Samsung KNOX

Samsung KNOX™ VPN Admin Guide

KNOX Version 2.0

July 2014

SAMSUNG

Document History

Date	Changes
July 9, 2014	Document updated for KNOX 2.0. Added information about per-app and per-container VPN setup.

Contact Support

See To get support.

Contents

What's new in KNOX 2.0 VPN

KNOX 2.0 allows IT admins to configure two containers on the same device. VPN settings reflect this change. In addition to configuring VPN connections for an entire device, IT admins can now configure per-container VPNs to ensure data separation between personal and KNOX containers. IT admins can also configure VPN settings for specific apps to ensure that enterprise data is protected.

New Features

- **Per-app VPN** – Increased separation of data between apps.
- Cloud solution integration with VPN Framework
    - **Split billing support** – Can identify container-specific data usage for enterprise billing purposes
    - **Traffic filtering** – Restrict network traffic for apps that aren't configured with VPN.

For the latest KNOX updates, go to the Samsung KNOX Portal.

Introduction

The popularity of Bring Your Own Device (BYOD) and Corporately Owned Personally Enabled (COPE) programs has increased the need for securing data-in-transit. Secure mobile access to server-based enterprise apps is a fundamental business requirement. However, compliance regulations and other factors require protection of data while in-transit. Data must be secure when using both cellular and Wi-Fi connections. VPN is a reliable solution that can be configured to suit an enterprise's security needs.

How VPN works in KNOX

By default, when you set up a VPN connection for a device, all app traffic uses the same VPN connection. With KNOX, you can create up to five separate, simultaneous VPNs, and assign apps to different VPNs. You can assign only enterprise apps to the KNOX VPNs so that personal apps do not congest enterprise resources.

A KNOX VPN client works in the KNOX container to set up VPN connections with a corporate VPN server. The KNOX VPN client does not come preloaded on devices so you must download it from the Samsung KNOX portal. You can then push the client onto employee devices through your MDM console.

About the VPN features

KNOX provides a comprehensive IPSec and SSL-based VPN solution for the most demanding enterprise requirements. An overview of the KNOX VPN features:

Connectivity	• Full-device VPN with split-tunnel mode • Per-app VPN inside and outside KNOX container • VPN chaining for multiple levels of encryption
Flexibility	• Up to 5 simultaneous VPNs • MDM support • Automatic tunnel re-establishment
High security applications	• FIPS mode configurable by MDM • CAC support for US Government applications • NSA Suite B algorithms • X.509 support with OCSP-based certificate checking
Broad industry support	• Cisco, Juniper, strongSwan • RSA token support • SSL support for Cisco, Juniper, F5
Separation between personal and enterprise	• Identify container-specific data usage for split building • Restrict network traffic for container

KNOX VPN technologies support:

- All current Internet Key Exchange (IKE)/IPsec IETF RFCs – IKEv1, IKEv2 with PSK, and certificate-based authentication
- IKEv1 – Main and aggressive IKE exchange modes with pre-shared key, certificates, Hybrid RSA, and EAP-MD5 authentications
- IKEv2 – Pre-shared key, certificates, EAP-MD5, EAP-MSCHAPv2 authentication methods, mobile extensions
- SSL support for Cisco, Juniper, F5
- Dead Peer Detection (DPD)
- Triple DES (56/168-bit), AES (128/256-bit) encryption with MD5 or SHA
- Split tunneling mode
- NSA Suite B Cryptography
- IKEv1 Suite B suites supported with PSK and ECDSA signature-based authentications
- IKEv2 Suite B suites supported with ECDSA signatures

KNOX implements a FIPS 140-2 Level 1 certified VPN client, a NIST standard for data-in-transit protection along with NSA suite B cryptography. The FIPS 140-2 standard applies to all federal agencies that use cryptographically strong security systems to protect sensitive information in computer and telecommunication systems. Many enterprises today deploy this cryptographically strong VPN support to protect against data-in-transit attacks.

About the VPN models

- **Device-wide VPN**
  - All outgoing traffic from the device goes through the same VPN connection.
  - You can use this type of VPN connection without a KNOX container.
  - You use the native Android VPN client that is pre-installed on the device.
- **Per-container VPN**
  - All outgoing traffic from a KNOX container goes through the same VPN connection.
  - You can use this type of VPN connection only if the device has a KNOX container installed.
  - You must install the KNOX VPN client.
- **Per-app VPN**
  - All outgoing traffic from selected apps goes through the same VPN connection.
  - Configure for apps inside and outside the container
  - You can use this type of VPN connection only if the device has KNOX container installed.
  - You must install the KNOX VPN client.

Device-wide VPN is not recommended as it is not as secure as per-container or per-app VPN. With a device-wide VPN setup, data from the entire device goes through the same VPN connection, including personal data. If you are not using KNOX, this is the only method available. If you are using enterprise KNOX with an MDM solution, you can configure per-container VPN and per-app VPN.

A VPN connection set up for the KNOX container cannot be used concurrently by apps inside and outside of the container.

To use a VPN connection outside the container, you can set up a device-wide VPN or specify the apps that you wish to use the VPN profile outside the container.

For a list of devices supported by each VPN model, contact your MDM provider.

About MDM setup

How you set up KNOX VPNs depends on the MDM system you are using. This guide illustrates MDM setup using the Samsung KNOX Enterprise Mobility Management (EMM) system, using the Active Directory setup on an on-premise server. For details on how to set up VPNs on your MDM system, see the documentation or online help provided with your system.

