drop-down list and select an App Catalog app.
Bundle ID/URL	After you select an app, the bundle ID or web clip URL is automatically filled in.
Actions	Select the **✗** button to delete an app or web clip.

8. Select the **Add** button below the Page 1 table to add apps, webclips, and folders to the first home screen page after the dock.

   A new row is added to the Page 1 table.

9. Use the following table as a guideline for adding an app, web clip, or folder to the home screen page.

Item	Description
Type	Select the drop-down list to select the type of item you want to add to the dock: **Application** or **Folder**.
App Name	Select the drop-down list and select an App Catalog app.
Bundle ID/URL	After you select an app, the bundle ID or web clip URL is automatically filled in.
Actions	Select the **✗** button to delete an app, web clip, or folder. Select the **Edit** button to edit a folder name.

10. If you want to add more pages to the home screen layout policy:

   • Select **Add New Page**. A new page appears.

   • Add apps or folders, as described in the previous step.

11. Select **Save**.

12. Go to **Actions > Apply To Label**.

13. Select the label or labels to apply from the **Apply To Label** dialog.

14. Select **Apply**.

Customizing a lock screen message

You can customize the lock screen message for supervised devices running iOS 9.3 or supported newer versions.

Lock screen messages can include:

- Lost device message: Instructions regarding the return of the device if lost.

- Asset tag information: A unique identifier for the device.

You can create more than one lock screen message, and prioritize the application of each.

ℹ️ This feature is supported on supervised devices running iOS 9.3 or supported newer versions.

Procedure

1. Go to **Policies & Configs > Policies**.

2. Click **Add New**.

3. Select **iOS and macOS > iOS Only > Lock Screen Message**.

   The New Lock Screen Message Policy dialog box opens.

4. Define a lock screen message policy, using the table, below, as a guideline.

5. Click **Save**.

6. Go to **Actions > Apply To Label**.

7. Select the label or labels to apply from the **Apply To Label** dialog.

8. Click **Apply**.

TABLE 1. LOCK SCREEN MESSAGE POLICY

Item	Description
Name	Enter a name for the lock screen message.
Status	Select **Active** to enable the lock screen message, or **Inactive** to disable it.
Priority	Set the priority of the lock screen message policies if there is more than one policy.

Item	Description
	If you want to place greater priority on this lock screen message policy than another, select **Higher than**, and then select the lock screen message policy over which this policy will take priority. If you want to place lesser priority on this lock screen message policy than another, select **Lower than**, and then select the lock screen message policy that will be used before the one you are defining.
Description	Enter a description for the lock screen message policy.
Lost Device Message	Enter the text you want to be displayed on the lock screen and login window, for example "If found, return to Acme Inc."
Asset Tag Information	Enter a unique identifier for the device. This identifier will be displayed on the lock screen. You can use variables, such as the following: • $DEVICE_SN$ • $DEVICE_ID$ • $DEVICE_UUID$ • $DEVICE_UDID$ • $CUSTOM_DEVICE_Atributename$ You can also use text or variable combinations, such as the following: • $DEVICE_ID$:$DEVICE_UUID$ • $DEVICE_ID$_$DEVICE_UUID$

Configuring notification settings

For each app installed on an iOS device, you can configure notification settings, such as whether to display alerts in the iOS Notification Center and on the locked screen.

> ℹ This feature is supported on supervised devices running iOS 9.3 or supported newer versions.

Procedure

1. Go to **Policies & Configs > Policies**.

2. Select **Add New > iOS and macOS > iOS Only > Notification Settings**.

   The New Notification Settings Configuration dialog box opens.

3. Define the status and priority of the notification setting, using the following table as a guideline.

Item	Description
Name	Enter a name for the notification message, for example, "Lock Screen message."
Status	Select **Active** to enable the notification settings configuration, or **Inactive** to disable it.
Priority	Set the priority of the notification settings configuration if there is more than one policy.
	If you want to place greater priority on this lock screen message policy than another, select **Higher than**, and then select the lock screen message policy over which this policy will take priority.
	If you want to place lesser priority on this lock screen message policy than another, select **Lower than**, and then select the lock screen message policy that will be used before the one you are defining.
Description	Enter a description for the lock screen message policy.

4. Under the Notification Settings header, select **The settings specified for the first app will be applied to all apps added after it**. This means that whatever notification settings you set for the first app added become the default setting for all subsequent apps. Once saved, any edits to the first app will not impact the second or third saved apps.

5. Click **Add+** to configure notification settings for an app.

   The New App Notification Settings Configuration dialog box opens.

6. In the Bundle Identifier drop-down, select an app whose notifications you want to configure. Alternately, type in the app name into the field.

7. Select the **Notifications Enabled** check box. The notification settings become enabled.

8. Choose the notification features you want to enable for the app, using the following table as a guideline.

iOS version	Item	Description
iOS All Versions	Show in Notification Center	Select to show notifications for this app in the Notification Center on iOS devices.
	Sounds Enabled	Select to allow notifications to produce an audible alert on iOS devices.
	Badges Enabled	Select to allow notification to be displayed on the app icon in badge form.
	Show in Lock Screen	Select to display notifications for this app when the iOS device screen is locked.
	Alert Type	Click the drop-down to select the type of notification you want to be displayed for the app: **None**, **Banner**, or **Alert**.
iOS 12	Allow critical alerts to be enabled (ignore "Do Not Disturb")	Select to mark the notification as critical and to ignore Do Not Disturb and ringer settings. Applicable for iOS 12 or supported newer versions.
	Show critical alert when using CarPlay	Select to indicate the critical alert displays when device user is using CarPlay. Applicable for iOS 12 or supported newer versions.
	Group Type	Select from the drop-down the type of grouping for this notification: • **Automatic:** Notifications from each app will appear in groups based on app alerts. For example, if the device user has multiple iMessage conversations going on with people, the notifications might be grouped by app (iMessage) but separated by person.

iOS version	Item	Description
		• **By App:** All notifications from each app will be grouped into single expandable alerts. This means all incoming notifications from a specific app are grouped together rather than intelligently separated. • **Off:** Notifications appear in the order they are received, without grouping. This setting disables Notification Grouping for the selected app entirely, which means the devuce user's incoming notifications for that app will all come in individually, like they did in iOS 11. Applicable for iOS 12 or supported newer versions.
iOS 14	Preview Type	Select to preview type to display in device notification message previews. • **None** - No setting selected. The device user controls the display message previews as per user settings for the apps on the device. • **Always** (default) - Display message previews. • **When Unlocked** - Display message previews only when a device is unlocked. • **Never** - Prevent apps from displaying message previews in Notifications.

9. In the App Notifications Settings dialog box, click **Apply**. In the New Notifications Settings Configurations dialog box, the new notification setting displays in the Bundle Identifier section.

10. **Add+** any additional apps to the Bundle Identifier section.

11. In the New Notification Settings Configuration dialog box, click **Save**.

12. Go to **Actions > Apply To Label**.

13. Select the label or labels to apply from the **Apply To Label** dialog box.

14. Click **Apply**.

tvOS policy settings

This section addresses tvOS policies.

TV remote policy

Applicable to supervised devices: iPads, iPhones, iPods, and Apple TV 11.3 or later. Apple TV will get all iOS MAC addresses regardless of supervision. The iOS device will only apply the policy if it is supervised.

Once the TV Remote policy is available, you will need to attach labels to the policy. Attach a label for your Apple TVs and attach another label for your iOS devices. They will both get the appropriate configurations to be able to communicate with each other.

Procedure

1. In the Admin portal, click **Policies** > **Policies & Configurations**.

2. Click **Add New** and select **Apple > iOS / tvOS > TV Remote**.

   The New TV Remote Policy dialog box opens.

Item	Description
Name	Enter a name for the TV Remote policy.
Status	Select **Active** to enable the TV Remote policy, or **Inactive** to disable it.
Priority	Set the priority of the TV Remote policy if there is more than one policy. If you want to place greater priority on this TV Remote policy than another, select **Higher than**, and then select the TV Remote policy over which this policy will take priority. If you want to place lesser priority on this TV Remote policy than another, select **Lower than**, and then select the TV Remote policy that will be used before the one you are defining.
Description	Enter a description for the TV Remote policy.

3. Click **Save**.

Conference room message policy

Applicable to tvOS 13 and later supported versions.

The Conference Room Message policy requires Apple TV supervised devices.

Once the policy is available, you will need to attach labels to the policy. Attach a label for your Apple TVs and attach another label for your iOS devices. They will both get the appropriate configurations to be able to communicate with each other.

Procedure

1. In the Admin portal, click **Policies** > **Policies & Configurations**.

2. Click **Add New** and select **Apple > iOS / tvOS > Conference Room Message**.

   The New Conference Room Message Policy dialog box opens.

Item	Description
Name	Enter a name for the Conference Room Message policy.
Status	Select **Active** to enable the Conference Room Message policy, or **Inactive** to disable it.
Priority	Set the priority of the Conference Room Message policy if there is more than one policy.
	If you want to place greater priority on this Conference Room Message policy than another, select **Higher than**, and then select the Conference Room Message policy over which this policy will take priority.
	If you want to place lesser priority on this Conference Room Message policy than another, select **Lower than**, and then select the Conference Room Message policy that will be used before the one you are defining.
Description	Enter a description for the Conference Room Message policy.
Conference Room Message	Enter the text you want to have displayed on the screen in the Conference Room.

3. Click **Save**.

Working with Windows Update policies

This feature is not supported on iOS or macOS devices.

Notifications of changes to the privacy policy

Device users receive notifications when you make changes to the privacy policy and the MDM enrollment profile in Ivanti EPMM.

FIGURE 1. PRIVACY POLICY WINDOWS
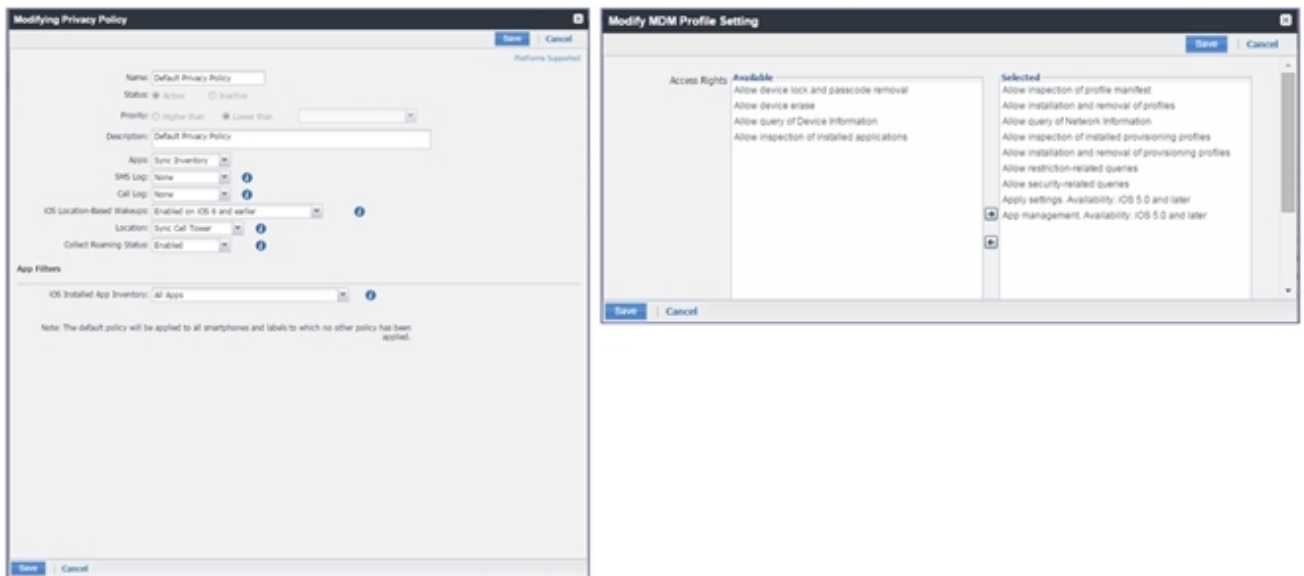
Device users will receive a privacy policy change notification under the following circumstances:

- any changes to the iOS Installed App Inventory option in the privacy policy settings on Ivanti EPMM, **except** for changes to the list of managed apps

- changes to the **Location** option in the privacy policy settings in Ivanti EPMM, including changes to the iOS location-based wake-up policy.

  When making changes to the location settings, bear in mind that the location of an iOS device is always accessible by the company, **except** under the following circumstances:

  - location sync is disabled, and location-based wake-ups are disabled,

    OR

  - location sync is disabled, and location-based wake-ups are enabled for iOS 5 through iOS 6 devices.

    > ℹ️ If the device user declines Ivanti EPMM access to their location, they will receive a notification regarding changes to the privacy policy.

- applying or removing privacy policies from a label, only if this results in changes to the privacy policies applied to the device.

- enabling the following MDM Profile Setting access rights:
  - **Allow device erase**
  - **Allow device lock and passcode removal**
  - **Allow query of device information**
  - **Allow inspection of installed applications**

> ℹ️ Changes involving only the removal of line items from policies will not produce user notifications. For example, if you remove **Allow Device Erase** from the MDM Profile Setting, users will not receive a notification of changes to the privacy policy.

Privacy policy change notifications on iOS: the administrator view

When making changes that will result in a user notification, Ivanti EPMM shows a message letting you know that users will receive privacy policy change notifications. The message asks you to confirm or cancel the change.
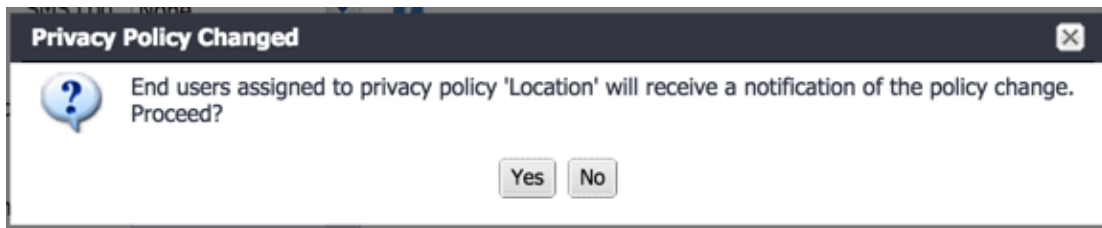
Select **Save** to go ahead with the change or **Cancel** to leave the privacy policy as is.

Privacy policy change notifications on iOS: the device user view

When changes are made to the privacy policy, device users receive a notification that the privacy policy had been updated.

Notifications are displayed when the app is in the foreground or background. When the app is in the foreground, the notification is always displayed in modal alert style. When the app is in the background, the notification format is controlled by iOS Notification Center settings, where users can disable these notifications if desired.

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.

This feature is supported on macOS devices.

Procedure

1. In the 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 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

This feature is supported on macOS devices.

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 Ivanti EPMM. Configurations are found on the **Policies & Configs > Configurations** page.

TABLE 35. DEVICE SETTINGS

Category	Configuration Type
Android	• Android for Work • Samsung Browser • Samsung Kiosk ⓘ Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. • Samsung Knox Container ⓘ Samsung Knox Container is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead.
Infrastructure	• Exchange • Email • Wi-Fi • VPN • Certificates • Certificate Enrollment
AppConnect	• App Configuration • Container Policy
Features	• Ivanti Docs@Work • Ivanti Web@Work
iOS and macOS	• General • CalDAV • CardDAV • Web Clips • Configuration Profile

TABLE 35. DEVICE SETTINGS (CONT.)

Category	Configuration Type
	• LDAP
iOS Only	• AirPlay (starting with iOS 7)
	• AirPrint (starting with iOS 7)
	• APN
	• Provisioning Profile
	• Restrictions
	• Subscribed Calendars
	• Web Content Filter (starting with iOS 7)
	• Managed App Config (starting with iOS 7)
	• Managed Domains
	• Single Sign-On Account (starting with iOS 7)

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.

> For User Enrollment configurations, Ivanti recommends using the label "Apple User Enrolled Device" + "Equals" + "True" or ios.apple_user_enrolled_device = true."

TABLE 36. 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.
# 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.

TABLE 36. CONFIGURATIONS PAGE OPTIONS (CONT.)

Field	Description
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 349 for information on quarantining devices.

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

Default configurations

ℹ️ The features described in this section are supported on macOS devices.

Ivanti EPMM provides the following default configurations.

TABLE 37. DEFAULT CONFIGURATIONS

Configuration Name	Type	Description	Devices applicable to
App Catalog Service	APP_CATALOG	Default configuration for App Catalog Service	
Ivanti Anti-phishing VPN	VPN	VPN Setting for Anti-phishing	
Ivanti Threat Defense Tunnel Config for Android	VPN	Default configuration for Ivanti Tunnel to enable Mobile Threat Defense	Android
Ivanti Threat Defense VPN	VPN	VPN setting for Mobile Threat Defense VPN	
System - Apps@Work AET	APPENROLLMENTTOKEN	Auto-created Windows Application Enrollment Token Setting	
System - FileVault Configuration	CERTIFICATE ENROLLMENT	Auto-created SCEP setting for the FileVault2 CA	

TABLE 37. DEFAULT CONFIGURATIONS (CONT.)

Configuration Name	Type	Description	Devices applicable to
System - iOS Enrollment CA Certificate	CERTIFICATE	System certificate to support the built-in CA server.	
System - iOS Enrollment SCEP	CERTIFICATE ENROLLMENT	System settings for the built-in SCEP server. Note that the default URL contains HTTP. Do not change this to HTTPS without configuring a third-party certificate. The default is a self-signed certificate, which iOS does not support with HTTPS.	
System - iOS Enterprise AppStore	WEBCLIP	System settings for Apps@Work web clip.	
System - iOS Enterprise AppStore SCEP	CERTIFICATE ENROLLMENT	This SCEP setting is automatically created for the iOS Enterprise App Store certificate. ⓘ If the iOS label is removed from this default configuration, Ivanti EPMM will re-apply the iOS label following system or web server reboot, and after upgrading from a previous version to the current version of Ivanti EPMM.	iOS macOS tvOS
System - iOS MDM	MDM	Default MDM profile for iOS MDM.	iOS tvOS

TABLE 37. DEFAULT CONFIGURATIONS (CONT.)

Configuration Name	Type	Description	Devices applicable to
System - macOS Enterprise AppStore Identity Preference	IDENTITY PREFERENCE	Auto-created IDENTITY_ PREFERENCE setting for MacOS Enterprise.	macOS
System - Multi-User Secure Sign-In	WEBCLIP	System settings for Secure Sign-In web clip, which enables access to multi-user function for iOS devices. See ""Multi-User Support" on page 229" for more information.	iOS
System - Mutual Auth CE setting	CERTIFICATE	Certificate Enrollment Setting For Mutual Authentication	
System - TLS Trust Certificate Chain for Mobile Management	CERTIFICATE	This certificate chain is used so that mobile devices will trust requests from Ivanti EPMM.	
Windows Cert Auth Root CA Certificate	CERTIFICATE	This setting is used for (non-enrollment) server authentication by Windows devices.	Windows
Windows Computer-level Cert Auth CE Setting	CERTIFICATE	This setting is used for computer-level certificate authentication by Windows clients.	Windows
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.	Windows

Editing default iOS MDM settings

iOS MDM settings are editable, though, in most cases, you should not change access rights here.

Besides the initial iOS / macOS device registrations, the MDM profile is pushed to the device during

- Ivanti Mobile@Work re-enroll option

- Changing of the MDM access rights. Choosing less access rights results in the MDM profile being updated automatically; more access rights require a user prompt which is done via Ivanti Mobile@Work . If the device does not have Ivanti Mobile@Work , the MDM profile does not get updated until the device is retired and re-registered.

> ℹ️ A re-push of the MDM profile will result in any applications with the **Send convert unmanaged to managed app request on device registration or sign-in (iOS 9 or later)** option selected. A repush of the MDM profile is considered a re-registration for the app install process. For more information, see the *Ivanti EPMM Apps@Work Guide*.

To edit the default iOS MDM settings:

1. Go to **Policies & Configs > Configurations**.

2. Select the **System - iOS MDM** configuration.

3. Select **Edit** to open the **Modify Profile MDM Setting** dialog box.

4. If changing an access right is necessary, select an access right in the **Available** list and select the appropriate arrow to move the access right to the **Selected** list. The table below summarizes these access rights.

5. If you want Ivanti EPMM to indicate that the MDM profile has been removed from iOS devices, select **Check out when MDM profile is removed**.

> ℹ️ Receipt of this alert is not guaranteed. Therefore, this setting does not ensure notification upon removal of the profile.

6. If you want to automatically alert iOS users when a new iOS MDM configuration is available, select **Send an APNs message to iOS 5 and later devices...**

7. Select **Save**.

TABLE 1. ACCESS RIGHTS

Access Right	Notes
Allow inspection of installed configuration profiles.	Enables inventory of configuration profiles.

Access Right	Notes
Allow installation and removal of configuration profiles.	Enables overall configuration tasks.
Allow device lock and passcode removal.	Enables remote lock and unlock capabilities.
Allow device erase.	Enables remote wipe.
Allow query of Device Information.	Enables inventory of standard device items, such as device capacity, serial number.
Allow query of Network Information.	Enables inventory of standard network items, such as phone/SIM numbers, MAC addresses.
Allow inspection of installed provisioning profiles.	Enables a device user to run select in-house apps.
Allow installation and removal of provisioning profiles.	Enables installation of select in-house apps.
Allow inspection of installed applications.	Enables app inventory.
Allow restriction-related queries.	Enables reports on the restrictions of each configuration profile on the device. These correspond to the settings in the iOS Restrictions and Passcode payloads.
Allow security-related queries.	Enables report on security items, such as whether a passcode is present.
Allow manipulation of settings.	Enables an administrator to turn on/off voice and data roaming.
Allow app management.	Enables the **managed apps** capability introduced in iOS 5 so that an administrator can push requests to install apps, prevent iCloud backup, and remove the apps and all app data on demand.

Restoring system web clips (iOS)

If you enable the **Removable** option for the Multi-User web clip or the Apps@Work web clip, and the device user removes one of these web clips, use one of the following methods to restore the web clip:

- Remove the MDM profile on the device and tap **Update Configuration Profile** in Ivanti Mobile@Work .

- Push the web clip from the **Devices** page by selecting the device and clicking **Push Profiles**.

Displaying configurations status

This feature is supported on macOS devices.

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**: Ivanti EPMM 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

This feature is supported on macOS devices.

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

This feature is supported on macOS devices.

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

This feature is supported on macOS devices.

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 Ivanti EPMM. You can export a configuration .json file for an existing setting, modify it, then import it to another configuration.

This feature is supported on macOS devices.

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. Select **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

This feature is supported on macOS devices.

To import a configuration:

1. Log into Ivanti EPMM.

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

3. Select **Import** to locate a saved exported configuration .json file.

4. Enter the name of the file or select **Browse** to locate it.

5. Read the warning message and select in the **I Agree** check box.

6. Select **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 Ivanti EPMM* for more information.

This feature is supported on macOS devices.

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.

This feature is supported on macOS devices.

Procedure

1. In the 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

- Ivanti Docs@Work setting

This feature is supported on macOS devices.

Creating DNS Proxy Configurations

As the Ivanti EPMM administrator, you can configure DNS Proxy settings using the DNS Proxy Configuration for users of iPhone and iPad devices. You can use the DNS Proxy payload to specify the application that provides the DNS proxy network extension and other vendor-specific values. The DNS Proxy payload cannot be installed by Apple Configurator and must be installed by MDM on devices running iOS 15 or later.

- Multiple DNS Proxy configurations can be created

- Applicable to supervised only in-house apps and App Store apps.

- You can import / export this configuration.

Procedure

1. Log in to the Ivanti EPMM Admin portal.

2. Go to **Policies & Configs > Configurations**.

3. Select **Add New > Apple > iOS/tvOS > DNS Proxy**. The DNS Proxy dialog box opens.

4. Enter a name and describe the configuration.

5. Enter the following DNS Proxy Configuration settings:

   - App Bundle Identifier (Required) - Enter the bundle ID of the app that contains the DNS proxy network extension.

   - Provider Bundle Identifier - Enter the bundle ID of the DNS proxy network extension to use.

   - Provider Configuration - use the **Upload Configuration** button to add the plist file to populate the field.

6. Click **Save**. The new policy displays in the Configurations page.

> ℹ️ Saved configurations will also display in the app's App Configurations tab as a new DNS Proxy App Configuration drop-down option.

7. You must apply a label to this new configuration.

8. Go to the app in the **App Catalog** and make sure that in **DNS Proxy Filter Setting** , the DNS Proxy configuration is selected.

9. Within the same app, add a widget to select the DNS Proxy list. You can display the DNS Proxy widget in Custom Spaces.

10. Add a label to the app. When applying a label to the app, the DNS Proxy will be applied based on the device label.

For more information, see [Setting DNS proxy for iOS and macOS apps](#) in the *Ivanti EPMM Apps@Work Guide*.

Configuring encrypted DNS settings

Encrypted DNS allows administrators to enhance security without needing to configure a VPN. These settings can be managed via MDM.

This feature is supported on iOS 14.0+ and macOS 11.0+ devices.

Procedure

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

2. Click **Add New > Apple > iOS/macOs/tvOS > Encrypted DNS.**

The Add Encrypted DNS Configuration dialog box opens.

3. Use the guidelines in the table below to complete this form.

4. Continue to the next section.

TABLE 38. ENCRYPTED DNS SETTINGS

Item	Description
Name	Enter a short phrase that identifies this encrypted DNS setting.
Description	Provide a description that clarifies the purpose of these settings.
DNS Protocol	Select one of the following distribution options: • HTTPS - the configuration will be transmitted over a secure web URL. This is the default option. • TLS - the configuration will be transmitted over a secure network server.
Server URL	If HTTPS was selected, this field displays. Enter the URL for the encrypted DNS. An example is: `https://dns.ivanti/dns-query`
Server Name	If TLS was selected, this field displays. Enter the server name for the encrypted DNS. An example is: `dns.ivanti`
Prohibit DNS Disabling	Select to prevent device users from disabling the DNS.
Server Addresses	For either HTTPS or TLS, you will need to add the server addresses. • An example IPv4 server address would be `10.0.0.1`. • An example IPv6 server address would be `2001:0db8:85a3:0000:0000:8a2e:0370:7334` 1. Click **Add+**. 2. Enter the server address in the displayed field. 3. Enter an optional description.
Supplement Match Domains	For either HTTPS or TLS, you will need to add the supplemental domains that match the Encrypted DNS. An example would be: `*.dns.ivanti.com` 1. Click **Add+**. 2; Enter the DNS match domain in the displayed field. 3. Enter an optional description.

TABLE 38. ENCRYPTED DNS SETTINGS (CONT.)

Item	Description
Demand Rules	Use Demand Rules to list domain strings that determine the DNS queries to use DNS server. See "On Demand Rules" below

On Demand Rules

Applicable to: iOS 14.0+ and macOS 11.0+

Whenever a network change is detected, the On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether Encrypted DNS On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. Encrypted DNS then acts according to the policy defined in the dictionary.

You can define sets of evaluation rules for each action that can be taken by Encryption DNS On Demand: **Connect**, **Disconnect**, **Evaluate Connection**. You can define more than one set of rules for each type of action that can be taken.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Click **Add+** to add a default rule.

   The following actions are available:

   - **Connect**: Unconditionally initiate an Encrypted DNS connection on the next network attempt.

   - **Disconnect**: Tear down the Encrypted DNS connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   If you select **Evaluate Connection**, a Domains table displays:

3. Click **Add+** to add a domain. A new field displays in the Domains table.

4. Enter the domain information and a description.

5. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

   - **Connect if needed**: The specified domains should trigger an Encrypted DNS connection attempt if the specified domain name resolution fails. For example, when the DNS server indicates that it cannot resolve the domain, it responds with a redirection to a different server, or fails to respond (timeout).

   - **Never connect**: The specified domains should never trigger an Encrypted DNS connection attempt.

6. In the Matching Rules section, click **Add+** to include any of the following evaluation types:

   - **Domain**: The domains for which this evaluation applies.

   - **Required DNS Server**: IP addresses of the DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, an Encrypted DNS connection is established in response. These Encrypted DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the **Connect if needed** domain action.*

   - **Required URL Probe**: An HTTPS URL to probe, using a GET request. If no HTTPS response code is received from the server, an Encrypted DNS connection is established in response. *You can only configure required URL probe evaluation types for the **Connect if needed** domain action.*

7. Add a value and optional description for each entry.

8. **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

9. **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTPS status code), this rule matches.

10. Click **Save** to save your domain action parameters.

Managing Compliance

Ivanti EPMM 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 (Login to forums.ivanti.com to access the following links) for more information on compliance:

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

The topics in this chapter include the following advanced topics:

- "Managing device compliance checks" below
- "Tiered compliance" on page 345
- "Compliance actions policy violations" on page 346
- "Viewing quarantine information" on page 354
- "Viewing configurations removed due to quarantine" on page 354
- "Custom compliance policies" on page 355

> **ⓘ** The features described in this section are supported on macOS devices.

Managing device compliance checks

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

Using Ivanti EPMM, 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

Ivanti EPMM receives information regarding device compliance status and last check-in only after devices actually check-in with Ivanti EPMM. 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 Ivanti EPMM performance problems.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Compliance Actions**.

2. Select **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 Ivanti EPMM performance.

4. Select **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 Ivanti EPMM. 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.

> ℹ️ 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. Select **Check Compliance** to display a message asking if you want to update compliance status for all devices.
3. Select **Yes** to check compliance status for all devices or select **No** to cancel the action.

> ℹ️ 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 Ivanti 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 Ivanti EPMM 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.	Send an alert when the device has been compromised.	Send an alert when administrator privileges have been removed.	Send an alert when it has been detected that the device as been decrypted.	Send an alert when the OS version is less than expected.

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
	You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email. The maximum number of characters allowed is 65,530.	You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email. The maximum number of characters allowed is 65,530.	You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email. The maximum number of characters allowed is 65,530.	You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email. The maximum number of characters allowed is 65,530.	You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email. The maximum number of characters allowed is 65,530.
Remove Apps • Android • iOS Removal of apps is only possible if the MDM profile is sent by Ivanti EPMM and is present on the device OR if the app settings have the "Remove app when device is quarantined of signed-out" check box selected.	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.
Quarantine All • Android • iOS	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.

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
All Android Enterprise apps and functionality are hidden, except Downloads, Google Play Store, and Ivanti Mobile@Work. (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)					
Quarantine All Except Wi-Fi • Android • iOS • macOS (For Android Enterprise apps, this is applicable only if the "Quarantine app when device is quarantined" check box is selected.)	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.

Managing Device Settings with Configurations

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
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 "Block" means blocking access to AppConnect apps.	not applicable	Block (unauthorized) or retire (unauthorize and wipe) AppConnect apps	not applicable	not applicable	not applicable

Local compliance conditions and actions

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

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 2. LOCAL COMPLIANCE CONDITIONS AND ACTIONS

Situation	OS	Action
When the device can communicate with Ivanti EPMM 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 (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 Play Store, and Ivanti Mobile@Work.
When the device can NOT communicate with Ivanti EPMM 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.

Situation	OS	Action
	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 Ivanti Mobile@Work.
	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, Ivanti EPMM sends users a second message and blocks the device.
3. If the device continues to violate the same policy another 24 hours later, Ivanti EPMM 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.

> **i** 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, Ivanti EPMM 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, Ivanti EPMM will not take action based on the next tier. Ivanti EPMM 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 Ivanti EPMM 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 Ivanti EPMM. You can also select custom compliance actions that you create.

FIGURE 1. COMPLIANCE ACTIONS POLICY VIOLATIONS

> ℹ️ To create the custom compliance actions, see "Custom compliance actions" on the next page.
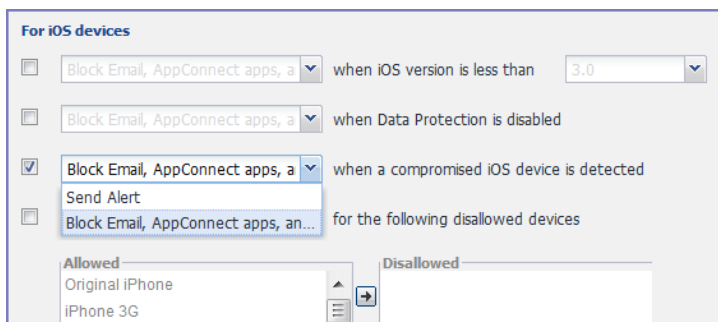
FIGURE 2. COMPLIANCE ACTION SETTINGS FOR IOS AND ANDROID DEVICES

> ℹ️ **IMPORTANT:** As you read this section, refer to the process diagram above. Note that references to "Core" mean Ivanti EPMM.

To view this diagram in full, see Compliance Action settings for iOS and Android devices.

Default compliance actions

The following table describes the default compliance actions:

TABLE 39. 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 830.
Block Email, AppConnect Apps And Send Alert	• Sends alert that you configured for the policy violation. • Restricts access to email via ActiveSync if you are using a Standalone Sentry for email access.

TABLE 39. DEFAULT COMPLIANCE ACTIONS TABLE (CONT.)

Default compliance action	Description
	ℹ️ If you manually block, allow, or wipe a device on the **ActiveSync Associations** page, blocking email access in a compliance action has no impact. The manual action overrides Ivanti EPMM's automatic decision-making about access to email via ActiveSync. See "Overridding and re-establishing Ivanti EPMM management of a device" in the *Ivanti Standalone Sentry Guide for EPMM*.
	- Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature. - This action blocks tunnels that AppConnect apps and iOS managed apps use. - Unauthorizes AppConnect apps. - AppConnect apps become unauthorized when the next app checkin occurs. When launched, an AppConnect app displays a message and exits. Some iOS AppConnect apps that have portions that involve only unsecured functionality can allow the user to use only those portions. - AppConnect apps become unauthorized when the next device checkin occurs. When the device user tries to launch an AppConnect app, the Secure Apps Manager displays a small pop-up message with the reason the app is unauthorized. - This action impacts AppConnect apps, as well as third-party AppConnect for Android apps.
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
- iOS 12.0 or supported newer versions: remove managed apps, and block new downloads

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.

> ℹ️   Access control for macOS devices does not control email.

Procedure

1. Log into the Admin Portal.

2. Go to **Policies & Configs > Compliance Actions**.

3. Select **Add+** to open the **Add Compliance Action** dialog box.

4. Select the appropriate fields as described in the "Add Compliance Action table" on the next page.

5. If you want to add another set of actions, select 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, select the plus (+) button and select the fields, as necessary, to complete the third compliance action.

7. Select **Save** to add the new compliance action for access control and compliance actions.

8. You can select them by going to:

- **Policies & Configs > Policies > Security policy > Edit > Access Control** section (1 tier only).

- **Policies & Configs > Compliance Policies > Add+ > Compliance Policy Rule > Compliance Actions** drop-down (1-4 tiers).

> ℹ️ Using Compliance Actions with the "Enforce Compliance Actions Locally on Devices" option enabled does not have any effect if used in Compliance Policies. Those are only supported in the Security policy.

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 macOS devices. Select this to enable the Ivanti Mobile@Work app to enforce compliance actions on the device for security violations without requiring action from Ivanti EPMM. Ivanti EPMM also continues to enforce compliance actions. For iOS, this option is only supported in the Security Policy under the "Apply compliance action when a compromised iOS device is detected."For more information, see Security policies in *Getting Started with Ivanti EPMM*. For any other uses in Security Policy or Compliance Policy Rule, this option has no effect on iOS devices.
ALERT: Send a compliance notification or alert to the user	This feature is not supported on macOS devices. Select if you want to trigger a message indicating that the violation has occurred. The Ivanti Mobile@Work app will send an alert to the device user based on the security policy violation, even without connection to Ivanti EPMM. To use this feature, you need to select this Compliance Action in Security Policies in *Getting Started with Ivanti EPMM*. If de-selected, Ivanti EPMM will send alerts to device users, administrators, or both. To configure the alert, see "Policy violations event settings" on page 830.

Item	Description

BLOCK ACCESS: Block email access and AppConnect apps	This feature is not supported on macOS devices.
	
	Selecting this option has the following impact to the device:
	
	• Restricts access to email via ActiveSync if you are using a Standalone Sentry for email access.
	
	   ⓘ If you manually block, allow, or wipe a device on the ActiveSync Associations page, blocking email access in a compliance action has no impact. The manual action overrides Ivanti EPMM's automatic decision-making about access to email via ActiveSync. See "Overriding and re-establishing Ivanti EPMM management of a device" in the *Ivanti Standalone Sentry Guide for EPMM*.
	
	• Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature.
	
	   This action blocks tunnels that AppConnect apps and iOS managed apps use.
	
	• Unauthorizes AppConnect apps.
	
	   AppConnect apps become unauthorized when the next app checkin occurs. When launched, an AppConnect app displays a message and exits. Some iOS AppConnect apps that have portions that involve only unsecured functionality can allow the user to use only those portions.
	
	   AppConnect apps become unauthorized when the next device check in occurs. When the device user tries to launch an AppConnect app, the Secure Apps Manager displays a small pop-up message with the reason the app is unauthorized.
	
	   This action impacts AppConnect apps, as well as third-party AppConnect for Android apps.
	
	• If the"Enforce Compliance Actions Locally on Devices" check box is selected, this action makes AppConnect apps unauthorized even without connection to Ivanti EPMM. To use this feature, you need to select this Compliance Action in the Security Policy under the condition "Apply compliance action when a compromised iOS device is detected." For more information, see [Security policies](#) in *Getting Started with Ivanti EPMM*.

Item	Description
QUARANTINE: Quarantine the device (Select this check box to display the other Quarantine options.)	This feature is not supported on macOS devices. Selecting this option has the following impact to the device: • Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature. This action blocks tunnels that iOS managed apps use. • AppConnect apps are retired, which means they become unauthorized *and their secure data is deleted (wiped)*. If the "Enforce Compliance Actions Locally on Devices" check box is selected, this action makes AppConnect apps unauthorized and wipes their secure data without connection to Ivanti EPMM. To use this feature, you need to select this Compliance Action in the Security Policy under the condition "Apply compliance action when a compromised iOS device is detected." For more information, see [Security policies](#) in *Getting Started with Ivanti EPMM*.
QUARANTINE: Remove All Configurations and SaaS Sign-on Policy	With the "Enforce Compliance Actions Locally on Devices" check box de-selected, select if you want to remove the configurations (i.e., profiles) that provides access to corporate resources. Requires AppConnect apps to be re-installed after the device is back in compliance. ⓘ This feature is not supported as an iOS local action as removal of configurations can only be done from the Ivanti EPMM server side.
QUARANTINE: Do not remove Wi-Fi settings for Wi-Fi only devices	Select if you want to retain the Wi-Fi configurations devices that do not have cellular access. Select this option to ensure that you can still contact these devices. The iOS version determines how Ivanti EPMM decides whether a device supports Wi-Fi only. Prior to iOS 4.2.6, the device model (e.g., iPod) is used. ⓘ This feature is not supported as an iOS local action as removal of configurations can only be done from the Ivanti EPMM server side.
QUARANTINE: Do not remove Wi-Fi settings for all devices (iOS and Android only)	This feature is not supported on macOS devices. Select this option to retain the Wi-Fi configurations for any device, regardless of whether it has cellular access. You might select this option to preserve limited network access despite the policy violation.

Item	Description
	ℹ This feature is not supported as an iOS local action as removal of configurations can only be done from the Ivanti EPMM server side.
QUARANTINE: Remove iBooks content, managed apps, and block new app downloads	This feature is not supported on macOS devices. Select this option to remove iBooks content and Managed Apps from the device as well as block access to Apps@Work when the device is not compliant. ℹ This feature is not supported as an iOS local action as removal of configurations can only be done from the Ivanti EPMM server side.
Retire: Retire the Work profile or factory reset the managed device	This feature is not supported on iOS or macOS devices.
Wipe	This feature is not supported on iOS or macOS 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
- The app check in interval for AppConnect for iOS
- Whether **Enforce Compliance Actions Locally on Devices** is selected

Once the change reaches the device, Ivanti EPMM 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 Ivanti Mobile@Work initiates the compliance action without requiring contact with Ivanti EPMM.

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 Ivanti EPMM has removed due to quarantine on the Configurations page.

1. Go to **Policies & Configs > Configurations**.
2. Select 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, select **Add** to add it.)

3. To see a list of all quarantined devices, select the quarantined category.

Custom compliance policies

Ivanti EPMM 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.

Ivanti EPMM 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 Ivanti EPMM during device check-in.

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

- "Assigning compliance roles" below
- "Managing compliance policy rules" on page 357
- "Managing compliance policy groups" on page 361
- "Device search fields for compliance rules" on page 364

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 select **Actions > Edit Roles**.

4. Select an Admin Space.

5. Scroll down the window to the **Compliance Policy Management** section.

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. Select **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 the next page
- "Viewing and modifying compliance policy rules" on page 360
- "Deleting compliance policy rules" on page 361
- "Searching for compliance policy rules" on page 361

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. Select **Compliance Policy Rule** tab and then select **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 57.

   > ℹ️ It is recommended to have one Condition set to include when Ivanti 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. If you don't want the search results to include retired devices, select the **Exclude retired devices from search results** check box.

10. Select **Save**.

TIP - We recommend that you create a Compliance Policy rule with one condition set to include when Ivanti Mobile@Work last checked in with Ivanti Endpoint Manager Mobile. This is helpful if you need assurance that Ivanti 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. Select **Compliance Policy Rule** tab and then select **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. Select **Save**.

Substitution variables for compliance policy rules

The following table lists the 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.

- $MI_APPSTORE_URL$
- $MODEL$
- $NULL$
- OU
- $PASSWORD$
- $PHONE_NUMBER$

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

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 select **Edit**.

4. Modify details, as necessary, including disabling the rule.

5. Select **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. Select **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. Select **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" on the next page
- "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 363

-
-
-

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. Select **Compliance Policy Group** tab.
4. Select **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. Select **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. Select **Save** in the **Details** section.
6. Select **Edit** in the Rules section.
7. Modify rules, as necessary, by adding or removing rules.
8. Select **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 for details.

Procedure

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

5. De-select one or more of the labels.

6. Select **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. Select **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. Select **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 40. 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,

TABLE 40. DEVICE SEARCH FIELDS FOR COMPLIANCE RULES (CONT.)

Category	Compliance policy objects
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,
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>

Independent, customized messages and email subject for each compliance action tier

In previous releases, only one customized message could be sent for all Compliance Action tiers supported in **Compliance Policies > Compliance Policy Rule**. Starting in this release, administrators have the ability to create and send independent, customized messages and email subject lines for each of the now 20 possible Compliance Action tiers.

Compliance actions are categorized as:

- V1, which are compliance actions that existed in Ivanti EPMM *before* Version 11.8.0.0.

- V2, which are compliance actions that are created *starting in* Ivanti EPMM 11.8.0.0.

The following table compares compliance actions between V1 (pre-version 11.8.0.0) and V2 (Version 11.8.0.0+):

TABLE 41. COMPLIANCE ACTIONS VERSIONS 1 & 2

Compliance actions Version 1	Compliance actions Version 2
Uses even center for alert-related settings.	Actions cannot use the event center configuration. Instead, all the settings related to alerts, message languages, and so on, are available in the action page in the **Settings** tab.
Compliance action messages are configured at rule level. Only one message can be configured for all tiers in an action	Compliance action messages can be configured in each tier.
Uses only single alert messages across all tiers in the action.	Administrators can configure alert messages and subjects in multiple languages selected in the action settings. The system default language is mandatory and cannot be ignored or removed. Once an administrator selects languages, they must enter the subject and message for all the selected languages. When the system dispatches messages to the devices, it picks the language specified in the device locale. If the device-specific locale is not configured in the action page, the system default language (for example, English) is used. For example, if an administrator configures messages in French and English, but the device locale (German), has not been configured, the subject and messages use the system default language (English) in alerts.
Uses event center.	Administrators can configure different messages for each tier in multiple languages and configure the alert severity levels and alert frequency settings for each tier in an action. Alert recipients and message languages can be configured at an action level in the compliance action page > **Settings** tab.
Existing behavior is unchanged.	For V2 actions, the maximum length of the message = 800 chars, including substitution variables. The maximum length of the subject = 150 chars, including substitution variables.

TABLE 41. COMPLIANCE ACTIONS VERSIONS 1 & 2 (CONT.)

Compliance actions Version 1	Compliance actions Version 2
After upgrading to Ivanti EPMM 11.8.0.0, *existing* V1 actions can be used. New V2 actions can also be used. New actions can only be created as V2 actions. Administrators can upgrade/migrate V1 actions to V2 actions. When they edit V1 actions, they can apply V2 action features to V1 actions and upgrade/migrate the V1 action to a V2 action using the **Upgrade to New Compliance Action** checkbox in the **Edit Compliance Action** page. This upgrade is non-reversible, that is, the upgraded/migrated V1 cannot be reverted if it has been successfully migrated to V2.	After upgrading/migrating to Ivanti EPMM 11.8.0.0, new actions can only be created as V2 actions.
Supports templates in the event center.	Templates Administrators can insert the following variables (that are exposed in the **Insert Variable** section) in the subject and message content: • `$SEVERITY$` - Localized, device's locale used. • `$USER_NAME$`
Supports templates in the event center.	Templates Administrators can insert the following variables (that are exposed in the **Insert Variable** section) in the subject and message content: • `$SEVERITY$` - Localized, device's locale used. • `$USER_NAME$`
Existing behavior is unchanged.	Alert frequency time has granularity to hours and days. For example, administrators can send up to 5 alerts in 5 hours, or 10 alerts in 2 days. Two days duration = 24 * 2 = 48 hours.

TABLE 41. COMPLIANCE ACTIONS VERSIONS 1 & 2 (CONT.)

Compliance actions Version 1	Compliance actions Version 2
	Delay of the next tier should be greater than or equal to the `Sendupto` value of the current tier in the V2 action.
	After upgrading to Ivanti EPMM 11.8.0.0+, a default system-generated event of type `Compliance Rule Violation Event` is generated in the **EventSettings** page. This event cannot be edited or deleted.
	When a compliance policy rule violation occurs, the system uses tier-specific alert preferences. Security policies continue to use the alert preferences from the event center.

Configuring Email

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

- "Exchange settings" below
- "Configuring POP and IMAP email settings (for iOS and macOS)" on page 378
- "Enabling per-message S/MIME for iOS" on page 383
- "Enabling S/MIME encryption and signing on iOS devices" on page 392
- "Synchronizing Google account data" on page 396
- "Synchronizing Google calendar and contacts without ActiveSync " on page 402

Exchange settings

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

For macOS 10.10 Yosemite:

Contacts, Email, Notes, Reminders, and Calendar are synchronized. ActiveSync is not supported.

For iOS:

- If an Exchange profile already exists on the device, then attempts to distribute new ActiveSync settings using Ivanti Endpoint Manager Mobile will fail.

For iOS and macOS:

- iOS/macOS can take advantage of the optional Save User Password feature under **Settings > Preference**s to facilitate Exchange configuration.

Note that AppConnect-enabled Ivanti Email+ for iOS or Android do not use an Exchange setting. Instead, you configure the email clients using an AppConnect app configuration.

The following table describes the Exchange settings you can specify.

TABLE 42. 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 email 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. • 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 Ivanti Standalone Sentry Guide for EPMM.

TABLE 42. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	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 Ivanti EPMM. 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 Ivanti EPMM. This password allows device users to access their Email, Contacts, and Calendar data on their managed devices. When selected, Ivanti EPMM grays out the **ActiveSync User Name** and **ActiveSync User Password**. This check box only appears if you have configured a Google account with Ivanti EPMM, as described in "Synchronizing Google account data" on page 396.
	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.

TABLE 42. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		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 $NULL$.
	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 Ivanti EPMM administrator.
		ℹ️ 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 42. 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 Ivanti EPMM** 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)	This feature is not supported for iOS macOS.
	Items to Synchronize (iOS)	Select to specify individual syncing of Outlook items: Email, Calendar, Contacts, Notes, and Reminders. All check boxes are selected by default. If **Allow User Override** is selected for a specific item, the device user will be able to change the service status on the device. At least one of the Outlook items settings must be enabled. If you disabled syncing for one of the Outlook items and allowed the device user to override that same item, the device user will still be able to enable the Outlook item. For example, if you disabled Calendar, but had Allow User Override selected, the device user will be able to enable calendar on the iOS device.
	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.

TABLE 42. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	Move/Forward Messages to Other Email Accounts	**Starting with iOS 5:** This feature specifies whether to block device users from moving or forwarding email from the managed email account.
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. You must select this option for the fields in the **S/MIME Signing** and **S/MIME Encryption** sections to apply to devices running iOS 9.3.3 or earlier.
S/MIME Signing	(Optional) S/MIME signing applies to iOS devices up to iOS 9.3.3.	
	S/MIME Signing: Enable	Disabled by default.Select the check box to enable S/MIME signing. Applicable to iOS 10.3 or supported newer versions.
	S/MIME Signing identity	Select a certificate enrollment setting as a signing identity. If you do not make a selection, then the device user will be prompted to select from the certificates that are already installed on the device. If the device has no certificate, then S/MIME signing will not be functional on the device. Applicable to iOS 9.0 or supported newer versions. **Related topics** "Certificate Enrollment settings" on page 656.
	Signing Identity: User Overrideable	Applicable to iOS 12.0 or supported newer versions. Select to allow the user to select the signing identity on the device.
	S/MIME Signing: User Overrideable	iOS 12 or supported newer versions. Select to allow the user to enable and disable S/MIME signing in device settings.
S/MIME Encryption	S/MIME encryption applies only to iOS devices.	
	Encryption by Default	Disabled by default.Select to enable S/MIME encryption.
	Encryption Identity	Select a certificate enrollment setting as an encryption identity. If you do not make a selection, then the device user will be prompted to select from the certificates that are already installed on the device. If the device has no certificate, then S/MIME encryption will not be functional on the device.

TABLE 42. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		Related topics "Certificate Enrollment settings" on page 656.
	Encryption Identity: User Overrideable	iOS 12.0 or supported newer versions. Select to allow the user to set the S/MIME encryption identity and enable encryption.
	Encryption by Default: User Overrideable	iOS 12.0 or supported newer versions. Select to allow the user to enable or disable S/MIME encryption by default in the device settings.
	Per-Message Encryption Switch	This feature is not supported for Mac OS devices.Per-message S/MIME for iOS allows device users to enable or disable S/MIME encryption for each email they send. ⓘ S/MIME encryption is incompatible with Sentry attachment encryption.
ActiveSync		Not for iOSmacOS.
	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.
	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 Mac OS devices.

TABLE 42. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	Email access to Third-Party apps	Specifies whether third-party apps can use the account for email access.
	Recent Address syncing (iOS 6 and later)	Specifies whether recently used email addresses can be synchronized.
	Use OAuth for Authentication: Enable	iOS 12.0 or supported newer versions. Select the check box to enable OAuth for Authentication. When selected, Ivanti EPMM will not send the password and OAuth will be used. For devices pre-iOS 12.0, the OAuth selection will be ignored by the devices, so you should fill in the ActiveSync User Password field.
	OAuth Sign In URL	This field is visible if **Use OAuth for Authentication** is enabled. Enter the URL for the OAuth server.
	OAuth Token Request URL	This field is visible if **Use OAuth for Authentication** is enabled. Enter the URL for the OAuth ticketing server.
	Communication Service Rules (iOS 10 and later)	Select a default audio service or app to be associated with the device user's accounts on the Exchange, CardDAV, LDAP, and Google servers. All calls initiated on the iOS device to contacts from contact lists stored on the server will use the selected audio service by default. This feature is supported on devices running iOS 10 or supported newer versions. To enable communication service rules: • Select **Choose a default app to be used when calling contacts from this account**. A drop-down list of apps displays. • Select the drop-down list to select the default audio app or service.
Android		These features are not supported for iOS devices. These features are not supported for Mac OS devices.
	Windows 10 Desktop	This feature is not supported for iOS devices. This feature is not supported for Mac OS devices.

iOS and macOS Exchange profiles and password caching

To facilitate iOS and macOS deployments, Ivanti EPMM offers the option of caching a user's email password. This option is turned off by default. Cached passwords are encrypted, stored on the appliance, and used only for authentication. Note that the email password must match the LDAP password in order for this feature to be of use.

Configuring POP and IMAP email settings (for iOS and macOS)

Select **Policies & Configs > Configurations > Add New > Email** to set up POP or IMAP email. The following table describes the email settings you can specify:

TABLE 43. POP AND IMAP EMAIL SETTINGS (IOS AND MACOS)

Section	Field Name	Description
	Name	Enter brief text that identifies this group of email settings.
	Description	Enter additional text that clarifies the purpose of this group of email settings.
	Account Type	Select **POP** or **IMAP** to indicate the type of email account you are configuring. The Internet Service Provider (ISP) can give you information on which type of account is available.
	User Email	Specify the email address to use. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your email standard might be $EMAIL$_US for users in the United States. Custom attribute variable substitutions are supported. See "Supported variables" on page 382.
Incoming Mail Server Settings		
	Path Prefix	Specify the IMAP path prefix for the email client. A prefix is generally required when all IMAP folders are listed under the Inbox. ISPs that require prefixes usually provide information on the specific prefix to configure.
	Server Address	Specify the address for the server handling incoming mail. The Internet service provider (ISP) can give you this address.

TABLE 43. POP AND IMAP EMAIL SETTINGS (IOS AND MACOS) (CONT.)

Section	Field Name	Description
	Server Port	Specify the port number for the server handling incoming mail. The Internet service provider (ISP) can give you this information.
	Require SSL	Specify whether secure sockets layer (SSL) is required for incoming email transport. This is determined by the way in which the user mailboxes are set up. Your Internet service provider (ISP) can give you this information.
	User Name	Specify the email address to use. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. Custom attribute variable substitutions are supported. **Why:** Some enterprises have a strong preference concerning which identifier is exposed. See "Supported variables" on page 382
	Use Password Authentication	Specify whether to authenticate the password for email access.
	Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$. Custom attribute variable substitutions are supported. See "Supported variables" on page 382.
Outgoing (SMTP) Mail Server Settings		
	Server Address	Specify the address for the SMTP server handling outgoing mail.
	Server Port	Specify the port number for the SMTP server handling outgoing mail.
	Require SSL	Specify whether to use secure sockets layer (SSL) outgoing email transport.
	Require Authentication	Specify whether to use secure sockets layer (SSL) for outgoing email transport.

TABLE 43. POP AND IMAP EMAIL SETTINGS (IOS AND MACOS) (CONT.)

Section	Field Name	Description
	Use Same User Name and Password for Sending Email	Specify whether to use the same user name and password used for incoming email. If you select this option, then the **Server User Name** option is disabled.
	Server User Name	Specify the user name to use. The default value is $EMAIL$. Use this field to specify an alternate format. For example, your standard might be $USERID$. **Why:** Some enterprises have a strong preference concerning which identifier is exposed. See "Supported variables" on page 382
	Use Password Authentication	Specify whether to authenticate the password for email access.
	Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$. See "Supported variables" on page 382
Advanced Settings		Not for iOS, macOS
	Automatic Send/Receive	Specify how new email should be sent and retrieved. You can set an automatic time interval or select Manual to configure no automatic email exchange.
	Download Messages	Specify the number of messages to download to the device during send/receive.
	Message Format	Indicate whether messages should be formatted in plain text or HTML.
	Message Download Limit	Specify a size limit for a single message to be downloaded.
	Download Attachment	Specify a size limit for an attachment to be downloaded, or specify that attachments are not be downloaded.
iOS 5 or later Settings		
	Block move/forward messages to other email accounts	Enables the iOS 5 feature that prevents users from moving email messages to other email accounts or forwarding email from accounts other than the originating account.

TABLE 43. POP AND IMAP EMAIL SETTINGS (IOS AND MACOS) (CONT.)

Section	Field Name	Description
	Block email access to 3rd party apps	Prevents third-party apps from using the account for email access.
	Allow Recent Address syncing (iOS 6 and later)	Selected by default, indicates recent address syncing. If this check box is cleared, this email account is excluded from address recent syncing.
	Allow Mail Drop (iOS 9.2 and later)	De-selected by default, indicates allowance of Mail Drop. If this check box is selected, Mail Drop is allowed for this email account. Mail Drop limitations by Apple are applied.
		In Email settings on the users' device, the user can select the *Send large attachments with Mail Drop* option. This allows the user to upload attachments up to 5 GB and send a link or preview to email recipients.
S/MIME Setting	S/MIME settings apply only to iOS devices.	
S/MIME		
	Enable for iOS 9.3.3 (or earlier)	Select to enable S/MIME signing and encryption on devices running iOS 9.3.3 or earlier.
		You must select this option for the fields in the **S/MIME Signing** and **S/MIME Encryption** sections to apply to devices running iOS 9.3.3 or earlier.
S/MIME Signing	S/MIME signing applies only to iOS devices.	
	S/MIME Signing: Enable	Disabled by default. Select the check box to enable S/MIME signing.
	S/MIME Signing identity	Select a certificate enrollment setting as a signing identity. If you do not make a selection, then the device user will be prompted to select from the certificates that are already installed on the device. If the device has no certificate, then S/MIME signing will not be functional on the device. **Related topics** "Certificate Enrollment settings" on page 656.
	Signing Identity: User Overrideable	iOS 12.0 or supported newer versions. Select to allow the user to select the signing identity.

TABLE 43. POP AND IMAP EMAIL SETTINGS (IOS AND MACOS) (CONT.)

Section	Field Name	Description
	S/MIME Signing: User Overrideable	iOS 12 or supported newer versions. Select to allow the user to enable and disable S/MIME signing in device settings.
S/MIME Encryption		S/MIME signing applies only to iOS devices.
	Encryption by Default	Disabled by default.Select to enable S/MIME encryption.
	Encryption Identity	Select a certificate enrollment setting as an encryption identity. If you do not make a selection, then the device user will be prompted to select from the certificates that are already installed on the device. If the device has no certificate, then S/MIME encryption will not be functional on the device. **Related topics** "Certificate Enrollment settings" on page 656.
	Encryption Identity: User Overrideable	iOS 12.0 or supported newer versions. Select to allow the user to set the S/MIME encryption identity and enable encryption.
	Per-Message Encryption Switch	Per-message S/MIME for iOS allows device users to enable or disable S/MIME encryption for each email they send. ⓘ S/MIME encryption is incompatible with Sentry attachment encryption.

Supported variables

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

- For user name fields: $USERID$, $EMAIL$,$SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, CUSTOM_USER_Attributename$, or $NULL$

- $MANAGED_APPLE_ID$

> (i) For Shared iPad devices and User Enrolled devices only.

- For password fields: $USERID$, $EMAIL$, $PASSWORD$, $GOOGLE_AUTOGEN_PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, CUSTOM_USER_Attributename$, or $NULL$.

Custom attribute variable substitutions are supported.

Enabling per-message S/MIME for iOS

Per-message S/MIME for iOS allows iOS device users to decide whether they wish to enable or disable S/MIME encryption for individual emails. Allowing users to forgo encryption for emails that do not require such security precautions could save company resources such as bandwidth.

> (i) **WARNING:** S/MIME encryption is incompatible with Sentry attachment encryption. It is recommended that you enable either S/MIME encryption or Sentry attachment encryption, but not both. If you would like to enable attachment security along with S/MIME for email, you can use the Ivanti Docs@Work attachment control feature, in which all attachments can only be opened with a predefined set of device apps.

Organizations with varying security needs may wish to configure two Microsoft Exchange servers to handle default and optional use of S/MIME. An example might be an organization with one set of email users defined on one Exchange server that rarely need to encrypt their emails with S/MIME, and another set of email users defined on another Exchange server who use S/MIME encryption for most of their email.

In this scenario, Exchange profile 1 might be configured to enable S/MIME encryption on all email by default, and point to one particular Exchange server. Exchange profile 2 might be configured to enable S/MIME per-message encryption and point to a second Exchange server.

Note the following:

- Recipients of all emails sent with S/MIME encryption must have a certificate.

- A user sending an encrypted email must have the recipient's certificate so that its public key can be used to encrypt the message. This means that both the sender and recipient must be in the same organization, or if they are in different organizations, the sender and recipient must arrange to obtain their respective certificates prior to sending the first encrypted email.

- Both the sender and recipient must maintain historical archives of expired private keys, such that past emails encrypted by any expired certificates are still readable.

Procedure

The main steps for enabling per-message S/MIME encryption for iOS devices are as follows:

1. Upload a trusted root certificate to Ivanti EPMM from an in-house or public certificate authority ("Uploading a trusted root certificate to Ivanti EPMM" below).

2. Create a user-provided certificate enrollment setting ("Creating a user-provided certificate enrollment setting for S/MIME certificates" on the next page).

3. Upload the user-provided P12 certificates with the Ivanti EPMM user portal or the Web Services API ("Uploading user signing and encryption certificates with the User Portal" on page 386 and "Uploading user certificates with the Web Services API" on page 387).

4. Create an Email or Exchange setting that references the user-provided certificate enrollment setting you created ("Creating an Email setting for per message S/MIME encryption" on page 387 or "Creating an Exchange setting for per message S/MIME encryption" on page 389).

5. Push your settings to the relevant devices ("Pushing per-message S/MIME changes to devices" on page 391).

> **ⓘ**   iOS devices will not use SSL with an untrusted certificate.

For information about using per-message S/MIME encryption on an iOS device, see the following Apple article: http://support.apple.com/en-us/HT4979

Uploading a trusted root certificate to Ivanti EPMM

Upload a trusted root certificate to Ivanti EPMM, and then push the root certificate to iOS devices. The root certificate verifies the signature of the certificate authority presented with an email sender's transmission.

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

2. Select **Add New > Certificates**.

3. In the **New Certificate Setting** dialog box, fill in the following fields for the certificate setting:

   - **Name**: Enter a name for the certificate setting.

- **Description**: Enter a meaningful description for the certificate setting.

- **File Name**: Browse for the certificate file.

4. Select **Save**.

Creating a user-provided certificate enrollment setting for S/MIME certificates

Create a user-provided certificate enrollment setting that specifies the use of S/MIME certificates, and push the user-provided certificate enrollment setting to the relevant devices.

> ℹ️ If users are uploading both a signing certificate and an encryption certificate you must create two separate user-provided certificate enrollment settings.

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

2. Select **Add New > Certificate Enrollment > User-Provided**. The New User-Provided Certificate Enrollment Setting dialog box opens.

3. Fill in or select the following fields:

- **Name**: Enter brief text that identifies this group.

- **Description**: Enter additional text that clarifies the purpose of the setting.

- **Display Name**: Enter a name describing the purpose of a user-provided certificate. For example, enter "S/MIME Encryption". On the user portal, when the user uploads a certificate, the user selects a display name (called "Configuration" on the user portal). 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.

- **Require Password**: This is selected by default and is required for the certificate enrollment option.

- **Delete Private Keys After Days**: Select an option between None - 15 days.

4. Select **Save**.

5. The Configurations page refreshes with the new certificate enrollment.

6. (Optional) If users are uploading both a signing certificate and an encryption certificate, repeat these steps to create a second user-provided certificate enrollment setting.

Related topics

Uploading user signing and encryption certificates with the User Portal

Allowing users to control their own S/MIME encryption per message requires users to upload their personal PKCS 12 files containing their certificates and private keys. Users can upload their certificates through the user portal.

Alternatively, the certificates can be uploaded using the Web Services API, as described in "Uploading user certificates with the Web Services API" on the next page.

To upload an S/MIME certificate through the user portal:
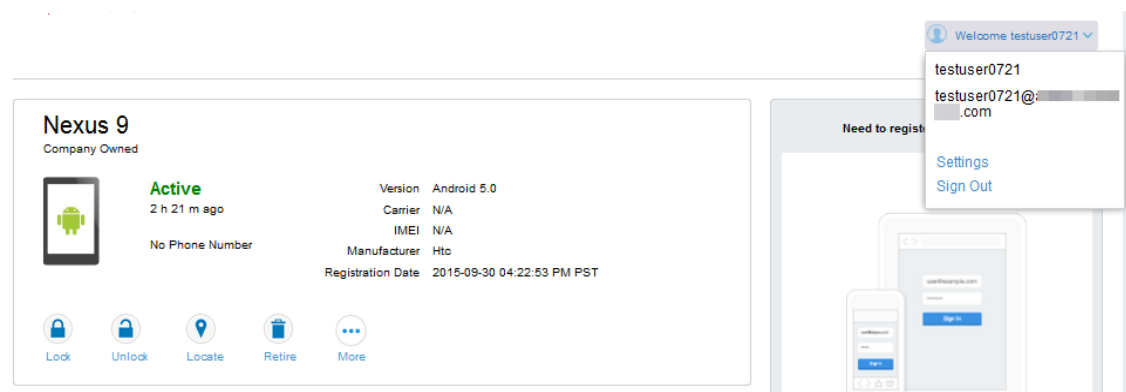
1. Go to https://*<IvantiEPMM_Server_FQDN>*/user.

2. Select on the device user's name in the top right corner.

3. Select on **Settings** in the drop down menu.

    The page including **User-Provided Certificate Management** appears.

4. Select **Upload New Certificate.**

    The **Upload User-Provided Certificate** page appears.

5. In the **Configuration** field, select the configuration for which you want the certificate to be used.

6. Select **Browse** to navigate to the location of the certificate and select the certificate.

7. Enter the **Password** associated with the certificate.

8. Select **Upload Certificate** to upload the certificate.

   The **User-Provided Certificate Management** page appears.

