Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.0.x for Android

AnyConnect for Android Release Notes

AnyConnect for Android Mobile Devices

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 and IPv6 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 Android devices.

The AnyConnect app is available on Google Play, except for the Kindle package, which is available on Amazon.com. 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

Cisco AnyConnect Android Beta Testing

Beta builds of AnyConnect are made available for pre-release testing.

To be eligible to receive these versions, opt-in to receive Beta builds using this Google Play link: https://play.google.com/apps/testing/com.cisco.anyconnect.vpn.android.avf

You may opt out later using this same Google Play link. After opting out, you will be required to uninstall the Beta build and reinstall the latest non-Beta version of AnyConnect.

Report issues found during beta testing promptly by sending email to Cisco at ac-mobile-feedback@cisco.com. The Cisco Technical Assistance Center (TAC) does not address issues found in Beta versions of AnyConnect.

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 4.0.09039 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices is a maintenance release for all devices running earlier versions of AnyConnect on Android. It addresses a compatibility issue with a pre-released version of Android.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.09038 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices is a maintenance release for all devices running earlier versions of AnyConnect on Android. See Resolved Issues in AnyConnect 4.0.09038 for Android, on page 21 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.09030 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices is a maintenance release for all devices running earlier versions of AnyConnect on Android. See Resolved Issues in AnyConnect 4.0.09030 for Android, on page 21 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.09029 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices is a maintenance release. It addresses a regression in the 4.0.05062 release: CSCve86218:Android: 4.0.09027 start up fails on Intel Android (x86) devices - Regression from 4.0.05062. See Resolved Issues in AnyConnect 4.0.09029 for Android, on page 21 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.09027 for Android Mobile Devices

This release of Cisco AnyConnect Secure Mobility Client for Android includes Network Visibility Module (NVM) capabilities for MDM configured Samsung KNOX mobile devices.

The Network Visibility Module (NVM) collects rich flow context from an endpoint on or off premise and provides visibility into network connected devices and user behaviors when coupled with a Cisco solution such as Stealthwatch, or a third-party solution such as Splunk. The enterprise administrator can then do capacity and service planning, auditing, compliance, and security analytics.

NVM for Mobile requires the following:

- Samsung devices that are running Samsung Knox 2.8 or later, which requires Android 7.0 or later. These devices must be configured using an MDM solution. Check with your MDM solution provider for availability and support of NVM.
- The AnyConnect Profile Editor from AnyConnect 4.4 MR 3 or later. Earlier releases do not support mobile NVM configurations.
- TND (Trusted Network Detection) configured in the AnyConnect VPN Profile for NVM to work.
- AnyConnect Apex licensing.

This version of Android is also a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.09027 for Android, on page 21 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05062 for Android Mobile Devices

This vesion of Android is a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.05062 for Android, on page 21 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05057 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices includes an enhancement for MDM deployments allowing them to manually re-connect.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05054 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices is a maintenance release to address a regression in the previous release, CSCvb32905, Android: Deflate compression does not work 4.0(5053). See Resolved Issues in AnyConnect 4.0.05054 for Android, on page 22 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05053 for Android Mobile Devices

This version of Android is a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.05053 for Android, on page 22 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05042 for Android Mobile Devices

This vesion of Android is a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.05042 for Android, on page 22 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05041 for Android Mobile Devices

This release of AnyConnect for Android contains the following updates:

- Updates for the May 2016 OpenSSL Vulnerabilities.
- The Android AnyConnect client now supports OCSP (Online Certificate Status Protocol).

  This allows the client to query the status of individual certificates in real time by making a request to the OCSP responder and parsing the OCSP response to get the certificate status. OCSP is used to verify the entire certificate chain. There is a five second timeout interval per certificate to access the OCSP responder.

  The Android user can enable or disable OCSP verification in the Anyconnect settings activity. We have added new API's in our framework which can be used by MDM administrators to control this feature remotely. Currently we are supporting Samsung and Google MDM.

- Android now supports Strict Certificate Trust Mode.

  If selected, when authenticating remote security gateways, AnyConnect disallows any certificate that it cannot verify. Instead of prompting the user to accept these certificates, the client fails to connect. This overrides the Block Untrusted Server setting and prompts. If not selected, the client prompts the user to accept the certificate. This is the default behavior.

