Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0.x

Revised: November 8, 2017,

AnyConnect User Guide

Install and Start AnyConnect

AnyConnect Overview

The Cisco AnyConnect Secure Mobility Client for Android provides seamless and secure remote access to enterprise networks. AnyConnect allows installed applications to communicate as though connected directly to the enterprise network. AnyConnect is a sophisticated networking application that also allows you to set preferences, control the operation of AnyConnect, and use diagnostic tools and facilities on your device as recommended by your administrator.

AnyConnect may be used in your enterprise in conjunction with Mobile Device Management software. If so, work with your administrator to abide by device management rulessince these rules may include restricting VPN access to a set of approved applications. Your organization may provide additional documentation on using AnyConnect for Android.

Your Android app store provides the application for initial installation and all upgrades. The Cisco Adaptive Security Appliance (ASA) is the secure gateway that admits access to the VPN, but it does not support updates of AnyConnect for mobile devices.

Open Software License Notices

- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
- This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Android Supported Devices

Full support for Cisco AnyConnect on Android is provided on devices running Android 4.0 (Ice Cream Sandwich) through the latest release of Android.

Cisco AnyConnect on Kindle is available from Amazon for the Kindle Fire HD devices, and the New Kindle Fire. AnyConnect for Kindle is equivalent in functionality to the AnyConnect for Android package.

Per App VPN is supported in managed and unmanaged environments. In a managed environment using Samsung KNOX MDM, Samsung devices running Android 4.3 or later with Samsung Knox 2.0, are required. When using Per App in an unmanaged environment, the generic Android methods are used.

For the Network Visibility Module (NVM) capabilities, Samsung devices that are running Samsung Knox 2.8 or later, which requires Android 7.0 or later, are required. For configuration of NVM, the AnyConnect Profile Editor from AnyConnect 4.4.3 or later is also required. Earlier releases do not support mobile NVM configurations.

See Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0 for installation and upgrade procedures.

Install the Android AnyConnect Application

AnyConnect for Android is available for download only from the Android Market for your Android device, or from Amazon for Kindle devices. You cannot download it from the Cisco website or after connecting to a secure gateway.

To install AnyConnect for Android, follow the normal procedures for downloading, installing or upgrading apps on your device.

Start AnyConnect

Procedure

Step 1 Tap the AnyConnect Icon to start the AnyConnect app.

Step 2 If this is the first time that you are starting AnyConnect after installing or upgrading you will see the following:

- An End User License Agreement (EULA), you must **Accept** this to continue.
- An Acceptable Use Policy (AUP) for data collection if this has been configured by your network administrator. Click **OK** to continue. Data collection is done by the Network Visibility Module (NVM) that is part of the AnyConnect client application.

Step 3 Tap **Connection** > **Add New VPN Connection** to configure a connection entry. See Adding Connection Entries Manually, on page 5 for details.

Step 4 (Optional) Tap **Details** to view summary and detailed statistics about the current active VPN connection. See View AnyConnect Statistics.

Step 5 (Optional) Tap **Menu** and choose:

- **Settings**, to specify AnyConnect application preferences. See Specifying Application Settings.
- **Diagnostics**, to carry out the following diagnostic activities:
  - Managing certificates; see About Certificates on Your AndroidDevice.
  - Managing AnyConnect profiles; see About AnyConnect Client Profiles.
  - Managing AnyConnect localization; see Managing Localization.
  - Viewing logging and system information; see Viewing Log Messages.
- **About**, to view AnyConnect version and license information. See Display the AnyConnect Version and Licenses.
- **Exit**, to exit AnyConnect. See Exiting AnyConnect.

What to Do Next

Follow instructions provided to you by your administrator to configure and establish a VPN connection to your network.

Android Device Permissions

The following permissions are declared in the Android manifest file for AnyConnect operation:

Manifest Permission	Description
uses-permission: android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks.

Manifest Permission	Description
uses-permission: android.permission.ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks.
uses-permission: android.permission.BROADCAST_STICKY	Allows an application to broadcast sticky intents. These are broadcasts whose data is held by the system after being finished, so that clients can quickly retrieve that data without having to wait for the next broadcast.
uses-permission: android.permission.INTERNET	Allows applications to open network sockets.
uses-permission: android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage.
uses-permission: android.permission.READ_LOGS	Allows an application to read the low-level system log files.
uses-permission: android.permission.READ_PHONE_STATE	Allows read only access to phone state, including the phone number of the device, current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device.
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the broadcast after the system finishes booting.

Configure a VPN Connection

AnyConnect requires the following to establish VPN connectivity:

- An address to a secure gateway for access to your network.

  This address is configured in a connection entry. Connection entries are listed on the AnyConnect home screen. The active connection entry is identified on the AnyConnect home screen or in the Connections list. VPN connection entries are configured on your device manually, or automatically configured by your enterprise administrator.

- Authentication information to successfully complete your connection.

  This will be in the form of a username and password you must remember, or it will be contained in a digital certificate that has been configured on your device. For some VPN connections, both authentication methods may be required. Digital certificates are configured on your device manually, or automatically configured by your device administrator.

Configure your AnyConnect client as directed by your administrator. Contact your administrator if you do not have clear instructions.

Configure Connection Entries

A connection entry specifies a secure gateway that provides access to your private network, as well as other connection attributes.

Select **Connections** from the AnyConnect home screen to view the entries already configured on your device. Multiple connection entries may be listed. Connection entries may have the following status:

- Active—This marked or highlighted connection entry is currently active.

