Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.5.x

Updated: September 10, 2012

This document describes the Cisco AnyConnect Secure Mobility Client 2.5.x for Android. It includes the following sections:

- Introduction
- Installing or Upgrading AnyConnect
- Supported Android Devices
- Getting Started with AnyConnect
- Connecting to a VPN
- Managing AnyConnect on your Android Device
- Responding to AnyConnect Notifications
- Obtaining AnyConnect Information
- Troubleshooting

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

Introduction

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 or Upgrading AnyConnect

Go to the Android Market to search for and obtain the appropriate AnyConnect package for your particular device:

Note Your device must have network connectivity via WiFi or 3G to initiate and complete installation of the AnyConnect application.

If Your Device	Install
Is one of the Supported Android Devices, Cisco provides brand-specific AnyConnect packages that offer full-featured VPN connections for the Android OS. These brand-specific AnyConnect clients are provided in partnership with device vendors and are the preferred AnyConnect clients for supported devices.	The brand-specific AnyConnect client: • For Samsung devices see Determining Which Samsung AnyConnect Package to Install. • For HTC devices see AnyConnect for HTC Devices. • For Lenovo devices install Lenovo AnyConnect 2.5.5125. • For Motorola devices install Motorola AnyConnect 2.5.5125. • For Kindle devices install Cisco AnyConnect Release 2.5.5125

If Your Device	Install
Is running Android 4.0 (Ice Cream Sandwich) or later, Cisco provides an AnyConnect client that 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.	AVF AnyConnect 2.5.51125. **Note**: Cisco recommends the AnyConnect AVF client for unsupported devices running Android 4.0 or later. Supported devices should use the brand-specific AnyConnect client regardless of the Android OS version.
Is rooted and running Android 2.1 or later, Cisco provides an AnyConnect package for rooted Android mobile devices for preview and testing purposes only. Cisco does not support this client. but it works on most rooted devices running 2.1+. 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.	Rooted AnyConnect 2.5.5125. **Caution:** Rooting your device could void your device warranty. Cisco does not officially 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.

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

Determining Which Samsung AnyConnect Package to Install

Cisco provides two AnyConnect packages for compatibility with Samsung devices:

- The Samsung AnyConnect 2.5.5131 package applies to devices produced or upgraded after September 2011.
- The Samsung AnyConnect Legacy 2.5.5125 package applies to older devices (produced before September 2011) that have 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."

Android Device Localization

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)

Localization data for these languages is installed on the Android device when AnyConnect is installed. 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 > Settings > Localization Management** screen.

See Managing Localization for localization activity and options post-installation.

Android AnyConnect Licensing

For our open source licensing acknowledgements, see *Open Source Used in Cisco AnyConnect Secure Mobility Client, Release 2.5 for Android*.

For the end-user license agreement, see *End User License Agreement*.

Supported Android Devices

AnyConnect supports devices from the following manufacturers:

- AnyConnect for Samsung Devices
- AnyConnect for HTC Devices
- AnyConnect for Lenovo Devices
- AnyConnect for Motorola Devices
- AnyConnect for Kindle Devices

Cisco also provides:

- AnyConnect for Android VPN Framework Devices
- AnyConnect for Rooted Devices

AnyConnect for Samsung Devices

Samsung AnyConnect Release 2.5.5131 and Samsung AnyConnect Legacy Release 2.5.5125 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 installation instructions in the AnyConnect for Android User Guide to determine which package applies to your device.

Product	Android Release	Model Numbers
ACE+		GT-S7500 GT-S7500L GT-S7500W
Galaxy Beam		GT-I8530
Galaxy Note		GT-N7000 GT-I9220
Galaxy Mini		GT-S5570 GT-S5570B GT-S5570BD1 GT-S5570L GT-S5578 SCH-I559 SGH-T499 SGH-T499V SGH-T499Y

Product	Android Release	Model Numbers
Galaxy S	2.3.3 or later	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-I9088 GT-I9070 GT-I9070P SC-02B SCH-I400 SCH-I405 SCH-I500 SCH-I809 SCH-I909 SGH-I896 SGH-I897 SGH-I927 SGH-I997R SGH-N013 SGH-T759 SGH-T959 SGH-T959D SGH-T959P SGH-T959V SGH-T959W SHW-M100S SHW-M110S SHW-M130K SHW-M130L SHW-M190S SHW-M220L' SHW-M340K SHW-M340L SHW-M340S SPH-D720

Product	Android Release	Model Numbers
Galaxy S II	2.3.3 or later	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-J001 SCH-W999 SGH-I727 SGH-I727R SGH-I757M SGH-I777 SGH-N033 SGH-N034 SGH-T989 SHV-E110S SHV-E120K SHV-E120L SHV-E120S SHW-M250K SHW-M250L SHW-M250S SPH-D170
Galaxy S III	4.0 or later	GT-I9300 SCH-I535 SGH-I747 SGH-T999 SPH-L710
Galaxy Tab 7 (WiFi only)[1]	2.3.3. or later	GT-P1000 GT-P1000M GT-P1000R GT-P1010 SC-01C SCH-I800
Galaxy Tab 7.0 Plus		GT-P6200 GT-P6210
Galaxy Tab 7.7		GT-P6800 SCH-I815
Galaxy Tab 8.9	3.0 or later	GT-P7300 GT-P7310