  We strongly recommend that you enable Strict Certificate Trust for the AnyConnect client. The Android user can enable or disable this mode in the Anyconnect settings activity. Also, there are API's in our framework which can be used by MDM administrators to control this feature remotely.

This vesion of Android is also a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.05041 for Android, on page 22 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05034 for Android Mobile Devices

This release of AnyConnect for Android contains the following updates:

- Certificate Import from the System Certificate Store to the AnyConnect Certificate Store can be accomplished using a new **keychainalias** parameter which is now part of the **create** URI action. This enhancement is for the Android mobile platform only.

  The following example creates a new connection entry named *SimpleExample* whose IP address is set to *vpn.example.com* with the certificate named *client* assigned to it for authentication.

  anyconnect://create/?name=*SimpleExample***&host=***vpn.example.com***&keychainalias=***client*

  See *Automate AnyConnect Actions Using the URI Handler* in the *AnyConnect on Mobile Devices* chapter of the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.0 for URI details.

- How the Device Unique Identifier is determined in AnyConnect.

  Upon a fresh installation, or after the user clears the application data, AnyConnect now generates a unique 256-byte device ID, which is based on the Android ID. This ID replaces the legacy 40-byte device ID based on the IMEI and MAC address generated in earlier releases.

  If an earlier version of AnyConnect is installed, a legacy ID has already been generated. After upgrading to this version of AnyConnect, this legacy ID continues to be reported as the Device Unique ID until the user clears the application data or uninstalls AnyConnect.

  Generated device IDs can be viewed after the initial 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, or on the **About** Screen.

  

  Note DAP policies on the secure gateway will need to be updated to use the new device IDs.

  See *Android Mobile Posture Device ID Generation* in the *AnyConnect on Mobile Devices* chapter of the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.0 for Device ID details.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05026 for Android Mobile Devices

This version of AnyConnect for Android is a maintenance release. See Resolved Issues in AnyConnect 4.0.05026 for Android, on page 23 for updates.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05024 for Android Mobile Devices

This version of AnyConnect for Android is a maintenance release. See Resolved Issues in AnyConnect 4.0.05024 for Android, on page 23 for updates.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05023 for Android Mobile Devices

This version of AnyConnect for Android includes the following changes:

- The previous Samsung Knox and AnyConnect ICS+ packages have been combined into a single package called AnyConnect for Android. This app requires Android 4.0 or later, and supports all features in the previous apps.
    - The equivalent AnyConnect for Kindle package is still available via the Amazon Appstore for Kindle devices.
    - As before, Per App VPN is supported in a managed environment when configured using Samsung KNOX MDM. This requires Samsung devices running Android 4.3 or later with Samsung Knox 2.0. Otherwise, Per App VPN uses the Android framework to implement Per App VPN.
- AnyConnect can now use the TIMA KeyStore for client certificates if it is enabled.
- 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. In Android 5.0 the user can turn battery saver off if desired. This can be done through the Notifications. AnyConnect will automatically reconnect when battery saver is turned off. This is the first thing to check if your VPN pauses unexpectedly.
    - In Android 6.0, when AnyConnect is paused the user will be taken to the Battery Optimization activity, **Settings -> Battery -> Battery Optimization**, where they can set the AnyConnect app as allowed. Add AnyConnect to the allowed list by selecting **All apps** from the drop down and setting AnyConnect to **Don't optimize**. After allowing AnyConnect a manual reconnect is necessary to bring AnyConnect out of the Paused state.
- Resolution of CSCux41420: OpenSSL December 2015 vulnerabilities. See Resolved Issues in AnyConnect 4.0.05023 for Android, on page 23 for other resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05016 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices is a maintenance release to address the following localization and UI issues.

