



User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.4.x for Android

Updated: September 15, 2011

Contents

This document describes the Cisco AnyConnect Secure Mobility Client 2.4.x for Android. It includes the following sections:

- [Introduction](#)
- [Features](#)
- [AnyConnect for Lenovo Device Requirements](#)
- [AnyConnect for Rooted Device Requirements](#)
- [AnyConnect for Samsung Device Requirements](#)
- [Installation and Upgrades](#)
- [What You Need Before You Connect](#)
- [Adding a VPN Connection Entry](#)
- [Connecting to a VPN](#)
- [Viewing the Connection Summary](#)
- [Using the AnyConnect Icon in the Status Bar](#)
- [Using the AnyConnect Widgets](#)
- [Viewing Overview Statistics](#)
- [Viewing Detailed Statistics](#)
- [Viewing and Managing Log Messages](#)
- [Modifying a VPN Connection Entry](#)
- [Deleting a Connection Entry](#)
- [Changing the Theme](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2004–2011 Cisco Systems, Inc. All rights reserved.

- [Displaying the AnyConnect Version and Licensing Details](#)
- [Responding to “Another Application has requested that AnyConnect...Do you want to allow this?”](#)
- [Known Issues and Bugs](#)
- [Troubleshooting](#)
- [Removing AnyConnect](#)
- [Licensing](#)

Introduction

The Cisco AnyConnect Secure Mobility Client 2.4.x for Android provides seamless and secure remote access to enterprise networks. The client lets any installed application communicate as though connected directly to the enterprise network.

The Android Market provides access to the installation app. You can install the app on all supported Samsung devices and on rooted Android devices.

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

Features

[Table 1](#) lists the features in AnyConnect 2.4.x for Android devices.

Table 1 ***AnyConnect 2.4.x for Android Features***

Feature	Description	Introduced in AnyConnect for Android Version
Control Launch on Startup	Allows the end-user to control if Android starts AnyConnect immediately when the mobile device starts up. The default behavior does not start AnyConnect on startup.	2.4.7073
Hide AnyConnect icon when idle	Allows users to determine if the AnyConnect icon should be shown or hidden when the mobile endpoint is not connected using AnyConnect. The configuration is accessible through the “Settings” button from the App menu. The default behavior is to hide the AnyConnect icon when not connected.	2.4.7073
Improved VPN Recovery	AnyConnect recovers its VPN connection more effectively when switching between networks.	2.4.7073

Table 1 **AnyConnect 2.4.x for Android Features**


Feature	Description	Introduced in AnyConnect for Android Version
IPv6 support for internal networks	Android users with a phone supporting IPv6 can now connect to a private network that assigns an IPv6 address and access network resources over IPv6.	2.4.7073
Quit AnyConnect	A new menu item allows users to disconnect AnyConnect.	2.4.7073
New icon indicating AnyConnect is “Paused”	Connection suspended due to lack of connectivity. 	2.4.7073
3G–WiFi roaming	AnyConnect maintains the VPN as users move between 3G and WiFi networks.	2.4.7030
AnyConnect widgets for home screen	Android widgets can be installed on the home screen for one-click VPN access.	2.4.7030
Application URI Handling	Lets other applications such as a web browser add VPN connection entries to the AnyConnect configuration, establish VPN connections, disconnect from a VPN, and import certificates. Your system administrator might choose to give you links to take advantage of this feature.	2.4.7030
Cisco AnyConnect VPN connection entries (AnyConnect user profile) import.	AnyConnect automatically imports available VPN connection profiles stored from the ASA when the device connects.	2.4.7030
Cisco SSL tunneling protocol and Cisco DTLS tunneling protocol	AnyConnect can establish a VPN connection using both Cisco SSL tunneling protocol and Cisco DTLS tunneling protocol.	2.4.7030
Email logs to AnyConnect administrator	Users can quickly email statistics, log messages and system information details to the AnyConnect system administrator for troubleshooting.	2.4.7030

Table 1 **AnyConnect 2.4.x for Android Features**

Feature	Description	Introduced in AnyConnect for Android Version
Multiple authentication methods	Authentication with username and password, group selection, pre-fill of usernames from a certificate, and double authentication. The configuration of the Cisco VPN secure gateway determines whether a certificate is required and, if so, supplies access to the certificate.	2.4.7030
Native Android alternative to the Cisco default user interface theme.	Users can configure an AnyConnect VPN connection using either the AnyConnect interface or the native Android VPN interface.	2.4.7030

AnyConnect for Lenovo Device Requirements

[Cisco AnyConnect for Lenovo](#), Release 2.4.x supports the Lenovo ThinkPad tablet product, provided the device is running the latest software update from Lenovo.

