



Ivanti EPMM 11.4.0.0 - 11.12.0.0 Device Management Guide

for Android and Android Enterprise Devices

Revised: April 2024

Revision history

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

Contents

Revision history	2
Android Deployment Models	8
Android Enterprise devices	8
Android devices using the device administrator	8
Android MAM-only devices	9
AppConnect for Android devices	9
Samsung Knox Workspace devices	9
Wear OS by Google	10
Setting up Ivanti EPMM for Android Enterprise	12
Android Enterprise Overview	12
Enabling Android Enterprise	15
Configuring the security policy for Android Enterprise devices	25
Configuring the lockdown policy for Android Enterprise devices	26
Removing Android Enterprise	26
Setting up Ivanti EPMM with a closed network / AOSP deployment	28
Use cases	29
Enabling a closed network / AOSP deployment in Ivanti EPMM	30
Creating a new Android Enterprise configuration	31
Provisioning the Android device	32
Managing the closed network / AOSP devices	33
Managing Devices	37
Enabling Server Name Lookup	37
Registering Devices	39
General management of devices	91
Searching for Devices	96
Securing Devices	126
Managing Custom Attributes	165
Custom Attributes	165
Assigning a custom attributes role	166
Adding custom attributes to users and/or devices	167
Viewing custom attributes available for users and/or devices	168
Viewing custom attributes assigned to users	168
Viewing custom attributes assigned to devices	168
Editing custom attributes for users and/or devices	168
Searching for custom attributes for users and/or devices	169
Exporting a log of the custom attributes for users and/or devices	169
Deleting custom attributes from users and/or devices	169
Setting custom attribute values for device or users	170
Viewing custom attribute changes	171
Pushing label attribute changes to devices and users	171
Managing Policies	173

Working with default policies	174
Importing and exporting policies	176
Viewing policy status and platform support	178
Security Policy	179
Global App Config Settings policy	180
Sync policies and battery use	191
Work Schedule policy	191
Country changes and alerts	194
Android devices and the Client Is Always Connected option	194
Enabling attestation on Android devices	194
Working with Windows Update policies	198
Working with Samsung Android kiosk policies	198
Working with Android Quick Setup policies	198
Working with Samsung general policies	200
Working with Wear OS device policies	207
Notifications of changes to the privacy policy	209
Exporting the devices in the WatchList	209
Managing Compliance	210
Managing device compliance checks	210
Tiered compliance	218
Compliance actions policy violations	219
Viewing quarantine information	227
Viewing configurations removed due to quarantine	227
Custom compliance policies	228
Managing Device Settings with Configurations	243
Management of device settings with configurations	243
Configurations page	244
Default configurations	245
Displaying configurations status	247
Adding new configurations	248
Editing configurations	249
Deleting configurations	249
Exporting configurations	249
Importing configurations	250
Applying configurations to labels	250
Android File Transfer Configurations	251
Android Enhanced Multiple-Slicing Support	256
Exporting the devices in the WatchList	256
Impact of changing LDAP server variables	257
Configuring Email	258
Exchange settings	258
Configuring POP and IMAP email settings (for iOS and macOS)	265
Synchronizing Google account data	266
Setting up Gmail with Android Enterprise	272

Managing Wi-Fi Settings	274
Wi-Fi settings	274
Wi-Fi profiles and password caching	277
Wi-Fi network priority for Android devices	277
Using Wi-Fi priority values	281
How an Android device chooses its Wi-Fi network	282
Wi-Fi network manual override behavior	283
Wi-Fi authentication types	284
Managing VPN Settings	300
VPN settings overview	300
Configuring new VPN settings	301
Cisco Legacy AnyConnect	301
F5 SSL	310
Juniper SSL	317
Tunnel (Android)	325
Tunnel (Samsung Knox Workspace)	325
OpenVPN	326
Palo Alto Networks GlobalProtect	328
PPTP	334
Pulse Secure SSL	339
Encrypting and Decrypting logs	346
Knox VPN Support	348
Managing Certificates and Configuring Certificate Authorities	367
Certificates overview	367
Managing certificates issued by certificate enrollment configurations	371
Configuring certificate pinning for registered devices	371
Supported certificate scenarios	373
Ivanti EPMM as a certificate authority	375
Configuring Ivanti EPMM as an independent root CA (Self-Signed)	376
Configuring Ivanti EPMM as an intermediate CA	381
Mutual authentication between devices and Ivanti EPMM	382
Certificates settings	395
Certificate Enrollment settings	397
Configuring a client-provided certificate enrollment setting	401
Configuring an Entrust CA	403
Configuring a GlobalSign CA	406
Configuring Ivanti EPMM as the CA	409
Configuring OpenTrust CA	411
Configuring a single file identity certificate enrollment setting	413
Configuring SCEP	415
Enabling Kerberos Authentication between EPMM and the SCEP and LDAP servers	420
Configuring Symantec Managed PKI	422
Configuring Symantec Web Services Managed PKI	425
Configuring a user-provided certificate enrollment setting	428

Android shared-kiosk mode overview	433
Setting up the Android shared-kiosk mode	433
Configuring the Android shared-kiosk mode	435
User experience for staging and shared kiosk users	444
Suggestions for configuring shared-kiosk mode	446
Working with Events	448
About events	448
Managing events	449
Event settings	454
Customizing Event Center messages	471
Viewing and Exporting Events	478
Troubleshooting Ivanti EPMM and devices	481
Pushing device profiles	481
About Ivanti EPMM logs	482
Audit log information	490
Before and after log information	491
Best practices: label management	491
Device events	493
ActiveSync Device information	495
MDM events	496
Certificate events	497
App Tunnel events	497
Audit Logs use cases	503
MDM Activity	507
Certificate Management	508
Service Diagnostic tests	511
Device log encryption on Android devices	513
Encrypting device logs with your own certificate	515
Pull client logs for client devices	516
Office 365	518
Office 365 App Protection overview	518
Office 365 App Protection policies	520
Office 365 App Protection configurations	528
Office 365 App Protection user groups	531
Office 365 App Protection reports	531
Office 365 App Protection settings	538
Zebra Support	539
Samsung Knox Settings	549
Azure Tenant	564
Overview	564
From the Ivanti EPMM administrator's point of view	566
From the device user's point of view	566
Apply the Intune license to device users	567
Adding Ivanti EPMM as a compliance partner	567

Creating a conditional access policy in Microsoft Endpoint Manager	570
Connecting Microsoft Azure to Ivanti EPMM	574
Creating a partner device compliance policy	580
De-provisioning of the Azure tenant	582
Installing Ivanti Mobile@Work for iOS and Android	583
Required client device user action and use cases	584
Help@Work for Android	586
About Help@Work for Android	586
How Help@Work for Android works	588
Help@Work for Android setup overview	589
Installing TeamViewer on your desktop	589
Requesting a TeamViewer account	590
Creating a TeamViewer app	592
Enabling Help@Work in Ivanti EPMM	594
Deploying the TeamViewer QuickSupport app	595
Starting a remote control session	596
Language Support	604
Translated versions of client apps	605
Selecting languages for Ivanti EPMM messages	605
Setting the system default language	606
Changing language selection from the Admin Portal	606
Samsung Android Kiosk Support	608
About Samsung Android kiosk	608
Setting up Samsung Android kiosk mode	609
Samsung Android kiosk policy	610
Creating a Samsung Android kiosk configuration for multiple-app mode	615
Enabling and Disabling Samsung Android kiosk mode	617
An example of Samsung Android kiosk mode	618
Information about Samsung Android kiosk mode in device details	619
Samsung Android kiosk mode deployment notes	619
Setting the kiosk policy for Android managed devices	620
The SMS Archive Feature	626
About the SMS & Call Log Archive feature	626
Supported devices	626
Setting Up the SMS & Call Log Archive feature	626
Setting up encrypted SMS and call log archive encryption	628
Monitoring the SMS & Call Log archive	629
Self-service User Portal	631
Setting up the self-service user portal	632
Using the self-service user portal	653
What is the self-service user portal?	677
Setting up Android Enterprise with the alternative method	679
Method 1: Setting up using AFW json file generated from google account	679
Managing users for Android Enterprise	688

Android Deployment Models

Ivanti EPMM supports these deployment models for Android devices that are registered to Ivanti EPMM:

- ["Android Enterprise devices" below](#)
- ["Android devices using the device administrator" below](#)
- ["Android MAM-only devices" on the next page](#)
- ["AppConnect for Android devices" on the next page](#)
- ["Samsung Knox Workspace devices" on the next page](#)
- ["Wear OS by Google" on page 10](#)



Different devices can have each of these deployment models.

Android Enterprise devices

Android Enterprise is Google's program for supporting Android devices for enterprise. Android Enterprise enables devices to have separate private and work profile deployments, and enables administrators to have broader control over enterprise owned and provisioned devices. Ivanti EPMM supports Android Enterprise.

Related topics

- ["Setting up Ivanti EPMM for Android Enterprise" on page 12](#)
- "Managing Mobile Apps for Android Enterprise" in the *Ivanti EPMM Apps@Work Guide*.

Android devices using the device administrator

In this deployment model, Ivanti Mobile@Work has Android device administrator privileges. With these privileges, Ivanti EPMM is the Mobile Device Management (MDM) server for a registered device. As the MDM server, Ivanti EPMM, with help from Ivanti Mobile@Work, can enforce many MDM features, such as device password requirements, device encryption requirements, lockdown requirements, Samsung-specific features, and more. Ivanti EPMM can also perform Mobile App Management (MAM) on the devices.

Android MAM-only devices

In this deployment model, Ivanti EPMM provides only Mobile App Management (MAM) features for a registered device. Ivanti EPMM supports app installations using Apps@Work and most policies and configurations. However, because Ivanti Mobile@Work does not have device administrator privileges, Ivanti EPMM provides no MDM features to the device.

Related topics

“Managing apps on MAM-only devices” in the *Ivanti EPMM Apps@Work Guide*.

AppConnect for Android devices

AppConnect for Android is Ivanti’s solution that containerizes apps to protect data on registered Android devices. Each AppConnect-enabled app becomes a secure container whose data is encrypted, protected from unauthorized access, and removable. Because each user has multiple business apps, each app container is also connected to other secure app containers. This connection allows the AppConnect-enabled apps to share data, like documents.

Ivanti EPMM supports AppConnect for Android only on:

- devices using the device administrator
- MAM-only devices

Ivanti EPMM does not support AppConnect for Android on:

- Android Enterprise devices
- Samsung Knox devices

Related topics

AppConnect Guide for EPMM

Samsung Knox Workspace devices

Ivanti EPMM supports Samsung Knox Workspace devices. Samsung Knox Workspace provides a secure container for corporate apps within a device.



IMPORTANT: You cannot deploy Samsung Knox Workspace and Android Enterprise containers on a device at the same time. Additionally, Ivanti EPMM does not support using both Samsung Knox Workspace and AppConnect apps on the same device.

Related topics

["Samsung Knox Settings" on page 549](#)

Wear OS by Google

Ivanti Mobile@Work for Android utilizes the Google Wear OS app as a companion app for Android phones and tablets. The Wear OS app works with Ivanti Mobile@Work in Android Enterprise deployments for Work managed device (DO) mode. The Wear OS app can be used by administrators to track the presence and inventory of apps on Wear OS devices in a corporate environment.

In Ivanti EPMM, the Devices & Users page displays the information gathered from the watch, in addition to displaying all watches paired with the local device. If the connection to the Wear OS device is not established up to 1 week, Ivanti EPMM will purge the data from the Device Details page > Wear OS tab. Ivanti Mobile@Work will not display watches paired with remote devices.



Ivanti Mobile@Work for Android (phone) receives Wear OS data from the Wear OS device (watch) and the Android system tends to cache this data for an unknown time frame. There is a possibility that the true value of the "Wear OS Client Installed" field in Device Details > Wear OS tab is delayed for several hours.

Procedure

1. Create a Wear OS policy (see ["Working with Wear OS device policies" on page 207.](#))
2. View the paired watch in the Device Details page > Wear OS tab. (see ["Viewing paired watch information " below.](#))
3. Search for watch information in ["Advanced searching " on page 97.](#)
4. ["Removing paired watch information" on the next page.](#)

Viewing paired watch information

Once you have a Wear OS policy in place, the Device Details page displays information about the Wear OS device that is connected to a mobile phone. This feature is applicable to Work managed device (DO) mode.

Procedure

1. Select **Devices & Users > Devices**.
2. Select the device. The device details display below.
3. Select the **Wear OS** tab. The Wear OS device details and application inventory display.

TABLE 1. WEAR OS TAB

Item	Description
Last Check-in Time	Lists the time stamp of the last time the Wear OS app checked in. The value field is updated when the device checks in.
Android Wear Make	Displays the make of the Wear OS device.
OS version	Displays the OS of the Wear OS device.
Model	Displays the model of the Wear OS device.
Brand	Displays the brand of the Wear OS device.
Serial Number	The serial number of the watch. The value of this item is blank if the device user has not granted permission on the watch app.

Below the initial Wear OS information, a table displays the name of the app, its version number and the app's identifier.

Removing paired watch information

When the Ivanti Mobile@Work client is erased (wiped) from the phone, the Wear OS data (including policies) stored in Ivanti EPMM is purged after a specific time frame, only if the device is retired and the purge data setting is active. For example, if the device is retired and the "Delete Retired Device" field is set for 1 day, the data is purged from the Wear OS tab after 1 day the device is retired. Administrators can change the purge time frame (1-365 days) in Settings >Users & Devices > Delete Retired Devices.

Related topics

- ["Working with Wear OS device policies" on page 207](#)

Setting up Ivanti EPMM for Android Enterprise

Ivanti EPMM supports Android Enterprise devices.

- ["Android Enterprise Overview " below](#)
- ["Enabling Android Enterprise" on page 15](#)
- ["Configuring the security policy for Android Enterprise devices" on page 25](#)
- ["Configuring the lockdown policy for Android Enterprise devices" on page 26](#)
- ["Managing users for Android Enterprise" on page 688](#)
- ["Removing Android Enterprise" on page 26](#)

Android Enterprise Overview

Android Enterprise is Google's program for supporting Android devices for enterprise. Android Enterprise enables devices to have separate private and work profile deployments, and enables administrators to have broader control over enterprise owned and provisioned devices. Ivanti EPMM supports Android Enterprise. This support requires you to perform setup tasks with Google, Ivanti (help.ivanti.com), and the Admin Portal.

Modes for Android Enterprise devices

Android Enterprise devices that are registered with Ivanti EPMM are in one of the following Android Enterprise modes:

- **Work Profile mode:** An Android Enterprise device is in Work Profile mode when it has a *work profile*. Corporate data and apps are secured in the *work profile*, while the user's private data and apps are in the separate *personal profile*. Ivanti EPMM has administrative control over the work profile. For more information see <https://developers.google.com/android/work/requirements/work-profile>.

- **Work Managed Device mode:** An Android Enterprise device that is in Work Managed Device mode is typically corporate-owned. The device has a single profile with corporate data and apps. This mode is only available on factory installed devices. If a device with this mode on it is wiped it will no longer be in Work Managed Device mode. Ivanti EPMM has administrative control over the device, with more lockdown features available than for device using a work profile. For more information see [Google's "Fully managed device" article](#).
- **Managed Device with Work Profile (COPE) mode:** An Android Enterprise device in this mode is an enterprise-owned device with personal data separate from the rest of the phone. It has a small client installed on it to separate personal data from the rest of the phone. This mode is only available on factory installed or factory reset devices. If a device in this mode is wiped it will no longer be in Work Managed Device mode. This mode requires:
- **Work Profile on Company Owned Devices mode:** This is similar to the Work Profile mode with a few additional device level configurations controlled from Work profile. Applies to Android versions 11 or supported newer versions.
 - Ivanti Mobile@Work 9.7 or supported newer versions.
 - Only works on Android versions 8-10.
 - A managed Google Play account
 - If the account is enrolled with Google Domain, the device will be registered in the Work Managed Device mode.



In Android developer documentation, "work profile" is referred to as "profile owner" and "work managed device" is referred to as "device owner".

Requirements for using Android Enterprise

To enable Android Enterprise for your enterprise and use it with Ivanti EPMM, you need:

- A Google account that is not tied to Managed Google Accounts. That is, any Google account that is not managed by an enterprise can be used for enrolling with Android Enterprise.

- Access to Google Play on Android devices and Ivanti EPMM.
- Access to these URLs through outbound HTTP proxy:
 - <https://accounts.google.com/o/oauth2/token>
 - <https://www.googleapis.com>
- See Outbound HTTP Proxy Set Up in the *On-Premise Installation Guide for Ivanti EPMM and Enterprise Connector*.

Requirements for using an Android Enterprise device in work profile mode

To enable an Android Enterprise device in work profile mode, the following is required:

- An Android Enterprise-capable device, running Android 6.0 or supported newer versions, with the Ivanti Mobile@Work for Android app installed



The Ivanti Mobile@Work app on Android devices shows whether the device is Android Enterprise-capable in the Settings > About > Product Details tab. Google provides a list of Android Enterprise-capable devices here: <https://enterprise.google.com/android/>.

- If using managed Google Play Accounts, Ivanti EPMM automatically generates a Google User based on the UUID of the user.
- An Android Enterprise setting on Ivanti EPMM (**Policies & Configs > Configurations**) applied by label to the device

Requirements for using an Android Enterprise device in work managed mode

To enable an Android Enterprise device in work managed mode, all the ["Requirements for using an Android Enterprise device in work profile mode"](#) above are necessary. In addition, for work managed mode devices, you must enroll devices with either NFC, QR code, "afw#" tokens, Knox Mobile Enrollment (KME), or Google's Zero-Touch. For more information, see ["Provisioning an Android Enterprise device" on page 75](#).

Requirements for using an Android Enterprise device in Managed Device with Work Profile mode and Work Profile on Company Owned Device mode

To enable an Android Enterprise device in Managed Device with Work Profile mode and Work Profile on Company Owned Device mode, all the ["Requirements for using an Android Enterprise device in work profile mode" on the previous page](#) and ["Requirements for using an Android Enterprise device in work managed mode" on the previous page](#) are necessary. In addition, for devices in this mode, you must select **Enable Managed Device with Work Profile on the devices** on the Android Enterprise setting. This setting applies to Android 8, 9, and 10 devices. For Work Profile on Company Owned Device mode, this setting applies to Android 11.0 devices.

Enabling Android Enterprise

To enable Ivanti EPMM to provide Android Enterprise features, you must perform setup steps with Google, Ivanti Support, and Ivanti EPMM. You will associate a managed Google Play Account with Ivanti EPMM. Note that this procedure does not share your enterprise's user names or email addresses with Google.

Depending on if you are a new or upgrading customer, the app distribution settings are different. If you are a new customer, the app distribution is set to per device by default. You cannot change this setting. For upgrading customers, you have a choice between apps distribution per user or per device. Also for upgrading customers, app distribution per user is selected by default. Many users have multiple devices. If a user has multiple devices, when app distribution is set per device then you can make a different set of apps available on each device.

Procedure

1. Log into help.ivanti.com.
2. Select **Android enterprise Enrollments**.
3. Select **Create New Android enterprise Enrollment**.

The screen **Android enterprise Setup - Step 1** displays.

4. Select **Begin**.

Do not select **Alternate Setup Method**. If you used the alternate setup method in the past, see ["Method 1: Setting up using AFW json file generated from google account" on page 679](#).

After selecting **Begin**, the screen **Android enterprise Setup - Step 2** displays.

5. Use the radio buttons to select a brand that matches the Ivanti EPMM you are using.

6. Select **Submit**.
7. The Bring Android to Work page displays. Select **Sign In**.
8. Sign in with a Google account.
9. Select **Get Started**.
10. Enter your Organization details: name and agree to the **managed Google Play agreement**.
11. Select **CONFIRM**.
12. Select **COMPLETE REGISTRATION**.
13. The **Android enterprise Enrollment** page displayed in help.ivanti.com.

Select **Download Google JSON Enrollment file**.

The downloadService JSON file is downloaded.

Store it in an accessible file location for later use, such as if you need to enable Android Enterprise on another Ivanti EPMM.

14. Log into the Admin Portal and go to **Services > Google**.
15. Upload the JSON file. Use the browse button to navigate to the JSON file you downloaded earlier in this procedure and select **Connect**.

The Google Play App Catalog dialog box opens with this warning message: If more than one Ivanti EPMM instance is publishing the Google Play layout, you will be sending redundant (possibly conflicting) layouts to Google. This does NOT affect the distribution of apps, only the layout visible in Google Play. To use a Custom Layout in the Google Play store see "Distributing your enterprise apps in the Google Play App catalog or in Apps@Work" in the *Ivanti EPMM Apps@Work Guide*. This step is optional.

16. Go to **Policies & Configs > Configurations > Add New > Android > Android enterprise** to go to the New Android enterprise (all modes) Setting dialog box.
17. Enter a Name and Description.
18. To make devices that this setting applies to be in a work profile, select **Enable Managed Device with Work Profile (on Android 10 and below.)** This setting applies to Android 8, 9, and 10 devices.

19. If you are in a European country that has GDPR requirements, Ivanti recommends selecting the **Prompt user for enabling location setting (Fully Managed, Managed Device with Work Profile and Work Profile on Company Owned Device)** check box. This is located in the Android 10 and higher only section of the New Android enterprise (all modes) Setting dialog box.



Administrators also need to select the **Prompt User to Enable Location Services if Wi-Fi/MTD configuration is pushed (Android enterprise)** check box in the Privacy Policy. If this is not selected, then Wi-Fi / MTD configurations will fail if the device user does not enable the device's location setting. For more information, see "Privacy policies" in *Getting Started with Ivanti EPMM*.

20. Ignore **Auto update Mobile@Work app on the devices**. This option is no longer applicable. Using Google Play on the device, a user can specify that apps should be updated automatically. Select **Save**.
21. Apply the Android Enterprise setting to a label that is also applied to Android Enterprise-capable devices.
For example, apply this setting to the built-in **Android** Label, or a custom label that is defined using the filter "android.afw_capable = true". For more details about labels, refer to *Getting Started with Ivanti EPMM*.

For information on the other fields on the Android Enterprise setting, see:

- ["Enabling run-time permissions for Android Enterprise apps" on the next page](#)
- ["Adding a Google account to an Android Enterprise managed device" on page 19](#)
- ["Enabling an Android Enterprise VPN client to be always on" on page 21](#)
- ["Samsung Knox Dual Encryption \(DualDAR\) support" on page 555](#)
- For more information, see ["VPN clients deployed either inside or outside Knox Workspace" on page 349](#).
- Refer to the *Ivanti EPMM Apps@Work Guide*.

Related topics

- ["Impact of removing the Android Enterprise setting from a device" on page 24](#)
- ["Removing Android Enterprise" on page 26](#)

Impact of Android Enterprise setting to devices that are not Android Enterprise-capable

There is no impact to devices that are not Android Enterprise-capable to have the Android Enterprise setting applied. Some devices might become Android Enterprise-capable in the future, if the carrier upgrades the device's firmware.

To view the status of the Android Enterprise setting for a device:

1. Go to **Devices & Users > Devices**.
2. Open the device details for the device.
3. Select the **Configurations** tab.
4. Look for the Android Enterprise setting. The **Status** column displays:
 - **Pending:** The device has not yet confirmed that it has received the setting.
 - **Applied:** The setting is applied.
 - **Sent:** The device is not Android Enterprise-capable; the setting is ignored by Ivanti Mobile@Work .

Determining if a device is Android Enterprise-capable

You can check if a device is Android Enterprise capable by doing the following:

- On the device, open Ivanti Mobile@Work . Tap the menu, and tap **Settings > About > Product Details**. Look for Android Enterprise (AFW) Support and see if its value is **Yes**.
- Once the device is registered, on Ivanti EPMM go to **Devices & Users > Devices** page. Find the device and select the caret next to the display name to view the **Device Details**. Look for the "Android enterprise Capable" row. The value is true if the device is capable.

Enabling run-time permissions for Android Enterprise apps

You can specify whether run-time permissions are automatically accepted or denied for Android Enterprise apps, or whether the device user is prompted to accept run-time permissions when each app requests them. You make this choice in the Android Enterprise setting. The choice you make applies to all Android Enterprise apps on devices that receive the Android Enterprise setting, based on the labels on the devices and the setting.

However, you can also specify run-time permissions for each permission for each app in the app's settings in the Ivanti EPMM App Catalog. The run-time permissions setting for the app in the App Catalog overrides the run-time permissions setting in the Android Enterprise setting.



The run-time permission settings are supported only on Android 6.0 or supported newer versions.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select an Android Enterprise setting.
3. Select **Edit**.
4. Select **Enable Runtime Permissions**.

The choices for run-time permissions display.

5. Select a run-time permission setting.
 - **User Prompt:** The device user is prompted to accept or deny each run-time permission that each app requests when it launches. This behavior also applies if you do not select **Enable Runtime Permissions**.
 - **Always Accept:** The run-time permissions are automatically accepted for each app when it launches. The device user is not prompted.
 - **Always Deny:** The run-time permissions are automatically denied for each app when it launches. The device user is not prompted.
6. Select **Save**.

Related topics

"Features specific to Android Enterprise devices" in the *Ivanti EPMM Apps@Work Guide*.

Adding a Google account to an Android Enterprise managed device

As an administrator, you can add an additional Google account to an Android Enterprise managed device. This action enables you to control which Google account can be added to the Android Enterprise account. This account can only be administered or modified by you, the device administrator. The device user cannot modify or remove the added account or add another account to the managed profile.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select an Android Enterprise setting.
3. Select **Edit**.
4. Select **Add Google Account** check box in the **For Android 6.0 and higher only** section.

A Google Account field displays.

5. Enter the name of a Google Account you want to add.

The added account must be an account with a Google domain. The name can include any of the following Ivanti EPMM substitution variables listed in the information popup next to the field. For example, you can enter:

- \$USER_CUSTOM1\$
- \$LAST_NAME\$. \$FIRST_NAME\$@mycompany.com
- \$DISPLAY_NAME\$@mycompany.com

6. Go to **Policies & Configs > Policies** and select the lockdown policy for this device.
7. Uncheck the **Allow the user to create and modify accounts** option if it is checked.

Searching for devices that are registered as Android Enterprise devices

The Device Details pane for a device indicates the registration status of Android Enterprise devices. These values are:

- **Work Profile**
- **Work Managed Device**
- **Managed Device with Work Profile**
- **Work Profile on Company Owned Device**

You can use advanced search to find devices with the registration statuses of interest to you, and create dynamic labels for those sets of devices, if desired.

Related topics

["Searching for Devices" on page 96](#)

Enabling an Android Enterprise VPN client to be always on

You can specify an Android Enterprise VPN client as an Always-On client.

Procedure

1. Go to **Policies & Configs > Configurations**.
2. Select an Android Enterprise setting.
3. Select **Edit**.
4. Select the **Always-On VPN** check box to display the **App Identifier** drop-down menu.
The drop-down menu lists only apps that are configured to be installed as Android Enterprise apps.
5. Select a VPN app to apply the Always-On setting.
6. Select **Save**.

Note the following:

The Android Enterprise setting displays in Device Details as Partially Applied with an error message in the following cases:

- The selected app is not installed on the device.
- The selected app is installed on the device, but it is not a VPN app, or it is a VPN app that does not support Always-On.

Related topics

- For Samsung Knox VPN settings, see ["Knox VPN Support" on page 348](#).
- For AOSP closed networks, see ["Always-On VPN for AOSP for Android Enterprise devices" on page 35](#).

Moving in-house apps to a Knox v3 Workspace

You can move your in-house apps to a Knox v3 Workspace.

Procedure

1. Go to **Policies & Configs > Configurations**.
2. Select **Add New > Android > Android enterprise**. The New Android enterprise (all modes) Setting dialog box is displayed.
3. Select the check box next to the **Move In-house app into workspace** field. Then the **Package Names** field is displayed.
4. Use the drop-down menu next to the **Package Names** field to select an app name.
5. Select **Save**.

For more information, see ["VPN clients deployed either inside or outside Knox Workspace" on page 349](#).

Requiring a password for accessing the work profile

Typically, a password for an enterprise work profile should not be the same as the device password; however, some devices allow the two passwords to be the same.

Within the Work Challenge section, having the "Block unified password" option selected will force the device user to enter a password twice – first to unlock the device, second to unlock the work profile. (Using the "Block unified password" field helps disable the use one lock option on the device to force device users to specify a security challenge for apps running in the work profile.) This feature is supported on devices using Android 7 or supported newer versions.

- For devices using Ivanti Mobile@Work 10.1.0.0 for Android and Android 9.0 or supported newer versions, select **Block unified password (device and work profiles)** in the Android Enterprise setting. This option appears when you select the **Work Challenge** option.
- For other devices, distribute an Android Enterprise setting with a work challenge configuration that has stricter requirements than the device passcode settings on the security policy for the devices. For example, stricter requirements include increasing the minimum password length in the **Minimum Password Length** field or increasing the number of complex characters in the **Minimum Number of Complex Characters** field.

For more information, see step 15 in the procedure below.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select an Android Enterprise setting.
3. Select **Edit**.
4. In the For Android 7.0 and higher only section, select the **Work Challenge** check box. When a work challenge is set, the administrator can block device passcode matching the work profile. This is to enforce separate work and device passwords so that device users do not unlock the work profile at the same time as unlocking the device.

The Password fields display for configuring your work challenge requirements.

5. Select the Password Type:
 - **Simple PIN:** Includes repeated characters, or ascending/descending characters, for example, 123 or CBA.
 - **Complex PIN:** Select **On** to include numbers that are not repeated and should not be in a sequence, for example, 1234, 2468, 9876. An example of repeating digits is 4444.
 - **Alphanumeric:** At least one letter and one number is required.
6. Set **Minimum Password Length** to the minimum password length ranging from 1 to 16 numbers or characters.
7. Set **Maximum Inactivity Timeout** to the maximum time allowed for the device to be inactive before the user must reenter the work challenge to access the work profile. This may be set to **Never** to prevent timeout.
8. Use **Minimum Number of Complex Characters** to set the minimum number of complex characters required in the password. Complex characters are special characters that are not numbers or letters, such as !, *, and #.
9. Set the **Maximum Password Age** to the number of days until the user must change the work challenge.
10. Set **Maximum Number of Failed Attempts** to the maximum number of attempts to enter the correct password in one login. The default value for failed attempts is 10. When the maximum number of attempts is reached, the work profile is retired.

11. Set **Password History** to how many old work challenge passwords are stored so that the device user cannot repeat them.
12. Select **Block Fingerprint** to prevent a device user from using a fingerprint to replace the work challenge password.



Both the **Block Iris Scan** and **Block Face unlock** fields require either a Samsung device running Samsung OS 7.0 or supported newer versions or a non-Samsung device running Android 9.0 or supported newer versions.

13. Select **Block Iris Scan (Android 9 or Samsung only)** to prevent a device user from using an iris scan to replace the work challenge password.
14. Select **Block Face unlock (Android 9 or Samsung only)** to prevent a device user from using a face scan to replace the work challenge password.
15. Select **Block unified password (device and work profiles)** - by selecting this option, the administrator forces the device user to set a secondary password for the work profile. The system shows the security challenge when the user attempts to open any work apps. This feature is supported on devices using Android 7 or supported newer versions. If this field is de-selected (default), then the device user can use the same password for unlocking the device and the work profile.

Impact of removing the Android Enterprise setting from a device

Removing the Android Enterprise setting from a device causes the device to become retired.

The Android Enterprise setting can be inadvertently removed from a device if:

- The setting is applied to a dynamic label instead of a built-in label, and the device is dynamically removed from the label for any reason, OR
- The Android Enterprise setting is manually removed from a label shared with a device.

Removing the setting from the device causes the following to happen:

TABLE 2. REMOVING ANDROID ENTERPRISE SETTING

Android Enterprise status	If Android Enterprise setting is removed:
Work Profile mode	<ul style="list-style-type: none"> Starting in Ivanti EPMM10.7.0.0, Ivanti EPMM will not display the device as registered. Instead, the Ivanti Mobile@Work app will notify Ivanti EPMM that the device is retired before deleting the work profile. User can re-register the device. The user must re-enable Ivanti Mobile@Work through the Google Play store.
Work Managed Device (DO) mode	<ul style="list-style-type: none"> The device becomes unregistered and performs a factory reset. The device can be re-registered at a later time.
Work Profile on Company Owned Device mode	<ul style="list-style-type: none"> Same as for Work Managed Device (DO) mode.

Related topics

["Removing an Android Enterprise configuration causes device to retire" on the next page](#)

Configuring the security policy for Android Enterprise devices

Most security policy settings for Android Enterprise devices are the same as the settings for other Android devices. However, note that a few settings in the security policy are specific to Android Enterprise devices. These settings are:

- **Block notifications on lock screen** (Android Enterprise Work Managed Devices only)
- **Allow only redacted notifications on lock screen** (for Android Enterprise Work Profile modes only)
- **Bypass Factory Reset Protection** (Applicable to Android Enterprise Work Managed Devices and Work Profile on Company Owned Devices.)

Also in the security policy, you specify compliance actions for various security violations. When a compliance action includes quarantine, on Android Enterprise devices, all Android Enterprise apps and functionality are hidden except for Downloads, Google Play Store, and the Ivanti Mobile@Work app.

When configuring Zebra OTA (Over-the-Air) service, only for Work Managed Zebra devices is supported.

Related topics

- "Security policies" in *Getting Started with Ivanti EPMM*
- "Add Compliance Action table" in *Ivanti EPMM Device Management Guide for Android and Android Enterprise devices*

Configuring the lockdown policy for Android Enterprise devices

You can configure the lockdown policy to apply lockdown settings to Android Enterprise devices. Whether a lockdown policy field applies to an Android Enterprise device depends on the Android Enterprise mode that the device is registered in. The modes - Work Profile Mode, Work Managed Device Mode, Managed Device with Work Profile (COPE) mode and Work Profile on Company Owned device - are described in the ["Android Enterprise Overview" on page 12](#)



For Android Enterprise Work Profile and Work Managed Device modes, only the camera and phone are included in the package identifier. Enable all system apps by logging into the Admin Portal and going to **Policies & Configs > Policies > Add New > Lockdown**.

Related topics

"Lockdown policies" in *Getting Started with Ivanti EPMM*

Removing Android Enterprise

This section addresses the removal of Android Enterprise-related items.

Removing an Android Enterprise configuration causes device to retire

When you enroll an Android device on a dynamic label using Android for Work with Work Profile mode, Work Managed Device mode, and Managed Device with Work Profile (COPE) mode and later modify the label criteria to exclude the device, the following occurs:

- The device's client configuration is removed.
- The device becomes retired and displays in the Retired Device's Dashboard.

This is applicable to Android Enterprise devices in all modes:

- Work Managed Device (Device Owner) mode - a device retire causes a factory reset
- Work Profile mode - a device retire causes deletion of the work profile
- Managed Device with Work Profile (COPE) mode - a device retire causes a factory reset. Applicable to Android devices versions 8-10.
- Work Profile on Company Owned device - a device retire causes a factory reset. Applicable to Android versions 11 or supported newer versions.

Removing the Android Enterprise account in Ivanti EPMM

You can remove the Android Enterprise account from Ivanti EPMM, severing Ivanti EPMM's connection with Google. This removal causes devices to retire when they check in.

Procedure

1. In the Admin Portal, go to **Services > Google**.
2. Under **Android enterprise**, select **Remove** to open the **Remove Account** dialog.
3. If you wish to remove the Android Enterprise account with Ivanti EPMM, select the check box for "I understand" and then select **Remove**.

Ivanti EPMM will retire Android Enterprise devices when they next check in.

Removing your managed Google Play account

You can remove your managed Google Play account if you no longer need it.

Procedure

1. Login to help.ivanti.com.
2. Select **Android enterprise Enrollments**.
3. Select on your managed Google Play Account.
4. The **Android enterprise Enrollment Detail** screen displays.
5. Select **Delete**.

Setting up Ivanti EPMM with a closed network / AOSP deployment

There are situations where the onboarding, registration and management of devices is limited and requires a different approach. Examples of these kinds of situations are:

- In an environment that does not have connectivity to Google mobile services (GMS) due to restrictions in the organization or due to a closed network.
- In countries where Google mobile services are not available.
- Where devices that do not have Google mobile services but vendors have enabled Android Enterprise AOSP (Android Open Source Project.)

With Ivanti EPMM version 11.0.0.0 and later, supports a new mode of deployment:

- **Integrated deployment (GMS/Non-GMS)** - the entire Ivanti EPMM instance serves devices in full Android Enterprise mode (for example, Samsung devices) and also devices that do not have GMS (for example, AR/VR devices.)

This feature applies to Android 6 or supported newer versions.

Ivanti recommends administrators set the device ownership for AOSP devices. This can be done at:

Settings > System Settings > Users & Devices > Device Registration.

- In the Ownership Settings section, in the "Default Ownership of Android devices using Google ZT or Samsung KME or non-GMS (AOSP) mode" field, select **Company owned** or **Employee owned**.
- If you want the Terms of Service to be displayed, select the **Show Terms of Service** check box. Otherwise, the Terms of Service will not display (default.) (To create a Terms of Service, see ["Configuring an end user Terms of Service agreement" on page 638.](#))

Devices that are non-GMS will be identified and reported to the Device Details page. Administrators can view individual devices and run a search for "Non GMS Device."

Use cases

AOSP deployment can work side-by-side with Android Enterprise deployment.

Supported modes of registration supported:

- Device Admin mode
- Device Owner mode

Below are the possible use cases for this feature.

TABLE 3. USE CASES FOR CLOSED NETWORK / AOSP DEPLOYMENT

Use Case	Expected Result
Only the AOSP configuration is pushed	AOSP in Device Admin or Device Owner mode.
Both AOSP and Android Enterprise configurations are pushed	Android Enterprise configuration takes priority over AOSP.
Device is registered in AOSP and the Android Enterprise configuration is pushed to the registered device	The registered device retains AOSP mode. Android Enterprise configuration applies only to fresh registrations.

Process of setting up:

1. ["Enabling a closed network / AOSP deployment in Ivanti EPMM" on the next page.](#)
2. ["Creating a new Android Enterprise configuration" on page 31.](#)
3. ["Provisioning the Android device" on page 32.](#)
4. ["Managing the closed network / AOSP devices" on page 33.](#)

Once you have AOSP deployment in place, you can [disable AOSP](#).

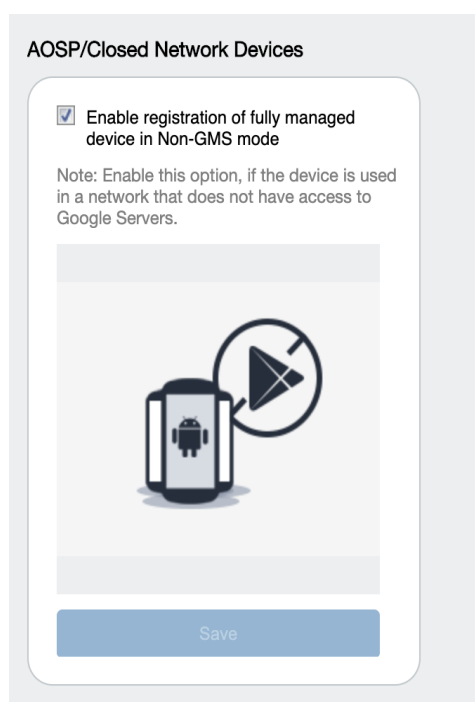
Enabling a closed network / AOSP deployment in Ivanti EPMM

With the Ivanti EPMM version 11.0.0.0 release, Administrators have the ability to enable a closed network / AOSP deployment in Ivanti EPMM whether Android Enterprise is already enabled or not. Once the closed network / AOSP is deployed, Administrators can optionally switch off Android Enterprise on the instance.

i Ivanti EPMM does not impose any "special" restrictions for Google calls, both on the client and on the server. It is completely the device user's own decision as to how to handle public apps pushed from Ivanti EPMM when the device is registered in Work Managed Device - Non-GMS mode.

Procedure

1. In Ivanti EPMM, go to **Services > Google**.
2. Scroll down and find the **AOSP/Closed Network Devices** tile.



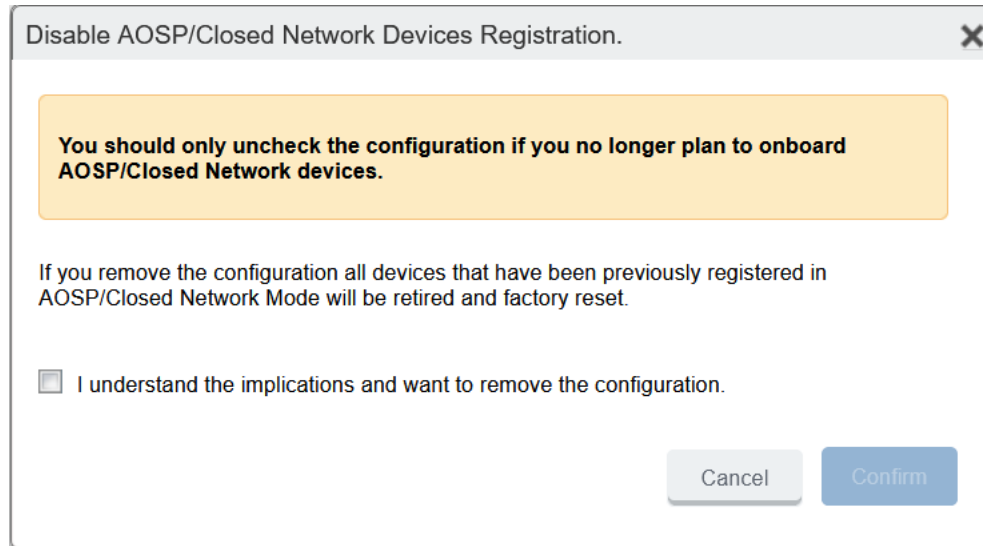
3. Select the **Enable registration of fully managed device in Non-GMS mode** check box and then click **Save**.

Disabling AOSP / closed network deployment

You can disable the AOSP / closed network deployment. Disabling AOSP in the Google Services page will cause the registered devices in Device Owner (DO) mode to retire. Devices in Device Admin (DA) mode will stay intact.

1. In the **AOSP/Closed Network Devices** tile, de-select the check box and then click **Save**.

The Disable AOSP/Closed Network Devices Registration dialog box opens.



2. Select the **I understand the implications and want to remove the configuration** check box and then click **Confirm**.

Creating a new Android Enterprise configuration

Administrators will need to create a new Android Enterprise configuration for the closed network or for an AOSP deployment, and then add the new configuration to a label.

1. Go to **Policies & Configs > Configs**.
2. Click **Add New > Android enterprise Setting**.
3. The New Android enterprise (all modes) Setting dialog box opens.
4. Enter a **Name** and **Description**.

5. Select the **Enable Closed Network/AOSP deployment** check box. All other options in the dialog box become hidden except Enable Runtime Permissions.
6. Click **Save**.
7. Apply a label to the configuration.

Important considerations:

If two Android Enterprise configurations (one with Android for Work and one with AOSP) are pushed to the same device, the Android for Work configuration takes priority.

As FCM services will not be available, Ivanti recommends administrators to modify the **Sync Policy > Sync Interval** field to 30 minutes or to the lowest value as needed by the administrator.



Once the **Enable Closed Network/AOSP deployment** check box in the Android Enterprise Setting (configuration) dialog box is enabled, after saving, the option will be greyed out. **There is no option for the administrator to disable it.** As a workaround, the administrator should either remove the label or delete the configuration.

Provisioning the Android device

For a closed network / AOSP deployment, only Android Enterprise devices in Work Managed Device mode can be provisioned. In order to provision the device, the administrator needs to download the Device Policy Controller (DPC.)

What the Administrator does:

- The Administrator adds the URL for the IIS server (where the Device Policy Controller (DPC) is hosted) into the Provisioner app and generates a QR code.
- The Android device is rebooted to factory setting.

For more information, see "[Provisioning Android Enterprise devices using a QR code or NFC bump](#)" on [page 75](#).

What the device user does:

Provisioning Non-GMS devices

1. Sideload and install the Ivanti Mobile@Work app onto the device.
2. Run the below command to provision the device into Device Owner (DO) mode. Be sure that the Ivanti Mobile@Work app is installed before running the command.

```
adb shell dpm set-device-owner com.mobileiron/.receiver.MIDeviceAdmin
```
3. Register the device by entering the server URL, username, and password.

Provisioning GMS devices

1. Device user scans the QR code. The DPC is downloaded onto the device.
2. Ivanti Mobile@Work client opens and requests the device user to enter the server URL.
3. The device user enters the server URL, username and password.
4. The device registration is completed.

Managing the closed network / AOSP devices

Listing details for Registration status, post-registration reception and provisions, and app management.

Registration status values

Upon registration to Ivanti EPMM, the device sends all device details to Ivanti EPMM. The **Device Details page > Registration Status** field lists the following values:

TABLE 4. REGISTRATION STATUS VALUES

Action	Registration Status value
Android Enterprise configuration sent to device	Work Managed Device
Closed network / AOSP configuration sent to device	Work Managed Device - Non GMS
Device does not receive the AOSP configuration	The device is retired (factory reset.)

Closed network / AOSP device capabilities

After successful registration, devices will be able to receive and provision the following:

TABLE 5. CLOSED NETWORK / AOSP DEVICE CAPABILITIES

Type	Description
Configurations	<ul style="list-style-type: none">• Android Enterprise• Android XML• Android APN• Exchange• MTD• Certificates• VPN• Wi-Fi
Policies	<ul style="list-style-type: none">• Android Quick Setup• Android Kiosk• Firmware policy• Security• Privacy• Lockdown• MTD local actions• MTD anti-phishing• Compliance policy• Sync policy
App Management	<ul style="list-style-type: none">• Support for in-house apps with configurations/restrictions• Apps@Work
Standard device management capabilities	All the supported device management commands of Android Enterprise work for closed network / AOSP deployment, except "Shared Kiosk- Signout."

App Management

- With a closed network / AOSP deployment, devices registered as a non-GMS device will have access to all in-house applications through Apps@Work.
- In non-closed networks / AOSP deployments, all apps need to be uploaded as in-house apps using their .apks since there is no access to Google's application bundles.
- When applying app restrictions, make sure to have the **Install this app for Android enterprise** and **Enable AOSP app restrictions** check boxes selected.

For more information about app management, see "Adding in-house apps for Android" in the *Ivanti EPMM Apps@Work Guide*.

Always-On VPN for AOSP for Android Enterprise devices

In AOSP mode, you can have Always-On VPN status for devices using Android 10 and later supported versions. Directing traffic from the device through the VPN is useful for highly regulated industries and for customers who would deploy AOSP functionality.

Before you begin

Be sure to have an Android Enterprise configuration in place with the **Always On** check box selected. See ["Enabling an Android Enterprise VPN client to be always on" on page 21](#).

Procedure

1. Go to **Services > Google** and select the **Enable AOSP/Closed Network Devices** check box (see ["Enabling a closed network / AOSP deployment in Ivanti EPMM" on page 30](#).)
2. Install a VPN app. When applying app restrictions, make sure to have the **Install this app for Android enterprise** and **Enable AOSP app restrictions** check boxes selected.
3. In **Services > Sentry**, add a new Standalone Sentry with a public certificate (see "Standalone Sentry certificate" in the *Ivanti Standalone Sentry Installation Guide*.)

4. In the Device Details page, the status of AOSP is displayed in the following fields:
 - **Registration Date** - Registration date of the device.
 - **Registration IMSI** - Registration of IMSI (international mobile subscriber identity) number.
 - **Registration Status** - Indicates the AOSP (non GMS) is registered as a Work Managed Device.
 - **Registration UUID** - Unique ID when registering from the client.
5. The result is on user's device > System Settings > VPN provided app > Always-On VPN is switched on.

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 39](#)
- ["General management of devices" on page 91](#)
- ["Searching for Devices" on page 96](#)
- ["Securing Devices" on page 126](#)

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 52](#)
- ["Visual privacy" on page 57](#)
- [" Invite users to register " on page 58](#)
- ["In-app registration for Android" on page 60](#)
- ["Registering Android devices" on page 42](#)
- ["Web-based registration for Android devices" on page 63](#)
- ["ActiveSync device registration" on page 64](#)
- ["Managing the Android Enterprise device life cycle" on page 68](#)
- ["Provisioning an Android Enterprise device" on page 75](#)
- ["Managing operators and countries" on page 81](#)
- ["Specifying eligible platforms for registration" on page 83](#)
- ["Setting the registration PIN code length for device user registration" on page 83](#)
- ["Customizing registration messages" on page 84](#)
- ["Configuring the default ownership for newly registered devices" on page 89](#)
- ["Disabling analytics data collection" on page 90](#)

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.



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 83](#)

The following registration methods are available:

- ["In-app registration" on the next page](#)
- ["Registering Android devices" on page 42](#)
- ["Registration methods" above](#)
- ["Registration methods" above](#)
- ["Users register additional devices" on page 48](#)
- ["Administrator registers ActiveSync devices" on page 48](#)
- ["Registration via user portal" on page 49](#)
- ["Registering Android devices via web portal \(MIRP\)" on page 49](#)
- ["Registering Samsung devices using Samsung Knox Mobile Enrollment" on page 50](#)

You can also register Android devices using the Provisioning app. See ["Provisioning an Android Enterprise device" on page 75](#)

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.



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.

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 device phone number, see ["Auto-populating the Ivanti EPMM server name based on email address " on page 61](#) for details.
 - To auto-populate based on the email address, you must register your VSP with Ivanti EPMM
- Schedule email reminders, see ["Customizing registration messages" on page 84](#)

Registering Android devices

In Ivanti EPMM 11.3.0.1 and newer versions, all new registrations for devices with Android 10 and later versions will be blocked by Ivanti EPMM by default IF they meet the following requirements:

- The Android 10+ device is in Device Admin mode (DA)
- There is no Android Enterprise configuration assigned to the correct label

Note the following:

- An Android 10+ device that is already registered on Ivanti EPMM in Device Admin mode will be allowed to migrate to Cloud.
- The Android 10+ device will be retired if there is no Android Enterprise configuration in place.
- MAM-only scenarios will still be supported, but the Quick setup policy with Device Admin mode will be disabled. However, in AppConnect, the Ivanti EPMM administrator will be able to register devices and SAM-wrapped apps using Android Quick Setup. For more information, see the *AppConnect Guide for EPMM*.

As with other types of devices, you can configure whether you want Android device users to enter a password, PIN, or both during registration. This can be done with managed and un-managed Android devices.

You can also set the device ownership to Company-owned or Employee-owned at registration.

If upgrading to Ivanti EPMM 10.6.0.0, and you have your Device Registration set to a specific authentication setting (Password, Registration PIN or Password and Registration PIN), the setting will be retained as a default. If you are registering devices for the first time using Ivanti EPMM 10.6.0.0 or supported newer version, the default setting is Password.

Before you begin

["Setting the registration PIN code length for device user registration" on page 83](#)

Procedure

1. Upload the APK file for Ivanti Mobile@Work for Android to a secure server. This server must be accessible to device users.

2. For unmanaged Android devices:
 - a. Go to **Settings > System Settings > Users & Devices > Device Registration**.
 - b. In the In-App Registration Requirement field, select one of the following:
 - **Password** - device user will be required to enter username and password.
 - **Registration PIN** - device user will be required to enter a registration PIN.
 - **Password and Registration PIN** - device user will be required to enter a username, password, and registration PIN.
 - **User and Registration PIN** - prompts device user to enter username and PIN. Device user is allowed five login attempts before Ivanti EPMM blocks the device. When this occurs, an error message "Authentication Failed: Invalid Credentials" displays.
 - c. Select **Save**.

3. For Zero Touch and Samsung Knox Android managed devices:
 - a. Go to **Settings > System Settings > Users & Devices > Device Registration**.
 - b. In the Zero Touch and Samsung Knox Mobile Enrollment field, select one of the following:
 - **Password** - device user will be required to enter username and password.
 - **Registration PIN** - device user will be required to enter a registration PIN.
 - **Password and Registration PIN** - device user will be required to enter a username, password, and registration PIN.
 - **User and Registration PIN** - prompts device user to enter username and PIN. Device user is allowed five login attempts before Ivanti EPMM blocks the device. When this occurs, an error message "Authentication Failed: Invalid Credentials" displays.
 - c. In the Ownership Settings section, in the "Default Ownership of Android devices using Google ZT or Samsung KME or non-GMS (AOSP) mode" field, select **Company owned** or **Employee owned**.
 - d. If you want the Terms of Service to be displayed, select the **Show Terms of Service** check box. Otherwise, the Terms of Service will not display (default.) (To create a Terms of Service, see ["Configuring an end user Terms of Service agreement" on page 638.](#))
 - e. Select **Save**.

For more information, see ["Provisioning Android Enterprise devices using Zero Touch" on page 79](#) and ["Registering Samsung devices using Samsung Knox Mobile Enrollment" on page 50](#)

4. For all other managed Android device types, in the Managed Devices/Device Owner (afw#, QR code, NFC) field, select one of the following:
 - **Password** - device user will be required to enter username and password.
 - **Registration PIN** - device user will be required to enter a registration PIN.
 - **Password and Registration PIN** - device user will be required to enter a username, password, and registration PIN.
 - **User and Registration PIN** - prompts device user to enter username and PIN. Device user is allowed five login attempts before Ivanti EPMM blocks the device. When this occurs, an error message "Authentication Failed: Invalid Credentials" displays.

For more information on registering using afw# token, QR code or NFC bump, see ["Provisioning an Android Enterprise device" on page 75](#).

5. Select **Save**.
6. In **Devices & Users > Add Single Device**, make sure:
 - the "Include Registration PIN only for Android Company-Owned Device Enrollment" field is selected.
 - the Device Ownership is set to **Company** or **Employee**.
7. Select **Register**.

The Registration Instructions dialog box opens.

8. Copy the Registration PIN for sending to the device user. If you are intending to send an email invitation to device users, you can skip this step.
9. Set up the email invitation template. See ["Customizing registration messages" on page 84](#)
10. Send the email invitation to device users. Ivanti EPMM will automatically add the Registration PIN within the invitation.

11. Once the device user has registered, monitor devices for status in **Devices & Users > Devices**. The Android Automated Enrollment field lists the values as appropriate for the type of Android setup:

- Google Zero Touch
- Knox Mobile Enrollment
- Non Zero Touch AE Enrollment



The Android Automated Enrollment field is valid for Ivanti EPMM 10.6.0.0 or supported newer versions. If an "Unknown" value displays, it indicates a previous version of Ivanti EPMM was used and 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.

Registration restrictions for Android devices

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

Before you begin

- Complete "[Registering Android devices](#)" on page 42.

Procedure

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

FIGURE 1. REGISTRATION RESTRICTIONS FOR ANDROID DEVICES

Restrictions for Android

Minimum OS Version

Minimum Security Patch Level Within days

Allowed/Blocked devices list ☒ None ?

- ☒ Create a list of Allowed devices
Only allow devices from these manufacturers to be registered
- ☐ Create a list of Blocked devices
Prevent devices from these manufacturers to be registered

MANUFACTURER NAME	MODEL	
Google	Pixel	✕
Samsung	<input type="text"/>	✕

Minimum SafetyNet Certification ☒ None ☐ Basic ☐ Certified

2. **Minimum OS version:** Select a minimum OS version from the drop-down menu from Android 6.0 or supported newer versions. The default is **None**.
3. **Minimum Security Patch Level:** Enter an integer specifying within how many days a device can be non-compliant for the minimum security patch level before rejecting the device. The default is **None**.

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

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

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

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

["Self-service User Portal" on page 631](#)

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

["ActiveSync device registration" on page 64](#)

Registration via user portal

The user portal can be used to streamline the registration process. See ["Self-service User Portal" on page 631](#) for more information.

Registering Android devices via web portal (MIRP)

Administrators who use web portals to initiate registrations can provide a URL in the web portal to help device users register Android devices with little or no typing. Users just download Ivanti Mobile@Work from Google Play and then tap the URL in the web portal from the device. Tapping the URL launches the Ivanti Mobile@Work app and populates the registration screen with the available information, such as the username. The information that is available depends on the web portal being used.

The URL is based on the Registration Protocol (MIRP). The link you provide on the web portal must have the following format:

`mirp://<Ivanti EPMM URL><parameters>`

The following parameters are available:

- user: The username for the device user.
- pin: The PIN generated for this user for PIN-based registration.

Examples:

- `mirp://myepmm.mycompany.com&user=android&pin=1234`

If you have configured Ivanti EPMM for PIN-only registration, device users will be automatically registered without having to enter any credentials.

- `mirp://myepmm.mycompany.com&user=android`

Device users will be prompted to enter credentials to complete registration. The credentials include either a PIN or password, depending on how you configured Ivanti EPMM.



The ampersand character is reserved. If you require an ampersand in a field value, it must be URL-escaped to a character code (i.e., %26).



Unsupported parameters will be ignored.

Registering Samsung devices using Samsung Knox Mobile Enrollment

Ivanti EPMM supports using the Samsung Knox Mobile Enrollment process to register qualified Samsung devices with Ivanti EPMM.

Using Samsung's Knox Mobile Enrollment process, once the process is set up, qualified devices are automatically enrolled and registered to Ivanti EPMM when the end user activates the device for the first time.

Requirements

- A CSV file that provides a list of device IMEI numbers or serial numbers, and optionally:
 - A username
 - A registration PIN and/or password

If you configured registration to use a PIN, include a PIN in the registration file. If you configured registration to use a password, include a password. If you configured registration to use both a password and a PIN, include only one of them in the CSV file. You configure the registration requirements on the Admin Portal at:

Settings > System Settings > User & Devices > Device Registration > Zero Touch and Samsung Knox Mobile Enrollment.

If username or PIN or password is not in the CSV file, the user must provide them.

- Optionally, you can set the device ownership as Company-owned or Employee-owned at registration at: **Settings > System Settings > Registration > Default ownership of Android devices using Google ZT or Samsung KME or non-GMS (AOSP) mode.**
- A Samsung Knox account and use of the Samsung Knox Mobile Enrollment portal
- Samsung Knox devices (see Samsung portal for a list of qualified devices)



Ivanti Mobile@Work for Android is automatically installed during the enrollment process.

Benefits

- Bulk enrollment of devices: No user interaction is required to download the Ivanti Mobile@Work app. The app is installed automatically as part of the enrollment process. No access to Google Play is required.
- No need for users to enter credentials (unless desired); credentials are populated in the background.
- Auto-Enrollment: Once a device is enrolled into an UEM/MDM via Samsung's mobile enrollment process, the MDM software is always be imposed even if the device is erased, inadvertently or maliciously, until you remove the device from the Samsung Knox Mobile Enrollment portal or retire

- Choice of enrollment options: you can choose to enroll the device using NFC bump, a URL, or automatic activation when a device is first powered on.
- Multiple Ivanti EPMM (or Ivanti Neurons for MDM) servers can participate in the program.

Instructions

Complete instructions for setting up and using the Samsung Knox Mobile Enrollment portal with Ivanti EPMM are available in the Ivanti, Inc knowledge base article, here:

[Samsung KNOX Mobile Enrollment for Android Enterprise KB article](#)

Related topics

You can also register Android devices using the Provisioning app. See "[Provisioning an Android Enterprise device](#)" on page 75

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 606](#).

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


Procedure


1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Registration**.
2. Scroll down to the **End User Terms of Service** section.
3. Click **Add+**.

4. Select the language for the terms of service.
5. For **Type**, select **System** for iOS, macOS and Android devices. Select **AAD enrollment** for Windows devices.
6. Enter the text for the terms of service.

You can adjust the editor to use rich or plain text by clicking the Source Edit icon.

7. Click **Save**.
8. Optionally, repeat steps 3 through 6 to add a terms of service agreement for each supported language, and for Windows devices versus iOS, macOS, and Android devices.

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

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

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 6. SEARCHABLE CRITERIA FOR TERMS OF SERVICE

Criterion	Description
Terms of Service Accepted	<p>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.</p> <p>A true value indicates the device user accepted the terms of service agreement at registration.</p>
Terms of Service Accepted Date	<p>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.</p>

TABLE 6. SEARCHABLE CRITERIA FOR TERMS OF SERVICE (CONT.)

Criterion	Description
AppConnect Terms of Service	<p>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.</p> <p>The value ACCEPTED indicates the device user accepted the terms of service agreement when logging into AppConnect.</p>
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 491](#).

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

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.

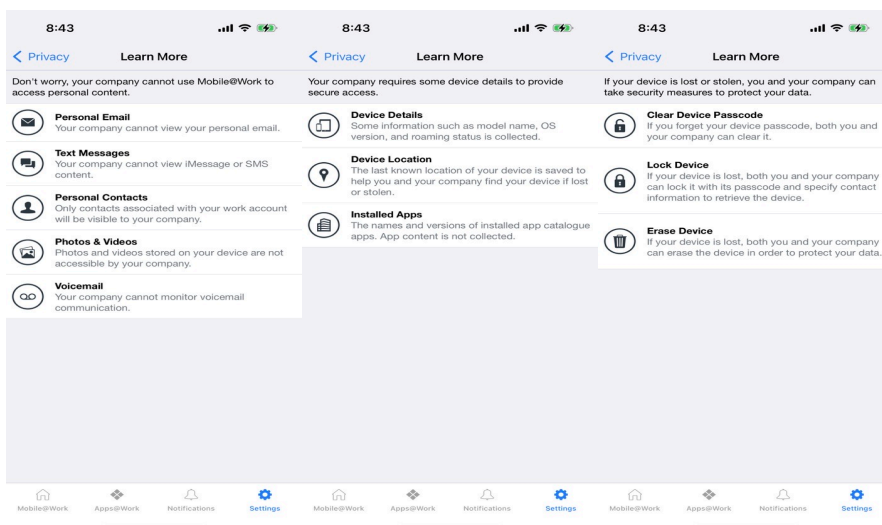
Users view the visual privacy information during registration, when they must accept the privacy policy.

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 device, 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**.



Invite users to register

Administrators can invite users to perform self-service registration through the user portal. See ["Self-service User Portal" on page 631](#) for information on this self-service user portal. The administrator sends invitations that provide the instructions necessary to complete the registration process.

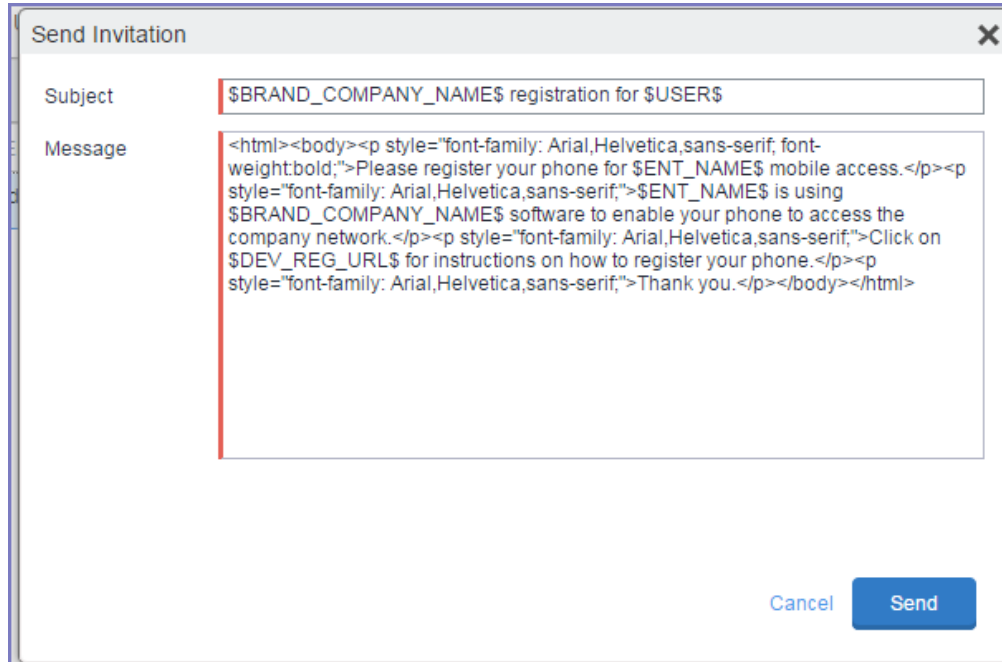


Language-specific templates are not currently available for invitations.

See ["Registration methods" on page 40](#) 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**.

A screenshot of a 'Send Invitation' dialog box. The dialog has a title bar with a close button (X). It contains two main sections: 'Subject' and 'Message'. The 'Subject' field is a text box containing the placeholder '\$BRAND_COMPANY_NAME\$ registration for \$USER\$'. The 'Message' field is a larger text box containing HTML-formatted text. At the bottom right, there are two buttons: 'Cancel' and 'Send'.

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 631](#) for information on what the user is expected to do to complete the registration process.

In-app registration for Android

You can ask Android device users to download Ivanti Mobile@Work from Google Play 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 40](#) 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

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

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 or the email address.



This feature is not supported for devices with Android v6.0 and above.

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)

Auto-populating the Ivanti EPMM server name based on the phone number

You can also auto-populate the Ivanti EPMM server name based on the device's phone number. The following setup is required:

- Ivanti EPMM access to the Ivanti, Inc Gateway. Configure the required ports. See the "Changing Firewall Rules" section in the *On-Premise Installation Guide for Ivanti EPMM and Enterprise Connector* for details.
- Enable server name look up in the Admin Portal on the **Settings > System Settings > Users & Devices > Device Registration** page.

To enable server name lookup:

1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Device Registration**.
2. Select **Enable Server Name Lookup**.
3. Select **Save**.

- Because this feature relies on a mobile number, it does not apply to iOS devices.
- The mobile number must also be present on the SIM in order for the **Enable Server Name Lookup** option to work.
- Registering Ivanti EPMM with Ivanti, Inc is not required.

Registering an Android device with Ivanti Mobile@Work

This registration method applies to registering Android devices using the following methods:

- Web-based registration - see "[Web-based registration for Android devices](#)" on the next page
- Using a QR code - see "[Provisioning Android Enterprise devices using a QR code or NFC bump](#)" on [page 75](#)
- Using email - see "[Invite users to register](#)" on [page 58](#)

Procedure

After the Ivanti Mobile@Work app is installed on your device, complete registration as a corporate device user.

1. Tap the Ivanti Mobile@Work app icon. The "Get Ready for Work with Ivanti Mobile@Work " page opens.
2. Enter your company's URL. You can also use the Scan QR code and Register with Email option.
3. Tap **Next**.
4. The Username page displays. Enter it and tap **Sign In**.
5. The Password field displays. Enter it and tap Sign In.
6. After your credentials are verified, the Home page opens.
7. Ivanti Mobile@Work checks for updates.
8. Once registration is complete, the Privacy statement displays for the device user to read.
9. Ivanti Mobile@Work guides the device user through the rest of the provisioning. The type of provisioning depends upon the policies and configurations set by the administrator.

Requiring device identifiers for enrollment

You have the option to make the collection of a device's hardware identifiers such as the IMEI number and the phone number optional before the device is enrolled. If you disable **Require device identifiers for enrollment**, the enrollment will still proceed, but the client will not collect the device identifier data. The device would be a "PDA" device such as a tablet.

Procedure

1. In Admin Portal, go to **Settings > System Settings > Users & Devices > Registration**.
2. Select **Require device identifiers for enrollment**.
This is supported on devices using Android 6.0 or supported newer versions.
3. Select **Save**.



Phone number lookup is supported on devices in Device Owner mode and using Android prior to Android 6.0.

Web-based registration for Android devices

You can instruct users to register with Ivanti EPMM through the web. Users enter the URL of the server with forward slash "go" appended to the end of the URL, which takes them through a guided web-based registration process. Device users must still install Ivanti Mobile@Work to complete the registration process.

Procedure

1. Make sure the user has a user record (local or LDAP) available in Ivanti EPMM. See "Managing Users" in *Getting Started with Ivanti EPMM*.
2. Instruct the user on downloading the app and registering. The 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)
3. Instruct the user to register with the Ivanti EPMM server at the following URL:

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

The Register your device for work page displays. It contains instructions for the device user to download Ivanti Mobile@Work for Android from Google Play.