Product	Android Release	Model Numbers
Galaxy Tab 10.1	3.1 or later with Samsung Touch Wiz updates	GT-P7300 GT-P7310 GT-P7500 GT-P7500D GT-P7500M GT-P7500R GT-P7510 SC-01D
Galaxy W		GT-I8150 SGH-T679
Galaxy Xcover		GT-S5690
Galaxy Y Pro		GT-B5510B GT-B5510L
Illusion		SCH-I110
Infuse		SCH-I997
Stratosphere		SCH-I405

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

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

AnyConnect for HTC Devices

HTC AnyConnect Release 2.5.5125 supports the HTC product lines listed at http://www.htcpro.com/enterprise/VPN, if they are running Android release 2.1-3.0 (Eclair-Honeycomb). These devices must be running the minimum software required as shown in the table. Go to **Settings > About phone > Software information > Software number** to determine the software number running on your device.

AnyConnect ICS+ Release 2.5.5125 must be used on the following HTC devices if they are running, or have been upgraded to, Android 4.0 (Ice Cream Sandwich) or later. If the HTC device was upgraded while HTC AnyConnect was installed, uninstall the HTC AnyConnect app and restart the device before downloading the AnyConnect ICS+ app.

- HTC Rhyme S510b
- HTC ADR6330VW
- HTC Vivid
- HTC EVO Design 4G
- HTC ThunderBolt ADR6400L
- HTC Sensation XE
- HTC Sensation
- HTC Amaze 4G
- HTC Sensation XL with Beats Audio
- HTC EVO 3D

- HTC EVO 3D
- HTC EVO 3D X515m
- HTC X515d
- HTC ADR6425LVW

The HTC Raider, also know as the HTC Holiday, does not work with Cisco AnyConnect. Cisco and HTC are working to address this issue, and on allowing the HTC AnyConnect app to work on all HTC devices, regardless of the Android release they are running.

AnyConnect for Lenovo Devices

Lenovo AnyConnect Release 2.5.5125 supports the Lenovo ThinkPad tablet product, provided the device is running the latest software update from Lenovo.

AnyConnect for Motorola Devices

Motorola AnyConnect Release 2.5.5125 supports the following Motorola product lines, provided the devices are running the latest software update from Motorola:

Product	Minimum Software Required
ATRIX 2	55.13.25
XYBOARD	
RAZR	6.12.173
RAZR MAXX	6.12.173
DROID 4	6.13.215

AnyConnect for Kindle Devices

Cisco AnyConnect Release 2.5.5125 is available from Amazon for the Kindle Fire HD devices, and the New Kindle Fire, these products will be shipping mid-September 2012. Anyconnect for Kindle is supported by the Android VPN Framework and is equivalent in functionality to the AnyConnect ICS+ package.

AnyConnect for Android VPN Framework Devices

AnyConnect ICS+ Release 2.5.5125 offers VPN connectivity supported by the Android VPN Framework (AVF) in Android 4.0 (Ice Cream Sandwich) 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.

Note Cisco recommends the AnyConnect AVF 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.

AnyConnect for Rooted Devices

Cisco provides Rooted AnyConnect Release 2.5.5125 for rooted Android mobile devices running Android 2.1 or later, for preview and testing purposes only. Cisco does not support this client, but it works on most rooted devices running 2.1+. If you encounter issues, please report them to android-mobile-feedback@cisco.com, 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.

Caution Rooting your device could void 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.

Getting Started with AnyConnect

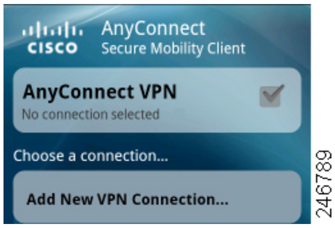
The AnyConnect Home Screen

When you tap the AnyConnect application icon (Figure 1),

Figure 1 AnyConnect Icon

the initial AnyConnect home screen opens (Figure 2).

