Release Notes for Cisco AnyConnect Secure Mobility Client 3.0.x, for Apple iOS

Updated: December 13, 2013

This document includes the following sections:

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

Introduction

These release notes provide only Apple iOS-specific information for the AnyConnect Secure Mobility client. This document supplements the Cisco AnyConnect Administrator Guides. You can deploy later releases of AnyConnect for other devices simultaneously with this release.

This release of 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).

This release provides seamless and secure remote access to enterprise networks. The client provides a full tunneling experience that allows any installed application to communicate as though connected directly to the enterprise network. It runs on the Apple iPhone, iPad, and iPod Touch supporting connections to IPv4 and IPv6 resources over an IPv4 network tunnel.

The client installation software is available on the Apple iTunes App Store. The App store provides all AnyConnect for Apple iOS distributions and updates.

Note The adaptive security appliance (ASA) does *not* provide AnyConnect for Apple iOS distributions and updates.

Supported Apple iOS Devices

(with Retina

Device	Apple iOS Release Required
iPad Air	7.0 or later
iPad 2	6.0 or later
iPad (3rd generation)	6.0 or later
iPad (4th generation)	6.0 or later
iPad mini	6.0 or later
iPad mini (with Retina display)	7.0 or later
iPhone 3GS	6.0 or later
iPhone 4	6.0 or later
iPhone 4S	6.0 or later
iPhone 5	6.0 or later
iPhone 5C	7.0 or later
iPhone 5S	7.0 or later
iPod Touch (4th generation)	6.0 or later
iPod Touch (5th generation)	6.0 or later

Note AnyConnect on the iPod Touch appears and operates as on the iPhone. Use the *iPhone User Guide for Cisco AnyConnect Secure Mobility Client* for this device.

New Features in AnyConnect 3.0.09231

AnyConnect is now compatible with the iPhone 5S (64-bit) as well as other iOS 7/ iOS 6 devices.

See Resolved Issues in AnyConnect 3.0.09231 for Apple iOS, for specific bugs fixed in this release. Cisco recommends that you upgrade to this latest release of AnyConnect.

New Features in AnyConnect 3.0.09179

AnyConnect 3.0.09179 contains bug fixes, and the following changes:

- This release supports Apple iOS 7.

  Apple iOS 7 does not support Connect on Demand (COD) *Always Connect* domains. Domains in this category will be treated as *Connect if Needed* domains on Apple iOS 7. See Using the Connect on Demand Feature in the *Cisco AnyConnect Secure Mobility Client Administrator Guide*, for additional information about using the Apple iOS Connect On Demand feature.

- This release no longer supports Apple iOS 5.

  Consequently, AnyConnect for Apple iOS no longer supports the 1st generation iPad device or the 3rd generation iPod Touch device. See the current list of Supported Apple iOS Devices.

- Curently, AnyConnect is not compatible with the iPhone 5S (64-bit). Cisco will provide compatibility information as soon as it is available.

- This release now supports full screen mode on iPhone 5 devices.

See Resolved Issues in AnyConnect 3.0.09179 for Apple iOS, for specific bugs fixed in this release. Cisco recommends that you upgrade to this latest release of AnyConnect.

New Features in AnyConnect 3.0.09115

AnyConnect 3.0.09115 is a maintenance release, see Resolved Issues in AnyConnect 3.0.09115 for Apple iOS. Cisco recommends that you upgrade to this latest release of AnyConnect.

New Features in AnyConnect 3.0.09097

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.

Note

- At AnyConnect 3.0 for Mobile release time, Apple iOS does not support ECDSA certificates. This problem is being addressed by Apple. Once fixed, the following requirement will apply:

  Apple iOS 5.0 or later is required for Suite B cryptography; this is the minimum Apple iOS 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.

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 certficiate 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

Apple has introduced a Trusted Network Detection (TND) enhancement to the Connect On Demand feature in iOS 6. This enhancement:

- Extends the Connect on Demand functionality by determining whether the user is on a trusted network.
- Applies to Wi-Fi connectivity only. When operating over other types of network connections, Connect on Demand does not use TND to determine whether a VPN should be connected.
- Is not a separate feature and cannot be configured or used outside of the Connect on Demand capabilities.

Contact Apple for more information about Connect on Demand Trusted Network Detection in iOS 6.

Note Releases prior to iOS 6 do not support discerning between trusted and untrusted networks.

Apple iOS UI Changes

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

- Application preferences are now set inside the AnyConnect application by choosing **Settings** from the AnyConnect menu. Additional application settings have been added:
  - A new **Block Untrusted VPN** setting has been added to the Settings screen. See the "Blocking Untrusted Servers" section for details.
  - A new FIPS Mode setting has been added to the Settings screen. See the "FIPS and Suite B Cryptography" section for details.