4. Instruct the user to tap the **Google play** button so as to download Ivanti Mobile@Work for Android.
5. Instruct the user to follow the on-screen instructions in Ivanti Mobile@Work , entering the user credentials and server name in the space provided.

Registering a device with Ivanti Mobile@Work using your company's URL

After the Ivanti Mobile@Work app is installed on your device, complete registration as a corporate user.

Procedure

After the Ivanti Mobile@Work app is installed on your device, complete registration as a corporate user.

1. Tap the Ivanti Mobile@Work app icon. The "Get Ready for Work with Ivanti Mobile@Work " page opens.
2. Enter your company's URL. You can also use the Scan QR code and Register with Email option.
3. Tap **Next**.
4. The Username page displays. Enter it and tap **Sign In**.
5. The Password field displays. Enter it and tap Sign In.
6. After your credentials are verified, the Home page opens.
7. Ivanti Mobile@Work checks for updates.
8. Once registration is complete, the Privacy statement displays for the device user to read.
9. Ivanti Mobile@Work guides the device user through the rest of the provisioning. The type of provisioning depends upon the policies and configurations set by the administrator.

ActiveSync device registration

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

See "[Registration methods](#)" on [page 40](#) 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.

Android Bulk Enrollment

Administrators with Add Device Role privileges can see the Android Bulk Enrollment screen under Devices & Users and can create bulk enrollment profiles by uploading a CSV file. For each profile, a token will be generated with a default expiration time of 7 days. This token can be further extended for 7 days minimum to 99 days maximum. Optionally, the token can be regenerated (a completely new token is created for the profile with a default of 7 days of expiration.)

- Serial number for each device is required (mandatory.)
- Duplicate CSV profiles are not allowed.
- Once devices are imported, they cannot be edited.
- Administrators cannot add more devices to an existing profile.

USE CASE: To save time, Administrators can do registration of Android 7+ devices in large batches (1000+) by uploading CSV file for many entries. Ivanti recommends you do not upload more than 4,000 devices in a single batch.

Android Modes supported:

- Work Managed Device mode
- Managed Device with Work Profile mode
- Work Profile on Company Owned Device mode
- AOSP mode

Process:

1. In "[Creating a new Android Bulk Enrollment](#) " below, you create a new Android Bulk Enrollment by using a CSV file. A token is generated and associated to the bulk enrollment profile.
2. Administrators can extend the lifetime of the token or use the "[Refreshing a Android Bulk Enrollment token](#)" on the next page option. This activity is recorded in the audit logs.
3. In the Android Bulk Enrollment Profiles page, you can view all bulk-enrolled profiles and source (admins will need to maintain the serial number data for devices.) You can also view the token expiration date and view devices (allows viewing of the CSV data.
4. In the Device Details page, you can:
 - see the profile's name under "Bulk Enrollment Profile Name"
 - Search using the same term
 - Download the CSV by selecting the **Export to CSV** button to the right of the **Add** button.

Creating a new Android Bulk Enrollment

Before you begin

- Read the process in "[Android Bulk Enrollment](#)" on the previous page
- Have a CSV file ready.



IMPORTANT: The serial numbers of the Android devices in the CSV is mandatory. This is alphanumeric and can be between 4-16 characters long.

All devices imported will share the same bulk enrollment token and expiration date. Multiple users can be added in a single CSV file.

Ivanti recommends you do not upload more than 4,000 devices in a single batch.

Procedure

1. In the Admin Portal, go to **Devices & Users > Android Bulk Enrollment** tab.
2. Select the **Add+** button. The Add Bulk Enrollment Profile dialog box opens.
3. Enter a **Bulk Profile Name**.
4. In the **Multiple Devices File** field, admins can use the Sample CSV file or they can **Browse** to find the CSV file and then select the **Import File** button.

5. Select the **Apply** button. The list of devices and information related to the devices display.

After successful import of devices, the device users will not get notified of the same via email or text messages. They will only get the QR code generated by the administrator with the token.

6. Select **Close**. The new Bulk Enrollment displays in the Android Bulk Enrollment page.

Related topics

- ["Refreshing a Android Bulk Enrollment token" below](#)

Refreshing a Android Bulk Enrollment token

Once you have created Android Bulk Enrollment profiles, you can update the token associated to the profile.



Refreshing a token will cause the token to be updated for all devices with the profile.

Procedure

1. Go to **Devices & Users > Android Bulk Enrollment**.
2. Select a profile.
3. Select **Actions > Refresh Bulk Enrollment Token**.
4. The Refresh Bulk Enrollment Token dialog box displays. Select one of the following:
 - a. **Extend validity by [7] days** (minimum 7 days, maximum 99 days)
 - b. **Regenerate Token** - Optionally, the token can be regenerated. This means a completely new token is created for the profile with a default of 7 days of expiration.
5. Select the **Update Token** button.
6. When the Bulk Enrollment Token action succeeds, select **OK**.

Deleting a profile and associated device

Once the administrator has uploaded the device CSV via Android Bulk Enrollment and a profile and its associated devices have been created, the administrator can delete the profile and its devices. Active and Retire Pending devices cannot be removed, but inactive devices can be deleted.

Because this action is not reversible, Ivanti recommends you download the device information prior to deleting the profile. Note that delete action is only supported from global space.

Before you begin

- ["Creating a new Android Bulk Enrollment " on page 66](#)
- [Download the device information prior to deleting the profile](#)

Procedure

1. Go to Devices & Users > Android Bulk Enrollment.
2. Select the Bulk Enrollment Profile Name and then select **Actions > Delete Profile and Devices**. The Delete Profile dialog box opens.
3. Select the check box **Are you sure you want to proceed with the selected action?** Doing so will delete the bulk enrollment profile and its associated inactive devices.
4. Select **Submit**.

In the Device Details page, the Bulk Enrollment Profile Name will list the device as deleted.

Managing the Android Enterprise device life cycle

Managing the life cycle of an Android Enterprise device includes the following steps:

- ["Provisioning a Work managed device for Android Enterprise" on the next page](#)
- ["Registering a Work managed device for Android Enterprise" on the next page](#)
- ["Migrating devices to Android Enterprise" on page 70](#)
- ["Preventing automatic migration" on page 70](#)
- ["Migration effects on a device" on page 70](#)
- ["Quarantine on Android Enterprise devices" on page 71](#)
- ["Retiring an Android Enterprise device" on page 72](#)
- ["Wiping an Android Enterprise device" on page 72](#)
- ["Locking an Android Enterprise device" on page 73](#)
- ["Unlocking an Android Enterprise device" on page 73](#)
- ["Setting the unlock PIN for a specific device" on page 74](#)

Related topics

["Removing Android Enterprise" on page 26](#)

Provisioning a Work managed device for Android Enterprise

Provisioning is necessary only for work managed devices. You can provision factory reset Android devices using one of these methods:

- The Provisioner app, which uses the NFC bump and QR code method.
- An afw# token
- Android Zero Touch
- Knox Mobile Enrollment (KME)

Provisioner (QR code) and Zero Touch can be used to provision Work Profile on Company Owned Devices. Once provisioned, a work-managed devices or Work Profile on Company Owned Devices can register with Ivanti EPMM.

Related topics

["Provisioning an Android Enterprise device" on page 75](#)

Registering a Work managed device for Android Enterprise

To register an Android Enterprise-capable device, the user follows the same registration process as for any Android device. The registration process detects if Ivanti EPMM and the device are Android Enterprise-capable, and performs the correct registration steps automatically.

To register an Android Enterprise-capable device to have an Android Enterprise work profile (as opposed to being registered as a regular Android device), the following must be in place:

- Ivanti EPMM has been set up for Android Enterprise as described in ["Enabling Android Enterprise" on page 15](#). To confirm the setup, go to **Services > Google**. In the **Android enterprise** section you should see **Account Settings:** information with **Status: Connected**.
- The **Android enterprise setting** is applied to an appropriate label.

The user follows the registration process in the Ivanti Mobile@Work app.

Once registered, to verify that the device is using Android Enterprise:

- On a device with a work profile, check that the Ivanti Mobile@Work app appears with the Android Enterprise badge
- On a work managed device that was provisioned, look for the Google Play store icon, which will show the Work version of the store.

Related topics

["In-app registration for Android" on page 60](#)

Migrating devices to Android Enterprise

"Migrating" refers to the actions devices take when they are already registered and running Ivanti Mobile@Work and an update to Ivanti EPMM or Ivanti Mobile@Work takes effect. This section describes migration and what to expect.

Migration does not apply to work managed devices, because such devices are enabled for Android Enterprise after factory reset. Migration applies only to device that are not in work profile mode, yet.

A registered device may migrate to an Android Enterprise profile (assuming Ivanti EPMM has Android Enterprise enabled, and the device has the Android Enterprise setting applied to it) when the following occurs:

- The device becomes Android Enterprise-capable after it receives a firmware update from the carrier
- Ivanti EPMM is newly enabled for Android Enterprise.

In these migration scenarios, the Android devices begin their migration to use work profile automatically.

Preventing automatic migration

When all the conditions required to enable Android Enterprise are met, a device will automatically migrate to use the work profile. If you want to prevent a device from automatically migrating, ensure the device does not have the **Android enterprise setting** applied.



If you applied the **Android** label to the **Android enterprise setting**, then all Android devices potentially have the setting, and all Android Enterprise-capable devices be will be automatically migrated. If this is not desired, do not use the **Android** label for this configuration.

Migration effects on a device

This section addresses the changes that occur on a registered device when it is migrated to work profile:

Procedure

1. User is prompted to uninstall all secure apps, in-house apps, and public apps.



The migration will not continue until the user completes this step or there are no secure or in-house apps installed.

2. All managed configurations are removed, except for Wi-Fi configurations.

As when a device is retired, no personal certificates are removed.

3. The Android Enterprise work profile is created.
4. The Ivanti Mobile@Work app icon appears with the Android Enterprise badge.
5. Configuration steps appear as needed.

Quarantine on Android Enterprise devices

When an Android Enterprise device is quarantined (with all configurations removed) due to a compliance violation, the following changes are made on the device:

TABLE 7. ANDROID ENTERPRISE QUARANTINE BEHAVIOR

Android Enterprise mode	"Quarantine app when device is quarantined" field is selected (checked)	"Quarantine app when device is quarantined" field is de-selected (not checked)
<ul style="list-style-type: none">• Work Profile• Work Managed Device• Managed Device with Work Profile (COPE) (Android versions 8-10 only)• Work Profile on Company Owned Devices (Android 11 or supported newer versions)	<ul style="list-style-type: none">• All the apps in the work profile are hidden, except:<ul style="list-style-type: none">◦ Google Play◦ Ivanti Mobile@Work◦ Downloads• Contacts are hidden.• The Wi-Fi configurations are kept or removed, based on the quarantine settings.	Users will still see the app on the device.



The quarantine behavior of individual Android Enterprise apps is controlled by setting the configuration of each Android Enterprise app in the App Catalog.

For more information, see "Adding in-house apps for Android" section or the "Adding an Android Enterprise public app using the app wizard in the Ivanti EPMM Admin Portal" section in the *Ivanti EPMM Apps@Work Guide*.

Retiring an Android Enterprise device

When an Android Enterprise device gets the **Retire** command, the following behavior occurs:

TABLE 8. ANDROID ENTERPRISE RETIRE BEHAVIOR

Android Enterprise status	Retire behavior
Work Profile	<ul style="list-style-type: none">The work profile is removed.All apps, data, and contacts in the work profile are removed.A user can re-register a retired device by re-enabling Ivanti Mobile@Work through Google Play.
<ul style="list-style-type: none">Work Managed Device	The device is reset to factory settings. The device can be re-provisioned by an administrator.
<ul style="list-style-type: none">Managed Device with Work Profile (COPE)Work Profile on Company Owned Devices	<ul style="list-style-type: none">The work profile is removed.

Related topics

["Removing an Android Enterprise configuration causes device to retire" on page 26](#)

Wiping an Android Enterprise device

When an Android Enterprise device gets the **Wipe** command, the following behavior occurs:

TABLE 9. ANDROID ENTERPRISE WIPE BEHAVIOR

Android Enterprise status	Wipe behavior
Work Profile	<ul style="list-style-type: none">• The work profile is removed. (No changes are made to any apps or data on the personal profile.)• All apps, data, and contacts in the work profile are removed.• A user can re-register a wiped device by re-enabling Ivanti Mobile@Work in Google Play.
<ul style="list-style-type: none">• Work Managed Device• Managed Device with Work Profile (COPE)• Work Profile on Company Owned Devices	<p>The device is reset to factory settings.</p> <p>The device can be re-provisioned by an administrator.</p>

Locking an Android Enterprise device

The **Lock** command locks the screen of an Android Enterprise device. To lock the device:

1. Go to **Devices & Users > Devices**.
2. Select the device.
3. Select **Actions > Lock**.

For work managed devices, the Lock command locks the entire device. The user must enter the device password to unlock the device.

For work profile devices, the Lock command locks the work profile if a Work Challenge was set (Android 7.0 through etc).

Unlocking an Android Enterprise device

The **Unlock** command unlocks the screen of an Android Enterprise device. Before unlocking Samsung devices running in Device Administrator mode, the password must be reset in the DevicePolicyManager resetpassword() API. For unlocking devices with Knox licenses, administrators will need to make sure the Knox license is activated (Samsung General Policy in Policies & Configs) and then reset the password. This is applicable to Android 7 or supported newer versions.

To unlock the device:

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

The following table shows unlock support on Android Enterprise devices:

TABLE 10. SUPPORT FOR UNLOCKING THE DEVICE ON ANDROID ENTERPRISE DEVICES

Android Enterprise device	Prior to Android 7.0	Android 7.0 or supported newer versions
<ul style="list-style-type: none">• Work Managed Devices• Managed Device with Work Profile (COPE)	Supported	Supported
<ul style="list-style-type: none">• Work Profile Devices• Work Profile on Company Owned Devices	Supported	Not supported

Setting the unlock PIN for a specific device

For Android Enterprises, the device user can, in the Self Service User portal, reset the PIN using the Unlock option. For this reason, and because employees can leave an organization without sharing the device's PIN, administrators can use the default setting of 0000 or create a custom 6-8 digit unlock PIN for specific devices.



Ivanti recommends using six numbers only, as the alphanumeric method can cause problems with different keyboards in different languages.

The Custom Unlock PIN feature is supported in direct boot mode.

If this setting is used, "Unlock Device with Custom Pin <Pin Value>" will display in the audit logs. You can also view the custom PIN in **Devices & Users > Devices**.

- Select the "View Logs for Device" link.
- If you need to, search on "Extended filters."

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the Android device.
3. Select **Actions > Unlock Device**.
4. In **Enter minimum six digit unlock PIN**, enter a 6-8 digit passcode. Alphanumeric characters are supported but not recommended.
5. Select **Unlock Device**.

Provisioning an Android Enterprise device

Administrators register Android Enterprise devices, by registering a “work profile” and by provisioning “work managed” devices on a master device.

- Register a “work profile” device by following the regular registration process to install Ivanti Mobile@Work .
- Provision Work Managed Devices and Work Profile on Company Owned Devices using a master device that is running the Provisioner app. For details, see the following sections.
 - ["Provisioning Android Enterprise devices using a QR code or NFC bump" below](#)
 - ["Provisioning Android Enterprise devices using an afw# token" on page 78](#)
 - ["Provisioning Android Enterprise devices using Zero Touch" on page 79](#)

Before registering using a QR code for devices in a closed network or using AOSP deployment, see ["Setting up Ivanti EPMM with a closed network / AOSP deployment" on page 28](#).

Related topics

["In-app registration for Android" on page 60](#)

Provisioning Android Enterprise devices using a QR code or NFC bump

To provision Android Enterprise devices using QR code or near field communication (NFC) bump, you will need to download and install the Provisioner app from Google Play on the master device.

Using this method, you can provision Android devices in a closed network or with a AOSP (Android Open Source Project) deployment. For more information, see ["Setting up Ivanti EPMM with a closed network / AOSP deployment" on page 28](#).

Requirements to provision an Android Enterprise device

To provision an Android Enterprise device to be a work managed device, you need to:

- Ensure the required **Android Enterprise Configuration** is defined and applied to a recommended label.
- Enable Android Enterprise on the server.
- In **Devices & Users > Add Single Device**, make sure the "Include Registration PIN only for Android Company-Owned Device Enrollment" field is selected.
- In **Settings > Device Registration**, have the "Managed Devices / Device Owner (afw#, QR code, NFC)" field set to Password, Registration PIN or Password and Registration PIN.
- In **Settings > Device Registration**, verify that the option **Display QR Code and Registration URL** is enabled. To disable sending users a QR code and registration URL, see .
- Have an NFC-capable Android device (only if NFC is used) to serve as the master, with the Provisioner app installed.
- Have Android Enterprise-capable devices to provision.

Enabling the Android beam for use with NFC bump

Procedure

1. Go to **Settings** on the device.
2. Go to **Networks > Wireless Networks**.
3. In the **Connectivity section** select **Share & connect**.
4. Slide the **NFC** switch to **On**.
5. Slide the **Android Beam** switch to **On**.



The steps to enable the Android beam and NFC may vary on different devices.

Provisioning Android Enterprise devices to become work managed devices

This section applies to Work Managed Devices and Work Profile on Company Owned Devices.

Procedure

1. Using the Android master device, download the **Provisioner** app from Google Play and install the app.
 2. Launch Provisioner on the master device.
 3. Select **NFC** or **QR code** for the Provisioning method.
-

4. Tap **App for Provisioning**, and choose the client app to be installed on the provisioned device:

Select this client app:	To register with this EMM server:
Ivanti Mobile@Work	Ivanti EPMM
MDM	Deutsche Telekom Ivanti EPMM
Vodafone Ivanti Mobile@Work	Vodafone Ivanti EPMM

5. Fill out the remaining fields in the Provisioner app. Some fields may auto-populate if a supported Wi-Fi type is present. The Wi-Fi fields are not shown if QR code is selected. Use these guidelines:

Field	Value
Select app for provisioning	Ivanti Mobile@Work
Time Zone	Enter the time zone to be configured on the device
Locale	Enter the locale to be configured on the device
Enable All System Apps	Select the check box to enable all system apps
Wi-Fi Network SSID	Enter the Wi-Fi SSID the target device is to use
Wi-Fi Security Type	Enter the Wi-Fi security type
Wi-Fi Password	Enter the password for the Wi-Fi
Bulk Enrollment	Bulk enrollment is optional along with the hostname and username. Optionally select the Quick Start check box to use Quick Start feature. If a username is entered or Quick Start is checked, then a hostname is required.

6. Tap **Continue**.
7. If you selected **NFC**, tap **Continue**. The screen **Bump the devices!** appears on the master device. Continue with the NFC Bump section below.
8. If you selected QR code, the screen Scan this QR code! appears on the master device. Continue with the QR Code section below.

9. Configure NFC Bump.
 - a. Confirm that the target device is displaying the Android Welcome screen.
 - b. Press the master device back-to-back with the target device to initiate an NFC transfer. If the NFC transfer succeeds, the target device may make a sound, and then proceed to downloading the client app. If a Wi-Fi connection cannot be established, or if the device is unable to download the client app, the device will automatically do a factory reset.
 - c. If you hear the sound or see a screen other than the Welcome screen, you can decouple the devices. This typically takes a few seconds. If the device is not encrypted, it will start the encryption process before continuing.
 - d. You can continue to provision additional devices by “bumping” the devices to the master device. The target device must be showing the Welcome screen, and the master device must be showing the “Bump the devices!” screen.
10. Configure QR Code provisioning.
 - a. Confirm that the target device is displaying the Android Welcome screen.
 - b. Tap the Android Welcome screen on the target device 6 times on the same place on the screen.
 - c. You will be prompted to configure a WiFi network so the setup wizard can download a QR code reader to the target device.
 - d. After the QR code reader is downloaded, the camera is launched.
 - e. Hold the target device a few inches above the master device until the QR code is scanned successfully. The setup wizard will then proceed to download the client app. If it is unable to download the client app, it will automatically do a factory reset.
 - f. You can continue to provision additional devices by scanning the QR code on the master device. The target device must have a camera ready to scan, and the master device must show the “Scan this QR code!” screen.
 - g. The QR code can also be exported by tapping the Share icon. The options offered for exporting will vary by device.

Provisioning Android Enterprise devices using an afw# token

You can provision an Android Enterprise device in Device Owner mode using an afw# token instead of using the NFC bump or QR code methods. This method enables you to sign on a device with a token in the form afw#mobileiron.core which facilitates an automatic installation of the Ivanti Mobile@Work client and provisioning in Device Owner mode.



Device Owner mode is supported on devices provisioned with Managed Google Play Accounts, using Android 6 or supported newer versions. For details see the [Android EMM Developers guide](#).

Before you begin

- You must be enrolled with an Android Enterprise account.
- The device must be Android Enterprise-capable.
- The device must use Android 6 or supported newer versions.
- In **Devices & Users > Add Single Device**, make sure the "Include Registration PIN only for Android Company-Owned Device Enrollment" field is selected.
- In **Settings > Device Registration**, have the "Managed Devices / Device Owner (afw#, QR code, NFC)" field set to Password, Registration PIN or Password and Registration PIN.
- You must have an Android Enterprise token for Ivanti EPMM or a client branded token such as:
 - Ivanti EPMM: **afw#mobileiron.core**
 - Deutsche Telekom: **afw#telekom.mi**
 - Vodafone: **afw#vodafone.mi**
- You must have a new or factory reset device.

Procedure

1. Power on the device and enter your WI-FI password.
Your device may prompt you for a different password.
2. In the **Verify your account** screen enter your Android Enterprise token. Select **Next**.
3. On the **Google Services** screen select **Install**.
4. Accept the Terms and Conditions.
5. On the Setup work device screen select **Next**.
The Ivanti Mobile@Work client downloads and installs on the device. The device now enters Device Owner mode.

Provisioning Android Enterprise devices using Zero Touch

For information on Android Zero Touch provisioning, see the [Android Zero Touch Provisioning Guide](#).

- In **Devices & Users > Add Single Device**, make sure the "Include Registration PIN only for Android Company-Owned Device Enrollment" field is selected.
- In **Settings > Device Registration**, have the "Zero Touch and Samsung Knox Mobile Enrollment" field set to Password, Registration PIN or Password and Registration PIN.

Zero Touch enrollment with custom attributes

Administrators can specify certain custom device attributes at the time of initial provisioning. This works with the Provisioner app, QR code, Knox Mobile Enrollment (KME) and Zero Touch (ZT) for devices in Work managed device mode (DO) or corporate-owned personal-enabled (COPE) mode. It also works with all modes of registration, including PIN based and password based registration.

At initial registration and during any check-in, these custom attributes are passed on to Ivanti EPMM to categorize the device and place it in the correct group and assign the correct labels. The client sends property (customAttributes) consisting of the device custom attribute keys (variable name) and values that client wants Ivanti EPMM to set for that device. The client also sends to Ivanti EPMM updated values with the existing keys for the (customAttributes) key. If the client does not send a (customAttributes) key, the existing custom attributes values will not change.

Zero Touch enrollment with custom attributes is supported for custom attributes of type: String, Boolean, and Integer. The Provisioner App only supports String type.



It is the responsibility of the administrator to make sure that the custom attributes are setup correctly in Ivanti EPMM beforehand and match what is being sent by the Provisioner app or Zero Touch portal.

Use Case examples

Example - BOOLEAN

- Attribute Name – COPE
- Attribute Description – Enabled COPE Mode
- Value Type – Boolean
- Variable Name – True

Example - INTEGER

- Attribute Name – OrgID
- Attribute Description – Organization ID
- Value Type – Integer
- Variable Name – 3456

Example - STRING

- Attribute Name – AEmode
- Attribute Description – Android Enterprise Mode

- Value Type – String
- Variable Name – DO

For information on how to set custom attributes, see ["Adding custom attributes to users and/or devices" on page 167](#).

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.



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 setting Android registration authentication, see ["Registering Android devices" on page 42](#).

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.



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

Edit Registration Template: iOS (English)

Language: English
Platform: iOS

[Variables Supported](#)

Registration SMS

Phones	PDAs
Go to \$REG_LINK\$. For full instructions, please check your email.	N/A

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

Push Notification Reminder to Complete Registration

Phones/Devices	PDAs
Your MDM profile is ready to be installed from Settings. For more details please check your email.	N/A

Registration Email

	Phones	PDAs
Subject	\$ENT_NAME\$ device registration instructions for \$USER\$ (\$ENT_NAME\$ device registration instructions for \$USER\$ (
Body	<html><body><p style="font-family: Arial,Helvetica,sans-serif;">\$ENT_NAME\$ is using \$BRAND_COMPANY_NAME\$'s Platform to enable access to corporate resources.</p><p style="font-family: Arial,Helvetica,sans-serif;">To allow you to easily register your device with this system. If you selected	<html><body><p style="font-family: Arial,Helvetica,sans-serif;">\$ENT_NAME\$ is using \$BRAND_COMPANY_NAME\$'s Platform to enable access to corporate resources.</p><p></p><p style="font-family: Arial,Helvetica,sans-serif;">From your device.</p></body></html>
Reminder Subject	Reminder: \$ENT_NAME\$ device registration instructions fo	Reminder: \$ENT_NAME\$ device registration instructions fo
Reminder Body	<html><body><p style="font-family: Arial,Helvetica,sans-serif;">\$ENT_NAME\$ is using \$BRAND_COMPANY_NAME\$'s Platform to enable access to corporate resources.</p><p style="font-family: Arial,Helvetica,sans-serif;">To allow you to easily register your device with this system. If you selected	<html><body><p style="font-family: Arial,Helvetica,sans-serif;">\$ENT_NAME\$ is using \$BRAND_COMPANY_NAME\$'s Platform to enable access to corporate resources.</p><p></p><p style="font-family: Arial,Helvetica,sans-serif;">From your device.</p></body></html>

Values for \$INAPP_REG_STEPS\$ ⓘ

[Save](#) | [Cancel](#)

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"](#) below for additional details.
5. Select **Save**.

Next steps

["Customizing registration messages" on page 84](#)

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 11. 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	
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 12. 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/a/ for Android).
\$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.

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

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 677](#)
- 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-Serve 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.

- c. For the **Default ownership of Android devices using Google ZT or Samsung KME or non-GMS (AOSP) mode** setting, select the relevant radio button **Company owned** or **Employee owned**.
 - Select **Show Terms of Service** to have them displayed on the client. Otherwise, they will not display (default.) (To create a Terms of Service, see "[Configuring an end user Terms of Service agreement](#)" on page 638.) This feature is only applicable to company-owned devices.
3. Select **Save**.

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.



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" below](#)
- ["Setting wallpapers for devices" below](#)
- ["App Updates for Android Enterprise" on the next page](#)

Sending a company-branded email

You can send a company-branded HTML email to single or bulk users. You can also send branded email messages using **Settings > Templates** - see ["Customizing Event Center messages" on page 471](#).

Before you begin

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

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the device(s) you want to send your email to.
3. Click **Actions > Send Message**. The Send Message dialog box opens.
4. Select the **Email** check box.
5. Select **Send HTML email instead of plain text email**. More fields display.
6. Copy and paste the HTML email into the **Message (HTML Email)** field.
7. (Optional) You can select the **Data Channel** option to use for any of the message modes.
8. Click **Send Message**.

Setting wallpapers for devices

The device wallpaper configuration defines a default wallpaper image for the Home screen and Lock screen of Android (10.0 devices in Work Managed Device mode).



The uploaded image must be in .jpg or .png format.

The wallpaper will be applied automatically to the device. Refer to the device manufacturer's specifications for screen resolution. Ivanti recommends to create separate configurations with appropriate screen size and resolution of the device type.

Procedure

To define a default wallpaper image for Android devices:

1. Go to **Policies & Configurations > Policies**.
2. Click **Add New > Android > Wallpaper**.
3. Use the following guidelines to complete the form:

Setting	What To Do
Name	Required. Enter a descriptive name for this policy.
Description	Enter an explanation of the purpose of this policy.
Upload Android Wallpaper	
Use the same image for Home screen and Lock Screen	Select to upload a single image for both the screens.
Home Screen	Drag and drop the image file or click Choose File to select it.
Lock Screen	Drag and drop the image file or click Choose File to select it.

4. Click **Done**.

App Updates for Android Enterprise

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

Auto-Update Maintenance Window

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

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

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

Update Priority

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

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

Minimum Code Version

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



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

Considerations:

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

Example:

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

Considerations for both Update Priority and Minimum Code Version



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



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

Inventory MAC address

To preserve device user privacy, on Android 7+ devices, Ivanti EPMM accepts a randomized MAC address for inventory purposes. **Inventory MAC** is the hardware-based MAC that is reported after a device is registered and is only available for company-owned modes, namely Device Owner mode and Work Profile on Company Owned Devices. Inventory MAC supports substitution variables.

Procedure

1. In Ivanti EPMM, go to **Admins** and select an admin.
2. Select **Actions > Edit Roles**.
3. Under the Privacy Control section, select the **View device IP and MAC address** check box and **Save** your settings.
4. After pushing to devices, you can view the **Inventory MAC** in the Device Details page, or conduct a search. For more information, see "[Advanced searching](#) " on page 97

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 the next page](#)
- ["Using the query builder" on page 118](#)
- ["Using a manually edited search expression" on page 119](#)
- ["Using both the query builder and manual editing" on page 119](#)
- ["Negative operators with advanced search" on page 121](#)
- ["Clearing an advanced search" on page 123](#)
- ["Searching for retired devices" on page 124](#)
- ["Searching for blocked devices" on page 124](#)
- ["Saving a search criterion to a label" on page 124](#)

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

Basic search for devices

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

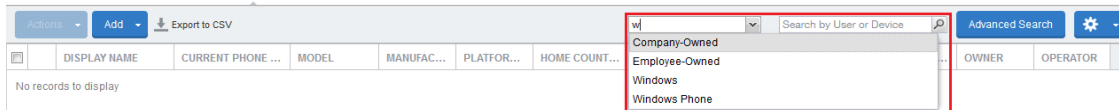
- Label
- User Principal/ID
- User Email Address
- User First/Last Name

To search by label, you can:

- Select the appropriate label name from the **Labels** list.
- Enter the initial letters of the label name in the **Labels** list.

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

FIGURE 1. SEARCH BY LABEL



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

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



The prefixes mail: and name: are optional. All others are required. For example, to find the devices registered with the email address jdoe@ivanti.com, you can enter the following:
mail:jdoe@ivanti.com or 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 118](#) and ["Using both the query builder and manual editing" on page 119](#).) 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](#)" below.
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 491.



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 13. 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.

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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: <ul style="list-style-type: none"> • 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
	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.

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Battery Charge Cycles (OEM)	<p>This field will only populate if the device is a Zebra device; otherwise blank.</p> <p>Docs: Number of charge cycles completed in total for supported device manufacturers such as Zebra devices.</p> <p>Field Name: Battery Charge Cycles property: battery_usage_num possible values: Integer</p>
	Battery Health Percentage (OEM)	<p>This field will only populate if the device is a Zebra device; otherwise blank.</p> <p>Docs: Battery health in percentage for supported device manufacturers such as Zebra devices.</p> <p>Field Name: Battery Health Percentage property: health_percentag possible values: Integer</p>
	Battery Manufacture Date (OEM)	<p>This field will only populate if the device is a Zebra device; otherwise blank.</p> <p>Docs: Battery manufactured date for supported device manufacturers such as Zebra devices.</p> <p>Field Name: Battery Manufacture Date. property: mfd possible values: String yyyy-mm-dd</p>
	Brand	Brand of the device.
	C2DM Token	C2DM token of the device if present, otherwise blank.
	Code Name	Code name of the Ivanti Mobile@Work client
	Data Protection Enabled	<p>Finds devices where the passwords are non-compliant.</p> <p>Property: data_protection_enabled possible values: True or False</p>
	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.

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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.
	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.

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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 174.
	Platform Flags	Internal string representing the capabilities of the Ivanti Mobile@Work application.
	Registration Status	<p>Registration status of the device. Registration Status can be used as part of a dynamic label evaluation and criteria for tier compliance.</p> <p>In the Select Type drop-down, select one of these options:</p> <ul style="list-style-type: none"> • Device Admin • Device Admin Not Required • Work Managed Device • Managed Device with Work Profile • Work Profile • 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.

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)


Device Type	Field	Description
	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	<p>True if the device supports Samsung E-FOTA, false otherwise.</p> <hr/> <p> 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" on page 557.</p> <hr/>
	Samsung KNOX Version	Knox version, if present.
	Samsung Model Number	Samsung Model Number.
	Samsung SAFE Version	Samsung Safe Version.
	Screenlock PIN Change Prompt – Showing	<p>Indicates if device user was prompted to change the device's screen lock password / PIN and the device user skipped the prompt. Values are:</p> <ul style="list-style-type: none"> • Unknown - If coming from an older client device, value is unknown. • 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.)

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		The value listed stays until the device user successfully changes the password /PIN on the device. See "Working with default policies" on page 174 .
	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@Work installed on the Wear OS device.
	Wear OS Device is Paired	True if one or more Wear OS device is paired to device via Bluetooth.
	Wi-Fi Security Level	<p>Lists the security level of the Wi-Fi the device is currently connected to:</p> <ul style="list-style-type: none"> • 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. <p>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 <i>Getting Started with Ivanti EPMM</i>.</p>

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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	<ul style="list-style-type: none"> • 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.
	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.

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	AppConnect Terms of Service Date	Represents the date/time the AppConnect Terms of Service was accepted.
	Authenticator Only	True/false if the device is registered in Authenticator Only mode.
	Azure Client Status Code	<p>Indicates whether device is connected to Azure. The possible values are:</p> <ul style="list-style-type: none"> • Success - Able to retrieve device ID. • Internal_Error - An unrecoverable error occurred 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	<p>Lists the device's compliance status in Azure. Possible values are:</p> <ul style="list-style-type: none"> • In-progress • Compliant • Failed

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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: <ul style="list-style-type: none"> • 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 with Ivanti Mobile@Work client.
	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).

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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.
	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

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)


Device Type	Field	Description
	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. IMEI information about the device information on active and inactive SIM slots is displayed in Ivanti EPMM. In addition, CSV-exported data includes the information for inactive slots.
	IMSI	ISI (International Mobile Subscriber Identity) number.
	IP Address	Current IP address of the device. <div> 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.</div>
	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.
	Model	Model of the device.

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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 preregistered 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/false if SD card is encrypted.
	Security State	Security state of the device.
	Serial Number	Serial number of the device.
	Status	Status of the device.

TABLE 13. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	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 13. 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 13. 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	True 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 13. 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	<p>Rapid Security Response fields:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>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.</p>

TABLE 13. 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 13. 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	<p>The SIM ID of the carrier assigned to the SIM of a specific device. The EID will be included in the response of the <code>simdetails</code> API call. (For more information, see the <i>Ivanti EPMM V2 API Guide</i>.)</p> <p>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.</p>
	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	<ul style="list-style-type: none"> • 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 13. 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 EPMU.
	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 13. 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.

The screenshot shows a search expression builder interface. At the top, there are two buttons: 'All' (selected) and 'Any'. Below them is a text input field containing the expression: "common.retired" = false AND "common.compliant" = false. To the left of this field is a green status icon. Below the input field is a checkbox labeled "Exclude retired devices from search results" which is checked. The interface is clean and modern with a light gray background.

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

The screenshot shows the Query Builder interface. At the top, there are two tabs: "All" and "Any", with "Any" selected. Below the tabs, it says "of the following rules are true". There are three rows of criteria:

- Row 1: Platform (dropdown) Equals (dropdown) iOS (dropdown). There are plus and minus icons to the right.
- Row 2: Platform (dropdown) Equals (dropdown) Android (dropdown). There are plus and minus icons to the right.
- Row 3: Home Operator Name (dropdown) Equals (dropdown) United States (dropdown) AT&T (dropdown). There are plus and minus icons to the right.

Below the criteria rows, there is a text box containing the expression: `("common.platform" = "iOS" OR "common.platform" = "Android") AND "common.home_operator_name" = "AT&T"`. To the left of the text box is a green checkmark icon, and to the right is a "Reset" button.

At the bottom, there is a checkbox labeled "Exclude retired devices from search results" which is checked. To the right of the checkbox are three buttons: "Search", "Save to Label", and "Clear".

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" = "AT&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).

The screenshot shows an advanced search rule editor. At the top, there are tabs for 'All' and 'Any' of the following rules are true. Below this, there are three rows of conditions, each with a dropdown for the field, a dropdown for the operator, and a dropdown for the value. The first row is 'Platform' equals 'iOS'. The second row is 'Platform' equals 'Android'. The third row is 'Home Operator Name' equals 'United States' and 'AT&T'. Below the conditions, there is a text box containing the expression: `("common.platform" = "iOS" OR "common.platform" = "Android") AND "common.home_operator_name" = "AT&T"`. To the right of the text box is a 'Reset' link. At the bottom, there is a checkbox labeled 'Exclude retired devices from search results' which is checked. To the right of the checkbox are 'Search', 'Save to Label', and 'Clear' buttons.

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 14. 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.	<p>Select:</p> <ul style="list-style-type: none"> • Home Country Name as the field • Does not equal in Operator • United States in Country Name <p>The search returns a list of devices that do not have United States as their home country name.</p>
Does not contain	<p>Returns a list of devices that do not contain the string specified in the selected field.</p> <ul style="list-style-type: none"> • Used only with strings. • Available only in the expression field. 	<p>Select or enter:</p> <ul style="list-style-type: none"> • 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 <p>The search returns a list of devices that are not assigned to the Global space.</p>

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 491](#).

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 491](#).

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.

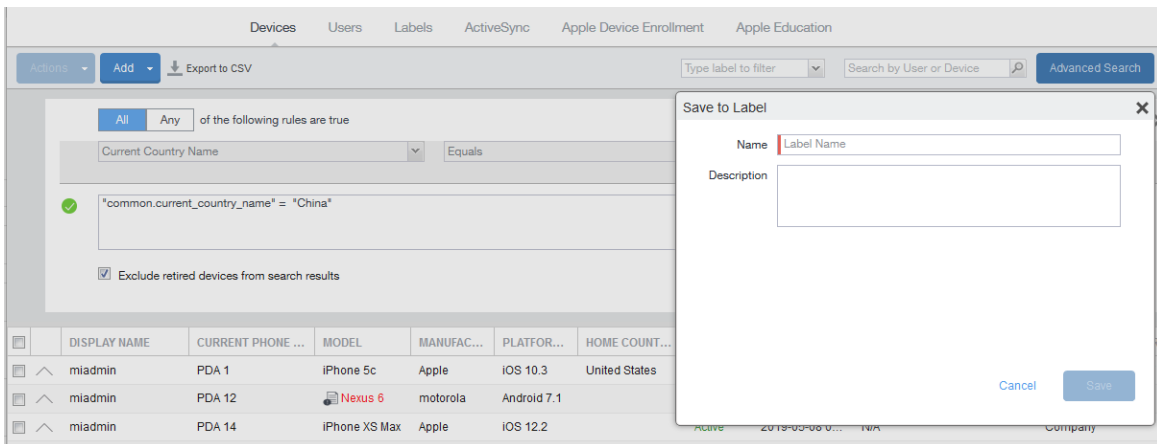
Searching for blocked devices

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 491](#).

Securing Devices

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

- ["Registration-related features and tasks" on the next page](#)
- ["Reprovisioning a device" on the next page](#)
- ["Using self service security features" on page 128](#)
- ["Retiring a device" on page 129](#)
- [Deletion of retired devices](#)
- ["Security-related features and tasks" on page 138](#)
- ["Lock" on page 139](#)
- ["Unlock" on page 140](#)
- ["Unlock AppConnect container" on page 142](#)
- ["Encryption" on page 142](#)
- ["Android Security Patch level" on page 142](#)
- ["Wipe" on page 144](#)
- ["Cancel Wipe" on page 145](#)
- ["Selective Wipe" on page 146](#)
- ["Block AppTunnels" on page 146](#)
- ["Lost" on page 147](#)
- ["Found" on page 147](#)
- ["Locate" on page 147](#)
- ["Reset device PIN" on page 148](#)
- ["Force Device Check-In" on page 149](#)
- ["Setting up background check-ins with APNs" on page 149](#)
- ["Managed iBooks" on page 149](#)
- ["Personal hotspot on/off switch" on page 149](#)
- ["Using custom APN with Android devices" on page 150](#)
- ["Custom Configuration support for Zebra devices" on page 160](#)
- ["Reporting on managed devices" on page 161](#)
- ["Setting the time zone of a device" on page 164](#)

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 15. 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

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.

Rebooting a device

Administrators can remotely reboot devices using Ivanti EPMM. In the Device Details page, **Elapsed Time Since Reboot (minutes)** indicates the amount of time, in minutes, since the device(s) was last rebooted.

Applicable to Android 7.0 managed devices, Managed Device with Work Profile, and Samsung Device Admin (DA).

This feature is not applicable for Android devices 7.0 or below, or for non-managed devices (Work Profile and Device Admin modes.)

"Reboot" displays in the audit logs with the number of minutes since the last device reboot.

Procedure

1. In the Admin Portal, select **Devices & Users**.
2. Select device(s) and then select **Actions > Android Only > Reboot**.

The Reboot dialog box opens.

3. Confirm by selecting **Reboot**.
4. A Reboot status displays, listing the successful reboot for supported devices and the unsupported / failed reboots.

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 Android device means the device user cannot access any AppConnect apps or data. For details, see the *AppConnect Guide for EPMM*.

Client device users can also retire devices, see ["Retiring a device in Ivanti Mobile@Work for Android" on the next page](#).

If you have duplicate devices, see [Managing Duplicate Devices](#).

For Ivanti EPMM 11.10.0.0 and later

For devices with "Retire Pending" state in the following modes, when the administrator uses the **Retire** command on these devices, a warning displays notifying that the Retire command is not supported on these devices.

- Work Managed Device mode
- Work Managed Device - Non-GMS mode (AOSP)
- Managed Device with Work profile mode

When the administrator uses the Retire command on devices, a warning displays notifying that one or more devices in this list are corporate owned Android devices in Fully Managed mode (Device Owner) or Managed Device with Work Profile (Android 8-10 devices, COPE.) The Retire command is not supported on these devices. Wipe command is supported in these modes. (Previously, in Ivanti EPMM 11.9.0.0 and before, the warning message was different and was applicable to Work Managed Device and Work Profile for Company Owned Device modes.)

If the administrator selects Retire after acknowledging this warning, and if any of the selected devices are in Work Managed Device mode, Managed Device with Work Profile mode, then Retire will not work on those devices. A message will display stating "Mobile Platform not Supported."

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 133.



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

6. In the **One or more devices in this list...** section, select the check box to indicate your understanding that the Retire command on devices in Fully Managed or Managed Device with Work Profile mode is not supported. This check box applies to Android devices only.
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*.

Retiring a device in Ivanti Mobile@Work for Android

Ivanti Mobile@Work client 11.8.0.0 and later

- For devices in Work Managed Device mode, Work Managed Device - Non GMS mode, and Managed Device with Work Profile mode, the **Retire** action will not display in the client's My Devices tab.
- For Android 11+ devices in Work Profile for Company Owned Device mode, Retire initiated from the client's My Devices tab is disallowed.

Ivanti Mobile@Work client 11.7.0.0 and lower

When the client initiates the **Retire** action in the My Devices tab:

- Devices in Work Profile mode and Work Profile for Company Owned Device mode will have work profile data removed.
- Devices in Work Managed Device mode, Work Managed Device - Non GMS mode, Managed Device with Work Profile mode will display an error message. Retire action is disallowed.

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.



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.

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 16. 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 populates 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. <ul style="list-style-type: none"> • 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.



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 132](#).

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 17. DELETING OF DEVICES IN SELECTED STATES

Field	Description
Select the states to take actions on	Select all or just the desired options: <ul style="list-style-type: none">• 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 populates 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. <ul style="list-style-type: none">• 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 17. DELETING OF DEVICES IN SELECTED STATES (CONT.)

Field	Description
	<ul style="list-style-type: none">• 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 ["Assigning an administrator the role to delete retired devices" on page 132.](#)

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 18. RETIRE THE RETIRE PENDING DEVICES

Field	Description
Retire the Retire Pending Devices that have not been checked in for more than	<ul style="list-style-type: none"> • 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 populates the search with the regular expression for the search. Select Search .
Maximum Retire Pending devices to Retire in Each Session	<p>Select 100 (default), 500, or 1000.</p> <p>The cleanup session may have an impact on the overall system performance. Configure the maximum limit for your environment.</p>
Automatically Retire the Retire Pending Devices on a schedule	<p>Selecting this check box expands the Retire the Retire Pending Devices Schedule Configuration section.</p> <ul style="list-style-type: none"> • 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.



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 132.](#)


Security-related features and tasks

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

TABLE 19. 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	Accessing the device when the passcode has been forgotten or reassigning the device to a different user <hr/> <div> For security reasons, it is inadvisable to execute this command on lost or stolen devices. </div> <hr/>
Unlock AppConnect Container	Unlocks the AppConnect container (clears the AppConnect passcode)	The device user has forgotten the AppConnect passcode.
Device Encryption Status	Displays the encryption status of the device in the Device Details tab.	Dealing with lost and stolen devices.
Android Security Patch level	Displays the Android Security patch level of the device in the Device Details tab.	Enables an admin to verify that the deployed devices have the latest Android security patches.
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.

TABLE 19. SECURITY-RELATED FEATURES AND TASKS (CONT.)

Feature	Description	Use Case
		 Wipe cannot be reversed after it completes.
Block AppTunnels	This feature is not supported on Android devices.	
Lost	Flags a device as lost	Dealing with lost and stolen devices
Found	Flags a device as found	Dealing with lost and stolen devices
Locate	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.	

Related topics

"Samsung Knox Dual Encryption (DualDAR) support" on page 555

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. Locking an Android device also causes the device user to be locked out of AppConnect apps. For details, see the *AppConnect Guide for EPMM*.

Procedure

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



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

To remove the lock create a new Security policy that specifies that passwords are optional and assign it to the device. This task enables the user to remove the restriction on their phone. The phone will continue to request a password until the user turns off the restriction on the phone. Also, because only one active policy of the same type can be applied to a phone, you may choose to remove this policy from the phone once the user has successfully turned off the lock. You can do this by applying the previous policy or removing the phone from the policy used to remove the lock. See "Using Labels to Establish Groups" in the *Getting Started with Ivanti EPMM* for information on working with labels.

Unlock

Unlocking the device passcode is supported as follows:

TABLE 20. SUPPORT FOR UNLOCKING THE DEVICE PASSCODE ON ANDROID DEVICES

Android Enterprise device	Prior to Android 7.0	Android 7.0 or supported newer versions
Work Managed Devices	Supported	Supported
Work Profile Devices	Supported	Not supported
Work Profile on Company Owned Devices	N/A	Not supported
Android (not using Android Enterprise)	Supported	Not supported Unlock is not supported because these versions of Android do not allow a command to change the device passcode.

IMPORTANT: The Unlock command clears passcodes and TouchIDs from the managed device, compromising device security. Never use this feature on lost or stolen devices.

Procedure

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

Unlock behavior on Android:

- The Unlock command causes Ivanti Mobile@Work for Android to attempt to remove the existing passcode from an Android device. If the attempt is successful, the user will be able to access the device with the default Swipe.
- On devices with Ivanti Mobile@Work , the default passcode is always set to 0000. For Ivanti EPMM 11.8.0.0+, administrators can **Enter minimum six digit unlock pin**. See ["Setting the unlock PIN for a specific device" on page 74](#).
- If the Administrator forces a password reset, the Ivanti Mobile@Work client itself will try to unlock the device, if possible, or the user can unlock the device using the default password, 0000. The user is forced to change that password to one that conforms to password requirements defined in the Security policy. This applies to devices in:
 - Device Admin or Device Owner modes using an OS older than Android 7 or supported newer versions.
 - Managed Device with Work Profile (COPE) mode (Android versions 8-10 only) and Work Profile on Company Owned Devices mode (Android 11 or supported newer versions.)
 - Profile Owner supporting Work Challenge using Android 6 or supported newer versions. Device user of Android 6 device in Profile Owner without Work Challenge support may unlock with "0000" (the default) password, but is not forced to change the password.
- The passcode reset flow would only be triggered when the profile/device is locked. If the administrator sends a "Unlock" command and the profile is not locked then Ivanti EPMM will not reset it to 0000 and not bring up the password reset screens. Otherwise, the only time Ivanti EPMM will reset to 0000 and bring up the reset screens would be when the profile or Android device is locked. This is applicable to Ivanti Mobile@Work 11.1.0.0 or supported newer versions and to the following Android Enterprise modes:
 - Device Admin mode (on some devices)
 - Device Owner mode
 - Work Profile mode
 - Managed Device with Work Profile mode
 - Work Profile on Company Owned Device mode

- Android Enterprise Work Managed mode-registered devices that are in kiosk mode move out of kiosk when you send the UNLOCK command from Ivanti EPMM. This only happens when the password is mandatory as per the Security Policy on Ivanti EPMM.
- For Android Enterprise devices, see ["Unlocking an Android Enterprise device" on page 73](#).

Unlock AppConnect container

To unlock the AppConnect container (clear the AppConnect passcode):

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

Encryption

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

To check the encryption status of a device:

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

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

Android Security Patch level

The security patch level of an Android device is reported on the device details tab. This is available on Android devices using Android 6 or supported newer versions. To check the security patch level of an Android device:

1. Go to **Device & Users > Devices**.
2. Select an Android device.
3. Use the drop-down menu to configure search rules to find the patch level.
4. In the first drop-down menu, select **Security Patch Level**.

5. Use the other fields to define your search.
6. Optionally, select the **Exclude retired devices from search** results check box.
7. Click **Search** or click **Save to Label**.

If you click **Save to Label** and 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 491.

8. Go to **Device & Users > Devices > Device Detail**.

The **Security Patch Level** displays in the **Device Details** tab.

Relinquishing ownership of a device

Applicable to Android devices in Work Profile on Company Owned Device mode.

For Ivanti EPMM 11.10.0.0 and later

When administrators use the Relinquish Ownership option, a warning displays stating that the action has been replaced with [Retire](#). If you need to remove organizational information and apps from devices, use **Actions > Retire** in the **Devices & Users** page. Personal data is not lost and the end user can then use the device as a personal device, with full access to all device controls and settings.

After Upgrading to Ivanti EPMM 11.10.0.0

For Work Profile for Company Owned Device mode in Android 11+ devices:

- In Relinquish Pending state - the work profile gets relinquished.
- Selecting **Devices & Users > Actions > Android Only > Relinquish Ownership** will display a warning message.
- Selecting the **Devices & Users > Actions > Retire** will remove the work profile (organizational data and apps.) (Previously, in Ivanti EPMM 11.9.0.0 and before, the Retire action would factory reset the device.)

For Work Managed Device mode, Work Managed Device - Non-GMS mode, and Managed Device with Work Profile modes in Android 8-10 devices:

- The Retire action is only available from the local compliance action in Ivanti EPMM's security policy. Administrators will need to use the [Wipe](#) action instead.

For Ivanti EPMM 11.3.0.0 - 11.9.0.0

Relinquishing Ownership of a device in Work Profile on Company Owned Device mode removes the work profile and [Retires](#) the device from Ivanti EPMM, without affecting personal apps and data. The end user can then use the device as a personal device, with full access to all device controls and settings.



The device needs to be removed from Google Zero Touch or Knox Mobile Enrollment portal.

You might relinquish ownership of a device if:

- the user left the company
- the user has replaced the device

You may see "Relinquish_Pending" in Advanced search results.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the device.
3. Select **Actions > Relinquish Ownership**. The Relinquish Ownership dialog box opens.
4. Enter any descriptive information into the **Note** field.
5. Select **Relinquish Ownership**. The device is removed from Ivanti EPMM.

Wipe



This feature can also be used on SD cards, for most devices.

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**.



If the Ivanti Mobile@Work app on the selected device is currently connected, then this action will be applied immediately. However, if the Ivanti Mobile@Work app is not currently connected, then Ivanti EPMM will attempt to complete the operation by means of the SMTP configuration.

Related topics

- ["Cancel Wipe" below](#)

Cancel Wipe

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

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

Cancel Wipe is supported for Android devices with status: **Wipe pending**.

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

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



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

6. Click **Cancel Wipe**.

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

Related topics

["Wipe" on page 144](#)

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.
- For Exchange through integration with selected devices and email apps.

Block AppTunnels



This feature is not supported on Android devices.

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.

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" below](#)

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.

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



Android devices use both cell towers and GPS to locate the device. On Android 6.0 devices, Location Permissions must be granted to the app at runtime.

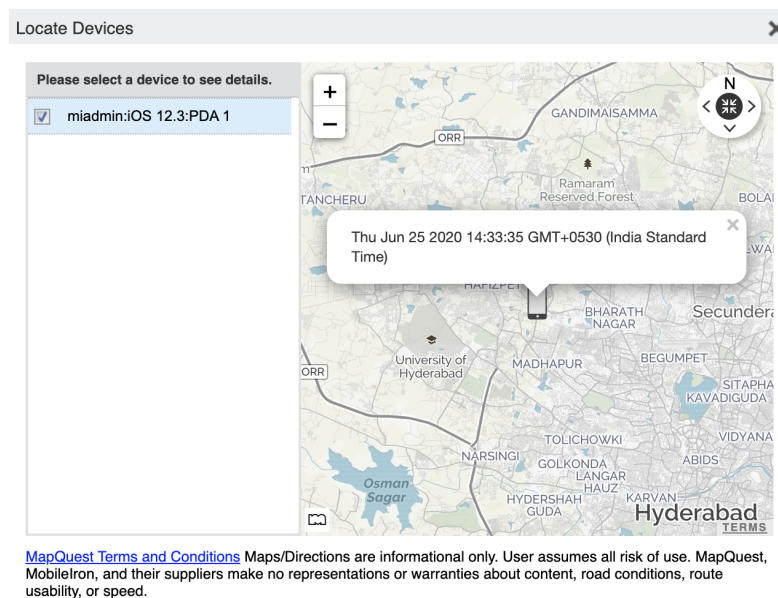
Most registered phones can be located on a map using cell tower IDs. When locating a device via cell tower IDs, Ivanti Mobile@Work records tower data until the next time data is synchronized between Ivanti Mobile@Work and Ivanti EPMM. See "Sync policies" in *Getting Started with Ivanti EPMM* for information 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



This feature is not supported on Android 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.



Both the **Force Device Check-in** option on the Admin Portal and the Ivanti Mobile@Work for Android update the policies and settings related to AppConnect. The app check-in interval on the AppConnect global policy does not apply to Android 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**.

Setting up background check-ins with APNs

This feature is not supported on Android devices.

Managed iBooks

This feature is not supported on Android devices.

Personal hotspot on/off switch

This feature is not supported on Android devices.

Using custom APN with Android devices

Your device uses the APN or Access Point Name settings to set up a connection to the gateway between the carrier's network and the internet. You can configure a custom APN on Android devices in Work Managed Device mode and Managed Device with Work Profile (COPE) mode on Android version 9.0 or supported newer versions. You can also configure custom APNs on Samsung devices. Multiple APN's can be set up for each Android device, but only one configuration is allowed per APN.



The Android APN Settings Configuration takes precedence over other APN settings if already configured in the device manually or by the network operator.

To enter the custom setting for APN:

1. Go to **Policies & Configs > Configurations > Add New > Android > Android APN**.
2. In the New Android APN Setting dialog box, enter the values. Settings with fields marked in red are required. See:
 - ["APN settings for Samsung devices" below](#)
 - ["APN settings for Android devices" on page 152](#)
 - ["APN settings for Android devices" on page 152](#)
3. Click **Save**.

APN settings for Samsung devices

Below are the settings for having an APN on Samsung devices.

TABLE 21. NEW APN SETTINGS FOR SAMSUNG DEVICES

Item	Description
Samsung	Select if this APN is directed to Samsung devices. If you want non-Samsung devices, go to "APN settings for Android devices" on page 152 .
Preferred APN	Select On to set this APN as preferred. Note that having more than one APN as preferred on a device will be flagged as error by the Ivanti Mobile@Work client.
Name	Enter a unique name that, together with the Access Point Name, will be displayed on the device.

TABLE 21. NEW APN SETTINGS FOR SAMSUNG DEVICES (CONT.)

Item	Description
Description	Enter a description for the APN.
Access Point Name	Enter the name of the access point.
Authentication Type	<p>Select the type of authentication protocol from the following options:</p> <ul style="list-style-type: none"> • Not Set - default • None - Select to not have an 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. • Select to have Ivanti EPMM choose PAP or CHAP, whichever is available first.
Mobile Country Code	Enter the mobile country code.
Mobile Network Code	Enter the mobile network code.
MMS Proxy Address	Enter the MMS proxy address.
MMS Port Number	Enter the MMS port number (numeric values between 1 to 65535.)
MMS Server Address	Enter the MMS server address.
User Name	Specify the user name to use.
Password	Specify the password to use.
Confirm Password	Confirm the password to use.
Port Number	Enter the port number (numeric value between 1 to 65535.)
Proxy Address	Enter the proxy address.
Server Address	Enter the IP address, hostname, or URL for the server.
Access Point Type	<p>Select the access point type from the following options:</p> <ul style="list-style-type: none"> • default • SUPL • MMS

TABLE 21. NEW APN SETTINGS FOR SAMSUNG DEVICES (CONT.)

Item	Description
	<ul style="list-style-type: none"> • Custom

APN settings for Android devices

Below are the settings for having an APN on Android devices.

TABLE 22. NEW APN SETTINGS FOR ANDROID DEVICES

Item	Description
Android 9+	Select if this APN is directed to Android devices 9.0 or supported newer versions.
Name	Enter a unique name that, together with the Access Point Name, will be displayed on the device.
Description	Enter a description for the APN.
Access Point Name	Enter the name of the access point.
Authentication Type	<p>Select the type of authentication protocol from the following options:</p> <ul style="list-style-type: none"> • Not Set - default • None - Select to not have an 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. • Select to have Ivanti EPMM choose PAP or CHAP, whichever is available first.
Access Point Type	<p>Select one or more access point type(s) from the following options:</p> <ul style="list-style-type: none"> • Default • DUN • IMS • Emergency

TABLE 22. NEW APN SETTINGS FOR ANDROID DEVICES (CONT.)

Item	Description
	<ul style="list-style-type: none">• MMS• HIPRI• CBS• MCX• SUPL• FOTA• IA
MVNO Type	Select the type of Mobile Virtual network Operator from the following options: <ul style="list-style-type: none">• Not Set (default)• SPN• IMSI• GID• ICCID
Bearer	(Optional) Select one or more types of bearer service(s) used for data transmission from the following options: <ul style="list-style-type: none">• 1xRTT• EHRPD• EVDO_B• HSDPA• CDMA• EVDO_O• GPRS

TABLE 22. NEW APN SETTINGS FOR ANDROID DEVICES (CONT.)

Item	Description
	<ul style="list-style-type: none">• HSPA• EDGE• EVDO_A• GSM• HSPPAP• HSUPA• IDEN• IWLAN• LTE• NR• TD_SCDMA• UMTS
APN Protocol	Select the APN protocol required for the APN from the following options: <ul style="list-style-type: none">• Not Set (default)• IPV4• IPV6• IPV4_OR_IPV6• NON_IP• PPP• UNSTRUCTURED
APN Roaming Protocol	Select the APN roaming protocol required for the APN from the following options:

TABLE 22. NEW APN SETTINGS FOR ANDROID DEVICES (CONT.)

Item	Description
	<ul style="list-style-type: none">• Not Set (default)• IPV4• IPV6• IPV4_OR_IPV6• NON_IP• PPP• UNSTRUCTURED
Enable / Disable APN	Select On to enable APN; default is off.
Carrier ID	Enter the numeric value of the carrier ID.
Mobile Country Code	Enter the mobile country code.
Mobile Network Code	Enter the mobile network code.
MMS Proxy Address	Enter the MMS proxy address.
MMS Port Number	Enter the MMS port number (numeric value between 1 to 65535.)
MMS Server Address	Enter the MMS server address.
User Name	Enter the login username.
Password	Enter the login password.
Confirm Password	Confirm the login password.
Port Number	Enter the port number (numeric value between 1 to 65535.)
Proxy Address	Enter the proxy address.

APN settings for Android Enterprise devices

Below are the settings for having an APN on Android Enterprise devices. This is requirement for enterprise APNs with 4G deployments.

Applicable to Android Enterprise devices in all modes.

TABLE 23. NEW APN SETTINGS FOR ANDROID ENTERPRISE DEVICES

Item	Description
Android 9+	Select if this APN is directed to Android devices 9.0 or supported newer versions.
APN Roaming Protocol	Sets the protocol to use to connect to this APN when the device is roaming. Default is Not Set .
Name	Enter a unique name that, together with the Access Point Name, will be displayed on the device.
Description	Enter a description for the APN.
Access Point Name	Enter the name of the access point.
Authentication Type	Select the type of authentication protocol from the following options: <ul style="list-style-type: none"> • Not Set - default • None - Select to not have an 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. • Select to have Ivanti EPMM choose PAP or CHAP, whichever is available first.
Access Point Type	Select one or more access point type(s) from the following options: <ul style="list-style-type: none"> • Default • DUN • IMS • Emergency • MMS • HIPRI • CBS

TABLE 23. NEW APN SETTINGS FOR ANDROID ENTERPRISE DEVICES (CONT.)

Item	Description
	<ul style="list-style-type: none">• MCX• SUPL• FOTA• IA• BIP• VSIM• XCAP• ENTERPRISE
MVNO Type	Select the type of Mobile Virtual network Operator from the following options: <ul style="list-style-type: none">• Not Set (default)• SPN• IMSI• GID• ICCID
Bearer	(Optional) Select one or more types of bearer service(s) used for data transmission from the following options: <ul style="list-style-type: none">• 1xRTT• EHRPD• EVDO_B• HSDPA• CDMA• EVDO_0

TABLE 23. NEW APN SETTINGS FOR ANDROID ENTERPRISE DEVICES (CONT.)

Item	Description
	<ul style="list-style-type: none">• GPRS• HSPA• EDGE• EVDO_A• GSM• HSPAP• HSUPA• IDEN• IWLAN• LTE• NR• TD_SCDMA• UMTS
APN Protocol	<p>Select the APN protocol required for the APN from the following options:</p> <ul style="list-style-type: none">• Not Set (default)• IPV4• IPV6• IPV4_OR_IPV6• NON_IP• PPP• UNSTRUCTURED

TABLE 23. NEW APN SETTINGS FOR ANDROID ENTERPRISE DEVICES (CONT.)

Item	Description
APN Roaming Protocol	<p>Select the APN roaming protocol required for the APN from the following options:</p> <ul style="list-style-type: none"> • Not Set (default) • IPV4 • IPV6 • IPV4_OR_IPV6 • NON_IP • PPP • UNSTRUCTURED
Enable/Disable APN	<p>Select On to enable APN; default is off.</p> <p>Note that having more than one APN as preferred on a device will be flagged as error by the Ivanti Mobile@Work client.</p>
Carrier ID	Select to set the Carrier ID for this APN.
Mobile Country Code	Enter the mobile country code.
Mobile Network Code	Enter the mobile network code.
MMS Proxy Address	Enter the MMS proxy address.
MMS Port Number	Enter the MMS port number (numeric values between 1 to 65535.)
MMS Server Address	Enter the MMS server address.
User Name	Specify the user name to use. Default is miadmin .
Password	Enter the password to use.
Confirm Password	Confirm the password to use.
Port Number	Select or enter the port number (numeric value between 1 to 65535.)
Proxy Address	Enter the proxy address.
Available on Android 13 and later	
MTUV4	Set the default MTU (Maximum Transmission Unit) size in bytes of the IPv4 routes brought up by this APN setting. Minimum value is 1068 bytes, maximum value is 64 KB.

TABLE 23. NEW APN SETTINGS FOR ANDROID ENTERPRISE DEVICES (CONT.)

Item	Description
MTUV6	Set the default MTU (Maximum Transmission Unit) size in bytes of the IPv6 routes brought up by this APN setting. Minimum value is 1294 bytes, maximum value is 64 KB.
Set Persistent	Set if the APN setting should be persistent/non-persistent in modem. Default is deselected.
APN Type	The following are the newly added APN Types: <ul style="list-style-type: none">• ApnSetting.TYPE_XCAP Supporting OS-Android R11• ApnSetting.TYPE_BIP Supporting OS-Android S12• ApnSetting.TYPE_VSIM Supporting OS-Android S12• ApnSetting.TYPE_ENTERPRISE Supporting OS-Android T13

Custom Configuration support for Zebra devices

You can deploy a custom configuration for your Zebra devices using XML configuration files from Zebra's StageNow software. The custom XML configuration file is uploaded to Ivanti EPMM as a text file, and applied to a label. This XML configuration is then pushed to the Zebra device. To deploy the XML configuration file:

1. Go to **Policies & Configs > Configurations > Add New > Android > Android XML Configuration** to display the New Android XML Configuration page.
2. Enter the **Name** and **Description** of the configuration.
3. In the Configuration Type field, select **Zebra**.
4. Select **Browse** to navigate to and select the XML configuration file.

5. Read the warning and select the **I Agree** check box.
6. Select **Save**.



XML configuration files is supported on Zebra 4.4 devices, see [Zebra devices and Stage Now software](#).

Ivanti EPMM supports Android remote control of Zebra devices with TeamViewer. For more information, see knowledge base article [Support for Help@work on Zebra devices for Ivanti EPMM](#).

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*.

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 to your computer.


Export to CSV Field Options

Below describes what is contained inside a .CSV file.

TABLE 24. 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\$
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)

TABLE 24. EXPORT TO CSV FIELD OPTIONS (CONT.)

Type	Supported Variables
User Attributes	<p>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</p> <hr/> <p> If defined in LDAP settings, custom attributes appear here also.</p>
Common Device Attributes	<p>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</p>
Android Attributes	<p>User ID, Device UUID, Admin Activated, Android Client Version Code, Android Enterprise Capable, Attestation, Brand, C2DM Token, Code Name, Device, Device Encryption Status, Device Roaming Flag, GCM/FCM Token Present, ICCID, Incremental, Kiosk Enabled, Manufacturer OS Version, MDM Enabled, Media Card Capacity, Media Card Free, Multi MDM, OS Build Number, OS Update Path, OS Update Status, Platform Flags, Registration Status, Samsung Knox Version, Secure Apps Enabled, Secure Apps Encryption Enabled, Secure Apps Encryption Mode, Security Detail, Security Patch Level, Security Reason, USB Debugging</p>

Setting the time zone of a device

For setting time zones in Android devices, see ["Provisioning an Android Enterprise device" on page 75](#).

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 97](#).

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**.

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 167](#)
- ["Viewing custom attributes available for users and/or devices" on page 168](#)
- ["Viewing custom attributes assigned to users" on page 168](#)
- ["Viewing custom attributes assigned to devices" on page 168](#)
- ["Editing custom attributes for users and/or devices" on page 168](#)
- ["Searching for custom attributes for users and/or devices" on page 169](#)
- ["Exporting a log of the custom attributes for users and/or devices" on page 169](#)
- ["Deleting custom attributes from users and/or devices" on page 169](#)
- ["Setting custom attribute values for device or users" on page 170](#)
- ["Pushing label attribute changes to devices and users" on page 171](#)

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.
Attribute Description	Enter a meaningful description for the custom attribute.
Value Type	Select one of three value types: boolean, integer or string. For information on Android Zero Touch custom attributes, see "Zero Touch enrollment with custom attributes" on page 80 .
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.
6. In the **Custom User Attributes** section, click **Add+**.
7. Referring to the table above, enter the information for the custom user attributes.
8. Click **Save**. The new custom user attribute is created and displays in the table.
9. (Optional) Repeat the steps, as needed.

Viewing custom attributes available for users and/or devices

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > System Settings > Users & Devices > Custom Attributes**.
3. View all available custom attributes for users and/or devices.

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

Viewing custom attributes assigned to users

Procedure

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

Viewing custom attributes assigned to devices

Procedure

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

Editing custom attributes for users and/or devices

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.



