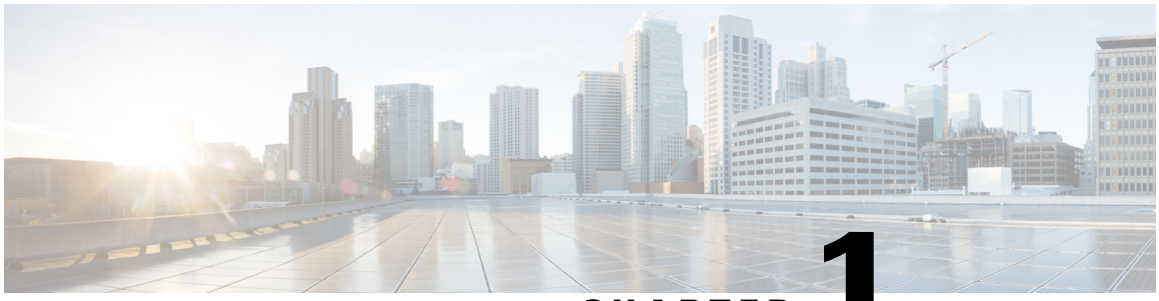
Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.x

First Published: October 22, 2012

Last Modified: February 15, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Installing and Starting AnyConnect

Overview

The Cisco AnyConnect Secure Mobility Client for Android provides seamless and secure remote access to enterprise networks. AnyConnect allows any installed application to communicate as though connected directly to the enterprise network.

Your organization may provide additional documentation on using AnyConnect for Android.

Installing the AnyConnect Application

Note AnyConnect for Android is available for download only from the Android Market. You cannot download it from the Cisco website or after connecting to a secure gateway.

Procedure

Step 1 Determine if your device is one of the supported devices and install the appropriate brand-specific AnyConnect package.

Cisco provides brand-specific AnyConnect packages that offer full-featured VPN connections for these devices. These brand-specific AnyConnect clients are provided in partnership with the device vendors and are the preferred AnyConnect clients for supported devices.

a) For Samsung Devices:

- Install Samsung AnyConnect if your device was produced or upgraded after September 2011.

- Install Samsung AnyConnect Legacy if your device was produced before September 2011 and has not received an upgrade.

If an install attempt results in one of the following error messages, try the other Samsung package:

- "Installation Error: Unknown reason -8"
- "Incompatible with other application(s) using the same shared user ID."

b) For HTC Devices, install HTC AnyConnect.

c) For Kindle Devices, install Cisco AnyConnect (Kindle Tablet Edition).

Step 2 Otherwise, determine if your device is running Android 4.0 (Ice Cream Sandwich) or later to install AnyConnect ICS+.

This AnyConnect client offers VPN connectivity supported by the Android VPN Framework (AVF) in Android 4.0 or later. AVF provides only basic VPN connectivity. The AnyConnect AVF client, dependent upon these basic VPN capabilities, is unable to provide the full set of VPN features available in the brand-specific packages.

Step 3 Otherwise, determine if your device is rooted and running Android 2.1 or later, install Rooted AnyConnect.

Note Cisco provides this AnyConnect package for preview and testing purposes only. Cisco does not support this client, but it works on most rooted devices running 2.1 or later.

Both a tun.ko module and iptables are required. AnyConnect displays an error message informing you about what is missing when you attempt to establish a VPN connection. If the tun.ko module is missing, obtain or build it for your corresponding device kernel and place it in the /data/local/kernel_modules/ directory.

Caution Rooting your device voids your device warranty. Cisco does not support rooted devices, nor do we provide instructions to root your device. If you choose to root your device, you do so at your own risk.

Supported Android Devices

Cisco provides AnyConnect brand-specific apps to support mobile devices from the following manufacturers:

- Samsung Devices
- HTC Devices
- Kindle Devices

Cisco also provides the following AnyConnect apps to support Android devices:

- Android VPN Framework Devices
- Rooted Devices

Note Cisco no longer provides or supports the brand-specific AnyConnect apps for Lenovo and Motorola devices. Lenovo and Motorola devices that run Android version 4.0 (Ice Cream Sandwich) or later can use the AnyConnect ICS+ app. Uninstall the old brand-specific AnyConnect package before upgrading to AnyConnect 3.0.