   Device users can view, replace, or delete the S/MIME certificate.

Uploading user certificates with the Web Services API

Instead of having users upload their certificates to the Ivanti EPMM user portal, you can upload the user certificates using a Web Services API. For more information about using the API, see the *Ivanti EPMM V2 API Guide*.

> If you used the now unavailable V1 API to upload user certificates to Ivanti EPMM, the API associated the user certificate with a certificate type: All, WIFI, VPN, SMIMESIGNING, SMIMEENCRYPTION, EMAIL or EXCHANGE. Ivanti EPMM still supports using those certificates and their associated type. However, you should migrate to uploading certificates that are associated with a user-provided certificate enrollment setting by using the V2 API .

Creating an Email setting for per message S/MIME encryption

Create an email setting so that device users can access their email with the ability to toggle S/MIME encryption per message.

If your email is managed by an Exchange Server, or you are using ActiveSync, you can create an Exchange setting instead, as described in "Exchange settings" on page 370.

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

2. Select **Add New > Email**. The New Email Setting dialog box opens.

3. Enter the information requested, as described in the table of settings in "Configuring POP and IMAP email settings (for iOS and macOS)" on page 378.

4. Configure the following to enable per-message S/MIME encryption using the options listed in the table below.

5. Select **Save**.

TABLE 1. PER-MESSAGE S/MIME ENCRYPTION OPTIONS

Section	Field Name	Description
S/MIME Settings		
S/MIME		
	Enable for iOS 9.3.3 (or earlier)	Select to enable S/MIME signing and encryption on Android devices and devices running iOS 9.3.3 or earlier. You must select this option for the fields in the **S/MIME Signing** and **S/MIME Encryption** sections to apply to devices running iOS 9.3.3 or earlier.
S/MIME Encryption		
	Encryption by Default	Disabled by default.Select to enable S/MIME encryption.
	Encryption Identity	Select a certificate enrollment setting as an encryption identity. If you do not make a selection, then the device user will be prompted to select from the certificates that are already installed on the device. If the device has no certificate, then S/MIME encryption will not be functional on the device. **Related topics** "Certificate Enrollment settings" on page 656.
	Encryption Identity: User Overrideable	iOS 12.0 or supported newer versions. Select to allow the user to set the S/MIME encryption identity and enable encryption.
	Per-Message Encryption Switch	Per-message S/MIME for iOS allows device users to enable or disable S/MIME encryption for each email they send. ⓘ S/MIME encryption is incompatible with Sentry attachment encryption.

Creating an Exchange setting for per message S/MIME encryption

If your organization uses Microsoft Exchange Server or ActiveSync to manage email, create an Exchange setting to enable devices to access email.

ℹ If an Exchange profile already exists on managed devices, then attempts to distribute new ActiveSync settings using Ivanti Endpoint Manager Mobile will fail.

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

2. Select **Add New > Exchange**. The New Exchange Setting dialog box opens.

3. Enter the following ActiveSync information.

Section	Field Name	Description
	ActiveSync User Name	Enter a variable such as $USERID$. This feature supports custom device and user attributes variable names. $MANAGED_APPLE_ID$ can be used for Shared iPad devices and User Enrolled devices only.
	ActiveSync User Email	Enter a variable such as $USERID$. This feature supports custom device and user attributes variable names. $MANAGED_APPLE_ID$ can be used for Shared iPad devices and User Enrolled devices only.

4. Configure the following to enable per-message S/MIME encryption:

Section	Field Name	Description
S/MIME Settings		
S/MIME		
	Enable for Android and iOS 9.3.3 (or earlier)	Select to enable S/MIME signing and encryption on Android devices and devices running iOS 9.3.3 or earlier. You must select this option for the fields in the **S/MIME Signing** and **S/MIME Encryption** sections to apply to devices running iOS 9.3.3 or earlier.
S/MIME Encryption		
	Encryption by Default	Disabled by default.Select to enable S/MIME encryption.
	Encryption Identity	Select a certificate enrollment setting as an encryption identity. If you do not make a selection, then the device user will be prompted to select from the certificates that are already installed on the device. If the device has no certificate, then S/MIME encryption will not be functional on the device. **Related topics** "Certificate Enrollment settings" on page 656.
	Encryption Identity: User Overrideable	iOS 12.0 or supported newer versions. Select to allow the user to set the S/MIME encryption identity and enable encryption.
	Per-Message Encryption Switch	Per-message S/MIME for iOS allows device users to enable or disable S/MIME encryption for each email they send.

Section	Field Name	Description
		i S/MIME encryption is incompatible with Sentry attachment encryption.

5. Configure the following for iOS settings:

Section	Field Name	Description
iOS 5 or later Settings	Email access to Third-Party apps: Block	Select to prevent third-party apps from using the account for email access.
	Allow Recent Address syncing (iOS 6 and later)	Selected by default, indicates recent address syncing. If this check box is cleared, this email account is excluded from address recent syncing.
	Use OAuth for Authentication: Enable	For iOS 12.0 and later. If selected, do not require a password.
	Communication Service Rules (iOS 10 and later)	Select to choose a default app to be used when calling contacts from this account.

6. Continue configuring the Exchange settings as needed.

   For more information about configuring an Exchange setting, see "Exchange settings" on page 370.

7. Select **Save**.

Pushing per-message S/MIME changes to devices

To push changes to devices:

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

2. From the list of settings, select the Certificate and Email or Exchange settings you created in previous sections, then select **Actions > Apply to Label**.

   The **Apply to Label** dialog box opens.

> ℹ️ Do not apply the user-provided certificate enrollment setting to any labels.

3. Select the labels to which you want to apply the Certificate setting, Email setting or Exchange setting.

4. Select **Apply**.

    The settings will be pushed to the devices you specified per the Sync Interval defined in your sync policy, or at the next forced device check-in.

5. Instruct users to enable S/MIME on their devices as follows:

    a. Go to **Settings > Mail, Contacts, Calendars**.

    b. Select the email account associated with your client certificate.

    c. Tap the Account button with your email address.

    d. On the Account window, tap **S/MIME**.

    e. Enable signing by tapping **Sign** and selecting your certificate.

    f. Enable encryption by tapping **Encrypt**, and then select your certificate.

6. Email users the following link for more information on signing and encrypting email on an iOS device:

    http://support.apple.com/en-us/HT4979

Enabling S/MIME encryption and signing on iOS devices

Note the following:

- Recipients of all emails sent with S/MIME signing and encryption must have a certificate.

- A user sending an encrypted or signed email must have the recipient's certificate so that its public key can be used to encrypt the message. This means that both the sender and recipient must be in the same organization, or if they are in different organizations, the sender and recipient must arrange to obtain their respective certificates prior to sending the first encrypted or signed email.

- Both the sender and recipient must maintain historical archives of expired private keys, such that past emails encrypted by any expired certificates are still readable.

Main steps

The main steps for enabling S/MIME encryption and signing for iOS devices are as follows:

1. Upload a trusted root certificate to Ivanti EPMM from an in-house or public certificate authority ("Uploading a trusted root certificate to Ivanti EPMM" on page 384).

2. Create a user-provided certificate enrollment setting ("Creating a user-provided certificate enrollment setting for S/MIME certificates" on page 385).

3. Upload the user-provided P12 certificates with the Ivanti EPMM user portal or the Web Services API ("Uploading user signing and encryption certificates with the User Portal" on page 386 and "Uploading user certificates with the Web Services API" on page 387).

4. Create an Email or Exchange setting that references the user-provided certificate enrollment setting you created ("Configuring S/MIME encryption and signing for iOS devices" below).

5. Push your settings to the relevant devices ("Pushing per-message S/MIME changes to devices" on page 391).

> **ⓘ**   iOS devices will not use SSL with an untrusted certificate.

Configuring S/MIME encryption and signing for iOS devices

You can configure S/MIME encryption and/or signing settings for your ActiveSync server. The S/MIME settings you configure allow managed iOS devices to use S/MIME encryption and signing features, depending on how you have configured them.

For example, you can enable S/MIME encryption only, without signing, or you can enable both S/MIME encryption and signing, while also allowing device users to decide whether they want to use these features. You can also specify separate certificates for signing and encryption. If you do not specify a certificate, then the device user will be prompted to select from the certificates that are already installed on the device.

> **ⓘ**   If an Exchange profile already exists on managed devices, then attempts to distribute new ActiveSync settings using Ivanti Endpoint Manager Mobile will fail.

Before you begin

You need to complete the following tasks before configuring S/MIME for iOS devices:

1. "Uploading a trusted root certificate to Ivanti EPMM" on page 384

2. "Creating a user-provided certificate enrollment setting for S/MIME certificates" on page 385

3. "Uploading user signing and encryption certificates with the User Portal" on page 386

   or

   "Enabling per-message S/MIME for iOS" on page 383

Procedure

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

   a. If using an Exchange setting:

   b. Select the Exchange setting you want to modify, and select **Edit**.

      Alternatively, create a new Exchange setting by selecting **Add New > Exchange**.

2. Continue configuring the Exchange settings as needed. For more information, see "Exchange settings" on page 370.

   a. If using an Email setting:

   b. Select the Email setting you want to modify, and select **Edit**.

      Alternatively, create a new Email setting by selecting **Add New > Email**.

3. Enter the information required to configure your mail server, as described in "Configuring POP and IMAP email settings (for iOS and macOS)" on page 378.

4. Configure your S/MIME Settings using the table below.

5. Select **Save**.

6. Push your settings to devices, as described in "Pushing per-message S/MIME changes to devices" on page 391.

TABLE 1. S/MIME SETTINGS

Section	Field Name	Description
S/MIME	Enable for iOS 9.3.3 (or earlier)	Select to enable S/MIME signing and encryption on devices running iOS 9.3.3 or earlier. You must select this option for the fields in the **S/MIME Signing** and **S/MIME Encryption** sections to apply to devices running iOS 9.3.3 or earlier.
S/MIME Encryption	Encryption by Default	Disabled by default.Select to enable S/MIME encryption.
	Encryption Identity	Select a certificate enrollment setting as an encryption identity. If you do not make a selection, then the device user will be prompted to select from the certificates that are already installed on the device. If the device has no certificate, then S/MIME encryption will not be functional on the device. **Related topics** "Certificate Enrollment settings" on page 656.
	Encryption Identity: User Overrideable	iOS 12.0 or supported newer versions. Select to allow the user to set the S/MIME encryption identity and enable encryption.
	Per-Message Encryption Switch	Per-message S/MIME for iOS allows device users to enable or disable S/MIME encryption for each email they send. ⓘ S/MIME encryption is incompatible with Sentry attachment encryption.

Synchronizing Google account data

You can synchronize email, contacts, calendar, and tasks with mail apps on devices managed by Ivanti EPMM. 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 Ivanti EPMM. 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 Ivanti EPMM.

Main steps

Synchronizing Google Apps data involves the following main steps:

- "Using OAuth to enable access to Google APIs" below
- "Uploading OAuth credentials to the Google Admin Console" on the next page
- "Linking Google Apps credentials with Ivanti EPMM" on page 398
- "Setting up your Exchange setting for access to Google Apps data" on page 399
- "Renewing the Google Apps password for a given set of users" on page 402 (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 Ivanti EPMM

You must upload the JSON credentials file you downloaded from the Google Developers console to link your Google credentials with Ivanti EPMM. For more information, see "Using OAuth to enable access to Google APIs" on page 396.

> ℹ️ If the Google password has expired, iOS will not necessarily be aware of the expiration, and synchronization could fail. Manually regenerate the Google password from the Google Developers Console.

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, select **Browse**.

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

   a. Select **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. Select **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.

     > ℹ️ 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 Ivanti EPMM.

9. Select **Save**.

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

Setting up your Exchange setting for access to Google Apps data

Create an Exchange setting to connect Ivanti EPMM 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 Ivanti EPMM pushes the new setting to the correct devices. The Exchange setting must include the Google Apps Password flag, which tells Ivanti EPMM to generate a Google Apps password and send it to Google servers.

When sending an event to a device, Ivanti EPMM 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 Ivanti EPMM sends the password to Google first before sending the Exchange setting to the device.

If Ivanti EPMM cannot find a user on Google, Ivanti EPMM 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 402.

Note the following:

- If you intend to distribute an AppConnect email app to devices, such as Ivanti 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 EPMM*.

- 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. Select **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, Inc Professional Services. For more information about configuring Sentry, see the *Ivanti Standalone Sentry Guide for EPMM*.
Use SSL	Select to use secure connections.

Item	Description
	ⓘ 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 Ivanti EPMM. This password allows device users to access their mail, contacts, and calendar data on their managed devices. When selected, Ivanti EPMM grays out the **ActiveSync User Name** and **ActiveSync User Password**. This check box only appears if you have configured a Google account with Ivanti EPMM, as described in "Synchronizing Google account data" on page 396.
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.
Email access to Third-Party apps	Disable this option, so that third-party apps can use the account for email access.

4. Select **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 select **Apply**.

> ⓘ   For information on calling contacts using your Google email account, see "Google Account " on page 761.

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, Ivanti EPMMre-queues the event. Ivanti EPMM tracks the number of attempts to send updated passwords to Google. If it reaches the preset maximum number of attempts to contact Google servers, Ivanti EPMM 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 Admin Portal. After you generate it, Ivanti EPMM 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. Select **Renew Google Apps Password**.

   The Admin Portal sends the request to renew the Google Apps password for the selected users.
5. Select **Close**.

Synchronizing Google calendar and contacts without ActiveSync

Ivanti EPMM allows you to configure managed iOS devices to synchronize with Google calendar and contact data directly, rather than through ActiveSync. Synchronizing Google calendar and contact data with iOS devices using a CalDAV or CardDAV configuration allows data to synchronize more quickly with devices and without an ActiveSync configuration.

Create a CalDAV or CardDAV configuration so that users will be able to access their Google calendar and contact data.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Click **Add New**.

3. Select **Apple > iOS and macOS > CardDAV** or **CalDAV**.

4. Use the following guidelines to fill in the form:

Item	Description
Name	Enter brief text that identifies this group of iOS and macOS CalDAV or CarDAV settings.
Description	Enter additional text that clarifies the purpose of this group of iOS and macOS CalDAV or CarDAV settings.
HostName	Enter the host name of the calendar server.
Port	Enter the port for the calendar server.
Principal URL	Enter the URL for accessing calendar services.
Use SSL	Select to use SSL for data transfer.
Use Google Apps Password	Select to use the Google Apps password.

5. Click **Save**.
6. Apply the new CalDAV or CardDAV setting to the relevant devices.

Managing Wi-Fi Settings

This section addresses the Wi-Fi settings.

> ℹ️   All Wi-Fi settings and features supported by iOS devices are also supported by tvOS devices.

- "Wi-Fi settings" below
- "Wi-Fi profiles and password caching" on the next page
- "Wi-Fi authentication types" on page 406

> ℹ️   The features described in this section are supported on macOS devices.

Wi-Fi settings

To configure wireless network access, in the Admin Console, go to **Policies & Configs > Configurations.** Select **Add New > Wi-Fi** to create a new configuration. Wi-Fi settings are done based on the authentication type set by the administrator. See "Wi-Fi authentication types" on page 406.

Only the WPA Enterprise and EAP type of TTLS are supported for macOS devices.

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.

> ℹ️   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, Ivanti EPMM offers the option of caching a user's Wi-Fi password. This option is turned off by default. Cached passwords are encrypted, stored on Ivanti EPMM, 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" below
- "Shared authentication" on page 410
- "WPA Enterprise authentication" on page 415
- "WPA2 / WPA3 Enterprise authentication" on page 419
- "WPA Personal authentication" on page 423
- "WPA2 / WPA3 Personal authentication" on page 428
- "Supported variables for Wi-Fi authentication" on page 430

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 44. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Ivanti EPMM.
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.
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	Not Applicable for iOS.
Network Key	Not Applicable for iOS.
Key Index	WEP encryption

TABLE 44. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	If using multiple network keys, select a number indicating the memory position of the correct encryption key.
Confirm Network Key	This feature is not supported on iOS devices.
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 430
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 Ivanti EPMM 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 430.
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.

TABLE 44. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	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 You can make multiple selections. **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 Mac OS devices.
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 44. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Auto Join	Specifies whether devices should automatically join the corresponding Wi-Fi network. If this option is not selected, device users must tap the network name on the device to join the network.
Disable Captive Network Detection	Select to disable Apple's Captive Network Assistant, which automatically detects captive networks. When this option is selected, device users must manually open a web browser to trigger the portal login for the captive network. This feature is supported on devices running iOS 10 and macOS 10 or supported newer versions.
Disable MAC address randomization	Select to disable MAC address randomization for that Wi-Fi network while associated with the network. It also disables the Private Address. Device users will see a "Privacy Warning" message on their Wi-Fi settings indicating that the network has reduced privacy protections. Note the following: • The device user will still have the ability to set the device to report a random address for new connections instead of the device's actual Wi-Fi MAC address. • MDM will always get the actual MAC address. This property only affects the MAC address that the device reports to the server. Applicable to iOS 14.0 or supported newer versions.
Proxy Type	Specifies whether a proxy is configured, and which type. Available types are Manual and Auto.
Proxy PAC URL	Optional. Specifies the URL for the proxy auto-configuration (PAC) file.
Proxy Server	Specifies the proxy server's IP address.
Proxy User Name	For manual proxies, specifies the optional user name for server access.
Proxy Password	For manual proxies, specifies the optional password for server access.
Priority	Enter a number between 1 and 100 to set the priority for the Wi-Fi setting, or leave the field blank. If multiple Wi-Fi settings are applied, the device selects the Wi-Fi setting with the higher priority. Higher numbers signify higher priority.
Cisco QoS fast lane	Supported on devices running iOS 10 or supported newer versions.

TABLE 44. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Restrict QoS marking	Select to restrict Cisco Quality of Service (QoS) "fast lane" prioritization to particular whitelisted iOS apps. Disabled by default, such that any iOS app may benefit from fast lane prioritization.
Disable L3 marking and only allow L2 marking for traffic sent to the Wi-Fi network	Select to mark traffic sent to the Wi-Fi network as L2 only.
Whitelist audio and video calls for L2 and L3 marking	Select to allow all voice and video calls to be marked as L2 and L3 traffic. ℹ️ If you disable L3 marking and whitelist audio and video for L2 and L3 marking, then audio and video calls will be marked as L2 only.
Apps that will be whitelisted for L2 and L3 marking for traffic	Mark the check box to select specific apps you want to whitelist for L2 and L3 traffic marking. • Select the Add (+) button to add a row to the table of apps. A new row is added to the table. In the App Name column, select the drop-down list to select an App Catalog app. • Repeat for any other apps you want to whitelist for L2 and L3 traffic marking.
Windows Settings	These features are not supported on iOS devices. These features are not supported on Mac OS devices.

Related topics

- "Shared authentication" below
- "WPA Enterprise authentication" on page 415
- "WPA2 / WPA3 Enterprise authentication" on page 419
- "WPA Personal authentication" on page 423
- "WPA2 / WPA3 Personal authentication" on page 428
- "Supported variables for Wi-Fi authentication" on page 430

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 45. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Ivanti EPMM.
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.
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	This feature is not supported on iOS devices.
Network Key	This feature is not supported on iOS devices.
Key Index	WEP encryption If using multiple network keys, select a number indicating the memory position of the correct encryption key.
Confirm Network Key	This feature is not supported on iOS devices.
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 430.
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 Ivanti EPMM administrator. Note the following: • If you specify $PASSWORD$, also enable **Save User Password** under **Settings > System Settings > Users & Devices > Registration**.

TABLE 45. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS (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. See "Supported variables for Wi-Fi authentication" on page 430.
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 You can make multiple selections.

TABLE 45. WI-FI SHARED 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	
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.
Auto Join	Specifies whether devices should automatically join the corresponding Wi-Fi network. If this option is not selected, device users must tap the network name on the device to join the network.
Disable Captive Network Detection	Select to disable Apple's Captive Network Assistant, which automatically detects captive networks. When this option is selected, device users must manually open a web browser to trigger the portal login for the captive network. This feature is supported on devices running iOS 10 and macOS 10 or supported newer versions.
Disable MAC address randomization	Select to disable MAC address randomization for that Wi-Fi network while associated with the network. Device users will see a "Privacy Warning" message on their Wi-Fi settings indicating that the network has reduced privacy protections. Changing this option will disable the Private Address. ⓘ The device user will still have the ability to set the device to report a random address for new connections instead of the device's actual Wi-Fi MAC address. Applicable to iOS 14.0 or supported newer versions.

TABLE 45. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Proxy Type	Specifies whether a proxy is configured, and which type. Available types are Manual and Auto.
Proxy PAC URL	Specifies the URL for the proxy auto-configuration (PAC) file.
Proxy Server	Specifies the proxy server's IP address.
Priority	Enter a number between 1 and 100 to set the priority for the Wi-Fi setting, or leave the field blank. If multiple Wi-Fi settings are applied, the device selects the Wi-Fi setting with the higher priority. Higher numbers signify higher priority.
Cisco QoS fast lane	Supported on devices running iOS 10 or supported newer versions.
Restrict QoS marking	Select to restrict Cisco Quality of Service (QoS) "fast lane" prioritization to particular whitelisted iOS apps. Disabled by default, such that any iOS app may benefit from fast lane prioritization.
Disable L3 marking and only allow L2 marking for traffic sent to the Wi-Fi network	Select to mark traffic sent to the Wi-Fi network as L2 only.
Whitelist audio and video calls for L2 and L3 marking	Select to allow all voice and video calls to be marked as L2 and L3 traffic. ℹ️ If you disable L3 marking and whitelist audio and video for L2 and L3 marking, then audio and video calls will be marked as L2 only.
Apps that will be whitelisted for L2 and L3 marking for traffic	Mark the check box to select specific apps you want to whitelist for L2 and L3 traffic marking. • Select the Add (+) button to add a row to the table of apps. A new row is added to the table. In the App Name column, select the drop-down list to select an App Catalog app. • Repeat for any other apps you want to whitelist for L2 and L3 traffic marking.
Android Settings	These settings apply only to Android devices.
Windows Settings	These settings apply only to Windows devices.

Related topics

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 46. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Ivanti EPMM.
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.
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	This feature is not supported on iOS devices. This feature is not supported on Mac macOS devices.
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 430
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 Ivanti EPMM administrator. If you specify $PASSWORD$, also enable Save User Password under **Settings > System Settings > Users & Devices > Registration**.

TABLE 46. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	ℹ 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 430
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 You can make multiple selections. **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 46. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS (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	
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.
Auto Join	Specifies whether devices should automatically join the corresponding Wi-Fi network. If this option is not selected, device users must tap the network name on the device to join the network.
Disable Captive Network Detection	Select to disable Apple's Captive Network Assistant, which automatically detects captive networks. When this option is selected, device users must manually open a web browser to trigger the portal login for the captive network. This feature is supported on devices running iOS 10 and macOS 10 or supported newer versions.
Disable MAC address randomization	Select to disable MAC address randomization for that Wi-Fi network while associated with the network. Device users will see a "Privacy Warning" message on their Wi-Fi settings indicating that the network has reduced privacy protections. Changing this option will disable the Private Address. ⓘ The device user will still have the ability to set the device to report a random address for new connections instead of the device's actual Wi-Fi MAC address. Applicable to iOS 14.0 or supported newer versions.
Proxy Type	Specifies whether a proxy is configured, and which type. Available types are Manual and Auto.
Proxy PAC URL	Specifies the URL for the proxy auto-configuration (PAC) file.
Proxy Server	Specifies the proxy server's IP address.

TABLE 46. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Priority	Enter a number between 1 and 100 to set the priority for the Wi-Fi setting, or leave the field blank. If multiple Wi-Fi settings are applied, the device selects the Wi-Fi setting with the higher priority. Higher numbers signify higher priority.
Cisco QoS fast lane	Supported on devices running iOS 10 or supported newer versions.
Restrict QoS marking	Select to restrict Cisco Quality of Service (QoS) "fast lane" prioritization to particular whitelisted iOS apps. Disabled by default, such that any iOS app may benefit from fast lane prioritization.
Disable L3 marking and only allow L2 marking for traffic sent to the Wi-Fi network	Select to mark traffic sent to the Wi-Fi network as L2 only.
Whitelist audio and video calls for L2 and L3 marking	Select to allow all voice and video calls to be marked as L2 and L3 traffic. ⓘ If you disable L3 marking and whitelist audio and video for L2 and L3 marking, then audio and video calls will be marked as L2 only.
Apps that will be whitelisted for L2 and L3 marking for traffic	Mark the check box to select specific apps you want to whitelist for L2 and L3 traffic marking. • Select the Add (+) button to add a row to the table of apps. A new row is added to the table. In the App Name column, select the drop-down list to select an App Catalog app. • Repeat for any other apps you want to whitelist for L2 and L3 traffic marking.
Android Settings	These settings apply only to Android devices.
Windows Settings	These settings apply only to Windows devices.

Related topics

- "Open authentication" on page 406
- "Shared authentication" on page 410
- "WPA2 / WPA3 Enterprise authentication" on the next page
- "WPA Personal authentication" on page 423
- "WPA2 / WPA3 Personal authentication" on page 428
- "Supported variables for Wi-Fi authentication" on page 430

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 47. 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.
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	This feature is not supported on iOS devices.
User Name	Specify the variable to use as the user name when establishing the Wi-Fi connection. See "WPA2 / WPA3 Enterprise authentication" above.
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 Ivanti EPMM administrator. ⓘ If you specify $PASSWORD$, also enable **Save User Password** under **Settings > System Settings > Users & Devices > Registration**.

TABLE 47. 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 You can make multiple selections. **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 47. 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	
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.
Auto Join	Specifies whether devices should automatically join the corresponding Wi-Fi network. If this option is not selected, device users must tap the network name on the device to join the network.
Disable Captive Network Detection	Select to disable Apple's Captive Network Assistant, which automatically detects captive networks. When this option is selected, device users must manually open a web browser to trigger the portal login for the captive network. This feature is supported on devices running iOS 10 and macOS 10 or supported newer versions.
Disable MAC address randomization	Select to disable MAC address randomization for that Wi-Fi network while associated with the network. Device users will see a "Privacy Warning" message on their Wi-Fi settings indicating that the network has reduced privacy protections. Changing this option will disable the Private Address. ⓘ The device user will still have the ability to set the device to report a random address for new connections instead of the device's actual Wi-Fi MAC address. Applicable to iOS 14.0 or supported newer versions.
Proxy Type	Specifies whether a proxy is configured, and which type. Available types are Manual and Auto.
Proxy PAC URL	Specifies the URL for the proxy auto-configuration (PAC) file.
Proxy Server	Specifies the proxy server's IP address.

TABLE 47. WI-FI WPA2 / WPA3 ENTERPRISE AUTHENTICATION FIELD DESCRIPTION (CONT.)

Item	Description
Priority	Enter a number between 1 and 100 to set the priority for the Wi-Fi setting, or leave the field blank. If multiple Wi-Fi settings are applied, the device selects the Wi-Fi setting with the higher priority. Higher numbers signify higher priority.
Cisco QoS fast lane	Supported on devices running iOS or supported newer versions.
Restrict QoS marking	Select to restrict Cisco Quality of Service (QoS) "fast lane" prioritization to particular whitelisted iOS apps. Disabled by default, such that any iOS app may benefit from fast lane prioritization.
Disable L3 marking and only allow L2 marking for traffic sent to the Wi-Fi network	Select to mark traffic sent to the Wi-Fi network as L2 only.
Whitelist audio and video calls for L2 and L3 marking	Select to allow all voice and video calls to be marked as L2 and L3 traffic. ⓘ If you disable L3 marking and whitelist audio and video for L2 and L3 marking, then audio and video calls will be marked as L2 only.
Apps that will be whitelisted for L2 and L3 marking for traffic	Mark the check box to select specific apps you want to whitelist for L2 and L3 traffic marking. • Select the Add (+) button to add a row to the table of apps. A new row is added to the table. In the App Name column, select the drop-down list to select an App Catalog app. • Repeat for any other apps you want to whitelist for L2 and L3 traffic marking.
Android Settings	These settings apply only to Android devices.
Windows Settings	These settings apply only to Windows devices.

Related topics

- "Open authentication" on page 406
- "Shared authentication" on page 410
- "WPA Enterprise authentication" on page 415
- "WPA Personal authentication" below
- "WPA2 / WPA3 Personal authentication" on page 428
- "Supported variables for Wi-Fi authentication" on page 430

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 48. WI-FI WPA PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Ivanti EPMM.
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.
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	This feature is not supported for iOS devices.
Network Key	This feature is not supported for iOS devices.
Confirm Network Key	This feature is not supported for iOS devices.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
Apple 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.
Auto Join	Specifies whether devices should automatically join the corresponding Wi-Fi network. If this option is not selected, device users must tap the network name on the device to join the network.

TABLE 48. WI-FI WPA PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Disable Captive Network Detection	Select to disable Apple's Captive Network Assistant, which automatically detects captive networks. When this option is selected, device users must manually open a web browser to trigger the portal login for the captive network. This feature is supported on devices running iOS 10 and macOS 10 or supported newer versions.
Disable MAC address randomization	Select to disable MAC address randomization for that Wi-Fi network while associated with the network. Device users will see a "Privacy Warning" message on their Wi-Fi settings indicating that the network has reduced privacy protections. Changing this option will disable the Private Address. ⓘ The device user will still have the ability to set the device to report a random address for new connections instead of the device's actual Wi-Fi MAC address. Applicable to iOS 14.0 or supported newer versions.
Proxy Type	Specifies whether a proxy is configured, and which type. Available types are Manual and Auto.
Proxy PAC URL	Specifies the URL for the proxy auto-configuration (PAC) file.
Proxy Server	Specifies the proxy server's IP address.
Priority	Enter a number between 1 and 100 to set the priority for the Wi-Fi setting, or leave the field blank. If multiple Wi-Fi settings are applied, the device selects the Wi-Fi setting with the higher priority. Higher numbers signify higher priority.
Cisco QoS fast lane	Supported on devices running iOS 10 or supported newer versions.
Restrict QoS marking	Select to restrict Cisco Quality of Service (QoS) "fast lane" prioritization to particular whitelisted iOS apps. Disabled by default, such that any iOS app may benefit from fast lane prioritization.
Disable L3 marking and only allow L2 marking for traffic sent to the Wi-Fi network	Select to mark traffic sent to the Wi-Fi network as L2 only.
Whitelist audio and video calls for L2 and L3 marking	Select to allow all voice and video calls to be marked as L2 and L3 traffic.

TABLE 48. WI-FI WPA PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	ⓘ If you disable L3 marking and whitelist audio and video for L2 and L3 marking, then audio and video calls will be marked as L2 only.
Apps that will be whitelisted for L2 and L3 marking for traffic	Mark the check box to select specific apps you want to whitelist for L2 and L3 traffic marking. • Select the Add (+) button to add a row to the table of apps. A new row is added to the table. In the App Name column, select the drop-down list to select an App Catalog app. • Repeat for any other apps you want to whitelist for L2 and L3 traffic marking.
Android Settings	These settings apply only to Android devices.
Windows Settings	These settings apply only to Windows devices.

WPA2 Personal authentication

Use the following guidelines to configure WPA2 Personal authentication.

TABLE 49. WI-FI WPA2 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Ivanti EPMM.
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.
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	This feature is not supported for iOS devices.
Network Key	This feature is not supported for iOS devices.
Confirm Network Key	This feature is not supported for iOS devices.

TABLE 49. WI-FI WPA2 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
EAP Type	Not applicable.
Connects To	Select Internet or Work.
Apple Settings	
Auto Join	Specifies whether devices should automatically join the corresponding Wi-Fi network. If this option is not selected, device users must tap the network name on the device to join the network.
Disable Captive Network Detection	Select to disable Apple's Captive Network Assistant, which automatically detects captive networks. When this option is selected, device users must manually open a web browser to trigger the portal login for the captive network. This feature is supported on devices running iOS 10 and macOS 10 or supported newer versions.
Disable MAC address randomization	Select to disable MAC address randomization for that Wi-Fi network while associated with the network. Device users will see a "Privacy Warning" message on their Wi-Fi settings indicating that the network has reduced privacy protections. Changing this option will disable the Private Address. ⓘ The device user will still have the ability to set the device to report a random address for new connections instead of the device's actual Wi-Fi MAC address. Applicable to iOS 14.0 or supported newer versions.
Proxy Type	Specifies whether a proxy is configured, and which type. Available types are Manual and Auto.
Proxy PAC URL	Specifies the URL for the proxy auto-configuration (PAC) file.
Proxy Server	Specifies the proxy server's IP address.
Priority	Enter a number between 1 and 100 to set the priority for the Wi-Fi setting, or leave the field blank. If multiple Wi-Fi settings are applied, the device selects the Wi-Fi setting with the higher priority. Higher numbers signify higher priority.
Cisco QoS fast lane	Supported on devices running iOS or supported newer versions.
Restrict QoS marking	Select to restrict Cisco Quality of Service (QoS) "fast lane" prioritization to particular whitelisted iOS apps. Disabled by default, such that any iOS app may benefit from fast lane prioritization.

TABLE 49. WI-FI WPA2 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Disable L3 marking and only allow L2 marking for traffic sent to the Wi-Fi network	Select to mark traffic sent to the Wi-Fi network as L2 only.
Whitelist audio and video calls for L2 and L3 marking	Select to allow all voice and video calls to be marked as L2 and L3 traffic. ⓘ If you disable L3 marking and whitelist audio and video for L2 and L3 marking, then audio and video calls will be marked as L2 only.
Apps that will be whitelisted for L2 and L3 marking for traffic	Mark the check box to select specific apps you want to whitelist for L2 and L3 traffic marking. • Select the Add (+) button to add a row to the table of apps. A new row is added to the table. In the App Name column, select the drop-down list to select an App Catalog app. • Repeat for any other apps you want to whitelist for L2 and L3 traffic marking.
Android Settings	These settings apply only to Android devices.
Windows Settings	These settings apply only to Windows devices.

Related topics

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 50. WI-FI WPA2 / WPA3 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Ivanti EPMM.
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.
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	This feature is not supported for iOS devices.
Network Key	This feature is not supported for iOS devices.
Confirm Network Key	This feature is not supported for iOS devices.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
Apple 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.
Auto Join	Specifies whether devices should automatically join the corresponding Wi-Fi network. If this option is not selected, device users must tap the network name on the device to join the network.
Disable Captive Network Detection	Select to disable Apple's Captive Network Assistant, which automatically detects captive networks. When this option is selected, device users must manually open a web browser to trigger the portal login for the captive network.

TABLE 50. Wɪ-Fɪ WPA2 / WPA3 ᴘᴇʀsᴏɴᴀʟ ᴀᴜᴛʜᴇɴᴛɪᴄᴀᴛɪᴏɴ ꜰɪᴇʟᴅ ᴅᴇsᴄʀɪᴘᴛɪᴏɴs (Cᴏɴᴛ.)

Item	Description
	This feature is supported on devices running iOS 10 and macOS 10 or supported newer versions.
Disable MAC address randomization	Select to disable MAC address randomization for that Wi-Fi network while associated with the network. Device users will see a "Privacy Warning" message on their Wi-Fi settings indicating that the network has reduced privacy protections. Changing this option will disable the Private Address. ⓘ The device user will still have the ability to set the device to report a random address for new connections instead of the device's actual Wi-Fi MAC address. Applicable to iOS 14.0 or supported newer versions.
Proxy Type	Specifies whether a proxy is configured, and which type. Available types are Manual and Auto.
Proxy PAC URL	Specifies the URL for the proxy auto-configuration (PAC) file.
Proxy Server	Specifies the proxy server's IP address.
Priority	Enter a number between 1 and 100 to set the priority for the Wi-Fi setting, or leave the field blank. If multiple Wi-Fi settings are applied, the device selects the Wi-Fi setting with the higher priority. Higher numbers signify higher priority.
Cisco QoS fast lane	Supported on devices running iOS 10 or supported newer versions.
Restrict QoS marking	Select to restrict Cisco Quality of Service (QoS) "fast lane" prioritization to particular whitelisted iOS apps. Disabled by default, such that any iOS app may benefit from fast lane prioritization.
Disable L3 marking and only allow L2 marking for traffic sent to the Wi-Fi network	Select to mark traffic sent to the Wi-Fi network as L2 only.
Whitelist audio and video calls for L2 and L3 marking	Select to allow all voice and video calls to be marked as L2 and L3 traffic. ⓘ If you disable L3 marking and whitelist audio and video for L2 and L3 marking, then audio and video calls will be marked as L2 only.
Apps that will be whitelisted for L2 and L3 marking for traffic	Mark the check box to select specific apps you want to whitelist for L2 and L3 traffic marking.

TABLE 50. WI-FI WPA2 / WPA3 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	• Select the Add (+) button to add a row to the table of apps. A new row is added to the table. In the App Name column, select the drop-down list to select an App Catalog app. • Repeat for any other apps you want to whitelist for L2 and L3 traffic marking.
Android Settings	These settings apply only to Android devices.
Windows Settings	These settings apply only to Windows devices.

Related topics

- "Open authentication" on page 406
- "Shared authentication" on page 410
- "WPA Enterprise authentication" on page 415
- "WPA2 / WPA3 Enterprise authentication" on page 419
- "WPA Personal authentication" on page 423
- "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 406
- "Shared authentication" on page 410

Managing VPN Settings

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

- "VPN settings overview" below
- "Configuring new VPN settings" on the next page
- "Check Point Capsule" on page 434
- "Cisco AnyConnect (iOS only)" on page 440
- "Cisco Legacy AnyConnect" on page 455
- "F5 SSL" on page 472
- "IKEv2 (iOS Only)" on page 488
- "IPSec (Blue Coat)" on page 508
- "IPSec (Cisco)" on page 509
- "Juniper SSL" on page 521
- "L2TP" on page 539
- "Ivanti Tunnel (iOS and macOS)" on page 545
- "NetMotion Mobility VPN (iOS)" on page 545
- "Palo Alto Networks GlobalProtect" on page 555
- "PPTP" on page 571
- "Pulse Secure SSL" on page 576
- "SonicWall Mobile Connect" on page 594
- "Custom SSL" on page 610

> For macOS devices, use any VPN settings marked as supported on macOS devices.

VPN settings overview

This section covers VPN settings. If the item is not listed in the specific *Ivanti EPMM Device Management Guide* of your chosen OS, it does not apply to that OS.

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 Ivanti EPMM.
- 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.

Ivanti Mobile@Work uses the VPN client and the VPN setting to enable access to corporate networks.

> ℹ️   VPN Configurations are not supported with User Enrolled devices.

Configuring new VPN settings

In the Admin Portal, go to **Policies & Configs > Configurations** and select **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 Ivanti Tunnel (Android) in the Connection Type field.

For macOS devices, distribute the VPN configurations to either the Device Channel (effective for all users on a device) or the User Channel (effective only for the currently registered user on a device). Regardless of the user logged into the device, the configuration is effective for all users at the device level.

> ℹ️   When the bottom entry of the Safari domains list is clicked in a VPN configuration, the scroll bar automatically scrolls all the way to the top. New edit option introduced for Safari Domains on Windows integrated touch devices, you can now edit Safari Domains information, such as domain name and description, in the Edit VPN Setting window from the Windows UI touch screen.

Check Point Capsule

This VPN connection type is supported on iOS, macOS, and Windows devices only.

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

- "Proxy - None (default)" below

- "Proxy - Manual " on page 436

- "Proxy - Automatic" on page 438

Within these selections, you may make settings for:

- "Custom Data" on page 440

Proxy - None (default)

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

TABLE 51. 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 436 or "Proxy - Automatic" on page 438.
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 51. 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.
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.

Proxy - Manual

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

TABLE 52. 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 438.
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 $PASSWORD$.
Proxy Domains (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.

TABLE 52. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	Select **Add+** to add a domain.
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. ℹ️ 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.

TABLE 52. 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.

Proxy - Automatic

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

TABLE 53. 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 436
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)	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. Select **Add+** to add a domain.

TABLE 53. PROXY – AUTOMATIC SETTINGS (CONT.)

Item	Description
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.
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.

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.

- "Proxy - None (default)" below

- "Proxy - Manual " on page 443

- "Proxy - Automatic" on page 446

Within these selections, you may make settings for:

- "On Demand Rules" on page 449

- "Domains" on page 453

- "Custom Data" on page 455

Proxy - None (default)

Use the following guidelines to configure a Cisco AnyConnect VPN 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.
Connection Type	Select **Cisco AnyConnect (iOS 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 page 443 or "Proxy - Automatic" on page 446.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as:

TABLE 54. PROXY - NONE 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	Select to enable VPN On Demand. The "On Demand Rules" on page 449 field displays. On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location.

TABLE 54. PROXY - NONE 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. For instructions, see "On Demand Rules" on page 449.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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.

TABLE 54. PROXY - NONE SETTINGS (CONT.)

Item	Description
	• Edit an in-house app or an App Store app in the App Catalog.
	ℹ 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS apps.

Proxy - Manual

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

TABLE 55. PROXY - MANUAL SETTINGS

Item	Description
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)	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.

TABLE 55. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	Click **Add+** to add a domain.
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.
	ℹ️ 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:
	$USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $NULL$
	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	Select to enable VPN On Demand.
	The "On Demand Rules" on page 449 field displays.

TABLE 55. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	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. • 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. For instructions, see "On Demand Rules" on page 449.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS apps.

Proxy - Automatic

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

TABLE 56. PROXY - AUTOMATIC SETTINGS

Item	Description
Proxy Server	Enter the name for the proxy 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)	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	If you selected **Username/Password** as the EAP authentication type, enter a value for the username. Required. Include at least one of the following variables:

TABLE 56. 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	Select to enable VPN On Demand. The "On Demand Rules" on page 449 field displays. On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location.

TABLE 56. PROXY - AUTOMATIC 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. For instructions, see "On Demand Rules" on the next page.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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.

TABLE 56. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	• 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS apps.

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

- **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

- **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

- **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

- **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

- **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

   The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

   - **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

   - **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

- **Domain**: The domains for which this evaluation applies.

- **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the **Connect if needed** domain action.*

- **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the **Connect if needed** domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

> ⓘ   You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see .

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 Legacy AnyConnect

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

Use the following guidelines to configure Cisco Legacy AnyConnect VPN.

-

-

-

Within these selections, you may make settings for:

- "On Demand Rules" on page 466

- "Domains" on page 470

- "Custom Data" on page 472 (does not apply to Android devices)

Proxy - None (default)

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

TABLE 57. 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 page 459 or "Proxy - Automatic" on page 463.
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 57. 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. ℹ️ 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	Select to enable VPN On Demand. The "On Demand Rules" on page 466 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:

TABLE 57. PROXY - NONE SETTINGS (CONT.)

Item	Description
	• 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. For instructions, see .
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for iOS devices. The Provider Type field displays. 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.

TABLE 57. PROXY - NONE SETTINGS (CONT.)

Item	Description
	ℹ️ 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 *Ivanti EPMM 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**.

Proxy - Manual

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

TABLE 58. 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.

TABLE 58. 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 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)	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. Select **Add+** to add a domain.
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.

TABLE 58. PROXY – MANUAL SETTINGS (CONT.)

Item	Description
	• **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	Select to enable VPN On Demand. The 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 **58.** P**ROXY -** M**ANUAL SETTINGS** (C**ONT.**)

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. For instructions, see "On Demand Rules" on page 466.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for iOS devices. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS 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**.

Proxy - Automatic

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

TABLE 59. 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)	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. Select **Add+** to add a domain.
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: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$

TABLE 59. 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 $PASSWORD$. 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	Select to enable VPN On Demand. The "On Demand Rules" on page 466 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.

TABLE **59.** P**ROXY** - A**UTOMATIC SETTINGS** (C**ONT.**)

Item	Description
	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. For instructions, see "On Demand Rules" on the next page.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for iOS devices. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS 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**.

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

- **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

- **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

- **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

- **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

- **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

   The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

   - **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

   - **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

- **Domain**: The domains for which this evaluation applies.

- **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the* **Connect if needed** *domain action.*

- **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the* **Connect if needed** *domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

> ℹ️   You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

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 476

- "Proxy - Automatic" on page 479

Within these selections, you may make settings for:

-

-

-

Proxy - None (default)

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

TABLE 60. 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 **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 476 or "Proxy - Automatic" on page 479.
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 60. 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. 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.
VPN On Demand	Select to enable VPN On Demand. The "On Demand Rules" on page 482 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.

TABLE 60. PROXY - NONE SETTINGS (CONT.)

Item	Description
	• 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. For instructions, see "On Demand Rules" on page 482.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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.

TABLE 60. PROXY – NONE SETTINGS (CONT.)

Item	Description
	See the *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS 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 .

Continue to .

Proxy - Manual

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

TABLE 61. 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 **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 479.

TABLE 61. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
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)	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.
	Select **Add+** to add a domain.
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:

TABLE 61. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• 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.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS apps. For instructions, see "On Demand Rules" on page 482.

TABLE 61. PROXY – MANUAL SETTINGS (CONT.)

Item	Description
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 .

Continue to .

Proxy - Automatic

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

TABLE 62. 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 **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 Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.

TABLE 62. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Proxy Domains (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. Select **Add+** to add a domain.
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 62. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
VPN On Demand	Select to enable VPN On Demand. The "On Demand Rules" on the next page 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. • 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	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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 62. PROXY - AUTOMATIC 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS apps. For instructions, see "On Demand Rules" below.
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**.

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

- **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

- **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

- **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

- **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

- **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

- **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

- **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

The following actions are available:

- **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

- **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

- **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

- **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

   The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

   - **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

   - **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

   - **Domain**: The domains for which this evaluation applies.

   - **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the* **Connect if needed** *domain action.*

   - **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the* **Connect if needed** *domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

> ⓘ   You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

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.

Internet Key Exchange version 2 (IKEv2) is the default VPN setting for iOS. The IKEv2 is used to create a security association in the IPSec (Internet Protocol Security) suite. A security association (SA) establishes shared security attributes between two network entities to support secure communication.

Use the following guidelines to configure the IKEv2 VPN connection type.

- "Proxy - None (default)" on page 495
- "Proxy - Manual " on page 497
- "Proxy - Automatic" on page 499

Within these selections, you may make settings for:

- "On Demand Rules" on page 501
- "Domains" on page 506

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.

TABLE 63. IKEV2 SETTINGS (IOS)

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 (iOS Only)**.
Always-on VPN (supervised only)	Select to enable the VPN connection to remain on at all times. More settings display, including Celluar settings and Service Exceptions.

TABLE 63. IKEv2 SETTINGS (IOS) (CONT.)

Item	Description
	This setting applies only to supervised devices.
Allow user to disable automatic connection	Select to allow device users to disconnect automatically triggered connections. This setting applies only to supervised devices.
Use same tunnel configuration for Cellular and Wi-Fi	Select to configure one VPN tunnel for both cellular and wi-fi data. This setting applies only to supervised devices.
Cellular / Wi-Fi (Cellular and Wi-Fi configurations appear separately when you select Always-on VPN.)	
Server	Enter the IP address, hostname, or URL for the VPN server.
Local Identifier	Required. Enter the local identifier of the IKEv2 client in one of the following formats: • FQDN • UserFQDN • Address • ASN1DN
Remote Identifier	Required. Enter the remote identifier in one of the following formats: • FQDN • UserFQDN • Address • ASN1DN
Dead Peer Detection Rate	Optional. Defaults to Medium. Select one of the following: • None (Disable) • Low (keepalive sent every 30 minutes) • Medium (keepalive sent every 10 minutes) • High (keepalive sent every 1 minute)
Use IPv4/IPv6 Internal Subnet Attributes	Optional. If selected, negotiations should use IKEv2 Configuration Attribute INTERNAL_IP4_SUBNET and INTERNAL_IP6_SUBNET. Disabled by default. Available in iOS 9.0 or supported newer versions.

TABLE 63. IKEv2 SETTINGS (IOS) (CONT.)

Item	Description
Disable Mobility and Multihoming	Select to disable mobility and multihoming (MOBIKE). Available in iOS 9.0 or supported newer versions.
Disable redirects	Optional. If selected, disables IKEv2 redirect. If not selected, the IKEv2 connection would be redirected if a redirect request is received from the server. By default, not selected. Available in iOS 9.0 or supported newer versions.
Enable NAT keepalive	Optional. Select to enable Network Address Translation (NAT) Keepalive offload for Always On VPN IKEv2 connections. Keepalive packets are used to maintain NAT mappings for IKEv2 connections. These packets are sent at regular intervals when the device is awake. If selected, Keepalive packets would be sent by the chip even while the device is asleep. The default interval for the Keepalive packets for Always On VPN is 20 seconds over WiFi and 110 seconds over Cellular interface. Available in iOS 9.0 or supported newer versions.
NATKeepAliveInterval	Optional. Controls the interval over which Keepalive packets are sent by the device. The minimum value is 20 seconds. If no key is specified, the default is 20 seconds. Available in iOS 9.0 or supported newer versions.
EnablePFS	Optional. Select to enable Perfect Forward Secrecy for IKEv2 connections. By default, not selected. Available in iOS 9.0 or supported newer versions.
Authentication	
Machine Authentication	Select **None**, **Shared Secret /Group Name**, or **Certificate**. • If selecting **None**, be sure to enable EAP. • If **Certificate** is selected, Server Certificate Issuer Common Name should be added.
Shared Secret	If you select **Shared Secret / Group Name**, enter shared secret to be used for IKE authentication.

TABLE 63. IKEV2 SETTINGS (IOS) (CONT.)

Item	Description
Identity 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.
Server Certificate Issuer Common Name	Optional. Selecting this field will cause IKE to send a certificate request based on this certificate issuer to the server. This field is required if Machine Authentication is set to **Certificate**.
Server Certificate Common Name	Optional. The Common Name of the server certificate. This name is used to validate the certificate sent by the IKE server. If not set, the Remote Identifier will be used to validate the certificate.
Enable EAP	Select to enable extended authentication. If **Machine Authentication** is set to **None**, you must select an EAP authentication method.
IKE SA Params (A Security Association establishes shared security attributes between two network entities to support secure communication.)	
Encryption algorithm	Optional. Select one of the following: • DES • 3DES • AES-128 • AES-256 (Default) • AES-128-GCM • AES-256-GCM • ChaCha20Poly1305
Integrity algorithm	Optional. Select one of the following: • SHA1-96 • SHA1-160 • SHA2-256 (Default) • SHA2-384 • SHA2-512

TABLE 63. IKEv2 SETTINGS (IOS) (CONT.)

Item	Description
Diffie-Hellman Group	Optional. Select one of the following: 1, 2, 5, 14 (Default), 15, 16, 17, 18, 19, 20, 21, 31.
	ℹ If you upgrade from a version of Ivanti EPMM that allowed the value 0 for this field, edit the VPN configuration to use a different Diffie-Hellman Group value. Ivanti EPMM will send the configuration to devices only after you save the change.
Lifetime In Minutes	Optional security association lifetime (re-key interval) in minutes. Valid values are 10 through 1440. Defaults to 1440 minutes.
Child SA Params (A Child SA is any SA that was negotiated via the IKE SA.)	
Encryption algorithm	Optional. Select one of the following: - DES 3DES - AES-128 - AES-256 (Default) - AES-128-GCM - AES-256-GCM - ChaCha20Poly1305
Integrity algorithm	Optional. Select one of the following: - SHA1-96 - SHA1-160 - SHA2-256 (Default) - SHA2-384 - SHA2-512
Diffie-Hellman Group	Optional. Select one of the following: 1, 2, 5, 14 (Default), 15, 16, 17, 18, 19, 20, 21. 31

TABLE 63. IKEv2 SETTINGS (IOS) (CONT.)

Item	Description
	ⓘ If you upgrade from a version of Ivanti EPMM that allowed the value 0 for this field, edit the VPN configuration to use a different Diffie-Hellman Group value. Ivanti EPMM will send the configuration to devices only after you save the change.
Lifetime In Minutes	Optional security association lifetime (rekey interval) in minutes. Valid values are 10 through 1440. Defaults to 1440 minutes.
Wi-Fi see Cellular / Wi-Fi	
Service Exceptions (Configure exceptions to VPN tunnel. This section is only displayed if the **Always-on VPN (supervised only)** option is selected at the top of the window.)	
Voice Mail	Select one of the following options for voicemail: • Allow traffic via tunnel • Allow traffic outside tunnel • Drop traffic
Air Print	Select one of the following options for Air Print: • Allow traffic via tunnel • Allow traffic outside tunnel • Drop traffic
Allow traffic from captive web sheet outside the VPN tunnel	Select to allow traffic from captive web sheets outside the VPN tunnel.
Allow traffic from all captive networking apps outside the VPN tunnel	Select to allow traffic from all captive networking apps outside the VPN tunnel. When selecting this item, skip to the proxy server section.
Captive Networking App Bundle Identifiers	Specify the apps whose traffic you want to allow outside the VPN tunnel. Captive networking apps may require additional entitlements to operate in a captive environment. Select **Add+** to add the bundle ID of a relevant app to the list of apps allowed outside the VPN tunnel.

TABLE 63. IKEV2 SETTINGS (IOS) (CONT.)

Item	Description
	ℹ️ This section is only displayed if the **Allow traffic from all captive networking apps outside the VPN tunnel** option is not selected.

Proxy - None (default)

Use the following guidelines to configure an IPKEv2 (iOS Only) VPN proxy setting type.

TABLE 64. PROXY - NONE (DEFAULT) SETTINGS

Item	Description
Proxy	**None** is the default setting. To configure a **Manual** or **Automatic** proxy, go to Proxy - Manual or Proxy - Automatic.
VPN On Demand	Select to enable VPN On Demand. The "On Demand Rules" on page 501 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.

TABLE 64. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
	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. For instructions, see On Demand Rules.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS apps.

Continue to .

Continue to .

Proxy - Manual

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

TABLE 65. PROXY - MANUAL SETTINGS

Item	Description
Proxy	Select **Manual**. To configure a or **Automatic** proxy, go to <u>Proxy - Automatic</u>.
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)	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. Select **Add+** to add a domain.
VPN On Demand	Select to enable VPN On Demand. The "On Demand Rules" on page 501 field displays.

TABLE 65. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	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. • 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. For instructions, see On Demand Rules.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature.

TABLE 65. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	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.
	ℹ 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS apps.

Proxy - Automatic

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

TABLE 66. PROXY - AUTOMATIC SETTINGS

Item	Description
Proxy	Select **Automatic** proxy. To configure a **Manual** proxy, go to Proxy - Manual.
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.

TABLE 66. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Proxy Domains (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. Select **Add+** to add a domain.
VPN On Demand	Select to enable VPN On Demand. The "On Demand Rules" on the next page 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. • 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.

TABLE 66. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	• For each matching rule you can create up to 50 Type and Value pairs. For instructions, see On Demand Rules.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS apps.

Continue to .

Continue to .

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

- **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

- **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

- **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

- **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

- **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

   The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

   - **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

   - **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

- **Domain**: The domains for which this evaluation applies.

- **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the **Connect if needed** domain action.*

- **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the **Connect if needed** domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

> ℹ️ You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

IPSec (Blue Coat)

This VPN connection type is supported on iOS devices.

This connection type is used with Ivanti EPMM integration with the Blue Coat Mobile Device Security (MDS) service. This connection type is results in an always-on VPN on the device.

Use the following guidelines to configure an IPSec (Blue Coat) VPN.

TABLE 67. IPSEC (BLUE COAT) SETTINGS

Item	Description
Name	Enter brief text that identifies this VPN setting.
Description	Enter additional text that clarifies the purpose of this VPN setting.
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 67. IPSEC (BLUE COAT) SETTINGS (CONT.)

Connection Type	Select **IPsec (Blue Coat)**.
Identity Certificate	Select a Blue Coat certificate enrollment setting from the drop-down list.

IPSec (Cisco)

This VPN connection type is supported on iOS and macOS devices.

Use the following guidelines to configure IPSec (Cisco) VPN.

Within these selections, you may make settings for:

Proxy - None (default)

Use the following guidelines to configure a IPSec (Cisco) VPN without a proxy.

TABLE 68. 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 **IPSec (Cisco)**.
Server	Enter the IP address, hostname, or URL for the VPN server.

TABLE 68. PROXY - NONE SETTINGS (CONT.)

Item	Description
Proxy	**None** is the default setting. To configure a **Manual** or **Automatic** proxy, go to "Proxy - Manual " on page 512 or "Proxy - Automatic" on page 516.
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 authentication method to use: Shared Secret / Group Name or Certificate.
Group Name	Shared Secret / Group Name authentication. Specify the name of the group to use. If Hybrid Authentication is used, the string must end with "[hybrid]".
Shared Secret	Shared Secret / Group Name authentication. The shared secret passcode. This is not the user's password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Shared Secret / Group Name authentication. Re-enter the shared secret to confirm.
Use Hybrid Authentication	Shared Secret / Group Name authentication. Select to specify hybrid authentication, i.e., server provides a certificate and the client provides a pre-shared key.
Prompt for Password	Shared Secret / Group Name authentication. Specify whether the user should be prompted for a password when connecting.

TABLE 68. PROXY - NONE SETTINGS (CONT.)

Item	Description
XAuth Enabled	Specifies that IPsec XAuth authentication is enabled. Select this option if your VPN requires two-factor authentication, resulting in a prompt for the password. This option is enabled by default.
Password	Specify the password to use. 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.
VPN On Demand	Select to enable VPN On Demand. 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. • A matching rule is not required. The Default Rule is applied if a matching rule is not defined.

TABLE 68. PROXY - NONE SETTINGS (CONT.)

Item	Description
	• 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	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS 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 .

Proxy - Manual

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

TABLE 69. PROXY - MANUAL SETTINGS

Item	Description
Proxy	Select **Manual**. To configure a or Automatic proxy, go to "Proxy - Automatic" on page 516.
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)	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 $USERID$. 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.

TABLE 69. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
User Authentication	Select the authentication method to use: Shared Secret / Group Name or Certificate.
Group Name	Shared Secret / Group Name authentication.
	Specify the name of the group to use. If Hybrid Authentication is used, the string must end with "[hybrid]".
Shared Secret	Shared Secret / Group Name authentication.
	The shared secret passcode. This is not the user's password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Shared Secret / Group Name authentication.
	Re-enter the shared secret to confirm.
Use Hybrid Authentication	Shared Secret / Group Name authentication.
	Select to specify hybrid authentication, i.e., server provides a certificate and the client provides a pre-shared key.
Prompt for Password	Shared Secret / Group Name authentication.
	Specify whether the user should be prompted for a password when connecting.
XAuth Enabled	Specifies that IPsec XAuth authentication is enabled. Select this option if your VPN requires two-factor authentication, resulting in a prompt for the password. This option is enabled by default.
Password	Specify the password to use. 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.
VPN On Demand	Select to enable VPN On Demand.
	On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location.

TABLE 69. 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	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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:

TABLE 69. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• add the app in the App Catalog.
	• edit an in-house app or an App Store app in the App Catalog.
	ℹ️ 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS 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 with .

Proxy - Automatic

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

TABLE 70. PROXY - AUTOMATIC SETTINGS

Item	Description
Proxy	Select **Automatic**. To configure a Manual proxy, go to
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)	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.

TABLE 70. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
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 authentication method to use: Shared Secret / Group Name or Certificate.
Group Name	Shared Secret / Group Name authentication. Specify the name of the group to use. If Hybrid Authentication is used, the string must end with "[hybrid]".
Shared Secret	Shared Secret / Group Name authentication. The shared secret passcode. This is not the user's password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Shared Secret / Group Name authentication. Re-enter the shared secret to confirm.
Use Hybrid Authentication	Shared Secret / Group Name authentication. Select to specify hybrid authentication, i.e., server provides a certificate and the client provides a pre-shared key.
Prompt for Password	Shared Secret / Group Name authentication. Specify whether the user should be prompted for a password when connecting.
XAuth Enabled	Specifies that IPsec XAuth authentication is enabled. Select this option if your VPN requires two-factor authentication, resulting in a prompt for the password. This option is enabled by default.

TABLE 70. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Password	Specify the password to use. 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.
VPN On Demand	Select to enable VPN On Demand.
	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.
	• 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.

TABLE 70. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	• 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	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS 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 with .

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

ℹ   You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

Juniper SSL

This VPN connection type is supported on iOS, macOS, Android and Windows devices.

ℹ   Ivanti, Inc 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 525
- "Proxy - Automatic" on page 529

Within these selections, you may make settings for:

- "On Demand Rules" on page 532
- "Domains" on page 537
- "Custom Data" on page 539

Proxy - None (default)

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

TABLE 71. 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 **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 page 525 or "Proxy - Automatic" on page 529.

TABLE 71. PROXY - NONE SETTINGS (CONT.)

Item	Description

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.
	
	ℹ️ 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	Select to enable VPN On Demand. The "On Demand Rules" on page 532 field displays. On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location.

TABLE 71. PROXY - NONE 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. You can enable per-app VPN for an app when you:

TABLE 71. PROXY - NONE SETTINGS (CONT.)

Item	Description
	• 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 *Ivanti EPMM 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**.

Proxy - Manual

Use the following guidelines to configure a Juniper SSL VPN with a manual proxy.

TABLE 72. 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 **Juniper SSL**.

TABLE 72. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
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 529.
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)	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. Select **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: • $USERID$:$EMAIL$

TABLE 72. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• $USERID$_$EMAIL$ 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.
Role	Specify the Juniper user role to use as a restriction.
Realm	Specify the Juniper realm to use as a restriction.
VPN On Demand	Select to enable VPN On Demand. The "On Demand Rules" on page 532 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:

TABLE 72. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• 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. 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.

TABLE 72. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	ℹ️ 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 *Ivanti EPMM 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**.

Proxy - Automatic

Use the following guidelines to configure a Juniper SSL VPN with an automatic proxy.

TABLE 73. 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.

TABLE 73. 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 525.
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)	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. Select **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. ℹ️ 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:

TABLE 73. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	$USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ 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	Select to enable VPN On Demand. The "On Demand Rules" on the next page 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. • 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.

TABLE 73. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	• 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 *Ivanti EPMM 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**.

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

    The following actions are available:

    - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

    - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

    - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

    - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

    - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

- **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

- **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

- **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

- **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

- **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

   The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

   - **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

   - **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

    •   **Domain**: The domains for which this evaluation applies.

    •   **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the **Connect if needed** domain action.*

    •   **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the **Connect if needed** domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

> ℹ You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

•   **Add+** - Click to add a domain.

•   **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

•   **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see .

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)

Use the following guidelines to configure a L2TP VPN without a proxy.

TABLE 74. 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 **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 543.
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.

TABLE 74. Proxy - None settings (Cont.)

Item	Description
	ℹ️ 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 L2TP VPN with a manual proxy.

TABLE 75. 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.

TABLE 75. 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)	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: • $USERID$:$EMAIL$

TABLE 75. PROXY – MANUAL SETTINGS (CONT.)

Item	Description
	• $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ℹ️ 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 76. 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 76. 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 541.
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)	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.

User Authentication	Select the authentication method to use:**Password** or **RSA SecureID**.

TABLE 76. PROXY - AUTOMATIC 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.

Ivanti Tunnel (iOS and macOS)

Use this connection type to configure Ivanti Tunnel VPN for iOS and macOS devices.

Information on how to set up and configure Ivanti Tunnel VPN for Tunnel for iOS and macOS devices, can be found on the Ivanti Product Documentation page in the following Guides:

- *Ivanti Tunnel for iOS Guide*
- *Ivanti Tunnel for macOS Guide*

To download the Guides:

- Click on the link above.
- Scroll down the page to **Ivanti Tunnel** and click on the title.
- Under the appropriate version, select the needed Guide.

The linked item will appear in a new browser window.

NetMotion Mobility VPN (iOS)

This VPN connection type is supported on iOS devices.

Use the following guidelines to configure a NetMotion Mobility VPN.

-
-
-

Within these selections, you may make settings for:

- "Domains" on page 553
- "Custom Data" on page 555

Proxy - None (default)

Use the following guidelines to configure a NetMotion Mobility VPN connection without a proxy.

TABLE 77. 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 **NetMotion Mobility VPN (iOS)**.
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 548 or "Proxy - Automatic" on page 550.
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.

TABLE 77. PROXY - NONE SETTINGS (CONT.)

Item	Description
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.
VPN on Demand	This setting applies to iOS and macOS devices only. Select to enable this VPN connection to be available on demand.
Per-app VPN	Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit apps.

Proxy - Manual

Use the following guidelines to configure a NetMotion Mobility VPN connection with a manual proxy.

TABLE 78. 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 **NetMotion Mobility VPN (iOS)**.
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 550.
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 $PASSWORD$.

TABLE 78. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Proxy Domains (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. • 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.
VPN on Demand	This setting applies to iOS and macOS devices only.

TABLE 78. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	Select to enable this VPN connection to be available on demand.
Per-app VPN	Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit apps.

Proxy - Automatic

Use the following guidelines to configure a NetMotion Mobility VPN connection with an automatic proxy.

TABLE 79. 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.

TABLE 79. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	• User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **NetMotion Mobility VPN (iOS)**.
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 548.
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)	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. ℹ️ 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 79. PROXY – AUTOMATIC 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.
VPN on Demand	This setting applies to iOS and macOS devices only. Select to enable this VPN connection to be available on demand.
Per-app VPN	Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit apps.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

ℹ️   You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

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.