- An **Advanced** screen has been added to the Connection Editor to configure connection settings beyond the required Server Address and Description: Network Roaming, Certificate, Connect On Demand, and the IPsec Tunnel Protocol settings.
- 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.

Apple iOS AnyConnect Features

The following AnyConnect features are supported in AnyConnect 3.0.x for Apple iOS:

- Tunnel Protocols
  - Cisco SSL Tunneling Protocol (CSTP)
  - Cisco DTLS Tunneling Protocol (CDTP)
  - IPsec IKEv2
- SSL Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - RC4-SHA
  - RC4-MD5
  - DES-CBC-SHA
- DTLS Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - DES-CBC-SHA
- Suite B (IPsec only)
- FIPS 140-2 Level 1
- Authentication
- Client Certificate Authentication
- Auto Reconnect (regardless of the Auto Reconnect profile specification, AnyConnect Mobile always attempts to maintain the VPN as users move between cellular and WiFi networks)
- Routing Policy
  - Tunnel All
  - Split Include
  - Split Exclude
- Rekey
- Network Roaming
- TLS Compression
- Cisco Profile Support
- Profile Update
- IPv6 over IPv4
- Post-Login Banner
- Dead Peer Detection
- Tunnel Keepalive

- Backup Server List
- Default Domain
- Cluster Support
- DNS Server Configuration
- Private-side Proxy Support
- Network Change Monitoring
- Statistics
- Graphical User Interface
- Pre-login Banner
- Secure Certificate Enrollment Protocol (SCEP)
- SCEP Proxy
- Certificate Management
  - Import a certificate using the client interface or URI command.
  - Delete a certificate or all certificates on the device.
- Connect on Demand (compatible with Apple iOS Connect on Demand)
- Mobile Posture
- Localization

Adaptive Security Appliance Requirements

ASA models support the Cisco AnyConnect Secure Mobility client for Apple iOS. 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 Apple iOS 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 AnyConnect License Requirements

AnyConnect for Apple iOS connections require the following licenses on the ASA:

- An AnyConnect core license granting VPN access for a total number of simultaneous sessions. Satisfy this requirement with one of the following options, each which supports full client access from the desktop: Cisco AnyConnect Essentials license or Cisco AnyConnect Premium Clientless VPN Edition license.
- AnyConnect Mobile license for mobile device access.

These licenses are mutually exclusive per ASA, but you can configure a mixed network. Both 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 *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.3*.

Known Issues and Limitations

Guidelines and Limitations

- Cisco IOS routers do not support the Cisco AnyConnect Secure Mobility client for Apple iOS at this time.
- This release of AnyConnect for Apple iOS supports only the features that are strictly related to remote access.
- AnyConnect supports the following types of VPN configurations:
  - Manually generated.
  - AnyConnect VPN client profile imported.
  - iPhone Configuration Utility generated. For details about the iPhone Configuration Utility see http://www.apple.com/support/iphone/enterprise/
- The VPN configurations generated by the iPhone Configuration Utility do not support Network Roaming. If your users require Network Roaming, use an AnyConnect profile.
- The Apple iOS device supports no more than one AnyConnect VPN client profile. The contents of the generated configuration always matches the most recent profile. For example, if a user goes to vpn.example1.com and then goes to vpn.example2.com, the AnyConnect VPN client profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.
- This release supports the tunnel keepalive feature; however, it can reduce the battery life of the device. Increasing the update interval value can mitigate that issue.

Apple iOS Connect On Demand Considerations

- Apple iOS 7 does not support Connect on Demand (COD) *Always Connect* domains. Domains in this category will be treated as *Connect if Needed* domains.
- AnyConnect collects device information when the UI is launched and a VPN connection is initiated. Therefore, there are circumstances in which AnyConnect can mis-report mobile posture information if the user relies on iOS's Connect On Demand feature to make a connection initially, or after device information, such has the OS version, has changed.
- To ensure proper establishment of Connect On Demand VPN tunnels after updating AnyConnect, users must manually start the AnyConnect app and establish a connection. If this is not done, upon the next iOS system attempt to establish a VPN tunnel, the error message "The VPN Connection requires an application to start up" will display.

Also see Using the Connect on Demand Feature in the *Cisco AnyConnect Secure Mobility Client Administrator Guide*, for additional information about using Connect On Demand.

Known Issues in Apple iOS Impacting VPN

We have reported the following iOS issues to Apple. They may be resolved in a future iOS release.

- A DTLS packet received while the device is asleep does not awaken it. TLS packets, however, awaken the device if notifications or Facetime is enabled. AnyConnect automatically disconnects the DTLS tunnel when the device goes to sleep to allow packets received over the TLS connection to wake the device. The DTLS tunnel is restored when the device resumes.