Samsung Devices

Samsung AnyConnect and Samsung AnyConnect Legacy support the Samsung product lines listed below. The devices must be running the latest software update from Samsung and the identified Android releases. See the Android installation procedure to determine which package applies to your device.

Note Samsung rebrands devices in these product lines for each mobile service provider.

Product Name	Product Model
ACE+	GT-S7500, GT-S7500, GT-S7500W
ACE II	GT-I8160
Conquer 4G	SPH-D600
Galaxy Appeal	SGH-I827
Galaxy Beam	GT-I8530
Galaxy Exhilarate	SGH-I577
Galaxy Mini	GT-S5570, GT-S5570B, GT-S5570BD1, GT-S5570L, GT-S5578, SCH-I559, SGH-T499 , SGH-T499V, SGH-T499Y,
Galaxy Note	GT-I9220, GT-N7000, GT-N7000B, SHV-E160K, SHV-E160S, SHV-E160L, SCH-I889, SCH-I717M, SCH-I717R, SCH-I717D, SGH-NO54, SCH-I717
Galaxy Note 10.1	GT-N8000, GT-N8005, SHW-M480S, SHW-M480K, GT-N8010, GT-N8013, SHW-M480W
Galaxy Rush	SPH-M830

Galaxy S	GT-I9000, GT-I9000B, GT-I9000L, GT-I9000LD1, GT-I9000M, GT-I9000T, GT-I9001, GT-I9003, GT-I9003B, GT-I9003L, GT-I9008, GT-I9008L, GT-I9018, GT-I9070, GT-I9070P, GT-I9088, SC-02B, SCH-I400, SCH-I405, SCH-I500, SCH-I809, SCH-I909, SGH-I896, SGH-I897, SGH-I927, SGH-I997R, SGH-N013, SGH-T699, SGH-T759, SGH-T769, SGH-T959, SGH-T959D, SGH-T959P, SGH-T959V, SGH-T959W, SHW-M100S, SHW-M110S, SHW-M130L, SHW-M190S, SHW-M220L, SHW-M340K, SHW-M340L, SHW-M340S, SPH-D720
Galaxy S II	GT-I9100, GT-I9100G, GT-I9100M, GT-I9100T, GT-I9100P, GT-I9103, GT-I9108, GT-I9210, GT-I9210T, SC-O2C, SC-O3D, SCH-I510, SCH-I919, SCH-I919U, SCH-I929, SCH-J001, SCH-W999, SGH-I727, SGH-I727R, SGH-I757M, SGH-N033, SGH-N034, SGH-T989, SCH-T989D, SHV-E110S, SHV-E120K, SHV-E120L, SHV-E120S, SHW-M250K, SHW-M250L, SHW-M250S, SPH-D170
Galaxy S III	GT-I9300, SCH-I535, SGH-I747, SGH-T999, SHV-E210K, SHV-E210L, SHV-E210S, SPH-L710
Galaxy S 4	GT-I9500, GT-I9505, SCH-I545, SGH-I337
Galaxy Stellar	SCH-I200
Galaxy Tab 7 (WiFi only) [1]	GT-P1000, GT-P1000L, GT-P1000M, GT-P1000N, GT-P1000R, GT-P1000T, GT-P1010, SC-01C, SCH-I800, SGH-I849, SGH-I987, SHW-M180L, SHW-M180S
Galaxy Tab 7.0 Plus & 7.7	GT-P6200, GT-P6201, GT-P6210, GT-P6211, GT-P6800, GT-P6801, GT-P6810, GT-P6811, SCH-I815, SGH-N024, SGH-T869, SHV-E150S, SHW-M430W
Galaxy Tab 8.9	GT-P7300, GT-P7300B, GT-P7310, GT-P7320, GT-P7320T, SCH-P739, SGH-I957, SGH-I957M, SGH-I957R, SHV-E140K, SHV-E140L, SHV-E140S, SHW-M300S, SHW-M300W, SHW-M305W
Galaxy Tab 10.1	GT-P7500, GT-P7500D, GT-P7500M, GT-P7500R, GT-P7500V, GT-P7501, GT-P7503, GT-P7510, GT-P7511, SC-01D, SCH-I905, SGH-T859, SHW-M380K, SHW-M380S, SHW-M380W
Galaxy Tab 2 7.0	GT-P3100, GT-P3110, GT-P3113, SCH-I705
Galaxy Tab 2 10.1	GT-P5100, GT-P5110, GT-P5113
Galaxy W	GT-I8150, SGH-T679

Galaxy Xcover	GT-S5690
Galaxy Y Pro	GT-B5510B, GT-B5510L
Illusion	SCH-I110
Infuse	SCH-I997
Rugby	SGH-I847
Stratosphere	SCH-I405
Stratosphere II	SCH-I415
Transform Ultra	SPH-M930

[1] We do not support the Sprint distribution of the Samsung Galaxy Tab 7 mobile device.