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 98](#).

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 149.
- **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 176
- "Viewing policy status and platform support" on page 178
- "Security Policy" on page 179
- "Device log encryption on Android devices" on page 513
- "Sync policies and battery use" on page 191
- "Global App Config Settings policy" on page 180
- "Work Schedule policy" on page 191
- "Country changes and alerts" on page 194
- "Android devices and the Client Is Always Connected option" on page 194
- "Working with Samsung Android kiosk policies" on page 198
- "Working with Android Quick Setup policies" on page 198
- "Working with Samsung general policies" on page 200
- "Notifications of changes to the privacy policy" on page 209
- "Exporting the devices in the WatchList" on page 256
- "Impact of changing LDAP server variables" on page 257



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

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.

Setting an alert that a device's PIN change request was skipped

You can set an alert to have the device user change the password / PIN. You can also identify devices that have prompted the device user to change the password / PIN but the device user skipped the prompt.

Procedure

1. In your security policy, indicate the value in the Maximum Password Age field the number of days a password is valid for. See *Getting Started with Ivanti EPM* for details.
2. Create a compliance action with the desired number of days (1,2,3...up to 7) that the administrator wants to give as a grace period before taking a compliance action. For example, if the administrator wants to have immediate effect, the value would be 7 (days.) If the administrator wants to give a grace period of 5 days, the value would be 2 (days.). See ["Adding custom attributes to users and/or devices" on page 167](#).
3. Using ["Advanced searching " on page 97](#), create a search that searches for devices that are less than 7 days (for example) of the device's password expiration date. Utilize the Android > Password/PIN Days Before Expiring field as part of your search criteria.



If the Maximum Password Age is 0, that means the PIN is set to never expire. When this happens, it means the Screenlock PIN Change Prompt – Showing value will always display as false and the **Password/PIN Days Before Expiring** displays as 0. Thus, the compliance policy cannot be a simple rule of just **Password/PIN Days Before Expiring > Is less than or equal to > 7**. It needs to be **Password/PIN Days Before Expiring > Is less than or equal to > 7** and **Password/PIN Days Before Expiring > Is greater than > 0** (see below).

The screenshot shows a search builder interface with the following elements:

- Logic: **All** of the following rules are true
- Rule 1: Password/PIN Days Before Expiring **Is less than or equal to** 7
- Rule 2: Password/PIN Days Before Expiring **Is greater than** 0
- Generated Query: `"android.priv_password_expiration_timeout" <= 7 AND "android.priv_password_expiration_timeout" > 0`
- Buttons: Search, Save to Label, Clear
- Checkbox: ☒ Exclude retired devices from search results

4. Select **Save to Label**.

Apply the saved search to the appropriate labels (**Actions > Apply to Labels**).

5. To view the results, go to Device Details page and in the Details tab, view the values for the following fields:
 - **Screenlock PIN Change Prompt - Showing** - Indicates if device user was prompted to change the device's screen lock password / PIN and the device user skipped the prompt. Values are:
 - Unknown - If coming from an older client device, value is unknown.
 - True - Indicates the PIN is to expire in 7 days or less.

- 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.

- **Password/PIN Days before expiring field** - 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.

Importing and exporting policies

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

- ["Exporting policies or configurations" below](#)
- ["Importing policies or configurations" on the next page](#)



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 page 176.](#)

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

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" on the next page](#)

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. For Android devices, expand the **DETAILS** section of the Policies tab to see the verifiable results for Security and Lockdown policies.
- **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. For Android devices, expand the **DETAILS** section of the Policies tab to see the verifiable results.

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

The screenshot shows a 'New Security Policy' dialog box. It has a title bar with 'New Security Policy' and a close button. The dialog contains several fields and options: 'Name' (text input), 'Status' (radio buttons for Active and Inactive), 'Priority' (radio buttons for Higher than and Lower than, followed by a dropdown), 'Description' (text input), and a 'Password' section. The 'Password' section has radio buttons for Mandatory and Optional, and a 'Password Type' section with checkboxes for Simple, Alphanumeric, and Don't care. A 'Platforms Supported' link is highlighted with a red box.

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

Security Policy

Security policies specify how Ivanti EPMM addresses several areas of mobile security. Ivanti, Inc recommends you create separate policies for each platform to avoid inconsistencies.

For more information on creating or editing a security policy, see "Security policies" in the *Getting Started with Ivanti EPMM*.

Proactive password security policy

When certificates are applied to the device as certificate settings, certificate enrollment settings, or via a Wi-Fi configuration, Ivanti Mobile@Work proactively applies a password policy that meets the Android OS certificate installation requirements.

With the proactive password policy, Ivanti Mobile@Work prompts the user to create a screen lock for their device, even if Ivanti EPMM does not enforce a privacy policy.

Password policy attributes

For all password policy attributes, Ivanti EPMM only displays "Unsupported" for Ivanti Mobile@Work for Android 10.6 or supported newer versions. This Android 10 or above device needs to be in Device Admin (DA) mode. If the device is still using an old version of Ivanti Mobile@Work, it will not report "Unsupported."

You can view this information in Devices & Users > Device > Device tab. "Unsupported" will display for the following password policy attributes:

- Password
- Password Type
- Minimum Password Length
- Maximum Password Age

Ivanti EPMM will not quarantine the device, the security policy will display as "Applied," and the device status will be compliant.

Ivanti EPMM will no longer consider Unsupported for the above password policy attributes as a policy violation if the device is Android 10 or above and in Device Admin mode.

Previously if the security policy was in violation, a compliance action could be triggered if one was set. Some compliance actions could be: Send an alert, Block email or Quarantine.

Related topics

["Device log encryption on Android devices" on page 513](#)

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 25. EXAMPLE A - LABEL SETTINGS

Item	Description
Apps:	<ul style="list-style-type: none">• Gmail has label_1.• AnyConnect has label_2.
App Config Setting Policies:	<ul style="list-style-type: none">• 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 26. EXAMPLE B - LABEL SETTINGS

Item	Description
Apps:	<ul style="list-style-type: none"> Gmail has label_1. AnyConnect has label_2.
App Config Setting Policies:	<ul style="list-style-type: none"> 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 27. EXAMPLE C - LABEL SETTINGS

Item	Description
Apps:	<ul style="list-style-type: none"> Gmail has label_1. AnyConnect has label_2.
App Config Setting Policies:	<ul style="list-style-type: none"> 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 28. EXAMPLE D - LABEL SETTINGS

Item	Description
Apps:	<ul style="list-style-type: none"> Gmail has label_2.
App Config Setting Policies:	<ul style="list-style-type: none"> Policy_1 has label_1.
Device:	If device has label_1 and label_2, then the Gmail app will choose App Catalog settings.

TABLE 29. EXAMPLE E - LABEL SETTINGS

Item	Description
Apps:	<ul style="list-style-type: none"> Gmail has label_1 and label_2.
App Config Setting Policies:	<ul style="list-style-type: none"> 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" on the next page](#).
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 250](#).
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 30. 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 31. IOS SETTINGS - MANAGED APP SETTINGS



Field	Description
Prevent backup of the app data	<p>Select to ensure that iTunes will not attempt to back up possibly sensitive data associated with the given app.</p> <hr/> <p> This setting is not displayed for iOS apps when Ivanti EPMM is configured for MAM-only iOS devices.</p> <hr/>
Remove app when device is quarantined or signed out	<p>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.</p> <p>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.</p>

TABLE 31. iOS SETTINGS - MANAGED APP SETTINGS (CONT.)

Field	Description
	<ul style="list-style-type: none"> 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. <p>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.</p> <p>For more information, see Using Secure Sign-In and Sign-Out.</p>
Send installation request on device registration or sign in	<p>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.</p> <p>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.</p>
Send installation request to quarantine devices	<p>Select to send an installation request to quarantine devices. Deselected by default.</p>
Remove app when MDM profile is removed	<p>Selected by default, this option removes the app from the device when the MDM profile is removed from the device.</p> <hr/> <p> This setting is not displayed for iOS apps when Ivanti EPMM is configured for MAM-only iOS devices.</p> <hr/>
Prevent user from removing and offloading app	<p>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."</p> <p>De-select to allow the device users to remove and uninstall the app.</p> <p>Applicable to iOS 14.0 or newer versions.</p>

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 32. 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	<p>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.</p> <p>De-selecting the check box means the device user will need to manually install the app.</p> <p>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.</p> <hr/> <p> 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 <i>Ivanti EPMM Apps@Work Guide</i>.</p> <hr/> <p>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.</p> <p>Applicable to:</p> <ul style="list-style-type: none"> • 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.

TABLE 32. ANDROID SETTINGS TAB (CONT.)


Field	Description
	<p>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.</p> <p>Use the version enforcement feature to:</p> <ul style="list-style-type: none"> • 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. <p>See Enforcement of specific app versions for mandatory in-house apps in the <i>Ivanti EPMM Apps@Work Guide</i>.</p>
Require the user to install the latest version of the app in order to run it.	<p>Select to ensure the device user installs the latest version of this app.</p> <hr/> <p> 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.</p> <hr/> <p>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 <i>Ivanti EPMM Apps@Work Guide</i>.</p>
Silent install for work managed devices	<p>This feature is specifically for private in-house Android Enterprise apps and applies only to devices that support silent installation.</p> <p>Clearing the check box means the device user will need to manually install the app.</p> <p>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.</p>

TABLE 32. ANDROID SETTINGS TAB (CONT.)


Field	Description
	<p>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.</p> <hr/> <p> Silent install is not supported for MAM-only Android devices.</p> <hr/> <p>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.</p> <p>Auto Install Mode - Self hosted apps will not be auto installed.</p> <ul style="list-style-type: none"> • Force Install (default) • Auto Install Once - recommended by Ivanti. <p>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.</p> <ul style="list-style-type: none"> • Low • Medium (default) • High <p>Install only when connected to Wi-Fi - Default is de-selected.</p> <p>Install only when charging - Default is de-selected.</p> <p>Install only when Idle - Default is de-selected.</p> <p>For more information, see Silent install and uninstall of mandatory apps in the <i>Ivanti EPMM Apps@Work Guide</i>.</p> <p>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.</p>
Silently install Mandatory Apps	<p>This feature only applies to devices that support silent installation. This feature is not supported for MAM-only Android devices. Selected by default.</p>

TABLE 32. ANDROID SETTINGS TAB (CONT.)


Field	Description
	<p>De-selecting the check box means the device user will need to manually install the app.</p> <p>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.</p> <hr/> <p> 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 <i>Ivanti EPMM Apps@Work Guide</i>.</p> <hr/> <p>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.</p>
Block Widget on Home Screen	<p>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.</p> <p>Applicable only to apps installed in the Managed profile.</p>
Block Uninstall	<p>Selected by default, this feature prevents the device user from uninstalling the app.</p>
Quarantine app when device is quarantined	<p>Required for Work Profile mode, Work Managed Device mode, and Managed Device with Work Profile mode.</p> <p>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.</p> <p>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.</p>

TABLE 32. ANDROID SETTINGS TAB (CONT.)


Field	Description
	 If you change the setting after the app is added, the changed setting will be applied to the app.
Auto Launch Application on Install	<p>Selected by default. After installation, the Ivanti Mobile@Work app would be in the foreground when launching apps.</p> <p>Applicable to Android devices in:</p> <ul style="list-style-type: none"> • 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	<p>Select this check box to modify runtime permissions for other apps.</p> <ul style="list-style-type: none"> • Applicable to public / private apps on Work Managed Device mode on Android 8.0 or newer versions • 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	<p>Select this check box to delegate third-parties to have permission to hide and suspend the selected app.</p> <ul style="list-style-type: none"> • 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.

TABLE 32. ANDROID SETTINGS TAB (CONT.)

Field	Description
	<ul style="list-style-type: none">• 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.

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.

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" on the next page](#)
- ["Applying a Work Schedule policy" on the next page](#)
- ["Managing a Work Schedule policy" on page 193](#)
- ["Setting up Work Schedule policy notifications" on page 193](#)

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.



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.

Android devices and the Client Is Always Connected option

Android devices support the Client is Always Connected option on the sync policy. Enable this option only when FCM (previously GCM) cannot be used. These situations include:

- Regions and countries in which FCM is not available.
- Select commercial and government use cases.
- Devices which do not support FCM, such as the Amazon Kindle.



Google shut down GCM service on May 29, 2019. GCM is replaced by Firebase Cloud Messaging (FCM). Ivanti EPMM 8.0.0.0 and Ivanti Mobile@Work for Android 10.2.1.0 or supported newer versions now use FCM. See [Customer Notice - GCM Batch End of life](#).

Ivanti EPMM uses FCM to immediately send lock, unlock, retire, and wipe, commands to devices. You can also send notification messages to devices using FCM. With **Always Connected** option enabled, Ivanti EPMM can send these commands and notification messages to the device at any time without using FCM.

Ivanti recommends that you enable **Always Connected** mode on a maximum of 5000 devices per Ivanti EPMM instance. The reason is that the device generates a regular connection status check to Ivanti EPMM when using **Always Connected** mode. This status check can impact the device as follows:

- It will cause a small increase in battery power consumption on the device.
- It will cause a small increase in bandwidth usage on the device, which sometimes is a concern when using cellular networks.

Enabling attestation on Android devices

In the Admin Portal, you can enable Google PlayIntegrity attestation on Android devices to verify the integrity of the devices' software and hardware. This action provides Ivanti EPMM with the devices' PlayIntegrity attestation status. With this status, you can:

- Take actions on untrusted devices.
- Deliver policies, configurations, and apps to only trusted devices.
- Assess whether the Ivanti Mobile@Work app running on a device is valid, or if it is a malicious app pretending to be Ivanti Mobile@Work .

This feature attests, or verifies, various information about the device. Specifically, this feature:

- Certifies the manufacturer and model of devices
- Provides information about Ivanti Mobile@Work
- Certifies the device is intact and has not been tampered with
- Verifies that the Google Play version installed on the device supports SafetyNet/PlayIntegrity

SafetyNet/PlayIntegrity attestation works with any Android deployment, including work profiles, managed devices, and managed devices with work profiles. It also works when the device is in Device Admin mode.

If SafetyNet/PlayIntegrity is enabled on the security policy of the device, Ivanti EPMM initiates a SafetyNet/PlayIntegrity attestation check when:

- The device has been rebooted or
- The last SafetyNet/PlayIntegrity check was performed more than 24 hours ago.

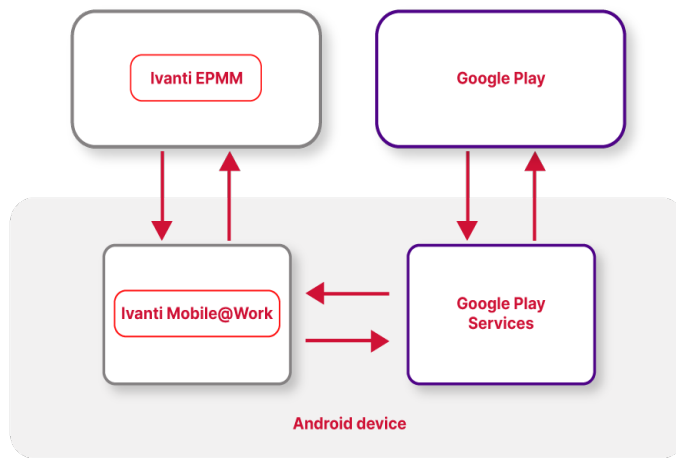


SafetyNet/PlayIntegrity attestation requires that the device is running Ivanti Mobile@Work 10.1 for Android or supported newer versions.

SafetyNet attestation flow

When Ivanti EPMM initiates a SafetyNet attestation check for a device, it sends a request to Ivanti Mobile@Work . Ivanti Mobile@Work requests Google Play Services to do the check, and Google Play Services communicates with Google Play. Google Play Services returns the results to Ivanti Mobile@Work , which returns the results to Ivanti EPMM. The following figure illustrates this flow.

FIGURE 1. SAFETYNET ATTESTATION FLOW



PlayIntegrity attestation flow

With this release, Ivanti EPMM switches to PlayIntegrity from SafetyNet. Play Integrity attestation workflow is supported on Android 14 devices and above. The older OS version devices go through the safety net attestation workflow. As a fallback, if the Android 14 devices are unable to attest via Play integrity, then the attestation falls back to Safety Net.

Setting PlayIntegrity attestation

To configure Ivanti EPMM to initiate PlayIntegrity attestation for devices, do the following.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Select a security policy and select **Edit**.

Alternatively, create a new security policy by selecting **Add New > Security**.

1. Scroll down to the **Android** section.
2. Select **"Require Google PlayIntegrity Attestation"**.

3. Select **Save**.

Related topics

"Security policies" in *Getting Started with Ivanti EPMM*

PlayIntegrity attestation information in device details

In the Admin Portal, in the **Device Details** of a device at **Devices & Users > Devices**, you can view the following fields about PlayIntegrity attestation. You can also use these fields in Advanced Search, including creating labels.

TABLE 1. PLAYINTEGRITY ATTESTATION INFORMATION

Status on Device	Description
PlayIntegrity Enabled	Indicates whether the security policy applied to the device has PlayIntegrity enabled.
PlayIntegrity Exception	Indicates an exception occurred while running PlayIntegrity attestation on the device.
PlayIntegrity Timestamp	The date and time when Ivanti EPMM last received a PlayIntegrity attestation response from the device.
PlayIntegrity Status	The results of the last PlayIntegrity attestation, described in the next table.

The following table explains the values of the PlayIntegrity Status field in a device's Device Details.

TABLE 2. STATUS VALUES

Ivanti EPMM Status	Description for SafetyNet	Description for PlayIntegrity
Compatible	Ivanti EPMM received a successful response, indicating a positive response to both the basic integrity test and the CTS profile verification.	Ivanti EPMM received a successful response, indicating a positive response to both the basic integrity test and the Meets Device Integrity Verdict.
Basic	Ivanti EPMM received a successful response to the basic integrity check, but received a failed response to the CTS profile verification.	Ivanti EPMM received a successful response to the basic integrity check, but received a failed response to the Meets Device Integrity Verdict.

Ivanti EPMM Status	Description for SafetyNet	Description for PlayIntegrity
Fail	Ivanti EPMM received a response, but received failed responses to basic integrity and CTS profile. This status indicates that a device is uncertified.	Ivanti EPMM received a response, but received failed responses to basic integrity and CTS profile. This status indicates that a device is uncertified.
Unknown	<p>Either Ivanti Mobile@Work timed out waiting for results, or Ivanti EPMM did not receive results in the acceptable time interval.</p> <p>Examples of legitimate reasons for an Unknown state are when a user is in airplane mode or has lost network connectivity. Therefore, be cautious about the actions you assign to devices that display this status.</p>	<p>Either Ivanti Mobile@Work timed out waiting for results, or Ivanti EPMM did not receive results in the acceptable time interval.</p> <p>Examples of legitimate reasons for an Unknown state are when a user is in airplane mode or has lost network connectivity. Therefore, be cautious about the actions you assign to devices that display this status.</p>
Tampered Client	Ivanti EPMM received a response that Ivanti Mobile@Work is not valid, indicating the device has been tampered with.	Ivanti EPMM received a response that Ivanti Mobile@Work is not valid, indicating the device has been tampered with.
Error	Either an exception occurred when calling SafetyNet or there was some other error.	Either an exception occurred when calling PlayIntegrity or there was some other error.

Working with Windows Update policies

This feature is not supported on Android devices.

Working with Samsung Android kiosk policies



Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See ["Setting the kiosk policy for Android managed devices" on page 620](#).

See ["Samsung Android kiosk policy" on page 610](#) for information on configuring this policy.

Working with Android Quick Setup policies

The Android Quick Setup policy offers additional options for getting devices configured quickly:

- Optional Device Administrator role for Ivanti Mobile@Work
- Cache registration password for Exchange and Wi-Fi configuration.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Click **Add New > Android > Android Quick Setup**.
3. Use the following guidelines to complete the form:

Action	Example
Name	<p>Required. Enter a descriptive name for this policy. This is the text that will be displayed to identify this policy throughout the Admin Portal. This name must be unique within this policy type.</p> <p>Tip: Though using the same name for different policy types is allowed (e.g., Executive), consider keeping the names unique to ensure clearer log entries.</p>
Status	<p>Select Active to turn on this policy. Select Inactive to turn off this policy.</p> <p>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.</p>
Priority	<p>Specifies the priority of this custom policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is associated with a specific device.</p> <p>Select "Higher than" or "Lower than", then select an existing policy from the drop-down list. For example, to give "Policy A" a higher priority than Policy B, you would select "Higher than" and "Policy B".</p> <p>Because this priority applies only to custom policies, this field is not enabled when you create the first custom policy of a given type.</p>
Description	<p>Enter an explanation of the purpose of this policy.</p>

Action	Example
Policy Parameters	<p>Clear the Device Administrator option to complete registration without applying the Device Administrator role to the Ivanti Mobile@Work app. Clearing this option streamlines the registration process by eliminating the need for the device user to approve granting the Device Administrator role.</p> <p>Clearing the option also disables the following features on the device:</p> <ul style="list-style-type: none"> • Password requirements • Device encryption • Device lock/unlock • Wipe • Camera lock • Lockdown policies • Samsung Knox features • Samsung native email configuration • Samsung Knox container • Kiosk mode
Use registration password for	<p>Select the Exchange and/or Wi-Fi check box to cache the registration password on the device for use in configuring the Exchange and/or Wi-Fi settings.</p> <p>Selecting these options streamlines the configuration process if you are using LDAP for authentication as part of the registration and Exchange/Wi-Fi configuration processes.</p> <p>Note that the password is cached in memory only. Terminating the app drops the password from memory.</p>

4. Click **Save**.
5. Apply the policy to the appropriate labels (**Actions > Apply to Labels**).


Working with Samsung general policies

Use the Samsung general policy to manage Samsung Knox license keys on Samsung devices.

Upgrade Note: The Samsung Knox license key for Samsung Knox activation has been moved from the Samsung (Knox) Container policy (**Policies & Configs > Configurations**) to the Samsung General policy (**Policies & Configs > Policies**). If a license key is configured in the Container policy, then a new Samsung general policy is automatically created.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select **Add New > Android > Samsung General**.
3. Use the following guidelines to complete this form:

Item	Description
Name	Enter a unique name for the policy.
Status	Select Active to turn on this policy. Select Inactive to turn off this policy.
Priority	Select Higher than or Lower than, then select an existing policy from the drop-down list. If you have multiple policies, use the Priority setting to select which policy gets applied. See "Prioritizing policies" in <i>Getting Started with Ivanti EPMM</i> .
Description	Enter a description for the policy.
KNOX License Key	Enter the Samsung Knox license key <div> Important: Ivanti EPMM does not validate the Knox license key. If the license key is invalid, AppConnect apps on the device cannot be used.</div>
KNOX Device Attestation Enabled	To enable attestation, first select the "I understand" check box, then select Knox Device Attestation Enabled. See also: "Attestation support for Samsung Knox" on the next page
Audit Collection Controls	Select Enable to enable event logging to the device logs on Samsung Knox devices. See "Configuring audit collection controls for Samsung Knox devices" on page 206 .

4. Select **Save**.

Attestation support for Samsung Knox

It is possible for employees to use rooted Android devices with customized firmware. An enterprise can validate a device's integrity before it installs a Samsung Knox container on the device using the attestation feature.

The attestation feature requires Samsung Android devices that are attestation capable.

Attestation works by sending a challenge to the device to test its integrity. The device responds, and Ivanti EPMM returns its final verification. A device responds to the challenge in one of three ways:

- Correctly, resulting in attestation state of PASS
- Incorrectly, resulting in attestation state of FAIL
- No response, resulting in attestation state of UNKNOWN

A device without attestation support does not respond. A device that supports attestation may also not respond, for example, if it has no network connectivity, or if it was compromised and sends no response.

An attestation challenge is sent to a device when the device checks-in with Ivanti EPMM, but not more frequently than once per hour. The attestation result determines whether a Samsung Knox container is removed, installed, or left unchanged. Additional compliance actions triggered by an attestation fail can be defined in a security policy.



For all Samsung Android devices, whether or not they are attestation-capable, enabling attestation for the device removes a pre-existing Samsung Knox container from the device.

See ["Attestation behavior on the device" on page 205](#) for more details.

Configuring attestation on Ivanti EPMM

Before you begin

- You must have a Samsung Knox License Key to enable attestation.
- Samsung Android devices that support attestation are required to take advantage of this feature.

Recommendations

- For the best user experience, apply attestation to a new device deployment. If you enable attestation on a previously deployed device, any existing Samsung Knox container will be removed, and replaced only if the device passes the attestation challenge.

- Ivanti recommends enabling attestation in a homogeneous environment where all the devices are known to support attestation. For example, where all attestation-capable Samsung devices are corporate owned and assigned to an LDAP group.
- Ivanti strongly recommends against enabling attestation to groups of devices where attestation support is unknown or mixed.

Configuring attestation step-by-step

Follow these steps to enable attestation, create a related security policy with optional custom compliance actions, and assign the policy to devices.

Procedure

1. Create a label to use for attestation-related policies and devices:
 - a. Go to **Device & Users > Labels**.
 - b. Select **Add Label**. Name the label "Attestation Label", for example.
2. Enable attestation in the Samsung General Policy:
 - a. Go to **Policies & Configs > Policies**.
 - b. Select **Add New > Android > Samsung General**. The **New Samsung General Policy** dialog appears.
 - c. Enter the **Name**.
 - d. Enter the **Knox License Key**.
 - e. Read the **Caution** statement, and then select the "I understand" beneath it.
 - f. Select **Knox Device Attestation Enabled**.
 - g. Select **Save**.
3. Assign the Samsung General Policy to a label:
 - a. Select the policy.
 - b. Select **Actions > Apply to Label**.

- c. Select the desired label (for example, Attestation Label).
 - d. Select **Apply**.
4. Optionally, create a custom compliance action to use in the attestation security policy:
 - a. Go to **Policies & Configs > Compliance Actions**.
 - b. Select **Add**.
 - c. Select the actions to take if attestation fails.
 - d. Select **Save**.
5. Create a security policy to define the consequences when attestation fails:
 - a. Go to **Policies & Configs > Policies**.
 - b. Select **Add New > Security**. The **New Security Policy** dialog appears.
 - c. Enter a name. For example, "Attestation Security Policy".
 - d. Scroll down to **Access Control** and find the **For Android devices** section.
 - e. Select the check box for "**when Samsung Knox device attestation fails**".
 - f. Choose the compliance action from the drop-down. If you created a custom compliance action for attestation, it appears as one of the options.
 - g. Select **Save**.
6. Assign the Security Policy to a label:
 - a. Select the policy.
 - b. Select **Actions > Apply to Label**.
 - c. Select the desired label (for example, Attestation Label).
 - d. Select **Apply**.
7. Assign devices to the label with the attestation policies.
 - a. Go to **Device & Users > Devices**.
 - b. Select attestation-capable Samsung device(s).

- c. Select **Actions > Apply to Label**.
- d. Select the label with attestation policies (for example, Attestation Label).
- e. Select **Apply**.



WARNING: For all Android devices, Knox containers that were created before attestation is enabled are removed when the attestation policy is applied.

Attestation behavior on the device

A label that includes a Samsung Global Policy with the attestation feature enabled is applied to a device. Ivanti EPMM sends attestation challenges to the device periodically. The behavior of each device type is detailed below.



Applying attestation to non-attestation capable devices is not recommended.

Android devices that are not attestation-capable

- Attestation state is reported as UNKNOWN in Device Details in the Admin Portal.
- Attestation state will always be UNKNOWN because the device is incapable of responding to an attestation challenge.
- Any existing Samsung Knox container is removed from the device.
- No new Samsung Knox container is installed.

Android devices that are attestation-capable

An attestation-capable device will respond to the attestation challenge. A challenge result can be **PASS**, **FAIL**, or **UNKNOWN**.

If the attestation result is **PASS**:

- Attestation state is reported as PASS in Device Details in the Admin Portal.
- For a new device deployment, a Samsung Knox container is installed.
- For an existing device which has a Knox container that was installed before attestation was enabled:
 - Pre-attestation Knox container is removed.
 - New Knox container is installed.
- For a device that previously passed, the Knox container remains unchanged.

If the attestation result is **FAIL**:

- Attestation state is reported as FAIL in Device Details in the Admin Portal.
- Samsung Knox container is removed.
- Additional compliance actions are taken based on the security policy in effect for the device, triggered by the “when Samsung Knox device attestation fails” condition.

If there is no response, the attestation result is **UNKNOWN**:

- Attestation state is reported as UNKNOWN in Device Details in Ivanti EPMM.
- If the device has previously passed attestation, it continues to function as if it has passed. The Knox container remains unchanged.
- If the device has not ever passed attestation, then:
 - Any pre-attestation Knox container is removed.

Configuring audit collection controls for Samsung Knox devices

The Samsung General Policy provides audit collection control settings. These settings control what audit events are logged to the device logs on Samsung Knox devices based on an event’s severity, outcome, and audit group. These settings impact logs collected on the Samsung device: logs made by the Samsung platform, as well as logs made by Ivanti Mobile@Work .

You pull these device logs to Ivanti EPMM, and then can access them using the System Manager.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Policies**.
2. Select the Samsung General Policy that you are using.
3. Select **Edit**.
4. For **Audit Collection Controls**, select **Enable**.
5. For **Severity Rule**, select the severity level of events you want to collect. Only audit events of the chosen severity level or higher will be collected. For example, if you select **Error**, only **Error**, **Critical**, and **Alert** audit events will be collected. The severity levels are, from most severe to least severe, are:
 - Alert

- Critical
 - Error (the default)
 - Warning
 - Notice
6. For **Outcome Rule**, select whether you want to collect only events indicating success, events indicating failure, or all.
 7. For **Audit Groups**, select the groups of events you want to collect. Select one or more of **Security**, **System**, **Network**, **Events**, or **Application**. The default is that all of the groups are selected.
 8. If you selected **Events** in the **Audit Groups** field, the **Audit Events** field is enabled. The possible individual events in the **Events** group are displayed in the **Audit Events** drop-down. Select the individual events that you want to collect.
 9. In the **UID** section, select the + sign to add a UID. Each UID is an integer, defined by Samsung, for enabling Samsung-specific logging.
 10. Select **Save**.

Related topics

- ["Pull client logs for client devices" on page 516](#)

Working with Wear OS device policies

The Wear OS policy is used to send various Wear OS details to the server. If there isn't a policy in place or the watch app is not installed, then the Wear OS tab will not be displayed. If there is a policy and there are no watches paired to Ivanti Mobile@Work, the Wear OS tab does not display. If there is a policy and the watch is paired (via Bluetooth) to the phone but the watch app is not installed on the watch, then Wear OS tab will not display. Once the policy has been implemented, the device continues to report watch details and inventory even when the device is quarantined.



Ivanti Mobile@Work for Android (phone) receives Wear OS data from the Wear OS device (watch) and the Android system tends to cache this data for an unknown time frame. There is a possibility that the true value of the "Wear OS Client Installed" field in Device Details > Wear OS tab is delayed for several hours.

Procedure

1. Select **Policies & Configs > Policies**.
2. Select **Add New > Android > Wear OS policy**.
3. In the Add Wear OS Policy dialog box, use the guidelines to complete this form.
4. Select **Save**.
5. Apply the policy to a label.

TABLE 33. WEAR OS POLICY SETTINGS



Item	Description
Name	Enter a name for the Wear OS policy.
Status	<p>Select the relevant radio button to indicate whether the policy is Active or Inactive.</p> <p>You can have multiple active policies, and assign different labels to the various policies, but because only one policy is assigned to any given device, the highest-priority policy for a device is assigned.</p>
Priority	<p>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.</p> <p>Select Higher than or Lower than, then select an existing policy from the dropdown list.</p> <p>For example, to give Policy A higher priority than Policy B, you would select "Higher than" and "Policy B".</p>
Description	Enter an explanation of the purpose of this policy.
Collect Wear OS device details	<ul style="list-style-type: none"> • Enables (default) the collection of the device's Wear OS details to the server. • De-select to turn off the collection of Wear OS device details, including app inventory. <hr/> <p> If the "Collect Wear OS device details" and "Collect Wear OS application inventory" fields are both selected, the collection of both device inventory and app inventory will occur.</p> <hr/>
Collect Wear OS application inventory	<ul style="list-style-type: none"> • Select to enable the collection of Wear OS application inventory.

TABLE 33. WEAR OS POLICY SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none">De-select (default) to turn off the collection of Wear OS application inventory. Once this field is de-selected, old application inventory data will display in the Wear OS tab until the client explicitly sends a report to Ivanti EPMM with no application inventory details or updated inventory details. <hr/> <div> De-selecting this field will also de-select the "Collect Wear OS device details" field.</div>

Related topics

- ["Viewing paired watch information " on page 10](#)

Notifications of changes to the privacy policy

This feature is not available on Android devices.

Exporting the devices in the WatchList

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

Procedure

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

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

3. Click Export to export the list of devices.
4. The list is downloaded as .CSV file.

Managing Compliance

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 218
- "Compliance actions policy violations" on page 219
- "Viewing quarantine information" on page 227
- "Viewing configurations removed due to quarantine" on page 227
- "Custom compliance policies" on page 228

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.



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.



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 <ul style="list-style-type: none"> • 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
	<p>You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.</p> <p>The maximum number of characters allowed is 65,530.</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>
Remove Apps <ul style="list-style-type: none"> Android iOS <p>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.</p>	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 <ul style="list-style-type: none"> 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
<p>All Android Enterprise apps and functionality are hidden, except Downloads, Google Play Store, and Ivanti Mobile@Work.</p> <p>(Applicable only if the "Quarantine app when device is quarantined" check box is selected.)</p>					
<p>Quarantine All Except Wi-Fi</p> <ul style="list-style-type: none"> Android iOS macOS <p>(For Android Enterprise apps, this is applicable only if the "Quarantine app when device is quarantined" check box is selected.)</p>	Remove all configurations except for Wi-Fi.	Remove all configurations except for Wi-Fi when compromised.	Remove all configurations except for Wi-Fi when administrator privileges have been removed.	Remove all configurations except for Wi-Fi when the device has been decrypted.	Remove all configurations except for Wi-Fi when the OS version is less than expected.

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
Quarantine All Except Wi-Fi on Wi-Fi Only <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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.

TABLE 2. LOCAL COMPLIANCE CONDITIONS AND ACTIONS

Situation	OS	Action
When the device can communicate with Ivanti EPMM to perform a Compliance Check	Alert <ul style="list-style-type: none"> Android iOS 	<p>Send an alert when the device is out of contact.</p> <p>Alerts are sent to device users, admins, or both users and admins, using SMS, push notifications, or email.</p>
	Block AppConnect apps <ul style="list-style-type: none"> Android iOS 	Blocks access to AppConnect apps.
	Quarantine <ul style="list-style-type: none"> iOS <p>(Applicable only if the "Quarantine app when device is quarantined" check box is selected.)</p>	When the device is out of contact, all configurations, managed apps and iBooks content are removed. New app downloads are disallowed.
	Quarantine <ul style="list-style-type: none"> Android <p>(Applicable only if the "Quarantine app when device is quarantined" check box is selected.)</p>	When the device is out of contact, all configurations and managed apps are removed. New app downloads are disallowed.
	Quarantine <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Android iOS 	<p>Send an alert when the device is out of contact.</p> <p>Alerts are sent to device users, admins, or both users and admins, using SMS, push notifications, or email.</p>
	Block AppConnect apps <ul style="list-style-type: none"> Android iOS 	Blocks access to AppConnect apps.

Situation	OS	Action
	Quarantine <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Android Enterprise 	All Android Enterprise apps and functionality are hidden, except Downloads, Google settings, Google Play Store, and Ivanti Mobile@Work.
	Retire <ul style="list-style-type: none"> Android Enterprise 	The work profile is deleted or the managed device will be factory reset. <div>  This action is not reversible. </div>

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.



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

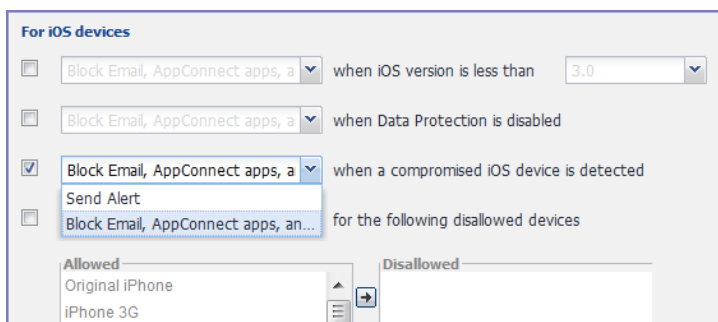
Tiered compliance behavior

- 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

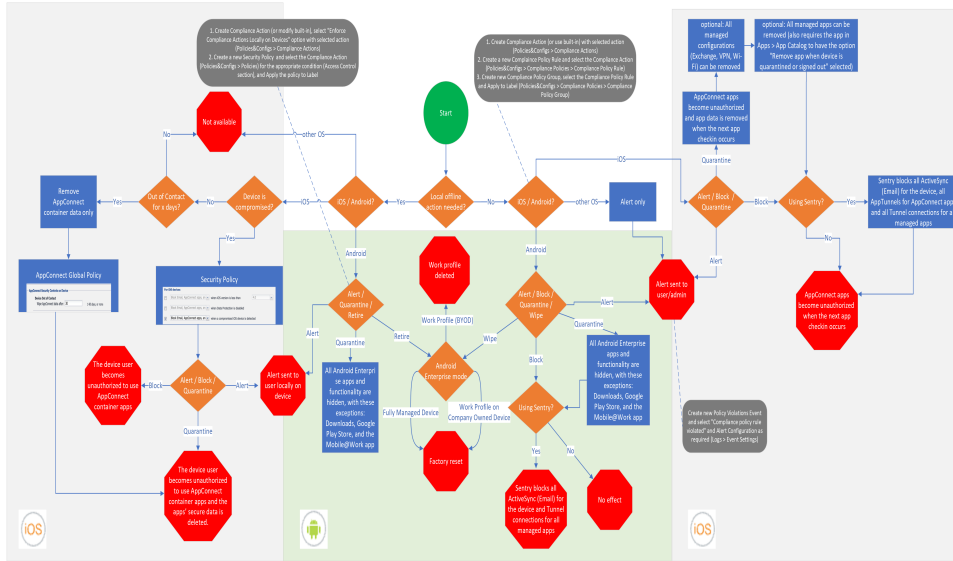
You can assign compliance actions for security policy violations and for compliance policy violations. When you configure access control in either type of policy, you can select default compliance actions that are provided with Ivanti EPMM. You can also select custom compliance actions that you create.

FIGURE 1. COMPLIANCE ACTIONS POLICY VIOLATIONS



To create the custom compliance actions, see ["Custom compliance actions" on page 221](#).

FIGURE 2. COMPLIANCE ACTION SETTINGS FOR IOS AND ANDROID DEVICES



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 34. 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 464 .
Block Email, AppConnect Apps And Send Alert	<ul style="list-style-type: none"> • 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 34. DEFAULT COMPLIANCE ACTIONS TABLE (CONT.)

Default compliance action	Description
	<p>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 <i>Ivanti Standalone Sentry Guide for EPMM</i>.</p> <ul style="list-style-type: none"> Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature. Unauthorizes AppConnect apps. 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

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

Creating a compliance action

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

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Compliance Actions**.
3. 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](#).



If you have selected **Show** for the **Custom ROM Related Functions** in **Settings > System Settings > Android > Android Custom ROM**, then the wipe action is available. To enable wipe, first read and select the caution statement. You can then select **Wipe the device**. The wipe option applies to Android devices only.

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).





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	<p>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.</p> <hr/> <p> Associated action is only applied for policy violations configured in a security policy.</p> <hr/>
ALERT: Send a compliance notification or alert to the user	<p>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 <i>Getting Started with Ivanti EPMM</i>.</p> <p>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 464.</p>
BLOCK ACCESS: Block email access and AppConnect apps	<p>Selecting this option has the following impact to the device:</p> <ul style="list-style-type: none"> Restricts access to email via ActiveSync if you are using a Standalone Sentry for email access. <hr/> <p> 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 <i>Ivanti Standalone Sentry Guide for EPMM</i>.</p> <hr/> <ul style="list-style-type: none"> Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature. <p>This action blocks tunnels that AppConnect apps and iOS managed apps use.</p>

Item	Description
	<ul style="list-style-type: none"> Unauthorizes AppConnect apps. <p>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.</p> <p>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.</p> <p>This action impacts AppConnect apps, as well as third-party AppConnect for Android apps.</p>
<p>QUARANTINE: Quarantine the device (Select this check box to display the other Quarantine options.)</p>	<p>Selecting this option has the following impact to the device:</p> <ul style="list-style-type: none"> Immediately blocks access to the web sites configured to use the standard and Advanced AppTunnel feature. <p>This action blocks tunnels that AppConnect apps use.</p> <ul style="list-style-type: none"> AppConnect apps are retired, which means they become unauthorized <i>and their secure data is deleted (wiped)</i>. <p>AppConnect apps become unauthorized <i>and their secure data is wiped</i> 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.</p> <p>AppConnect apps become unauthorized <i>and their data is wiped</i> 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.</p> <p>This action impacts AppConnect apps, as well as third-party AppConnect for Android apps.</p> <ul style="list-style-type: none"> For Android Enterprise devices, all Android Enterprise apps and functionality are hidden, with these exceptions: Downloads, Google Play Store, and the Ivanti Mobile@Work app. (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)

Item	Description
	<p> In the App Catalog, the individual setting configured on each app takes precedence over this quarantined action. If the app config setting associated with the individual (specific) app is not selected to "Quarantine app when device is quarantined", then the app will be quarantined when the user device is quarantined.</p>
<p>QUARANTINE: Remove All Configurations and SaaS Sign-on Policy</p>	<p>Select to remove the following configurations:</p> <ul style="list-style-type: none"> • Exchange • VPN • Wi-Fi • Ivanti Docs@Work <p>However, because of Android limitations, this action does not remove any certificates used in Certificate Enrollment, Certificate, and Wi-Fi configurations. These certificates are installed into the device's credential storage. Only the device user can remove them by using the Clear Credential Storage command in the Android Settings app on the device. Certificates used in Exchange and VPN configurations are removed because these certificates are stored in the respective apps.</p> <p>Also, certificates installed in a Samsung Knox device's credential store <i>are</i> removed.</p>
<p>QUARANTINE: Do not remove Wi-Fi settings for Wi-Fi only devices</p>	<p>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.</p>
<p>QUARANTINE: Do not remove Wi-Fi settings for all devices (iOS and Android only)</p>	<p>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.</p>
<p>QUARANTINE: Remove iBooks content, managed apps, and block new app downloads</p>	<p>Select this option to remove Managed Apps from the device and block access to Apps@Work when the device is not compliant. (Applicable only for Android Enterprise apps and only if the "Quarantine app when device is quarantined" check box in the App Catalog is selected.)</p>

Item	Description
Retire: Retire the Work profile or factory reset the managed device	<p>Select to trigger a local retire action on an Android Enterprise device. See the "Retiring an Android Enterprise device" section in the "Managing the Android Enterprise device life cycle" on page 68 topic for the specific actions that are taken. This selection protects work profile data from data leakage by retiring the work profile on a personal device or performing a factory reset on a managed device. These actions are performed only locally on the device by Ivanti Mobile@Work . Also, the Retire action is only visible when you select the Enforce Compliance Actions Locally on Devices check box and it is only available in tier 1.</p> <hr/> <p> WARNING - This action cannot be reversed.</p>
Wipe	<p>Retires the Work Profile or Factory resets the managed device.</p> <p>Select to trigger a local retire action on an Android Enterprise device. See the "Retiring an Android Enterprise device" section in the "Managing the Android Enterprise device life cycle" on page 68 topic for the specific actions that are taken. This selection protects work profile data from data leakage by retiring the work profile on a personal device or performing a factory reset on a managed device.</p>

When the compliance action takes effect

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

- Sync interval
- Time the device last checked in
- Battery level
- Number of changes already queued
- Whether **Enforce Compliance Actions Locally on Devices** is selected

Once the change reaches the device, 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 230](#)
- ["Managing compliance policy groups" on page 234](#)
- ["Device search fields for compliance rules" on page 238](#)

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.

Edit Roles - miadmin

Admin Roles

☐ Select all admin roles

► Device Management

► Privacy Control

► Label Management

► User Management

► App Management

► Configuration Management

► Policy Management

▼ Compliance Policy Management

☐ View compliance policy

☒ Modify compliance policy

☒ Apply and remove compliance policy labels

Selected Permissions

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

Available Permissions

Cancel Save

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 233](#)
- ["Deleting compliance policy rules" on page 234](#)
- ["Searching for compliance policy rules" on page 234](#)

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 97](#).



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	<p>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.</p> <ul style="list-style-type: none"> • \$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\$ <hr/> <p> For Shared iPad devices and User Enrolled devices only.</p> <hr/> <ul style="list-style-type: none"> • \$MI_APPSTORE_URL\$ • \$MODEL\$ • \$NULL\$ • \$OU\$ • \$PASSWORD\$ • \$PHONE_NUMBER\$

Category	Substitution variable
	<ul style="list-style-type: none">• \$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 page 236](#)

- ["Applying compliance policy groups to labels" on the next page](#)
- ["Removing compliance policy groups from labels" on the next page](#)
- ["Deleting compliance policy groups" on page 237](#)
- ["Searching for compliance policy groups" on page 237](#)

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 ["Creating compliance policy rules" on page 230](#) 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 35. 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

TABLE 35. DEVICE SEARCH FIELDS FOR COMPLIANCE RULES (CONT.)

Category	Compliance policy objects
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, PasscodesCompliantWithProfiles, PasscodesCompliant, Personal Hotspot Enabled, SerialNumber, Supervised, SIM MCC, SIM MNC, Subscriber Carrier Network, Voice Roaming Enabled, osUpdateStatus,
Windows	The following search fields are available for use in compliance rules for all Windows devices: dm_client_version, wp_firmware_version, wp_hardware_version, wp_os_edition, health_data_issued, health_data_aik_present, health_data_dep_policy, health_data_bit_locker_status, health_data_boot_manager_rev_list_version, health_data_code_integrity_rev_list_version, health_data_secure_boot_enabled, health_data_boot_debugging_enabled, health_data_os_kernel_debugging_enabled, health_data_code_integrity_enabled, health_data_test_signing_enabled, health_data_safe_mode, health_data_win_pe, health_data_elam_driver_loaded, health_data_vsm_enabled, health_data_pcr0, health_data_sbcp_hash,
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 36. 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.	<p>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.</p> <p>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.</p>
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 36. COMPLIANCE ACTIONS VERSIONS 1 & 2 (CONT.)

Compliance actions Version 1	Compliance actions Version 2
<p>After upgrading to Ivanti EPMM 11.8.0.0, <i>existing</i> V1 actions can be used. New V2 actions can also be used. New actions can only be created as V2 actions.</p> <p>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.</p>	<p>After upgrading/migrating to Ivanti EPMM 11.8.0.0, new actions can only be created as V2 actions.</p>
Supports templates in the event center.	<p>Templates</p> <p>Administrators can insert the following variables (that are exposed in the Insert Variable section) in the subject and message content:</p> <ul style="list-style-type: none"> • \$SEVERITY\$ - Localized, device's locale used. • \$USER_NAME\$
Supports templates in the event center.	<p>Templates</p> <p>Administrators can insert the following variables (that are exposed in the Insert Variable section) in the subject and message content:</p> <ul style="list-style-type: none"> • \$SEVERITY\$ - Localized, device's locale used. • \$USER_NAME\$
Existing behavior is unchanged.	<p>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.</p>

TABLE 36. 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 <code>Sendupto</code> 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 <code>Compliance Rule Violation Event</code> 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.

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" below](#)
- ["Configurations page " on the next page](#)
- ["Default configurations" on page 245](#)
- ["Displaying configurations status" on page 247](#)
- ["Adding new configurations" on page 248](#)
- ["Editing configurations" on page 249](#)
- ["Deleting configurations" on page 249](#)
- ["Exporting configurations" on page 249](#)
- ["Importing configurations" on page 250](#)
- ["Applying configurations to labels" on page 250](#)
- ["Android File Transfer Configurations" on page 251](#)
- ["Android Enhanced Multiple-Slicing Support" on page 256](#)
- ["Exporting the devices in the WatchList" on page 256](#)
- ["Impact of changing LDAP server variables" on page 257](#)

Management of device settings with configurations

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

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

TABLE 37. DEVICE SETTINGS

Category	Configuration Type
Android	<ul style="list-style-type: none"> • Android for Work • Samsung Browser • Samsung Kiosk <hr/> <p> Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead.</p> <hr/> <ul style="list-style-type: none"> • Samsung Knox Container <hr/> <p> Samsung Knox Container is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead.</p> <hr/>
Infrastructure	<ul style="list-style-type: none"> • Exchange • Email • Wi-Fi • VPN • Certificates • Certificate Enrollment
AppConnect	<ul style="list-style-type: none"> • App Configuration • Container Policy
Features	<ul style="list-style-type: none"> • Ivanti Docs@Work • Ivanti Web@Work

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 38. 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.
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 222 for information on quarantining devices.

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

Default configurations

TABLE 39. DEFAULT CONFIGURATIONS

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	

TABLE 39. DEFAULT CONFIGURATIONS (CONT.)


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	
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	<p>This SCEP setting is automatically created for the iOS Enterprise App Store certificate.</p> <hr/> <p> 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.</p> <hr/>	<p>iOS</p> <p>macOS</p> <p>tvOS</p>

TABLE 39. DEFAULT CONFIGURATIONS (CONT.)

System - iOS MDM	MDM	Default MDM profile for iOS MDM.	iOS tvOS
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 " 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

Displaying configurations status

To see the status of configurations for each device:

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

The statuses you will see are:

- **Pending:** The process of applying the settings has been started.
- **Sent:** The settings have been successfully sent to the device.
- **Applied:** Ivanti EPM has confirmed that the verifiable settings appear to have been applied to the device. Use the **View Details** button to see the verifiable results.
- **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. Use the **View Details** button to see the verifiable results.
- **Update Pending:** The administrator has edited the setting in the Admin Portal. The process of applying the updated setting has begun.

Click the **View Details** button to see information on each configuration.

Adding new configurations



Add new configurations through integration with selected devices and email apps plus Sentry and ActiveSync.

To add new configurations:

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

Editing configurations



Add new configurations through integration with selected devices and email apps plus Sentry and ActiveSync.

To edit configurations:

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

A pop-up displays.

5. Click **Yes** to continue.

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

Deleting configurations



Add new configurations for Android devices through integration with selected devices and email apps plus Sentry and ActiveSync.

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.

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

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.

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**.

Android File Transfer Configurations

As part of Android 11, Google made significant changes in storage access on device from apps, which also impacted how enterprises manage sending files to specific apps on these devices.

With these changes in mind, many large enterprises face challenges in distributing files to devices and apps as devices are upgrading to Android 11 and beyond.

Any approach that is dependent on specific APIs from hardware vendors limits enterprises in having the same approach across different devices from different manufacturers and OS versions.

Ivanti developed a file transfer solution that is agnostic of Android version and hardware vendor. This solution relies on Android's standard Content-Provider capability. Content-Provider allows the Ivanti Mobile@Work app to generate a unique on-device location for each file pushed via UEM.

The File Transfer Configuration is available for Android devices in Fully Managed device modes. Using this configuration, the administrator can provide an option to transfer files on the device to be shared between different allowed apps present on the same device. Other apps can use the files for whatever reason needed. An example use case is initializing app configuration using JavaScript or displaying corporate information using PDFs or videos.

Every file uploaded into Ivanti's File Transfer configurations is downloaded by Ivanti Mobile@Work when it receives the corresponding config and associated file. The file is securely stored within Ivanti Mobile@Work's app sandbox.

Other apps can not access this file arbitrarily.

Every downloaded file inside the app sandbox is reference by a unique location, also referred to as ContentURI or URI.

Custom Attributes are used to hold the ContentURI value on the server for every file on a device and can help administrators determine a file's availability on device, form dynamic device groups and are required to communicate ContentURI to target app using managed app config, etc.



IMPORTANT: For non-Ivanti apps, administrators should check with third-party app developers on their support for this approach that is commonly referred to as "Consuming FileProvider based ContentURI."

Procedure

1. Go to **Policies & Configs > Configurations**.
2. Select **Add New > Android > File Transfer**. The Create File Transfer Configuration dialog box opens.
3. Enter a name for the configuration in the **Name** box.
4. Enter a **Description** of the configuration.
5. In the **File to Transfer** section, select the **Upload** button and choose the file. By default, the maximum limit of a file size is 50 MB.
6. Select one or more of the following **Download to device options** (optional):
 - **Allow download over metered Network** - Select to continue downloading the file even on a metered network
 - **Require Charging** - Select to make sure that the device is charging during the file transfer process
 - **Require Device Idle** - Select to keep the device idle during the file transfer process

In the **Share file with other app(s)** section, you can use either "[Transfer using Android Managed App Config](#)" below or "[Transfer using On-device Intent](#)" on page 254 options.

Transfer using Android Managed App Config

Use this option only if the target app can consume Content URI using its Managed App Config.

Configuring the File transfer config

1. In the **Add a new device based custom attribute to store file's device URI** field, enter a new custom attribute name, for example, **Custom-File-name**.



The custom attribute name should be a new, unique attribute solely used for this file transfer operation.

2. **Provide access to the following apps and/or Package Names:** You can select app names from the App Names selector and add Package Names.
 - **App Names** - You can select app names from the App names selector.
 - **Package Names** - You can enter the Bundle IDs in this area, for example, `com.mobileiron.filetransfer.android3`. Separate multiple package names with semicolons(;).
3. Select **Save**. The new File Transfer configuration displays in the Configurations page.

Configuring the target app

1. Go to **Apps > App Catalog**.
2. Select the target app that will receive the file.
3. Select the **Edit** option for this app.
4. Create a new configuration or use an existing configuration.
5. An app may have a setting such as "Manifest Info." For Ivanti Velocity app as an example, in the App Configuration dialog box > **Fetch Configurations > Manifest Info** field, enter the substitution variable defined in Step 1 of "[Configuring the File transfer config](#)" above for example, `$Custom-File-Name$`.
6. Select **Add** (if adding a new configuration) and then select **Save**.
7. Select your labels and save the settings for the app.

Verifying file download status

Custom Attributes are used to hold the location (ContentURI) value on the server for every file on each device and can help administrators determine a file's availability on the device.

1. Go to **Device & Users > Devices**.
2. Select a specific device the File Transfer configuration was deployed to.
3. In the Device Details page, select the device and then select **Actions > Force Device check-in**.

4. In the **Configurations** tab, check that the File Transfer configuration displays with the status of Applied.
5. In the **Custom Attributes** tab, check that the name of the new custom attribute displays (for example, "deviceIntent") with its related value. This provides the information about the storage location of the file on the device and showcases that file has been locally downloaded to the device available within the Ivanti Mobile@Work app sandbox.
6. Transferring/Sharing of file with other apps can only be verified by collecting logs from the target app or from the device.

Transfer using On-device Intent

Intents are app-specific. To share a file using this option, see the target app's documentation and provide information in the intents section below. Intents allow Ivanti Mobile@Work app to broadcast a message on the device once the file is available to be shared to the apps.

Working with File Transfer config

1. In the **Add a new device based custom attribute to store file's device URI** field, enter a new custom attribute name, for example, **deviceIntentURI**.



Custom Attributes are used to hold the location (URI / ContentURI) value on the server for every device and can help administrators determine a file's availability on device.

2. In the **Provide access to specific app or package name** field, enter the **App Name** or the **Package Name**, for example, Velocity.

3. In the **Intents-Standard** section:
 - a. **Operation Type** - From the drop-down list, select **Start Activity / Start Service** or other similar choice as per the app. Choose the right value for this field depending on the target app's developer guidance.
 - b. **Class Name** - (optional) Choose the right value for this field depending on the target app's developer guidance.
 - c. **Action** - Set the action to: `com.wavelink.nameofapp.action.INSTALL_CONFIG` or similar, as per the app.
 - d. **Category** - Enter values separated by a semicolon (;).
 - e. **Mime Type** - (optional) In the administrator's host server, the custom.mobileconfig file should be set with a MIME type of application/configuration so that the MDM profile for the device is downloaded and installed on the device. Choose the right value for this field depending on the target app's developer guidance.
 - f. **Flags** - (optional) Select the number of flags to be used. Choose the right value for this field depending on the target app's developer guidance.
4. Provide the **Intents-Extras** values under KEY, TYPE, and VALUE (optional.) For more specific parameters, see the OEM app documentation. Choose the right value for this field depending on the target app's developer guidance.
5. Click **Save**.
6. In the Configurations page, select the new File Transfer Configuration and then select **Actions > Apply to Label**. The Apply To Label dialog box opens.
7. Choose a suitable label and then select **Apply**.

Verifying file download status


Custom Attributes are used to hold the location (ContentURI) value on the server for every file on each device and can help administrators determine a file's availability on the device.

1. Go to **Device & Users > Devices**.
2. Select a specific device the File Transfer configuration was deployed to.
3. In the Device Details page, select the device and then select **Actions > Force Device check-in**.
4. In the **Configurations** tab, check that the File Transfer configuration displays with the status of Applied.
5. In the **Custom Attributes** tab, check that the name of the new custom attribute displays (for example, "deviceIntent") with its related value. This provides the information about the storage location of the file on the device and showcases that file has been locally downloaded to the device and is available within the Ivanti Mobile@Work app sandbox.


6. Transferring/Sharing of file with other apps can only be verified by collecting logs from the target app or from the device.

Android Enhanced Multiple-Slicing Support

Preferential Network Service on Android 13 allows admins to define fine network slices on a 5G network and map different UIDs (apps) to each slice.

 Ensure that the 5G slicing option is enabled in Lockdown policy to use these configurations.

To create a configuration, select **Configurations > Add New > Android > Enhanced Network Slicing**.

Label	Description
Name	Enter a name that identifies this configuration
Description	Enter a description that clarifies the purpose of this configuration.
App Catalog Apps	You can either search from Apps that available in the app catalog which contain public, private, and in-house apps or you can manually add apps using the package id. You can assign a slice to an app from the drop-down menu in the app catalog.
Enhanced Slice	<div>Displays app that was assigned in the respective slice.</div> <div> An application can use only one slice. Use the Enable automatic fallback to ensure that the application can use an alternative network in case of failure.</div>

 Ivanti Mobile Network Client currently does not support Network Slicing.

You can also edit an existing configuration.

Exporting the devices in the WatchList

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

Procedure

1. In the 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

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 265](#)
- ["Synchronizing Google account data" on page 266](#)
- ["Setting up Gmail with Android Enterprise" on page 272](#)

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 Android:

The Exchange configuration works:

- Through Sentry and ActiveSync
- With Samsung Knox devices running the Samsung native email app and the Android versions listed in the *Ivanti Mobile@Work for Android*.

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.

Samsung exchange support was deprecated by Samsung starting from Android 9.0.

Android Enterprise email clients are configured using AppConnect app configurations. See ["Setting up Gmail with Android Enterprise" on page 272](#).

The following table describes the Exchange settings you can specify.

TABLE 40. EXCHANGE SETTINGS


Section	Field Name	Description
<i>General</i>	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	<p>Enter the address of the ActiveSync server.</p> <p>If you are using Standalone Sentry, do the following:</p> <ul style="list-style-type: none"> • 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. <p>When using Integrated Sentry, set the server address to Microsoft Exchange Server's address.</p> <hr/> <div>  <p>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.</p> </div> <hr/> <p>For more information about configuring Sentry, see the Ivanti Standalone Sentry Guide for EPM.</p>

TABLE 40. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	Use SSL	Select to use secure connections. SSL is always used, regardless of whether this setting is selected.
	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	<p>This check box only appears if you have configured a Google account with Ivanti EPMM.</p> <p>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.</p> <p>When selected, Ivanti EPMM grays out the ActiveSync User Name and ActiveSync User Password.</p> <p>This check box only appears if you have configured a Google account with Ivanti EPMM, as described in "Synchronizing Google account data" on page 266.</p>
	ActiveSync User Name	<p>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.</p> <p>You can also specify custom formats, such as \$USERID\$_US. Custom attribute variable substitutions are supported.</p> <p>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.</p>
	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\$.

TABLE 40. EXCHANGE SETTINGS (CONT.)


Section	Field Name	Description
		<p>\$MANAGED_APPLE_ID\$ can be used for Shared iPad devices and User Enrolled devices only.</p> <p>You can also specify custom formats, such as \$USERID\$_US. Custom attribute variable substitutions are supported.</p> <p>Typically, you use \$EMAIL\$ in this field; you cannot use \$NULL\$.</p>
	ActiveSync User Password	<p>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.</p> <p>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.</p> <hr/> <p> 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.</p> <hr/>
	Identity Certificate	Select the Certificate Enrollment entry you created for supporting Exchange ActiveSync, if you are implementing certificate-based authentication.

TABLE 40. EXCHANGE SETTINGS (CONT.)


Section	Field Name	Description
		<p>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.</p> <p> 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.</p>
	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.
	Items to Synchronize (iOS)	This feature is not supported on Android devices.
	Past Days of Email to Sync	<p>Specify the maximum amount of email to synchronize each time by selecting an option from the drop-down list.</p> <p>This setting works only with these email apps:</p> <ul style="list-style-type: none"> • Samsung Knox devices' native email app (NOTE: Samsung exchange support was deprecated by Samsung starting from Android 9.0.) • Ivanti Email+
	Move/Forward Messages to Other Email Accounts	This feature is not supported for Android devices.
<i>S/MIME</i>	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.
<i>S/MIME Signing</i>		

TABLE 40. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	S/MIME Signing: Enable	This feature is not supported for Android devices.
	S/MIME Signing identity	This feature is not supported for Android devices.
	Signing Identity: User Overrideable	This feature is not supported for Android devices.
	S/MIME Signing: User Overrideable	This feature is not supported for Android devices.
<i>S/MIME Encryption</i>		
	Encryption by Default	This feature is not supported for Android devices.
	Encryption Identity	This feature is not supported for Android devices.
	Encryption Identity: User Overrideable	This feature is not supported for Android devices.
	Encryption by Default: User Overrideable	This feature is not supported for Android devices.
	Per-Message Encryption Switch	This feature is not supported for Android devices.
<i>ActiveSync</i>		Limited support for Android.
	Sync during	
	Peak Time	Select the preferred synchronization approach for peak times. This feature is not supported for Android devices.
	Off-peak Time	Select the preferred synchronization approach for off-peak times. This feature is not supported for Android devices.
	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.

TABLE 40. EXCHANGE SETTINGS (CONT.)


Section	Field Name	Description
	End Time	Specify the end of the peak period for all peak days.
iOS 5 and Later Settings		These features are not supported for Android devices.
Android		
	Exchange App Priority	<p>Drag and drop email configurations to specify which are allowed. Change the order of selected configurations to specify priority.</p> <p>If there are no email apps specified in the Selected column, then Ivanti Mobile@Work uses the following provisioning priority:</p> <ol style="list-style-type: none"> 1. Ivanti Email+ for Android (AppConnect-enabled) 2. Ivanti Email+ for Android 3. Native email app
General		
	Accept all SSL certificates: Enable	<p>Enables device users to set Android devices to accept all SSL certificates. This setting applies to Ivanti Email+ for Android and Samsung Knox email and is intended for use when the Sentry uses self-signed certificates.</p> <hr/> <p> Use caution when enabling this setting, as device users might unknowingly expose the device to attack.</p> <hr/>
	Copy/Paste: Enable	Prevents use of the copy and paste commands in Ivanti Email+ for Android.
	Allow access to secure info from outside container	<p>Specify whether to publish contacts and calendar items to non-secure email clients running on the same device.</p> <p>For Secure Ivanti Email+ for Android, you can allow access to both contacts and calendar.</p>
	NitroDesk TouchDown	Enter the license key.
Samsung SAFE (Knox)	Supported on all Samsung Knox devices	

TABLE 40. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	NOTE: Samsung Knox Workspace support was deprecated by Samsung starting from Android 10.0.	
	HTML Email : Allow	Select this option to allow viewing of HTML email. This option is not enabled by default, which prevents rendering of HTML-based email.
	SmartCard Authentication: Enable	This feature is not supported.
	<i>Windows 10 Desktop</i>	This feature is not supported for Android devices.

Multiple Exchange Support for Android

Multiple Exchange mailboxes are supported for devices running Android versions no earlier than 4.0 or Samsung Knox 4.0 devices, using either Ivanti Email+ for Android or Samsung Native Email client apps. For Samsung Native Email client, Certificate Enrollment is not supported as the authentication method with multiple mailboxes.

The Ivanti EPMM administrator can configure and apply up to two Exchange settings for each device. Exchange settings are found in the Admin Portal under **Policies & Configs > Configurations**. When it receives the configuration, the device must be running Ivanti Mobile@Work version 6.0 or supported newer versions.

On the device, both mailboxes appear in a single email app. The email app is determined by 1) the email app's priority as specified in the Exchange Setting's **Exchange App Priority**, and 2) the email app's availability on the device. For example, if both Samsung Native Email and Ivanti Email+ are available on the device, the app with the highest priority is used.



Ivanti Mobile@Work 's **Options > Email Status** is not supported for multiple Exchange accounts.

Configuring POP and IMAP email settings (for iOS and macOS)

This feature is not supported for Android devices.

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 268](#)
- ["Setting up your Exchange setting for access to Google Apps data" on page 269](#)
- ["Renewing the Google Apps password for a given set of users" on page 271 \(optional\)](#)

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 file 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 266](#).

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**.

Google Apps API

- 1 Download the Public and Private key pair as a JSON file from Google Developers Console.
- 2 Use your Google Apps domain admin account to enable API access and allow OAuth for your domain.
- 3 Enter your Google Apps admin username below, and upload the JSON file you downloaded in Step 1

Google Admin Username:

JSON File:
 Browse...

Save

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.



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 271](#).

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
<i>General</i>	
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	<p>Enter the address of the mail server, such as m.google.com.</p> <p>If you are using Standalone Sentry, do the following:</p> <ul style="list-style-type: none"> • 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. <p>For more information about configuring Sentry, see the <i>Ivanti Standalone Sentry Guide for EPMM</i>.</p>
Use SSL	<p>Select to use secure connections.</p> <hr/> <p> You must use SSL to link to Google Apps.</p> <hr/> <p>SSL is always used, regardless of whether this setting is selected.</p>

Item	Description
Google Apps Password	<p>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.</p> <p>When selected, Ivanti EPMM grays out the ActiveSync User Name and ActiveSync User Password.</p> <p>This check box only appears if you have configured a Google account with Ivanti EPMM, as described in "Synchronizing Google account data" on page 266.</p>
ActiveSync User Email	<p>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\$.</p> <p>\$MANAGED_APPLE_ID\$ can be used for Shared iPad devices and User Enrolled devices only.</p> <p>You can also specify custom formats, such as \$USERID\$_US. Custom attribute variable substitutions are supported.</p> <p>Typically, you use \$EMAIL\$ in this field.</p>
Items to Synchronize	Select the items you want to synchronize with Google Apps: Contacts, Calendar, Email, Tasks.

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**.

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 EPMM sends the old password to the device. 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**.

Setting up Gmail with Android Enterprise

You can deploy Gmail to Android Enterprise devices if you have set up Ivanti EPMM for Android Enterprise.



If you want to set up Ivanti Email+ with Android Enterprise, please see *Ivanti Email+ for Android Guide*.


Add Gmail to the App Catalog on Ivanti EPMM as you would any Android Enterprise app. In the Admin Portal, in **Apps > App Catalog**, add Gmail from Google Play. When adding it, be sure to select **Install this app for Android enterprise**.

When you add the Gmail app, its app configurations are displayed in the **Configuration Choices** section. Edit these choices according to the following table:

TABLE 41. GMAIL CONFIGURATION PARAMETERS

Settings	Description
Email Address	<p>Enter substitution variables to define the email address.</p> <p>Typically, you enter \$EMAIL\$.</p> <p>You can also enter combinations of these variables, depending on your ActiveSync server requirements:</p> <p>\$USERID\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$</p>
Hostname or Host	<p>Enter the host name of the mail server to use. Enter the fully qualified domain name of the Exchange server or the Standalone Sentry you are using.</p>

TABLE 41. GMAIL CONFIGURATION PARAMETERS (CONT.)