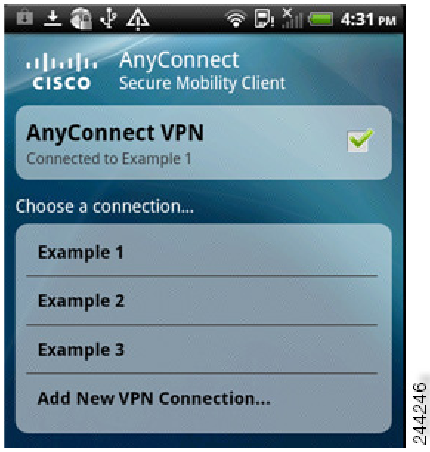
Figure 2 AnyConnect Home Screen



- **AnyConnect VPN**: Identifies the current VPN connection entry. The check box indicates if the connection is active or idle. Tap the AnyConnect VPN area to connect or disconnect this VPN.
- **Choose a connection...**: After connection entries have been added, this area lists all the configured VPN connection entries from which you can choose. This list includes both XML profile defined entries and entries you configured. Tap a connection to make it the current VPN and initiate connectivity.
- **Add New VPN Connection**: Manually define a connection entry. Tap this to enter the Description, Server Address, and Certificate policy for a connection.

After connection entries have been added, the AnyConnect home screen displays them (Figure 3):

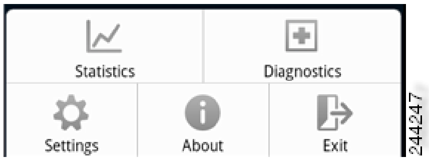
Figure 3 AnyConnect Connection Entries



The AnyConnect Menu

Tap or press Menu to see the AnyConnect Menu options (Figure 4):

Figure 4 AnyConnect Menu

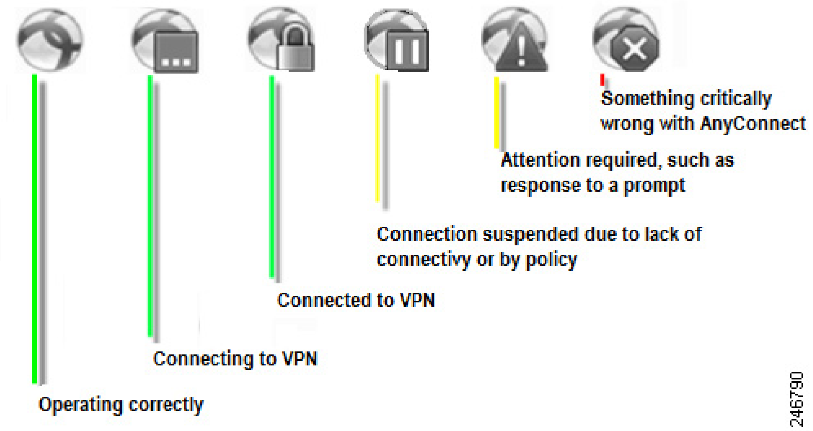


- **Statistics**: View overview and detailed statistics about the current active VPN connection. See Viewing Statistics for more information.
- **Diagnostics**: View, send and clear AnyConnect log messages. See Viewing and Managing Log Messages for more information.
- **Settings**: Specify application preferences and manage aspects of AnyConnect configuration. See Managing AnyConnect on your Android Device for more information.
- **About**: View AnyConnect version and license information. See Displaying the AnyConnect Version and Licensing Details for more information.
- **Exit**: Terminate AnyConnect.

Understanding 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 5).

Figure 5 AnyConnect Notification Icons in Android Status Bar


Something critically wrong with AnyConnect
Attention required, such as response to a prompt
Connection suspended due to lack of connectivy or by policy
Connected to VPN
Connecting to VPN
Operating correctly
246790

What You Need Before You Connect

You must have a connection entry defined on your device to initiate a VPN connection.

To configure a connection entry manually, you must obtain one or more of the following, depending on your network requirements, from your administrator. Use this information when Adding a VPN Connection Entry.

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

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

Connecting to a VPN

You connect to a VPN by selecting one of the connection entries listed in the AnyConnect home screen. The list of connections consists of entries created in one of the following ways:

- Manually configured connection entries. See Adding a VPN Connection Entry for how to add connection entries.
- Connection entries added after clicking on a link provided by administrators of your corporate network.
- Connection entries defined in the current AnyConnect XML profile, downloaded from the secure gateway upon VPN connectivity.

Adding a VPN Connection Entry

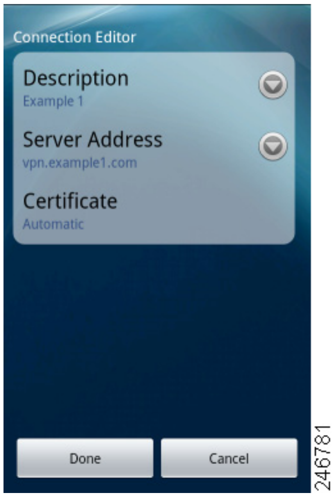
Before attempting to establish a VPN connection for the first time, add a VPN connection entry to identify the VPN secure gateway, as follows:

Step 1 Tap the AnyConnect icon.

Step 2 On the AnyConnect home screen tap **Add New VPN Connection**.

The Add VPN Connection window shows the VPN connection parameters (Figure 6).

Figure 6 ***Add VPN Connection with Example Values***



Connection Editor

Description
Example 1

Server Address
vpn.example1.com

Certificate
Automatic

Step 3 Tap a parameter field to assign a value.

