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

AnyConnect for Apple iOS Release Notes

AnyConnect for Apple iOS 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 Apple iOS devices.

The AnyConnect app is available on the Apple iTunes App Store only. 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: 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 Beta Testing with TestFlight

Beta builds of AnyConnect are made available for pre-release testing on TestFlight. Follow this link to participate in TestFlight testing: https://testflight.apple.com/join/N0QLSq2c.

You may opt out later using this same TestFlight 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.

AnyConnect Versions Available for Apple iOS

Cisco AnyConnect for Apple iOS is currently available in multiple versions:

- ***Cisco AnyConnect***

  This is the initial release of this new app. *Cisco AnyConnect* is the latest and recommended version available for Apple iOS. To ensure you are always receiving the latest Apple iOS bug fixes, upgrade to the latest version. (During the Beta cycle, this version of AnyConnect was named *AnyConnect 2017*.)

  We recommend using this version with Apple iOS 10.3 and later. It uses the New Extension Framework, provided by iOS, to implement VPN and all its features. Per App VPN tunneling is a fully supported feature, and the New Extension Framework allows support of both TCP and UDP applications. Moving forward, this new Cisco AnyConnect version will be the only one to contain all enhancements and bug fixes.

- ***Cisco Legacy AnyConnect***

  Legacy AnyConnect 4.0.05x is not supported on iOS beyond 11.x. For compatibility with later versions of iOS, install the latest AnyConnect application available in the App Store.

  Legacy AnyConnect is the version supporting Apple iOS 6.0 and later that has been available on the app store for some time now. This version will be phased out over time but currently remains available to ease the transition to the latest and recommended version.

  The Per App VPN tunneling feature in this Legacy AnyConnect app will not receive TAC support. Customers wanting to use Per App VPN should migrate to the new version.

  Legacy AnyConnect will only be updated for critical security issues. This release continues to be numbered 4.0.05x.

Cisco AnyConnect and Legacy AnyConnect are different apps with different app IDs. Hence:

- Using the new extension framework in AnyConnect 4.0.07x (and later) causes the following changes in behavior from legacy AnyConnect 4.0.05x: AnyConnect considers traffic for tunnel DNS server to be tunneled, even if it is not in split-include network.
- You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to AnyConnect 4.0.07x or 4.6.x (or later). Cisco AnyConnect 4.0.07x (or 4.6.x and later) is a separate app, installed with a different name and icon.
- The different versions of AnyConnect can co-exist on the mobile device, but this is not supported by Cisco. The behavior may not be as expected if you attempt to connect while having both versions of AnyConnect installed. Make sure you have only one AnyConnect app on your device, and it is the appropriate version for your device and environment.
- Certificates imported using Legacy AnyConnect version 4.0.05069 and any earlier release cannot be accessed or used by the new AnyConnect app release 4.0.07072 or later. MDM deployed certificates can be accessed and used by both app versions.
- App data imported to the Legacy AnyConnect app, such as certificates and profiles, should be deleted if you are updating to the new version. Otherwise they will continue to show in the system VPN settings. Remove app data before uninstalling the Legacy AnyConnect app.
- Current MDM profiles will not trigger the new app. EMM vendors must support VPNType (VPN), VPNSubType (com.cisco.anyconnect) and ProviderType (packet-tunnel). For integration with ISE, they must be able to pass the UniqueIdentifier to AnyConnect since AnyConnect no longer has access to this

in the new framework. Consult your EMM vendor for how to set this up; some may require a custom VPN type, and others may not have support available at release time.

Using the New Extension Framework in AnyConnect 4.0.07x and later causes the following changes in behavior from Legacy AnyConnect 4.0.05x:

- The Device ID sent to the head end is no longer the UDID in the new version, and it is different after a factory reset unless your device is restored from a backup made by the same device.
- You may use MDM deployed certificates, as well as certificates imported using one of the methods available in AnyConnect: SCEP, manually through the UI, or via the URI handler. The new version of AnyConnect can no longer use certificates imported via email or any other mechanism beyond these identified ones.
- When creating a connection entry using the UI, the user must accept the iOS security message displayed.
- A user-created entry with the same name as a downloaded host entry from the AnyConnect VPN profile will not be renamed until it disconnects, if it is active. Also, the downloaded host connection entry will appear in the UI after this disconnect, not while it remains connected.
- AnyConnect considers traffic for tunnel DNS server to be tunneled even if it is not in split-include network.

