Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.6.x for Android

AnyConnect for Release Notes

AnyConnect for

The AnyConnect Secure Mobility Client provides remote users with secure VPN connections to the Cisco ASA 5500 Series. It provides seamless and secure remote access to enterprise networks allowing installed applications to communicate as though connected directly to the enterprise network. AnyConnect supports connections to IPv4 resources over an IPv4 or IPv6 tunnel.

This document, written for system administrators of the AnyConnect Secure Mobility Client and the Adaptive Security Appliance (ASA) 5500, provides release specific information for AnyConnect running on

The AnyConnect app is available on Cisco does not distribute AnyConnect mobile apps. Nor can you deploy the mobile app from the ASA. You can deploy other releases of AnyConnect for desktop devices from the ASA while supporting this mobile release.

AnyConnect Mobile Support Policy

Cisco supports the AnyConnect version that is currently available in the app store; however, fixes and enhancements are provided only in the most recently released version.

AnyConnect Licensing

To connect to the ASA headend, an AnyConnect 4.x Plus or Apex license is required, trial licenses are available, see the Cisco AnyConnect Ordering Guide.

For the latest end-user license agreement, see Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 4.x.

For our open source licensing acknowledgments, see Open Source Software Used In Cisco AnyConnect Secure Mobility Client Release 4.x for Mobile

Android Supported Devices

Full support for Cisco AnyConnect on Android is provided on devices running Android 4.0 (Ice Cream Sandwich) through the latest release of Android.

Cisco AnyConnect on Kindle is available from Amazon for the Kindle Fire HD devices, and the New Kindle Fire. AnyConnect for Kindle is equivalent in functionality to the AnyConnect for Android package.

Per App VPN is supported in managed and unmanaged environments. In a managed environment using Samsung KNOX MDM, Samsung devices running Android 4.3 or later with Samsung Knox 2.0, are required. When using Per App in an unmanaged environment, the generic Android methods are used.

For the Network Visibility Module (NVM) capabilities, Samsung devices that are running Samsung Knox 2.8 or later (including 3.2), which requires Android 7.0 or later, are required. For configuration of NVM, the AnyConnect Profile Editor from AnyConnect 4.4.3 or later is also required. Earlier releases do not support mobile NVM configurations.

New Features

New Features in AnyConnect 4.6.01109 for Android Mobile Devices

This release of Cisco AnyConnect Secure Mobility Client for Android provides the following new capabilities:

- Support for SAML authentication

  The feature requires ASA version of 9.7.1.24, 9.8.2.28, 9.9.2.1 or above. Make sure that both the client and server versions are up-to-date to use this feature.

- Support for Remember Password

  This is an administrator-controlled feature through MDM configuration.

This release is also a maintenance release for all devices running earlier versions of AnyConnect on Android.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 6 and Known Compatibility Issues, on page 6 to be aware of current operational considerations.

Android AnyConnect Feature Matrix

The following table indicates the remote access features that are supported by Cisco AnyConnect on Android:

Category: Feature	Android VPN
Deployment and Configuration:	
Install or upgrade from application store.	Yes
Cisco VPN Profile support (manual import)	Yes
Cisco VPN Profile support (import on connect)	Yes
MDM configured connection entries	Yes
User-configured connection entries	Yes
Tunneling:	
TLS	Yes
Datagram TLS (DTLS)	Yes
IPsec IKEv2 NAT-T	Yes
IKEv2 - raw ESP	Yes
Suite B (IPsec only)	Yes
TLS compression	Yes
Dead peer detection	Yes

Category: Feature	Android VPN
Tunnel keepalive	Yes
Multiple active network interfaces	No
Per App Tunneling	Yes, Android 5.0+ or Samsung Knox
Full tunnel (OS may make exceptions on some traffic, such as traffic to the app store).	Yes
Split tunnel (split include).	Yes
Local LAN (split exclude).	No
Split-DNS	Yes, works with split include.
Auto Reconnect / Network Roaming	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
VPN on-demand (triggered by application)	No
Rekey	Yes
IPv4 public transport	Yes
IPv6 public transport	Yes, requires Android 5.0 or later.
IPv4 over IPv4 tunnel	Yes
IPv4 over IPv6 tunnel	Yes
IPv6 over IPv4 tunnel	Yes
IPv6 over IPv6 tunnel	Yes
Default domain	Yes
DNS server configuration	Yes
Private-side proxy support	Only support direct proxy mode on Android 10.
Proxy Exceptions	No
Public-side proxy support	No
Pre-login banner	Yes
Post-login banner	Yes
DSCP Preservation	Yes
Connecting and Disconnecting:	
VPN load balancing	Yes
Backup server list	Yes
Optimal Gateway Selection	No
Authentication:	

