Release Notes for Cisco AnyConnect Secure Mobility Client 2.5.x for Android Mobile Devices

Updated: September 10, 2012

This document includes the following sections:

- Introduction
- Supported Android Devices
- Changes in AnyConnect 2.5.5131
- Changes in AnyConnect 2.5.5125
- New Features in AnyConnect 2.5.5116 and 2.5.5118
- Android AnyConnect Feature Matrix
- Adaptive Security Appliance Requirements
- Known Issues and Limitations
- Troubleshooting
- Support Policy
- Licensing
- Related Documentation

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

Introduction

AnyConnect provides remote users with secure VPN connections to the Cisco ASA 5500 Series using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol. It also provides seamless and secure remote access to enterprise networks. The AnyConnect client provides a full tunneling experience that allows any installed application to communicate as though connected directly to the enterprise network.

This document, written for system administrators of AnyConnect Secure Mobility Client and the Adaptive Security Appliance (ASA) 5500, provides Android-specific information for the following 2.5.x releases of the Cisco AnyConnect Secure Mobility Client:

- Cisco AnyConnect Release 2.5.5131, available on
  - Samsung devices
- Cisco AnyConnect Release 2.5.5125, available on:
  - Samsung legacy devices
  - HTC devices
  - Lenovo devices
  - Motorola devices
  - Kindle devices
  - Android 4.0 (Ice Cream Sandwich) or later devices using the Android VPN Framework (AVF)
  - Rooted devices running Android 2.1 or later.

The Cisco AnyConnect for Android releases are available on the Android Market. The Android Market provides all AnyConnect Android distributions and updates.

Note For Android device requirements, installation instructions, and user information, see the *Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.5*.

This document supplements the *AnyConnect Administrators Guide*. You can deploy later releases of AnyConnect for other devices simultaneously with this release.

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.

Changes in AnyConnect 2.5.5131

No new features have been added to this release. See Issues Fixed in AnyConnect 2.5.5131for changes in this release.

Changes in AnyConnect 2.5.5125

No new features have been added to this release. See Issues Fixed in AnyConnect 2.5.5125 for changes in this release.

New Features in AnyConnect 2.5.5116 and 2.5.5118

- User Interface and Message Localization
- Trusted Network Detection (TND)
- Certificate Management
- Profile Management
- Mobile-Specific Additions to the AnyConnect VPN Client Profile
- Additional URI Handler Commands
- External Control of AnyConnect URI Commands
- AnyConnect Lifetime and Notification Enhancements

- Troubleshooting Improvements

User Interface and Message Localization

AnyConnect Secure Mobility Client, Release 2.5.x for Android, now supports localization, adapting the AnyConnect user interface and messages to the user's locale.

Pre-packaged 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.

Downloaded Localization

From the ASA

For languages not in the AnyConnect package, administrators can add localization data to the ASA that is downloaded to the Android device upon AnyConnect VPN connectivity. See Localizing the AnyConnect GUI for instructions on configuring localization on an ASA.

All localization data files matching the device's language specification are downloaded to the device. AnyConnect then determines the best match based on the region specification. The selected localization data is used for translation immediately, AnyConnect does not have to be restarted for it to take effect. Users have the option to restore installed localization data in the Localization Management screen.

If the ASA does not contain localization data for the device's locale, the installed localization data from the AnyConnect application package continues to be used.

URI Localization Support

An additional way to get localization data onto a user's device is for the administrator to provide the user with an AnyConnect URI for importing localization data. For example:

```
anyconnect://import?type=localization&host=asa.example.com&lang=ja-jp
```

See *Using the URI Handler to Automate AnyConnect Actions* in the AnyConnect Administrators Guide for a full explanation of using URIs to administer AnyConnect.

User Localization Management

Android users can manage localization data on their own device in the **Menu > Settings > Localization Management** screen. Users can perform these localization activities:

- Import localization data from a specified server. The user selects **Server Localization Import** and then specifies 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.
- Restore default localization data. Selecting **Restore Localization** restores the use of the pre-loaded localization data from the AnyConnect package and delete all imported localization data.