Settings	Description
Username	Use variables to define the username for the email account.
SSL Required	Select if you want secure communication using https: to the server that you specified for Exchange host.
Trust all certificates	Select only if you want the app to automatically accept untrusted certificates. Use this option only for debugging or development when working in a test environment.
Login certificate alias	<p>Enter the alias for the login certificate. The value should be a string alias representing a certificate with private key stored in the work profile keystore. For example: \$CERT_ALIAS:<certificate config name>\$</p> <hr/> <div>  <p>When a certificate alias is used with a password, Gmail does not send the certificate alias to the server and an "Unable to connect to server" error is displayed. This is a Google issue.</p> </div> <hr/>
Default email signature	\$USERID\$
Default sync window	Use the Default sync window drop-down menu to select an interval in minutes for the device to sync with app or data updates.

Related topics

- ["Setting up Ivanti EPM for Android Enterprise" on page 12](#)
- "Deploying public Android Enterprise apps" in the *Ivanti EPM Apps@Work Guide*

Managing Wi-Fi Settings

This section addresses the Wi-Fi settings.

- ["Wi-Fi settings" below](#)
- ["Wi-Fi profiles and password caching" on page 277](#)
- ["Wi-Fi network priority for Android devices" on page 277](#)
- ["Using Wi-Fi priority values" on page 281](#)
- ["How an Android device chooses its Wi-Fi network" on page 282](#)
- ["Wi-Fi network manual override behavior" on page 283](#)
- ["Wi-Fi authentication types" on page 284](#)

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 284](#).



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.

See additional information relating to specific Android versions:

- ["Android 13 devices" on the next page](#)
- ["Android 10 devices" on page 276](#)

Android 13 devices

MAC Address Randomization

On Android 13 devices or supported newer versions, upon installation or upgrade, the administrator can enable or disable the MAC Address Randomization for the Wi-Fi configuration. If the MAC Address Randomization is not selected (default setting state after Ivanti EPMM upgrade), the randomization type is not pushed; the Wi-Fi and Inventory MAC Address are the same for a device.

In the Device Details page > **Inventory MAC Address** field states the phone's MAC address. The same occurs in the Android device > MAC address type, it will also state the phone's MAC address.

Applicable to Wi-Fi configurations for all authentication types in:

- Work Managed Device (DO) mode
- Work Profile (PO) mode
- Work Profile on Company Owned Device (EPO) mode
- Work Managed Device Non-GMS (AOSP) mode

Procedure

1. Go to **Policies & Configs > Configurations**.
2. Add **New > Wi-Fi Configuration**. The New Wi-Fi Setting dialog box opens.
3. Under Android Settings, the **MAC Address Randomization** check box is deselected by default. This means the Wi-Fi configuration will be used. Select the check box and then select from the drop-down:
 - **Disabled** (default) - Use the factory MAC address when connecting to this network.
 - **Enabled - Auto** - Let the Wi-Fi framework automatically decide the MAC randomization strategy.
 - **Enabled - Non-persistent** - Use a randomly-generated MAC address for connections to this network. This option does not persist the randomized MAC address.
 - **Enabled - Persistent** - Generate a randomized MAC address and reuse it for all connections to this network.
4. Select **Save**.

When set, the information displays in the "Android MAC Address Randomization" field in the Wi-Fi configuration.

Android 10 devices

On Android 10 devices or supported newer versions, upon installation or upgrade, device users can configure Wi-Fi and location settings in specific modes.



Administrators are required to leave in all modes of deployment to enable Wi-Fi and MTD configurations to be successfully applied. This means having the Allow the user to turn on location sharing lockdown field selected (checked.)

The table below depicts the behavior changes in different configuration modes:

TABLE 42. WI-FI CHANGES IN SPECIFIC CONFIGURATION MODES

Item	Description
All modes	Disconnect Wi-Fi local action is disabled in all modes on Android 10 devices. For all modes of deployment, to enable Wi-Fi and MTD configurations to be successfully applied, the Allow the user to turn on location sharing lockdown field must be selected.
(Android Enterprise) <ul style="list-style-type: none"> • Work Profile mode • Work Profile on Company Owned devices (Android 11 or supported newer versions) 	Device users are requested to activate location for the device and for the managed profile. In order for administrators to update Wi-Fi and to have Mobile Threat Defense detect Wi-Fi-based threats, device users must activate location. If the device user chooses No, the device will be flagged with an unblocking error for non-compliance and Ivanti EPMM will report a configuration error. Administrators will not be able to disable Wi-Fi through UEM configurations in Work managed device mode on Android 10 devices.
(Android Enterprise) <ul style="list-style-type: none"> • Work Managed Device (COPE) mode 	In the background, Ivanti EPMM will turn on the location services setting without device user intervention. Wi-Fi and MTD configurations should be successful with no errors. If there is no MTD configuration or a Wi-Fi configuration, the device user can switch location service on or off.
Device Administrator (DA) mode	Wi-Fi configurations will not be supported and will show as Sent on the server with config error. MTD configurations will be still accepted for non-network threats but the Wi-Fi related threats will not work for Device Administrators and MAM. Administrators will not be able to disable Wi-Fi through UEM configurations in Device Administrator mode on Android 10 devices.
Kiosk mode	Administrators wanting users to enable/disable Wi-Fi but not connect to any other Wi-Fi network settings are not supported. Options available to administrators are:

TABLE 42. WI-FI CHANGES IN SPECIFIC CONFIGURATION MODES (CONT.)

Item	Description
	<p>Scenario 1 - Administrators wanting users to enable/disable Wi-Fi and connect to any available Wi-Fi will need to have the following settings in Kiosk mode: Lockdown settings: Allow Wi-Fi (de-selected) and Allow Wi-Fi to be configured (de-selected). Kiosk Mode Settings: Allow users to Access Wi-Fi Settings (selected).</p> <p>Scenario 2 - Administrators wanting to block users from any Wi-Fi controls will need to have the following Lockdown settings:</p> <ul style="list-style-type: none"> - Allow Wi-Fi (selected) - Allow Wi-Fi to be configured (selected).

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 network priority for Android devices



Wi-Fi priority values do not work with Android devices from version 8 and higher.

Within the Ivanti EPMM user interface, you set the Wi-Fi network priority for Android devices in two places in the user interface. First, set the Lockdown policy option for Android Wi-Fi devices, then you can set the Wi-Fi configuration. The Lockdown policy option "**Always Connect Device to Managed Wi-Fi**" ensures that Android devices pro-actively connect to the highest priority managed Wi-Fi network in range. By enabling this field in the Lockdown policy and using Wi-Fi priority settings, administrators can control which Wi-Fi network a device connects to. In addition, the Wi-Fi network configuration settings allow you specify a direct or automatic Wi-Fi connection to a Wi-Fi proxy setting, increasing the network security of your Wi-Fi devices. Both the Wi-Fi network priority and the **Always Connect Device to Managed Wi-Fi** lockdown policy option apply to *all* Android devices.

With **Always Connect Device to Managed Wi-Fi**:

- **ENABLED**: an Android device will always connect to the highest priority managed Wi-Fi network available, actively disconnecting from any unmanaged networks.

- The Wi-Fi Priority value you set provides a preference for the highest priority network if multiple managed networks are available.
- The connection to the managed Wi-Fi network is maintained as long as the signal is in range, even if a managed Wi-Fi network with a higher priority becomes available.
- Exception: a newly received Wi-Fi configuration goes into effect after the current Wi-Fi connection disconnects.
- **DISABLED:** an Android device will connect to the highest priority Wi-Fi network as determined by Android.

CAUTION: When enabling **Always Connect Device to Managed Wi-Fi** in the Lockdown policy, because the device will actively connect to managed Wi-Fi SSID with the highest priority, if there is an error in the Wi-Fi configuration it is possible for the device to lose Wi-Fi access.



When **Always Connect Device to Managed Wi-Fi** is enabled and a managed Wi-Fi network is in range, the user cannot override the Wi-Fi connection choice and cannot choose to connect to an unmanaged network.

Setting up enforced Wi-Fi network priority

First, set up the Lockdown policy to enable **Always Connect Device to Managed Wi-Fi** and apply the policy to the device.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select **Add New > Lockdown**.
3. In the New Lockdown Policy dialog box, enter a **Name**.
4. Scroll down to the Android section. For **Always Connect Device to Managed Wi-Fi**, select **Enable**.
5. Fill out the rest of the Lockdown policy as needed.
6. Select **Save**.
7. Apply the policy to a label to assign it to the appropriate Android devices.

Next, provide values for network priority settings for all Wi-Fi configurations. From this menu, you can select a direct or automatic proxy server as well as specific servers to exclude.

In the Admin Portal:

1. Go to **Policies & Configs > Configurations**.
2. Select an existing **Wi-Fi** configuration, and select **Edit** in the right-side panel.
3. Locate the **Android Settings** section in the dialog box.
4. For **Priority**, enter a number between 1 (lowest priority) and 100 (highest priority), inclusive, or leave it blank (default priority).



Devices use the priority that is provided when the Wi-Fi configuration is provisioned. Future changes to the priority value are not sent to the device.

5. Select an optional **Proxy Type** that is supported on Android 8.0 or supported newer versions. Use the drop-down menu to select from the following options:

- a. **None**: This is the default value, indicating that no proxy server is specified.
- b. **Direct**: Select to specify a direct connection to a proxy server. After you make this selection, the menu expands and the following fields are displayed:

Host Exclusions List: Select + to enter one or more domains of traffic that will not be proxied. This setting applies to the URL traffic, but it does not apply to the proxy server.

Proxy Server: Enter the host name or IP address of a proxy server.

Proxy Port: Specify a proxy server port.

- c. **Auto**: Select to specify an automatic connection to the proxy server. After you make this selection, the following field is displayed:

PAC URL: Enter the proxy auto-config (PAC) URL of the Wi-Fi proxy server. The PAC URL provides a mapping of URLs that the software uses to locate the proxy server automatically.

6. Select **Save**.

The Wi-Fi configuration is now pushed to *all* devices that have the configuration's labels applied. The Priority designation applies to both newly provisioned and previously provisioned network settings.

7. Apply the Wi-Fi configurations to a label to assign them to the appropriate devices.

When the Wi-Fi configuration and the Lockdown policy as described are applied to a device, the highest priority Wi-Fi network is enforced.

Android 10 specific Wi-Fi settings

On Android 10 devices or supported newer versions, upon installation or upgrade, device users can configure Wi-Fi and location settings in specific modes.

Note the following:

- For all modes of deployment, to enable Wi-Fi and MTD configurations to be successfully applied, the Allow the user to turn on location sharing lockdown field must be selected.
- Administrators will not be able to disable Wi-Fi through UEM configurations in Work managed device mode and Device Administrator mode on Android 10 devices.
- Administrators are required to leave in all modes of deployment to enable Wi-Fi and MTD configurations to be successfully applied.

Wi-Fi configuration now requires end users to allow location services on the device. The behavior changes in different configuration modes and is documented in the table below.

TABLE 43. ANDROID 10 WI-FI SETTINGS


Item	Description
(Android Enterprise) Work Profile mode	Device users are requested to activate location for the device and for the Managed Profile. In order for administrators to update Wi-Fi and to have Mobile Threat Defense detect Wi-Fi-based threats, device users must activate location. If the device user chooses No, the device will be flagged with an unblocking error for non-compliance and Ivanti EPMM will report a configuration error.
(Android Enterprise) <ul style="list-style-type: none"> • Work Managed Device mode • Managed Device with Work Profile (COPE) 	In the background, Ivanti EPMM will programmatically turn on the location services setting without device user intervention. Wi-Fi and MTD configurations should be successful with no errors. <div>  If there is no MTD configuration or a Wi-Fi configuration, the device user can switch location service on or off. </div>
Device Administrator (DA) Mode	Wi-Fi configurations will not be supported and will show as Sent on the server with config error. MTD configurations will be still accepted for non-network threats but the Wi-Fi related threats will not work for Device Administrators and MAM.

TABLE 43. ANDROID 10 Wi-Fi SETTINGS (CONT.)

Item	Description
Kiosk Mode	<p>Administrators wanting users to enable/disable Wi-Fi but not connect to any other Wi-Fi network settings are not supported. Options available to administrators are:</p> <ul style="list-style-type: none">• Scenario 1: Administrators wanting users to enable/disable Wi-Fi and connect to any available Wi-Fi will need to have the below settings in Kiosk.<ul style="list-style-type: none">◦ Lockdown settings > Allow Wi-Fi (de-selected)◦ Lockdown settings > Allow Wi-Fi to be configured (de-selected)◦ Kiosk Mode Settings > Allow users to Access Wi-Fi Settings (selected)• Scenario 2: Administrators wanting to block users from any Wi-Fi controls.<ul style="list-style-type: none">◦ Lockdown Settings > Allow Wi-Fi (selected)◦ Lockdown Settings > Allow Wi-Fi to be configured (selected)

Using Wi-Fi priority values

Administrators can use the Wi-Fi priority feature to influence the network connections that devices make. The table below describes how to set Wi-Fi priorities to achieve the noted results.



Wi-Fi priority values do not work with Android devices from version 8 and later releases.

TABLE 44. WI-FI PRIORITY VALUES

Desired outcome	Settings required
Allow any Wi-Fi connection, equally	(This is the default state.) For Always Connect Device to Managed Wi-Fi in Lockdown policy: Disable For Wi-Fi configuration: The Priority field is ignored
Ensure that managed Wi-Fi networks always get priority over non-managed networks; actively disconnect from unmanaged networks when a managed network is available. Do not allow users to override the Wi-Fi connection choice with an unmanaged network.	For Always Connect Device to Managed Wi-Fi in Lockdown policy: Enable For Wi-Fi configuration: set the Priority field for each Wi-Fi configuration. 1 = lowest, 100 = highest.

How an Android device chooses its Wi-Fi network

If a device has multiple Wi-Fi networks configured, then it will automatically connect to an SSID in the following priority order, assuming a signal is available:

1. A managed SSID with the highest priority as set by the administrator (if **Always Connect Device to Managed Wi-Fi** is enabled.)
2. An unmanaged SSID, (or a managed SSID if **Always Connect Device to Managed Wi-Fi** is disabled) as chosen by the Android operating system.

When multiple Wi-Fi networks have the same priority, the Android operating system typically prioritizes the most recently used SSID.

When the device receives a new highest-priority Wi-Fi configuration, the configuration takes effect after the current Wi-Fi connection is ended for any reason.

When multiple Wi-Fi signals become available

In Ivanti Mobile@Work with the Lockdown policy setting **Always Connect Device to Managed Wi-Fi** set to **Enable**, an existing unmanaged Wi-Fi connection is pro-actively disconnected if a managed SSID signal comes into range.

For example, if a user connects to an unmanaged network, and walks into range of one or more managed networks, the device disconnects from the unmanaged network and connects to the highest-priority managed network.

With the Lockdown policy setting **Always Connect Device to Managed Wi-Fi** set to Disable, Wi-Fi connections are not actively disconnected. The next time the Wi-Fi connection is reestablished, Android will automatically choose the highest priority network.

Wi-Fi network manual override behavior

A user’s ability to manually choose a Wi-Fi network depends on the **Always Connect Device to Managed Wi-Fi** setting in the Lockdown policy, as shown in the table.

TABLE 45. WI-FI NETWORK MANUAL OVERRIDE BEHAVIOR

Lockdown Policy Setting	Wi-Fi SSID manual override behavior
Always Connect Device to Managed Wi-Fi: Disable	A user can select and override a Wi-Fi SSID connection by connecting manually.
For Always Connect Device to Managed Wi-Fi: Enable	<p>A user can attempt to select an SSID by connecting manually, however, if at any time a higher priority network is in range, the device disconnects from an unmanaged network and connects to the highest priority managed network.</p> <p>If the user manually connects to a managed network, the connection is maintained even if a higher priority managed network comes into range.</p>

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 287](#)
- ["WPA Enterprise authentication" on page 290](#)
- ["WPA2 / WPA3 Enterprise authentication" on page 292](#)
- ["WPA Personal authentication" on page 295](#)
- ["WPA2 / WPA3 Personal authentication" on page 297](#)
- ["Supported variables for Wi-Fi authentication" on page 299](#)

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 46. 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	Select the data encryption method associated with the selected authentication type. The selection affects which of the following fields are displayed. For Open authentication, the following encryption options are available: <ul style="list-style-type: none">• Disabled

TABLE 46. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	<ul style="list-style-type: none"> • WEP
Network Key	<p>WEP encryption</p> <p>Enter the network key necessary for accessing this network. The network key should be 5 or 13 ASCII characters or 10 or 26 hexadecimal digits.</p>
Key Index	<p>WEP encryption</p> <p>If using multiple network keys, select a number indicating the memory position of the correct encryption key.</p>
Confirm Network Key	Re-enter the network key to confirm.
User Name	<p>WEP Enterprise encryption</p> <p>Specify the variable to use as the user name when establishing the Wi-Fi connection. See "Supported variables for Wi-Fi authentication" on page 299</p>
Password	<p>WEP Enterprise encryption</p> <p>Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is \$PASSWORD\$.</p> <p>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 EPMU administrator.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • 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. <p>See "Supported variables for Wi-Fi authentication" on page 299.</p>
Apply to Certificates	<p>WEP Enterprise encryption</p> <p>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.</p>

TABLE 46. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
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: <ul style="list-style-type: none"> • PEAP • TLS • TTLS <p>You must select only one protocol.</p> <p>If you select EAP-FAST, then you also need to specify the Protected Access Credential (PAC).</p> <p>If you select TLS, then you must specify an Identity Certificate.</p> <p>If you select TTLS, then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity, which on Android devices is propagated to the Anonymous Identity field in the Android system Wi-Fi settings.</p>
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Android devices.
Windows Settings	These features are not supported on Android devices.

Related topics

- ["Shared authentication" on the next page](#)
- ["WPA Enterprise authentication" on page 290](#)

- ["WPA2 / WPA3 Enterprise authentication" on page 292](#)
- ["WPA Personal authentication" on page 295](#)
- ["WPA2 / WPA3 Personal authentication" on page 297](#)
- ["Supported variables for Wi-Fi authentication" on page 299](#)

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 47. 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	Select the data encryption method associated with the selected authentication type. The selection affects which of the following fields are displayed. For Shared authentication, the following encryption options are available: <ul style="list-style-type: none">• Disabled• WEP
Network Key	WEP encryption Enter the network key necessary for accessing this network. The network key should be 5 or 13 ASCII characters or 10 or 26 hexadecimal digits.
Key Index	WEP encryption If using multiple network keys, select a number indicating the memory position of the correct encryption key.

TABLE 47. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Confirm Network Key	Re-enter the network key to confirm.
User Name	WEP Enterprise encryption Specify the variable to use as the user name when establishing the Wi-Fi connection. See "Supported variables for Wi-Fi authentication" on page 299 .
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: <ul style="list-style-type: none"> 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 299 .
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 47. WI-FI SHARED 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: <ul style="list-style-type: none"> • PEAP • TLS • TTLS <p>You must select only one protocol.</p> <p>If you select EAP-FAST, then you also need to specify the Protected Access Credential (PAC).</p> <p>If you select TLS, then you must specify an Identity Certificate.</p> <p>If you select TTLS, then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity, which on Android devices is propagated to the Anonymous Identity field in the Android system Wi-Fi settings.</p>
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Android devices.
Android Settings	See "Wi-Fi network priority for Android devices" on page 277 .
Windows Settings	These settings apply only to Windows devices.

Related topics

- ["Open authentication" on page 284](#)
- ["WPA Enterprise authentication" on the next page](#)
- ["WPA2 / WPA3 Enterprise authentication" on page 292](#)
- ["WPA Personal authentication" on page 295](#)
- ["WPA2 / WPA3 Personal authentication" on page 297](#)
- ["Supported variables for Wi-Fi authentication" on page 299](#)

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 48. 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	<p>Select the data encryption method associated with the selected authentication type. For WPA Enterprise authentication, the following encryption options are available:</p> <ul style="list-style-type: none"> • AES • TKIP
User Name	Specify the variable to use as the user name when establishing the Wi-Fi connection. See "Supported variables for Wi-Fi authentication" on page 299
Password	<p>Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is \$PASSWORD\$.</p> <p>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.</p> <hr/> <p> If you specify \$PASSWORD\$, also enable Save User Password under Settings > System Settings > Users & Devices > Registration.</p> <hr/>

TABLE 48. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS (CONT.)


Item	Description
	<p> 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.</p> <p>See "Supported variables for Wi-Fi authentication" on page 299</p>
Apply to Certificates	<p>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.</p> <p>If you configure multiple certificates, either as root certificates in separate files, or chain certificates in a single file, they appear in the CA cert drop-down on the client, however, "unspecified" is the selected value for the certificate.</p>
Trusted Certificate Names	<p>This feature is not supported on Android devices.</p> <p>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.</p>
Allow Trust Exceptions	<p>This feature is not supported on Android devices.</p> <p>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.</p>
Use Per-connection Password	<p>This feature is not supported on Android devices.</p> <p>Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.</p>
EAP Type	<p>Select the authentication protocol used:</p> <ul style="list-style-type: none"> • PEAP • TLS • TTLS <p>You must select only one protocol.</p> <p>If you select EAP-FAST, then you also need to specify the Protected Access Credential (PAC).</p>

TABLE 48. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	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, which on Android devices is propagated to the Anonymous Identity field in the Android system Wi-Fi settings.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Android devices.
Android Settings	See "Wi-Fi network priority for Android devices" on page 277 .
Windows Settings	These settings apply only to Windows devices.

Related topics

- ["Open authentication" on page 284](#)
- ["Shared authentication" on page 287](#)
- ["WPA2 / WPA3 Enterprise authentication" below](#)
- ["WPA Personal authentication" on page 295](#)
- ["WPA2 / WPA3 Personal authentication" on page 297](#)
- ["Supported variables for Wi-Fi authentication" on page 299](#)

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 49. 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	<p>Select one:</p> <ul style="list-style-type: none"> WPA2 Enterprise WPA2 Enterprise (iOS 8 or later except Apple TV) WPA3 Enterprise (iOS 13 or later)
Data Encryption	<p>Select the data encryption method associated with the selected authentication type. For WPA2 Enterprise authentication, the following encryption options are available:</p> <ul style="list-style-type: none"> AES TKIP
User Name	Specify the variable to use as the user name when establishing the Wi-Fi connection. See "WPA2 / WPA3 Enterprise authentication" on the previous page .
Password	<p>Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is \$PASSWORD\$.</p> <p>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.</p> <hr/> <p> If you specify \$PASSWORD\$, also enable Save User Password under Settings > System Settings > Users & Devices > Registration.</p> <hr/> <p> 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.</p> <hr/>

TABLE 49. WI-FI WPA2 / WPA3 ENTERPRISE AUTHENTICATION FIELD DESCRIPTION (CONT.)

Item	Description
Apply to Certificates	<p>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.</p> <p>If you configure multiple certificates, either as root certificates in separate files, or chain certificates in a single file, they appear in the CA cert drop-down on the client, however, "unspecified" is the selected value for the certificate.</p>
Trusted Certificate Names	This feature is not supported on Android devices.
Allow Trust Exceptions	This feature is not supported on Android devices.
Use Per-connection Password	This feature is not supported on Android devices.
EAP Type	<p>Select the authentication protocol used:</p> <ul style="list-style-type: none"> • PEAP • TLS • TTLS <p>You must select only one protocol.</p> <p>If you select EAP-FAST, then you also need to specify the Protected Access Credential (PAC).</p> <p>If you select TLS, then you must specify an Identity Certificate.</p> <p>If you select TTLS, then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity, which on Android devices is propagated to the Anonymous Identity field in the Android system Wi-Fi settings.</p>
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Android devices.
Android Settings	See " Wi-Fi network priority for Android devices " on page 277.
Windows Settings	These settings apply only to Windows devices.

Related topics

- ["Open authentication" on page 284](#)
- ["Shared authentication" on page 287](#)
- ["WPA Enterprise authentication" on page 290](#)
- ["WPA Personal authentication" below](#)
- ["WPA2 / WPA3 Personal authentication" on page 297](#)
- ["Supported variables for Wi-Fi authentication" on page 299](#)

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 50. 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	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: <ul style="list-style-type: none">• AES• TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.

TABLE 50. WI-FI WPA PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Confirm Network Key	Re-enter the network key to confirm.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Android devices.
Android Settings	See "Wi-Fi network priority for Android devices" on page 277.
Windows Settings	These settings apply only to Windows devices.

WPA2 Personal authentication

Use the following guidelines to configure WPA2 Personal authentication.

TABLE 51. 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	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: <ul style="list-style-type: none">• AES• TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.
Confirm Network Key	Re-enter the network key to confirm.

TABLE 51. WI-FI WPA2 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
EAP Type	Not applicable.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Android devices.
Android Settings	See "Wi-Fi network priority for Android devices" on page 277.
Windows Settings	These settings apply only to Windows devices.

Related topics

- ["Open authentication" on page 284](#)
- ["Shared authentication" on page 287](#)
- ["WPA Enterprise authentication" on page 290](#)
- ["WPA2 / WPA3 Enterprise authentication" on page 292](#)
- ["WPA2 / WPA3 Personal authentication" below](#)
- ["Supported variables for Wi-Fi authentication" on page 299](#)

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 52. 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.

TABLE 52. Wi-Fi WPA2 / WPA3 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select one: <ul style="list-style-type: none">• WPA2 Personal• WPA3 Personal (iOS 13 or later)
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: <ul style="list-style-type: none">• AES• TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.
Confirm Network Key	Re-enter the network key to confirm.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Android devices.
Android Settings	See "Wi-Fi network priority for Android devices" on page 277 .
Windows Settings	These settings apply only to Windows devices.

Related topics

- ["Open authentication" on page 284](#)
- ["Shared authentication" on page 287](#)
- ["WPA Enterprise authentication" on page 290](#)
- ["WPA2 / WPA3 Enterprise authentication" on page 292](#)
- ["WPA Personal authentication" on page 295](#)
- ["Supported variables for Wi-Fi authentication" on the next page](#)

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 284](#)
- ["Shared authentication" on page 287](#)
- ["WPA Personal authentication" on page 295](#)
- ["WPA2 / WPA3 Personal authentication" on page 297](#)
- ["WPA Enterprise authentication" on page 290](#)
- ["WPA2 / WPA3 Enterprise authentication" on page 292](#)

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](#)
- ["Cisco Legacy AnyConnect" on the next page](#)
- ["F5 SSL" on page 310](#)
- ["Juniper SSL" on page 317](#)
- [Tunnel \(Android\)](#)
- ["Tunnel \(Samsung Knox Workspace\)" on page 325](#)
- ["OpenVPN" on page 326](#)
- ["Palo Alto Networks GlobalProtect" on page 328](#)
- ["PPTP" on page 334](#)
- ["Pulse Secure SSL" on page 339](#)
- [Knox VPN Support](#)
- [Samsung Knox IPsec](#)
- [SonicWall Mobile Connect](#)

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.

You determine how the user obtains the VPN client app. You can, for example, add the app as a Google Play Store app to the App Catalog. See "Managing Mobile Apps for Android" in the *Ivanti EPMM Apps@Work Guide*.

If the device has a VPN already set on the device before installing the VPN client app, Ivanti Mobile@Work displays an error message. The message instructs the device user to install the VPN client app before setting the VPN connection setting.

- 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.



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.

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.



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.

Cisco Legacy AnyConnect

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

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

- Per-app inside the Knox container
- Per-app outside the Knox container
- Per-container (Knox)

- Per-device (Knox)
- Per-device (Android)

Use the following guidelines to configure Cisco Legacy AnyConnect VPN.

- ["Proxy - None \(default\)" below](#)
- ["Proxy - Manual " on page 304](#)
- ["Proxy - Automatic" on page 307](#)

Within these selections, you may make settings for:

- ["Custom Data" on page 310](#) (does not apply to Android devices)

Proxy - None (default)

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

TABLE 53. 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: <ul style="list-style-type: none">• 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	When selecting this option, a Samsung Knox license is required. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data. This option is available only if you select the Samsung Knox option. See:

TABLE 53. PROXY - NONE SETTINGS (CONT.)



Item	Description
	<ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351 "Configuring VPN modes when VPN client is inside the Knox container" on page 358
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 307 .
Username	<p>Specify the user name to use. The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$ \$USERID\$_ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> Password - see next row for information. Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:

TABLE 53. PROXY - NONE SETTINGS (CONT.)

Item	Description
	<p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Group Name	Specify the name of the group to use.
VPN On Demand	If the Samsung Knox and per-App VPN fields are both selected, then select this option to use VPN On Demand.
Per-App VPN	<p>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.</p> <p>You can enable per-app VPN for an app when you:</p> <ul style="list-style-type: none"> • Add the app in the App Catalog. • Edit an in-house app or an App Store app in the App Catalog. <hr/> <p> 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.</p> <hr/> <p>See the <i>Ivanti EPMM Apps@Work Guide</i> for information about how to add or edit apps.</p>
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" on page 310](#).

Proxy - Manual

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

TABLE 54. 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.

TABLE 54. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Channel	<p>For macOS only. Select one of the following distribution options:</p> <ul style="list-style-type: none"> • 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	<p>When selecting this option, a Samsung Knox license is required.</p> <p>A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device.</p> <p>This setting is ignored on non-Android devices.</p>
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p> <p>See:</p> <ul style="list-style-type: none"> • "Configuring VPN modes when VPN client is outside the Knox container" on page 351 • "Configuring VPN modes when VPN client is inside the Knox container" on page 358
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	<p>Enter the port number for the proxy server.</p> <p>Type - Select Static or Variable for the type of authentication to be used for the proxy server.</p>
Proxy Server User Name	<p>If the authentication type is Static, enter the user name for the proxy server.</p> <p>If the authentication type is Variable, the default variable selected is \$USERID\$.</p>
Proxy Server Password	If the authentication type is Static , enter the password for the proxy server. Confirm the password in the field below.

TABLE 54. PROXY - MANUAL SETTINGS (CONT.)



Item	Description
	If the authentication type is Variable , the default variable selected is \$PASSWORD\$.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	<p>Specify the user name to use. The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>

TABLE 54. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Group Name	Specify the name of the group to use.
VPN on Demand	If the Samsung Knox and per-App VPN fields are both selected, then select this option to use VPN On Demand.
Per-App VPN	<p>Select Yes to create a per-app VPN setting.</p> <p>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.</p> <p>You can enable per-app VPN for an app when you:</p> <ul style="list-style-type: none"> • Add the app in the App Catalog. • Edit an in-house app or an App Store app in the App Catalog. <hr/> <p> 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.</p> <hr/> <p>See the <i>Ivanti EPMM Apps@Work Guide</i> for information about how to add or edit iOS apps.</p>
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" on page 310](#).

Proxy - Automatic

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


TABLE 55. 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	<p>For macOS only. Select one of the following distribution options:</p> <ul style="list-style-type: none"> • Device channel - the configuration is effective for all users on a device. This is the typical option.

TABLE 55. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select Cisco Legacy AnyConnect .
Samsung Knox	<p>When selecting this option, a Samsung Knox license is required.</p> <p>A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device.</p> <p>This setting is ignored on non-Android devices.</p>
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p> <p>See:</p> <ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351 "Configuring VPN modes when VPN client is inside the Knox container" on page 358
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy Server URL	<p>Enter the URL for the proxy server.</p> <p>Enter the URL of the location of the proxy auto-configuration file.</p>
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$ \$USERID\$_ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>
User Authentication	Select the user authentication to use:

TABLE 55. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL:\$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Group Name	Specify the name of the group to use.
VPN On Demand	If the Samsung Knox and per-App VPN fields are both selected, then select this option to use VPN On Demand.
Per-App VPN	<p>Select Yes to create a per-app VPN setting.</p> <p>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.</p> <p>You can enable per-app VPN for an app when you:</p> <ul style="list-style-type: none"> • Add the app in the App Catalog. • Edit an in-house app or an App Store app in the App Catalog. <hr/> <p> 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.</p> <hr/> <p>See the <i>Ivanti EPMM Apps@Work Guide</i> for information about how to add or edit iOS apps.</p>
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" on the next page.](#)

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, , 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 \(default\)" below](#)
- ["Proxy - Manual " on page 312](#)
- ["Proxy - Automatic" on page 315](#)

Within these selections, you may make settings for:

- ["Custom Data" on page 317](#)

Proxy - None (default)

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

TABLE 56. 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: <ul style="list-style-type: none">• 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 .

TABLE 56. PROXY - NONE SETTINGS (CONT.)


Item	Description
Samsung Knox	<p>When selecting this option, a Samsung Knox license is required.</p> <p>A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device.</p> <p>This setting is ignored on non-Android devices.</p>
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p> <p>See:</p> <ul style="list-style-type: none"> • "Configuring VPN modes when VPN client is outside the Knox container" on page 351 • "Configuring VPN modes when VPN client is inside the Knox container" on page 358
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 315 .
Username	<p>Specify the user name to use. The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$ _ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	Select the user authentication to use:

TABLE 56. PROXY - NONE SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL:\$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
VPN On Demand	If the Samsung Knox and per-App VPN fields are both selected, then select this option to use VPN On Demand.
Per-App VPN	When selecting this option, a Samsung Knox license is required.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" on page 317](#).

Proxy - Manual

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


TABLE 57. 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 57. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> • 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	<p>When selecting this option, a Samsung Knox license is required.</p> <p>A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device.</p> <p>This setting is ignored on non-Android devices.</p>
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p> <p>See:</p> <ul style="list-style-type: none"> • "Configuring VPN modes when VPN client is outside the Knox container" on page 351 • "Configuring VPN modes when VPN client is inside the Knox container" on page 358
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select Manual . For an Automatic proxy, see "Proxy - Automatic" on page 315 .
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	<p>Enter the port number for the proxy server.</p> <p>Type - Select Static or Variable for the type of authentication to be used for the proxy server.</p>
Proxy Server User Name	<p>If the authentication type is Static, enter the user name for the proxy server.</p> <p>If the authentication type is Variable, the default variable selected is \$USERID\$.</p>
Proxy Server Password	<p>If the authentication type is Static, enter the password for the proxy server. Confirm the password in the field below.</p> <p>If the authentication type is Variable, the default variable selected is \$PASSWORD\$.</p>

TABLE 57. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	<p>Specify the user name to use. The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Per-App VPN	When selecting this option, a Samsung Knox license is required.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" on page 317.](#)

Proxy - Automatic

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

TABLE 58. 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: <ul style="list-style-type: none"> 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	When selecting this option, a Samsung Knox license is required. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data. This option is available only if you select the Samsung Knox option. See: <ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351 "Configuring VPN modes when VPN client is inside the Knox container" on page 358
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select Automatic . For a manual proxy, see "Proxy - Manual " on page 312
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Specify the user name to use (required.) The default value is \$USERID\$. Include at least one of the following variables:

TABLE 58. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	<p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
VPN On Demand	<p>This setting does not apply to Windows devices.</p> <p>If the Samsung Knox and per-App VPN fields are both selected, then select this option to use VPN On Demand.</p>
Per-App VPN	When selecting this option, a Samsung Knox license is required.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" on the next page.](#)

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.

Juniper SSL

This VPN connection type is supported on iOS, macOS, Android and Windows devices.



Ivanti, Inc recommends that you use Pulse Secure SSL instead of Juniper SSL.

The Juniper SSL VPN type supports Juniper SSL VPN definitions created in previous versions of Ivanti EPM. Juniper SSL VPN definitions are routed to the Pulse Secure VPN client. Use the type for new VPN definitions.

Use the following guidelines to configure Juniper SSL VPN.

- ["Proxy - None \(default\)" below](#)
- ["Proxy - Manual " on page 320](#)
- ["Proxy - Automatic" on page 322](#)

Within these selections, you may make settings for:

- ["Custom Data" on page 325](#)

Proxy - None (default)

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

TABLE 59. 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: <ul style="list-style-type: none">• Device channel - the configuration is effective for all users on a device. This is the typical option.

TABLE 59. PROXY - NONE SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select Juniper SSL .
Samsung Knox	<p>Select this option to use per-app VPN (either inside or outside the Knox Workspace) or per-container VPN. A Samsung Knox license is required.</p> <p>A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device.</p> <p>This setting is ignored on non-Android devices.</p>
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p> <p>See:</p> <ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351 "Knox VPN Support" on page 348
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	None is the default setting. Proxy is not supported on Android devices.
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$ \$USERID\$_ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>

TABLE 59. PROXY - NONE SETTINGS (CONT.)



Item	Description
	 Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> Password - see next row for information. Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	<p>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\$</p> <p>You can use combinations such as \$EMAIL:\$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Role	Specify the Juniper user role to use as a restriction.
Realm	Specify the Juniper realm to use as a restriction.
VPN On Demand	On-Demand VPN is supported for Android only if the Samsung Knox and Per-app VPN checkboxes are selected. On Demand VPN for Android means that the Juniper SSL VPN connection is activated only when an app associated with it is launched. When all apps associated with this VPN connection type are stopped, VPN is disconnected.
Per-app VPN	<p>Select Yes to create a per-app VPN setting. An additional license may be required for this feature.</p> <p>The Provider Type field displays.</p> <p>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.</p> <p>You can enable per-app VPN for an app when you:</p> <ul style="list-style-type: none"> add the app in the App Catalog. edit an in-house app or an App Store app in the App Catalog.

TABLE 59. PROXY - NONE SETTINGS (CONT.)

Item	Description
	<p> 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.</p> <p>See the <i>Ivanti EPMM Apps@Work Guide</i> for information about how to add or edit apps.</p>
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" on page 325](#).

Proxy - Manual

Use the following guidelines to configure a Juniper SSL VPN with a manual proxy.

TABLE 60. 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	<p>For macOS only. Select one of the following distribution options:</p> <ul style="list-style-type: none"> • 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	<p>Select this option to use per-app VPN (either inside or outside the Knox Workspace) or per-container VPN. A Samsung Knox license is required.</p> <p>A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device.</p> <p>This setting is ignored on non-Android devices.</p>
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p>

TABLE 60. PROXY - MANUAL SETTINGS (CONT.)


Item	Description
	<p>See:</p> <ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351 "Knox VPN Support" on page 348
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Proxy is not supported on Android devices.
Proxy Server	This setting is not supported on Android devices.
Proxy Server Port	This setting is not supported on Android devices.
Type	This setting is not supported on Android devices.
Proxy Server User Name	This setting is not supported on Android devices.
Proxy Server Password	This setting is not supported on Android devices.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$ \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> Password - see next row for information.

TABLE 60. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL:\$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Role	Specify the Juniper user role to use as a restriction.
Realm	Specify the Juniper realm to use as a restriction.
VPN On Demand	On-Demand VPN is supported for Android only if the Samsung Knox and Per-app VPN checkboxes are selected. On Demand VPN for Android means that the Juniper SSL VPN connection is activated only when an app associated with it is launched. When all apps associated with this VPN connection type are stopped, VPN is disconnected.
Per-app VPN	
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" on page 325](#).

Proxy - Automatic

Use the following guidelines to configure a Juniper SSL VPN with an automatic proxy.

TABLE 61. 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:

TABLE 61. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> 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	<p>Select this option to use per-app VPN (either inside or outside the Knox Workspace) or per-container VPN. A Samsung Knox license is required.</p> <p>A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device.</p> <p>This setting is ignored on non-Android devices.</p>
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p> <p>See:</p> <ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351 "Knox VPN Support" on page 348
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Proxy is not supported on Android devices.
Proxy Server URL	This setting is not supported on Android devices.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$

TABLE 61. PROXY - AUTOMATIC SETTINGS (CONT.)



Item	Description
	<ul style="list-style-type: none"> • \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Role	Specify the Juniper user role to use as a restriction.
Realm	Specify the Juniper realm to use as a restriction.
VPN On Demand	On-Demand VPN is supported for Android only if the Samsung Knox and Per-app VPN checkboxes are selected. On Demand VPN for Android means that the Juniper SSL VPN connection is activated only when an app associated with it is launched. When all apps associated with this VPN connection type are stopped, VPN is disconnected.
Per-app VPN	<p>Select Yes to create a per-app VPN setting. An additional license may be required for this feature.</p> <p>The Provider Type field displays.</p> <p>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.</p> <p>You can enable per-app VPN for an app when you:</p>

TABLE 61. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> add the app in the App Catalog. edit an in-house app or an App Store app in the App Catalog. <hr/> <p> 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.</p> <hr/> <p>See the <i>Ivanti EPMM Apps@Work Guide</i> for information about how to add or edit apps.</p>
Provider Type	This setting applies to iOS and macOS devices only.

Continue to ["Custom Data" below](#).

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.

Tunnel (Android)

Use this setting to configure Tunnel VPN for Android. For information on how to set up and configure Tunnel VPN for Tunnel for Android, see the *Ivanti Tunnel for Android Guide* on the [Ivanti Product Documentation page](#). These instructions also include how to configure VPN chaining with Tunnel. VPN chaining is the nesting of a VPN tunnel in another VPN tunnel for added security.

Tunnel (Samsung Knox Workspace)

This VPN connection type is supported on Android devices only.

Use this setting to configure Tunnel VPN for Samsung Knox Workspace. For information on how to set up and configure Tunnel VPN for Tunnel for Samsung Knox, see the *Ivanti Tunnel for Android Guide* on the [Ivanti Product Documentation page](#). These instructions also include how to configure VPN chaining with Tunnel. VPN chaining is the nesting of a VPN tunnel in another VPN tunnel for added security.

OpenVPN

This VPN connection type is supported on Android devices.



With Samsung Android 10 and above devices, OpenVPN support has been deprecated by Samsung.

Use the OpenVPN connection type to configure Samsung "OpenVPN net.openvpn.knox.connect" for Samsung Knox devices. This configuration is available only to limited customers as approved by Samsung.

Contact Samsung to get the correct OpenVPN package. It is supported only on devices with the Samsung Knox option selected in the VPN setting.

Open VPN is NOT supported with a third-party Open VPN vendor that is not Samsung.

Open VPN is supported with Samsung Knox without using VPN chaining.

Use the following guidelines to configure OpenVPN:

TABLE 62. OPENVPN 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: <ul style="list-style-type: none">• 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 OpenVPN . Only fields relevant to OpenVPN are displayed.
Samsung Knox	Always select this option. A Samsung Knox license is required. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.

TABLE 62. OPENVPN SETTINGS (CONT.)


Item	Description
	<p>This option is available only if you select the Samsung Knox option.</p> <p>See "Configuring VPN modes when VPN client is outside the Knox container" on page 351</p>
Package Name	Provide the Android package name of the OpenVPN client app: net.openvpn.knox.connect
Server	Enter the IP address, hostname or URL for the VPN server.
Username	<p>Specify the user name to use. The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	<p>Click the radio button for Password or Certificate to specify user authentication type.</p> <p>If you select Password, specify the password to use. The default value is \$PASSWORD\$. You can specify a custom format, for example, \$PASSWORD\$_\$USERID\$. Other password formats available are:</p> <p>If you select Certificate, specify Password, and then provide the two other settings added to the page:</p> <ul style="list-style-type: none"> • Identity Certificate (required): Enter the identity certificate number. • CA Certificate (optional): Select the CA Certificate from the list of available certificates.

TABLE 62. OPENVPN 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 Chaining	Select Enable to set up VPN chaining with Tunnel VPN. See "Configuring VPN chaining" in <i>Ivanti Tunnel for Android Guide</i> .
Per-app VPN	When selecting this option, a Samsung Knox license is required.
Proxy Server Port	Enter the port number for the connection. (Required)
Protocol	Select from drop-down.
Cipher	Select from drop-down.
Packet Auth Digest	Select from drop-down.

Palo Alto Networks GlobalProtect

This VPN connection type is supported on iOS 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 331](#)
- ["Proxy - Automatic" on page 332](#)

Proxy - None (default)

Use the following guidelines to configure a Palo Alto Networks GlobalProtect VPN without a proxy.

TABLE 63. 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: <ul style="list-style-type: none"> 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 331 or " Proxy - Automatic " on page 332.
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$ \$USERID\$_ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> Password - see next row for information. Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>

TABLE 63. PROXY - NONE SETTINGS (CONT.)

Item	Description
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
VPN On Demand	<p>This setting applies to iOS and macOS devices only. Select to enable VPN On Demand.</p> <p>The "Palo Alto Networks GlobalProtect" on page 328 field displays.</p> <p>On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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 63. PROXY - NONE SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> For each matching rule you can create up to 50 Type and Value pairs. <p>For instructions, see "Palo Alto Networks GlobalProtect" on page 328.</p>
Per-App VPN	<p>This setting applies to iOS and macOS devices only.</p> <p>See the <i>Ivanti EPMM Apps@Work Guide</i> for information about how to add or edit apps.</p>
Provider Type	<p>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).</p> <p>Select app-proxy (default) or packet-tunnel.</p>

Proxy - Manual

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

TABLE 64. PROXY - MANUAL SETTINGS

Item	Description
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	<p>Enter the port number for the proxy server.</p> <p>Type - Select Static or Variable for the type of authentication to be used for the proxy server.</p>
Proxy Server User Name	<p>If the authentication type is Static, enter the username for the proxy server.</p> <p>If the authentication type is Variable, the default variable selected is \$USERID\$.</p>
Proxy Server Password	<p>If the authentication type is Static, enter the password for the proxy server. Confirm the password in the field below.</p> <p>If the authentication type is Variable, the default variable selected is \$PASSWORD\$.</p>
Proxy Domains (iOS only)	
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$.</p> <p>Include at least one of the following variables:</p>

TABLE 64. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	<p>\$USERID\$, \$EMAIL\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
VPN On Demand	
Per-App VPN	This setting applies to iOS and macOS devices only.
Provider Type	This setting is not available on Android devices.

Proxy - Automatic

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

TABLE 65. 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)	
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
VPN On Demand	
Per-App VPN	This setting applies to iOS and macOS devices only.
Provider Type	This setting applies to iOS and macOS devices only.

PPTP

This VPN connection type is supported on iOS, Android, and Windows devices.

Use the following guidelines to configure the PPTP VPN connection type.

- ["Proxy - None \(default\)" below](#)
- ["Proxy - Manual" on the next page](#)
- ["Proxy - Automatic" on page 337](#)


Proxy - None (default)

Use the following guidelines to configure a PPTP VPN without a proxy.

TABLE 66. 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: <ul style="list-style-type: none">• Device channel - the configuration is effective for all users on a device. This is the typical option.• User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select PPTP .
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	None is the default setting. To configure a Manual or Automatic proxy, go to "Proxy - Manual" on the next page or "Proxy - Automatic" on page 337
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:

TABLE 66. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
	<p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	Select the authentication method to use: Password or RSA SecureID .
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>

Proxy - Manual

Use the following guidelines to configure a PPTP VPN with a manual proxy.


TABLE 67. 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	<p>For macOS only. Select one of the following distribution options:</p> <ul style="list-style-type: none"> • Device channel - the configuration is effective for all users on a device. This is the typical option.

TABLE 67. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> 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 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	<p>If the authentication type is Static, enter the username for the proxy server.</p> <p>If the authentication type is Variable, the default variable selected is \$USERID\$.</p>
Proxy Server Password	<p>If the authentication type is Static, enter the password for the proxy server. Confirm the password in the field below.</p> <p>If the authentication type is Variable, the default variable selected is \$PASSWORD\$.</p>
Proxy Domains (iOS only)	This setting does not apply to Android devices.
Encryption Level	Select None , Automatic or Maximum (128 bit).
Domain	Specify the network domain.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$ \$USERID\$_\$EMAIL\$

TABLE 67. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	<p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	Select the authentication method to use: Password or RSA SecureID .
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL:\$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>


Proxy - Automatic

Use the following guidelines to configure a PPTP VPN with an automatic proxy.

TABLE 68. 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	<p>For macOS only. Select one of the following distribution options:</p> <ul style="list-style-type: none"> • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select PPTP .
Server	Enter the IP address, hostname, or URL for the VPN server.

TABLE 68. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Proxy	Select Automatic . To configure a manual proxy, go to "Proxy - Manual" on page 335 .
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting does not apply to Android devices.
Encryption Level	Select None , Automatic or Maximum (128 bit).
Domain	Specify the network domain.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
Username	<p>Specify the user name to use (required.) The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
User Authentication	Select the authentication method to use: Password or RSA SecureID .
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>

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 341](#)
- ["Proxy - Automatic" on page 344](#)

Within these selections, you may make settings for:

- ["Custom Data" on page 346](#)

Proxy - None (default)

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

TABLE 69. 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: <ul style="list-style-type: none">• 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	Select this option to use per-app VPN (either inside or outside the Knox Workspace) or per-container VPN. A Samsung Knox license is required. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.

TABLE 69. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p> <p>See:</p> <ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	This setting is not supported on Android devices.
Username	<p>Enter a value for the username (required.) The default value is \$USERID\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$ \$USERID\$_ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> Password - see next row for information. Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Use this field to specify a custom format, such as \$PASSWORD\$_ \$USERID\$.</p> <p>Include at least one of the following variables:</p>

TABLE 69. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
	<p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Role	Specify the Pulse user role to use as a restriction.
Realm	Specify the Pulse realm to use as a restriction.
VPN On Demand	If the Samsung Knox and per-App VPN fields are both selected, then select this option to use VPN On Demand.
Per-app VPN	When selecting this option, a Samsung Knox license is required.
Provider Type	This setting applies to iOS and macOS devices only.

Continue with ["Custom Data"](#) on page 346.

Proxy - Manual

Use the following guidelines to configure a Pulse Secure SSL VPN with a manual proxy.


TABLE 70. 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	<p>For macOS only. Select one of the following distribution options:</p> <ul style="list-style-type: none"> 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	Select this option to use per-app VPN (either inside or outside the Knox Workspace) or per-container VPN. A Samsung Knox license is required.

TABLE 70. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	<p>A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device.</p> <p>This setting is ignored on non-Android devices.</p>
Deploy inside Knox Workspace	<p>Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data.</p> <p>This option is available only if you select the Samsung Knox option.</p> <p>See:</p> <ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	This setting is not supported on Android devices.
Proxy Server	This setting is not supported on Android devices.
Proxy Server Port	This setting is not supported on Android devices.
Type	This setting is not supported on Android devices.
Proxy Server User Name	This setting is not supported on Android devices.
Proxy Server Password	This setting is not supported on Android devices.
Proxy Domains (iOS only)	This field applies to iOS and macOS devices only.
Username	<p>Enter a value for the username (required.) The default value is \$USERID\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> \$USERID\$: \$EMAIL\$ \$USERID\$_ \$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>
User Authentication	Select the user authentication to use:

TABLE 70. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> Password - see next row for information. Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Use this field to specify a custom format, such as \$PASSWORD\$_\$USERID\$.</p> <p>Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Role	Specify the Pulse user role to use as a restriction.
Realm	Specify the Pulse realm to use as a restriction.
VPN On Demand	If the Samsung Knox and per-App VPN fields are both selected, then select this option to use VPN On Demand.
Per-app VPN	<p>When selecting this option, a Samsung Knox license is required.</p> <p>Select Yes to create a per-app VPN setting.</p> <hr/> <p> 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.</p> <hr/> <p>See the <i>Ivanti EPMM Apps@Work Guide</i> for information about how to add or edit apps.</p>
Provider Type	This setting applies to iOS and macOS devices only.

Continue with "Custom Data" on page 346.

Proxy - Automatic

Use the following guidelines to configure a Pulse Secure SSL VPN with an automatic proxy.

TABLE 71. 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: <ul style="list-style-type: none"> 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	Select this option to use per-app VPN (either inside or outside the Knox Workspace) or per-container VPN. A Samsung Knox license is required. A VPN setting with this option selected cannot be successfully applied to a non-Samsung Android device. This setting is ignored on non-Android devices.
Deploy inside Knox Workspace	Select this option to deploy the VPN client app inside the Knox Workspace (container). Deploying the app inside the container means that the Knox security platform protects the app and its data. This option is available only if you select the Samsung Knox option. See: <ul style="list-style-type: none"> "Configuring VPN modes when VPN client is outside the Knox container" on page 351
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	This setting is not supported on Android devices.
Proxy Server URL	This setting is not supported on Android devices.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Enter a value for the username (required.) The default value is \$USERID\$. Include at least one of the following variables:

TABLE 71. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	<p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_\$EMAIL\$ <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p>
User Authentication	<p>Select the user authentication to use:</p> <ul style="list-style-type: none"> • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. <p>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.</p>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Use this field to specify a custom format, such as \$PASSWORD\$_\$USERID\$.</p> <p>Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL\$: \$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
Role	Specify the Pulse user role to use as a restriction.
Realm	Specify the Pulse realm to use as a restriction.
VPN On Demand	If the Samsung Knox and per-App VPN fields are both selected, then select this option to use VPN On Demand.
Per-app VPN	When selecting this option, a Samsung Knox license is required.
Provider Type	This setting applies to iOS and macOS devices only.

Continue with "Custom Data" below.

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.

Encrypting and Decrypting logs

To encrypt logs

1. Navigate to **Core > Config > Add New > LogEncryption**.
Add the certificate for encryption.
2. Save and apply the config to the devices.
The client logs are encrypted with the given certificate.

Decrypting logs

To decrypt logs:

Prerequisite:

Ensure OpenSSL is installed.

Procedure

1. Run the following command in terminal
Openssl version LibreSSL 2.8.3
openssl smime -decrypt -in logs-encrypted.pc7 -inform DER -inkey privatekey.p12 -recip c.crt -out
decrypted_file.zip
2. Enter pass phrase for privatekey.p12: <enter the password here to decrypt if any>

-decrypt: This option tells OpenSSL that you want to decrypt a file.

-in logs-encrypted.pc7: Specifies the input encrypted file.

-inform DER: Specifies the input format of the encrypted file (DER format).

-inkey privatekey.p12: Specifies the private key file to use for decryption.

-recip c.crt : Specifies the recipient's certificate file.

-out decrypted_file.zip: Specifies the output file where the decrypted content is available.

Knox VPN Support

As part of Ivanti, Inc's support of Samsung Knox, Ivanti Mobile@Work for Android together with Ivanti EPMM support the following Virtual Private Network (VPN) clients:

- Pulse Secure (previously called Junos Pulse) (SSL)
- F5 BIG-IP Edge Client (SSL)
- Cisco AnyConnect (SSL)
- OpenVPN (SSL)
- Tunnel for Samsung Knox

Ivanti Mobile@Work 9.0.0.0 for Android or supported newer versions adds:

- Cisco AnyConnect (universal app for Android and for Samsung Knox)

Ivanti EPMM supports all of these VPN clients on Samsung Knox 2.0 or supported newer versions.

The following VPN connection types are supported with other Android devices:

- Cisco AnyConnect
- Pulse Secure
- F5 SSL
- Ivanti Tunnel
- Palo Alto Networks GlobalProtect

Basic Requirements to use Samsung Knox Features

To use any Samsung Knox Premium features that Ivanti EPMM supports, including VPN, the following are required:

- The user must have a Samsung Knox-capable mobile device.
- A Samsung General Policy with a Samsung Knox license key must be defined and applied to a label. To create this policy, in the Admin Portal go to **Policies & Configs > Policies**. Select **Add New > Android > Samsung General**.
- The device must have the Samsung General Policy label applied.

VPN clients deployed either inside or outside Knox Workspace

VPN client apps are deployed either inside or outside the Knox Workspace (container). When deployed inside the container, the VPN client and its data are protected by the Knox security platform.

Whether the VPN client is deployed inside or outside the container depends on:

- the version of Ivanti Mobile@Work on the device
- an option you set in the VPN setting

Ivanti Mobile@Work 9.1 for Android

When a device is running Ivanti Mobile@Work 9.1 for Android, you can set an option in the VPN setting to deploy the VPN client inside the container. The following VPN clients you can use with Samsung devices to deploy inside or outside the container are:

- Pulse Secure SSL (previously Junos Pulse)
- Cisco AnyConnect
- F5 SSL
- OpenVPN
- Tunnel for Samsung Knox

The option in the VPN setting is called **Deploy inside Knox workspace**. **When you choose this option, be sure to add the VPN client app to the Apps** section of the Samsung Knox Container setting. Tunnel for Samsung Knox is always deployed inside the container.

See also:

- ["Configuring VPN modes when VPN client is outside the Knox container" on page 351](#)

VPN Modes

For Android devices using the Samsung Knox Workspace, there are four VPN modes you can configure in Ivanti EPM. They are:

Per-Device VPN

- If a VPN client is installed outside the Knox container:
 - all apps outside the container use the same VPN connection.
 - a per-device VPN does not apply inside the Knox container for Samsung Knox 2.0 or supported newer versions.
- If a VPN client is installed inside the Knox container, per-device VPN provides similar functionality to per-container VPN:
 - all apps inside the Knox container use the same VPN connection.
 - a per-device VPN does not apply to apps outside the Knox container.
- Available for all Android devices.

Per-Container VPN

- All apps inside the Knox container use the same VPN connection.
- Requires a Samsung Knox license.

Per-App VPN for apps inside of Knox Container


- Applies to individual apps inside a Knox container.
- Each app can be individually assigned to a VPN connection. We recommend using a single VPN profile from a single provider. (The new feature allows you to cross providers.)
- Any number of apps can share a single VPN connection. (Check this is true for the cross provider feature. It may only be one app.)
- Requires a Samsung Knox license. See ["Working with Samsung general policies" on page 200](#).

Per-App VPN for apps outside of Knox Container

- Applies to apps outside of a Knox container (a Knox container may or may not be present.)
- Each app can be individually assigned to a VPN connection.
- Requires a Samsung Knox license.

All of these modes are supported by the following VPN clients on Samsung Knox devices:

TABLE 72. VPN CLIENTS

VPN Client Name	Appears in VPN Setting as Connection Type:
Pulse Secure (previously: Junos Pulse)	"Pulse Secure SSL"  The connection type "Juniper SSL" is only for VPN settings created in previous versions of Ivanti EPMM.
F5 BIG-IP Edge Client	"F5 SSL"
OpenVPN	"OpenVPN"
Cisco AnyConnect	"Cisco AnyConnect"

The following VPN clients are supported for non-Samsung Android devices using per-device mode:

- Cisco AnyConnect
- F5 SSL
- Ivanti Tunnel
- Pulse Secure
- Palo Alto Networks GlobalProtect

Configuring VPN modes when VPN client is outside the Knox container

If the VPN client is installed outside the Knox container, you can configure the VPN client to be used in one of these modes:

- per-device
- per-container
- per-app

In addition, you can configure a per app Android Enterprise VPN within the Knox v3 workspace. See ["Creating per container and per app Android Enterprise VPNs within the Knox v3 workspace" on page 353.](#)

The following table provides an overview of what you need to configure for each mode.

TABLE 73. MODE CONFIGURATIONS - VPN CLIENT IS OUTSIDE KNOX CONTAINER

	per-device mode	per-container mode	per-app mode
Description	The VPN client configured for per-device use can be used by appropriately labeled apps that are outside the Knox container.	The VPN client configured for per-container use can be used by any apps inside the Knox container.	The VPN client configured for per-app use can be used only by apps specifically configured to use it. The apps can be either inside or outside the Knox container.
VPN setting	Options in VPN setting: <ul style="list-style-type: none"> • per-app VPN: No • Samsung Knox: Select ONLY if using OpenVPN. • Deploy inside Knox Workspace: Not selected Apply label to VPN setting	Options in VPN setting <ul style="list-style-type: none"> • per-app VPN: Yes • Samsung Knox: Selected • Deploy inside Knox Workspace: Not selected Apply label to VPN setting	Options in VPN setting <ul style="list-style-type: none"> • per-app VPN: Yes • Samsung Knox: Selected • Deploy inside Knox Workspace: Not selected Apply label to VPN setting
App in App Catalog	<ul style="list-style-type: none"> • Apply label to app • Per App VPN Settings in app: not applicable 	<ul style="list-style-type: none"> • App label is not applicable to VPN usage • Per App VPN Settings in app: not applicable 	For apps outside the Knox container: <ul style="list-style-type: none"> • Apply label to app • Per App VPN Settings in app: set to VPN setting
Samsung Knox Container setting		<ul style="list-style-type: none"> • In the App Settings section, in the VPN field, select the VPN setting from the drop-down list. 	For apps inside the Knox container: <ul style="list-style-type: none"> • In the Apps section, for the specific app, select the VPN setting from the drop-down list.

TABLE 73. MODE CONFIGURATIONS - VPN CLIENT IS OUTSIDE KNOX CONTAINER (CONT.)

	per-device mode	per-container mode	per-app mode
		<ul style="list-style-type: none"> In the Apps section, for a specific app, make no VPN selection. Apply label to Samsung Knox Container setting 	<ul style="list-style-type: none"> In the App Settings section, in the VPN field, make no selection. Apply label to Samsung Knox Container setting
Android enterprise	N/A	(Managed device with Work Profile mode) <ul style="list-style-type: none"> Enable Managed Device with Work Profile (on Android 10 and below) Selected Enable Samsung Per-container VPN: Selected 	(Managed device with Work Profile mode) <ul style="list-style-type: none"> In the App Catalog: Per App VPN by Label Only: Selected (applicable for in-house apps only) Install this app for Android enterprise: Selected

Creating per container and per app Android Enterprise VPNs within the Knox v3 workspace

In Work Profile mode, Managed Device with Work Profile mode, and Work Profile on Company Owned Device mode, administrators can configure Knox VPN settings for per container and per app deployment devices to communicate with services securely. Within the Knox workspace, administrators can create per-app VPNs that they can assign to apps in the Apps catalog. Additionally, a special case of a per app deployment (Ivanti Tunnel + OpenVPN) supports VPN chaining, see "Configuring VPN chaining" procedure in *Ivanti Tunnel for Android Guide*.

Work Profile mode, Managed Device with Work Profile mode, and Work Profile on Company Owned Device mode works with the following VPN connection types:

- Cisco AnyConnect
- F5 SSL

- Pulse Secure SSL
- OpenVPN
- Tunnel (Samsung Knox Workspace)

These methods of configuring VPNs are not supported:

- Configuring VPNs via App restrictions and using Knox VPN APIs
- Support for device-wide VPN in Managed device with Work Profile mode

Android Enterprise VPN is configured using a password and certificate-based credentials. KLM licenses must be applied.

Creating per container Android Enterprise VPN with Knox 3 workspace

This section covers configuring Knox VPN settings for per container Android Enterprise. The below procedure is applicable for Managed device with Work Profile mode for Android version 8.0.

Procedure

1. Register the device, in Work Profile mode, to Ivanti EPMM using the procedure described in ["Setting the registration PIN code length for device user registration" on page 83](#).
2. Create a Samsung General Policy. See ["Working with Samsung general policies" on page 200](#).
3. Create a Android Enterprise configuration.
 - a. Click **Add New > Android > Android enterprise**.

The New Android enterprise (all modes) Setting dialog box opens.

- b. Enter the Name and Description of the configuration.
 - c. Select the **Enable Managed Device with Work Profile (on Android 10 and below)** check box. This field applies to Android 8, 9, and 10 devices.
 - d. Click **Save**.
4. Apply the configuration to a device label.

5. Create a VPN configuration for Android Enterprise.
 - a. Click **Policies & Configurations > Configurations**.
 - b. Select **Add New > VPN**. The Add VPN Setting dialog box opens.
 - c. Select a Connection Type in the drop-down:
 - Cisco Legacy AnyConnect
 - OpenVPN
 - F5 SSL
 - Pulse Secure SSL
 - Tunnel (Samsung Knox Workspace)
 - d. Select the **Samsung KNOX** check box.
 - e. Select the **Deploy inside Knox Workspace** check box.
 - f. Select the Per-app VPN **Yes** radio button.
 - g. Click **Save**.
6. Apply the VPN configuration to a device label.
7. Edit the Android Enterprise configuration.
 - a. In the For Samsung Knox v3 (Android 8.0) section, select the **Enable Samsung Per-container VPN** check box.
 - b. In the VPN Config Name field, select the VPN configuration you just created.
 - c. Click **Save**.

In Devices & Users > Devices > Device Details page, the Managed Device with Work Profile displays your setting, for example, Workspace > Tunnel.

Creating per app Android Enterprise VPN with Knox 3 workspace

This section covers configuring Knox VPN settings for per app Android Enterprise. The below procedure is applicable for Managed device with Work Profile mode.



Before you begin this procedure, follow the "Configuring VPN chaining" procedure in *Ivanti Tunnel for Android Guide* to populate the **VPN Config Name** field.

1. Register the device, in Work Profile mode, to Ivanti EPMU using the procedure described in ["Setting the registration PIN code length for device user registration" on page 83](#).
2. Create a Samsung General Policy. See ["Working with Samsung general policies" on page 200](#).
3. Apply the policy to a device label.
4. Add a new Android Enterprise app in the App Catalog, for example, Google Chrome.
 - a. Click **Apps > App Catalog > Add**.
 - b. In the Android Enterprise section, select the **Install this app for Android enterprise** check box.
 - c. Click **Save**.
5. Apply the app to a device label.
6. Create a VPN configuration for Android Enterprise.
 - a. Click **Policies & Configurations > Configurations**.
 - b. Select **Add New > VPN**. The Add VPN Setting dialog box opens.
 - c. Select a Connection Type in the drop-down:
 - Cisco Legacy AnyConnect
 - OpenVPN
 - F5 SSL
 - Pulse Secure SSL
 - Tunnel (Samsung Knox Workspace)
 - d. Select the **Samsung Knox** check box.
 - e. Select the **Deploy inside Knox Workspace** check box.
 - f. Select the Per-app VPN **Yes** radio button.
 - g. **Save** the new configuration.
7. Import another app and install this app for Android Enterprise. In the Per App VPN Settings section, select the new perApp VPN you created.

Next steps

["Move Android Enterprise in-house apps to inside Knox Workspace" on the next page](#)

Move Android Enterprise in-house apps to inside Knox Workspace

Once you have set up VPN for Knox Workspaces, you can move in-house apps from outside of the workspace to inside the Knox workspace. This is applicable to:

- Managed Device with Work Profile mode on Android devices with an activated Knox premium license.
- devices with Knox version 3.x and above only.

You cannot copy or move apps from the personal side of the device into Work Profile mode or Managed Device with Work Profile mode on Samsung devices. The in-house apps should be assigned to a device label so they can be installed in a personal (outside of the container) space. This Android Enterprise-only capability allows you to move previously-installed in-house apps into the container (Knox V3 workspace) using whitelisting of apps in the Android Enterprise configuration. The app being moved must be whitelisted prior to moving inside the Knox workspace, see ["Android Samsung Knox Container Settings" on page 550](#).

Procedure

This procedure is applicable for Android OS version 8.0 or supported newer versions.

1. Complete the procedure in ["Creating per container Android Enterprise VPN with Knox 3 workspace" on page 354](#) or ["Creating per app Android Enterprise VPN with Knox 3 workspace" on page 355](#).
2. Add a new Android Enterprise app in the App Catalog.
3. Apply the app to a device label.
4. If needed, force device check in.
5. In **Policies & Configs > Configurations**, **Edit** the Android Enterprise configuration and select the **Move In- House app into workspace** check box.
6. In the Package Name field, select the name of the app or hold the Shift key down and select multiple apps.
7. Click **Save**.

On the device, the app is moved to the Knox Workspace. In the device's Settings > Workspace option, the Install apps option is disabled.

Remove Android Enterprise apps from Knox Workspace

If the whitelist of apps is modified and an app is no longer listed inside the Knox workspace, that app will be moved back to the personal space. If the whitelist of apps is removed, all previously installed in-house apps will be moved back into the personal space.

Procedure

1. In **Policies & Configs > Configurations**, **Edit** the Android Enterprise configuration.
2. In the Package Name field, de-select the name of the app or hold the Shift key down and de-select multiple apps.
3. Click **Save**.
4. Force device check in.

On the device, the app is moved out of Knox Workspace to the personal space.