AnyConnect for Rooted Device Requirements

[Cisco AnyConnect for Rooted](#), Release 2.4.x, runs on most rooted devices running Android 2.1 or later. A rooted device is a requirement unless the device is a supported Samsung device.



Caution

Rooting your device could void your device warranty. We do 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.

The AnyConnect client download for Samsung does not work on rooted devices; you must use the rooted version of AnyConnect on rooted devices.

Both a tun.ko module and IP tables are required. AnyConnect displays an error message informing you about what is missing when you attempt to establish a VPN. 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.

AnyConnect for Samsung Device Requirements

Cisco AnyConnect for Samsung, Release 2.4.x, supports the following Samsung product lines, provided the devices are running the latest software update from Samsung:

- Galaxy S running Android 2.3.3 or later.
- Galaxy S II running Android 2.3.3 or later.
- Galaxy Tab 7 (WiFi only) running Android 2.3.3 or later.



Note We do not support the Sprint distribution of the Samsung Galaxy Tab 7 mobile device.

- Galaxy Tab 8.9 running Android 3.0 or later.
- Galaxy Tab 10.1 running Android 3.1 or later with Samsung TouchWiz updates.



Note

Samsung rebrands the devices in these product lines for each carrier.

Installation and Upgrades

To install or upgrade AnyConnect for Android, go to the Android Market for the app that matches the device:

- “Cisco AnyConnect for Samsung” for [supported Samsung devices](#).
- “Cisco AnyConnect for Rooted” for rooted devices running Android 2.1 or later.



Note

Cisco AnyConnect does not work on Android devices that do not meet one of these two criteria.

What You Need Before You Connect

You must obtain one or more of the following from your system administrator, depending on your network requirements, before you can set up AnyConnect to establish a VPN session:

- Server Address—Domain name, IP address, or optional group URL of the Cisco Adaptive Security Appliance to be used as the VPN secure gateway.
- Username and password—Credentials needed to access the VPN.
- Digital certificate.

Alternatively, your system administrator may supply a link on your corporate network that you can tap to add the required connection entries to your device.

Adding a VPN Connection Entry

Before attempting to establish a VPN connection for the first time, add a VPN connection entry to identify the VPN secure gateway, as follows:

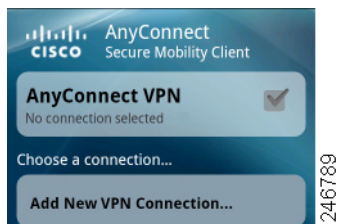
- Step 1** Tap the AnyConnect icon ([Figure 1](#)).

Figure 1 *AnyConnect Icon*



AnyConnect shows the VPN connection status in the AnyConnect home window ([Figure 2](#)).

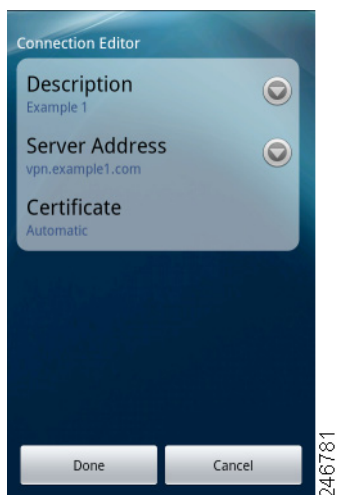
Figure 2 *AnyConnect Home (New Installation)*



- Step 2** Tap **Add New VPN Connection**.

The Add VPN Connection window shows the VPN connection parameters ([Figure 3](#)).

Figure 3 *Add VPN Connection with Example Values*



- Step 3** Tap a parameter field to assign a value.