Before you begin

On the VPN server, check the VPN setup, for example:

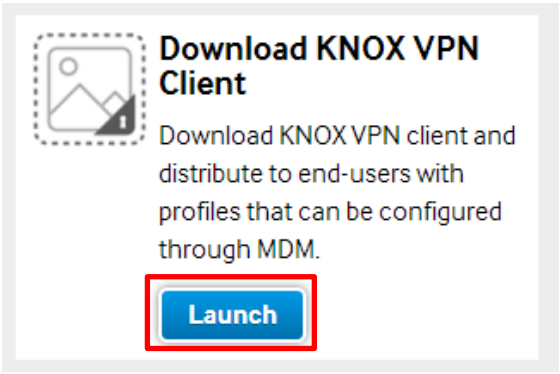
- IP address of the VPN server
- User login and password
- VPN type and settings
- Type of authentication
- PFS
- Dead peer detection (for IPSec)
- DH Group (for IPSec
- IKE Mode (IPSec)
- IKE identity (IPSec)

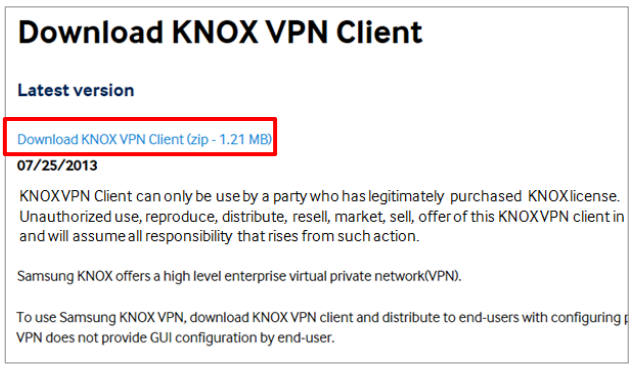
Before setting up VPN for your users, ensure you do the following:

- Connect all devices to Wi-Fi
- Download the KNOX VPN Client
- Ensure your VPN settings are correct

To download the KNOX VPN Client

1. Log in to the Samsung KNOX portal.
2. Select **Support** > **Tools** (located below the solution's resource section) > **KNOX VPN Client** > **Launch.**
3. Click **Download KNOX VPN Client**.





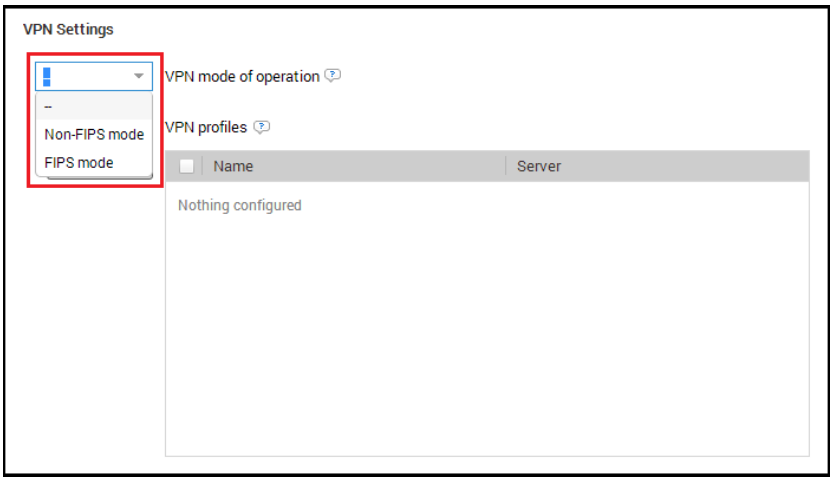
4. Log in to the KNOX EMM Admin client.
5. Click **Apps** > **Add App**.
6. In the **Applications Catalog**, enter **Andr** and search.
7. Select **Android InHouse** and click **Add App**.
8. Under **Application Name**, enter a name for your VPN.
9. Click **Application Settings** and upload the KNOX VPN client you downloaded in **Step 3** and click **Save**.

To set up VPN using KNOX EMM

To create a device-wide VPN policy using KNOX EMM

This policy will ensure that all data from the user's device will go through the VPN connection. Both personal and container data will go through a device-wide VPN connection.

1. Log in to KNOX EMM Admin Portal.
2. From the top menu bar, navigate to **Policy > Add Policy Sets**.
3. Enter a **Name** and **Description** for your VPN connection.
4. From the left pane, click **Policies** > **Mobile** > **Samsung KNOX Device Settings** > **VPN Settings**.
5. In the **VPN profiles** dialog, enter your VPN information.
    - Ensure you have selected VPN is for the whole device.
6. From the **VPN mode of operation** dropdown menu, select the appropriate mode.



Caution! If you don't make a selection, your VPN connection won't work.

7. Click **Add**, in the dialog, enter your settings and click **Save**.
   The VPN settings will be pushed onto your users' devices and they will receive a notification.
8. Under **Policy**, ensure you have selected **Push Policy** for your VPN settings.

To create a per-app VPN policy using KNOX EMM

This policy creates a VPN policy that applies to some apps on the user's device. These apps can be in or outside the container. You may choose to configure different VPN connections for each app.