Palo Alto Networks GlobalProtect

This VPN connection type is supported on iOS, macOS, and Android devices.

Use the following guidelines to configure the Palo Alto Networks GlobalProtect VPN connection type.

- "Proxy - None (default)" below

- "Proxy - Manual " on page 558

- "Proxy - Automatic" on page 562

Within these selections, you may make settings for:

- "On Demand Rules" on page 564

- "Domains" on page 569

- "Custom Data" on page 571

Proxy - None (default)

Use the following guidelines to configure a Palo Alto Networks GlobalProtect VPN without a proxy.

TABLE 80. 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 80. 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 **Palo Alto Networks GlobalProtect**.
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 558 or "Proxy - Automatic" on page 562.
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: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$

TABLE 80. PROXY - NONE SETTINGS (CONT.)

Item	Description
	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	Select to enable VPN On Demand.
	The "On Demand Rules" on page 564 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.
	• 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.
	For instructions, see "On Demand Rules" on page 564.
Per-App VPN	

TABLE 80. PROXY - NONE SETTINGS (CONT.)

Item	Description
	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions.
	Select **Yes** to create a per-app VPN setting. An additional license may be required for this setting.
	The Provider Type field displays.
	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.
	ℹ 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 *Ivanti EPMM 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**.

Proxy - Manual

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

TABLE 81. PROXY - MANUAL SETTINGS

Item	Description
Proxy Server	Enter the name for the proxy server.

TABLE 81. 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)	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 $USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $NULL$ 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.

TABLE 81. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	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	Select to enable VPN On Demand. The "On Demand Rules" on page 564 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. • 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.

TABLE 81. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• You can create up to 10 On Demand matching rules. • For each matching rule you can create up to 50 Type and Value pairs. • For instructions, see "On Demand Rules" on page 564.
Per-App VPN	Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this setting. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS 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 with .

Continue with .

Proxy - Automatic

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

TABLE 82. PROXY - AUTOMATIC SETTINGS

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)	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 $USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $NULL$ 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:

TABLE 82. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	$USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ 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	Select to enable VPN On Demand. The "On Demand Rules" on the next page 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. • 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. • For instructions, see "On Demand Rules" on the next page.

TABLE 82. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Per-App VPN	.Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. Select **Yes** to create a per-app VPN setting. An additional license may be required for this setting. The Provider Type field displays. 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit iOS 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**.

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

   - **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

   - **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

   - **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

   - **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

   - **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

   If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

   The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

- **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

- **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

- **Domain**: The domains for which this evaluation applies.

- **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the **Connect if needed** domain action.*

- **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the **Connect if needed** domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

ℹ️   You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

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.

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.

ⓘ   iOS 10 and macOS Sierra iOS 10 and macOS Sierra through the latest version of Ivanti EPMM do not support the PPTP VPN connection type.

- "Proxy - None (default)" below
- "Proxy - Manual" on page 573
- "Proxy - Automatic" on page 575

Proxy - None (default)

Use the following guidelines to configure a PPTP VPN without a proxy.

TABLE 83. 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 83. 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 **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 575
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. ⓘ 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 83. PROXY - NONE (DEFAULT) 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.

Proxy - Manual

Use the following guidelines to configure a PPTP VPN with a manual proxy.

TABLE 84. 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.
Proxy	Select **Manual**. To configure an automatic proxy, go to "Proxy - Automatic" on page 575
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.

TABLE 84. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (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. Select **Add+** to add a domain.
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. ℹ 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 84. 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 password.

Proxy - Automatic

Use the following guidelines to configure a PPTP VPN with an automatic proxy.

TABLE 85. 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.
Proxy	Select **Automatic**. To configure a manual proxy, go to "Proxy - Manual" on page 573.
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)	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. Select **Add+** to add a domain.
Encryption Level	Select **None**, **Automatic** or **Maximum** (128 bit).

TABLE 85. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
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 $EMAIL$:$PASSWORD$ 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, Inc 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 580
- "Proxy - Automatic" on page 584

Within these selections, you may make settings for:

- "On Demand Rules" on page 588
- "Domains" on page 592
- "Custom Data" on page 594

Proxy - None (default)

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

TABLE 86. 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 **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 page 580 or "Proxy - Automatic" on page 584.
Username	Enter a value for the username (required.) The default value is $USERID$. Include at least one of the following variables:

TABLE 86. PROXY - NONE (DEFAULT) 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 $PASSWORD$. 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	Select to enable VPN On Demand. The "On Demand Rules" on page 588 field displays.

TABLE 86. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
	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. • 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. For instructions, see "On Demand Rules" on page 588.
Per-app VPN	Select **Yes** to create a per-app VPN setting. The "On Demand Rules" on page 588 section displays. Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. An additional license may be required for this feature.

TABLE 86. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
	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.
	ℹ 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 *Ivanti EPMM 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**.

Proxy - Manual

Use the following guidelines to configure a Pulse Secure SSL VPN with a manual proxy.

TABLE 87. 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 87. 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 584.
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)	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. Select **Add+** to add a domain.
Username	Enter a value for the username (required.) The default value is $USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$

TABLE 87. PROXY – MANUAL 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.
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	Select to enable VPN On Demand. The "On Demand Rules" on page 588 field displays. On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location.

TABLE 87. 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. For instructions, see "On Demand Rules" on page 588.
Per-app VPN	Select **Yes** to create a per-app VPN setting. The "On Demand Rules" on page 588 section displays. Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. An additional license may be required for this feature.

TABLE 87. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	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 *Ivanti EPMM 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**.

Proxy - Automatic

Use the following guidelines to configure a Pulse Secure SSL VPN with an automatic proxy.

TABLE 88. 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.

TABLE 88. PROXY - AUTOMATIC 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 **Automatic**. To configure a manual proxy, go to "Proxy - Manual" on page 580
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)	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. Select **Add+** to add a domain.
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.

TABLE 88. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	• 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	Select to enable VPN On Demand. The "On Demand Rules" on page 588 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.

TABLE 88. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	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. For instructions, see "On Demand Rules" on the next page.
Per-app VPN	Select **Yes** to create a per-app VPN setting. Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. An additional license may be required for this feature. 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 *Ivanti EPMM 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**).

TABLE 88. PROXY – AUTOMATIC SETTINGS (CONT.)

Item	Description
	Select **app-proxy** (default) or **packet-tunnel**.

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

- **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

- **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

- **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

- **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

- **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

- **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

- **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

- **Domain**: The domains for which this evaluation applies.

- **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the **Connect if needed** domain action.*

- **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the **Connect if needed** domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

> ℹ️   You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

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.

SonicWall Mobile Connect

This VPN connection type is supported on iOS, macOS, and Windows devices.

Use the following guidelines to configure a SonicWall Mobile Connect VPN.

- "Proxy - None (default)" on the next page
- "Proxy - Manual " on page 596
- "Proxy - Automatic" on page 600

Within these selections, you may make settings for:

- "On Demand Rules" on page 603
- "Domains" on page 608

- "Custom Data" on page 610

Proxy - None (default)

Use the following guidelines to configure a SonicWall Mobile VPN connection without a proxy.

TABLE 89. 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 600
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.

TABLE 89. PROXY - NONE SETTINGS (CONT.)

Item	Description
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.

Proxy - Manual

Use the following guidelines to configure a SonicWall Mobile VPN connection with a manual proxy.

TABLE 90. 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 90. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
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 600
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. Select **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: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$

TABLE 90. 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. ℹ️ 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 "On Demand Rules" on page 603 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.

TABLE 90. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• 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. 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.

TABLE 90. PROXY – MANUAL SETTINGS (CONT.)

Item	Description
	See the *Ivanti EPMM 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**.

Proxy - Automatic

Use the following guidelines to configure a SonicWall Mobile VPN connection with an automatic proxy.

TABLE 91. 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 **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 596
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.

TABLE 91. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	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.
	Select **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.
	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.

TABLE 91. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
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 "On Demand Rules" on the next page 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. • 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.

TABLE 91. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	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 *Ivanti EPMM 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**.

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

   The following actions are available:

- **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

- **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

- **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

- **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

- **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

- **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

- **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

- **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

- **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

   If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

   The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

   - **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

   - **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

   - **Domain**: The domains for which this evaluation applies.

   - **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the **Connect if needed** domain action.*

   - **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the **Connect if needed** domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

> ℹ️   You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

Custom Data

- **Add+** - Select 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.

The Custom SSL connection type is for SSL VPN solutions that have a third-party app in the App Store. Use the following guidelines to configure a Custom SSL VPN.

- "Proxy - None (default)" below

- "Proxy - Manual" on page 613

- "Proxy - Automatic" on page 617

Within these selections, you may make settings for:

- "On Demand Rules" on page 620

- "Domains" on page 624

- "Custom Data" on page 626

iOS VPN profiles and password caching

To facilitate iOS deployments, Ivanti EPMM offers the option of caching a user's VPN password. This option is turned off by default. Cached passwords are encrypted, stored on the appliance, and used only for authentication. Note that the password must match the LDAP password in order for this feature to be of use.

Proxy - None (default)

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

TABLE 92. 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 **Custom SSL** (iOS and macOS 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 page 613 or "Proxy - Automatic" on page 617.
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 92. 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.
Identifier	App Store identifier for the VPN app being configured. The app creator should provide this information.
VPN on Demand	This setting applies to iOS and macOS devices only.
	Select to enable VPN On Demand.
	The "On Demand Rules" on page 620 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.
	• 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.

TABLE 92. PROXY - NONE SETTINGS (CONT.)

Item	Description
	• 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 through the most recently released version of iOS 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit apps.

Proxy - Manual

Use the following guidelines to configure a Custom SSL VPN connection with a manual proxy.

TABLE 93. 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 93. 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 **Custom SSL** (iOS and macOS 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 617.
Proxy Server URL	*Automatic Proxy* Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
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)	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. Select **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: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$

TABLE 93. PROXY – MANUAL 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.
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.
Identifier	App Store identifier for the VPN app being configured. The app creator should provide this information.
VPN on Demand	This setting applies to iOS and macOS devices only. Select to enable VPN On Demand. The "On Demand Rules" on page 620 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:

TABLE 93. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• 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 through the most recently released version of iOS 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.

TABLE 93. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	See the *Ivanti EPMM Apps@Work Guide* for information about how to add or edit apps.

Proxy - Automatic

Use the following guidelines to configure a Custom SSL VPN connection with an automatic proxy.

TABLE 94. 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 **Custom SSL** (iOS and macOS 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 613.
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)	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. Select **Add+** to add a domain.

TABLE 94. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
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. ℹ️ 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.
Identifier	App Store identifier for the VPN app being configured. The app creator should provide this information.
VPN on Demand	This setting applies to iOS and macOS devices only. Select to enable VPN On Demand. The "On Demand Rules" on page 620 field displays. On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location.

TABLE 94. PROXY - AUTOMATIC 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 through the most recently released version of iOS 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.

TABLE 94. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	ⓘ 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 *Ivanti EPMM Apps@Work Guide* for information about how to add or edit apps.

On Demand Rules

Applicable to: iOS 7 and later

Whenever a network change is detected, the VPN On Demand service compares the newly connected network against the match network criteria specified in each set of rules (in order) to determine whether VPN On Demand should be allowed or not on the newly-joined network.

Rule sets are checked sequentially, beginning with the first. A rule set matches the current network only if all of the specified policies in that rule set match.

If a rule set matches the current network, a server probe is sent if a URL is specified in the profile. VPN then acts according to the policy defined in the dictionary (for example, Allow, Ignore, Evaluate Connection, Connect, or Disconnect).

Define sets of evaluation rules for each action that can be taken by VPN On Demand: **Allow**, **Connect**, **Disconnect**, **Evaluate Connection**, and **Ignore**. You can define more than one set of rules for each type of action that can be taken. For each set of evaluation rules, the number of rules defined for that set is indicated in the No. of Rules column.

Procedure

1. Select **Add+** to add a new set of On Demand evaluation rules.

   A rule creation dialog box opens.

2. From the **On Demand Action** drop-down list, select the action you want to be taken when the rules you create below are matched.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

   - **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

3. Matching Rules - For each rule you create, enter one of the following types:

- **DNS domain**: This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list. A wildcard '*' prefix is supported. For example, *.example.com matches against either mydomain.example.com or yourdomain.example.com.

- **DNS Server Address**: This rule matches if any of the network's specified DNS servers match any entry in the list. Matching with a single wildcard is supported. For example, 17.* matches any DNS server in the class A 17 subnet.

- **SSID**: A list of SSIDs to match against the current network. If the network is not a Wi-Fi network, or if the SSID does not appear in this list, the match fails. Omit this rule and the corresponding list to match against any SSID.

- **Interface Type**: If specified, this rule matches only if the primary network interface hardware matches the specified interface type. Choose **Ethernet**, **Wifi**, or **Cellular**.

- **URL String Probe**: A URL to probe. If this URL is successfully fetched without redirection (returning a 200 HTTP status code), this rule matches.

4. Enter a value for each rule type and an optional description.

5. After adding your rules, select **OK**.

Default Rules

Define a default rule that simply specifies a default VPN On Demand action in case none of the On Demand rules match, or if no On Demand rules have been defined.

Procedure

1. From the **On Demand Action** drop-down list, select the action you want to be taken by default, if none of the rules match or none are defined.

2. Select Add+ to add a default rule.

   The following actions are available:

   - **Allow**: (Deprecated by iOS.) Allow VPN On Demand to connect if triggered.

   - **Connect**: Unconditionally initiate a VPN connection on the next network attempt.

   - **Disconnect**: Tear down the VPN connection and do not reconnect on demand as long as this dictionary matches.

   - **Evaluate Connection**: Evaluate the action parameters for each connection attempt.

- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as this dictionary matches.

If you select **Evaluate Connection**, a domain actions table displays:

3. Select **Add+** to add a domain action.

   The **Action Parameters** dialog box opens.

4. From the **Domain Action** drop-down list, select one of the following actions to be taken for the domains listed in the table:

   - **Connect if needed**: The specified domains should trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout).

   - **Never connect**: The specified domains should never trigger a VPN connection attempt.

5. Select **Add+** to include any of the following evaluation types:

- **Domain**: The domains for which this evaluation applies.

- **Required DNS Server**: IP addresses of DNS servers to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers should be either internal DNS servers or trusted external DNS servers. *You can only configure required DNS server evaluation types for the* **Connect if needed** *domain action.*

- **Required URL Probe**: An HTTP or HTTPS (preferred) URL to probe, using a GET request. If no HTTP response code is received from the server, a VPN connection is established in response. *You can only configure required URL probe evaluation types for the* **Connect if needed** *domain action.*

6. Add a value and optional description for each entry.

7. Select **OK** to save your domain action parameters.

Domains

Safari Domains

Applicable to: Safari Domains (iOS 7 and later; macOS 10.11 and later)

> ℹ️ You must update your VPN software to a version that supports Per-app VPN.

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Safari Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Once the configuration has been saved, you can edit the Safari Domain information by clicking the Edit icon.

Calendar Domains

Deprecated in iOS 13.4 and later.

Applicable to: Calendar Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Calendar Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Contact Domains

Deprecated in iOS 13.4 and later.

Applicable to: Contact Domains (iOS 13 and earlier; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Contact Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Mail Domains

Deprecated in iOS 13.4 and later.

Applicable to: Mail Domains (iOS 13 and later; macOS 10.15 and later)

If the server ends with one of these domain names, a VPN connection is started automatically.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Associated Domains

Applicable to: Associated Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are associated with the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

Excluded Domains

Applicable to: Excluded Domains (iOS 14.3 and later; macOS 11.0 and later). Applicable to MDM devices only.

Connections to servers within one of these domains are excluded from the per-app VPN.

- **Add+** - Click to add a domain.

- **Mail Domain** - Enter a domain name. Only alphanumeric characters and periods (.) are supported.

- **Description** - Enter a description for the domain.

For more information, see "Managed domains settings" on page 762.

Custom Data

- **Add+** - Select 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.

Managing Certificates and Configuring Certificate Authorities

This section addresses components related to managing certificates and certificate authorities.

Ivanti EPMM supports the use of certificates and certificate-related features for tvOS devices in every instance where iOS devices are supported. Certificates can be used for macOS devices, except in the case of certificates for AppConnect.

Certificates overview

Ivanti EPMM 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.

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

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 Ivanti EPMM as a local certificate authority, an intermediate certificate authority, or as a proxy for a trusted certificate authority.

Types of certificates

Ivanti EPMM uses the following types of certificates:

TABLE 95. CERTIFICATE TYPES

Certificate type	Description
Portal HTTPS	The identify certificate and its certificate chain, including the private key, that identifies Ivanti EPMM, allowing a client (such as a browser or app) to trust Ivanti EPMM. Typically, this certificate is the same certificate as the Client TLS and iOS Enrollment certificates. Ivanti EPMM sends this certificate to the client as part of the TLS handshake over port 443 or 8443 when the client initiates a request to Ivanti EPMM. ℹ️ 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 *Ivanti EPMM System Manager Guide*.
Client TLS	The identify certificate and its certificate chain, including the private key, that identifies Ivanti EPMM, allowing Ivanti Mobile@Work for iOS and Android to trust Ivanti EPMM. Typically, this certificate is the same certificate as the Portal HTTPS and iOS Enrollment certificates. Ivanti EPMM sends this certificate to Ivanti Mobile@Work for iOS or Android as part of the TLS handshake over port 9997 when Ivanti Mobile@Work initiates a request to Ivanti EPMM. **Related topics** "Certificates you configure on the System Manager" in the *Ivanti EPMM System Manager Guide*.
Ivanti EPMM server SSL	Can be either self-signed or third-party certificates. By default, Ivanti EPMM 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.
TLS trust certificate chain for mobile management	Allows iOS mobile devices to trust requests from Ivanti EPMM. Validates profile authenticity for iOS. Enables the MDM feature set for iOS devices. Uses port 2195 to communicate with Apple APNS.

TABLE 95. CERTIFICATE TYPES (CONT.)

Certificate type	Description
(formerly known as the iOS MDM certificate)	
iOS Enrollment	The identify certificate and its certificate chain, including the private key, that identifies Ivanti EPMM.
	Ivanti EPMM uses this identity certificate to sign the Apple MDM configurations that it sends to iOS and macOS devices. Typically, this certificate is the same certificate as the Client TLS and Portal HTTPS certificates.
	Related topics
	• "IKEv2 (iOS Only)" on page 488
	• "Certificates you configure on the System Manager" in the *Ivanti EPMM System Manager Guide.*
Client identity	Verifies the identity of users and devices and can be distributed through Certificate Enrollment.

The following diagram illustrates where each certificate type is used in the Ivanti EPMM architecture:

FIGURE 2. CERTIFICATE TYPES IN THE IVANTI EPMM ARCHITECTURE
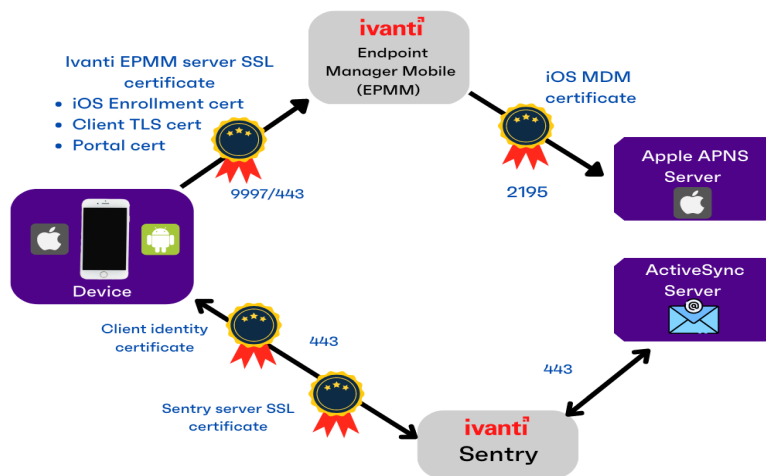
Managing certificates issued by certificate enrollment configurations

Ivanti EPMM 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), Ivanti EPMM 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.

Configuring certificate pinning for registered devices

Implementing TLS server authentication certificate pinning in the client ensures that the application's traffic is protected against rogue "trusted" certificates. These are fake certificates that may have been maliciously installed on the client in an effort to impersonate the Ivanti EPMM server and are commonly referred to as Man-in-the-Middle attacks. Pinning a certificate is one method of preempting this type of attack and ensuring the client connects to the true Ivanti EPMM server.

Pinning occurs when, during the TLS handshake, a client verifies the certificate sent by the server against an authoritative statement residing on the client and containing the certificates the client is expecting from the server. Certificate pinning protects against Man-in-the-middle attacks that compromise confidential data.

Example case study: Man-in-the-middle attacks would allow the attacker to impersonate your Ivanti EPMM server and send commands to the device. This could result in device compromise and confidential data leakage.

Ivanti recommends creating a Certificate Pinning policy so that Ivanti Mobile@Work will only trust legitimate Ivanti EPMM TLS server certificates in the certificate pinning policy. The Certificate Pinning policy works on Ivanti Mobile@Work 11.3.0.1 for Android and supported newer versions. Ivanti Mobile@Work 12.11.31 for iOS and supported newer versions also works with Certificate Pinning.

Implementing this feature is applicable for steady state assurance that the client is connecting to an authentic Ivanti EPMM that presents a TLS server certificate that is under your control.

For daily use cases such as check-in, Ivanti EPMM implements the TLS server authentication certificate pinning policy in Ivanti Mobile@Work . Ivanti Mobile@Work will only trust Ivanti EPMM if it presents one of the pinned certificates in its pinning configuration. Once a device is registered to Ivanti EPMM, Ivanti Mobile@Work will hold the pinned certificates and it will fail if presented with an unexpected certificate.

Steady state pinning must be used in conjunction with the mutual authentication client identity feature. Pinning is only implemented on port 443, not on port 9997. As a result, pinning only has effect when mutual authentication is active and devices are accessing port 443 exclusively. For more information, see "Mutual authentication between devices and Ivanti EPMM" on page 641.

A certificate pinning policy supports multiple entries to enable a smooth transition when the Ivanti EPMM server's certificate is about to expire. Administrators can include the renewal certificate before it is active on the server and keep the expiring certificate in this policy for seamless transition to the renewed certificate.

Procedure

1. In Ivanti EPMM, go to **Policies & Configs > Configurations**.

2. Select **Add New > Certificates**.

   The New Certificate Setting dialog box opens.

3. Enter the Name, Description and upload the certificate file that is referenced to by the Pinned Server Certificate Policy.

4. Select **Save**.

   > ℹ️ Administrators can do the above steps multiple times if the current certificate is about to expire and already have the new one.

5. Go to **Policies & Configs > Policies**.

6. Select **Add New > Pinned Server Certificate Policy**.

   The Add Pinned Server Certificate Policy dialog box opens.

7. Use the information in the Pinned Server Certificate Policy Entries table below to enter your settings.

8. Select **Save**.

TABLE 1. PINNED SERVER CERTIFICATE POLICY ENTRIES

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Trusted Certificates	1. In Trusted Certificates, select the **Add+** button. 2. A new drop-down field displays; **select an option** based on the new certificate you just created. ℹ Administrators can delete unwanted certificates by selecting the **x** in the row.

The new Pinned Server Certificate policy displays in the Policies page.

Related topics

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 *Ivanti EPMM System Manager Guide*.

Supported certificate scenarios

Ivanti EPMM supports the following certificate scenarios:

- "Ivanti EPMM as a certificate authority" on the next page
- "Using Ivanti EPMM as a certificate proxy" on the next page

Ivanti EPMM as a certificate authority

You can configure Ivanti EPMM as a local certificate authority (CA) for the following scenarios:

- Ivanti EPMM as an Independent Root CA (self-signed)—Configure Ivanti EPMM 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 Ivanti EPMM as the certificate authority.
- Ivanti EPMM as an Intermediate CA—Use this option when your company already has its own certificate authority. Using Ivanti EPMM as an Intermediate CA gives your mobile device users the advantage of being able to authenticate to servers within your company intranet.

Using Ivanti EPMM as a certificate proxy

Ivanti EPMM 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 Ivanti EPMM 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
- Ivanti EPMM can manage certificates by checking status against a CA's CRL, deactivating revoked certificates and requesting replacement when certificates are about to expire
- Ivanti EPMM 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.

- ActiveSync is supported with Ivanti Email+ and the iOS native mail client.
- VPN is supported on and on iOS with IPSec, Cisco AnyConnect, and JunOS Pulse.
- Wi-Fi.

The following certificates are supported for iOS devices:

- Microsoft NDES Certificate Enrollment
- Entrust
- Local CA
- User provided certificates
- Open Trust
- Client-Provided certificates
- Client-provided certificates using the native SCEP client on iOS

For information about how to create certificate enrollment settings in Ivanti EPMM, see "Certificate Enrollment settings" on page 656.

Ivanti EPMM as a certificate authority

You can configure Ivanti EPMM as a local certificate authority for the following scenarios:

- **Ivanti EPMM as an Independent Root CA (self-signed)**— Configure Ivanti EPMM 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 Ivanti EPMM as the certificate authority.

  See "Configuring Ivanti EPMM as an independent root CA (Self-Signed)" below.

- **Ivanti EPMM as an Intermediate CA**—Use this option when your company already has its own certificate authority. Using Ivanti EPMM as an Intermediate CA gives your mobile device users the advantage of being able to authenticate to servers within your company intranet.

  See "Configuring Ivanti EPMM as an intermediate CA" on page 640.

Configuring Ivanti EPMM as an independent root CA (Self-Signed)

Configuring Ivanti EPMM as an independent root CA requires configuring your infrastructure to trust Ivanti EPMM as an independent root CA.

To configure Ivanti EPMM 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
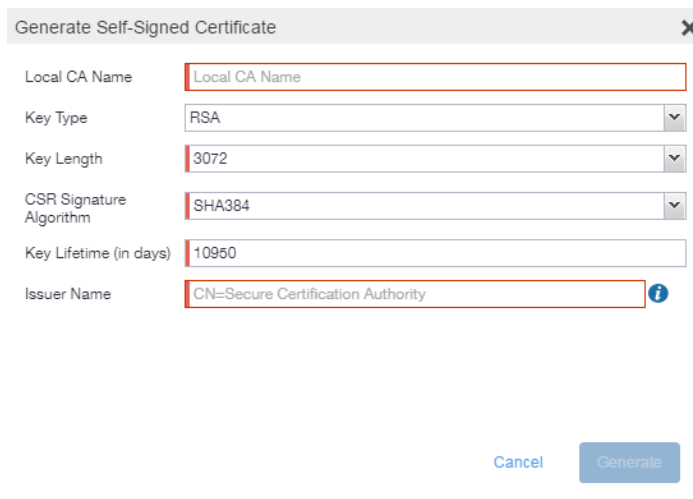
   See "Creating a local certificate enrollment setting" on page 639.

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**.

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. Select **Generate**.

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, Inc 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. Select **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 Ivanti EPMM generates the certificates and caches the generated keys.

1. Log into the Admin Portal.

2. Go to **Policies & Configs > Configurations.**

3. Select **Add New > Certificate Enrollment > Local**.

4. 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.

   - **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.

   - **Local CAs**: Use the drop-down list to select **localCA**.

   - **Key Type**: Specify the key type.

   - **Subject**: Use the drop-down list to select **CN=$EMAIL$**.

   - **Subject Common Name Type**: Select the CN type specified in the certificate template. If you enter the $EMAIL$ variable in the Subject field, select None from the drop-down list.

   - **Microsoft User Security Identifier**: Select the check box to include a non-critical extension with OID 1.3.6.1.4.1.311.25.2 and the value of substitution variable $USER_SID$. If the LDAP user has no SID, the extension will not be included.

   - **Key Usage**: Specify acceptable use of the key by Signing, encryption or Encryption & Signing.

   - **Key Length**: The value is 2048 (by default).

   - **CSR Signature Algorithm**: The value is SHA384 (by default).

5. (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.

6. Click **Save**.

> ℹ️ To ensure continuous connectivity, admins can add secondary CRL URL's for Local CA's and choose the preference of the CRL by using the Prefer Primary CRL URL checkbox.

For more information on configuring the settings, see "Certificate Enrollment settings" on page 656.

Pruning revoked CRL certificates

Revoked certificates can be automatically pruned from an Ivanti EPMM 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. Select the caret to the left of **CA Certificate** to open the section.

4. Select **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 Ivanti EPMM regenerates the list. The default is **168 hours** (7 days).

7. Select **Save**. Expired certificates beyond the revocation date are pruned from the CRL.
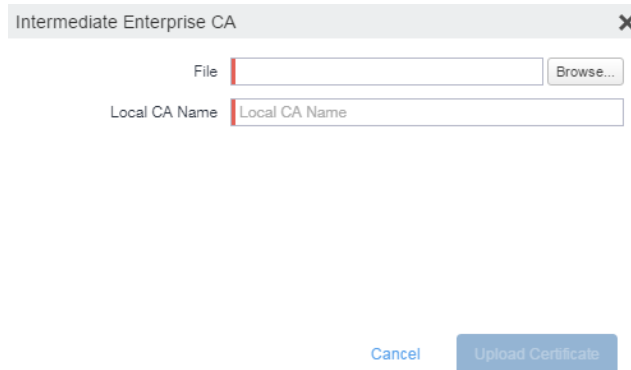
Configuring Ivanti EPMM as an intermediate CA

When you configure Ivanti EPMM as an intermediate certificate authority, the managed device users can authenticate to servers within your company intranet; not just the Ivanti EPMM system.

After you get the certificate from your certificate vendor, you can add the certificates to Ivanti EPMM to create the intermediate certificate authority (CA).

Procedure

1. In the 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 Ivanti EPMM

Ivanti EPMM supports mutual authentication (MA), which means that not only must the device trust Ivanti EPMM, but Ivanti EPMM must trust the device. Therefore, with mutual authentication, a registered device can continue to communicate with Ivanti EPMM only if the device provides the right certificate to Ivanti EPMM. Mutually authenticated communication between the device and Ivanti EPMM enhances security.

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

A device authenticating to Ivanti EPMM with a certificate is also known as certificate-based authentication to Ivanti EPMM.

- "Benefits of mutual certificate authentication" below
- "Scenarios that can use mutual authentication" below
- "Ivanti EPMM port usage with devices, with and without mutual authentication" on the next page
- "The mutual authentication setting on Ivanti EPMM" on page 644
- "Mutual authentication between devices and Ivanti EPMM" on the previous page
- "Mutual authentication identity certificate for Ivanti EPMM" on page 647
- "Mutual authentication client identity certificate" on page 647
- "Supported custom attributes for mutual authentication certificates" on page 648
- "New endpoint for mutual certification authentication" on page 649
- "Mutual authentication between devices and Ivanti EPMM" on the previous page
- "Handling client identity certificate expiration for iOS devices" on page 651
- "Mutual authentication and Apps@Work" on page 651
- "Enabling mutual authentication for Apple and Android devices" on page 652
- "Enabling TLS inspecting proxy support when using mutual authentication" on page 653
- "Enabling mutual authentication for Apple and Android devices" on page 652
- "Enabling mutual authentication for Apple and Android devices" on page 652

Benefits of mutual certificate authentication

Without mutual certificate authentication, only the mobile client verifies Ivanti EPMM's certificate. The client is not required to provide its certificate to the server.

With mandatory mutual certificate authentication, Ivanti EPMM demands that the client also provide its certificate. Ivanti EPMM then verifies the certificate provided by the client.

Mutual certificate authentication improves security as it is not easy for an attacker to produce a certificate to impersonate the client.

Ivanti strongly recommends that you enable mutual authentication.

Scenarios that can use mutual authentication

The device can present a client identity certificate to Ivanti EPMM in the following cases:

TABLE 96. MUTUAL AUTHENTICATION USAGE BY PLATFORM

Platform	Mutual Authentication usage
iOS	• Ivanti 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	• Ivanti Mobile@Work for macOS device check-in • macOS MDM device check-in
Android	• Ivanti 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 Ivanti Mobile@Work registers with Ivanti EPMM, because the device receives its identity certificate during the registration process.

Ivanti EPMM port usage with devices, with and without mutual authentication

The following table summarizes Ivanti EPMM 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 97. IVANTI EPMM PORT USAGE WITH DEVICES WITH AND WITHOUT MUTUAL AUTHENTICATION

	Without mutual authentication	With mutual authentication
Ivanti Mobile@Work for iOS	9997	443
Ivanti Mobile@Work for Android	9997	443
Ivanti Mobile@Work for macOS	Not applicable. Ivanti Mobile@Work for macOS always uses mutual authentication with Ivanti EPMM.	443

TABLE 97. IVANTI EPMM PORT USAGE WITH DEVICES WITH AND WITHOUT MUTUAL AUTHENTICATION (CONT.)

	Without mutual authentication	With mutual authentication
iOS and macOS MDM agent provisioning and agent check-in	443	443
Windows 10	Not applicable. Windows 10 always uses mutual authentication with Ivanti EPMM.	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 Ivanti EPMM

The setting on Ivanti EPMM to enable mutual authentication (MA) 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 98. SETTING FOR MUTUAL AUTHENTICATION ON NEW INSTALLS AND UPGRADES

	Setting to enable mutual authentication
New installations	Enabled by default.
Upgrade from a previous version of Ivanti EPMM in which mutual authentication was **not** enabled.	Not selected. Mutual authentication is **not** enabled.
Upgrade from a previous version of Ivanti EPMM in which mutual authentication **was** enabled.	Selected. Mutual authentication **is** enabled.

IMPORTANT: Once mutual authentication is enabled on Ivanti EPMM, it cannot be disabled.

The mutual authentication setting impacts mutual authentication usage only on:

- Ivanti Mobile@Work for Android and iOS
- iOS MDM
- macOS MDM

The mutual authentication setting has no impact on mutual authentication usage on:

- Versions of Ivanti Mobile@Work for iOS prior to Ivanti Mobile@Work 9.8. These versions of Ivanti Mobile@Work for iOS **never** use mutual authentication.
- Apps@Work for iOS. Apps@Work for iOS **always** uses mutual authentication from Ivanti EPMM 11.3.0.1 and newer versions.
- Ivanti Mobile@Work for macOS. Ivanti Mobile@Work for macOS **always** uses mutual authentication.
- Windows 10 devices. Windows 10 devices **always** uses mutual authentication.

The following table summarizes when devices use mutual authentication and the port they use in communication with Ivanti EPMM.

TABLE 99. IVANTI EPMM MUTUAL AUTHENTICATION (MA) SETTING IMPACT TO DEVICE COMMUNICATION

	Ivanti EPMM upgrade in which: MA setting was NOT enabled before upgrade	Ivanti EPMM upgrade in which MA setting WAS enabled	New Ivanti EPMM installation
Mutual authentication setting	Not enabled	Enabled	Enabled
Device client			
Android: Ivanti Mobile@Work (all Ivanti Mobile@Work versions that Ivanti EPMM supports)	Port: 9997 MA: not used	Devices that register after enabling MA: • Port: 443 • MA: used Devices that were already registered: Once the device has checked in with Ivanti EPMM, the device will transition from non-mutual to mutual authentication. • Before the transition, use port 9997.	Port: 443 MA: used

TABLE 99. IVANTI EPMM MUTUAL AUTHENTICATION (MA) SETTING IMPACT TO DEVICE COMMUNICATION (CONT.)

	Ivanti EPMM upgrade in which: MA setting was NOT enabled before upgrade	Ivanti EPMM upgrade in which MA setting WAS enabled	New Ivanti EPMM installation
		• After the transition, use port 443.	
iOS: Ivanti 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: Once the device has checked in with Ivanti EPMM, the device will transition from non-mutual to mutual authentication. • Before the transition, use port 9997. • After the transition, use port 443.	Port: 443 MA: used
iOS: iOS MDM check-in	Port: 443 MA: not used	Port: 443 MA: used	Port: 443 MA: used.
macOS: Ivanti Mobile@Work	Port: 443 MA: used	Port: 443 MA: used	Port: 443 MA: used
macOS	Port: 443 MA: not used	Port: 443 MA: used	Port: 443 MA: used

TABLE 99. IVANTI EPMM MUTUAL AUTHENTICATION (MA) SETTING IMPACT TO DEVICE COMMUNICATION (CONT.)

	Ivanti EPMM upgrade in which: MA setting was NOT enabled before upgrade	Ivanti EPMM upgrade in which MA setting WAS enabled	New Ivanti EPMM installation
macOS MDM agent check-in			
Windows 10	Port: 443 MA: used	Port: 443 MA: used	Port: 443 MA: used

Disabling Sync TLS port 9997

- **For new installations**: You can directly disable the Sync TLS port.

- **For upgrades**: The client mutual authentication settings page displays the number of pending devices that are due to enable mutual authentication. If all devices are using mutual authentication, you can then disable the Sync TLS port in the System Manager in **Settings > Port Settings > Sync TLS Port**.

Mutual authentication identity certificate for Ivanti EPMM

You provide an identity certificate for Ivanti EPMM 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 Ivanti EPMM, allowing the devices to trust Ivanti EPMM. 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 Ivanti EPMM is generated.

By default, the certificate enrollment setting for mutual authentication is generated with Ivanti EPMM 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 684

Bridging old and new client mutual authentication CA certificates

For Ivanti EPMM systems prior to 11.5.0.0, updating a Certificate Authority (CA) certificate for client mutual authentication required re-registering all devices currently enrolled under that certification. With Ivanti EPMM 11.5.0.0 and supported newer versions, you can:

- Upload and select a new client mutual authentication certificate for devices going forward
- Retire the previous certificate, while still allow existing devices to check in.

Procedure

1. From the Admin portal, navigate to **Settings > System Settings > Security > Certificate Authentication**.

2. From the Client Mutual Certificate Authentication page, select the **Certificate Enrollment Setting** where the updated certificate will be in effect.

3. Click **Upload CA Chain** and follow the prompts. Once uploaded, the new CA will be in effect for new installations, while the older CA is still accessible to devices with older installations. You can see these older CA certificates in the **Previously Trusted Certificates Enrollment Settings** table, below the **Upload** button.

Related topics

See "Mutual authentication between devices and Ivanti EPMM" on page 641 and "Handling client identity certificate expiration for iOS devices" on page 651

Supported custom attributes for mutual authentication certificates

From Ivanti EPMM release 10.8.0.0 through the latest release supported by Ivanti, Inc, Ivanti EPMM 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, Ivanti EPMM 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 Ivanti EPMM 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.

Below is an example scenario of the old OAuth versus the new endpoint:

TABLE 100. 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 Ivanti Mobile@Work clients (both iOS and Android) and on the watchOS app, however, it will mean less security. Ivanti, Inc 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 Ivanti Mobile@Work for iOS, OR an old or updated Ivanti 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.

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 101. 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.
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	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 iOS devices

Ivanti Mobile@Work for iOS handles the expiration of the client identity certificate used for mutual authentication between Ivanti Mobile@Work for iOS and Ivanti EPMM. 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 Ivanti Mobile@Work determines the renewal window has begun, it requests a new certificate from Ivanti EPMM.

- If Ivanti Mobile@Work is out of contact with Ivanti EPMM during the renewal window, but is in contact again within 30 days after the expiration, Ivanti Mobile@Work requests a new certificate from Ivanti EPMM.

- If Ivanti Mobile@Work is not in contact with Ivanti EPMM either during the renewal window or within 30 days after the expiration, the device will be retired and will need to re-register with Ivanti EPMM.

- Ivanti Mobile@Work versions prior to 11.1.0 do not support certificate expiration. When the certificate expires, the device user must re-register Ivanti 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 270. A blank value defaults to 270 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 by default. It does *not* depend on the mutual authentication setting at **Settings > System Settings > Security > Certificate Authentication.**

Related topics

- "Setting up Apps@Work for iOS and macOS" in the *Ivanti EPMM Apps@Work Guide*
- "Apps@Work in Ivanti Mobile@Work for Android in the *Ivanti EPMM Apps@Work Guide*

Enabling mutual authentication for Apple and Android devices

The Ivanti EPMM mutual authentication setting enables mutual authentication for:

- Ivanti Mobile@Work for Android
- Ivanti Mobile@Work for iOS.
- iOS MDM
- macOS MDM

Mutual authentication is automatically enabled in the cases described in "The mutual authentication setting on Ivanti EPMM" on page 644.

> **i** **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 647, 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 Ivanti EPMM**

   For details, see "Certificate Enrollment settings" on page 656.

   > **i** 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 Ivanti EPMM. Those devices will need to re-register with Ivanti EPMM. 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, Inc recommends port 7443. However, you can use any port except 443 or 8443 which are reserved for other EPMM services.

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 *Ivanti EPMM Apps@Work Guide*
- "Port settings" in the *Ivanti EPMM System Manager Guide*
- "Apps@Work for Android authentication to Ivanti EPMM" in the *Ivanti EPMM Apps@Work Guide*

Enabling TLS inspecting proxy support when using mutual authentication

Contact Ivanti, Inc Professional Services or an Ivanti, Inc certified partner to set up this deployment.

Ivanti EPMM can support a TLS inspecting proxy to handle HTTPS requests from your devices to Ivanti EPMM 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 Ivanti EPMM, it re-encrypts and forwards the traffic to Ivanti EPMM. The devices that register to Ivanti EPMM (using port 443) must send HTTPS requests to the TFE rather than to Ivanti EPMM. 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 *Ivanti EPMM System Manager Guide*

Migrating Ivanti Mobile@Work for Android and iOS to use mutual authentication

For devices that register after enabling mutual authentication, Ivanti Mobile@Work uses port 443 for device check-ins. However, devices that were already registered continue to use port 9997. Ivanti facilitates the ability to migrate Ivanti M@W from using port 9997 without mutual authentication to using port 443 with mutual authentication. The device users do not need to re-register with Ivanti EPMM.

Before you begin

Instruct Android and iOS device users to upgrade to Ivanti Mobile@Work 10.1 for Android or or Ivanti Mobile@Work 12.11.10 for iOS or supported newer versions. Prior Ivanti 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, make sure that **Migrate Mobile@Work Client** is enabled.

4. Click **Save**.

5. Click **OK**.

On the next device check-in, Ivanti EPMM 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 Ivanti EPMM 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

"Mutual authentication between devices and Ivanti EPMM" on page 641

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 Ivanti EPMM, use the certificate enrollment setting called single file identity.

You configure Ivanti EPMM 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 Ivanti EPMM setting, and apply the appropriate labels to the referencing setting. Only the following settings can reference a certificate setting:

  - An AppConnect app configuration, Ivanti Web@Work setting, or Ivanti 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.

When upgrading from an Ivanti EPMM prior to Ivanti EPMM 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 an Ivanti EPMM prior to Ivanti EPMM 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 Ivanti EPMM. 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

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 Ivanti EPMM 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 Ivanti EPMM user portal to upload their identity certificates to Ivanti EPMM.

- To specify that AppConnect apps on devices use derived credentials.

The available options are:

- **Blue Coat**: Use to create a Blue Coat certificate enrollment setting for integrating with the Blue Coat Mobile Device Security service.

- **Client-Provided**: Use if you want AppConnect apps to use derived credentials for authentication, digital signing, or encryption.

- **Entrust**: Use if you are using the Entrust Datacard certificate enrollment solution.

- **GlobalSign**: Use if you are using GlobalSign as the CA for certificate enrollment.

- **Local**: Use if you are using Ivanti EPMM as the CA.

- **OpenTrust**: Use if you are using the OpenTrust integration. See "Configuring OpenTrust CA" on page 679.

- **Single File Identity**: Use to upload an identity certificate for distribution to devices.

- **SCEP**: Use for standard certificate-based authentication using a separate CA.

  > ℹ️ SCEP Configurations created before upgrading to Ivanti EPMM 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 Ivanti EPMM 9.4.0.0.

- **Symantec Managed PKI**: Use if you are using Symantec's Certificate Enrollment solution. See "Configuring Symantec Managed PKI" on page 691 for more information.

- **Symantec Web Services Managed PKI**: Use if you are using the Symantec Web Services Managed PKI solution. See "Configuring Symantec Web Services Managed PKI " on page 694for more information.

- **User-Provided**: Use 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 Ivanti EPMM as an intermediate or root CA. See "Certificate Enrollment settings" on the previous page 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):

- $EMAIL$
- $USERID$
- $FIRST_NAME$
- $LAST_NAME$
- $DISPLAY_NAME$
- $USER_DN$

- $USER_SID$
- $USER_UPN$
- $USER_LOCALE$
- $DEVICE_UUID$
- $DEVICE_UUID_NO_DASHES$
- $DEVICE_UDID$
- $DEVICE_IMSI$
- $DEVICE_IMEI$
- $DEVICE_SN$
- $DEVICE_ID$
- $DEVICE_MAC$
- $DEVICE_CLIENT_ID$
- $USER_CUSTOM1$
- $USER_CUSTOM2$
- $USER_CUSTOM3$
- $USER_CUSTOM4$
- $REALM$
- $TIMESTAMP_MS$
- $RANDOM_16$
- $RANDOM_32$
- $RANDOM_64$
- $CONFIG_UUID$*

* 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).

Monitoring modifications to certificate enrollment settings

When administrators modify a certificate enrollment (CE) setting, they cause changes to configurations that use that CE setting. The modification history field identifies the administrator who made the CE setting change as the administrator who caused the configuration changes.

Certificate generation time

Certificate enrollment settings can be referenced from other settings on Ivanti EPMM that require an identity certificate. Some settings that can reference certificate enrollment settings are Exchange settings, Email settings, Wi-Fi settings, VPN settings, AppConnect app configuration settings, Ivanti Docs@Work settings, and Ivanti Web@Work settings.

Most certificate enrollment settings cause an identity certificate to be generated. The identity certificate is generated at one of these times:

- "Early generation" below

- "On-demand generation" on the next page

> Some certificate enrollment settings do not cause an identity certificate to be generated. Specifically, for user-provided certificate enrollment settings and single file identity certificate enrollment settings, the certificate is available on Ivanti EPMM. For client-provided certificate enrollment settings, the certificate is available in Ivanti Mobile@Work.

Early generation

Early generation occurs when you apply a label to a setting that references the certificate enrollment setting. Ivanti EPMM generates identity certificates at this time for:

- AppConnect app configurations

- Ivanti Docs@Work settings

- Ivanti Web@Work settings

For each device that has the same label as the setting, Ivanti EPMM does the following:

- For devices running Ivanti Mobile@Work 9.1.0.0 for iOS or earlier, Ivanti EPMM generates an identity certificate for the device for *each* setting that references the certificate enrollment setting.

- For devices running Ivanti Mobile@Work 9.5.0.0 for iOS, Ivanti EPMM generates *exactly one* identity certificate for the device regardless how many settings reference the certificate enrollment setting

> After Ivanti EPMM generates an identity certificate, if Ivanti EPMM does not send the certificate to a device within 14 days, Ivanti EPMM deletes the certificate from its file system. The certificate will be generated on-demand.

On-demand generation

On-demand generation occurs when Ivanti EPMM sends a setting that references the certificate enrollment setting to the device. On-demand generation occurs for all settings (that reference a certificate enrollment setting) that are not listed in the early generation list above. A setting, including the certificate, is delivered to a device when the device checks in with Ivanti EPMM.

Certificate delivery time for AppConnect-related certificates

This feature is not supported on macOS devices.

When an AppConnect-related setting (AppConnect app configuration, Ivanti Web@Work setting, or Ivanti Docs@Work setting) specifies a certificate enrollment setting, the time that Ivanti EPMM *delivers* the identity certificate to the device depends on the Ivanti Mobile@Work version on the device.

> Certificate delivery from Ivanti EPMM to the device is not applicable in these cases:
> - The certificate enrollment setting specifies decentralized mode.
> - The certificate enrollment setting type is client-provided.

Certificate delivery for Ivanti Mobile@Work 9.1 for iOS and earlier versions

Ivanti EPMM delivers the identity certificate to the device when the AppConnect-related setting is delivered to the device. An AppConnect-related setting is delivered to the device when Ivanti Mobile@Work does an app check-in with Ivanti EPMM and either:

- The AppConnect app launched for the first time.

- The AppConnect-related setting changed.

> These versions of Ivanti Mobile@Work do not store the certificates.

Certificate delivery for Ivanti Mobile@Work 9.5.0.0 for iOS

Ivanti EPMM delivers an identity certificate to Ivanti Mobile@Work on the device when the *first* AppConnect app that uses the certificate launches. Ivanti Mobile@Work stores the identity certificate. *Subsequent* AppConnect apps which use the same certificate receive the certificate from Ivanti Mobile@Work without any involvement from Ivanti EPMM.

When an AppConnect app launches, control switches to Ivanti Mobile@Work so that Ivanti Mobile@Work can check in with Ivanti EPMM to receive the AppConnect-related configurations and identity certificates for the app. The time it takes to switch control back to the app is longer when the app needs many identity certificates and it is the first AppConnect app that needs those certificates.

Note the following:

- Ivanti Mobile@Work stores the certificates securely on the device, encrypting them the same way it encrypts AppConnect-related data such as AppConnect app configurations. Ivanti Mobile@Work displays general information about each stored certificate, such as its expiration date.

- When a device user upgrades Ivanti Mobile@Work from version 9.1 or earlier, existing AppConnect apps that already have their certificates continue to use those certificates. Such apps receive replacement certificates from Ivanti Mobile@Work only when their AppConnect-related setting changes on Ivanti EPMM.

- The delivery strategy has no impact on AppConnect apps themselves. The apps do not need to be rebuilt or rewrapped.

Related topics

- "[Viewing certificates stored in Ivanti Mobile@Work](#)" in *AppConnect Guide for EPMM*.

Performance impact

When a device uses Ivanti Mobile@Work 9.5 for iOS, the generation and delivery strategy of certificates to a device improves performance on Ivanti EPMM and on the device.

The Ivanti EPMM performance improvements are:

- When multiple AppConnect apps' AppConnect-related settings use the same certificate enrollment setting, Ivanti EPMM generates and delivers the certificate to the device only once.

- With prior versions of Ivanti Mobile@Work, Ivanti EPMM generates and delivers a separate certificate for each AppConnect app.

- When you modify an AppConnect-related setting field that does not involve the certificate:

  - Ivanti EPMM does not regenerate the certificate.

  - With prior versions of Ivanti Mobile@Work, Ivanti EPMM regenerated the certificate unless you had selected **Store keys on Ivanti EPMM** on the certificate enrollment setting.

  - Ivanti EPMM does not re-deliver the certificate to the device.

  - With prior versions of Ivanti Mobile@Work, Ivanti EPMM redelivered the certificate.

These improvements are especially significant when Ivanti EPMM has many registered devices, each with many AppConnect apps.

The device user experiences improved launch time when launching an AppConnect app other than the first AppConnect app. The improvement is because:

- The app does not have to wait for Ivanti EPMM to deliver the certificate.

- The app does not have to wait for Ivanti EPMM to generate the certificate when non-certificate fields have changed.

Related topics

"Certificate generation time" on page 659

Configuring ACME Certificates

Managed Device Attestation ensures that only legitimate devices can connect to your servers. If attestation is enabled, your device can request a client certificate from an Automated Certificate Management Environment (ACME) server.

The device generates an asymmetric key pair based on the `KeyType`, `KeySize`, and `HardwareBound` fields. If attest is true, the device requests an attestation of the key and device properties. The ACME server authenticates the device, provide the attestation, and requests a matching certificate based on the `ClientIdentifier`, `Subject`, `SubjectAltName`, `KeyUsage`, and `ExtendedKeyUsage` fields. When the ACME server issues a certificate, the device installs it in the keychain. Other payloads can use `PayloadUUID` to reference the resulting client identity.

To request a client certificate from an ACME server, navigate to **Configurations > Add New > Certificate Enrollment > ACME > New ACME configuration**. The new configuration is found in the Certificate Enrollment.

FIGURE 1. NEW ACME CONFIGURATION

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 Ivanti 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 Ivanti 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.

- Ivanti 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

- Ivanti 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 Ivanti 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: Ivanti Mobile@Work prior to 8.5	iOS: Ivanti Mobile@Work 8.5 and 8.6	iOS: Ivanti Mobile@Work 9.0 or supported newer versions	Android: All versions of Secure Apps Manager supported or compatible with Ivanti EPMM
In key-value pairs	Not supported	Supported	Supported	Supported
In AppTunnel rules	Not supported	Not supported	Supported	Not supported

Related topics

- *Ivanti Derived Credentials Guide for EPMM*

- *PIV-D Manager for iOS Release Notes*

- *PIV-D Manager 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: • **Authentication** • **Decryption** • **Encryption** • **Signing**
Provider	Select the derived credential provider.

4. Click **Save**.

Configuring Blue Coat Mobile Device Security service integration

Ivanti EPMM supports integration with the Blue Coat Mobile Device Security (MDS) service. This integration allows you to manage your iOS devices' traffic to the Internet, by directing all the traffic to the Blue Coat MDS service first. The service can then, for example, stop access to specific web sites based on corporate security rules that you set up on a Blue Coat site. The Blue Coat MDS service also provides traffic analytics. This integration is supported only with iOS devices.

Overview of how to set up Ivanti EPMM integration with the Blue Coat MDS service

To set up Ivanti EPMM to integrate with Blue Coat MDS, do the following high-level steps:

1. Work with Blue Coat to set up Ivanti EPMM as your Unified Endpoint Management (UEM) vendor on the Blue Coat MDS service.

2. Get a Blue Coat customer ID from Blue Coat.

3. Get the certificate that Ivanti EPMM uses to authenticate to the Blue Coat MDS service so that Ivanti EPMM can interact with the service. An example of such an interaction is when Ivanti EPMM informs the MDS service about what iOS devices are registered.

4. Set up a Blue Coat certificate enrollment setting.

5. This setting contains the information necessary for Ivanti EPMM to request the Blue Coat MDS service for an identity certificate for a device. This certificate authenticates the device to the Blue Coat MDS service when the device's traffic is directed to the MDS service.

6. For details, see "Configuring the Blue Coat certificate enrollment setting" below.

7. Set up a IPsec (Blue Coat) VPN setting on Ivanti EPMM.

8. This always-on VPN is how all device traffic is always directed first to the Blue Coat MDS service.

9. For details, see "Configuring the IPsec (Blue Coat) VPN setting" on page 669.

Limitations when integrating with the Blue Coat MDS service

Because all device traffic is directed to the Blue Coat MDS service using an always-on VPN:

- You **cannot** use any other VPNs on the device.

- You **cannot** use Tunnel (AppTunnel with TCP tunneling) on the device because it uses a VPN.

ⓘ Using AppTunnel with HTTP/S tunneling with AppConnect apps on the device is compatible with using the Blue Coat MDS service.

Configuring the Blue Coat certificate enrollment setting

Before you begin:

- Set up Ivanti EPMM as your Unified Endpoint Management (UEM) vendor on the Blue Coat MDS service.

- Get your Blue Coat customer ID.

- Get the certificate and certificate password that Ivanti EPMM uses to authenticate to the Blue Coat MDS service.

Procedure

1. Go to **Policies & Configs > Configurations** and select **Add New > Certificate Enrollment > Blue Coat**.

2. In the New Blue Coat Certificate Enrollment Setting dialog box, use the following guidelines to specify the 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.
Store keys on Ivanti EPMM	Specifies whether Ivanti EPMM stores the private key sent to each device. When storing keys is enabled, private keys are encrypted and stored on the local Ivanti EPMM. If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.
Blue Coat Customer ID / MDM Identifier	Specifies your Blue Coat customer ID. The customer ID is also known to Blue Coat as the MDM Identifier.
API URL	Specifies the URL that Ivanti EPMM uses to interact with the Blue Coat MDS service. This field is set to: `https://mobility.threatpulse.com:9443` Typically, you do not change this field unless you are working with Blue Coat in a special test environment.
Certificate 1	Upload the certificate that Ivanti EPMM uses to authenticate to the Blue Coat MDS service. This certificate is available from Ivanti.
Password 1 (Optional)	Enter the password for the certificate. This password is available from Ivanti. ⓘ Although you can select **Add Certificate** to add additional certificates and their corresponding passwords, no reason currently exists to do so.
Device Name	Optionally enter an Ivanti EPMM substitution variable that identifies the device. This device name is used by the Blue Coat MDS service.

	The device name allows you to differentiate multiple devices belonging to one use on Blue Coat MDS reports.
User ID	Enter the email address for the user. Blue Coat requires that the User ID is the user's email address.
	Typically, you use the Ivanti EPMM substitution variable $EMAIL$.

3. (Optional) Select **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. The **Issue Test Certificate** dialog box opens.

> ℹ️ Although this step is optional, it is recommended. A real certificate is not generated.

4. Enter a user's email address that Blue Coat can validate.

5. Select **OK**.

6. Select **Save**.

> ℹ️ 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.**

Configuring the IPsec (Blue Coat) VPN setting

Before you begin: Configure the Blue Coat certificate enrollment setting.

Procedure

1. Go to **Policies & Configs > Configurations** and select **Add New > VPN**.

2. Use the following guidelines to specify the settings.

Item	Description
Name	Enter brief text that identifies this VPN setting.
Description	Enter additional text that clarifies the purpose of this VPN setting.
Connection Type	Select **IPsec (Blue Coat)**.
Identity Certificate	Select a Blue Coat certificate enrollment setting from the drop-down list.

3. Select **Save**.

4. Select the VPN setting that you just created.

5. Select **Actions > Apply To Label**.

6. Select the appropriate labels.

7. Select **Apply**.

Revoking the certificate

You can revoke a Blue Coat certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the Blue Coat service. When a device authenticates with Ivanti EPMM, 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. Select **Actions > Revoke**.

Configuring an Entrust CA

Ivanti EPMM supports integration with the Entrust Administration Services (EAS). This integration allows Ivanti EPMM to work with Entrust to obtain certificates directly from the CA. This type of interaction is called centralized mode. Alternatively, Ivanti EPMM can work with Entrust to enable mobile devices with native SCEP clients to obtain certificates from the Entrust CA. This interaction is called decentralized mode.

Entrust Prerequisites

The information in this section assumes the following:

- You have the URL for your Entrust server (received from Entrust).

- You have the Administrator ID and password.

Entrust decentralized mode

Entrust decentralized mode allows iOS devices to communicate directly with Entrust by embedding the SCEP challenge string in the MDM configuration. Managed devices generate PKI key pairs and CSRs, obtaining certificates directly from Entrust CA without going through Ivanti EPMM as a proxy. In this way, using decentralized mode improves security in that the private key never leaves the device.

When implementing decentralized mode, confirm the managed device:

- has a native SCEP client

- can work with the encryption algorithm and key lengths supported by Entrust

- accepts the CSR signature algorithm used by Entrust, if the selected algorithm is overridden

The mobile device will notify the device user when the Entrust certificate has been installed successfully. Additionally, the device reports the retrieved certificate to Ivanti EPMM as part of the standard device certificate inventory report. You can view the certificate data by going to **Devices & Users > Devices**, clicking the carat (^) symbol next to the device, and clicking the **Logs** tab. You can also view the certificate by going to **Logs > Certificate Management**, and clicking the **View** link under the Content column next to the relevant device.

Note the following:

- Currently, iOS only supports the RSA key type with key lengths of 1024 and 2048.

- If you configure multiple app settings (such as email, VPN, and Wi-Fi) to consume the same decentralized Entrust certificate enrollment setting, and apply a label to the app settings all at once, then Entrust fails to return the certificate to the devices with that label. Instead, configure each certificate enrollment consumer to reference different Entrust certificate enrollment settings, which themselves reference different certificate profiles.

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 credentials to log into the Entrust server.

- **Admin Password**: Enter the administrator password.

- **Group**: The Entrust group associated with users. Custom attribute variable substitutions are supported.

  > ℹ️ 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.

  > ℹ️ 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.

  If using decentralized mode, select a profile that supports decentralized mode.

- **Profile Description**: Pre-populated based on the profile you select.

- **Application Description**: Pre-populated based on the profile you select.

- **Centralized**: Select to allow Ivanti EPMM 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 Ivanti EPMM**: Specifies whether Ivanti EPMM stores the private key sent to each device. When storing keys is enabled, private keys are encrypted and stored on the local Ivanti EPMM.

  - If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.

  - This option is disabled when selecting **Decentralized** mode.

- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

  This option is disabled when selecting **Decentralized** mode.

- **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 656 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**.

> ℹ️ 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 Ivanti EPMM, 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

Ivanti EPMM 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 Ivanti EPMM, 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 Ivanti EPMM 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 Ivanti EPMM**: Specifies whether Ivanti EPMM stores the private key sent to each device. When storing keys is enabled, private keys are encrypted and stored on the local Ivanti EPMM.

  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 Ivanti EPMM 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 657 for more information.)

- **Microsoft User Security Identifier**: Select the check box to include a non-critical extension with OID 1.3.6.1.4.1.311.25.2 and the value of substitution variable $USER_SID$. If the LDAP user has no SID, the extension will not be included.

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**.

ℹ️ 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 Ivanti EPMM, 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 Ivanti EPMM as the CA

This section describes how to configure Ivanti EPMM 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 Ivanti EPMM**: Specifies whether Ivanti EPMM stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Ivanti EPMM.

     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 657 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 657 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**.

> ℹ️ 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 Ivanti EPMM, 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

Ivanti EPMM supports integration with the OpenTrust Mobile Provisioning Server (MPS). This integration enables OpenTrust to perform the proxy tasks that would normally be performed by Ivanti EPMM. The following describes the configuration in Ivanti EPMM.

Note the following:

- This integration does not support the pushing Certificate Authorities Bundles to devices, which is offered by OpenTrust.

- Ivanti EPMM 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 Ivanti EPMM 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 Ivanti EPMM**: Specifies whether Ivanti EPMM stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Ivanti EPMM.

- 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 Ivanti EPMM 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.

- **MSSID**: You must use the profile for which Microsoft Security Identifier support has been added by OpenTrust. Use $USER_SID$ value from the drop-down list to generate a certificate with the SID extension, provided the LDAP user has the SID value.

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**.

ℹ️ 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 Ivanti EPMM, 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**.

Certificate Revocation Checking Configuration

This configuration allows the administrators to check an array of certificates revoked from a device. Administrators can specify a certificate authority (CA) that allows the configuration to enable revocation checking for all the certificates that are linked to the specified CA.

Applicable to: iOS 14.2+

Procedure

1. Go to **Policies & Configurations** > **Configurations**.

2. Click **Add New** > **Apple** > **iOS / tvOS** > **Certificate Revocation**.

   The New Certificate Revocation Setting dialog box opens.

3. Enter a **Name** and **Description** of the configuration.

4. Click the **Add+** button.

5. Select the **Hash Algorithm** (SHA 256 is the default) and enter the **Hash** of the root certificate.

   > ⓘ In Hash, you have to enter a Base64 encoded (binary) SHA-256 hash of the certificate's
   > public key. See Apple documentation for the available trusted root certificates for Apple
   > operating systems. You can add multiple root certificates in this configuration.

6. Click **Save**.

Configuring a single file identity certificate enrollment setting

Use a single file identity certificate enrollment setting to upload an identity certificate to Ivanti EPMM 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:

  o The private key and its password.

  o The public certificate.

  o 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:

  o A .p12 or .pfx file containing a an identity certificate and its private key and password, plus additional .pem files containing the intermediate certificates.

  o 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 Ivanti EPMM. 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 *Ivanti EPMM 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**: Ivanti EPMM retrieves certificates on behalf of devices. Ivanti EPMM also manages the certificate lifetime and triggers renewals. See .

     > ⓘ   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 652.

- **Store keys on Ivanti EPMM**:

  Specifies whether Ivanti EPMM stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Ivanti EPMM.

  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 Ivanti EPMM**:

  This feature is not available for iOS devices.

  This feature is not available for MAC devices.

  When this option is enabled, Ivanti EPMM 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=ivanti,OU=InfoTech or

  CN=www.ivanti.com.

  You can also customize the Subject by appending a variable to the OID. For example, CN=www.ivanti.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.

- **Microsoft User Security Identifier**: Select the check box to include a non-critical extension with OID 1.3.6.1.4.1.311.25.2 and the value of substitution variable $USER_SID$. If the LDAP user has no SID, the extension will not be included. Using this option may not have any impact on decentralized requests for some OS platforms. Refer to the below 'Subject Alternative Name Value' section as an alternative.

- **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, Uniform Resource Identifier 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 the certificate request does not support the extension to use "Microsoft User Security Identifier", such as a decentralized request from an Apple device, instead you can use a SAN URL with **tag:microsoft.com,2022-09-14:sid:$USER_SID$**, provided the LDAP user has the SID value.

  > 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 102. 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
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

> ℹ️ 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.

- Ivanti EPMM can detect and address revoked and expired certificates.

Uploading a Certificate Authority chain for SCEP enrollment configurations

With Ivanti EPMM 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 684. If you do not upload a CA chain, Ivanti EPMM 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 Ivanti EPMM.

- Client mutual authentication must be enabled to use this feature. See "Mutual authentication client identity certificate" on page 647.

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**.

Enabling Kerberos Authentication between EPMM and the SCEP and LDAP servers

You can use Kerberos authentication to communicate between Ivanti EPMM and the SCEP and LDAP servers. The following sections discuss how to enable Kerberos authentication on servers and Ivanti EPMM.

Pre-configuration steps

1. In the Active Directory server, check that a service account is available.

2. In the SCEP Server, check that the service account is a member of the local `IIS_USRS` group.

3. In the CA server certificate template that is being provisioned, check that the service account has `enroll` permission.

4. In the CA server certificate template that is being provisioned, check that the service account has enroll permission.