- CSCux39537— Language localization does not work on AnyConnect 4.0.05015
- CSCux05758—Android M displays anyconnect icons in monochrome/black&white color

The following Android packages have been updated:

- AnyConnect ICS+, for all Android 4.0 and later devices.
- Cisco AnyConnect (Kindle Tablet Edition), AnyConnect ICS+ re-packaged for Kindle devices.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05015 for Android Mobile Devices

Cisco AnyConnect 4.0.05015 adds support for:

- Android 6.0 (Marshmallow)
- 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
  - 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.
- Improved support for Nexus 5X and 6P phones
- More consistent OS support for IPv6

Also see additional Resolved Issues in AnyConnect 4.0.05015 for Android, on page 23.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01372 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices is a maintenance release to address regressions. The following Android packages have been updated:

- AnyConnect ICS+, for all Android 4.0 and later devices.
- Cisco AnyConnect (Kindle Tablet Edition), AnyConnect ICS+ re-packaged for Kindle devices.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01366 for Android Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Android devices is a maintenance release to address a URI Handler regression in 4.0.01359. The following Android packages have been updated:

- AnyConnect ICS+, for all Android 4.0 and later devices.
- Cisco AnyConnect (Kindle Tablet Edition), AnyConnect ICS+ re-packaged for Kindle devices.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01359 for Android Mobile Devices

The following Android packages have been updated:

- AnyConnect ICS+, for all Android 4.0 and later devices.
- Cisco AnyConnect (Kindle Tablet Edition), AnyConnect ICS+ re-packaged for Kindle devices.

This update of Cisco AnyConnect Secure Mobility Client for Android devices addresses OpenSSL 2015 Vulnerabilities for June and July. It is also a maintenance release for Android devices running earlier versions. See Resolved Issues in AnyConnect 4.0.01359 for Android, on page 24 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01332 for Android Mobile Devices

AnyConnect 4.0.01332 for Android is a maintenance release for the AnyConnect ICS+ package only. It addresses a compatibility issue with Android M Dev Preview / Android 5.1.1 which prevented AnyConnect from operating on certain devices.

See Resolved Issues in AnyConnect 4.0.01332 for Android, on page 24 for all resolved issues

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01302 for Android Mobile Devices

AnyConnect 4.0.01302 for Android is a maintenance release for the Samsung AnyConnect package only. It addresses a critical issue (CSCuu04642) in the previous release of this package.

Note This is the last release of this package. Transition to using the AnyConnect ICS+ or AnyConnect for Samsung Knox package.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01287 for Android Mobile Devices

The following packages are available with this release:

- AnyConnect for Samsung Knox, for Per App VPN support on Samsung devices.
- Samsung AnyConnect, for legacy Samsung device support.

Note This is the last release of this package. Transition to using the AnyConnect ICS+ or AnyConnect for Samsung Knox package.

- AnyConnect ICS+, for all Android 4.0 and later devices.
- Cisco AnyConnect (Kindle Tablet Edition), AnyConnect ICS+ re-packaged for Kindle devices.

Cisco AnyConnect release 4.0.01287 includes the following:

- Support for Android 5.0 on Samsung devices
- Additional localization support, see below
- Resolution of CSCut46503: MARCH 2015 OpenSSL Vulnerabilities

It is also a maintenance release for Android devices running earlier versions. See Resolved Issues in AnyConnect 4.0.01287 for Android, on page 25 for all resolved issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Android Known Compatibility Issues, on page 17 to be aware of current operational considerations.

Additional Localization

AnyConnect 4.0 for mobile devices now includes the following additional language translations in the AnyConnect Android app:

- Chinese (Taiwan) (zh-tw)
- Dutch (nl-nl)
- French (fr-fr)
- Hungarian (hu-hu)
- Italian (it-it)
- Portuguese (Brazil) (pt-br)
- Russian (ru-ru)
- Spanish (es-es)

See *Localization on Mobile Devices* in the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.0 for mobile localization options and details.

New Features in AnyConnect 4.0.01233 for Android Mobile Devices

Cisco AnyConnect 4.0.01233 resolves CSCus42726: JANUARY 2015 OpenSSL Vulnerabilities.

It is also a maintenance release for Android devices running earlier versions, and it includes a fix for CSCus37382 which was causing Intel Android devices to fail to connect. See Resolved Issues in AnyConnect 4.0.01233 for Android, on page 25 for all resolved issues.