Trusted Network Detection (TND)

Trusted Network Detection (TND) is an AnyConnect feature that automatically disconnects or pauses the VPN connection when the Android device roams into a trusted network where a VPN is not required, and then automatically reconnects or resumes the VPN session when the user enters an untrusted network.

TND is configured in the AnyConnect Client Profile by administrators. See Configuring Trusted Network Detection in the AnyConnect Administrator Guide for details and procedures.

TND requires the AnyConnect application to be running on the Android device. Upon download of a profile specifying TND, **Launch at Startup**, an AnyConnect application preference, is automatically enabled to ensure this. If AnyConnect has been exited, TND cannot re-connect the VPN session on an untrusted network.

TND does not interfere with the ability of the user to manually establish a VPN connection while on a trusted network, and it does not disconnect such a connection. TND only disconnects or pauses the VPN session, complying with the configured policy, if the user connects in an untrusted network and then roams into a trusted network For example, TND disconnects or pauses the VPN session if the user makes a VPN connection at home and then moves into the corporate office.

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

Certificate Management

Android users now have the ability to view system certificates and manage certificates in the AnyConnect certificate store in the **Menu > Settings > Certificate Management** activity screen.

On the **System** tab, which shows root certificates used for verifying server certificates, the user can browse certificates in the System store and view details of each certificate by long pressing the certificate and choosing **View certificate details**.

On the **AnyConnect** tab, which shows the client certificates used for VPN authentication, the user can perform these tasks:

- Browse certificates in the AnyConnect store and view details of each certificate by long pressing the certificate and choosing **View certificate details**.
- Delete an individual certificate by long pressing the certificate and choosing **Delete certificate**.
- Import a certificate chain by tapping the **Import** button and selecting a certificate file from the local file system. Provide the user with a password if needed.
- Clear all certificates from the AnyConnect store by tapping the **Clear All** button.

Profile Management

Profile Overview

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 the endpoint device as well as other connection attributes, policies and constraints. These connection entries, in addition to the VPN connections configured locally on the mobile device by the user, are listed on the AnyConnect home screen to choose from when initiating a VPN connection.

Administrators use the AnyConnect Profile Editor to edit the VPN Client Profile XML file, configuring connection entries and client features for mobile devices. Administrators choose how to distribute the client profile by configuring the security appliance to upload a client profile onto the mobile device upon VPN connectivity, by providing the user with an AnyConnect URI link to import a client profile, or by defining a procedure for the user to manually import a client profile. See the *AnyConnect Administrators Guide* for details and procedures on configuring and deploying Client Profiles.

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 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 a profile associated with it, the existing profile is deleted upon startup of that VPN.

User Profile Management

Android users manage the AnyConnect Profile on their device in the **Menu > Settings > Profile Management** activity screen, the user can perform these tasks:

- View current XML profile details by expanding the identified XML profile.
- Delete the current AnyConnect XML profile by tapping the **Delete Profile** button and confirming this action. When deleted, connection entries that were defined in the profile are cleared from the AnyConnect home screen and AnyConnect client behavior conforms to default client specifications.
- Import an XML profile by tapping the **Import Profile** button and selecting an XML profile file from the local 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.

URI Profile Import Support

Administrators can provide Android device users with an AnyConnect URI for importing localization data. For example:

```
anyconnect://import?type=localization&host=asa.example.com&lang=ja-jp
```

See *Using the URI Handler to Automate AnyConnect Actions* in the AnyConnect Administrators Guide for a full explanation of using URIs to administer AnyConnect.

Mobile-Specific Additions to the AnyConnect VPN Client Profile

Starting in release 2.5.x AnyConnect administrators can now specify the **CertificatePolicy** and the **ActivateOnImport** attribute for VPN connections in the AnyConnect VPN Client Profile.

Note Configuring an AnyConnect VPN Client Profile with these features requires AnyConnect VPN Profile Editor, release 3.0.1047 or later.