Step 4 Complete the fields, as follows:

Description—(Optional, defaults to Server Address) Enter a unique name for the connection entry to appear in the connection list of the AnyConnect home screen. 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,

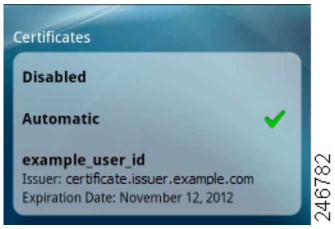
```
Example 1
```

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

```
vpn.example.com
```

Certificate—(Optional, depending on VPN requirements) Your administrator will provide you with instructions for Installing a Certificate on Your Mobile Device if one is necessary to establish a VPN session. You can tap a Certificate to view 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 7).

Figure 7 Example Certificate



Certificates

Disabled

Automatic ✓

example_user_id
Issuer: certificate.issuer.example.com
Expiration Date: November 12, 2012

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 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.

Installing a Certificate on Your Mobile Device

In order to authenticate your device to the secure gateway using a certificate, you need to import a certificate onto your device and then associate that certificate with a connection entry. A certificate can be imported in the following ways:

- Importing Certificates From Hyperlinks
- Importing Certificates using SCEP
- Importing Certificates Manually

See Viewing and Managing Certificates for additional certificate activities.

Importing Certificates From Hyperlinks

Your administrator can provide you a hyperlink to the location of a certificate that you can install on your device.

Note You need to set External Control to either Prompt or Enable within the AnyConnect settings to allow this activity. See Controlling External Use of AnyConnect for more information.

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 you are prompted, provide the authentication code for the certificate that was provided to you.

Importing Certificates using SCEP

Your administrator can configure a connection entry that distributes certificates using the SCEP protocol. Your AnyConnect administrator needs to provide you with the name of the VPN configuration entry that uses this method.

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, and enter your username and password.

The secure gateway downloads the certificate to your device. Your VPN session is disconnected. You then receive the message that certificate enrollment was successful, and you need to manually assign the certificate to a group.

Importing Certificates Manually

Your administrator can provide you with a certificate file to be installed on your device:

Step 1 Go to the AnyConnect home window.

Step 2 Tap or press the AnyConnect menu button.

Step 3 Tap **Settings.**

Step 4 Tap **Certificate Management**.

Step 5 Tap the **AnyConnect** tab.

Step 6 Import a certificate from the file system by tapping the **Import** button and selecting a certificate file from the local file system.

Note A certificate file must be present on the Android device to manually import a certificate in this way.

Establishing 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.

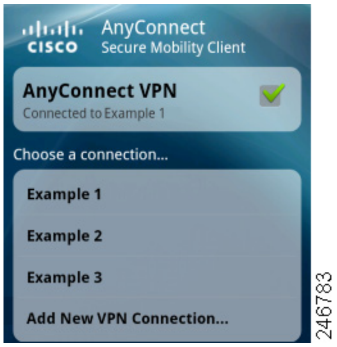
AnyConnect disconnects any VPN connection currently in use.

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

- Enter your credentials. If your administrator has configured double authentication you may also be prompted for secondary credentials.
- Tap **Get Certificate**, then 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.

The top row of the AnyConnect home window highlights the checkmark, indicating the VPN connection is established (Figure 8).

Figure 8 AnyConnect Home (Connected)



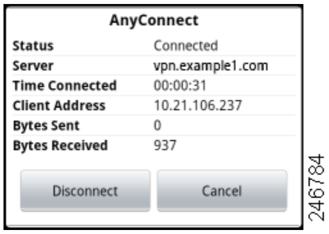
Depending on the VPN secure gateway configuration, AnyConnect may add connection entries to the list in the AnyConnect home window.

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 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 current connection under `Choose a connection`. Figure 9 shows an example connection summary window.

Figure 9 Connection Summary



AnyConnect

Status	Connected
Server	vpn.example1.com
Time Connected	00:00:31
Client Address	10.21.106.237
Bytes Sent	0
Bytes Received	937

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.

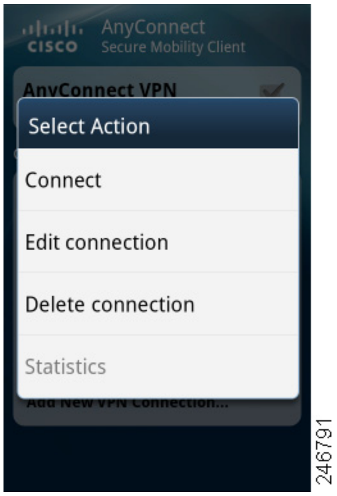
To modify a connection entry:

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 10).

Figure 10 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 see 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 Other Connection Entries

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 by deleting the current AnyConnect XML profile.

Step 1 Open the AnyConnect home window.

Step 2 Tap the Menu button.