Configuring Windows servers

1. Run the following command on a domain controller:

   ```
   setspn -s http/<SCEP-SERVER-FQDN> <domain>\<service account>
   ```

2. In **Active Directory Users and Computers** click the **Delegation** tab of the service account:

   a. Under **Trust this user for delegation to specified services only**, select **Use Kerberos Only**.

   b. Click **Add** and add the SCEP server name.

   c. Select the http service.

   d. Click **OK**.

3. Do the following in the IIS server to make sure that Application Pool credentials are used to decrypt Kerberos tickets:

   a. Check that the SCEP Application Pool is running under the service account.

   b. Disable Kernel mode and enable `useAppPoolCredentials`.

4. Make sure that **Negotiate** is the first choice in the **Authentication > Providers** dialog box.

5. Restart the IIS service.

Configuring Kerberos

This section discusses how to configure Kerberos on Ivanti EPMM server.

Configuring Kerberos settings in Ivanti EPMM

In **Ivanti EPMM Admin Portal > Settings > System Settings > Security > Outbound Kerberos Authentication**, enter the following:

TABLE 103. OUTBOUND KERBEROS AUTHENTICATION

UI Section	Choice
Active Directory's Kerberos Realm	IVANTI.COM
Corresponding Key Distribution Center (KDC) server	kdc.ivanti.com
Domains for outbound communication with Microsoft AD Certificate Services (Hostnames (not case sensitive) must end in `.ivanti.com` or `.IVANTI.COM`) - LDAP server: You can also use hostnames, such as: `ad.ivanti.com` - SCEP/NDES server: You can also use hostnames, such as: `ndes.ivanti.com` or `scep.ivanti.com`	
Service user credentials	`user@realm` For example: `serviceuser@IVANTI.COM`

Enabling Kerberos authentication on the Microsoft SCEP Certificate Enrollment configuration

To enable Kerberos authentication, in the **Edit SCEP Certificate Enrollment Setting** window (**Policies&Configs > Configurations > Edit existing or Add new > Certificate Enrollment > SCEP**) enable the checkbox **Prefer Kerberos authentication**.

Enabling Kerberos authentication on the LDAP configuration

To change the LDAP configuration, in the **Modifying LDAP Setting** window (**Services > LDAP**), enable the **Kerberos authentication method** in the **Advanced** options.

> **Note:** LDAP Kerberos authentication is supported only in direct mode. Ivanti does not yet support Kerberos authentication in LDAP with connector mode.

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

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**: Ivanti EPMM retrieves certificates on behalf of devices. Ivanti EPMM also manages the certificate lifetime and triggers renewals. See ""Using a proxy" on page 694".

     > **ⓘ**   Select this option for certificates used for email on devices with multi-user sign-in.

   - **Decentralized**: Devices retrieve their own certificates.

     - This feature is not available for iOS devices.

     - This feature is not available for MAC devices.

   - **Store keys on Ivanti EPMM**: Specifies whether Ivanti EPMM stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Ivanti EPMM.

     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 Ivanti EPMM**:

  - This feature is not available for iOS devices.

  - This feature is not available for MAC devices.

  - When this option is enabled, Ivanti EPMM 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.

> ℹ️ 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 657 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 657 for more information.)

> ℹ️ 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**.

> ℹ️ 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.

- Ivanti EPMM 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 Ivanti EPMM.

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 Ivanti EPMM 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 Ivanti EPMM 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 Ivanti EPMM SCEP settings should map the Ivanti EPMM email address attribute to the Symantec SeatID.

Ivanti EPMM 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 Ivanti EPMM the default is set to pki-ws.symauth.com.

  - The Registration Authority (RA) certificate Ivanti EPMM 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 Ivanti EPMM**: Specifies whether Ivanti EPMM 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 Ivanti EPMM.

- **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 Ivanti EPMM.

- **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 Ivanti EPMM 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.

- **ms_sid**: You must use the profile for which Microsoft Security Identifier support has been added by DigiCert. Use $USER_SID$ value from the drop-down list to generate a certificate with the SID

extension, provided the LDAP user has the SID value.

- **mail_email**: Use drop-down list to select $EMAIL$.

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 Ivanti EPMM, 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

Following are the instructions for configuring this type of certification.

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 Ivanti Mobile@Work for iOS, when Ivanti Mobile@Work for iOS prompts the user for the private key password.

- Ivanti Mobile@Work prompts for the password if a password was not required when the user uploaded the certificate to the user portal. Ivanti 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. Ivanti EPMM 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 Ivanti EPMM and associating the certificates with a user-provided certificate enrollment setting.

  - See the *Ivanti EPMM V2 API Guide*.

- The V1 API that uploaded user certificates to Ivanti EPMM is no longer available. If you used the V1 API to upload user certificates, Ivanti EPMM 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

    > ℹ️ Note that the V1 API associated the user certificate with a certificate type: All, WIFI, VPN, SMIMESIGNING, SMIMEENCRYPTION, EMAIL or EXCHANGE. Although Ivanti EPMM still supports using these certificates and their associated type, the user portal does not display these certificates in the user portal.

Ivanti EPMM 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. Ivanti EPMM stores the file, which includes the certificate and its private key. Ivanti EPMM 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 Ivanti 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, Ivanti 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 Ivanti Mobile@Work for iOS.

2. Ivanti Mobile@Work prompts the device user for the private key password.

3. The device user enters the password.

   > If the device user exits Ivanti Mobile@Work without providing the password, when the AppConnect app next launches, Ivanti 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, Ivanti EPMM 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 Ivanti EPMM file system. Whether you want the private key and password deleted from Ivanti EPMM 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 Ivanti EPMM deletes private keys and passwords older than some number of days.

IMPORTANT: When the private key and associated password is deleted, Ivanti EPMM 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, Ivanti EPMM 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 Ivanti EPMM, 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

-
- *Ivanti EPMM 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 select **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 Ivanti Mobile@Work if the app 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 699.

- **Delete Private Keys After Days**: Select the number of days after a user-provided certificate is uploaded to Ivanti EPMM after which Ivanti EPMM deletes the private key and, if provided, its password, from Ivanti EPMM.

The default is **None**, which means Ivanti EPMM does not delete the private key and its password.

3. Select **Save**.

Certificate Transparency Payload

In late 2018, Apple introduced a new Certificate Transparency policy. All certificates issued after October 15, 2018 must meet Apple's requirements to be trusted by Apple products. Aa Certificate Authority should issue a leaf certificate that meets Apple's Certificate Transparency policy by submitting it to a Certificate Transparency log and including the Signed Certificate Timestamp (SCT) when the certificate is signed, or the SCT must be provided during TLS handshake.

A Certificate Transparency payload specifies which domains or certificates to bypass Certificate Transparency enforcement.

This feature is applicable to:

- iOS 12.1.1

- MacOS 10.14.2

- tvOS 12.1.1

Procedure

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

2. Click **Add New > Apple > iOS/macOS /tvOS > Certificate Transparency**. The New Certificate Transparency Setting dialog box opens. Fill in the entries using the Certificate Transparency Settings table below.

3. Click **Save**.

The new configuration displays in the Configurations page.

TABLE 1. CERTIFICATE TRANSPARENCY SETTINGS

Item	Description
Name	Enter a name for the certificate transparency configuration.
Description	Enter a description of the certificate transparency configuration.
Domains	Clicking the **Add+** button adds another field in the Domains section.
	A leading period can be used to match subdomains, but a domain matching rule must not match all domains within a top level domain.
	For example: .sampledomain.com and .sampledomain.co.uk are allowed while .com and .co.uk are not allowed.
Certificate Hash for Certificates	Clicking the **Add+** button adds a drop-down field for you to select.
	• Hash Algorithm - string. Must be sha256. Required field.
	• Hash - Created by applying the specified hash algorithm to the DER-encoding of the certificate's `subjectPublicKeyInfo`. See "Creating the certificate hash for certificates" below.

Creating the certificate hash for certificates

To generate the data specified by the Hash key in the `subjectPublicKeyInfo` dictionary, use this CLI command for a PEM encoded certificate:

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin -
```

```
outform der | openssl dgst -sha256 -binary | base64
```

If your certificate is DER encoded, use this CLI command:

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin -
outform der | openssl dgst -sha256 -binary | base64
```

If your certificate does not have a .pem or .der extension, use the CLI file command to identify its encoding type.

```
$ file example_certificate.crt
example_certificate.crt: PEM certificate
$ file example_certificate.cer
example_certificate.cer: data
```

For more information, see the [Apple Configuration Profile Reference Guide](#).

Configuring iOS and macOS settings and restrictions

This section addresses settings and restrictions relating to iOS and macOS devices.

-
-
-
-
-
-

iOS and macOS settings

The following settings are available:

-
-
-
-
-
-

General settings (iOS and macOS)

You can configure a general settings configuration that determines when configuration profiles can be removed from iOS and macOS devices.

> ℹ️ General settings can be set once; if you want to use this screen to change these settings, then the user must manually delete the profile.

Procedure

1. Go to **Policies & Configs > Configurations.**

2. Select **Add New > Apple > iOS and macOS > General** to specify the basic information for interactions with the iOS and macOS configuration profiles.

3. Configure the general settings as described in "General iOS and macOS settings " below.

4. Select **Save**.

TABLE 104. GENERAL IOS AND MACOS SETTINGS

Item	Description
Name	Enter brief text that identifies this group of iOS and macOS general settings.
Description	Enter additional text that clarifies the purpose of this group of iOS and macOS general settings.
Identifier	Specify the profile identifier. It must uniquely identify this profile. Use the format com.companyname.identifier where identifier describes the profile, as in com.mycompany.work.
Organization	Specify the issuing organization of the profile, as it will be shown to the user.
Control when the profile can be removed	**Not for iOS with MDM:** Specify when configuration profiles should be removed: Always: always removable. With Authentication: removable with authentication. Never: never removable. Select this option to prevent users from removing the profile.

CalDAV settings (iOS and macOS)

CalDAV configurations allow you to specify parameters for connecting to CalDAV-compliant calendar servers. CalDAV (or Calendaring Extensions to WebDAV), is a remote calendar access standard supported by iOS and macOS.

ⓘ   Users may be prompted for any settings you do not specify.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select **Add New > Apple > iOS and macOS > CalDAV**.

3. Specify parameters for connecting to CalDAV-compliant calendar servers, as described in "CalDAV settings (iOS and macOS) " below.

4. Select **Save**.

TABLE 105. CALDAV SETTINGS (IOS AND MACOS)

Item	Description
Name	Enter brief text that identifies this group of iOS and macOS CalDAV settings.
Description	Enter additional text that clarifies the purpose of this group of iOS and macOS general settings.
HostName	Enter the host name of the calendar server.
Port	Enter the port for the calendar server.
Principal URL	Enter the URL for accessing calendar services.
Use SSL	Select to use SSL for data transfer.
Use Google Apps Password	Select to use the Google Apps password. For more information about configuring the Google Apps password, see [].
User Name	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format. **Why:** Some enterprises have a strong preference concerning which identifier is exposed. See "Supported Variables for CalDAV Settings" below.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_US. See "Supported Variables for CalDAV Settings" below.

Supported Variables for CalDAV Settings

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

- $USERID$

- $EMAIL$

- $MANAGED_APPLE_ID$

> **i** For Shared iPad devices and User Enrolled devices only.

- $NULL$

- $USER_CUSTOM1$... $USER_CUSTOM4$ (custom fields defined for LDAP)

CardDAV settings (iOS and macOS)

CardDAV configurations allow you to specify parameters for connecting to CardDAV-compliant address book servers. CardDAV (or vCard Extensions to WebDAV), is a remote contact data access standard supported by iOS and macOS.

> **i** This configuration is supported on iOS and macOS v10.8. macOS v10.7 Lion is not supported.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select **Add New > Apple > iOS and macOS > CardDAV** to configure access to subscription address books compatible with this protocol.

3. Configure your CardDav settings as described in "CardDAV settings (iOS and macOS) " below.

4. Select **Save**.

TABLE 106. CARDDAV SETTINGS (IOS AND MACOS)

Item	Description
Name	Enter brief text that identifies this group of iOS and macOS subscribed address book settings.
Description	Enter additional text that clarifies the purpose of this group of iOS and macOS subscribed address book settings.
HostName	Enter the hostname or IP address of the CardDAV account.
Port	Enter the port number of the CardDAV account.

TABLE 106. CARDDAV SETTINGS (IOS AND MACOS) (CONT.)

Item	Description
Principal URL	Enter the Principal URL for the CardDAV account.
Use SSL	Select to use SSL for data transfer.
Use Google Apps Password	Select to use the Google Apps password. For more information about configuring the Google Apps password, see [].
User Name	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format. **Why:** Some enterprises have a strong preference concerning which identifier is exposed. See "Supported variables for CardDAV Settings" below.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$. See "Supported variables for CardDAV Settings" below.
Communication Service Rules (iOS 10 and later)	Select a default audio service or app to be associated with the device user's accounts on the Exchange, CardDAV, LDAP, and Google servers. All calls initiated on the iOS device to contacts from contact lists stored on the server will use the selected audio service by default. This feature is supported on devices running iOS 10 or supported newer versions. To enable communication service rules: • Select **Choose a default app to be used when calling contacts from this account**. A drop-down list of apps is displayed. • Select the drop-down list to select the default audio app or service.

Supported variables for CardDAV Settings

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

- $USERID$

- $EMAIL$

- $MANAGED_APPLE_ID$

  > ⓘ   For Shared iPad devices and User Enrolled devices only.

- $NULL$

- $USER_CUSTOM1$... $USER_CUSTOM4$ (custom fields defined for LDAP)

Web Clips settings (iOS and macOS)

You can send web clips to the home screens of managed devices by creating a web clip setting.

Procedure

1. Go to **Policies & Configs > Configurations.**

2. Select **Add New > Apple > iOS and macOS > Web Clips** to add web clips to the home screen of users' devices.

3. Use "Web clips settings " below to make your configurations.

TABLE 107. WEB CLIPS SETTINGS

Item	Description
Web Clips Set Name	Enter brief text that identifies this group of iOS and macOS web clips settings.
Description	Enter additional text that clarifies the purpose of this group of iOS and macOS web clips settings.

4. Under the Web Clips field, select **Add New**. The **Add Web Clip** dialog box opens.

5. Use the table below as a guide to completing your web clip entry.

TABLE 108. WEB CLIPS SETTINGS (IOS AND MACOS)

Item	Description
Name	Enter a name that identifies this configuration.
Address/URL	Enter the address or URL for the target of the web clip. Ensure the URL you enter includes the prefix http:// or https://.
Icon	Select an icon to display for the web clip.
Removable	Clear the Removable check box to prevent users from removing the web clip once it is pushed out to their phones.
Full Screen	By default, Full Screen is selected. When selected, the web clip is displayed as a full-screen application.

TABLE 108. WEB CLIPS SETTINGS (IOS AND MACOS) (CONT.)

	(i) Apple does not currently support the display of full screen web clips in full screen mode on devices running iOS 8, iOS 8.1, and iOS 8.1.1.
Precomposed	By default, Precomposed is selected. When selected, iOS will not add the bezel shading effect to the icon.
Ignore Manifest Scope	Deselected (default) means Safari UI appears when device user navigates away from the web clip's URL. Selected means a full screen web clip can navigate to an external web site without showing Safari UI. If Full Screen is deselected, this field has no effect.
Target Bundle Identifier	The application bundle identifier that specifies the application that opens the URL. To use this property, the profile must be installed through an MDM.

6. In the New Web Clips Setting dialog box, select **Add New** for additional web clips.

7. When finished, select **Save**.

Configuration profile settings (iOS, tvOS, and macOS)

Occasionally, you may want to upload an iOS, tvOS, or macOS configuration profile generated from outside of Ivanti EPMM and push it to devices.

For example, you can send devices an Apple Configurator payload by exporting the payload from Apple Configurator and pushing it to devices as a .plist file. This is particularly useful for edge case scenarios, where the command you wish to execute on the device is not otherwise available.

(i) When pushing a configuration profile to iOS and macOS devices applied to a particular label, Ivanti EPMM also pushes the profile to any Apple TV devices applied to that label.

(i) When using this option, it is required to only have the portion of the .plist that is inside the array of the "PayloadContent", essentially "<dict>...</dict>". Any substitution variables will not be substituted. The file will not be validated and will be added to the payload without any modifications.

Another use case is if you wish to deploy a signed .mobileconfig file, for example, Apple debug configurations via MDM. Because Ivanti EPMM does not expect a signed file, it would not be able to parse it and inject a substitution variable because it would change the signature of the signed file. To get around this, select the **Send File Verbatim - do not parse or use substitution variables** check box. Files uploaded with this option selected are sent as is to the device without parsing, validating, or signing of the file by Ivanti EPMM.

> Ivanti EPMM server will not attempt to process the file by parsing for substitution variables, sign the configuration when delivering to a device, or make any additions or modifications to the configuration. File must be in a valid .mobileconfig format and should be signed.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select **Add New > Apple > iOS and macOS > Configuration Profile**.

3. In the **Name** field, enter a name for the configuration profile setting.

4. Select **Choose File** and navigate to the relevant .plist file.

5. You can hide or display the contents of the file as follows:

   - Select **Allow Viewing of Content** to make the file contents visible.

   - Deselect **Allow Viewing of Content** to hide the file contents.

6. Select **User** or **Device** channel.

7. If the file is a signed .mobileconfig file, select **Send File Verbatim - do not parse or use substitution variables** check box.

8. Select **Save**.

9. Select the configuration profile you created and apply it to a relevant label or labels.

LDAP settings (iOS and macOS)

You can configure an LDAP profile for iOS and macOS devices.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select **Add New > iOS and macOS > LDAP** to configure an LDAP profile for iOS and macOS devices.

   The New LDAP Setting dialog box opens.

3. Use the guidelines in the table below to complete this form.

TABLE 109. ADD NEW LDAP CONFIGURATION

Item	Description
Name	Descriptive name to use when referencing this configuration.
Account Description	Optional. Description of the LDAP account.
Account Username	Optional. Username for accessing the LDAP account.
Account Password	Optional. Password that corresponds to the Account Username value. The password applies to encrypted accounts.
Confirm Account Password	Optional. Confirms the password entered in the Account Password field.
Account Hostname	The hostname for the LDAP server.
Use SSL	Whether to use SSL.
Search Settings	Should have at least one entry for the account. Each entry represents a node in the LDAP tree from which to start searching. Select the + button to add a new entry, then edit the entry. An entry consists of the following values: Description: Explains the purpose of the search setting. Scope: Select Base, Subtree, or One Level to indicate the scope of the search. Base indicates just the node level, Subtree indicates the node and all children, One Level indicates the node and one level of children. Search Base: The conceptual path to the specified note (e.g., ou=people, o=mycorp).
Communication Service Rules (iOS 10 and later)	Select a default audio service or app to be associated with the device user's accounts on the Exchange, CardDAV, LDAP, and Google servers. All calls initiated on the iOS device to contacts from contact lists stored on the server will use the selected audio service by default. This feature is supported on devices running iOS 10 or supported newer versions.

TABLE 109. ADD NEW LDAP CONFIGURATION (CONT.)

Item	Description
	To enable communication service rules: • Select **Choose a default app to be used when calling contacts from this account**. A drop-down list of apps is displayed. • Select the drop-down list to select the default audio app or service.

4. Select **Save**.

Extensible Single Sign-On

Extensible Single Sign-On is an Apple feature that allows you to configure single sign-on for users accessing enterprise resources from iOS and macOS devices that are registered with Ivanti EPMM. The extension can be used by identity providers to deliver a seamless experience as users sign in to enterprise resources. App users on the device need to authenticate once. The initial user authentication can be done using enterprise credentials or through an identity provider (IdP) setup. User are not prompted for authentication for subsequent access.

This configuration does not require an Ivanti Tunnel or a Sentry deployment.

- An app, also referred to as an app extension, that performs the SSO is required.

- If you are configuring an identity provider (IdP), the IdP must have an app extension.

  ○ The **Extensible Single Sign-On** configuration is supported with ADFS.

- The feature is supported with iOS 13.0 ad macOS 10.15 or supported newer versions.

You configure Extensible Single Sign-On on the Admin Portal. Go to **Policies & Configs > Configurations > Apple > iOS / macOS / tvOS > Extensible Single Sign-On**. To distribute the configuration, save and apply it to a label that contains the target devices.

> ℹ️ Extensible Single Sign-on requires an identity provide (IdP) app extension. Please refer to the vendor-specific documentation for setup procedures.

The following table describes the fields and settings in the configuration.

TABLE 110. EXTENSIBLE SINGLE SIGN-ON FIELD DESCRIPTION

Item	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Channel	The Channel options are applicable to macOS only. Select one of the following: • User: Select to apply to only specific users on the device. • Device: Select to apply to all users on the device. ⓘ The User option is not supported on macOS 10.15 devices .
Extensible Single Sign-On	
Choose SSO Type	Select the initial sign on method. • Credentials: Select this option if the initial authentication method uses your enterprise credentials. • Redirect: Select this option if the enterprise resource uses an identity provider to authenticate users.
Host	If you select **Credentials** as the **SSO Type**, enter one or more host names or domain names that can be authenticated through the app extension. Host or domain name matching is not case sensitive. The host and domain names must be unique. Hosts that begin with a "." are wildcard suffixes. Wildcard suffixes will match all sub-domains. Otherwise, the host or domain name must be an exact match.
URL	If you select **Redirect** as the **SSO Type**, enter one or more URL prefixes of identity providers where the app extension performs SSO. The URLs must begin with http:// or https://. The scheme and host name matching is not case sensitive. Do not use query parameters and URL fragments. The URLs must be unique.
Extension Identifier	Enter the bundle ID of the app extension that performs the single sign-on for the specified URLs.
Team Identifier	Enter the team identifier of the app extension. The team identifier is required on macOS. However, it is ignored on iOS.
Realm	If you select **Credentials** as the **SSO Type**, enter the realm name.

TABLE 110. EXTENSIBLE SINGLE SIGN-ON FIELD DESCRIPTION (CONT.)

Item	Description
	The realm name is case sensitive and must be an exact match.
Custom Data	Enter one or more custom data as key-value pairs.

> If you are configuring an identity provider (IdP), the IdP must have an app extension. Please refer to the vendor-specific documentation for setup procedures.

Extensible Single Sign-On Kerberos

Extensible Single Sign-On is an Apple feature that allows you to configure single sign-on for users accessing enterprise resources from iOS and macOS devices that are registered with Ivanti EPMM. App users on the device need to authenticate once. Users are not prompted for authentication for subsequent access.

Use this configuration to do single sign-on if your enterprise uses Kerberos authentication.

This configuration does not require an Ivanti Tunnel or a Sentry deployment.

IMPORTANT:

- An app, also referred to as an app extension, that performs the SSO is required.

- The feature is supported with iOS 13.0 ad macOS 10.15 or supported newer versions.

You configure Extensible Single Sign-On with Kerberos on the Admin Portal. Go to **Policies & Configs > Configurations > Apple > iOS / macOS / tvOS > Extensible Single Sign-On Kerberos**. To distribute the configuration, save and apply it to a label that contains the target devices.

The following table describes the fields and settings in the configuration.

TABLE 111. EXTENSIBLE SINGLE SIGN-ON KERBEROS FIELD DESCRIPTION

Item	Description
Name	(Required) Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Channel	The Channel options are applicable to macOS only. Select one of the following: • User: Select to apply to only specific users on the device.

TABLE 111. EXTENSIBLE SINGLE SIGN-ON KERBEROS FIELD DESCRIPTION (CONT.)

Item	Description
	• Device: Select to apply to all users on the device.
	ℹ The User option is not supported on macOS 10.15 devices .
Extensible Single Sign-On Kerberos	
Principal Name	(Required) Enter the Kerberos Principal Name.
Realm	(Required) Enter the Kerberos Realm.
Certificate	(Required) Select the certificate to use to renew the Kerberos credential.
Host	Enter the Kerberos domain name that can be authenticated through the app extension.
	Host or domain name matching is not case sensitive. The host and domain names must be unique Hosts that begin with a "." are wildcard suffixes. Wildcard suffixes will match all sub-domains. Otherwise, the host or domain name must be an exact match.
Allow Automatic Login	Allows passwords to be saved in the keychain. By default, the option is selected.
	If the option is deselected, passwords are not saved in the keychain.
Delay User Setup	Applicable to macOS 11 or supported newer versions.
	Select the option so that users are not prompted to set up the app extension for Kerberos.
	If the option is selected users are prompted to set up the app extension for Kerberos only if the administrator enables app extension with the app-SSO tool or the user sees a Kerberos challenge.
Require User Presence	Select the option to require users to provide Touch ID, Face ID, or their passcode to access the keychain entry.
Monitor Credential Cache	Applicable to macOS 11 or supported newer versions.
	By default, the option is selected.
	Deselect the option to request credentials on the next matching Kerberos challenge or network state change.
	If the credentials expire, a new is created.
Cache Name	Enter the Generic Security Service (GSS) name of the Kerberos cache to use.
Domain Realm Mapping	
Domain	Select **+Add** to add a domain and DNS suffixes.
	For Domain, enter the name of realm.
	For value, enter one or more DNS suffixes that map to the realm.

TABLE 111. EXTENSIBLE SINGLE SIGN-ON KERBEROS FIELD DESCRIPTION (CONT.)

Item	Description
Default Realm	Enter the default realm if there is more than one Kerberos extension configuration.
Use Site Auto Discovery	The option is selected by default. If selected, the Kerberos extension automatically uses LDAP and DNS to determine its Active Directory (AD) site name.
Site Code	Enter the name of the Active Directory site that the Kerberos extension should use.
Replication Time	Applicable to macOS 11 or supported newer versions. Enter the time, in seconds, required to replicate changes int he Active Directory domain. The Kerberos extension uses the configured replication time to check the password age.
Credential Bundle IDACL	
Credential Bundle	Select Add+ to enter an app bundle ID allowed to access the Ticket Granting Ticket (TGT).
Include managed Apps in Bundle IdACL	Applicable to iOS 14 or supported newer versions. Select the check box to allow only managed apps to access and use the credential. This option is used in addition to the Credential Bundle.
Custom Username Label	Applicable to macOS 11 or supported newer versions. Enter the custom user name label used in the Kerberos extension instead of the "Username."
Help Text	Applicable to iOS 14 or supported newer versions. Enter text to display at the bottom of the Kerberos log in window. ⓘ The text can be a disclaimer or help information.
Credential Use Mode	Select one of the following options to specify how the Kerberos extension credential is used by other processes: Always (default): The extension credential is always used if the service principal name (SPN) matches the Kerberos Extension Hosts array. The credential is not used if the calling app is not in the configured in **Credential Bundle**. When Not Specified: The credential is only used when another credential has not been specified by the caller and the SPN matches the Kerberos Extensions Hostsarray. The credential will not be used if the calling app is not in in **Credential Bundle**. Kerberos Default: The default Kerberos processes for selecting credentials is used which normally uses the default Kerberos credential. This is the same as turning off this capability.

TABLE 111. EXTENSIBLE SINGLE SIGN-ON KERBEROS FIELD DESCRIPTION (CONT.)

Item	Description
Require TLS for LDAP	Select to require TLS for the LDAP.
Password Settings	
The **Password Settings** options are applicable to macOS 10.15 or supported newer versions.	
Allow Password Change	The option is selected by default. Deselect to disable password changes.
Password Change URL	Enter the URL to launch when they initiate a password change. The URL is launched in the user's default web browser.
Allow Password Complexity	If selected, passwords must meet Active Directory's definition of "complex."
Minimum Password Length	Enter the minimum length, in characters, of passwords on the domain.
Password Expiry Notification	Enter the number of days prior to password expiration when a notification of password expiration is sent to the user. The default value is 15 days.
Password Expiry Override	Enter the number of days that passwords can be used on this domain. For most domains, this can be calculated automatically.
Password Required Text	Enter the domain's password requirements. Use only if pwReqComplexity or pwReqLength are not specified.
Password History Count	Enter the number of prior password that cannot be re-used on this domain.
Password Minimum Age	Enter the minimum age, in days, of the password before it can be changed on this domain.
Allow Syncing Local Password	Select to enable password syncing. ⓘ The setting is not applied if the user is logged in with a mobile account.

iOS / tvOS settings

The following settings are available. Note that they apply to tvOS devices only when specified.

AirPlay settings

This feature is only supported for iOS 7 or supported newer versions.

AirPlay is an iOS feature that allows you to mirror the content displayed on your iOS device on to a destination device, for example, an HDTV.

For iOS 7 or supported newer versions, you can now configure your Ivanti EPMM to control the AirPlay resources that supervised devices can access. You can configure the following settings:

- Specify the passcode for the AirPlay destination device so that devices can connect seamlessly.

- Specify a whitelist of destination devices to which you can mirror the content that is displayed on the screen of your supervised device.

ℹ️   This setting does not apply to tvOS devices.

Procedure

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

2. Select **Add New > Apple > iOS / tvOS > AirPlay**. The New AirPlay Configuration dialog box opens.

3. Enter a name for the AirPlay Configuration.

4. Enter additional information that describes the AirPlay Configuration.

5. In the AirPlay Destination Devices section, select + to add a new destination device.

6. For each destination device, enter the following information:

Field	Description
Device Name	Enter the name of the destination device.
Password	Enter the password for the destination device.
Description	Enter additional information that describes this destination device.
-	Select if you want to delete this device.

7. In the AirPlay Whitelist Devices section, select + to add a new destination device to the whitelist.

> ℹ️ Whitelists are only supported on supervised devices.

8. For each destination device in the whitelist, enter the following information:

Field	Description
Device MAC Address	Enter the Bonjour Device ID.
Description	Enter additional information that describes this destination device.
-	Select if you want to delete this device.

9. Select **Save**.

AirPrint settings

This feature is only supported on iOS 7 or supported newer versions.

AirPrint is an iOS feature that allows you to print to an AirPrint printer from your iOS device without the need to install drivers or download software.

You can configure your Ivanti EPMM to control the printing resources that devices can access. You can specify a whitelist of AirPrint printers that devices can access.

> ℹ️ This setting does not apply to tvOS devices.

Procedure

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

2. From the **Add New** drop-down menu, go to **Apple > iOS / tvOS > AirPrint**. The New AirPrint Configuration dialog box opens.

3. Enter a Name for the AirPrint configuration.

4. Enter a Description that clarifies the purpose of this configuration.

5. Enter additional information that describes the AirPrint Configuration.

6. In the **AirPrint Destination** section, click **Add+** to add a new destination printer.

7. For each destination printer, enter the following information:

Field	Description
IP Address / Hostname	Enter the IP address of the AirPrint printer.
Path	Enter the Resource Path associated with the AirPrint printer. This corresponds to the rp parameter of the _ipps.tcp Bonjour record. For example: • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. ⓘ The resource path is case sensitive.
Port	Enter the listening port of the AirPrint destination. ⓘ If this is not specified, AirPrint will use the default port. For details on Apple standard ports, visit https://support.apple.com/en-us/HT202944
Force TLS	Allows you to enable the connection to be secured by Transport Layer Security(TLS). By default, it is disabled.
Description	Enter additional information that describes this destination device.

8. Click **Save**.

After installation of AirPrint configuration on the macOS, the printer details are pushed through the AirPrint configuration to the device. In the Add screen, the device user must select Default and then select the required print profile. This adds the required printer to the Printers & Scanners.

App restrictions configuration setting

The App Restrictions configuration setting allows you to whitelist or blacklist managed apps in the App Catalog on Ivanti EPMM. Creating a whitelist restricts device users to viewing on their devices only apps explicitly listed in the whitelist. Creating a blacklist restricts device users from viewing or launching blacklisted apps on their devices. You can also blacklist apps from the Apple App Store.

You can create more than one whitelist or blacklist, but Ivanti EPMM will only send one app restriction setting to devices. There is no default app restrictions configuration. If you configure both a blacklist and a whitelist, then Ivanti EPMM removes all blacklisted apps from the whitelist, and sends only the whitelist to devices. If you apply one or more App Restriction configurations to a label, then Ivanti EPMM combines all App Restriction configurations and sends it to the devices belonging to that label.

After you have created a blacklist, you cannot convert it to a whitelist.

> ℹ️ This feature applies only to supervised devices running iOS 9.3 or supported newer versions.

> ℹ️ This setting applies to tvOS 11.0+ or supported newer versions.

Whitelisting managed iOS apps

Creating a whitelist of managed apps allows you to specify the apps you want to be visible to device users on their devices. You can whitelist apps from the App Catalog in Ivanti EPMM. Ivanti EPMM hides from the device user any app that is not whitelisted.

> ℹ️ This feature applies only to supervised devices running iOS 9.3 or supported newer versions. You cannot whitelist a web clip. This is an Apple limitation.

Procedure

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

2. Select **Add New**.

3. Select **Apple > iOS / tvOS > App Restrictions.** The New App Restrictions Configurations dialog box opens.

4. In the **Name** field, enter a name for the app restriction configuration. Optionally, enter a description for the app restriction configuration in the **Description** field.

5. Under **App Restrictions**, select **Create a Whitelist**.

6. Select **Add > App Catalog**.

   A new row is added to the table of apps.

7. In the table, select the cell in the **App Name** column, and begin typing the app name you want to blacklist.

   A drop-down list of App Catalog apps appears.

8. From the drop-down list, select the App Catalog app you want to blacklist.

9. Repeat steps 6-8 for any additional apps you would like to whitelist.

10. Select **Save**.

11. Select the app restrictions configuration you created.

12. Select **Actions > Apply to Label**.

13. Select the labels to which you want to apply the provisioning profile, such as **iOS**.

14. Select **Apply**. Once you have applied the label, the App Restrictions configuration is automatically pushed to the devices.

Blacklisting iOS apps

Creating a blacklist allows you to specify particular apps you want to prevent device users from viewing or running.

You can select apps to blacklist in the following ways:

- **From an Apple App Store**: You can blacklist a public app from a particular Apple App Store by first choosing the Apple App Store and then searching for the app.

- **From the App Catalog**: You can blacklist a particular managed app from the App Catalog on Ivanti EPMM.

- **Manually**: You can blacklist a particular app by manually entering its name or bundle ID.

This feature applies only to supervised devices running iOS 9.3 or supported newer versions.

Procedure

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

2. Select **Add New**.

3. Select **Apple > iOS / tvOS > App Restrictions.** The New App Restrictions Configurations dialog box opens.

4. In the **Name** field, enter a name for the app restriction configuration. Optionally, enter a description for the app restriction configuration in the **Description** field.

5. Under **App Restrictions**, select **Create a Blacklist**.

6. To blacklist an app from the Apple App Store:

   - Select **Add > iTunes Store** to select the particular Apple App Store where the app can be found. A row is added to the table of apps.

   - In the App Name column, search for the app in the App Store by entering the app name.

   - From the drop-down list that appears, select the relevant app.

7. To blacklist an app from the App Catalog on Ivanti EPMM:

   - Select **Add > App Catalog**. A row is added to the table of apps.

   - In the table, select the cell in the **App Name** column, and begin typing the app name you want to blacklist.

   - From the drop-down list that appears, select the App Catalog app you want to blacklist.

8. To blacklist an app manually:

   - Select **Add > Enter Bundle ID**. A row is added to the table of apps.

   - In the table, select the cell in the **App Name** column and enter the name of the app you want to blacklist.

   - Alternatively, select the cell in the **Bundle ID** column, and enter the bundle ID of the app you want to blacklist.

9. For any other apps you want to blacklist, repeat steps 6, 7 or 8.

10. Select **Save**.

11. Select the app restrictions configuration you created.

12. Select **Actions > Apply to Label**.

13. Select the labels to which you want to apply the provisioning profile, such as **iOS**.

14. Select **Apply**. Once you have applied the label, the App Restrictions configuration is automatically pushed to the devices.

iOS and tvOS restrictions settings

Select **Policies & Configs > Configurations > Add New > Apple > iOS / tvOS > Restrictions** to specify lockdown capabilities for iOS and tvOS devices.

There are restrictions available on all iOS/tvOS devices. Each restriction has a default value that is determined by Apple. Without a restrictions configuration, the values in Ivanti EPMM's Restrictions tab will be the default ones as defined by Apple. When Ivanti EPMM sends a restriction configuration, the values will be set based on that configuration. The next Restrictions "report" will display in the **Device Details page > Restrictions tab** and will list the new values based on the configurations sent and what was sent by the device.

The Restrictions report may not display each and every restriction that was sent.

> ℹ️ When iOS 13 devices upgrade to Ivanti EPMM, restrictions are enabled by default. However, when tvOS 12.2 and 13.0 devices upgrade, the restrictions are not enabled by default.

If User Enrollment through Apple Business Manager was done, the Restrictions tab may not display the table and instead display "No Data." This is because no data was returned listing which restrictions were set and what the values were.

If Notes for Audit Logs is enabled, after selecting **Save**, a text dialog box opens. Enter the reason for the change and then select **Confirm**. For more information, see "Best practices: label management" on page 860.

> ℹ️ When there are two iOS restrictions of the same key and are pushed to the device with conflicting values, Ivanti EPMM will send both restrictions to device. However, when two restriction configuration are sent to device with different values, Apple states that the most restrictive option takes precedence. There is no clear documentation from Apple about this behavior. Best practice is to have a single restriction setting with the desired value set instead of multiple settings with same key, which results in having value conflicts.

The following table summarizes the settings.

TABLE 112. RESTRICTIONS SETTINGS (IOS)

Item	Description	Enabled by default
Name	Enter brief text that identifies this group of iOS restriction settings.	N/A
Description	Enter additional text that clarifies the purpose of this group of iOS restriction settings.	N/A
Device Functionality		
Allow use of camera	`allowCamera` Select to disable the camera and remove its icon from the Home screen. Users will be unable to take photographs. Clearing this restriction also disables the Allow FaceTime restriction.	Yes
Allow FaceTime	`allowVideoConferencing` When deselected, disables video conferencing. As of iOS 13, requires a supervised device.	Yes
Allow screenshots and screen recording	`allowScreenShot` When deselected, users are unable to save screenshots or record video of the display. When deselected, this restriction prevents the Classroom app from observing remote screens. Available for iOS 9.0 or supported newer versions.	Yes
Allow AirPlay and View Screen by Classroom (supervised devices only)	`allowRemoteScreenObservation` Select to enable remote screen observation. Available for iOS 9.3 or supported newer versions.	Yes
Allow Classroom to perform AirPlay and View Screen without prompting (iOS 10.3 and later with supervised devices only)	`forceClassroomUnpromptedScreenObservation` Select to enable remote screen observation without prompting. Available for iOS 10.3 or supported newer versions.	Yes
Allow AirDrop (supervised devices only)	`allowAirDrop` If deselected, AirDrop is disabled.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow iMessage (supervised devices only)	`allowChat` When deselected, disables the use of the Messages app with supervised devices.	Yes
Allow Apple Music (with supervised devices only)	`allowMusicService` If disabled, Music service is disabled and Music app reverts to classic mode. Available for iOS 9.3 or supported newer versions.	Yes
Allow Radio (supervised devices only)	`allowRadioService` If disabled, iTunes Radio is disabled. Available for iOS 9.3 or supported newer versions.	Yes
Allow voice dialing while device is locked	`allowVoiceDialing` When deselected, disables voice dialing.	Yes
Allow Siri	`allowAssistant` When deselected, disables Siri.	Yes
Allow Siri while device is locked	`allowAssistantWhileLocked` When deselected, the user is unable to use Siri when the device is locked. This restriction is ignored if the device does not have a passcode set.	Yes
Enable Siri profanity filter (supervised devices only)	`forceAssistantProfanityFilter` When selected, forces the use of the profanity filter assistant. Available for iOS 8.0 or supported newer versions.	No
Show user-generated content in Siri (supervised devices only)	`allowAssistantUserGeneratedContent` If deselected, prevents Siri from querying user-generated content from the web.	Yes
Allow Siri Suggestions (supervised devices only)	`allowSpotlightInternetResults` If deselected, prevents Siri from offering suggestions for apps, people, search results, and more.	Yes
Allow server-side logging of Siri commands (iOS 12.2 and later)	`allowSiriServerLogging` If deselected, disables server-side Siri logging. Applicable to iOS 12.2 or supported newer versions.	Yes
Allow Apple Books (supervised devices only)	`allowBookstore` Select to allow access to iBookstore.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow installing apps using Apple Configurator and iTunes (supervised devices only)	`allowAppInstallation` When deselected, the App Store is disabled and its icon is removed from the Home screen. Users are unable to install or update their applications. This setting does not affect installation of in-house apps.	Yes
Allow installing apps using App Store (supervised devices only)	`allowUIAppInstallation` When deselected, the App Store is disabled and its icon is removed from the Home screen. However, users may continue to use host apps (iTunes, Configurator) to install or update their apps. Available for iOS 9.0 or supported newer versions. ⓘ This restriction is unavailable if **Allow installing apps using Apple Configurator and iTunes** is deselected.	Yes
Allow automatic app downloads (supervised devices only)	`allowAutomaticAppDownloads` If deselected, prevents automatic downloading of apps purchased on other devices. Does not affect updates to existing apps. If selected, apps purchased by the device user will be automatically downloaded. ⓘ This restriction is unavailable if **Allow installing apps using Apple Configurator and iTunes** is deselected.	Yes
Allow removing apps (supervised devices only)	`allowAppRemoval` If deselected, disables removal of apps from iOS devices. Available for iOS 9.0 or supported newer versions.	Yes
Allow System App Removal (iOS 11.0 and later with supervised devices only)	`allowSystemAppRemoval` When deselected, disables the removal of system apps from the device. Available for iOS 11.0 or supported newer versions.	Yes
Allow App Clips (iOS 14.0 and later with supervised devices only)	`allowAppClips` When deselected, prevents a device user from adding any App Clips and removes any existing App Clips on the device. Available for iOS 14.0 or supported newer versions.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow Personalized Advertising (iOS 14.1 and later)	`allowApplePersonalizedAdvertising` When deselected, limits personalized advertising. Available for iOS 14.1 or supported newer versions.	Yes
Allow NFC (iOS 14.2 and later)	`allowNFC` When deselected, NFC is not allowed on the device. This is not specific to device registration. Available for iOS 14.2 or supported newer versions.	Yes
Force Dictation Processing Only on Device (iOS 14.3 and later)	`forceOnDeviceOnlyDictation` When selected, uses the native dictation program that sends information such as voice input, contacts, and location to Apple (when necessary) for processing your requests. Available for iOS 14.3 or supported newer versions.	No
Force on-device only language translation	`forceOnDeviceOnlyTranslation` If true, the device won't connect to Siri servers for the purposes of translation. Available in iOS 15 and later. Boolean. Default: false	No
Allow In-App Purchases	`allowInAppPurchases` When deselected, prohibits in-app purchasing.	Yes
Require iTunes Store password for all purchases	`forceITunesStorePasswordEntry` When selected, forces device users to enter their iTunes password for each App Store transaction.	Yes
Allow iCloud backup	`allowCloudBackup` When deselected, disables backing up the device to iCloud.	Yes
Allow iCloud documents & data	`allowCloudDocumentSync` When deselected, disables document and key-value syncing to iCloud.	Yes
Allow iCloud Keychain	`allowCloudKeychainSync` If deselected, disables iCloud Keychain synchronization.	Yes
Allow managed apps to store data in iCloud	`allowManagedAppsCloudSync` If deselected, prevents managed applications from using cloud sync.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow backup of enterprise books	`allowEnterpriseBookBackup` Select to allow device users to back up enterprise-managed books to iCloud. Available for iOS 8.0 or supported newer versions.	Yes
Allow notes and highlights sync for enterprise books	`allowEnterpriseBookMetadataSync` Select to allow device users to synchronize with iCloud their notes and highlights in enterprise-managed books. Available for iOS 8.0 or supported newer versions.	Yes
Allow iCloud photo sharing	`allowSharedStream` If deselected, Shared Photo Stream will be disabled.	Yes
Allow iCloud Photo Library	`allowCloudPhotoLibrary` If deselected, disables iCloud Photo Library. Any photos not fully downloaded from iCloud Photo Library to the device will be removed from local storage. Available for iOS 9.0 or supported newer versions.	Yes
Allow My Photo Stream (disallowing can cause data loss)	`allowPhotoStream` When deselected, disables Photo Stream.	Yes
Allow automatic sync while roaming	`allowGlobalBackgroundFetchWhenRoaming` When deselected, disables global background fetch activity when an iOS phone is roaming. Background fetch allows apps to update data in the background in anticipation of users accessing the app data.	Yes
Force encrypted backups	`forceEncryptedBackup` When selected, encrypts all backups. Automatically selected due to SCEP requirements.	Yes
Force limited ad tracking	`forceLimitAdTracking` If selected, limits ad tracking.	No
Allow Erase All Content and Settings (supervised devices only)	`allowEraseContentAndSettings` Deselect to disable the "Erase All Content and Settings" option in the Reset section of iOS devices. Applicable to iOS 8 and later, and macOS 12 and later.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow user to accept untrusted TLS certificates	`allowUntrustedTLSPrompt` Select to allow the device user to accept untrusted HTTPS certificates. If this option is not selected, then the device will automatically reject untrusted HTTPS certificates without prompting the device user.	Yes
Allow automatic updates to certificate trust settings	`allowOTAPKIUpdates` If deselected, over-the-air PKI updates are disabled. Setting this restriction to false does not disable CRL and OCSP checks.	Yes
Allow trusting new enterprise app authors	`allowEnterpriseAppTrust` If deselected, prevents trusting enterprise apps from other companies. Available for iOS 9.0 or supported newer versions.	Yes
Allow installing configuration profiles (supervised devices only)	`allowUIConfigurationProfileInstallation` If deselected, the user is prohibited from installing configuration profiles and certificates interactively.	Yes
Allow adding VPN configurations (iOS 11.0 and later with superviseed devices only)	`allowVPNCreation` When selected, allows the creation of VPN configurations. Available for iOS 11.0 or supported newer versions.	Yes
Allow Classroom to lock to an app and lock the device without prompting (iOS 11.0 and later with supervised devices only)	`forceClassroomUnpromptedAppAndDeviceLock` If selected, allow the teacher to lock apps or the device without prompting the student. Available for iOS 11.0 or supported newer versions.	Yes
Automatically join Classroom classes without prompting (iOS 11.0 and later with supervised devices only)	`forceClassroomAutomaticallyJoinClasses` If selected, automatically give permission to the teacher's requests without prompting the student. Available for iOS 11.0 or supported newer versions.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Require teacher permission to leave Classroom unmanaged classes (iOS 11.3 and later with supervised devices only)	`forceClassroomRequestPermissionToLeaveClasses` Requires teacher approval for a student to leave a Classroom unmanaged classes from their device. Available for iOS 11.3 or supported newer versions.	Yes
Allow modifying account settings (supervised devices only)	`allowAccountModification` Select to allow users to modify accounts settings, such as adding or removing mail accounts and modifying iCloud and iMessage settings, and so on.	Yes
Allow modifying Bluetooth settings (iOS 10.0 and later supervised devices only)	`allowBluetoothModification` If deselected, prevents the modification of Bluetooth settings. For supervised devices only. Available in iOS 10.0 or supported newer versions.	Yes
Allow modifying cellular data app settings (supervised devices only)	`allowAppCellularDataModification` If deselected, changes to cellular data usage for apps are disabled.	Yes
Allow modifying cellular plan settings (iOS 11.0 and later with supervised devices only)	`allowCellularPlanModification` If deselected, changes to cellular plan settings are disabled.	Yes
Allow modifying device name (supervised devices only)	`allowDeviceNameModification` If deselected, prevents device name from being changed. Available for iOS 9.0 or supported newer versions.	Yes
Allow modifying Find my Friends settings (supervised devices only)	`allowFindMyFriendsModification` If deselected, changes to the Find My Friends app are disabled.	Yes
Allow modifying notification settings (supervised devices only)	`allowNotificationsModification` If disabled, notification settings cannot be modified. Available for iOS 9.3 or supported newer versions.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow modifying passcode (supervised devices only)	`allowPasscodeModification` iOS 9.0 and later with supervised devices only. If deselected, prevents device passcode from being added, changed, or removed.	Yes
Allow modifying Touch ID fingerprints / Face ID faces (supervised devices only)	`allowFingerprintModification` If deselected, prevents device users from changing their TouchID or Face ID settings. This restriction is automatically deselected if the preceding restriction [**Allow modifying passcode (iOS 9.0 and later with supervised devices only)**] is deselected. Available for iOS 9.0 or supported newer versions.	Yes
Allow Screen Time (supervised devices only)	`allowEnablingRestrictions` For iOS 9.0- 11.x - If deselected, disables the "Enable Restrictions" option in Settings > Restrictions on iOS devices. For iOS 12.0 or supported newer versions - If this option is deselected, the "Enable Screen Screen Time" option on iOS devices will be disabled (Settings > Restrictions.)	Yes
Allow modifying Wallpaper supervised devices only)	`allowWallpaperModification` If deselected, prevents wallpaper from being changed. Available for iOS 9.0 or supported newer versions.	Yes
Allow modifying Personal Hotspot settings (iOS 12.2 and later with supervised devices only)	`allowPersonalHotspotModification` Deselecting disables the device user's ability to modify the personal hotspot. Available for iOS 12.2 or supported newer versions.	Yes
Allow changing USB restricted in Settings (supervised devices only)	`allowUSBRestrictedMode` Select to enable USB restricted mode. Available for iOS 12.0 or supported newer versions.	Yes
Allow pairing with non-Configurator hosts (supervised devices only)	`allowHostPairing` Select to allow host pairing for iTunes synchronization. Disabling this option disables all host pairing with the exception of the supervision host. If no supervision host certificate has been configured, all pairing is disabled. Host pairing lets the administrator control which devices an iOS device can pair with.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow documents from managed apps to unmanaged apps	`allowOpenFromManagedToUnmanaged` Select to allow documents in managed apps and accounts to be opened in unmanaged apps and accounts. Disabling this option prevents exchange of documents from managed to unmanaged apps and accounts. For example, you might want to keep enterprise documents from being opened with personal apps. ⓘ If you have enabled the "Open only with Ivanti Docs@Work, and protect with encryption" option for attachment control, it is recommended to disable this restriction. Enabling this restriction, may cause • .secure attachments to not open in Ivanti Mobile@Work . • .secure and .attachctrl attachments to not open in the Ivanti Docs@Work app for iOS. A '?' icon will be visible on the attachment. See "iOS managed app configuration" in the *Ivanti EPMM Apps@Work Guide.*	Yes
Allow documents from unmanaged apps to managed apps	`allowOpenFromUnmanagedToManaged` Select to allow documents in unmanaged apps and accounts to be opened in managed apps and accounts. Disabling this option prevents exchange of documents from unmanaged to managed apps and accounts. For example, you might want to keep users from sending personal documents using company email.	Yes
Treat AirDrop as unmanaged destination	`forceAirDropUnmanaged` If selected, AirDrop will not be displayed as a sharing destination. This prevents confidential data from being shared through AirDrop. This restriction requires deselecting the `allowOpenFromManagedToUnmanaged` restriction. Available for iOS 9.0 or supported newer versions.	Yes
Allow Handoff	`allowActivityContinuation` Select to enable the Handoff feature, which allows users to seamlessly continue working where they left off using any Apple device on which they are logged in with their Apple ID.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
	Available for iOS 8.0 or supported newer versions.	
Allow sending diagnostic and usage data to Apple	`allowDiagnosticSubmission` When deselected, this prevents the device from automatically submitting diagnostic reports to Apple.	Yes
Allow modifying diagnostics settings (supervised devices only)	`allowDiagnosticSubmissionModification` When deselected, the diagnostic submission and app analytics settings in the Diagnostics & Usage pane in Settings cannot be modified. Available for iOS 9.3.2 or supported newer versions.	Yes
Allow Touch ID / Face ID to unlock device	`allowFingerprintForUnlock` Selected (default) means a PIN is required instead of FaceID to unlock device. De-selected means the use of FaceID is allowed in place of a PIN.	Yes
Force Apple Watch Wrist Detection	`forceWatchWristDetection` If selected, paired Apple Watches are forced to use the wrist detection feature. Wrist detection allows the WatchOS to determine when the watch is being worn, and enable security features (such as a passcode) accordingly. Available for iOS 8.2 or supported newer versions.	No
Allow pairing with Apple Watch (supervised devices only)	`allowPairedWatch` If deselected, the device user will not be able to pair their device with an Apple Watch. Currently paired Apple Watches are unpaired and erased. Available for iOS 9.0 or supported newer versions.	Yes
Require passcode on first AirPlay pairing	`forceAirPlayOutgoingRequestsPairingPassword` If set to true, forces all devices receiving AirPlay requests from this device to use a pairing password when pairing for the first time.	No
Allow setting up new nearby devices (iOS 11.0 and later with supervised devices only)	`allowProximitySetupToNewDevice` If deselected, device users cannot use their Apple devices to set up and configure other Apple devices. Available for iOS 11.0 or supported newer versions.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow AirPrint (iOS 11.0 and later and supervised devices only)	`allowAirPrint` When deselected, disables Air Print feature. Available for iOS 11.0 or supported newer versions.	Yes
Allow storage of AirPrint credentials in Keychains (iOS 11.0 and later with supervised devices only)	`allowAirPrintCredentialsStorage` Supervised only. When disabled, prohibits keychain storage of username and password for Airprint. Available for iOS 11.0 or supported newer versions.	Yes
Disallow AirPrint to destinations with untrusted certificates (iOS 11.0 and later with supervised devices only)	`forceAirPrintTrustedTLSRequirement` When selected, requires trusted certificates for TLS printing communication. Available for iOS 11.0 or supported newer versions.	No
Allow discovery of AirPrint printers using iBeacons (iOS 11.0 and later and supervised devices only)	`allowAirPrintiBeaconDiscovery` When selected, disables iBeacon discovery of AirPrint printers, preventing spurious AirPrint Bluetooth beacons from phishing for network traffic. Available for iOS 11.0 or supported newer versions.	Yes
Allow predictive keyboard (supervised devices only)	`allowPredictiveKeyboard` If deselected, disables the predictive keyboard. Available for iOS 8.1.3 or supported newer versions.	Yes
Allow keyboard shortcuts (with supervised devices only)	`allowKeyboardShortcuts` If deselected, keyboard shortcuts cannot be used. Available for iOS 9.0 or supported newer versions.	Yes
Allow auto correction (supervised devices only)	`allowAutoCorrection` If deselected, disables keyboard auto-correction. Available for iOS 8.1.3 or supported newer versions.	Yes
Allow spell check (supervised devices only)	`allowSpellCheck` If deselected, disables spell check. Available for iOS 8.1.3 or supported newer versions.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow Define (supervised devices only)	`allowDefinitionLookup` If deselected, disables definition look-up. Available for iOS 8.1.3 or supported newer versions.	Yes
Allow dictation (iOS 10.3 and later with supervised devices only)	`allowDictation` When deselected, disables dictation input method. Disabled automatically when using Advanced Audio Coding (AAC) mode. Available for iOS 10.3 or supported newer versions.	Yes
Allow Wallet notifications in Lock screen	`allowPassbookWhileLocked` If deselected, Wallet notifications will not be shown on the lock screen.	Yes
Show Control Center in Lock screen	`allowLockScreenControlCenter` If disabled, prevents Control Center from appearing on the Lock screen.	Yes
Show Notification Center in Lock screen	`allowLockScreenNotificationsView` If deselected, the Notifications view in Notification Center on the lock screen is disabled.	Yes
Show Today view in Lock screen	`allowLockScreenTodayView` If deselected, the Today view in Notification Center on the lock screen is disabled.	Yes

Defer software updates for __days (iOS 11.3, tvOS 12.2 and later with supervised devices only)	`enforcedSoftwareUpdateDelay`
	`forceDelayedSoftwareUpdates`
	
	Enter the number of days by which you want to defer software updates. The default is 30 days, and the maximum is 90 days.
	
	Available for iOS 11.3 and tvOS 12.2 or supported newer versions.
		No

Force Password on AirPlay incoming requests (tvOS up to 10.1)	`forceAirPlayIncomingRequestsPairingPassword` Select to force the usage of a password for all AirPlay incoming requests for device pairing. Available for tvOS 11.3 or supported newer versions.	No
Allow incoming AirPlay requests (tvOS 11.3 and later)	`allowAirPlayIncomingRequests` Select to allow incoming AirPlay requests. Available for tvOS 11.3 or supported newer versions.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow pairing with Remote app (tvOS 11.3 and later)	`allowPairingRemoteApp` Select to allow pairing with a remote app. Available for tvOS 11.3 or supported newer versions.	Yes
Force automatic date & time setting (iOS 12.0, tvOS 12.2 and later with supervised devices only)	`forceAutomaticDateAndTime` When selected, the user cannot turn it off. Note that the device's time zone will only be updated when the device can determine its location. Available for iOS 12.0 and tvOS 11.3 or supported newer versions.	No
Allow AutoFill Password (iOS 12.0 and later with supervised devices only)	`allowPasswordAutoFill` Select to allow password autofill. Available for iOS 12.0 or supported newer versions.	Yes
Allow nearby devices to request passwords (iOS / tvOS 12.0, and later with supervised devices only)	`allowPasswordProximityRequests` Select to allow nearby devices to request device passwords. Available for iOS 12.0 and tvOS 12.0 or supported newer versions.	Yes
Allow users to share their passwords using AirDrop Passwords feature (iOS 12.0 and later with supervised devices only)	`allowPasswordSharing` Select to allow users to share their device passwords using Airdrop Passwords feature. Available for iOS 12.0 or supported newer versions.	Yes
Allow managed apps to write contacts to unmanaged contacts account (iOS 12.0 and later)	`allowManagedToWriteUnmanagedContacts` Select to allow managed apps to write contacts to unmanaged contacts account. Available for iOS 12.0 or supported newer versions.	Yes
Allow unmanaged apps to read from managed contacts account (iOS 12.0 and later)	`allowUnmanagedToReadManagedContacts` Select to allow unmanaged apps to read from managed contacts account. Available for iOS 12.0 or supported newer versions.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Allow modifying the eSim configuration (iOS 12.1 and later with supervised devices only)	`allowESIMModification` Select to allow modifying the eSim configuration, which allows adding or removing a cellular plan. Available for iOS 12.1 or supported newer versions.	Yes
Allow continuous path keyboard (iOS 13.0 and later with supervised devices only)	`allowContinuousPathKeyboard` Select to allow continuous path keyboard on supervised devices. Available for iOS 13.0 or supported newer versions.	Yes
Allow device sleep (tvOS 13.0 and later with supervised devices only)	`allowDeviceSleep` Select to allow device to sleep. Available for tvOS 13.0 or supported newer versions.	Yes
Allow Find My Device (iOS 13.0 and later with supervised devices only)	`allowFindMyDevice` Select to allow Find My Device in the Find My app for supervised devices. Available for iOS 13.0 or supported newer versions.	Yes
Allow Find My Friends (iOS 13.0 and later with supervised devices only)	`allowFindMyFriends` Select to allow Find My Friends for supervised devices. Available for iOS 13.0 or supported newer versions.	Yes
Force Wi-Fi power on (iOS 13.0 and later with supervised devices only)	`forceWiFiPowerOn` Select to force Wi-Fi power on/off for supervised devices. Available for iOS 13.0 or supported newer versions.	No
Allow USB drive access in Files app (iOS 13.0 and later with supervised devices only)	`allowFilesUSBDriveAccess` Select to allow USB drive access in Files app. Available for iOS 13.0 or supported newer versions.	Yes
Allow Network drive access in Files app (iOS 13.0 and later with supervised devices only)	`allowFilesNetworkDriveAccess` Select to allow network drive access in the Files app. Available for iOS 13.0 or supported newer versions.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Join only WiFi networks installed by a WiFi payload (iOS 14.5 and later supervised devices only)	`forceWiFiToAllowedNetworksOnly` If selected, limits device to only join Wi-Fi networks set-up via configuration profile. Requires a supervised device.	No
Allow auto unlock (iOS 14.5 and later)	`allowAutoUnlock` Selected by default, allows the ability to unlock Face ID-enabled phone with an associated Apple Watch. If deselected, disallows auto unlock.	Yes
Allow putting into recovery mode from an unpaired device (iOS 14.5 and later supervised only)	`allowUnpairedExternalBootToRecovery` If selected, allows devices to be booted into recovery by an unpaired device. Requires a supervised device.	No
Force Translation Processing Only on Device (iOS 15.0 and later)	`forceOnDeviceOnlyTranslation` When selected, the device will not connect to Siri servers for translation.	No
Require Managed Pasteboards (iOS 15.0 and later)	`requireManagedPasteboard` Select to make device users' copy and paste managed. If not selected, device users will see a "paste not allowed" notification when trying to paste content from a managed app.	No
Allow Cloud Private Relay (iOS 15.0 and later)	`allowCloudPrivateRelay` When selected, allows device to use iCloud Private Relay, making all browser traffic encrypted.	Yes
Allow Mail Privacy Protection (iOS 15.2 and later)	`allowMailPrivacyProtection` If de-selected, disables Mail Privacy Protection on the device. Selected, this optin helps protect device users' privacy by preventing senders from learning about device users' email activities. When the Allow Mail Privacy Protection configuration is installed and enabled from Ivanti EPMM, the Protect Mail Activity toggle is enabled on the device and the following options are visible to the device user:	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
	• Hide IP Address - The email sender cannot link the email to the device user's online activity or determine location. • Block All Remote Content - Prevents the email sender from seeing the device user's email activities.	
Allow Apple TV's automatic screen saver (tvOS 15.4 and later)	`allowAutomaticScreenSaver` If de-selected, disables Apple TV's automatic screen saver.	Yes
Allow Rapid Security Response Installation (iOS 16.0 and later supervised devices only)	`allowRapidSecurityResponseInstallation` To disable the responses. The user cannot install rapid security responses. Administrators can use the iOS or macOS policies software updates to update devices to the latest Rapid Security Response updates. Use the **Update to the latest version** option. The **Update to a specific version** option is not supported in iOS for Rapid security response update formats from either the iOS Software update policy or the **Device** actions menu.	Yes
Allow Rapid Security Response Removal (iOS 16.0 and later supervised devices only)	`allowRapidSecurityResponseRemoval` To block the user from being able to undo the responses. The user cannot remove rapid security responses. This feature can be used once Apple implements the functionality.	Yes
Allow iPhone widgets on a Mac (iOS 17 and later supervised devices only)	`allowiPhoneWidgetsOnMac` Select to allow the iPhone widget on Mac 14 devices. Deselect to disallow iPhone widget on Mac 14 devices. Note: Both are signed in with the same Apple ID.	Yes
Application Restrictions		
Allow Use of iTunes Store	`allowiTunes`	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
	When deselected, the iTunes Music Store is disabled and its icon is removed from the Home screen. Users cannot preview, purchase, or download content.	
Allow News (supervised devices only)	`allowNews` If deselected, prevents the device user from accessing News. Available for iOS 9.0 or supported newer versions.	Yes
Allow Podcasts (supervised devices only)	`allowPodcasts` Select to display the default Apple Podcast app. Deselect to hide the Apple Podcast app. Available for iOS 8.0 or supported newer versions.	Yes
Allow use of Game Center (supervised devices only)	`allowGameCenter` When deselected, Game Center is disabled and its icon is removed from the Home screen.	Yes
Allow multiplayer gaming	`allowMultiplayerGaming` When deselected, prohibits multiplayer gaming. Disabled when **Allow use of Game Center** is deselected.	Yes
Allow adding Game Center friends	`allowAddingGameCenterFriends` When deselected, prohibits adding friends to Game Center. Disabled when **Allow use of Game Center** is deselected.	Yes
Allow use of Safari	`allowSafari` Deselect to disable the Safari web browser, remove its icon from the Home screen, and prevent users from opening web clips. When deselected, the following restrictions are also disabled: Enable autofill, Force fraud warning, Enable Javascript, Block pop-ups, Accept cookies. ⓘ Safari is required for updating configurations on iOS devices that are not managed with Apple's MDM protocol.	Yes
Enable autofill	`safariAllowAutoFill` Select to turn on the autofill feature for fields displayed in Safari.	Yes

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
Force authentication before AutoFill (iOS 11.3 and later with supervised devices only, Face ID only)	`forceAuthenticationBeforeAutoFill` Select to require Face ID authentication before AutoFill Available for iOS 11.3 or supported newer versions.	Yes
Force fraud warning	`safariForceFraudWarning` Select to prompt Safari to attempt to prevent users from visiting websites identified as being fraudulent or compromised.	No
Enable Javascript	`safariAllowJavaScript` Select to turn on Javascript support for Safari.	Yes
Block pop-ups	`safariAllowPopups` Select to block pop-ups for Safari.	No
Accept cookies	`safariAcceptCookies` Select an option from the drop-down list to control when Safari browser accepts cookies on devices. Options include Never, From visited sites, From Websites I Visit, and Always.	Always
Media Content Ratings		
Ratings region	Select a region from the drop-down list to change the region associated with the rating selections for applications, TV shows, and movies.	United States
Allowed content ratings: Movies	Select a rating limit for movies stored on the device: Don't Allow Movies G PG PG-13 R NC-17 Allow All Movies	Allow All Movies
Allowed content ratings: TV Shows	Select a rating limit for TV shows stored on the device: Don't Allow TV Shows TV-Y TV-Y7 TV-G	Allow All TV shows

TABLE 112. RESTRICTIONS SETTINGS (IOS) (CONT.)