Configuring VPN modes when VPN client is inside the Knox container

If the VPN client is installed inside the Knox container, you can configure the VPN client to be used in one of these modes:

- per-device, but when the VPN client is installed inside the Knox container, per-device mode is really another way to configure per-container mode. Apps outside the container cannot use the VPN client.
- per-container
- per-app

The following table provides an overview of what you need to configure for each mode.

TABLE 74. MODE CONFIGURATIONS - VPN CLIENT IS INSIDE KNOX CONTAINER

	per-device mode	per-container mode	per-app mode
Description	The VPN client configured for per-device use can be used by any apps inside the Knox container.	The VPN client configured for per-container use can be used by any apps inside the Knox container.	The VPN client configured for per-app use can be used only by apps specifically configured to use it. The apps can be either inside or outside the Knox container.

TABLE 74. MODE CONFIGURATIONS - VPN CLIENT IS INSIDE KNOX CONTAINER (CONT.)

	per-device mode	per-container mode	per-app mode
	Therefore, per-device mode when the VPN client is inside the container is really a way of configuring per-container mode.		
VPN setting	Options in VPN setting: <ul style="list-style-type: none"> • per-app VPN: No • Samsung Knox: Selected • Deploy inside Knox Workspace: Selected Apply label to VPN setting	Options in VPN setting <ul style="list-style-type: none"> • per-app VPN: Yes • Samsung Knox: Selected • Deploy inside Knox Workspace: Selected Apply label to VPN setting	Options in VPN setting <ul style="list-style-type: none"> • per-app VPN: Yes • Samsung Knox: Selected • Deploy inside Knox Workspace: Selected Apply label to VPN setting
App in App Catalog	<ul style="list-style-type: none"> • App label is not applicable to VPN usage • Per App VPN Settings in app: not applicable 	<ul style="list-style-type: none"> • App label is not applicable to VPN usage • Per App VPN Settings in app: not applicable 	For apps outside the Knox container: <ul style="list-style-type: none"> • Apply label to app • Per App VPN Settings in app: set to VPN setting
Samsung Knox Container setting	<ul style="list-style-type: none"> • Include the VPN client in the Apps section. <p>Note: Do not apply a label to the VPN client app itself. This reference to the app will result in the app being deployed in the device's Knox container.</p>	<ul style="list-style-type: none"> • Include the VPN client in the Apps section. <p>Note: Do not apply a label to the VPN client app itself. This reference to the app will result in the app being deployed in the device's Knox container.</p>	<ul style="list-style-type: none"> • Include the VPN client in the Apps section. <p>Note: Do not apply a label to the VPN client app itself. This reference to the app will result in the app being deployed in the device's Knox container.</p>

TABLE 74. MODE CONFIGURATIONS - VPN CLIENT IS INSIDE KNOX CONTAINER (CONT.)

	per-device mode	per-container mode	per-app mode
	<ul style="list-style-type: none"> • Apply label to Samsung Knox Container setting 	<ul style="list-style-type: none"> • In the App Settings section, in the VPN field, select the VPN setting from the drop-down list. • In the Apps section, for a specific app, make no VPN selection. • Apply label to Samsung Knox Container setting 	<ul style="list-style-type: none"> • For apps inside the container, in the Apps section, for the specific app, select the VPN setting from the drop-down list. • In the App Settings section, in the VPN field, make no selection. • Apply label to Samsung Knox Container setting

VPN Behavior on the Device

When a VPN setting is installed on a device, the following behavior is observed:

- The VPN client displays its VPN connection status in the notifications bar.
- For per-app VPN configurations, the connection is automatically established when the user opens an app or accesses data that requires the connection.
- For per-device VPN, the user must manually establish the connection through the VPN client app.

Disconnecting or attempting to remove VPN behaves as follows:

- A user cannot disconnect a per-app or per-container VPN connection manually. The connection is automatically disconnected if:
 - Device is removed from the label that provides VPN.
 - Device is retired.
- A user can disconnect a per-device VPN connection manually.
- A user cannot uninstall a VPN client on Samsung devices if a VPN connection exists using the client.

Usage Notes

For all VPN clients:

- Knox 1.2 supports using per-app VPN outside of the Knox container, but not inside. Per-device VPN works inside Knox 1.2 container.
- Knox 2.0 or supported newer versions is required to use per-app VPN inside of the Knox container. Per-device VPN is not available inside these versions of the Knox container.

For the F5 BIG-IP Edge Client, Pulse Secure (previously Junos Pulse), OpenVPN, and Cisco AnyConnect:

- To use per-app VPN with Pulse Secure, F5 BIG-IP Edge Client, OpenVPN, or Cisco AnyConnect, you must select Samsung Knox in the VPN Settings. An invalid configuration can result if Samsung Knox is not selected.

For Juniper (Pulse Secure, previously Junos Pulse):

- For the Pulse Secure client, the user must accept the app's EULA before Ivanti Mobile@Work can install the VPN setting.
- To use Pulse Secure for per-app VPN, a license is required from Juniper Networks that is applied to the VPN gateway.
- Ivanti Mobile@Work supports the PulseSecure client, not the "Junos for Samsung" client.

Regarding migrating to Pulse Secure from Junos Pulse:

Only Ivanti Mobile@Work 9.0.0.0 and prior prompts the device user to install Pulse Secure if the device is using the Junos Pulse VPN app. Otherwise, device users are not prompted, but can uninstall the Junos Pulse app and then install Pulse Secure. When Junos Pulse is uninstalled, the Junos Pulse configurations will be removed only if the device is running Ivanti Mobile@Work 9.0.0.0 or prior.

If you prefer device users to be prompted to migrate, Ivanti, Inc recommends users stay on Ivanti Mobile@Work 8.5 (8.5.0.0 through 8.5.0.3) until after they have upgraded to Pulse Secure. See:

- [Action Required by September 30, 2015 to Support Junos Pulse VPN on Newly Enrolled iOS and Android Devices](#)

Limitations for VPN connections and settings

- Per-container VPN for the Knox container cannot be combined with per-app VPN for apps inside the container. You must choose to use one VPN mode or the other.

To do so, in the **New Samsung Knox Container Setting** dialog, you must either provide a VPN selection for individual apps in the **Apps** section, or provide a VPN selection in the **App Settings** section, but not both

- Ivanti, Inc recommends using a single VPN client and a single VPN connection per device.

How to set up VPN for apps both outside and inside the Knox container

In Knox 2.0 or supported newer versions, when you install a VPN client outside of the Knox container, a per-device VPN does not provide VPN inside the Knox container. If you want VPN working for apps both inside and outside the Knox container when the VPN client is outside the Knox container, set up:

- a per-device VPN for apps outside of the container, and
- a per-container VPN for the apps inside of the container.

We recommend using the same VPN client for each. You will need to create a separate VPN setting for each, however. One VPN setting sets its per-app VPN option to yes, and the other sets it to no.

See ["Configuring VPN modes when VPN client is outside the Knox container" on page 351](#).

Using certificates with VPN

When using certificates with VPN settings, depending on the VPN client, you will need to add the certificate in the VPN setting, and in some cases also assign the certificate to a label.

The following tables indicate the rules for each VPN client and certificate type.

TABLE 75. RULES FOR USER AUTHENTICATION CERTIFICATES

VPN Client	Rules for User Authentication Certificates
Pulse Secure (previously: Junos Pulse), OpenVPN	Provide user authentication certificate in the VPN setting.
Mocana KeyVPN, F5 Big-IP Edge Client	Provide user authentication certificate in the VPN setting only. Do not apply certificate to a label.

TABLE 76. RULES FOR CA (ROOT) CERTIFICATES

VPN Client	Rules for CA (Root) Certificates
Pulse Secure (previously: Junos Pulse), F5 Big-IP Edge Client	Apply CA certificate to a label.
Mocana KeyVPN, OpenVPN	Provide CA certificate in the VPN setting only. Do not apply certificate to a label.

Samsung Knox IPsec

This VPN connection type is supported on Android devices.

This section applies to Android devices with Samsung Knox only. Samsung Knox IPsec is used for VPN access in the Samsung Knox container - see ["Android Samsung Knox Container Settings" on page 550](#).

Use the following guidelines to configure Samsung Knox IPsec.

TABLE 77. SAMSUNG KNOX IPSEC 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: <ul style="list-style-type: none"> 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 Samsung Knox IPsec .
Server	Enter the IP address, hostname, or URL for the VPN server.
Backup Server	Enter the IP address, hostname, or URL for the fallback server to use in the event that the primary server is not available.
Authentication Type	Select the authentication method to use:

TABLE 77. SAMSUNG KNOX IPSEC SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none"> • Pre-Shared Key - When selected, the Shared Secret and Group Name fields display. • Certificate - When selected, the Identity Certificate and CA Certificate fields display.
Shared Secret	<p>This field displays when Pre-Shared Key is selected as the Authentication Type.</p> <p>Enter the shared secret passcode. This is not the user's password; the shared secret must be specified to initiate a connection.</p>
Confirm Shared Secret	Re-enter the Shared Secret passcode to confirm.
Group ID Type	<p>This field displays when Certificate is selected as the Authentication Type.</p> <p>Select the Group ID type your IPsec VPN server uses to authenticate to IKE peers.</p>
User Authentication	<p>This field displays when Certificate is selected as the Authentication Type.</p> <p>Select to enable user authentication as an additional factor.</p>
Group Name	<p>This field displays when Pre-Shared Key is selected as the Authentication Type. Enter the group name for your Samsung Knox IPsec VPN server. This name corresponds to the value selected in Group ID Type.</p>
Identity Certificate	<p>This field displays when Certificate is selected as the Authentication Type.</p> <p>Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.</p>
CA Certificate	<p>This field displays when Certificate is selected as the Authentication Type.</p> <p>Select the entry you created for supporting VPN, if you are implementing certificate-based authentication.</p>
Username	<p>Specify the user name to use. The default value is \$USERID\$. Use this field to specify an alternate format, such as:</p> <p>\$USERID\$, \$EMAIL\$, \$SAM_ACCOUNT_NAME\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as the following:</p> <ul style="list-style-type: none"> • \$USERID\$: \$EMAIL\$ • \$USERID\$_\$EMAIL\$

TABLE 77. SAMSUNG KNOX IPSEC SETTINGS (CONT.)



Item	Description
	<p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.</p> <hr/> <p> Some enterprises have a strong preference concerning which identifier is exposed.</p> <hr/>
Password	<p>Specify the password to use (required.) The default value is \$PASSWORD\$. Include at least one of the following variables:</p> <p>\$USERID\$, \$EMAIL\$, \$PASSWORD\$, \$USER_CUSTOM1\$, \$USER_CUSTOM2\$, \$USER_CUSTOM3\$, \$USER_CUSTOM4\$, \$CUSTOM_DEVICE_Attributename\$, \$CUSTOM_USER_Attributename\$, \$NULL\$</p> <p>You can use combinations such as \$EMAIL:\$PASSWORD\$</p> <p>Enter \$NULL\$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.</p>
IKE Version	<p>The IPsec VPN server uses the IKE to negotiate the protocols and algorithms used for the connection, and to generate the encryption and authentication keys. Select one:</p> <ul style="list-style-type: none"> • Phase 1 - When Phase 1 is selected, the Phase 1 Mode field displays. • Phase 2
Phase 1 Mode	<p>If you selected IKE Phase 1, select the mode of operation in use by your IPsec VPN server:</p> <ul style="list-style-type: none"> • Main - Has three two-way exchanges between the initiator and the receiver. • Aggressive - Fewer exchanges are made, and with fewer packets.
Per-app VPN	<p>Select Yes to create a per-app VPN setting. A Samsung Knox key / license is required for this feature.</p> <p>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.</p> <p>You can enable per-app VPN for an app when you:</p> <ul style="list-style-type: none"> • add the app in the App Catalog.

TABLE 77. SAMSUNG KNOX IPSEC SETTINGS (CONT.)

Item	Description
	<ul style="list-style-type: none">• edit an in-house app or an App Store app in the App Catalog. <hr/> <p> 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.</p> <hr/> <p>See the <i>Ivanti EPMM Apps@Work Guide</i> for information about how to add or edit apps.</p>

Managing Certificates and Configuring Certificate Authorities

This section addresses components related to managing certificates and certificate authorities.

- ["Certificates overview" below](#)
- ["Managing certificates issued by certificate enrollment configurations" on page 371](#)
- ["Configuring certificate pinning for registered devices" on page 371](#)
- ["Supported certificate scenarios" on page 373](#)
- ["Ivanti EPMM as a certificate authority" on page 375](#)
- ["Configuring Ivanti EPMM as an independent root CA \(Self-Signed\)" on page 376](#)
- ["Configuring Ivanti EPMM as an intermediate CA" on page 381](#)
- ["Mutual authentication between devices and Ivanti EPMM" on page 382](#)
- ["Certificates settings" on page 395](#)
- ["Certificate Enrollment settings" on page 397](#)
- ["Configuring a client-provided certificate enrollment setting" on page 401](#)
- ["Configuring an Entrust CA" on page 403](#)
- ["Configuring a GlobalSign CA" on page 406](#)
- ["Configuring Ivanti EPMM as the CA" on page 409](#)
- ["Configuring OpenTrust CA" on page 411](#)
- ["Configuring a single file identity certificate enrollment setting" on page 413](#)
- ["Configuring SCEP" on page 415](#)
- ["Configuring Symantec Managed PKI" on page 422](#)
- ["Configuring Symantec Web Services Managed PKI " on page 425](#)
- ["Configuring a user-provided certificate enrollment setting" on page 428](#)

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 78. CERTIFICATE TYPES

Certificate type	Description
Portal HTTPS	<p>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.</p> <p>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.</p> <hr/> <p> This certificate must be a publicly trusted certificate from a well-known Certificate Authority if you are using mutual authentication.</p> <hr/> <p>Related topics</p> <p>“Certificates you configure on the System Manager” in the <i>Ivanti EPMM System Manager Guide</i>.</p>
Client TLS	<p>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.</p> <p>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.</p> <p>Related topics</p> <p>“Certificates you configure on the System Manager” in the <i>Ivanti EPMM System Manager Guide</i>.</p>
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.
Client identity	Verifies the identity of users and devices and can be distributed through Certificate Enrollment.

Enrollment specific identification

Prior to setting up enrollment, it is important to decide whether a unique ID will be used for devices. This feature is part of the work profile enrollment of your organization and provides a unique ID that is guaranteed to be the same value for the same device, enrolled into the same organization by the same managing app. It will remain stable across factory resets or new profile inflation.

- ENROLLMENT_ID key is saved in the mi_device_detail table.
 - Enrollment ID is visible under device details page.
- Devices can be filtered using Enrollment id.

The enrollment-specific ID is reported and presented in device details page for new installs and post upgrade to Android 12. If a device is factory reset, and re-enrolled to the same Ivanti EPMM instance, the re-enrolled device shall REPLACE the previous device based on the Enrollment ID. A new unique ID is presented when the device registers to a new tenant.



Access to other hardware identifiers of the device such as IMEI, MEID, or serial number, is removed for personal devices with a work profile in Android 12.

This identifier is effective for new installs and post-upgrade to Android 12. Following are the supported modes:

- Work Profile
- Work Managed Device
- Work Profile on Company Owned Device



Please note that the ID will change when the same device is enrolled to the same tenant but uses a different managing package; a new unique ID is presented when the device registers to a new Ivanti EPMM instance.

Samsung Knox devices and certificates managed by Ivanti EPMM

Certificates managed by Ivanti EPMM are automatically removed from a Samsung Knox device when the device is retired, or when the label that applied the certificate to the device is removed from the certificate.

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 382](#).

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**.




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	<p>Select the relevant radio button to indicate whether the policy is Active or Inactive.</p> <p>Only one active policy can be applied to a device.</p>
Priority	<p>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.</p> <p>Select Higher than or Lower than, then select an existing policy from the drop-down list.</p> <p>For example, to give Policy A higher priority than Policy B, you would select "Higher than" and "Policy B".</p>
Description	Enter an explanation of the purpose of this policy.
Trusted Certificates	<ol style="list-style-type: none"> 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. <hr/> <p> Administrators can delete unwanted certificates by selecting the x in the row.</p>

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](#)
- ["Supported certificate scenarios" above](#)

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 TouchDown
- VPN is supported on Android with Cisco AnyConnect .
- Wi-Fi.

The following certificates are supported for Android devices:

- Microsoft NDES Certificate Enrollment
- Entrust
- Local CA
- Symantec Managed PKI
- User provided certificates
- Open Trust
- Symantec Web Services Managed PKI
- Client-Provided certificates

For information about how to create certificate enrollment settings in Ivanti EPMM, see ["Certificate Enrollment settings" on page 397](#).

Kerberos constrained delegation

You can use Kerberos constrained delegation (KCD) for authenticating the device to the ActiveSync server, the app server, and to Sentry.

For detailed information about how to configure Ivanti EPMM to use Kerberos authentication, see, "Device and server authentication support for Standalone Sentry" in the *Ivanti Standalone Sentry Guide for EPMM*.

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 \(Self-Signed\)" on the next page](#).

- **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 381](#).

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 379](#).

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**.

Certificate Template ✕

► CA Certificate

▼ Client Certificate Template

Hash Algorithm

SHA384

Minimum Key Size Allowed

2048

Key Lifetime (days)

365

Key Lifetime Limited by CA

☒

Enhanced Key Usage

☒ Client Authentication
☐ IPSEC
☐ Smart Card Logon

Custom OIDs

Cancel

Save

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**.



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 397](#).

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.

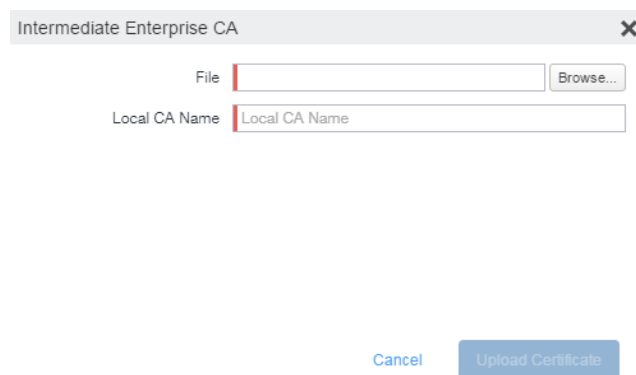
Configuring Ivanti EPMM as an intermediate CA

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" on the next page](#)
- ["Ivanti EPMM port usage with devices, with and without mutual authentication" on the next page](#)
- ["The mutual authentication setting on Ivanti EPMM" on page 384](#)
- ["Mutual authentication between devices and Ivanti EPMM" above](#)
- ["Mutual authentication identity certificate for Ivanti EPMM" on page 387](#)
- ["Mutual authentication client identity certificate" on page 388](#)
- ["Supported custom attributes for mutual authentication certificates" on page 389](#)
- ["New endpoint for mutual certification authentication" on page 389](#)
- ["Handling client identity certificate expiration for Android devices" on page 391](#)
- ["Mutual authentication between devices and Ivanti EPMM" above](#)
- ["Mutual authentication and Apps@Work" on page 392](#)
- ["Enabling mutual authentication for Apple and Android devices" on page 392](#)
- ["Enabling TLS inspecting proxy support when using mutual authentication" on page 394](#)
- ["Enabling mutual authentication for Apple and Android devices" on page 392](#)
- ["Enabling mutual authentication for Apple and Android devices" on page 392](#)

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 79. MUTUAL AUTHENTICATION USAGE BY PLATFORM

Platform	Mutual Authentication usage
iOS	<ul style="list-style-type: none">Ivanti Mobile@Work for iOS device check-inAppConnect for iOS check-iniOS MDM device check-inApps@Work for iOS communicationCertificate pinning policy
macOS	<ul style="list-style-type: none">Ivanti Mobile@Work for macOS device check-inmacOS MDM device check-in
Android	<ul style="list-style-type: none">Ivanti Mobile@Work for Android device check-in, which includes AppConnect check-inApps@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 80. 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
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 81. 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 82. 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	Port: 9997 MA: not used	Devices that register after enabling MA: <ul style="list-style-type: none"> • Port: 443 • MA: used Devices that were already registered:	Port: 443 MA: used

TABLE 82. 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
(all Ivanti Mobile@Work versions that Ivanti EPMM supports)		<p>Once the device has checked in with Ivanti EPMM, the device will transition from non-mutual to mutual authentication.</p> <ul style="list-style-type: none"> Before the transition, use port 9997. After the transition, use port 443. 	
iOS: Ivanti Mobile@Work 9.8 or supported newer versions	Port: 9997 MA: not used	<p>Devices that register after enabling MA:</p> <ul style="list-style-type: none"> Port: 443 MA: used <p>Devices that were already registered:</p> <p>Once the device has checked in with Ivanti EPMM, the device will transition from non-mutual to mutual authentication.</p> <ul style="list-style-type: none"> 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.

TABLE 82. 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: Ivanti Mobile@Work	Port: 443 MA: used	Port: 443 MA: used	Port: 443 MA: used
macOS macOS MDM agent check-in	Port: 443 MA: not used	Port: 443 MA: used	Port: 443 MA: used
Windows 10	Port: 443 MA: used	Port: 443 MA: used	Port: 443 MA: used

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 415](#)

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 ["Handling client identity certificate expiration for Android devices" on page 391](#) and ["Mutual authentication between devices and Ivanti EPMM" on page 382](#)

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 83. 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.

- Use the below guidelines to complete this form.

TABLE 84. 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	<p>a. When selecting the Disable legacy OAuth Endpoint box, a confirmation displays. Click Disable.</p> <p>b. A second confirmation dialog box displays, click Disable.</p> <p>Once disabled, the WatchOS app will no longer work. This setting can be reversed by de-selecting it.</p> <hr/> <p> Before disabling the legacy OAuth endpoint, make sure that all devices are migrated to the new endpoint.</p> <hr/>

- Click **Save**.

Handling client identity certificate expiration for Android devices

Ivanti Mobile@Work for Android handles the expiration of the client identity certificate used for mutual authentication between Ivanti Mobile@Work for Android 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 10.1 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 384](#).



Important After you enable mutual authentication, you cannot disable it.

Before you begin

1. As discussed in ["Mutual authentication client identity certificate" on page 388](#), 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 397](#).



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 382](#)

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 411](#).
- **Single File Identity:** Use to upload an identity certificate for distribution to devices.
- **SCEP:** Use for standard certificate-based authentication using a separate CA.



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 422](#) 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 425 for 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 EPM 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" on the next page](#)
- ["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:

- Exchange settings for Android devices
- Email settings for Android devices
- Wi-Fi settings for Android devices
- VPN settings for Android devices
- AppConnect app configurations
- Ivanti Docs@Work settings
- Ivanti Web@Work settings

For each device that has the same label as the setting, Ivanti EPMM generates an identity certificate for the device for *each* setting that references the certificate enrollment setting. Ivanti EPMM delivers the identity certificate to the device at a later time when Ivanti EPMM delivers the setting to the device. Ivanti EPMM delivers a setting to a device when the device checks in with Ivanti EPMM.



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.

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: <ul style="list-style-type: none">• Authentication• Decryption• Encryption• Signing
Provider	Select the derived credential provider.

4. Click **Save**.

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.

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.

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.



If the profile you selected contains an iggroup variable, then the you must configure the same value here as well

- **Key Usage:** Use these options to filter out the certificates returned by Entrust, which may return multiple certificates with different uses depending on the selected profile.



When multiple certificates are returned by a DigitalID profile, the first one that matches the selected key usage flags is used. If none of the returned certificates match the selected key usage flags, an error is raised. Use the **Issue Test Certificate** feature to ensure the expected certificate is selected.

- **Profile:** Use these options to filter out the certificates returned by Entrust, which may return multiple certificates with different uses depending on the selected profile.

Select a profile template from Entrust. Once you select this profile, more options (required and optional variables) are available to you based on the profile you select. Entrust refers to profiles as DigitalIDs.

- **Profile Description:** Pre-populated based on the profile you select.
- **Application Description:** Pre-populated based on the profile you select.
- **Centralized:** Select to allow 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.
 - **User Certificate:** Specifies that the certificate is distributed to multiple devices assigned to a single user.
 - **Device Certificate:** Specifies that the certificate is bound to the given device.
 - **Entrust SCEP CA:**
 - **URL:** Enter the URL of the Entrust SCEP CA.
 - **Key Type:** Select RSA.
 - **Subject Alternative Names table:** Select a type and value. At run-time, these variables are resolved into user values. (See "[Certificate Enrollment settings](#)" on page 397 for more information.) Custom attribute variable substitutions are supported.
3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
 4. Click **Save**.



If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview**.

Revoking the certificate

You can revoke an Entrust API Version 9 certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the Entrust manager. When a device authenticates with 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 398](#) 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**.



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 398](#) 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 398](#) for more information.

4. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
5. Click **Save**.



If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview**.

Revoking the certificate

You can revoke a local certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). When a device authenticates with 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**.



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**.

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:

- The private key and its password.
- The public certificate.
- The supporting certificates in the certificate chain. The root certificate is not necessary if it is from a well known certificate authority.

- **Examples of combinations** you can upload are:

- A .p12 or .pfx file containing a an identity certificate and its private key and password, plus additional .pem files containing the intermediate certificates.
- A .pem file containing the private key and password, a .pem file containing the public certificate, plus additional .pem 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 [""SCEP proxy functions" on page 419"](#).



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 392](#).

- **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 Android 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 85. 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



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 415](#). 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 388](#).

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 86. 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 425"](#).
-
-  Select this option for certificates used for email on devices with multi-user sign-in.
-
- **Decentralized:** This feature is not available for Android devices. Devices retrieve their own certificates.
 - **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 Android 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.

- **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 398](#) 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 398](#) for more information.)



The Required Fields and Optional Fields for the certificate are displayed based on how the MDM (Web Service Client) profile was set up in the Symantec PKI manager.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.



If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview**.

Using a proxy

Choosing to enable proxy functions has the following benefits:

- A single certificate verifies Exchange ActiveSync, Wi-Fi, and VPN configurations
- There is no need to expose a SCEP listener to the Internet.
- 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



Note that the V1 API associated the user certificate with a certificate type: All, WIFI, VPN, SMIMESIGNING, SMIMEENCRIPTION, 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

- ["Viewing, replacing, and deleting certificates in the user portal" on page 674](#)
- *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 430](#).
- **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**.

Android shared-kiosk mode overview

For task-worker deployments, companies may offer dedicated Android devices that are customized for a specific user role. Depending on a user's profile, different apps and configurations may be presented on a device. For example, a user in a technical role may have a specific set of apps presented for their use, while another user in a maintenance role may have access to a different set of apps. For more details, see:

- ["Setting up the Android shared-kiosk mode" below](#)
- ["Configuring the Android shared-kiosk mode" on page 435](#)
- ["User experience for staging and shared kiosk users" on page 444](#)
- ["Suggestions for configuring shared-kiosk mode" on page 446](#)

Setting up the Android shared-kiosk mode

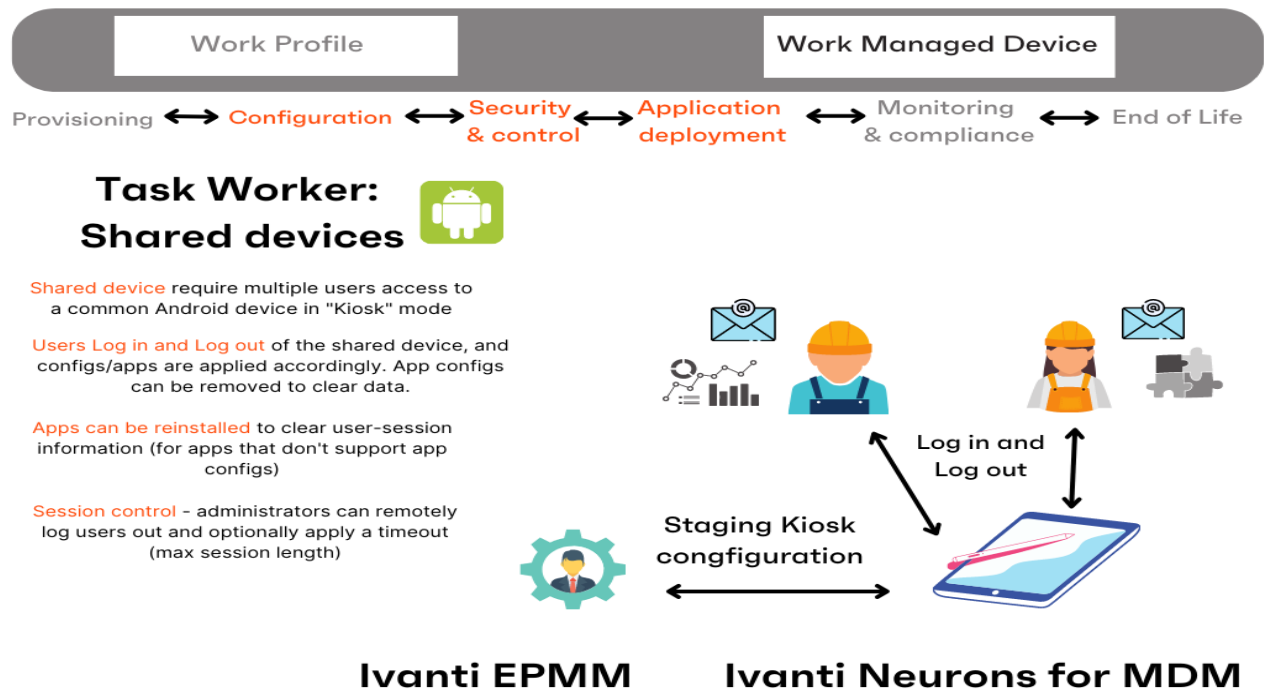


Samsung Kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead.

For task-worker deployments, companies may offer dedicated Android devices that are customized for a specific user role. Depending on a user's profile, different apps and configurations may be presented on a device. For example, a user in a technical role may have a specific set of apps presented for their use, while another user in a maintenance role may have access to a different set of apps.

The Android shared-kiosk mode acts as an app filter for different groups of users who share devices. A user who is logged in to the shared kiosk is only able to view the apps appropriate for their role. One of the main advantages to the shared-kiosk mode is that you can allow individual user groups access to different sets of apps from the same device. When a user logs out of an Android shared kiosk, their apps and user data, including history, are cleared from the display of the next user who logs onto the device. The shared kiosk requires connectivity to the Ivanti EPMM for the user login and logout actions to take effect. In addition, the shared kiosk is only available to Android Enterprise deployments with Managed Google Play accounts.

FIGURE 1. TASK WORKERS IN ANDROID SHARED KIOSK MODE



The shared kiosk requires two types of users, a staging user and a shared kiosk user, and at least two policies that correspond to these users. The staging user is used to prompt the login screen to appear on a shared device. In effect, the staging user is the logged out device owner (default owner) when a shared user is not logged into the device. Also, the staging user is a special type of admin user who allows other users to login to the actual kiosk device. After the shared kiosk user logs in successfully, then the staging policy is replaced by a shared kiosk policy. The kiosk user has access to the apps installed on the device according to the policy assigned to it. Although you can create multiple shared kiosk policies, there is only one kiosk policy active on a kiosk device at a time. When the kiosk user logs out of the shared kiosk, the device reverts to the staging user and, consequently, the staging policy.

Since the staging user only has the ability to access the login page, you need to create a staging policy that is dedicated to this user. In contrast, the shared kiosk users are able to access the set of apps that you define in their policy. (Naturally, you also need to install the permitted apps on the shared kiosk devices.) The shared kiosk policy allows you to create a filter of permitted apps from all of the apps you have installed previously. You cannot directly upload apps into an Android-shared-kiosk-mode policy. Often you want to dedicate a shared-kiosk-mode policy to a type of shared kiosk user, or user group, depending on your organization. For example, a company may have day-shift and night-shift employees that have different roles and require access to separate sets of apps. In this case, you need to create a day-shift policy and a night-shift policy.



Android shared kiosk only supports work-managed devices.

Configuring the Android shared-kiosk mode

To configure the Android shared-kiosk mode, you need to create a staging user role. Then you need to create one kiosk policy for the staging user as well as one or more policies for the shared kiosk users. For example, you can create one policy for managers and another one for employees. Within each policy, you can define the apps that the users, or user group, can access. Then you need to create and add a label to the device. Finally, you need to apply labels to both the staging and shared kiosk policies.



You define user groups with a user group feature, such as LDAP. You cannot define user groups within the Android shared kiosk mode.

To configure the Android shared-kiosk mode, do the following:

1. ["Configuring a staging user" below](#)
2. ["Creating a staging policy for the staging user" on the next page](#)
3. ["Creating a shared-kiosk-mode policy for the shared kiosk users" on page 437](#)
4. ["Creating and Adding labels to Android shared kiosk policies" on page 441](#)
5. ["Applying a label to the staging policy" on page 443](#)
6. ["Applying a label to a shared kiosk policy" on page 443](#)

Configuring a staging user

The first step in allowing users to access the Android shared-kiosk mode is to assign a user to the staging role. The staging user must have the same login as the person in your organization who registered Ivanti Mobile@Work during the initial setup of the software. Also, this user needs to have the Google Device Account role. Ivanti, Inc suggests that you make this user name easy to distinguish by using a name such as "staging-user."



A Google Device Account applies only to Managed Google Play Accounts and **new** managed devices. The device account allows the staging user to enroll large numbers of managed devices, that is more than ten devices, without applying the limits imposed by Google.

Procedure

1. In Admin Portal, go to **Devices & Users**. Then select **Users**.
2. Select the check box next to a user.
3. From **Actions**, select **Assign Roles**. The **Assign Role(s)** screen displays.
4. Select the check box next to **Use Google Device Account (for Android enterprise device only)**.
5. Click **Save**.

Creating a staging policy for the staging user

You need to create a policy that is dedicated to the staging user. This policy is not active until you apply a label to the staging policy.

Procedure

1. In Admin Portal, go to **Policies & Configs > Policies**.
2. Click **Add New > Android > Android Kiosk Mode**.
3. In the New Android Kiosk App Setting Policy dialog box, enter a **Name** and **Description** for the policy.
4. Select **Active** for the **Status** field to enable this policy.
5. Scroll down to the lower part of the Kiosk Settings section:
 - **Disable Quick Settings** - Select so that the device will not display the system notification drop-down menu at the top of the screen. If you enable the following options, the settings are displayed as menu items in the shared-kiosk mode on the device.
 - **Allow User to Access WIFI Settings**. This is an optional setting.
 - **Allow User to Access Bluetooth Settings**. This is an optional setting.
 - **Allow User to Access Location Settings**. This is an optional setting.
 - Enter a 4 - 6 digit PIN in the **Kiosk Exit PIN** field.
You can assign a pin to the staging user kiosk policy. However, it is not mandatory. Without a kiosk exit pin, the staging user cannot exit the kiosk mode .

- Select the **Enable Shared Device** check box. This is a mandatory setting.
 - **Enable Login (Only for Staging user)** - This option does not apply to shared-kiosk mode.
 - **Enable Logout** - Select to use and then set the number of hours in the **Logout user is session exceeds (0) hours** drop-down.
- 6. Scroll up to the Kiosk Branding section, customize the kiosk with a background color and background image if desired. See ["Branding the Android kiosk screen" below](#).
- 7. Click **Save**.

Creating a shared-kiosk-mode policy for the shared kiosk users

You want to create one or more policies for the shared kiosk user who has access to the apps on the shared device based on their assigned policies. Each shared kiosk policy specifies a different set of apps available to the assigned user or user groups. For example, one policy could be for day-shift workers and a second one for night-shift workers. Also within these policies, you may want to configure branding to customize the device. This policy is not active until you apply a label to the shared kiosk policy.



You need to install any apps that you wish to include in the kiosk using the App Catalog page before you begin this procedure. You cannot install apps from within the shared-kiosk -mode policy. You can only use the shared-kiosk -mode policy to setup which apps are displayed.

Procedure

1. Go to **Policies & Configs > Policies**
2. Click **Add New > Android > Android Kiosk Mode**.

The New Android Kiosk App Setting Policy dialog box opens.

3. Enter a **Name** and **Description** for the policy.
4. Select **Active** for the **Status** field to turn on this policy.

Branding the Android kiosk screen

You can brand the Android kiosk page to make its appearance more familiar to your device users.

1. Select **Enable Top Banner**. De-select If you want to turn off the banner.
2. Click the **Banner Background Color** field to display a color palette to select from or enter the hex number for the color you prefer.
3. Click the **Banner Border Color** field to display a color palette to select from or enter the hex number for the color you prefer.
4. Select **Image/Logo or Text** to set the banner content.
5. If you selected **Image/Logo**, drag and drop the image file or click **Choose File** to select one.
6. If you selected **Text**, type the text you want to display in the banner.
7. To change the **Background Image**:
 - a. Delete the default image.
 - b. Drag and drop the preferred image or click Choose File to select one.
 - c. Select the preferred layout.
8. Select the image **Layout** preferred: Fit, Center, or Tile.

Kiosk Settings

1. In the Kiosk Settings section, select **Enable Lock Task Mode**, thus enabling Android Enterprise devices connected to Android Kiosk to increase the level of security on the user devices in kiosk mode by limiting access to whitelisted kiosk and system apps. When a device user swipes away from an app, they will only have access to the white listed and system apps. This feature is only applicable to Android 9 devices in Device Owner (DO) mode. Further options display:
 - a. **System Info** - When selected, displays the date / time, connectivity, battery, and vibration mode in the status bar. Not enabled by default.
 - b. **Keyguard** - Enables the keyguard in lock task mode. Enabled by default.
 - c. **Global Actions** - Enables the menu that is displayed when the device user long-presses the power button. If this option is disabled, the device user may not be able to power off the device. Enabled by default.
 - d. **Home button** - Disabled by default. When enabled, displays the following sub-options:

- Overview button- Enables the Overview button and the Overview screen during lock task mode. When using the **Enable Single App Kiosk** mode, Ivanti recommends the Overview button to be de-selected.
- Notifications - Enables notifications during lock task mode. This includes notification icons on the status bar, heads-up. notifications, and the expandable notification shade. Note: These options are only applicable for Android 9 devices.

2. Make choices for further options:

- **Disable Quick Settings**

If you select this option, the device does not display the system notification pull-down menu at the top of the shared kiosk screen.

If you enable the following options, the settings are displayed as menu items in the shared-kiosk mode on the device.

- **Allow User to Access WIFI Settings.** This is an optional setting.
- **Allow User to Access Bluetooth Settings.** This is an optional setting.
- **Allow User to Access Location Settings.** This is an optional setting.
- **Enter Kiosk Mode Immediately on Registration** - Selecting this will make the device enter Kiosk mode automatically upon registration. Disabled by default.
- **Kiosk Exit PIN** - Create 4-6 Digit PIN for existing Kiosk Mode from device. This PIN applies to all devices in Kiosk mode.
- Select the **Enable Shared Device** check box and then click the **Enable Logout** radio button. This is a mandatory setting.
 - In **Logout user if session exceeds [0 is default] hours**, select a number from the drop-down.
- **Enable Single App Kiosk** - Starting with Ivanti EPMM 11.8.0.0, administrators can select the **Enable Single App Kiosk** check box and then select the (single) app to pin to the device screen.

This setting allows one app to be pinned to the device screen in most conditions. The dedicated single app mode will allow other apps to be available on the device, but they will not be available for the device user to directly launch. These other apps will only be launched through the pinned app. For example, Email is the pinned single app, and the device user receives an email with a link to the Gmail Maps app. When the device user taps on that link, it opens the Gmail Maps app.

The pinned single app will be launched only when it is part of the Allowed App list, the Kiosk Mode Allowed Apps list, *and* installed on the device. The Allowed Apps listed are from the App Catalog Apps section.

Ivanti recommends this be used with Lock Task mode and to have the Overview button de-selected.

Applicable to Work Managed Device mode (DO) and Work Managed Device - non-GMS mode (AOSP.)



Note the following:

- The Lock Task mode can only be enabled when the screen is in the foreground. If the dedicated single-app is in the foreground, then it is not possible to enable Lock Task mode. Workaround: Device user needs to tap the back or home button; the Lock Task mode becomes enabled.
- On devices Android 9 and below, when the Single App Kiosk is disabled, then the device user may need to tap the back/home button to see the Kiosk grid screen again. The launched app may remain pinned to the foreground and the Kiosk grid screen may not display due to Android limitations.

Choose Apps

1. In the **Choose Apps** section, select the app or apps that will be available to the shared kiosk user.
2. Add the permitted apps to the **Built-in Apps** section.
 - a. Click **+Add** in the Built-in Apps to add apps such as the Built-in Camera or Built-In Dialer to the **Kiosk Mode Allowed Apps** section.



The built-in apps must be enabled in Device Owner mode and be for Android 6+ devices. This may not be the case with all manufacturers.

3. Add apps from the **App Catalog Apps** section by clicking **+Add**.
4. Add apps manually by entering a Package ID in the **Manually Add Apps with Package ID** field. Then click **+Add**.

5. The order that the apps appear in the **Kiosk Mode Allowed Apps** section reflects how they appear on the device user's screen. To change the position of an app on the screen, change its position in the **Kiosk Mode Allowed Apps** list by selecting it and dragging it up or down.
6. All apps allowed in the **Kiosk Mode Allowed Apps** section have a "broom" icon/option. Based on the specific app's settings, the Ivanti Mobile@Work app will:
 - a. Broom with Check mark icon = clear app data when the user logs out of shared kiosk.
 - b. Broom with "Not allowed" icon = do not clear app data when the user logs out of shared kiosk.
7. All apps allowed in the **Kiosk Mode Allowed Apps** section have a "gear" icon/option. Based on the specific app's settings, the Ivanti Mobile@Work app will:
 - a. Gear with Check mark icon = allows device-wide settings for the selected app to be made available to the device user. Some apps may need this to get support from Android OS for activities such as completing bluetooth pairing. This is only available in Lock Task Mode. If Lock Task Mode is de-selected, the gear icon will not display.
 - b. Gear with "Not allowed" icon = disallows device-wide settings for the selected app to be made available to the device user.
8. Optionally, hide an app. Select an app in the **Kiosk Mode Allowed Apps** section and click the "eye" icon to hide the app.
 - a. When an app is hidden it can be used by other apps, but not available to launch in the kiosk. For example, a browser can be added to the kiosk but hidden so that it can be used to open URLs from an email app.
 - b. The Kiosk itself does not install any app. You need to install any app that you include in the kiosk using Apps@Work or other method.
9. Click **Save**.

Creating and Adding labels to Android shared kiosk policies

After you create the staging policy and one or more shared kiosk policies, you need to create and add a filtered label to the policies to push the configuration to the target devices. You must create a label for the staging user and each of the shared kiosk users.

Procedure

1. Go to **Devices & Users > Labels**.
2. Click **Add Label**. The "Add a label" page is displayed.
3. Enter a name and description of the label.
4. Click the **Filter** radio button.
5. Create a rule for the label based on the type of user logged into the device. In the Criteria section, use the **Field**, **Operator**, and **Value** fields (or enter the rule in the **Type search expression here** field):

- **Field:** Enter the user id as "user.user_id".
- **Operator:** Enter "Equals" or some other operator to return a single username.
- **Value:** Enter the user account name

Here is an example of a rule for a staging user:

"user.user_id" = "<StagingUsername>" AND common.retired = "false"

See the following image for an example of a rule for a kiosk user:

The screenshot shows the 'Add Label' form with the following details:

- Name:** DonaldDay
- Description:** Applies the DonaldDay Kiosk when user DonaldDay logs in
- Type:** Filter (selected)
- Criteria:**
 - Logic: All of the following rules are true
 - Rule 1: User ID Equals DonaldDay
 - Rule 2: "user.user_id" = "DonaldDay"

For more information about field definitions, see ["Device field definitions" on page 98](#).

6. Click **Save**.
7. Apply this label to the related policy. See the following sections.



The Display Name field on the "Add a label" page changes to reflect the user logged in. This is how the Filtered Label distinguishes which Kiosk Policy is applied.

Apply labels to Android shared kiosk policies

After you create the staging policy and one or more shared kiosk policies, you need to apply a label to the policies to push the configuration to the target devices.



You must assign mutually exclusive labels to the staging and shared kiosk policies. In other words, the labels cannot resolve to a device that could be assigned to both policies at the same time. If that situation occurs, the policy with the higher priority is assigned to the device.

Applying a label to the staging policy

The label must contain local users or LDAP user group information (or some way of associating the target users). These are the users that will use the policy.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select the check box next to the staging policy.
3. Select **Actions > Apply to Label**. The Apply to Label dialog box opens.
4. Select the check box next to the label.
5. Click **Apply**.

Applying a label to a shared kiosk policy

The label must contain local users or LDAP user group information. These are the users that will use the policy.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select the check box next to the shared kiosk user policy.
3. Select **Actions > Apply to Label**. The Apply to Label screen dialog box opens.
4. Select the check box next to the label.

5. Click **Apply**.
6. If needed, repeat the procedure to assign an additional label to another shared kiosk policy.

User experience for staging and shared kiosk users

The staging and shared kiosk users have different user experiences when logging in and out of the kiosk. If you have defined a pin in the staging kiosk policy, the staging user has access to the Exit Kiosk menu command within **Settings**. However, the shared kiosk user has access to their permitted apps as well as to the **Logout Kiosk** command.



Both the login and logout operations must be done when the device is online which allows a connection to the Ivanti EPMM server during these operations.

Staging user experience

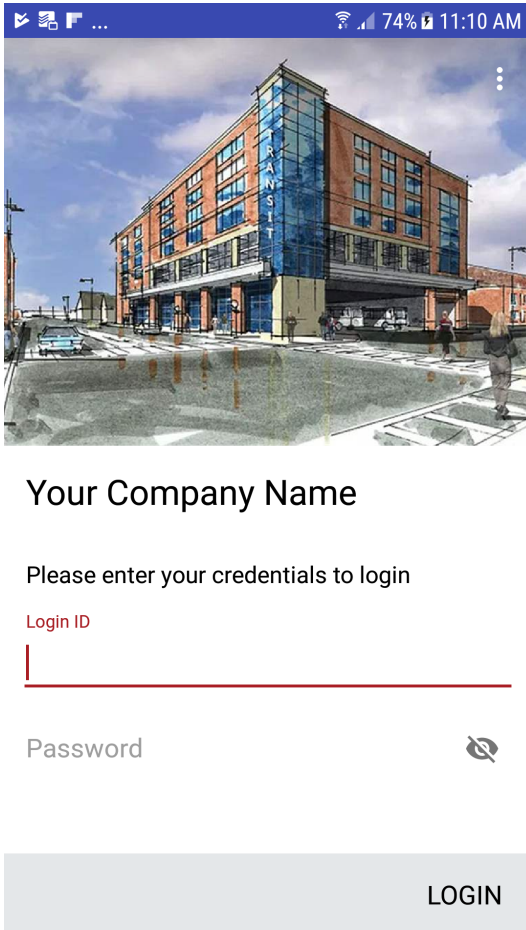
Procedure

1. Select the **Ivanti Mobile@Work** menu on the device and then select **Kiosk** to put the device into kiosk mode. The banner and background image are displayed on the screen of the staging user if they have been configured.
2. Select the **Settings** icon--the **Exit Kiosk** command as well as the **WIFI**, **Bluetooth**, and **Location Settings** options are displayed.
3. To exit the kiosk, select **Settings** icon and then select **Exit Kiosk**. Then you are prompted to enter a pin.
4. After you enter the pin, the shared kiosk mode is released and the Android home screen is displayed. See the following ["Android shared-kiosk login screen example" on the next page](#).



To re-engage in shared-kiosk mode, repeat step 1.

FIGURE 1. ANDROID SHARED-KIOSK LOGIN SCREEN EXAMPLE



Shared-kiosk mode user experience

Procedure

1. The staging login page is displayed.
2. Enter the shared-kiosk user credentials. It can take up to 30 seconds for the login to complete. Then the shared-kiosk screen is displayed. The **Settings** icon as well as the icons of the available apps are displayed on this screen. Any branding settings, such as banner, background color, or background image, are also displayed.
3. Use any of the allowed apps. (The shared kiosk user has access to at least one app.)
4. Select the **Settings** option, and then the **WIFI**, **Bluetooth**, and **Location Settings** options are displayed. along with the **Logout Kiosk** command.

5. To exit, select **Settings > Logout Kiosk** command. Then the staging login page is displayed on the device.

Monitor Android shared-kiosk mode

While you are setting up the shared-kiosk mode, you may want to verify which user, staging or shared, is logged into a device.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the check box next to a shared-kiosk device.
3. Select the **Devices** panel to display users who are currently logged in. When a shared-kiosk user successfully logs in, the display name on the **Devices** panel is updated accordingly.

Suggestions for configuring shared-kiosk mode

As the administrator, you must ensure that the configuration for staging and shared kiosk users is accurate in regards to placing users in the correct user group. (The Ivanti EPMM software cannot verify that a user is included in the correct group for your organization.) In addition, session control for shared-kiosk users is described.



When a user who does not have shared kiosk permission logs into a kiosk, the user receives an error but stays in the staging user mode.

Configuration Example for shared-kiosk mode

See the following figure for an example of a configuration that employs a staging user as well as two shared-kiosk-mode user groups, "User Group 1" and "User Group 2."

TABLE 87. ANDROID SHARED KIOSK MODE CONFIGURATION EXAMPLE

	Staging User	User Group 1	User Group 2
	Presents Login screen, entry state.	Set of users with unique set of apps & configs	Set of users with unique set of apps & configs
User	Must set Device Account ==TRUE.	Any user on Ivanti EPMM / Ivanti Neurons for MDM	Any user on Ivanti EPMM / Ivanti Neurons for MDM
Device	Enrolled as Managed Device (Device Owner)		
Apps	Common set of apps distributed to all groups		
App configs	Null	App config per-user or per-group	App config per-user or per-group
Kiosk config / policy	Assigned with "Login"==TRUE	Assigned with "Logout"==TRUE Subset of apps; some apps may be "force re-installed"	Assigned with "Logout"==TRUE Subset of apps; some apps may be "force re-installed"

Session Control for shared kiosk devices

You can control the length of a user session in shared kiosk mode using two methods. Within the ["Creating a shared-kiosk-mode policy for the shared kiosk users" on page 437](#) procedure, you can set the number of hours before a shared kiosk user is automatically logged out with the **Logout user** field. After the timeout period is reached, the device triggers a log out on the device and the device returns to the staging user.

Also, you can immediately force a shared kiosk user off the device by forcing a log out with the Shared Kiosk - Sign Out device command.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the check box next to a shared-kiosk device.
3. Select **Actions > Android Only > Shared Kiosk - Sign Out**.

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 454](#)
- ["Customizing Event Center messages" on page 471](#)
- ["Viewing and Exporting Events" on page 478](#)

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" on the next page](#)
- ["Deleting an event" on the next page](#)
- ["Ensuring the alert is sent to the correct recipients" on the next page](#)
- ["Applying the event to a label" on page 451](#)
- ["Setting alert retries" on page 451](#)
- ["Setting device push notifications" on page 452](#)
- ["Android notification sync policy" on page 453](#)

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 454](#) 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**.

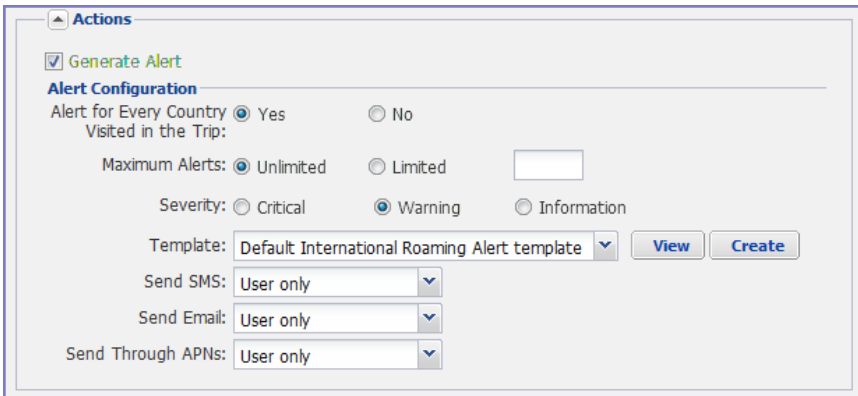
Deleting an event

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.



The screenshot shows the 'Alert Configuration' section within an 'Actions' panel. It includes a checkbox for 'Generate Alert' which is checked. Below this, there are radio buttons for 'Alert for Every Country Visited in the Trip' (set to 'Yes') and 'Maximum Alerts' (set to 'Unlimited'). There are also radio buttons for 'Severity' (set to 'Warning'). A 'Template' dropdown is set to 'Default International Roaming Alert template', with 'View' and 'Create' buttons next to it. At the bottom, there are three dropdown menus for 'Send SMS', 'Send Email', and 'Send Through APNs', all set to 'User only'.

For each type of alert (i.e. SMS, email, and C2DM 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

The screenshot shows a dialog box titled 'CC to Admins'. It has two main sections: 'Available' and 'Selected'. The 'Available' section is on the left and contains a list of devices. The 'Selected' section is on the right and is currently empty. Between the two sections are two arrows: a right-pointing arrow (→) and a left-pointing arrow (←). At the bottom of the dialog box are two buttons: 'Save' and 'Cancel'.

i 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**.

Setting device push notifications

The Send Message feature provides device push notification support. The service enables you to:

- Check the validity and CRL of the certificate for every incoming request.
- Check for pending notifications for the device, if not maintain the connection for the configured time.
- Send a response if a pending event has been created.



The notification pushed to the device might include an active URL. This URL can be opened in the Android client by selecting **GO TO LINK** in the notification.

Procedure

1. In the Admin Portal, go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Select **Actions > Send Message**. The **Send Message** dialog appears.
4. Select the **Push Notification** check box.
5. Select **Send Message**.

Android notification sync policy

The Android Notification Sync Policy allows you to specify the frequency and content of device updates.

Procedure

To set the Android Notification Sync Policy:

1. Go to **Policies & Configs > Policies**.
2. Select **Add New > Sync** to display the **New Sync Policy** dialog box.
If there is already an existing Sync policy the **Modify Sync Policy** screen will be displayed.
3. Enter the name of the policy and a description if needed.
4. Enter the name of the ServerIP/Host Name.
5. Select the **Use TLS** check box.
6. Use the **Sync While Roaming** drop-down menu to specify what if any content is synced while the device is roaming.
7. Choose a type of notification using the **Android Notification Mechanism** drop-down menu.
8. Enter a **Hearbeat Interval** in minutes.
9. Enter a **Sync Interval** in minutes.
10. Enter an IOS Location-Based WakeUps Interval in minutes.

11. Enter a **MTD wakeup interval** in minutes. This interval determines how often Ivanti Mobile@Work wakes up and scans a device. Setting this value to a low interval, such as 5 minutes, is more taxing on the device's battery than setting it at a higher interval such as 30 minutes.
12. 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 457
- "Memory size exceeded event settings" on page 458
- "System event settings" on page 461
- "System event field description" on page 461
- "Policy violations event settings" on page 464
- "Policy violations event field description" on page 465
- "Device status event settings" on page 469

International roaming event settings



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.

Field	Description
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 471 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.
Apply to Labels	Associate this event with the selected labels. See the "Using labels to establish groups" section in the <i>Getting Started with Ivanti EPMM</i> 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

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**.



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.

Field	Description
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 471 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 <i>Getting Started with Ivanti EPMM</i> 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 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 471 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 <i>Getting Started with Ivanti EPMM</i> 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 88. 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 Admin Portal and device certificates.


TABLE 88. SYSTEM EVENT FIELD DESCRIPTIONS (CONT.)

Field	Description
Provisioning Profile Expired	This feature is not supported for Android devices.
SMTP Relay server is unreachable	Applies a compliance action if the configured SMTP relay (used for SMS archive) does not respond to a ping or SMTP ping.
SMTP Relay server error	Applies a compliance action if the configured SMTP relay (used for SMS archive) returns an error. The alert includes available details to enable troubleshooting.
System storage threshold has been reached	Applies a compliance action if the system storage threshold has been reached. Refer to <i>Ivanti EPMM System Manager Guide</i> 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.
Android enterprise app requires new permission approval	Generates an alert if an Android Enterprise app has new permissions that the administrator needs to approve in the App Catalog.
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.

TABLE 88. SYSTEM EVENT FIELD DESCRIPTIONS (CONT.)

Field	Description
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 210 and "Creating an event" on page 449 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 471 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 Android C2DM, and whether to send it to the user, administrator, or both. Specify users in the Apply to Users section or by selecting a label in the Apply to Labels section. If you select "Admin only" or "User + Admin", then the CC to Admins section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Send the alert to users in the selected labels. See the "Using labels to establish groups" section in <i>Getting Started with Ivanti EPMM</i> for more information.

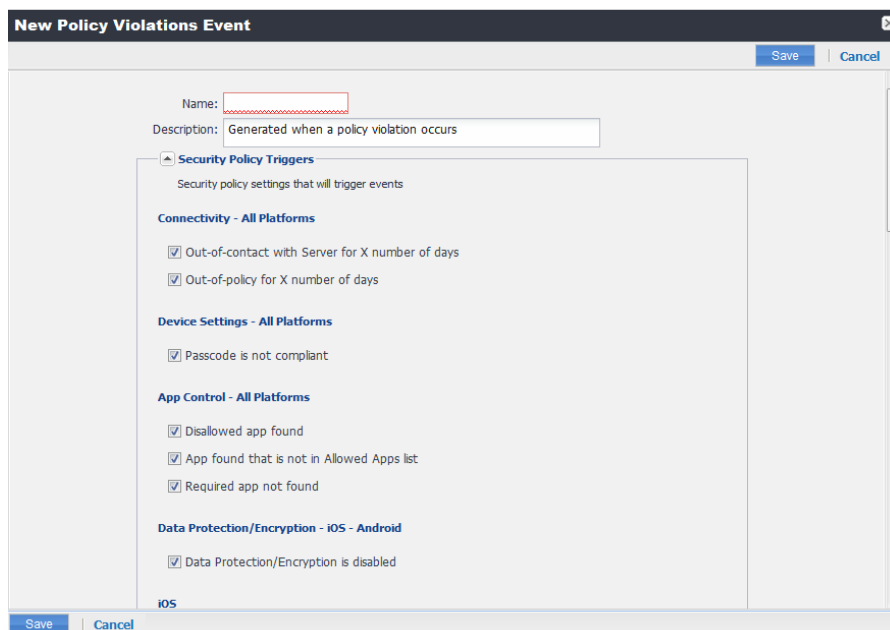
TABLE 88. SYSTEM EVENT FIELD DESCRIPTIONS (CONT.)

Field	Description
	 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.



New Policy Violations Event

Name:

Description:

Security Policy Triggers

Security policy settings that will trigger events

Connectivity - All Platforms

- ☒ Out-of-contact with Server for X number of days
- ☒ Out-of-policy for X number of days

Device Settings - All Platforms

- ☒ Passcode is not compliant

App Control - All Platforms

- ☒ Disallowed app found
- ☒ App found that is not in Allowed Apps list
- ☒ Required app not found

Data Protection/Encryption - iOS - Android

- ☒ Data Protection/Encryption is disabled

iOS

4. Follow the guidelines in "[Policy violations event field description](#)" 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 89. POLICY VIOLATION EVENT FIELD DESCRIPTION

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Connectivity	
Out-of-contact with Server for X number of days	Select this option to send an alert when a device has been out of contact for the number of days specified in the Security policy assigned to it.
Out-of-policy for X number of days	Select this option to send an alert when a policy has been out of date for the number of days specified in the Security policy assigned to it.
Device Settings	
Passcode is not compliant	Applies a compliance action if a device is detected having a passcode that does not meet the requirements specified in the associated security policy.
App Control	
Disallowed app found	Applies a compliance action if an app that is specified as Disallowed is installed on a device. Apps are specified as Required , Allowed , or Disallowed under Apps > App Control .
App found that is not in Allowed Apps list	Applies a compliance action if an app that does not appear on the list of allowed apps has been detected on a device.

TABLE 89. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

Field	Description
	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 an Android device has its Data Encryption feature turned off.
Security - Windows	
OS Build is less than the required OS build	Select this option to apply a compliance action if the device build is less than the OS build defined in the Security policy.
Last Hotfix is less than the required hotfix	Select this option to apply a compliance action if the device OS build is less than the hotfix build defined in the Security policy.
Last Hotfix installation date is out of date	Select this option to apply a compliance action if the device OS has not been updated in the time interval defined in the Security policy.
iOS	
Disallowed iOS model found	Select this option to apply a compliance action when a restricted iOS model is registered.
Disallowed iOS version found	Select this option to apply a compliance action when a restricted iOS version is registered.
Compromised iOS device	Select this option to apply a compliance action when a compromised iOS is registered or connects to the server. That is, an iOS device has been compromised by circumventing the operator and usage restrictions imposed by the operator and manufacturer.
iOS Configuration not compliant	Applies a compliance action if an iOS device does not have the expected security policy or app settings. This state may indicate that a setting was changed or was not applied successfully.
Restored Device connected to server	Applies a compliance action if a previously wiped device has been restored and attempts to connect through the 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.

TABLE 89. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)


Field	Description
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.
Device administrator not activated for DM client or agent	<p>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.</p> <hr/> <p> The Samsung DM Agent is not required on Samsung MDM 4.x, starting with Ivanti Mobile@Work for Android version 5.9.</p> <hr/>
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 .

TABLE 89. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

Field	Description
Template	<p>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.</p> <p>See "Customizing Event Center messages" on page 471 for information on creating a new template.</p>
Send SMS	<p>Specifies whether to send an alert in a text message, and whether to send it to the user, the administrator, or both.</p> <p>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.</p>
Send Email	<p>Specifies whether to send an alert in an email, and whether to send it to the user, the administrator, or both.</p> <p>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.</p>
Send through Push Notification	<p>Specifies whether to send a message via Android C2DM, and whether to send it to the user, the administrator, or both.</p> <p>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.</p> <p>The length of the message is limited to 255 characters.</p>
Apply to Labels	Send the alert to users in the selected labels. See the "Using labels to establish groups" section in <i>Getting Started with Ivanti EPMM</i> 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.

New Device Status Event

Name:

Description:

Triggers when:

- ☒ Device status is changed
- ☒ Android device reports policy/config errors
- ☒ Android device reports policy/config warnings
- ☒ Work schedule policy applied

Actions

☒ Generate Alert

Alert Configuration

Severity: ☐ Critical ☒ Warning ☐ Information

Template:

Send SMS:

Send Email:

Send Through Push Notification:

Apply to Labels:

Available	Selected
All Smartphones	
Android	
Company-Owned	
Employee-Owned	

Search Users:

Apply to:

4. Use the following guidelines to complete the form:
5. Select **Save**.



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: <ul style="list-style-type: none"> • 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)
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.

Field	Description
	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 <i>Getting Started with Ivanti EPMM</i> 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 191](#)

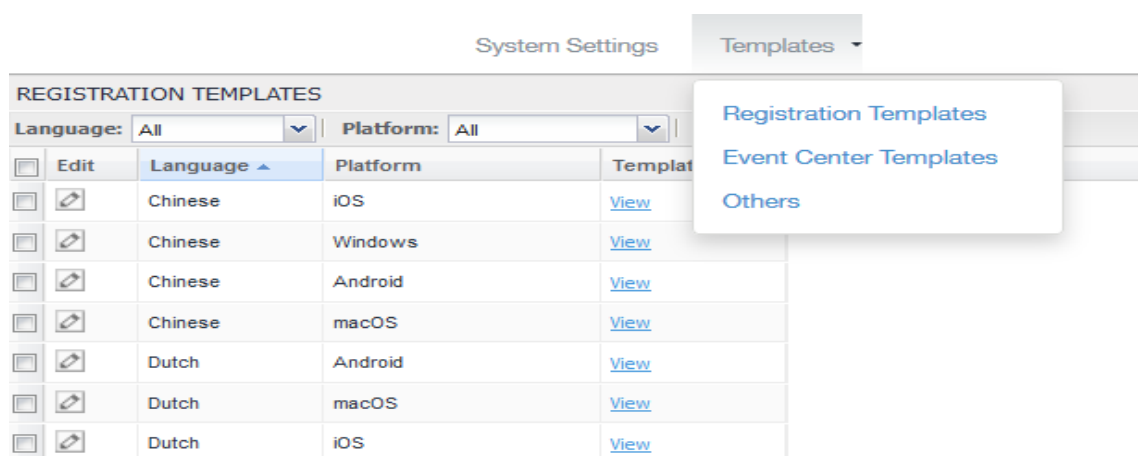
Customizing Event Center messages

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.

View Messages of Template Default Policy Violation Alert template				
Language	SMS	Email Subject	Email Body	Push Notification
Chinese	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESS
Dutch	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESS
English	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESS
French	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESS
German	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESS
Italian	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESS
Japanese	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESSA	\$SEVERITY:\$PHONE_NUMBER (\$USER_NAME) \$DEFAULT_POLICY_VIOLATION_MESS
	\$SEVERITY:\$PHONE_NUMBER	\$SEVERITY:\$PHONE_NUMBER	\$SEVERITY:\$PHONE_NUMBER	\$SEVERITY:\$PHONE_NUMBER

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.

Add New Event Center Template

Variables Supported

Name:

Event Type:

Languages Supported: English, Japanese, Korean, German, French, Spanish, Chinese, Portuguese

Edit Template For:

Email Subject:

Email Body:

SMS:

Push Notification:

2. Event Center messages are displayed with the HTML markup that provides the basic formatting for the content.
3. In the **Name** field, enter a name for the template.

The name must be unique for events of the same type.

4. In the **Edit Template for** field, select the language this template will be used for.

Note that only those languages that have been enabled for the system will be displayed in this list.

5. Make changes to the displayed messages.



For creating a company-branded Event Center email, you can copy and paste an HTML email message into the **Email Body** field. For more information, see ["Sending a company-branded email" on page 92](#).

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.

Message Type	Template
Wipe Email Subject:	Wipe has been requested for your phone \$PHONE\$
Wipe Email Body:	<pre><html><body><p></p><p>Dear \$USER\$,</p><p>Your mobile phone \$PHONE\$ has been returned to factory default settings. Contact your administrator to determine whether a backup snapshot can be used to restore your phone.</p></body></html></pre>

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

["Customizing registration messages" on page 84](#)

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 90. 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 90. 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 91. 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	<p>The hard-coded message associated with the policy violation that triggered the alert.</p> <hr/> <p> Due to the length limits of SMS and C2DM, the text might be truncated.</p> <hr/>
\$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 91. 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" on page 92](#)
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 92. 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.

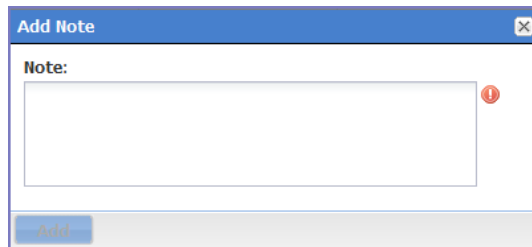
Exporting event history

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**.

A screenshot of a software dialog box titled "Add Note" with a close button (X) in the top right corner. Inside the dialog, there is a label "Note:" followed by a large, empty rectangular text input field. To the right of the input field is a small red circular icon with a white exclamation mark. At the bottom of the dialog, there is a blue button labeled "Add".

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.

- ["Pushing device profiles" below](#)
- ["About Ivanti EPMM logs" on the next page](#)
- ["Audit log information" on page 490](#)
- ["Audit Logs use cases" on page 503](#)
- ["MDM Activity" on page 507](#)
- ["Certificate Management" on page 508](#)
- ["Service Diagnostic tests" on page 511](#)
- ["Device log encryption on Android devices" on page 513](#)
- ["Encrypting device logs with your own certificate" on page 515](#)
- ["Pull client logs for client devices" on page 516](#)

Pushing 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.

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.

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.