The following packages are available with this release:

- Samsung Knox AnyConnect
- Samsung AnyConnect
- AnyConnect ICS+
- Cisco AnyConnect (Kindle Tablet Edition)

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01196 for Android Mobile Devices

The following packages are available with this release:

- Samsung Knox AnyConnect
- Samsung AnyConnect
- AnyConnect ICS+
- Cisco AnyConnect (Kindle Tablet Edition)
- HTC AnyConnect

  This first 4.0 release of HTC Anyconnect includes the previously announced TLS 1.2 capabilities and is available for Android 4.x releases only. HTC AnyConnect does not support Android 5.0 and therefore Per App VPN. HTC devices running Android 5.0 or later must install the AnyConnect ICS+ package.

Note This is the last release of HTC AnyConnect. Please transition to the AnyConnect ICS+ package as soon as possible.

Other Updates

Cisco AnyConnect 4.0.01196 is a maintenance release for Android devices running earlier versions. See New Features in AnyConnect 4.0.01196 for Android Mobile Devices, on page 10.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01176 for Android Mobile Devices

The following packages are available with this release:

- Samsung Knox AnyConnect

  This initial release of AnyConnect for Samsung Knox offers full 4.0 feature support including Per App VPN and TLS 1.2.

- Samsung AnyConnect

  This initial 4.0 release of Samsung Anyconnect includes TLS 1.2, but does not support Per App VPN.

- AnyConnect ICS+

  This is an update of AnyConnect ICS+, which has previously included support for both TLS 1.2 and Per App VPN.

- Cisco AnyConnect (Kindle Tablet Edition)

  This update of AnyConnect Kindle now includes TLS 1.2, but does not support Per App VPN.

Other Updates

Cisco AnyConnect 4.0.01176 is also a maintenance release for Android devices running earlier versions. See Resolved Issues in AnyConnect 4.0.01176 for Android, on page 25.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01156 for Android Mobile Devices

Note Only the AnyConnect ICS+ package is available with this release. Additional Cisco AnyConnect packages will be forthcoming.

TLS 1.2

AnyConnect 4.0 now supports TLS version 1.2 with the following additional cipher suites:

- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-SHA256
- AES256-SHA256
- AES128-SHA256

Note AnyConnect TLS 1.2 requires a secure gateway that also supports TLS 1.2. This is available in release 9.3(2) of the ASA on 5500-X models.

Other Updates

Cisco AnyConnect 4.0.01156 is a maintenance release for Android devices running earlier versions of the AnyConnect ICS+ package. See Resolved Issues in AnyConnect 4.0.01156 for Android, on page 25.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01110 for Android Mobile Devices

Note

- Only the AnyConnect ICS+ package is available with release 4.0.01110. Additional Cisco AnyConnect packages will be forthcoming.
- The new AnyConnect Per App VPN Tunneling feature is available for devices running Android 5.0 (Lollipop) or later only.

Per App VPN Tunneling

AnyConnect 4.0 for mobile devices has been enhanced to provide Per App VPN tunneling in addition to traditional system-tunneling. Per App VPN tunneling requires:

- ASA 9.3.1 or later to configure Per App VPN tunneling.
- An AnyConnect v4.0 Plus or Apex license.

Note AnyConnect Essentials or Premium licenses do not support Per App VPN. Customers with Premium or Essentials licenses are eligible for AnyConnect 4.0 migration licenses, see the Cisco AnyConnect Ordering Guide for details.

Traditional VPN system-tunneling, as a full-tunneling or split-tunneling configuration, directs packets over the tunnel or in-the-clear based on the destination address. Per App VPN tunneling, operating at Layer 7, directs data over the tunnel or in-the-clear based on the originating app. Per App VPN is split tunneling that allows only data from approved apps to reach the enterprise network.

In Per App VPN tunneling mode, a connection is established for a specific set of apps on the mobile device. The set of apps which AnyConnect tunnels data for are defined by the administrator on the ASA headend using the AnyConnect Enterprise Application Selector tool and the ASA Custom Attributes mechanism. This list of identified and approved apps is sent to the AnyConnect client and used to enforce Per App VPN tunneling on the device. For all other apps not on the list, data is sent outside of the tunnel or in-the-clear.

If you are using a Mobile Device Manager in your environment to configure and control mobile devices on your network, your MDM must configure mobile devices to tunnel the same list of apps that AnyConnect is configured to tunnel. A discrepancy in the set of tunneled apps between the ASA headend and the Mobile Device Manager may cause unexpected app behavior.