1. Log in to KNOX EMM Admin Portal.
2. Navigate to **Policy** > **Add Policy Sets.**
3. Enter a **Name** and **Description** for your VPN connection.
4. From the left pane, click **Policies** > **Add Policy Set > Mobile** > **Samsung KNOX Workspace Settings** > **VPN Settings**.
5. Enter a **Name** and **Description** for your VPN connection.
6. From the left pane, click **Policies** > **Mobile** > **Samsung KNOX Workspace Settings** > **VPN Settings**.
7. Click **Add**.
8. In the **VPN profiles** dialog, enter your VPN information.
    - Ensure you select **VPN is only for selected applications**.
9. From the **VPN mode of operation** dropdown menu, select the appropriate mode.
10. From the left pane, navigate to **Samsung KNOX Workspace Settings** > **Device Settings** > **Enable start VPN automatically**.
11. Click **Add**, enter the package name for the app and the name of your VPN connection.
    - To find the package name for the app, on the device, navigate to **Settings** > **Application manager** > **All** and tap on the package name of the app you want to set up (for example, for S Browser, the package name is com.sec.android.app.sbrowser).
12. Click **Save**.
13. Select the packages you want to connect through VPN and click **Save**.


Note

Once you set up per-app VPN, the connection will run in the background even if the user does not open the app.

To create a per-container VPN policy using KNOX EMM

1. Log in to KNOX EMM Admin Portal.
2. Navigate to **Policy** > **Add Policy Sets**.
3. Enter a **Name** and **Description** for your VPN connection.
4. From the left pane, click **Policies** > **Mobile** > **Samsung KNOX Workspace Settings** > **VPN Settings**.

5. Enter a **Name** and **Description** for your VPN connection.
6. From the left pane, click **Policies** > **Mobile** > **Samsung KNOX Device Settings** > **VPN Settings**
7. In the **VPN profiles** dialog, enter the appropriate information.
    - Ensure you select **VPN is for whole device**.
8. From the **VPN mode of operation** dropdown menu, select the appropriate mode and click **Add**.
9. From the left pane, navigate to **Samsung KNOX Workspace Settings** > **Device Settings** > **Enable start VPN automatically**.

KNOX VPN policies

KNOX supports the following VPN policies. The policies you can set depend on your MDM. Not all MDM solutions support the same level of functionality. For a list of the KNOX policies supported by different MDM systems, see the KNOX MDM Feature List. Consult your MDM solution's documentation and contact their Support for additional details.

- Authentication method for the connection profile.
- Enable or disable the backup VPN Server.
- Set the IP Address of backup VPN Server.
- Enable or disable Dead Peer Detection option.
- Set the forward routes when split Tunnel Type is set to manual for per-container and device-wide VPN.
- Group name sets the IPsec Group ID Type Value for the connection profile.
- IPsec Group ID Type for the connection profile.
- IKE version for the connection profile.
- Per-app or per-container VPN
- Enable/disable user authentication.
- Enable or disable mobile option.
- Diffie-Hellman Group value for the connection profile.
- IKE Phase 1 key exchange mode for the VPN connection profile.
- Password used for login.
- PFS (perfect forward secrecy) value for the connection profile.
- Pre-shared key for the connection profile.
- Split Tunneling (either auto, manual or disabled) for per-container and device-wide VPN.
- Suite B Type (GCM-128, GCM-256, GMAC-128, GMAC-256 or none).
- Username used for login.
- Set up a VPN profile map that enables the system to start VPN automatically for an application.
- Enable or disable Default Route option.
- List all Enterprise VPN connections depending upon the type of VPN Type Connection.
- List of packages in the auto start list for a given profile.
- List of CA Certificates for the specified profile.
- VPN Connection details belonging to a particular profile.
- Forward route value for the given per-container and device-wide VPN Connection.
- User Certificate for the specified profile.
- Delete an enterprise VPN Profile.
- Remove an application from an auto start VPN list.
- Allows app to configure the CA certificate for a VPN profile.
- Create a new Enterprise VPN Connection or update an existing connection for KNOX 2.0.
- Allows app to configure the User certificate for a VPN profile.
- Set VPN mode of operation to either FIPS or non-FIPS mode.

To remove VPN policies

To remove a standalone VPN policy

1. Log in to KNOX EMM Admin Portal.
2. Click **Policy**, select policy with VPN you want to remove.
3. Click on the VPN you want to remove.
4. Click Applies to and select Set policy to inactive.
5. Click **Save**.

To remove a VPN that is a part of another policy

1. Log in to KNOX EMM Admin Portal
2. Click **Policy**, select the policy with the VPN you want to remove.
3. To remove device-wide VPN, navigate to **Policies** > **Mobile** > **Samsung KNOX Device Settings** > **VPN Settings**.
   - Or, to remove per-app or per-container VPN, navigate to **Policies** > **Mobile** > **Samsung KNOX Device Settings** > **VPN Settings**
4. Select the name of the VPN profile and click **Delete**.
5. Click **Save**.

If you install a trusted certificate with a VPN connection, users may see a warning message. This message is automatically included in Android 4.4.2. You can't disable the message, but you can edit the message by modifying this code from the Android Open Source Project. (AOSP). For more information, see Security Enhancements in Android 4.4.

To set up VPN using an MDM or MCM

Specific VPN configuration steps vary depending on the MDM or MCM you are using. Contact your MDM or MCM for more information.