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 Android MDM 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

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Account Sync Completed	Failed	misystem	2019-05-23 12:35:2...	2019-05-23 12:35:2...	DEP Account	Check update...
Account Sync Completed	Success	misystem	2019-05-23 12:35:2...	2019-05-23 12:35:2...	DEP Account	Check update...
Account Sync Completed	Failed	misystem	2019-05-23 12:20:2...	2019-05-23 12:20:2...	DEP Account	Check update...
Account Sync Completed	Success	misystem	2019-05-23 12:20:2...	2019-05-23 12:20:2...	DEP Account	Check update...
Account Sync Completed	Failed	misystem	2019-05-23 12:05:2...	2019-05-23 12:05:2...	DEP Account	Check update...
Account Sync Completed	Success	misystem	2019-05-23 12:05:2...	2019-05-23 12:05:2...	DEP Account	Check update...
Account Sync Completed	Failed	misystem	2019-05-23 11:50:2...	2019-05-23 11:50:2...	DEP Account	Check update...
Account Sync Completed	Success	misystem	2019-05-23 11:50:2...	2019-05-23 11:50:2...	DEP Account	Check update...
Account Sync Completed	Failed	misystem	2019-05-23 11:35:2...	2019-05-23 11:35:2...	DEP Account	Check update...

Searching the information in the audit logs

Procedure

1. In Admin Portal, go to **Logs**.

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**.

Filters

Search by Performed (On|By)/Details

Action Date
Select time... ▼

- ▶ Device (1133)
- ▶ ActiveSync Device (0)
- ▶ MDM (0)
- ▶ Certificate (73)
- ▶ App Tunnel (0)
- ▶ App (72)
- ▶ Policy (97)
- ▶ Compliance Action (0)
- ▶ Configuration (176)
- ▶ DEP (0)
- ▶ Admin (119)

Reset Search

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" on the next page](#))
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**.

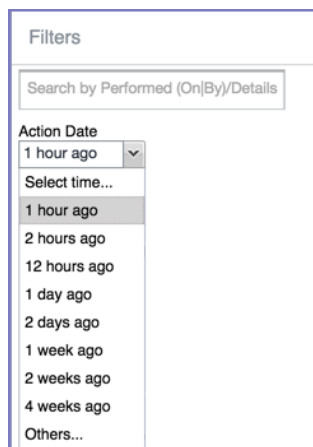
Setting event time criteria in audit logs

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 489](#)). 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 93. TIME CRITERIA SELECTION EXAMPLES

Time criteria selected	Value selected	Result
<p>In the left column, select both:</p> <ul style="list-style-type: none"> • 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.
<p>In the left column, select both:</p> <ul style="list-style-type: none"> • 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.
<p>In the left column, select both:</p> <ul style="list-style-type: none"> • 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.
<p>In the left column, select:</p> <ul style="list-style-type: none"> • Others • Select date <p>In the right column, select:</p> <ul style="list-style-type: none"> • a time interval from Select time 	<p>In the left column:</p> <ul style="list-style-type: none"> • Select April 10th from the calendar <p>In the right column:</p> <ul style="list-style-type: none"> • Select 1 day ago 	Displays all events matching your criteria that occurred between April 10th and 24 hours ago.
<p>In the left column, select:</p> <ul style="list-style-type: none"> • Others • Select hour 	<p>In the left column:</p> <ul style="list-style-type: none"> • Select 2AM <p>In the right column:</p>	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.

TABLE 93. TIME CRITERIA SELECTION EXAMPLES (CONT.)

Time criteria selected	Value selected	Result
In the right column, select: • a time interval from Select time	• Select 1 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 483](#) 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)

Filters		Export to CSV				
Search by Performed (On)By/Details		ACTION	STATE	PERFORMED BY	ACTION DATE	PERFORMED ON
Action Date Select time... Device <input type="checkbox"/> Allow App Tunnel <input type="checkbox"/> Apply Label <input type="checkbox"/> Block App Tunnel <input type="checkbox"/> Cancel Wipe <input type="checkbox"/> Change Language <input type="checkbox"/> Change Ownership <input type="checkbox"/> Check Compliance <input type="checkbox"/> Disable Activation Lock		Add LDAP	Success	miadmin	2015-06-05 05:33:42...	LDAP - ldap://ESWin2003002.a...
		Admin Portal Sign In	Success	miadmin	2015-06-05 05:39:22...	Admin Portal - 10.10.19.88
		Add Standalone Sentry	Success	miadmin	2015-06-05 05:39:34...	Standalone Sentry - app1077.a...
		Admin Portal Sign In	Success	miadmin	2015-06-05 05:40:18...	Admin Portal - 10.10.19.88
		Admin Portal Sign In	Success	miadmin	2015-06-05 05:42:19...	Admin Portal - 10.10.19.88
		Admin Portal Sign In	Success	miadmin	2015-06-05 05:42:19...	Admin Portal - 10.10.19.88
		Add Configuration	Success	miadmin	2015-06-05 05:42:19...	Exchange - ExchangeStep1 : V...
		Add Label	Success	miadmin	2015-06-05 05:42:20...	labelastcheckin
		Add Label	Success	miadmin	2015-06-05 05:42:21...	labelusername
		Add Label	Success	miadmin	2015-06-05 05:42:22...	labelldapname

- **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 503](#)
- ["App information" on page 498](#)

Audit log information

Several categories of information are available for you to view and audit. The category list, displayed on the left side of the Audit Logs page, includes:

- **Device**
- **ActiveSync Device**
- **MDM**
- **Certificate**
- **App Tunnel**
- **App**
- **Policy**
- **Compliance Action**
- **Configuration**
- **DEP (Device Enrollment)**
- **Admin**
- **User**
- **LDAP**
- **Other**
- **Label**
- **Sentry**
- **AfW**
- **Custom Attributes**
- **Compliance Policy**
- **E-FOTA**
- **Migration**
- **MTD (Mobile Threat Defense)**
- **Access Integration**
- **Derived Credential Provider**
- **Zebra FOTA**

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.

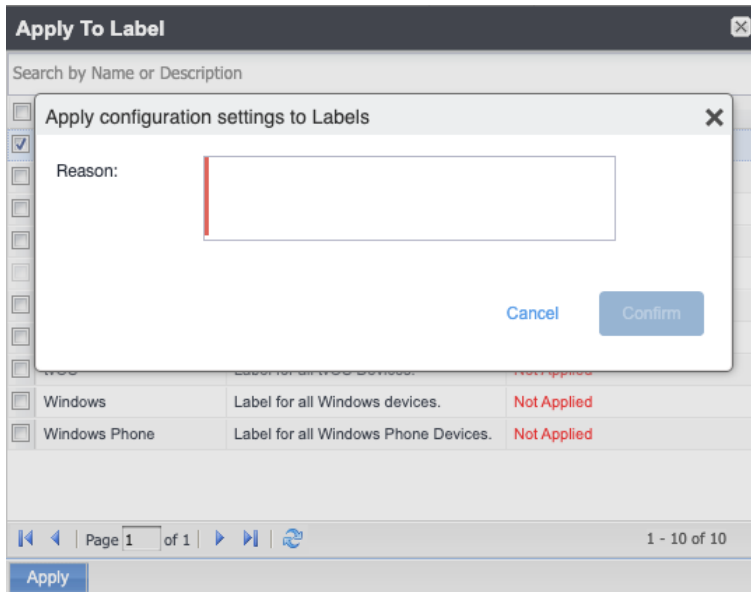
To display the **Changes - Before & After** panel, click on any policy or configuration in the **Policies & Configurations > Configurations** tab to display the **Configuration Details** side panel to the right of the window. Click **Modification History**, and click the box corresponding to the change.

Related topics

- ["About Ivanti EPMM logs" on page 482](#)
- ["Audit Logs use cases" on page 503](#)
- ["App information" on page 498](#)

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."

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

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.



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.



The contents of the **Logs > Certificate Management** shows information about certificates, such as their expiration dates. It allows you to take actions, such as re-enroll, remove, and revoke on the certificates.

App Tunnel events

To monitor actions involving app tunnels, select one or more of the logged app tunnel actions in the **Filters** panel.

- **Allow App Tunnel:** Permit the specified app tunnel.
- **App Tunnel Comment:** Add a comment on the selected app tunnel.
- **Block App Tunnel:** Do not allow the specified app tunnel.
- **Remove App Tunnel:** Delete the selected app tunnel configuration.

App information

To monitor actions involving apps, select one or more of the logged app actions in the **Filters** panel.

- **Add App:** Add an app to the app catalog.
- **Add App Control Rule:** Add an app control rule.
- **Add App Dependency:**
- **Add App Resource:** Add screenshots or icons for an app.
- **Apply Label to App:** Associate a label with an app.
- **Delete App Control Rule:** Remove an app control rule.
- **Edit App Control Rule:** Change one or more attributes of an app control rule.
- **Install App:** Send installation request for the selected app.
- **Manage VPP Labels:** Specify labels and account for Apple License app distribution.
- **Modify App:** Edit app catalog entry.
- **Remove App:** Delete entry from the app catalog.
- **Remove Label From App:** End the association between an app and a label.
- **Uninstall App:** Remove the app from the device based on managed app criteria.

Policy information

To monitor actions involving policies, select one or more of the logged policy actions in the **Filters** panel.

- **Activate Policy:** Set flag to make the selected policy active.
- **Add Policy:** Create a new policy.
- **Apply Label to Policy:** Associate a policy and a label.
- **Deactivate Policy:** Clear flag to make the selected policy inactive.
- **Delete Policy:** Delete a policy.
- **Export Policy:** Export a policy from 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.

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.

Android Enterprise events

These events are only for Android devices.

- **Accept permissions for Android enterprise App:** Accept permissions on behalf of all users.
- **Apps@work setting modified:**
- **Connect Ivanti EPMM to Android enterprise:** Establish binding between Ivanti EPMM and Android Enterprise.
- **Disconnect Ivanti EPMM from Android enterprise:** Remove binding between Ivanti EPMM and Android Enterprise.
- **Save Restrictions for Android enterprise App:** Apply new or changed Android Enterprise restrictions.
- **Sync Google Users with Ivanti EPMM:** Synchronize user data between Google and Ivanti EPMM.
- **Update catalog setting modified:**

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**.

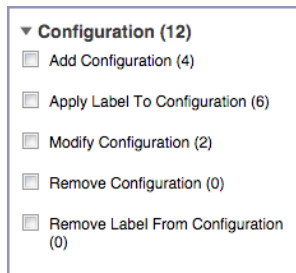
7. Click **Search**.
8. View the results of the search to determine:
 - When the devices were wiped
 - How many devices were wiped
 - Which administrator user issued the wipe commands

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

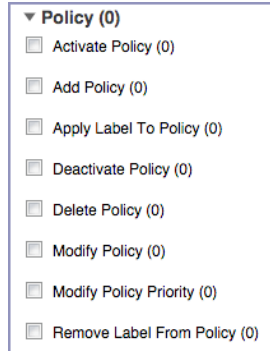
Users are prompted to create passwords

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.

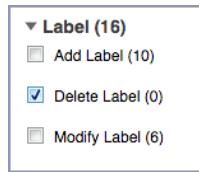


For Android devices 11.0 or supported newer versions, the administrator does not have the ability to manage app installs on the personal side.

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. Error details are not available for Android devices.

Certificate Management

The **Logs > Certificate Management** tab displays certificate-related log entries. You can:

- View certificate log entries
- Search certificate log entries
- Remove selected certificates from the log
- Revoke selected certificates from the log
- Re-enroll selected certificates from the log



Actions on certificates are logged in **Logs > Audit Logs** in the **Certificate** category.

How to search for certificate entries

When viewing the **Certificate Management** page, you can search for entries based on:

- Expiration date
- User
- Setting

Procedure

1. In the Admin Portal, go to **Logs > Certificate Management**.
2. Specify one or more of the criteria in the following steps to describe the certificates you want to display.
3. (Optional) To specify a time range within which the certificates expired:
 - In the **Expiration Date Range** field, click the calendar next to the field, and then click on a date. This date is the earliest day the certificates you are searching for expired.

- In the **To** field click the calendar next to the field, and then click on a date. This date is the latest day the certificates you are searching for expired.



An error message displays if you select a day in the **Expiration Date Range** field earlier than the day specified in the **To** field. For example you receive an error message if you:

- An error message displays if you select a day in the **Expiration Date Range** field earlier than the day specified in the **To** field. For example you receive an error message if you:

Select November 13th in the Expired Date Range field (earliest time a certificate expired).

Select October 15th in the To field (latest time a certificate expired).



The search can return fewer than all the certificates that expired during the specified time period if you specify other criteria in Step 4.

4. (Optional) In **Search by User/Setting Name**, enter a username or a setting name.

Item	Description
Certificate Enrollment	Displays the name of the Certificate Enrollment setting.
Setting	<p>Displays the configuration using the Certificate Enrollment.</p> <p>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.</p> <p>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.</p> <p>For Android devices, the Setting Name displays only for APPCONFIG, APPPOLICY, and WEB@WORK settings; otherwise a "-" displays.</p>

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 Android 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 94. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS

Service	Test
AFW	Checks to see if: <ul style="list-style-type: none"> • Authentication server is reachable. • API server is reachable.
APNS	Checks to see if: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Certificate Enrollment : System - iOS Enrollment SCEP is reachable.

TABLE 94. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS (CONT.)

Service	Test
	<ul style="list-style-type: none"> • 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	<p>Two tests are run:</p> <ul style="list-style-type: none"> • 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	<p>Two tests are run:</p> <ul style="list-style-type: none"> • 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 94. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS (CONT.)

Service	Test
SENTRY_WITH_ACTIVASYNC	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

Device log encryption on Android devices

Log files can be emailed by using the **Send Log** option in Ivanti Mobile@Work for Android. You can choose whether the log files are encrypted when they are provided to the email app. The choice affects the log files of the following:

- Ivanti Mobile@Work for Android
- Secure Apps Manager
- AppConnect-enabled apps (including what the app logs and what the AppConnect wrapper around the app logs)

The security policy for a device contains the option for choosing whether the emailed log files are encrypted. The default setting is to **not** encrypt the files.

By default, encrypted log files can be decrypted only by Ivanti Technical Support. If you want to encrypt the log files using your own certificate, see ["Encrypting device logs with your own certificate" on page 515](#).



Regardless of the device log encryption setting, the log files never include passwords, certificate content, license information, or other sensitive authentication data.

By encrypting the emailed log files, you improve security because the data is readable only by Ivanti Technical Support when using the default encryption, or by your own enterprise when using your certificate for encryption. Since emailing logs for troubleshooting is a common practice, you typically choose to encrypt the logs.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Select the security policy for the appropriate devices.
3. Click **Edit**.
4. In the **Data Encryption** section, for **Device Log Encryption**, select **On**.
5. Click **Save**.

Security and logging enablement

Ivanti Mobile@Work version 11.5.0.0 and later can configure security and network logging on the device according to the state of "Enable Security Logging on Android" and "Enable Network Logging on Android" options of the Security Policy.

- If Security Logging is enabled for the device, then Ivanti Mobile@Work will be able to receive batches of security log events from Android for collecting and processing. Security logging is supported now for the devices registered in Work Managed Device mode, Managed Device with Work Profile mode, and Work Profile on Company Owned Device mode.
- If Network Logging is enabled for the device, then Ivanti Mobile@Work will be able to receive batches of network log events (DNS and Connect) from Android for collecting and processing. Network logging is supported now for the devices registered in Work Managed Device mode and Work Profile on Company Owned Device mode.

Security and network logs, along with the regular client logs, are included in a zip file created by Ivanti Mobile@Work on demand of device user with "Send logs" command (Settings menu) or as a response to the "Pull Client Logs" administrator command.

The set of the latest security log events in the form of JSON-formatted strings up to 10 MB total may be found in files with names beginning with a "security" prefix. The most recent log events will be represented by readable security.txt file (up to 1MB). Older security log events will be zipped in a series of zip files, i.e., security1.zip, security2.zip, etc. The same applies to network logs, except the file names begin with the "network" prefix.



JSON formatting for security and network logs is a compromise between the human-friendly readability and potential automated logs processing on the server side.

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 10.0.0.0 for Android or supported newer versions
- Secure Apps Manager 8.3.0.0 or supported newer versions
- On the security policy, device log encryption must be on.

Related Topics

["Device log encryption on Android devices" on page 513](#)

Before you begin

Upload a certificate to Ivanti EPMM, as described in ["Certificates settings" on page 395](#).

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.

Field	Description
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.

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. See ["Device log encryption on Android devices" on page 513](#) for instructions on how to set device log encryption for Android devices.

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" below](#)
- ["Office 365 App Protection policies" on page 520](#)
- ["Office 365 App Protection configurations" on page 528](#)
- ["Office 365 App Protection user groups" on page 531](#)
- ["Office 365 App Protection reports" on page 531](#)
- ["Office 365 App Protection settings" on page 538](#)

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 Android devices.



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 EPM 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 528](#) 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 522](#)



Before using this feature, complete the prerequisites described in the following section:
["Prerequisites for using Office 365 App Protection" on page 518.](#)

Related topics

- ["Office 365 App Protection overview" on page 518](#)
- ["Office 365 App Protection configurations" on page 528](#)
- ["Office 365 App Protection user groups" on page 531](#)
- ["Office 365 App Protection reports" on page 531](#)
- ["Office 365 App Protection settings" on page 538](#)

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 522](#) for details.

4. In the ["Compliance Actions" on page 526](#) section, select a Setting, enter the value, and select an Action. Refer to the ["App protection policies fields " on page 523](#) table.
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 526](#) section, select a Setting, enter the value, and select an Action. Refer to the ["App protection policies fields " on page 523](#) table.
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 95. 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 Android backups	Choose Yes to prevent this app from backing up data to the Android Backup Service. Choose No to allow this app to back up data. (The default is Yes .)
Allow app to transfer data to other apps	<p>Use this option to specify what apps can receive data from this app. The options are listed below.</p> <ul style="list-style-type: none"> • 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. <p>When any of the above options except <i>All apps</i> are selected, the exempted apps are listed to the right of the <i>Allow app to receive data from other apps</i> field. Modifying these settings changes how data is transferred to other applications.</p>
Allow app to receive data from other apps	<p>Select an option to specify what apps can transfer data to this app.</p> <ul style="list-style-type: none"> • Policy managed apps - Allow app to receive data from only other policy-managed apps. • 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 "	<p>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.)</p> <p>Selecting Prevent Save As activates the Select which storage services corporate data can be saved to field. The options are:</p> <ul style="list-style-type: none"> • OneDrive for Business

TABLE 95. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
	<ul style="list-style-type: none"> • SharePoint • Local Storage
Restrict cut, copy and paste with other apps	<p>Specifies when cut, copy, and paste actions can be used with this app. The options are listed below.</p> <ul style="list-style-type: none"> • 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.)
Block screen capture and Android assistant	Check this to block the ability to use screen captures and block Android assistant. Default is allowed.
Encrypt app data	Select to encrypt app data that is associated with an Intune mobile application management policy. Encryption is provided by Microsoft. Data is encrypted synchronously during file I/O operations according to the setting in the mobile application management policy. Managed apps on Android use AES-128 encryption in CBC mode utilizing the platform cryptography libraries. The encryption method is not FIPS 140-2 certified. SHA-256 encryption is supported as an explicit instruction using the SigAlg parameter and will only work on devices 4.2 and above. Content on the device storage is always encrypted.
Disable app encryption when device encryption is enabled	This field activates when the <i>Encrypt app data</i> field is selected. Disables app encryption when the device encryption is enabled . Default is de-selected.
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	<p>Check this to enforce web links in the app to be opened in the Managed Browser app.</p> <p>Uncheck this to open web links in Chrome. Default is de-selected.</p>

TABLE 95. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
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.
Allow simple PIN	<p>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.)</p> <ul style="list-style-type: none"> • PIN length: Specify the minimum number of digits in a PIN sequence. (The default value is 4.) <p>When the <i>Require PIN for access</i> field is de-selected, this field is deactivated.</p>
Allow fingerprint of PIN (Android 6.0+)	<p>Select this to allow the user to use Touch ID instead of a PIN for app access. (The default is checked.)</p> <p>When the <i>Require PIN for access</i> field is de-selected, this field is deactivated.</p>
Override fingerprint with PIN after timeout (minutes)	<p>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.</p> <p>Inactivity timeout: Specify a time in minutes after which the PIN will override the use of a fingerprint.</p> <p>When the <i>Require PIN for access</i> field is de-selected, this field is deactivated.</p>
Disable app PIN when device PIN is managed	<p>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.)</p> <p>When the <i>Require PIN for access</i> field is de-selected, this field is deactivated.</p>

TABLE 95. APP PROTECTION POLICIES FIELDS (CONT.)

Fields	Description
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)	<p>Timeout for access requirements is measured in terms of the time of inactivity between any policy-managed application.</p> <ul style="list-style-type: none">• 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 96. COMPLIANCE ACTION SETTINGS

Setting	Description
Max PIN attempts (default)	<p>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:</p> <ul style="list-style-type: none"> • 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)	<p>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.)</p>
Offline grace period (default)	<p>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.</p>
Jailbroken/rooted device	<ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

TABLE 96. COMPLIANCE ACTION SETTINGS (CONT.)

Setting	Description
	<ul style="list-style-type: none"> • 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 Patch version	<p>Select to require devices have a minimum Android security patch released by Google. Select the calendar icon to select the date for the action below to occur:</p> <ul style="list-style-type: none"> • Block access - The device user will be blocked from access if the Android 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 Android version on the device does not meet the requirement. This notification can be dismissed.
Device manufacturer(s)	<p>Specify a device manufacturer that is required to use this app. Actions include:</p> <ul style="list-style-type: none"> • Block access - Only devices that match the specified manufacturer can use the app. All other devices are blocked. • 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" below](#)
- ["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 518.](#)

Related topics

- ["Office 365 App Protection overview" on page 518](#)
- ["Office 365 App Protection policies" on page 520](#)
- ["Office 365 App Protection user groups" on page 531](#)
- ["Office 365 App Protection reports" on page 531](#)
- ["Office 365 App Protection settings" on page 538](#)

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 518.](#)

Related topics

- ["Office 365 App Protection overview" on page 518](#)
- ["Office 365 App Protection policies" on page 520](#)
- ["Office 365 App Protection configurations" on page 528](#)
- ["Office 365 App Protection reports" below](#)
- ["Office 365 App Protection settings" on page 538](#)

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" below
- "Managing Out of Compliance Users reports" below
- "Managing Selective Wipe reports" on the next page
- "Downloading App Protection reports" on page 534
- "Downloading App Configuration reports" on page 536



Before using this feature, complete the prerequisites described in the following section:
"Prerequisites for using Office 365 App Protection" on page 518.

Related topics

- "Office 365 App Protection overview" on page 518
- "Office 365 App Protection policies" on page 520
- "Office 365 App Protection configurations" on page 528
- "Office 365 App Protection user groups" on the previous page
- "Office 365 App Protection settings" on page 538

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 97. 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 98. 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 99. 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 100. 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 518](#)
- ["Office 365 App Protection policies" on page 520](#)
- ["Office 365 App Protection configurations" on page 528](#)
- ["Office 365 App Protection user groups" on page 531](#)
- ["Office 365 App Protection reports" on page 531](#)

Zebra Support

Ivanti EPMM enables administrators to apply firmware updates to Zebra Devices using Zebra's Cloud OTA (Over the Air) service. Zebra devices are managed without OTA. From Ivanti EPMM version 10.6 or supported newer versions, Zebra OTA firmware update is supported. This allows you to activate the Zebra OTA service for your Ivanti EPMM, thus enabling you to receive firmware updates for OTA-capable Zebra Devices through firmware policies.

Process for Zebra support:

1. ["Adding a Google account to an Android Enterprise managed device" on page 19](#)
2. ["Enrolling in the Zebra OTA \(Over The Air\) service" below](#)
3. ["Setting the firmware policy for Zebra devices" on page 544](#)
4. ["Checking the Zebra device firmware download status" on page 547](#)

Enrolling in the Zebra OTA (Over The Air) service

You can activate the Zebra OTA (Over The Air) service for your Ivanti EPMM that would enable you to receive firmware updates for OTA capable Zebra devices through firmware policies. Ivanti EPMM uses OAuth 2.0 for authentication with Zebra.

Before you begin

- Be sure you have [added a Google account to the Android Enterprise managed device](#).
- You will need to write down your Zebra OTA account credentials, when you get them.
- The enrollment process needs to be completed within ten minutes, otherwise the token expires.

Procedure

1. In the Admin Portal, go to **Services > Zebra**. The **Zebra OTA Enrollment** page displays.
2. In section one, click the **Begin** button. A new browser window opens the Zebra login page.

3. Enter your Zebra login credentials and click **Sign In**. If you do not have credentials, contact Zebra.

https://pi.zebra.com/as/user_authz.oauth2?user_code=KQRT-GXQH


Android Enterpris... MDM Android Jira... Android Enterpris... EMM Community |... Android developer... Android Portfoli

Sign In

Please enter your Username & Password

Username
@.com

Password

 **ZEBRA**

Sign In


[Forgot your username?](#)
[Don't know your password?](#)
[Need to change your password?](#)
[Need additional password assistance?](#)

4. The Connect a device page displays with the Activation code already inserted. Click **Confirm**.

Connect a device

Confirm the activation code displayed on your device.

Activation code
123456789012

 **ZEBRA**

Confirm


5. The Request for Approval page displays. Make sure all the check boxes are selected and then click **Allow**.

Request for Approval

Logged in as @.com

Client is requesting permission for the following:

- ☒ Access to your username
- ☒ Zebra user's unique id
- ☒ openid

 **ZEBRA**

Allow Don't Allow

6. The Connect a device page displays. When the device is connected, a confirmation displays.


Connect a device

The device is now authorized.



7. Return to the **Ivanti EPMM > Services > Zebra** browser page.
8. In section two, click the **Complete Verification** button.
9. A confirmation displays confirming successful enrollment with Zebra's OTA service, along with your email ID.

After you have completed Step 1, click on the button below to complete the setup.
If successful, you will see a message confirming the connection with Zebra's OTA service.

 **Enrollment Successful**

Email ID: [redacted] @ [redacted] .com

<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; display: inline-block; margin-bottom: 10px;">Revoke</div> <p>Cancel enrollment. Current credentials will be removed and policies linked to the service will be affected.</p>	<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; display: inline-block; margin-bottom: 10px;">Refresh</div> <p>Re-enroll with Zebra OTA. Policies currently linked to the service will remain intact.</p>
---	---

After enrollment, you can enable the Zebra firmware policy (see "[Setting the firmware policy for Zebra devices](#)" on page 544) which the Ivanti Mobile@Work client receives and applies to Zebra devices (running on Android version 8.0 or supported newer versions) in Work Managed Device (Device Owner) mode and Managed Device with Work Profile (COPE) mode. When the policy is applied, the firmware is downloaded and installed on the device as scheduled in the configuration.

Re-enrolling with Zebra OTA

You can do re-enroll with Zebra OTA service and not lose your existing configurations. For example, in the Services > Zebra page, if you see "Enrollment status cannot be verified," then you need to refresh or re-enroll the Zebra OTA service.

Procedure

1. Go to the **Services > Zebra** page.
2. In section two, click the **Refresh** button.

After you have completed Step 1, click on the button below to complete the setup.
If successful, you will see a message confirming the connection with Zebra's OTA service.



Enrollment Successful

Email ID: [redacted]@[redacted].com

Revoke

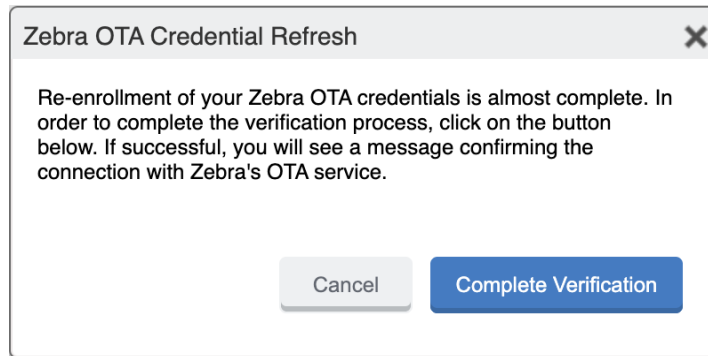
Cancel enrollment. Current credentials will be removed and policies linked to the service will be affected.

Refresh

Re-enroll with Zebra OTA. Policies currently linked to the service will remain intact.

3. Repeat the enrollment steps in ["Enrolling in the Zebra OTA \(Over The Air\) service"](#) on page 539.

4. The Zebra OTA Credential Refresh dialog box opens. Click **Complete Verification**.



Revoking the Zebra OTA service

If you want to discontinue using Zebra OTA service, you can remove the Zebra OTA service credentials. The Revoke action removes all Zebra OTA configurations from the existing configurations.

Procedure

1. Go to the **Services > Zebra** page.
2. In section two, click the **Revoke** button.

After you have completed Step 1, click on the button below to complete the setup.
If successful, you will see a message confirming the connection with Zebra's OTA service.



Enrollment Successful

Email ID: [redacted]@[redacted].com

Revoke

Cancel enrollment. Current credentials will be removed and policies linked to the service will be affected.

Refresh

Re-enroll with Zebra OTA. Policies currently linked to the service will remain intact.

3. Click **Confirm**.

To enroll again, you will need to start at the beginning of the enrollment process. See ["Enrolling in the Zebra OTA \(Over The Air\) service"](#) on page 539.

Next steps

["Setting the firmware policy for Zebra devices"](#) below

Setting the firmware policy for Zebra devices

Administrators can limit device updates to Zebra OTA (Over The Air) firmware releases using this feature. While creating the firmware policy, the administrator needs to also configure the firmware with respect to the device models. When applying the label to the policy, the policy is pushed to all the devices that meets that label criteria.

The administrator can create and apply multiple policies to a single label. The policy with the highest priority is applied in case of conflicts between multiple policies.

Before you begin

- Activate your Zebra OTA (Over The Air) service. See ["Enrolling in the Zebra OTA \(Over The Air\) service" on page 539](#).
- Verify that affected devices are running Ivanti Mobile@Work version 10.6 or supported newer versions.



Earlier Zebra firmware had patch updates as well as full upgrades. From Android versions 11 and above, patch upgrades are not supported. Upgrade option is available from android 11 and above for Zebra firmware policy.



To test any inactive firmwares published by Zebra, open a support case. Inactive firmwares may possibly cause devices to factory reset and could cause data loss.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Select **Add New > Android > Firmware policy**. The Add Android Firmware Policy dialog box opens.
4. Enter a unique name for the policy in the **Name** field.
5. Select a **Status**.
 - **Active**: to turn on this policy.
 - **Inactive**: to turn off this policy.
6. Select **Priority** then select **Higher than** or **Lower than** to select an existing policy from the drop-down list.

This option is only available if there is more than one policy.

7. Enter a **Description** (optional).
8. Select the **Enable Zebra OTA Firmware Policy** check box. The section expands.
9. See the following table for a description of the fields in the Zebra firmware policy.

Item	Description
Device Model	Lists the model of the Zebra device(s), for example, TC51, TC52.
Current Build ID	Lists the Build ID currently on the selected Zebra device.

Item	Description
Device Count	Lists the number of Zebra devices with the current build ID and device model.
Action	<p>Leaving the selection to None indicates no action will be taken.</p> <p>Selecting the None link opens a drop-down box to choose:</p> <ol style="list-style-type: none"> Full Upgrade - Zebra Android Device firmware upgrade, from selected version to the next major version (for example, from version 1.0 to 2.0.) Includes Build ID, Security Patch Date, OS Version and Description of the firmware. Patch Upgrade - Zebra Android Device firmware upgrade for patch releases, for example, from version 1.1 to 1.2. Includes Build ID, Security Patch Date, OS Version and Description of the firmware.
Target Build ID	<p>Defines the build selected by the administrator for the firmware upgrade. Ivanti EPMM only displays the firmware that is above the Current device build; device firmware downgrade is not supported.</p> <p>Administrator can select on the link of the target build and modify the selected version.</p>
Date	Defines the date when the firmware is released.
OS Version	Operating System version of the Zebra device.
Download over Metered Network	Disabled by default. Select to require the Zebra Firmware be downloaded over a metered network.
Require Charging	Enabled by default. Require the Zebra device be plugged in and charging at the time of the firmware download / upgrade.
Require Device Idle	Enabled by default. Require the Zebra device be idle / not being used at the time of the firmware download / upgrade.
Apply Schedule for Download	<p>Selecting the check box activates the section.</p> <p>Select the day(s) of the week, the Start Time and End Time of the download. The time referenced is the local time of the Zebra device.</p>

Item	Description
Apply Schedule for Update	Selecting the check box activates the section. Select the Start Date, End Date, Start Time and End Time of the upgrade. The time referenced is the local time of the Zebra device.

10. Select **Save**.
11. Select the policy then select **Actions > Apply to Label**.
12. Select one or more labels.
13. Select **Apply**.

Related topics

["Setting the firmware policy for Samsung devices" on page 559](#)

Checking the Zebra device firmware download status

You can check the status of the system update for a Zebra Android device by going to the Device details page and viewing the values in the **Zebra Build Fingerprint**, **Zebra Device Build Id**, **Zebra Device System Update**, **Zebra OTA Capable**, and the **Zebra Patch Version** fields.

Procedure

1. In the Admin portal, go to **Devices & Users > Devices**.
2. In the Advance search field, use the **Zebra Device System Update** option as part of your search criteria.

3. The following values can be returned (listed alphabetically):

Setting	Description
Available (Android 8 or Zebra devices)	A system update is currently available for this device.
Downloading (Zebra only)	System update is currently being downloaded to the Zebra device.
Pending (Zebra devices only)	The system update policy has been applied but the update has not been downloaded or applied.
Current	The most current update is installed (applicable for Zebra Android 8.0 or supported newer versions.)
Unknown	Not supported by client or OS version.

4. Alternately, you can expand a device and in the Device Details tab, scroll to the bottom to the **Zebra Device System Update** field.

Samsung Knox Settings

This chapter includes the following topics:

- "Android Samsung browser settings" below
- "Android Samsung Knox Container Settings" on the next page
- "Activating the Samsung firmware E-FOTA license " on page 557
- "Setting the system update policy for Android devices" on page 558
- "Setting the firmware policy for Samsung devices" on page 559
- "AppConnect for Samsung Knox devices" on page 561
- "Samsung Knox support" on page 562

Android Samsung browser settings

Go to **Policies & Configs > Configurations** and click **Add New > Android > Samsung Browser** to configure web browser options for Samsung KNOX devices (API 4.x). This setting also requires the **Samsung KNOX Container** configuration.

The following settings are available:

TABLE 101. SAMSUNG BROWSER OPTIONS



Setting	Description
Name	Enter a name for the Samsung browser setting.
Description	Enter an optional description of the new Samsung browser setting.
Enable Auto Fill	Select to enable automatic completion of web forms.
Allow Cookies	Select to allow use of cookies.
Enable Javascript	Select to enable Javascript.
Allow Pop-ups	Select to allow pop-ups.
Enable Show Security Warning	Select to display browser security warnings.
	 Not supported for Samsung Galaxy S4.

TABLE 101. SAMSUNG BROWSER OPTIONS (CONT.)

Setting	Description
Enable SmartCard Authentication	This feature is not supported.

Android Samsung Knox Container Settings

A Samsung Knox container configuration creates a secure container on Samsung Knox devices (API 4.0+). Apps in the Knox container cannot communicate with apps outside of the container. Data in the secure container cannot be sent outside of the container.

 Sharing Bluetooth data from within the Knox Workspace is controlled by a device-level setting by the user. You must enable Bluetooth in the Lockdown policy by going to **Policy & Configs > Policies > Lockdown** and selecting the Bluetooth **Enable** radio button.

To configure the Samsung Knox Workspace mode:

1. In the Admin Portal, go to **Policies & Configs > Configurations > Add New > Android > Samsung KNOX Container**. The New Samsung Knox Container Setting dialog box opens.
2. In the **Authentication** section, enter the password rules and behavior you want to enforce.
3. In the **App Settings** section, use the drop-downs to select settings for Browser, Exchange, and VPN in the container.

See ["Samsung Knox support" on page 562](#) for information about configuring Samsung Knox.

Use these settings to:

- Specify requirements for the container password.
- Specify which apps to install in the container.
- Specify restrictions.
- Select the Android Samsung browser configuration to use in the container.
- Select the Exchange configuration to use in the container.
- Select the VPN configuration to use in the container.


 Make sure only one Samsung Knox container setting applies to each device.

TABLE 102. SAMSUNG KNOX CONTAINER SETTINGS

Item	Description
Name	Enter brief text that identifies this group of Samsung Knox container settings.
Description	Enter additional text that clarifies the purpose of this group of Samsung Knox container settings.
<i>Authentication</i>	
Enforce Multi-Factor Authentication	<p>Select On to require the device user to enter both a password and a fingerprint to access the Samsung Knox container.</p> <p>Therefore, the device user must create a fingerprint on the device.</p> <p>The default is Off.</p> <p>Enforcing multi-factor authentication requires the following on the device:</p> <ul style="list-style-type: none"> • Ivanti Mobile@Work 9.1 for Android • Samsung Knox 2.2 or supported newer versions <p>Important: After multi-factor authentication has been enforced on a device, changing this setting to Off has no impact on the device. Multi-factor authentication is still enforced, as designed by Samsung.</p>
Password Type	<p>Select the kind of password to require:</p> <ul style="list-style-type: none"> • Simple: (Supported only on devices with Ivanti Mobile@Work 8.0 and Knox version 2.0). • Alphanumeric: Must include at least one alphabetic and one numeric character. • Complex: Must include at least one alphabetic, one numeric, and one special character (i.e., a symbol).
Min Password Length	Specify a minimum length for the password. Valid range is 4-16. The default value is 6.
Min Number of Complex Characters	<p>Specify the minimum number of complex characters for the passcode. Valid range is 0-10.</p> <p>For example, to require at least two complex characters in the passcode, enter 2.</p>

TABLE 102. SAMSUNG KNOX CONTAINER SETTINGS (CONT.)

Item	Description
Max Character Occurrences	Specify a limit for the number of times a specific character can occur in the passcode. For example, to prevent a specific character from occurring 3 or more times, enter 2.
Max Character Sequence Length	Specify a limit for the number of characters that can appear in sequence in a passcode. For example, to prevent <i>abc</i> from occurring in a passcode, enter 2.
Max Numeric Sequence Length	Specify a limit for the number of numeric characters that can appear in sequence in a passcode. For example, to prevent "123" from occurring in a passcode, enter 2.
Min Character Change Length	Specify a minimum number of characters that must change when the passcode is reset. For example, to ensure that at least 2 characters change, enter 2.
Forbidden Strings	Specify any strings that must not be present in the passcode. To add a string: <ol style="list-style-type: none"> 1. Select + to add an entry. 2. Select the "Name" placeholder in the new entry. 3. Replace "Name" with the string you want to add. For example, to prevent the passcode from including the user's email address or last name, enter \$EMAIL\$, \$LAST_NAME. Use the tool tip to see a list of substitution variables you can use here.
Max Inactivity Timeout	Specify the idle time duration after which the lock should be enabled. If the password is set, the user is prompted for a password when unlocking the container.
Max Password Age	Specify the number of days after which the password expires.
Stored Password History	Specify the number of previous passwords that are stored and cannot be used when setting a new password.
Max Number of Failed Attempts	Specify the maximum number of failed password attempts to allow. When this number is exceeded, the Knox container is disabled.
Password Visible Option	Select Off to disable the "Make password visible" option.
<i>Apps</i>	
	Select the in-house apps to be installed in the container:

TABLE 102. SAMSUNG KNOX CONTAINER SETTINGS (CONT.)



Item	Description
	<p>Select the + button.</p> <p>Select an app from the Name list.</p> <p>The Version and Identifier fields are filled in automatically.</p>
<i>Restrictions</i>	
Google Play Store	The default setting is Off . Select the On radio button to enable whitelisting Google accounts.
Whitelist Google Accounts	Enter the domains of accounts that can be added in the Knox container.
Allow Camera	<p>Select to allow the device user or third-party apps to use the photo camera, video camera, and video telephony features.</p> <hr/> <p> If the camera is allowed in the Knox container restriction policy, but not allowed via the device lockdown policy, the camera does not function in the Knox container.</p> <hr/>
Allow Content Sharing (i.e., Share Via)	Select to allow use of the Share Via List, which is displayed in certain apps that share content with other apps.
Allow Email Account Creation	Select to allow the user to create email accounts. By default, this is unselected and end users cannot create email accounts in the Knox container.
Allow Non-Secure Keypad	Select to allow keyboards inside the container, regardless of whether they are pre-loaded or third-party keyboards.
Allow Samsung KNOX App Store	Select to allow device users to download apps from the Samsung Knox app store (www.samsungknox.com).
Allow Screen Capture	Select to allow user to take a screenshot to help with troubleshooting.
Allow Remote Control	Select to allow alternate provisioning of the Knox container.
Allow NFC	Select to allow enrollment of the device using the NFC bump.
Allow USB	Select to allow so that apps that need USB access function properly.
Install all CA certificates inside KNOX workspace	Select to deploy CA certificates inside and outside of the Knox container to secure traffic on apps inside the Work Profile mode with a self-signed or well-known certificate. If you deselect this option, CA certificates are only installed on the outside of the container and certificates installed on the inside of the container are removed.
<i>App Settings</i>	

TABLE 102. SAMSUNG KNOX CONTAINER SETTINGS (CONT.)

Item	Description
Browser	Specifies the Android Samsung Browser configuration to use in the Knox container. You need to create the Samsung Browser configuration separately. Otherwise, this list will be empty.
Exchange	Specifies the Exchange configuration to use in the Knox container. You need to create the Exchange configuration separately. Otherwise, this list will be empty.
VPN	<p>Specifies the VPN configuration to use for Samsung Knox IPsec in the container. You need to create the configuration separately. Otherwise, this list will be empty.</p> <hr/> <p> The Knox VPN client must be installed on the device <i>before</i> you push the Knox VPN configuration.</p> <hr/> <p>Download the Knox VPN client from the Samsung Knox portal: https://developer.samsungknox.com/dashboard/download</p> <p>or refer to general documentation at https://docs.samsungknox.com/dev/knox-sdk/vpn-features.htm</p> <ol style="list-style-type: none"> 1. Go to Resources -> Tools (at the bottom) -> Download Knox VPN Client. To create a user ID in the Samsung Knox portal, an active Knox license key (trial or product) is required. 2. Upload the Knox VPN client to the App Catalog. 3. Create a new VPN configuration with Samsung Knox IPsec specified as the connection type (Policies & Configs > Configurations > Add New > VPN). 4. Select the new VPN configuration in the Samsung Knox container (go to Policies & Configs > Configurations, then select Add New > Android > Samsung KNOX Container).

Supported variables

You can use the following substitution variables in the Forbidden Strings field in the Samsung Knox Container Setting:

- \$EMAIL\$
- \$USERID\$
- \$FIRST_NAME\$
- \$LAST_NAME\$
- \$DISPLAY_NAME\$
- \$USER_CUSTOM1\$
- \$USER_CUSTOM2\$
- \$USER_CUSTOM3\$
- \$USER_CUSTOM4\$
- \$NULL\$

You can also enter strings, such as:

- 12345
- Example password

Samsung Knox Dual Encryption (DualDAR) support

Using two layers of encryption, Dual Encryption (DualDAR) secures and protects sensitive data on devices - even when they are powered off or in an unauthenticated state. This reduces the possibility of enterprise work data becoming compromised. Samsung Knox includes a FIPS 140-2 certified encryption module within the inner layer. (FIPS (Federal Information Processing Standard Publication) 140-2 is a U.S. government computer security standard used to approve cryptographic modules.)

Within the workspace, there are two storage locations available to an app: Credential Encrypted (CE) storage and Device Encrypted (DE) storage. From an apps standpoint, the Workspace storage is DualDAR-protected and works as CE storage. For apps that do not have DualDAR protection, the Knox framework prevents any apps from writing data to any storage space.

DualDAR is applicable to Knox v3 on Android 8.0 or supported newer versions.

DualDAR is applicable to Android Enterprise:

- Work Profile mode
- Managed Device with Work Profile mode
- Work Profile on Company Owned Device mode

Procedure

1. Edit the Android Enterprise configuration. The Android enterprise (all modes) Setting dialog box opens.
2. Select the **Enable DualDAR** check box. By default, this check box is de-selected.



DualDAR is only supported on Knox 3.3+ devices. DualDAR requires a special license that can be used instead of the Samsung General policy configurator.

3. Enter the Knox License key into the **Samsung DualDAR Version** field.
4. Select **Save**.

The Ivanti EPMM server will push the new Samsung DualDAR report to the device upon device registration. If enabled, the Ivanti Mobile@Work for Android client will report the Samsung DualDAR version in the **Device Details > Samsung KNOX Version** field. If not enabled or the device is in Device Owner mode, "unsupported" will display in the **Samsung KNOX Version** field.

Samsung Knox Workspace support for Google Play

You can enable users to use Google Play inside the Samsung Knox Workspace. Account whitelisting is supported for Google Play Services account types. Other account types, such as accounts defined by an application such as Gmail or Facebook, are not exempted by this whitelist as they are of a different account type. Therefore, it is important to avoid whitelisting applications that can allow undesired accounts into the Knox Workspace.



Users are only permitted to download apps that are whitelisted for the Samsung Knox Container, but they are still able to browse the entire contents of the Google Play Store.

To enable Samsung Knox Workspace support for Google Play:

1. In the Admin Portal, go to **Policies & Configs > Configurations > Add New > Android > Samsung KNOX Container** to open the New Samsung KNOX Container Settings dialog box.
2. In the **Restrictions** section, select **Google Play Store: On** radio button to enable the Google Play Store. It is set to **Off** by default.
3. Optionally, in the **Whitelist Google Accounts** field, select the **Account** check box to enter the domain URL or wildcard domain. This specifies which Google accounts or wildcard domains may be

used inside the Knox Container.

4. **Save** your changes.

Tunnel support in the Samsung Knox Workspace

You can configure Tunnel support on Android devices. For detailed information on support and setup for Tunnel in the Samsung Knox container, see the *Ivanti Tunnel for Android Guide*.

On-Demand Support for Samsung Knox VPN connections

You can enable On-Demand for Samsung Knox for VPN apps that support On-Demand connections.



On-Demand is not supported for container-wide VPN apps.

To enable On-Demand for Samsung Knox:

1. In the Admin Portal, go to **Policies & Configs > Configurations > Add New > VPN**. The Add VPN Setting dialog box opens.
2. In the **Connection Type** drop-down menu, select the **Samsung KNOX IPSec** check box. This is a VPN app that supports On-Demand.
3. Enter the information for the Server, Username, and Password.
4. Select the **VPN on Demand** check box.
5. Select the **Per-app VPN Yes** radio button.
6. Select **Save**.

Activating the Samsung firmware E-FOTA license

NOTE - Samsung Firmware E-FOTA has been decommissioned: As of August 2022, Samsung discontinued the Samsung E-FOTA service. As a result, upon upgrade to Ivanti EPMM 11.8.0.0, the following occurs:

- In Policies > Add New > Android Firmware Policy dialog box, the "Enable Samsung Firmware Policy" field is disabled.

- Upon upgrade, in the existing policy and new policy (in the case where the license has not yet been deactivated), the "Enable Samsung Firmware" field will still be visible but it will be read-only. The administrator will need to delete the existing policies and deactivate the license before creating the new policy.
- The Services > Samsung > Samsung Firmware E-FOTA License Management page is disabled; the administrator cannot activate or deactivate an E-FOTA license. If you have an existing E-FOTA license already set up, the Deactivate button is enabled and the administrator will need to manually deactivate the Samsung Firmware E-FOTA License.

For more information on end of life and alternatives, see [Samsung Knox EOL article](#).

Setting the system update policy for Android devices

Administrators can limit device users from managing system updates on Android 6.0 devices (or later releases that are supported by Ivanti, Inc). When multiple policies are applied to devices, you can select a priority for applying the policy to avoid conflicts.

The System update policy applicable to:

- Work Managed Device mode
- Managed Device with Work Profile (COPE) mode
- Work Profile on Company Owned Device mode

It is not applicable to Work Profile mode.

Before you begin

- Verify that effected devices are running Android 6.0 (or later releases that are supported by Ivanti, Inc).

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Click **Add New > Android > Firmware policy**.
4. Enter a unique name for the policy in the **Name** field.
5. Select a **Status**.
 - **Active**: to turn on this policy.
 - **Inactive**: to turn off this policy.

6. Select **Priority** then select **Higher than** or **Lower than** to select an existing policy from the drop-down list.
7. This option is only available if there is more than one priority.
8. Enter a **Description** (optional).
9. Select the **System Update Policy for Android 6.0 or higher** check box and enable the following options:
 - **Automatic**: silently apply the policy whenever new firmware is available.
 - **Update Window**: schedule a time period to silently apply the new firmware.
 - Select a start and end time to schedule the firmware update.
 - **Postpone**: this is hard-coded by the OS and skips any OS updates for up to 30 days after which it becomes automatic.
10. (Optional) In the **Freeze Period** section, click **+Add Freeze Date**. The Start Date and End Date fields display. The Freeze Period cannot be more than 90 days and the next Freeze Period can be selected only after 60 days from the previous calendar end date.



The Freeze Period spans the calendar year. It cannot span over two calendar years, for example, from December to January.

Click in the field or on the calendar icon. A calendar displays. Click on the desired date. You must have both a start date and end date entered.

11. Click **Save**.
12. Select the policy then select **Actions > Apply to Label**.
13. Select one or more labels.
14. Click **Apply**.

Setting the firmware policy for Samsung devices

NOTE - Samsung Firmware E-FOTA has been decommissioned: As of August 2022, Samsung discontinued the Samsung E-FOTA service. As a result, upon upgrade to Ivanti EPMM 11.8.0.0, the following occurs:

- In Policies > Add New > Android Firmware Policy dialog box, the "Enable Samsung Firmware Policy" field is disabled. Existing policy will not be impacted, but the administrator will need to manually delete the policy.

- The Services > Samsung > Samsung Firmware E-FOTA License Management page is disabled; the administrator cannot activate or deactivate an E-FOTA license. If you have an existing E-FOTA license already set up, the Deactivated button is enabled and the administrator will need to manually deactivate the Samsung Firmware E-FOTA License.

For more information on end of life and alternatives, see [Samsung Knox EOL article](#).

Administrators can limit device updates to specific firmware releases using this feature. If the device model and carrier code matches what is defined in the policy, the firmware is applied to the device to which the labels are applied. If the device model and the carrier code matches what is defined in the firmware, the label is applied to the device to which the labels is applied. Administrators can create and apply multiple policies to each device. The policy with the highest priority is applied in case of conflicts between multiple policies.

Before you begin

- Activate your Samsung license
- Verify that effected devices are running Samsung Knox version 2.7.1 and above.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Select **Add New > Android > Firmware policy**. The Add Android Firmware Policy dialog box opens.
4. Enter a unique name for the policy in the **Name** field.
5. Select a **Status**.
 - **Active**: to turn on this policy.
 - **Inactive**: to turn off this policy.
6. Select **Priority** then select **Higher than** or **Lower than** to select an existing policy from the drop-down list.

This option is only available if there is more than one priority.

7. Enter a **Description** (optional).
8. Select the **Enable Samsung Firmware Policy** check box.
9. Select **Save**.
10. Select the policy then select **Actions > Apply to Label**.
11. Select one or more labels.
12. Select **Apply**.

Related topics

["Setting the firmware policy for Zebra devices" on page 544](#)

AppConnect for Samsung Knox devices

In Ivanti EPMM deployments that use AppConnect, AppConnect for Knox is automatically used on Samsung devices that meet the following requirements:

- Device has Samsung Knox 2.1
- Device is running Ivanti Mobile@Work 7.0 for Android or supported newer versions.
- A Samsung General Policy with a valid Samsung KLM license is applied to a label that is also applied to the device. The Samsung license is required to take advantage of any Knox-related feature.

No changes are required to AppConnect configurations on Ivanti EPMM.

About AppConnect for Knox

AppConnect is an Ivanti feature that containerizes apps to protect data on the device from unauthorized access. In AppConnect for Knox, Ivanti Mobile@Work uses Samsung Knox Platform features to provide an added layer of security. Specifically:

- Knox SE for Android (Security Enhancements for Android)

AppConnect uses an *SE for Android* container for an added layer of security for the container and AppConnect-enabled apps.

Knox TIMA Keystore

- AppConnect's Secure Apps key is protected using the TIMA keystore.

No user interface changes in Ivanti Mobile@Work or Ivanti EPMM are associated with this feature.

The Samsung Knox container, known as the Knox Workspace, is not supported with AppConnect apps. Specifically:

- The Samsung Knox container does not support any AppConnect apps running inside the Knox container.
- Ivanti EPMM does not support using both a Knox container and AppConnect container on the same device.

Samsung Knox support

The Samsung Knox Container enables the creation of a secure container for corporate apps within each device. This container secures access to corporate apps and data.

To configure support for the Samsung Knox Container:

1. Create a **Samsung Browser** configuration.

If you do not intend to specify browser behavior in the container, you can skip this step.

See ["Android Samsung browser settings" on page 549](#).

2. Create an **Exchange** configuration for the container.

If you do not intend to specify email client behavior in the container, you can skip this step.

3. Create a **Samsung Knox Container** configuration.

The Samsung Knox Container configuration will specify the **Samsung Browser** configuration and the **Exchange** configuration you created for the container.

See ["Android Samsung Knox Container Settings" on page 550](#).

4. Create one or more labels to identify the devices that will receive the Samsung Knox Container configuration.
5. Assign the **Samsung Knox Container** configuration to the appropriate labels.

Once the configuration is present on the device, then the device begins creating the container as specified.

Disabling the container

To manually disable the Samsung Knox container:

1. Go to **Device & Users > Devices**. Select the devices that have received the **Samsung Knox Container** configuration.
2. Click **Actions > Android Only > Disable Samsung Knox Container**.
3. Choose the container you want to disable from the **Container** list.
4. Click **Disable Samsung Knox Container**.

The container remains disabled until you manually re-enable it.

Re-enabling the container

A Samsung Knox container can be automatically disabled by policy, such as when the device user enters the container password incorrectly too many times. You can manually disable the container using the **Disable Samsung Knox Container** action.

To manually re-enable the Samsung Knox container:

1. Go to **Device & Users > Devices**. Select the devices on which the container has been disabled.
2. Click **Actions > Android Only > Enable Samsung Knox Container**.
3. Choose the container you want to enable from the **Container** list.
4. Click **Enable Samsung Knox Container**.

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.



If you do not have a link to your Ivanti EPMM instance, contact your Ivanti Customer Success Manager.

- Ivanti Mobile@Work for Android (client) – version 8.0 or supported newer versions.

Supported OS versions

- Android 8.0 or supported newer versions

The Microsoft website states:

- Office for Android (including Outlook for Android) can be installed on tablets and phones running any of the supported versions of Android and have an ARM-based or Intel x86 processor. Starting on July 1, 2019, support will be limited to only the last four major versions of Android.
- For more information on supported OS versions, see [Microsoft 365 Office resources](#).

Unsupported OS versions

Behavior if unsupported device OS versions is used:

- Device users can complete the device registration for AAD and are able to authenticate Microsoft apps (Outlook).

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



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 the next page](#).
4. Administrator creates the Conditional Access policy for the apps. See ["Creating a conditional access policy in Microsoft Endpoint Manager" on page 570](#).
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 574](#).
6. Administrator creates the device compliance policy in Ivanti EPMM. See ["Creating a partner device compliance policy" on page 580](#).
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 582](#).



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 583.
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 584.)
 - 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

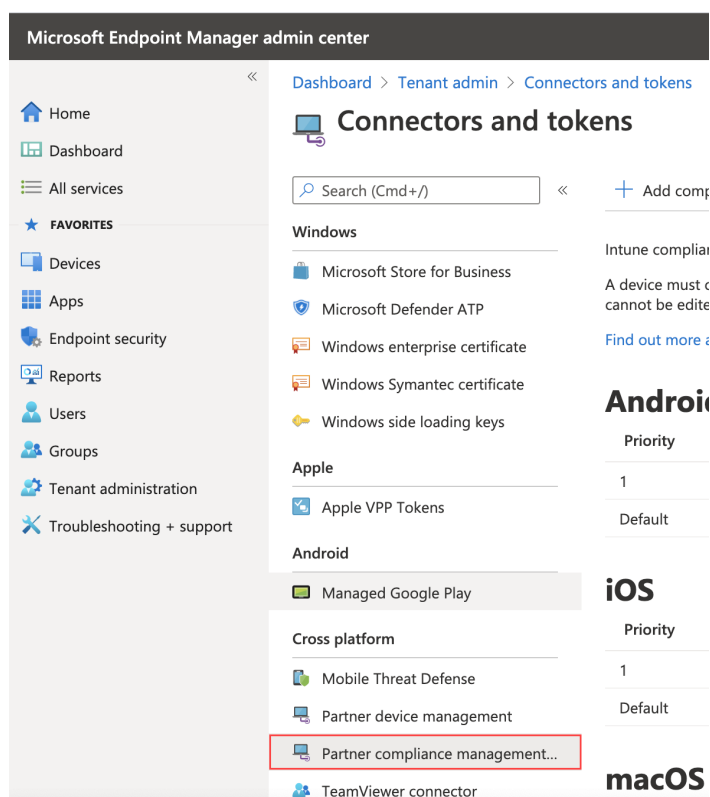
<https://docs.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide>

Adding Ivanti EPMM as a compliance partner

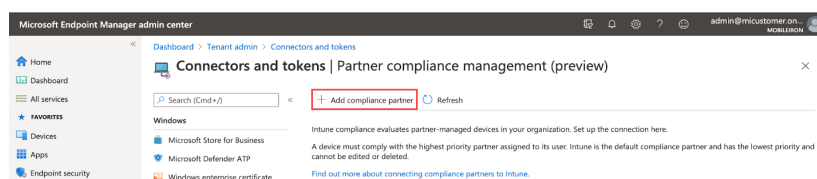
This section addresses adding Ivanti EPMM as an Azure compliance partner. Ivanti EPMM integration as compliance partner with Azure Active Directory in Common Criteria mode is supported.

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.

Home > Tenant admin > Connectors and tokens >

Create Compliance Partner

1 Basics 2 Assignments 3 Review + create

Compliance partner * Device Compliance On-prem

Platform *

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.

Home > Connectors and tokens >

Create Compliance Partner

✓ Basics 2 Assignments 3 Review + create

Included groups

Assign to Selected groups

Selected groups

No groups selected

+ Select groups to include

Excluded groups

i When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Selected groups

No groups selected

+ Select groups to exclude

7. Select **Next**.
8. Click the **Create** button.

- 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."

Home > Tenant admin > Connectors and tokens

Connectors and tokens | Partner compliance management (preview)

partner c Add compliance partner Refresh

Windows

- Microsoft Store for Business
- Microsoft Defender ATP
- Windows enterprise certificate
- Windows Symantec certificate

Cross platform

- Partner device management
- Partner compliance management...
- TeamViewer connector
- Certificate connectors
- Telecom expense management
- Derived Credentials

Intune compliance evaluates partner-managed devices in your organization. Set up the connection here.

A device must comply with the highest priority partner assigned to its user. Intune is the default compliance partner and has the lowest priority and cannot be edited or deleted.

[Find out more about connecting compliance partners to Intune.](#)

Android

Priority	Partner	Assigned	Partner status	Last Successful Sync
1	Device Compliance On-prem	Yes	Active	06/11/2020, 15:19:11
Default	Intune	N/A	N/A	N/A

iOS

Priority	Partner	Assigned	Partner status	Last Successful Sync
1	Device Compliance On-prem	Yes	Active	06/11/2020, 15:19:11
Default	Intune	N/A	N/A	N/A

Creating a conditional access policy in Microsoft Endpoint Manager

This section addresses defining the conditional access policy in Microsoft Endpoint Manager.

Procedure

- Log in to Microsoft Endpoint Manager <https://endpoint.microsoft.com>.
- In the Microsoft Endpoint Manager administrator center page, go to **Home > Endpoint Security > Conditional Access**.
- Click on Policies and then click **+ New Policy**.

Microsoft Endpoint Manager admin center

Home > Endpoint security > Conditional Access

Conditional Access | Policies

Azure Active Directory

+ New policy What if Refresh Got feedback?

New Conditional Access policies now apply to all client app types when not configured, including legacy authentication and Exchange ActiveSync. →

Policy Name	State
-------------	-------

The New conditional access policy page opens.

4. Enter the Name of the conditional access policy.

Microsoft Endpoint Manager admin center

Home > Endpoint security > Conditional Access >

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ >
0 users and groups selected

Cloud apps or actions ⓘ >
No cloud apps or actions selected

Conditions ⓘ >
0 conditions selected

Access controls

Grant ⓘ

Enable policy

Report-only On Off

5. In Assignments, click to assign the policy to users and groups.

Home > Endpoint security > Conditional Access >

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ ! >

Specific users included

Cloud apps or actions ⓘ ! >

No cloud apps or actions selected

Conditions ⓘ >

0 conditions selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users [Learn more](#)

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☐ 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.

Home > Endpoint security > Conditional Access >

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ >

0 users and groups selected

Cloud apps or actions ⓘ ! >

No cloud apps or actions selected

Conditions ⓘ >

Control user access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps User actions

Include Exclude

☐ None

☐ All cloud apps

☒ Select apps

Select

Cloud apps

Search

☒ Office 365 (preview) ⓘ

☐ Azure Analysis Services
4ac7d521-0382-4770-8098-7e1d9585ca2

☐ AM Azure Media Service
803ee1ca-3f71-4824-bd6e-0b99d720c35c

☐ azure-tenant-validation-app
764eb756-c256-450c-967d-9a29b9b3f047

☐ Common Data Service

Selected items

☒ Office 365 (preview) ⓘ Remove

7. In the New conditional access policy page, click on Conditions and then click on **Device Platform**. Select the appropriate device platforms.

Home > Endpoint security > Conditional Access >

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

No cloud apps or actions selected

Conditions ⓘ

0 conditions selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk (Preview) ⓘ

Not configured

Sign-in risk ⓘ

Not configured

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure ⓘ

Yes **No**

Include **Exclude**

☐ Any device

☒ Select device platforms

☐ Android

☐ iOS

☐ Windows Phone

☐ Windows

☐ macOS

8. In the **New conditional access policy page > Access controls**, click on **Grant** and make the access and block selections.

Grant ×

Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multi-factor authentication ⓘ

☒ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
[See list of approved client apps](#)

☐ Require app protection policy (Preview) ⓘ
[See list of policy protected client apps](#)

☐ Require password change (Preview) ⓘ

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

9. To enable the new policy, click **On**.

Enable policy

Report-only On Off

Create

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 97 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**.

Permissions requested Review for your organization

Mobileiron Device Compliance On-prem
www.mobileiron.com

This application is not published by Microsoft or your organization.

This app would like to:

- ✓ Read all applications
- ✓ Sign in and read user profile
- ✓ Read all applications
- ✓ Manage partner compliance policies with Microsoft Intune.
- ✓ Send device attributes to Microsoft Intune

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>.

Important: Only accept if you trust the publisher and if you downloaded this app from a store or website you trust. Microsoft is not involved in licensing this app to you.

Does this app look suspicious? [Report it here](#)

Cancel

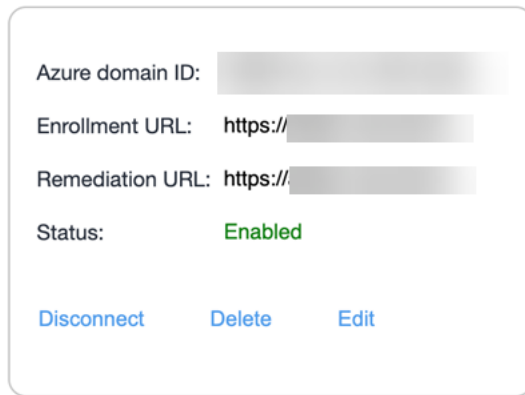
Accept



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.



Azure domain ID: [Redacted]

Enrollment URL: [https://\[Redacted\]](https://[Redacted])

Remediation URL: [https://\[Redacted\]](https://[Redacted])

Status: **Enabled**

[Disconnect](#) [Delete](#) [Edit](#)

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 580](#).

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 575](#).



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 582](#).

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 ["Connecting the account" on page 575](#).

Deleting an account

The delete option removes the saved tenant details from Ivanti EPMM.



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.

► App (12)		Preference Config Changes	Success	msystem	2020-10-13 ...	2020-10-13 ...	System	Modify Preference azure intune tenant provisioning status from TENANT_DEPROVISIONING_SUCCESS to TENANT_PROVISIONING_SU...
► Policy (10)		Preference Config Changes	Success	msystem	2020-10-13 ...	2020-10-13 ...	System	Modify Preference azure intune tenant provisioning status from TENANT_PROVISIONING_SUCCESS to TENANT_DEPROVISIONING_SU...
►		Admin Portal Sign In	Success	miadmin	2020-10-13 ...	2020-10-13 ...	Admin Port...	Successfully Signed In
Compliance Action (0)		Wakeup	Success	miadmin	2020-10-13 ...	2020-10-13 ...	tu6 (iOS 13...	Request for Force Device Check-In

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 574](#).

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	<p>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 574.</p> <p>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:</p> <ul style="list-style-type: none"> • 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 103. 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 219](#).

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.



Disconnecting requires an active connection to Azure using valid credentials.

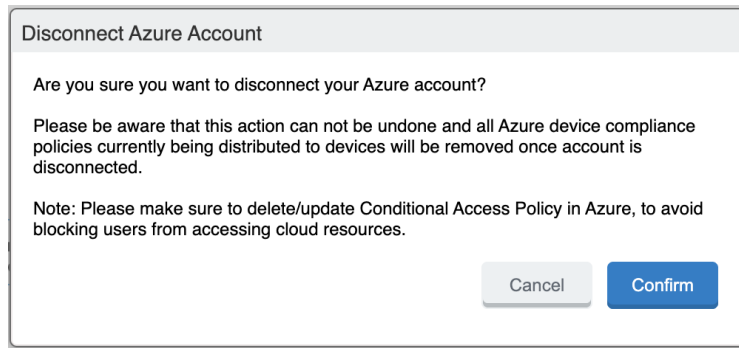
Procedure

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**.



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.



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
<ol style="list-style-type: none">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.	<ol style="list-style-type: none">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.

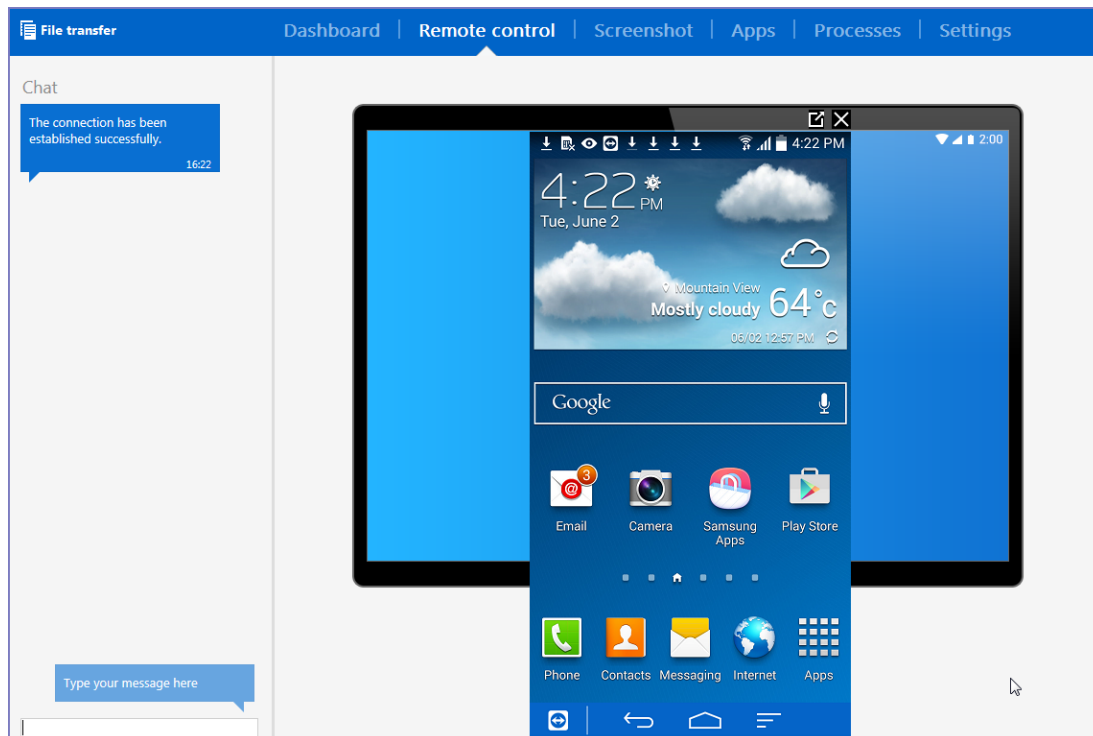
Help@Work for Android

This section addresses Help@Work for Android with TeamViewer.