Item	Description	Enabled by default
	TV-PG TV-14 TV-MA Allow All TV Shows	
Allowed content ratings: Apps	Select a rating limit for applications on the device: Don't Allow Apps 4+ 9+ 12+ 17+ Allow All Apps	Allow All Apps
Allow playback of explicit music, podcasts, & iTunes U media (iOS and tvOS 11.3 and later)	`allowExplicitContent` When de-selected, explicit music or video content purchased from the iTunes Store is hidden. Explicit content is marked as such by content providers, such as record labels, when sold through the iTunes Store. Available for iOS 11.3 and tvOS 11.3 or supported newer versions.	Yes
Allow explicit sexual content in iBooks Store (iOS and tvOS 11.3 and later)	`allowBookstoreErotica` Select to allow users to download iBookstore material that has been tagged as erotica. Available for iOS 11.3 and tvOS 11.3 or supported newer versions.	Yes

TABLE 113. RESTRICTIONS SETTINGS (IOS)

Item	Description	Enabled by default
App whitelist for Single App Mode	Specify a list of apps that can autonomously enter single app mode on supervised devices running iOS 7-9.1. For example, you can specify custom exam apps for students. As soon as the student launches the app, the app enters single app mode to ensure that the student cannot use other resources while taking the exam. **This feature applies to supervised iOS devices only, and apps with the ability to autonomously enter single-app mode.** Use the following guidelines to complete each entry: • Enter the app name defined in the app's bundle. • Enter the bundle identifier for this app. One way to find the bundle identifier is to add the app to the App Catalog in Ivanti EPMM. After you add the app, edit the app entry to see the Inventory Apps field, which lists the bundle ID for the app. • Enter an optional description for the app. ⓘ This feature is different from single-app mode policy, which enables an administrator to configure a specific app to run in single-app mode on devices to the exclusion of any other apps. For more information about setting a single-app mode policy, see "Single-app mode policies" on page 288.	N/A

Subscribed Calendars settings

Select **Policies & Configs > Configurations > Add New > Apple > iOS / tvOS > Subscribed Calendars** to configure read-only calendar subscriptions for the device's Calendar application.

A list of public calendars you can subscribe to is available at www.apple.com/downloads/macosx/calendars/.

ⓘ   This setting does not apply to tvOS devices.

The following table describes the settings for subscribed calendars.

TABLE 114. SUBSCRIBED CALENDARS SETTINGS (IOS)

Item	Description
Name	Enter brief text that identifies this group of iOS subscribed calendar settings.
Description	Enter additional text that clarifies the purpose of this group of iOS subscribed calendar settings.
URL	Enter the URL for accessing the subscribed calendar.
Use SSL	Select to use SSL for data transfer.
User Name	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format. $MANAGED_APPLE_ID$ can be used for Shared iPad devices and User Enrolled devices only. Custom attribute variable substitutions are supported. **Why:** Some enterprises have a strong preference concerning which identifier is exposed. See "Supported variables" below.
Password	Specify the password to use. The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$. Custom attribute variable substitutions are supported. See "Supported variables" below.

iOS devices accept settings for up to four subscribed calendars. Therefore, any additional calendar settings applied to an iOS device will be ignored.

Supported variables

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

- $USERID$

- $EMAIL$

- $NULL$

- $MANAGED_APPLE_ID$

  > ⓘ   This can be used for Shared iPad devices and User Enrolled devices only.

- $USER_CUSTOM1$... $USER_CUSTOM4$ (custom fields defined for LDAP)

Custom attribute variable substitutions are supported.

APN settings

Select **Policies & Configs > Configurations > Add New > Apple > iOS / tvOS > APN** to define parameters for access point interactions, which define how the device accesses the operator's network.

IMPORTANT:

- Apple disabled APN settings in iOS 9.0, but re-enabled APN settings in iOS 9.0.1. Apple has replaced the APN setting with a cellular policy. Ivanti, Inc strongly recommends creating a cellular policy for new configurations. To create a cellular policy, see "Cellular policies" on page 295.

- Ivanti EPMM supports the use of APN settings for iOS devices running iOS 7 through iOS 8.4, as well as iOS 9.0.1 through iOS 9.0.2. APN settings cannot be used on iOS 9.0 devices, as Apple does not support APN settings on iOS 9.0.

APN settings do not apply to macOS devices.

ⓘ   This setting does not apply to tvOS devices.

The following table describes the APN settings.

TABLE 115. APN SETTINGS (IOS)

Item	Description
Access Point Name	Identifier available from the operator.
Description	Enter additional text that clarifies the purpose of this group of iOS APN settings.
User Name	Enter a user name authorized for this access point.
Password	Enter the password corresponding to the user name entered.
Proxy Server	Enter the IP address or URL of the APN proxy.
Port	Enter the port number of the APN proxy.

Cellular Private Network

Ivanti EPMM added a new Cellular Private Network configuration to support iOS 17 or above devices. EPMM allows you to configure several settings to geofence and to prefer cellular over Wi-Fi for security purposes.

Some device settings for an organisation's private 5G and LTE network can be configured using an MDM solution or a configuration profile containing a Private Mobile Network payload. Only one Private Mobile Network payload is supported at a time.

Configuring cellular private network

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select **Add New > Apple > iOS / tvOS > Cellular Private Network**. The Add Cellular Private Network dialog box opens.

3. Configure the settings as described in Cellular Private Network settings.

4. Click **Add +** to add a new row for **Geofences** configuration as described in Geofence properties. Ivanti EPMM allows to add 1000 rows to define geolocation for private network activation.

5. Click **Save**.

The following table summarizes the cellular private network settings:

Item	Description	Enable by default
Name	Enter a name for the cellular private network configuration.	N/A
Description	Enter a brief description that explains the purpose of this configuration.	N/A
Cellular Data Preferred (Boolean)	Set to true to prefer this private network over Wi-Fi.	False
Data Set Name (String) (Required)	The name of the private network configuration data set.	N/A
Enable NR Standalone (Boolean)	Set to true if this private network is NR Standalone.	False

Item	Description	Enable by default
Version Number (String) (Required)	The version number of this dataset that the system uses to track updates.	N/A

The following table summarizes the Geofence properties:

Item	Description
Geofence Id (String) (Required)	A geofence identifier that's unique within a list of geofences.
Latitude (Number) (Required)	The latitude of the geofence. Minimum Value: -90 Maximum Value: 90 .
Longitude (Number) (Required)	The longitude of the geofence. Minimum Value: -180 Maximum Value: 180
Radius (Number) (Required)	Specifies the radius of the geofence in meters. Set this value slightly greater than the private cellular network coverage area. Minimum Value: 100 Maximum Value: 6500

Network Relay

Network relays work as a replacement for VPNs. Administrators can configure relays to access private company resources without needing tunnels or VPNs.

A new built-in relay supports secure and transparent tunnelling of traffic as an alternative to using a VPN when accessing internal resources. Using the new `com.apple.relay.managed` payload, a secure HTTP/3 or HTTP/2 relay can be configured to proxy all TCP and UDP traffic. The configuration allows defining match and exclusion domains and can apply to managed apps, domains, or the entire device.

Configuring network relay

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select **Add New> Apple > iOS / tvOS > Network Relay**. The Add Network Relay dialog box opens.

3. On the Add Network Relay page, provide the details for the following fields:

   - Name: Enter the relay name.

   - Description: Enter the description.

   - Click **Add Network Relay Settings** to add multiple network relay settings.

   - Network Relay Settings: Enter the following details:

     ◦ HTTP/3 Relay URL: Enter the URL.

     ◦ HTTP/2 Relay URL: Enter the URL.

     ◦ In the **Additional HTTP Headers Fields** section, click **Add +** to add additional header fields.

     ◦ In the **Certificate** field, click the drop down to select a certificate.

     ◦ Click **Add +** to add raw public keys.

     ◦ Click **Save**.

   - In the **Match Domains** section, click **Add +** to add domains, which can apply to managed apps.

   - In the **Excluded Domains** section, mention the excluded domains, which can apply to managed apps.

4. Click **Save**.

Provisioning Profile settings

A provisioning profile is a file containing verification information for an app. Apps are not usable on iOS without a current provisioning profile. There are two types of provisioning profile: app-specific, and wildcard, which works for more than one app. Provisioning profiles are required for distributing in-house apps through the Ivanti EPMM Admin Portal.

> **i** This setting does not apply to tvOS devices.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Click **Add New > Apple > iOS / tvOS > Provisioning Profile**. The New Provisioning Profile Setting dialog box opens.

3. In the space provided, enter a name and description for the provisioning profile, such as MyInHouseApp1Prov and "Provisioning profile for in-house app 1".

4. Click **Choose File**.

5. Browse for the provisioning profile and click **Open**.

6. Click **Save**.

7. Select the provisioning profile you created.

8. Select **Actions > Apply to Label**.

9. Select the labels to which you want to apply the provisioning profile, such as **iOS**.

10. Click **Apply**.

Web content filter settings

Starting with iOS 7, supervised iOS devices support web content filtering. Web content filtering restricts the web sites that any browser on a supervised device can access. This feature is useful, for example, in fleet-based lock down environments, such as retail stores or schools.

Ivanti EPMM supports configuring web content filters on the Admin Portal. You can do one of the following:

- Block access to sites containing adult content.

- Configure the device's set of accessible sites.

> **i** This setting does not apply to tvOS devices.

Configuring the web content filter

Procedure

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

2. Select **Add New > iOS / tvOS > Web Content Filter**. The New Web Content Configuration dialog box opens.

3. Use the following guidelines to create or edit a web content configuration:

TABLE 116. WEB CONTENT FILTER CONFIGURATION SETTINGS

Item	Description
Name	Enter brief text that identifies this web content configuration.
Description	Enter additional text that clarifies the purpose of this web content configuration.
Allowed Websites	• Limit Adult Content - Select this option if you want to block access to web sites based on iOS automatic filters. These filters attempt, with a high degree of accuracy, to block websites with inappropriate content. • Specific Web Sites Only - Select this option if you want to manually list the accessible web sites.
Permitted URLs	Available only if you selected Limit Adult Content. These URLs are accessible even if the iOS automatic filters block them.
	To add a permitted URL, select **+**. To delete a permitted URL, select -. You can add up to 50 permitted URLs.
URL	Enter the permitted URL. The URL must begin with either: • http:// • https:// ⓘ If you want to permit both http:// and https:// for the same site, include a row for each URL.

TABLE 116. WEB CONTENT FILTER CONFIGURATION SETTINGS (CONT.)

Item	Description
	All URLs for which the initial characters match the given permitted URL are accessible.
	Example:
	http://www.someCompanySite.com
	permits access to the following:
	http://www.someCompanySite.com
	http://www.someCompanySite.com/jobs
	http://www.someCompanySite.com/products
Description	Enter additional text that clarifies the purpose of this permitted URL.
Blacklisted URLs	Available only if you selected Limit Adult Content.
	These URLs are blocked even if the iOS automatic filters allow them.
	To add a blacklisted URL, select +.
	To delete a blacklisted URL, select -.
	You can add up to 50 blacklisted URLs.
URL	Enter the blacklisted URL. The URL must begin with either:
	• http://
	• https://
	ⓘ If you want to block both http:// and https:// for the same site, include a row for each URL.
	All URLs for which the initial characters match the given Blocklisted URL are blocked.
	Example:
	http://www.someCompanySite.com
	blocks access to the following:
	http://www.someCompanySite.com
	http://www.someCompanySite.com/jobs
Description	Enter additional text that clarifies the purpose of this blacklisted URL.

TABLE 116. WEB CONTENT FILTER CONFIGURATION SETTINGS (CONT.)

Item	Description
Specific Websites	Available only if you selected Specific Web Sites Only.
	These URLs are the only accessible sites. Any existing bookmarks on Safari are disabled.
	To add an accessible URL, select +.
	To delete an accessible URL, select -.
URL	Enter the URL of a website you want to make accessible. The URL must begin with either:
	• http://
	• https://
	ⓘ If you want to make both http:// and https:// for the same site accessible, include a row for each URL.
	If you are using the Apps@Work or Secure Sign-in web clips, include an entry for the URL of Ivanti EPMM. Otherwise, these web clips will not work.
Name	The title of the bookmark in Safari.
Bookmark	Optionally enter the folder into which the bookmark should be added in Safari.
	Example:
	/Sales/Products/
	If absent, the bookmark is added to the default bookmarks directory.
Description	Optionally enter additional text that clarifies the purpose of this URL.

4. Select **Save**.

5. Select the web content configuration you just created.

6. Select **Actions > Apply To Label**.

7. Select the labels to which you want to apply this web content configuration.

8. Select **Apply**.

Browser impact

The web content filter feature impacts *all browsers and web views* on the device including:

- Safari

  When using the option "Specific Web Sites Only", only Safari displays the bookmarks that you specify. Other browsers do not.

- Ivanti Web@Work

- Apps@Work

- the Secure Sign-in web clip

- other browsers and web views

Therefore, if you use the option "Specific Web Sites Only", be sure to include the URL for your Ivanti EPMM so that the Apps@Work and Secure Sign-in web clips work.

Removing a Web content configuration from a device

A web content configuration is removed from a device when:

- You remove the label associated with the device from the setting, and the device checks in.

- You remove the web content configuration, and the device checks in.

- You retire the device.

Multiple web content configurations on a device

If you apply multiple web content configurations to a device, web access works as follows:

- The URL is accessible only if *all* of the web content configurations on the device allow it and *none* of the web content configurations block it.

- The URL is blocked if *any* of the web content configurations block it.

Managed App Config settings that use plists

An additional license is required for this feature.

Select **Policies & Configs > Configurations > Add New > Apple > iOS / tvOS > Managed App Config** to provide app configuration to a managed app. In this setting, you provide a property list (plist) file as specified by the app vendor or developer.

When a managed app gets its configuration from Ivanti EPMM, the device user does not have to manually enter the configuration. This feature results in easier app deployment and fewer support calls for you, and a better user experience for the device user.

Note the following:

- This setting does not apply to tvOS devices.

- The AppConfig Community (AppConfig.org) describes another mechanism for managed app configuration. Using the AppConfig Community mechanism on Ivanti EPMM is described in in "Managed App Configuration settings in the app in the App Catalog" in the *Ivanti EPMM Apps@Work Guide.*

- By default, the managed app configuration settings in the app in the App Catalog (AppConfig Community mechanism) override the Managed App Config setting that uses a plist. However, you can specify that the Managed App Config setting has precedence, as described in "Precedence of the iOS managed app configuration in the App Catalog versus the Managed App Config setting" in the*Ivanti EPMM Apps@Work Guide.*

Managed App Config with plist overview

Providing a managed app with an app configuration involves these high-level steps:

1. You get a plist file containing the app configuration from the app vendor or developer. The plist is a text file in XML format.

2. Edit the file as directed by the app's managed app configuration documentation. For example, documentation can instruct you to replace a default server value in the plist with a URL for one of your enterprise servers.

3. You create a Managed App configuration setting on Ivanti EPMM.

4. When you create the setting, you upload the plist file to Ivanti EPMM.

5. You apply labels to the setting to indicate which devices the setting applies to.

6. Ivanti EPMM sends the setting to the device when the device checks in.

7. The managed app installed on the device accesses the configuration using iOS programming interfaces.

ⓘ You can apply a Managed App Config setting to a device before the app is installed on the device. When the app is installed, it accesses the configuration. Until then, the configuration has no impact on the device.

Configuring the Managed App Config setting

Before you begin

Edit the provided plist with values specific to your enterprise, as directed by the app documentation. You can use any text editor or plist editor. Put the edited plist file into a folder accessible from your Admin Portal.

Procedure

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

2. Select **Add New > Apple > iOS / tvOS > Managed App Config**. The New Managed App Config Setting dialog box opens.

3. Use the following guidelines to create or edit a Managed App Config setting:

Item	Description
Name	Enter brief text that identifies this Managed App Config setting.
Description	Enter additional text that clarifies the purpose of this Managed App Config setting.
BundleId	Enter the bundle ID of the managed app.
File	Select Choose File. Select the plist file that contains the app configuration for the app. ⓘ Ivanti EPMM does not validate the plist file's type or contents.

4. Select **Save**.

5. Select the Managed App Config setting you just created.

   Ivanti EPMM assigns the setting the type MDM APP CONFIG.

6. Select **Actions > Apply To Label**.

7. Select the labels you want to apply this Managed App Config setting to. For Shared iPad devices, select either **Allow only Temporary Session** or **Set Timeout for User Session - Seconds**.

8. Select **Apply**.

Note the following:

- You cannot edit the Managed App Config setting, including uploading a different plist file. If changes are necessary, delete the Managed App Config setting and create a new one. Be sure to re-apply labels.

- You can apply only one Managed App Config setting for each app to each device, including when more than one version of the app is installed on a device.

- The configuration information is not encrypted on the device. The configuration should therefore not contain any sensitive information, such as passwords or private keys.

Viewing the plist file

Procedure

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

2. Select a Managed App Config setting.

3. Select **View File Data in App Settings Detail** pane.

   A pop-up displays the file contents.

4. Close the pop-up when you are done viewing the file contents.

Removing a Managed App Config setting from a device

A Managed App Config setting is removed from a device when:

- You remove the label associated with the device from the setting, and the device checks in.

- You remove the Managed App Config setting, and the device checks in.

- You retire the device.

When the Managed App Config setting is removed, the managed app automatically removes its use of the configuration.

Supported variables

The plist can use the Ivanti EPMM variables described in the following table:

TABLE 1. IVANTI EPMM VARIABLES FOR PLIST FILES

Variable	Description
$DEVICE_MAC$	The Wi-Fi MAC (Media Access Control) address of the device.
$DEVICE_UDID$	The unique device identifier of the device.
$DISPLAY_NAME$	The display name of the device user.
$EMAIL$	The email address of the device user. ℹ️ $MANAGED_APPLE_ID$ needs to be used for Shared iPad devices and User Enrolled devices only.
$FIRST_NAME$	The first name of the device user.
$LAST_NAME$	The last name of the device user.
$USERID$	The user ID of the device user. ℹ️ $MANAGED_APPLE_ID$ needs to be used for Shared iPad devices and User Enrolled devices only.

When Ivanti EPMM sends the configuration to a device, it substitutes the appropriate values for the variables.

Sample plist

A plist is a text file in XML format. The XML content vary for each app, and the contents have been validated by the app developer. The following is a sample plist, included here only to illustrate the format you can expect:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
```

```
<plist version="1.0">
<dict>
    <key>Server</key>
    <string>http://www.somecompanyserver.com</string>
    <key>Some Dict</key>
    <dict>
        <key>A</key>
        <string>$DISPLAY_NAME$</string>
        <key>C</key>
        <string>$DEVICE_UDID$</string>
    </dict>
    <key>Some Array</key>
    <array>
        <string>abc</string>
        <string>val</string>
        <string>$DEVICE_MAC$</string>
    </array>
</dict>
</plist>
```

Google Account

You can set up a Google email account for communication service rules for an audio service. All calls initiated on iOS devices to the contacts on the Google contact list will be using the default audio service. Each Google payload sets up a Google email address as well as any other Google services the device user enables after authentication.

Procedure

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

2. Select **Add New > Apple > iOS and tvOS > Google Account**.

3. In the New Google Account Configuration dialog box, enter the following:

Item	Description
Name	Enter brief text that identifies this email account.
Description	Enter additional text that clarifies the purpose of this Google account.

Item	Description
Google Account Name	When an email is sent from this Google account, the name entered here displays who the email is from.
	You can use substitution variables in this field. Ivanti, Inc recommends using $DISPLAY_NAME$.
Email Address	Enter the Google email address of this account. Typically, you use the Ivanti EPMM substitution variable $EMAIL$.
	$MANAGED_APPLE_ID$ can be used for Shared iPad devices and User Enrolled devices only.
	For more information on substitution variables, see "Custom compliance policies" on page 355.
Communication Service Rules (iOS 10 and Later)	Select a default audio service or app to be associated with the device user's accounts on the Google servers. All calls initiated on the iOS device to contacts from contact lists stored on the server will use the selected audio service by default. This feature is supported on devices running iOS 10 or supported newer versions.
	To enable communication service rules:
	• Select **Choose a default app to be used when calling contacts from this account**. A drop-down list of apps is displayed.
	• Select the drop-down list to select the default audio app or service.

4. Select **Save**.

5. In the Configurations page, select the box next to the Google email account configuration you created, and select **Actions > Apply To Label**.

6. In the Apply to Label dialog box, select the label(s) to which you want to apply the Google email account and select **Apply**.

Once pushed to devices, the device user is invited to go to Settings > Passwords & Accounts to enter the password to the Google email account.

Managed domains settings

Managed domains enable you to specify which domains are trusted for Mail and Safari on iOS and macOS devices. Once the configuration is applied to the device:

- Email from domains that are not specified in the configuration will be highlighted (untrusted) in the native Mail app.

- Documents downloaded from domains that are specified in the configuration will be considered managed for the purposes of the Safari on the device. Use this configuration combined with restrictions to control the data downloads allowed in Safari.

- Device users will be unable to use the Safari autofill feature for passwords unless the URLs they access have been specifically configured as managed Safari password autofill domains.

Managed domains work together with the managed app options in the restrictions configuration. Ivanti EPMM requires a special license for using these options.

> ℹ️ This setting does not apply to tvOS devices.

Configuring managed domains

Procedure

1. In the Admin Portal, select **Policies & Configs.**

2. Select **Add New > Apple > iOS / tvOS > Restrictions**. The New Restrictions Setting dialog box opens.

3. Create a restrictions configuration with at least the following settings not checked:

   - **Allow documents from managed apps to unmanaged apps**

   - **Allow documents from unmanaged apps to managed apps**

4. Apply the configuration to an appropriate label to distribute it to target devices.

5. In the Admin Portal, select **Policies & Configs > Configurations**.

6. Select **Add New** > **Apple > iOS / tvOS > Managed Domains**. The Managed Domains Configuration dialog box opens.

7. Use the following guidelines to complete the form:

Item	Description
Name	Enter brief text to identify this configuration. Note that this text will display in the iOS Settings app on the device.
Description	Enter optional text to clarify the purpose of this configuration.
Email Domains	Select **Add+** to enter an email domain, such as mycompany.com. Email domains may not include the wild card format "/*". Any email address lacking a suffix specified in the list of managed email domains will be highlighted as out-of-domain in the Mail app. Note that the www prefix and trailing slashes are ignored.
Web Domains	Select **Add+** to enter a web domain, as in mycompany.com. Note that the www prefix and trailing slashes are ignored. See "Domain formats" on the next page for more information.
Managed Safari Password Auto Fill Domains (iOS 9.3+ Supervised Only)	Select **Add+** to enable password auto-fill and auto-save for URLs matching a specific Safari web domain. Supported on supervised devices running iOS 9.3 or supported newer versions. Notes: • The managed Safari password auto-filled domain feature is disabled on multi-user devices. • Safari will only save and auto-fill passwords on web pages that are configured for auto-fill. Password auto-fill will not work on domains where auto-fill is not configured, even if you add the domain to the list. • The www prefix and trailing slashes are ignored. • If a managed Safari password auto-fill domain contains a port number, Safari will only manage URLs that specify that port number. Otherwise, the domain will be matched without regard to the specified port number. For example, the pattern `*.example.com:8080` will match `http://site.example.com:8080/page.html`, but not `http://site.example.com/page.html`. The pattern `*.example.com` will match both URLs.

Item	Description
	• Be sure to enable saving passwords on all iOS devices before enabling this feature. On the iOS device, select **Settings** > **Safari** > **Autofill** > **Names and Passwords** > **Enable**.

8. Apply the configuration to an appropriate label to distribute it to target devices.

Domain formats

Use the following table as a guideline for entering both web domains and managed Safari password auto-fill domains:

TABLE 1. WEB DOMAIN AND MANAGED SAFARI PASSWORD AUTO-FILL DOMAIN FORMATS

Enter	To match	To exclude
company.com	company.com/*	site.company.com/
site.company.com	site.company.com/*	company.com/ site2.company.com/
*.company.com	site.company.com/* site2.company.com/*	company.com/
company.com/folder	company.com/folder/*	company.com/
*.company.com/folder	foo.company.com/folder bar.company.com/folder	company.com foo.company.com/
foo.company.com/folder	foo.apple.com/folder foo.apple.com/folder2 foo.apple.com/folder/folder	company.com company.com/sub foo.company.com/ bar.company.com/folder
*.co	company.co beats.co company.co/folder	company.co.uk company.com

ℹ️ If you specify a port number, then only addresses that specify that port number will be matched. Otherwise, port 80 will be assumed for http and port 443 will be assumed for https.

Managed domains example

Acme, Inc. wants to use managed domains to do the following:

- provide a cue to users who are about to email content outside of Acme, Inc.
- prevent users from emailing confidential documents downloaded from their website

They have created the following managed domain configuration and assigned it to a label that identifies all iOS 8 devices:

FIGURE 1. MANAGED DOMAINS CONFIGURATION EXAMPLE

They have also created a restrictions configuration and assigned it to the same label as the managed domains configuration. The restrictions configuration has the managed apps options disabled, as shown in the following figure.

FIGURE 2. RESTRICTIONS SETTING EXAMPLE
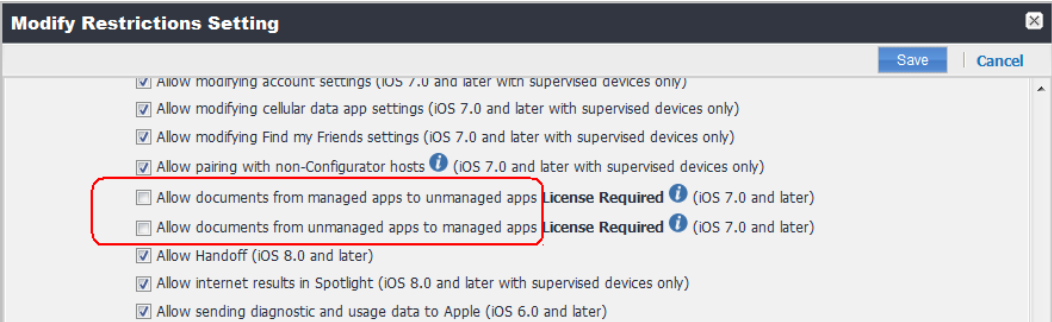
As a result of these two configurations, external addresses are highlighted in red when a user composes an email in the native Mail app:

FIGURE 3. HIGHLIGHTED EXTERNAL ADDRESSES IN EMAIL
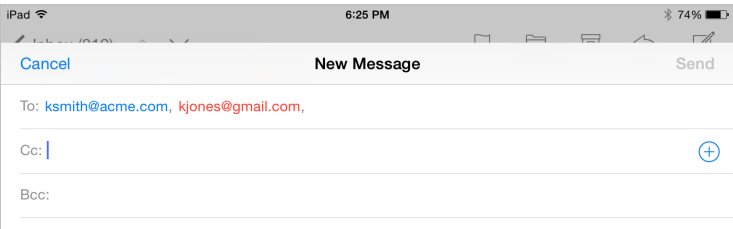
Also, users who use Safari to download documents from acme.com/confidential find that the usual Mail and Message apps are not available for these documents because they are not managed apps.

FIGURE 4. UNMANAGED APPS ARE NOT AVAILABLE
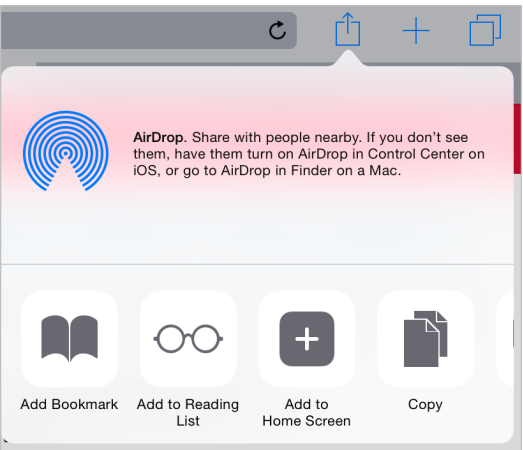
Network usage rules settings

Ivanti EPMM allows you to control the cellular network usage for any given managed app on iOS 9 or supported newer versions. With a network usage configuration, you can prohibit specific managed apps from using cellular data when roaming, or from using cellular data at all. For example, you can configure YouTube as a managed app to be used only when connected to Wi-Fi.

Note the following:

- If you create a cellular data rule with the wildcard value `com.*`, this rule will prohibit the use of other apps when using a cellular data connection, as the `com.*` rule takes precedence over any other allowed apps beginning with `com.*` (such as `com.ivanti.helpatwork`). This is an Apple issue

- Given an iPad managed by Ivanti EPMM with a network usage configuration prohibiting the use of cellular data for a given managed app, if the iPad is removed from Ivanti EPMM management, the app continues to prohibit the use of cellular data in that app until the device is factory reset. This is an Apple issue.

- This setting does not apply to tvOS devices.

Configuring network usage for managed apps

Network usage configurations allow you to control whether device users can access the managed apps you specify while roaming or using the cellular data network. Network usage configurations can thus lower the cost of cellular data usage for your organization.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select **Add New**.

3. Go to **Apple > iOS / tvOS > Network Usage Rules**. The New Network Usage Rules Configuration dialog box opens.

4. Use the following guidelines to fill in the form:

Item	Description
Name	Enter a name for the network usage rules configuration.
Description	Enter a brief description that explains the purpose of this configuration.
Network Usage Rules	
Disallow Roaming on Cellular Data	Select **Add** to list the bundle IDs of apps for which you want to prohibit roaming on cellular data. Select the relevant app from the drop-down list that appears.
	Alternatively, enter a wildcard match for the URLs you want to prohibit roaming on cellular data. A wildcard must appear after a period, and can only be used once at the end of the search string. For example: `com.example.*`
	To delete a rule, select the **X** icon next to it.
Disallow Cellular Data	Select **Add** to list the bundle IDs of apps for which you want to prohibit the use of cellular data. Select the relevant app from the drop-down list that appears.
	Alternatively, enter a wildcard match for the URLs you want to prohibit the use of cellular data. A wildcard must appear after a period, and can only be used once at the end of the search string. For example: `com.example.*`
	To delete a rule, select the **X** icon next to it.

FIGURE 1. NETWORK USAGE RULES CONFIGURATION: DISALLOW ROAMING ON CELLULAR DATA

FIGURE 2. NETWORK USAGE RULES CONFIGURATION: DISALLOW CELLULAR DATA

5.   Select **Save**.

6.   Select the network usage rule configuration you just created.

7. Go to **Actions > Apply to label**.

8. Select the labels you want to apply.

9. Select **Apply**.

What device users see

Device users will be able to run managed apps prohibited from accessing cellular networks when roaming or prohibited from using cellular data. However, when attempting any action requiring the use of cellular data, they will receive a timeout or similar error.

FIGURE 3. TIMEOUT ERROR IF ROAMING OR CELLULAR DATA IS DISALLOWED
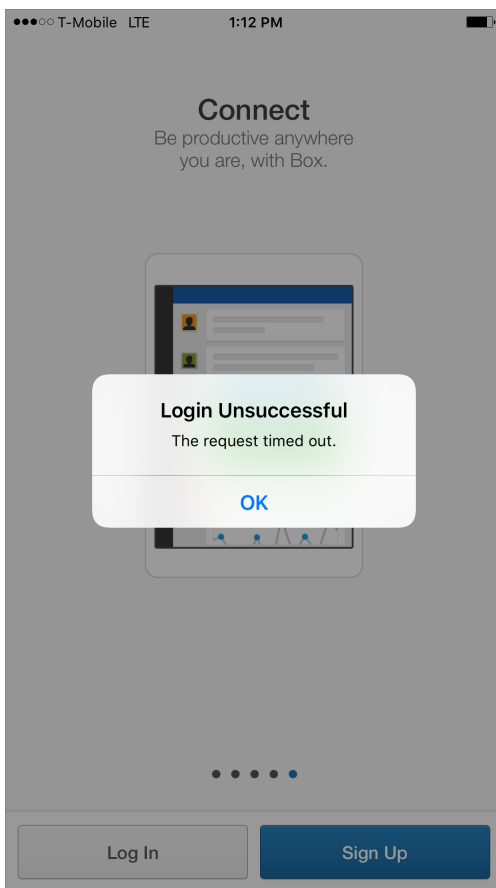
Enterprise single sign-on account settings with Kerberos

With enterprise single sign-on (SSO) with Kerberos, device users can log into your internal backend resources without having to re-enter their enterprise credentials. Creating a single sign-on account configuration is part of a larger configuration to set up single sign-on using Kerberos. The single sign-on setup using Kerberos requires Standalone Sentry and Ivanti Tunnel.

> ℹ️ This setting does not apply to tvOS devices.

URLs and bundle IDs in enterprise single sign-on settings

When you configure enterprise SSO, you specify the URLs of the backend resources that the device user can access using SSO. The backend resource must support Kerberos based authentication.You can also specify bundle IDs (app IDs). If you specify any bundle IDs, then only the specified apps use enterprise SSO when accessing the specified URLs. If you specify no bundle IDs, then all apps that support enterprise SSO use it when accessing the specified URLs.

Identity certificates in enterprise single sign-on settings

When you configure enterprise SSO, you can optionally specify an identity certificate. The app uses this certificate to authenticate the device user to a backend resource when the Kerberos ticket has expired. Once authenticated, the Kerberos ticket is silently renewed.

If you do not provide an identity certificate, the device user is prompted to enter a user ID and password when the Kerberos ticket has expired. Therefore, providing an identity certificate results in a better device user experience.

Configuring a Single Sign-on Account Configuration

For a complete set of configuration tasks for setting up enterprise single sign-on using Kerberos, and for a description of the fields in the single sign-on account configuration, see the *Ivanti Tunnel for iOS Guide*.

macOS settings

Ivanti EPMM allows you to define a number of macOS restrictions.

All restrictions are available to devices running macOS 10.12 or supported newer versions. Some restrictions are available on other versions of macOS. These are usually indicated by an information icon in the user interface.

- "macOS Kernel Extension settings" below
- "macOS restrictions" on the next page
- "macOS Apple App Store restrictions" on page 783
- "Disc settings for macOS" on page 786
- "Media Control setting for macOS" on page 788

- Accessibility Settings Restrictions

macOS Kernel Extension settings

Starting from macOS High Sierra 10.13.2, Apple introduced the concept of "User Approved" MDM Enrollment. This optional enrollment type allows MDM management of certain security-sensitive settings. Using the macOS Kernel Extension loading enables the device user to one of the following:

- Device user manually installs an MDM enrollment profile using System Preferences
- All Device-enrolled Macs are considered user-approved enrollment.

The Kernel Extension Policy payload is designated by specifying com.apple.syspolicy.kernel-extension-policy as the PayloadType. This payload controls restrictions and settings for User Approved Kernel Extension Loading on macOS v10.13.2 and later. The profile containing the payload must be delivered via a User Approved MDM server, and it must be installed as a device profile.

In addition to the settings common to all payloads, this payload defines the following keys.

Procedure

1. Go to **Policies & Configs > Configurations**.

2. Select **Add New > Apple > macOS Only > macOS Kernel Extensions**. The New macOS Kernel Extension Setting dialog box opens.

3. Select **Add+** and configure the settings as described in the table below.

Item	Description	Example
Name	Enter the name of the kernel extension policy. This will display in the Configurations page.	Test_kext
Description	Enter an optional description for the policy.	Kernel Ext Policy Name
Allow User Overrides	Select this check box to allow device users to approve additional kernel extensions not explicitly allowed by this configuration.	N/A
Allowed Team Identifiers	Enter the name of team identifiers that all validly-signed kernel extensions are allowed to load. The type used should be string.	PXPZ95SK77 (for Application: Global Protect VPN)
Allowed Kernel Extensions	Enter a dictionary that represents a set of validly-signed kernel extensions that will always be allowed to load on the user's device.	com.paloaltonetworks.kext.pangpd This corresponds to Allowed Team Identifier example PXPZ95SK77

4. Repeat step 3 for any additional team identifiers and kernel extensions.

5. Select **Save**. The kernel extension displays in the Configurations page.

macOS restrictions

The macOS restrictions setting can be configured for the user or device channel. For devices running macOS 10.12 or supported newer versions, the default is user channel. If you want to apply the restrictions setting to macOS devices regardless of what user is logged in, select Device channel. If you want the restrictions setting to apply to a specific user, select User channel.

A macOS device should only have a single managed user. However, a macOS device may also have an administrator user. If you want the restrictions setting to apply to the whole device regardless of whatever user logs in, select Device channel.

Procedure

1. Go to **Policies & Configs > Configurations.**

2. Select **Add New > Apple > macOS Only > macOS Restrictions** to specify lockdown capabilities for macOS.

3. Configure the settings as described in "macOS restrictions settings " below.

4. Select **Save**.

5. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then select **Confirm**. For more information, see "Best practices: label management" on page 860.

macOS restrictions settings

The following table describes the macOS restrictions settings.

TABLE 117. MACOS RESTRICTIONS SETTINGS

Item	Description	Enabled by Default
Name	Enter a name for the macOS restriction setting.	N/A
Description	Enter a description for the macOS restriction setting.	N/A
Restrictions channel	• **User**: Select to apply restrictions to the user signed in to the macOS device. • **Device**: Select to apply restrictions to the macOS device, regardless of the user currently signed in.	User
Allow use of camera	`allowCamera` Deselect to disable the camera and remove its icon from the Home screen. Users will be unable to take photographs. Available for macOS 10.11 or supported newer versions.	Yes
Allow document and key-value sync to iCloud	`allowCloudDocumentSync` When deselected, disables document and key-value syncing to iCloud. Available for macOS 10.11 or supported newer versions.	Yes
Allow iCloud Photo Library	`allowCloudPhotoLibrary`	Yes

TABLE 117. MACOS RESTRICTIONS SETTINGS (CONT.)

Item	Description	Enabled by Default
	If deselected, disables iCloud Photo Library. Any photos not fully downloaded from iCloud Photo Library to the device will be removed from local storage.	
Allow definition lookup	`allowDefinitionLookup` If deselected, disables definition look-up. Available for macOS 10.11.2 or supported newer versions.	Yes
Allow Back to My Mac iCloud service	`allowCloudBTMM` When deselected, disables macOS Back to My Mac iCloud service.	Yes
Allow Find My Mac iCloud service	`allowCloudFMM` When deselected, disables macOS Find My Mac iCloud service.	Yes
Allow iCloud Bookmark sync	`allowCloudBookmarks` When deselected, disables macOS iCloud Bookmark sync.	Yes
Allow iCloud Mail service	`allowCloudMail` When deselected, disables macOS Mail iCloud services.	Yes
Allow iCloud Calendar service	`allowCloudCalendar` When deselected, disables macOS iCloud Calendar services.	Yes
Allow iCloud Reminder service	`allowCloudReminders` When deselected, disables iCloud Reminder services.	Yes
Allow iCloud Address Book service	`allowCloudAddressBook` When deselected, disables macOS iCloud Address Book services.	Yes
Allow iCloud Notes service (supervised only)	`allowCloudNotes` When deselected, disables macOS iCloud Notes services.	Yes
Allow iCloud Keychain synchronization	`allowCloudKeychainSync` When deselected, disables Cloud keychain synchronization.	Yes
Allow Music service	`allowMusicService` If disabled, Music service is disabled and Music app reverts to classic mode.	Yes

TABLE 117. MACOS RESTRICTIONS SETTINGS (CONT.)

Item	Description	Enabled by Default
Allow Spotlight Internet search results	`allowSpotlightInternetResults` If deselected, Spotlight will not return Internet search results. Available for macOS 10.11 or supported newer versions.	Yes
Allow Touch ID to unlock a device	`allowFingerprintForUnlock` If selected, allows Touch ID to unlock a device. Available for macOS 10.12.4 or supported newer versions.	Yes
Allow macOS auto unlock	`allowAutoUnlock` If deselected, disables macOS auto unlock.	Yes
Allow iTunes File Sharing	`allowiTunesFileSharing` If deselected, disables iTunes application file sharing services. Available for macOS 10.13 or supported newer versions.	Yes
Allow Content Caching	`allowContentCaching` Allow content caching to reduce bandwidth usage and speed up installation by storing software updates, apps, and other content on the device. Available for macOS 10.13 or supported newer versions.	Yes
Allow iCloud desktop and documents service	`allowCloudDesktopAndDocuments` If deselected, disables macOS iCloud desktop and document services. Defaults to true. Available for macOS 10.12.4 or supported newer versions.	Yes
Allow Air Print	`allowAirPrint` When deselected, disables Air Print feature. Available for macOS 10.13 or supported newer versions.	Yes
Disallow AirPrint to destinations with untrusted certificates	`forceAirPrintTrustedTLSRequirement` When selected, requires trusted certificates for TLS printing communication. Available for macOS 10.13 or supported newer versions.	No
Allow discovery of AirPrint printers using iBeacons	`allowAirPrintiBeaconDiscovery`	Yes

TABLE 117. MACOS RESTRICTIONS SETTINGS (CONT.)

Item	Description	Enabled by Default
	When selected, disables iBeacon discovery of AirPrint printers, preventing spurious AirPrint Bluetooth beacons from phishing for network traffic. Available for macOS 10.13 or supported newer versions.	

Delay OS Software Update	`forceDelayedSoftwareUpdates`
	
	When selected, two additional options become available:
	
	• Enforced Software Update Delay
	
	  `forceDelayedMajorSoftwareUpdates`
	
	  Sets the delay of a software update on the device. Select between 1-90 days. The device user will not see a software update until the set number of days after the software release date. Available in macOS 11.3.0.0 and later.
	
	• Enforced Software Update MinorOS Delay
	
	  `enforcedSoftwareUpdateMinorOSDeferredInstallDelay`
	
	  Sets the delay of minor software updates to the device. Select between 1-90 days to delay a minor OS software update on the device. The device user will not see a software update until the set number of days after the software release date. Available in macOS 11.3.0.0 and later.
		No

Delay App Software Update	`forceDelayedAppSoftwareUpdates`
	
	When selected, two additional options become available:
	
	• Enforced Software Update Delay
	
	  `forceDelayedMajorSoftwareUpdates`
	
	  Sets the delay of a software upgrade on the device. Select between 1-90 days. The device user will not see a software update until the set number of days after the software release date. Available in macOS 11.3.0.0 and later.
		No

TABLE 117. MACOS RESTRICTIONS SETTINGS (CONT.)

Item	Description	Enabled by Default
	• Enforced Software Update NonOS Delay `enforcedSoftwareUpdateNonOSDeferredInstallDelay` Sets the delay of non-OS software updates to the device. Select between 1-90 days to delay a non-OS software update on the device. The device user will not see a software update until the set number of days after the software release date. Available in macOS 11.3.0.0 and later.	

Delay Major Software Upgrade	`forceDelayedMajorSoftwareUpdates`
	
	When selected, an additional option becomes available:
	
	• Enforced Software Upgrade MajorOS Delay
	
	`enforcedSoftwareUpdateMajorOSDeferredInstallDelay`
	
	Sets the delay of the device user visibility of major software *upgrade* on the device. Select between 1-90 days. The device user will not see a major software upgrade until the set number of days after the software release date. Available in macOS 11.3.0.0 and later.
		No

Allow ARD Remote Management Modification (Boolean)	If false, prevents modifying the Remote Management Sharing setting in System Settings. Available in macOS 14 and later.	Yes
Allow Bluetooth Sharing Modification (Boolean)	If false, prevents modifying Bluetooth setting in System Settings. Available in macOS 14 and later.	Yes
Allow Cloud Freeform (Boolean)	If false, disallows iCloud Freeform services. Available in macOS 14 and later.	Yes

TABLE 117. MACOS RESTRICTIONS SETTINGS (CONT.)

Item	Description	Enabled by Default
Allow File Sharing Modification (Boolean)	If false, prevents modifying File Sharing setting in System Settings. Available in macOS 14 and later.	Yes
Allow Internet Sharing Modification (Boolean)	If false, prevents modifying Internet Sharing setting in System Settings. Available in macOS 14 and later.	Yes
Allow Local User Creation (Boolean)	If false, prevents creating new users in System Settings. Available in macOS 14 and later.	Yes
Allow Printer Sharing Modification (Boolean)	If false, prevents modifying Printer Sharing setting in System Settings. Available in macOS 14 and later.	Yes
Allow Remote Apple Events Modification (Boolean)	If false, prevents modifying Remote Apple Events Sharing setting in System Settings. Available in macOS 14 and later.	Yes
Allow Startup Disk Modification (Boolean)	If false, prevents modification of Startup Disk setting in System Settings. Available in macOS 14 and later.	Yes
Allow Time Machine Backup (Boolean)	If false, prevents modification of Time Machine settings in System Settings. Available in macOS 14 and later.	Yes
Allow modifying passcode (supervised devices)	`allowPasscodeModification` If deselected, prevents device passcode from being added, changed, or removed.	Yes
Allow password AutoFill	`allowPasswordAutoFill` Select to allow password autofill. Available for macOS 10.14 or supported newer versions.	Yes

TABLE 117. MACOS RESTRICTIONS SETTINGS (CONT.)

Item	Description	Enabled by Default
Allow proximity based password sharing requests	`allowPasswordProximityRequests` Select to allow nearby devices to request device passwords. Available for macOS 10.14 or supported newer versions.	Yes
Allow password sharing	`allowPasswordSharing` Select to allow users to share their device passwords using Airdrop Passwords feature. Available for macOS 10.14 or supported newer versions.	Yes
Allow screenshots and screen recording	`allowScreenShot` When deselected, users are unable to save screenshots or record video of the display. When deselected, this restriction also prevents the Classroom app from observing remote screens. Available for macOS 10.14.4 or supported newer versions.	Yes
Allow remote screen observation	`allowRemoteScreenObservation` If this is de-selected, remote screen observation by the Classroom app is disabled. Available for macOS 10.14.4 or supported newer versions.	Yes
Automatically join Classroom classes without prompting (supervised only)	`forceClassroomAutomaticallyJoinClasses` When selected, automatically gives permission to the teacher's requests without prompting the student. Available for macOS 10.14.4 or supported newer versions.	No
Require teacher permission to leave Classroom unmanaged classes (supervised only)	`forceClassroomRequestPermissionToLeaveClasses` When selected, a student enrolled in an unmanaged course via Classroom will request permission from the teacher when attempting to leave the course. Available for macOS 10.14.4 or supported newer versions.	No
Allow Classroom to lock an app and lock the device without prompting (supervised only)	`forceClassroomUnpromptedAppAndDeviceLock` When selected, alls the teacher to lock apps or the device without prompting the student. Available for macOS 10.14.4 or supported newer versions.	No

TABLE 117. MACOS RESTRICTIONS SETTINGS (CONT.)

Item	Description	Enabled by Default
Allow Classroom to perform AirPlay and View Screen without prompting (supervised only)	`forceClassroomUnpromptedScreenObservation` If selected, and the **Apple Education > Screen Observation Modification Control** field is also selected, a student enrolled in a managed course via the Classroom app will automatically give permission to that course's teacher's requests to observe the student's screen without prompting the student. Available for macOS 10.14.4 or supported newer versions.	No
Allow Handoff	`allowActivityContinuation` Select to enable the Handoff feature, which allows users to seamlessly continue working where they left off using any Apple device on which they are logged in with their Apple ID. Available for macOS 10.15 or supported newer versions.	Yes
Allow use of Game Center (supervised devices only)	`allowGameCenter` When deselected, Game Center is disabled and its icon is removed from the Home screen. Available for macOS 10.13 or supported newer versions.	Yes
Allow adding Game Center friends (supervised device)	`allowAddingGameCenterFriends` When deselected, prohibits adding friends to Game Center. Disabled when **Allow use of Game Center** is deselected. Available for macOS 10.13 or supported newer versions.	Yes
Allow multiplayer gaming (supervised device)	`allowMultiplayerGaming` When deselected, prohibits multiplayer gaming. Disabled when **Allow use of Game Center** is deselected. Available for macOS 10.13 or supported newer versions.	Yes
Allow AirDrop (supervised device)	`allowAirDrop` If deselected, AirDrop is disabled. Available for macOS 10.13 or supported newer versions.	Yes
Allow sending diagnostic and usage data to Apple	`allowDiagnosticSubmission` When deselected, this prevents the device from automatically submitting diagnostic reports to Apple. Available for macOS 10.13 or supported newer versions.	Yes
Allow dictation	`allowDictation`	Yes

TABLE 117. MACOS RESTRICTIONS SETTINGS (CONT.)

Item	Description	Enabled by Default
(supervised device)	When deselected, disables dictation input method. Disabled automatically when using Advanced Audio Coding (AAC) mode. Available for macOS 10.13 or supported newer versions.	
Allow modifying Wallpaper (supervised device)	`allowWallpaperModification` If deselected, prevents wallpaper from being changed. Available for macOS 10.13 or supported newer versions.	Yes
Allow Safari AutoFill (supervised device)	`allowSafari` Deselect to disable the Safari web browser, remove its icon from the Home screen, and prevent users from opening web clips. Available for macOS 10.13 or supported newer versions.	Yes
Allow Erase All Content and Settings (supervised devices only)	`allowEraseContentAndSettings` Deselect to disable the "Erase All Content and Settings" option in the Reset section of iOS devices. Applicable to iOS 8 and later, and macOS 12 and later.	Yes

macOS Apple App Store restrictions

The macOS Apple App Store restrictions setting allows you to restrict user or device interactions with the Apple App Store. For example, you can restrict app installations and updates to administrator users only, or to MDM-installed apps in updates only.

Procedure

1. Go to **Policies & Configs > Configurations.**

2. Select **Add New > Apple > macOS Only > macOS App Store Restrictions** to specify App Store lockdown capabilities for macOS.

3. Configure the settings as described in "macOS App Store Restrictions options " on the next page.

4. Select **Save**.

5. Select the setting you just created.

6. Go to **Actions > Apply to label**.

7.   Select the labels you want to apply.

8.   Select **Apply**.

macOS AppStore restriction options

The following table describes the macOS App Store restrictions.

TABLE 118.   MACOS APP STORE RESTRICTIONS OPTIONS

Item	Description	Selected by Default
Name	`com.apple.app.appstore` Enter a name for the macOS App Store Restrictions setting.	N/A
Description	Enter a description for the setting.	N/A
Restrictions Channel	Select one of the following: • **User**: Select to apply restrictions to the user signed in to the macOS device. • **Device**: Select to apply restrictions to the macOS device, regardless of the user currently signed in. For devices running macOS 10.12 or supported newer versions, the default is user channel. If an you want the restrictions setting to apply to macOS devices regardless of what user is logged in, select Device channel. If you want the restrictions setting to apply to a specific user, select User channel.	User
Restrict app installations to admin users only	`restrict-store-require-admin-to-install` Select to restrict the installation of apps to admins only. Available on macOS devices running macOS 10.9 or supported newer versions.	Yes
Restrict app installations to software updates only	`restrict-store-softwareupdate-only` Select to restrict updates to apps already installed to managed macOS devices.	Yes

TABLE 118. MACOS APP STORE RESTRICTIONS OPTIONS (CONT.)

Item	Description	Selected by Default
	Available on macOS devices running macOS 10.10 or supported newer versions.	
Disable app adoption	`restrict-store-disable-app-adoption` Select to prevent users from managing apps through the Apple App Store that were not originally purchased through the Apple App Store. Available on macOS devices running macOS 10.10 or supported newer versions.	Yes
Disable software updates notifications	`DisableSoftwareUpdateNotifications` Select to prevent app update notifications from appearing on managed macOS devices. Available on macOS devices running macOS 10.10 or supported newer versions.	Yes
Restrict app installations to MDM-installed apps and software updates (macOS 10.11 and later)	`restrict-store-mdm-install-softwareupdate-only` Select to restrict app installations and updates to MDM-installed apps only. Available on macOS devices running macOS 10.11 or supported newer versions.	Yes
Allow Universal Control	Prohibits the control of multiple Apple devices - including an iMac, MacBook, and iPad - all with the same keyboard and mouse.	Yes
Allow UI Configuration Profile Installation	Prohibits the user from installing configuration profiles and certificates interactively. Requires a supervised device. Available in iOS 6 and later and macOS 13 and later.	Yes
Allow USB Restricted Mode	If disabled, allows the device to always connect to USB accessories while locked. On macOS, allows new USB accessories to connect without authorization. Available in macOS 11.3.0.0 and later.	Yes

> ℹ️ The new restrictions are not automatically pushed to the devices when you upgrade. Instead, to force-push the restriction to all devices, open it and save it.

Disc settings for macOS

You can use the Finder and Disc Burning restriction settings to restrict the ability of managed macOS devices to burn data to disc. You must configure both settings to control the burning of data to disc on managed macOS devices.

Configuring Finder disc burning settings for macOS

The Finder restriction for macOS devices allow you to disable disc burning capabilities using macOS Finder on managed macOS devices. Disabling disc burning through Finder using this restriction setting will also disable disc burning regardless of the disc burning restriction setting described in "Configuring the Disc Burning setting for macOS" on the next page.

Procedure

1. Go to **Policies & Configs > Configurations.**

2. Select **Add New > Apple > macOS Only > Disc > Finder**.

3. Enter a name for the Finder restriction setting.

4. Select **Disable Finder's Disc Burning Support** to disable the disc burning capability on managed macOS devices. If you want to enable support for burning to disc using Finder, leave this option unchecked.

5. Select **Save**.

6. Select the setting you just created.

7. Go to **Actions > Apply to label**.

8. Select the labels you want to apply.

9. Select **Apply**.

Configuring the Disc Burning setting for macOS

The Disc Burning restriction allows you to control whether users can burn data to disc on managed macOS devices. You can enable or disable disc burning, or allow the burning of data to disc only after users have gone through an authentication process. You must also create a Finder restriction in addition to the Disc Burning restriction to control disc burning on managed macOS devices.

Procedure

1. Go to **Policies & Configs > Configurations.**

2. Select **Add New > Apple > macOS Only > Disc > Disc Burning**.
   The New Disc Burning dialog box opens.

3. Configure the settings as described in "Disc Burning settings (macOS) " on the next page.

4. Select **Save**.

5. Select the setting you just created.

6. Go to **Actions > Apply to label**.

7. Select the labels you want to apply.

8. Select **Apply**.

Disc burning settings (macOS)

The following table describes the settings for disc buning.

TABLE 119. DISC BURNING SETTINGS (MACOS)

Item	Description
Name	Enter a name for the disc burning setting.
Description	Enter a description for the disc burning setting (optional).
Burn Support	Select one of the following: • **Off**: Select to disable support for burning data to disc on a managed macOS device. You must also disable disc burning in the Finder setting to disable disc burning on managed macOS devices. • **On**: Select to enable support for burning data to disc on a managed macOS device. You must also enable disc burning in the Finder setting to enable disc burning on managed macOS devices. • **Authenticate**: Select to require managed macOS device users to enter their login information before burning data to disc.

Media Control setting for macOS

The Media Control setting allows you to permit or forbid users to mount, unmount, and eject on logout a variety of media, such as DVDs, network disks, and external drives. This setting enables you to fine-tune your control over media use on macOS devices, for example, you can configure all blank DVDs to be rejected by the macOS media drive, or require user authentication when connecting to a network drive.

The Supported media types are:

- BD
- Blank BD
- Blank CD
- Blank DVD
- CD
- Disk Image
- DVD
- Hard Disk External
- Hard Disk Internal
- Network Disk

Procedure

1. Go to **Policies & Configs > Configurations.**

2. Select **Add New > Apple > macOS Only > Media Control**.
   The New Media Control Setting dialog box opens.

3. Configure the settings as described in "Media Control Setting (macOS) " below.

4. Select **Save**.

5. Select the setting you just created.

6. Go to **Actions > Apply to label**.

7. Select the labels you want to apply.

8. Select **Apply**.

TABLE 120. MEDIA CONTROL SETTING (MACOS)

Item	Description
Name	Enter a name for the Media Control setting.
Description	Enter a description for the Media Control setting.
Logout Eject	Logout Eject rules cause the selected medium to be ejected when the macOS user logs out. 1. Select **Add** to select a medium from the drop-down list and configure settings for that medium. 2. For the rule you are creating, select any of the following: • **Authenticate**: Requires macOS device users to authenticate before interacting with the medium. • **Read only**: Makes the medium read-only. • **Deny**: Denies access to the medium. • **Eject**: Causes the medium to eject when macOS users attempt to access it. 3. Repeat for any other media for which you would like to create a rule.

TABLE 120. MEDIA CONTROL SETTING (MACOS) (CONT.)

Item	Description
Mount Controls	Creating rules for Mount Controls allows you to govern the media that can be mounted on managed macOS devices. 1. Select **Add** to select a medium from the drop-down list and configure settings for that medium. 2. For the rule you are creating, select any of the following: • **Authenticate**: Requires macOS device users to authenticate before interacting with the medium. • **Read only**: Makes the medium read-only. • **Deny**: Denies access to the medium. • **Eject**: Causes the medium to eject when macOS users attempt to access it. 3. Repeat for any other media for which you would like to create a rule.
Unmount Controls	Creating rules for Unmount Controls allows you to govern the media that can be unmounted from managed macOS devices. 1. Select **Add** to select a medium from the drop-down list and configure settings for that medium. 2. For the rule you are creating, select any of the following: • **Authenticate**: Requires macOS device users to authenticate before interacting with the medium. • **Deny**: Denies access to the medium. 3. Repeat for any other media for which you would like to create a rule.

Accessibility Settings Restrictions

A new Accessibility Settings Restrictions is added, which will provide the administrator to control the Mac device accessibility settings.

• Bold Text Enabled (Boolean): If true, enables bold text.
• Increase Contrast Enabled (Boolean): If true, enables increase contrast.

- Reduced Motion Enabled (Boolean): If true, enables reduced motion.
- Reduce Transparency Enabled (Boolean): If true, enables reduced transparency.
- Text Size: The accessibility text size apps that support dynamic text use. 0 is the smallest value, and 11 is the largest value available. Default 4 possible values.
- Touch Accommodations Enabled (Boolean): If true, enables touch accommodations.
- Voice Over Enabled (Boolean): If true, enables voice over.
- Zoom Enabled (Boolean): If true, enables zoom.

iOS and macOS Ivanti EPMM settings differences

The following table outlines important differences in feature support between iOS and macOS.

TABLE 121. DIFFERENCES BETWEEN IOS AND MACOS

Feature	macOS	iOS
CalDAV	MDM authenticates the account before pushing profiles. Therefore, if Ivanti EPMM does not have valid credentials, it will not push the profile. The **Save user password** field in **Settings > System Settings > Users & Devices > Registration** must be enabled.	MDM does not authenticate the account before pushing profiles. The device user is prompted to enter a password.
CardDAV	MDM does not authenticate the account. If no credentials are available, the contacts will not be synchronized and the device user will not be prompted for a password.	MDM does not authenticate the account before pushing profiles. The device user is prompted to enter a password.
Exchange	Only Contacts are synchronized. SSL is required.	Email, contacts, tasks, and appointments are synchronized.
web clip	Profiles will not be pushed if the size of the web clip image is greater than 20K.	Profiles will be pushed, regardless of the size of the web clip image.

Using Ivanti Mobile@Work for iOS

This section addresses the management of Ivanti Mobile@Work for iOS.

-
-
-
-
-
-

> ℹ️ In iOS 13, the option to "Allow Always" was removed from the iOS Settings app. Instead, a dialog box displays requesting device users to enable tracking when the Ivanti Mobile@Work app is running. Ivanti Mobile@Work opens iOS Settings where device users can choose "Ask Next Time" or "Never". Ivanti, Inc recommends device users to enable tracking. This change applies to all versions of iOS 13 or supported newer versions. Ivanti Mobile@Work for iOS does not track device users' location without consent.

Device management with the Ivanti Mobile@Work My Devices tab

Ivanti Mobile@Work includes a self-service feature that allows device users to manage the device they are currently using, as well as any other devices that they have registered with Ivanti EPMM. The device management actions device users can take in the My Devices tab are generally similar to those available in the Ivanti EPMM User Portal.

The self-service feature is in the My Devices page in Ivanti Mobile@Work, and includes the following tabs:

- **Actions**: Actions a device user can take on the device currently in use, or other devices registered to that user, such as locking, unlocking, wiping, and re-enrolling the device with Ivanti EPMM.
- **Info**: Details about the selected device, such as the device model number, OS version, and device registration date.
- **Map**: The precise street location of the selected device.

Actions you can take on the current device

In the My Devices tab, you can take the following actions on the device you are currently using:

- Check for Updates
- Re-enroll Device
- Retire Device (only if the device user has the correct permissions to retire a device)

Actions you can take on your other devices

You can also use the My Devices tab to take the following actions on other devices registered to you, even if those devices are not currently at your disposal:

- Unlock Device
- Lock Device
- Retire Device
- Wipe Device

You can lock, unlock, retire, or wipe one of your devices if you have the relevant roles assigned to you. If you only have one registered device, you cannot unlock, lock, or wipe that device in the My Devices tab.

Device status

The My Devices tab lists all devices registered to the device user who is logged in to Ivanti Mobile@Work. Each device shows the status of any actions taken on that device. For example, if you initiated a wipe on the third device in your list of devices, the status of that device might be "Wipe Pending".

Related topics

- "Assigning and removing device user roles" in *Getting Started with Ivanti EPMM*
- "Self-service User Portal" on page 945
- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on the next page
- "Checking for Ivanti EPMM updates with Ivanti Mobile@Work" on page 795
- "Re-enrolling a device with Ivanti Mobile@Work " on page 795
- "Retiring a device with Ivanti Mobile@Work " on page 796
- "Unlocking a device with Ivanti Mobile@Work " on page 797
- "Locking a device with Ivanti Mobile@Work " on page 798
- "Wiping a device with Ivanti Mobile@Work " on page 799

-
-

Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work

You must authenticate with Ivanti EPMM when:

- Managing your devices with the My Devices tab for the first time
- The connection between Ivanti EPMM and Ivanti Mobile@Work has timed out
- After you have exited and re-opened Ivanti Mobile@Work.

> ⓘ   Ivanti Mobile@Work only persists the username if you successfully authenticate with Ivanti EPMM.

Procedure

1. In Ivanti Mobile@Work, tap **My Devices**.

2. Tap **Show my devices**.

   Ivanti Mobile@Work shows the **Authentication Required** popup.

3. When authenticating for the first time after upgrading from previous versions of Ivanti Mobile@Work, enter the device username and password in the space provided.

4. When authenticating thereafter, enter the device password at the prompt.

   Ivanti Mobile@Work shows the devices registered to the authenticated device user in the My Devices tab, with the device currently in use at the top of the list.

Related topics

-
-
-
-
-
-
-
-

Checking for Ivanti EPMM updates with Ivanti Mobile@Work

The My Devices tab in Ivanti Mobile@Work allows you to check for any updates available from Ivanti EPMM. Updates may include modified Mobile Device Management (MDM) profiles, AppConnect policies, and certificate enrollment settings, for example. If updates are available, Ivanti EPMM sends the updates to the device. You can check for updates with the device you are currently using.

> **i**   You can only check for Ivanti EPMM updates on the device currently in use.

Procedure

1. In Ivanti Mobile@Work, tap **My Devices**.

2. Tap the device on which you wish to take action.

   Ivanti Mobile@Work shows the **Device Details** page.

3. Tap **Actions** > **Check for Updates**.

   Ivanti Mobile@Work communicates with Ivanti EPMM to check for updates.

Related topics

- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on the previous page
- "Re-enrolling a device with Ivanti Mobile@Work " below
- "Retiring a device with Ivanti Mobile@Work " on the next page
- "Unlocking a device with Ivanti Mobile@Work " on page 797
- "Locking a device with Ivanti Mobile@Work " on page 798
- "Wiping a device with Ivanti Mobile@Work " on page 799
- "Viewing device details in the Ivanti Mobile@Work My Devices tab" on page 800
- "Locating an iOS device in the Ivanti Mobile@Work My Devices tab" on page 801

Re-enrolling a device with Ivanti Mobile@Work

You can re-enroll the device you are currently using with Ivanti EPMM. After requesting re-enrollment, Ivanti EPMM pushes the relevant profiles and configurations to the device again.

> **i**   You can only re-enroll the device currently in use.

Procedure

1. In Ivanti Mobile@Work , tap **My Devices**.

2. Tap the device on which you wish to take action.

   Ivanti Mobile@Work shows the **Device Details** page.

3. Tap **Actions** > **Re-enroll Device**.

   Ivanti Mobile@Work sends a request to Ivanti EPMM to re-register the device.

Related topics

- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on page 794
- "Checking for Ivanti EPMM updates with Ivanti Mobile@Work" on the previous page
- "Retiring a device with Ivanti Mobile@Work " below
- "Unlocking a device with Ivanti Mobile@Work " on the next page
- "Locking a device with Ivanti Mobile@Work " on page 798
- "Wiping a device with Ivanti Mobile@Work " on page 799
- "Viewing device details in the Ivanti Mobile@Work My Devices tab" on page 800
- "Locating an iOS device in the Ivanti Mobile@Work My Devices tab" on page 801

Retiring a device with Ivanti Mobile@Work

You can remove from Ivanti EPMM management your current device, or any device you have registered with Ivanti EPMM.

> You need to have the relevant role assigned to your user name to take this action. The role is a user portal role. For more information, see "Assigning user portal device management roles" on page 954.

Procedure

1. In Ivanti Mobile@Work , tap **My Devices**.

2. Tap the device on which you wish to take action.

   Ivanti Mobile@Work shows the **Device Details** page.

3. Tap **Actions** > **Retire Device**.

4. At the prompt, tap **Retire Device**.

5. Enter your password.

   Ivanti Mobile@Work sends a request to Ivanti EPMM to retire the device.

Related topics

- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on page 794
- "Checking for Ivanti EPMM updates with Ivanti Mobile@Work" on page 795
- "Re-enrolling a device with Ivanti Mobile@Work " on page 795
- "Unlocking a device with Ivanti Mobile@Work " below
- "Locking a device with Ivanti Mobile@Work " on the next page
- "Wiping a device with Ivanti Mobile@Work " on page 799
- "Viewing device details in the Ivanti Mobile@Work My Devices tab" on page 800
- "Locating an iOS device in the Ivanti Mobile@Work My Devices tab" on page 801

Unlocking a device with Ivanti Mobile@Work

You can unlock another device you have registered with Ivanti EPMM from Ivanti Mobile@Work on the registered device you are currently using.

> You need to have the relevant role assigned to your user name to take this action. The role is a user portal role. For more information, see "Assigning user portal device management roles" on page 954.

Procedure

1. In Ivanti Mobile@Work , tap **My Devices**.

2. Tap the device on which you wish to take action.

   Ivanti Mobile@Work shows the **Device Details** page.

3. Tap **Actions** > **Unlock Device**.

4. At the prompt, tap **Unlock Device**.

5. Enter your password.

   Ivanti Mobile@Work sends a request to Ivanti EPMM to unlock the device.

Related topics

- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on page 794
- "Checking for Ivanti EPMM updates with Ivanti Mobile@Work" on page 795
- "Re-enrolling a device with Ivanti Mobile@Work " on page 795
- "Retiring a device with Ivanti Mobile@Work " on page 796
- "Locking a device with Ivanti Mobile@Work " below
- "Wiping a device with Ivanti Mobile@Work " on the next page
- "Viewing device details in the Ivanti Mobile@Work My Devices tab" on page 800
- "Locating an iOS device in the Ivanti Mobile@Work My Devices tab" on page 801

Locking a device with Ivanti Mobile@Work

You can lock another device you have registered with Ivanti EPMM from Ivanti Mobile@Work on the registered device you are currently using.

> You need to have the relevant role assigned to your user name to take this action. The role is a user portal role. For more information, see "Assigning user portal device management roles" on page 954.

Procedure

1. In Ivanti Mobile@Work , tap **My Devices**.

2. Tap the device on which you wish to take action.

   Ivanti Mobile@Work shows the **Device Details** page.

3. Tap **Actions** > **Lock Device**.

4. At the prompt, tap **Lock Device**.

5. Enter your password.

   Ivanti Mobile@Work sends a request to Ivanti EPMM to lock the device.

Related topics

- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on page 794
- "Checking for Ivanti EPMM updates with Ivanti Mobile@Work" on page 795

- "Re-enrolling a device with Ivanti Mobile@Work " on page 795
- "Retiring a device with Ivanti Mobile@Work " on page 796
- "Unlocking a device with Ivanti Mobile@Work " on page 797
- "Wiping a device with Ivanti Mobile@Work " below
- "Viewing device details in the Ivanti Mobile@Work My Devices tab" on the next page
- "Locating an iOS device in the Ivanti Mobile@Work My Devices tab" on page 801

Wiping a device with Ivanti Mobile@Work

You can wipe the app data and user data from another device you have registered with Ivanti EPMM, using Ivanti Mobile@Work on your current device.

ⓘ   You need to have the relevant role assigned to your user name to take this action. The role is a user portal role. For more information, see "Assigning user portal device management roles" on page 954.

Procedure

1. In Ivanti Mobile@Work , tap **My Devices**.

2. Tap the device on which you wish to take action.

   Ivanti Mobile@Work shows the **Device Details** page.

3. Tap **Actions** > **Wipe Device**.

4. At the prompt, tap **Wipe Device**.

5. Enter your password.

   Ivanti Mobile@Work sends a request to Ivanti EPMM to wipe the device.

Related topics

- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on page 794
- "Checking for Ivanti EPMM updates with Ivanti Mobile@Work" on page 795
- "Re-enrolling a device with Ivanti Mobile@Work " on page 795
- "Retiring a device with Ivanti Mobile@Work " on page 796
- "Unlocking a device with Ivanti Mobile@Work " on page 797
- "Locking a device with Ivanti Mobile@Work " on the previous page

- "Viewing device details in the Ivanti Mobile@Work My Devices tab" below
- "Locating an iOS device in the Ivanti Mobile@Work My Devices tab" on the next page

Viewing device details in the Ivanti Mobile@Work My Devices tab

You can use My Devices to view details about any device registered to the device user, such as model number, iOS version number, registration date, and so on.

Procedure

1. In Ivanti Mobile@Work , tap **My Devices**.

2. Tap the device whose details you wish to examine.

   Ivanti Mobile@Work shows the **Device Details** page.

3. Tap **Info**.

4. Ivanti Mobile@Work shows the information available about the device, as shown in "The device details page in Ivanti Mobile@Work " below.

ℹ️   Any unavailable device information appears as N/A.

Reference

TABLE 1. THE DEVICE DETAILS PAGE IN IVANTI MOBILE@WORK

Item	Description
Model	The model number of the iOS device.
Version	The version of iOS installed to the device.
Registration Date	The date and time the device was registered with Ivanti EPMM.
Owner	The owner of the device, either company or employee.
Phone Number	The phone number assigned to the device, if relevant.
Carrier	The cellular operator to which the device is registered, if relevant.
IMEI	A 15 digit number unique to the mobile device.
Manufacturer	The manufacturer of the device.

Related topics

- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on page 794
- "Checking for Ivanti EPMM updates with Ivanti Mobile@Work" on page 795
- "Re-enrolling a device with Ivanti Mobile@Work " on page 795
- "Retiring a device with Ivanti Mobile@Work " on page 796
- "Unlocking a device with Ivanti Mobile@Work " on page 797
- "Locking a device with Ivanti Mobile@Work " on page 798
- "Wiping a device with Ivanti Mobile@Work " on page 799
- "Locating an iOS device in the Ivanti Mobile@Work My Devices tab" below

Locating an iOS device in the Ivanti Mobile@Work My Devices tab

The My Devices tab allows you to view the map location and street address of any device registered to your username.

- Ivanti Mobile@Work can only locate devices on which you have enabled location services.

  > In iOS 13, the option to "Allow Always" was removed from the iOS Settings app. Instead, a dialog box displays requesting device users to enable tracking when the Ivanti Mobile@Work app is running. Ivanti Mobile@Work opens iOS Settings where device users can choose "Ask Next Time" or "Never". Ivanti, Inc recommends device users to enable tracking. This change applies to all versions of iOS 13 or supported newer versions. Ivanti Mobile@Work for iOS does not track device users' location without consent.

- You cannot copy addresses from the map.

Procedure

1. In Ivanti Mobile@Work , tap **My Devices**.

2. Tap the device whose details you wish to examine.

   Ivanti Mobile@Work shows the **Device Details** page.

3. Tap **Map**.

   Ivanti Mobile@Work shows a map with a green indicator for the device.

4. Tap the green indicator to view the exact street address where the device is located.

5. Tap the blue indicator to view the location of another device registered to the same user.

Related topics

- "Authenticating with Ivanti EPMM from the My Devices tab in Ivanti Mobile@Work" on page 794
- "Checking for Ivanti EPMM updates with Ivanti Mobile@Work" on page 795
- "Re-enrolling a device with Ivanti Mobile@Work " on page 795
- "Retiring a device with Ivanti Mobile@Work " on page 796
- "Unlocking a device with Ivanti Mobile@Work " on page 797
- "Locking a device with Ivanti Mobile@Work " on page 798
- "Wiping a device with Ivanti Mobile@Work " on page 799
- "Viewing device details in the Ivanti Mobile@Work My Devices tab" on page 800

Managing notifications in Ivanti Mobile@Work for iOS

Ivanti Mobile@Work for iOS includes a Notifications tab shows notifications received from Ivanti EPMM. The Notifications tab allows you to manage notifications, including the ability to receive notifications on the home screen and view, save, or dismiss them. Notifications from Ivanti Mobile@Work are displayed in the device Notifications Center.

Notifications can be received and viewed when the device is locked. When Ivanti Mobile@Work is running in the background, all new notifications are sent to both Ivanti Mobile@Work and the Notifications Center. When Ivanti Mobile@Work is running in the foreground, all new notifications are sent to Ivanti Mobile@Work only. When Ivanti Mobile@Work is not running, all notifications are delivered only to the device Notification Center. Tapping the message in the Notification Center opens Ivanti Mobile@Work and delivers that particular message to Ivanti Mobile@Work . For example, if three messages have been sent to the Notification Center, the device user must tap each message to deliver it to Ivanti Mobile@Work .

Procedure

- You can do the following in the Notifications tab in Ivanti Mobile@Work :
  - View additional notification details by tapping the chevron (>) next to a notification in the Ivanti Mobile@Work Notifications tab.
  - Swipe right to left to delete a given notification.
  - Delete all notifications by tapping **Delete All** on the top right of the Notifications tab.
  - Save notifications by tapping them one at a time.

Logging and enhanced logging for Ivanti Mobile@Work

If iOS device users experience issues with Ivanti Mobile@Work , they can reproduce the issue and send the logs (log level Debug) to their support administrator. Enhanced Logging encrypts the logs for safe transport to the support Admin.

> ℹ This feature is for troubleshooting, and is disabled by default. Logging requires Ivanti Mobile@Work 9.0 or supported newer versions.

Sending Ivanti Mobile@Work logs to Ivanti, Inc Support

Procedure

1. Open Ivanti Mobile@Work .

2. Tap **Settings**.

3. To enable encrypted logging of your phone information, tap **Enhanced Logging**.

   If you do not require encryption, make sure **Enhanced Logging** is toggled off.

4. Reproduce the issue on the device.

5. Go back to Ivanti Mobile@Work , and tap **Settings > Send Mobile@Work Logs**.

   Select a method to send the log information to Ivanti Endpoint Manager Mobile support. Options include email, SMS, AirDrop, and others.

6. Enter a support address and tap **Send**.

Remote Enhanced Logging for Managers

In circumstances where issues are intermittent or random in nature, enhanced logging can be remotely enabled on a set of devices by the manager. This includes the ability to pull the logs remotely. Once the needed information is collected, the logging can be disabled. At the device, the user can override this command; the override will be in the report to Ivanti EPMM at the next checkin.

Procedure

1. Open **Actions** > **More Actions** > **Enhanced Logging**.

2. Enter the device(s) to be affected.

3. Select **Enable Enhanced Logging**.

4. Create any notes and select **Update**.

When the manager has the enhanced logs, return to the Enhanced Logging screen and select **Disable Enhanced Logging** to stop the action.

Remote activation of enhanced logging for iOS Ivanti Mobile@Work

The ability to remotely enable enhanced logging helps managers monitor devices where the nature of an issue is intermittent or random. This option allows the manager to enable enhanced logging remotely using the device manager for a set of devices in order to collect the logging needed, and then to disable the feature once finished. This feature is currently supported in Ivanti EPMM 11.4.0.0 and later.

This feature is engaged as a command or action off of the device menu and will be sent to the iOS Ivanti Mobile@Work client.

Procedure

1. At the Device Menu: go to Actions > More Actions > Enhanced Logging
2. Dialog appears with Enable enhanced logging or Disable enhanced logging options as well as a location to identify the devices and a place to make Notes.
   a. Enter the devices to be engaged.
   b. Select whether Enable or Disable the functionality.
   c. Make any Notes needed for your project.
3. Accept the changes.

If enabled, a new property will be sent from the Client, `EnhancedLoggingEnabled`, with True/False as the options. The property is available for labels, advanced search, and shown in the device details.

> ⓘ   If this is not sent, DO NOT set a default as that means the value is unknown, the client is older.

Opening Ivanti Mobile@Work for iOS logs in other apps

Ivanti Mobile@Work for iOS allows you to use the iOS Open In feature for Ivanti Mobile@Work logs. You can open Ivanti Mobile@Work log files in any app that supports that file type.

Procedure

1. On an iOS device, run Ivanti Mobile@Work .

2. In Ivanti Mobile@Work , tap **Settings > Send Mobile@Work Logs**.

3. Select Open In.

4. Open the log file in any available app.

Encrypting device logs with your own certificate

You can define a log encryption configuration that enables device users to send encrypted logs to an administrator's email address from their devices. The configuration includes a certificate for encrypting logs and an email address to which encrypted logs are to be sent. Devices sync with Ivanti EPMM and receive the configuration after you assign the configuration to the relevant labels.

This feature requires Ivanti Mobile@Work 10.0.0 for iOS or supported newer versions.

Before you begin

Upload a certificate to Ivanti EPMM, as described in "Certificates settings" on page 654.

Procedure

1. In the Admin Portal, select **Policies & Configs**> **Configurations**.

2. Select **Add New** and select **LogEncryption**. The New Log Encryption Setting dialog box opens.

3. Fill in the following:

Field	Description
Name	Enter a name for the configuration.
Email Address	Enter an email address to which encrypted logs may be sent. The **To:** field of the email is automatically filled with this address. If you do not enter an email address here, the device user fills in the **To:** field.
Certificate	From the drop-down list, select a certificate you have already uploaded to Ivanti EPMM.

4. Select **Save**.

5. On the Configurations page, select the configuration you just defined.

6. Select **Actions** > **Apply to Label**, and select the label to which you want to apply the log encryption configuration.

Screen orientation

Ivanti Mobile@Work 10.1.0.0 or supported newer versions supports only portrait mode. It does not rotate to landscape mode.

Using Ivanti Mobile@Work for macOS

This section addresses the management of Ivanti Mobile@Work for macOS.

Running shell scripts on macOS devices

This section addresses the components related to running shell scripts on macOS devices.

Shell scripts on macOS devices

Ivanti EPMM allows you to create and sign your own macOS shell scripts, which you can then upload to Ivanti EPMM and run on managed macOS devices. You can write a script that configures any setting within macOS System Preferences on macOS devices. Or, you may wish to run scripts that:

- force device users to change their passwords monthly
- lock the screen after 5 minutes of idle time
- or configures a secured Wi-Fi network.

After uploading scripts to Ivanti EPMM and configuring macOS script configuration and policy components, Ivanti EPMM executes your scripts on macOS devices using Ivanti Mobile@Work for macOS. Ivanti Mobile@Work for macOS polls Ivanti EPMM periodically to check whether there are any scripts awaiting execution. If there are scripts in the queue, Ivanti Mobile@Work for macOS downloads and runs the scripts on macOS devices according to settings you define on Ivanti EPMM. Ivanti Mobile@Work runs the scripts as the device user or as root, depending on how you signed the script. Ivanti Mobile@Work then returns the script execution results to Ivanti EPMM, which are shown in the audit logs.

Components required to run shell scripts on macOS devices

To run shell scripts on macOS devices, you need:

- Ivanti Mobile@Work for macOS on macOS devices
- Ivanti EPMM 9.7.0.0, or supported newer versions, configured with mutual authentication
- Script signing tool, provided by Ivanti, Inc
- macOS script configuration on Ivanti EPMM
- macOS script policy on Ivanti EPMM

Main steps of running shell scripts on macOS devices

Running shell scripts on macOS devices involves the following main steps:

Creating certificates for your shell scripts for macOS

This section includes the following main steps:

Creating a certificate authority for your macOS scripts

Create a certificate authority for signing your macOS scripts.You can optionally use the certificate authority you create as your default.

Procedure

1. On a macOS device, run the Keychain Access utility.

2. From the Keychain Access menu, choose **Certificate Assistant** > **Create a Certificate Authority**.

3. Enter a name for the certificate authority, noting it for later use.

4. For the user certificate type, select **Code Signing**.

5. Enter your email address.

6. In Keychain Access, select **My Certificates** to view the certificate authority.

Related topics

Creating a certificate authority using Keychain Access

Creating a script signing identity for your macOS scripts

Create a signing identity certificate so that you can sign your scripts.

Before you begin

"Creating a certificate authority for your macOS scripts" on the previous page

Procedure

1. On a macOS device, run the Keychain Access utility.

2. From the Keychain Access menu, choose **Certificate Assistant** > **Create a Certificate**.

3. Enter a name for the signing identity, noting it for later use.

4. For the identity type, select **Leaf**.

5. For the certificate type, select **Code Signing**.

6. Create the leaf.

7. Choose an issuer. Select the certificate authority you created.

8. Create the certificate.

9. In Keychain Access, select **My Certificates** to view the signing identity you created.

Related topics

Code Signing Tasks on the Apple Developer website

Exporting the CA public key certificate for your macOS scripts

You must now export the certificate authority you created and upload it to Ivanti EPMM.

Before you begin

"Creating a script signing identity for your macOS scripts" above

Procedure

1. On a macOS device, run the Keychain Access utility.

2. Select **Certificates** in the left pane.

3. Select the certificate of the certificate authority you created in "Creating a certificate authority for your macOS scripts" on page 809.

4. Select **File > Export Items**.

5. For **File Format**, select **Certificate (.cer)**.

6. Select **Save**.

   Note where you saved the .cer file

7. Open the Terminal application.

8. Navigate to the directory where you exported the certificate.

9. Execute the following openssl command to convert the .cer file to a .pem file. (In this example, the certificate was saved in Certificate.cer.)