- Connected—This connection entry is the active one and is currently connected and operating.
- Disconnected—This connection entry is the active one but is currently disconnected and not operating.

Procedure

Connection entries are configured on your device manually or automatically in the following ways:

- Manually configured.

  You must know the address of the secure gateway to your network. The address is the domain name or the IP address of the secure gateway, and it may also specify a group that you belong to. Other connection attributes can also configured. See Adding Connection Entries Manually, on page 5.

- Automatically configured by clicking on a link provided by your administrator.

  An AnyConnect URI link may be included in an email or published on a web page. The application preference **External Control** must be set to either **Prompt** or **Enable** to allow this on your device. See Control the External Use of AnyConnect, on page 13

- Automatically configured after connecting to a secure gateway that downloads an AnyConnect client profile containing connection entries. See Managing the AnyConnect Client Profile, on page 16.

- Configured by your enterprises' Mobile Device Management software. Device management profiles may be found on your device under the General Settings.

Adding Connection Entries Manually

Add a VPN connection entry to identify the VPN secure gateway to which you want to connect.

Procedure

Step 1 From the AnyConnect home window, tap **Connection > Add New VPN Connection** to open the connection editor. **Cancel** out of the connection editor at any time.

Step 2 (Optional) Choose **Description** to enter a descriptive name for the connection entry.
Enter a unique name for this connection entry. If not specified, the **Server Address** is used as the default. Use any letters, spaces, numbers, or symbols on the keyboard display. This field is case-sensitive.

Step 3 Choose **Server Address** to enter the address of the secure gateway.
Enter the domain name or IP address of the secure gateway, including a group if specified by your administrator.

Step 4 (Optional) Tap **Advanced Preferences** to change advanced certificate and protocol settings. **Cancel** out of the Advanced Connection Editor window at any time.

Step 5 (Optional) Tap **Certificate** to specify how user certificates are used for this connection.

- Tap **Disabled** to specify that certificates will not be used for this connection.
- Tap **Automatic** to specify that a certificate will be used to establish a connection only if it is required by the secure gateway.
- Tap the certificate that your administrator instructs you to use.

Your administrator will provide you with instructions for installing a user certificate on your mobile device if one is necessary to establish a VPN session. Tap any certificate in the list to view its details.

Step 6 (Optional) Tap **Connect with IPsec** to use IPsec instead of SSL for this VPN connection.
This connection attribute is provided to you by your administrator.

The **Authentication** parameter becomes active if you choose IPsec for your VPN connection protocol.

Step 7 (Optional) Tap **Authentication** and choose the authentication method for this IPsec connection.
This connection attribute is provided to you by your administrator.

- EAP-AnyConnect (default authentication option)
- IKE-RSA
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2

Your authentication option is shown in the **Advanced Connection Editor** window.

Step 8 (Optional) If you have specified EAP-GTC, EAP-MD5, or EAP-MSCHAPv2 to be used for authentication, tap **IKE Identity** to enter the identity information given to you by your administrator.

Step 9 Tap **Done** in both the **Advanced** window and the **Connection Editor** window to save the connection values.
AnyConnect adds the new connection entry.

Modifying a Connection Entry

Change a VPN connection entry to correct a configuration error or comply with an IT policy change.

Note You cannot modify the description or server address of connection entries downloaded from a secure gateway.

Procedure

Step 1 From the AnyConnect home window, tap **Connection**. Then, long-press the connection entry to display the **Select Action** window.

Step 2 Tap **Edit connection**.
The **Connection Editor** window displays the parameter values assigned to the connection entry.

Step 3 Tap the value to be modified, use the on-screen keyboard to enter the new value, and tap **OK**.

Step 4 Tap **Done**.
AnyConnect saves the modified connection entry.

Delete a Connection Entry

This procedure deletes a manually configured VPN connection entry. The only way to remove a connection entry imported from a VPN secure gateway is to remove the downloaded AnyConnect profile that contains the connection entries.

Procedure

Step 1 From the AnyConnect home window, tap **Connection**. Then, long-press the connection entry to display the **Select Action** window.

Step 2 Tap **Delete connection**.

Configure Certificates

About Certificates on Your AndroidDevice

Certificates are used to digitally identify each end of the VPN connection: the secure gateway, or the server, and the AnyConnect client, or the user. A server certificate identifies the secure gateway to AnyConnect, and a user certificate identifies the AnyConnect user to the secure gateway. Certificates are obtained from and verified by Certificate Authorities (CAs).

When establishing a connection, AnyConnect always expects a server certificate from the secure gateway. The secure gateway expects a certificate from AnyConnect only if it has been configured to do so. Expecting the AnyConnect user to manually enter credentials is another way to authenticate a VPN connection. In fact, the secure gateway can be configured to authenticate AnyConnect users with a digital certificate, with manually entered credentials, or with both. Certificate-only authentication allows VPNs to connect without user intervention.

Distribution to and use of certificates by, the secure gateway and your device, are directed by your administrator. Follow directions provided by your administrator to import, use, and manage server and user certificates for AnyConnect VPNs. Information and procedures in this document related to certificates and certificate management are provided for your understanding and reference.

AnyConnect stores both user and server certificates for authentication in its own certificate store on the Android device. The AnyConnect certificate store is managed from the **Menu** > **Diagnostics** > **Certificate Management** screen; you can also view Android System certificates here.

About User Certificates
In order for you, the AnyConnect user, to authenticate to the secure gateway using a digital certificate, you need a user certificate in the AnyConnect certificate store on your device. User certificates are imported using one of the following methods, as directed by your administrator:

- Imported automatically after clicking a hyperlink provided by your administrator in an email or on a web page.
- Imported manually by you from the device's file system, from the device's credential storage, or from a network server.
- Imported when connecting to a secure gateway that has been configured by your administrator to provide you with a certificate.