- "About Help@Work for Android " below
- "How Help@Work for Android works" on page 588
- "Help@Work for Android setup overview" on page 589
- "Installing TeamViewer on your desktop" on page 589
- "Requesting a TeamViewer account" on page 590
- "Creating a TeamViewer app" on page 592
- "Enabling Help@Work in Ivanti EPMM" on page 594
- "Deploying the TeamViewer QuickSupport app" on page 595
- "Starting a remote control session " on page 596

About Help@Work for Android

Help@Work for Android with TeamViewer is an integration that enables administrators to get remote control access to supported Android devices managed by Ivanti EPMM. VPN is not required. After initiating a remote control session from the Admin Portal using FCM, administrators can configure Android 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.



Prerequisites

Help@Work for Android requires:

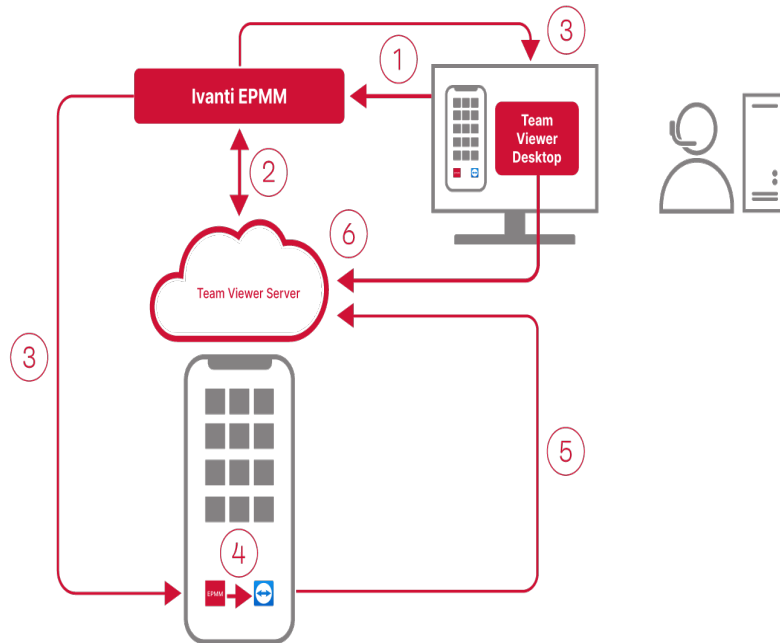
- access to the [Ivanti Support site](#) during initial setup for one-time license activation
- a company email address (belonging to an organization rather than an individual) that can be used for the TeamViewer account
- appropriate firewall rules to support FCM (see the *On-Premise Installation Guide for Ivanti EPMM and Enterprise Connector*)
- TeamViewer 10 Desktop edition

Supported devices

For information on supported Android devices, go to <https://www.teamviewer.com/En/help/341-How-can-I-control-my-Android-device-with-TeamViewer.aspx>.

How Help@Work for Android works

The following diagram illustrates how Help@Work for Android with TeamViewer establishes a remote control session.



1. Administrator selects a target device in the Admin Portal Devices > Devices.
2. Ivanti EPMM contacts the TeamViewer Server to create a remote session and retrieve a session ID.
3. Ivanti EPMM sends a command to Ivanti Mobile@Work on the device to start a remote session using the session ID. Ivanti EPMM also launches the TeamViewer software on your desktop with the session ID.
4. The Ivanti Mobile@Work app sends a message (intent message object) containing the session ID to the TeamViewer app to start a remote session.
5. TeamViewer app connects to the TeamViewer Server.
6. Administrator takes remote control of the device.

Help@Work for Android setup overview

The following diagram illustrates the setup process for Help@Work for Android:



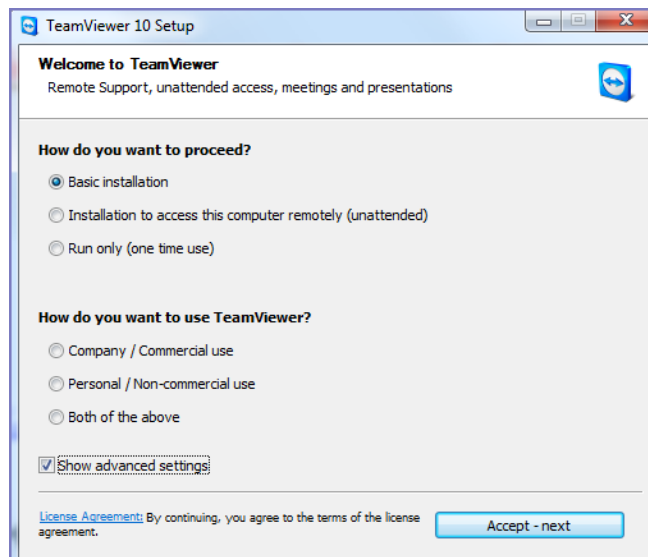
Installing TeamViewer on your desktop

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/>

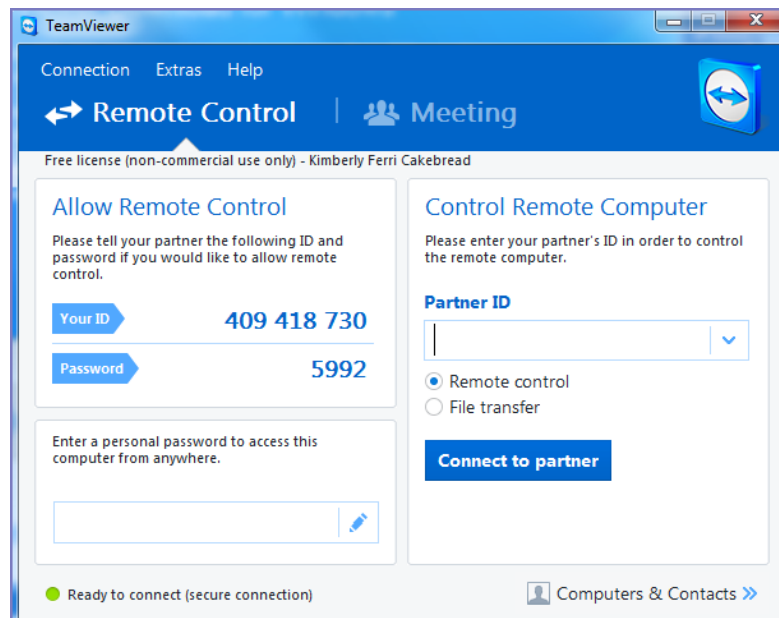
2. Launch the TeamViewer installation program.



3. Select **Basic Installation**.
4. Select **Company / Commercial use**.

5. Click **Accept - next**.

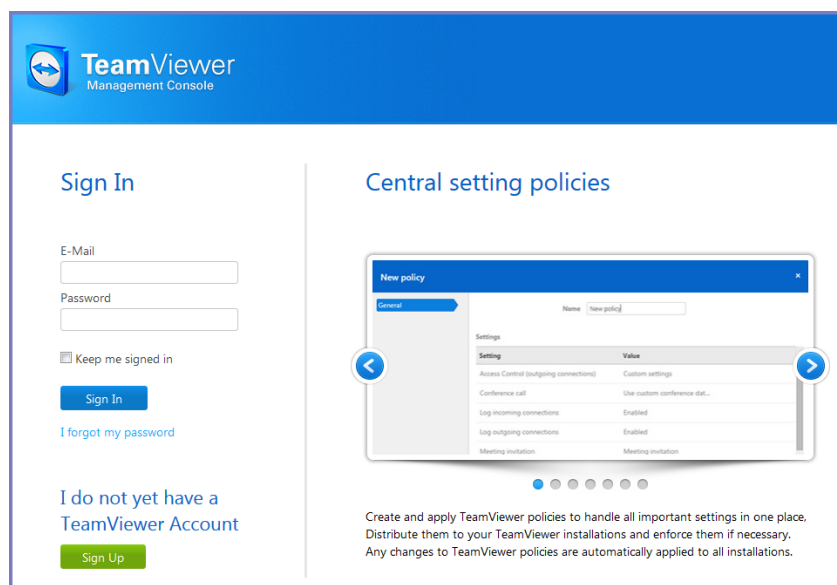
When the installation is complete, the following screen displays.



Requesting a TeamViewer account

This section explains how to get a TeamViewer account.

1. Go to <https://login.teamviewer.com/LogOn#register>.

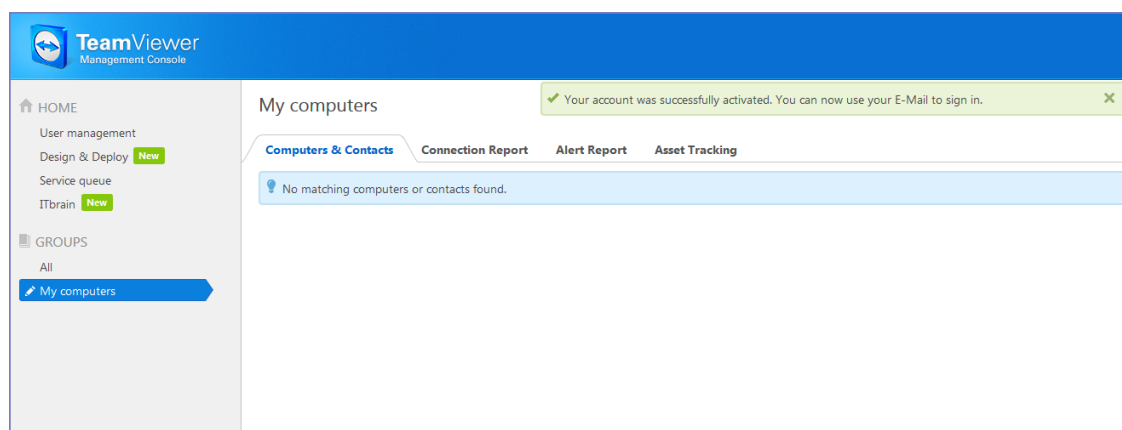


2. Click **Sign Up**.
3. Set a TeamViewer email address and password.
4. Check the email account for a TeamViewer activation email.

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:

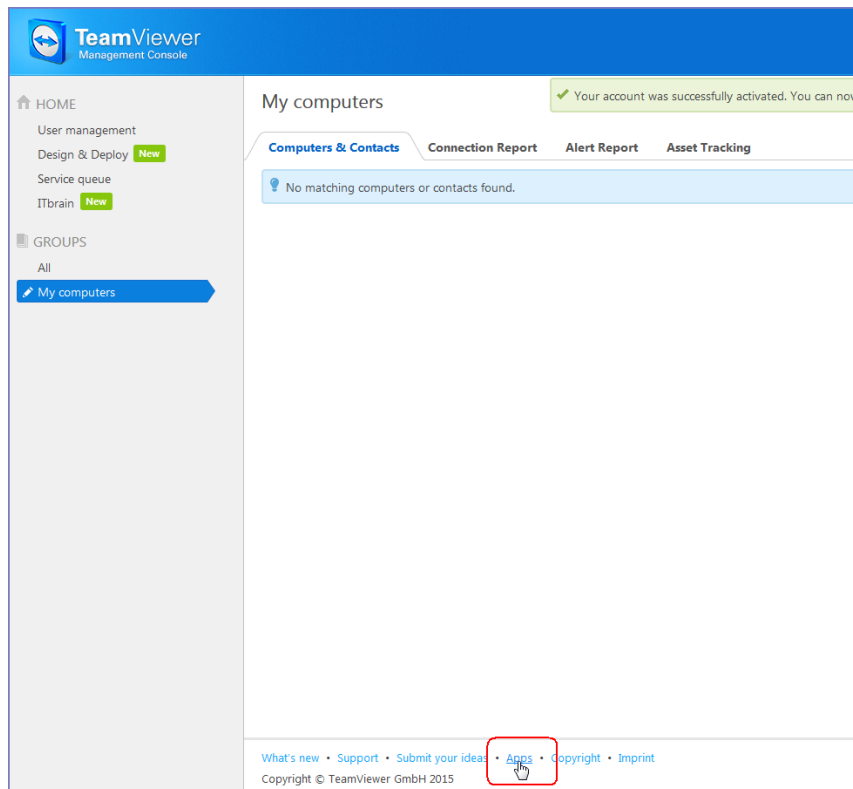


6. Bookmark this page for future reference.

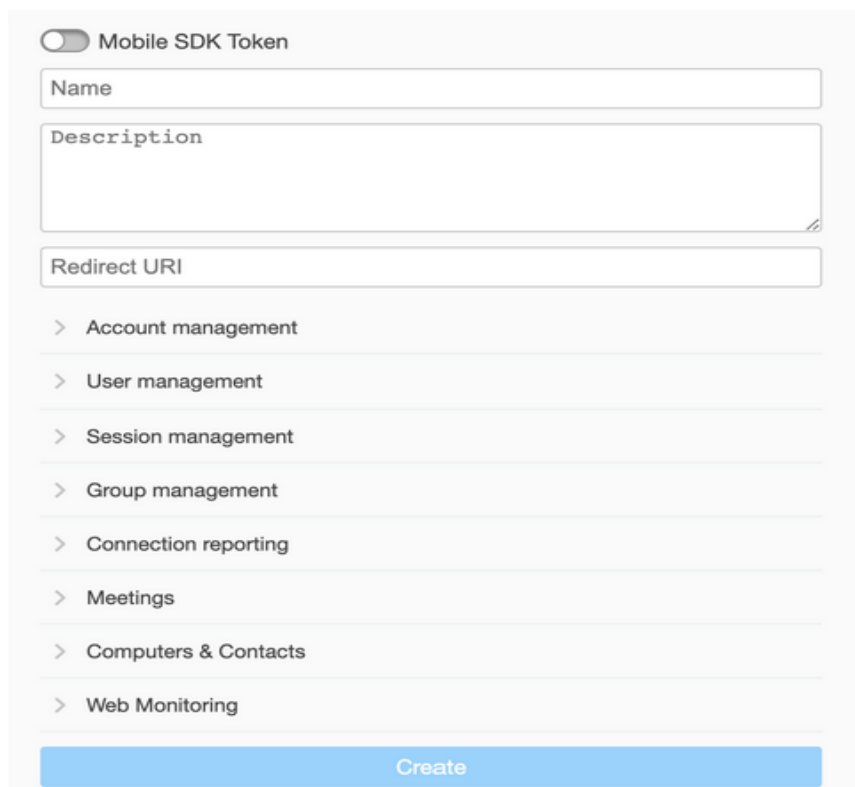
Creating a TeamViewer app

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 590](#).
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.



☒ Mobile SDK Token

Name

Description

Redirect URI

- > Account management
- > User management
- > Session management
- > Group management
- > Connection reporting
- > Meetings
- > Computers & Contacts
- > Web Monitoring

Create

- Name** - Enter at least five characters.
- Description** is optional
- Redirect URI** - Enter it in the form of `https://<ivantiepm>/mifs/teamViewerRedirect`, where `<ivantiepm>` is the URL of your Ivanti EPMM installation.



Using a redirect URI is required.

- 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 592](#).
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**.

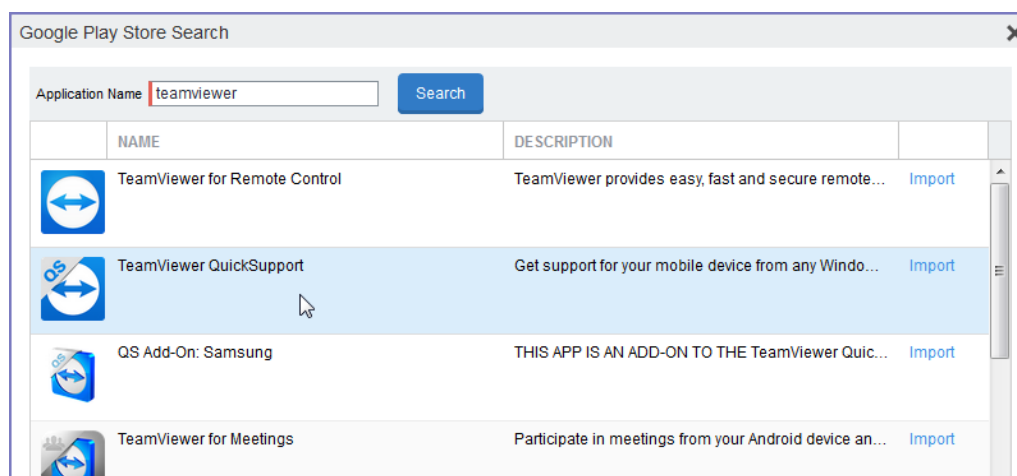


Though your license is now activated, your TeamViewer software will still display a notice about trial software. Your licensing applies to the session established using the integration, so the trial notice remains in the console.

Deploying the TeamViewer QuickSupport app

This section explains how to deploy the TeamViewer QuickSupport app to Android devices managed by Ivanti EPM.

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **Quick Import**.
3. Select **Google Play**.
4. In the **Application Name** field, enter teamviewer.
5. Select **Search**.



6. Find the app in the search results.
7. Select **Import**.
8. Dismiss the displayed message and the Google Play Store Search dialog box.
9. Under **Apps > App Catalog**, select the app you just imported.
10. Select **Actions > Apply To Labels**.

11. Select labels that represent the devices that should have the app added to the app catalog.
12. Select **Apply**.
13. Instruct Android device users to install the app.
14. Instruct Android device users to launch the app.

If an add-on is available for the device, the device user will be prompted to install it.

15. Instruct device users to install the add-on if prompted to do so.

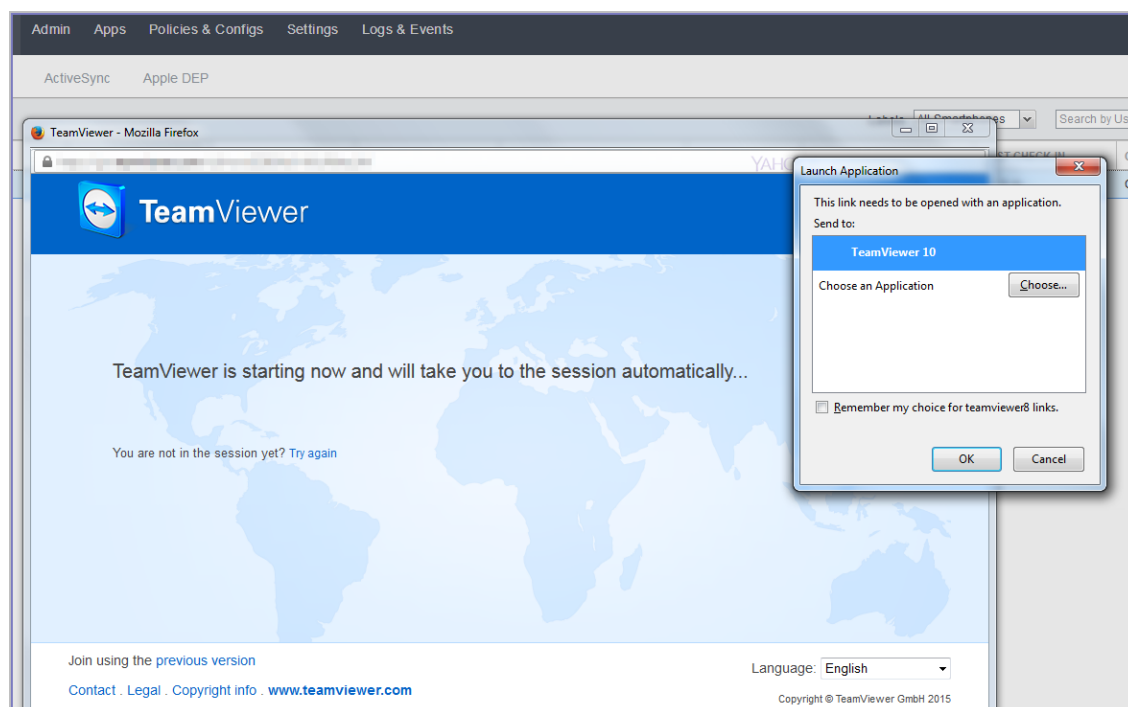
Starting a remote control session

This section explains how to start a Help@Work for Android remote control session.

1. Ask the device user to install the TeamViewer QuickSupport app.

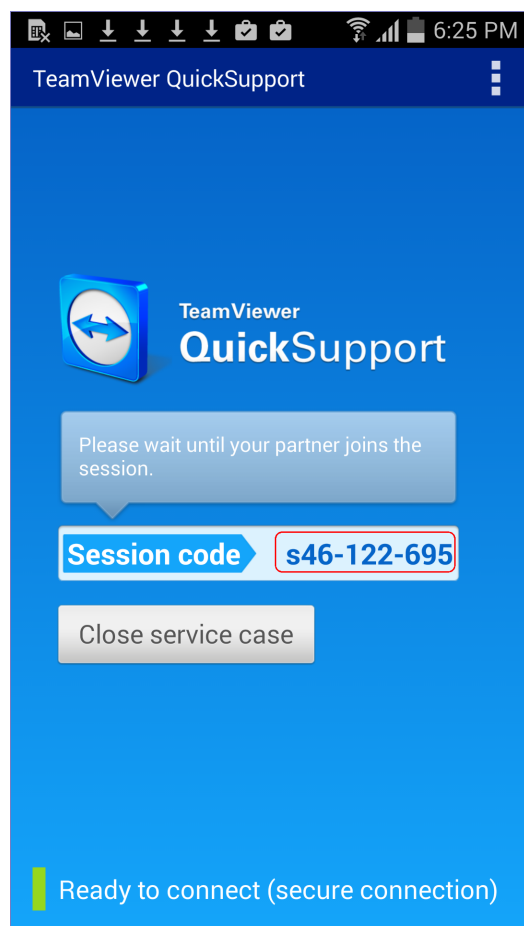
It should be displayed in the Ivanti EPMU app catalog on the device.

2. In the Admin Portal, go to **Devices & Users > Devices**.
3. In the Devices page, select the entry for the device.
4. Confirm that the device is supported by Help@Work for Android. See "[Help@Work for Android](#)" on [page 586](#)
5. Select **Actions > Android Only > Remote Control**.
6. If a page requesting a session ID displays, ignore it.

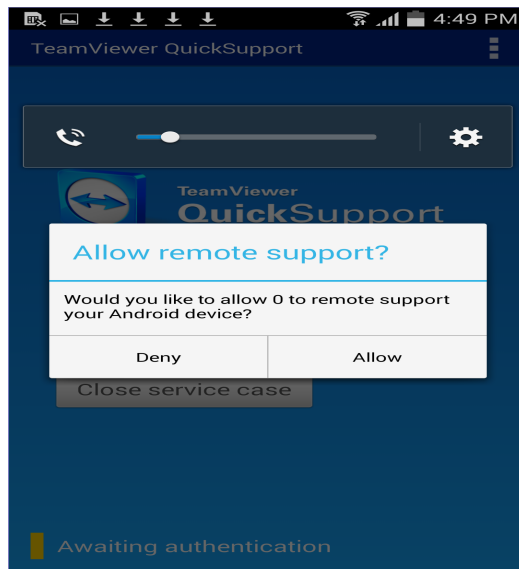


7. Launch the TeamViewer 10 application when prompted.
8. If your browser has pop-up blocking enabled, then allow pop-ups for your Ivanti EPMM URL.
9. If the TeamViewer QuickSupport app does not launch on the device, ask the device user to tap the Ivanti Mobile@Work icon.

The required session ID is automatically displayed on the device.

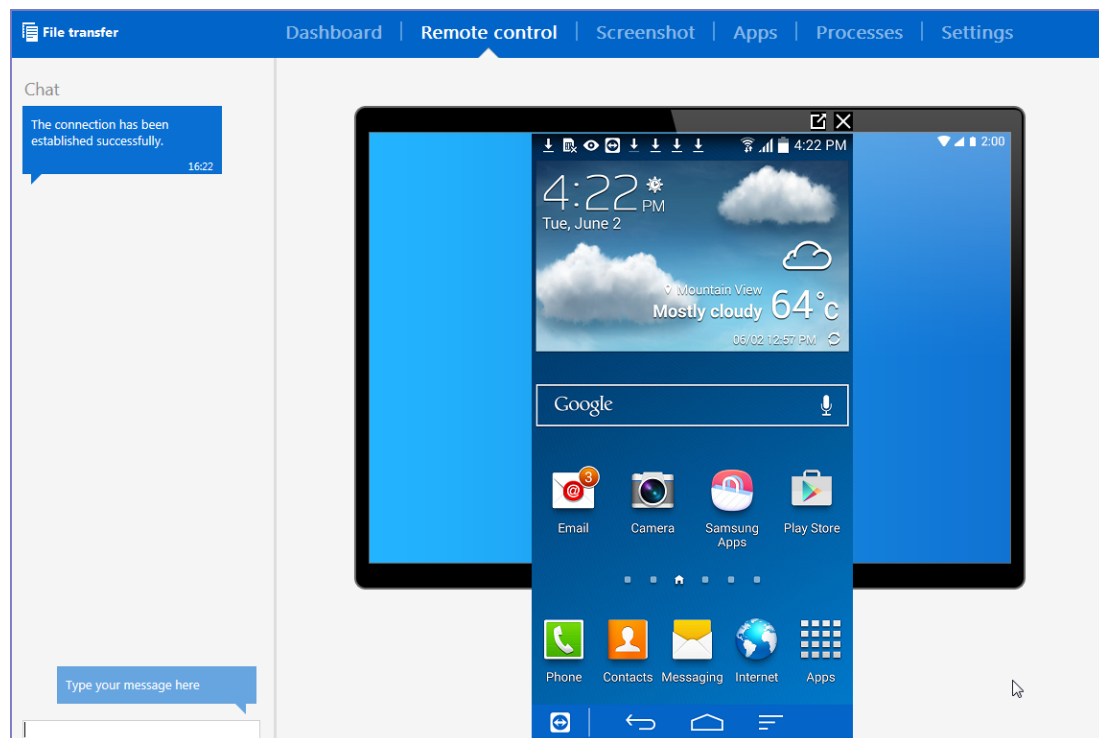


The device user should then see a prompt similar to the one below.



10. Ask the device user to tap **Allow**.

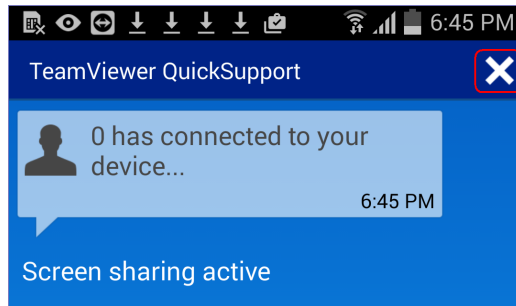
You should now see the remote control session displayed on your screen.



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.

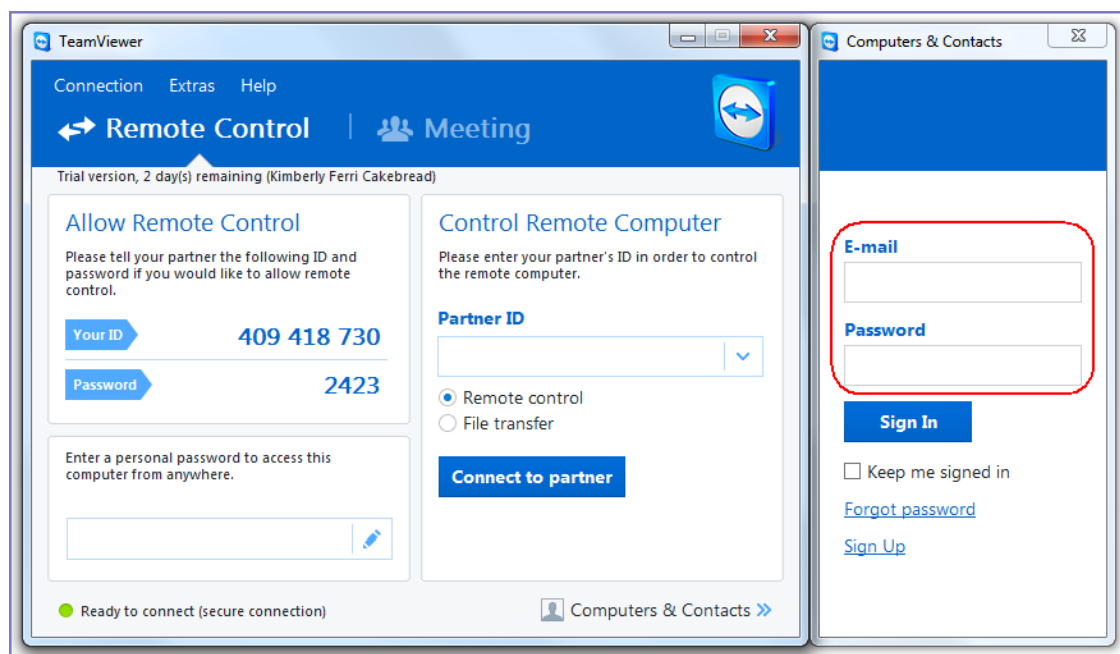


2. Tap the X in the upper right corner of the TeamViewer QuickSupport app.

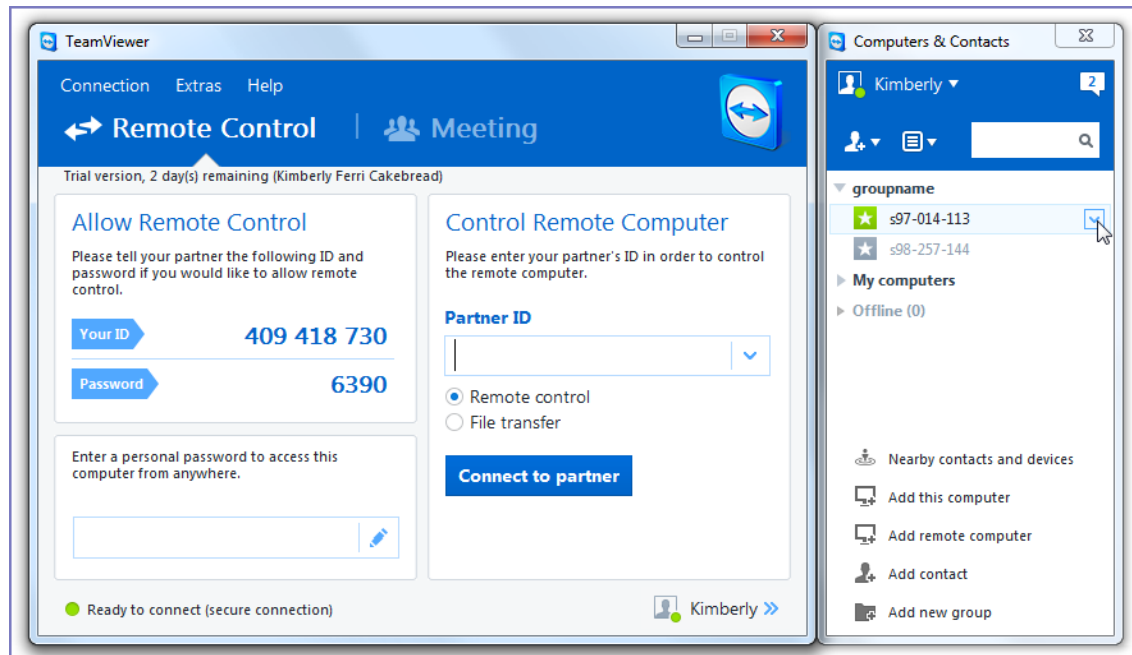
To close a remote control session from the desktop

To close a remote control session from the desktop:

1. Launch the TeamViewer desktop.



2. Sign in using your TeamViewer credentials.



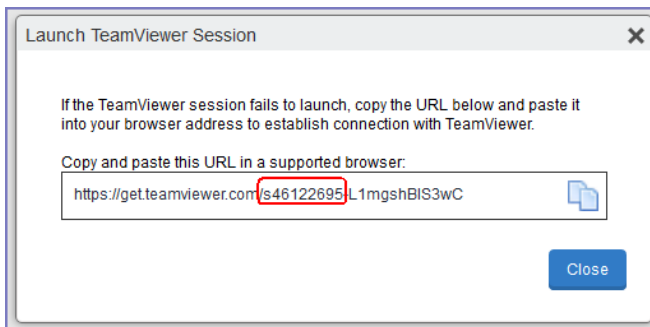
3. Select the session.
4. Select **Close**.

For more information on using remote control

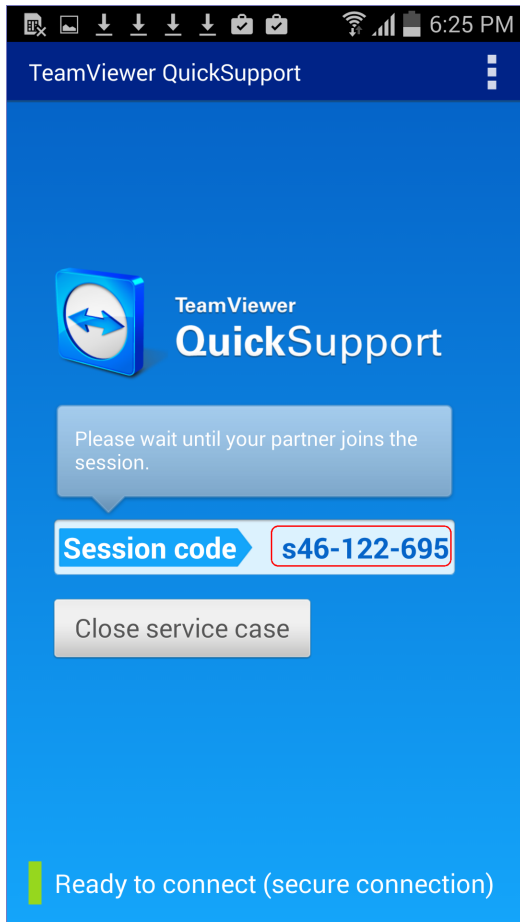
For information on how to use TeamViewer remote control, see <http://downloadus1.teamviewer.com/docs/en/v10/TeamViewer10-Manual-Remote-Control-en.pdf>

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" on the next page](#)
- ["Selecting languages for Ivanti EPMM messages" on the next page](#)
- ["Setting the system default language " on page 606](#)
- ["Changing language selection from the Admin Portal" on page 606](#)

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**.

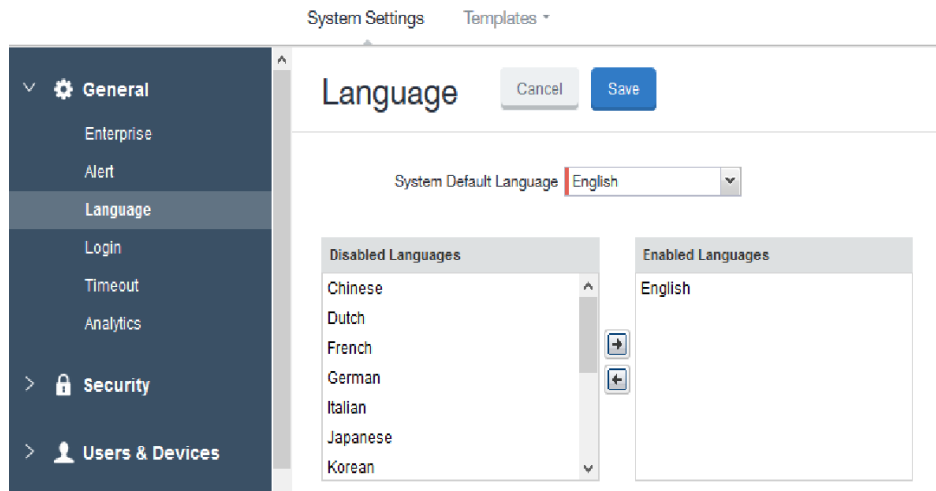
Please refer to the *Ivanti EPMM Release Notes and Upgrade Guide* for each release to see which languages and locales are supported.

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**.

Samsung Android Kiosk Support

- ["About Samsung Android kiosk" below](#)
- ["Setting up Samsung Android kiosk mode" on the next page](#)
- ["Samsung Android kiosk policy" on page 610](#)
- ["Creating a Samsung Android kiosk configuration for multiple-app mode" on page 615](#)
- ["Enabling and Disabling Samsung Android kiosk mode" on page 617](#)
- ["An example of Samsung Android kiosk mode" on page 618](#)
- ["Information about Samsung Android kiosk mode in device details" on page 619](#)
- ["Samsung Android kiosk mode deployment notes" on page 619](#)
- ["Setting the kiosk policy for Android managed devices" on page 620](#)

About Samsung Android kiosk

The Samsung Android kiosk feature enables you to configure supported Samsung Android devices to use only specified apps. Samsung Android kiosk mode is intended for devices that serve very specific functions for an organization.

Examples include:

- A retail store might want to use tablets to provide one or two custom apps for customers to use while shopping.
- A school might want to distribute tablets that present only appropriate apps for the user who signs in.



Though the Samsung Android kiosk feature allows multiple users to log in on a given device, it does not represent full multi-user support. It is intended as a view filter for apps. The profiles on the device do not change when different users log in. Instead, a custom list of apps displays based on the current user.

The kiosk feature has two modes of operation:

- single-app mode, where only one app is allowed to run on the device
- multiple-app mode, where multiple designated apps are allowed to run on the device



AppConnect apps are supported only in multiple-app mode. They are not supported in single-app mode. Multiple-app mode support with AppConnect apps is not available prior to Ivanti Mobile@Work 9.1 for Android.

Requirements

- Samsung Android kiosk mode is available on Samsung Knox devices.

Setting up Samsung Android kiosk mode

To set up a Samsung Android kiosk device for single-app mode:

- Create an Android kiosk policy.

To set up a Samsung Android kiosk device in multiple-app mode:

1. Create an Android kiosk policy.
2. Create one Android kiosk configuration for each combination of LDAP group and accessible apps.

Device users must belong to the designated LDAP groups.

The *policy* specifies the kiosk type. The *configuration* specifies which apps to display to which users in multiple-app mode.

The following instructions assume that the apps are already installed on the devices. If an app specified in the kiosk setup is not installed on the device, that app is represented by a blank icon.

Finding the package name for an Android app

For public apps available on the Google Play store:

1. Use a web browser to locate the app in Google Play.
2. Select the app.
3. Examine the URL displayed in the browser.

FIGURE 1. FINDING THE PACKAGE NAME FOR AN ANDROID APP

https://play.google.com/store/apps/details?id=com.mobileiron&feature=search_result#?t=W251bGwsMSwyLDEsImNvbS5tb2JpbGVpcml0

The package name is included in the URL, as shown in ["Finding the package name for an Android app" on the previous page](#).

For in-house apps:

1. Open the .apk as a zip file.
2. Use a text editor to open AndroidManifest.xml.
3. Locate the "package manifest" entry.

This entry is set to the package name.

Samsung Android kiosk policy

The Samsung Android kiosk policy defines the behavior of a kiosk device, determining if the kiosk mode is for a single app or for multiple apps.



Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See ["Setting the kiosk policy for Android managed devices" on page 620](#).

Setting up a single-app kiosk policy

A single-app kiosk policy specifies one app for use on the designated devices. For example, if the device is intended to run an in-house app for staff in a hospital recovery room, you can define a single-app kiosk policy to prevent users from accessing other apps and device resources on that device.

Procedure

1. Go to **Policies & Configs > Policies**
2. Click **Add New > Android > Samsung Kiosk**. The New Android Kiosk Policy dialog box opens.

Single App is selected by default.

3. Use ["Samsung Android kiosk policy" above](#) to complete remaining options.
4. Click **Save**.
5. Assign the policy to the appropriate label to push it to the target devices.

Single-app kiosk policy

See the following table for a description of the fields in a single-app kiosk policy.

TABLE 104. SAMSUNG KIOSK SINGLE APP POLICY

Item	Description
Single App package name	<p>Enter the package name for the app. The typical package name has the following format:</p> <p>com.company.app</p> <p>Important: Do not add the Ivanti Mobile@Work package name here. The device must already have Ivanti Mobile@Work installed and be registered with Ivanti EPMM when it receives the kiosk policy.</p>
<i>Enable Android functions</i>	
System bar	System bars are screen areas dedicated to navigation and the display of notifications and status. Clear this option if you want to hide the system bar when the device is acting as a single-app kiosk.
Task manager	The task manager enables device users to open an app that is currently running on the device. Select this option if you want device users to be able to access the built-in task manager on the device.
Notification bar expansion	The notification bar typically displays at the top of the device. Swiping down expands the bar to the full size of the screen so that the device user can see notification details. Select this option if you want device users to be able to expand the notification bar.
Navigation bar	<p>For Android 4.0, the navigation bar is present only on devices that don't have the traditional hardware keys. It contains the Back, Home, and Recents controls. Select this option to allow device users to access the navigation bar.</p> <p>Note: For tablets, the status and navigation bars are combined into a single bar at the bottom of the screen.</p>
Status bar	<p>The status bar displays pending notifications, and status such as time, battery level, or signal strength.</p> <p>Note: For tablets, the status and navigation bars are combined into a single bar at the bottom of the screen.</p>
Share via	When "Share via" is enabled, the user can share data from apps that offer data sharing. Select this option to allow data sharing.

Setting up a multiple-apps kiosk policy

A multiple-app kiosk policy specifies behavior for a device that will run multiple apps. You must also define at least one Android kiosk configuration to specify the permitted apps.

The multiple-app Kiosk Policy provides these additional options:

- Multiple user login support
- Inactivity logout interval
- Administrative access to exit kiosk mode
- Branding options for the kiosk launcher/desktop

To specify a multiple-app kiosk policy:

1. Go to **Policies & Configs > Policies**
2. Click **Add New > Android > Samsung Kiosk**. The New Android Kiosk Policy dialog box opens.
3. In the Android (Samsung Safe) section select the **Multiple Apps** radio button.
4. Use ["Samsung Android kiosk policy" on page 610](#) to complete the remaining options.
5. Click **Save**.
6. Assign the policy to the appropriate label to push it to the target devices.
7. Create an Android kiosk configuration to specify the apps to be used.

Multiple-apps kiosk policy

See the following table for a description of the fields in a multi-app kiosk policy.

TABLE 105. MULTIPLE-APPS KIOSK POLICY

Item	Description
Kiosk multi-user login	<p>Enable this option to allow different users to log in. Device users enter their Ivanti EPMM credentials to access the kiosk. The credentials entered determine who is recorded as the current user, the apps to display, and whether that user has permission to exit kiosk mode from the device.</p> <p>Note: The credentials entered do not affect the profiles installed on the device.</p>
Inactivity logout	Select the duration of inactivity after which the user will be signed out. This option applies to multiple-user kiosks only.
Administrative access to exit Kiosk mode	<p>If you want to specify users who have permission to disable kiosk mode from the device, specify the corresponding LDAP groups for those users.</p> <p>You can choose from the LDAP groups that you specified in Services > LDAP for each LDAP server.</p>
<i>Branding</i>	
Background Color	Enter the hexadecimal triplet for the color you want to apply to the kiosk display background.
Banner Color	Enter the hexadecimal triplet for the color you want to apply to the banner at the top of the kiosk display.
Banner Text Color	Enter the hexadecimal triplet for the color you want to apply to the text in the banner at the top of the kiosk display.
Banner Text	Enter the text you want to display in the banner at the top of the kiosk display.
Banner Logo	<p>Click Browse to select a logo. The logo must be a JPEG or PNG graphic.</p> <p>Image pixel size: Image sizes vary for different devices. For most smaller screened devices, 120x120 pixels is appropriate. For most tablets or larger screens, 180x180 pixels is appropriate .</p> <p>Image file size: must be smaller than 100 KB.</p>
<i>Enable Android functions</i>	
System bar	System bars are screen areas dedicated to navigation and the display of notifications and status. Clear this option to hide the system bar.

TABLE 105. MULTIPLE-APPS KIOSK POLICY (CONT.)

Item	Description
Task manager	The task manager enables device users to open an app that is currently running on the device. Select this option if you want device users to be able to access the built-in task manager on the device.
Notification bar expansion	The notification bar typically displays at the top of the device. Swiping down expands the bar to the full size of the screen so that the device user can see notification details. Select this option if you want device users to be able to expand the notification bar.
Multi Window	Multi window is a Samsung feature that enables users to multitask by viewing two apps at the same time. Select this option to allow the multi window feature.
Navigation bar	For Android 4.0, the navigation bar is present only on devices that don't have the traditional hardware keys. It contains the Back, Home, and Recents controls. Select this option to allow device users to access the navigation bar. Note: For tablets, the status and navigation bars are combined into a single bar at the bottom of the screen.
Status bar	The status bar displays pending notifications, and status such as time, battery level, or signal strength. Note: For tablets, the status and navigation bars are combined into a single bar at the bottom of the screen.
Share via	When "Share via" is enabled, the user can share data from apps that offer data sharing. Select this option to allow data sharing.

Creating a Samsung Android kiosk configuration for multiple-app mode

The Samsung Android kiosk configuration has the following functions:

- Specifies the apps to be displayed for multiple-app devices
- Specifies which LDAP groups, (and, therefore, which users) have access to those apps

You can apply more than one kiosk configuration to a single device. The union of the configurations determines which apps to display.



The LDAP group access specified in the configuration would effectively disable the specified apps on a single-app mode device.

Do not add the Ivanti Mobile@Work app to an Android Kiosk Configuration. This usage is not supported and can cause errors.

Procedure

1. Go to **Policies & Configs > Configurations**.
2. Select **Add New > Android > Android Kiosk Mode**.

The **New Android Kiosk App Setting** dialog box opens.

3. If you intend to use LDAP groups to restrict access to apps on kiosk devices, then select the LDAP groups you want to allow. You can choose from the LDAP groups that you specified in **Services > LDAP** for each LDAP server.

These users will have access to the specified apps on kiosk devices, that is, those devices that have a kiosk policy applied.

To enable all kiosk users to have access to all specified apps, do not select any LDAP groups.

The available LDAP groups are based on the last sync between Ivanti EPMM and the LDAP server. If you made a recent change to LDAP data, it will not be reflected until the next sync (scheduled or manual).

4. Select the apps you want to make accessible for kiosk devices that receive this configuration. See ["Setting the kiosk policy for Android managed devices" on page 620](#) for how to do this.

Note that the name displayed is the common name for the app. The package name is the unique identifier determined by the app developer.

Do not add the Ivanti Mobile@Work app to an Android Kiosk Configuration. This usage is not supported and can cause errors.

5. Select **Save**.
6. Assign the configuration to the appropriate label to push it to the target devices. One or more kiosk configurations may be applied to a single device.

Enabling and Disabling Samsung Android kiosk mode

The first time the necessary policy and configuration are pushed to the device, a kiosk item displays in the Apps@Work screen on the device. Tap **Kiosk Mode** to initiate kiosk mode.

Afterwards, you can enable and disable Android kiosk mode from the Admin Portal. Users with assigned privileges can also disable kiosk mode on a kiosk device.

- ["Enabling Samsung Android kiosk mode from the Admin Portal " below](#)
- ["Disabling Samsung Android kiosk mode from the Admin Portal" below](#)
- ["Enabling Samsung Android kiosk mode from the device" below](#)
- ["Disabling Samsung Android kiosk mode from the device" on the next page](#)

Enabling Samsung Android kiosk mode from the Admin Portal



Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See ["Setting the kiosk policy for Android managed devices" on page 620](#).

To enable:

1. Select the device in the **Device & Users > Devices** page.
2. Click **Actions > Android Only > Enable Kiosk**.

Disabling Samsung Android kiosk mode from the Admin Portal

To disable:

1. Select the device in the **Device & Users > Devices** page.
2. Click **Actions > Android Only > Disable Kiosk**.

Enabling Samsung Android kiosk mode from the device

To enable:

1. Start the Ivanti Mobile@Work app.
2. Tap **Kiosk Mode**.

 Kiosk Mode displays only if the kiosk policy has been configured and sent to the device.

Disabling Samsung Android kiosk mode from the device

Only users configured for administrative access in the kiosk policy can disable kiosk mode from the device. The kiosk must be configured to support multiple apps and multiple users.

To disable:

1. Log in as a kiosk administrator.
2. Tap the **Exit Kiosk** icon at the top of the screen.

An example of Samsung Android kiosk mode

 Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See ["Setting the kiosk policy for Android managed devices" on page 620](#).

Consider a school that wants to install the followings apps on several tablets. Although all the apps are installed on each tablet, the apps that are displayed depend on which user has logged in.

This section covers the apps and the LDAP groups that should have access to them.

TABLE 106. ANDROID KIOSK MODE EXAMPLE: LDAP GROUPS AND APPS

LDAP Groups	Apps			
	View	Update	Send 2 Parents	Send 2 Teachers
Teachers	yes	yes	yes	yes
Tutors	yes	yes		yes
Students	yes			

The following table shows one way to implement this scenario.

TABLE 107. ANDROID KIOSK MODE EXAMPLE: ANDROID CONFIGURATIONS WITH LDAP GROUPS AND APPS

Android Kiosk configurations	LDAP Groups	Apps			
		View	Update	Send 2 Parents	Send 2 Teachers
KioskTeachers	Teachers	yes	yes	yes	yes
KioskTutors	Tutors	yes	yes		yes
KioskStudents	Students	yes			

Information about Samsung Android kiosk mode in device details

The **Device Details** pane in the Admin Portal displays the following information about kiosk mode:

- whether kiosk mode has been enabled
- the device user currently logged in on the device.

To view device details:

1. Go to **Device & Users > Devices**
2. Expand device details by clicking the caret next to the check box for the device of interest.
3. Look for the kiosk attributes in the Device Details tab.

Samsung Android kiosk mode deployment notes

Following are general notes for the Samsung kiosk:

- Samsung kiosk mode is deprecated in Android 8.1 and above. You must implement Android kiosk mode instead. See ["Setting the kiosk policy for Android managed devices" on the next page](#).
- Samsung Android kiosk mode is a viewing filter only
 - Kiosk mode is not an app blocking feature. It only restricts the viewing of apps which can be launched.
 - Apps must be installed on the device for them to launch from the kiosk.

- Distribute apps with the silent install option enabled to ease the deployment process.
- Configuring which apps to run
 - Single app mode uses the **Android Samsung Kiosk policy** on the **Policies** page.
 - Multiple app mode uses the **Android Samsung Kiosk policy** on the **Policies** page, and one or more **Android Samsung Kiosk configurations** on the **Configurations** page.
 - Apps defined in kiosk configurations with no LDAP groups selected apply to ALL kiosk users.
 - For multiple app mode, the union of all kiosk configurations applicable for a kiosk user (based on their LDAP group membership) determines the list of apps to display, and whether or not they are allowed to bypass kiosk mode.
- If the device loses its connection to Ivanti EPMM, then kiosk mode cannot be disabled. You must do a factory reset.
- After a Samsung kiosk policy and Samsung kiosk configuration (for multi-app kiosk mode) have been pushed to a device, press the Home button on the device or restart the device. These actions avoid Android OS issues which leave the Android home screen available. Similarly, press the Home button or restart the device when kiosk mode is re-entered after having been exited due to administrator action or device maintenance.

Setting the kiosk policy for Android managed devices

As a Space or Global administrator, you can set up a policy to customize the look of the Android Kiosk as well as the apps which it contains. In addition, you can select to switch to the Kiosk mode automatically. This feature is supported on devices in Device Owner mode with Android Enterprise.

For Android shared-kiosk mode, see ["Configuring the Android shared-kiosk mode" on page 435](#).


1. Go to **Policies & Configs > Policies**
2. Select **Add New > Android > Android Kiosk Mode** to display the New Android Kiosk App Setting Policy dialog box.
If a Kiosk App policy exists, the Edit Android Kiosk App Setting Policy page opens.
3. Enter a **Name** for the new policy.
4. Ensure the Status field is set to **Active**.
5. (Optional) Customize the kiosk with a banner, background color or background image. See

"Branding the Android kiosk screen" on page 437.

6. In the Kiosk Settings section, select the appropriate check boxes for your implementation:

Field	Definition	Enabled by default?
Enable Lock Task Mode	Enables the Lock Task Mode on the Android Enterprise devices connected to Android Kiosk to increase the level of security on the user devices in kiosk mode by limiting access to white listed kiosk and system apps. When a device user swipes away from an app, they will only have access to the white listed and system apps. This feature is only applicable to Android 9 devices in Device Owner (DO) mode.	Yes
System Info (Android 9+ only)	When selected, displays the date / time, connectivity, battery, and vibration mode in the status bar.	No
Keyguard (Android 9+ only)	Enables the keyguard in lock task mode.	Yes
Global Actions (Android 9+ only)	Enables the menu that is displayed when the user long-presses the power button. If this option is disabled, the user may not be able to power off the device.	Yes
Home button (Android 9+ only)	When enabled, displays the following sub-options: <ul style="list-style-type: none"> Overview button - Enables the Overview button and the Overview screen during lock task mode. When using the Enable Single App Kiosk mode, Ivanti recommends the Overview button to be de-selected. Notifications - Enables notifications during lock task mode. This includes notification icons on the status bar, heads-up. notifications, and the expandable notification shade. Note: These options are only applicable for Android 9 devices. 	No

Field	Definition	Enabled by default?
Disable Quick Settings	Select so that the device will not display the system notification drop-down menu at the top of the screen. If the following settings are enabled, the settings will be display as kiosk Settings menu items. The user can customize each of the settings for use in the kiosk.	No
Allow User to Access Wi-Fi Settings	Select to permit the device user to access Wi-Fi settings.	No
Allow User to Access Bluetooth Settings	Select to permit the device user to access Bluetooth settings.	No
Allow User to Access Location Settings	Select to permit the device user to access Location settings.	No
Enter Kiosk Mode Immediately on Registration	The device will enter Kiosk mode automatically on registration.	No
Kiosk Exit Pin	Enter a 4 - 6 digit PIN into the field. If the Kiosk Exit PIN field is left blank, it disables the ability to exit Kiosk mode. The user will not be able to exit Kiosk mode without a Kiosk exit PIN.	No
Enable Shared Device	This option is used for shared-kiosk mode. See "Configuring the Android shared-kiosk mode" on page 435 .	No
Enable Single App Kiosk	<p>Starting with Ivanti EPMM 11.8.0.0, administrators can select the Enable Single App Kiosk check box and then select the (single) app to pin to the device screen.</p> <p>This setting allows one app to be pinned to the device screen in most conditions. The dedicated single app mode will allow other apps to be available on the device, but they will not be available for the device user to directly launch. These other apps will only be launched through the pinned app. For example, Email is the pinned single app, and the device user receives an email with a link to the Gmail Maps app. When the device user taps on that link, it opens the Gmail Maps app.</p>	No

Field	Definition	Enabled by default?
	<p>The pinned single app will be launched only when it is part of the Allowed App list, the Kiosk Mode Allowed Apps list, <i>and</i> installed on the device. The Allowed Apps listed are from the App Catalog Apps section.</p> <p>Ivanti recommends this be used with Lock Task mode and to have the Overview button de-selected.</p> <p>Applicable to Work Managed Device mode (DO) and Work Managed Device - non GMS mode (AOSP.)</p> <hr/> <p> Note the following:</p> <hr/> <ul style="list-style-type: none"> • Device users can exit Kiosk remotely. Ivanti Mobile@Work displays the toast message "Kiosk Exit" in the app but the dedicated single-app may still remain on pinned, as it can not be closed due to Android limitations. • The Lock Task mode can only be enabled when the screen is in the foreground. If the dedicated single-app is in the foreground, then it is not possible to enable Lock Task mode. Workaround: Device user needs to tap the back or home button; the Lock Task mode becomes enabled. • On devices Android 9 and below, when the single app Kiosk is disabled, then the device user may need to tap the back/home button to see the Kiosk grid screen again. The launched app may remain pinned to the foreground and the Kiosk grid screen may not display due to Android limitations. 	
Enable Driver Safety	Driver safety allows the admin to define apps that are enabled for the user when a specific velocity is detected.	No

7. In the **Choose Apps** section, optionally choose to:

- a. allow any third-party phone or camera app by manually adding the package name (ID).
- b. The **Built-in apps** must be enabled in Device Owner mode. This may not be the case with all manufacturers.
- c. Add apps from the **App Catalog Apps**.
- d. Set the apps allowed in **Kiosk Mode Allowed Apps**.
- e. Add apps manually by entering a Package ID in the **Manually Add Apps with Package ID** field and click **+Add**.



You can now group applications within a folder. Currently, a parent folder and sub-folder structure is supported. Apps can be reorganized in different folders to change availability of the app.

8. After an app has been installed and is listed in the **Kiosk Mode Allowed Apps** section of the **Edit Android Kiosk App Setting Policy** page, it can be dragged up or down to change the order of appearance in the kiosk.
9. All apps allowed in the **Kiosk Mode Allowed Apps** section have an additional "broom" icon/option. Based on the specific app's settings, the Ivanti Mobile@Work app will:
 - a. Broom with Check mark icon = clear app data when the user logs out of shared kiosk.
 - b. Broom with "Not allowed" icon = do not clear app data when the user logs out of shared kiosk.
10. All apps allowed in the **Kiosk Mode Allowed Apps** section have a "gear" icon. Based on the specific app's settings, the Ivanti Mobile@Work app will:
 - a. Gear with Check mark icon = allows device-wide settings for the selected app to be made available to the device user. Some apps may need this to get support from Android OS for activities such as completing bluetooth pairing. This is only available in Lock Task Mode. If Lock Task Mode is de-selected, the gear icon will not display.
 - b. Gear with "Not allowed" icon = disallows device-wide settings for the selected app to be made available to the device user.
11. Optionally, hide an app. Select an app in the **Kiosk Mode Allowed Apps** section and click the "eye" icon to hide the app.
 - a. When an app is hidden it can be used by other apps, but not available to launch in the kiosk. For example, a browser can be added to the kiosk but hidden so that it can be used to open URLs

from an email app.

- b. The Kiosk itself does not install any app. You need to install any app that you include in the kiosk using Apps@Work or other method.
12. For shared kiosk mode, you can ["Choose Apps" on page 440](#) and make settings for those apps.
13. Click **Save**.

The SMS Archive Feature

The SMS archive feature is available for Samsung Knox (Android) devices only.

- ["About the SMS & Call Log Archive feature" below](#)
- ["Supported devices" below](#)
- ["Setting Up the SMS & Call Log Archive feature" below](#)
- ["Setting up encrypted SMS and call log archive encryption" on page 628](#)
- ["Monitoring the SMS & Call Log archive" on page 629](#)

About the SMS & Call Log Archive feature

The optional SMS & Call Log Archive feature enables organizations to:

- Address regulatory requirements for archiving inbound and outbound SMS messages and calls.
- Encrypt SMS and call logs.

Supported devices

The **SMS archive feature** and the **call log archive feature** are only supported for Samsung Knox devices.

Setting Up the SMS & Call Log Archive feature

Complete the following steps to set up the SMS & Call Log Archive feature.

Procedure

1. In the Admin Portal, go to **Settings > System Settings**.
2. Go to **Android > SMS & Call Log Archive**.
3. Select the type of archive:
 - Email
 - Splunk

- Store and Forward to Internal Server
 - Do not archive to turn off the feature
4. If you select **Email**, use the following guidelines to complete the settings in **Email Configuration**:

Setting	Description
Default From Address	Enter the email address to include in the From field of the emails generated for archiving the SMS and call log messages.
Destination Email Addresses	Enter the email addresses for the archival systems to which the generated emails are being sent. Separate the email addresses with commas (,).
Host/IP Addresses	Enter the host name or IP address of each SMTP server to use for relaying the email to the SMS archival destinations. You may specify the same SMTP server that you specified when you configured Ivanti EPMM. If you specify multiple addresses, then Ivanti EPMM attempts to connect to each in the order specified until a successful connection is established.
TLS Enabled	Select Yes if you want to enable TLS for communication with the SMTP relay server.
STARTTLS Required	If you selected Yes for the TLS Enabled option, indicate whether the STARTTLS protocol is required for the specified SMTP servers.
Check SMTP Connection	Select this option to confirm SMTP access.

- Because most archival systems are designed for archiving email (and, therefore, parsing SMTP content), the Ivanti EPMM SMS & Call Log Archive feature can forward SMS content and other data via email. MMS data is not captured as part of this feature.
5. If you select **Splunk Forwarder**, make sure that Splunk Forwarder is configured in System Manager (see *Ivanti EPMM System Manager Guide* for details).
6. If you select **Store and Forward to Internal Server**, use the following guidelines to complete the settings in **Server Configuration**:

Setting	Description
Forward using	Select either SFTP or SCP as the protocol
Host/IP	Host name or IP address of the server (required)
Port Number	22 (default port number on the server)

Setting	Description
Username	Username of user associated with the server
Password	Password for user specified in Username
Confirm Password	Enter the password again to confirm
Server Path	Path to the server
Check Server Connection	Select to test the connection to the specified server

7. If you requested encryption of the logs, select **Upload Encryption Certificate** to upload the certificate.
8. In **Archive Settings**, enter the number of hours that Ivanti EPMM should wait before forwarding collected messages to their archival destinations. The default value is 4.
9. (Optional) Select **Send Now** to immediately archive all currently collected messages.
10. Select **Save**.

Setting up encrypted SMS and call log archive encryption

Ivanti EPMM privacy policies specify whether SMS and call log content is encrypted. These policies impact whether SMS and call log content is archived as well.

Procedure

1. Go to **Policies & Configs > Policies**.
2. Locate and select the privacy policy intended for supporting SMS and call log archive devices.
3. Select **Edit**. The Modify Privacy Policy dialog box opens.
4. Set the **SMS Log** option to:
 - **Sync Content- Clear Text** to specify the logs are not to be encrypted
 - **Sync Content - Encrypted** to specify the logs are to be encrypted
 - **None** to stop archiving SMS messages.
5. Set the **Call Log** option to:
 - **Sync Content - Clear Text** to specify the logs are not to be encrypted
 - **Sync Content - Encrypted** to specify the logs are to be encrypted
 - **None** to stop archiving SMS messages.
6. Select **Save**.

7. If the policy has not already been applied to the SMS or call log archive devices, apply the policy to the proper labels (select **Actions** > **Apply To Label**).

Monitoring the SMS & Call Log archive

You can monitor:

- the number of messages queued for delivery
- the health of the SMS & Call Log Archive feature using Events

Overriding the SMS and call log delivery interval

When you set up the SMS & Call Log Archive feature, you specify the **SMS Delivery Interval**, which determines how often Ivanti EPMM forwards the collected messages to the archival destinations.

Procedure

1. Go to **Settings** > **System Settings** > **Android** > **SMS & Call Log Archive**.
2. Select **Send Now**.



Note that **Send Now** is enabled only if there are queued SMS or call log messages.

Checking the number of delivered SMS and call log messages

Ivanti EPMM keeps a perpetual count of the SMS and call log messages delivered to archival destinations.

Procedure

1. Go to **Policies & Configs** > **Policies**.
2. Select and open the privacy policy that supports the SMS & Call Log Archive feature.

The details for the policy are displayed to the right of the policy list.

3. Note the number of messages listed in **Call Logs** and **SMS Logs** at the bottom of the section.

Event Center options

The following Event Center options are available to help manage the health of the SMS Archive feature:

- SMTP Relay server is unreachable
- SMTP Relay server error
- SMS Message archive queue is full

See "[System event settings](#)" on [page 461](#) for information on these events.

Self-service User Portal

This section addresses the settings an administrator needs to configure and maintain a self-service user portal for client devices.

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](#)
- [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](#)
- [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](#)
- [Retiring devices in the self-service user portal](#)

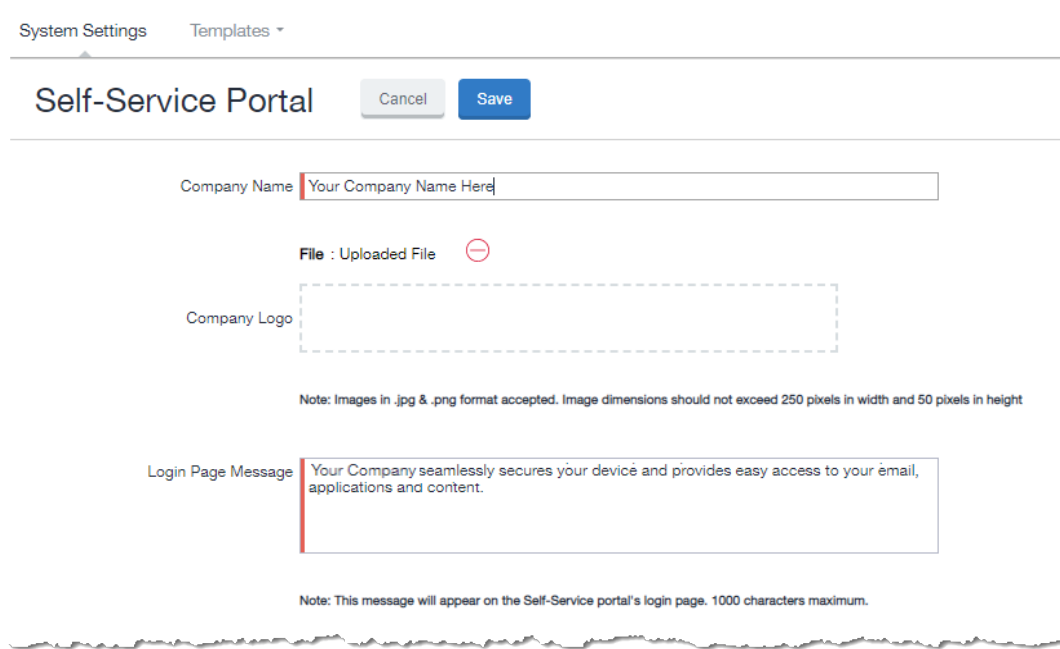
Customizing the self-service user portal

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.



The screenshot shows the 'Self-Service Portal' configuration page. At the top, there are tabs for 'System Settings' and 'Templates'. Below the tabs, the title 'Self-Service Portal' is displayed next to 'Cancel' and 'Save' buttons. The form contains three main sections: 'Company Name' with a text input field containing 'Your Company Name Here'; 'Company Logo' with a dashed box for the logo and a note: 'Note: Images in .jpg & .png format accepted. Image dimensions should not exceed 250 pixels in width and 50 pixels in height'; and 'Login Page Message' with a text area containing 'Your Company seamlessly secures your device and provides easy access to your email, applications and content.' and a note: 'Note: This message will appear on the Self-Service portal's login page. 1000 characters maximum.'

2. **Company Name:** Enter a customized company name.
3. **Company Logo:** Upload a customized company logo. Images can be JPG or PNG format, and must not exceed 250 by 50 pixels.
4. **Login Page Message:** Modify or replace the existing message that displays on the Self-Service Portal's log in page, up to 1,000 characters.
5. **Background color:**
 - a. Check **Enable customized background color** and either:
 - Type in a HEX color value, or
 - Open the **Background color** menu.