CertificatePolicy

The CertificatePolicy attribute associated with a connection entry specifies how certificates are handled for this connection. Valid values are Automatic, Manual, or Disabled:

- **Automatic**: AnyConnect enumerates all certificates on the client at connection time, matching them against the CertificateMatch rules in the profile and choosing the appropriate one.
- **Manual**: AnyConnect tries to find a certificate on the mobile device to associate with the connection by applying the CertificateMatch rules when the client profile is imported. If one is found, the matched certificate is associated with the imported connection as if the user had manually selected it. If no matching certificate is found, the Certificate Policy resets to Automatic.
- **Disabled**: This connection does not use certificates.

ActivateOnImport

The ActivateOnImport flag associated with a connection entry identifies the connection that becomes active after the Client Profile is imported, and the current connection is disconnected. The active connection entry’s description is displayed under **AnyConnect VPN** on the AnyConnect home screen.

If more than one connection entry has this flag set, the AnyConnect client sets the first flagged connection entry as the active connection.

Additional URI Handler Commands

The AnyConnect URI handler services action requests in the form of Universal Resource Indicators (URIs). To simplify the AnyConnect user setup process, administrators can embed the URIs as links on webpages or email messages and give users instructions to access them.

Previously, URIs could be used to provision VPN connection entries, connect to or disconnect from a VPN, and import certificates. AnyConnect 2.5.x and later provides these additional URI handler features:

- **Credential pre-fill**: Use the URI handler **connect** command to provide a pre-filled username and pre-filled password in addition to name and host parameter for the connect action.

  Note Credential pre-fill should only be used in conjunction with a One Time Password (OTP) infrastructure.

- **Import of Localization translation**: Use the URI handler **import** command to distribute localization files to AnyConnect clients.
- **Import of a Client Profile**: Use the URI handler **import** command to distribute a profile to an AnyConnect client.

Note AnyConnect URI handling is **Disabled** by default. Android device users can allow this functionality by selecting **Menu > Settings > Application Preferences > External Control** and then choosing **Enable**. They can be notified of URI activity and allow or disallow it at request time by choosing **Prompt.**

External Control of AnyConnect URI Commands

The new **Menu > Settings > Application Preferences > External Control** setting allows the user to specify how the AnyConnect application responds to AnyConnect URIs. The External Control setting can be set to Enabled, Disabled (default), or Prompt:

- **Enabled**: The AnyConnect application allows all URI commands, and the user is not notified of URI actions.
- **Disabled**: The AnyConnect application disallows all URI commands.
- **Prompt**: The AnyConnect application prompts the user each time an AnyConnect URI is clicked on the device.

AnyConnect Lifetime and Notification Enhancements

In previous AnyConnect Android releases, all components of AnyConnect automatically launch at device startup time. Android users now have control over when AnyConnect starts on their device and AnyConnect does not launch at device startup time by default. The user can enable this by checking the **Launch at Startup** preference in the **Menu > Settings > Application Preferences** activity. If left unchecked, AnyConnect will not launch until the user starts it.

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

Troubleshooting Improvements

The following improvements have been made to simplify troubleshooting activities on the Android devices:

- Android users now have direct access to the **Diagnostics** activity by choosing **Menu > Diagnostics**, and they no longer have to go through the **Statistics** activity.

- The **Diagnostics** activity has been modified to provide Mobile Posture information for the device including the Client Version, the Platform Version, the Device, and the Device Type. This information can be viewed by expanding **Device Identifiers** at the bottom of the **System** tab.
- The user can send log directly to Cisco or to an administrator by choosing **Send to Cisco** or **Send to Admin**.
- When choosing **Send to Cisco** the "To:" field now defaults to the ac-mobile-feedback@cisco.com mailer list. Users have the option to remove this Cisco mailer or add more addresses before sending the email.

Android AnyConnect Feature Matrix

Table 1 lists the features in the following AnyConnect 2.5.x for Android packages.

Android Brand-specific AnyConnect

For supported devices, Cisco provides brand-specific AnyConnect packages that offer a full-featured VPN experience across Android operating systems. These brand-specific AnyConnect packages are provided in partnership with device vendors and are the preferred AnyConnect clients for supported devices.

Android VPN Framework AnyConnect

For other Android devices unable to use the brand-specific AnyConnect packages above, Cisco provides an AnyConnect client that offers VPN connectivity supported by the Android VPN Framework (AVF) introduced in Android 4.0 (Ice Cream Sandwich). 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 device-specific packages. These discrepancies are shown in the table.

