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

First Published: 2023-08-10

Last Modified: 2026-09-24

Cisco Secure Client for Android Mobile Devices

Cisco Secure Client (including AnyConnect) for Android Mobile Devices provides remote Android and ChromeOS 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. Administrators can also choose to configure Network Visibility Module (NVM) and Cisco Umbrella capabilities for additional functionality.

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 Android devices.

The Cisco Secure Client app is available on Google Play, except for the Kindle package, which is available on Amazon.com. 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 Android Beta Testing

Beta builds of Cisco Secure Client are made available for pre-release testing.

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

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

Android Supported Devices

Full support for Cisco Secure Client on Android is provided on devices running Android 4.4 (KitKat) through the latest release of Android.

In order to use the Umbrella module for Cisco Secure Client for Android, you must have Android 6.0 or later.

Cisco Secure Client for Kindle Fire HD is available from Amazon for the Kindle Fire HD devices, and the New Kindle Fire. Secure Client for Kindle is equivalent in functionality to the Secure Client for Android package.

For all current Chromebooks, Cisco Secure Client and Zero Trust Access for Android is officially supported and strongly recommended for the optimal Cisco Secure Client and Zero Trust Access experience on ChromeOS. The native ChromeOS client is intended only for legacy Chromebooks incapable of running Android applications.

ChromeOS Flex is supported and is configured and utilized the same way as ChromeOS.

Per-App VPN is supported in managed and unmanaged environments. In a managed environment using Samsung KNOX MDM, Samsung devices running Android 4.3 or later with Samsung Knox 2.0, are required. When using Per App in an unmanaged environment, the generic Android methods are used.

For the Network Visibility Module (NVM) capabilities, Samsung devices that are running Samsung Knox 2.8 or later (including 3.3), which requires Android 7.0 or later, are required. For configuration of NVM, the Cisco Secure Client Profile Editor from Secure Client 5.x is also required. Earlier releases do not support mobile NVM configurations.

As per the Cisco Secure Client policy of day-zero support, we can ensure full compatibility and functionality with a new operating system version on the very day that the new OS version is released to the public. We have proactively tested our product against the upcoming OS release and ensured that it works without issues, errors, or security vulnerabilities as part of same-day support. We provide this service to prevent disruptions, maintain data security, and allow users to leverage new OS features immediately.

Umbrella Module for Cisco Secure Client for Android

In release 5.x, Android offers the Cisco Umbrella module for Cisco Secure Client for Android 6.0.1 and later devices. This roaming client for managed and unmanaged Android devices provides DNS-layer protection, and this protection extends to both apps and browsing covered by the work profile.

A mobile device management system (MDM) is required to deploy this client to Android devices and to push the Umbrella configuration to the Android devices. For a list of supported MDMs and other prerequisites, see Prerequisites for Deploying the Umbrella Module for Cisco Secure Client on Android OS.

Some features may have limitations in functionality:

- Per-app VPN does not work with the Umbrella Module because of OS restrictions. If remote access VPN is active, Umbrella protection will only apply to DNS traffic that is intercepted by the VPN tunnel. If remote access is configured for per-app VPN, Umbrella protection only applies to DNS traffic for the tunneled applications.
- Always-On VPN should not be used with the lockdown (Fail Close) option when using Umbrella protection because it stops internet access for the user when the VPN server is not reachable. Refer to your MDM guide to turn off the lockdown setting when Always-On is turned on.

For an explanation of the complete Umbrella feature set, refer to the Umbrella Module for AnyConnect (Android OS) documentation.

Licensing Requirements for Umbrella on Android

You can enable the Umbrella module for Cisco Secure Client for Android with or without a license. Refer to Cisco Secure Client Ordering Guide for Secure Client software license details. Trial Premier licenses are available for administrators at http://www.cisco.com/go/license. Android for Secure Client requires a Cisco Secure Firewall ASA image. For licensing questions and evaluation licenses, contact ac-temp-license-request@cisco.com and include a copy of **show version** from your Cisco Secure Firewall ASA.

Umbrella licenses are required for the Umbrella module on Cisco Secure Client. Click https://learn-umbrella.cisco.com/datasheets/cisco-umbrella-package-comparison-2 for additional information.

Prerequisites for Deploying the Umbrella Module for Cisco Secure Client on Android OS

Note Cisco Secure Client monitors traffic generated from apps and browsers within the work profile created in an MDM and blocks or allows browsing accordingly. Any traffic generated outside the work profile by apps and/or browsers is not monitored.

- Mobile device management system (MDMs) for deploying the software and pushing the Umbrella configuration to the mobile devices. Current tested versions are Mobile Iron, Meraki, VMWare workspace 1 (Airwatch), or Microsoft Intune.
- Android (Samsung/Google Pixel) mobile devices with Android OS version 6.0.1 and above.
- Umbrella license to configure DNS policies, manage registered Android devices, and for reporting.
- Umbrella organization ID for enabling the feature.
- For Trusted Network Detection (TND):
  - If the Umbrella module detects a virtual appliance (VA) with HTTPS enabled, it deactivates itself; however, if the VA does not support HTTPS, the Umbrella module continues.
  - All VA FQDN in umbrella_va_fqdns must be enabled.

New Features

New Features in Cisco Zero Trust Access 5.1.19.6982 for Android Mobile Releases

This version of Cisco Zero Trust Access for Android includes support for the following, and resolves the bug listed in Resolved Issues for Zero Trust Access 5.1.19.6982 for Android, on page 17:

- TIA/TND support—Now available on Generic Android. Enables the recognition of a predefined trusted network. For additional details, see Trusted Networks for Zero Trust Access Connections in the *Cisco Secure Access Help*.
- Localization support.

- Support for Pause Proxy Configuration—Now available on Generic Android. Refer to Updates to Zero Trust Access Module Tile for details about this feature. For configuration details and pausing options, refer to Add a Zero Trust Access Profile in the *Cisco Secure Access Help*.

New Features in Cisco Zero Trust Access 5.1.18.6001 for Android Mobile Releases

Sept 14. 2026

This version of Secure Client Zero Trust Access includes the following new features:

- Support for Pause Proxy Configuration—Only available on Android Samsung Knox version 3.13. Refer to Updates to Zero Trust Access Module Tile for details about this feature. For configuration details and pausing options, refer to Add a Zero Trust Access Profile in the *Cisco Secure Access Help*.
- OS Profile Support—Ability to set up profiles for Zero Trust Access that are specific to each operating system (such as one for Windows and one for Android). Within Secure Access, you can set up different profiles so that each operating system is configured with its own specific Zero Trust Access behaviors and features.
- Added profile name and organization name in Enrollment settings.

New Features in Cisco Zero Trust Access 5.1.15.4264 for Android Mobile Releases

This version of Cisco Zero Trust Access for Android includes support for the following:

Samsung Knox 3.13 TIA/TND support to enable the recognition of a predefined trusted network. Trusted networks are used in universal Zero Trust Network Access configuration so the threat defense devices can enforce rules for the private resources associated with them, based on the assigned trusted network. For additional details, see Trusted Networks for Zero Trust Access Connections in the Cisco Secure Access Help.

New Features in Cisco Secure Client 5.1.15.344 for Android Mobile Releases

This version of Cisco Secure Client for Android includes resolves the bug listed in Resolved Issues in Cisco Secure Client 5.1.15.344 for Android, on page 17.

New Features in Cisco Secure Client 5.1.15.295 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.1.15.295 for Android, on page 17 and includes the following new feature:

Support for Network Visibility Module profile delivery for those Samsung Android devices using Knox NPA deployment without an MDM that supports that Knox NPA vendor-specific configuration. Refer to Managed Configuration Keys Supported by Cisco Secure Client for additional details.

New Features in Cisco Zero Trust Access 5.1.13.3431 for Android Mobile Releases

This release of Cisco Secure Access Zero Trust Access resolves the CSCws00283 defect listed in Resolved Issues for Zero Trust Access 5.1.13.3431 for Android, on page 17.

CSCws00283—(Zero Trust Access module fails to start when trust bundle signing certificate has expired.) The defect only affects users running the Zero Trust Access module of Cisco Secure Client, versions 5.1.8 through 5.1.12. In affected versions (5.1.8–5.1.12), the Zero Trust Access module incorrectly validates a code-signing certificate expiration date. If the client has not been upgraded to 5.1.13 or later before the expiration date has been reached, the module will stop functioning.

Affected Cisco Secure Client Zero Trust Access module versions:

- 5.1.9: Must be upgraded to 5.1.13 or above before January 14, 2026
- 5.1.10: Must be upgraded to 5.1.13 or above before Jauary 14, 2026
- 5.1.11: Must be upgraded to 5.1.13 or above before June 4, 2026
- 5.1.12: Must be upgraded to 5.1.13 or above before Jun 4 2026

New Features in Cisco Secure Client 5.1.11.416 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.1.11.416 for Android, on page 17.

New Features in Cisco Secure Client 5.1.9.115 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.1.9.115 for Android, on page 17.

New Features in Cisco Secure Client 5.1.11.416 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.1.11.416 for Android, on page 17.

New Features in Cisco Zero Trust Access 5.1.9.1302 for Android Mobile Releases

This release provides updates to the Zero Trust Access offering (which is an additional Cisco Secure Client app for Android) and resolves the bugs listed in Resolved Issues in Cisco Zero Trust Access 5.1.9.1302 for Android, on page 18.

New Features in Cisco Zero Trust Access 5.1.8.757 for Android Mobile Releases

This release provides updates to the Zero Trust Access offering (which is an additional Cisco Secure Client app for Android) and includes the following features and known issues, and resolves the bugs listed in Resolved Issues in Cisco Zero Trust Access 5.1.8.757 for Android, on page 18.

Android 15 (Knox 3.11+) on supported Samsung devices now has Knox Unmanaged support. Zero Trust Access uses Knox by default in unmanaged user spaces with no configuration necessary. In prior Android 14+ versions, generic Android (VPN) was supported, as well as the Knox Managed (Knox 3.10+) framework, upon configuration by an administrator.

Known Issues:

- CSCwo07036—VPN Mobile: ZTNA app forced shutdown not closing interceptor
- CSCwo15171—Samsung ZTA: Brave browser not reaching private resources with ZTA enrolled
- CSCwo26917—Samsung ZTA: ZTA+VPN active, disconnect VPN, ZTA status shows 'Access issues found'
- CSCwo26959—Android ZTA Generic: Data failing after app upgrade until app is opened
- CSCwo27051—Android Generic ZTA: Unable to reach private resources after network transition

New Features in Cisco Secure Client 5.1.8.110 for Android Mobile Releases

This version of Cisco Secure Client for Android includes the following known issue, and resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.1.8.110 for Android, on page 18.

Known Issues:

CSCwn53818—NVM: Android: NVM is not reporting end flows on Android 14. Refer to Samsung ticket ID 00310883 for additional information.

New Features in Cisco Secure Client 5.1.7.84 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.1.7.84 for Android, on page 18.

New Features in Cisco Zero Trust Access 5.1.6.7550 for Android Mobile Releases

This maintenance release provides updates to the Zero Trust Access offering, which is an additional Cisco Secure Client app for Android, and includes the following new features and functionalities:

- Generic Android Support—Zero Trust Access can now run on any device with Android 14 or greater, and not just on Samsung devices. The table below highlights the differences between Generic Android and Samsung Knox.
- Addition of Zero Trust Configuration section—A new config viewer that shows the configuration that is being used by the enrollment.
- Improved step-up authentication UX—Adds a new alert card which can be used for user notifications regarding access.
- When Zero Trust Access is active and you activate another VPN, you'll get a "Zero Trust Access is paused" notification. The user will need to open the app and resume it to get access again.

Zero Trust Access is available as a new application, downloaded separately from Cisco Secure Client, on the Google Play Store.

For the Knox implementation only, you must have a device running Android 14 with Samsung Knox 3.10 (or later). The Samsung Knox Service Plugin (KSP) is also available in the Google PlayStore and is required when configuring an MDM vendor (such as Ivanti MobileIron) for device enrollment with Zero Trust.

Refer to Set up the Zero Trust Access App for Android on Samsung Devices for the 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.

Table 1: Advantages of Zero Trust Access Running on Samsung Knox Versus Generic Android

Zero Trust Access Details	Samsung Knox	Generic Android
Simultaneous compatibility with third-party security solutions that leverage VPN framework (such as Cisco AnyConnect VPN, Cisco Umbrella, and Mobile Threat Defense solutions)	Yes	No
Real-time process-level flow metadata	Yes	No, which restricts the type of supported policies
Exempt from packet and route injection attacks like a VPN	Yes	No
Apps unable to bypass DNS interception	Yes	No

Zero Trust Access Details	Samsung Knox	Generic Android
Process-level pico-segmentation of traffic all the way from endpoint to destination	Yes	No
Process-level split DNS	Yes	No
Tamper protection using Knox warranty bit	Yes	No

New Features in Cisco Secure Client 5.1.6.113 for Android Mobile Releases

This maintenance release of Cisco Secure Client provides necessary updates to the Android Mobile release.

New Features in Cisco Secure Client 5.1.5.56 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.1.5.56 for Android, on page 18.

New Features in Cisco Secure Client 5.1.4.61 for Android Mobile Releases

This version of Cisco Secure Client for Android includes the following feature and resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.1.4.61 for Android, on page 18:

Added support for FedRAMP with the Umbrella Android client.

New Features in Cisco Zero Trust Access 5.1.4.6263 for Android Mobile Releases

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

Zero Trust Access is available as a new application, downloaded separately from Cisco Secure Client, on the Google Play Store. You must have a device running Android 14 with Samsung Knox 3.10 (or later). The Samsung Knox Service Plugin (KSP) is also available in the Google PlayStore and is required when configuring an MDM vendor (such as Ivanti MobileIron) for device enrollment with Zero Trust.

Refer to Set up the Zero Trust Access App for Android on Samsung Devices for the 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.

Known Issues:

- CSCwj81408—ZTA/Android: Interceptor error after reboot when Zero Trust Access app is loaded
- CSCwj81415—ZTA/Android: UI may get stuck if device is rotated during enrollment
- CSCwj81423—ZTA/Android: iperf udp does not work with some Apps
- CSCwj80873—ZTA/Android: App may crash while using split screen mode and rotating device orientation

New Features in Cisco Secure Client 5.0.05042 for Android Mobile Releases

This version of Cisco Secure Client for Android includes the following new behavior for the Umbrella Module running on Android 14 and resolves the bug listed in Resolved Issues in Cisco Secure Client 5.0.05042 for Android, on page 19.

- The Umbrella service now displays a notification before starting Umbrella Protection in the background.

Known Issue: CSCwh30940—App crash attempting to use inserted yubikey

New Features in Cisco Secure Client 5.0.03085 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bug listed in Resolved Issues in Cisco Secure Client 5.0.03085 for Android, on page 19.

New Features in Cisco Secure Client 5.0.03084 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.0.03084 for Android, on page 19.

New Features in Cisco Secure Client 5.0.02078 for Android Mobile Releases

This version of Cisco Secure Client for Android includes the following feature and support updates, and resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.0.02078 for Android, on page 19.

- Support for additional ports (53 and 5353) to communicate to Umbrella resolvers when sending encrypted DNS requests. A new port is checked when the current 443 port fails, and a new socket channel is created for the new port with any changes. (CSCwe69440).
- We do not support upgrades on devices running a version prior to Android 4.2.
- Android Quick Setting Tile support for VPN connection and disconnection enabled by default, when added.
- Enhancements available with MDM configuration:
  - Allow or block users on Android from creating new VPN connections
  - Block Untrusted Server

Known Issues: As a result of migration to Android SDK 31 and its OS limitations, the Cisco Secure Client app requires the "Alarms & Reminders" Android permission to run the Umbrella Protection Service. In both managed and unmanaged Android deployments, users who choose to disable this permission may cause the app to stop working.

New Features in Cisco Secure Client 5.0.01253 for Android Mobile Releases

This version of Cisco Secure Client for Android upgrades the Umbrella functionality to target Android SDK 31 and resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.0.01253 for Android, on page 19.

New Features in Cisco Secure Client 5.0.01251 for Android Mobile Releases

This version of Cisco Secure Client for Android includes the following feature and support updates, and resolves the bug listed in Resolved Issues in Cisco Secure Client 5.0.01251 for Android, on page 19.

- Support for TLS 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 Secure Firewall 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.

- If you are using certificates with biometric authentication enabled, you will receive an error message that your headed can no longer accept the certificate. You must delete and reimport the certificate.

New Features in Cisco Secure Client 5.0.00247 for Android Mobile Releases

This version of Cisco Secure Client for Android resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.0.00247 for Android, on page 20.

New Features in Cisco Secure Client 5.0.00238 for Android Mobile Releases

This version of Cisco Secure Client for Android includes the following features and resolves the bugs listed in Resolved Issues in Cisco Secure Client 5.0.00238 for Android, on page 20. An open issue is listed in Open Issues in Cisco Secure Client 5.0.00238 for Android, on page 20.

- Support for split exclude tunneling

Note The split exclude configuration must have less than 100 IPv4 routes and less than 20 IPv6 routes.

- Dark theme

In the next Android Mobile release, the medium widget will be deprecated.

Known Issues with Google on Android

Because of a limitation from Google on Android OS, the application download may fail in the Google Play store after enabling the Umbrella Cisco Secure Client module. To avoid this, download the applications before enabling the Umbrella module. Google has fixed this behavior in Android OS "Q." For more information, see the Google issue tracker.

Android Cisco Secure Client Feature Matrix

The following table indicates the remote access features that are supported by Cisco Secure Client on Android:

Category: Feature	Android VPN
Zero Trust Access	Yes
Samsung Knox 3.13 TIA/TND	Yes

Category: Feature	Android VPN
OS profile support	Yes
Profile name and org name in Enrollment settings	Yes
Pause proxy config	Yes. Only Samsung Knox version 3.13+.
Deployment and Configuration:	
Localization support	Yes
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	Yes
Suite B (IPsec only)	Yes
TLS compression	Yes
Dead peer detection	Yes
Tunnel keepalive	Yes
Multiple active network interfaces	No
Per-App Tunneling	Yes, Android 5.0+ or Samsung Knox
Per-App Tunneling (Disallowed Apps Mode)	Yes
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, works with split include
Auto Reconnect / Network Roaming	Yes, regardless of the Auto Reconnect profile specification, Cisco Secure Client Mobile always attempts to maintain the VPN as users move between 3G and WiFi networks
VPN on-demand (triggered by destination)	No
VPN on-demand (triggered by application)	No

Category: Feature	Android VPN
Rekey	Yes
IPv4 public transport	Yes
IPv6 public transport	Yes, requires Android 5.0 or later
IPv4 over IPv4 tunnel	Yes
IPv4 over IPv6 tunnel	Yes
IPv6 over IPv4 tunnel	Yes
IPv6 over IPv6 tunnel	Yes
Default domain	Yes
DNS server configuration	Yes
Private-side proxy support	Direct proxy support on Android 10+. PAC proxy support on Android 11+. See note below.
Proxy Exceptions	Yes
Public-side proxy support	No
Pre-login banner	Yes
Post-login banner	Yes
DSCP Preservation	Yes
Connecting and Disconnecting:	
VPN load balancing	Yes
Backup server list	Yes
Optimal Gateway Selection	No
Authentication:	
Touch ID	No
SAML 2.0	Yes
Client Certificate Authentication	Yes
Online Certificate Status Protocol (OCSP)	Yes
Manual user certificate management	Yes
Manual server certificate management	Yes
SCEP legacy enrollment Please confirm for your platform.	Yes
SCEP proxy enrollment Please confirm for your platform.	Yes
Automatic certificate selection	Yes
Manual certificate selection	Yes
Smart card support	No

Category: Feature	Android VPN
Username and password	Yes
Tokens/challenge	Yes
Double authentication	Yes
Group URL (specified in server address)	Yes
Group selection (drop-down selection)	Yes
Credential prefill from user certificate	Yes
Save password	No
User interface:	
Standalone GUI	Yes
Native OS GUI	No
API / URI Handler (see below)	Yes
UI customization	No
UI localization	Yes, app contains pre-packaged languages
User preferences	Yes
Home screen widgets for one-click VPN access	Yes
Cisco Secure Client specific status icon	Optional
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 Visbility Module support	Yes, with specific Samsung Knox and MDM requirements
URI Handling:	
Add connection entry	Yes
Connect to a VPN	Yes
Credential pre-fill on connect	Yes
Disconnect VPN	Yes
Import certificate	Yes
Import localization data	Yes
Import XML client profile	Yes
External (user) control of URI commands	Yes
Reporting and Troubleshooting:	
Statistics	Yes

Category: Feature	Android VPN
Logging / Diagnostic Information (DART)	Yes
Certifications:	
FIPS 140-2 Level 1	Yes

* The split exclude configuration must have less than 100 IPv4 routes and less than 20 IPv6 routes.

Refer to Set up the Zero Trust Access App for Android on Samsung Devices for additional information.



Note Before deploying a PAC proxy configuration for Cisco Secure Client on Android, ensure that your application is compatible with PAC proxy.

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.

Android on Google Play Store

Cisco highly recommends that all users run the current version of our Android release, which is available on the Google play store. Additionally, an .apk version is available on Cisco.com for the current version only. In the unlikely event that the Google play store is unavailable, administrators who have access to the Cisco Secure Client software download page can get this version.

Known Compatibility Issues

- If you are experiencing connectivity issues with the VPN tunnel on Android 10, try disabling Android 10 Private DNS functionality.
- IPv6 on public and private interfaces.

  IPv6 is supported on both private and public transports using Cisco Secure Client 4.05015 (and later), on Android 5 (and later). With this combination the following is now allowed: IPv4 over an IPv6 tunnel, IPv6 over an IPv6 tunnel.

  This is in addition to the previously allowed tunnel configurations on earlier Cisco Secure Client and Android releases: IPv4 over an IPv4 tunnel, and IPv6 over an IPv4 tunnel.

Note Due to Google issue 65572, IPv6 over IPv4 does not work on Android 4.4. You must use Android 5 or later.

- Battery saver and Cisco Secure Client:
  - Android 5.0 introduced battery saver capabilities that block background network connectivity on your device. When battery saver is enabled, Cisco Secure Client will transition to the Paused state if it is in the background. To work around this on Android 5.0, users may turn off battery saver via the device settings: Settings -> Battery -> Battery saver or from the notification bar.
  - In Android 6.0+, when Cisco Secure Client transitions to the Paused state as a result of battery saver, you see a popup with the option to make Cisco Secure Client part of the allowed list from battery saver mode. Making Cisco Secure Client part of the allowed list provides a battery savings without impacting it's ability to run in the background.
  - Once Cisco Secure Client is paused due to the batter saver, a manual reconnect is necessary to bring Cisco Secure Client out of the Paused state, regardless of your action to turn off battery saver or to add Secure Client to the allowed list.
- Split DNS does not work on any Android 4.4 device, and also does not work on Samsung 5.x Android devices. For Samsung devices, the only workaround is to connect to a group with split DNS disabled. On other devices you must upgrade to Android 5.x to receive the fix for this problem.

  This is due to a known issue that is present in Android 4.4 (Issue #64819), fixed in Android 5.x, but not incorporated into Samsung 5.x android devices.
- Due to a bug in Android 5.x (Google Issue #85758, Cisco Issue # CSCus38925), if the Secure Client app is closed from the recent apps screen, it may not operate properly. To restore proper operation, terminate Secure Client in **Settings** and then restart it.
- On Samsung mobile devices the **Settings > Wi-Fi > Smart network switch** allows switching from Wifi to LTE to maintain a stable Internet connection (when the WiFi connection is not optimum). This also results in a pause and reconnect of the active VPN tunnel. Cisco recommends turning this off, since it may result in continuous reconnects.
- On Android 5.0 (Lollipop), which supports multiple active users, the VPN connection tunnels data for a single user only, not for all users on the device. Background data flow may be occurring in the clear.

- Due to a bug in Android 4.3.1(Google Issue #62073), users using the Cisco Secure Client ICS+ package cannot enter non-fully qualified domain names. For example, users cannot type "internalhost," they must type "internalhost.company.com."
- The AT&T firmware updates on HTC One to Android 4.3 (software version: 3.17.502.3) do not support "HTC Cisco Secure Client." Customers must uninstall "HTC Cisco Secure Client" and install "Cisco Secure Client ICS+." (HTC Secure Client will work on the international edition, with software version of 3.22.1540.1). Check your software version on your device at **Settings > About > Software information > Software number**.
- We are pleased to report that Google Issue #70916 (VPN connections will fail to connect if the administrator has set the MTU for Android tunnels lower than 1280) has been resolved in Android 5.0 (Lollipop). The following problem information is provided for reference:

  Due to a regression in Android 4.4.3,(Google Issue #70916, Cisco CSCup24172), VPN connections will fail to connect if the administrator has set the MTU for Android tunnels lower than 1280. This issue has been reported to Google and will require a new version of the OS to correct the regression introduced in Android 4.4.3. To workaround this problem, ensure that the headend administrator has not configured the tunnel MTU to be lower than 1280.

  When encountered, the message displayed to the end user is: `System configuration settings could not be applied. A VPN connection will not be established`, and Secure Client debug logs will report:

```
E/vpnandroid( 2419): IPCInteractionThread: NCSS: General Exception occured, telling
client
E/vpnandroid( 2419): java.lang.IllegalStateException: command '181 interface fwmark
rule add tun0'
failed with '400 181 Failed to add fwmark rule (No such process)'
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1473)
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1419)
E/vpnandroid( 2419): at
com.cisco.android.nchs.aidl.IICSSupportService$Stub$Proxy.establish
(IICSSupportService.java:330)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.VpnBuilderWrapper.establish
(VpnBuilderWrapper.java:137)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.NCSSIPCServer.callServiceMethod
(NCSSIPCServer.java:233)
E/vpnandroid( 2419): at
com.cisco.android.nchs.ipc.IPCInteractionThread.handleClientInteraction
(IPCInteractionThread.java:230)
E/vpnandroid( 2419): at com.cisco.android.nchs.ipc.IPCInteractionThread.run
(IPCInteractionThread.java:90)
E/acvpnagent( 2450): Function: ApplyVpnConfiguration
File: NcssHelper.cpp Line: 740 failed to establish VPN
E/acvpnagent( 2450): Function: PluginResult AndroidSNAKSystem::configDeviceForICS()
File: AndroidSNAKSystem.cpp Line: 665 failed to apply vpn configuration
E/acvpnagent( 2450): Function: virtual PluginResult
AndroidSNAKSystem::ApplyConfiguration()
File: AndroidSNAKSystem.cpp Line: 543 Failed to Configure System for VPN.
```

- We are pleased to report that Android 4.4 (KitKat) bug Google Issue #61948 (Secure Client users will experience High Packet Loss over their VPN connection /users will experience timeouts) has been resolved in Google's release of Android 4.4.1 which Google has begun distributing to some devices via Software Update. The following problem information is provided for reference:

  Due to a bug in Android 4.4 (Issue #61948, also see the Cisco Support Update), Secure Client users will experience High Packet Loss over their VPN connection. This has been seen on the Google Nexus 5 running Android 4.4 with Secure Client ICS+. Users will experience timeouts when attempting to access

certain network resources. Also, in the Secure Firewall ASA logs, a syslog message will appear with text similar to "Transmitting large packet 1420 (threshold 1405)."

Until Google produces a fix for Android 4.4, VPN administrators may temporarily reduce the maximum segment size for TCP connections on the Cisco Secure Firewall ASA by configuring the following sysopt connection tcpmss <mss size>. The default for this parameter is 1380 bytes. Reduce this value by the difference between the values seen in the ASA logs. In the above example, the difference is 15 bytes; the value should thus be no more than 1365. Reducing this value will negatively impact performance for connected VPN users where large packets are transmitted.

- Cisco Secure Client for Android may have connectivity issues when connecting to a mobile network using the IPv6 transition mechanism known as 464xlat. Known affected devices include the Samsung Galaxy Note III LTE connecting to the T-Mobile US network. This device defaults to an IPv6 only mobile network connection. Attempting a connection may result in a loss of mobile connectivity until the device is rebooted.

  To prevent this problem, use the Cisco Secure Client ICS+ app, and change your device settings to obtain IPv4 network connectivity or connect using a Wi-Fi network. For the Samsung Galaxy Note III LTE connecting to the T-Mobile US network, follow the instructions provided by T-Mobile to set the Access Point Name (APN) on your device, making sure APN Protocol is set to IPv4.

- The Cisco Secure Client ICS+ package may have issues when a private IP address range within the VPN overlaps with the range of the outside interface of the client device. When this route overlap occurs, the user may be able to successfully connect to the VPN but then be unable to actually access anything. This issue has been seen on cellular networks which use NAT (Network Address Translation) and assign addresses within the 10.0.0.0 - 10.255.255.255 range. It is due to Cisco Secure Client having limited control of routes in the Android VPN framework. The vendor specific Android packages have full routing control and may work better in such a scenario.

- An Asus tablet running Android 4.0 (ICS) may be missing the tun driver. This causes AVF Cisco Secure Client to fail.

- Android security rules prevent the device from sending and receiving multimedia messaging service (MMS) messages while a VPN connection is up. Most devices and service providers display a notification if you try to send an MMS message while the VPN connection is up. Android permits sending and receiving of messages when the VPN is not connected.

- Due to Google Issue 41037, when pasting text from the clipboard, a space is inserted in front of the text. In Cisco Secure Client, when copying text such as a one time password, the user has to delete this erroneous white space.

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 5.1.19.6982 for Android

Identifier	Headline
CSCwt52351	Android zta: Android devices enrolled with Secure Access ZTNA trying to use IPv6 DNS server with no scope ID

Resolved Issues in Cisco Secure Client 5.1.15.344 for Android

Identifier	Headline
CSCwt95655	Registration is failing in Fedramp SSE Stage and Prod environments

Resolved Issues in Cisco Secure Client 5.1.15.295 for Android

Identifier	Headline
CSCwo96323	CSC: Silent notification triggered and stays persistent after always on triggered after idle timeout with always-on
CSCwt20725	Deployment key is visible in Cisco Secure Client for Android SSE
CSCwt33407	Support NVM profile via managed app configuration for Knox NPA deployments

Resolved Issues for Zero Trust Access 5.1.13.3431 for Android

Identifier	Headline
CSCws00283	Zero Trust Access module fails to start when trust bundle signing certificate has expired

Resolved Issues in Cisco Secure Client 5.1.11.416 for Android

Identifier	Headline
CSCwh30940	App crash attempting to use inserted yubikey
CSCwo26748	Android 16 beta: Yubikey attempts redirects to demo page (library update needed)

Resolved Issues in Cisco Secure Client 5.1.9.115 for Android

Identifier	Headline
CSCwm10943	Android: Not able to import profile or certificates with active VPN
CSCwn77955	CSC/Umbrella network pause and reconnect regression triggered ADB fatal exception
CSCwo67465	Suppress modal dialog box error messages from being displayed when Always On is enabled on Android

Resolved Issues in Cisco Zero Trust Access 5.1.9.1302 for Android

Identifier	Headline
CSCwo26959	Android ZTA Generic: Data failing after app upgrade until app is opened
CSCwo67465	Suppress modal dialog box error messages from being displayed when Always On is enabled on Android

Resolved Issues in Cisco Zero Trust Access 5.1.8.757 for Android

Identifier	Headline
CSCwj94669	Android ZTA enrollment flow should auto-advance to SSO after allowing notifications
CSCwk68094	Enable ZTNA logs before first successful enrollment

Resolved Issues in Cisco Secure Client 5.1.8.110 for Android

Identifier	Headline
CSCwn83287	Identify Android VPN client on ChromeOS as "chromeos"

Resolved Issues in Cisco Secure Client 5.1.7.84 for Android

Identifier	Headline
CSCwi58890	Vulnerabilities in gson 2.8.6 CVE-2022-25647
CSCwn15682	Umbrella crashed after install/startup in managed work profile
CSCwn34977	ADB crash with MDM managed Always On after restart/power off-on and viewing Secure Client app in split mode

Resolved Issues in Cisco Secure Client 5.1.5.56 for Android

Identifier	Headline
CSCwh43185	Cannot deploy user certificates using MDM to AnyConnect Certificate store on Android
CSCwi22666	SAML + Cert failing on Android 12+ for keychain certs

Resolved Issues in Cisco Secure Client 5.1.4.61 for Android

Identifier	Headline
CSCvu83459	AnyConnect on Android takes hostname as localhost
CSCwf11486	Keychain cert import fails on Android when always-on is enabled

Resolved Issues in Cisco Secure Client 5.0.05042 for Android

Identifier	Headline
CSCwh01153	AnyConnect notification "VPN connection is required by your Device Administrator" touch does nothing

Resolved Issues in Cisco Secure Client 5.0.03085 for Android

Identifier	Headline
CSCwh50136	Secure Client fails to import certificate

Resolved Issues in Cisco Secure Client 5.0.03084 for Android

Identifier	Headline
CSCwd15758	Android always-on retry mechanism not working after device low memory
CSCwf49544	AnyConnect Android app on ChromeOS fails to authenticate with client cert error
CSCwf86725 (Umbrella)	CSC 5.0 - Adding support for sending unencrypted DNS on port 53
CSCwf88091	App crash attempting connection with split-DNS configuration

Resolved Issues in Cisco Secure Client 5.0.02078 for Android

Identifier	Headline
CSCwe44665	ENH: Add Block Untrusted Servers feature in the Managed Configuration Keys for Android
CSCwe60126	AnyConnect failing to connect to Meraki MX via SAML
CSCwe67925	ENH: Android AnyConnect users are able to create new connection
CSCwe69440	CSC 5.0 - Adding support for port 53 and 5353 for Umbrella Android Client

Resolved Issues in Cisco Secure Client 5.0.01253 for Android

Identifier	Headline
CSCwe41637	Android: "Failed to Bind to VPNService" after upgrade to 5.0.01251
CSCwe42138	Android: Legacy VPN sdk not working in 5.0.01251

Resolved Issues in Cisco Secure Client 5.0.01251 for Android

Identifier	Headline
CSCwd86009	Android managed configuration should be checked when GUI is reopened

Resolved Issues in Cisco Secure Client 5.0.00247 for Android

Identifier	Headline
CSCwb57297	Medium widget missing component and behaves inconsistently (remove support)
CSCwb90260	IP and route information not available in logging system tab (Android 11+)
CSCwc04300	VPN configuration fails for Cisco Secure Client Android using MobileIron Core
CSCwc24658	Android always-on not auto reconnecting after disconnect due to idle timeout
CSCwc53813	SSO external browser closes when focus is lost

Resolved Issues in Cisco Secure Client 5.0.00238 for Android

Identifier	Headline
CSCwb64589	AnyConnect 4.10 delay on Android reconnections between IPv6 enabled cellular network and IPv4 Wi-Fi
CSCwb70409	Android - Add UI preference to customize PAC Proxy behavior

Open Issues in Cisco Secure Client 5.0.00238 for Android

Identifier	Headline
CSCwb90260	IP and route information not available in logging system tab (Android 11+)

Cisco Secure Client Mobile Related Documentation

For more information refer to the following documentation:

- Cisco Secure Client Release Notes
- Cisco Secure Client Administrator Guides
- Cisco Secure Firewall ASA Documentation Landing Page

© 2022–2026 Cisco Systems, Inc. All rights reserved.