Step 4 Complete the fields, as follows:

Description—Enter a unique name for the connection entry to appear in the connection list of the AnyConnect home window. You can use any letters, spaces, numbers, or symbols on the keyboard display. AnyConnect retains the letters in the upper- or lower-case letters you specify. For example,

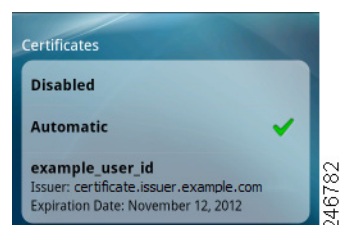
Example 1

Server Address—Enter the domain name, IP address, or Group URL of the Cisco Adaptive Security Appliance with which to connect. For example,

vpn.example.com

Certificate—(Optional, depending on VPN requirements) Your system administrator will provide you with instructions to install a certificate if one is necessary to establish a VPN session. You can tap Certificate to view summary details of any certificates enrolled on the device and to select one for use when establishing a VPN connection. The Certificates window displays the summary information for the installed certificates ([Figure 4](#)).

Figure 4 Example Certificate



The options are as follows:

- **Disabled**—Indicates that using a certificate is not an option.
- **Automatic**—Uses a certificate only if one is required by the security appliance.
- **List of individual certificates (for example, user_user_id)**—Tap the certificate your system administrator instructs you to use. The Certificate window reopens.

Step 5 Tap **Done** to save the connection values.

AnyConnect closes the Add VPN Connection window and adds the entry to the home window.

Connecting to a VPN

To establish a VPN connection,

Step 1 Ensure you have a Wi-Fi connection or a connection to your service provider.

Step 2 Go to the AnyConnect home window.

Step 3 Tap the connection entry to be used.

AnyConnect disconnects any VPN connection currently in use.

Step 4 If necessary, do either of the following in response to the appropriate prompts:

- Enter your credentials. If prompted to do so, also enter your secondary credentials to support double authentication.
- Tap **Get Certificate**, then enter the certificate enrollment credentials supplied by your system administrator. AnyConnect saves the certificate and reconnects to the VPN secure gateway to use the certificate for authentication.

The top row of the AnyConnect home window highlights the checkmark, indicating the VPN connection is established ([Figure 5](#)).

Figure 5 *AnyConnect Home (Connected)*



Depending on the VPN secure gateway setup, AnyConnect retrieves connection entries and adds them to the VPN connection list in the AnyConnect home window.



Caution

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 you tapped.

Viewing the Connection Summary

To display a summary view of a connected VPN session, tap the name in the AnyConnect home window associated with the connection under *Choose a connection*. [Figure 6](#) shows an example connection summary window.

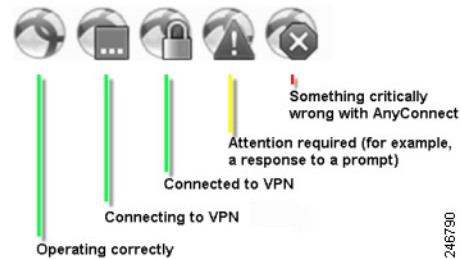
Figure 6 *Connection Summary*



Using the AnyConnect Icon in the Status Bar

By default, AnyConnect reveals its status by changing its icon in the Android status bar at the top of the Android windows (Figure 7).

Figure 7 *AnyConnect Notification Icons in Android Status Bar*



To reveal a text description of the status of AnyConnect, drag the status bar down. Then, to go to the AnyConnect home window, tap **AnyConnect**.

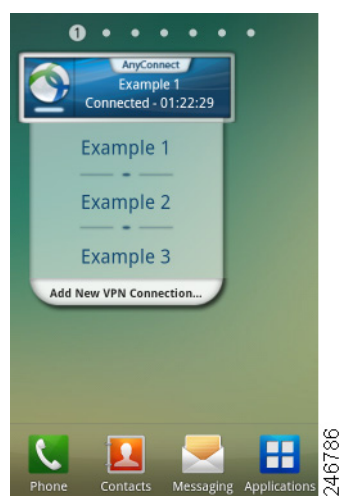
Using the AnyConnect Widgets

AnyConnect provides three optional widgets you can add to your home screen: large, medium, and small. The following sections show the widgets and describe how to place one on your Android home window.

Widget Descriptions

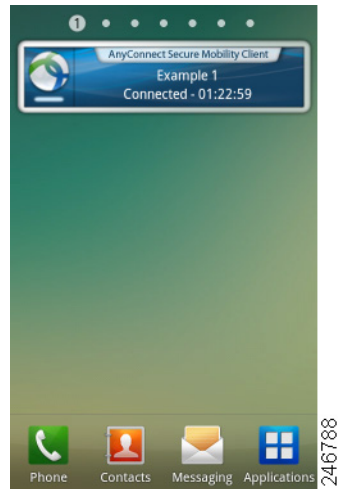
The large widget provides easy access to both the AnyConnect status information and controls. [Figure 8](#) shows how the large widget looks on the Android home window.