```
openssl x509 -inform der -in Certificate.cer -out root.pem
```

You will later upload this .pem file to Ivanti EPMM.

Creating a shell script for macOS

You can create any shell script you want for execution on macOS devices, as long as the script can run within a shell script file. You can use wrappers if necessary. The execution of binary files from within a shell script is not supported.

You can copy and modify existing scripts, or create your own.

Before you begin

Before you can run shell scripts on macOS devices, you must have instructed macOS device users to:

- Download and install Ivanti Mobile@Work for macOS

- Register with Ivanti EPMM using Ivanti Mobile@Work for macOS

Related topics

"Registering macOS devices with Ivanti EPMM using Ivanti Mobile@Work for macOS" on page 40

Shell scripting primer (on the Apple website)

Testing your shell script for macOS

Ivanti, Inchighly recommends you test your shell scripts before running them on macOS devices to ensure their robustness and quality. Run your script locally, and correct any errors that result.

Signing your shell script for macOS

Ivanti EPMM requires you to sign your shell scripts using the Ivanti EPMM script signing tool.

Before you begin

"Testing your shell script for macOS" above

Procedure

1. Download the Ivanti EPMM signing tool and place it in your `$PATH`. You can download it from [Ivanti Support]; a login may be required.
2. Open a terminal window.
3. Sign your script by issuing a command with the following syntax:

   `sign -s "My Signer"  -r yes` *script_name*`.sh`

   `"My Signer"` is the signing identity you created in "Creating certificates for your shell scripts for macOS" on page 809

   -r yes is an optional parameter. Include it only if you want to run the script as root because the script requires root permissions. Without `-r yes`, the script runs as the device user. This parameter is applicable to Ivanti Mobile@Work 1.1.0 for macOS or supported newer versions.

   script_name is the name of your macOS script.

The script signing tool produces a signed script called *script_name*`.sh.p7s`, where *script_name* is the name of the script.

Configuring a macOS script configuration on Ivanti EPMM

Create a macOS script configuration for your macOS shell script. You can upload only one script file per configuration, but the file can include more than one signed shell script. You must then apply the macOS script configuration to a label or labels, so that you can run the script or set of scripts on a subset of macOS devices.

> ℹ️ After you have created a macOS script configuration, you cannot edit the configuration, for example, by uploading a different script file to a configuration you had previously created. A macOS script configuration is read-only after you create and save it. If you want to change a particular macOS script configuration, delete the old configuration and create a new one.

Procedure

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

2. On the **Configurations** page, click **Add New**, and select **Apple > macOS Only > Mobile@Work macOS Script**.

3. In the Ivanti Mobile@Work macOS Script Configuration dialog box, add your macOS shell script.

Item	Description
Name	Enter a name for the configuration.
Description	Enter an explanation of the purpose of this configuration.
Select File	Click **Browse** and select the signed script file you want to use.

4. Select **Save**.

5. Select the configuration you just created, and apply it to the relevant labels.

Configuring a macOS script policy on Ivanti EPMM

Create a policy for the macOS shell scripts you intend to run on macOS devices. The macOS script policy includes the root certificate used to sign your scripts. Ivanti Mobile@Work for macOS uses the certificate to validate the scripts before running them.

Procedure

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

2. On the **Policies** page, select **Add New.**

3. Select **iOS and macOS > macOS Only > Mobile@Work macOS Script**.

4. In the Add Mobile@Work macOS Script Policy dialog box, add the root certificate for your macOS shell script, as described in "Exporting the CA public key certificate for your macOS scripts" on page 810.

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**.
	Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available.
	Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list.
	For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.
Upload Public Key	Upload the .pem certificate file to the script policy.
Public Key	Once uploaded, the public key displays here.
Max Response Size (in KB)	Enter the maximum response size for any macOS scripts you run on devices. The maximum response size limits the size of data Ivanti Mobile@Work for macOS returns to Ivanti EPMM after running a script. This is the stdout or stderr data that is returned when running a macOS script.

5. Select **Save**.

6. Select the policy you just created, and apply it to the relevant labels.

Viewing macOS script execution logs

You can confirm the execution of macOS scripts sent to macOS devices by searching the logs for macOS script execution results. Each log entry has a status, indicating whether the script ran successfully, and details regarding the output of the script execution.

Procedure

1. Select **Logs** > **Audit Logs**.
2. On the list of filters, click **Device**.
3. Select the check box for **Ivanti Mobile@Work client script execution results**.

4. Click **Search**.

    The logs for macOS script execution are displayed.

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 820
- "Customizing Event Center messages" on page 838
- "Viewing and Exporting Events" on page 845

ⓘ The features described in this section are supported on macOS devices, unless otherwise stated.

About events

The Event Center enables Ivanti EPMM 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, email, or through a push notification. 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 the 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" below
- "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 819
- "Setting alert retries" on page 819

Creating an event

Procedure

To create an event, in the Admin Portal:

1. Go to **Logs > Event Settings**.

2. Select **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 820 for information on the settings.

5. Select **Save**.

Editing an event

Procedure

1. Go to **Logs > Event Settings**.

2. Select the event you want to edit.

3. Select **Edit**.

4. Make your changes.

5. Select **Save.**
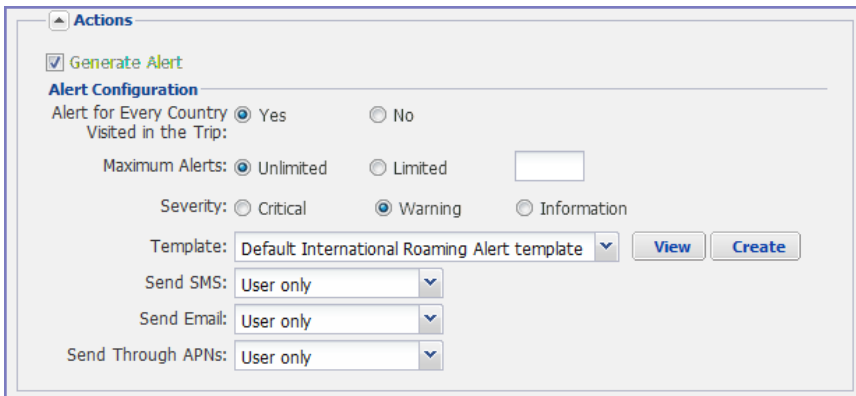
Deleting an event

Procedure

1. Go to **Logs > Event Settings**.

2. Select the event you want to delete.

3. Select **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.

For each type of alert (i.e. SMS, email, and APNs push notification), 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 administrator 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. Ivanti EPMM 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

ℹ️   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 Ivanti EPMM 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. Select **Save**.

Setting Ivanti EPMM 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. In 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. Select **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" below

- "SIM changed event settings" on page 823

- "Memory size exceeded event settings" on page 825

- "System event settings" on page 827

- "System event field description" on page 827

- "Policy violations event settings" on page 830

- "Policy violations event field description" on page 831

- "Device status event settings" on page 835

International roaming event settings

This event type is not supported for macOS devices.

> International roaming detection is not supported for dual-mode devices (that is, devices that switch between GSM and CDMA).

Procedure

To create an international roaming event, in the Admin Portal:

1. Go to **Logs > Event Settings**.

2. Select **Add New**.

3. Select **International Roaming Event** from the drop-down menu. The New International Roaming Event dialog box opens.

4. Use the guidelines in the table below to create an international roaming event.

5. Select **Save**.

> If more than one international roaming event applies to a device, only the last one you edited and saved is triggered.

TABLE 1. INTERNATIONAL ROAMING EVENT OPTIONS

Field	Description
Name	Identifier for this notification.
Description	Additional text to clarify the purpose of this notification.
Generate Alert	Turns on/off the alert defined for this event.
Alert for Every Country Visited in the Trip	Applies a compliance action for each country visited after the user leaves the home country.
Maximum Alerts	Specifies whether there is a limit on the number of alerts generated for all countries within a given trip. If you select **Limited**, then you can specify the number of alerts to allow. Once the user returns to the home country, the count is returned to 0.
Severity	Specifies the severity defined for the alert: **Critical**, **Warning**, and **Information**.
Template	Specifies the template to populate the resulting alert. Select **View** to display the content of the current template. Select an alternate template from the drop-down or select **Create** to create a new template. See "Customizing Event Center messages" on page 838 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 admin, 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 admin, 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 via, and whether to send it to the user, the admin, 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 displays. 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	Associate this event with the selected labels. See the "Using labels to establish groups" section in the *Getting Started with Ivanti EPMM* for more information.
Search Users	Enter the user ID to find devices to which you want to apply this event.
Apply to Users	Associate this group of settings with the selected users.
Search Admins	Enter the administrator ID to find devices to which you want to apply this event.
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.

SIM changed event settings

This event type is not supported for macOS devices.

Procedure

1. Go to **Logs > Event Settings**.

2. Select **Add New**.

3. Select **SIM Changed Event** from the drop-down menu. The New SIM Changed Event dialog box opens.

4. Use the guidelines listed in the table below for creating a SIM change event.

5. Select **Save**.

> ℹ️ If more than one SIM changed event applies to a device, only the last one you edited and saved is triggered.

TABLE 2. GUIDELINES FOR CREATING A SIM CHANGE EVENT

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this event.
Generate Alert	Turns on/off the alert defined for this event.
Severity	Specifies the severity defined for the alert: Critical, Warning, and Information.
Template	Specifies the template to populate the resulting alert. Select **View** to display the content of the current template. Select an alternate template from the drop-down or select **Create** to create a new template. See "Customizing Event Center messages" on page 838 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 admin, 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 admin, 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 admin, 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	Associate this event with the selected labels. See the "Using labels to establish groups" section in *Getting Started with Ivanti EPMM* for more information.
Search Users	Enter the **user ID** to find devices to which you want to apply this event.
Apply to Users	Associate this group of settings with the selected users.
CC to Admins	If you selected "Admin only" or "User + Admin", then the **CC to Admins** section displays. Use this section to specify administrative users who should receive the alert.

Memory size exceeded event settings

This event type is not supported for macOS devices.

This section address how to create a memory size exceeded event.

Procedure

1. Go to **Logs > Event Settings**.

2. Select **Add New**.

3. Select **Memory Size Exceeded Event** from the drop-down menu.

4. Use the guidelines in the table below to create a memory size exceeded event.

5. Select **Save**.

> Memory exceeded events are sent only once per week when the configured memory limit is reached. If more than one memory size exceeded event applies to a device, only the last one you edited and saved is triggered.

TABLE 3. GUIDELINES FOR A MEMORY SIZE EXCEEDED EVENT.

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Used Memory Size Exceeds	Specifies the percentage of total memory that triggers the alert.
Generate Alert	Turns on/off the alert defined for this event.

Field	Description
Alert every	Specifies the time, in days, after which the alert count is reset.
Severity	Specifies the severity defined for the alert: **Critical**, **Warning**, and **Information**.
Template	Specifies the template to populate the resulting alert. Select **View** to display the content of the current template. Select an alternate template from the drop-down or select **Create** to create a new template. See "Customizing Event Center messages" on page 838 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 admin, 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 admin, 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 admin, 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	Associate this event with the selected labels. See the "Using labels to establish groups" section in *Getting Started with Ivanti EPMM* for more information.
Search Users	Enter the user ID to find devices to which you want to apply this event.
Apply to Users	Associate this group of settings with 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.

System event settings

A system event applies a compliance action when a component of an Ivanti EPMM implementation is not working. System alerts are intended for relevant administrators.

Procedure

1. In the Admin Portal, go to **Logs > Event Settings**.

2. Select **Add New**.

3. Select **System Event** from the drop down menu.

4. Use the guidelines in "System event field description" below to complete the form:

5. Select **Save**.

System event field description

TABLE 122. 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 Ivanti EPMM is unable to contact the Sentry.
Ivanti gateway is unreachable	Select this option to send an alert if Ivanti EPMM cannot connect to the Ivanti EPMM gateway.
LDAP server is unreachable	Select this option to send an alert if Ivanti EPMM cannot connect to any of the configured LDAP servers.
DNS server is unreachable	Select this option to send an alert if Ivanti EPMM cannot connect to one of the configured DNS servers.
Mail server is unreachable	Select this option to send an alert if Ivanti EPMM cannot connect to the configured SMTP server.
NTP server is unreachable	Select this option to send an alert if Ivanti EPMM 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 MDM APNS/Client (iOS only), Admin Portal, and device certificates.

TABLE 122. SYSTEM EVENT FIELD DESCRIPTIONS (CONT.)

Field	Description
Provisioning Profile Expired	Generates an alert if an iOS provisioning profile distributed via Ivanti EPMM has expired. In general, this profile will be associated with an in-house app.
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 *Ivanti EPMM 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. Ivanti EPMM 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 Ivanti EPMM 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.
Certificate Revoked (MDM APNS)	Generates an alert if an iOS Mobile Device Management (MDM) Apple Push Notification Service (APNS) certificate has been revoked.
Apple License Percentage Used. Alert Threshold	Generates an alert if the licenses used for an iOS app purchased via Apple Licenses reaches the specified level.

TABLE 122. SYSTEM EVENT FIELD DESCRIPTIONS (CONT.)

Field	Description
	The default threshold is 99 percent. An alert is generated when 99 percent of the license for any Apple License purchased-app have been redeemed.
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 337 and "Creating an event" on page 817 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. Select **View** to display the content of the current template.
	Select an alternate template from the drop-down or select **Create** to create a new template. See "Customizing Event Center messages" on page 838 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 via Apple Push Notification service, and whether to send it to the user, administrator, or both.

TABLE 122. SYSTEM EVENT FIELD DESCRIPTIONS (CONT.)

Field	Description
	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 Ivanti EPMM*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

Procedure

1. In the Admin Portal, go to **Logs > Event Settings**.

2. Select **Add New**.

3. Select **Policy Violation Event** from the drop-down menu. The New Policy Violations Event dialog box opens.

4. Follow the guidelines in "Policy violations event field description" below to complete the form.

5. Select **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 123. POLICY VIOLATION EVENT FIELD DESCRIPTION

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Connectivity	

TABLE 123. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

Field	Description
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**.
Data Protection/Encryption - iOS - Android	
Data Protection/Encryption is disabled	Applies a compliance action if data protection/encryption is disabled on an iOS device.
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	

TABLE 123. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

Field	Description
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 Ivanti EPMM deployment.
Ivanti 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.
macOS	
Disallowed macOS version found	Applies a compliance action if Ivanti EPMM finds a registered device running a prohibited version of macOS.
Device MDM deactivated	Applies a compliance action if Ivanti EPMM detects that MDM (Mobile Device Management) has been deactivated on a registered macOS device.
FileVault encryption disabled	Applies a compliance action if Ivanti EPMM 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.

TABLE 123. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

Field	Description
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 Ivanti 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. Select **View** to display the content of the current template. Select an alternate template from the drop down or select **Create** to create a new template. See "Customizing Event Center messages" on page 838 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 via Apple Push Notification service, 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.

TABLE 123. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

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 Ivanti EPMM* 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. Select **Add New**.

3. Select **Device Status Event** from the drop-down menu. The New Status Event dialog box opens.

4. Use the following guidelines to complete the form:

5. Select **Save**.

---

i   If more than one device status event applies to a device, only the last one you edited and saved is triggered.

TABLE 4. GUIDELINES FOR DEVICE STATUS EVENTS

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 • Work schedule policy applied (Android and iOS)

Field	Description
Actions	
Severity	Specifies the severity you define for this alert. Select **Critical**, **Warning**, or **Information**.
Template	Specifies the template to populate the resulting alert. Select **View** to display the content of the current template. Select an alternate template from the drop-down or Select **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.
Apply to Labels	Send the alert to users in the selected labels. See the "Using labels to establish groups" section in *Getting Started with Ivanti EPMM* 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.

Related Topics

"Work Schedule policy" on page 285

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**.
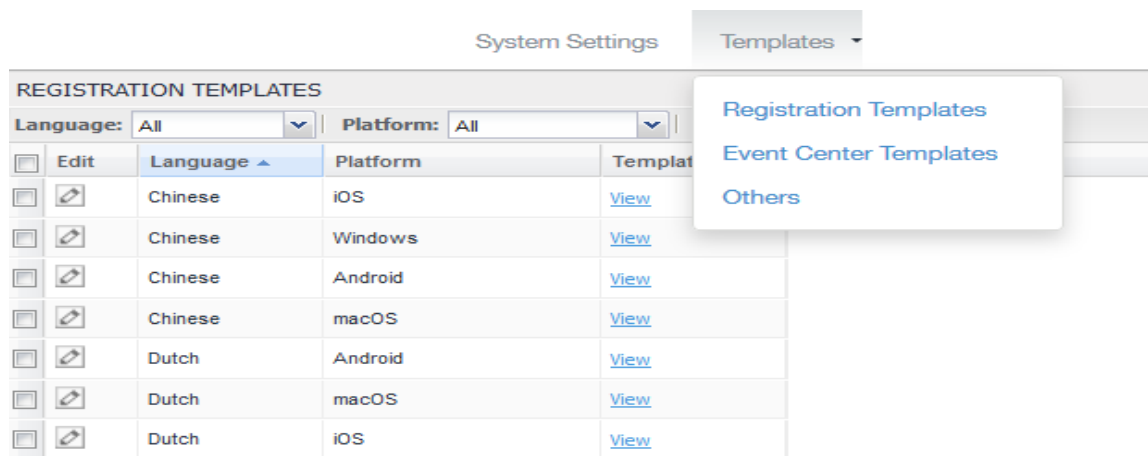
2. Select **Event Center Templates**.

   This list includes the default templates for each Event Center type. Default templates are not editable.

3. Select the **View** link for the message template you want to view.

The $SERVER_IDENT variable was removed from the $DEFAULT_POLICY_VIOLATION_MESSAGE variable and is now part of the Event Center template. Add the $SERVER_IDENT variable to the template to display server identity in an alert message. The $SERVER_IDENT variable is also a substitution variable in compliance actions. Use of this variable depends on whether the compliance action was updated from version 1 to version 2. For V1 actions, include this variable in the Event Center template or as part of the alert message text in the compliance action. For V2 actions, include this variable only as part of the alert message text in a compliance action.

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.

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.

ℹ️ 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.

---

6. Select **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. Select **Templates > Others**.

   The Others template page displays.

3. Find the language you want the template to display in and then select the **Edit** icon.

   The Edit Template dialog box opens. For this example, the Edit Template: Wipe (English) dialog box opens.

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" on the next page

5. When finished, select **Save**.

Related topics

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 select the **Variables Supported** link to display this information. Note that, unlike variables used for registration variables, Event Center variables do not end with $.

TABLE 124. 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 $SEVERITY $USER_NAME
Memory Size Exceeded	$FREE_MEMORY_SIZE $MEMORY_SIZE_LIMIT $PHONE_NUMBER $SEVERITY $TOTAL_MEMORY_SIZE

TABLE 124. VARIABLES IN EVENT CENTER MESSAGES (CONT.)

Template Type	Required Variables
	$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 125. 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 Ivanti EPMM, 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. ⓘ Due to the length limits of SMS and APNs, 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.

TABLE 125. VARIABLE DESCRIPTIONS (CONT.)

Variable	Description
$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 select 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**.

2. Select the edit icon for the custom template you want to edit.

3. Make your changes. See Sending a company-branded email

4. Select **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. Select **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 126. 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.
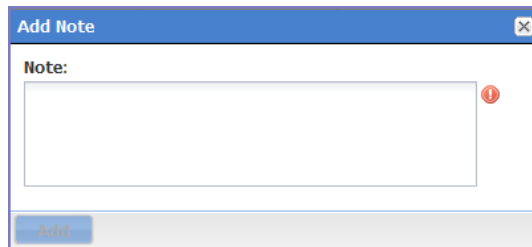
Exporting event history

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 Ivanti EPMM and devices

This section addresses troubleshooting various aspects of Ivanti EPMM and devices.

ℹ️   The features described in this section are supported on macOS devices.

- "Pushing and removing device profiles" below
- "About Ivanti EPMM logs" on page 850
- "Audit log information" on page 859
- "Audit Logs use cases" on page 873
- "MDM Activity" on page 877
- "Certificate Management" on page 878
- "Service Diagnostic tests" on page 881
- "Encrypting device logs with your own certificate" on page 805
- "Pull client logs for client devices" on page 883

Pushing and removing device profiles

Push Profile is an option that lists the device's configurations and policies. Administrators can essentially 'force push' the selected profile and/or configurations associated to the device. This is similar to an override if something failed and the administrator does not want to do a full check-in, but instead just send the selected profile(s) to the device.

Remove Profile is like Push Profile except the selected profile and/or configuration is excluded from the device. Remove Profile can only be used for configurations, not policies.

This feature is helpful for troubleshooting specific devices, for example, overriding the default label for that device. Applicable to iOS and macOS devices only.

Procedure

1. Expand the device details panel by clicking the up arrow next to the check box.

2. Click the **Push/Remove Profiles** button, found at the top left of the Device Details panel. The device profile page opens.

3. The profiles/configurations are displayed by Name, Type and Status.

4. Select the profile(s) / configuration(s) and then, above the table,

   a. select the **Push Profile** link. The Status field updates with Pending, Applied, or Failed.

   b. select **Remove Profile** link. The Status field of the selected profile updates with Excluded.

      To re-instate the excluded profile / configuration, select it and then click the **Push Profile** link.

For the 11.9.0.0 release, there are two new Push/Remove user profiles:

- **Push profiles in device details** - Administrators can push profile information to a device or custom space using this role.

- **Remove profiles in device details** - Administrators can remove profile information from a device or custom space using this role.

Troubleshooting configurations

If you are having trouble with your configuration, consider checking the following:

- Look in the Audit logs (see "About Ivanti EPMM logs" below) and / or MDM logs (see "MDM Activity" on page 877). Look for the managed app configuration installation request. Once there, note what the error statement is.

- Depending upon the error, in order to proceed, you will need to consider:

  - Is the app configuration correct? If not, can it be corrected?

  - Is the "managed app" actually not managed?

  - Is the managed app the wrong version?

  - Is a substitution variable not being updated in the managed app configuration? What type of substitution variable was it? See "Supported variables" on page 760.

About Ivanti EPMM 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 Ivanti EPMM instance. Ivanti EPMM logs many actions that can impact your Ivanti EPMM 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 Ivanti EPMM log entries to find the information you need.

- **Audit Logs**: for Ivanti EPMM device management entries

- **MDM Activity**: for iOS and macOS entries

- **Certificate Management**: for certificate-related entries

Note the following:

- Logs are stored in the Ivanti EPMM file system, not in the Ivanti EPMM database. Therefore, the size of the logs does not impact Ivanti EPMM performance.

- Ivanti EPMM 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 Ivanti EPMM 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

Searching the information in the audit logs

Procedure

1. In Admin Portal, go to **Logs**.

   Ivanti EPMM 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**.
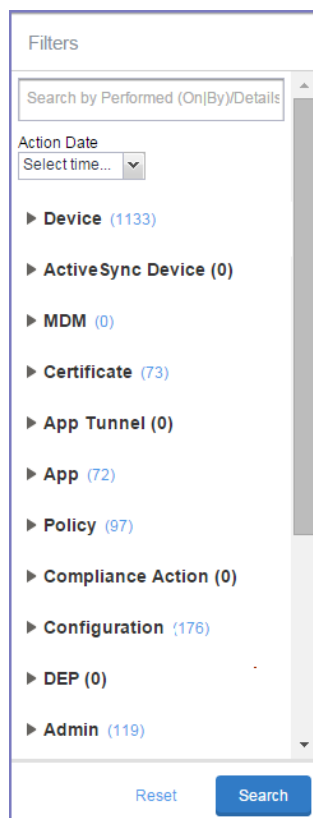
3. Alternatively, click to expand one of the information types that you want to view (for example, **App**).

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 Ivanti 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 857). 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, Ivanti EPMM will display a message asking you to reset your time criteria because 1 hour ago happens after 1 day ago.

TABLE 127. 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 right column, select:	In the left column: • Select **April 10th** from the calendar In the right column: • Select **1 day ago**	Displays all events matching your criteria that occurred between April 10th and 24 hours ago.

TABLE 127. TIME CRITERIA SELECTION EXAMPLES (CONT.)

Time criteria selected	Value selected	Result
• a time interval from **Select time**		
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 Ivanti EPMM records for your Ivanti EPMM 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 852 for details.

Procedure

1. In Admin Portal, go to **Logs**.

   Ivanti EPMM displays the Audit Logs page. The information panel displays:

   Action (for example, Admin Portal sign-in)

- **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 Ivanti EPMM. 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 Ivanti EPMM retains log information.

3. Click **Apply**.

Related topics

- "Audit Logs use cases" on page 873
- "App information" on page 867

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**
- **Content**
- **VPP**
- **Custom Attributes**
- **Compliance Policy**
- **E-FOTA**
- **Migration**
- **MTD (Mobile Threat Defense)**
- **Access Integration**
- **Derived Credential Provider**
- **Zebra FOTA**

Before and after log information

Changes in the modification history for configurations, policies, labels, compliance groups, rules, and actions attributes are displayed in the **Configuration Details** page, which shows before and after content. You can view the logs from the **Ivanti EPMM Logs > Audit Logs** page. Logs with before and after values display an icon you can click to see the new information. The new log information is generated for the following actions:

- **Create** - The "Before" column will be empty.

- **Edit** or **change** - Both before and after values display.

- **Delete** - The "After" column will be empty.

In Ivanti EPMM version 11.10.0.0 and later versions, the before and after values can be readily identified from unchanged content because they are highlighted and in blue text in the **Changes - Before & After** panel.

To display the **Changes - Before & After** panel, click on any policy or configuration in the **Policies & Configurations > Configurations** tab to display the **Configuration Details** side panel to the right of the window. Click **Modification History**, and click the box corresponding to the change.

Related topics

- "About Ivanti EPMM logs" on page 850
- "Audit Logs use cases" on page 873
- "App information" on page 867

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.
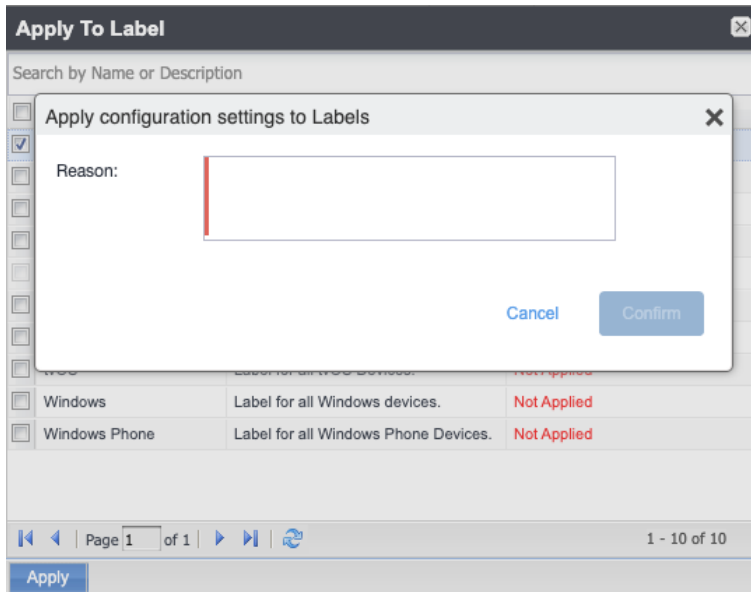
Example text to enter would be a change ticket order number. This information then displays in the Audit logs, in the Details column as "Reason."

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 Ivanti EPMM.*

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.

- **Ivanti 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 Ivanti EPMM.

- **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 Ivanti EPMM.
- **Sign Out**: End session between the client and Ivanti EPMM.
- **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 Ivanti EPMM actually sends the request to the device. Ivanti EPMM sometimes delays sending requests to regulate Ivanti EPMM 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 Ivanti EPMM.

- **Remove**: End the association between the Ivanti EPMM 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 an Ivanti EPMM 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.

> ℹ️ This MDM log information is also provided in the **Logs > MDM Activity** tab.

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 Ivanti EPMM.
- **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.

> ℹ 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

These events do not apply to Mac devices.

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.

ⓘ   For iOS devices, Ivanti EPMM does not log the action if users:

- install apps using Apps@Work
- uninstall apps

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 Ivanti EPMM.
- **Import Policy**: Import a policy into Ivanti EPMM.

- **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 Ivanti EPMM.
- **Import Configuration**: Import a configuration to Ivanti EPMM.
- **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.

Apple Device Enrollment related events

These events are only for iOS devices.

- **Account Sync Completed**:
- **Add Apple Device Enrollment Account**: Specify an Apple Device Enrollment account for use with Ivanti EPMM.

- **Add Apple Device Enrollment Profile**: Specify an Apple Device Enrollment profile for use with Ivanti EPMM.
- **Assign Devices To Apple Device Enrollment Profile**: Associate devices to an Apple Device Enrollment profile.
- **Check Updates For Apple Device Enrollment Accounts**: Sync with Apple servers to update device enrollment information.
- **Delete Apple Device Enrollment Account**: Remove an Apple Device Enrollment account from Ivanti EPMM.
- **Delete Apple Device Enrollment Profile**: Remove an Apple Device Enrollment profile from Ivanti EPMM.
- **Disable iOS Education**:
- **Enable iOS Education**:
- **Modify Apple Device Enrollment Account**: Make changes to an Apple Device Enrollment account associated with Ivanti EPMM.
- **Modify Apple Device Enrollment Profile**: Make changes to an Apple Device Enrollment profile associated with Ivanti EPMM.
- **Sync iOS Education with ASM**:Sync with Apple School Manager.

Administrator 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 administrator access from the user.
- **Modify Space**: Make changes to rules that define a space.
- **Remove Admin From Space**: Remove the administrator 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 Ivanti EPMM user.
- **Delete User**: Remove an Ivanti EPMM user.
- **Link to LDAP User**: Associate a local Ivanti EPMM 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 Ivanti EPMM password.
- **Send Invitation**: Invite a user to register with Ivanti EPMM.
- **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 Ivanti EPMM.
- **Delete Admin LDAP Entity**: Delete an Administrator LDAP entity that has no roles.
- **Delete LDAP**: End the integration between an LDAP server and Ivanti EPMM.
- **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 Ivanti EPMM.

Other events

- **Application Started**: Start Ivanti EPMM services.
- **Application Stopped**: Stop Ivanti EPMM 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 Ivanti EPMM.
- **Delete Label**: Remove a label from Ivanti EPMM.
- **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 Ivanti EPMM and an Integrated Sentry.
- **Add Standalone Sentry**: Establish a relationship between Ivanti EPMM and a Standalone Sentry.
- **Delete Integrated Sentry**: End the relationship between Ivanti EPMM and an Integrated Sentry.
- **Delete Standalone Sentry**: End the relationship between Ivanti EPMM and a Standalone Sentry.
- **Disable Integrated Sentry**: Suspend the interaction between Ivanti EPMM and an Integrated Sentry.
- **Disable Standalone Sentry**: Suspend the interaction between Ivanti EPMM 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 Ivanti EPMM and an Integrated Sentry.
- **Enable Standalone Sentry**: Start the interaction between Ivanti EPMM 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.

Content events

Content events indicate changes to iBooks on Ivanti EPMM. These events apply only to iOS and Mac devices.

- **Add iBook**: Add an iBook to Ivanti EPMM.
- **Apply Label to iBook**: Associate a label with an iBook.
- **Install iBook:** Install an iBook.
- **Modify iBook**: Edit the iBook entry in Ivanti EPMM.
- **Remove iBook**: Delete the iBook from Ivanti EPMM.
- **Remove Label from iBook**: End the association between an iBook and a label.
- **Uninstall iBook:** Uninstall an iBook.

VPP events

VPP events indicate changes made to apps that are part of Apple's Volume Purchase Program (VPP).

- **Account Sync Completed**: Complete a sync for a VPP account.
- **Apply VPP Labels**: Apply VPP labels to the VPP app.
- **Change VPP License Type**: Change the VPP license from user-based to device-based, or vice versa.
- **Remove VPP Labels**: Remove labels associated with the VPP app.
- **Revoke All VPP Licenses**: Revoke all licenses for a VPP app.
- **Revoke VPP License**: Revoke the license for a VPP app from a given device.

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 Ivanti EPMM 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 Ivanti EPMM. A change to app control rules can result in Ivanti EPMM 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
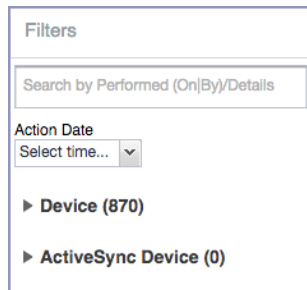
Suppose several of your users report that the personal information on their phones was wiped. How can you figure out how this happened? Using the audit logs, you can check the wipe actions recorded in the logs, and discover:

- Who issued the Wipe commands
- When they occurred
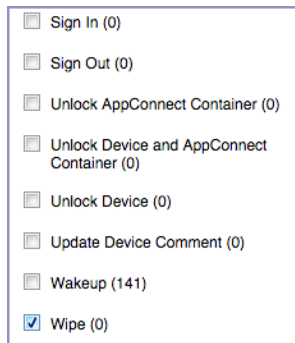
- How many users are impacted

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**.

7. Click **Search**.
8. View the results of the search to determine:

   - When the devices were wiped

   - How many devices were wiped

   - Which administrator 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.
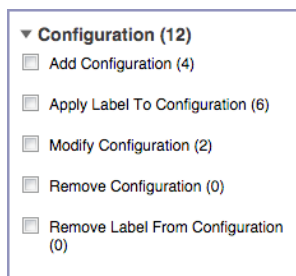
6. Select **Modify Configuration**.

7. Click **Search**.

8. View the results of the search to determine:

   - What changes were made recently to the Exchange policy

   - Which administrator 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 Ivanti EPMM. 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.
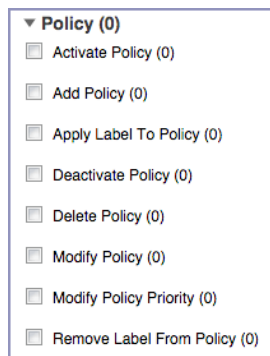
6. Select **Modify Policy**.

7. Click **Search**.

8. View the results of the search to determine:

   - What changes, if any, were made recently to the Security policy

   - Which administrator 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 Ivanti EPMM:

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.
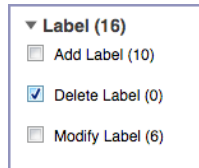
6. Select **Delete Label**.

7. Click **Search**.

8. View the results of the search to determine:

   - What labels, if any, were deleted recently

   - Which administrator user made the changes

MDM Activity

The **Logs > MDM Activity** displays MDM-specific log entries.

> Many of these entries are also available in **Logs > Audit Logs** in the **MDM** category.

Filter the log entries using the following criteria:

- Platform
- Date range
- States
- Actions
- User
- Device
- Error text

- Detail text

- Date range

Viewing Errors

Errors result in the display of a **View Error** link in the **Error** column.

Click the link to display error details.

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 Ivanti 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 Ivanti EPMM, 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

This feature is not supported on iOS Mac devices.

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 Ivanti EPMM instance can connect to these services. An error indicates that you cannot reach the service.

The services checked are:

TABLE 128. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS

Service	Test
AFW	Checks to see if: • Authentication server is reachable. • API server 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.ivanti.com:2196) is not reachable.
APPCONFIG_ COMMUNITY_REPO	Checks to see if the AppConfig Community Repository server is reachable.
APP_GATEWAY	Checks to see if App Gateway server is reachable.
BYPASS	Checks the connection between your Ivanti EPMM instance and the Apple activation lock bypass server
CERTIFICATE ENROLLMENT	Checks to see if: • Certificate Enrollment : System - iOS Enrollment SCEP is reachable.

TABLE 128. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS (CONT.)

Service	Test
	• Certificate Enrollment : System - iOS Enterprise AppStore SCEP is reachable.
	• Certificate Enrollment : System - Windows Phone Enrollment SCEP is reachable.
CONFIGURATIONS	Tests the connection to the Certificate Enrollment server from your Ivanti EPMM instance.
CONNECTOR	Two tests are run: • 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 Ivanti EPMM instance to each Connector configured, checking whether the Connector can communicate with your Ivanti EPMM instance
DEP	Sends a sample GET request to test the connection between your Ivanti EPMM instance and the MDM server using Device Enrollment.
FCM	Checks whether Google Firebase Cloud Messaging (FCM) is reachable from your Ivanti EPMM instance.
HEALTH_ATTESTATION_ SERVICE	Checks if the Health Attestation Service server is reachable.
LDAP	Two tests are run: • Checks LDAP from Ivanti EPMM to verify the communication channel • For each Connector configured, checks the communication channel for the path from the LDAP server to Ivanti EPMM, then Ivanti EPMM to Connector, and finally from Connector to the LDAP server
MAPQUEST	Checks if the MapQuest Service server is reachable.
PROXY	No proxy is configured.
SENTRY	Checks the connection between your Ivanti EPMM instance and the Sentry used (either integrated standalone). As part of this test, the connection between ActiveSync server and Sentry is checked also.

TABLE 128. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS (CONT.)

Service	Test
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 Ivanti EPMM and the Apple License server.

Running Service Diagnostic tests

Procedure

1. Go to **Services > Overview**.
2. To test one or all of the services:
   - Select **Verify All** to test the listed services
   - Select **Verify** next to a specific service to test that service

Pull client logs for client devices

To troubleshoot challenging technical support issues when working with Ivanti, Inc Technical Support, you can pull client logs of an Android or iOS client device without requiring any interaction from the end user. From the Admin Portal, use the Pull client log command to obtain client logs. The Pull client log action as well as the success or failure of the event is captured in the Audit logs. This feature does not work on Windows and chromeOS devices.

> The Pull client log command is not available to delegated administrator roles; only administrators who have the Manage Devices role can use this feature.

When the Pull client logs command is delivered to the device, it instructs the Ivanti Mobile@Work client to collect logs running on the device. This may include logs from all the secure apps running on the device. These logs are pulled to the server's file storage.

Potentially, there is one interaction that may cause a message to be displayed to a device user. If the device has an AppConnect configuration and a number of secure apps installed, then the Ivanti Mobile@Work client may momentarily go to the foreground of the device display and request secure apps logs from the Secure AppManager application. Under these conditions, a message is displayed on the device that states a device administrator is pulling Ivanti Mobile@Work client logs and logs from the secure applications for analysis. Also, the message states that this is a short interruption.

When you have an AppConnect configuration that is running and SecureApps Manager and the SecureApps Manager does not communicate with Ivanti Mobile@Work in a timely fashion, then the end user may be prompted to log in again.

> You can retrieve the client logs from the System Manager. Select **Troubleshooting** > **Logs** in the Export Logs section. Select **Show Tech (All Logs)**. For more information see "Exporting logs" in the *Ivanti EPMM System Manager Guide*.

Before you pull a client log, you may want to set log encryption and then upload this configuration on the device. When you enable log encryption, the client will encrypt logs when the Pull client log action is taken. By default, log encryption is set to off. To set log encryption, you can use the default log encryption certification or custom certification.

To access the Pull client log command:

1. Go to **Devices & Users > Devices**.
2. Select the check box next to a device. You may only select one device.
3. Click the **Actions** button.
4. Select **Pull Client Logs**. The Pull Client Logs dialog box displays. The **Devices** field displays the name of the device that you selected. You cannot add additional devices here.
5. (Optional) Add any notes about this action in the **Notes** section.
6. Click the **Pull Client Logs** button to launch this request to the server.

Office 365

This section contains the overview, policies, configurations, user groups, reports and settings as pertains to Office 365:

Office 365 App Protection overview

Office 365 App Protection provides important Data Loss Prevention (DLP) for Office 365 apps, such as Microsoft Word, Excel, PowerPoint, and so on. It allows administrators to manage policies and configurations that secure data in Office 365 apps on iOS devices.

> ℹ️   Some Graph APIs can be in beta. Use this feature accordingly.

You can manage Office 365 apps by:

- Enforcing PIN for Office 365 apps
- Disabling contacts to sync from Office 365 apps
- Preventing users from printing from Office 365 apps
- Preventing outbound data sharing from Office 365 apps

Prerequisites for using Office 365 App Protection

Before you can use Office 365 App Protection, you must have:

- A valid Ivanti EPMM license.
- A valid Intune subscription or a Microsoft EMS subscription that includes Intune.

- A valid Office Enterprise or Business subscription with access to Office 365 apps on a mobile device.

- One or more Office 365 apps.

- Synced your Active Directory users to your Azure Active Directory.

- One Drive for Business installed on devices to protect data on Word, Excel, and PowerPoint.

- Intune Company Portal app installed on Android devices.

- Device users are not required to sign in, but this app must be installed on the device to protect data on device.

Office 365 App Protection window

> Before you register Ivanti EPMM as an Azure app, only the **Services > Microsoft Graph > Settings** tab is enabled. Once you register Ivanti EPMM as an Azure app, all the tabs are enabled.

Access the Office 365 App Protection window by logging into the Admin Portal and going to Services > Microsoft Graph. This window includes the following options:

- **Policies**: Use this tab to add and manage Office 365 DLP policies. You can perform the following actions on each policy:

    - Assign one or more User groups to the policy.

    - Assign apps to the policy.

    - Delete the policy.

  See "Adding Office 365 App Protection policies" on the next page for details on how to add a Office 365 App Protection policy.

- **Configurations**: Use this tab to add and manage Office 365 DLP configurations. You can perform the following actions on each policy:

    - Assign one or more User groups to the configuration.

    - Assign apps to the configuration.

    - Delete the configuration.

  See "Office 365 App Protection configurations" on page 896 for details on how to add a Office 365 App Protection configuration.

- **User Groups**: Use this tab to search for and view user groups available to add to a policy or configuration.

- **Reports**: Use this tab to view and download user and app reports and manage wipe requests. These reports are populated with data that comes from Azure Active Directory during real-time syncs.

- **Settings**: Use this tab to register Ivanti EPMM as an Office 365 app. These reports are populated with data that comes from Azure Active Directory during real-time syncs.

Office 365 App Protection policies

Once you register Ivanti EPMM as an Azure app you can add and manage Office 365 App Protection policies in the Microsoft Azure cloud for Office 365 apps.

This section includes the following topics:

- "Adding Office 365 App Protection policies" below
- "Editing Office 365 App Protection policies" on the next page
- "Managing Office 365 App Protection policies" on the next page
- "Add Office 365 App Protection policies window" on page 889

ⓘ Before using this feature, complete the prerequisites described in the following section: *"Prerequisites for using Office 365 App Protection" on page 885*.

Related topics

- "Office 365 App Protection overview" on page 885
- "Office 365 App Protection configurations" on page 896
- "Office 365 App Protection user groups" on page 898
- "Office 365 App Protection reports" on page 899
- "Office 365 App Protection settings" on page 905

Adding Office 365 App Protection policies

Policies use data populated from Azure Active Directory during real-time syncs.

Procedure

1. Log into the Admin Portal.

2. Go to **Services > Microsoft Graph > Policies > Add**.

3. Complete the **App protection policies** form.

   Refer to "Add Office 365 App Protection policies window" on page 889 for details.

4. In the "Compliance Actions" on page 894 section, select a Setting, enter the value, and select an Action. Refer to the "App protection policies fields " on page 890table.

5. Select **+Add** to configure additional compliance actions.

6. Select **Save** to add the policy to the list of DLP policies on the **Policies** table.

Editing Office 365 App Protection policies

Policies use data populated from Azure Active Directory during real-time syncs.

Procedure

1. Log into the Admin Portal.

2. Go to **Services > Microsoft Graph > Policies**.

3. Select the name of a policy you want to edit.

4. Complete the **App protection policies** form.

   Refer to "Add Office 365 App Protection policies window" on the next page for details.

5. In the "Compliance Actions" on page 894 section, select a Setting, enter the value, and select an Action. Refer to the "App protection policies fields " on page 890table.

6. Select **+Add** to configure additional compliance actions.

7. Select **Save** to save the policy edits.

Managing Office 365 App Protection policies

You can take any of the following actions on each Office 365 App Protection policy:

- Assign User Groups
- Assign Apps
- Delete Policies

Procedure

1. Log into the Admin Portal.

2. Go to **Services > Microsoft Graph > Policies**.

3. Locate a policy you want to manage and go to the **Actions** column.

4. Assign user groups to the App Protection policy.

    a. Select the **Assign User Groups** icon.

    b. Search for user groups.

    c. Select one or more user groups to add to the policy.

    d. Select **Save**.

5. Assign Office 365 apps to the app protection policy.

    a. Select the **Assign Apps** icon.

    b. Search for apps.

    c. Select one or more apps to add to the policy.

    d. Select **Save**.

6. Delete an Office 365 App Protection policy.

    a. Select the **Delete Policy** icon.

    b. Select **Yes** to confirm deletion of the policy.

The Office 365 App Protection policies take affect:

- After assigning the policy to a user group.

- A user from the assigned user group logs into an Office 365 app using AAD credentials.

Add Office 365 App Protection policies window

Access this window by logging into the Admin Portal and selecting **Services > Microsoft Graph > Policy** and selecting **Add** or selecting a policy to edit.

The following table summarizes fields and descriptions in the **Add App Policies** window. Also, refer to the "App protection policies fields " on the next page table.

TABLE 129. APP PROTECTION POLICIES FIELDS

Fields	Description
Name	This required field is the name used to track the Office 365 App Protection policy in Ivanti EPMM.
Description	Describes the profile's purpose (optional).
Platform	Select the platform for the Office 365 apps. The options are: **iOS** or **Android**. Some of the other options on this form will change depending on which platform you select. Refer to the relevant platform's Device Management Guide.
Data Relocation	
Prevent iTunes and iCloud backups	Choose **Yes** to prevent this app from backing up data to iTunes and iCloud. Choose **No** to allow this app to back up data to iTunes and iCloud. (The default is **Yes**.)
Allow app to transfer data to other apps	Use this option to specify what apps can receive data from this app. The options are listed below. • **Policy managed apps**: Allow transfer only to other policy-managed apps. • **All apps**: Allow transfer to any app (default.) • **None**: Do not allow data transfer to any app, including other policy-managed apps. • **Policy managed apps with OS sharing**: Only allow transfer only to other policy managed apps and file transfer to other MDM managed apps on enrolled devices. • **Policy managed apps with Open-In/Share filtering**: Allow transfer only to other policy managed apps and filter OS Open-In/Share dialogs to only display policy managed apps. When any of the above options except *All apps* are selected, the exempted apps are listed to the right of the *Allow app to receive data from other apps* field. Modifying these settings changes how data is transferred to other applications.
Allow app to receive data from other apps	Select an option to specify what apps can transfer data to this app. • **Policy managed apps** - Allow app to receive data from only other policy-managed apps. • **All apps With Incoming Org Data** - Treat all incoming data without a user identity as data from your organization.

TABLE 129. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
	• **All apps** Allow app to receive data from other apps (default.) • **None** - Do not allow app to receive data from any app, including other policy-managed apps.
Prevent "Save As "	Select to disable the use of the Save As (a new document) option in any app that uses this policy. De-select if you want to allow the use of Save As. (Default is unchecked.) Selecting Prevent Save As activates the **Select which storage services corporate data can be saved to field**. The options are: • OneDrive for Business • SharePoint • Local Storage
Restrict cut, copy and paste with other apps	Specifies when cut, copy, and paste actions can be used with this app. The options are listed below. • **Blocked**: Do not allow cut, copy, and paste actions between this app and any other app. • **Policy managed apps**: Allow cut, copy, and paste actions between this app and other policy-managed apps. • **Policy managed with paste in**: Allow cut or copy between this app and other policy-managed apps. Allow data from any app to be pasted into this app. • **Any app**: No restrictions for cut, copy, and paste to and from this app. (This is the default.)
Encrypt app data	Select to encrypt app data that is associated with an Intune mobile application management policy, data is encrypted when the device is locked (the operating system provides device-level encryption). When a PIN or fingerprint identification is required, the data is encrypted per the settings in the mobile application management policy. The module used by iOS 7 are FIPS 140-2 certified. These values determine when the data is encrypted: • **When device is locked**: All app data that is associated with this policy is encrypted while the device is locked. (This is the default.)

TABLE 129. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
	• **When device is locked and there are open files**: All app data associated with this policy is encrypted while the device is locked, except for data in the files that are currently open in the app. • **After device restart**: All app data associated with this policy is encrypted when the device is restarted, until the device is unlocked for the first time. • **Use device settings**: App data is encrypted based on the default settings on the device.
Disable contact sync	When this setting is enabled, users cannot sync contacts to the native address book. Default is un-checked.
Disable printing	Select this to block printing protected data from the app. Default is un-checked.
Restrict web content to display in the Managed Browser	Check this to enforce web links in the app to be opened in the Managed Browser app. Uncheck this to open web links in Safari. Default is de-selected.
Block third party keyboards	When this setting is enabled, a third-party keyboard cannot be used with protected apps.
Access	
Require PIN for access	Select this to require users to enter a PIN to access this app. The user is prompted to set up this PIN the first time the app is run. Default is selected, which activates all the fields in the Access section of this page. You can also let users prove their identity by using Touch ID instead of a PIN. When users tries to use this app with their account, they are prompted to provide their fingerprint identity instead of entering a PIN. When this setting is enabled, the App-switcher preview image will be blurred while using the account. (The default is checked.)
Allow simple PIN	**Allow simple PIN**: Check this to allow users to use simple PIN sequences like 1234 or 1111. Choose No to prevent them from using simple sequences. (The default value is checked.) • **PIN length**: Specify the minimum number of digits in a PIN sequence. (The default value is **4**.)