Android Rooted AnyConnect

Cisco also provides an AnyConnect package for rooted Android devices equivalent in functionality to the brand-specific packages. This package works on most rooted devices running Android 2.1 or later. Brand-specific AnyConnect packages do not work on rooted devices; therefore you must use the rooted version of AnyConnect on rooted devices.

Table 1 AnyConnect Android Features

AnyConnect Feature	Sub Feature	Android Brand-Specific AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Tunneling	TLS/DTLS	Yes	Yes
	IKEv2 - NAT-T	No	No
	IKEv2 - raw ESP	No	No
	Suite B support	No	No
	TLS compression	Yes	Yes
	Dead peer detection	Yes	Yes
	Tunnel keepalive	Yes	Yes
Tunnel Establishment	Optimal Gateway Selection	No	No
	VPN load balancing	Yes	Yes
	Backup server list	Yes	Yes
	Activate a Host Entry on profile import	Yes	Yes
	URI connect credential pre-fill	Yes	Yes

Table 1 AnyConnect Android Features

AnyConnect Feature	Sub Feature	Android Brand-Specific AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Tunnel Policy	All/full tunnel	Yes	Yes
	Split tunnel (split include)	Yes	Yes
	Local LAN (split exclude)	**Yes**	**No**
	Split-DNS	**Yes**	**Will work with split include.**
	Always-on enforcement	No	No
	Auto-reconnect: maintains the VPN as users move between 3G and WiFi networks	Yes	Yes
	VPN on-demand (triggered by destination)	No	No
	VPN on-demand (triggered by application)	No	No
	Trusted network detection (TND)	Yes	No
	Rekey	Yes	Yes
	ASA group profile support	Yes, limited	Yes, limited
	IPv4 public transport	Yes	Yes
	IPv6 public transport	No	No
	IPv4 over IPv4 tunnel	Yes	Yes
	IPv6 over IPv4 tunnel	Yes	Yes
	Default Domain	Yes	Yes
	DNS server configuration	Yes	Yes
	Private-side proxy support	No	No, WiFi proxies are disabled when VPN established.
	Pre-login banner	Yes	Yes
	Post-login banner	Yes	Yes
	Scripting	No	No
	Reconfigure VPN	Yes	Yes
Tunnel Security	Network change monitoring	Yes	Yes
	Shim intercept/filtering	No	No
	Embedded firewall rules	No	No
	Filter Support (iptables)	**Yes**	**No**

Table 1 AnyConnect Android Features

AnyConnect Feature	Sub Feature	Android Brand-Specific AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Authentication	Manual certificate import (get certificate)	Yes	Yes
	SCEP enrollment	Yes	Yes
	Automatic certificate selection	Yes	Yes
	Manual certificate selection	Yes	Yes
	Non-exportable certificate	N/A	N/A
	Smart card support	No	No
	Username and password	Yes	Yes
	Tokens/challenge	Yes	Yes
	Double authentication	Yes	Yes
	Group selection	Yes	Yes
	Credential Prefill	Yes	Yes
	Save password	No	No
User interface	Standalone GUI	Yes	Yes
	Native OS GUI	No	No
	CLI	No	No
	API	Yes, Java not C++	Yes, Java not C++
	UI customization	Yes (themes)	Yes (themes)
	UI Localization	Yes	Yes
	User Preferences	Yes	Yes
	Certificate Confirmation Reasons	Yes	Yes
	Home screen widgets for one-click VPN access	Yes	Yes
	Paused icon when connection suspended for TND	Yes	Yes
	Hide AnyConnect icon when idle	Yes	Yes
	Launch on startup of mobile device	Yes	Yes
	Exit AnyConnect	Yes	Yes
	User Certificate Management	Yes	Yes
	User Profile Management	Yes	Yes
	User Localization Management	Yes	Yes