Once imported, the certificate can be associated with a particular connection entry or selected automatically during connection establishment to authenticate.

You can delete user certificates from the AnyConnect store if they are no longer needed for authentication.

About Server Certificates

A server certificate received from the secure gateway during connection establishment automatically authenticates that server to AnyConnect, if and only if it is valid and trusted. Otherwise:

- A valid, but untrusted server certificate can be reviewed, authorized, and imported to the AnyConnect certificate store. Once a server certificate is imported into the AnyConnect store, subsequent connections made to the server using this digital certificate are automatically accepted.
- An invalid certificate cannot be imported into the AnyConnect store. It can be accepted to complete the current connection, but this is not recommended.

Server certificates in the AnyConnect store can be deleted if they are no longer needed for authentication.

Importing Certificates from Hyperlinks

Your administrator will provide you with a hyperlink to install a certificate on your device.

Before You Begin

Set **External Control** to either **Prompt** or **Enable** within the AnyConnect settings.

Procedure

Step 1 Tap the hyperlink provided by your administrator.

The link may be included in an email or published on an intranet web page.

Step 2 If prompted, provide the authentication code for the certificate that was provided to you.

The certificate is installed in the AnyConnect certificate store on your Android devce and can be viewed, assigned to a connection entry, or removed.

Importing Certificates Manually

The following explains all possible options for manually importing a user certificate to the AnyConnect store for VPN authentication purposes.

Before You Begin

Obtain the specific certificate import procedures from your administrator.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Certificate Management**.

Step 2 Tap the **User** tab.

Step 3 Tap **Import** to import a certificate.

Step 4 Select your import source:

- Tap **File System** to import a certificate file from the local file system.
- Tap **Network Location (URI)** to import a certificate from a server on the network.

- Tap **Device Credential Storage** to link to a certificate currently in the Device Credential Storage.

  The source certificate is not actually copied into the AnyConnect certificate store. If the certificate is removed from Credential Storage, the link to the certificate will also be removed.

  Note
  - This option is available only on devices running Android 4.0 (Ice Cream Sandwich) or later.
  - When attempting to import a certificate from the Device Credential Storage on Android 4.1 (Jelly Bean), the client shows the error message "This feature is not supported on this version of Android." Import the certificate directly into the AnyConnect store instead of using the Android native store.

Importing Certificates Provided by a Secure Gateway

Before You Begin

Your administrator configures a secure gateway to enable the distribution of certificates and provides you with connection information to that secure gateway.

Procedure

Step 1 Open AnyConnect.

Step 2 In the **Choose a connection** area, tap the name of the connection capable of downloading a certificate to your mobile device.

Step 3 If present, tap **Get Certificate**, or select the group configured to download a certificate to your mobile device.

Step 4 Enter authentication information provided by your administrator.

The secure gateway downloads the certificate to your device. Your VPN session is disconnected, and you receive the message that certificate enrollment was successful.

Viewing Certificates

View user and server certificates that have been imported into the AnyConnect certificate store, and Android system certificates.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Certificate Management**.

Step 2 Tap the **User** or **Server** tab to view certificates in the AnyConnect certificate store.

Long-press a certificate and tap:

- **View certificate details** to see the contents of a certificate.
- **Delete certificate** to remove this certificate from the AnyConnect store.

Step 3 Tap the **System** tab to view certificates in the Android Credential Storage.

Long-press a certificate and tap **View certificate details** to see the contents of a certificate.

Removing Certificates

Remove certificates from the AnyConnect certificate store only; certificates in the System certificate store cannot be removed.

Certificates are deleted individually or cleared from the AnyConnect certificate store all at once.

Deleting a Single Certificate

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Certificate Management**.

Step 2 Tap the **User** or **Server** tab to display user or server certificates in the AnyConnect certificate store.

Step 3 Long-press a certificate.

The **Certificate Options** display.

Step 4 Choose **Delete certificate** and confirm that you want to delete this particular certificate.

Clearing All Certificates

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Certificate Management**.

Step 2 Tap the **User** or **Server** tab to display user or server certificates in the AnyConnect certificate store.

Step 3 Tap **Clear All** to remove all certificates from the AnyConnect certificate store.

Establish a VPN Connection

You connect to a VPN by tapping the checkbox or slider associated with the active connection shown in the **AnyConnect VPN** panel, or selecting one of the other connection entries listed in the AnyConnect home screen.

Before You Begin

- You must have an active Wi-Fi connection, or a connection to your service provider to connect to a VPN.
- To initiate a VPN connection, you must have at least one connection entry listed under **Choose a Connection** on your AnyConnect home window.
- To complete a VPN connection, you must have the authentication information expected by your secure gateway.

Procedure

Step 1 Go to the AnyConnect home window.

Step 2 Tap **Connection** then the connection entry to be used.

AnyConnect disconnects any VPN connection currently in use and makes this connection entry the current connection as it initiates the VPN connection.

Step 3 If necessary, do one of the following in response to authentication prompts:

- Enter your username and password credentials. If your administrator has configured double authentication, you may also be prompted for secondary credentials.
- Tap **Get Certificate** and enter the certificate enrollment credentials supplied by your administrator. AnyConnect saves the certificate and reconnects to the VPN secure gateway to use the certificate for authentication.