AnyConnect determines which mode it operates in based on configuration information received from the ASA headend. Specifically, the presence or absence of a Per App VPN custom attribute in the Group Policy or Dynamic Access Policy (DAP) associated with the connection when the session is being established. If the Per App VPN list is present, AnyConnect operates in Per App VPN mode; if it is absent, AnyConnect operates in system-tunneling mode.

Other Updates

Cisco AnyConnect 4.0.01110 is a maintenance release for Android devices running earlier versions of the AnyConnect ICS+ package. See Resolved Issues in AnyConnect 4.0.01110 for Android, on page 26.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01093 for Android Mobile Devices

Cisco AnyConnect 4.0.01093 supports the Android 5.0 (Lollipop) OS.

Note

- Only the AnyConnect ICS+ package is available with release 4.0.01093. Additional Cisco AnyConnect packages will be forthcoming.
- Developer preview versions of Android 5.0 are not supported by AnyConnect. You must use the released version after it is made available.

This AnyConnect release is also a maintenance release for Android devices running earlier versions of AnyConnect 3.0 for Android. See Resolved Issues in AnyConnect 4.0.01093 for Android, on page 26.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Guidelines and Limitations for AnyConnect on Android, on page 17 and Known Compatibility Issues, on page 17 to be aware of current operational considerations.

Refer to the following AnyConnect 3.0 documents when using this release:

- Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.0.x for Android
- Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0

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

Category: Feature	Android VPN
IPsec IKEv2 NAT-T	Yes
IKEv2 - raw ESP	Yes
Suite B (IPsec only)	Yes
TLS compression	Yes
Dead peer detection	Yes
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

Category: Feature	Android VPN
Connecting and Disconnecting:	
VPN load balancing	Yes
Backup server list	Yes
Optimal Gateway Selection	No
Authentication:	
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

Category: Feature	Android VPN
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:	
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 9.3.2 or later to use Per App VPN tunneling mode.
- 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

- AnyConnect for Android supports only the VPN features that are strictly related to remote access.
- AnyConnect for Android supports only the Network Visibility Module. It does not support any other AnyConnect modules.
- The ASA does not provide distributions and updates for AnyConnect for Android. They are available only on Google Play.
- AnyConnect for Android supports connection entries that the user adds and connection entries populated by an AnyConnect profile pushed by an ASA. 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 macOS to decompress AnyConnect log files.

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
CSCuu08852	Android 5.0 Samsung: Split DNS fails
CSCuz90837	Android: IPv6 LTE user not able to access v4-only head-end
CSCvb26006	Android 7.0 - DNS not functioning in split DNS configurations
CSCvf05743	Android: Wi-Fi Assistant feature conflicts with AnyConnect

Resolved Issues in AnyConnect 4.0.09039 for Android

Identifier	Headline
CSCvf62248	Android: 9038 fails to start - Pixel XL with Android O pre-release - Failed to bind VpnService

Resolved Issues in AnyConnect 4.0.09038 for Android

Identifier	Headline
CSCve16765	Android: AUP should be displayed whenever there is a update in AUP string in NVM profile.
CSCve93100	Android: NVM doesn't start after upgrade from unsupported to supported AC.
CSCvf15961	Android: Exporter crashes when new NVM profile is registered
CSCvf19436	Android: AC App crashed when upgrading AC from unsupported to supported NVM after VPN connection
CSCvf19976	NVM service does not show up in the process status after NVM installation .
CSCvf27193	[android] Incorrect local IP parsed for ppp interface
CSCvf33882	Android: AUP is not updating when AUP screen is open and admin pushing new profile.
CSCvf40976	Android: Cached packets are not seen after device reboot.