Figure 8 **Large Widget**



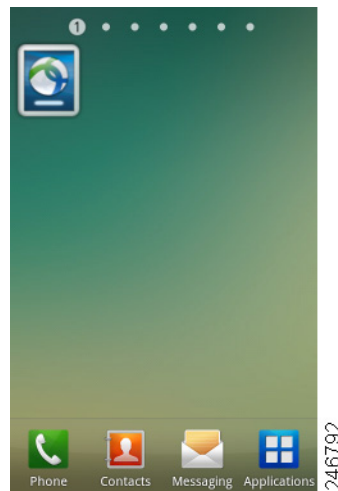
The large widget shows the AnyConnect icon, app name, default VPN secure gateway, and VPN status. It shows the name of the VPN secure gateway to which AnyConnect is connected or the default connection if it is not. The color of the bar below the icon reveals the VPN status. You can tap the icon to connect to or disconnect from the VPN secure gateway, tap a connection entry to disconnect and connect to the VPN secure gateway you chose, or tap **Add New VPN Connection** to specify connection details for a new VPN secure gateway.

[Figure 9](#) shows how the medium widget looks on the Android home window.

Figure 9 Medium Widget

The medium widget provides the same data as the large one, except for the list of connection entries. Tap the widget to connect to or disconnect from the VPN secure gateway indicated.

[Figure 10](#) shows how the small widget looks on the Android home window.

Figure 10 Small Widget

The small 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 default VPN secure gateway.

Placing a Widget on Your Android Home Window

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

-
- Step 1** Go to an Android home screen that has enough space for the widget.
 - Step 2** Tap or press the menu button.
 - Step 3** Tap **Add**.
 - Step 4** Tap **Widgets**.
 - Step 5** Tap the AnyConnect widget you want to use.
Android adds the widget to the home screen.
 - Step 6** Long-press the widget if you want to reposition it, then move it after it responds.
-

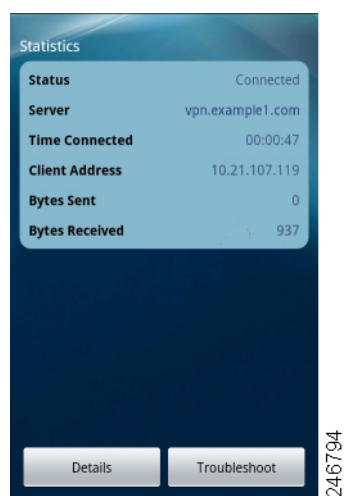
Viewing Overview Statistics

AnyConnect records statistics when a VPN connection is present.

To view the overview statistics for the current VPN connection,

-
- Step 1** Go to the AnyConnect home window.
 - Step 2** Tap or press the **Menu** button.
 - Step 3** Tap **Statistics**.
The Statistics Overview window opens ([Figure 11](#)).

Figure 11 **Statistics Overview**



The Statistics window displays the following:

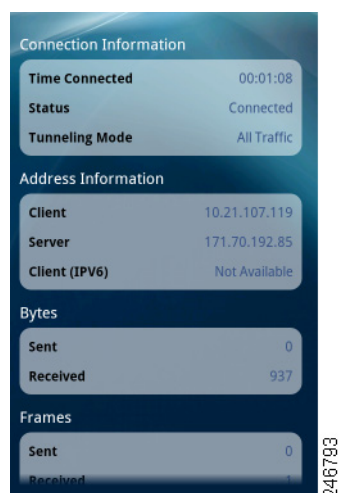
- Status (of the VPN connection).
- Server (address).
- Time Connected.
- Client Address.
- Bytes Sent.
- Bytes Received.
- **Details**—Tap to view detailed statistics (described in the next section).
- **Troubleshoot**—Tap to view the log files.

Viewing Detailed Statistics

To view the detailed statistics for the current VPN connection,

- Step 1** Go to the AnyConnect home window.
 - Step 2** Tap or press the **Menu** button.
 - Step 3** Tap **Statistics**.
 - Step 4** The Statistics window opens.
 - Step 5** Tap **Details**.
- The Detailed Statistics window opens ([Figure 12](#)).