Depending on the VPN secure gateway configuration, AnyConnect may add connection entries to the list in the AnyConnect home window. The top row of the AnyConnect home window highlights the checkmark, indicating that the VPN connection is established.

Note Tapping another VPN connection in the AnyConnect home window disconnects the current VPN connection and connects to the VPN secure gateway associated with the one that you tapped.

Respond to AnyConnect Notifications

Respond to Untrusted VPN Server Notifications

The type of **Untrusted VPN Server** notification displayed depends on the **Block Untrusted VPN Server** application preference:

- If enabled, a blocking **Untrusted VPN Server!** notification displays, choose:
  - **Keep Me Safe** to keep this setting and this blocking behavior.
  - **Change Settings** to turn off blocking.

    After changing the **Block Untrusted VPN Server**, re-initiate the VPN connection.
- If not enabled, a nonblocking **Untrusted VPN Server!** notification displays, choose:
  - **Cancel** to abort the VPN connection to the untrusted server.
  - **Continue** to make the connection to the untrusted server; this option is not recommended.
  - **View Details** to view certificate details and decide whether to import the server certificate into the AnyConnect certificate store for future acceptance and continue the connection.

Respond to Another App

To protect your device, AnyConnect alerts you when an external app attempts to use AnyConnect. This occurs when the AnyConnect application preference **External Control** is set to **Prompt**.

Ask your administrator whether to tap **Yes** in response to the following prompts:

- `Another application has requested that AnyConnect create a new connection to host. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect connect to host. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect disconnect the current connection. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import localization files. Do you want to allow this? [Yes | No]`
- `Another application has requested that AnyConnect import profiles. Do you want to allow this? [Yes | No]`

Respond to MMS Notifications

While an AnyConnect VPN is connected, you are unable to retrieve or send Multimedia (MMS) messages. If attempted and blocked, an MMS notification icon is displayed in the status bar. To acknowledge this notification:

Procedure

Step 1 Tap the notification icon to view the notification.

Step 2 Tap the notification to view the service impact.

Step 3 Check the **Do not show this again** check box if you no longer want to receive MMS notifications.

Attention This is a permanent selection. You will not be able to reverse this action in the future.

Step 4 Tap **OK**.

Optional AnyConnect Configuration and Management

Specifying Application Settings

Launch AnyConnect at Startup

You have control over when AnyConnect launches on your device. By default, AnyConnect does not automatically launch at device startup. If checked, Launch at Startup is enabled.

Note Launch at Startup is automatically enabled if a profile specifying Trusted Network Detection is download or imported.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings**.

Step 2 Tap the **Launch at Startup** checkbox to enable or disable this preference.

Hide the AnyConnect Status Bar Icon

The AnyConnect icon in the notification bar can be hidden when AnyConnect is not active.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings**.

Step 2 Tap the **Hide Icon** checkbox.

If left unchecked, the icon displays persistently.

Control the External Use of AnyConnect

The External Control application setting specifies how the AnyConnect application responds to external URI requests. External requests create connection entries; connect or disconnect a VPN; and import client profiles, certificates, or localization files.

External requests are typically provided by your administrator in emails or on web pages. Your administrator will instruct you to use one of the following values:

- Enabled—The AnyConnect application automatically allows all URI commands.
- Disabled—The AnyConnect application automatically disallows all URI commands.
- Prompt—The AnyConnect application prompts you each time an AnyConnect URI is accessed on the device. You allow or disallow the URI request. See Respond to Another App, on page 12 for details.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings**.

Step 2 Tap **External Control**.

Step 3 Tap **Enabled**, **Disabled**, or **Prompt**.

Block Untrusted Servers

This application setting determines if AnyConnect blocks connections when it cannot identify the secure gateway. This protection is ON by default; it can be turned OFF, but this is not recommended.

AnyConnect uses the certificate received from the server to verify its identify. If there is a certificate error due to an expired or invalid date, wrong key usage, or a name mismatch, the connection is blocked.

When this setting is ON, a blocking **Untrusted VPN Server!** notification alerts you to this security threat.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings**.

Step 2 Tap the **Block Untrusted Servers** checkbox to enable or disable this preference.

Set FIPS Mode

FIPS Mode makes use of Federal Information Processing Standards (FIPS) cryptography algorithms for all VPN connections.

Before You Begin

Your administrator will inform you if you need to enable FIPS mode on your mobile device for connectivity to your network.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings**.

Step 2 Tap **FIPS Mode** to enable or disable this preference.

Upon confirmation of your FIPS mode change, AnyConnect exits and must be restarted manually. Upon restart, your FIPS mode setting is in effect.

Set OCSP Revocation

The Android AnyConnect client supports OCSP (Online Certificate Status Protocol). This allows the client to query the status of individual certificates in real time by making a request to the OCSP responder and parsing the OCSP response to get the certificate status. OCSP is used to verify the entire certificate chain. There is a five second timeout interval per certificate to access the OCSP responder.

Before You Begin

Your administrator will inform you if you need to enable OCSP Revocation on your mobile device for connectivity to your network.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings**.

Step 2 Tap **OCSP Revocation** to enable or disable this preference.

Upon the next connectivity attempt, OCSP will be used, or not, to determine the revocation status of the certificate received from the head-end.

Strict Certificate Trust

If selected, when authenticating remote security gateways, AnyConnect disallows any certificate that it cannot verify automatically without user intervention. Instead of prompting the user to accept these certificates, the client fails to connect. This setting overrides Block Untrusted Server.

If not selected, the client prompts the user to accept the certificate or not. This is the default behavior.

