Release Notes for Cisco AnyConnect Secure Mobility Client 3.0.x for Android Mobile Devices

Updated: January 23, 2014

This document includes the following sections:

- Introduction
- New Features in AnyConnect 3.0.09269
- New Features in AnyConnect 3.0.09242
- New Features in AnyConnect 3.0.09220
- New Features in AnyConnect 3.0.09156
- New Features in AnyConnect 3.0.09140
- New Features in AnyConnect 3.0.09129
- New Features in AnyConnect 3.0.09093
- New Features in AnyConnect 3.0.09073
- Supported Android Devices
- Android AnyConnect Feature Matrix
- Adaptive Security Appliance Requirements
- Known Issues and Limitations
- Troubleshooting
- AnyConnect Support Policy
- AnyConnect License Agreements
- 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, or Internet Protocol Security (IPsec) Internet Key Exchange version 2 (IKEv2). It 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 current 3.0.09xxx releases of the Cisco AnyConnect Secure Mobility Client:

- Cisco AnyConnect Release 3.0.09269, available on:
  - Samsung devices
  - HTC 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.

All AnyConnect Android packages are available for installation and upgrading from Google Play except for the Kindle package, which is available on Amazon.com.

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

For Android device requirements, installation instructions, and user information, see the *Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.*

New Features in AnyConnect 3.0.09269

AnyConnect 3.0.09269 is a maintenance release, see Resolved Issues in AnyConnect 3.0.09269 for Mobile Devices. Cisco recommends that you upgrade to this latest release of AnyConnect.

Review the Android Known Compatibility Issues to be aware of current operational considerations.

New Features in AnyConnect 3.0.09242

AnyConnect 3.0.09242 resolves a critical problem in previous releases affecting DNS resolution on Android 4.3.x devices. It is also a maintenance release for all Android devices, see Resolved Issues in AnyConnect 3.0.09242 for Mobile Devices.

Cisco recommends that you upgrade to this latest release of AnyConnect.

Review the Android Known Compatibility Issues to be aware of current operational considerations.

New Features in AnyConnect 3.0.09220

AnyConnect 3.0.09220 includes updates for HTC devices running Android 4.3. This version of AnyConnect is for HTC devices only.

Review the Android Known Compatibility Issues to be aware of current operational considerations.

New Features in AnyConnect 3.0.09156

AnyConnect 3.0.09156 is a maintenance release, see Resolved Issues in AnyConnect 3.0.09156 for Mobile Devices. Cisco recommends that you upgrade to this latest release of AnyConnect.

Review the Android Known Compatibility Issues to be aware of current operational considerations.

New Features in AnyConnect 3.0.09140

AnyConnect 3.0.09140 is a maintenance release, see Resolved Issues in AnyConnect 3.0.09140 for Mobile Devices. Cisco recommends that you upgrade to this latest release of AnyConnect.

New Features in AnyConnect 3.0.09129

AnyConnect 3.0.09129 is a maintenance release, see Resolved Issues in AnyConnect 3.0.09129 for Mobile Devices. Cisco recommends that you upgrade to this latest release of AnyConnect.

New Features in AnyConnect 3.0.09093

AnyConnect 3.0.09093 is a maintenance release, see Resolved Issues in AnyConnect 3.0.09093 for Mobile Devices. Cisco recommends that you upgrade to this latest release of AnyConnect.

New Features in AnyConnect 3.0.09073

IPsec IKEv2

The AnyConnect Secure Mobility Client for mobile devices now supports Internet Protocol Security (IPsec) Internet Key Exchange version 2 (IKEv2) tunneling in addition to SSL tunneling.

The AnyConnect client uses a proprietary AnyConnect EAP authentication method with ASA secure gateways. Standards-based EAP authentication methods are also available, however, using the standards-based method disables some AnyConnect features. The client supports the following standards-based authentication methods:

- EAP methods: GTC, MD5, and MSCHAPv2
- IKEv2 methods: RSA

On the ASA, you enable IPsec connections for users in the group policy. For the AnyConnect client, you specify the primary protocol (IPsec or SSL) for each ASA in the server list of the client profile.

On the mobile device, the user chooses **Connect with IPsec** when adding a VPN connection.