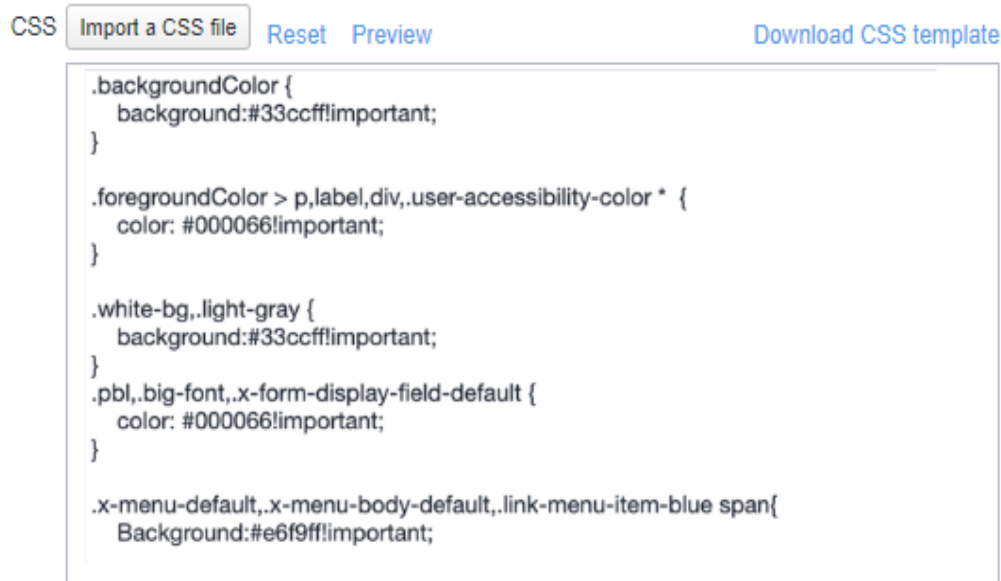
- b. Select or enter a value for the background color.



Based on your choice of background color, Ivanti EPMM will automatically determine 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 643](#).

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: <ul style="list-style-type: none">• Up to 24 digits for numbers beginning with the + symbol.• Up to 22 digits for numbers without the + symbol. If you are entering multiple phone numbers, enter a comma-separated list.
Email(s)	Enter one or more email addresses. If you are entering multiple email addresses, enter a comma-separated list.



Either a phone number or an email address is required.

Related topics

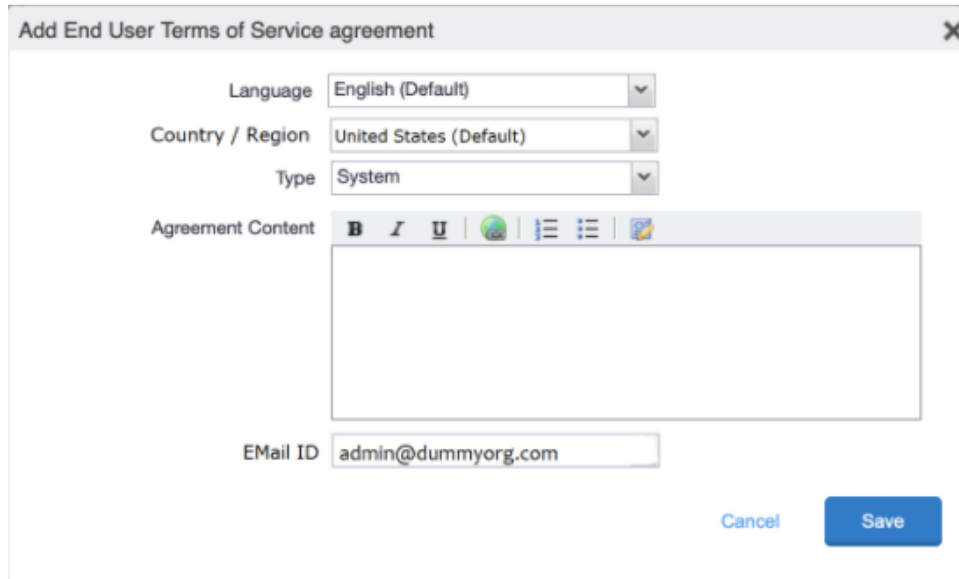
["Viewing the help desk contact information" on page 676.](#)

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.



Add End User Terms of Service agreement

Language: English (Default)

Country / Region: United States (Default)

Type: System

Agreement Content

EMail ID: admin@dummyorg.com

Cancel Save

3. In the **Language** drop-down, select the language for the agreement.
4. In the **Country / Region** drop-down, select the primary country or region.
5. In the **Type** drop-down, select the type of agreement:
 - a. **System** - Select for iOS, macOS and Android devices.
 - b. **AAD enrollment** - Select for Windows devices.
6. In the **Agreement Content** text box, enter your agreement text. The text field permits basic formatting.
7. In the **EMail ID** field, enter an email address to receive confirmation emails when the users accept the agreement.
8. Click **Save**. Your new agreement appears in the End User Terms of Service table.

End User Terms of Service

Add an End User Terms of Service agreement that will be displayed to end users when they register. End users must accept the agreement in order to complete registration.

LANGUAGE	EUTS.TYPE	LAST MODIFIED	ACTIONS
Chinese	SYSTEM	2020-06-09 01:21:54 PM IST	Edit Preview Delete
English (Default)	SYSTEM	2020-06-04 08:58:03 PM IST	Edit Preview Delete

[Add+](#)

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)

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*.

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 version 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" on page 74](#).
 - **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**.

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 482](#)
- ["Audit Logs use cases" on page 503](#)
- ["App information" on page 498](#)

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**.

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 397](#)

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 Android 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*.

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

Device Registration

☐ Enable Server Name Lookup

☐ Allow registration when password change is required

In-App Registration Requirement ☐ Password
☒ Registration PIN
☐ Password and Registration PIN

☐ Allow silent in-app registration only once. (iOS only)

Silent in-app registration time limit (minutes). (iOS only) Within minutes

Apple Web-based Registration Requirement ☒ Password
☐ Registration PIN
☐ Password and Registration PIN
☐ User and Registration PIN

Zero Touch and Samsung Knox Mobile Enrollment ☐ Password
☒ Registration PIN
☐ Password and Registration PIN

Managed Devices / Device Owner (afw#, QR code, NFC) ☐ Password
☒ Registration PIN
☐ Password and Registration PIN

- 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.

Password and Registration PIN

Users who can register devices can also request and receive device passwords and registration PINs. To allow managed Android device users to request a password and registration PIN, the **Password and Registration PIN** radio buttons for Zero Touch and Samsung Knox Mobile Enrollment OR Managed Devices / Device Owner (afw#, QR code, NFC) fields must be selected in **Settings > System Settings > Users & Devices > Device Registration**.

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:

Per-User Device Limit

Standard device limit takes precedence over LDAP membership specific device limit to all applicable users

Per-User Device Limit (1-50, or none)

LDAP group specific device limit

LDAP SERVER	LDAP GROUP	DEVICE LI...	ACTIONS
No records to display			

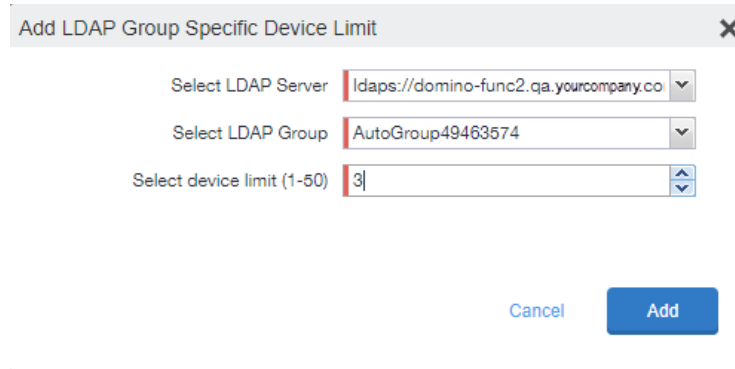
Note: Standard device limit will apply to LDAP groups that are not mentioned above.

[Add+](#)

Device limit precedence setting ☒ Standard device limit takes precedence over LDAP membership specific device limit to all applicable users
☐ LDAP group specific device limit takes precedence over standard device limit to all applicable users

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.

A screenshot of a dialog box titled "Add LDAP Group Specific Device Limit" with a close button (X) in the top right corner. The dialog contains three fields: "Select LDAP Server" with a dropdown menu showing "ldaps://domino-func2.qa.yourcompany.co", "Select LDAP Group" with a dropdown menu showing "AutoGroup49463574", and "Select device limit (1-50)" with a text input field containing the number "3" and a small up/down arrow icon to its right. At the bottom right of the dialog are two buttons: "Cancel" and "Add".

- 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.

Per-User Device Limit

Standard device limit takes precedence over LDAP membership specific device limit to all applicable users

Per-User Device Limit (1-50, or none)

LDAP group specific device limit

LDAP SERVER	LDAP GROUP	DEVICE LI...	ACTIONS
ldaps://domino-func2.qa.mobi...	AutoGroup2821488	4	Edit Delete

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.

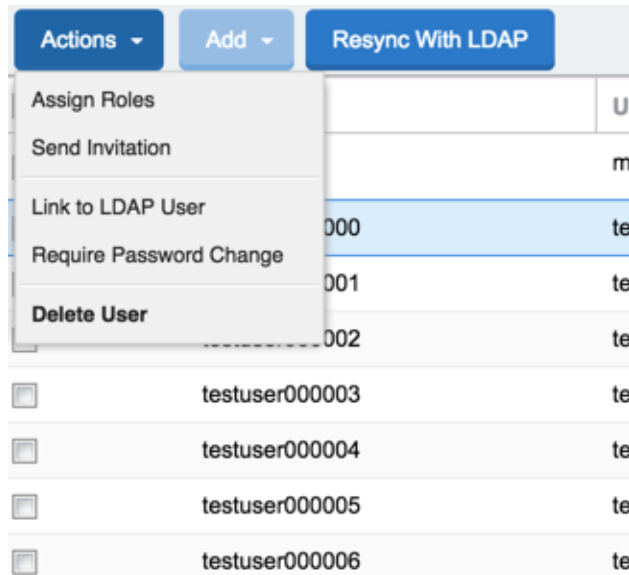
Requiring user portal password change

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 Android 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 Android devices**.
9. Select **Allow Android users to recover their passcode**.
10. Select **Save**.

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 129](#).

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 665](#).
- **Helpdesk** - Configure the help desk contact information to display in the user portal. See ["Configuring help desk contact information" on page 637](#).
- **Settings** - View user portal settings.
- **Sign Out** - Sign out of the self-service user portal.

If Register Device role is enabled

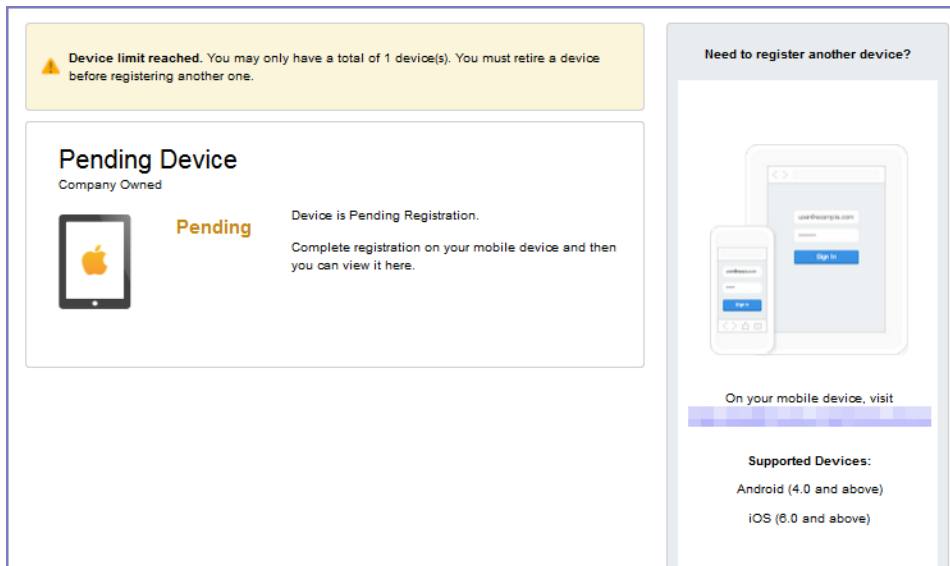
If the **Register Device** role is enabled, device users will be able to send an invitation from the user portal to register their device.

FIGURE 1. SEND INVITATION TO REGISTER

The screenshot shows the Ivanti user portal interface. At the top left is the Ivanti logo. At the top right, a user profile dropdown shows 'Welcome miadmin'. The main content area is divided into two panels. The left panel, titled 'Send Invitation', contains a form with the following fields: 'Platform' (dropdown menu), 'Device Language' (dropdown menu), a checkbox for 'My device has no phone number', 'Country' (dropdown menu), 'Phone Number (No space or leading zero)' (text input), 'Operator' (dropdown menu), 'Device ownership' (radio buttons for 'Company' and 'Employee'), and a checkbox for 'Notify User By SMS'. At the bottom of this panel are 'Cancel' and 'Send Invitation' buttons. The right panel, titled 'Need to register another device?', features an illustration of a smartphone and a tablet. Below the illustration, it says 'Send registration instructions via SMS message and email to register a new device.' with a 'Send Invitation' button. Further down, it says 'On your mobile device, visit <https://saop026.eapq.engdevroot.com/qc>' and 'Or, click on the button below to generate a QR code version of this URL that you can scan with any code scanning app.' with a 'Generate QR Code' button.

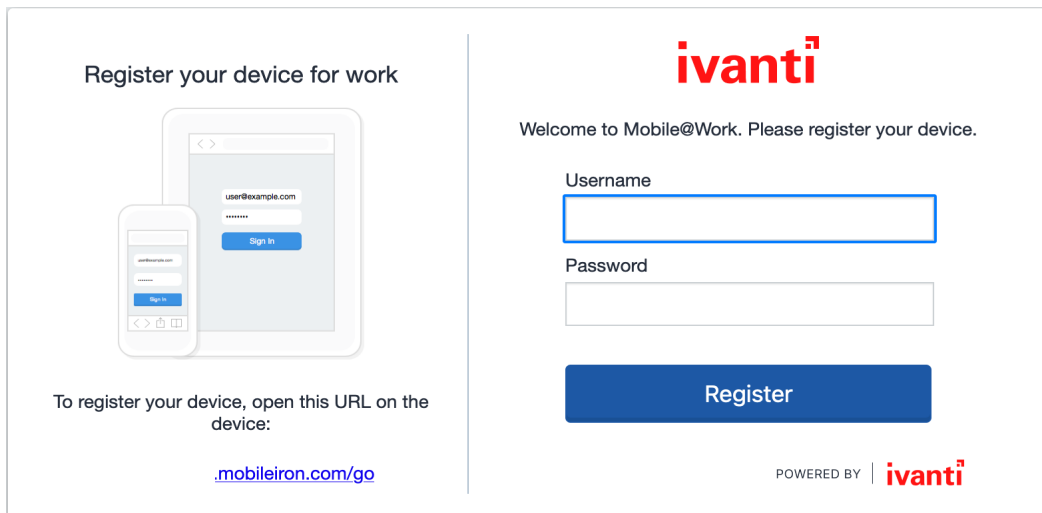
After the invitation is sent, the device status is seen as **Pending**.

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

**Device limit reached.** You may only have a total of 1 device(s). You must retire a device before registering another one.

iPhone 6 Plus

Company Owned



Active

2 m 0 s ago

Version

iOS 8.3

Carrier

T-Mobile

IMEI

35439206439141

No Phone Number


Manufacturer

Apple

Registration Date

2015-09-30 12:14:00 PM PST

Need to register another device?



On your mobile device, visit

Supported Devices:

Android (4.0 and above)

iOS (8.0 and above)

Registration instructions

On Android devices, users can follow the prompts to download Ivanti Mobile@Work and complete the registration.

If PIN-based registration is enabled

If PIN-based registration is enabled, device users will see **Request Registration PIN**.



Welcome miadmin

[← Back](#)

Request Registration PIN

Provide information about your device to receive a SMS message with the registration instructions. You will also receive a registration email in your company email inbox.

Platform

Select Platform

Device Language

English

☒ My device has no phone number

Device ownership ☐ Company ☒ Employee

[Cancel](#)[Request PIN](#)

Need to register another device?



Your organization requires you to have a valid PIN to register a device.

[Request Registration PIN](#)

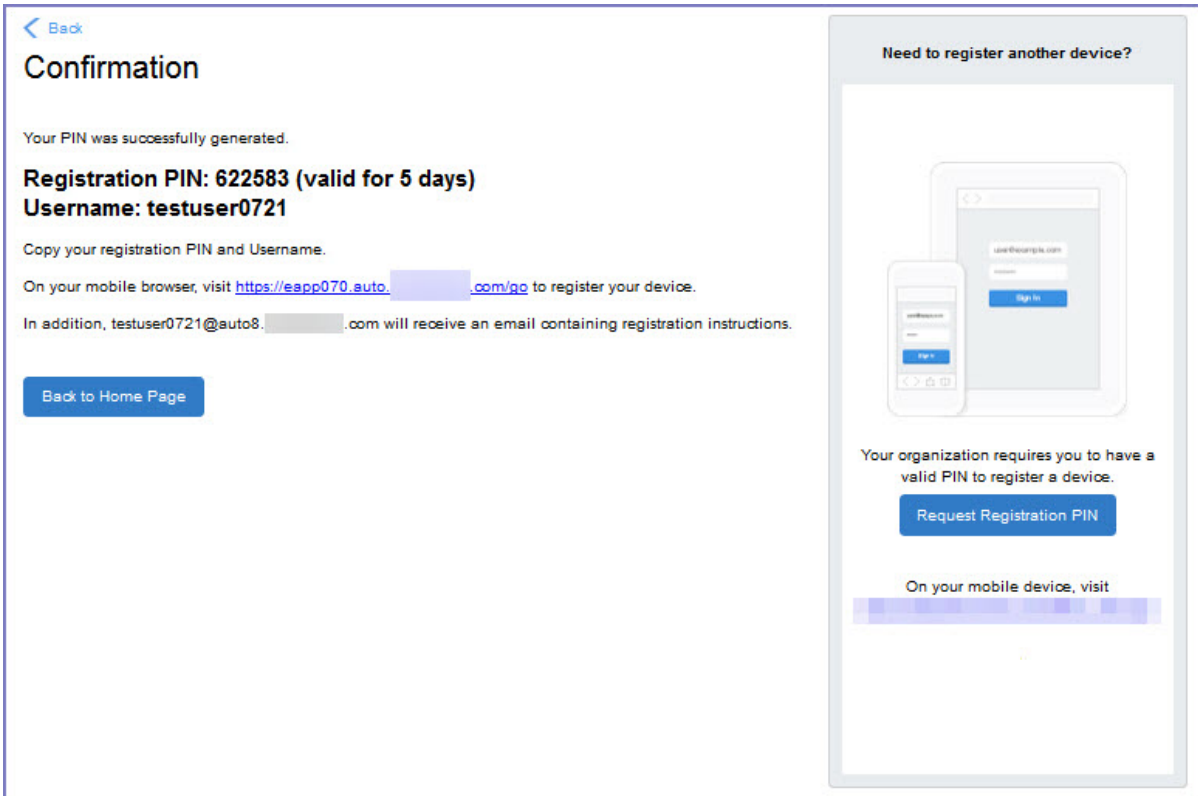
On your mobile device, visit
<https://san-vm178.hyd.mobileiron.com/go>

Or, click on the button below to generate a QR code version of this URL that you can scan with any code scanning app.

[Generate QR Code](#)

Selecting **Request PIN** allows device users to send an invitation for registration as well as generate a PIN.

FIGURE 5. REGISTRATION WITH 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.

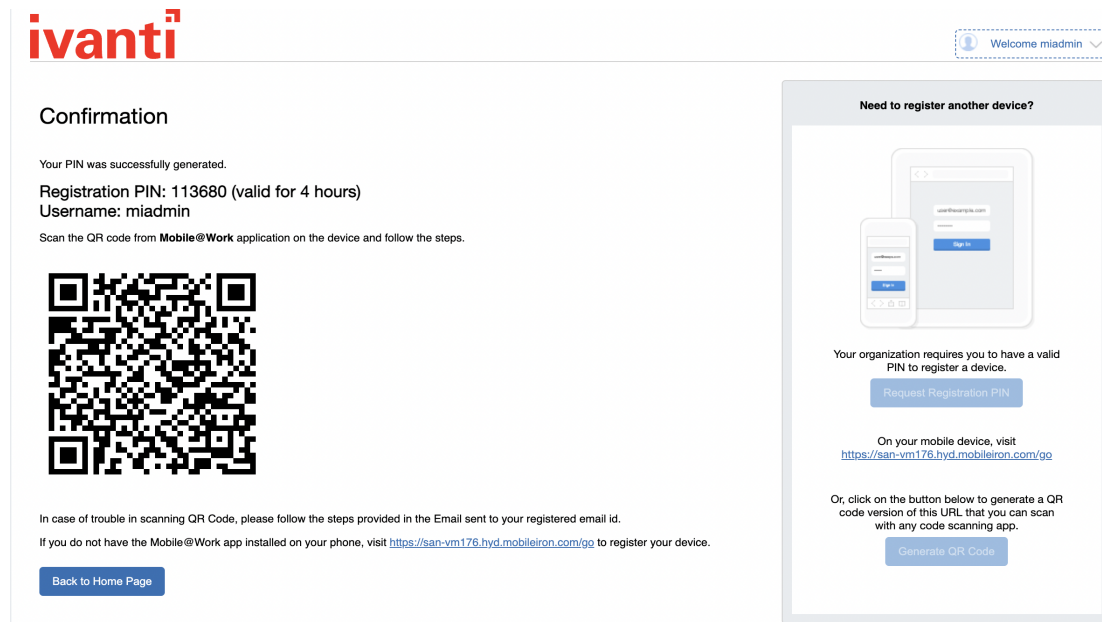
When users log into the Self-service portal (SSP) home page, they can select one of two registration buttons:

- 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.

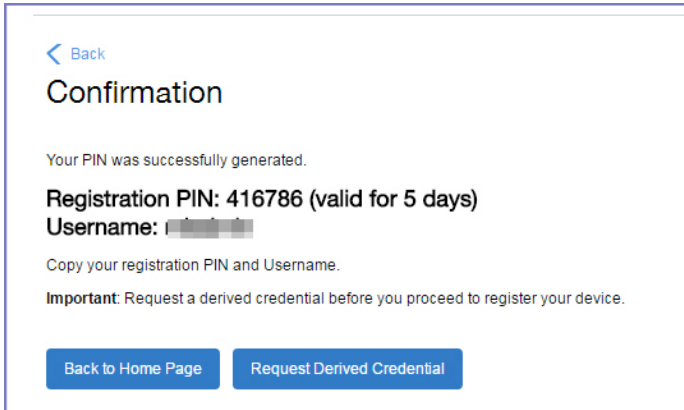
FIGURE 6. REGISTRATION WITH QR CODE



If getting an Entrust derived credential is enabled

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



< Back

Confirmation

Your PIN was successfully generated.

Registration PIN: 416786 (valid for 5 days)

Username: [REDACTED]

Copy your registration PIN and Username.

Important: Request a derived credential before you proceed to register your device.

[Back to Home Page](#) [Request Derived Credential](#)

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.

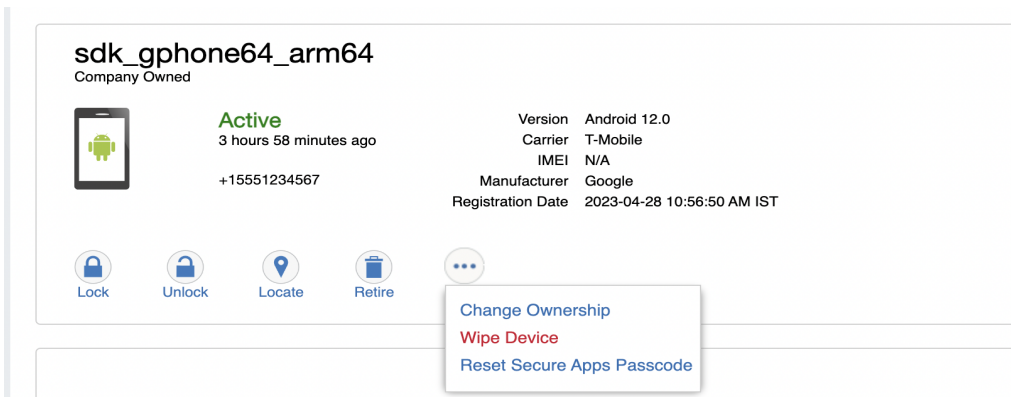
The user then does the following:

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

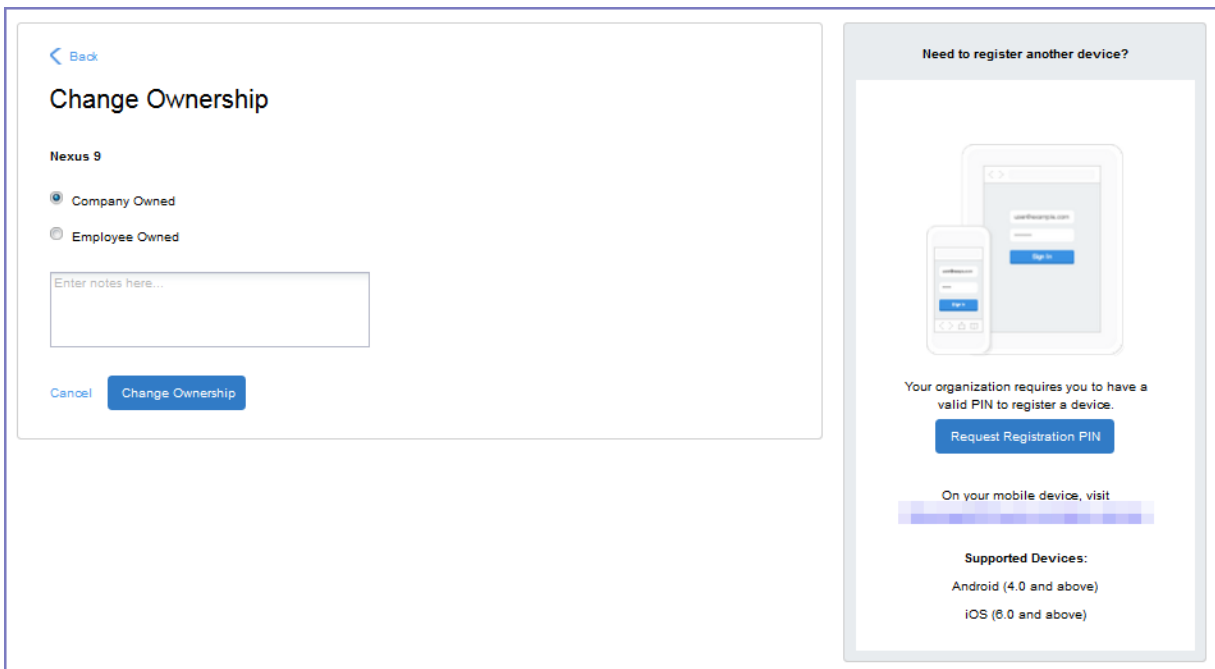
If the **Change Device Ownership** role is enabled, device users will see the option to change the device ownership.

FIGURE 8. CHANGE DEVICE OWNERSHIP OPTION



Selecting **Change Ownership** allows the user to change the device ownership.

FIGURE 9. CHANGE DEVICE OWNERSHIP SETTINGS



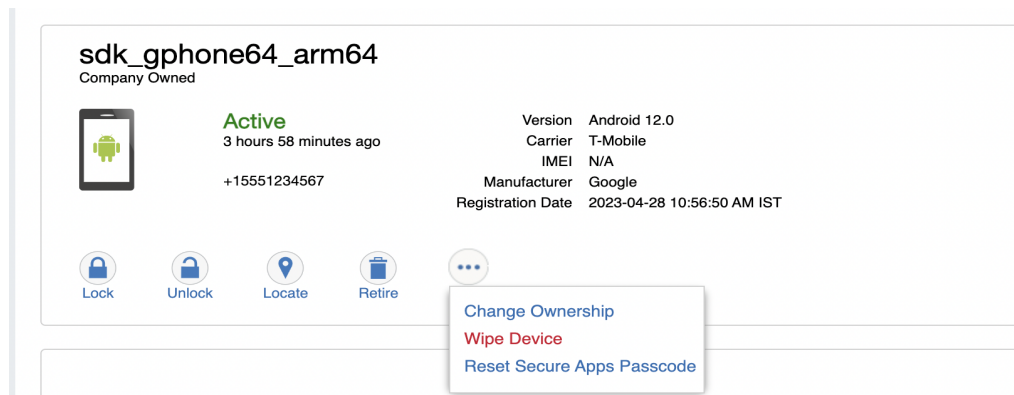
If Default ownership for devices is enabled for Device users

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 "[What is the self-service user portal?](#)" on page 677, 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 637](#).
- **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

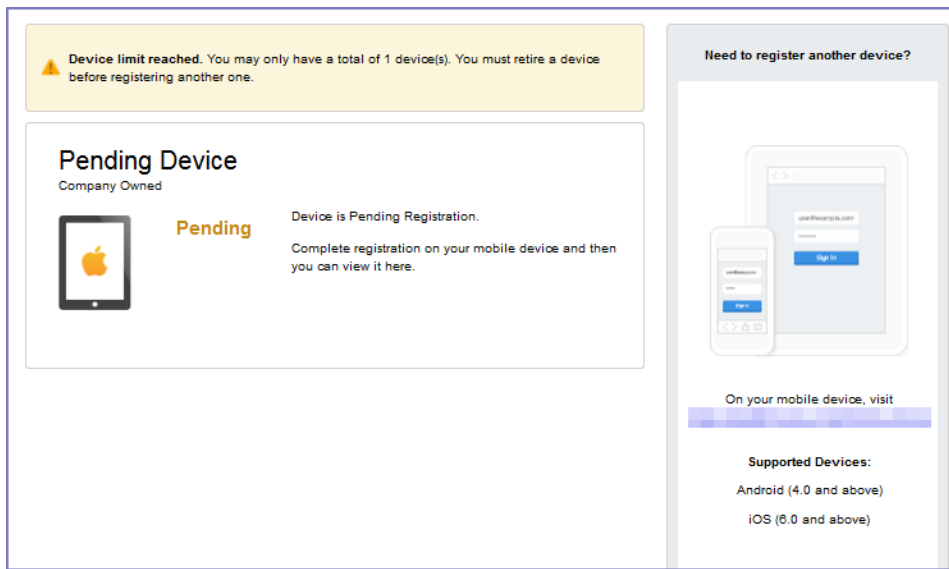
The screenshot displays the Ivanti self-service user portal interface. At the top left is the Ivanti logo. A user profile dropdown in the top right shows 'Welcome miadmin'. The main content area is titled 'Send Invitation' and includes a 'Back' button. Below the title, a message states: 'Provide information about your device to receive a SMS message with the registration instructions. You will also receive a registration email in your company email inbox.' The form contains the following fields and options:

- Platform:** A dropdown menu with 'Select Platform' as the current selection.
- Device Language:** A dropdown menu with 'English' as the current selection.
- ☐ My device has no phone number
- Country:** A dropdown menu with 'United States' as the current selection.
- Phone Number (No space or leading zero):** A text input field starting with '+1'.
- Operator:** A dropdown menu with 'Operator Name' as the current selection.
- Device ownership:** Radio buttons for 'Company' and 'Employee', with 'Employee' selected.
- ☐ Notify User By SMS

At the bottom of the form are 'Cancel' and 'Send Invitation' buttons. To the right of the form is a side panel titled 'Need to register another device?'. It features an illustration of a smartphone and a tablet displaying the registration process. The panel includes the text: 'Send registration instructions via SMS message and email to register a new device.' with a 'Send Invitation' button. Below this, it says: 'On your mobile device, visit <https://eapco056.eapc.engdevroot.com/qc>'. At the bottom, it states: 'Or, click on the button below to generate a QR code version of this URL that you can scan with any code scanning app.' with a 'Generate QR Code' button.

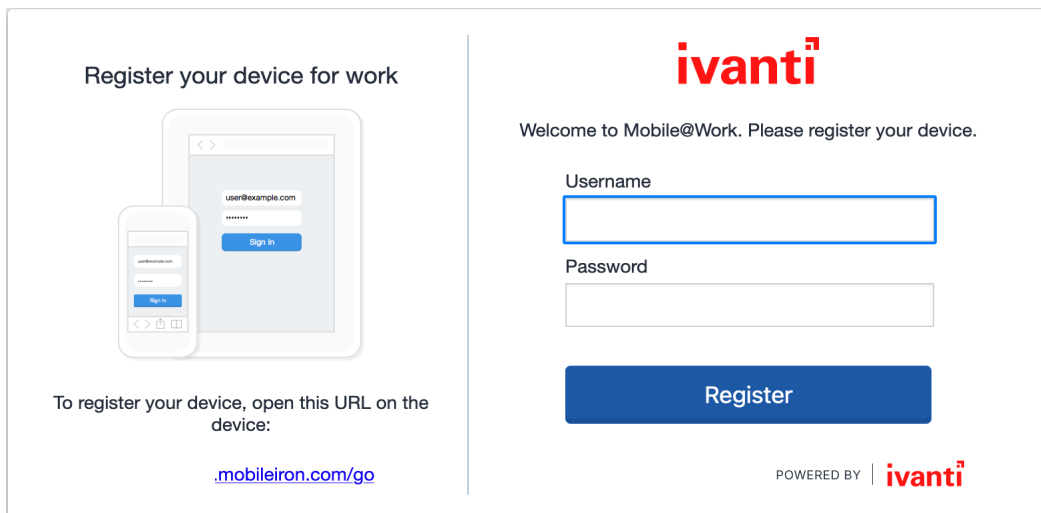
After the invitation is sent, the device status is seen as **Pending**.

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

Device limit reached. You may only have a total of 1 device(s). You must retire a device before registering another one.

iPhone 6 Plus


Company Owned



Active
2 m 0 s ago

Version: iOS 8.3
Carrier: T-Mobile
IMEI: 35439206439141
No Phone Number
Manufacturer: Apple
Registration Date: 2015-09-30 12:14:00 PM PST

Need to register another device?



On your mobile device, visit

Supported Devices:

Android (4.0 and above)

iOS (8.0 and above)

Copyright © 2023, Ivanti, Inc. All Rights Reserved. [Privacy and Legal](#).

Page 667 of 690

Registration instructions

On Android devices, users can follow the prompts to download Ivanti Mobile@Work and complete the registration.

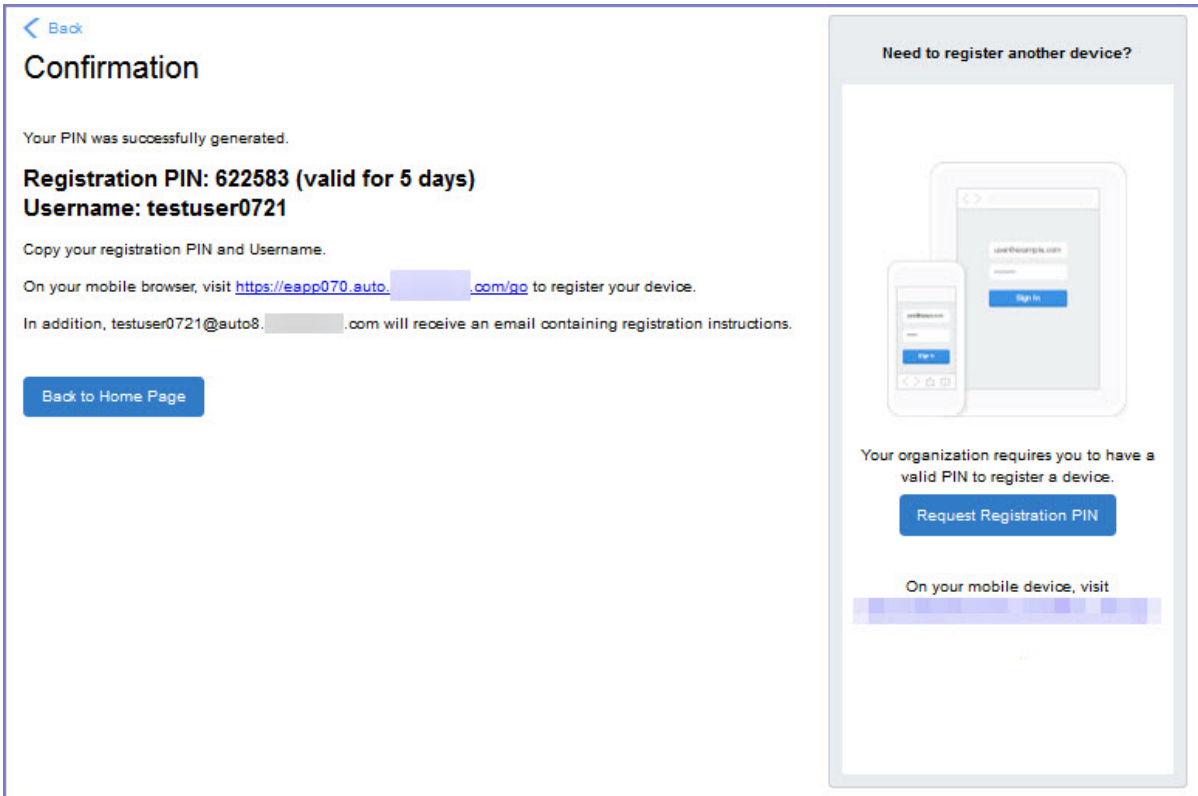
If PIN-based registration is enabled

If PIN-based registration is enabled, device users will see the Request Registration PIN page.

The screenshot displays the Ivanti Mobile@Work user portal. At the top left is the Ivanti logo. At the top right, a user is logged in as 'miadmin'. The main content area is titled 'Request Registration PIN' and includes a 'Back' button. Below the title, instructions state: 'Provide information about your device to receive a SMS message with the registration instructions. You will also receive a registration email in your company email inbox.' The form contains three dropdown menus: 'Platform' (with 'Select Platform' as the current selection), 'Device Language' (set to 'English'), and 'Device ownership' (with radio buttons for 'Company' and 'Employee', where 'Employee' is selected). A checkbox labeled 'My device has no phone number' is checked. At the bottom right of the form are 'Cancel' and 'Request PIN' buttons. To the right of the main form is a sidebar titled 'Need to register another device?'. It features an illustration of a smartphone and tablet displaying the app's login screen. Below the illustration, it states: 'Your organization requires you to have a valid PIN to register a device.' and includes a 'Request Registration PIN' button. Further down, it says: 'On your mobile device, visit <https://san-vm176.hyd.mobileiron.com/go>'. At the bottom of the sidebar, it says: 'Or, click on the button below to generate a QR code version of this URL that you can scan with any code scanning app.' and includes a 'Generate QR Code' button.

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.

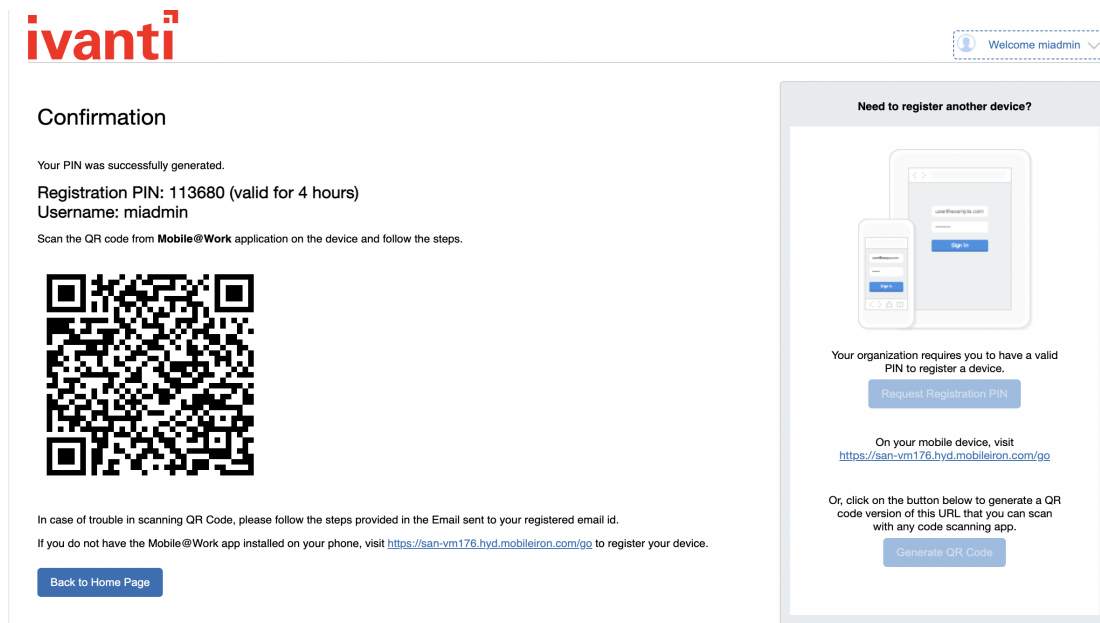
When users log into the Self-service portal (SSP) home page, they can click one of two registration buttons:

- 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.

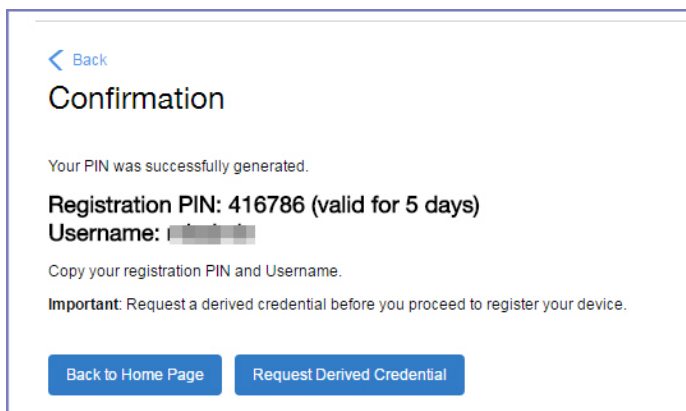
FIGURE 1. REGISTRATION WITH QR CODE



If getting an Entrust derived credential is enabled

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 EPM, 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.

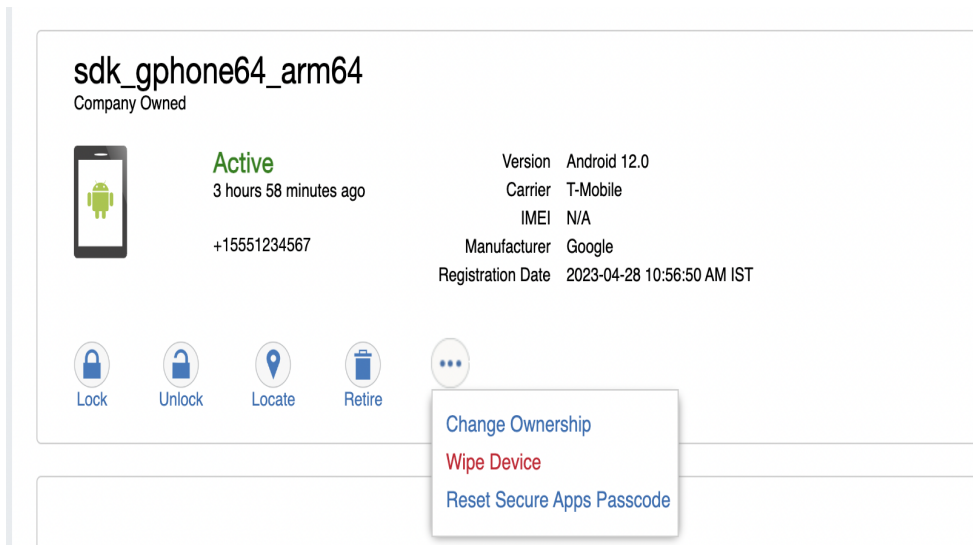
The user then does the following:

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

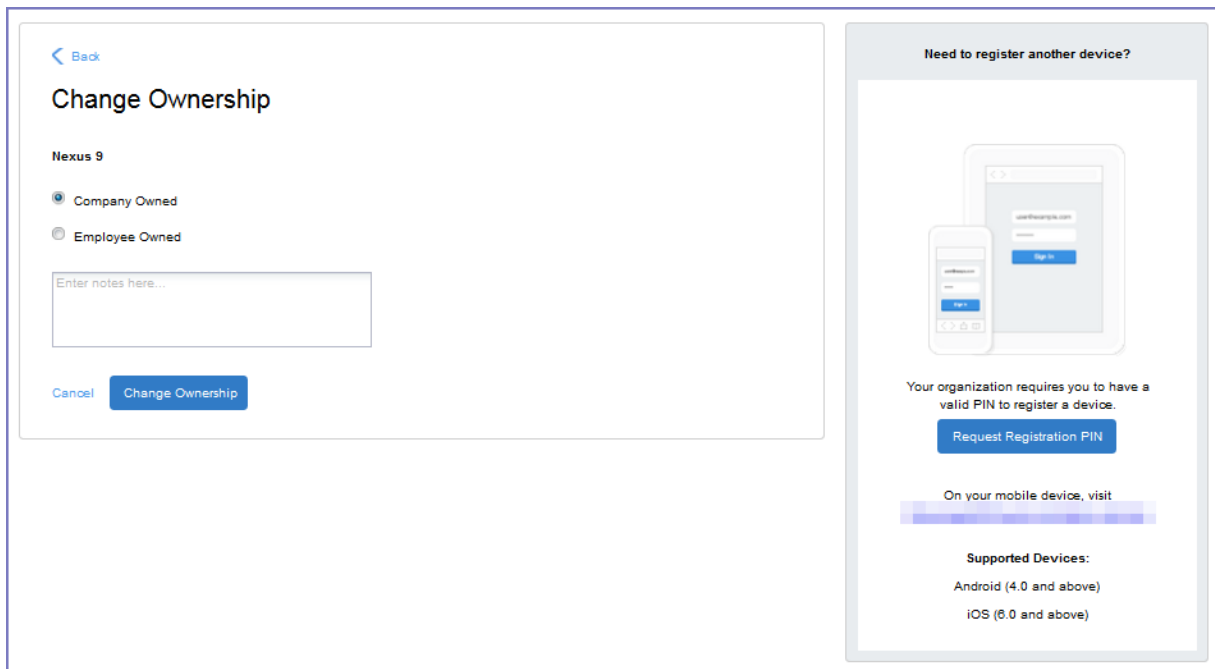
If the **Change Device Ownership** role is enabled, device users will see the option to change the device ownership.

FIGURE 1. CHANGE DEVICE OWNERSHIP OPTION



Clicking on **Change Ownership** allows the user to change the device ownership.

FIGURE 2. CHANGE DEVICE OWNERSHIP SETTINGS



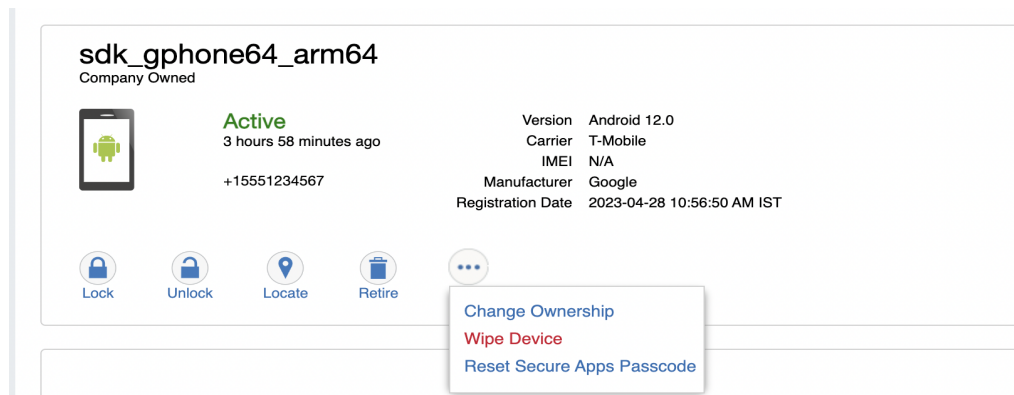
If Default ownership for devices is enabled

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 "What is the self-service user portal?" on page 677, 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



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.

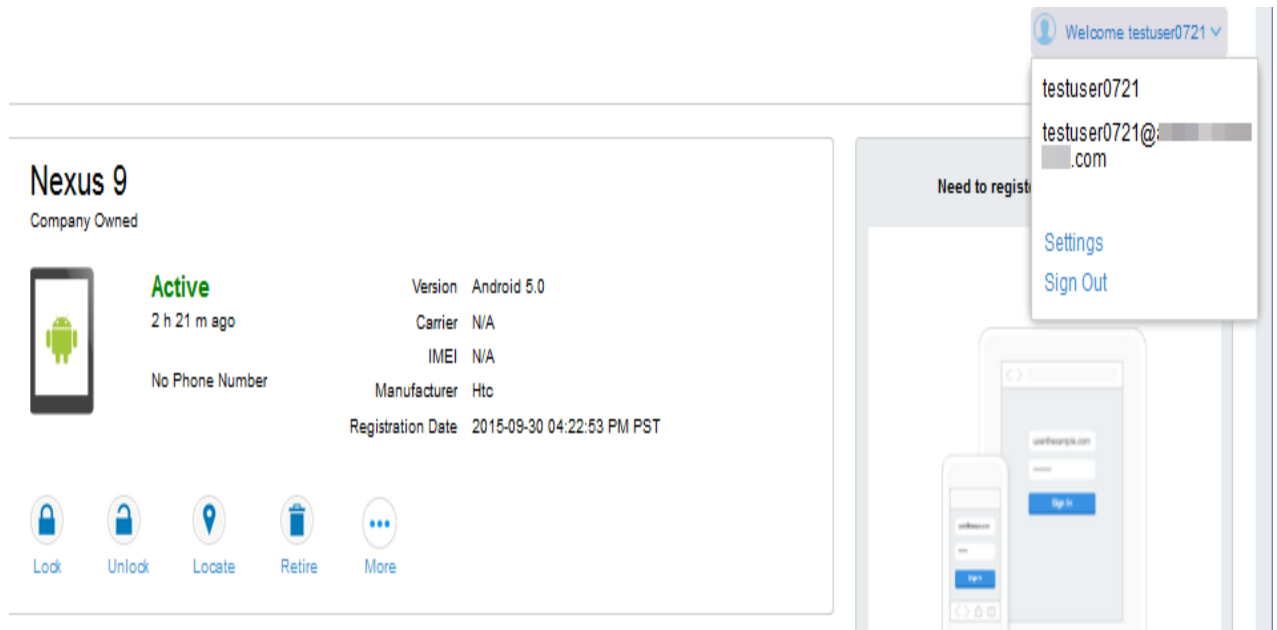
Uploading certificates in the user portal on a desktop computer

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.

FIGURE 1. USER PROVIDED CERTIFICATE MANAGEMENT



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

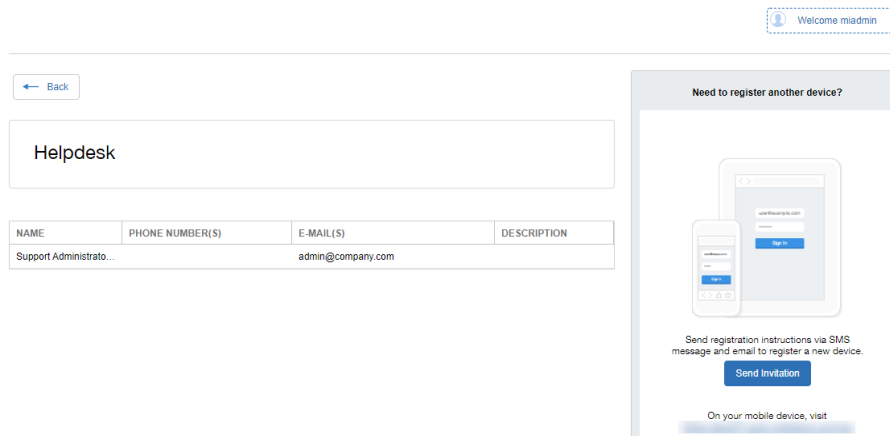
If the help desk contact information is configured in the Admin Portal, device users can view the contact information in the self-service user portal.

For information about configuring the help desk contact information see, ["Configuring help desk contact information" on page 637](#)

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



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 Android Enterprise with the alternative method

The alternative method enables you to use Android Enterprise and requires sharing your user information with Google and binding your domain with Google. Each of your end users must have a Google account. However, Ivanti recommends setting up your Android Enterprise account *without* binding your domain with Google as described in ["Enabling Android Enterprise" on page 15](#).

- ["Method 1: Setting up using AFW json file generated from google account" below](#)
- ["Managing users for Android Enterprise" on page 688](#)

Method 1: Setting up using AFW json file generated from google account

The alternative setup method consists of the following steps:

- ["Step 1: Sign up for Android Enterprise with Google and get the EMM Token" on the next page](#): in the Google Admin Console.
- ["Step 2: Create a Google service account and get a JSON file" on page 681](#): in the Google Admin Console
- ["Step 3: Generate the JSON enrollment file" on page 682](#): from the Ivanti Support site
- ["Step 4: Bind Ivanti EPMM with Android Enterprise" on page 683](#): in Ivanti EPMM
- ["Step 5: Authorize Ivanti EPMM to view and manage your Google users" on page 683](#): in Ivanti EPMM
- ["Step 6: Create the Android Enterprise setting" on page 685](#): in Ivanti EPMM

After completing these steps, continue to ["Managing users for Android Enterprise" on page 688](#).

Step 1: Sign up for Android Enterprise with Google and get the EMM Token

Follow Google's set up instructions to sign up for Android Enterprise, and then receive the EMM Token.

Prerequisite:

- Your company has a corporate Google Account or will create one following Google's instructions

You will need:

- Access to your company's Google administrator account



This step is performed on Google's website and is subject to change by Google.

In a web browser:

1. Go to Google's Android Enterprise sign up page:
"Sign up for Android Enterprise"
https://www.google.com/a/signup/u/0/?enterprise_product=ANDROID_WORK
2. Follow Google's instructions
 - Your setup may involve several steps, depending on whether or not your domain is already a Google Apps customer.
 - You may need to verify ownership of your domain with Google.
 - You may be directed to create a service account. The instructions for the service account are in Step 2.

You will need to set up a service account, because it authenticates interactions between Ivanti EPM in your domain and the Google EMM Play API. Follow Google's instructions to do so here:
"Setup with a third-party EMM provider"

<https://support.google.com/work/android/answer/6174046>

Next, generate an EMM Token.

1. Sign in to the Google Admin Console (admin.google.com) with your super administrator credentials.
2. Navigate to **Security > Android enterprise Settings**. The page shows a token if one was generated

in the last 30 days, or a button to generate a new token.

3. Copy this token (as text) to use in Step 3.

Step 2: Create a Google service account and get a JSON file

In this step, you create a Google project and a service account with the EMM API enabled. You then receive a JSON file that holds a public/private key pair used to authorize interactions between apps on your domain and Google APIs.



This step is performed on Google's website and is subject to change by Google. These instructions are based on: "Setup with a third-party EMM provider"
<https://support.google.com/work/android/answer/6174046>



You will need access to your company's Google administrator account

In a web browser:

1. Go to Google's Developers Console: <https://console.developers.google.com>
2. Log in with your Google administrator account credentials.
3. Create a new project.
4. With the dashboard showing the new project, click "Enable and manage APIs".
5. Search for "Google Play EMM API". Click the search result to select the API.
6. Click "Enable" to enable Google Play EMM API for your project.
7. Click "Credentials" in the left navigation pane.
8. Click "Create credentials" and choose "Service account key".
9. For "Service account", select "New service account" and type in a name.
10. Select "Furnish a new private key"
11. For "Key type", select JSON.
12. Click "Create".

The JSON file will be downloaded to your computer. Check that the download file is given the name as indicated in the confirmation dialog with a ".json" extension, as some browsers may use a generic filename.

Important: Store this file securely.

Step 3: Generate the JSON enrollment file

In this step, you will use the EMM Token and JSON file you obtained from Google to receive the **ActivateAfWForCore.json** enrollment file from the Ivanti Support portal. You can use the same enrollment file to enroll or re-enroll any number of Ivanti EPMM instances that run on your domain.

You will need:

- Your company's login account for the [Ivanti Support site](#)
- To get a login account, go to [Login Request](#)
- Administrator access to Ivanti EPMM
- The EMM Token from Step 1
- The Google JSON file from Step 2

In Ivanti EPMM:

1. Log in to the support portal at [Ivanti Support site](#).
2. Select **Android enterprise Enrollments**.
3. Click **Create New Android enterprise Enrollment**.
4. Click **Use Alternate Setup** to fill out the dialog with your EMM Token and domain URL.
5. Click **Choose file** to upload the Google JSON file from "[Step 2: Create a Google service account and get a JSON file](#)" on the previous page.
6. Click **Submit**.

The enrollment file will be generated.

7. Click **Download Google JSON Enrollment file**.

8. The **ActivateAfWForCore.json** enrollment file is downloaded to your computer.

Some browsers may save the enrollment file with another name. Rename the file to *ActivateAfWForCore.json* before continuing.

Store the *ActivateAfWForCore.json* file securely.

You can use the same *ActivateAfWForCore.json* file to enable Android Enterprise on multiple Ivanti EPMM instances that belong to the same domain. You can also reuse the same file if you remove Android Enterprise from Ivanti EPMM, and then want to re-enroll it following the next steps again.

When this step completes successfully, Ivanti will be your Unified Endpoint Management (UEM) provider for Android Enterprise, and will appear in the Security > Android Enterprise settings on admin.google.com,

Step 4: Bind Ivanti EPMM with Android Enterprise

In this step, you upload the enrollment file from Step 3 to Ivanti EPMM, in order to bind Ivanti EPMM with your domain's Android Enterprise account.

You will need:

- Administrator access to Ivanti EPMM
- The *ActivateAfWForCore.json* file from Step 3

In Ivanti EPMM:

1. Go to **Services > Google**.
2. Click **Browse** in the **Android Enterprise** section, in the box labeled "2".
3. Select the **ActivateAfWForCore.json** file you collected in Step 3.
4. Click **Connect**.
5. When the Google Account is connected successfully, box 2 will show a confirmation including **Status: Connected**.

Step 5: Authorize Ivanti EPMM to view and manage your Google users

In this step, you give Ivanti EPMM permission to read Android Enterprise user IDs from existing Google user accounts. Users with Google user accounts are eligible to use Android Enterprise.

By default, Ivanti EPMM uses the substitution value \$EMAIL\$ as the Google user account name. You can change this value to match your environment. You make this change by modifying the **User Sync Variable** field in this step. You can use any Ivanti EPMM substitution variables along with hard-coded strings, as long as the format of the string after variable substitution has the format of a Google email address.

The following table gives some examples:

TABLE 108. EXAMPLES OF IVANTI EPMM SUBSTITUTION VARIABLES FOR THE GOOGLE USER ACCOUNT NAME

User Sync Variable value	Use this value when...
\$USER_CUSTOM1\$	<p>You have set \$USER_CUSTOM1\$ in your LDAP setting in the Admin Portal (at Services > LDAP) to be the Google email address of an LDAP user.</p> <p>For example, after substitution: jdoe@someComany.com</p>
\$USERID\$@someCompany.com	<p>\$USERID\$ of an LDAP user is the same as the user name part of the user's Google email address.</p> <p>For example, after substitution: jdoe@someCompany.com</p>
\$USERID\$@\$USER_CUSTOM2\$ \$USERID\$@someSubDomain.\$USER_CUSTOM2\$	<ul style="list-style-type: none"> The Google account domain has a subdomain. \$USERID\$ of an LDAP user is the same as the user name part of the user's Google email address. You have set \$USER_CUSTOM2\$ in your LDAP setting in the Admin Portal (at Services > LDAP) to the LDAP user domain. <p>For example, after substitution: jdoe@someSubDomain.someCompany.com</p>

You will need:

- Steps 1 -4 completed

In Ivanti EPMM:

1. Go to **Services > Google**.
2. Change \$EMAIL\$ in the **User Sync Variable** field if \$EMAIL\$ is not the Google user account name that you have set up for your users.



Changing the User Sync Variable later requires you to remove the Android Enterprise account as described in ["Removing the Android Enterprise account in Ivanti EPMM" on page 27](#).

3. Click **Authorize** in the **Android Enterprise** section, in the box labeled "3".

When authorization completes successfully, the Android Enterprise section replaces the three steps with your account settings.

Step 6: Create the Android Enterprise setting

In this step, you create the Android Enterprise setting in Ivanti EPMM. This setting must be applied to each Android Enterprise-capable device in order for the device to have Android Enterprise functionality.

In the Ivanti EPMM Admin Portal:

1. Go to **Policies & Configs > Configurations**
2. Click **Add New > Android > Android enterprise**. The New Android enterprise (all modes) Setting dialog box opens.
3. Type a name for this setting (for example, "Android Enterprise enabled")
4. Click **Save**.
5. Apply it to a label that is also applied to Android Enterprise-capable devices.
Important Recommendation: Apply this setting to the built-in **Android** label, or a custom label that is defined using the filter "android.afw_capable = true". For more details, refer to the *Getting Started with Ivanti EPMM*.

Method 2: Setting up directly via Ivanti EPMM without generating AFW json file

The alternative setup method allows enterprises that are non G Suite users to be enrolled with Android enterprise without sending any personal information (email addresses to Google). Ivanti EPMM will provision and manage users automatically with Google. Authorise Android Enterprise with an admin Google account by:

- ["Step 1: Bind Ivanti EPMM with Android Enterprise"](#) below:

After completing these steps, continue to ["Managing users for Android Enterprise"](#) on page 688.

Step 1: Bind Ivanti EPMM with Android Enterprise

In Ivanti EPMM:

1. Go to **Services > Google**.
2. Click Authorise Google.
This opens Google Play where you need to add the Admin account.
3. In the Bring Android to Work page, click Get Started and integrate Ivanti EPMM with the Google account.
4. Add Contact Details.
5. Click Complete Registration.
6. When the Google Account is connected successfully, box 2 will show a confirmation including **Status: Connected**.

Step 2: Create the Android Enterprise setting

In this step, you create the Android Enterprise setting in Ivanti EPMM. This setting must be applied to each Android Enterprise-capable device in order for the device to have Android Enterprise functionality.

In the Ivanti EPMM Admin Portal:

1. Go to **Policies & Configs > Configurations**
2. Click **Add New > Android > Android enterprise**. The New Android enterprise (all modes) Setting dialog box opens.
3. Type a name for this setting (for example, "Android Enterprise enabled")
4. Click **Save**.
5. Apply it to a label that is also applied to Android Enterprise-capable devices.
Important Recommendation: Apply this setting to the built-in **Android** label, or a custom label that is defined using the filter "android.afw_capable = true". For more details, refer to the *Getting Started with Ivanti EPMM*.

Impact of Android Enterprise setting to devices that are not Android Enterprise-capable

There is no impact to devices that are not Android Enterprise-capable to have the Android Enterprise setting applied. Some devices might become Android Enterprise-capable in the future, if the carrier upgrades the device's firmware.

To view the status of the Android Enterprise setting for a device:

- Go to **Devices & Users > Devices**.
- Open the device details for the device.
- Click the **Configurations** tab.
- Look for the Android Enterprise setting. The **Status** column will show:
 - **Pending**: The device has not yet confirmed that it has received the setting.
 - **Applied**: the setting is applied.
 - **Sent**: the device is not Android Enterprise-capable; the setting is ignored by Ivanti Mobile@Work.

Managing users for Android Enterprise

User accounts in Ivanti EPMM that are meant for Android Enterprise use are added, edited, and deleted in the same way as any Ivanti EPMM user accounts. However, when you bind your user domain with Google, a user can register an Android Enterprise device only if the user is added as a user in your corporate Google Account.

Ivanti EPMM automatically syncs with your corporate Google Account to enable Android Enterprise for eligible users.

Syncing Google user accounts with Ivanti EPMM

When you enabled Android Enterprise on Ivanti EPMM, you provided Ivanti EPMM with access to view your corporate Google Account including the list of users. Ivanti EPMM has read-only access to the Google user accounts, which means Ivanti EPMM cannot add or modify your users' Google accounts.

Therefore, Ivanti EPMM keeps a list of which of its users have Google user accounts, thereby linking each Ivanti EPMM user account with its corresponding Google user account.

Ivanti EPMM automatically syncs the users in Ivanti EPMM with the users in your corporate Google Account. However, the sync behavior depends on whether you use \$EMAIL\$ for the Google user accounts, as specified in the user sync variable.



Removing a Google account for Ivanti EPMM causes any Android Enterprise devices to retire when they check in.

TABLE 109. IVANTI EPMM BEHAVIOR AND THE USER SYNC VARIABLE

Sync time	User sync variable is \$EMAIL\$	User sync variable is NOT \$EMAIL
Upon authorizing Ivanti EPMM to view the Google Account, when first enabling Android Enterprise	Ivanti EPMM adds users to its list of Google user accounts if the user is in Google's list.	No action.
On periodic intervals (approximately every 15 hours; subject to change)	Ivanti EPMM adds users to and deletes users from its list of Google user accounts based on Google's list.	Ivanti EPMM deletes users from its list of Google user accounts based on Google's list.
On demand when a new user is added in Ivanti EPMM	No action.	No action.
On demand when a user registers a device to Ivanti EPMM	Ivanti EPMM adds the user to its list of Google user accounts if the user is in Google's list.	Ivanti EPMM adds the user to its list of Google user accounts if the user is in Google's list.

Note: Ivanti EPMM ignores Google user accounts that have no corresponding user account in Ivanti EPMM.










Adding a new user in Ivanti EPMM

For the Ivanti EPMM administrator, there are no differences to the process for adding new users when working with Android Enterprise. Users can be added as local users, or automatically through LDAP, as usual.

Using Android Enterprise on a device

To be eligible to use Android Enterprise on a device, the user must have a Google account. This feature is applicable to Work Profile mode, Work managed device mode, and Managed device with work profile mode.

When the Google Play authentication token expires or changes were made (password, permissions, etc) requiring re-authorization, Ivanti Mobile@Work will inform Ivanti EPMM to reissue a new authorization token. This triggers Ivanti EPMM to send a new authorization token to Ivanti Mobile@Work in order to reauthorize Google Play. Ivanti Mobile@Work can make up to 10 re-authorization requests within a 24-hour period. Upon the 11th request, an error message displays on the device, the device will be considered non-compliant and retired. In the Dashboard, a non-compliant icon displays next to the device to indicate to the administrator that there is a problem. The administrator should retire the device instance. It is recommended that all devices associated to that Google user ID to resync with Ivanti EPMM. The device user will need to re-register with Google Play. Below is a log showing the client re-authorization requests and eventual revocation of token.

	Client requested Google...	Success	miadmin	2019-05-09 03:56:50...	2019-05-09 03:56:50...	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Google re-authorization token			2019-05-09 03:55:50...	2019-05-09 03:55:50...	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Google...	Success	miadmin	2019-05-09 03:55:44...	2019-05-09 03:55:44...	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Google...	Success	miadmin	2019-05-09 03:54:36...	2019-05-09 03:54:36...	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Google...	Success	miadmin	2019-05-09 03:53:48...	2019-05-09 03:53:48...	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Google...	Success	miadmin	2019-05-09 03:53:37...	2019-05-09 03:53:37...	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Google...	Success	miadmin	2019-05-09 03:53:33...	2019-05-09 03:53:33...	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Client requested Google...	Success	miadmin	2019-05-09 03:52:53...	2019-05-09 03:52:53...	miadmin (Android 7.1 - PDA 12)	Client reported reauth token re
	Revoking Google User ...	Success	miadmin	2019-05-09 03:36:44...	2019-05-09 03:36:44...	miadmin (Android 7.1 - PDA 12)	Revoking Google user token

Additional information on Android Enterprise apps and related settings can be found in the *Ivanti EPMM Apps@Work Guide*.

Google account method for Android Enterprise profile provisioning

On the Google Admin Console, you can enforce EMM policies on Android devices. If enforced, when a device user adds a managed Google account to a device, such as from Settings, Ivanti Mobile@Work is automatically downloaded and launched. Once the user has registered Ivanti Mobile@Work with Ivanti EPMM and the work profile is created, the account is automatically added to the work profile.

On work managed devices, after factory reset, when the device user logs in with the managed Google account, Ivanti Mobile@Work is automatically downloaded and launched. Once the user has registered Ivanti Mobile@Work with Ivanti EPMM, the device is enrolled with Ivanti EPMM as a work managed device.