Apple iOS Supported Devices

Cisco AnyConnect 4.0.07x and later is the latest and recommended version available on all iPhones, iPads, and iPod Touch devices running Apple iOS 10.3 and later.

If a device does not support Apple iOS 10.3 or later, only **Legacy AnyConnect 4.0.05x** , available on all iPhones, iPads, and iPod Touch devices running Apple iOS 6.0 and later, can be used. Per App tunneling in Legacy AnyConnect requires Apple iOS 8.3 or later.

Note AnyConnect on the iPod Touch appears and operates as on the iPhone.

Upgrade AnyConnect on Apple iOS

Upgrades to AnyConnect are managed through the Apple App Store. After the Apple App Store notifies users that the Cisco AnyConnect or Legacy AnyConnect upgrade is available, they follow this procedure.

Note You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to AnyConnect 4.0.07x or 4.6.x (or later). Cisco AnyConnect 4.0.07x (or 4.6.x and later) is a separate app, installed with a different name and icon.

See AnyConnect Versions Available for Apple iOS, on page 2 before installing the new version. Cisco recommends you remove all Legacy AnyConnect app data, remove the Legacy AnyConnect app, and then install the new version.

Before you begin

Before upgrading your device, you must disconnect an AnyConnect VPN session, if one is established, and close the AnyConnect application, if it is open. If you fail to do this, AnyConnect requires a reboot of your device before using the new version of AnyConnect.

Note This only applies in your environment if you are running a Legacy AnyConnect release earlier than 4.0.05032, or an Apple iOS release earlier than 9.3 while using Apple Connect-on-Demand capabilities. 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" displays.

Procedure

Step 1 Tap the **App Store** icon on the iOS home page.

Step 2 Tap the **AnyConnect upgrade notice**.

Step 3 Read about the new features.

Step 4 Click **Update**.

Step 5 Enter your **Apple ID Password**.

Step 6 Tap **OK**.

The AnyConnect update proceeds.

New Features in AnyConnect 4.0.07x for Apple iOS

New Features in AnyConnect 4.0.07077 for Apple iOS Mobile Devices

This update of AnyConnect is a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.07077 Apple iOS, on page 17 for a complete list of resolved issues.

Cisco recommends that you upgrade to this release of AnyConnect if your device supports iOS 10, and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.07075 for Apple iOS Mobile Devices

This update of AnyConnect is a maintenance release for devices running earlier versions. See #unique_11 for a complete list of resolved issues.

Cisco recommends that you upgrade to this release of AnyConnect if your device supports iOS 10, and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.07074 for Apple iOS Mobile Devices

This update of AnyConnect is a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.07074 Apple iOS, on page 17 for a complete list of resolved issues.

Cisco recommends that you upgrade to this release of AnyConnect if your device supports iOS 10, and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.07072 for Apple iOS Mobile Devices

This release of ***Cisco AnyConnect*** is the latest and recommended version available for Apple iOS. This version supports iOS 10.3 and later. It uses the New Extension Framework, provided by iOS, to implement VPN and all its features. During the Beta cycle this version of AnyConnect was named *AnyConnect 2017*. In addition to the new framework, Per App tunneling, described below, is now fully supported in this release.

Note Certificates imported using Legacy AnyConnect version 4.0.05069 and any earlier release cannot be accessed or used by the new AnyConnect app release 4.0.07072 or later. MDM deployed certificates can be accessed and used by both app versions.

Moving forward, this Cisco AnyConnect version will be the only one to contain all enhancements and bug fixes. It will be numbered 4.0.07xxx.

This update of AnyConnect is also a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.07072 Apple iOS, on page 17 for a complete list of resolved issues.

Cisco recommends that you upgrade to this release of AnyConnect if your device supports iOS 10, and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

Per App VPN

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.