HTC Devices

HTC AnyConnect supports the HTC product lines listed at http://www.htcpro.com/enterprise/VPN.

Devices must be running the minumum software required. Go to **Settings > About phone > Software information > Software number** to determine the software number running on your device.

Kindle Devices

Cisco AnyConnect (Kindle Tablet Edition) Release 3.0.x is available from Amazon for the Kindle Fire HD devices, and the New Kindle Fire. Anyconnect for Kindle is supported by the Android VPN Framework and is equivalent in functionality to the AnyConnect ICS+ package

Android VPN Framework Devices

AnyConnect ICS offers VPN connectivity supported by the Android VPN Framework (AVF) in Android 4.0 (Ice Cream Sandwich) or later.

The AVF provides only basic VPN connectivity. The AnyConnect client, dependent upon these basic VPN capabilities, is unable to provide the full set of VPN features available in the brand-specific packages.

Note Cisco recommends the AVF AnyConnect client for unsupported devices running Android 4.0 or later. Supported devices should use the brand-specific AnyConnect client regardless of the version of the Android operating system.

Rooted Devices

Cisco provides Rooted AnyConnect for rooted Android mobile devices running Android 2.1 or later. This client is provided for preview and testing purposes only. Cisco does not support this client, but it works on

most rooted devices running Android 2.1 or later. If you encounter issues, please report them to android-mobile-feedback@cisco.com, and we will make our best effort to resolve them.

Both a tun.ko module and iptables are required. AnyConnect displays an error message informing you about what is missing when you attempt to establish a VPN connection. If the tun.ko module is missing, obtain or build it for your corresponding device kernel and place it in the `/data/local/kernel_modules/` directory.

Note Rooting your device voids your device warranty. Cisco does not support rooted devices, nor do we provide instructions to root your device. If you choose to root your device, you do so at your own risk.

Starting AnyConnect

Procedure

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

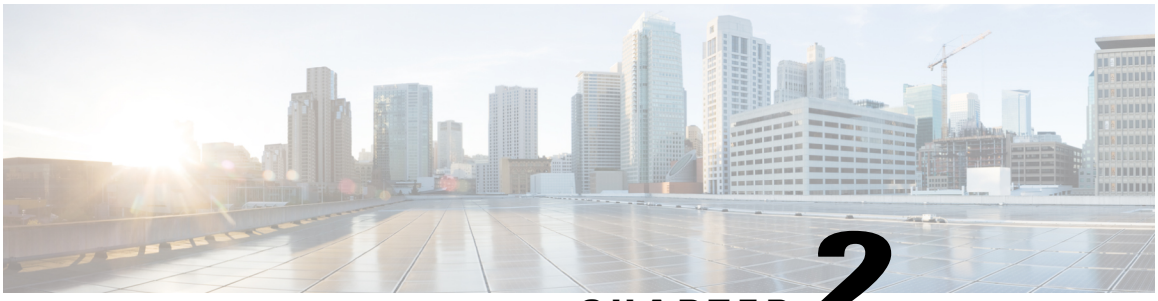
Step 2 If this is the first time that you are starting AnyConnect after installing or upgrading, accept the displayed End User License Agreement to continue.

Step 3 **Add New VPN Connection** or tap **Menu** and choose:

- **Statistics**, to view summary and detailed statistics about the current active VPN connection. See Viewing AnyConnect Statistics.
- **Settings**, to specify AnyConnect application preferences. See Specifying Application Preferences.
- **Diagnostics**, to carry out the following diagnostic activities:
  - Managing certificates; see About Certificates on Your Android Device.
  - Managing AnyConnect profiles; see About AnyConnect Client Profiles.
  - Managing AnyConnect localization; see About Android Device Localization.
  - Viewing logging and system information; see Viewing Log Messages.
- **About**, to view AnyConnect version and license information. See Displaying the AnyConnect Version and Licensing Details.
- **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.