Resolved Issues in AnyConnect 4.0.09030 for Android

Identifier	Headline
CSCvf14983	Android: Airwatch Knox incompatibility

Resolved Issues in AnyConnect 4.0.09029 for Android

Identifier	Headline
CSCve86218	Android: 4.0.09027 start up fails on Intel Android (x86) devices- Regression from 4.0.05062

Resolved Issues in AnyConnect 4.0.09027 for Android

Identifier	Headline
CSCuz52238	Android: Portuguese translation error crianças s/b conectad
CSCve49663	iOS/Android: Backup connection entry fails to be tried on ATT LTE

Resolved Issues in AnyConnect 4.0.05062 for Android

Identifier	Headline
CSCuy12161	AnyConnect Should No Longer Require KeyAgreement in Server Certificate
CSCuz21058	Upgrade from 4.0.05026 to 5.0.05034 and connection entry not displayed
CSCvb99286	Android 5.1.1 Fails to locate Gateway on 4G network
CSCvc09205	Android 6+ RA-VPN sessions shown with the dummy mac address 02:00:00:00:00:00 in ISE

Resolved Issues in AnyConnect 4.0.05057 for Android

Identifier	Headline
CSCva72042	[Android Knox] Cannot manually reconnect after managed config disconnect

Resolved Issues in AnyConnect 4.0.05054 for Android

Identifier	Headline
CSCvb32905	Android: Deflate compression does not work 4.0(5053)

Resolved Issues in AnyConnect 4.0.05053 for Android

Identifier	Headline
CSCuh85179	LAT 1 - AnyConnect - JA - Android - banner - English
CSCul21034	Loc:English Strings in Creating connection profile using URI Handler GUI
CSCuo47016	XMLSoft libxml2 Decoding Heap-Based Buffer Underflow Vulnerability
CSCuz46926	LAT1-Anyconnect-Mobile-Global-Step 1-5-Harcoded-item-loc
CSCuz46930	LAT1_ Anyconnect_Mobile_step4_GL_Hardcorded-Item-Loc
CSCuz46941	LAT1-Anyconnect-Global-Mobile-Step 9-Hardcoded-Item-Loc
CSCuz52238	Android: Portuguese translation error crianas s/b conectado
CSCva72042	[Android Knox] Cannot manually reconnect after managed config disconnect
CSCvb18501	[Android] Support always-on for managed profiles.

Resolved Issues in AnyConnect 4.0.05042 for Android

Identifier	Headline
CSCuz52238	Android: Portuguese translation error criancas s/b conectado

Resolved Issues in AnyConnect 4.0.05041 for Android

Identifier	Headline
CSCuz52506	Evaluation of anyconnect for OpenSSL May 2016

Resolved Issues in AnyConnect 4.0.05034 for Android

None

Resolved Issues in AnyConnect 4.0.05026 for Android

Identifier	Headline
CSCuy54600	Evaluation of anyconnect for OpenSSL March 2016
CSCuy79577	Android: AnyConnect fails to start on Android N

Resolved Issues in AnyConnect 4.0.05024 for Android

Identifier	Headline
CSCux05472	[Android] Split DNS broken on M

Resolved Issues in AnyConnect 4.0.05023 for Android

Identifier	Headline
CSCux41420	OpenSSL December 2015 vulnerabilities
CSCux42287	AC status becomes Paused (no network) on Marshmallow.

Resolved Issues in AnyConnect 4.0.05016 for Android

Identifier	Headline
CSCux05758	[android] M displays anyconnect icons in monochrome/black&white color
CSCux39537	Language localization does not work on AnyConnect 4.0.05015

Resolved Issues in AnyConnect 4.0.05015 for Android

Identifier	Headline
CSCui67259	Android SecureRandom vulnerability affects AnyConnect
CSCup35390	[Tunnel All DNS] It is always set to true on the mobile platform
CSCut46503	MARCH 2015 OpenSSL Vulnerabilities
CSCuv38716	unable to import certificate using URI handler on Android 5.0.1
CSCuw22064	Unable to make all necessary routing table modifications

Resolved Issues in AnyConnect 4.0.05005 for Android

Identifier	Headline
CSCui67259	Android SecureRandom vulnerability affects AnyConnect

Identifier	Headline
CSCup35390	[Tunnel All DNS] It is always set to true on the mobile platform
CSCur34245	iOS - Wrong UDID reported - changing device and restoring from backup
CSCut46503	MARCH 2015 OpenSSL Vulnerabilities
CSCuv38716	unable to import certificate using URI handler on Android 5.0.1