Your Mobile Device Managermust 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. For a seamless, automatic configuration, configure *App on Demand* in your MDM configuration, and use digital certificates for connectivity to the headend.

New Features in Legacy AnyConnect 4.0.05x for Apple iOS

New Features in Legacy AnyConnect 4.0.05069 for Apple iOS Mobile Devices

This version of AnyConnect is now named ***Legacy AnyConnect***.

Legacy AnyConnect is the version supporting Apple iOS 6.0 and later that has been on the app store for some time now. It remains available to ease the transition to the latest and recommended version of ***Cisco AnyConnect***.

Legacy AnyConnect will only be updated for critical customer issues that cannot be solved by upgrading to the latest release. This release continues to be numbered 4.0.05x. See New Features in Legacy AnyConnect 4.0.05x for Apple iOS, on page 5.

This update of AnyConnect is also a maintenance release for devices running earlier versions. See Resolved Issues in Legacy AnyConnect 4.0.05069 Apple iOS, on page 18 for a complete list of Resolved Issues.

Cisco recommends that you upgrade to this release of AnyConnect only if your device DOES NOT support iOS 10. Review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05066 for Apple iOS Mobile Devices

This update of AnyConnect is a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.05066 Apple iOS, on page 18 for a complete list of Resolved Issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

Note Email questions and feedback related to the Per App VPN Beta feature to ac-mobile-feedback@cisco.com directly, do not raise them to the Cisco TAC.

New Features in AnyConnect 4.0.05055 for Apple iOS Mobile Devices

This release of Cisco AnyConnect for Apple iOS updates the support of the Disconnect on Suspend, Auto Reconnect Behavior introduced in the previous release.

Now, when Disconnect On Suspend is chosen, AnyConnect disconnects and releases the resources assigned to the VPN session when the device sleeps, for On Demand connections ONLY. Once disconnected in this way, AnyConnect will reconnect only in response to a user's manual connection or an On Demand connection (if configured).

This update of AnyConnect is also a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.05055 Apple iOS, on page 18 for a complete list of Resolved Issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

Note Email questions and feedback related to the Per App VPN Beta feature to ac-mobile-feedback@cisco.com directly, do not raise them to the Cisco TAC.

New Features in AnyConnect 4.0.05052 for Apple iOS Mobile Devices

This release of Cisco AnyConnect for Apple iOS now supports the Disconnect on Suspend, Auto Reconnect Behavior if selected by the administrator in the VPN Client Profile. When Disconnect On Suspend is chosen, AnyConnect disconnects and releases the resources assigned to the VPN session when the device sleeps. It will reconnect only in response to a user's manual connection or an On Demand connection (if configured).

This update of AnyConnect is also a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.05052 Apple iOS, on page 19 for a complete list of Resolved Issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

Note Email questions and feedback related to the Per App VPN Beta feature to ac-mobile-feedback@cisco.com directly, do not raise them to the Cisco TAC.

New Features in AnyConnect 4.0.05046 for Apple iOS Mobile Devices

This update of Cisco AnyConnect Secure Mobility Client for Apple iOS devices addresses the most recent OpenSSL vulnerabilities. It is also a maintenance release for devices running earlier versions. See Resolved Issues in AnyConnect 4.0.05046 Apple iOS, on page 19 for a complete list of Resolved Issues.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

Note Email questions and feedback related to the Per App VPN Beta feature to ac-mobile-feedback@cisco.com directly, do not raise them to the Cisco TAC.

New Features in AnyConnect 4.0.05038 for Apple iOS Mobile Devices

This version of AnyConnect for Apple iOS is a maintenance release to address regressions in 4.0.05036. See Resolved Issues in AnyConnect 4.0.05038 Apple iOS, on page 19 for details.

Note Email questions and feedback related to the Per App VPN Beta feature to ac-mobile-feedback@cisco.com directly, do not raise them to the Cisco TAC.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05036 for Apple iOS Mobile Devices

This version of AnyConnect for Apple iOS is a maintenance release to address a regression in 4.0.05032. See Resolved Issues in AnyConnect 4.0.05036 Apple iOS, on page 19 for details.