CHAPTER 2

Configuring a VPN Connection

Overview of AnyConnect Configuration

AnyConnect requires the following information for configuring VPN connectivity:

- An address to a secure gateway for access to your network.
- Authentication information to successfully complete your connection, in the form of a username and password, a digital certificate, or both.

Configure your AnyConnect client as directed by your administrator; contact your administrator if you do not have clear instructions. Your administrator provides you with one of the following:

- Addressing and authentication information, and other connection attributes if needed, to manually configure your device.
- Procedures to automate configuration using this information.

You, the AnyConnect user, should be familiar with:

- Connection entries: VPN connections configured on your device manually or automatically. Connection entries are listed on the AnyConnect home screen. The current active connection entry is identified in the **AnyConnect VPN** panel on the app's home screen.

- How to establish a VPN connection: manually tap the connection entry in the connection list, or tap the checkbox or slider in the **AnyConnect VPN** panel. VPN connections can also be made automatically using procedures provided by your administrator.
- The authentication method used to establish a connection: remembering your username and password or importing and assigning a user certificate to a connection entry.

AnyConnect is a sophisticated networking application that also allows you to carry out the following activities:

- Set preferences for the application, controlling the appearance and operation of AnyConnect.
- Use diagnostic tools and management facilities on your device as recommended by your administrator.

About AnyConnect Connection Entries

A connection entry specifies a secure gateway that is accessible to this device, as well as other connection attributes. Connection entries are configured in the following ways:

- Added automatically: After clicking a link provided by your administrator to configure connection entries.
- 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; it may also specify a group that you are connecting to.

Connection entries are also defined in an AnyConnect client profile that is downloaded from a Cisco ASA secure gateway upon connectivity.

Related Topics

Adding Connection Entries from Hyperlinks, on page 8
Adding Connection Entries Manually, on page 9
Modifying a Connection Entry, on page 19
Deleting Connection Entries, on page 20

Adding Connection Entries from Hyperlinks

Your administrator will provide you with a hyperlink to add a connection entry.

Before You Begin

Set **External Control** to either **Prompt** or **Enable** within the AnyConnect settings. See Controlling External Use of AnyConnect, on page 25

Procedure

Tap the hyperlink provided by your administrator.

The link may be included in an e-mail or published on an intranet web page.

The connection entry is added to your list of connections on the AnyConnect home window.

Related Topics

About AnyConnect Connection Entries, on page 8

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 **Add new VPN Connection** to open the Connection Editor.

Cancel out of the Connection Editor window 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 Connection Editor** window and the **Connection Editor** window to save the connection values.

AnyConnect adds the new connection entry to the list in the home window.

Related Topics

About AnyConnect Connection Entries, on page 8

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 e-mail 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.

Related Topics

Importing Certificates from Hyperlinks, on page 10
Importing Certificates Manually, on page 11
Importing Certificates Provided by a Secure Gateway, on page 12
Viewing Certificates, on page 22
Removing Certificates, on page 22

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 e-mail 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.

Related Topics

About User Certificates, on page 10

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 adinistrator.

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.

Related Topics

About User Certificates, on page 10

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.

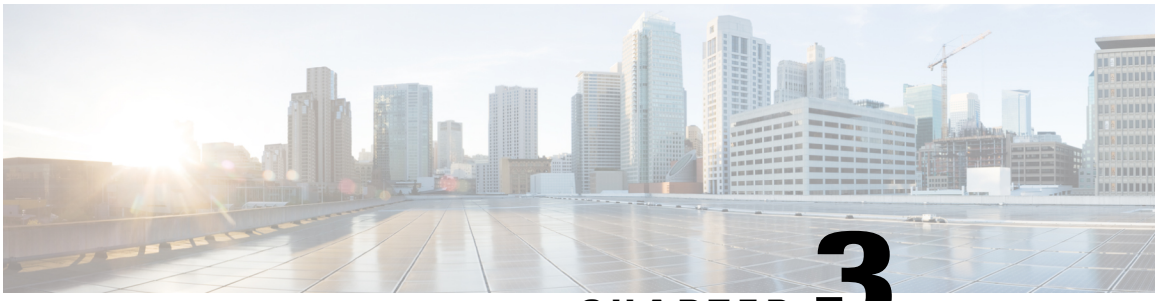
Step 3 If present, tap **Get Certificate**, or select the group configured to download a certificate to your mobile device.

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.