Category: Feature	Android VPN
Touch ID	No
SAML 2.0	Yes
Client Certificate Authentication	Yes
Online Certificate Status Protocol (OCSP)	Yes
Manual user certificate management	Yes
Manual server certificate management	Yes
SCEP legacy enrollment Please confirm for your platform.	Yes
SCEP proxy enrollment Please confirm for your platform.	Yes
Automatic certificate selection	Yes
Manual certificate selection	Yes
Smart card support	No
Username and password	Yes
Tokens/challenge	Yes
Double authentication	Yes
Group URL (specified in server address)	Yes
Group selection (drop-down selection)	Yes
Credential prefill from user certificate	Yes
Save password	No
User interface:	
Standalone GUI	Yes
Native OS GUI	No
API / URI Handler (see below)	Yes
UI customization	No
UI localization	Yes, app contains pre-packaged languages.
User preferences	Yes
Home screen widgets for one-click VPN access	Yes
AnyConnect specific status icon	Optional
Mobile Posture: (AnyConnect Identity Extensions, ACIDex)	
Serial number or unique ID check	Yes
OS and AnyConnect version shared with headend	Yes
AnyConnect NVM support	Yes, with specific Samsung Knox and MDM requirements.
URI Handling:	

Category: Feature	Android VPN
Add connection entry	Yes
Connect to a VPN	Yes
Credential pre-fill on connect	Yes
Disconnect VPN	Yes
Import certificate	Yes
Import localization data	Yes
Import XML client profile	Yes
External (user) control of URI commands	Yes
Reporting and Troubleshooting:	
Statistics	Yes
Logging / Diagnostic Information (DART)	Yes
Certifications:	
FIPS 140-2 Level 1	Yes

Adaptive Security Appliance Requirements

A minimum release of the ASA is required for the following features:

Note Refer to the feature matrix for your platform to verify the availability of these features in the current AnyConnect mobile release.

- You must upgrade to ASA 9.7.1.24, 9.8.2.28, 9.9.2.1 or later to use the SAML authentication feature. Make sure that both the client and server versions are up-to-date.
- You must upgrade to ASA 9.3.2 or later to use TLS 1.2.
- You must upgrade to ASA 9.0 to use the following mobile features:
  - IPsec IKEv2 VPN
  - Suite B cryptography
  - SCEP Proxy
  - Mobile Posture
- ASA Release 8.0(3) and Adaptive Security Device Manager (ASDM) 6.1(3) are the minimum releases that support AnyConnect for mobile devices.

Other Cisco Headend Support

AnyConnect SSL connectivity is supported on Cisco IOS 15.3(3)M+/15.2(4)M+.

AnyConnect IKEv2 connectivity is supported on Cisco ISR g2 15.2(4)M+

AnyConnect SSL and IKEv2 is supported on Cisco Firepower Threat Defense, release 6.2.1 and later.

Guidelines and Limitations for AnyConnect on Android

- The ASA does not provide distributions and updates for AnyConnect for Android. They are available only on Google Play.
- AnyConnect for Android supports only the Network Visibility Module, it does not support any other AnyConnect modules.
- The Android device supports no more than one AnyConnect profile, which is the last one received from a headend. However, a profile can consist of multiple connection entries.
- If users attempt to install AnyConnect on devices that are not supported, they receive the pop-up message`Installation Error: Unknown reason -8`. This message is generated by the Android OS.
- When users have 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.
- **DHE Incompatibility**

  With the introduction of DHE cipher support in AnyConnect release 4.6, incompatibility issues result in ASA versions before ASA 9.2. If you are using DHE ciphers with ASA releases earlier than 9.2, you must disable DHE ciphers on those ASA versions.

Known Compatibility Issues

- IPv6 on public and private interfaces.

  IPv6 is supported on both private and public transports using AnyConnect 4.05015 and later, on Android 5 and later. With this combination the following is now allowed: IPv4 over an IPv6 tunnel, IPv6 over an IPv6 tunnel.

  This is in addtion to the previously allowed tunnel configuratons on earlier AnyConnect and Android releases: IPv4 over an IPv4 tunnel, and IPv6 over an IPv4 tunnel.

  Note Due to Google issue 65572, IPv6 over IPv4 does not work on Android 4.4. You must use Android 5 or later.

- Battery saver and AnyConnect:

  - Android 5.0 introduced battery saver capabilities that block background network connectivity on your device. When battery saver is enabled, AnyConnect will transition to the Paused state if it is in the background. To work around this on Android 5.0, users may turn off battery saver via the device settings: Settings -> Battery -> Battery saver or from the notification bar.
  - In Android 6.0+, when AnyConnect transitions to the Paused state as a result of battery saver, you see a popup with the option to make AnyConnect part of the allowed list from battery saver mode. Making AnyConnect part of the allowed list provides a battery savings without impacting AnyConnect's ability to run in the background.
  - Once AnyConnect is paused due to the batter saver, a manual reconnect is necessary to bring AnyConnect out of the Paused state, regardless of your action to turn off battery saver or to add AnyConnect to the allowed list.

- Split DNS does not work on any Android 4.4 device, and also does not work on Samsung 5.x Android devices. For Samsung devices, the only workaround is to connect to a group with split DNS disabled. On other devices you must upgrade to Android 5.x to receive the fix for this problem.

  This is due to a known issue that is present in Android 4.4 (Issue #64819), fixed in Android 5.x, but not incorporated into Samsung 5.x android devices.