Note Email questions and feedback related to the Per App VPN Beta feature to ac-mobile-feedback@cisco.com directly, do not raise them to the Cisco TAC.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.05032 for Apple iOS Mobile Devices

This release of AnyConnect 4.0 now supports: public IPv6 tunneling and private IPv6 split tunneling.

Also, the following limitation has been removed for devices running AnyConnect 4.0.05032 or later, in conjunction with Apple iOS 9.3 or later: After upgrading, if the Apple iOS Connect On Demand feature is used on your device to make VPN connections automatically, you must launch the AnyConnect app and

establish a VPN 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.

Note Questions and feedback related to the Per App VPN Beta feature should be mailed to ac-mobile-feedback@cisco.com directly, not raised to the Cisco TAC

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.03021 for Apple iOS Mobile Devices

This release of AnyConnect 4.0 is an upgrade for Apple iOS devices running earlier versions of AnyConnect. It resolves the latest Open SSL vulnerabilities and addresses other issues. See Resolved Issues in AnyConnect 4.0.03021 Apple iOS, on page 20 for details.

Note Questions and feedback related to the Per App VPN Beta feature should be mailed to ac-mobile-feedback@cisco.com directly, not raised to the Cisco TAC

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.03016 for Apple iOS Mobile Devices

This release of AnyConnect 4.0 is an upgrade for Apple iOS devices running earlier versions of AnyConnect. It resolves the latest Open SSL vulnerabilities and addresses issues seen in the initial release of 4.0. See Resolved Issues in AnyConnect 4.0.03016 for Apple iOS for details.

Note Questions and feedback related to the Per App VPN Beta feature should be mailed to ac-mobile-feedback@cisco.com directly, not raised to the Cisco TAC

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.03004 for Apple iOS Mobile Devices

This release of AnyConnect 4.0 is an upgrade for Apple iOS devices running earlier versions of AnyConnect. It resolves the latest Open SSL vulnerabilities and addresses issues seen in the initial release of 4.0. See Resolved Issues in AnyConnect 4.0.03004 for Apple iOS, on page 20 for details.

Note Questions and feedback related to the Per App VPN Beta feature should be mailed to ac-mobile-feedback@cisco.com directly, not raised to the Cisco TAC.

Cisco recommends that you upgrade to this latest release of AnyConnect and review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

New Features in AnyConnect 4.0.01324 for Apple iOS Mobile Devices

This release of AnyConnect 4.0 is an upgrade for Apple iOS devices running earlier versions of AnyConnect and contains the following new features described below:

- TLS 1.2
- Additional Localization
- Per App VPN (Beta availability and support only)

Note Questions and feedback related to this feature should be mailed to ac-mobile-feedback@cisco.com directly, not raised to the Cisco TAC.

Cisco recommends that you upgrade to this latest release of AnyConnect. Review the Known Issues and Limitations, on page 14 to be aware of current operational considerations.

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.

Additional Localization

AnyConnect 4.0 for mobile devices now includes the following additional language translations in the AnyConnect Apple iOS 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.

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:

- Apple iOS 8.3 or later
- Devices must be configured to use Per App using a Mobile Device Management (MDM) solution.
- ASA 9.3.2 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.

Your Mobile Device Managermust 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. For a seamless, automatic configuration, configure *App on Demand* in your MDM configuration, and use digital certificates for connectivity to the headend.

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.

Apple iOS AnyConnect Feature Matrix

The following features are supported in AnyConnect for Apple iOS devices:

Category: Feature	Apple iOS
Deployment and Configuration:	
Install or upgrade from application store.	Yes
Cisco VPN Profile support (manual import)	Yes

Category: Feature	Apple iOS
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	No
Suite B (IPsec only)	Yes
TLS compression	Yes, 32-bit devices only
Dead peer detection	Yes
Tunnel keepalive	Yes
Multiple active network interfaces	No
Per App Tunneling	Yes, requires Cisco AnyConnect 4.0.09xxx and iOS 10.3 or later.
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).*	Yes
Split-DNS	Yes
Auto Reconnect / Network Roaming	Yes
VPN on-demand (triggered by destination)	Yes, compatible with Apple iOS Connect on Demand.
VPN on-demand (triggered by application)	Yes, when operating in Per App VPN mode only.
Rekey	Yes
IPv4 public transport	Yes
IPv6 public transport	Yes
IPv4 over IPv4 tunnel	Yes
IPv6 over IPv4 tunnel	Yes
IPv6 over IPv4 tunnel	Yes
IPv6 over IPv6 tunnel	Yes
Default domain	Yes
DNS server configuration	Yes
Private-side proxy support	Yes