Step 3 Tap **Settings.**

Step 4 Tap **Profile Management.**

Step 5 Tap **Delete Profile**.

Step 6 **Confirm** this deletion.

Managing AnyConnect on your Android Device

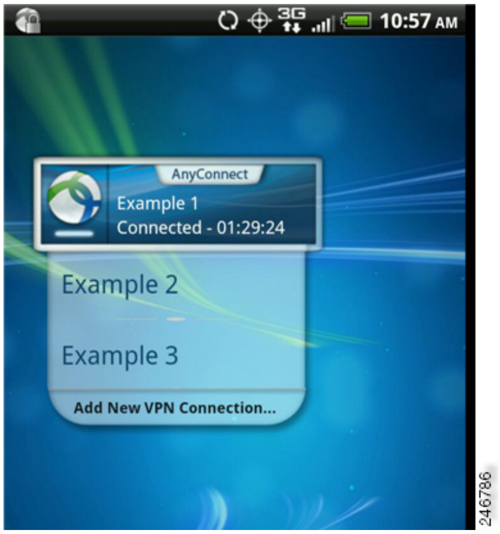
Using the AnyConnect Widgets

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 11 shows how the large widget looks on the Android home window.

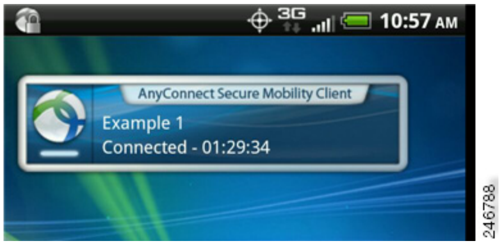
Figure 11 Large Widget



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 12 shows how the medium widget looks on the Android home window.

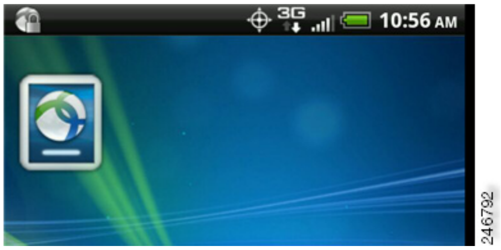
Figure 12 Medium Widget



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 13 shows how the small widget looks on the Android home window.

Figure 13 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 **Personalize**.

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.

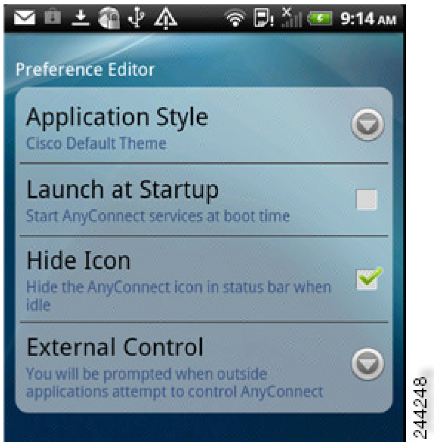
Specifying Application Preferences

Step 1 Go to the AnyConnect home window.

Step 2 Tap or press the AnyConnect menu button.

Step 3 Tap **Settings** (Figure 14):

Figure 14 AnyConnect Application Preferences



Preference Editor

Application Style
Cisco Default Theme

Launch at Startup □
Start AnyConnect services at boot time

Hide Icon ☑
Hide the AnyConnect icon in status bar when idle

External Control
You will be prompted when outside applications attempt to control AnyConnect

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.

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.

Launching AnyConnect at Startup

You have control over when AnyConnect launches on your device. By default, AnyConnect does not automatically launch at device startup. To change this setting and launch AnyConnect at device startup,

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 Preferences.**

Step 5 Tap the **Launch at Startup** check box.

If left unchecked, AnyConnect will not launch until the you start it.

Note **Launch at Startup** will be automatically enabled if a profile specifying Trusted Network Detection is downloaded or imported.

Hiding the AnyConnect Status Bar Icon

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

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 Preferences.**

Step 5 Tap the **Hide Icon** check box.

If left unchecked, the icon persistently displays.

Controlling External Use of AnyConnect

You can specify how AnyConnect responds to requests from external applications. These external requests can create connection entries, connect or disconnect a VPN, and import client profiles, certificates, or localization files. These external requests are URIs, typically provided by your administrator in emails or on web pages.

The External Control application preference specifies how the AnyConnect application responds to these external URI requests:

- **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 clicked on the device. You can allow or disallow the URI request. See Responding to "Another Application has requested that AnyConnect...Do you want to allow this?" section for notification and prompt details.

To specify how you want to control external URI requests:

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 Preferences.**

Step 5 Tap **External Control**

Step 6 Tap **Enabled, Disabled** or **Prompt**.

Viewing and Managing Certificates

You can view system certificates and view or manage certificates in the AnyConnect certificate store in the **Menu > Settings > Certificate Management** activity screen. This screen contains two tabs, one for the Android System certificate store, and one for the AnyConnect certificate store.