- Due to a bug in Android 5.x (Google Issue #85758, Cisco Issue # CSCus38925), if the AnyConnect app is closed from the recent apps screen it may not operate properly. To restore proper operation, terminate AnyConnect in **Settings** and then restart it.

- On Samsung mobile devices the **Settings > Wi-Fi > Smart network switch** allows switching from WIFI to LTE to maintain a stable Internet connection (when the Wi-Fi connection is not optimum). This also results in a pause and reconnect of the active VPN tunnel. Cisco recommends turning this off, since it may result in continuous reconnects.

- On Android 5.0 (Lollipop), which supports multiple active users, the VPN connection tunnels data for a single user only, not for all users on the device. Background data flow may be occurring in the clear.

- Due to a bug in Android 4.3.1(Google 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). Check your software version on your device at **Settings > About > Software information > Software number**.

- We are pleased to report that Google Issue #70916, VPN connections will fail to connect if the administrator has set the MTU for Android tunnels lower than 1280, has been resolved in Android 5.0 (Lollipop). The following problem information is provided for reference:

  Due to a regression in Android 4.4.3,(Google Issue #70916, Cisco CSCup24172), VPN connections will fail to connect if the administrator has set the MTU for Android tunnels lower than 1280. This issue has been reported to Google and will require a new version of the OS to correct the regression introduced in Android 4.4.3. To workaround this problem, ensure that the head-end administrator has not configured the tunnel MTU to be lower than 1280.

  When encountered, the message displayed to the end user is: `System configuration settings could not be applied. A VPN connection will not be established`, and AnyConnect debug logs will report:

```
E/vpnandroid( 2419): IPCInteractionThread: NCSS: General Exception occured, telling
client
E/vpnandroid( 2419): java.lang.IllegalStateException: command '181 interface fwmark
rule add tun0'
failed with '400 181 Failed to add fwmark rule (No such process)'
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1473)
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1419)
E/vpnandroid( 2419): at
com.cisco.android.nchs.aidl.IICSSupportService$Stub$Proxy.establish
(IICSSupportService.java:330)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.VpnBuilderWrapper.establish
(VpnBuilderWrapper.java:137)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.NCSSIPCServer.callServiceMethod
(NCSSIPCServer.java:233)
E/vpnandroid( 2419): at
com.cisco.android.nchs.ipc.IPCInteractionThread.handleClientInteraction
(IPCInteractionThread.java:230)
E/vpnandroid( 2419): at com.cisco.android.nchs.ipc.IPCInteractionThread.run
(IPCInteractionThread.java:90)
E/acvpnagent( 2450): Function: ApplyVpnConfiguration
File: NcssHelper.cpp Line: 740 failed to establish VPN
E/acvpnagent( 2450): Function: PluginResult AndroidSNAKSystem::configDeviceForICS()
File: AndroidSNAKSystem.cpp Line: 665 failed to apply vpn configuration
E/acvpnagent( 2450): Function: virtual PluginResult
AndroidSNAKSystem::ApplyConfiguration()
File: AndroidSNAKSystem.cpp Line: 543 Failed to Configure System for VPN.
```

- 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.
- Android security rules prevent the device from sending and receiving multimedia messaging service (MMS) messages while a VPN connection is up. Most devices and service providers display a notification if you try to send an MMS message while the VPN connection is up. Android permits sending and receiving of messages when the VPN is not connected.
- Due to Google Isssue 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.

Open and Resolved AnyConnect Issues

The Cisco Bug Search Tool, https://tools.cisco.com/bugsearch/, has detailed information about the following open and resolved issues in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://tools.cisco.com/RPF/register/register.do.

Open Issues in AnyConnect for Android

Identifier	Headline
CSCuz90837	Android: IPv6 LTE user not able to access v4-only head-end
CSCvb26006	Android 7.0 - DNS not functioning in split DNS configurations

Resolved Issues in AnyConnect 4.6.02078 for Android

Identifier	Headline
CSCvb26006	Android 7.0 - DNS not functioning in split DNS configurations.

Resolved Issues in AnyConnect 4.6.1110 for Android

Identifier	Headline
CSCvk64883	Android Enterprise per-app VPN (whitelist) config not working

Resolved Issues in AnyConnect 4.6.00143 for Android

Identifier	Headline
CSCtu30260	AnyConnect support on Chromebook
CSCvf71607	[android] connection editor has blank text on buttons in android 8.0
CSCvf80233	[android] Knox setAutoRetryOnConnectionError should apply to postauth connect failures

Identifier	Headline
CSCvi29881	[android]Missing IPsec Auth Mode Mapping for KNOX JSON profile parsing

Defect Resolution

Problem: Samsung devices are triggering UnrecoverableKeyException, causing the cert to be deleted and the cert auth to fail

Solution: Move the UnrecoverableKeyException handling code from KsCertStore to AndroidKeyStore

AnyConnect Mobile Related Documentation

For more information refer to the following documentation:

- AnyConnect Release Notes
- AnyConnect Administrator Guides
- Navigating the Cisco ASA Series Documentation