System Requirements for IPsec IKEv2

• ASA running version 9.0 or later

• ASDM 7.0.1 or later

• AnyConnect Essentials license or an AnyConnect Premium SSL VPN Edition license

FIPS and Suite B Cryptography

AnyConnect 3.0 for mobile devices incorporates Cisco Common Cryptographic Module (C3M), the Cisco SSL implementation which includes FIPS 140-2 compliant cryptography modules and NSA Suite B cryptography as part of its Next Generation Encryption (NGE) algorithms.

In AnyConnect 3.0 for mobile devices, Suite B cryptography is available for IPsec VPNs only; FIPS-compliant cryptography is available for both IPsec and SSL VPNs.

Use of cryptography algorithms is negotiated with the headend while connecting. Negotiation is dependent on the capabilities of both ends of the VPN connection. Therefore, the secure gateway must also support FIPS-compliant and Suite B cryptography.

The user configures AnyConnect to accept only NGE algorithms during negotiation by enabling **FIPS Mode** in the AnyConnect settings. When FIPS Mode is disabled, AnyConnect also accepts non-FIPS cryptography algorithms for VPN connections.

AnyConnect 3.0 for mobile devices includes the following Suite B algorithms:

- AES-GCM support (128-, 192-, and 256-bit keys) for symmetric encryption and integrity
  - IKEv2 payload encryption and authentication (AES-GCM only)
  - ESP packet encryption and authentication
- SHA-2 (SHA with 256/384/512 bits) support for hashing
  - IKEv2 payload authentication
  - ESP packet authentication
- ECDH support for key exchange
  - Groups 19, 20, and 21 IKEv2 key exchange and IKEv2 PFS
- ECDSA support (256-, 384-, 512-bit elliptic curves) for digital signature, asymmetric encryption, and authentication
  - IKEv2 user authentication and server certificate verification
- Other cipher suite dependencies between algorithms promote support for the following:
  - Diffie-Hellman Groups 14 and 24 for IKEv2
  - RSA certificates with 4096 bit keys for DTLS and IKEv2

Requirements

- FIPS and/or Suite B support is required on the secure gateway. Cisco provides Suite B capability on the ASA version 9.0 and later, and FIPS capability on the ASA version 8.4.1 and later.
- An AnyConnect Premium license is required for FIPS or Suite B remote access connections to the ASA.
- Android 4.0 (Ice Cream Sandwich) or later is required for Suite B cryptography; this is the minimum Android version that supports ECDSA certificates used in Suite B.

- VPN connections require server certificates that contain Key Usage attributes of Digital Signature and Key Encipherment, as well as an Enhanced Key Usage attribute of Server Authentication, or IKE Intermediate for IPsec. Server certificates not containing a Key Usage are considered invalid for all Key Usages. Similarly, a server certificate not containing an Enhanced Key Usage is considered invalid for all Enhanced Key Usages.

Guidelines and Limitations

- Suite B is available only for IKEv2/IPsec.
- A device that is running in FIPS mode is not compatible with using SCEP to provide mobile users with digital certificates, proxy method or legacy method. Plan your deployment accordingly.
- No EAP methods support SHA-2 except in TLS-based EAP when validating certificates signed using SHA-2.
- ECDSA certificates must have a Digest strength equal to or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
- VPN connections perform name verification on server certificates. The following rules are applied to name verification:
  - If a Subject Alternative Name extension is present with relevant attributes, name verification uses only the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates and also include IP address attributes, if the connection is being performed to an IP address.
  - If a Subject Alternative Name extension is not present, or is present but contains no relevant attributes, name verification uses any Common Name attributes found in the Subject of the certificate.
  - If a certificate uses a wildcard for the purposes of name verification, the wildcard must be in the first (left-most) subdomain only and must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance is ignored for the purposes of name verification.

Additional URI Handler Enhancements

The AnyConnect URI Handler simplifies AnyConnect setup and activities by servicing requests in the form of Universal Resource Indicators (URIs). Administrators embed URIs as links on web pages or in e-mail messages and then give users instructions to access them. The following enhancements have been made to the URI Handler in AnyConnect 3.0:

- Parameters have been added to the **anyconnect:create** command to create IPsec connection entries, for example:

  ```
  anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec&authentication=eap-md5&ike-identity=012A4F8B29A9BCD
  ```

  Where:

  - **protocol**: Specifies the VPN protocol used for this connection. The valid values are SSL or IPsec. This parameter is optional and defaults to SSL if unspecified.
  - **authentication**: Specifies the authentication method used for an IPsec VPN connection. The valid values are EAP-AnyConnect, EAP-GTC, EAP-MD5, EAP-MSCHAPv2, or IKE-RSA. This parameter is optional; it applies when `protocol` specifies `IPsec` only and defaults to EAP-AnyConnect if unspecified.