To create a device-wide VPN policy using an MDM or MCM

This policy will ensure that all data from the user's device will go through the VPN connection. Data from personal mode and all containers will go through on VPN connection. The device-wide VPN policy will not apply to your KNOX container.

1. Download the KNOX VPN client from the Samsung KNOX website.
2. In your MDM or MCM client, upload the VPN client.
3. Enter a name for this VPN connection.
4. Select the VPN type. The available types depend on the device, but might include:
   - PPTP
   - L2TP/IPSec PSK
   - L2TP/IPSec RSA
   - IPSec Xauth PSK
   - IPSec Xauth RSA
   - IPSec Hybrid PSK
5. Enter the IP address of the VPN server.
6. Configure the VPN settings so that they match or are compatible with the VPN server settings.

To create a per-app VPN policy using an MDM or MCM

Per-App VPN capability is available for apps inside and outside of the KNOX container. However, the same VPN connection cannot be used by apps inside and outside the container.

- For apps inside the KNOX container, a VPN connection is initiated once an app is connected with that network.
- For apps outside the KNOX container, a VPN connection is initiated immediately after the VPN policy is enforced by mapping an app with the VPN profile.

For detailed MDM or MCM-specific VPN setup information, contact your MDM or MCM provider.

1. Download the VPN client from the Samsung KNOX website.
2. In your MDM or MCM, upload the package.

3. Enter the appropriate settings for your VPN connection.
4. Select the users that you'd like to deploy the VPN connection to.
5. Enter the package name for the app and the name of your VPN connection.
    - To find the package name for the app, on the device, navigate to **Settings** > **Application manager** > **All** and tap on the package name of the app you want to set up (for example, for S Browser, the package name is com.sec.android.app.sbrowser).
6. Save your VPN setup.


Note

Once you set up per-app VPN, the connection will run in the background even if the user does not open the app.

To create a per-container VPN policy using an MDM or MCM

The following steps illustrate the workflow for setting up a per-container VPN policy. For detailed MDM or MCM-specific VPN setup information, contact your MDM or MCM provider.

1. Download the VPN client from the Samsung KNOX website.
2. In your MDM or MCM, upload the package.
3. Enter the appropriate settings for your VPN connection
4. Select the users that you'd like to deploy the VPN connection to.
5. Indicate that the container that the VPN applies to.
6. Deploy the VPN policy.

To set up VPN using Active Directory

To set up the device

Use the VPN client that is preloaded onto the device or use the KNOX VPN client.

1. Select **Settings** > **Network Connections > More networks > VPN** and tap **+**
   This path is for the Samsung Galaxy S5. The exact path depends on the device, but most KNOX devices have a similar path.

2. Enter a name for this VPN connection.

3. Select the VPN type. The available types depend on the device, but might include:
   - PPTP
   - L2TP/IPSec PSK
   - L2TP/IPSec RSA
   - IPSec Xauth PSK
   - IPSec Xauth RSA
   - IPSec Hybrid PSK
4. Enter the IP address of the VPN server.

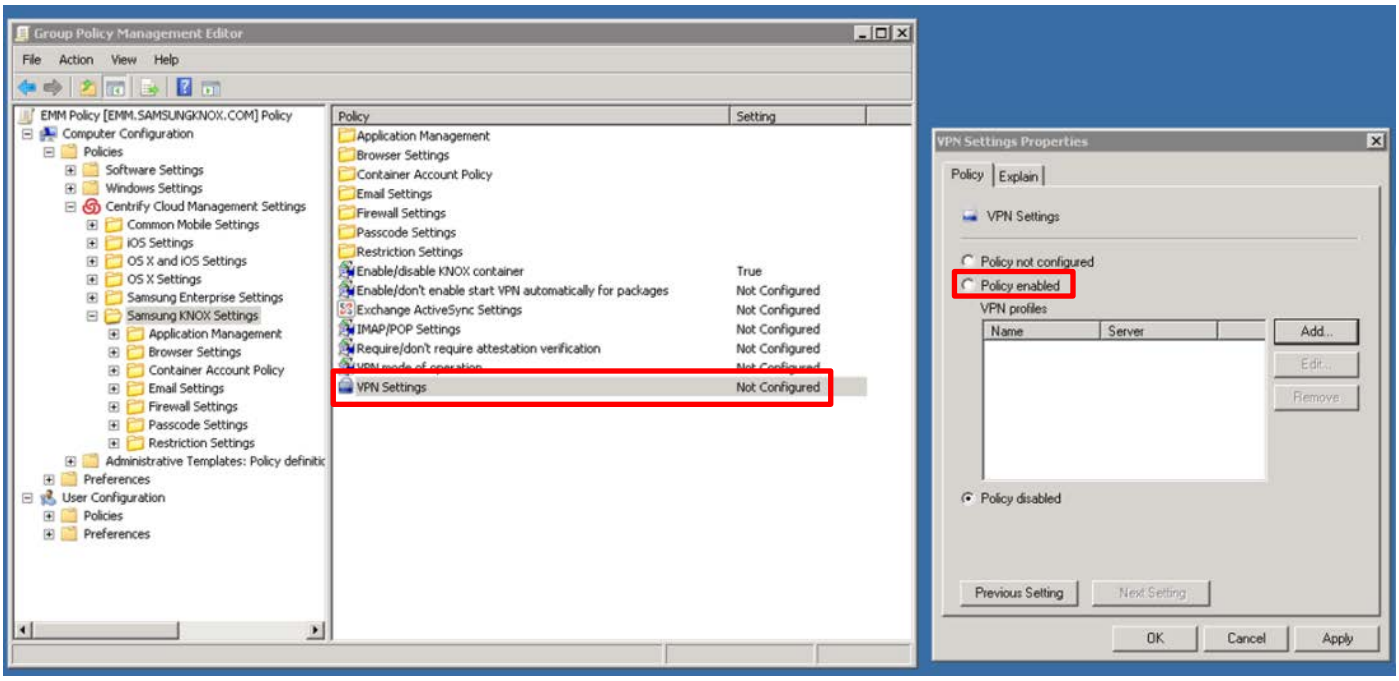
5. Configure the VPN settings so that they match or are compatible with the VPN server settings.