Table 1 AnyConnect Android Features

AnyConnect Feature	Sub Feature	Android Brand-Specific AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Deployment	WebLaunch (browser-initiated)	No	No
	Web redirect to application store	No	No
	Standalone installer	No	No
	Preinstalled by OEM	No	No
	Install or Upgrade from the ASA	No	No
	Install or upgrade from Android Market	Yes	Yes
	Pre-packaged localization for some languages	Yes	Yes
Configuration	XML Client Profile import on connect.	Yes	Yes
	URI handler support for importing XML Client Profile	Yes	Yes
	User configured connection entries	Yes	Yes
Posture Assessment	Device check (pin lock, encryption, etc)	No	No
	Running or installed apps	No	No
	Serial number or unique ID check	No	No
	Mobile Posture	Yes	Yes
URI Handling	Add connection entry	Yes	Yes
	Connect to a VPN	Yes	Yes
	Credential pre-fill on connect	Yes	Yes
	Disconnect VPN	Yes	Yes
	Import certificate	Yes	Yes
	Import localization data	Yes	Yes
	Import XML client profile	Yes	Yes
	External (user) control of URI commands	Yes	Yes

Table 1 AnyConnect Android Features

AnyConnect Feature	Sub Feature	Android Brand-Specific AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Troubleshooting	Statistics	Yes	Yes
	Logging	Yes	Yes
	Email statistics, log messages and system information	Yes	Yes
	Direct feedback to Cisco	Yes	Yes
	DART	No	No
Certifications	FIPS 140-2 Level 1	No	No
	Common criteria	No	No

Adaptive Security Appliance Requirements

ASA Release Requirements

ASA models support the Cisco AnyConnect Secure Mobility client for Android. See the *Adaptive Security Appliance VPN Compatibility Reference* for a complete list of compatibility requirements.

Table 2 shows the minimum Cisco ASA 5500 software images that support AnyConnect.

Table 2 Software Images that Support AnyConnect, Release 2.5 for Android

Image Type	Version
ASA Boot image	8.0(3) or later
Adaptive Security Device Manager (ASDM)	6.1(3) or later

Note Any Cisco router running Cisco IOS version 15.1(1)T or later also supports the Cisco AnyConnect Secure Mobility client for Android.

ASA License Requirements

AnyConnect for Android connections require the following licenses on the ASA:

- One of the following AnyConnect core license options:
  - Cisco AnyConnect Essentials license (L-ASA-AC-E-55XX=), sufficient for ASA Release 8.2 or later.
  - Cisco AnyConnect Premium Clientless SSL VPN Edition license (L-ASA-AC-SSL-YYYY=), required for ASA Releases 8.0(3) or later.
- AnyConnect Mobile license (L-ASA-AC-M-55XX=).

The XX in the license code represents the last two digits of your ASA model number. The YYYY represents the number of simultaneous users.

These licenses are mutually exclusive per ASA, but you can configure a mixed network. The AnyConnect Essentials and AnyConnect Mobile licenses are nominally priced. We offer the following trial options:

- If you have an AnyConnect Essentials or Premium license and you would like to obtain a three-month trial Mobile AnyConnect license, go to the following website: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=717
- If you would like to obtain both an AnyConnect Essentials or Premium license and an AnyConnect Mobile license, or you have questions about licensing, email us a request with the **show version** output from your ASA to ac-mobile-license-request@cisco.com.

For brief descriptions and example product numbers (SKUs) of the AnyConnect user license options, see *Cisco Secure Remote Access: VPN Licensing Overview*.

For the latest details about the AnyConnect user license options, see “Managing Feature Licenses” in the latest Cisco ASA 5500 Series Configuration Guide.

Restricting Android Mobile Connections

ASAs running release 8.2(5+) and 8.4(2) feature AnyConnect Mobile Posture for mobile device detection. Mobile Posture lets you accept or restrict mobile connections without Cisco Secure Desktop, earlier releases require Cisco Secure Desktop.

Mobile Posture requires an AnyConnect Premium and an AnyConnect Mobile license.