Figure 12 *Detailed Statistics*



- Step 6** Scroll down to see the remaining statistics.

The Detailed Statistics window shows the following:

- Connection Information
 - Time Connected
 - Status
 - Tunneling Mode
 - Address Information
 - Client
 - Server
 - Client (IPv6)
 - Bytes
 - Sent
 - Received
 - Frames
 - Sent
 - Received
 - Control Frames
 - Sent
 - Received
 - Transport Information
 - Protocol
 - Cipher
 - Compression
 - Feature Configuration: FIPS Mode
 - 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.
-

Viewing and Managing Log Messages

To view, send, or clear AnyConnect log messages:

Step 1 Go to the AnyConnect home window.

Step 2 Tap or press the **Menu** button.

Step 3 Tap **Statistics**.

Step 4 The Statistics window opens.

Step 5 Tap **Troubleshoot**.

AnyConnect retrieves its messages from Android and displays them in the Messages window (Figure 13).

Figure 13 Messages



Use this window to do any of the following:

- **Messages**—Tap to display the log messages.
- **System**—Tap to display the following types of AnyConnect information: memory, interface, route, filter (collected for Samsung only), permissions, process, system properties, memory map,
- **Debug**—Tap to display the log messages used by system administrators and the Cisco Technical Assistance Center (TAC) to analyze AnyConnect issues.
- **Send Logs**—Tap to package the log messages and all profile data into a .zip file to insert it into an email message or use Bluetooth to transmit it locally. Bluetooth must be enabled on both the sending and receiving devices first. Use the email option to send the log files to your system administrator if you are reporting a problem with AnyConnect.
- **Clear Debug Logs**—Tap to remove all messages.

Step 6 Scroll the window to view additional messages.

Modifying a VPN Connection Entry

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

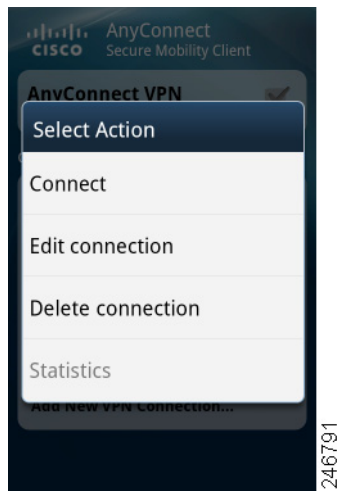

Note

You cannot modify the description or server address of connection entries pushed by a VPN secure gateway.

To modify a connection entry:

- Step 1** Open the AnyConnect home window.
- Step 2** Long-press the VPN connection entry to be modified.
AnyConnect displays the Select Action window ([Figure 14](#)).

Figure 14 **Select Action**



- Step 3** Tap **Edit connection**.
The Connection Editor window displays the parameter values assigned to the connection entry.
- Step 4** Tap the value to be modified, use the on-screen keyboard to enter the new value, and tap **OK**.
For parameter instructions, use the online help or go to “[Adding a VPN Connection Entry](#).”
- Step 5** Tap **Done**.
AnyConnect saves the entry and reopens the AnyConnect window.

Deleting a Connection Entry

AnyConnect provides two procedures for deleting a connection entry, depending on whether you added it or a VPN secure gateway added it.

Deleting a Connection Entry You Added

To permanently delete a VPN connection entry you added manually:

-
- Step 1** Open the AnyConnect home window.
- Step 2** Long-press the VPN connection entry to be modified.
AnyConnect displays the Select Action window.
- Step 3** Tap **Delete connection**.
AnyConnect removes the entry and reopens the AnyConnect window.
-

Clearing all AnyConnect Data

The only way to remove a connection entry imported from a VPN secure gateway is to clear all of the AnyConnect connection entries from the device.



Caution

If you clear all AnyConnect data, all certificates, connection entries, and profile data will need to be created or imported again.

To clear all data, go to the Android home window and tap **Applications > Settings > Applications > Manage Applications > AnyConnect > Clear Data**.

Changing the Theme

AnyConnect provides the following themes:

- Cisco Default Theme (default)—Color contrast, emphasizing shades of blue, similar to the AnyConnect on Apple iOS interface.
- 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.