NOTE – You can also download VPN apps from the Google Play store for additional features.

To set up the MDM system

If you are using KNOX, disable the KNOX VPN so that the KNOX container apps use the native Android VPN client. How you do this depends on your MDM system. The following example shows how to do this through the KNOX EMM Active Directory:

1. In the Group Policy Management Editor, navigate to **Samsung KNOX Settings**.
2. Open the VPN Settings Properties by clicking Enable/don't enable start VPN automatically for packages.
3. Select **Policy disabled**, then select **Apply** and **OK**.



NOTE – You can use the KNOX Standard Settings (SAFE) to configure a VPN profile and policies for this native Android VPN client.

To set up per-container VPN

Follow these steps to set up a single VPN for all apps in the KNOX container:

1. Download the KNOX VPN client from the KNOX web portal.
2. Deploy the KNOX VPN client to enterprise devices.
3. Configure the VPN profile.
4. Configure the VPN policies.

To deploy the KNOX VPN client on devices

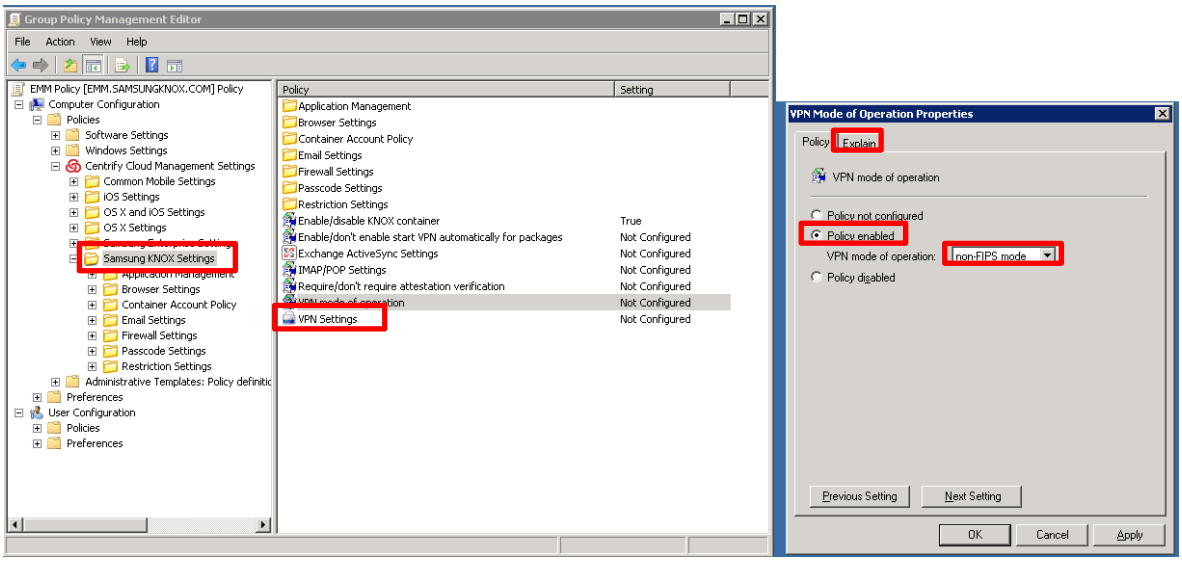
How you do this depends on your MDM system, which might use Active Directory on an on-premise server, a proprietary app on a network server, or a cloud-based manager.

To configure the VPN profile

The following steps illustrate an Active Directory-based system.

1. Select the VPN mode of operation:
    a. Go to **Samsung KNOX Settings** > **VPN mode of operation**.
    b. Select **Policy enabled**.