- On the **System** tab, you can browse certificates in the System store and view details of each certificate.

Note You cannot import or delete a system certificate, you can only view certificates in the System store.

- On the **AnyConnect** tab, you can browse imported certificates and view the details of each one, delete individual certificates, or delete all certificates in the AnyConnect certificate store, and manually import certificates.

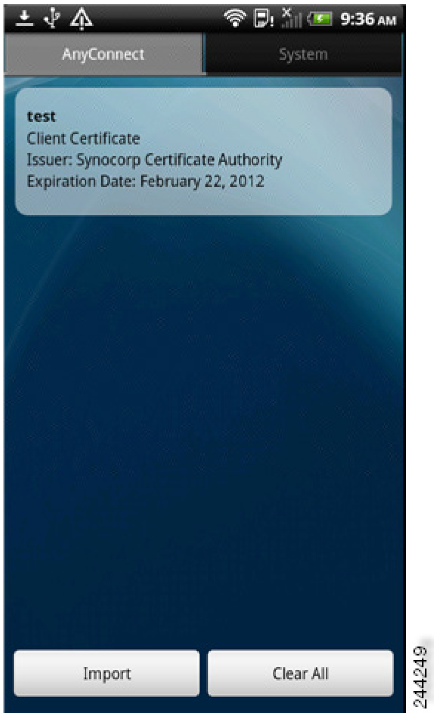
Step 1 Go to the AnyConnect home window.

Step 2 Tap or press the AnyConnect menu button.

Step 3 Tap **Settings.**

Step 4 Tap **Certificate Management** (Figure 15).

Figure 15 AnyConnect Certificate Management Screen



test
Client Certificate
Issuer: Synocorp Certificate Authority
Expiration Date: February 22, 2012

Step 5 Tap the **System** tab to view all certificates in the Android System store. You can long press a certificate and choose **View certificate details** to see the contents of a certificate.

Step 6 Tap the **AnyConnect** tab to view all certificates in the AnyConnect certificate store. You can do the following:

- View certificate details by long pressing the certificate and choosing **View certificate details**.
- Delete a certificate by long pressing the certificate and choosing **Delete Certificate**.
- Clear all certificates from the AnyConnect certificate store by tapping the **Clear All** button.
- Import a certificate from the file system by tapping the **Import** button and selecting a certificate file from the local file system. A certificate file must be present on the Android device to manually import a certificate in this way.

See Installing a Certificate on Your Mobile Device for other certificate import methods.

Viewing and Managing the AnyConnect Profile

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 you configured locally on the device, are listed on the AnyConnect home screen to choose from when initiating a VPN connection.

Note 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 will replace the current profile with the imported profile.
- Upon startup of an automatic or manual VPN connection the new connection's profile will replace the current profile.
- If a VPN connection does not have a a profile associated with it, the existing profile will be deleted upon startup of that VPN.

You can view or delete the AnyConnect Profile currently on the device or import a new one:

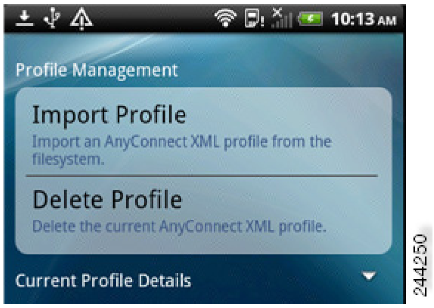
Step 1 Go to the AnyConnect home window.

Step 2 Tap or press the AnyConnect menu button.

Step 3 Tap **Settings.**

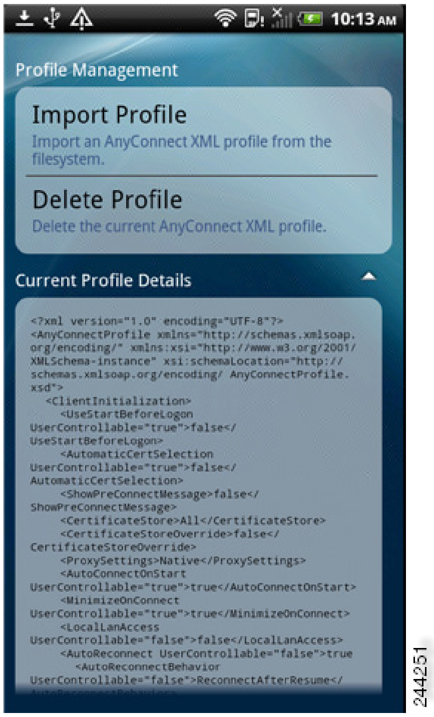
Step 4 Tap **Profile Management** (Figure 16).

Figure 16 AnyConnect Profile Management


10:13 AM
Profile Management
Import Profile
Import an AnyConnect XML profile from the filesystem.
Delete Profile
Delete the current AnyConnect XML profile.
Current Profile Details
244250

- Tap the expansion icon for the **Current Profile Details**. The XML file is displayed. Scroll down to see the whole file(Figure 17):

Figure 17 AnyConnect Profile Details



Profile Management

Import Profile

Import an AnyConnect XML profile from the filesystem.