Category: Feature	Apple iOS
Proxy Exceptions	Yes, but wildcard specifications not supported
Public-side proxy support	No
Pre-login banner	Yes
Post-login banner	Yes
DSCP Preservation	No
Connecting and Disconnecting:	
VPN load balancing	Yes
Backup server list	Yes
Optimal Gateway Selection	No
Authentication:	
SAML 2.0	Yes
Client Certificate Authentication	Yes
Online Certificate Status Protocol (OCSP)	No
Manual user certificate management	Yes
Manual server certificate management	Yes
SCEP legacy enrollment	No
SCEP proxy enrollment	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	Yes, limited functions
API / URI Handler (see below)	Yes
UI customization	No

Category: Feature	Apple iOS
UI localization	Yes, app contains pre-packaged languages.
User preferences	Yes
Home screen widgets for one-click VPN access	No
AnyConnect specific status icon	No
Mobile Posture: (AnyConnect Identity Extensions, ACIDex)	
Serial number or unique ID check	Yes
OS and AnyConnect version shared with headend	Yes
AnyConnect NVM support	No
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

* Local LAN access is enabled for iOS devices regardless of the configuration of the ASA due to operating system implementation.

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.

Known Issues and Limitations

Known Compatibility Issues

In AnyConnect 4.6.xxxxx

- Split tunneling to the ASA headend does not work when tunneling IPv6 only (no IPv4 address assigned) in a split exclude configuration.

  All traffic should be tunneled except for the exclude list entries, yet the split exclude list is not honored, all IPv6 traffic is excluded. Refer to CSCvb80768: IPv6 Split Exclude & IPv4 DropAll will exclude all v6 traffic from the tunnel. (RADAR 29623849).

- If the AnyConnect UI remains open and iOS mistakenly disconnects the Inter-Process Communication (IPC) between the UI and the internal AnyConnect extension, any UI activity will fail with an error or an incorrect response.

  To recover from this, you must close and restart the AnyConnect UI which will re-establish the IPC. If the unexpected IPC disconnect occurs when the UI is closed, the next time you open the UI, it will be re-established. Refer to CSCvb95722: Fails to get to Paused state (RADAR 29313229).

- For On Demand connections, the AnyConnect UI must be opened when an updated VPN connection profile has been pushed to the client by the ASA. If the UI is not opened, the updated profile will not be synchronized and therefore the changes will not be used.

  Unfortunately, there is no indication to the user to open the UI to sync the new profile (as in Legacy AnyConnect), so it is possible that the updated connection entry is never used. There is no workaround at this time. Refer to CSCvc35923: Using On-Demand AC cannot inform users that they must open AC to sync an updated connection profile (RADAR 30173053).

- In a managed Per App configuration, app traffic, configured for Per App, flows over a user-created (unmanaged) VPN connection when it should not.

  Refer to CSCvc36024: PerApp - Apps can pass traffic over non-PAV full tunnel (RADAR 29513803).

Guidelines and Limitations for AnyConnect on Apple iOS

AnyConnect for Apple iOS supports only features that are related to remote VPN access such as:

- AnyConnect can be configured by the user (manually), by the AnyConnect VPN Client Profile, generated by the iPhone Configuration Utility (http://www.apple.com/support/iphone/enterprise/), or using an Enterprise Mobile Device Manager.
- The Apple iOS device supports no more than one AnyConnect VPN client profile. The contents of the generated configuration always match the most recent profile. For example, you connect to vpn.example1.com and then 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 reduces battery life of the device. Increasing the update interval value mitigates this issue.