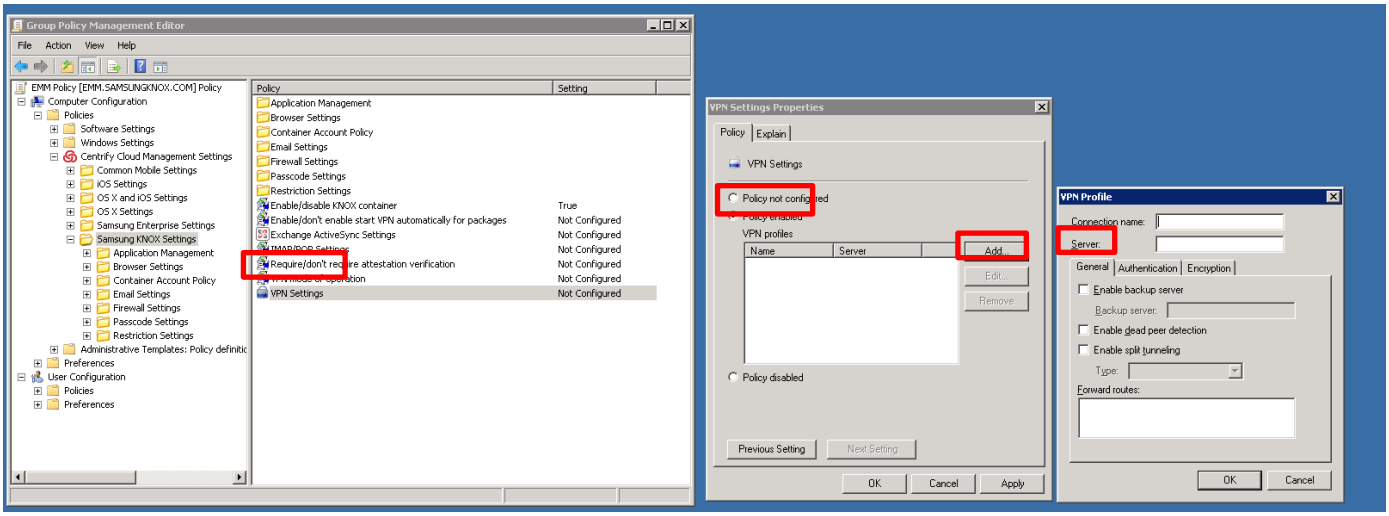
c. Select the **VPN mode of operation**.
More information about the modes is available under the **Explain** tab.



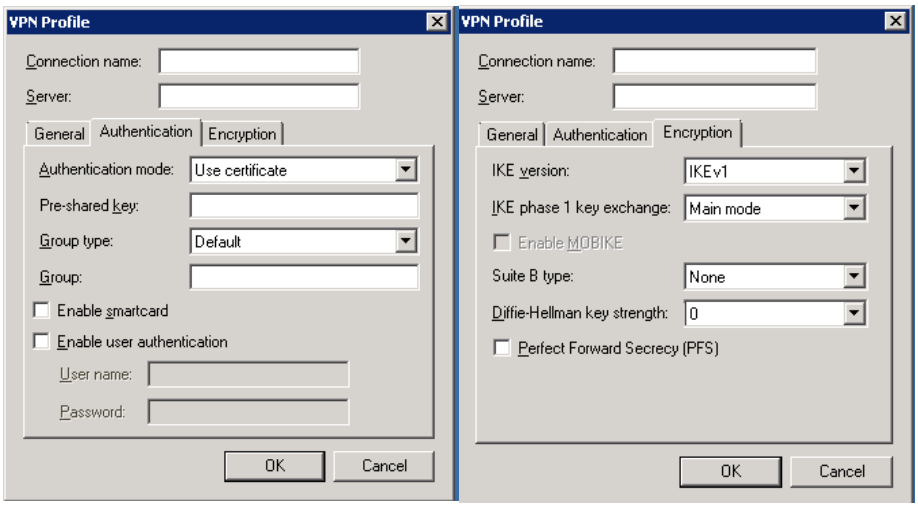
2. Create a VPN profile:
   a. Go to **Samsung KNOX Settings** > **VPN settings**.

   b. Select **Policy enabled**.

   c. Click **Add** to create a new VPN profile. For Server, enter the VPN server's IP address.



3. Use the **General**, **Authentication** and **Encryption** tabs to configure your VPN, for example, a pre-shared key, or an IKE version.



4. Define the profile. Profile initialization parameters include the profile name of the VPN connection and IP address of the VPN server.

Name	Definition	Example
profileName	profile Name of the VPN Connection	adminVPN
Host	IP address of the VPN server	12.3.456.79
isUserAuthEnabled	parameter need to specify if user authentication is required to establish VPN connection.	True/false
VPN_type	specifies whether the particular VPN connection is an ipsec or ssl connection.	ipsec
VPN_route_type	Specifies whether the VPN is a system or a per-app VPN	0: system VPN 1: per-app VPN (splitTunnelType should be set to 0 or disabled)

5. Set the SSL and IPSec Parameters.

6. The VPN profile is pushed to the device during enrollment or on-demand, and takes effect immediately.

To configure VPN policies

You can configure KNOX to meet your enterprise's VPN policy requirements. The policies available depend on your MDM. Not all MDM solutions support the same level of functionality. For a list of the

KNOX policies supported by different MDM systems, see the KNOX MDM Feature List. Consult your MDM solution's documentation and contact their Support for additional details.

The steps for configuring VPN policies depend on your MDM system. To configure VPN policies with the KNOX EMM Active Directory:

1. Go to **Configuring KNOX** > **Workspace Policies** > **VPN Profile Policies**.
2. Be sure to set the following policies:
    - The IP address or host name of the VPN server.
    - The connection name (profile name), which is used to identify the connection.
    - The VPN type. This can be VPN_TYPE_ANYCONNECT.
      This provides the policies required to set up an Enterprise Premium VPN profile and install certificates to the Enterprise VPN credential storage.

To configure the Enterprise Premium VPN policies:

- Go **to Configuring KNOX** > **Workspace Policies** > **Premium VPN Policies**.

To set up per-app VPN

Per-app VPN capability is available for apps inside and outside of the KNOX container. However, the same VPN connection cannot be used by apps inside and outside the container.