Delete Profile

Delete the current AnyConnect XML profile.

Current Profile Details

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.
org/encoding/" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:schemaLocation="http://
schemas.xmlsoap.org/encoding/ AnyConnectProfile.
xsd">
   <ClientInitialization>
      <UseStartBeforeLogon
UserControllable="true">false</
UseStartBeforeLogon>
      <AutomaticCertSelection
UserControllable="true">false</
AutomaticCertSelection>
      <ShowPreConnectMessage>false</
ShowPreConnectMessage>
      <CertificateStore>All</CertificateStore>
      <CertificateStoreOverride>false</
CertificateStoreOverride>
      <ProxySettings>Native</ProxySettings>
      <AutoConnectOnStart
UserControllable="true">true</AutoConnectOnStart>
      <MinimizeOnConnect
UserControllable="true">true</MinimizeOnConnect>
      <LocalLanAccess
UserControllable="false">false</LocalLanAccess>
      <AutoReconnect UserControllable="false">true
         <AutoReconnectBehavior
UserControllable="false">ReconnectAfterResume</
```

- Tap **Delete Profile** and confirm to delete this current profile.

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

- 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 profiles' client specifications.

Managing Localization

Upon AnyConnect installation, your Android device is localized according to the device's locale specified in **Settings > Language and Keyboard > Select locale**. See Android Device Localization for the list of languages supported at installation time.

Caution Localization management on your Android device should be carried out based on instructions provided by your administrator.

Importing Additional Localization Data

After installation, localization data for languages not supported in the AnyConnect package can be 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 webpage, that imports localization data when clicked. This method uses the AnyConnect URI handler, a feature available to administrators for simplifying AnyConnect configuration and management for the user.

  Note You need to allow this AnyConnect activity by setting External Control to either Prompt or Enable within the AnyConnect settings. See Controlling External Use of AnyConnect 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.

- Using the **Server Localization Import** option on the AnyConnect Localization Management Activity Screen to manually import localization data from a specified server.

User Localization Management Activities

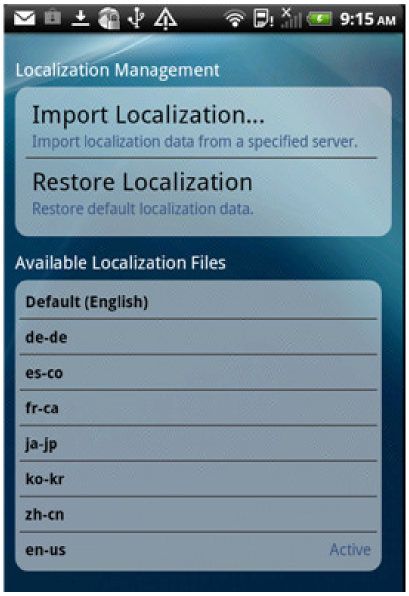
You can manage AnyConnect localization on the Localization Management screen:

Step 1 Go to the AnyConnect home window.

Step 2 Tap or press the AnyConnect menu button.

Step 3 Tap **Settings.**

Step 4 Tap **Localization Management:**



9:15 AM

Localization Management

Import Localization...
Import localization data from a specified server.

Restore Localization
Restore default localization data.

Available Localization Files

Default (English)
de-de
es-co
fr-ca
ja-jp
ko-kr
zh-cn
en-us Active

244252

- 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.
- 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.**

Removing AnyConnect

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

Obtaining AnyConnect Information

Viewing Statistics

AnyConnect records statistics when a VPN connection is present. To view the statistics for the current VPN connection,

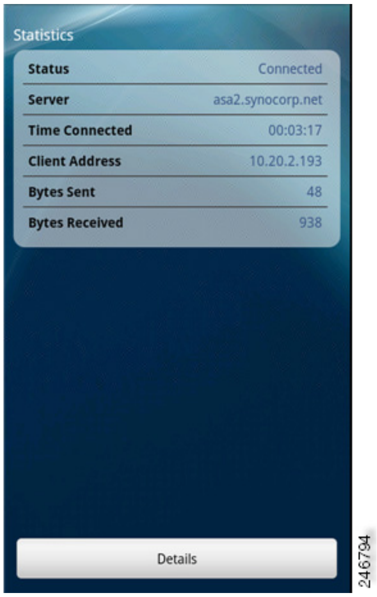
Step 1 Go to the AnyConnect home window.

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

Step 3 Tap **Statistics**.

The Statistics Overview window opens (Figure 18).

Figure 18 Statistics Overview



Statistics

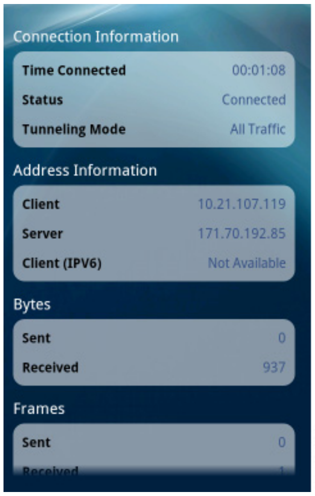
Status	Connected
Server	asa2.synocorp.net
Time Connected	00:03:17
Client Address	10.20.2.193
Bytes Sent	48
Bytes Received	938

The Statistics window displays the following:

- Status (of the VPN connection).
- Server (address).
- Time Connected.
- Client Address.
- Bytes Sent.
- Bytes Received.

- Tap **Details** to view detailed statistics (Figure 19).

Figure 19 Detailed Statistics



Connection Information

Time Connected	00:01:08
Status	Connected
Tunneling Mode	All Traffic

Address Information

Client	10.21.107.119
Server	171.70.192.85
Client (IPV6)	Not Available

Bytes

Sent	0
Received	937

Frames

Sent	0
Received	

Step 4 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

Use this procedure to view, send, or clear AnyConnect log messages:

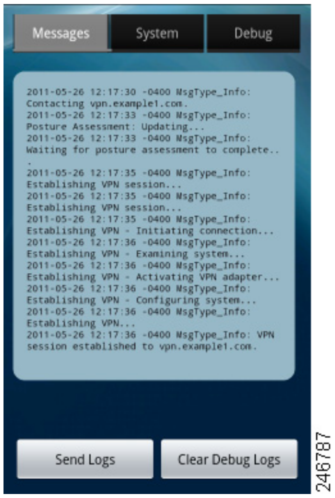
Step 1 Go to the AnyConnect home window.

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

Step 3 Tap **Diagnostics**.

AnyConnect retrieves its messages from Android and displays them in the Messages window (Figure 20).

Figure 20 Messages