Apple iOS Connect On-Demand Considerations:

- VPN sessions, which are automatically connected as a result of iOS On-Demand logic and have Disconnect on Suspend configured, are disconnected when the device sleeps. After the device wakes up, On-Demand logic will reconnect the VPN session when it is necessary again.
- AnyConnect collects device information when the UI is launched and a VPN connection is initiated. Therefore, there are circumstances in which AnyConnect can misreport mobile posture information if the user relies on iOS's Connect On-Demand feature to make a connection initially, or after device information, such as the OS version has changed.
- This only applies in your environment if you are running a Legacy AnyConnect release earlier than 4.0.05032, or an Apple iOS release earlier than 9.3 while using Apple Connect-on-Demand capabilities. 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" displays.

Cisco AnyConnect and Legacy AnyConnect are different apps with different app IDs. Hence:

- Using the new extension framework in AnyConnect 4.0.07x (and later) causes the following changes in behavior from legacy AnyConnect 4.0.05x: AnyConnect considers traffic for tunnel DNS server to be tunneled, even if it is not in split-include network.
- You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to AnyConnect 4.0.07x or 4.6.x (or later). Cisco AnyConnect 4.0.07x (or 4.6.x and later) is a separate app, installed with a different name and icon.
- The different versions of AnyConnect can co-exist on the mobile device, but this is not supported by Cisco. The behavior may not be as expected if you attempt to connect while having both versions of AnyConnect installed. Make sure you have only one AnyConnect app on your device, and it is the appropriate version for your device and environment.

- Certificates imported using Legacy AnyConnect version 4.0.05069 and any earlier release cannot be accessed or used by the new AnyConnect app release 4.0.07072 or later. MDM deployed certificates can be accessed and used by both app versions.
- App data imported to the Legacy AnyConnect app, such as certificates and profiles, should be deleted if you are updating to the new version. Otherwise they will continue to show in the system VPN settings. Remove app data before uninstalling the Legacy AnyConnect app.
- Current MDM profiles will not trigger the new app. EMM vendors must support VPNType (VPN), VPNSubType (com.cisco.anyconnect) and ProviderType (packet-tunnel). For integration with ISE, they must be able to pass the UniqueIdentifier to AnyConnect since AnyConnect no longer has access to this in the new framework. Consult your EMM vendor for how to set this up; some may require a custom VPN type, and others may not have support available at release time.

Using the New Extension Framework in AnyConnect 4.0.07x and later causes the following changes in behavior from Legacy AnyConnect 4.0.05x:

- The Device ID sent to the head end is no longer the UDID in the new version, and it is different after a factory reset unless your device is restored from a backup made by the same device.
- You may use MDM deployed certificates, as well as certificates imported using one of the methods available in AnyConnect: SCEP, manually through the UI, or via the URI handler. The new version of AnyConnect can no longer use certificates imported via email or any other mechanism beyond these identified ones.
- When creating a connection entry using the UI, the user must accept the iOS security message displayed.
- A user-created entry with the same name as a downloaded host entry from the AnyConnect VPN profile will not be renamed until it disconnects, if it is active. Also, the downloaded host connection entry will appear in the UI after this disconnect, not while it remains connected.
- AnyConnect considers traffic for tunnel DNS server to be tunneled even if it is not in split-include network.

Open and Resolved Issues in AnyConnect 4.0.7x for Apple iOS

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.

Note that some cross platform bugs defined in the desktop release notes (https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect410/release/notes/release-notes-anyconnect-4-10.html) may apply to the mobile releases. Once a bug has been reported as fixed, it becomes available on all operating system platforms (including mobile operating systems) with a higher AnyConnect release number. Those bugs with vpn, core, nvm, and similar components that apply across platform will not be duplicated in the subsequent mobile releases. For example, a vpn component bug resolved in desktop release 4.9.00086 will not be listed again in iOS release 4.9.00512 because the iOS version is greater than the release version where the bug was reported as fixed.