TABLE 129. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
	When the *Require PIN for access* field is de-selected, this field is deactivated.
Allow Touch ID instead of PIN for access (iOS 8+)	Select to allow the device user to use Touch ID instead of PIN for access. Applicable for iOS 8 or supported newer versions. When the *Require PIN for access* field is de-selected, this field is deactivated.
Override Touch ID with PIN after timeout (minutes)	If required, depending on the timeout (minutes of inactivity), a PIN prompt will override Touch ID prompts. If this timeout value is not met, the Touch ID prompt will continue to show. This timeout value specified under "Recheck the access requirements after (minutes of Activity)". On iOS, this feature requires the app to have Intune SDK version 8.1.1 or above. **Inactivity timeout**: Specify a time in minutes after which the PIN will override the use of a Touch ID. When the *Require PIN for access* field is de-selected, this field is deactivated.
Disable app PIN when device PIN is managed	Select to disable the app PIN when a device lock is detected on an enrolled device. If you select this option, it overrides the requirements for PIN or Touch ID. (The default is unchecked.) When the *Require PIN for access* field is de-selected, this field is deactivated.
Require corporate credentials for access	Select to require corporate credentials instead of a PIN for app access. Not selecting this option overrides the requirements for PIN or Touch ID. The user will be prompted to provide their corporate credentials. (The default is unchecked.)
Recheck the access requirements after (minutes)	Timeout for access requirements is measured in terms of the time of inactivity between any policy-managed application. • **Timeout**: Enter the number of minutes before the access requirements (defined earlier in the policy) are rechecked. For example, an administrator turns on PIN in the policy, which means a when device user opens a app, a PIN must be entered. When using the Recheck the access requirements setting, the device user would not have to re-enter the PIN on any app for another 30 minutes. (The default is 30.)

Compliance Actions

Use the Compliance Actions Settings to set the security requirements for your access protection policy. Several settings are provided with pre-configured values and actions.

Procedure

1. Select a Setting, enter the value, and select an Action. Refer to the table below.

2. Select **+Add** to configure additional compliance actions.

3. At the top of the Policies tab, select **Save**.

TABLE 130. COMPLIANCE ACTION SETTINGS

Setting	Description
Max PIN attempts (default)	Specify the number of tries the device user has to successfully enter the correct PIN before the configured action is taken. (Default value is 30 minutes.) Actions include: • **Reset PIN** - The user must reset their PIN. • **Wipe data** - The user account that is associated with the application is wiped from the device.
Offline grace period (default)	This is the number of minutes that apps can run offline. Specify the time (in minutes) before the access requirements for the app are rechecked. After this period is expired, the app will **Block Access**. The default is 720 minutes (12 hours.)
Offline grace period (default)	This is the number of minutes that apps can run offline. Specify the time (in days) before the access requirements for the app are rechecked. After this period is expired, the app will **Wipe data**. The default is 90 days.
Jailbroken/rooted device	• **Block access** - Prevent this app from running on jailbroken or rooted devices. The device user continues to be able to use this app for personal tasks, but will have to use a different device to access data in this app. • **Wipe data** - The device user account that is associated with the application is wiped from the device
Min OS version	Select this to require a minimum operating system to use this app. Enter the value in the following format [major].[minor] and select one of the following actions:

TABLE 130. COMPLIANCE ACTION SETTINGS (CONT.)

Setting	Description
	• **Block access** - The device user will be blocked from access if the version on the device does not meet the requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device. • **Warn** - The user will see a notification if the operating system version on the device does not meet the requirement. This notification can be dismissed.
Min App version	Check this option to require a minimum app version to use the app. The user will be blocked from access if the app version on the device does not meet the requirement. • **Block access** - The device user will be blocked from access if the app version on the device does not meet this requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device. • **Warn** - The user will see a notification if the app version on the device does not meet the requirement. This notification can be dismissed.
Min SDK version	Select to require devices to have a minimum iOS security patch released by Apple. The value must be in the following format: [Major].[Minor] or [Major].[Minor].[Build] or [Major].[Minor].[Build].[Revision] Example: 1.5 or 1.5.50 or 1.5.50.101 Set the Action: • **Block access** - The device user will be blocked from access if the iOS version on the device does not meet this requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device.
Device model(s)	Specify a device manufacturer that is required to use this app. Actions include: • **Block access** - Only devices that match the specified manufacturer can use the app. All other devices are blocked.

TABLE 130. COMPLIANCE ACTION SETTINGS (CONT.)

Setting	Description
	• **Wipe data** - The user account that is associated with the application is wiped from the device.

Office 365 App Protection configurations

Once you register Ivanti EPMM as an Azure app you can create custom configurations for Office 365 apps. App Configurations can be used to specify custom app configurations for Office 365 apps. Configurations can include setting a local encryption scheme for OneDrive, setting Skype parameters, and so on.

This section includes the following topics:

- "Creating Office 365 App Protection configurations" below
- "Editing a Office 365 App Protection configuration" on the next page
- "Managing Office 365 App Protection configurations " on the next page

> Before using this feature, complete the prerequisites described in the following section: "*Prerequisites for using Office 365 App Protection*" *on page 885*.

Related topics

- "Office 365 App Protection overview" on page 885
- "Office 365 App Protection policies" on page 887
- "Office 365 App Protection user groups" on page 898
- "Office 365 App Protection reports" on page 899
- "Office 365 App Protection settings" on page 905

Creating Office 365 App Protection configurations

Configurations use data populated from Azure Active Directory during real-time syncs.

1. Log into the Admin Portal.

2. Go to **Services > Microsoft Graph > Configurations > Add**.

3. Add a name (required) and description (optional).

4. Select **Add+** to add one or more key-value pairs.

   The values are strings with no limitations or restrictions.

5. Select **Save** to add the configuration to the list in the configurations table.

Editing a Office 365 App Protection configuration

Configurations use data populated from Azure Active Directory during real-time syncs.

Procedure

1. Log into the Admin Portal.

2. Go to **Services > Microsoft Graph > Configurations**.

3. Select the name of a configuration you want to edit.

   Use the search field to search by name.

4. Make any necessary changes.

5. Select **Save** to update the configuration edits.

Managing Office 365 App Protection configurations

You can take any of the following actions on each Office 365 App Protection configuration:

- Assign User Groups
- Assign Apps
- Delete Policies

Procedure

1. Log into the Admin Portal.

2. Go to **Services > Microsoft Graph > Configurations**.

3. Locate a configuration you want to manage and go to the **Actions** column.

   a. Assign user groups to the app protection configuration.

   b. Select the **Assign User Groups** icon.

   c. Search for user groups.

   d. Select one or more user groups to add to the configuration.

   e. Select **Save**.

4. Assign Office 365 apps to the app protection configuration.

   a. Select the **Assign Apps** icon.

   b. Search for apps.

   c. Select one or more apps to add to the configuration.

   d. Select **Save**.

5. Delete an Office 365 App Protection configuration.

   a. Select the **Delete Configuration** icon.

   b. Select **Yes** to confirm deletion of the configuration.

Changes to the configurations take affect after:

- assigning the configuration to a user group.
- a user from the assigned user group logs into an Office 365 app using AAD credentials.

Office 365 App Protection user groups

Use the **User Groups** tab to search for and view user groups available to add to one or more Office 365 App Protection policies or configurations. Access a list of user groups by logging into the Admin Portal and selecting **Services > Microsoft Graph > User Groups**.

> Before using this feature, complete the prerequisites described in the following section: *"Prerequisites for using Office 365 App Protection" on page 885*.

Related topics

- "Office 365 App Protection overview" on page 885
- "Office 365 App Protection policies" on page 887
- "Office 365 App Protection configurations" on page 896
- "Office 365 App Protection reports" below
- "Office 365 App Protection settings" on page 905

Office 365 App Protection reports

Reports for out of compliance data, devices, apps, and users, is populated from Azure Active Directory during real-time syncs. Access the reports by logging into the Admin Portal and selecting **Services > Microsoft Graph > Reports**. Use the **Reports** tab to:

- search, view, or download a .csv report by user
- search, view, or download a .csv report by app
- create and manage wipe requests
- refresh reports

This section includes the following topics:

- "Office 365 App Protection reports window" on the next page
- "Managing Out of Compliance Users reports" on the next page
- "Managing Selective Wipe reports" on the next page
- "Downloading App Protection reports" on page 901
- "Downloading App Configuration reports" on page 903

Before using this feature, complete the prerequisites described in the following section: *"Prerequisites for using Office 365 App Protection" on page 885*.

Related topics

- "Office 365 App Protection overview" on page 885
- "Office 365 App Protection policies" on page 887
- "Office 365 App Protection configurations" on page 896
- "Office 365 App Protection user groups" on the previous page
- "Office 365 App Protection settings" on page 905

Office 365 App Protection reports window

Manage reports from the Admin Portal by going to **Services > Microsoft Graph** to open the Office 365 App Protection window. This window includes several options, which are listed in the left pane. When you select one, the right pane changes to include details of the selected option.

- **Out of Compliance Users**: This option is selected by default. Use it to manage reports on users who are out of compliance.
- **Selective Wipe**: Use this option to request Azure Active Directory wipe Office 365 app data from selected devices.
- **App Protection Reports**: Use this tab to view and download app protection reports by users and by apps. These reports are populated with data from Azure Active Directory during real-time syncs.
- **App Configuration Reports**: Use this tab to view and download app configuration reports by users and by apps. These reports are populated with data from Azure Active Directory during real-time syncs.

Managing Out of Compliance Users reports

Use this option to manage reports on users who are out of compliance.

Procedure

1. Log into the Admin Portal.

2. Select **Services > Microsoft Graph > Reports > Out of Compliance Users**.

3. Click **Download Report** to download a .csv report from Azure Active Directory of users who are out of compliance.

4. Click **Refresh Report** to get the most recent data from Azure Active Directory after the latest sync.

5. Select one or more of the users listed in the report or select all.

6. Click **Wipe Apps Data** to send a wipe request to Azure Active Directory for users.

Managing Selective Wipe reports

Use this option to create and manage requests you send to Azure Active Directory to wipe Office 365 app data from selected devices.

Creating wipe requests

Procedure

1. Log into the Admin Portal.

2. Select **Services > Microsoft Graph > Reports**.

3. Expand **Selective Wipe**.

4. Click **Create Wipe Request**.

5. Enter or search for a user name, then select one or more of the user's devices.

6. Click **Create Wipe Request** to request Azure Active Directory wipe Office 365 app data from one or more selected devices.

Managing wipe requests

Procedure

1. Log into the Admin Portal.

2. Select **Services > Microsoft Graph > Reports**.

3. Expand **Selective Wipe**.

4. Click **Wipe Request**.

5. Select one or more pending wipe requests and click **Cancel Wipe Request**.

6. Click **Refresh** to update the status of the pending wipe requests.

Downloading App Protection reports

App Protection Reports show applications protected by the policies that are created and assigned to them from the **Policies** tab. Use this option to download app protection .csv reports by users or apps.

Downloading App Protection reports by user

Procedure

1. Log into the Admin Portal.

2. Select **Services > Microsoft Graph > Reports**.

3. Expand **App Protection Reports**.

4. Click **User**.

5. Search for, or enter a user name.

   See "App Protection User reports table" below for details.

6. Click **Download Report**.

App Protection User reports table

Select this option to view and download reports and to refresh the report data. This option provides app information for a specified user. These reports are populated with data that comes from Azure Active Directory during real-time syncs.

TABLE 131. APP PROTECTION USER REPORTS FIELDS

Fields	Description
Bundle ID/Package ID	This column lists the unique identifier for the app.
Device Name	This column lists the name of the device.
Device Type	This column lists the type of device.
Policies	This column lists the app protection policies assigned to this app.
Status	This column lists the sync status of the app. The options for this column are: **Synced**, **Synced, but out of date**, and **Not synced**.
Last Check-In	This column lists the time stamp of the last time this app synced with Azure.

Downloading App Protection reports by app

Procedure

1. Log into the Admin Portal.

2. Select **Services > Microsoft Graph > Reports**.

3. Click **App**.

4. Complete the form.

   See "App Protection App reports table" below for details.

5. Click **Download Report**.

6. Expand **App Protection Reports**.

App Protection App reports table

This option provides user data for selected apps.These reports are populated with data that comes from Azure Active Directory during real-time syncs.

TABLE 132. APP PROTECTION APP REPORTS

Fields	Description
Platform	Select the OS platform for which you want to see apps. The options are Android and iOS.
App	Select the single app for which you want to receive a report. This list changes depending on the platform you select.
Status	Select the user's protection status from the list. The options are **Protected** and **Unprotected.**
User	This column lists the users that match the search criteria.
Email	This column provides the user's email address.

Downloading App Configuration reports

App Configuration Reports show applications with configurations defined and assigned to them under the **Configuration** tab. Use this option to download app configuration .csv reports by users or apps.

Downloading App Configuration reports by user

Procedure

1. Log into the Admin Portal.

2. Select **Services > Microsoft Graph > Reports**.

3. Expand **App Configuration Reports**.

4. Click **User**.

5. Search for, or enter a user name.

   See "App Configuration User reports table" below for details.

6. Click **Download Report**.

App Configuration User reports table

Select this option to view and download reports and to refresh the report data. This option provides app information for a specified user. These reports are populated with data that comes from Azure Active Directory during real-time syncs.

TABLE 133. APP CONFIGURATION USER REPORTS FIELDS

Fields	Description
Bundle ID/Package ID	This column lists the unique identifier for the app.
Device Name	This column lists the name of the device.
Device Type	This column lists the type of device.
Configurations	This column lists the app protection configurations assigned to this app.
Last Check-In	This column lists the time stamp of the last time this app synced with Azure.

Downloading App Configuration reports by app

Procedure

1. Log into the Admin Portal.

2. Select **Services > Microsoft Graph > Reports**.

3. Expand **App Protection Reports**.

4. Click **App**.

5. Complete the form.

   See "App Configuration App reports table" below for details.

6. Click **Download Report**.

App Configuration App reports table

This option provides user data for selected apps.These reports are populated with data that comes from Azure Active Directory during real-time syncs.

TABLE 134. APP CONFIGURATION APP REPORTS

Fields	Description
Platform	Select the OS platform for which you want to see apps. The options are Android and iOS.
App	Select the single app for which you want to receive a report. This list changes depending on the platform you select.
User	This column lists the users that match the search criteria.
Email	This column provides the user's email address.

Office 365 App Protection settings

Use the **Settings** tab to set up Office 365 App Protection policies to help protect your company's data.

License Required: This feature requires a separate license. In addition, this feature requires an Intune subscription from Microsoft. Prior to using this feature, ensure your organization has purchased the required licenses.

Related topics

- "Office 365 App Protection overview" on page 885
- "Office 365 App Protection policies" on page 887
- "Office 365 App Protection configurations" on page 896
- "Office 365 App Protection user groups" on page 898
- "Office 365 App Protection reports" on page 899

Azure Tenant

Overview

This section contains information describing the process for setting up Ivanti EPMM to Microsoft Azure Tenant.

A growing number of organizations are using Microsoft's productivity apps on mobile devices, such as Microsoft 365, OneDrive, etc. These kind of deployments give device users access to their organization's resources using various devices and apps from anywhere and using only their credentials. If the credentials get compromised, any unauthorized person can also login and get complete access to the organization's data. Just focusing on who can access the organization's resources is no longer sufficient; IT administrators must know how and from which device the organization's resource is accessed from. They have to make sure that data is accessed from the devices that meets the corporate compliance policy and have these corporate policies on each and every device. Administrators should also be able to block access to unauthorized devices by defining conditional access policies.

Using Microsoft's Intune device compliance APIs allow organizations to update the device compliance status in the Microsoft Azure Active Directory (AAD.) Using conditional access from AAD, if the device is non-compliant, administrators can block the device from accessing apps. By connecting Ivanti EPMM to the AAD, administrators will be able to use the device compliance status of Ivanti EPMM's managed devices for conditional access to Microsoft 365 apps.

Requirements

Microsoft

Ivanti EPMM customers must have a valid subscription to Microsoft Intune and assign a Microsoft Intune license to device users supported by this integration.

Please also see: [Microsoft licensing for Microsoft 365 App services.](#)

Ivanti EPMM

- Ivanti EPMM - Administrators will need Ivanti EPMM version 11.0.0.0 or supported newer versions.

  - For instructions on how to set up Android Enterprise, see the *Ivanti EPMM Device Management Guide for Android and Android Enterprise devices*.

ℹ️ If you do not have a link to your Ivanti EPMM instance, contact your Ivanti Customer Success Manager.

- Ivanti Mobile@Work for iOS (client) – version 12.0 or supported newer versions.

Supported OS versions

- iOS 12.0 or supported newer versions

The Microsoft website states:

- Office for iPad® and iPhone® (including Outlook for iOS) is supported on the two most recent versions of iOS and iPadOS. When a new version of iOS or iPadOS is released, the Office Operating System requirement becomes the two most recent versions: the new version of iOS or iPadOS and the previous version.

- For more information on supported OS versions, see [Microsoft 365 Office resources](#).

Unsupported OS versions

Behavior if unsupported device OS versions is used:

- For unsupported version iOS 11.4, the device user can complete the device registration for AAD and the device details are successfully uploaded to the Azure portal. However, Microsoft Apps (for example, Outlook, Excel, Word and OneDrive) are not available in the App Store for the unsupported version.

Multiple Ivanti EPMM support

If you have multiple Ivanti EPMMs connected to the same Azure tenant, you should not disconnect from a single Ivanti EPMM from Azure tenant. Your options are:

- Disconnect from all Ivanti EPMMs

- Disable compliance policy for AAD compliance integration from a specific (single) Ivanti EPMM so that it does not upload device data to Azure

ℹ️ Be sure to disable the compliance policy prior to disconnecting Ivanti EPMM.

Technical support

For additional help with this feature, contact Ivanti Technical Support.

From the Ivanti EPMM administrator's point of view

Below lists the process from the Ivanti EPMM administrator's perspective.

1. Administrator applies Intune licenses to device users. See "Apply the Intune license to device users" on the next page.

2. Administrator logs into Azure Portal.

3. Administrator adds Ivanti EPMM as an Azure compliance partner. See "Adding Ivanti EPMM as a compliance partner" on page 910.

4. Administrator creates the Conditional Access policy for the apps. See "Creating a conditional access policy in Microsoft Endpoint Manager" on page 912.

5. Administrator sets up the connection between Ivanti EPMM and Azure. This allows client devices to report compliance status to Azure. See "Connecting Microsoft Azure to Ivanti EPMM" on page 916.

6. Administrator creates the device compliance policy in Ivanti EPMM. See "Creating a partner device compliance policy" on page 922.

7. When the device checks in, the device compliance status is sent to the Azure portal.

8. The Conditional Access policy goes into effect. Depending upon whether the device is compliant or not, the access to the app(s) is granted or denied.

9. Administrator can disconnect from Azure. See "De-provisioning of the Azure tenant" on page 924.

ℹ️ Ivanti recommends the administrator run tests on each and every Microsoft app: Outlook, Word, Excel, Powerpoint, OneDrive, etc.

From the device user's point of view

Below lists the process from the device user's perspective.

1. Device user's device is enrolled with Ivanti Mobile@Work. See "Installing Ivanti Mobile@Work for iOS and Android" on page 925.

2. Log into the AAD account. This requires the Authenticator app to be installed on the device (see "Required client device user action and use cases" on page 926.)

   - If Authenticator is available on device, device user logs into AAD account using their Microsoft credentials.

   - If Authenticator is not installed on the device, device user is guided to install the Authenticator and then log in using their Microsoft credentials.

Note the following:

- If the device is compliant, device user can access Microsoft 365 apps.

- If the device is not compliant, an error displays stating the app cannot be opened.

Apply the Intune license to device users

Ivanti EPMM customers must have a valid subscription to Microsoft Intune and assign a Microsoft Intune license to device users supported by this integration.

To bulk assign licenses to existing device users, follow the instructions listed below.

Group based assignment

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

Powershell based assignment

https://docs.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide

Adding Ivanti EPMM as a compliance partner

This section addresses adding Ivanti EPMM as an Azure compliance partner. Ivanti EPMM integration as compliance partner with Azure Active Directory in Common Criteria mode is supported.

Procedure

1. Login into: https://endpoint.microsoft.com.

2. In the left panel of the Microsoft Endpoint Manager administrator center page, click on **Tenant Administrator**. Click on **Connectors and Tokens > Partner Compliance Management**.
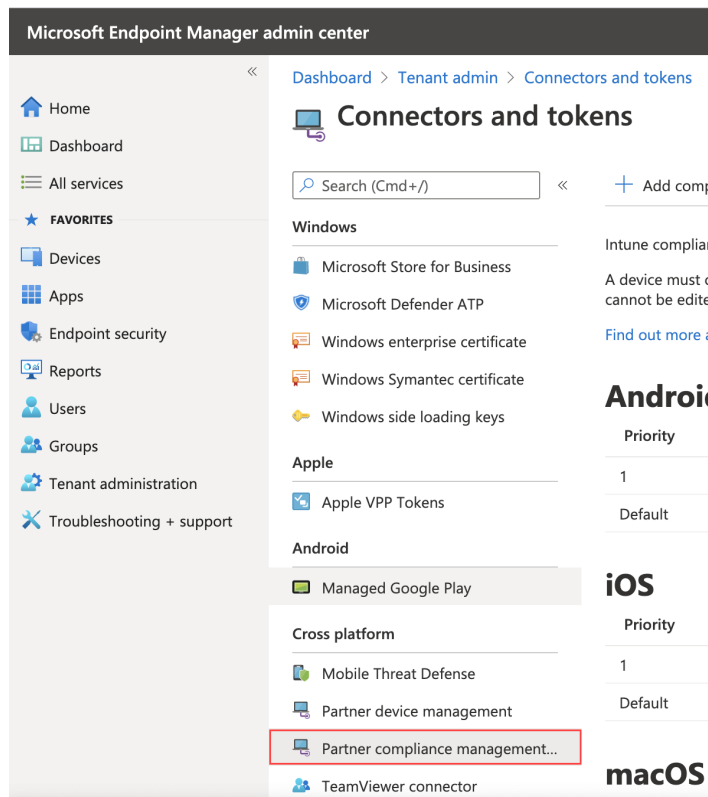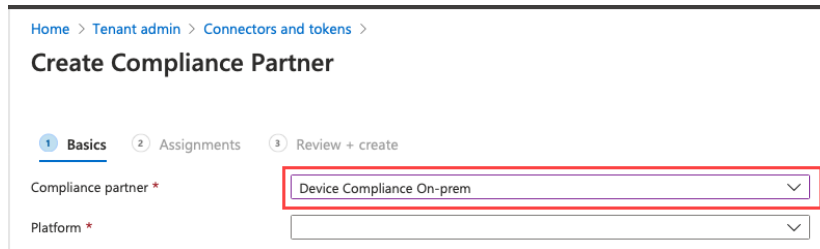
3. To the right of the Search field, click **+ Add compliance partner**.
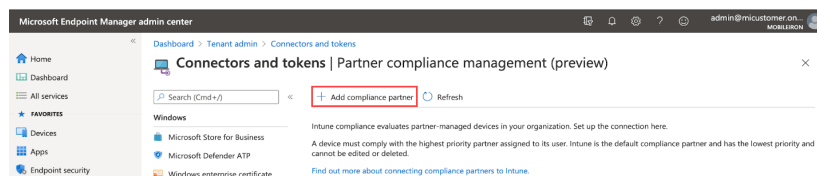
The Create Compliance Partner page displays.

4. In the Basics tab, select **Device Compliance On-prem** from the drop-down of the Compliance partner field.

5. In the Platform field, select iOS or Android and then click **Next**.

6. Click the **Assignments** tab. In the Assign to drop-down, select the user / group of device users the compliance status is for. Make sure to select the user / group that has the license.

7. Select **Next**.

8. Click the **Create** button.

9. The new compliance partner is created and displays on the Partner compliance management page under the appropriate OS system. Once the consent is provided by the administrator on the Admin Portal, the partner status will change from "Pending" to "Active."

Creating a conditional access policy in Microsoft Endpoint Manager

This section addresses defining the conditional access policy in Microsoft Endpoint Manager.

Procedure

1. Log in to Microsoft Endpoint Manager https://endpoint.microsoft.com.

2. In the Microsoft Endpoint Manager administrator center page, go to **Home > Endpoint Security > Conditional Access**.

3. Click on Policies and then click **+ New Policy**.

The New conditional access policy page opens.

4. Enter the Name of the conditional access policy.

5. In Assignments, click to assign the policy to users and groups.

6. In the New conditional access Policy page, click **Cloud apps or actions** and then click **Select**. Search for and select the apps that are required to be protected as part of this new policy.

7. In the New conditional access policy page, click on Conditions and then click on **Device Platform**. Select the appropriate device platforms.

8. In the **New conditional access policy page > Access controls**, click on **Grant** and make the access and block selections.

9. To enable the new policy, click **On**.

10. Click the **Create** button. The new conditional access policy displays in the Conditional Access > Policies page.

Connecting Microsoft Azure to Ivanti EPMM

This section covers setting up Ivanti EPMM to report the device compliance status to Microsoft Azure.

To view the Azure information about the device, go to the Device Details page. See "Advanced searching " on page 57 for definitions.

Multiple Azure tenants

Starting from Ivanti EPMM 11.7.0.0, device users can connect to multiple Azure details and upload the device compliance status to its respective Azure tenant. A maximum of 36 tenants can be configured in Ivanti EPMM to push the Compliance status to.

Connecting the account

Procedure

1. Log in to Ivanti EPMM and go to **Settings > System Settings**.

2. In the left navigational pane, select **Microsoft Azure > Device Compliance for iOS & Android**. The Device Compliance for iOS & Android page opens.

3. Select the **Standard** tenant type:

   > ⓘ Once a tenant type is selected and added, this section will be disabled. Administrator can change the tenant type only after deleting all the added tenants.

4. Select **Submit**.

5. Select **Add New Tenant**.

6. Enter the information for the following fields:

- **Azure Domain ID** - This is the AAD Tenant ID.

- **Enrollment URL** - (Optional) If the device is not MDM enrolled, device users will be pointed to this URL for enrollment. When configuring, use HTTPS format. If you host a page in your organization to redirect your device users for Enrollment information, add that link here. For example: `https://<fqdn_of_EPMM>/mifs/aadIntuneEnrollment.jsp`. If this field is left empty, the device user will be directed to a default enrollment URL / page that is hosted by Ivanti EPMM.

- **Remediation URL** - (Optional) If the device is not in compliance, device users will be pointed to this URL for remediation. When configuring, use HTTPS format. If you host a page in your organization to redirect your device users for Remediation information, add that link here. For example: `https://<fqdn_of_EPMM>/mifs/aadIntuneRemediation.jsp`. If this field is left empty, the device user will be directed to a default enrollment URL / page that is hosted by Ivanti EPMM.

7. Select **Connect Account**. The Connect Azure Account dialog box opens.

8. Select **Continue**. The Microsoft Azure login page opens.

9. **Log in** using your Azure credentials.

   > Ivanti recommends using a global administrator privileged user to enable this feature.

10. A Microsoft partnership page displays asking permission to connect Azure to Ivanti EPMM. Review the permissions and then click **Accept**.

> If you log in and the page refreshes asking that you log in again, close the browser tab / window.

Once the necessary permissions are provided, Ivanti EPMM will be connected to Microsoft Azure, and, upon successful connection, the Administrator will be navigated back to Ivanti EPMM.

11. In the Connect Azure Account dialog box, select the **I have provided the consent** check box and then click **Confirm**.

12. The Device Compliance for iOS & Android page refreshes to display **Status: Enabled** and three link options.

13. Repeat the above steps for adding multiple Microsoft Azure tenants.

14. Now that your Azure account is connected, add a new "Partner Device Compliance" policy to start reporting device compliance status to Azure. See "Creating a partner device compliance policy" on page 922.

Editing the account

The Administrator can edit the saved Azure tenant information.

- If the tenant status is **Enabled**, administrator will be able to modify the **Enrollment URL**, or **Remediation URL** fields. The **Azure domain ID** field will be disabled.

- If the status is **Not Enabled**, administrator can modify all fields.

- Selecting **Cancel** in the Edit screen cancels editing and returns the administrator to the Device Compliance for iOS & Android page.

- Validation of the **Enrollment URL**, or **Remediation URL** fields occur as per existing checks for single-tenant flow.

Procedure

1. In the Device Compliance for iOS & Android page, select the **Edit** link. The page goes into Edit mode.

2. Once the updated values are entered, Select the **Connect** button.

3. Follow the process in "Connecting the account" on page 917.

If the device user changes the password for the AD account in the Azure portal, all the device users who have authenticated their clients (Ivanti Mobile@Work) using the same user (Azure) account will need to re-authenticate their Ivanti Mobile@Work. The device user will be prompted with a setup screen on Ivanti Mobile@Work to re-login via Authenticator.

Syncing the Device Compliance status of devices

Administrators can sync the Device Compliance status of any device(s) from Ivanti EPMM to Azure. In order for the sync to perform, at least one tenant is required to be connected. Syncing the Device Compliance status works only when the device is in active state.

When syncing for non-authenticated / non-related Azure devices, an error message displays listing device names. When the administrator performs a manual sync, a detailed Audit Log is generated for the device (s).

Applicable to all types of Azure tenants, for example: Standard, GCC_High, and DOD.

Procedure

1. In the Admin Portal, go to **Devices & Users > Devices**.

2. Select device and choose **Actions > Update Intune Compliance Status**.

Disconnecting the account

To disconnect the account, select the **Disconnect** link. Ivanti EPMM will be disconnected from Microsoft Azure.

This is not the same as "Deleting an account" on the next page.

For more information, see "De-provisioning of the Azure tenant" on page 924.

Re-connecting a disconnected account

Procedure

1. Once the account is disconnected (Status displays as **Not Enabled**), a **Connect** link displays.

2. Follow the process in .

Deleting an account

The delete option removes the saved tenant details from Ivanti EPMM.

> ℹ️ **IMPORTANT:** This operation cannot be reverted.

Procedure

1. To delete the account, click on the **Delete** link.

2. A dialog box opens asking confirmation of deletion. Select **Yes**.

3. The account is disconnected and deleted.

What the device user sees

Device users may see screens that invite the device user to take action.

- How do I access Microsoft 365 apps on my device?

- Device out of compliance? Here's how to fix

Instructions for iOS and Android devices are provided on those pages for the device user to follow.

Azure account activity recorded in the logs

All activity of adding, editing, and deactivating an account are recorded in the Logs.

Creating a partner device compliance policy

Create a partner device compliance policy on Ivanti EPMM and apply the desired label. The partner compliance policy reports the device compliance status to Azure for conditional access. This is done through Microsoft Intune APIs. Once the policy is pushed to the device enrolled in Ivanti EPMM and after the first check-in of the device, the device's compliance status will be reported to Azure. Thereafter, whenever there is a change in compliance status of the device - or once a week - the status will be reported. If there is no change in the compliance status, the status is reported to Intune once a week, as required by Microsoft. To view the Azure device compliance status, go to the Device Details page under the specific device.

Before you begin

You must have an Azure Tenant ID set up. See "Connecting Microsoft Azure to Ivanti EPMM" on page 916.

Procedure

1. In Ivanti EPMM, go to **Policies & Configurations > Policies**.

2. Click **Add New > Partner Device Compliance**. The Add Partner Device Compliance Policy dialog box opens.

3. Use the below form to enter your settings:

Item	Description
Name	Enter a name for the policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. Only one active policy can be applied to a device.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select **Higher than** or **Lower than**, then select an existing policy from the drop-down list. For example, to give Policy A higher priority than Policy B, you would select "Higher than" and "Policy B".
Description	Enter an explanation of the purpose of this policy.

Item	Description
Report Device Compliance Status to Azure for iOS and Android devices	Selected by default. If you do not see this field, you need to set up your Azure Tenant ID first. See "Connecting Microsoft Azure to Ivanti EPMM" on page 916. If the Report Device Compliance Status to Azure for iOS and Android devices check box is enabled, and the compliance policy is applied to the client, the client will display the option in Settings under "Microsoft 365 Access." The compliance status of the device will be then reported to Azure under the following conditions: • when device is out of compliance • when the device is compliant • when the device returns to compliance after being out of compliance • If there is no change in the status, a report is sent once a week / every seven days.

4. Click **Save**.

Device status reporting

For the following cases, Ivanti EPMM reports device inventory and compliance status to Azure.

- On-device compliance state change
- On-device inventory change, for example, an OS upgrade
- Once a week, Ivanti EPMM reports compliance and inventory status to Azure

Depending on the action chosen in the compliance policy, the following device status will be sent to Azure:

TABLE 135. ACTIONS IN COMPLIANCE POLICY

Action	What Ivanti EPMM sends to Azure
Block Email, AppConnect Apps	Non-compliant to Azure
Send Alert	Compliant to Azure

For more information, see "Compliance actions policy violations" on page 346.

De-provisioning of the Azure tenant

This section covers how to disconnect or de-provision the Azure tenant.

If multiple Ivanti EPMMs are enabled to use the same Azure tenant, do not de-provision from one Ivanti EPMM; instead, de-provision from all Ivanti EPMMs. If a single Ivanti EPMM needs to stop using Azure, you can disable the partner compliance policy for that Ivanti EPMM only.

If the administrator performs a disconnect on Ivanti EPMM, then Ivanti EPMM stops reporting the device inventory and compliance status to Azure.

> ℹ️   Disconnecting requires an active connection to Azure using valid credentials.

Procedure

Microsoft

1. Log in to Microsoft Azure.

2. Go to **Intune > Conditional Access**. Make sure the conditional access policy is disabled.

Ivanti EPMM

1. Log in to Ivanti EPMM and go to **System Settings**.

2. In the left navigational pane, click **Microsoft Azure > Device Compliance for iOS & Android**. The Device Compliance for iOS & Android page opens.

3. Click on **Disconnect Account**.

Disconnect Azure Account

Are you sure you want to disconnect your Azure account?

Please be aware that this action can not be undone and all Azure device compliance policies currently being distributed to devices will be removed once account is disconnected.

Note: Please make sure to delete/update Conditional Access Policy in Azure, to avoid blocking users from accessing cloud resources.

Cancel   Confirm

4. In the Disconnect Azure Account dialog box, click **Confirm**.

Retiring a device from Azure

Upon device retirement, Ivanti EPMM reports to Azure that the device is no longer under management and is non-compliant.

Azure deletes the retired device entry after 90 days.

Installing Ivanti Mobile@Work for iOS and Android

This section addresses Ivanti Mobile@Work for iOS or Android can be installed onto devices.

> ℹ️ Azure Device Compliance is not supported on branded MDM Android and iOS clients.

Installing Ivanti Mobile@Work for iOS

The administrator needs to have Ivanti Mobile@Work version 12.11.0 or supported newer versions connected to Ivanti EPMM as a Mandatory Silent App and applied to devices.

The device user needs to follow the instructions below.

Procedure

1. Install Ivanti Mobile@Work from the Apple Store.

2. Launch the Ivanti Mobile@Work client and complete the Registration.

Installing Ivanti Mobile@Work for Android

The administrator needs to have Ivanti Mobile@Work 11.0.0.0 or supported newer versions connected to Ivanti EPMM as a Mandatory Silent App and applied to devices.

The device user needs to follow the instructions below.

Procedure

1. Install Ivanti Mobile@Work from the Google Play Store.

2. Launch the Ivanti Mobile@Work client and complete the Registration.

3. Device users are to follow instructions based on the device type:

    - On non-Samsung devices, device users will be prompted to update the latest Ivanti Mobile@Work as part of the Mandatory Apps Manager.

    - On Samsung devices, Ivanti Mobile@Work is installed silently.

Required client device user action and use cases

This section lists the required action that a device user needs to take in the Ivanti Mobile@Work client.

Client device user action

Device users will see a notification in the Ivanti Mobile@Work app.

Android client

Procedure

1. On the Android device, device user taps on the Ivanti Mobile@Work icon to open the app.

2. Tap Settings.

3. Tap on the Microsoft 365 Access button.

4. Device user logs in.

- If the Authenticator app is installed on the device – device user will be redirected to the Authenticator app to enter login credentials.

- If the Authenticator app is not installed on the device – device user will be redirected to the Google Play Store to download the app before proceeding to next steps.

5. Once logged in, the Ivanti Mobile@Work Home page displays.

iOS client

Procedure

1. On the iOS device, device user taps on the Ivanti Mobile@Work icon to open the app.

2. Tap Settings. The Settings page opens.

3. Tap the Microsoft 365 Access button.

4. Device user logs in.

If Authenticator app is installed on device	If Authenticator app is NOT installed on device
1. The device user will be redirected to the Authenticator app to enter login credentials. 2. Device user signs in with username and password and then taps Register. 3. When registration is completed, the device user is returned to the Settings page with Microsoft 365 Access checked.	1. The device user will be redirected to the Apple App Store to download the app. 2. Once downloaded, open Ivanti Mobile@Work and tap on Settings. 3. Tap on Microsoft 365 Access. 4. Device user is redirected to the Authenticator app to enter login credentials. Device user signs in with username and password and then taps Register. 5. When registration is completed, the device user is returned to the Settings page with Microsoft 365 Access checked.

Help@Work for iOS

This section addresses the components related to Help@Work for iOS with TeamViewer.

About Help@Work for iOS

Help@Work for iOS with TeamViewer is an integration that enables administrators to remotely view supported iOS devices managed by Ivanti EPMM. VPN is not required. After initiating a remote control session from the Admin Portal, administrators can configure iOS devices and troubleshoot issues without having the devices in hand. The remote control session displays on the administrator's desktop, enabling point-and-click navigation of the device.

Help@Work requires that the TeamViewer QuickSupport app is installed on the iOS device. The TeamViewer QuickSupport app must be an iOS managed app. That is, you must add it to the App Catalog on Ivanti EPMM for distribution to iOS devices.

> Because the TeamViewer QuickSupport app must be an iOS managed app, which requires iOS MDM (Mobile Device Management), Ivanti EPMM does not support Help@Work on MAM-only devices.

Prerequisites

Help@Work for iOS requires:

- access to the ([Ivanti Community Portal](#)) during initial setup for one-time license activation
- a company email address (belonging to an organization rather than an individual) that can be used for the TeamViewer account

TeamViewer components

- TeamViewer 10 Desktop edition
- TeamViewer QuickSupport app

Supported devices

Ivanti EPMM supports Help@Work using the TeamViewer QuickSupport app on iOS 10 or supported newer versions.

However, on iOS 10 devices, the TeamViewer QuickSupport app is limited to sharing screenshots. On iOS 11 and later, the TeamViewer QuickSupport app supports real-time screensharing.

How Help@Work for iOS works

The following steps illustrate how Help@Work for iOS with TeamViewer establishes a remote control session.

1. Administrator selects a target device in the Admin Portal at **Devices & Users > Devices**.

2. Ivanti EPMM contacts the TeamViewer Server to create a remote session and retrieve a session ID.

3. Ivanti EPMM sends an iOS managed app configuration to the TeamViewer QuickSupport app so that the app will be able to start a remote session using the session ID.

4. Ivanti EPMM launches the TeamViewer software on your desktop with the session ID.

5. The iOS device user launches the TeamViewer QuickSupport app.

6. TeamViewer app connects to the TeamViewer Server, using the session ID that it received from Ivanti EPMM.

7. Administrator can view the device remotely.

Help@Work for iOS setup overview

The following diagram illustrates the setup process for Help@Work for iOS:
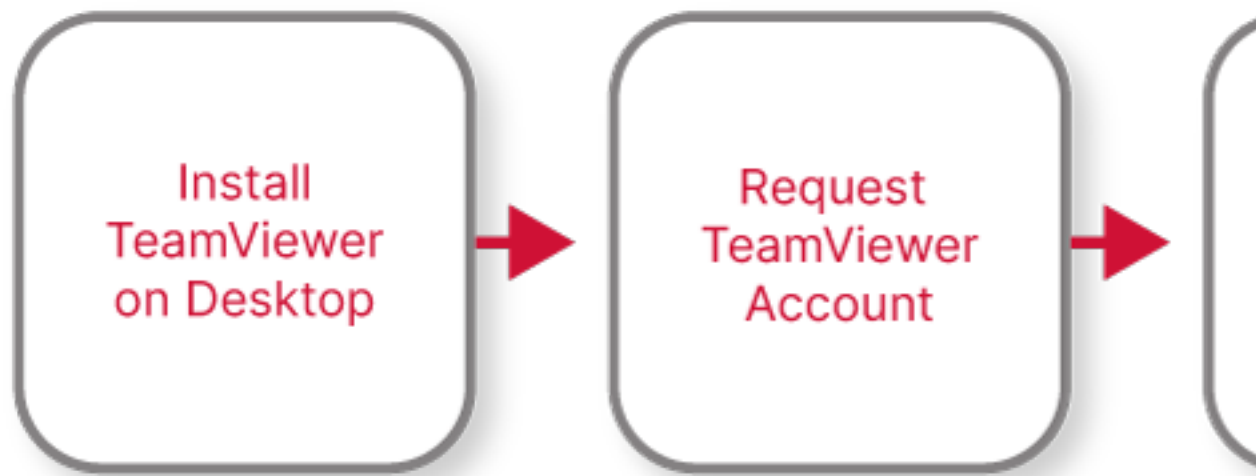
Installing TeamViewer on your desktop

This section explains how to install the TeamViewer full version software on your Windows or macOS computer.

1. Download the installation package for the TeamViewer full version for Windows or macOS from the following location:

   https://www.teamviewer.com/en/download/

2. Launch the TeamViewer installation program.
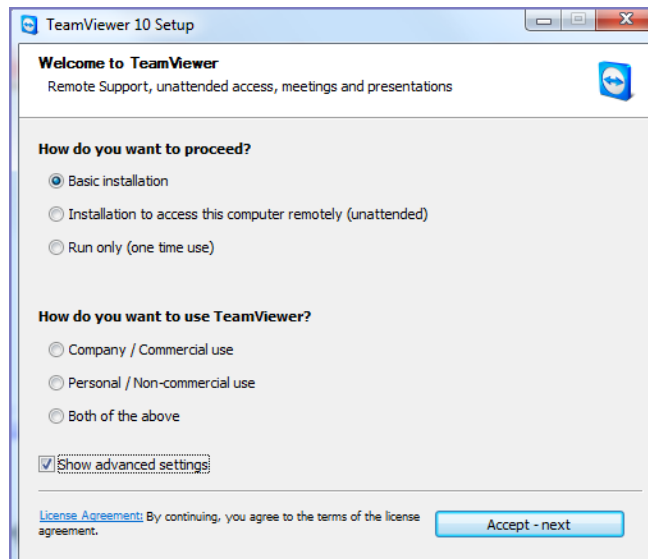
3. Select **Basic Installation.**

4. Select **Company / Commercial use.**

5. Click **Accept - next.**

When the installation is complete, the following screen displays.
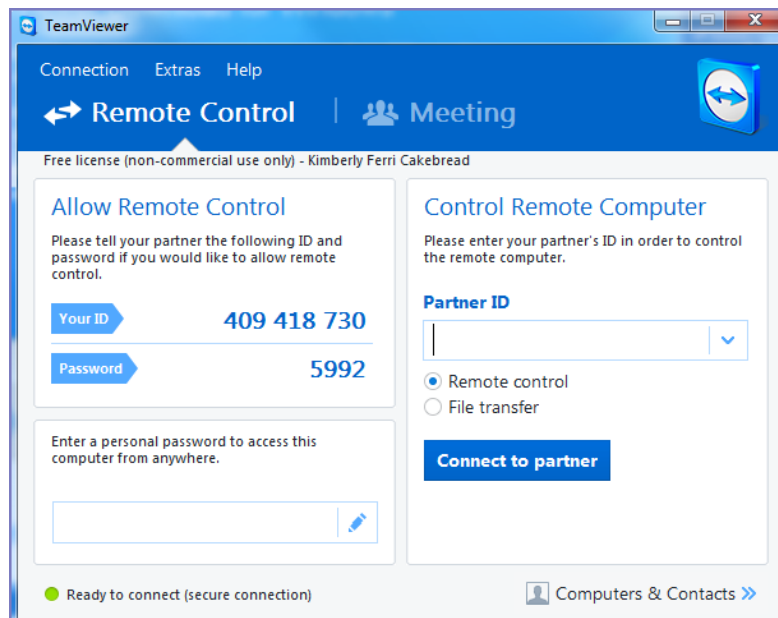
Requesting a TeamViewer account

This section explains how to get a TeamViewer account.

1. Go to https://login.teamviewer.com/LogOn#register.

2. Click **Sign Up.**

3. Set a TeamViewer email address and password.

4. Check the email account for a TeamViewer activation email.

   It might take several minutes for this email to arrive.

5. Complete the instructions in the email to activate your account.

   When the account has been activated, the following page displays:

6. Bookmark this page for future reference.
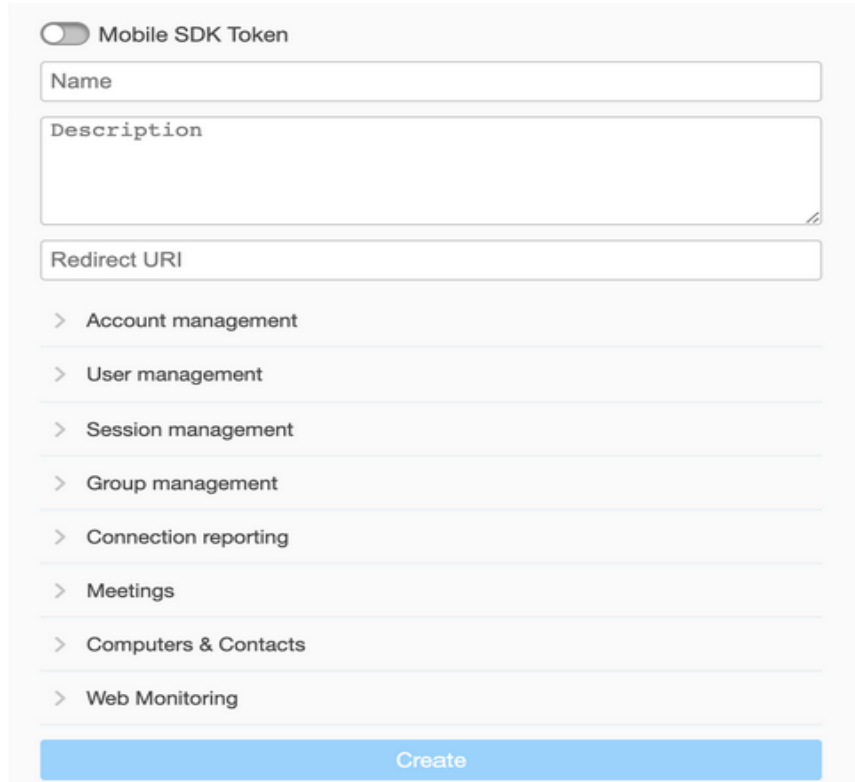
Creating a TeamViewer app

This section explains how to create a TeamViewer app for use with your Ivanti EPMM.

1. If you are not already logged in after TeamViewer account activation, to the TeamViewer Home page you bookmarked in "Requesting a TeamViewer account" on page 932.

2. Select the **Apps** link at the bottom of the TeamViewer Home page (displayed after account activation).
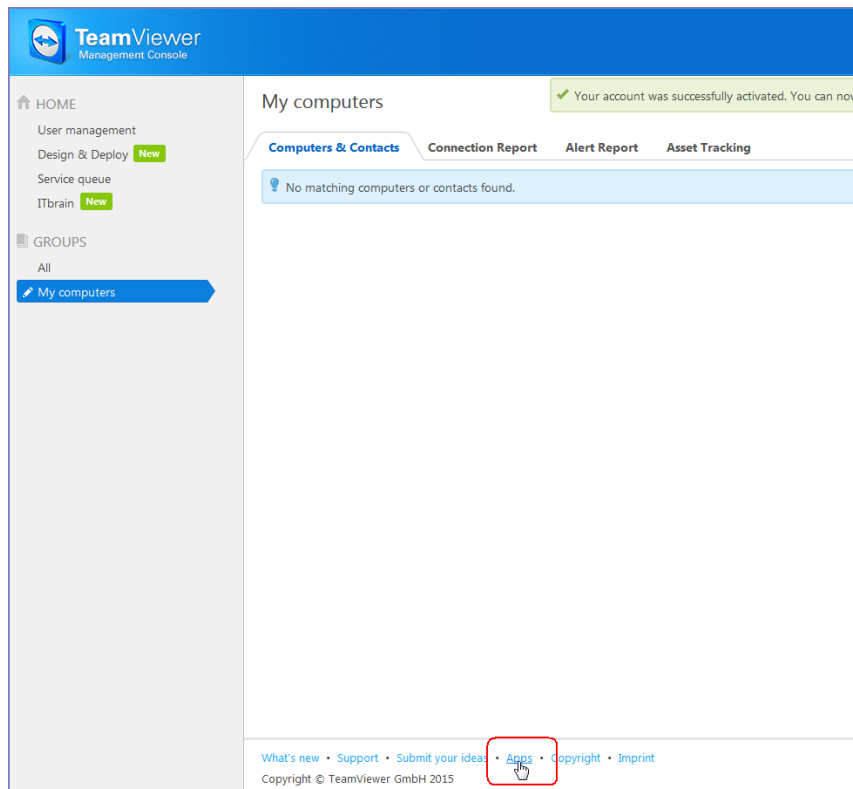
3. The Apps and Scripts accessing your account dialog box opens. Select **Create app**.

4. Enter the Name, Description and Redirect URI information.

a. **Name** - Enter at least five characters.

b. **Description** is optional

c. **Redirect URI** - Enter it in the form of `https://<ivantiepmm>/mifs/teamViewerRedirect`, where `<ivantiepmm>` is the URL of your Ivanti EPMM installation.

> ℹ️ Using a redirect URI is required.

5. For **Session management**, select:

   - View own sessions

   - View all sessions

   - Edit own sessions

   - Create sessions

6. Select **Save**.

7. In the App created successfully dialog box, copy and save the displayed Client ID and Client secret.

   You will need this information for "Enabling Help@Work in Ivanti EPMM" below.

8. Select **OK** to close the dialog box.

Enabling Help@Work in Ivanti EPMM

This section explains how to enable Help@Work for Android and iOS in the Ivanti EPMM Admin Portal.

1. Log into the Admin Portal.

2. Select **Settings > System Settings**.

3. Select **Additional Products > Licensed Products**.

4. Select **Help@Work for Android and iOS 10 and higher**.

5. Accept the displayed TeamViewer license agreement and to open the Help@Work wizard.

6. Paste the **Client ID** and **Client secret** values you copied in "Creating a TeamViewer app" on page 934.

7. Select **Validate**.

8. In the displayed TeamViewer page, enter your TeamViewer email and password.

9. Select **Allow** to provide Ivanti EPMM with session management permission for your TeamViewer app.

10. Select **Sign In**.

11. Select **Activate** in the wizard to open the Customer Support login screen:

12. Enter your Ivanti, Inc Customer Support credentials.

13. Select **Login**.

14. Enter the email address you used for your TeamViewer account.

15. Select **Submit**.

> ℹ️ Though your license is now activated, your TeamViewer software will still display a notice about trial software. Your licensing applies to the session established using the integration, so the trial notice remains in the console.

Deploying the TeamViewer QuickSupport app

This section explains how to deploy the TeamViewer QuickSupport app to iOS devices managed by Ivanti EPMM.

1. In the Admin Portal, go to **Apps > App Catalog**.

2. Click **Quick Import > iOS**.

3. In the **Application Name** field, enter teamviewer.

4. Click **Search**.

5. Find the TeamViewer QuickSupport app in the search results.

6. Click **Import**.

7. Dismiss the displayed message and the App Store Search dialog.

8. Under **Apps > App Catalog**, select the TeamViewer QuickSupport app.

9. Select **Actions > Apply To Labels.**

10. Select labels that represent the devices that should have the TeamViewer QuickSupport app added to the app catalog.

11. Click **Apply**.

12. Instruct iOS users to install the app.

13. Instruct iOS users to set iOS settings as described in [How can I share the screen on my iPad/iPhone with TeamViewer?](#)

14. Instruct iOS users to launch the app.

Starting a remote control session

This section explains how to start a Help@Work for iOS remote control session.

1. Ask the device user to install the TeamViewer QuickSupport app, if it is not already installed.

   It should be displayed in the Ivanti EPMM App Catalog on the device.

2. In the Admin Portal, go to **Devices & Users > Devices**.

3. Select the entry for the device.

4. Confirm that the device is supported by Help@Work for iOS.

   See "Supported devices" on page 929.

5. Select **Actions > iOS Only > Remote Display**.

   > ⓘ   This option is available only if you have added the TeamViewer QuickSupport app to the Ivanti EPMM App Catalog.

6. If a page requesting a session ID displays, ignore it.
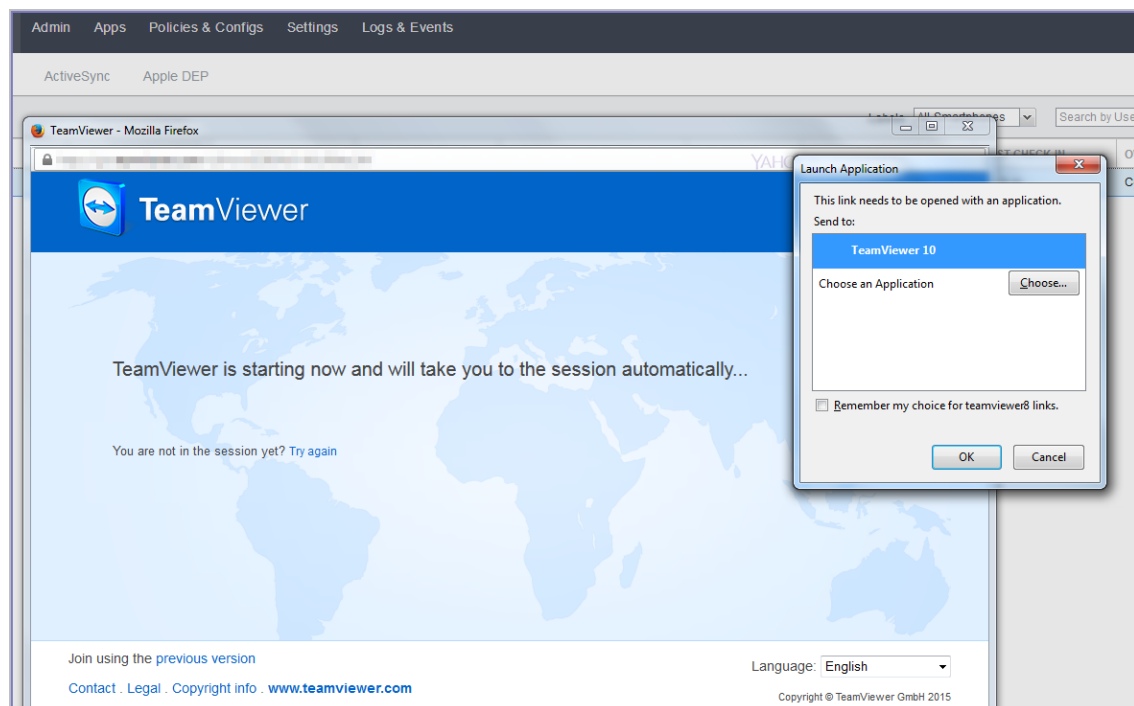
7. Launch the TeamViewer 10 application when prompted.

8. If your browser has pop-up blocking enabled, then allow pop-ups for your Ivanti EPMM URL.

9. On the device, launch the TeamViewer QuickSupport app.

You should now see the remote control session displayed on your desktop screen.

To close a remote control session from the device

To close a remote control session from the desktop:

1. Tap the TeamViewer QuickSupport app icon.
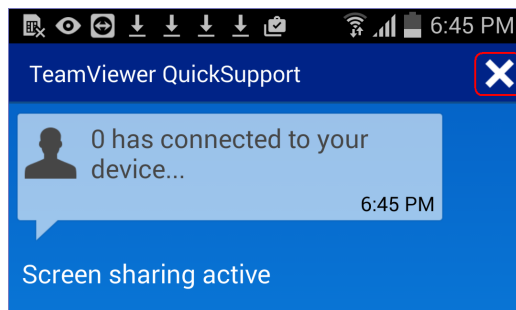
2. Tap the X in the upper right corner of the TeamViewer QuickSupport app.

To close a remote control session from the desktop

To close a remote control session from the desktop:

1. Launch the TeamViewer desktop.
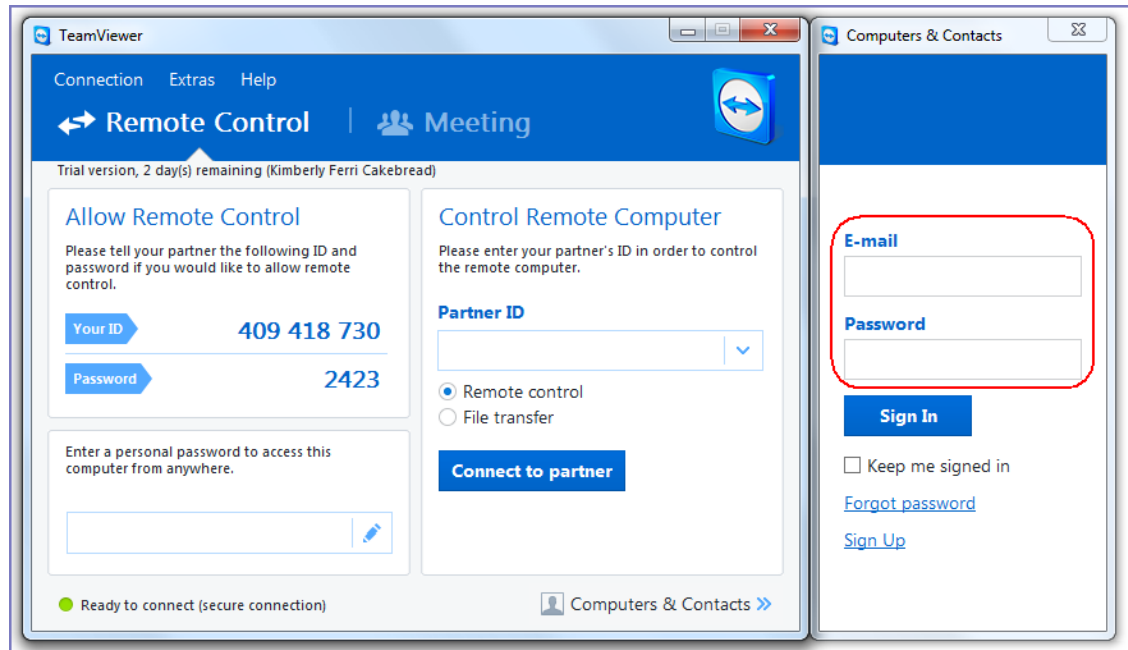
2. Sign in using your TeamViewer credentials.
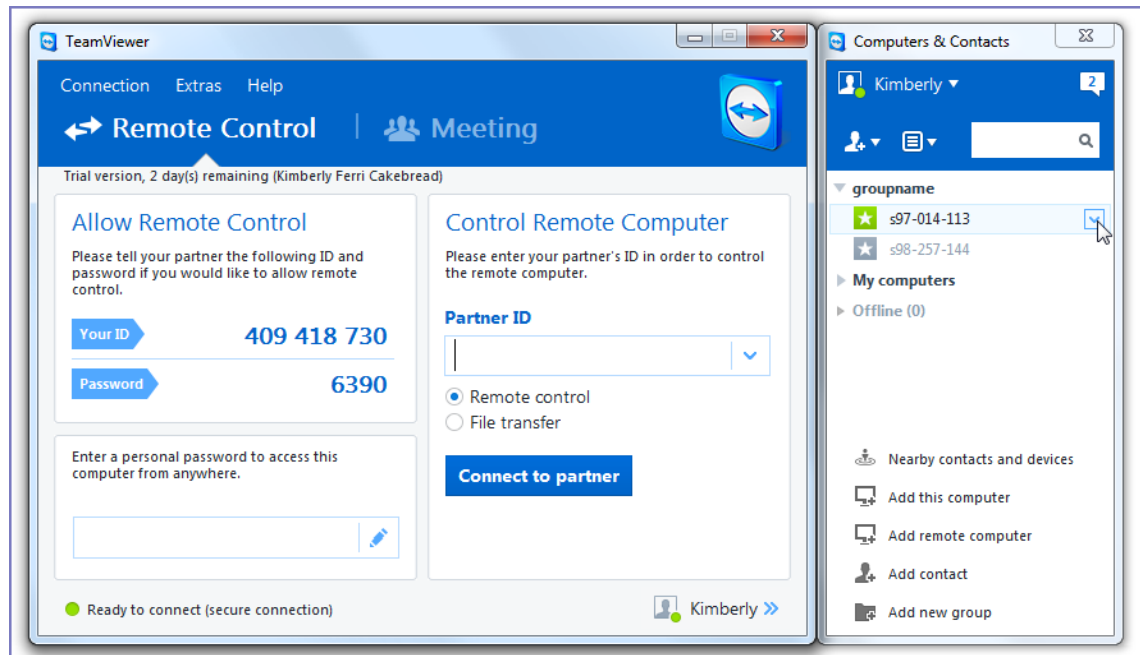
3. Select the session.

4. Select **Close**.

For more information on using remote control

See [TeamViewer remote control](#) for more information.

If you accidentally close the session

If you close the session window on your desktop, you can re-establish the session using the URL displayed in the Launch TeamViewer Session dialog.
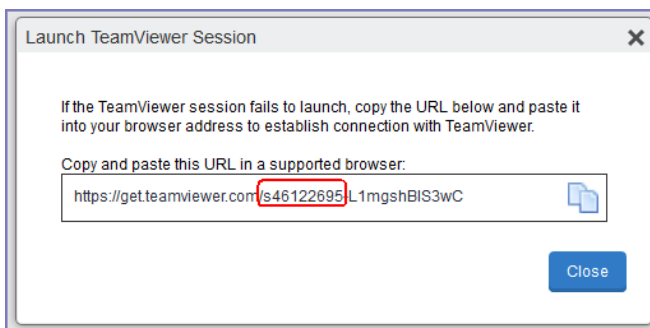
This dialog displays at the beginning of each session, but might be hidden behind other windows. Copy and paste the displayed URL in a browser window to regain access to the session. Make sure the session ID displayed in the dialog matches the one displayed in the TeamViewer app on the device.

Language Support

This section addresses the language settings for Ivanti Mobile@Work . For the current list of supported languages, see the *Ivanti EPMM Release Notes and Upgrade Guide.*

- "Translated versions of client apps" below
- "Selecting languages for Ivanti EPMM messages" below
- "Setting the system default language " on the next page
- "Changing language selection from the Admin Portal" on the next page

> ℹ️   The features described in this section are supported on macOS devices.

Translated versions of client apps

Ivanti, Incclient apps (Ivanti Mobile@Work) 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 Ivanti EPMM, Ivanti EPMM sends messages to the device in the selected language, assuming the language is supported and selected in Ivanti EPMM's **Settings > System Settings > General > Language**.

Please refer to the *Ivanti EPMM Release Notes and Upgrade Guide* for each release to see which languages and locales are supported.

Selecting languages for Ivanti EPMM messages

You can enable or disable languages for the messages sent from Ivanti EPMM 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**.
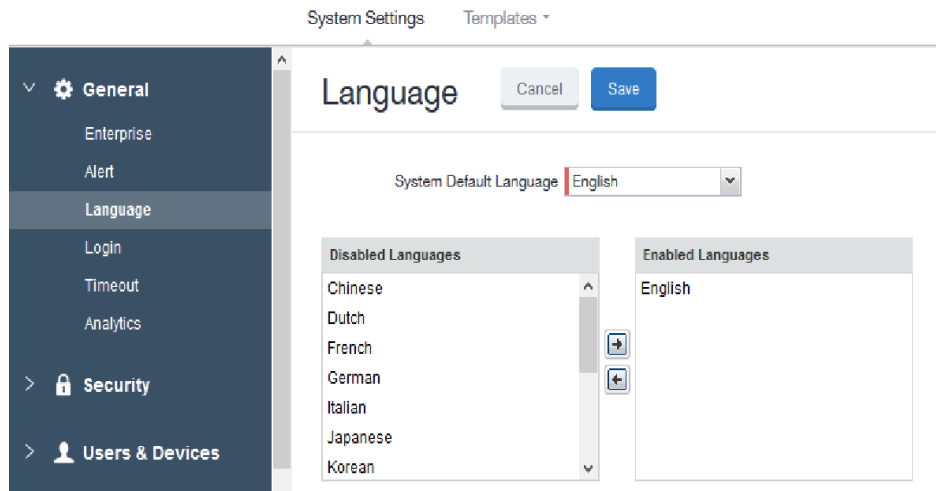
3. Move the languages you want to support from **Disabled Languages** to **Enabled Languages**.
4. Select **Save**.

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 Ivanti EPMM (e.g., Event Center alerts). If the device later reports a different locale, then Ivanti EPMM 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. Select **Actions > Change Language**.

The **Change Language** dialog appears.

4. From the **Set Language** drop-down, select the preferred language.

5. Select **Change Language**.

Self-service User Portal

This section addresses the settings an administrator needs to configure and maintain a self-service user portal for client devices.

What is the self-service user portal?

The Ivanti EPMM self-service user portal (SSP) is a platform that device users can use to manage their own devices. Access to the SSP gives users the ability to perform device management tasks, which:

- 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.

As an administrator, you have the following responsibilities:

- 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 iOS devices.

  Devices are impacted when they check-in with Ivanti EPMM, depending on the labels their devices have applied to them.

- Define which users have access to which device management actions by assigning Roles. See Assigning user portal device management roles.
- Provide your users with the information they need to use the user portal. See Using the self-service user portal.

Tasks and information are grouped into two sections:

- **Administrators**: Setting up the self-service user portal
- **Client users**: Using the self-service user portal

Setting up the self-service user portal

This section describes how a device administrator can configure and enable the features of the user portal.

- [Customizing the self-service user portal](#)
- [Configuring help desk contact information](#)
- [Configuring an end user Terms of Service agreement](#)
- [Disabling options in the SSP](#)
- [Enabling the iOS Trust/UnTrust option](#)
- [User portal authentication options](#)
- [Assigning user portal device management roles](#)
- [Associating a certificate with a user-provided certificate enrollment setting](#)
- [When a user-provided certificate is deleted](#)
- [Before enabling device registration in the User Portal (iOS only)](#)
- [Registering devices in the user portal](#)
- [Limiting devices per user by LDAP group membership](#)
- [Requiring user portal password change](#)
- [Generating a one-time PIN for resetting a secure apps passcode](#)
- [Unlocking a macOS device](#)
- [Retiring devices in the self-service user portal](#)
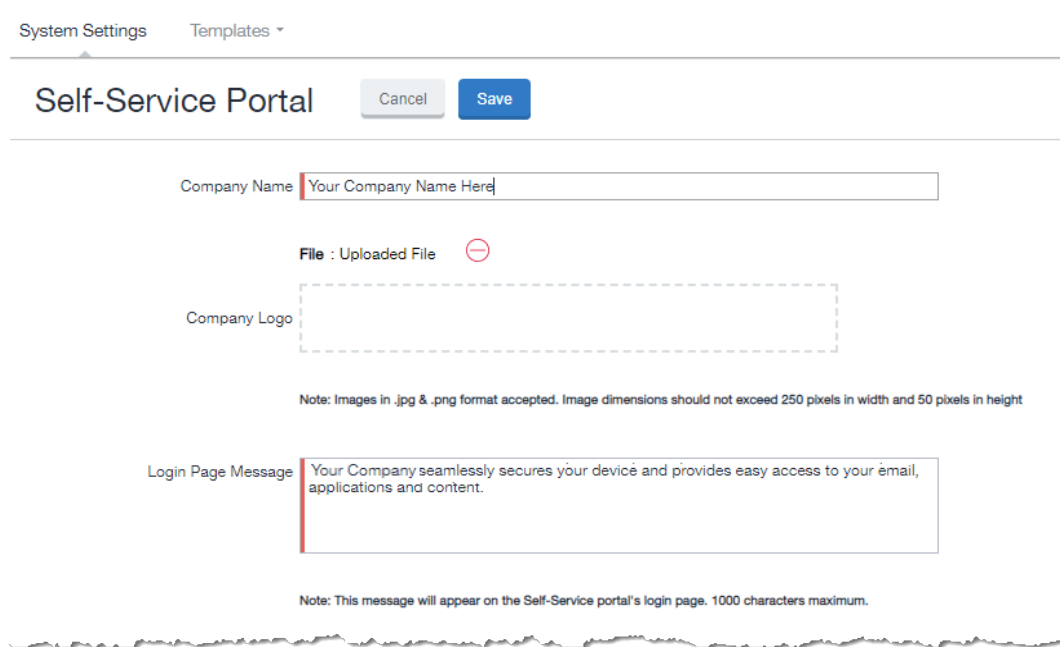
Customizing the self-service user portal

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.

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.

   b. Select or enter a value for the background color.

   > ℹ️ Based on your choice of background color, Ivanti EPMM will automatically determine

> ℹ️   the highest-contrast text color (black or white) for that color.

   c. Select **OK** to exit the menu.

6. **CSS**: By default, your message is formatted using the default cascading style sheet (CSS) supplied by Ivanti EPMM. You can import and edit a custom CSS file, modify the default CSS file, or leave the default.
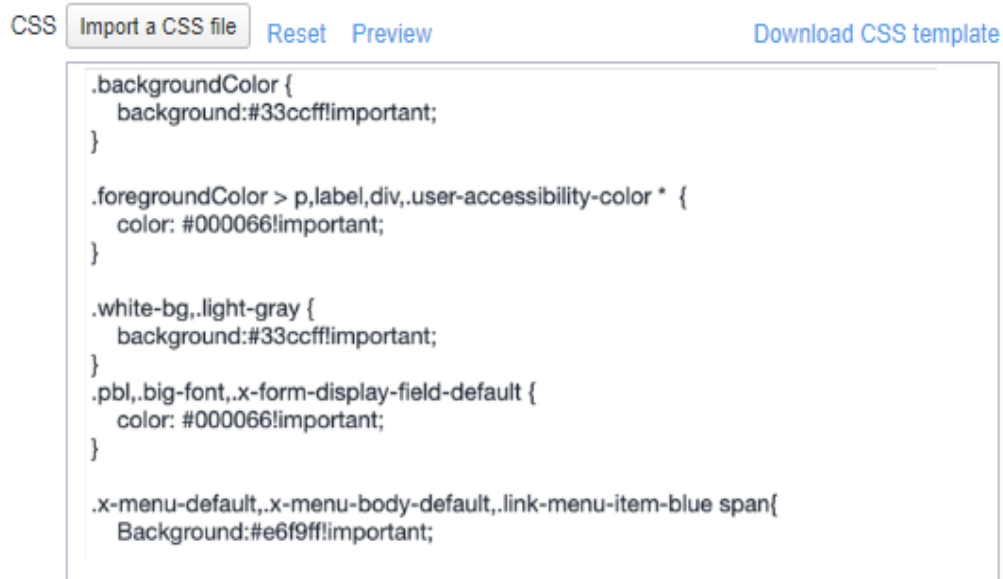
Options are:

- **Import a CSS file**: Select to browse to a valid CSS file on your local drive. Select the file and select **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**: Select to reset the style sheet to the default values. You will be asked to confirm the reset.

- **Preview**: Select 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. When all of your changes are made, select **Save** (at the top of the page) to keep your options. A confirmation message displays.

8. Verify the new custom portal page on Ivanti EPMM by substituting your Ivanti EPMM 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;
}
```