- Voice applications running in the background on an iPod Touch cannot receive packets over VPN. This functionality works as expected on iPhone devices.
- If a VPN configuration contains a large number of routes or split-dns rules, the Apple device cannot establish a VPN connection. This bug occurs, for example, if, upon connection, an ASA configuration pushes a VPN split-include list that has 70 or more rules that direct traffic to individual subnets. To prevent this bug from impacting users, apply a tunnel-all configuration or reduce the number of rules.
- AnyConnect may become slow or crash when there are a large number of VPN connections configured on the mobile device.
- Apple iOS Permits All Local LAN Traffic with Tunnel-all:Apple iOS permits traffic that is essential for the core operation of the device, regardless of whether a tunnel-all policy is in force. Examples of traffic that Apple iOS sends in the clear regardless of the tunnel policy include:
  - All local LAN traffic
  - Scoped routes for preexisting connections (for example, a video being streamed before VPN comes up)
  - Core Apple services (for example, Visual Voice mail traffic)

Open Issues in AnyConnect 3.0.09321 for Apple iOS

Identifier	Headline
CSCti21635	Apple APIs are blocking, causing multiple problems
CSCub11301	iphone - unable to enable after upgrade
CSCub50878	Apple's vpnagent crashes upon connection establishment in Apple iOS 6
CSCub56534	Unable to import ECDSA certificates on Apple iOS
CSCuc29522	AnyConnect performance issues with iPhone 4
CSCuc69491	Slow timeout on untrusted server prompt cancel for load balanced IKEv2
CSCuc84313	connect-if-needed connection disconnects when network interface changes
CSCud05728	android/iphone - misleading error when AAA server is down
CSCud38824	Automatic legacy SCEP does not work on iPhone 5 and iPad mini
CSCud41884	AC unable to get device info for use in SCEP template on iPhone 5
CSCud50975	VPNAgent crash sometimes when toggle wifi after airplane mode disabled
CSCuf21614	ACIDx fails to report "endpoint.anyconnect.devicetype" correctly
CSCug19553	Adapt client to Apple VPN-on-Demand changes
CSCuh39511	Anyconnect 3.0.09115 on Iphones get VPN Server could not parse request
CSCui183079	Mobile client can't handle some special characters in tunnel group names
CSCuj72299	iOS 64-bit: Add support for deflate (TLS) compression

Resolved Issues in AnyConnect 3.0.09231 for Apple iOS

Identifier	Headline
CSCuj34373	iPhone cant connect to backup IOS gateway if primary is not reachable
CSCuj39321	[iOS 7] INCORRECT_TUNNEL_MTU causing constant reconnects

Resolved Issues in AnyConnect 3.0.09179 for Apple iOS

Identifier	Headline
CSCud39214	GroupURL on unlocked 4s t-mobile EDGE network doesn't connect
CSCud51537	iPhone backup server list does not work with DNS round robin
CSCuh09909	IKEv2 connections with IPv6 fail with Cisco IOS 15.4
CSCui48888	Group-url does not work with iOS 7

Resolved Issues in AnyConnect 3.0.09115 for Apple iOS

Identifier	Headline
CSCue01052	Unable to connect to / resolve server address from client profile

CSCud72301	group url + DNS hijacking results in connection timeout
CSCue06318	plugins are out of sync after profile download with same description

Resolved Issues in AnyConnect 3.0.09097 for Mobile Devices

Identifier	Headline
CSCto94510	AC non-WinX clients are not requesting entire certificate chain
CSCtt44916	iPhone: Message at the bottom of the "Domain List" should be modified
CSCty45690	SCEP request not made with multiple certs and auto cert selection
CSCub43452	SCEP enrollment fails if CA doesn't send complete cert chain
CSCuc65697	iphone - URI handler option usecert=false doesn't disable auto cert
CSCuc83667	android-iOS client behaving differently during certificate auth
CSCud12339	Remove EKU/KU certificate check

AnyConnect Support Policy

Cisco supports all AnyConnect software versions downloaded from the iTunes App Store; however, fixes and enhancements are provided only in the most recently released version. Cisco is not able to provide earlier versions of AnyConnect for Apple iOS as only the most recently released version is available from the iTunes App Store.

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 related documentation:

User Guide

- *iPhone User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0*
- *iPad User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0*

Release Notes

- *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.0*

Administrator Guide

- *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0*

Other

- *Navigating the Cisco ASA 5500 Series Documentation*

Additional information on using VPN connections with Apple iOS devices is available from Apple:

- http://developer.apple.com/library/ios/search/?q=VPN+Server+Configuration
- http://support.apple.com/kb/HT1424