Resolved Issues in AnyConnect 4.0.01372 for Android

Identifier	Headline
CSCuv61121	One time Crash after user upgrades from previous version of AC
CSCuv65592	Android AC - Head-end profiles disappear when reboot or exit AC UI

Resolved Issues in AnyConnect 4.0.01366 for Android

Identifier	Headline
CSCuv61128	URI Handler no longer works on Android - Regression

Resolved Issues in AnyConnect 4.0.01359 for Android

Identifier	Headline
CSCuq29287	AnyConnect Android Un-restrictive Activity Access Vulnerability
CSCuu60485	Android: Remove Dependency Busybox
CSCuu83398	OpenSSL June 2015 Vulnerabilities - AnyConnect
CSCuv07004	Cannot switch to different group during VPN profile creation
CSCuv26246	OpenSSL July 2015 vulnerability - AnyConnect

Resolved Issues in AnyConnect 4.0.01332 for Android

Identifier	Headline
CSCur31959	Enhancement: Android DSCP preservation support
CSCut21232	Localization Selection string search criteria needs to be optimized
CSCuu18508	[UE] AnyConnect Warming notification message needs a different color
CSCuu53359	Android: LoggingActivity crash
CSCuu59997	AnyConnect fails to connect on Android M Dev Prev MPZ44Q / Nexus 6 5.1.1

Resolved Issues in AnyConnect 4.0.01302 for Android

Identifier	Headline
CSCuu04642	VPN: Android Samsung AnyConnect (Legacy) package does not work

Resolved Issues in AnyConnect 4.0.01287 for Android

Identifier	Headline
CSCuq64158	Samsung AC client doesn't query ASA VPN DNS servers for SRV type records
CSCus73367	Samsung packages broken with Android 5.0 Selinux CTS update
CSCut46503	MARCH 2015 OpenSSL Vulnerabilities

Resolved Issues in AnyConnect 4.0.01233 for Android

Identifier	Headline
CSCuo24940	AnyConnect renders UI dialog from arbitrary host.
CSCur30168	Knox: No way to reconnect profile if user Cancel vpn connection
CSCus37382	Android IA: The local network may not be trustworthy - unable to connect
CSCus42726	JANUARY 2015 OpenSSL Vulnerabilities

Resolved Issues in AnyConnect 4.0.01196 for Android

Identifier	Headline
CSCui83079	Mobile client can't handle some special characters in tunnel group names
CSCuq29214	AnyConnect 3.0.09431 Android OS least-privilege Vulnerability
CSCuq99308	AnyConnect closes IPsec connection upon rekey
CSCur934938	Android:AC 4.0 IKEv2 EAP-MD5 failing to ASR

Resolved Issues in AnyConnect 4.0.01176 for Android

Identifier	Headline
CSCur97471	TLS 1.2 Update: AC Mobile fails cert auth connecting to ASA v.9.3.2

Resolved Issues in AnyConnect 4.0.01156 for Android

Identifier	Headline
CSCup18505	AnyConnect Widget disappears after 10 second of connection

Identifier	Headline
CSCur37528	Android: AnyConnect 4.0 DART zip does not open properly on W7 (corrupt?)
CSCur49254	Android: Username/pw prompt unavailable after return via notification
CSCur51577	Android: AnyConnect 4.0 not fully exiting with Menu->Exit
CSCur72442	Android 5.0: Clear App Data needed - Lollipop upgrade with AC installed
CSCur72497	AnyConnect 4.0: Online User Guide link needs to point to 4.x user guide

Resolved Issues in AnyConnect 4.0.01110 for Android

Identifier	Headline
CSCur38052	Android: AirWatch MDM profile push fails with AnyConnect 4.0
CSCur36841	Android: AnyConnect 4.0 requests Location and other unnecessary perms
CSCur44572	Android: Text hints should not be offered when entering a password

Resolved Issues in AnyConnect 4.0.01093 for Android

Identifier	Headline
CSCup07733	Android: Incorrect Intel Android architecture check on some devices
CSCup83003	Android: AnyConnect should not auto-disconnect on CLAT46 Network
CSCur31571	AnyConnect vulnerable to POODLE attack (CVE-2014-3566) Android

AnyConnect Mobile Related Documentation

For more information refer to the following documentation:

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