  - **ike-identity**: The IKE identify when AUTHENTICATION is set to EAP-GTC, EAP-MD5, or EAP-MSCHAPv2. This parameter is invalid when used for other authentication settings.

  For URI details, see "Using the URI Handler to Generate a VPN Connection Entry" section in Chapter 13, "Administering AnyConnect for Mobile Devices" of the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* manual.

- Extensions have been made to the **anyconnect:connect** command to open a specified URL or close the AnyConnect UI based on the results of the connect action. For example:

  anyconnect://connect?host=vpn.company.com**&onerror**=http%3A%2F%2Fwww.cisco.com%2Ffailure.html**&onsuccess**=http%3A%2F%2Fwww.cisco.com

  anyconnect://connect?host=vpn.company.com**&onsuccess**=anyconnect%3A%2F%2Fclose

  - **onerror**—Specify the URL to be opened when this connection transitions into the disconnected state, or use the **anyconnect%3A%2F%2Fclose** command to close the AnyConnect GUI.
  - **onsuccess**—Specify the URL to be opened when this connection transitions into the connected state, or use the **anyconnect%3A%2F%2Fclose** command to close the AnyConnect GUI.

  For URI details, see Using the URI Handler to Establish a VPN Connection section in Chapter 13, "Administering AnyConnect for Mobile Devices" of the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* manual.

User Certificate Management Enhancements

AnyConnect 3.0 provides additional options for importing user certificates into the AnyConnect certificate store depending on the Android release on the device. In addition to importing a user certificate directly from the device's file system, AnyConnect users can now do the following:

- Import certificates from a Network Location by specifying the URI of the certificate. This applies to all Android releases.
- Import certificates from the device's Credential Storage to the AnyConnect store. This applies to Android 4.0/ICS and later.

For details, see "Importing Certificates Manually" in the *Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.x.*

Server Certificate Management Enhancements

AnyConnect now imports user-authorized server certificates to the AnyConnect certificate store during the connection process.

A user is given the opportunity to import a server certificate if it is not automatically accepted by AnyConnect. Only valid, trusted server certificates are automatically accepted by AnyConnect. See Blocking Untrusted Servers below for the procedure to do this.

Valid, but untrusted server certificates are reviewed, authorized, and imported by the user. Once this server certificate is imported into the AnyConnect store, subsequent connections made to the server using this digital certificate are automatically accepted. The server certificate can be removed from the AnyConnect certificate store if it is no longer needed.

Invalid certificates are not imported into the AnyConnect store, but can be accepted by the user to complete the current connection. This is not recommended.

Blocking Untrusted Servers

AnyConnect has been updated to provide improved security protection when accessing secure gateways.

A new **Block Untrusted Servers** application setting determines how AnyConnect blocks connections if it cannot identify the secure gateway. This protection is ON by default; it can be turned OFF by the user, but this is not recommended.

AnyConnect uses the digital certificate received from the server to verify its identify. If the certificate is invalid (there is a certificate error due to an expired or invalid date, wrong key usage, or a name mismatch), or if it is untrusted (the certificate cannot be verified by a Certificate Authority), or both, the connection is blocked. A blocking message displays, and the user must choose how to proceed.

When **Block Untrusted Servers** is ON, a blocking **Untrusted VPN Server** notification alerts the user to this security threat. The user can choose:

- **Keep Me Safe** to terminate this connection and remain safe.
- **Change Settings** to turn the **Block Untrusted Servers** application preference OFF, but this is not recommended. After the user disables this security protection, they must reinitiate the VPN connection.

When **Block Untrusted Servers** is OFF, a nonblocking **Untrusted VPN Server** notification alerts the user to this security threat. The user can choose to:

- **Cancel** the connection and remain safe.
- **Continue** the connection, but this is not recommended.
- **View Details** of the certificate.