Table 3 AnyConnect Requirements for ASA Releases

Requirements	ASA Release 8.2(5+)and 8.4(2) and later[1]	ASA Releases 8.0(4) – 8.2(4), and 8.4(1)
Cisco Secure Desktop enabled?	Not required	Yes
Dynamic access policy (DAP) endpoint configuration	Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add** or **Edit** > **Add** to the right of the Endpoint Attributes table, change the Endpoint Attribute Type to **AnyConnect**, and change the Platform to **Android**. ASDM displays a drop-down list next to Device Type, however, the drop-down options are not supported. Enter the model name into the Device Type field. Add one endpoint attribute to a DAP for each device to assign a policy to it. Use the tabs in the Access/Authorization Policy Attributes section of the Add or Edit Dynamic Access Policy window to continue, terminate, or impose restrictions on Android connections.	Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add** or **Edit**, click **Advanced**, and enter the following line into the Logical Expressions box to grant, restrict, or deny access to Android connections: EVAL(endpoint.os.version, "EQ", "Android", "string") Use the tabs in the Access/Authorization Policy Attributes section of the Add or Edit Dynamic Access Policy window to continue, terminate, or impose restrictions on Android connections. **Note**: The Android user sees the message entered in the message box on the Action tab of the ASDM Add or Edit Dynamic Access Policy window only if the regular expression fails to match.

[1] If you already have AnyConnect Premium and Cisco Secure Desktop, and the ASA is running 8.0(4) or later, you have the option to add the logical expression shown in the third column.

Known Issues and Limitations

The following sections describe the known issues and limitations in the AnyConnect 2.5.x releases.

Open Issues in Anyconnect 2.5.5131

Identifier	Headline
CSCty38958	Anyconnect cert store will show client and root certs after upgrade
CSCty61878	DNS servers not properly restored when split-dns is configured
CSCty75051	java.lang.NullPointerException @ VpnConnection.IsProfileImportDupeOf
CSCty75092	Certificate store unavailable after application upgrade causing hang

Issues Fixed in AnyConnect 2.5.5131

Identifier	Headline
CSCua94635	Removal of v6 address on public interface causes system to overwrite DNS
CSCtq33166	Unable to send/receive MMS messages while connected
CSCty52537	ENH: iPhone Roaming Profile Configuration via Third Party Management AppENH: iPhone Roaming Profile Configuration via Third Party Management App
CSCtz24420	Application memory leaks
CSCtz24424	vpnagent memory leaks

Open Issues in AnyConnect 2.5.5125

Identifier	Headline
CSCua94635	Removal of v6 address on public interface causes system to overwrite DNS
CSCtq33166	Unable to send/receive MMS messages while connected
CSCty38958	Anyconnect cert store will show client and root certs after upgrade
CSCty61878	DNS servers not properly restored when split-dns is configured
CSCty75051	java.lang.NullPointerException @ VpnConnection.IsProfileImportDupeOf
CSCty75092	Certificate store unavailable after application upgrade causing hang

Issues Fixed in AnyConnect 2.5.5125

Identifier	Headline
CSCty43494	Need clearer error msg for users trying to run rooted on non-rooted devices
CSCty45810	Non-root packages should not attempt root access
CSCty54946	Denying SU for rooted version on ICS tries to fall back to AVF but fails
CSCty61866	Stuck in reconnect when split-dns configured after rc'ing multiple times
CSCty80399	Unable to connect to Cisco IOS head-ends.

Issues Fixed in AnyConnect 2.5.5116 and 2.5.118

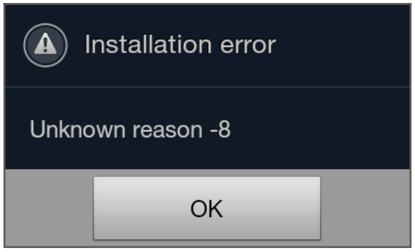
Bug ID	Headline
CSCto11909	IPv6 traffic going in the clear when physical interface has IPv6 address
CSCtu43391	Memory Leak in AC will cause AC to crash
CSCtu53427	AC mobile disconnects due to a multi-thread issue
CSCtx92325	AnyConnect needs to be installed before API can be used

The OpenSSL upgrade in AnyConnect 2.5.x fixed the following OpenSSL vulnerabilities: CSCtw73326, CSCtw73351,CSCtw73360, CSCtw73368, CSCtw73379, CSCtw73387, CSCtw73394, CSCtw73399, CSCtw73407, CSCtw73414, CSCtw73419, CSCtw73423, CSCtw73430, CSCtw73434, CSCtw73439, and CSCtw73444. These vulnerabilities are not confirmed to be exploitable for Cisco AnyConnect, however Cisco is improving AnyConnect product security by upgrading to a Cisco-maintained version of OpenSSL that contains the appropriate fixes.

Guidelines and Limitations

- AnyConnect for Android supports only the features that are strictly related to remote access.
- The ASA does not provide distributions and updates for AnyConnect for Android. They are available only on the Android Market.
- AnyConnect for Android supports connection entries that the user adds and connection entries populated by an AnyConnect profile pushed by an ASA. For example, if a user goes to vpn.example1.com and then goes to vpn.example2.com, the configuration profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.The Android device supports no more than one AnyConnect profile. However, a profile can consist of multiple connection entries.
- The AnyConnect AVF package provides VPN features that can be supported in the AVF only, some AnyConnect features available in the brand-specific packages are not supported in the AVF package. See the Android AnyConnect Feature Matrix for the specific features supported in AVF AnyConnect.
- If users attempt to install AnyConnect on devices that are not supported, they receive a pop-up message saying, “Installation Error: Unknown reason -8.” This message is generated by the Android OS. Figure 1 shows the installation error message.

Figure 1 Android Installation Error



Installation error

Unknown reason -8

- When the user has an AnyConnect widget on their home screen, the AnyConnect services are automatically started (but not connected) regardless of the “Launch at startup” preference.

- AnyConnect for Android requires UTF-8 character encoding for extended ASCII characters when using pre-fill from client certificates. The client certificate must be in UTF-8 if you want to use prefill, per the instructions in KB-890772 and KB-888180.
- AnyConnect blocks voice calls if it is sending or receiving VPN traffic over an EDGE connection per the inherent nature of EDGE and other early radio technology.
- Some known file compression utilities do not successfully decompress log bundles packaged with the use of the AnyConnect Send Log button. As a workaround, use the native utilities on Windows and Mac OS X to decompress AnyConnect log files.

Known Compatibility Issues

- An Asus tablet running Android 4.0 (ICS) may be missing the tun driver. This causes AVF AnyConnect to fail.
- On a rooted device, in the superuser application preferences, Automatic response must be set to Prompt. Other settings may cause AnyConnect to hang.

Troubleshooting

Follow the user troubleshooting instructions in the latest Cisco AnyConnect Administrator Guide. If following those instructions does not resolve the issue, try the following suggestions:

- Ensure the AnyConnect Mobile license is installed on the ASAs.
- Determine whether the same problem occurs with the desktop client.
- Determine whether the same problem occurs with another supported mobile OS.
- If the VPN connection is not restored after the device wakes up, ensure that Auto-Reconnect is enabled in the profile.
- If certificate authentication fails, ensure the correct certificate has been selected. Ensure that the client certificate on the device has Client Authentication as an Extended Key Usage. Ensure the certificate matching rules in the AnyConnect profile are not filtering out the user’s selected certificate. Even if a user selected a certificate, it is not used for authentication if it does not match the filtering rules in the profile. If your authentication mechanism uses any associated accounting policy to an ASA, verify that the user can successfully authenticate. If problems persist, enable logging on the client and enable debug logging on the ASA.
- If you see an authentication screen when you are expecting to use certificate-only authentication, configure the connection to use a group URL and ensure that secondary authentication is not configured for the tunnel group. For details, refer to the Cisco ASA Configuration Guide associated with the version running on the ASA.

Support Policy

Cisco supports all AnyConnect software versions downloaded from the Android Market; however, fixes and enhancements are provided only in the most recently released version.

Licensing

For brief descriptions and example product numbers (SKUs) of the AnyConnect user license options, see *Cisco Secure Remote Access: VPN Licensing Overview*.

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*.

Related Documentation

For more information, refer to the following documentation:

- Cisco AnyConnect Secure Mobility Client Release Notes
- Cisco AnyConnect Administrator Guides
- *Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.5*
- *Navigating the Cisco ASA 5500 Series Documentation*

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.