```
2011-05-26 12:17:30 -0400 MsgType_Info:
Contacting vpn.example1.com.
2011-05-26 12:17:33 -0400 MsgType_Info:
Posture Assessment: Updating...
2011-05-26 12:17:33 -0400 MsgType_Info:
Waiting for posture assessment to complete..
.
2011-05-26 12:17:35 -0400 MsgType_Info:
Establishing VPN session...
2011-05-26 12:17:35 -0400 MsgType_Info:
Establishing VPN session...
2011-05-26 12:17:35 -0400 MsgType_Info:
Establishing VPN - Initiating connection...
2011-05-26 12:17:36 -0400 MsgType_Info:
Establishing VPN - Examining system...
2011-05-26 12:17:36 -0400 MsgType_Info:
Establishing VPN - Activating VPN adapter...
2011-05-26 12:17:36 -0400 MsgType_Info:
Establishing VPN - Configuring system...
2011-05-26 12:17:36 -0400 MsgType_Info:
Establishing VPN...
2011-05-26 12:17:36 -0400 MsgType_Info: VPN
session established to vpn.example1.com.
```

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, permissions, process, system properties, memory map, and unique device ID.

- **Debug**—Tap to display the log messages used by 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 administrator if you are reporting a problem with AnyConnect.
- **Clear Debug Logs**—Tap to remove all messages.

Step 4 Scroll the window to view additional messages.

Displaying the AnyConnect Version and Licensing Details

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 AnyConnect Notifications

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

To protect your device, AnyConnect alerts you when an external application attempts to add a connection entry, establish or disconnect a VPN connection, or import profiles, certificates or localization files. Ask your administrator whether to tap **Yes** in response to the following prompts:

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

- Localization files: `Another application has requested that AnyConnect import localization files. Do you want to allow this? [Yes | No]`
- Client Profiles: `Another application has requested that AnyConnect import profiles. Do you want to allow this? [Yes | No]`

Responding to MMS/HIPRI Notifications

While an AnyConnect VPN is connected you may be unable to retrieve or send Multimedia (MMS) messages, or use a High Priority (HPRI) service. This is dependent on the AnyConnect package version you are using, and your administrators configuration of the secure gateway,

If either activity is attempted and blocked by AnyConnect, the AnyConnect notification icon is displayed in the status bar. To acknowledge this notification,

Step 1 Click on the notification icon to view the AnyConnect notifications:

Step 2 Click on 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 notifications when MMS/HIPRI services are blocked.

Note Checking **Do not show this again** is a permanent selection. You cannot reverse this action in the future.

Step 4 Click **OK**.

Troubleshooting

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.
- Android security 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.

Addressing Common Problems

This section describes solutions to common problems. If you try a solution and the problem persists, contact your 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 administrator defined these connection entries in the AnyConnect Profile. See Viewing and Managing the AnyConnect Profile for instructions on deleting these profiles.

- **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 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 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 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 and tap or press the Menu button, then tap **Settings > Certificate Management**. 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 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 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.

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

  See Viewing and Managing the AnyConnect Profile.

- **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.

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.