  If the certificate that the user is viewing is valid but untrusted, the user can:

  – Import the server certificate into the AnyConnect certificate store for future use and continue the connection by selecting **Import and Continue**. Once this certificate is imported into the AnyConnect store, subsequent connections made to the server using this digital certificate are automatically accepted.

  – Go back to the previous screen and choose **Cancel** or **Continue**.

  If the certificate is invalid, for any reason, the user can only return to the previous screen and choose **Cancel** or **Continue**.

Leaving the **Block Untrusted Servers** setting ON, having a valid, trusted server certificate configured on your secure gateway, and instructing your mobile users to always choose **Keep Me Safe** is the safest configuration for VPN connectivity to your network.

SCEP Proxy

Simple Certificate Enrollment Protocol (SCEP) Proxy provides secure deployment of device certificates from third-party Certificate Authorities (CAs). It allows a mobile user to enroll with an internal CA without exposing the CA to external access.

With AnyConnect 3.0, an ASA 9.0 or later acts as a proxy for SCEP requests and responses that flow between the AnyConnect mobile device and the internal CA. Mobile devices rely on the ASA to know the identity of the CA, and do not access them directly. The received certificate is used to automatically connect after being imported into the AnyConnect certificate store on the mobile device.

For more information, see "Configuring Certificate Enrollment using SCEP" section in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* manual.

Guidelines and Limitations

- Depending on network characteristics, SCEP proxy activity can take more than a few seconds. The user receives a message when the certificate has been received by the AnyConnect client.
- Using SCEP for certificate enrollment, proxy method or legacy method, is not compatible with mobile devices running in FIPS mode. Plan your deployment accordingly.

Trusted Network Detection

Trusted Network Detection (TND) provides AnyConnect the ability to automatically disconnect a VPN when the user is inside the corporate network (on a trusted network) and to start the VPN connection when the user is outside the corporate network (on an untrusted network).

Administrators enable this feature in the AnyConnect client profile, define which networks are trusted or untrusted, and set behavior when it detects network transitions. For details, see the Configuring Trusted Network Detection section in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* manual.

AnyConnect 3.0 on Android allows users to disable and enable Trusted Network Detection (TND) on their own device if it has been configured by the administrator. To do this, users set the **Menu > Settings > Trusted Network Detection** option.

TND requires the AnyConnect app to be running. If the user has exited the application using **Menu > Exit** or has forced the app to stop using the Android settings, AnyConnect will be unable to detect a trusted network.

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

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

Mobile Posture Device ID Generation

The algorithm to generate mobile posture Device IDs on Android changed in AnyConnect 3.0. If you have DAP rules defined that use Device IDs generated from previous versions of AnyConnect, they will have to be updated to bind to the newly generated Device IDs.

AnyConnect 3.0 generates a unique 40-byte device ID at installation time. The generated device ID is based on the Android ID and one or both of the following values if they are available at installation time:

- MEID/IMEI (Mobile Equipment Identifier / International Mobile Equipment Identity)
- MAC-ADDRESS (MAC address of the device)

The device ID is generated depending on the availability of these values:

Available values	Generation Algorithm
If both values are retrievable at installation time:	`device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI + MAC-ADDRESS))`

If only the MEID/IMEI is retrievable at installation time:	`device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI))`
If only the MAC-ADDRESS is retrievable at installation time	`device-ID = bytesToHexString(SHA1(Android-ID + MAC-ADDRESS))`

Where:

- The Android-ID is set as follows:

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

- And the `bytes To Hex String` function is:

```
String bytesToHexString(byte[] sha1rawbytes)
{
     String hashHex = null;
      if (sha1rawbytes != null)
     {
         StringBuffer sb = new StringBuffer(sha1rawbytes.length * 2);
         for (int i = 0; i < sha1rawbytes.length; i++)
         {
             String s = Integer.toHexString(0xFF & sha1rawbytes[i]).toUpperCase();
             if (s.length() < 2)
             {
                 sb.append("0");
             }
             sb.append(s);
         }
         hashHex = sb.toString();
     }
      return hashHex;
}
```

Note If neither the MEID/IMEI nor MAC-ADDRESS values are retrievable at installation time, a random number is used with the `Android-ID` to generate the device-ID.