Related Topics

About User Certificates, on page 10



CHAPTER 3

Establishing a VPN Connection

Connecting to a VPN

You connect to a VPN by selecting one of the 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 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.

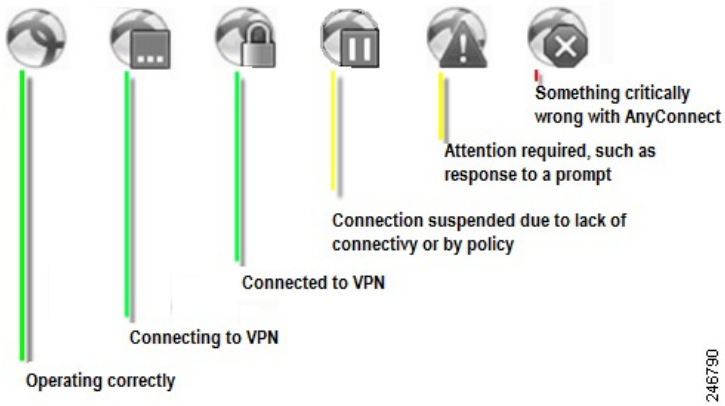
Depending on the VPN secure gateway configuration, AnyConnect may add connection entries to the list in the AnyConnect home window.

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.

Determining Connection Status

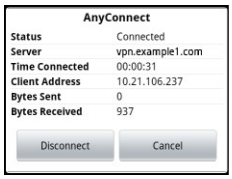
By default, AnyConnect reveals its status by changing its icon in the Android status bar at the top of the Android window. The icon indicates the current state of the AnyConnect connection:

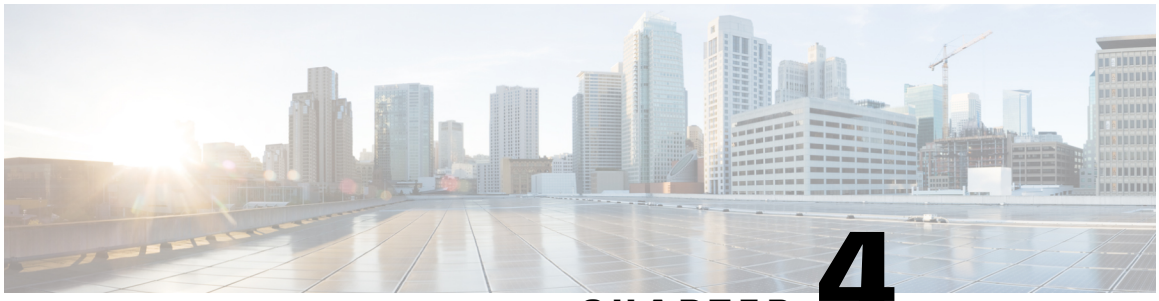


Viewing the Connection Summary

Procedure

From the AnyConnect home window, tap the name of the current connection under **Choose a connection**.





CHAPTER 4

Responding to AnyConnect Notifications

Responding 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.

Related Topics

About Server Certificates, on page 21

Responding 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**. See Controlling External Use of AnyConnect, on page 25 to set this preference.

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]`

Responding 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

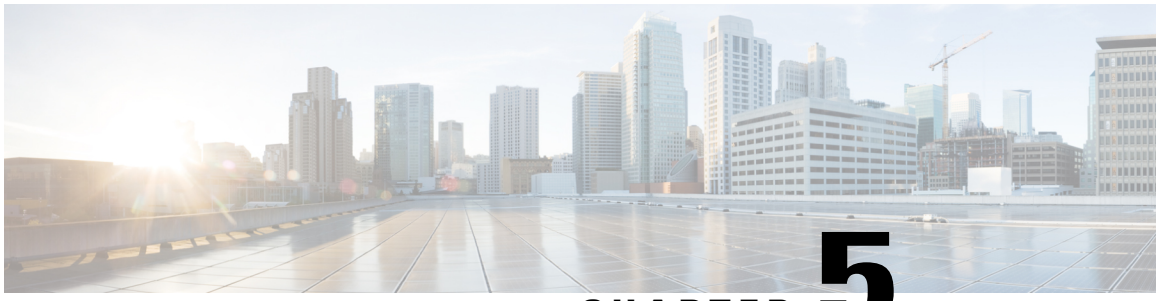
Step 1 Tap the notification icon to view the notification.

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**.



