Release Notes for Cisco Secure Client (including AnyConnect), Release 5 for Apple iOS

First Published: 2023-10-11

Last Modified: 2024-09-13

Cisco Secure Client for Apple iOS Mobile Devices

Cisco Secure Client (including AnyConnect) for iOS Mobile Devices provides remote iOS users with secure VPN connections to the Cisco Secure Firewall ASA and other Cisco-supported headend devices. It provides seamless and secure remote access to enterprise networks, allowing installed applications to communicate as though connected directly to the enterprise network. Cisco Secure Client supports connections to IPv4 and IPv6 resources over an IPv4 or IPv6 tunnel.

This document, written for system administrators of the Cisco Secure Client and the Cisco Secure Firewall ASA, provides release specific information for Secure Client running on Apple iOS devices.

The Cisco Secure Client app is available on the Apple iTunes App Store only. You cannot deploy the mobile app from the Secure Firewall ASA. You can deploy other releases of Cisco Secure Client for desktop devices from the ASA while supporting this mobile release.

Cisco Secure Client Mobile Support Policy

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

Cisco Secure Client Licensing

To connect to the Secure Firewall ASA headend, an Advantage or Premier license is required. Trial licenses are available: Cisco Secure Client Ordering Guide.

For the latest end-user license agreement, see Cisco End User License Agreement, Cisco Secure Client.

For our open source licensing acknowledgments, see Open Source Software Used in Cisco Secure Client for Mobile.

Cisco Secure Client Beta Testing with TestFlight

Beta builds of Cisco Secure Client 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 Cisco Secure Client.

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 Cisco Secure Client.

Cisco Secure Client Version for Apple iOS

Cisco Secure Client 5 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 13.0 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, all enhancements and bug fixes will be provided as part of the Cisco Secure Client 5 version.

Apple iOS Supported Devices

Cisco Secure Client 5 is the latest and recommended version available on all iPhones, iPads, and iPod Touch devices running Apple iOS 13.0 and later.

Cisco Secure Client 5 is the latest and recommended version available on all iPhones, iPads, and iPod Touch devices running Apple iOS 10.3 and later.

For the Zero Trust Access feature available as an application download separately from Cisco Secure Client, you must have a device running iOS/iPadOS 17.2 (or later).

Note Cisco Secure Client on the iPod Touch appears and operates as on the iPhone.

Upgrade Cisco Secure Client on Apple iOS

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

Note See Cisco Secure Client Version for Apple iOS, on page 2 before installing the new version.

Before you begin

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

Procedure

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

Step 2 Tap the Cisco Secure Client **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 Cisco Secure Client update proceeds.

New Features

New Features in Cisco Zero Trust Access 5.1.66944 for iOS Mobile Releases

This release of Cisco Zero Trust Access provides the bug fixes listed in Resolved Issues for Zero Trust Access 5.1.66944 for Apple iOS, on page 11 and has the following known issues for iOS 18.

- Apple FB14668204 has been opened to track and investigate CSCwk58308—Add relays failing during some enrollment attempts.
- Apple FB15148769 has been opened to track and investigate CSCwk92214—AnyConnect: App lockup handling large profile.

Cisco Zero Trust Access is available from the Apple App Store. You must have a device running iOS/iPadOS 17.2 (or later).

Refer to Get Started with Cisco Secure Client for the iOS first time use and enrollment procedures. With the resolving of CSCwm44730, the flow has changed: enrollment will fail if the user enrolls a device when the server config is empty. This behavior of keeping the user in unenrolled state is different from other platforms where the user is kept in the enrolled state and not applying empty config rule. Refer to Zero Trust Access Module in the *Cisco Secure Client Administrator Guide, Release 5.1* for details and operation of Zero Trust.

New Features in Cisco Zero Trust Access 5.1.4.46500 for iOS Mobile Releases

This maintenance release of Cisco Zero Trust Access provides the bug fix listed in Resolved Issues in Cisco Zero Trust Access 5.1.4.46500 for Mobile iOS Releases, on page 11.

Cisco Zero Trust Access is available from the Apple App Store. You must have a device running iOS/iPadOS 17.2 (or later).

Refer to Get Started with Cisco Secure Client for the iOS first time use and enrollment procedures. Refer to Zero Trust Access Module in the *Cisco Secure Client Administrator Guide, Release 5.1* for details and operation of Zero Trust.

Step-up authentication is unsupported on iOS.

Known Issues:

CSCwj61835—ZTA iOS: Client certificate not updated when cert is revoked

New Features in Cisco Zero Trust Access 5.1.4.6420 for iOS Mobile Releases

This version includes a new Cisco Zero Trust Access offering as an additional Cisco Secure Client module for iOS.

Cisco Zero Trust Access is available from the Apple App Store. You must have a device running iOS/iPadOS 17.2 (or later).

Refer to Get Started with Cisco Secure Client for the iOS first time use and enrollment procedures. Refer to Zero Trust Access Module in the *Cisco Secure Client Administrator Guide, Release 5.1* for details and operation of Zero Trust.

Due to an Apple relay, step-up authentication is not supported.

Known Issues:

CSCwj61835—ZTA iOS: Client certificate not updated when cert is revoked

CSCwk07978—ZTA iOS: Webview disappears after user leaves and reopens ZTA

New Features in Cisco Secure Client 5.0.05207 for iOS Mobile Releases

This maintenance release of Cisco Secure Client provides the bug fixes listed in Resolved Issues in Cisco Secure Client 5.0.05207 for Apple iOS, on page 11.

New Features in Cisco Secure Client 5.0.05206 for iOS Mobile Releases

This maintenance release of Cisco Secure Client provides the bug fixes listed in Resolved Issues in Cisco Secure Client 5.0.05206 for Apple iOS, on page 11.

New Features in Cisco Secure Client 5.0.05203 for iOS Mobile Releases

This maintenance release of Cisco Secure Client provides necessary updates.

New Features in Cisco Secure Client 5.0.02602 for iOS Mobile Releases

This maintenance release of Cisco Secure Client provides necessary updates.

New Features in Cisco Secure Client 5.0.02530 for iOS Mobile Releases

This maintenance release of Cisco Secure Client provides user interface improvements and has the following known limitation:

Known Issue:

CSCwf44072—Change Settings button in untrusted server prompt doesn't open Settings page

New Features in Cisco Secure Client 5.0.01256 for iOS Mobile Releases

This maintenance release of Cisco Secure Client provides the bug fixes listed in Resolved Issues in Cisco Secure Client 5.0.01256 for Apple iOS, on page 11.

New Features in Cisco Secure Client 5.0.01241 for iOS Mobile Releases

This maintenance release of Cisco Secure Client includes the following new features and provides the bug fixes listed in Resolved Issues in Cisco Secure Client 5.0.00246 for Apple iOS, on page 11.

- Support for TLS version 1.3 to encrypt VPN connections, with the following additional cipher suites: TLS_AES_128_GCM_SHA256 and TLS_AES_256_GCM_SHA384

Note Secure Client TLS 1.3 connections require a secure gateway that also supports TLS 1.3. In release 9.19(1) of the ASA, this support is available. Connections fall back to TLS versions that the headend supports.

DTLS 1.3 is not yet supported.

In the Tunnel Statistics in the UI, the data tunnel protocol is displayed; therefore, if DTLS is negotiated, that will be shown, even though the initial TLS connections may be TLS 1.3.

- The ability to import VPN xml profile via vendor data

Known Issue:

CSCwd93529—iOS Siri Connect to VPN shortcut not working

CSCwc01260—AnyConnect connections might show an unexplained disconnect after running for several days

New Features in Cisco Secure Client 5.0.00246 for iOS Mobile Releases

This maintenance release of Cisco Secure Client provides the bug fixes listed in Resolved Issues in Cisco Secure Client 5.0.00246 for Apple iOS, on page 11.

New Features in Cisco Secure Client 5.0.00230 for iOS Mobile Releases

This 5.0.00230 version introduces the new Cisco Secure Client for iOS, including AnyConnect.

Apple iOS Cisco Secure Client Feature Matrix

The following features are supported in Cisco Secure Client for Apple iOS devices:

Category: Feature	Apple iOS
Zero Trust Access	Yes
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
TLS 1.3	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 Secure Client 4.0.09xxx and iOS 10.3 or later.

Category: Feature	Apple iOS
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:	
YubiKey	Yes
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
Cisco Secure Client specific status icon	No
Mobile Posture: (AnyConnect Identity Extensions, ACIDex)	
Serial number or unique ID check	Yes
OS and Cisco Secure Client version shared with headend	Yes
Cisco Secure Client Network Visibility Module 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 Cisco Secure Firewall ASA due to operating system implementation.

Cisco Secure Firewall ASA Requirements

A minimum release of the Cisco Secure Firewall ASA is required to use the following features:

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

- SAML authentication —Secure Firewall ASA 9.7.1.24, 9.8.2.28, 9.9.2.1 or later. Make sure that both the client and server versions are up-to-date.
- TLS 1.3—Secure Firewall ASA 9.19.1 or later.
- TLS 1.2—Secure Firewall ASA 9.3.2 or later.
- Per-App VPN tunneling mode—Secure Firewall ASA 9.3.2 or later.
- IPsec IKEv2 VPN, Suite B cryptography, SCEP Proxy, or Mobile Posture—Secure Firewall ASA 9.0.

Other Cisco Headend Support

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

Cisco Secure Client IKEv2 connectivity is supported on Cisco ISR g2 15.2(4)M+.

Cisco Secure Client SSL and IKEv2 is supported on Cisco Secure Firewall Threat Defense, release 6.2.1 and later.

Guidelines and Limitations for Cisco Secure Client on Apple iOS

- (Cisco Zero Trust Access on iOS)—Because iOS does not support service processes, it uses push notifications to trigger a config sync. Therefore, instead of the config sync happening about every 10 minutes as it does on other platforms, it can take up to four hours.
- (iOS 14.0.x and later)—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 Cisco Secure Client 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.
- Cisco Secure Client can be configured by the user (manually), by the Cisco Secure Client VPN Profile, generated by the iPhone Configuration Utility (available in the Mac App Store), or using an Enterprise Mobile Device Manager.
- The Apple iOS device supports no more than one Cisco Secure Client VPN 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 Cisco Secure Client VPN profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.
- This release supports the tunnel keepalive feature; however, it reduces the battery life of the device. Increasing the update interval value mitigates this issue.
- DHE Incompatibility—With the introduction of DHE cipher support, incompatibility issues result in Cisco Secure Firewall ASA versions before 9.2. If you are using DHE ciphers with ASA releases earlier than 9.2, you must disable DHE ciphers on those Secure Firewall ASA versions.

  With the introduction of DHE cipher support, incompatibility issues result in Cisco Secure Firewall ASA versions before 9.2. If you are using DHE ciphers with ASA releases earlier than 9.2, you must disable DHE ciphers on those Secure Firewall 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.
- Cisco Secure Client collects device information when the UI is launched, and a VPN connection is initiated. Therefore, there are circumstances in which Cisco Secure Client 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.

Known Compatibility Issues

- Split tunneling to the Cisco Secure Firewall 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 Cisco Secure Client UI remains open and iOS mistakenly disconnects the Inter-Process Communication (IPC) between the UI and the internal Cisco Secure Client extension, any UI activity fails with an error or an incorrect response.

  To recover from this, you must close and restart the Cisco Secure Client 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 Cisco Secure Client UI must be opened when an updated VPN connection profile has been pushed to the client by the Cisco Secure Firewall ASA. If the UI is not opened, the updated profile will not be synchronized and therefore the changes will not be used.

- In a managed Per-App configuration, app traffic, configured for Per App, will flow 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). Apple confirmed this is expected behavior.

Cryptography Support

These less secure cipher suites have been removed:

- For SSL VPN, Cisco Secure Client no longer supports the following cipher suites from both TLS and DTLS: DHE-RSA-AES256-SHA and DES-CBC3-SHA
- For IKEv2/IPsec, Cisco Secure Client 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

Open and Resolved Cisco Secure Client 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 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 Cisco Secure Client 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 for Zero Trust Access 5.1.66944 for Apple iOS

Identifier	Headline
CSCwm44686	ZTA: Renewed cert not set in Relay via push notification if cfg rule not changed
CSCwm44730	Block enrollment when relay rules in config are empty

Resolved Issues in Cisco Zero Trust Access 5.1.4.46500 for Mobile iOS Releases

Identifier	Headline
CSCwk07978	ZTA iOS: webview disappears after user leaves and reopens ZTA

Resolved Issues in Cisco Secure Client 5.0.05207 for Apple iOS

Identifier	Headline
CSCwi51652	Unable to connect VPN with SAML auth

Resolved Issues in Cisco Secure Client 5.0.05206 for Apple iOS

Identifier	Headline
CSCwi39086	Embedded SAML auth failed to match cookie domain when cookie has subdomains
CSCwi40284	URI external control import profile failing with a crash

Resolved Issues in Cisco Secure Client 5.0.01256 for Apple iOS

Identifier	Headline
CSCwd94735	AnyConnect VPN crashes when vendor data are not configured correctly
CSCwe49458	ISE is not identifying Apple M1 devices correctly using AnyConnect VPN

Resolved Issues in Cisco Secure Client 5.0.01241 for Apple iOS

Identifier	Headline
CSCwd68196	AnyConnect iOS app hangs on M1/M2 macOS Ventura when connecting

Resolved Issues in Cisco Secure Client 5.0.00246 for Apple iOS

Identifier	Headline
CSCwc01260	iOS 15: Unable to establish VPN triggered by On Demand