Generated device IDs can be viewed after the initial AnyConnect application launch from the AnyConnect **Diagnostics -> Logging and System Information -> System -> Device Identifiers** screen, or inside the AnyConnect log in the device_identifiers.txt file.

In AnyConnect 2.5, the MEID/IMEI is used as the device ID. If the MEID/IMEI is not available, AnyConnect will try to use the MAC-ADDRESS. If this value is also not available, AnyConnect installation fails.

Android UI Changes

The following changes have been made to the AnyConnect UI running on Android devices:

- Upon the initial startup of AnyConnect after installation or upgrade, the user must accept the displayed End User License Agreement before AnyConnect runs.
- Changes in the AnyConnect **Settings** and **Diagnostics** options:
  - Management of certificates, profiles, and localization on the device has been moved from the **Settings** screen to the **Diagnostics** screen. Only AnyConnect application preference settings remain in Settings.

  - The user now must now tap **Diagnostics > Logging and System Information** to access the Logs and System screen.
  - A new FIPS Mode setting has been added to the Settings screen. See the FIPS and Suite B Cryptographysection for details.
  - A new **Block Untrusted VPN** setting has been added to the Settings screen. See the Blocking Untrusted Servers section for details.
  - A new **Trusted Network Detection** setting has been added to the Settings screen. See the Trusted Network Detection section for details.
  - On Android 4.0 (ICS) and later, the Holo theme is used for the Android Application Style setting.
- An **Advanced** screen has been added to the Connection Editor to configure all settings beyond the required Server Address and Description.
- Certificate Management enhancements:
  - In Android 4.0 (Ice Cream Sandwich) and later, the user also imports certificates from the device's Credential Storage to the AnyConnect store. This is in addition to importing directly from the file system and importing from a specified server. See the User Certificate Management Enhancements section for more details.
  - User-authorized server certificates are now imported and stored in the AnyConnect certificate store, see the Server Certificate Management Enhancements section for details.
- **Email Logs** now prompt the user for a problem description and reproduction steps.

Android AnyConnect User Guide Available in EPUB Format

The Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.x is now available in EPUB format for download. Users will need an EPUB reader to view this format on their device. It can be accessed from the AnyConnect home screen by tapping **Menu > About > Online User Guide**.

Supported Android Devices

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

- Samsung Devices
- HTC Devices
- Kindle Devices

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

- AnyConnect for Android 4.0 Devices and later (ICS+)
- AnyConnect for Rooted Devices

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

Samsung Devices

Samsung AnyConnect Release 3.0.x and Samsung AnyConnect Legacy Release 3.0.x support the Samsung product lines listed below. The devices must be running the latest software update from Samsung. See the installation instructions in the *AnyConnect for Android User Guide* to determine which package applies to your device.

- ACE+
- ACE II
- Conquer 4G
- Galaxy Appeal
- Galaxy Beam
- Galaxy Exhilarate
- Galaxy Mini
- Galaxy Note
- Galaxy Note II
- Galaxy NoteIII
- Galaxy Note 10.1
- Galaxy Rush
- Galaxy S
- Galaxy S II
- Galaxy S III
- Galaxy S 4
- Galaxy Stellar
- Galaxy Tab 7 (WiFi only)
- Galaxy Tab 7.0 Plus & 7.7
- Galaxy Tab 8.9
- Galaxy Tab 10.1
- Galaxy Tab 2 7.0
- Galaxy Tab 2 10.1
- Galaxy W
- Galaxy Xcover
- Galaxy Y Pro
- Illusion
- Infuse
- Rugby
- Stratosphere
- Stratosphere II
- Transform Ultra

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

HTC Devices

HTC AnyConnect Release 3.0.x supports the HTC product lines listed at http://www.htcpro.com/enterprise/VPN. 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.

Note

- Currently, HTC devices running Android 4.3 and later should use the Cisco AnyConnect ICS+ package. Uninstall HTC AnyConnect before installing this package.
- Currently, all AT&T HTC devices should use the Cisco AnyConnect ICS+ package. Uninstall HTC AnyConnect before installing this package.
- The HTC Raider, also know as the HTC Holiday, does not work with Cisco AnyConnect. Cisco and HTC are working to address this issue.