Open Issues in AnyConnect 4.0.07077 for Apple iOS

Identifier	Headline
CSCuu76224	Unable to resolve .local even SOA record is advertised
CSCuv44716	Split Tunnel Include Configuration May Fail to Work Properly

Identifier	Headline
CSCuy41307	AnyConnect connection status is out of sync
CSCuy99092	[ios] MTU needs to be 1380 or less on the tungrp to pass IPSec traffic
CSCuy99108	[ios] Anyconnect unable to drop IPv6 traffic
CSCuz38311	iOS 4.0.05032/5036 Slow connection establishment when AAAA response slow
CSCuz39092	iOS - 4.0.05036 Clarify Drop All Traffic text
CSCvb22398	OS not triggering VPN during dark wake - Radar # 27851312
CSCvb31542	iOS: PerApp SafariDom internal site with internal CRL fails R#28176408
CSCvb78548	VPN Fails to transition from Wi-Fi to Cellular using T-Mobile IPv6 Network
CSCve10517	iOS: Split DNS not working when set for subdomain

Resolved Issues in AnyConnect 4.0.07077 Apple iOS

Identifier	Headline
CSCuy37353	Unable to import user certificate while VPN is connected (iOS and Android)
CSCvf51745	Certificate import fails if certificate name has a space character (iOS)
CSCvf63546	Duplicate client certificate sent to ASA
CSCvf71658	Switching active config disables per-app config (iOS NF)

Resolved Issues in AnyConnect 4.0.07075 Apple iOS

Identifier	Headline
CSCvf07751	iOS: 4.0.7074 OS does not add default domain for split tunnel w/o split DNS

Resolved Issues in AnyConnect 4.0.07074 Apple iOS

Identifier	Headline
CSCvc35923	AC-NF Fails to inform users that they must open AC to sync an updated profile

Resolved Issues in AnyConnect 4.0.07072 Apple iOS

Identifier	Headline
CSCuq52458	Apple iOS: Group-P Default Domain is not used with Per App
CSCvb14706	AC on iOS 10 enable debug logs w/o active config displays error twice
CSCvb57807	ipad AC client certificate showing expiration date Dec 31, 1969 or Jan 01, 1970 in diagnostics
CSCve49663	iOS/Android: Backup connection entry fails to be tried on ATT LTE

Open and Resolved Issues in AnyConnect 4.0.5x for Apple iOS

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.

Note that some cross platform bugs defined in the desktop release notes (https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect410/release/notes/release-notes-anyconnect-4-10.html) may apply to the mobile releases. Once a bug has been reported as fixed, it becomes available on all operating system platforms (including mobile operating systems) with a higher AnyConnect release number. Those bugs with vpn, core, nvm, and similar components that apply across platform will not be duplicated in the subsequent mobile releases. For example, a vpn component bug resolved in desktop release 4.9.00086 will not be listed again in iOS release 4.9.00512 because the iOS version is greater than the release version where the bug was reported as fixed.

Open Issues in Legacy AnyConnect for Apple iOS

Open issues are only listed under the latest release, see Open and Resolved Issues in AnyConnect 4.0.7x for Apple iOS, on page 16.

Resolved Issues in Legacy AnyConnect 4.0.05072 Apple iOS

Identifier	Headline
CSCvh12708	iOS 11.2 and macOS 10.13.2 report mapped IPv6 address
CSCve49663	iOS/Android: Backup connection entry fails to be tried on ATT LTE

Resolved Issues in Legacy AnyConnect 4.0.05069 Apple iOS

No issues fixed in this release of Legacy AnyConnect.

Resolved Issues in AnyConnect 4.0.05066 Apple iOS

Identifier	Headline
CSCuv35459	Matching connection profile names are not renamed
CSCuy12161	AnyConnect Should No Longer Require KeyAgreement in Server Certificate
CSCvb48664	Evaluation of anyconnect for Openssl September 2016
CSCvb57807	ipad AC client certificate showing expiration date Dec 31, 1969 or Jan 01, 1970 in diagnostics
CSCvb59411	iOS: Deflate compression fails on 32-bit devices (i.e. iPhone 5C, 5, iPad 4 and older) with iOS 10+

Resolved Issues in AnyConnect 4.0.05055 Apple iOS

Identifier	Headline
CSCvb14706	AC on iOS 10 enable debug logs w/o active config displays error twice
CSCvb26000	AC iOS: ENH - Make DisconnectOnSuspend dependent on OS auto VPN