To change the theme of the AnyConnect user interface,

-
- Step 1** Go to the AnyConnect home window.
- Step 2** Tap or press the AnyConnect menu button.

- Step 3** Tap **Settings**.
- Step 4** Tap **Application Style**.
AnyConnect shows a green button next to the theme currently in use.
- Step 5** Tap the theme you want.
-

Displaying the AnyConnect Version and Licensing Details

To display a link to the online version of this guide, the AnyConnect version running on your device, and the copyright and licensing information,

- Step 1** Go to the AnyConnect home window.
- Step 2** Tap or press the **Menu** button.
- Step 3** Tap **About**.
AnyConnect displays the About window.



Tip Tap the link in the About window to open the latest updated version of this guide. Use the link as a resource if you need to use these instructions at a later time.

Responding to “Another Application has requested that AnyConnect...Do you want to allow this?”

To protect your device, AnyConnect alerts you when another application attempts to add a set of connection entries, import certificates, establish a VPN connection, or disconnect from a VPN. Please ask your system administrator whether to tap **Yes** in response to the following prompts:

- **Create**—Another application has requested that AnyConnect create a new connection to *host*. Do you want to allow this? [Yes or No]
- **Import**—Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store. Do you want to allow this? [Yes or No]
- **Connect**—Another application has requested that AnyConnect connect to *host*. Do you want to allow this? [Yes or No]
- **Disconnect**—Another application has requested that AnyConnect disconnect the current connection. Do you want to allow this? [Yes or No]

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 per the inherent nature of EDGE and other early radio technology.
- If a VPN connection is established over Wi-Fi and DHCP renews the IP address of the device, its media connection to the LAN breaks, but the control connection does not. To recover, disable and re-enable Wi-Fi.
- Android security filtering rules prevent the device from sending and receiving messages containing attachments, called *multimedia messaging service (MMS) messages*, while a VPN connection is up. Android displays an error message if you try to send an MMS message while the VPN connection is up, but does not notify you about a failure to receive one. Android permits the waiting MMS messages to be sent or received when the VPN connection ends.

Troubleshooting

This section describes solutions to common problems. If you try a solution and the problem persists, contact your system administrator.

- **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 system administrator set a policy that prevents the modification and removal of host entries imported from a VPN secure gateway. The only way to remove them is to [clear all AnyConnect data](#).

- **Connection time-outs and unresolved hosts.**

Internet connectivity issues, a low cell signal level, and a congested network resource are typical causes of time-outs and unresolved host errors. Try moving to an area with a stronger signal or use Wi-Fi. 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 time-outs 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, then tap **Certificate**. The Certificates window lists all certificates. Long-press the certificate name, then tap **View Certificate Details**. Check with your system administrator to make sure you are using the appropriate certificate for the connection.

- **Need to view available certificates on the device**

To view all the certificates imported by AnyConnect, go to the AnyConnect home window, tap **Add New VPN Connection**, then tap **Certificate**. The Certificates window lists all certificates. To see the details of a certificate, long-press the certificate name, then tap **View Certificate Details**.

- **Error connecting, device working OK**

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

- **Cannot connect to ASA, unresolvable host error**

Use the Internet browser to check the network connection. Try using the browser to go to <https://vpn.example.com>, where vpn.example.com is the URL of the VPN secure gateway to verify connectivity.

- **AnyConnect package fails to install from the Market**

Ensure that the device is rooted or is listed as a [supported Samsung device](#).

- **“Installation Error: Unknown reason -8”**

If users attempt to install AnyConnect on devices that are not supported, they receive this message. Ensure that the device is rooted or is listed as a [supported Samsung 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. It must be rooted or listed as a [supported Samsung device](#).

- **Problem: Need to view current AnyConnect VPN profile**

AnyConnect includes the current profile when you [email the logs](#).

- **Need to view device IMEI (Unique ID)**

Go to **Applications > Settings > About Phone -> Status**.

- **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.

Removing AnyConnect

To remove AnyConnect from the device, go to **Settings > Applications > Manage applications > AnyConnect**, then tap **Uninstall**.

Licensing

For our open source licensing acknowledgements, see [Open Source Used in Cisco AnyConnect Secure Mobility Client, Release 2.4 for Android](#).

For the end-user license agreement, see [End User License Agreement](#).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2004-2011 Cisco Systems, Inc. All rights reserved.