Before You Begin

Your administrator will inform you if you need to enable Strict Certificate Trust on your mobile device for connectivity to your network.

Procedure

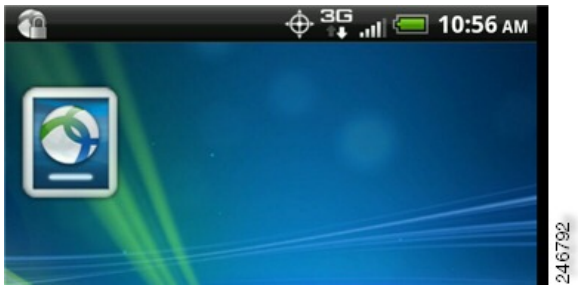
Step 1 From the AnyConnect home window, tap **Menu** > **Settings**.

Step 2 Tap **Strict Certificate Trust** to enable or disable this preference.
Upon the next connectivity attempt, Strict Certificate Trust will be used, or not, to determine if the user will be able to choose to accept an unverified certificate received from the head-end.

Using AnyConnect Widgets

AnyConnect provides widgets to add to your home screen:

- The smallest widget is the same size as the AnyConnect apps icon. The color of the bar below the icon reflects the VPN status. Tap the widget to connect to or disconnect from the current VPN connection.



- The larger widget shows the AnyConnect icon and name, the current VPN connection, and the VPN status. Tap the widget to connect to or disconnect from the VPN connection.

The instructions for placing a widget may vary, depending on the device and the Android version that you are using. Example instructions are provided.

Procedure

Step 1 Go to an Android home screen that has enough space for the widget that you want to use.

Step 2 Tap **Menu** > **Personalize** > **Widgets**.

Step 3 Tap the AnyConnect widget that you want to use.

Android adds the widget to the home screen.

Step 4 Long-press the widget if you want to reposition it. Move it after it responds.

Managing the AnyConnect Client Profile

About AnyConnect Client Profiles

The AnyConnect VPN Client Profile is an XML file that specifies client behavior and identifies VPN connections. Each connection entry in the VPN Client Profile specifies a secure gateway that is accessible to this device, as well as other connection attributes, policies, and constraints. These connection entries, in addition to the VPN connections that you configured locally on the device, are listed on the AnyConnect home screen to choose from when initiating a VPN connection.

AnyConnect retains only one VPN Client Profile on the Android device at a time. The following are some key scenarios that cause the current profile, if it exists, to be replaced or deleted:

- Manually importing a profile replaces the current profile with the imported profile.
- Upon startup of an automatic or manual VPN connection, the new connection's profile replaces the current profile.
- If a VPN connection does not have a profile associated with it, the existing profile is deleted upon startup of that VPN.

View or delete the AnyConnect profile currently on the device, or import a new one.

Viewing the AnyConnect Profile

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Profile Management**.

Step 2 Tap the expansion icon for the **Current Profile Details**. The XML file is displayed. Scroll down to see the whole file.

Importing an AnyConnect Profile

Before You Begin

A profile file must be present on the Android device to import it in this way. Your administrator provides you with the name of the profile file to be installed on your device.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Profile Management**.

Step 2 Tap **Import Profile** and choose the XML profile from the device's file system.

Connection entries defined in this profile appear in the AnyConnect home screen immediately, and AnyConnect client behavior conforms to this profile's specifications.

Removing the AnyConnect Profile

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Profile Management** .

Step 2 Tap **Delete Profile** and confirm to delete the current profile.

Connection entries defined in the profile are cleared from the AnyConnect home screen, and AnyConnect client behavior conforms to default client specifications.

Managing Localization

Viewing Installed Localization Data

Upon AnyConnect installation, your mobile device is localized if the device's specified locale matches one of the packaged language translations. The following language translations are included in the AnyConnect package:

- Canadian French (fr-ca)
- Chinese (Taiwan) (zh-tw)
- Czech (cs-cz)
- Dutch (nl-nl)
- French (fr-fr)
- German (de-de)
- Hungarian (hu-hu)
- Italian (it-it)
- Japanese (ja-jp)
- Korean (ko-kr)
- Latin American Spanish (es-co)
- Polish (pl-pl)
- Portuguese (Brazil) (pt-br)
- Russian (ru-ru)
- Simplified Chinese (zh-cn)
- Spanish (es-es)

The installed language is determined by the locale specified in **Settings** > **Language and Keyboard** > **Select locale**. AnyConnect UIs and messages are translated as soon as AnyConnect starts.

AnyConnect uses the language specification, then the region specification, to determine the best match. For example, after installation, a French-Switzerland (fr-ch) locale setting results in a French-Canadian (fr-ca) display.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Localization Management**.

Step 2 View the list of Localization Files installed on your mobile device.

The indicated language is the one currently being used by AnyConnect.

Importing Localization Data

After installation, localization data for languages not supported in the AnyConnect package is imported by:

- Clicking on a hyperlink provided to you by an administrator that has been defined to import localization data.

  Your administrator can provide a hyperlink in email, or on a web page, that imports localization data when clicked. This method uses the AnyConnect URI handler, a feature available to administrators for simplifying AnyConnect configuration and management.

  Note You must allow this AnyConnect activity by setting External Control to either Prompt or Enable within the AnyConnect settings. See Control the External Use of AnyConnect, on page 13 for how to set this.

- Connecting to a secure gateway that an administrator has configured to provide downloadable localization data upon VPN connection.

  If this method is to be used, your administrator will provide you with appropriate VPN connection information or a predefined connection entry in the XML profile. Upon VPN connection, localization data is downloaded to your device and put into play immediately.