- For apps inside the KNOX container, a VPN connection is initiated once an app is connected with that network.
- For apps outside the KNOX container, a VPN connection is initiated immediately after the VPN policy is enforced by mapping an app with the VPN profile.

  Follow these basic steps to set up a single VPN for all apps in the KNOX container:

1. Download the KNOX VPN client from the KNOX web portal.
2. Deploy the KNOX VPN client to enterprise devices.
3. Configure the VPN profiles.

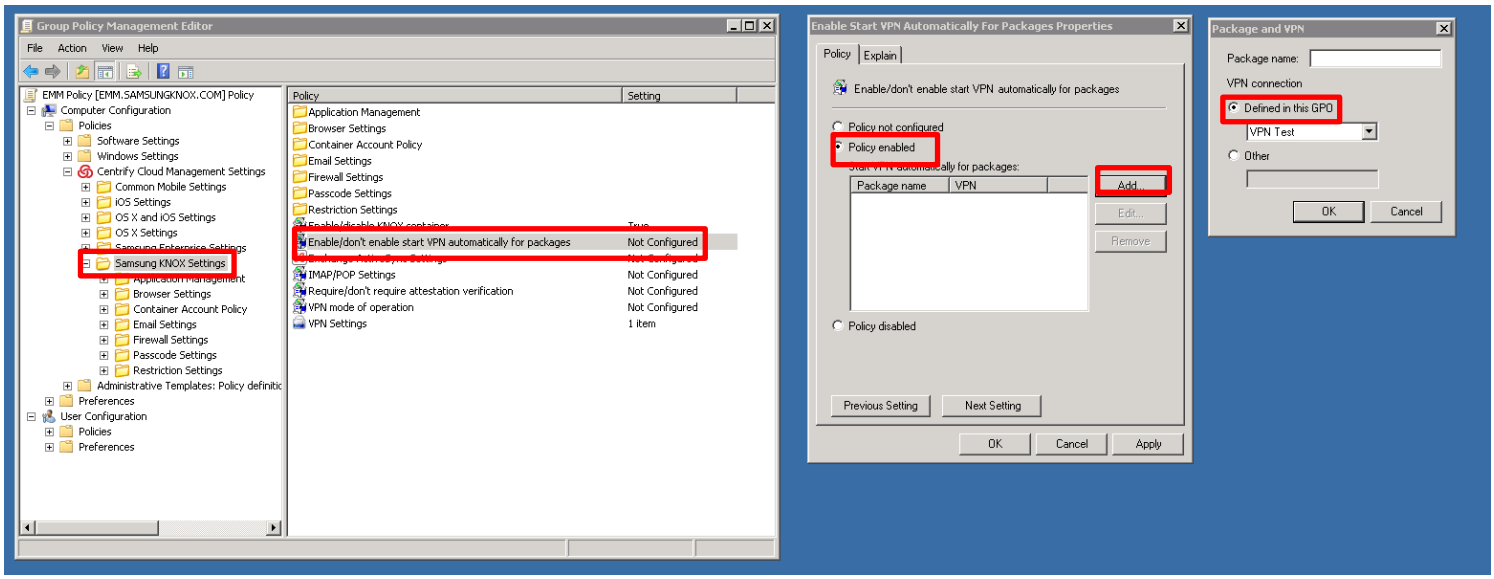
Steps 1, 2, and 4 are the same as those described in the last chapter for per-container VPN. Only step 3 is different, in that you can define multiple VPN profiles, for up to five separate VPNs, and assign apps to VPN profiles.

To configure the VPN profiles

To configure per-app VPN using KNOX EMM Active Directory:

1. Go to **Samsung KNOX Settings** > **Enable/Don't enable start VPN automatically for packages**.
2. Select **Policy Enabled**; select **Add**.
3. For **Package name**, enter the APK file name of an app that will use the VPN profile.

4. For VPN connection, select **Defined in this GPO** and select a VPN profile defined in the group policy.



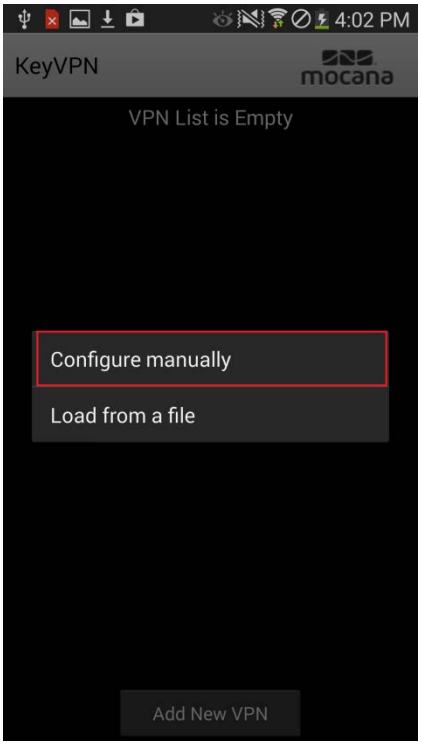
To manually configure a VPN connection

If your VPN connection doesn't work after you troubleshoot potential issues, manually configure a VPN connection to ensure that your settings are correct.

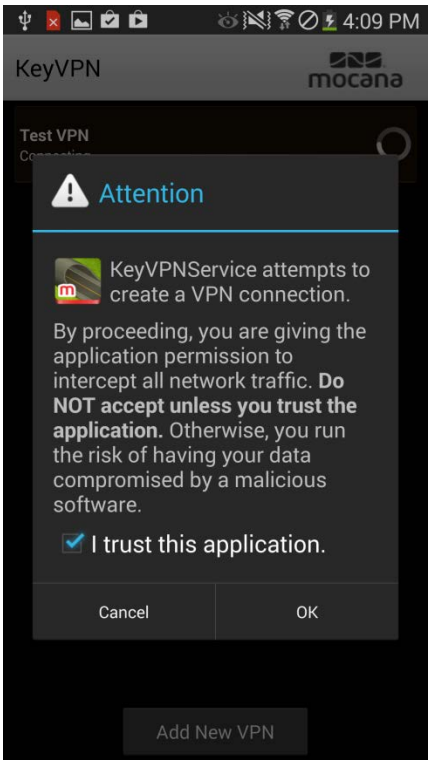
To configure the VPN Client

1. Sideload the unzipped VPN file onto your device.
2. Go to **My Files** > **Recent Files** and tap the VPN .apk file.

   If you get a security warning, go to **Settings** > **Security** > **Unknown sources** to allow the device to install apps from sources other than Google Play.
3. Tap **Add New VPN**, and select **Configure Manually**.



4. Enter a name for your VPN and enter your **Basic** and **Advanced** VPN settings.
5. Click **Save Settings**.
6. Tap to connect, select **I trust this application** and then click **OK**.



When the VPN connection is green, your device is connected.

To troubleshoot issues

The following are ways to troubleshoot general VPN issues. For more information, documents, FAQs or to submit a ticket please visit Samsung KNOX Support.

No VPN connection

An app that uses VPN is not able to access Internet, e.g., container-based browser cannot display web pages.

1. Check the underlying network connection:
    - Wi-Fi is **On**, with good Wi-Fi signal strength.
    - Cellular access is up, Mobile data is **On**.
2. Perform a device reboot. If symptoms persist:
3. Check if the VPN connection has ever worked. If it never has:
    - Using another device, test the app and VPN connection.
    - At the MDM console, check the VPN profile, policy settings.
    - Ensure that the VPN gateway is operational.

VPN access point times out

The VPN goes through an access point (like a wireless router at home) which has not been configured to enable VPN.

1. Check the access point firewall settings.
    - VPN requires UDP ports 500 and 4500 to communicate.
    - Enable VPN passthrough.
2. If symptoms persist, escalate the issue.

VPN connection not stable

An app that uses VPN to access to the Internet works sporadically. Due to user roaming, the device may be switching between Wi-Fi and cellular networks.

1. Check the underlying network connection:
    - Wi-Fi is on, with good Wi-Fi signal strength.
    - Cellular access is up, with good signal strength.
    - Device is not roaming when testing connection.
2. Check if the VPN server went down momentarily.
3. If symptoms persist, contact Samsung KNOX Support.

VPN host not found

VPN Observed Timeout/Host not found.

1. Ensure that you have good signal strength if you using a data connection.
2. Ensure that there is no firewall policy preventing access.
3. Verify there are no Wi-Fi Access Point restrictions imposed.
4. If symptoms persist, escalate the issue

VPN server down

1. Check to see if maintenance is scheduled for the VPN server.
2. Contact your network Admin.
3. Escalate the issue.

VPN policy not pushed onto user's devices

Changes made to your VPN policy on EMM aren't appearing on users' devices.

1. Check the underlying network connection:
    - Wi-Fi is on, with good Wi-Fi signal strength.
    - Cellular access is up, with good signal strength.
    - Device is not roaming when testing connection.
2. Check to see if you have selected a VPN mode of operation.
    - If you don't select either **Non-FIPS mode** or **FIPs mode**, your VPN will not work.
3. Tell users to wait, there is a slight delay between EMM policy changes and changes on users' devices.
4. Change the policy push delay setting to reduce the delay between EMM policy changes and changes on users' devices.
    - **Settings** > **Device Policy Management** > **Samsung Policy Service**

Decreasing the policy push delay may impact device battery life.

To get support

Where to get more information

The KNOX web portal provides a lot of additional information about KNOX. Check out these tabs:

- **Overview** — For a video introduction. If you want more detail about the security features, select from the drop-down menu bar along the top: **Overview** > **Technical Details**.
- **Resources** — For white papers, technical notes, glossary, guides, training materials, an interactive Flash simulator, and Frequently Asked Questions (FAQs).

Who to contact

If you encounter an issue that is not covered in To troubleshoot issues, contact your reseller or MDM partner or escalate to your Regional Samsung KNOX Support. Contact information can be found on the Samsung KNOX support portal.

What to Provide

To resolve your issue as fast as possible, be prepared to collect the following information:

VPN details:

- **VPN gateway** — Cisco, Juniper, Microsoft, strongSwan, and so on.
- **VPN gateway configuration** — VPN type (IKE v1/v2), authentication method, etc
- Logcat message from the device. To retrieve this information see the Samsung KNOX FAQs.

Device details:

From About Device:

- Model number
- Android version
- Build number
- Kernel version

From Device Status:

- Mobile network state
- Signal strength

From Wi-Fi Status:

- Status
- Signal strength

Get Dumpstate:

1. Open the phone app.
2. Enter ***#9900#**.
3. Tap **Run dumpstate/logcat/modem log**.
4. Tap **Copy to sdcard**.