CHAPTER 5

Optional AnyConnect Configuration and Management

Modifying and Deleting Connection Entries

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, long-press the VPN connection entry to be modified.

AnyConnect displays 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 and reopens the AnyConnect home window.

Related Topics

About AnyConnect Connection Entries, on page 8

Deleting Connection Entries

This procedure deletes a manually configured VPN connection entry.

Note 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 Open the AnyConnect home window and long-press the connection entry to be deleted.

AnyConnect displays the **Select Action** window.

Step 2 Tap **Delete connection**.

AnyConnect removes the connection entry and reopens the AnyConnect home window.

Related Topics

About AnyConnect Connection Entries, on page 8

Configuring Certificates

About Certificates on Your Android Device

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 e-mail 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.

Related Topics

Importing Certificates from Hyperlinks, on page 10

Importing Certificates Manually, on page 11

Importing Certificates Provided by a Secure Gateway, on page 12

Viewing Certificates, on page 22

Removing Certificates, on page 22

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.

Related Topics

Responding to Untrusted VPN Server Notifications, on page 17
Viewing Certificates, on page 22
Removing Certificates, on page 22

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.

Related Topics

About User Certificates, on page 10
About Server Certificates, on page 21

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.

Related Topics

About User Certificates, on page 10
About Server Certificates, on page 21

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.

Specifying Application Preferences

Procedure

From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

Changing the AnyConnect Theme

AnyConnect provides the following themes:

- Cisco Default Theme (default)—Color contrast, emphasizing shades of blue.
- Android—Android-like alternative to the Cisco default theme.

Note The assignment of the Android theme to AnyConnect has issues such as the whiteout of field values on some devices. Reapply the default theme if the Android theme is difficult to use.

Procedure

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

Step 2 Tap **Application Style**.

AnyConnect shows a green button next to the theme currently in use.

Step 3 Tap the theme that you want displayed.

Launching 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** > **Application Preferences**.

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

Hiding 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** > **Application Preferences**.

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

If left unchecked, the icon displays persistently.

Controlling External Use of AnyConnect

The External Control application preference 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 e-mails or on web pages. Your administrator will instruct you to set this preference to one 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 Responding to Another App, on page 17 for details.

Procedure

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

Step 2 Tap **External Control**.

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

Blocking 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** > **Application Preferences**.

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

Setting 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** > **Application Preferences**.

Step 2 Tap the **FIPS Mode** checkbox 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.

Setting Trusted Network Detection

Trusted Network Detection (TND) allows automatic initiation of a VPN connection when the device is outside of a trusted network and automatic suspension of the VPN connection when the device returns to a trusted network.

Your administrator enables this feature, defines which networks are trusted or untrusted, and determines AnyConnect behavior when it detects network transitions. For example, your administrator may configure TND to automatically connect while you are on your home network and then disconnect when you move into the corporate network.

If this feature has been enabled by your administrator, you are given the option to disable it on your own device. Keep in mind that this feature is provided for you convenience, automatically connecting and disconnecting the VPN so that you do not have to do so manually. Enable TND to reinstate this functionally.

TND does not interfere with your ability to manually establish a VPN connection or disconnect a VPN connection started while on a trusted network. TND disconnects the VPN session only if the device first connects (automatically or manually) in an untrusted network and then moves into a trusted network.

Before You Begin

Trusted Network Detection requires the AnyConnect app to be running. If you have exited the application using **Menu** > **Exit** or forced the app to stop using the Android settings, AnyConnect will be unable to detect a trusted network.

Note The Trusted Network Detection feature is not available in the AnyConnect ICS+ package, the Android VPN Framework package. It is only available in the brand-specific and rooted AnyConnect packages.

Procedure

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

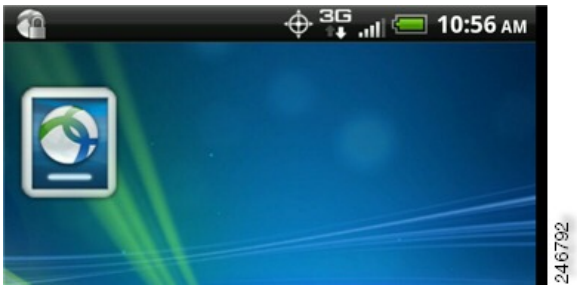
Step 2 Tap the **Trusted Network Detection** checkbox to enable or disable this preference.