Kindle Devices

Cisco AnyConnect (Kindle Tablet Edition) Release 3.0.x is available from Amazon for the following devices:

- Kindle Fire HD
- New Kindle Fire
- Kindle Fire HDX

Anyconnect for Kindle is supported by the Android VPN Framework and is equivalent in functionality to the AnyConnect ICS+ package.

AnyConnect for Android 4.0 Devices and later (ICS+)

AnyConnect ICS+ Release 3.0.x offers VPN connectivity supported by the Android VPN Framework (AVF) in Android 4.0 (Ice Cream Sandwich) or later. This package can be used on any Android device that is running ICS or later.

The 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 3.0.x 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 2.1or later. If you encounter issues, please report them to android-mobile-feedback@cisco.com, and we will make our best effort to resolve them.

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

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

Android AnyConnect Feature Matrix

Android Brand-Specific AnyConnect

For Samsung, HTC and Motorola supported and qualified 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 these devices.

Android AnyConnect Plus

For some Motorola supported and qualified devices (released after May 2012) Cisco provides this non-vendor specific packages that offers a full featured VPN experience that is equivalent in functionality to the brand-specific packages.

Android VPN Framework AnyConnect

For other Android devices that are unable to use the brand-specific AnyConnect package or AnyConnect Plus, 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. Kinde devices use this package also.

Android Rooted AnyConnect

Cisco also provides an AnyConnect package for rooted Android devices that is equivalent in functionality to the brand-specific packages. This package works on most rooted devices that are 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	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Tunneling	TLS/DTLS	Yes	Yes
	IPsec IKEv2	Yes	Yes
	IKEv2 - NAT-T	Yes	Yes
	IKEv2 - raw ESP	Yes	Yes
	Suite B support	Yes (IPsec only)	Yes (IPsec only)
	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 connection on profile import	Yes	Yes
	URI connect credential pre-fill	Yes	Yes

Table 1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted 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	Yes, regardless of the Auto Reconnect profile specification, AnyConnect Mobile always attempts to maintain the VPN as users move between 3G and WiFi networks.	
	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 the VPN is established.
	Pre-login banner	Yes	Yes
	Post-login banner	Yes	Yes
	Scripting	No	No
	Reconfigure VPN	Yes	Yes

Table 1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Tunnel Security	Network change monitoring	Yes	Yes
	Shim intercept/filtering	No	No
	Embedded firewall rules	No	No
	Filter support (iptables)	Yes	No
Authentication	Manual certificate import (get certificate)	Yes	Yes
	SCEP enrollment	Yes	Yes
	SCEP proxy	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

Table 1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
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
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

Table 1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
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
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	Yes	Yes
	Common criteria	No	No

Adaptive Security Appliance 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.

Note Cisco IOS routers do not support the Cisco AnyConnect Secure Mobility client for Android at this time.

ASA Release Requirements

- ASA Release 8.0(3) and Adaptive Security Device Manager (ASDM) 6.1(3) are the minimum releases that support AnyConnect for mobile devices.
- You must upgrade to ASA 9.0 to use the following mobile features:
  - IPsec IKEv2 VPN
  - Suite B cryptography
  - SCEP Proxy
  - Mobile Posture with AnyConnect 3.0 for mobile device

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.

Known Issues and Limitations

The following sections describe the known issues and limitations in the current AnyConnect 3.0.09xxx releases.

Known Compatibility Issues

- On Android 4.3 and later devices, the AnyConnect status icon may be duplicated, and also, may display regardless of the **Hide Icon** setting.
- Due to a bug in Android 4.3.1 (Issue #62073), users using the AnyConnect ICS+ package cannot enter non-fully qualified domain names. For example, users cannot type "internalhost", they must type "internalhost.company.com".
- The AT&T firmware updates on HTC One to Android 4.3 (software version: 3.17.502.3) do not support "HTC AnyConnect". Customers must uninstall "HTC AnyConnect", and install "AnyConnect ICS+". (HTC AnyConnect will work on the international edition, with software version of 3.22.1540.1). To check your software version do the following: Tap **Settings -> About -> Software information -> Software number**.
- Due to a known issue in Android 4.4 (Issue #64819) Split DNS will not work on Android 4.4. There is no workaround for this issue, a fix from Google is required.
- We are pleased to report that Android 4.4 (KitKat) bug Google Issue #61948 (AnyConnect users will experience High Packet Loss over their VPN connection /users will experience timeouts) has been resolved in Google's release of Android 4.4.1 which Google has begun distributing to some devices via Software Update. The following problem information is provided for reference:

  Due to a bug in Android 4.4 (Issue #61948, also see the Cisco Support Update), AnyConnect users will experience High Packet Loss over their VPN connection. This has been seen on the Google Nexus 5 running Android 4.4 with AnyConnect ICS+. Users will experience timeouts when attempting to access certain network resources. Also, in the ASA logs, a syslog message will appear with text similar to "Transmitting large packet 1420 (threshold 1405)."

