Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.9.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***

  Cisco AnyConnect 4.9 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.

  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 4.9 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 and later. They are separate apps, 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

New Features in AnyConnect 4.9.05043 for Apple iOS Mobile Devices

This release of AnyConnect resolves the defect described in Resolved Issues in AnyConnect 4.9.05043 for Apple iOS, on page 11.

New Features in AnyConnect 4.9.05041 for Apple iOS Mobile Devices

This release of AnyConnect includes the following enhancements and resolves the defects described in Resolved Issues in AnyConnect 4.9.05041 for Apple iOS, on page 11:

- Added support for Server Name Identification (SNI) for VPN connections.
- Added MDM configurable settings to block end users from adding VPN connections and to define AnyConnect local secure settings.

New Features in AnyConnect 4.9.00562 for Apple iOS Mobile Devices

This release of AnyConnect resolves the defects described in Resolved Issues in AnyConnect 4.9.00562 for Apple iOS, on page 12.

New Features in AnyConnect 4.9.00542 for Apple iOS Mobile Devices

This release of AnyConnect resolves the defects described in Resolved Issues in AnyConnect 4.9.00542 for Apple iOS, on page 12.

New Features in AnyConnect 4.9.00518 for Apple iOS Mobile Devices

This release of AnyConnect provides the following features and support updates:

- Support for multiple tunnel—You must do configuration in the MDM VPN profile to enable. Refer to the **AnyConnect on Mobile Devices** chapter in the Cisco AnyConnect Secure Mobility Client Adminstrator Guide, Release 4.9 for additional information.
- In the 4.9 AnyConnect releases, certain less secure cipher suites have been removed:
  - For SSL VPN, AnyConnect no longer supports the following cipher suites from both TLS and DTLS: DHE-RSA-AES256-SHA and DES-CBC3-SHA
  - For IKEv2/IPsec, AnyConnect no longer supports the following algorithms:
    - Encryption algorithms: DES and 3DES
    - Pseudo Random Function (PRF) algorithm: MD5
    - Integrity algorithm: MD5
    - Diffie-Hellman (DH) groups: 2, 5, 14, 24

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
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

Category: Feature	Apple iOS
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
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

Category: Feature	Apple iOS
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
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

Category: Feature	Apple iOS
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.

Guidelines and Limitations for AnyConnect on Apple iOS

- (iOS 14.0.x only)—When tunnel DNS servers are configured without a split DNS domain name specified, failure to resolve an address with the tunnel DNS servers does not result in a fallback to the device's public DNS servers. Changes in iOS caused this different behavior.
- (iOS 14.0.x only) CSCvv50495—After a network change, a transition from one network to another, or a network pause and resume, traffic stops. You can disable and re-enable your VPN connection to resume. This issue is fixed in iOS 14.1.
- CSCvs82209—While accessing client certificates that are imported via SCEP and that require biometrics for access, a "no valid certificate found" error results on iOS 13.3.1 and later. iOS 13.3.1 removed the ability for the AnyConnect Network Extension to use SCEP-imported certificates that have the security property requiring biometrics (TouchID / FaceID / passcode) for access. Until the client can be redesigned to accommodate this change, deploy certificates using SCEP without the biometric option.
- 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, if 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.
- **DHE Incompatibility**

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

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 has the OS version has changed.
- 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, the error message "The VPN Connection requires an application to start up" displays, upon the next iOS system attempt to establish a VPN tunnel.

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

- You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to the new version. The newer versions are separate apps, 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 4.6.x 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.

Known Compatibility Issues

In AnyConnect 4.7.xxxxx and later

- 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, and 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 fails 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).

Open and Resolved AnyConnect Issues

The Cisco Bug Search Tool 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://Cisco.com.

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.

Resolved Issues in AnyConnect 4.9.05043 for Apple iOS

Identifier	Headline
CSvw86231	AnyConnect iOS ATS limitation on TLS cipher suites can make SAML authentication fail

Resolved Issues in AnyConnect 4.9.05041 for Apple iOS

Identifier	Headline
CSCvv68121	AnyConnect application settings are not MDM configurable
CSCvv68142	AnyConnect should allow MDM to block end user from adding VPN connection
CSCvw37668	Remove ATS policy exception to follow Common Criteria guidelines

Resolved Issues in AnyConnect 4.9.00562 for Apple iOS

Identifier	Headline
CSCvv82012	iPhone/iOS AnyConnect user credentials are not kept after an app switch

Resolved Issues in AnyConnect 4.9.00542 for Apple iOS

Identifier	Headline
CSCvv36705	Third-party email link in copyright should not be clickable