Restricting user access to activity logs and Settings menu

Check boxes at the bottom of the Self-Service Portal page allow you to restrict device activity log and Settings information from your client users. For more information, see "Hide or display Activity Logs and Settings menu" on page 966.

Configuring help desk contact information

Ivanti EPMM 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 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.
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.

ℹ Either a phone number or an email address is required.

Related topics
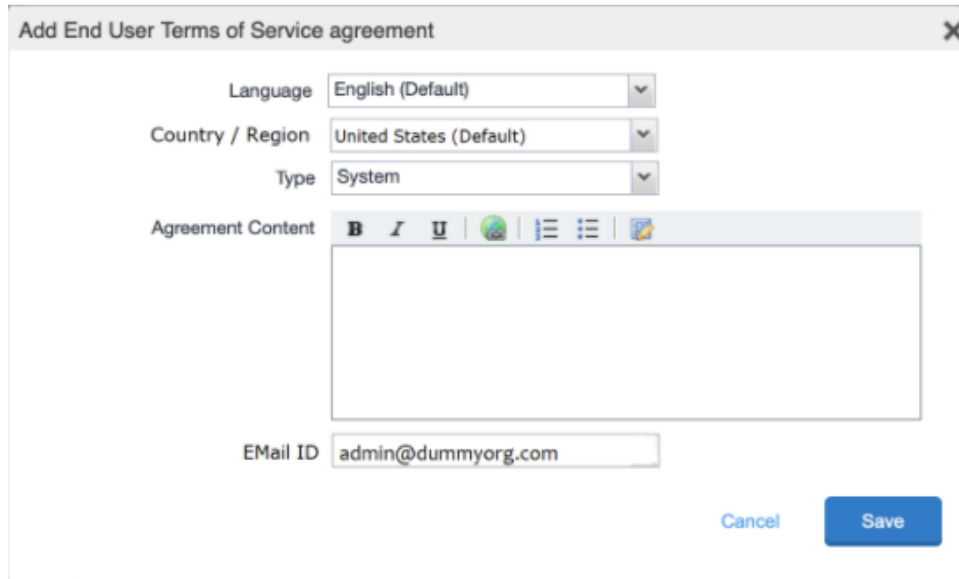
"Viewing the help desk contact information" on page 996.

Configuring an end user Terms of Service agreement

Device users must sign a Terms of Service (ToS) agreement to use Ivanti 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 administrator 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.

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.

Administrator 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)

Assigning user portal device management roles

One of your decisions when you distribute Ivanti EPMM management is whether or not to enable your users to manage one or more device actions such as locking or unlocking a device. You can assign users to different roles, giving them access to the set of actions you specify. The Ivanti EPMM 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.

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** – The Unlock Device feature works in Managed Device with Work Profile (COPE) mode for Android devices versions 8-10.

     ○ The Unlock Devices does not work for Android devices in Work Profile mode starting from Android 7 and higher.

     ○ Upon upgrade to Android 11, administrators do not have the ability to unlock the device; however, in Ivanti EPMM verison 11.8.0.0 +, administrators do. Additionally, administrators can set the PIN to the default setting or a to custom six-digit PIN. See Setting the unlock PIN for a specific device.

     ○ **IMPORTANT:** The **Unlock** command clears passcodes and TouchIDs from the managed device, compromising device security. Never use this feature on lost or stolen devices.

       - **Locate Device**
       - **Retire Device**
       - **Register Device**
       - **Change Device Ownership**
       - **Reset PIN** (for Windows 8.1 Phone and Windows Mobile 10 devices)
       - **Reset Secure Apps Passcode**
       - **Trust/Untrust** (for iOS devices)
       - **Use Google Device Account** (for Android Enterprise devices only)
       - **Enable Auth Only Role**

7. Click **Save**.

Enabling the iOS Trust/UnTrust option

You can enable an iOS feature that allows device users to protect the contents of their company device in risky locations. Once it is set up and they have been assigned the role, users can enable the feature on their devices. See "Trust and Untrust options for client users" on page 994.

ℹ️ Client users must be assigned the **Trust/Untrust** Role from the **Assign Roles** menu of the Admin Portal's **Devices & Users > Users** menu. For full information, see "Assigning user portal device management roles" on page 954

- **UnTrust**: Device users select this option to temporarily remove confidential information and applications from their device. They can use this option before entering a location where device security may be at higher than normal risk, such as in airports.
- **Trust**: Device users select this option to restore confidential information and applications on their device. They can use this option when no unusual device security risks exist.

To enable iOS Trust/UnTrust feature:

Procedure

1. From the Admin Portal, navigate to **Devices & Users > Labels**.

2. Create a filter label which includes the field "**ios.TrustedDevices**" and value **true**. For more information, see "Managing labels" in *Getting Started with Ivanti EPMM*.

3. Apply the label to the configurations, policies and apps you want to use *only* when the device is Trusted by the user.

4. Assign users the **Trust/Untrust** Role from the Ivanti EPMM **Users** page. See Assigning user portal device management roles.

ℹ️ Once enabled, when the user selects **UnTrust**, his device is no longer eligible for the items in the label, and they will be removed from the user device until he changes the status to **Trust**, when the items will reinstall.

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 Ivanti EPMM.
- **An identity certificate from a smart card** – This authentication method is supported only on desktop computers. It is not supported on mobile devices or Firefox browser.

You can allow one or both of these authentication mechanisms. You make your selection in the Ivanti EPMM System Manager **Security > Advanced > Portal Authentication** page. For information about how to configure the user portal authentication options, see "Advanced: Portal authentication" in the *Ivanti EPMM System Manager Guide.*

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 656
- "Enabling per-message S/MIME for iOS" on page 383.

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 Ivanti EPMM 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 Ivanti EPMM 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 Ivanti EPMM*. Because the private key was deleted from the Ivanti EPMM 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 Ivanti EPMM, you can view information about the certificate, such as its expiration date. This information can help you manage devices still using the certificate.

Getting Entrust derived credentials

When using certificate authentication to the user portal, you can set up Ivanti EPMM so that iOS device users can get their Entrust derived credentials when they get their Ivanti EPMM registration PIN. Specifically, in the System Manager, you provide Ivanti EPMM with the Entrust IdentityGuard Self-Service Module (SSM) URL. This URL is a deep link that points directly to the page on the Entrust self-service portal where a user can get a derived credential.

When the user requests a derived credential on the user portal, the user portal redirects the user to the URL you provided. The user interacts with the Entrust self-service portal to get a derived credential, after which the Entrust self-service portal redirects the user back to the Ivanti EPMM user portal. The user uses the PIV-D Entrust app on a device to activate the derived credential.

For information about how to enable the user to get a derived credential on the user portal, see "Advanced: Portal authentication" in the *Ivanti EPMM System Manager Guide.*

> This feature is not supported on macOS devices.

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.

   In the **Per-User Device Limit** section, enter the following information:

2. **Per-User Device Limit (1-50, or none)**: Set the default number of devices each user can register with Ivanti EPMM. 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).

3. **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, select **Add+**. The Add LDAP Group Specific Device Limit dialog box opens.

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. Select **Add**.
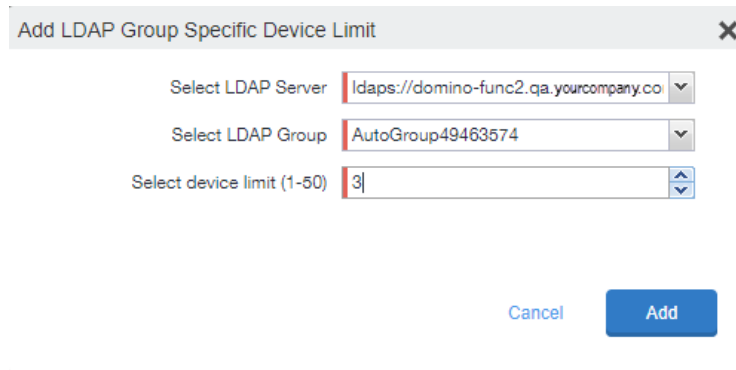
4. Select a device limit precedence setting:

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.

5. Select **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.

2. Select **Edit** to re-open the Add LDAP Group Specific Device Limit dialog.
3. Select **Delete** to delete the LDAP group-specific device limit.

Before enabling device registration in the User Portal (iOS devices)

On iOS devices, registering with Ivanti EPMM at http://*<EPMM_Server_FQDN>*/go does not automatically install Ivanti Mobile@Work on the device. You can prompt device users to install Ivanti Mobile@Work after they complete registration at http://*<EPMM_Server_FQDN>*/go.

To prompt device users to install Ivanti Mobile@Work, do the following:

1. In the Admin Portal, go to go to **Apps > App Catalog**.

2. Select **Quick Import > iOS** to manually import Ivanti Mobile@Work from the Apple App Store.

   The App Store Search window opens.

3. In **Application Name**, enter **Mobile@Work** and select **Search**.

4. Next to **Mobile@Work** client, select **Import > OK**.

5. Close the App Store Search window.

6. In the App Catalog's main page, select the **Mobile@Work** client.

7. Select **Edit**.

8. Under Managed App Settings, select **Select installation request or send convert unmanaged to managed app request (iOS 9 and later) on device registration or sign-in.**

9. Select **Save**.

10. Select the **Back to list** link in the upper left corner.

11. In the App Catalog's main page, select the **Mobile@Work** client and then select **Actions > Apply To Labels**.

12. Select the appropriate labels and then select **Apply**.

For detailed instructions, see "Manually importing iOS apps from the Apple App Store" in the *Ivanti EPMM Apps@Work Guide*.

Note that in this scenario, device users do not have to re-enter their credentials when they install and launch Ivanti Mobile@Work. However, for extra security, administrators can:

- Limit this silent registration with Ivanti Mobile@Work to one time only. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Device Registration** and select the **Allow slient in-app registration only once (iOS and macOS)** check box.

- Add a silent registration grace period in **Settings > System Settings > Users & Devices > Device Registration** and selecting **Silent in-app registration time limit (minutes) (iOS and macOS)** check box. The default value is 240 minutes (4 hours), which is good for the time it takes for the app to install on the device. You can modify this grace period based on your requirements. If the app is installed after the allotted time, the app will ask for the device users' credentials.

Before enabling device registration in the User Portal (macOS devices)

On macOS devices, registering with Ivanti EPMM at http://*<EPMM_Server_FQDN>*/go does not automatically install Ivanti Mobile@Work on the device. You can prompt device users to install Ivanti Mobile@Work after they complete registration at http://*<EPMM_Server_FQDN>*/go.

To prompt device users to install Ivanti Mobile@Work, do the following:

1. In the Admin Portal, go to **Settings > System Settings**.

2. Select **Users & Devices** > **Registration**.

3. Select the **Allow slient in-app registration only once (iOS and macOS)** check box. This limits the silent registration of Ivanti Mobile@Work to one time only.

4. Select the **Silent in-app registration time limit (minutes) (iOS and macOS)** check box. The default value is 240 minutes, which is good for the time it takes for the app to install on the device. You can modify this grace period based on your requirements. If the app is installed after the allotted time, the app will ask for the device users' credentials.

5. Go to **Apps > App Catalog** and select to import an in-house Apple app.

6. In the Choose page, import the Ivanti Mobile@Work for macOS app.

7. In the App Configuration page, make sure the **Send installation request on Device registration** check box is selected.

8. Select **Finish**.

9. In the App Catalog's main page, select the mac-Agent app (Ivanti Mobile@Work for macOS) in the list of apps and select **Actions > Apply To Labels**.

10. Select the appropriate labels and then select **Apply**.

    Once the label is applied to the app, Ivanti EPMM installs automatically when the device is registered with iReg or DEP, as per the **Send installation request on Device registration** selection. Otherwise, the administrator will need to send the app installation request manually.

Note that in this scenario, device users do not have to re-enter their credentials when they install and launch Ivanti Mobile@Work.

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.**

FIGURE 1. SETTING A PER-USER DEVICE LIMIT

Procedure
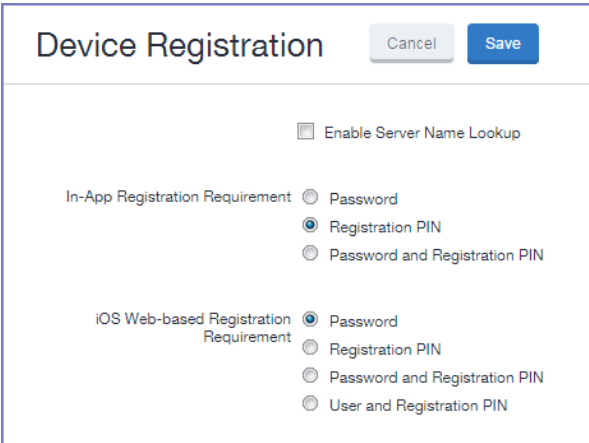
To configure standard device limits and LDAP group-specific device limits, follow these steps:

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.

FIGURE 2. SELECTING PIN-BASED REGISTRATION

- 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.

- If **Registration PIN** is selected for only iOS web-based registration, a PIN is generated and displayed in the user portal, but the PIN is not included in the registration email sent to the device user. However, if Registration PIN is selected for both In-app registration and iOS web-based registration, the PIN is included in the registration email to the device user.

Disabling options in the SSP

Some of the Self-Service Portal options that are enabled by default and could not be disabled in Ivanti EPMM 11.4.1.0 and earlier releases can now be disabled and re-enabled in Ivanti EPMM 11.5.0.0 and supported newer versions. These customization options determine whether or not clients can see different elements of the SSP.

Hide or display Activity Logs and Settings menu

Check boxes at the bottom of the Self-Service Portal page allow you to choose whether or not client users see the following menu links:

- Their device activity log
- The Settings menu, with local users and LDAP users configured separately.

Procedure

1. From the Admin Portal, navigate to **Settings > System Settings > General > Self-Service Portal** page.

2. Scroll to the bottom of the page, below the CSS import window, to the following check boxes:
   - **Show View Activity in SSP Portal** - Enabled by default. Deselect to hide client activity in the SSP portal.
   - **Show settings for local users** - Enabled by default. Deselect to hide the **Settings** menu for local users.
   - **Show settings for LDAP users** - Enabled by default. Deselect to hide the **Settings** menu for LDAP users.

3. Click **Save** at the top of the page to keep your selections.

Related topics

- "About Ivanti EPMM logs" on page 850
- "Audit Logs use cases" on page 873
- "App information" on page 867

Hide or display the QR code and registration URL

A configuration check box on the **Settings > System Settings > Users & Devices > Device Registration** page allows you to choose whether or not to show users a QR code and registration URL. This option is enabled by default. When deselected, the QR code and registration URL do not display to users.

Procedure

1. From the Admin Portal, navigate to **Settings > System Settings > Users & Devices > Device Registration** page.

2. **Display QR Code and Registration URL** - Enabled by default. Deselect to hide the QR code and registration URL to users.

3. Click **Save** at the top of the page to keep your selections.

Hide or display device history logs

When users log into the Ivanti, Inc 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 Ivanti EPMM 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 selecting it.

3. Select **Save**.

Enabling the iOS Trust/UnTrust option

You can enable an iOS feature that allows device users to protect the contents of their company device in risky locations. Once it is set up and they have been assigned the role, users can enable the feature on their devices. See "Trust and Untrust options for client users" on page 994.

> Client users must be assigned the **Trust/Untrust** Role from the **Assign Roles** menu of the Admin Portal's **Devices & Users > Users** menu. For full information, see "Assigning user portal device management roles" on page 954

- **UnTrust**: Device users select this option to temporarily remove confidential information and applications from their device. They can use this option before entering a location where device security may be at higher than normal risk, such as in airports.
- **Trust**: Device users select this option to restore confidential information and applications on their device. They can use this option when no unusual device security risks exist.

To enable iOS Trust/UnTrust feature:

Procedure

1. From the Admin Portal, navigate to **Devices & Users > Labels**.

2. Create a filter label which includes the field "**ios.TrustedDevices**" and value **true**. For more information, see "Managing labels" in *Getting Started with Ivanti EPMM*.

3. Apply the label to the configurations, policies and apps you want to use *only* when the device is Trusted by the user.

4. Assign users the **Trust/Untrust** Role from the Ivanti EPMM **Users** page. See Assigning user portal device management roles.

> ℹ️ Once enabled, when the user selects **UnTrust**, his device is no longer eligible for the items in the label, and they will be removed from the user device until he changes the status to **Trust**, when the items will reinstall.

Requiring user portal password change

You can require local users to change their user portal password the next time the device checks in with Ivanti EPMM. 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. Select **Users**.
3. Select one or more local users you want to change their user portal passwords the next time they check in with Ivanti EPMM.

4. Select **Actions**.
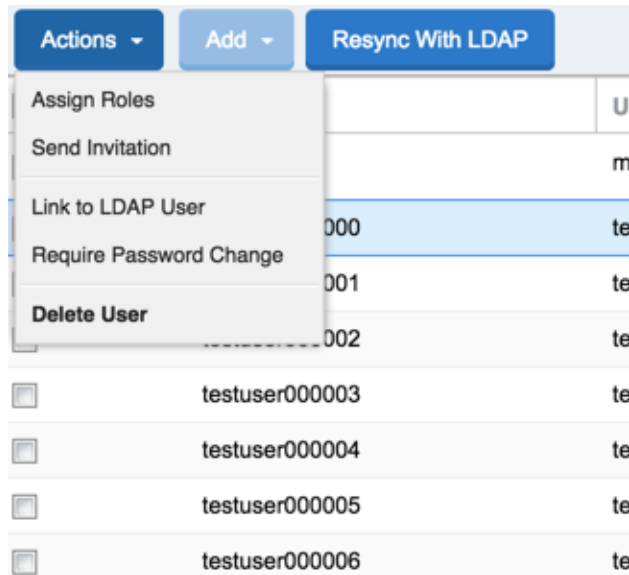
5. Select **Require Password Change**.

   Ivanti EPMM prompts you to confirm the requirement.

6. Select **Yes** to require the selected users to create a new password at the next check in.

Generating a one-time PIN for resetting a secure apps passcode

On the AppConnect global policy, you can configure Ivanti EPMM to allow iOS device users to reset their secure apps (AppConnect) passcode when they forget it. When you have configured this option, device users who registered with Ivanti EPMM using a user name and *password* can enter those credentials in Ivanti Mobile@Work for iOS > the Secure Apps Manager to authenticate themselves and then reset their secure apps passcode. However, device users who registered with Ivanti EPMM using a *registration PIN* need a different mechanism for authenticating themselves.

This mechanism involves these steps:

1. The user generates a one-time PIN on the user portal. The one-time PIN is valid for 24 hours.

2. In Ivanti Mobile@Work for iOS > the Secure Apps Manager on a device, the user follows the instructions for resetting a forgotten secure apps passcode.

3. When prompted for his user credentials, the user enters his user name and the one-time PIN.

4. The user resets his secure apps passcode.

Configuration requirements to allow the user portal to generate a one-time PIN

The user portal displays the option to generate a one-time PIN only if you have configured all of the following in the Admin Portal:

- The user portal role that allows the user to reset their secure apps passcode
- A license for AppConnect third-party and in-house apps, Ivanti Docs@Work, or Ivanti Web@Work
- An AppConnect global policy for the device that allows users to recover their AppConnect passcodes.

Configuring the user portal to generate a one-time PIN

Configure the following in the Admin Portal to allow the user portal to generate a one-time PIN:

1. In **Devices & Users > Users**, select the user.

2. Select **Actions > Assign Roles.**

3. In the Assign Role(s) dialog box, select **Reset Secure Apps Passcode**.

4. Select **Save**.

5. In **Settings > System Settings > Additional Products > Licensed Products**, select at least one of the following:
   - **AppConnect for Third-party and In-house Apps**
   - **Ivanti Docs@Work**
   - **Ivanti Web@Work**

6. In **Policies & Configurations > Policies**, select the AppConnect global policy for the device.

7. In the Policy Details panel, select Edit. The Modify AppConnect Global Policy dialog box opens

8. In the **AppConnect passcode** section, select **Passcode is required for iOS devices**.

9. Select **Allow iOS users to recover their passcode**.

10. Select **Save**.

Unlocking a macOS device

While it is possible to lock a macOS device from the User Portal, you cannot unlock a macOS device from the User Portal. Instead, unlocking a macOS device requires entering an unlock passcode on the device when prompted. The passcode can be found in the MDM logs for the macOS device, which are listed in the Admin Portal. The procedure is almost identical for unlocking wiped macOS devices.

For wiped macOS devices, you can push the Ivanti EPMM MDM profiles back to the device following recovery.

Important: The Unlock command clears passcodes and TouchIDs from the managed device, compromising device security. Never user this feature on lost or stolen devices.

Procedure

1. In the Admin Portal, go to **Devices & Users > Devices**.
2. Go to the locked or wiped macOS device and select the carat (^) next to it.
3. In the device details, select **Logs**.

4. A list of device logs is displayed.

5. Select **MDM Log**.

6. The mobile device management log is displayed.

7. Find the **Lock** or **Erase Device** action in the **Action** column.

Alternatively, you can search for the relevant action by selecting a date range and the name of the action from the **Actions** drop-down list on the left.

8. Make note of the corresponding PIN associated with the lock or wipe action.

   The PIN is located in the **Detail** column.

9. When prompted, enter the PIN on the macOS device you are trying to unlock.

   > If the macOS device has been locked and wiped, you must enter the corresponding PIN when prompted in the order that the actions occurred. For example, if you locked the device, and then wiped it, you would need to enter the lock PIN when prompted on the macOS device, follow the on-screen instructions, and then enter the wipe PIN when prompted.

10. For wiped devices:

    a. Retire the macOS device.

    b. Re-register the macOS device. Alternatively, instruct the user to register the device again.

Retiring devices in the self-service user portal

From the self-service user portal, the retire action is **Force Retired**. See "Retiring a device" on page 87.

The administrator can schedule retiring a device in .

Using the self-service user portal

This section presents the information that your users need to use the user portal.

- [Logging into the user portal with user name and password](#)
- [Logging into the user portal on a desktop computer with a certificate](#)
- [What users see after they login](#)
- [If Register Device role is enabled](#)
- [Registration instructions](#)
- [If Change Device Ownership role is enabled](#)
- [If Default ownership for devices is enabled](#)
- [If generating a one-time PIN for resetting the secure apps passcode is enabled](#)
- [What client users see after registering their device](#)
- [Trust and Untrust options](#)
- [Viewing, replacing, and deleting certificates in the user portal](#)
- [Uploading certificates in the user portal on a desktop computer](#)
- [Viewing the help desk contact information](#)

Logging into 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://*<Ivanti server>*, where *<Ivanti server>* is the address of your Ivanti 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 into the user portal on a desktop computer with a certificate

If set up by the Ivanti EPMM 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://*<Ivanti EPMM server>*, where *<Ivanti EPMM server>* is the address of your Ivanti EPMM 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** - View a list of all device activity. See "If Register Device role is enabled" on page 984.
- **Helpdesk** - Configure the help desk contact information to display in the user portal. See "Configuring help desk contact information" on page 951.
- **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 1. SEND INVITATION TO REGISTER

After the invitation is sent, the device status is seen as **Pending**.

FIGURE 2. REGISTRATION PENDING FOR DEVICE

Device users can complete the registration on their mobile device at https://*<EPMM_Server_FQDN>*/go.

FIGURE 3. COMPLETE DEVICE REGISTRATION

After registration is completed on the mobile device, the status for the device is changed to **Active**.

FIGURE 4. ACTIVE DEVICE STATUS

Registration instructions

On iOS devices, Ivanti Mobile@Work is installed only if it was set up for distribution through Ivanti EPMM. If not, users can download Ivanti Mobile@Work from the Apple App Store. Instructions for downloading Ivanti Mobile@Work from the Apple App Store are provided in the email sent to the device user.

If PIN-based registration is enabled

If PIN-based registration is enabled, device users will see **Request Registration PIN**.

Selecting **Request PIN** allows device users to send an invitation for registration as well as generate a PIN.
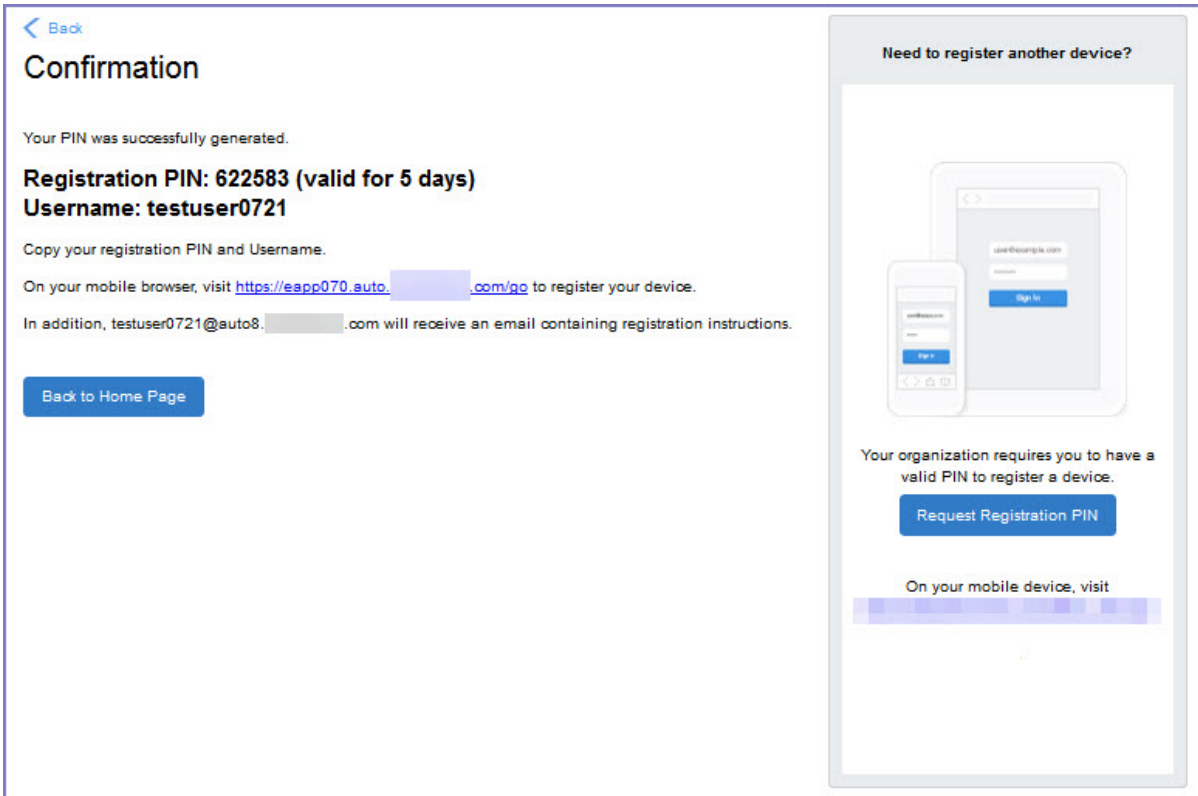
Device users can complete the registration on their mobile device at https://*<EPMM_Server_FQDN>*/go. They will have to enter the PIN if prompted.

If QR-code registration is enabled

If Quick Response (QR) code-based registration is enabled, device users will see **Generate QR Code**. Selecting **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 select 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 6. REGISTRATION WITH QR CODE
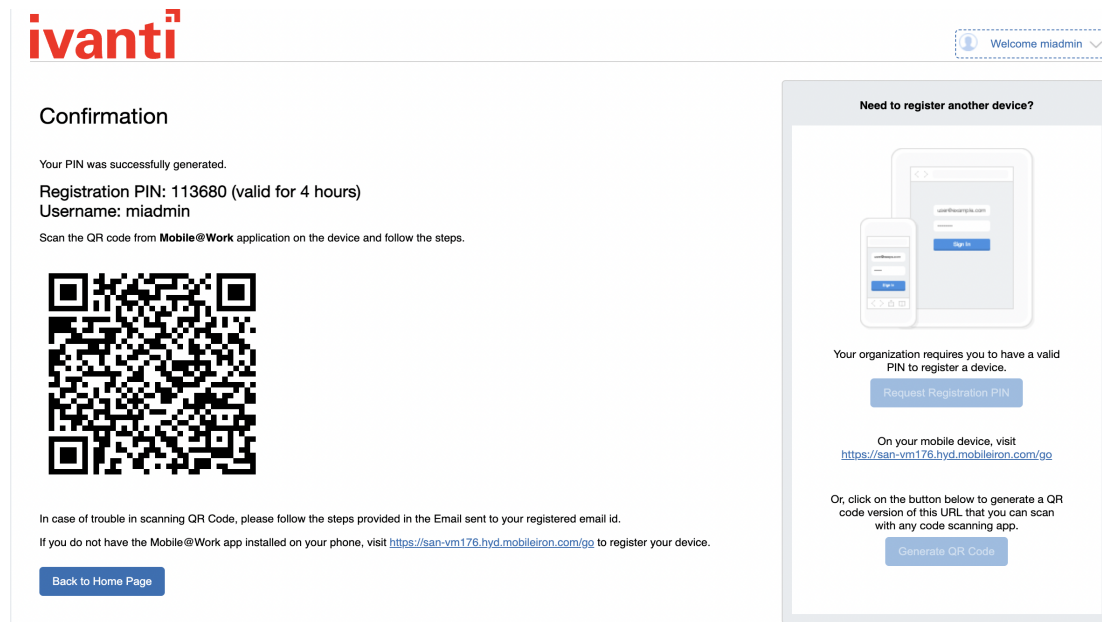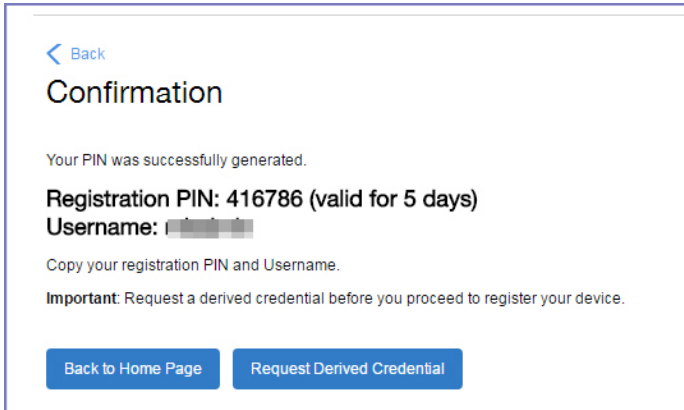
If getting an Entrust derived credential is enabled

> ℹ️ This feature is not supported on macOS devices.

If you enabled getting an Entrust derived credential in the System Manager, device users will see **Request Derived Credential** when they receive their registration PIN for a device. Before using the registration PIN to register Ivanti Mobile@Work to Ivanti EPMM, the device user should request a derived credential.

FIGURE 7. REQUEST DERIVED CREDENTIALS

To get a derived credential:

1. Select **Request Derived Credential.**

   The user is directed to the Entrust IdentityGuard self-service module URL that you specified in the System Manager.

2. The user interacts with the Entrust self-service portal to get a derived credential, including naming the derived credential.

   The Entrust self-service portal provides a Derived Mobile Smart Credential Activation Password.

   Important: The user must record this password for later use in activating the derived credential.

3. After recording the password, the user follows directions to indicate he is done.

   The user is directed back to the user portal. A brief message indicates whether getting the derived credential was successful. If it was successful, **Request Derived Credential** is disabled.

The user then does the following:

1. Use Ivanti Mobile@Work to register the device to Ivanti EPMM.
2. Use the PIV-D Entrust app on the device to activate the derived credential.

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
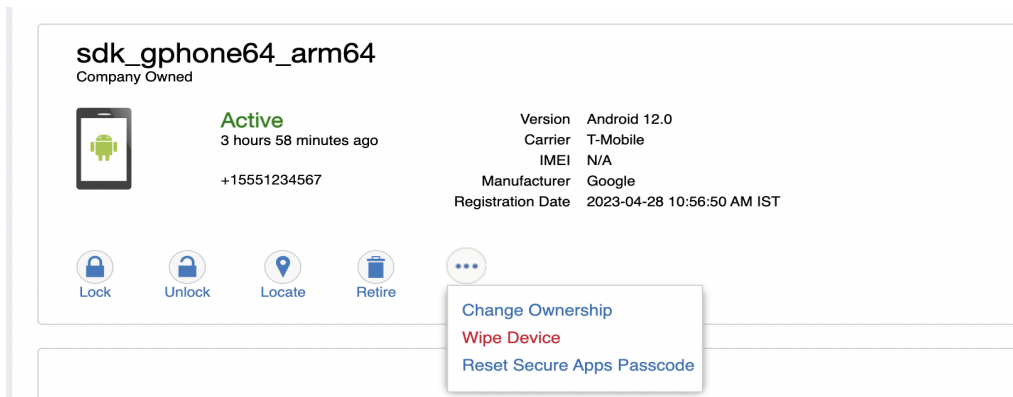
Selecting **Change Ownership** allows the user to change the device ownership.

FIGURE 9. CHANGE DEVICE OWNERSHIP SETTINGS
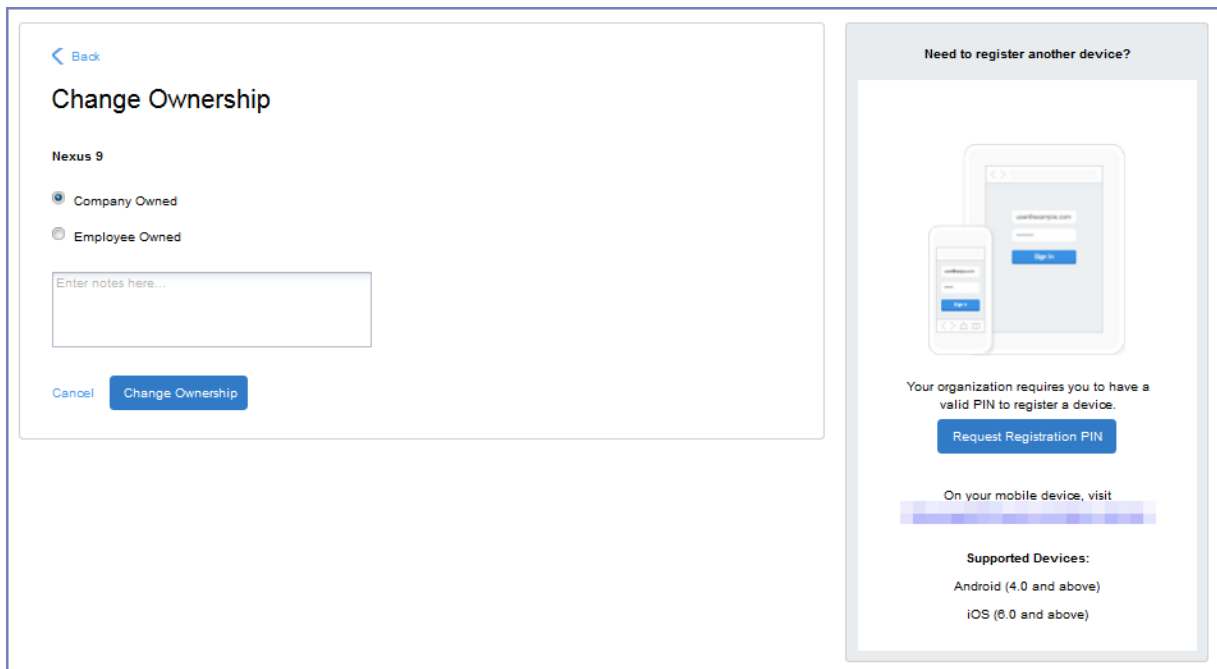
If Default ownership for devices is enabled for Device users

If your device administrator 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 administrator settings on the Registration page, see "Understanding the Registration page" in the Devices chapter of *Getting Started with Ivanti EPMM*.

If generating a one-time PIN for resetting the secure apps passcode is enabled

If you have configured Ivanti EPMM as described in , the device user sees the option **Reset Secure Apps Passcode**. This option is among the device management actions presented to the user for iOS and Android devices.

FIGURE 10. RESET SECURE APPS PASSCODE
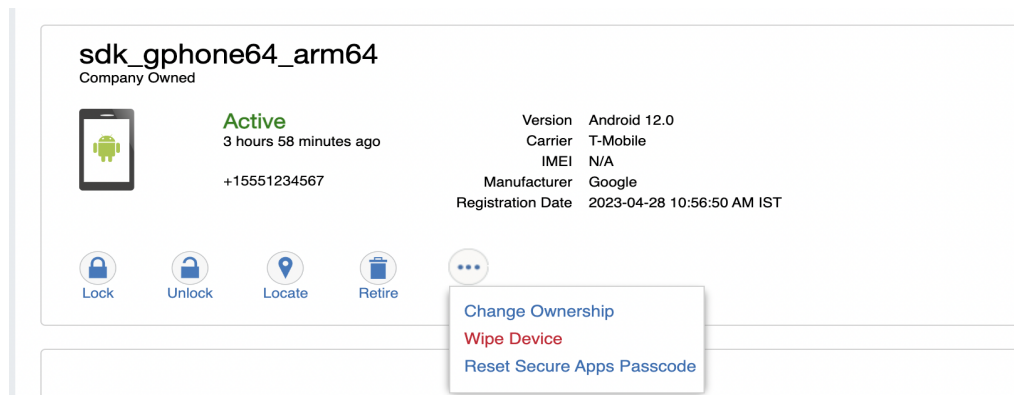
Procedure

1. Select **Reset Secure Apps Passcode**.
2. On the next screen, select the button **Reset Secure Apps Passcode.**
3. A dialog box displays containing the one-time PIN.
4. In Ivanti Mobile@Work on an iOS device, or in the Secure Apps Manager on an Android device, follow the instructions for resetting a forgotten secure apps passcode.
5. When prompted for user credentials, enter the user name and the one-time PIN.
6. Follow the instructions to create a new secure apps passcode.

What client users see after registering their device

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 Ivanti EPMM
- Accounts settings and certificates uploaded by the device user.
- Helpdesk contact information configured by the Ivanti EPMM administrator.

FIGURE 11. USER PORTAL SHOWING USER'S DEVICE INFORMATION

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.
- **Helpdesk** - Configure the help desk contact information to display in the user portal. See "Configuring help desk contact information" on page 951.

- **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 1. SEND INVITATION TO REGISTER

After the invitation is sent, the device status is seen as **Pending**.

FIGURE 2. REGISTRATION PENDING FOR DEVICE

Device users can complete the registration on their mobile device at https://<*Ivanti EPMM_Server_FQDN*>/go.

FIGURE 3. COMPLETE DEVICE REGISTRATION

After registration is completed on the mobile device, the status for the device is changed to **Active**.

FIGURE 4. ACTIVE DEVICE STATUS

Registration instructions

On iOS devices, Ivanti Mobile@Work is installed only if it was set up for distribution through Ivanti EPMM. If not, users can download Ivanti Mobile@Work from the Apple App Store. Instructions for downloading Ivanti Mobile@Work from the Apple App Store are provided in the email sent to the device user.

If PIN-based registration is enabled

If PIN-based registration is enabled, device users will see the Request Registration PIN page.

Selecting **Request PIN** allows device users to request registration and generate a PIN.

FIGURE 1. REGISTRATION WITH PIN
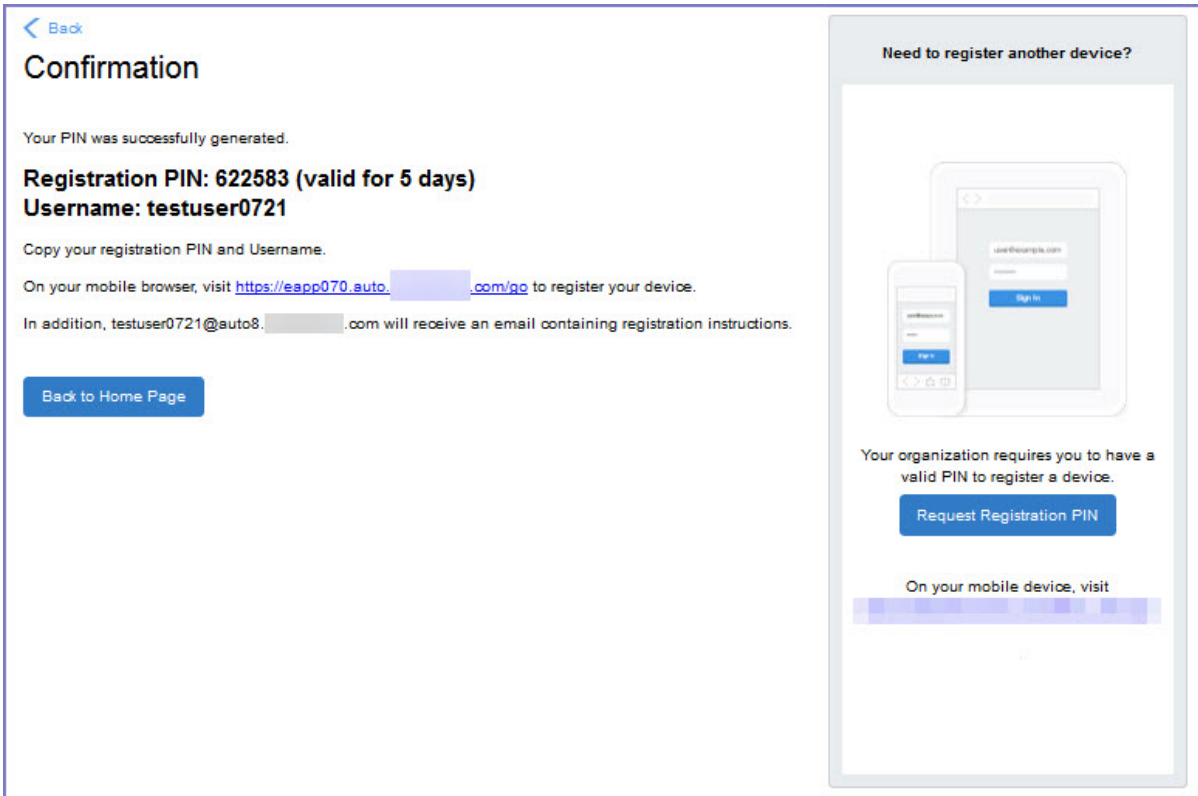
Device users can complete the registration on their mobile device at https://<*Ivanti EPMM_Server_FQDN*>/go. If prompted, they will need to enter the PIN.

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.
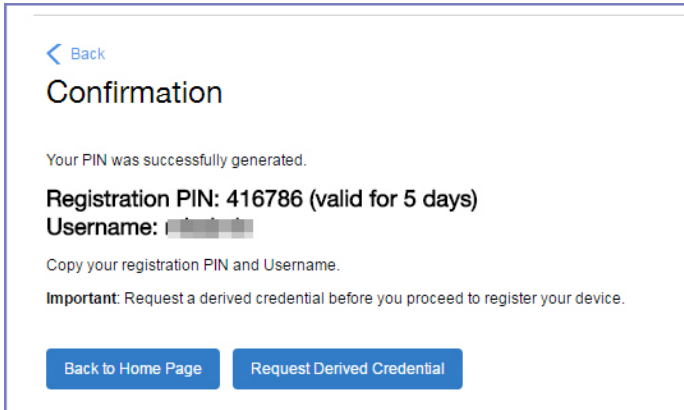
FIGURE 1. REGISTRATION WITH QR CODE
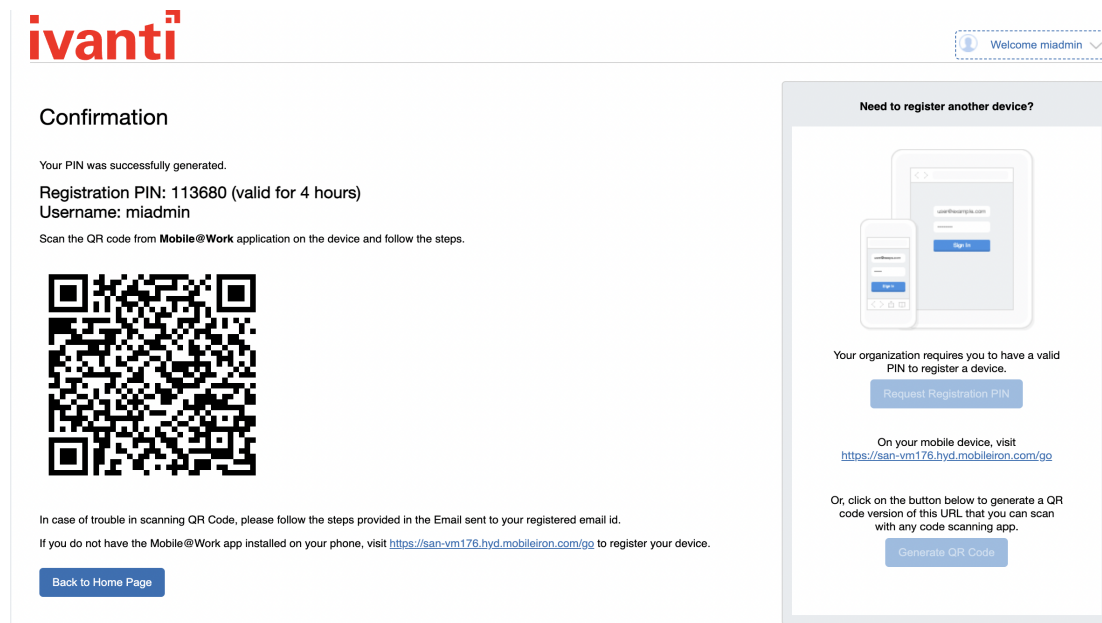
If getting an Entrust derived credential is enabled

ℹ️ This feature is not supported on macOS devices.

If you enabled getting an Entrust derived credential in the System Manager, device users will see **Request Derived Credential** when they receive their registration PIN for a device. Before using the registration PIN to register Ivanti Mobile@Work to Ivanti EPMM, the device user should request a derived credential.

FIGURE 1. REQUEST DERIVED CREDENTIALS

To get a derived credential:

1. Select **Request Derived Credential.**

    The user is directed to the Entrust IdentityGuard self-service module URL that you specified in the System Manager.

2. The user interacts with the Entrust self-service portal to get a derived credential, including naming the derived credential.

    The Entrust self-service portal provides a Derived Mobile Smart Credential Activation Password.

    Important: The user must record this password for later use in activating the derived credential.

3. After recording the password, the user follows directions to indicate he is done.

    The user is directed back to the user portal. A brief message indicates whether getting the derived credential was successful. If it was successful, **Request Derived Credential** is disabled.

The user then does the following:

1. Use Ivanti Mobile@Work to register the device to Ivanti EPMM.

2. Use the PIV-D Entrust app on the device to activate the derived credential.
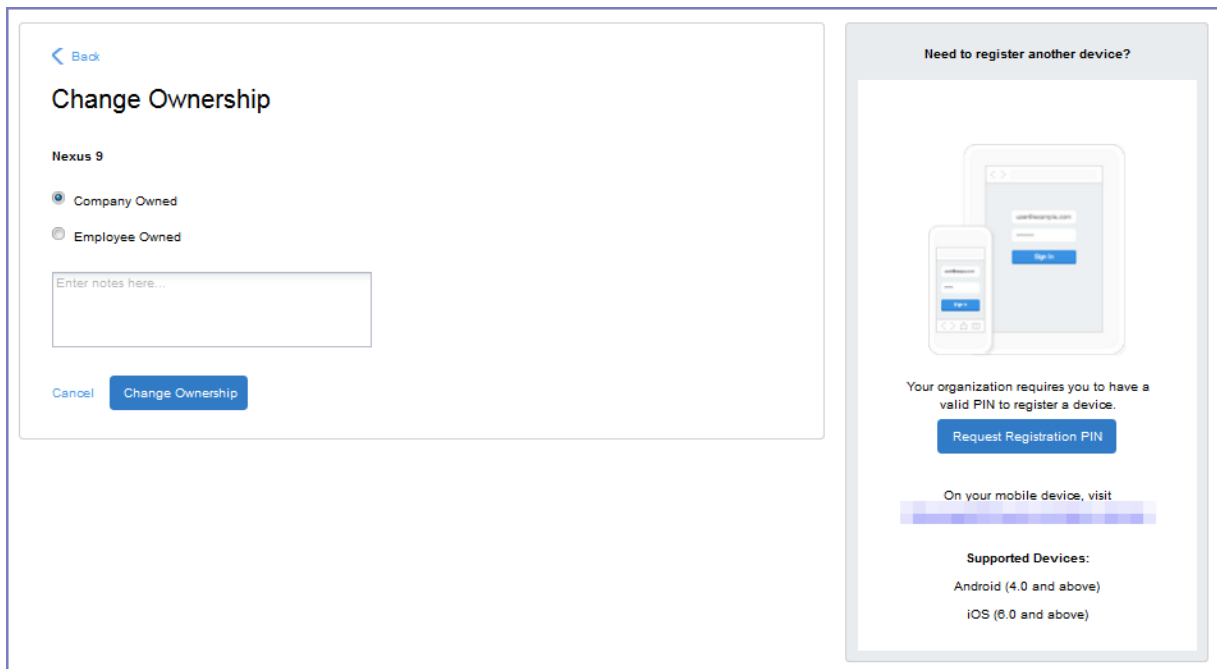
If Change Device Ownership role is enabled

If the **Change Device Ownership** role is enabled, device users will see the option to change the device ownership.

FIGURE 1. CHANGE DEVICE OWNERSHIP OPTION
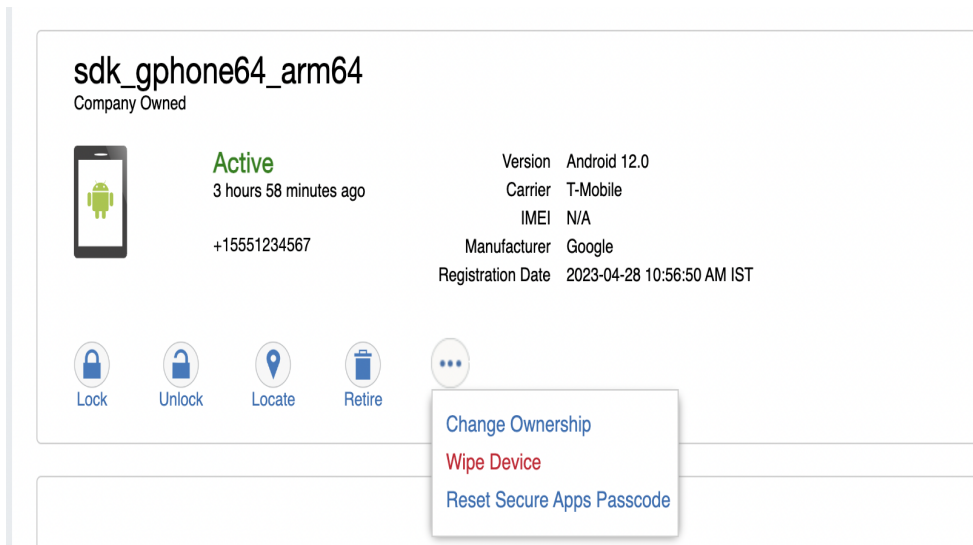
Clicking on **Change Ownership** allows the user to change the device ownership.

FIGURE 2. CHANGE DEVICE OWNERSHIP SETTINGS

If Default ownership for devices is enabled

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 Ivanti EPMM*.

If generating a one-time PIN for resetting the secure apps passcode is enabled

If you have configured Ivanti EPMM as described in , the device user sees the option **Reset Secure Apps Passcode**. This option is among the device management actions presented to the user for iOS and Android devices.

FIGURE 1. RESET SECURE APPS PASSCODE
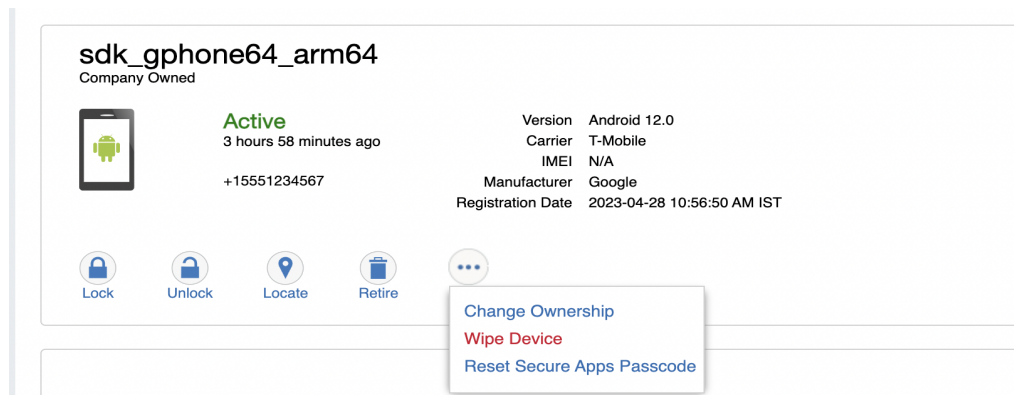
Procedure

1. Select **Reset Secure Apps Passcode**.

2. In the next screen, select the button **Reset Secure Apps Passcode.**

3. A dialog box displays containing the one-time PIN.

4. In Ivanti Mobile@Work on an iOS device, or in the Secure Apps Manager on an Android device, follow the instructions for resetting a forgotten secure apps passcode.

5. When prompted for user credentials, enter the user name and the one-time PIN.

6. Follow the instructions to create a new secure apps passcode.

What client users see after registering their device

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 Ivanti EPMM
- Accounts settings and certificates uploaded by the device user.
- Helpdesk contact information configured by the Ivanti EPMM administrator.

FIGURE 1. USER PORTAL SHOWING USER'S DEVICE INFORMATION

Trust and Untrust options for client users

If enabled, client users can use the **Trust** and **UnTrust** options to protect company data and applications in risky locations.

- **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 administrator must configure **Trust** and **UnTrust** labels for device users. See "Enabling the iOS Trust/UnTrust option" on page 967.
- Client device users must have the **Trust/Untrust** role assigned to them or to their LDAP group.

Procedure

To enable Trust and Untrust options on the device:

1. From a supported iPhone, click the Ivanti icon. The following pop-up message displays:

   Untrusted Enterprise Developer
   "iPhone Distribution: Ivanti" 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 Ivanti app will display there under **Enterprise App**.
4. Click the Ivanti 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.

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://*<Ivanti_EPMM_Server_FQDN>*/user.

2. Select on the device user's name in the top right corner.

3. Select on **Settings** in the drop down menu.
   The **User-Provided Certificate Management** page appears.

4. To view information about an uploaded certificate, select the "**i**" next to the certificate.

5. To replace a certificate, select the **edit** icon next to the certificate.

6. To delete a certificate, select the **delete** icon next to the certificate.

> **Note:** When you navigate to **MICS (System manager portal) > Security > Certificate Mgmt > iOS Enrollment certificate > View**, click on View Certificate in Ivanti EPMM, the entire iOS Enrollment Certification chain is visible, not just the immediate issuing CA certificate.

Uploading certificates in the user portal on a desktop computer
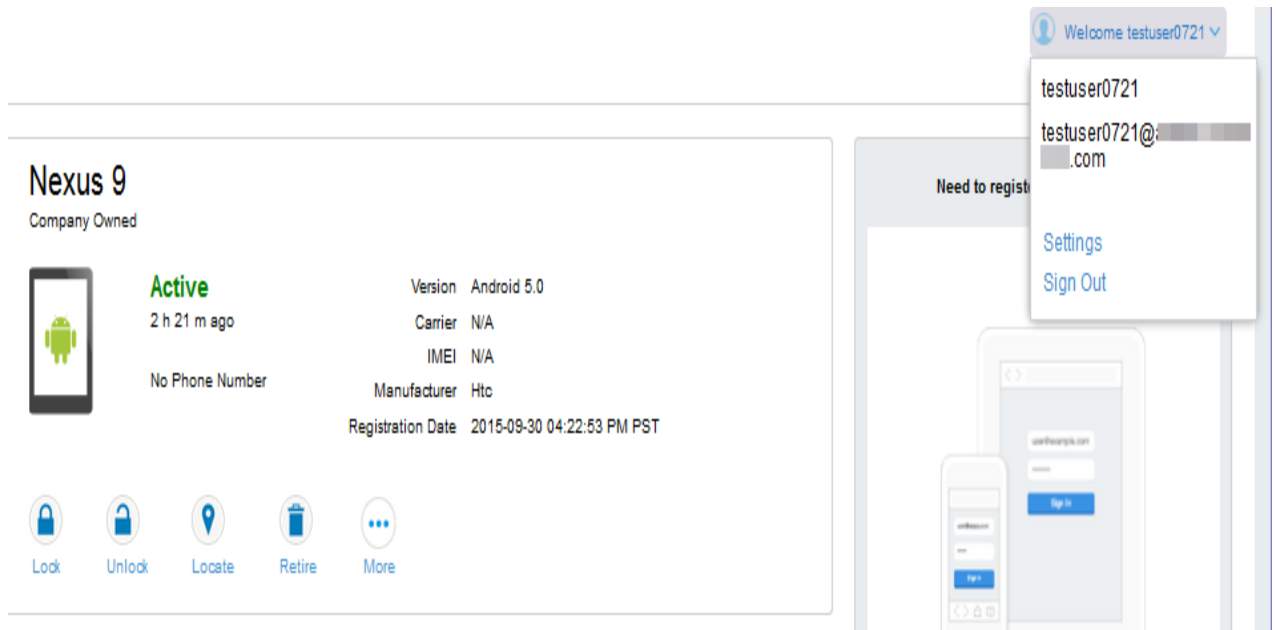
> This feature is not supported on macOS devices.

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://*<EPMM_Server_FQDN>*/user.

2. Select the device user's name in the top right corner.

3. Select **Settings** in the drop down menu.

4. Select **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. Select **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 the help desk contact information

If the help desk contact information is configured in the 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 951

Procedure

1. Go to https://*<EPMM_Server_FQDN>*/user.

2. Select on the device user's name in the top right corner.

3. Select **Helpdesk** in the drop down menu.
   The **Helpdesk** page appears.

FIGURE 1. HELPDESK CONTACT INFORMATION