Resolved Issues in AnyConnect 4.0.05052 Apple iOS

Identifier	Headline
CSCuv97696	Apple #22457371 iOS 9 - OnDemand first DNS fails with RequiredDNSServers
CSCva32660	AC iOS: client-bypass-protocol enable causes fail to connect
CSCva56275	AC iOS: ENH - Support DisconnectOnSuspend profile option
CSCva86673	iOS 10 - IPv6 APNS compatibility with v4-only tunneled networks

Resolved Issues in AnyConnect 4.0.05046 Apple iOS

Identifier	Headline
CSCut14163	3.0.12240 corrupted profile after connecting to FQDN with multiple IN As
CSCuy15657	Changing the selected VPN Profile fails
CSCuy77264	The word Advanced is not aligned correctly in UI
CSCuz33124	Tunnel All w v4 and Drop All v6 prevents traffic passing to private net
CSCuz38302	4.0.05036 corrupted profile after connecting to FQDN with multiple IN As
CSCuz38319	iOS 4.0.05032/5036 oMTU process strange behavior - disconnect/reconnect
CSCuz38432	iOS: 4.0.05036 no network connectivity -false message -unable to connect
CSCuz39090	iOS - 4.0.05036 Client Ver String incorrectly reported as Windows
CSCuz52506	Evaluation of anyconnect for OpenSSL May 2016
CSCuz94483	iOS AnyConnect 4.0.5036+ PAC URL not working
CSCva03743	AnyConnect iOS multiple reconnects
CSCva26758	iOS - Support connecting to IPv4 head-end via IP on DNS64/NAT64 networks
CSCva30253	AnyConnect dialog show incorrect font color in some situation

Resolved Issues in AnyConnect 4.0.05038 Apple iOS

Identifier	Headline
CSCuz38302	4.0.05036 corrupted profile after connecting to FQDN with multiple IN As
CSCuz38319	iOS 4.0.05032/5036 oMTU process strange behavior - disconnect/reconnect
CSCuz38432	iOS: 4.0.05036 no network connectivity -false message -unable to connect
CSCuz39090	iOS - 4.0.05036 Client Ver String incorrectly reported as Windows

Resolved Issues in AnyConnect 4.0.05036 Apple iOS

Identifier	Headline
CSCuo47016	XMLSoft libxml2 Decoding Heap-Based Buffer Underflow Vulnerability

Identifier	Headline
CSCuy15657	Changing the selected VPN Profile fails
CSCuz33124	Tunnel All w v4 and Drop All v6 prevents traffic passing to private net

Resolved Issues in AnyConnect 4.0.03021 Apple iOS

Identifier	Headline
CSCut56282	AnyConnect iPhone: On-Demand domains cannot be updated via Profile
CSCux38698	Anyconnect IKEv2 buffer overflow
CSCux41420	Evaluation of anyconnect for OpenSSL December 2015 vulnerabilities
CSCux81967	AC copyright needs to be changed to 2016
CSCuy25393	Sending email logs thru AnyConnect fails on iPad-Pro
CSCuy54600	Evaluation of anyconnect for OpenSSL March 2016

Resolved Issues in AnyConnect 4.0.03016 for Apple iOS

Identifier	Headline
CSCuv97696	Apple #22457371 iOS 9 - OnDemand first DNS fails with RequiredDNSServers
CSCuw11134	iOS 9 - Split Tunnel with Tunnel all DNS - AAAA DNS block causes DNS failure
CSCuw54786	iOS - Wrong UDID reported - changing device and restoring from backup

Resolved Issues in AnyConnect 4.0.03004 for Apple iOS

Identifier	Headline
CSCut46503	MARCH 2015 OpenSSL Vulnerabilities
CSCuu96241	Launch issue with enabling AC via external app after the upgrade for 4.0
CSCuu99043	Login screen is not available after leaving screen then returning

AnyConnect Mobile Related Documentation

For more information refer to the following documentation:

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

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

- https://developer.apple.com/library/ios/search/?q=vpn+server+configuration

- http://support.apple.com/kb/ht1424