- Manually imported using the **Import Localization** option on the AnyConnect Localization Management Activity Screen as described below.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Localization Management**.

Step 2 Tap **Import Localization**.

Step 3 Specify the address of the secure gateway and the locale.
The locale is specified per ISO 639-1, with the country code added if applicable (for example, en-US, fr-CA, ar-IQ, and so on).

This localization data is used in place of the pre-packaged, installed localization data.

Restoring Localization Data

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Localization Management**.

Step 2 Tap **Restore Localization**.

Restores the use of the pre-loaded localization data from the AnyConnect package and deletes all imported localization data.

The restored language is chosen based on the device's locale specified in **Settings** > **Language and Keyboard** > **Select locale**.

Exiting AnyConnect

Exiting AnyConnect terminates the current VPN connection and stops all AnyConnect processes. Use this action sparingly. Other apps or processes on your device may be using the current VPN connection and exiting AnyConnect may adversely affect their operation.

Procedure

From the AnyConnect home window, tap **Menu** > **Exit**.

In the event that AnyConnect is unable to gracefully exit all of its processes, you will be detoured to the Android application management screen to manually terminate AnyConnect by tapping **Force Stop**.

Removing AnyConnect

Procedure

Step 1 Go to the Android Settings for your device and proceed to the app or applications management area.

Step 2 Tap **Uninstall**.

Monitor and Troubleshoot AnyConnect

Display the AnyConnect Version and Licenses

Procedure

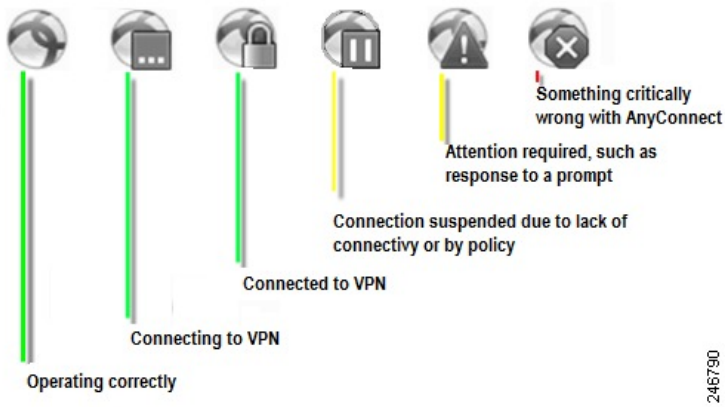
From the AnyConnect home window, tap **Menu** > **About**.

What to Do Next

Tap the link in the **About** window to open the latest version of this guide.

Determine Connection Status

By default, AnyConnect reveals its status by changing its icon in the Android status bar at the top of the Android window. The icon indicates the current state of the AnyConnect connection:



View AnyConnect Statistics

AnyConnect records statistics when a VPN connection is present.

Procedure

From the AnyConnect home screen, tap **Details**.

Detailed statistics include the following values:

- Secure Routes—An entry with the destination 0.0.0.0 and the subnet mask 0.0.0.0 means that all VPN traffic is encrypted and sent or received over the VPN connection.
- Non-Secure Routes—Shown only if 0.0.0.0/0.0.0.0 is present under SecureRoutes.Traffic destinations, as determined by the VPNsecure gateway, that are excluded from the encryptedconnection.

AnyConnect Logging

Viewing Log Messages

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Logging and System Information**.

AnyConnect retrieves its messages and displays them in the Messages, System and Debug windows.

Step 2 Tap the **Messages**, **System**, or **Debug** tab to view log messages or system information.

- Messages: Logs pertaining to AnyConnect activity.
- System: Information related to memory, interface, route, filter, permissions, process, system properties, memory map, and unique device ID.
- Debug: Logs used by administrators and Cisco Technical Assistance Center (TAC) to analyze AnyConnect issues.

Step 3 Scroll the window to view all messages.

Sending Log Messages

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Logging and System Information**.

Step 2 Tap **Menu** > **Send Logs**.

The log messages and all profile data are packaged into a .zip file and inserted into an email message. Use the email option to send the log files to your administrator if you are reporting a problem with AnyConnect. The problem statement and the steps to reproduce the problem must be specified before sending your log messages.

Use Bluetooth to transmit locally. Bluetooth must first be enabled on both the sending and receiving devices.

Clearing Debug Log Messages

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Logging and System Information**.

Step 2 Tap **Menu** > **Clear Debug Logs**.

Common Android Problems

I received a tun.ko error message

A tun.ko module is required if it is not already compiled into the kernel. If it is not included on the device or compiled with the kernel, obtain or build it for your corresponding device kernel and place it in the /data/local/kernel_modules/ directory.

I cannot edit/delete some connection entries

Your administrator defined these connection entries in the AnyConnect Profile. See Viewing and Managing the AnyConnect profile for instructions on deleting these profiles.

Connection timeouts and unresolved hosts

Internet connectivity issues, a low-cell signal level, and a congested network resource are typical causes of timeouts and unresolved host errors. Try moving to an area with a stronger signal or use WiFi. If a Wi-Fi network is within reach, try using your device Settings app to establish a connection to it first. Retrying multiple times in response to timeouts often results in success.

Certificate-based authentication does not work

Check the validity and expiration of the certificate if you succeeded with it before. To do so, go to the AnyConnect home window, long-press the connection entry, and tap **Certificate**. The Certificates window lists all certificates. Long-press the certificate name and tap **View Certificate Details**. Check with your administrator to make sure that you are using the appropriate certificate for the connection.