Using AnyConnect Widgets

About 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.

Placing a Widget on your Android Home Window

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.

Related Topics

Viewing the AnyConnect Profile, on page 28
Importing an AnyConnect Profile, on page 29
Removing the AnyConnect Profile, on page 29

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.

Related Topics

About AnyConnect Client Profiles, on page 28

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.

Related Topics

About AnyConnect Client Profiles, on page 28

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.

Related Topics

About AnyConnect Client Profiles, on page 28

Managing Localization

About Android Device Localization

Installed Localization

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

- Czech (cs-cz)
- German (de-de)
- Latin American Spanish (es-co)
- Canadian French (fr-ca)
- Japanese (ja-jp)
- Korean (ko-kr)
- Polish (pl-pl)
- Simplified Chinese (zh-cn)

The displayed language is determined by the locale specified in **Settings** > **Language and Keyboard** > **Select locale**. 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.

AnyConnect UIs and messages are translated as soon as AnyConnect starts. The selected localization is noted as Active in the AnyConnect **Menu** > **Diagnostics** > **Localization Management** screen.

Importing Localization

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 e-mail, 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 Controlling External Use of AnyConnect, on page 25 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.

Restoring Localization

Restoring the use of the pre-loaded localization data from the AnyConnect package deletes all imported localization data. The restored language is chosen by matching the specified device locale to the installed localization data.

Managing Localization Data

Procedure

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

What to Do Next

- **Import Localization**: Import localization data from a specified server.
- **Restore Localization**: Restore default localization data.
- **Localization Files**: View the list of localization files.

Importing Localization Data from a Server

Procedure

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

Step 2 Tap **Import Localization**.

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**.

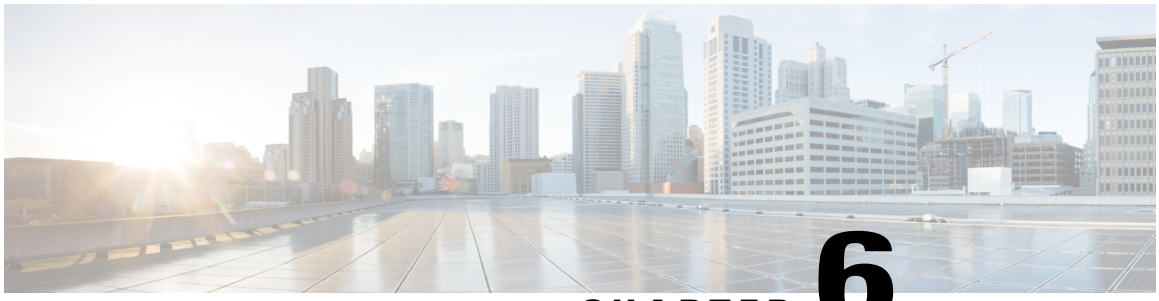
In the event that AnyConnect is unable to gracefully exit all of its processes, you will be detoured to the Android application management screen to manually terminate AnyConnect by tapping **Force Stop**.

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**.



CHAPTER 6

Monitoring and Troubleshooting AnyConnect

Displaying the AnyConnect Version and Licensing Details

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.

Viewing AnyConnect Statistics

AnyConnect records statistics when a VPN connection is present.

Procedure

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

Step 2 Tap **Details** to view more detailed statistics.

Statistic	Description
Secure Routes	Traffic destinations, as determined by the VPN secure gateway configuration, that go through the encrypted connection. AnyConnect displays each destination in the form IP address/subnet mask. An entry of 0.0.0.0/0.0.0.0 means that all VPN traffic is encrypted and sent or received over the VPN connection except for that which is specifically excluded.
Non-Secure Routes	Shown only if 0.0.0.0/0.0.0.0 is present under Secure Routes.Traffic destinations, as determined by the VPN secure gateway, that are excluded from the encrypted connection.

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 **Send Logs**.

The log messages and all profile data are packaged into a .zip file and inserted into an e-mail message. Use the e-mail 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 **Clear Debug Logs**.

Known Issues and Bugs

This release has the following known issues and bugs:

- AnyConnect blocks voice calls if it is sending or receiving VPN traffic over an EDGE connection because of the inherent nature of EDGE and other early radio technology.
- 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.

Common 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 e-mail logs because of a network connectivity issue

Try another Internet-accessible network. Save the log messages in a draft e-mail 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.