  Until Google produces a fix for Android 4.4, VPN administrators may temporarily reduce the maximum segment size for TCP connections on the ASA by configuring the following **sysopt connection tcpmss <mss size>**. The default for this parameter is 1380 bytes, reduce this value by the difference between the values seen in the ASA logs. In the above example, the difference is 15 bytes; the value should thus be no more than 1365. Reducing this value will negatively impact performance for connected VPN users where large packets are transmitted.
- AnyConnect for Android may have connectivity issues when connecting to a mobile network using the IPv6 transition mechanism known as 464xlat. Known affected devices include the Samsung Galaxy Note III LTE connecting to the T-Mobile US network. This device defaults to an IPv6 only mobile network connection. Attempting a connection may result in a loss of mobile connectivity until the device is rebooted.

  To prevent this problem, use the AnyConnect ICS+ app, and change your device settings to obtain IPv4 network connectivity or connect using a Wi-Fi network.

  – For the Samsung Galaxy Note III LTE connecting to the T-Mobile US network, follow the *instructions provided by T-Mobile* to set the Access Point Name (APN) on your device, making sure *APN Protocol* is set to IPv4
- The AnyConnect ICS+ package may have issues when a private IP address range within the VPN overlaps with the range of the outside interface of the client device. When this route overlap occurs, the user may be able to successfully connect to the VPN but then be unable to actually access

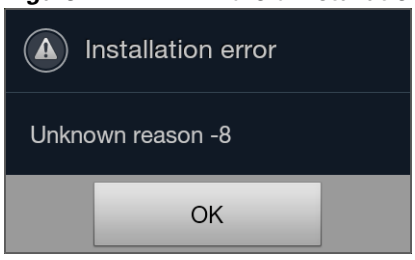
anything. This issue has been seen on cellular networks which use NAT (Network Address Translation) and assign addresses within the 10.0.0.0 - 10.255.255.255 range, and is due to AnyConnect having limited control of routes in the Android VPN framework. The vendor specific Android packages have full routing control and may work better in such a scenario.

- An Asus tablet running Android 4.0 (ICS) may be missing the tun driver. This causes AVF AnyConnect to fail.
- On a rooted device, in the superuser application preferences, Automatic response must be set to Prompt. Other settings may cause AnyConnect to hang.
- Due to Android issue 41037, when pasting text from the clipboard, a space is inserted in front of the text. In AnyConnect, when copying text such as a one time password, the user has to delete this erroneous white space.

Guidelines and Limitations

- Cisco IOS routers do not support the Cisco AnyConnect Secure Mobility client for Android at this time.
- 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



- 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.

Open Issues in AnyConnect 3.0.09269 for Mobile Devices

Identifier	Headline
CSCub83101	AC stuck in reconnecting, 'cannot initialize' msg, crash - Samsung only
CSCuc42233	AnyConnect automatically starts up after reboot on Samsung devices
CSCuc48692	Increase Android interface debounce timeout to 2 seconds, TND, wifi->3G
CSCuc58649	Some HTC devices get config files corrupted on device upgrade
CSCuc69491	Slow timeout on untrusted server prompt cancel for load balanced IKEv2
CSCuc88759	android - connect error sometimes with medium widget
CSCuc96528	Few strings remain untranslated
CSCud05728	android/iphone - misleading error when AAA server is down
CSCud06065	Interfaces shutting down on HTC Vigor/Rezound with ICS+ packages
CSCud18217	When tun is missing, display a clear, user-facing Critical Error msg
CSCui32781	Persistent AnyConnect icon in Android 4.3+
CSCud51366	AnyConnect cannot run under multiple users in Android Jelly Bean
CSCui07396	URI handler onerror and onsuccess params don't fire with AVF prompt
CSCui67259	Android SecureRandom vulnerability affects AnyConnect
CSCui83079	Mobile client can't handle some special characters in tunnel group names
CSCuj66504	DNS search domain not getting set on Android 4.3 (Google Bug ID#62073)
CSCuj97658	AnyConnect mobile incompatible with 464XLAT (IPv6 transition mechanism)
CSCul25513	VPN: libcurl getaddrinfo attempts to get ipv6 address but times out
CSCul33712	Additional support for different screen size and densities

Resolved Issues in AnyConnect 3.0.09269 for Mobile Devices

Identifier	Headline
CSCum74195	Split-DNS is not working under certain Carrier Network

Resolved Issues in AnyConnect 3.0.09242 for Mobile Devices

Identifier	Headline
CSCui45856	AnyConnect for Mobile cannot connect to non-default group non-std port
CSCul38446	DNS issues introduced by new Android API (4.3.1+)
CSCul38459	Unable to read external storage (Android 4.4+)

Resolved Issues in AnyConnect 3.0.09156 for Mobile Devices

Identifier	Headline
CSCuh09909	IKEv2 connections with IPv6 fail with Cisco IOS 15.4
CSCui30104	AnyConnect fails to initialize on Android 4.3

Resolved Issues in AnyConnect 3.0.09140 for Mobile Devices

Identifier	Headline
CSCuc58682	Device credential store functionality doesn't work on Jelly Bean
CSCug55568	Mobile anyconnect has to re-auth several times under cellular network
CSCug85145	[GCR] "Inefficient PackageManager Query"

Resolved Issues in AnyConnect 3.0.09129 for Mobile Devices

Identifier	Headline
CSCud00442	[UE] inconsistent behavior of Certificate URI Import timeout
CSCue57485	TND Profile settings are ignored when "Launch at startup" is enabled
CSCue81459	[Wording Issue] MMS Carrier Service notification needs to be reworded.

Resolved Issues in AnyConnect 3.0.09093 for Mobile Devices

Identifier	Headline
CSCuc91088	URI handler broken when device is localized to non-English language
CSCuc98877	AVF/ICS+ package unnecessarily requires iptables
CSCud02597	Cert Auth Fails Unexpectedly for Certain ASAs
CSCud02610	default certs generated by the asa cannot be verified by the client
CSCud02622	Server EKU bit settings cause openssl to mark cert as invalid
CSCud02741	android - TF201 Report of force close on connect after Jelly Bean update
CSCud02745	android - Nexus S: Report of a crash on connect
CSCud10778	android- Bad state if VpnService is destroyed during installation
CSCud12339	Server certificates missing EKU/KU fields should not be untrusted

Resolved Issues in AnyConnect 3.0.09073 for Mobile Devices

Identifier	Headline
CSCto94510	AC non-WinX clients are not requesting entire certificate chain
CSCtq33166	Unable to send/receive MMS messages while connected
CSCty38958	android - cert store shows both client and server certs after upgrade
CSCty45690	SCEP request not made with multiple certs and auto cert selection
CSCty61878	DNS servers not properly restored when split-dns is configured
CSCty75092	Certificate store unavailable after application upgrade causing hang
CSCtz15093	OpenSSL CMS PKCS #7 or S/MIME Decryption Routines MMA Security Bypass
CSCua16628	Device ID logic fails for Android tablets in 3G/4G only mode
CSCua21424	Spinning Issue and Error Message with URI handler
CSCua85457	AnyConnect: Could not get file list for /sdcard on HTC phones
CSCua94635	Removal of v6 address on public interface causes system to overwrite DNS
CSCuc06652	Investigate reduction of 2 second sleep to reduce wakeup/connect latency
CSCuc46848	AnyConnect fails to unparcel preferences from out of proc apps
CSCuc50965	Client may fail to start on config corruption

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.

AnyConnect 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.

AnyConnect License Agreements

For the end-user license agreement for this product, see Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 3.0.

For Open Source License information for this product, see Open Source Software Used in Cisco AnyConnect Secure Mobility Client, Release 3.0 for Mobile

Related Documentation

For more information, refer to the following documentation:

- Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.0
- Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0
- Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.x
- Navigating the Cisco ASA 5500 Series Documentation