Error connecting, device working OK

Ask your administrator if the VPN secure gateway is configured and licensed to permit mobile connections.

Cannot connect to ASA, unresolvable host error

Use an Internet browser to check the network connection. To verify network connectivity, go to https://`vpn.example.com`, where `vpn.example.com` is the URL of the VPN secure gateway.

AnyConnect package fails to install from the Market

Ensure that the device is listed as one of the Supported Android Devices.

"Installation Error: Unknown reason -8"

If you attempt to install a brand-specific AnyConnect package on devices that are not supported, they receive this message. Review the list of supported Android devices and instructions for installing or upgrading AnyConnect to download the proper AnyConnect package for your device.

AnyConnect error, "Could not obtain the necessary permissions to run this application. This device does not support AnyConnect."

AnyConnect does not work on this device. Review the list of supported Android devices and instructions for installing or upgrading AnyConnect to download the proper AnyConnect package for your device.

Cannot email logs because of a network connectivity issue

Try another Internet-accessible network. Save the log messages in a draft email message if you do not have network connectivity or you need to reset the device.

AnyConnect frequently connects by itself

This may be due to your Trusted Network Detection / Automatic VPN Policy. Disable the TND application preference in the AnyConnect settings to turn this functionality off.

Authentication using a one time password is not working

Due to an Android issue, when pasting text from the clipboard, a space is inserted in front of the text. In AnyConnect, when copying text such as a one time password, the user has to delete this erroneous white space.

Guidelines and Limitations for AnyConnect on Android

- AnyConnect for Android supports only the VPN features that are strictly related to remote access.
- AnyConnect for Android supports only the Network Visibility Module, it does not support any other AnyConnect modules.
- The ASA does not provide distributions and updates for AnyConnect for Android. They are available only on Google Play.

- AnyConnect for Android supports connection entries that the user adds and connection entries populated by an AnyConnect profile pushed by an ASA. The Android device supports no more than one AnyConnect profile, which is the last one received from a headend. However, a profile can consist of multiple connection entries.
- If users attempt to install AnyConnect on devices that are not supported, they receive the pop-up message `Installation Error: Unknown reason -8`. This message is generated by the Android OS.
- When users have an AnyConnect widget on their home screen, the AnyConnect services are automatically started (but not connected) regardless of the "Launch at startup" preference.
- AnyConnect for Android requires UTF-8 character encoding for extended ASCII characters when using pre-fill from client certificates. The client certificate must be in UTF-8 if you want to use prefill, per the instructions in KB-890772 and KB-888180.
- AnyConnect blocks voice calls if it is sending or receiving VPN traffic over an EDGE connection per the inherent nature of EDGE and other early radio technology.
- Some known file compression utilities do not successfully decompress log bundles packaged with the use of the AnyConnect Send Log button. As a workaround, use the native utilities on Windows and Mac OS X to decompress AnyConnect log files.

Known Compatibility Issues

- IPv6 on public and private interfaces.

  IPv6 is supported on both private and public transports using AnyConnect 4.05015 and later, on Android 5 and later. With this combination the following is now allowed: IPv4 over an IPv6 tunnel, IPv6 over an IPv6 tunnel.

  This is in addtion to the previously allowed tunnel configuratons on earlier AnyConnect and Android releases: IPv4 over an IPv4 tunnel, and IPv6 over an IPv4 tunnel.

  Note Due to Google issue 65572, IPv6 over IPv4 does not work on Android 4.4. You must use Android 5 or later.

- Battery saver and AnyConnect:
  - Android 5.0 introduced battery saver capabilities that block background network connectivity on your device. When battery saver is enabled, AnyConnect will transition to the Paused state if it is in the background. To work around this on Android 5.0, users may turn off battery saver via the device settings: Settings -> Battery -> Battery saver or from the notification bar.
  - In Android 6.0+, when AnyConnect transitions to the Paused state as a result of battery saver, a popup with the option to whitelist AnyConnect from battery saver mode will be povided. Whitelisting AnyConnect will allow the continued use of battery saver without impacting AnyConnect's ability to run in the background.
  - Once AnyConnect is paused due to the batter saver, a manual reconnect is necessary to bring AnyConnect out of the Paused state, regardless of your action to turn off battery saver or whitelist AnyConnect.

- Split DNS does not work on any Android 4.4 device, and also does not work on Samsung 5.x Android devices. For Samsung devices, the only workaround is to connect to a group with split DNS disabled. On other devices you must upgrade to Android 5.x to receive the fix for this problem.

  This is due to a known issue that is present in Android 4.4 (Issue #64819), fixed in Android 5.x, but not incorporated into Samsung 5.x android devices.

- Due to a bug in Android 5.x (Google Issue #85758, Cisco Issue # CSCus38925), if the AnyConnect app is closed from the recent apps screen it may not operate properly. To restore proper operation, terminate AnyConnect in **Settings** and then restart it.
- On Samsung mobile devices the **Settings > Wi-Fi > Smart network switch** allows switching from WIFI to LTE to maintain a stable Internet connection (when the Wi-Fi connection is not optimum). This also results in a pause and reconnect of the active VPN tunnel. Cisco recommends turning this off, since it may result in continuous reconnects.
- On Android 5.0 (Lollipop), which supports multiple active users, the VPN connection tunnels data for a single user only, not for all users on the device. Background data flow may be occurring in the clear.
- Due to a bug in Android 4.3.1(Google Issue #62073), users using the AnyConnect ICS+ package cannot enter non-fully qualified domain names. For example, users cannot type "internalhost", they must type "internalhost.company.com."
- The AT&T firmware updates on HTC One to Android 4.3 (software version: 3.17.502.3) do not support "HTC AnyConnect." Customers must uninstall "HTC AnyConnect", and install "AnyConnect ICS+." (HTC AnyConnect will work on the international edition, with software version of 3.22.1540.1). Check your software version on your device at **Settings > About > Software information > Software number**.
- We are pleased to report that Google Issue #70916, VPN connections will fail to connect if the administrator has set the MTU for Android tunnels lower than 1280, has been resolved in Android 5.0 (Lollipop). The following problem information is provided for reference:

  Due to a regression in Android 4.4.3,(Google Issue #70916, Cisco CSCup24172), VPN connections will fail to connect if the administrator has set the MTU for Android tunnels lower than 1280. This issue has been reported to Google and will require a new version of the OS to correct the regression introduced in Android 4.4.3. To workaround this problem, ensure that the head-end administrator has not configured the tunnel MTU to be lower than 1280.

  When encountered, the message displayed to the end user is: `System configuration settings could not be applied. A VPN connection will not be established`, and AnyConnect debug logs will report:

```
E/vpnandroid( 2419): IPCInteractionThread: NCSS: General Exception occured, telling client
E/vpnandroid( 2419): java.lang.IllegalStateException: command '181 interface fwmark rule add tun0'
failed with '400 181 Failed to add fwmark rule (No such process)'
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1473)
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1419)
E/vpnandroid( 2419): at
com.cisco.android.nchs.aidl.IICSSupportService$Stub$Proxy.establish
(IICSSupportService.java:330)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.VpnBuilderWrapper.establish
(VpnBuilderWrapper.java:137)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.NCSSIPCServer.callServiceMethod
(NCSSIPCServer.java:233)
E/vpnandroid( 2419): at
com.cisco.android.nchs.ipc.IPCInteractionThread.handleClientInteraction
(IPCInteractionThread.java:230)
E/vpnandroid( 2419): at com.cisco.android.nchs.ipc.IPCInteractionThread.run
(IPCInteractionThread.java:90)
E/acvpnagent( 2450): Function: ApplyVpnConfiguration
File: NcssHelper.cpp Line: 740 failed to establish VPN
E/acvpnagent( 2450): Function: PluginResult AndroidSNAKSystem::configDeviceForICS()
File: AndroidSNAKSystem.cpp Line: 665 failed to apply vpn configuration
E/acvpnagent( 2450): Function: virtual PluginResult AndroidSNAKSystem::ApplyConfiguration()
File: AndroidSNAKSystem.cpp Line: 543 Failed to Configure System for VPN.
```

- We are pleased to report that Android 4.4 (KitKat) bug Google Issue #61948 (AnyConnect users will experience High Packet Loss over their VPN connection /users will experience timeouts) has been resolved in Google's release of Android 4.4.1 which Google has begun distributing to some devices via Software Update. The following problem information is provided for reference:

  Due to a bug in Android 4.4 (Issue #61948, also see the Cisco Support Update), AnyConnect users will experience High Packet Loss over their VPN connection. This has been seen on the Google Nexus 5 running Android 4.4 with AnyConnect ICS+. Users

will experience timeouts when attempting to access certain network resources. Also, in the ASA logs, a syslog message will appear with text similar to "Transmitting large packet 1420 (threshold 1405)."

Until Google produces a fix for Android 4.4, VPN administrators may temporarily reduce the maximum segment size for TCP connections on the ASA by configuring the following sysopt connection tcpmss <mss size>. The default for this parameter is 1380 bytes. Reduce this value by the difference between the values seen in the ASA logs. In the above example, the difference is 15 bytes; the value should thus be no more than 1365. Reducing this value will negatively impact performance for connected VPN users where large packets are transmitted.

- AnyConnect for Android may have connectivity issues when connecting to a mobile network using the IPv6 transition mechanism known as 464xlat. Known affected devices include the Samsung Galaxy Note III LTE connecting to the T-Mobile US network. This device defaults to an IPv6 only mobile network connection. Attempting a connection may result in a loss of mobile connectivity until the device is rebooted.

  To prevent this problem, use the AnyConnect ICS+ app, and change your device settings to obtain IPv4 network connectivity or connect using a Wi-Fi network. For the Samsung Galaxy Note III LTE connecting to the T-Mobile US network, follow the instructions provided by T-Mobile to set the Access Point Name (APN) on your device, making sure APN Protocol is set to IPv4.

- The AnyConnect ICS+ package may have issues when a private IP address range within the VPN overlaps with the range of the outside interface of the client device. When this route overlap occurs, the user may be able to successfully connect to the VPN but then be unable to actually access anything. This issue has been seen on cellular networks which use NAT (Network Address Translation) and assign addresses within the 10.0.0.0 - 10.255.255.255 range, and is due to AnyConnect having limited control of routes in the Android VPN framework. The vendor specific Android packages have full routing control and may work better in such a scenario.

- An Asus tablet running Android 4.0 (ICS) may be missing the tun driver. This causes AVF AnyConnect to fail.

- Android security rules prevent the device from sending and receiving multimedia messaging service (MMS) messages while a VPN connection is up. Most devices and service providers display a notification if you try to send an MMS message while the VPN connection is up. Android permits sending and receiving of messages when the VPN is not connected.

- Due to Google Isssue 41037 , when pasting text from the clipboard, a space is inserted in front of the text. In AnyConnect, when copying text such as a one time password, the user has to delete this erroneous white space.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands