Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1

First Published: 2023-07-27

Last Modified: 2026-09-11

Release Notes for Cisco Secure Client, Release 5.1.20.333

These release notes provide information for Cisco Secure Client on Windows, macOS, and Linux. An always-on intelligent VPN helps Secure Client devices to automatically select the optimal network access point and adapt its tunneling protocol to the most efficient method.

Download the Latest Version of Cisco Secure Client

For optimal performance, feature availability, and security, Cisco recommends Cisco Secure Client 5.1.20.333 as the primary recommended release for all users. Future defect fixes for any of the 5.x.x.x releases will be addressed only within the 5.1.x.x path. For those currently running any 5.0.x.x release, an upgrade is required for the benefit of ongoing maintenance.

Before you begin

To download the latest version of Cisco Secure Client, you must be a registered user of Cisco.com.

Procedure

Step 1 Follow this link to the Cisco Secure Client product support page:

http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html.

Step 2 Log in to Cisco.com.

Step 3 Click **Download Software**.

Step 4 Expand the **Latest Releases** folder and click the latest release, if it is not already selected.

Step 5 Download Secure Client Packages using one of these methods:

- To download a single package, find the package you want to download and click **Download**.
- To download multiple packages, click **Add to cart** in the package row and then click **Download Cart** at the top of the Download Software page.

Step 6 Read and accept the Cisco license agreement when prompted.

Step 7 Select a local directory in which to save the downloads and click **Save**.

Step 8 See the Cisco Secure Client Administrator Guide, Release 5.x.

Cisco Secure Client Package Filenames for Web Deployment

OS	Cisco Secure Client Web-Deploy Package Names
Windows	cisco-secure-client-win-*version*-webdeploy-k9.pkg (for ARM64) cisco-secure-client-win-arm64-*version*-webdeploy-k9.pkg
macOS	cisco-secure-client-macos-*version*-webdeploy-k9.pkg
Linux (64-bit)	cisco-secure-client-linux64-*version*-webdeploy-k9.pkg (for ARM64) cisco-secure-client-linux-arm64-*version*-webdeploy-k9.pkg

Cisco Secure Client Package Filenames for Predeployment

OS	Cisco Secure Client Predeploy Package Name
Windows	cisco-secure-client-win-*version*-predeploy-k9.zip (for ARM 64) cisco-secure-client-win-arm64-*version*-predeploy-k9.zip
macOS	cisco-secure-client-macos-*version*-predeploy-k9.dmg
Linux (64-bit)	(for RPM installer*) cisco-secure-client-linux64-*version*-predeploy-rpm-k9.tgz (for DEB installer*) cisco-secure-client-linux64-*version*-predeploy-deb-k9.tgz (for RPM ARM64) cisco-secure-client-linux-arm64-version-predeploy-rpm-k9.tgz for DEB ARM64) cisco-secure-client-linux-arm64-version-predeploy-deb-k9.tgz

Cisco Secure Client 5.1.20.333 New Features

Sept 11, 2026

This release includes the following updates and features, and resolves the defects that are described in Cisco Secure Client 5.1.20.333, on page 53.

- Support for macOS 27 (Golden Gate)
- Support and deployment for Endpoint Data Loss Prevention (Windows and macOS predeploy and Apple silicon M only)—Enables you to protect sensitive data on endpoints by controlling what data is transferred to external devices. It extends your data protection policies and ensures that sensitive data remains secure and compliant with your security requirements. For information on managing endpoint data loss prevention, enrolling devices, and troubleshooting, refer to Manage Endpoint Data Loss Prevention Using Cisco Secure Client in Secure Access or Create Deployment in Cisco XDR.
- Fallback to machine authentication for Network Access Manager (CSCwt18945)—Currently when a smart card is removed, the network connection either drops or remains tied to user-level authorization, depending on the configuration. Now Network Access Manager automatically transitions to machine authentication in these scenarios, ensuring the device stays connected to the network even when the user session is no longer active. This update is essential for maintaining reliable, consistent connectivity and is a signficant efficiency boost for IT departments. It allows for the provisioning of generic PCs without

the need to pre-install individual user certificates. Once connected via machine fallback, the system can handle certificate enrollment or push updates seamlessly, which significantly reduces the manual effort of provisioning machines. Refer to Networks, Network Connection Type Pane in the *Secure Client Administrator Guide*.

- Release 5.1.20.333 contains the following versions for the various modules:
  - Zero Trust Access—5.1.20.7023
  - Secure Client UI—5.1.20.2493
  - Cisco AnyConnect VPN core—5.1.20.333
  - DART—5.1.20.333
  - Umbrella—5.1.20.333
  - SBL—5.1.20.333
  - Network Access Manager—5.1.20.333
  - Network Visibility Module—5.1.20.333
  - Secure Firewall Posture—5.1.20.333
  - Endpoint Data Loss Prevention (Windows and macOS only)—1.5.0.292
  - ThousandEyes—2.43.2
  - ISE Posture—5.1.20.333
  - Duo Desktop—7.20.0.0
  - Endpoint Visibility Module (Windows and macOS)—1.8.0.5
- **Known Issues**: CSCww61247—Linux CSC UI remains in English after changing system language to a supported locale

Cisco Secure Client 5.1.19.1862 New Features

July 31, 2026

This release includes the following updates and features, and resolves the defects that are described in Cisco Secure Client 5.1.19.1862, on page 54:

- Support in Linux for Zero Trust Access Secure Boot and Kernel Lockdown. Refer to Secure Boot and Kernel Lockdown in ZTA Linux for additional information.
- Restrict Communication to Trusted Applications—Only Cisco signed applications can communicate with VPN services across all desktop platforms. This enhancement manages inter-process communications between applications based on Cisco's code signing requirements. It impacts all client applications developed using the Secure Client's published API as well. The preference is enabled by default as a security measure in the local policy file. Refer to Local Policy Preferences.
- Zero Trust Access localized strings are supported for all OSs.

- Network Location support on Zero Trust Access—Ability to apply the right Zero Trust Access profile based on where a user's device is connecting from, such as a corporate branch, office subnet, data center, or remote network. Refer to Get Started with Network Location Objects for Zero Trust Access.
- Release 5.1.19.1862 contains the following versions for the various modules:
  - Zero Trust Access—5.1.19.6509
  - Secure Client UI—5.1.19.2351
  - Cisco AnyConnect VPN core—5.1.19.1862
  - DART—5.1.19.1862
  - Umbrella— 5.1.19.1862
  - SBL—5.1.19.1862
  - Network Access Manager—5.1.19.1862
  - Network Visibility Module—5.1.19.1862
  - Secure Firewall Posture—5.1.19.1862
  - Endpoint Data Loss Prevention (Windows only)—1.5.0.292
  - ThousandEyes—2.43.2
  - ISE Posture—5.1.19.1862
  - Duo Desktop—7.19.0.0
  - Endpoint Visibility Module—1.8.0.5 (Windows), 1.7.0.8 (macOS)
- For related documentation, refer to the Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1 with a new look and feel.

Cisco Secure Client 5.1.18.314 New Features

June 25, 2026

This release includes the following updates and resolves the defects that are described in Cisco Secure Client 5.1.18.314, on page 55:

- Support for Ubuntu 26.04.
- 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 a different 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.
- Release 5.1.18.314 contains the following versions for the various modules:
  - Zero Trust Access—5.1.18.5828
  - Secure Client UI—5.1.18.2164
  - Cisco AnyConnect VPN core—5.1.18.314

- DART—5.1.18.314
- Umbrella— 5.1.18.314
- SBL—5.1.18.314
- Network Access Manager—5.1.18.314
- Network Visibility Module—5.1.18.314
- Secure Firewall Posture—5.1.18.314
- Endpoint Data Loss Prevention (Windows only)—1.4.0.253
- ThousandEyes—2.40.1
- ISE Posture—5.1.18.314
- Duo Desktop—7.17.0.0
- Endpoint Visibility Module—1.6.0.7 (1.7.0.8 is recommended)

Known Issues:

- CSCwv02573—RHEL 9.8 ARM - Posture assessment failure in RHEL 9.8 ARM fresh client (5.1.18.307 as well as 5.1.18.314)
- CSCwv02626—Ubuntu26: Secure Firewall Posture module installation fails due to libxml2 dependency error
- For Windows, DART does not collect CM arm logs.

Cisco Secure Client 5.1.17.3394 New Features

May 11, 2026

This release resolves the defect that is described in Cisco Secure Client 5.1.17.3394, on page 56.

Release 5.1.17.3394 contains the following versions for the various modules:

- Zero Trust Access—5.1.17.5545
- Secure Client UI—5.1.17.1876
- Cisco AnyConnect VPN core—5.1.17.3394
- DART—5.1.17.3394
- Umbrella— 5.1.17.3394
- SBL—5.1.17.3394
- Network Access Manager—5.1.17.3394
- Network Visibility Module—5.1.17.3394
- Secure Firewall Posture—5.1.17.3394
- Endpoint Data Loss Prevention (Windows only)—1.4.0.253

- ThousandEyes—2.35.0
- ISE Posture—5.1.17.3394
- Duo Desktop—7.15.0.0
- Endpoint Visibility Module—1.6.0.7

Known Issue: CSCwu30750—VPN external browser SAML auth may not use the defined default browser - uses Edge instead

Cisco Secure Client 5.1.17.3382 New Features

April 30, 2026

Customers who use SAML authentication for VPN with external browsers should not upgrade to 5.1.17.3382. Refer to CSCwu25955 (SAML authentication using external OS browser fails with "VPN internal server error") for additional information.

This release includes the following new updates, and resolves the defects that are described in Cisco Secure Client 5.1.17.3382, on page 57.

- Linux x64 (GUI only) support for Zero Trust Access—Linux endpoints can enroll in and use client-based ZTA through Secure Client, extending secure access and traffic steering workflows to Linux environments. This release brings core ZTA capabilities from Windows and macOS to Linux, including DNS-based steering for service discovery use cases. This support introduces DEB/RPM package installers, as well as DART updates (logs and crash dumps). Refer to the *Secure Client Administrator Guide* for getting Zero Trust up and running on Linux, certificate enrollment, and any limitations and troubleshooting. For additional details on managing Zero Trust and SSO enrollment and such, refer to Get Started with Cisco Secure Client on Windows, macOS, and Linux Devices.
- Support and deployment for Endpoint Data Loss Prevention (Windows predeploy only)—Enables you to protect sensitive data on endpoints by controlling what data is transferred to external devices. It extends your organization's data protection policies and ensures that sensitive data remains secure and compliant with your security requirements. For information on managing endpoint data loss prevention, enrolling devices, and troubleshooting, refer to Manage Endpoint Data Lose Prevention Using Cisco Secure Client.
- When FIPS mode is enabled, any RSA-based cipher suites that do not provide Perfect Forward Secrecy are removed from the supported cipher list. Additionally, ECDH and MODP groups, which provide Perfect Forward Secrecy, remain supported and are the preferred key exchange mechanisms under FIPS.
- Continuous Reassessment for ISE Posture—Provides near real-time monitoring of endpoint posture. It detects posture changes as they occur for event-based conditions and at 10-minute intervals for poll-based conditions. No network disruptions occur, and there is no waiting for the next scheduled reassessment cycle (using Periodic Reassessment). Continuous Reassessment is supported only with Cisco Secure Client Full Agent. Agentless and Temporal agents are not supported. Refer to Continuous Reassessment in the *Cisco Secure Client Administrator Guide* for additional details. For further continuous reassessment configuration, refer to the Cisco Identity Services Engine Administrator Guide.
- Documentation change for macOS client deployment (CSCwt95756)—The deployment of Secure Client changed for macOS, regardless of whether you are distributing with or without client management. The Secure Client Administrator Guide describes the changes. For more details, refer to Deploying Cisco Secure Client on macOS via MDM/EMM Using the Headend Deployment Package if you are distributing

without client management. If you are distributing with client management, refer to Deploying Cisco XDR Client Management on macOS via MDM/EMM: Resolving the Hidden .Resources Dependency.

- Release 5.1.17.3382 contains the following versions for the various modules:
  - Zero Trust Access—5.1.17.5300
  - Secure Client UI—5.1.17.1876
  - Cisco AnyConnect VPN core—5.1.17.3382
  - DART—5.1.17.3382
  - Umbrella— 5.1.17.3382
  - SBL—5.1.17.3382
  - Network Access Manager—5.1.17.3382
  - Network Visibility Module—5.1.17.3382
  - Secure Firewall Posture—5.1.17.3382
  - Endpoint Data Loss Prevention (Windows only)—1.4.0.253
  - ThousandEyes—2.35.0
  - ISE Posture—5.1.17.3382
  - Duo Desktop—7.15.0.0
  - Endpoint Visibility Module—1.6.0.7
- **Known Issues:**
  - CSCwu25955—SAML authentication using external OS browser fails with "VPN internal server error"
  - CSCwu16405—ZTNA Linux - intermittent broken pipes only when using Firefox running speedtests uploads to www.speedtest.net
  - CSCwu08657—MacOS SCEP certificate import issue with CiscoSSL8 default PKCS12 format

Cisco Secure Client 5.1.16.194 New Features

March 11, 2026

This release includes the following new updates, and resolves the defects that are described in Cisco Secure Client 5.1.16.194, on page 59.

- Always On support added to management tunnel (CSCwq35829)—For a consistent user experience, you must use identical TND settings in both user and management VPN tunnel profiles. Endpoint network access restrictions are in place when Always On is enabled in user and management VPN tunnel profiles during tunnel transitions. Administrators cannot configure Always On child preferences, as the management VPN tunnel is transparent to the end user.
- Release 5.1.16.194 contains the following versions for the various modules:

- Zero Trust Access—5.1.16.4434
- Secure Client UI—5.1.16.1663
- Cisco AnyConnect VPN core—5.1.16.194
- DART—5.1.16.194
- Umbrella— 5.1.16.194
- SBL—5.1.16.194
- Network Access Manager—5.1.16.194
- Network Visibility Module—5.1.16.194
- Secure Firewall Posture—5.1.16.194
- ThousandEyes—2.31.1
- ISE Posture—5.1.16.194
- Duo Desktop—7.15.0.0

Cisco Secure Client 5.1.15.287 New Features

February 19, 2026

This release includes the following new updates, and resolves the defects that are described in Cisco Secure Client 5.1.15.287, on page 59.

- Secure Client Linux installer migration—A script installer is no longer available for Linux. Linux installation/uninstallation uses RPM or DEB binary packages. If configuration is required, ACTransforms.xml is used. Refer to Predeploying to Linux in the *Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1* for details. Additionally, new deployment considerations exist if you are using Network Visibility Module Standalone. Refer to Standalone NVM and Extend Linux Kernel Capabilities for details.
- Discontinuation of shell-script-based installation for Secure Client ISE Posture and a switch to .deb and .rpm packages. Compliance Module release version 4.3.4510.0 supports RPM/DEB.
- Release 5.1.15.287 contains the following versions for the various modules:
  - Zero Trust Access—5.1.15.4322
  - Secure Client UI—5.1.15.1561
  - Cisco AnyConnect VPN core—5.1.15.287
  - DART—5.1.15.287
  - Umbrella— 5.1.15.287
  - SBL—5.1.15.287
  - Network Access Manager—5.1.15.287
  - Network Visibility Module—5.1.15.287

- Secure Firewall Posture—5.1.15.287
- ThousandEyes—2.23.0
- ISE Posture—5.1.15.287

- **Known Issues**:
  - CSCwt27105—Client sporadically fails to establish user tunnel automatically after web-deploy upgrade
  - CSCwt18374—RPM/DEB: Linux ISE Compliance Module upgrade/downgrade issues from rpm to script
  - CSCwt31244—Compliance Module downgrade is not happening on SUSE/RHEL RPM platforms

Cisco Secure Client 5.1.14.145 New Features

December 19, 2025

This release includes the following new updates, and resolves the defects that are described in Cisco Secure Client 5.1.14.145, on page 61.

- Any 5.1.8 users who upgraded to 5.1.13 prior to November 20, 2025 require no further action to resolve the trust bundle issue described in Cisco Secure Client 5.1.13.177 New Features, on page 10. Users who are running 5.1.9 to 5.1.12 should refer to the expiry dates listed in Cisco Secure Client 5.1.13.177 New Features, on page 10 to avoid upgrade issues.

  Release 5.1.14 contains a fix for CSCws30211, which prevents an upgrade to those Windows devices not upgraded prior to the expiration dates detailed in CSCws02283.

  Those Windows users affected by CSCws00283 whose devices are beyond the specified expiration dates must upgrade to 5.1.14.145 (or later). MacOS users affected by CSCws00283, and Windows users affected by CSCws00283 whose machines have not yet reached the specified expiration dates, can upgrade to 5.1.13.177 (or later).

- Linux build filenames have changed:

Previous Name	**New Name**
cisco-secure-client-linux64-*version*-predeploy-k9.tar.gz	cisco-secure-client-linux64-*version*-predeploy
cisco-secure-client-linux64-*version*-predeploy-deb-k9.tar.gz	cisco-secure-client-linux64-*version*-predeploy
cisco-secure-client-linux64-*version*-predeploy-rpm-k9.tgz	cisco-secure-client-linux64-*version*-predeploy
cisco-secure-client-linux64-*version*-vpnapi.tar.gz	cisco-secure-client-linux64-*version*-vpnapi.tgz
cisco-secure-client-linux-arm64-*version*-predeploy-k9.tar.gz	cisco-secure-client-linux-arm64-*version*-prede
cisco-secure-client-linux-arm64-*version*-predeploy-deb-k9.tar.gz	cisco-secure-client-linux-arm64-*version*-predep
cisco-secure-client-linux-arm64-*version*-predeploy-rpm-k9.tar.gz	cisco-secure-client-linux-arm64-*version*-predep
cisco-secure-client-linux-arm64-*version*-vpnapi.tar.gz	cisco-secure-client-linux-arm64-*version*-vpna

- Release 5.1.14.145 contains the following versions for the various modules:
  - Zero Trust Access—5.1.14.3417
  - Secure Client UI—5.1.14.1452
  - Cisco AnyConnect VPN core—5.1.14.145
  - DART—5.1.14.145
  - Umbrella— 5.1.14.145
  - SBL—5.1.14.145
  - Network Access Manager—5.1.14.145
  - Network Visibility Module—5.1.14.145
  - Secure Firewall Posture—5.1.14.145
  - ThousandEyes—2.20.1
  - ISE Posture—5.1.14.145

Cisco Secure Client 5.1.13.177 New Features

This release includes the following new features and support updates, and resolves the defects that are described in Cisco Secure Client 5.1.13.177, on page 63.

- This release resolves 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:

  - 5.1.8: Must be upgraded to 5.1.13 or above before November 20, 2025.
  - 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 January 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 June 4 2026

- Updates to macOS UI:
  - Added a copy and paste functionality for data in the Statistics table with a *Select All* and *Copy* keyboard shortcut.
  - Added custom hover-over tooltips to the Statistics table to enable full viewing of the detailed content.
  - Ability to expand and collapse items within the Statistics page.

- XDR Forensic Diagnostics are now collected in DART for macOS and Windows.
- In Zero Trust Access, added the ability to detect and manage events triggered by user interactions and give the option to pause proxy configs on both Windows and macOS. Refer to Zero Trust Access Module for additional information.
- Zero Trust Access Module 5.1.13 includes Duo Desktop version 7.13.0. Duo Desktop is distributed and deployed with the Zero Trust Access Module for posture purposes.
- Linux ARM64 has FIPS 140-2 and 140-3 support (CSCwq60310).
- The Start Before Login preference in the profile editor was removed and can no longer be controlled by the administrator. If you have existing profiles that use this preference, they will still be treated as valid profiles. Those users who enabled the Start Before Login preference in a profile prior to 5.1.13 are impacted.
- If you choose to email a DART bundle, you are now required to enter **attach@cisco.com** to automatically attach the DART bundle to the case.
- Support for Healthcare Identity Integration with Imprivata badge system on Secure Web Gateway (SWG). This interaction with the Imprivata application sends the API and instantly returns the current user identity (username and department) to the headend. The feature requires Secure Client 5.1.13 and Imprivata version 25.2.
- Release 5.1.13.177 contains the following versions for the various modules:
  - Zero Trust Access—5.1.13.3159
  - Secure Client UI—5.1.13.1379
  - Cisco AnyConnect VPN core—5.1.13.177
  - DART—5.1.13.177
  - Umbrella—5.1.13.177
  - SBL—5.1.13.177
  - Network Access Manager—5.1.13.177
  - Network Visibility Module—5.1.13.177
  - Secure Firewall Posture—5.1.13.177
  - ThousandEyes—2.23.0
  - ISE Posture—5.1.13.177

Known Issue

CSCwr64930—ZTA TND probes may fail to reach trusted server with only AAAA FQDN in dual stack networks

Cisco Secure Client 5.1.12.146 New Features

This release includes the following new feature, and resolves the defects that are described in Cisco Secure Client 5.1.12.146, on page 65.

- Improvements to captive portal detection capabilities (CSCwj43435).
- Support for macOS 26 (Tahoe)
- Release 5.1.12.146 contains the following versions for the various modules:
  - Zero Trust Access—5.1.12.2345
  - Secure Client UI—5.1.12.1179
  - Cisco AnyConnect VPN core—5.1.12.146
  - DART—5.1.12.146
  - Umbrella—5.1.12.146
  - SBL—5.1.12.146
  - Network Access Manager—5.1.12.146
  - Network Visibility Module—5.1.12.146
  - Secure Firewall Posture—5.1.12.146
  - ThousandEyes—2.9.0
  - ISE Posture—5.1.12.146

Cisco Secure Client 5.1.11.388 New Features

This release includes the following new features and support updates, and resolves the defects that are described in Cisco Secure Client 5.1.11.388, on page 65.

- Addition of Zero Trust Access for All Internet Destinations—This capability enables organizations to secure all internet-bound TCP and UDP traffic with unified Secure Internet Access (SIA) enforcement using the same ZTA client/agent that supports both private and internet access. Within Cisco Secure Access, you can elect this Trusted Network Detection with *Use ZTA to secure all internet destinations*. For details on enabling ZTA for all internet destinations, refer to https://securitydocs.cisco.com/docs/csa/olh/118721.dita.
- Support for Linux ARM64. Refer to Cisco Secure Client Supported Operating Systems, on page 33 for specific details. Linux ARM64 has no FIPS 140-2 or 140-3 support (CSCwq60310). On Ubuntu ARM64 only, you cannot use NSS certificate store when doing certificate authentication (CSCwq74514).
- Extension of Linux Kernel capabilities within Network Visibility Module using the implementation of Berkeley Packet Filter (eBFP). Refer to Extend Linux Kernel Capabilities for additional details.
- Support for managing threat defense devices for Universal Zero Trust Network Access. You can configure threat defense devices as on-premises proxies and then manage the connection which allows user traffic to reach private resources in your network without compromising on security. Refer to Manage Threat Defense Devices for Universal Zero Trust Network Access in the Cisco Secure Access documentation.
- Support for RHEL 10.x. Refer to Cisco Secure Client Supported Operating Systems, on page 33.
- Added the platform option to import webvpn AnyConnect customization on Cisco Secure Firewall Adaptive Security Appliance (through CLI) or ASDM for ARM64 Windows and Linux (CSCwo80984 and CSCwq13403).

- Release 5.1.11.388 contains the following versions for the various modules:
  - Zero Trust Access—5.1.11.2143
  - Secure Client UI—5.1.11.927
  - Cisco AnyConnect VPN core—5.1.11.388
  - DART—5.1.11.388
  - Umbrella—5.1.11.388
  - SBL—5.1.11.388
  - Network Access Manager—5.1.11.388
  - Network Visibility Module—5.1.11.388
  - Secure Firewall Posture—5.1.11.388
  - ThousandEyes—2.9.0
  - ISE Posture—5.1.11.388

Cisco Secure Client 5.1.10.233 New Features

This release includes the following new features and support updates, and resolves the defects that are described in Cisco Secure Client 5.1.10.233, on page 67.

- TND used in Zero Trust Access Module—Trusted Network Detection (TND) gives you the ability to have the Secure Client automatically pause a Zero Trust Access configuration when the user is inside the corporate network and activate the Zero Trust Access configuration when the user is outside the corporate network.
- Split exclude failover (CSCwo32975)—Adds support for routing split exlude traffic via the VPN tunnel when a lack of network connectivity prevents its routing outside the tunnel. Refer to Split Exclude Failover.
- Tamper Protection for Network Visibility Module (CSCwo75993)—Protecting users from the stopping/blocking/uninstalling of XDR binaries or applications is now supported on Windows ARM64.
- Provided steps to set up and deploy the Network Visibility Module for cloud (XDR) use and run it as a standalone application without Secure Client VPN.
- AMP Enabler functionality has been removed from macOS (CSCwo08874).
- Ability to use Linux Secure Client inside a docker container.
- FIPS is enabled for Secure Firewall Posture using a FIPS-mode parameter in the local policy file on the user computer just as AnyConnect VPN (CSCwo59154).
- Ability to configure Windows Filtering Platform (WFP) Sublayer Weight (CSCwo25750)—For better compatibility and prioritization when operating with other WFP callout drivers (such as Microsoft GSA), adjust the Secure Client Socket interceptor driver's WFP sublayer weight. This enhancement ensures optimal handling of inline TCP flow redirection scenarios. To set the sublayer weight multiplier, run ***%ProgramFiles\(x86\)%\Cisco\Cisco Secure Client\acsocktool.exe" -slwm <sub-layer_weight_multiplier>*** via a privileged prompt, followed by reboot.

The multiplier (accepted values 1 to 10) determines the sublayer weight proportionally to the maximum allowed weight (universal sublayer weight minus 1).

- Ubuntu 20.04 and SUSE 12 have been removed from the list of supported operating systems.
- This version of Secure Client requires ThousandEyes Endpoint Agent version 6.3 or newer for Zero Trust Access to work as expected in Secure Access. Upgrade your ThousandEyes Endpoint Agent if you are running a version prior to 6.3.
- You can configure CIDR rules for IP-based flows and FQDN rules for name-based flows.
- Release 5.1.10.233 contains the following versions for the various modules:
  - Zero Trust Access—5.1.10.1720
  - Secure Client UI—5.1.10.813
  - Cisco AnyConnect VPN core—5.1.10.233
  - DART—5.1.10.233
  - Umbrella—5.1.10.233
  - SBL—5.1.10.233
  - Network Access Manager—5.1.10.233
  - Network Visibility Module—5.1.10.233
  - Secure Firewall Posture—5.1.10.233
  - ThousandEyes—1.240.2
  - ISE Posture—5.1.10.233

Cisco Secure Client 5.1.9.113 New Features

This release includes the following new features and resolves the defects that are described in Cisco Secure Client 5.1.9.113, on page 70.

- Enrollment with User Certificates—Without user action or awareness, you can enroll Windows and macOS devices in Zero Trust Access. Refer to Use Certificate Enrollment Without User Action in the administrator guide for additional information.
- Network Access Manager support for WPA3 SAE Transition (CSCwn15672)—Network Access Manager supports transition mode so that the client can connect to wireless networks that support both WPA2 and WPA3. Client devices can change the network profile from WPA2 PSK to WPA3 SAE, and from WPA2 Enterprise to WPA3 Enterprise, if a transition disable indication is received from an access point when connecting the network. Authentication policies must allow WPA3: if the policy does not allow Network Access Manager to change the configuration from WPA2 to WPA3, a popup is displayed upon receiving a transition disable indication.
- Network Visibility Module support for EVE integration—Allows Network Visibility Module to report EVE records.
- Network Visibility Module support for Linux browser plugins (CSCwn78412).

- Windows Server 2022 is supported for Network Visibility Module on-prem and XDR.
- By default, HTTP headers are excluded from the Network Visibility Module Data Collection Policy (CSCwn75887).
- In Umbrella Secure Web Gateway, added IPv4 link-local mapped IPv6 addresses to default exception list (CSCwe39164).
- The ISE Posture UI tile has been improved by removing the loader experience and replacing it with enhanced messages (CSCwn75759).
- Release 5.1.9.113 contains the following versions for the various modules:
  - Zero Trust Access—5.1.9.1200
  - Secure Client UI—5.1.9.460
  - AnyConnect VPN core—5.1.9.113
  - DART—5.1.9.113
  - Umbrella—5.1.9.113
  - SBL—5.1.9.113
  - Network Access Manager—5.1.9.113
  - Network Visibility Module—5.1.9.113
  - Secure Firewall Posture—5.1.9.113
  - ThousandEyes—1.229.2
  - ISE Posture—5.1.9.113

Cisco Secure Client 5.1.8.122 New Features

This release resolves the defects that are described in Cisco Secure Client 5.1.8.122, on page 73.

Those customers using Zero Trust Access or Umbrella should not download Secure Client release 5.1.8.105. Release 5.1.8.122 replaces it and corrects both a Zero Trust Access certificate renewal issue that caused a loss of connectivity (CSCwo32464), and a compatibility issue with Umbrella encryption. A cm-client 1.0.4.447 release fixes the issue related to certificate store usage on Windows.

Release 5.1.8.122 contains the following versions for the various modules:

- Zero Trust Access—5.1.8.741
- Secure Client UI—5.1.8.172
- AnyConnect VPN core—5.1.8.122
- DART—5.1.8.122
- Umbrella—5.1.8.122
- SBL—5.1.8.122
- Network Access Manager—5.1.8.122

- Network Visibility Module—5.1.8.122
- Secure Firewall Posture—5.1.8.122
- ThousandEyes—1.226.2
- ISE Posture—5.1.8.122

Cisco Secure Client 5.1.8.105 New Features

This release includes the following features and support updates, and resolves the defects that are described in Cisco Secure Client 5.1.8.105, on page 73:



Note We have identified issues with Secure Client Release 5.1.8.105 for those using Umbrella or Zero Trust Access. Secure Client Release 5.1.8.122 replaces it and corrects both a Zero Trust Access certificate renewal issue that caused a loss of connectivity, and a compatibility issue with Umbrella encryption and certificate store usage on Windows. If you are running version 5.1.8.105, you should upgrade to version 5.1.8.122 to avoid these issues. Refer to Cisco Secure Client 5.1.8.122 New Features, on page 15 and CSCwo32464.

- Always On is supported in Linux, and access to a specified list of hosts with IP addresses is allowed when VPN is disconnected. Refer to About Always-On VPN and Cisco Secure Client Profile Editor, Preferences (Part 2) for additional information.
- Addition of IKEv2 PSK and post quantum pre-shared key (PPK) authentication to connect with a Secure Firewall ASA using RFC 8784. Refer to CSCwi69392 or VPN Authentication Using Post-quantum Pre-Shared Keys for additional information.
- Due to a new macOS requirement, the ZTA module requires user approval before it can function. Refer to *Before You Begin* of the Getting Zero Trust Up and Running section and the Deployment on macOS 13 (or Later) Requires Admin Privileges, on page 40 section for additional information.
- ThousandEyes Endpoint Agent Profile Deployment Via Downloader (Windows only)—You can deploy the ThousandEyes json profile (C:\ProgramData\Cisco\Cisco Secure Client\ThousandEyes Endpoint Agent\ThousandEyes Endpoint Agent Configuration.json) with Downloader from VPN or ISE headends.
- Umbrella Module Updates—
  - In the Advanced window or the Umbrella Module tile of Secure Client, you can verify the state of the Secure Web Gateway. Secure Web Gateway added a telemetry report mapped to an integer rather than a string value with two new *Disabled* statuses: a) the VPN connection will show as disabled if the endpoint is connected to a full-tunnel VPN, and b) the trusted network will show as disabled if the endpoint is connected to Secure Client or a customer-trusted network.
  - Introduced the ability to traverse regional boundaries that are governed under differing regulations. Initial support for China region. (Windows, macOS)
  - Addressed an issue where DNS protection is impacted due to a conflict with other agents attempting to listen on port 53. (Windows, macOS)
  - Secure Client now reports Secure Web Gateway protection status to the dashboard. (Windows, macOS)

- In macOS, we support administrator control over dynamic split tunneling of CNAME DNS responses. Refer to About Dynamic Split Tunneling for additional information.
- In Linux Docker deployments, you can now activate logging. Refer to Activating Logging for Docker Deployments for additional information.
- Clear embedded browser cache (Windows and macOS)—Provides users with the ability to clear the embedded browser cache if issues are encountered. Refer to Clear Embedded Cache (Windows and macOS for additional details.
- Endpoint Tag in Network Visibility Module (CSCwn22005)—Identifies an endpoint with a custom tag as part of a sub group or profile. This tag helps identify endpoints across overlapping subnet spaces or when inconsistencies within the logged-in user account exist. You can create and then search for virtual sub-groups of endpoints within the organization. Refer to the Network Visibility Module Profile Editor for additional information.
- We are committed to enhancing accessibility and to providing a seamless experience for all users, by adhering to specific Voluntary Product Accessibility Template (VPAT) compliance standards. Refer to the Cisco Secure Client Features, Licenses, and OSs Guide, Release 5.1 for details.
- Release 5.1.8.105 contains the following versions for the various modules:
  - Zero Trust Access—5.1.8.363
  - Secure Client UI—5.1.8.172
  - AnyConnect VPN core—5.1.8.105
  - DART—5.1.8.105
  - Umbrella—5.1.8.105
  - SBL—5.1.8.105
  - Network Access Manager—5.1.8.105
  - Network Visibility Module—5.1.8.105
  - Secure Firewall Posture—5.1.8.105
  - ThousandEyes—1.226.2
  - ISE Posture—5.1.8.105

Known Issues:

(CSCwn39981)—Linux: Uninstalling VPN RPM package on RHEL or SUSE causes system to hang/freeze

(CSCwn72336)—ZTA Flow counts not updating when QUIC is enabled

(CSCwn92376)—ZTA stepup auth not prompting when QUIC is enabled

(CSCwn92381)—ZTA proxy alerts not being shown in UI when QUIC is enabled

Cisco Secure Client 5.1.7.80 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.7.80, on page 75:

- Addition of ThousandEyes 1.219.1—Contains support for integrating ThousandEyes with Secure Client Zero Trust Access and also the ability to read the new ThousandEyes.json profile, which improves the registration workflow for new installations.
- Tamper Protection for Network Visibility Module (CSCwk30374)—(Windows only) Protects user from stopping/blocking/uninstalling XDR binaries or applications. Refer to XDR Documentation for additional information.
- Some Secure Client Modules will not work on Windows 11 24H2 unless location permission is set (CSCwm80714). Details are found in Some Secure Client Modules Not Working on Windows 11 24H2 Unless Location Permission is Set, on page 40.
- When utilizing out-of-band deployment methods, whether manually or through SCCM, you should initiate pre-deploy installers for software upgrades. It is important to note that you should not remove any Cisco Secure Client (AnyConnect) registry entries within SCCM or other deployment scripts during the upgrade process. For upgrade-related issues, consult with Cisco.
- The Zero Trust Access Module is supported on Windows ARM64 (CSCwm67479).
- Support to override system proxy settings in macOS embedded browsers was added (CSCwj04530).
- Network Visibility Module Process Tree Hierarchy (CSCwm44074)—Until release 5.1.6, the flows reported by Network Visibility Module only included information about the process and its parent process, and not the further process lineage. Now you can choose to report the hierarchy by clicking the Process Tree Hierarchy checkbox in the Network Visibility Module profile editor. A separate record (Process Record) is sent for each process in the process hierarchy. The process records have a unique identifier (PUID) that you can use to link between process records and flow records. Refer to the Network Visibility Module Profile Editor for additional information.
- Release 5.1.7.80 contains the following versions for the various modules:
  - Zero Trust Access—5.1.7.7561
  - Secure Client UI—5.1.7.1336
  - AnyConnect VPN core—5.1.7.80
  - DART—5.1.7.80
  - Umbrella—5.1.7.80
  - SBL—5.1.7.80
  - Network Access Manager—5.1.7.80
  - Network Visibility Module—5.1.7.80
  - Secure Firewall Posture—5.1.7.80
  - ThousandEyes—1.219.1
  - ISE Posture—5.1.7.80
  - DUO—7.1.0.0

Known Issues:

(CSCwn39981)—Uninstalling VPN RPM packages in RHEL or SUS causes a black screen because the current user GUI/CLI login session gets terminated. Refer to the release note enclosure in the bug ID for a workaround.

(CSCwn72336)—ZTA Flow counts not updating when QUIC is enabled

(CSCwn92376)—ZTA stepup auth not prompting when QUIC is enabled

(CSCwn92381)—ZTA proxy alerts not being shown in UI when QUIC is enabled

Cisco Secure Client 5.1.6.103 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.6.103, on page 77:

- Support for macOS 15 (Sequoia). Subsequently, we will drop support for macOS 12 (Monterey). The following known issues exist for running Secure Client on macOS 15:
  - Network Visibility Module: CSCwm50168—Remote username is not reported in logged in user field
  - Network Visibility Module: CSCwm50228—macOS 15 Different Process Name and Parent Process Name are reported for NVM + SWG
  - OPSWAT-ISE: CSCwm12254—macOS 15 Beta: Gatekeeper built-in Firewall 15.x enable remediation functionality not working
- CSCwm31250—The Windows GUI has a new General tab in the Advanced Window for non-module-specific configurations. Because of the additional General tab and its settings, the Advanced window will always be fully extended. This General tab includes a Settings tab and a Web Browser tab. The Settings tab duplicates our current system menu option to toggle user notifications. Click **Show Notifications** to enable the UI capability. Within the new Web Browser tab, you can click **Clear Data** to clear the client's WebView2 browser cache.
- CSCwj04530—We added an enhancement to the macOS Secure Client Web Browser application to disable the use of System Proxy settings when accessing the Captive Portal through the client's embedded browser. This enhancement prevents potential issues with system proxy settings during the Captive Portal authentication process, for those clients running on macOS 14 (and later). Other client embedded browser authentication flows such as SAML are not impacted, as they will continue to use the system proxy settings.
- We have provided a different way to match certificates in the Profile Editor Certificate Match panel and include additional filtering of the Template Name and Template Information certificate fields. To minimize the number of certificates sent to the Secure Firewall ASA, you can provide a certificate Template Identifier. Refer to Cisco Secure Client Profile Editor, Certificate Matching for additional information.
- mDTLS for Network Visibility Module—Allows you to send data securely to the Network Visibility Module Collector. With mDTLS, the Collector can also verify the Network Visibility Module Client's identity before the connection is established and data is received. Refer to Network Visibility Module Profile Editor for additional information. The new feature has the following known issues:
  - CSCwm48552—NVM: Observed exporter is disabled and flows are not getting collected in mTLS setup
  - CSCwm53109—mTLS/DTLS is not working when using CA signed intermediate certificates for collector
  - CSCwm60665—mTLS connection fails when there is no matching criteria configured

- Release 5.1.6.103 contains the following versions for the various modules:
  - Zero Trust Access—5.1.6.6896
  - Secure Client UI—5.1.6.1307
  - AnyConnect VPN core—5.1.6.103
  - DART—5.1.6.103
  - Umbrella—5.1.6.103
  - SBL—5.1.6.103
  - Network Access Manager—5.1.6.103
  - Network Visibility Module—5.1.6.103
  - Secure Firewall Posture—5.1.6.103
  - ThousandEyes—1.206.0
  - ISE Posture—5.1.6.103

Cisco Secure Client 5.1.5.65 New Features

This release includes the following features, and resolves the defects described in Cisco Secure Client 5.1.5.65, on page 79:

- Option to send DART bundle directly to TAC. Refer to Run DART to Gather Data for Troubleshooting for additional information.
- Option to suppress connection retries after a connection failure or disconnection of a VPN session. The default is disabled; but when enabled, the client will stop periodic connection retries. Refer to Cisco Secure Client Profile Editor, Preferences (Part 2) for additional information.
- Additional posture settings for EDR updates (CSCwj05606)—New ASDM UI setting in Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Settings. When **For EDR update, Skip Internet Check before VPN is active** is enabled, the Endpoint Detection and Response (EDR) security software retrieves information from its respective server and performs posture assessment, without verifying if the security software is up-to-date. Refer to Cisco Secure Firewall ASA Series VPN ASDM Configuration Guide for additional information.
- Release 5.1.5.65 contains the following versions for the various modules:
  - Zero Trust Access—5.1.5.6663
  - Secure Client UI—5.1.5.1171
  - AnyConnect VPN core—5.1.5.65
  - DART—5.1.5.65
  - Umbrella—5.1.5.65
  - SBL—5.1.5.65
  - Network Access Manager—5.1.5.65

- Network Visibility Module—5.1.5.65
- Secure Firewall Posture—5.1.5.65
- ThousandEyes—1.200.1
- ISE Posture—5.1.5.65

Known Issues:

- CSCwi49003—Network Visibility Module is not reporting the Safari Browser Plugins for macOS
- CSCwj80335—On macOS, SWG backoff for noNetwork doesn't change the state when IPv4 alone is enabled
- CSCwm00171—On Mac M-series chip machine, TE is failing to install with CSC_5.1.5.58 build

Cisco Secure Client 5.1.4.74 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.4.74, on page 82:

- **Dual-Home Detection for Windows**—Disables untrusted interfaces so that a multi-homed endpoint doesn't switch from a corporate network to a public network, leaking private corporate information. It requires enabling Secure Trusted Network Detection in the profile, which sends an HTTPS probe to the configured trusted servers as an additional check once trusted network is detected by the static DNS setting. Refer to Cisco Secure Client Profile Editor, Preferences (Part 2) for more details on the *Disable interfaces without trusted server connectivity while in trusted network* checkbox.
- **Support for WPA3 Enterprise GCMP256**—However, WPA3 Enterprise GCMP256 networks require an Integrity Group Temporal Key (IGTK) for Protected Management Frames (PMF), and Network Access Manager is unable to set this using the OS Independent Hardware Vendor interface, as part of the WLAN component.

  You can disable the Network Access Manager setting of the PMF IGTK until a Windows fix becomes available. A Windows fix is available to set IGTK keys. Some older network drivers do not provide support for IGTK GMAC256.

  The IGTK fix is available in the following Windows releases:

  - Windows 10 22H2 KB5036979 OS Build 19045.4355
  - Windows 11 22H2 KB5036980 OS Build 22621.3527
  - Windows 11 23H2 KB5036980 OS Build 22631.3527
  - Windows 11 21H2 KB5037770 OS Build 22000.2960

  WPA3 Enterprise AES networks require setting the IGTK using CMAC128 keys. WPA3 Enterprise GCMP256 networks typically require setting the IGTK using GMAC256 keys.

  The setting of the PMF IGTK can be disabled to allow a connection to a network configured to provide Protection of Management Frames (PMF). If the Windows fix is not yet available, and you can't avoid connecting to a network with PMF enabled, you need to modify the Windows registry editor by adding the following registry key as a DWORD and setting it as described to disable the use of IGTK by the Network Access Manager:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client Network Access Manager\DisableIGTK
 set to 1
```

Note This IGTK fix only applies to WPA2/WPA3 Enterprise networks. It does not apply to WPA3 Personal (SAE) or WPA3 Open (OWE). We strongly discourage against disabling the PMF IGTK unless necessary as it provides protection of wireless management frames. Also, Network Access Manager currently supports only the following ciphers for the PMF IGTK:

CMAC128—which requires the OS fix

GMAC256—which requires the OS fix

- Cisco Secure Client Cloud Management 1.0.3.433 now supports deployment for macOS. To get started, install the XDR Default Deployment for macOS on your macOS devices or create new macOS deployments by clicking **Create New** on the Deployments page. Client Management documentation is available here.
- ZTA supports interoperability with Network Visibility Module.
- This Secure Client release coincides with Network Visibility Module Collector release 5.1.4.67.
- Release 5.1.4.74 contains the following versions for the various modules:
  - Zero Trust Access—5.1.4.6433
  - Secure Client UI—5.1.4.1158
  - AnyConnect VPN core—5.1.4.74
  - DART—5.1.4.74
  - Umbrella—5.1.4.74
  - SBL—5.1.4.74
  - Network Access Manager—5.1.4.74
  - Network Visibility Module—5.1.4.74
  - Secure Firewall Posture—5.1.4.74
  - ThousandEyes—1.195.0
  - ISE Posture—5.1.4.74

Known Issue:CSCwk42371—ZTA/Mac: non-US time format not shown correctly in Config Sync and Statistics UI

Cisco Secure Client 5.1.3.62 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.3.62, on page 85.

- macOS 11 is no longer supported.

- This 5.1.3.62 release will not support Ubuntu 24.04 LTS.
- Umbrella added support for FedRAMP in Secure Web Gateway (SWG) and Domain Name System (DNS) clients.
- Bypass Default Localization —a new preference in AnyConnect Local Policy file allows you to disable the default localization files embedded within the client.
- The Microsoft issue that was preventing the connections to networks with PMF enabled has been corrected and verified. As a result of the Windows update, the implementation to disable the setting of PMF IGTK within Network Access Manager or to modify the Windows registry is no longer necessary in the fixed versions of Windows, listed below. The Microsoft IGTK fix for WPA2/WPA3 Enterprise networks has been addressed for Windows 10 22H2 KB5036979, Windows 11 22H2 KB5036980, and Windows 11 23H2 KB5036980. Microsoft estimates that the fix for Windows 11 21H2 will be available in May 2024.
- Additional client details are now visible in the Zero Trust Access Module UI
- Release 5.1.3.62 contains the following versions for the various modules:
  - Zero Trust Access—5.1.3.6177
  - Secure Client UI—5.1.3.1110
  - AnyConnect VPN core—5.1.3.62
  - DART—5.1.3.62
  - Umbrella—5.1.3.62
  - SBL—5.1.3.62
  - Network Access Manager—5.1.3.62
  - Network Visibility Module—5.1.3.62
  - Secure Firewall Posture—5.1.3.62
  - ThousandEyes—1.189.1
  - ISE Posture—5.1.3.62
- **Known Issues:**
  - CSCwj92612—Service Unavailable: ISE Posture predeploy and NSA web deploy are broken on Windows 10 and 11 for non-English OSs when upgrading to Secure Client 5.1.3.62. To use ISE Posture without interruption, do not upgrade to Secure Client 5.1.3.62 until a fix is announced.
  - CSCwi98914—USB cases are working as expected still system scan is giving non-compliant on Windows 10
  - CSCwj81971—Network Visibility Module installation fails on Ubuntu 22.04.4

Cisco Secure Client 5.1.2.42 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.2.42, on page 87.

- (CSCwh29292) Dynamic split tunneling can now perform both dynamic exclusion from a tunnel and dynamic inclusion into a tunnel for a given configuration, as needed. For example, with enhanced dynamic split exclude tunneling, traffic matching a dynamic include domain may be dynamically included into a tunnel, if necessary to override a static split exclude network. Refer to About Dynamic Split Tunneling in the *Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5* for additional details.
- In the profile editor, wildcards can now be added at the beginning or end of the Host Address in Load Balancing Server List.
- We have implemented a Network Access Manager addition to disable the setting of PMF IGTK until a Windows fix becomes available. Microsoft estimates that fixes for Windows 10 22H2 and Windows 11 21H2 (and later) should be available in the first half of calendar year 2024, which will allow you to set the IGTK from the Network Access Manager. Until then, you can disable the setting of PMF IGTK and allow a connection to a network configured to provide Protection of Management Frames (PMF). If the Windows fix is not yet available, and you can't avoid connecting to a network with PMF enabled, you need to modify the Windows registry editor by adding the following registry key as a DWORD and setting it as described to disable the use of IGTK by the Network Access Manager:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client Network Access Manager\DisableIGTK
   set to 1
  ```

Note This IGTK fix only applies to WPA2/WPA3 Enterprise networks. It does not apply to WPA3 Personal (SAE) or WPA3 Open (OWE). We strongly discourage against disabling the PMF IGTK unless necessary as it provides protection of wireless management frames.

- You must have the appropriate AnyConnect VPN version (5.1.2.42) to interoperate with the Zero Trust Access Module (5.1.2.5191).
- Windows 10 ARM64 is no longer supported.

Cisco Secure Client 5.1.1.42 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.1.42, on page 88.

- Fatal error with webdeploy upgrade (CSCwi37384)—ASA or ISE webdeploy only on Windows 11 ARM64 results in a fatal error when upgrading from Cisco Secure Client 5.1.0.x to 5.1.1.x. You will need to uninstall Secure Client 5.1.0.x for a fresh install of 5.1.1.x as a workaround in order for webdeploy to work on Windows 11 ARM64 devices. Alternatively, you can upgrade from Windows 11 ARM64 devices from Secure Client 5.1.0.x to 5.1.1.x using predeploy.
- You must have the appropriate AnyConnect VPN version (5.1.1.42) to interoperate with the Zero Trust Access Module (5.1.1.4867).
- Web Deploy Upgrade on macOS Requires Admin Privileges (CSCwi69393)—Due to a new Apple API change, when using webdeploy to upgrade from Cisco Secure Client 5.0.x (or earlier) to 5.1.x (or later), you must have administrator privileges or manage the macOS devices via MDM to pre-approve the application extension.
- Updates to Network Visibility Module—

- Added HTTP Host as an additional Collection Parameter for HTTP 1.1 flows from Windows clients running Network Visibility Module.
- Extended the Collection Parameter Module Name List to include browser plugin information (name and version) for Chrome, Firefox, and MS Edge browser flows from Windows and macOS clients.
- **Known Issue:**CSCwi48979—The HTTP Host field for macOS is reported as empty instead of providing the proper destination host name for HTTP traffic.
- **Known Issue:**CSCwi49003—Network Visibility Module is not reporting the Safari Browser plugins for macOS.

- **Known Issue:**CSCwi49850—macOS 12: Hyperlinks not working in AnyConnect Embedded Browser during captive portal remediation

Cisco Secure Client 5.1.0.136 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.0.136, on page 89.

- Zero Trust Access Module—Reduces the attack surface by hiding applications, and expands your level of knowing, understanding, and controlling who and what is on your network. You must have the appropriate AnyConnect VPN version (5.1.0.136) to interoperate with the Zero Trust Access Module (5.1.0.4464). The Zero Trust Access module currently only supports the Cisco Secure Access service. Refer to Secure Access documentation for additional details.

  Duo Desktop will be packaged and installed automatically in the Zero Trust Access module installer (for Windows and macOS), even though it is a standalone application that is separate from Cisco Secure Client. However, on macOS, Duo Desktop requires additional setup requirements for certificate deployment. Refer to Getting Zero Trust Access Up and Running on Desktop for additional details.

Note Duo Health Application (DHA) has been rebranded to Duo Desktop.

DART was enhanced to collect Duo Desktop logs. On Windows, DART can only collect Duo Desktop logs if the Duo troubleshooting script is allowed to execute. Duo uses a PowerShell script to collect logs.

Current Limitations or Restrictions

- Cloud Management won't support the distribution of Zero Trust Access for Windows or macOS.
- The Zero Trust Access Module is not part of the webdeploy package for macOS.
- Zero Trust Access functionality is disabled when multiple users are logged in concurrently to an endpoint.
- No support for tunneling applications where server sends traffic first (ex:: MySQL).
- DART will not collect Duo Desktop logs on macOS for 5.1.
- With a macOS webdeploy, DART does not upgrade. You receive an error and can manually install for the DART collection.

- ASDM does not show Zero Trust Access as a module in the group-policy (Configuration > Remote Access VPN > Network (Client) Access > Secure Client Connection Profiles Edit Group-Policy, Advanced-Secure Client-Optional Modules to Download) drop-down menu. A defect has been assigned to the ASDM team to address.
- Zero Trust Access webdeploy is not supported on macOS.

Refer to the Zero Trust Access Module section in the *Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1* for additional information, limitations, and prerequisites.

- Network Access Manager added support for WPA3 802.11 CCMP128 encryption and Protected Management Frames (PMF). However, WPA3 will not work until Microsoft releases a fix that relates to Integrity Group Temporal Key generation. The fix is not available in a production environment, but we anticipate the fix in an upcoming Windows 11 release and Windows 10 22H2 update. While PMF can be used in WPA2, it is required for WPA3 Enterprise. If you have a WPA2 network with PMF required or optional, your connection to Secure Client 5.1.0.136 will fail until the Microsoft fix.

Secure Firewall Posture (Formerly HostScan) 5.1.20.333 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.20.333 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.20.333, on page 90.

Secure Firewall Posture (Formerly HostScan) 5.1.19.1862 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.19.1859 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.19.1862, on page 91.

Secure Firewall Posture (Formerly HostScan) 5.1.18.314 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.18.314 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.18.314, on page 91.

Secure Firewall Posture (Formerly HostScan) 5.1.17.3382 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.17.3382 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.17.3382, on page 92.

Secure Firewall Posture (Formerly HostScan) 5.1.16.194 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.16.194 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

Secure Firewall Posture (Formerly HostScan) 5.1.15.287 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.15.287 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.15.287, on page 92.

Secure Firewall Posture (Formerly HostScan) 5.1.14.145 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.14.145 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.14.145, on page 93.

Secure Firewall Posture (Formerly HostScan) 5.1.13.177 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.13.177 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

Secure Firewall Posture (Formerly HostScan) 5.1.12.146 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.12.146 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

Secure Firewall Posture (Formerly HostScan) 5.1.11.388 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.11.388 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.11.388, on page 93.

Secure Firewall Posture (Formerly HostScan) 5.1.10.295 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.10.295 release resolves the defect described in Secure Firewall Posture (Formerly HostScan) 5.1.10.295, on page 94.

Secure Firewall Posture (Formerly HostScan) 5.1.10.233 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.10.233 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.10.233, on page 94.

Secure Firewall Posture (Formerly HostScan) 5.1.9.113 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.9.113 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.9.113, on page 95.

Secure Firewall Posture (Formerly HostScan) 5.1.8.105 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.8.105 release includes the following new feature and resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.8.105, on page 95.

Secure Firewall Posture supports pure IPv6 devices and networks.

Secure Firewall Posture (Formerly HostScan) 5.1.7.80 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.7.80 release resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.7.80, on page 96.

Secure Firewall Posture (Formerly HostScan) 5.1.6.108 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.6.108 release includes the following known issue and resolves the defect described in Secure Firewall Posture (Formerly HostScan) 5.1.6.108, on page 96:

Known Issue

- CSCwm83734— macOS15: Firewall remediation is failing with Secure Firewall Posture upgrade from 5.1.5.65 to 5.1.6.108 on first attempt

Secure Firewall Posture (Formerly HostScan) 5.1.6.103 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.6.103 release includes the following known issue and resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.6.103, on page 97:

Known Issue

- CSCwm61544—Secure Firewall Posture detects macOS Firewall as enabled while it is disabled

Secure Firewall Posture (Formerly HostScan) 5.1.5.65 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.5.65 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.5.65, on page 97.

Secure Firewall Posture (Formerly HostScan) 5.1.4.74 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.4.74 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.4.74, on page 98.

Secure Firewall Posture (Formerly HostScan) 5.1.3.62 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.3.62 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects described in Secure Firewall Posture (Formerly HostScan) 5.1.3.62, on page 98.

Secure Firewall Posture (Formerly HostScan) 5.1.2.42 New Features

The Secure Firewall Posture, formerly HostScan, 5.1.2.42 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

Secure Firewall Posture (Formerly HostScan) 5.1.1.42 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.1.42 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defect listed in Secure Firewall Posture (Formerly HostScan) 5.1.1.42, on page 99.

Secure Firewall Posture (Formerly HostScan) 5.1.0.136 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.0.136 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defect listed in Secure Firewall Posture (Formerly HostScan) 5.1.0.136, on page 99.

System Requirements

This section identifies the management and endpoint requirements for this release. For endpoint OS support and license requirements for each feature, see Cisco Secure Client Features, Licenses, and OSs.

Cisco cannot guarantee compatibility with other VPN third-party clients.

Changes to the Cisco Secure Client Profile Editor

You must install Java, version 8 or higher, before launching the profile editor. Cisco Secure Client Profile Editor supports OpenJDK and also Oracle Java. For certain OpenJDK builds, Profile Editor may fail to launch when the JRE path cannot be determined. Navigate to the installed JRE path where you will be prompted to properly launch the Profile Editor.

ISE Requirements for Cisco Secure Client

- **Warning!**

  Incompatibility Warning: If you are an Identity Services Engine (ISE) customer running 2.0 (or later), you must read this before proceeding!

  The ISE RADIUS has supported TLS 1.2 since release 2.0; however, there is a defect in the ISE implementation of EAP-FAST using TLS 1.2, tracked by CSCvm03681. The defect has been fixed in

the 2.4p5 release of ISE. The fix will be made available in future hot patches for supported releases of ISE.

If Network Access Manager 4.7 (and later) is used to authenticate using EAP-FAST with any ISE releases that support TLS 1.2 prior to the above releases, the authentication will fail, and the endpoint will not have access to the network.

- ISE 2.6 (and later) with Cisco Secure Client 4.7MR1 (and later) supports IPv6 non-redirection flows (using stage 2 discovery) on wired and VPN flows.
- Cisco Secure Client temporal agent flows are working on IPv6 networks based on network topology. ISE supports multiple ways of IPv6 configuration on a network interface (for example, eth0/eth1).
- IPv6 networks with regards to ISE posture flows have the following limitations: [IPv6] ISE posture discovery is in infinite loop due to specific type of network adapters (for example, Microsoft Teredo virtual adapter) (CSCvo36890).
- ISE 2.0 is the minimum release capable of deploying Cisco Secure Client software to an endpoint and posturing that endpoint using the new ISE Posture module in Cisco Secure Client 4.0 and later.
- ISE 2.0 can only deploy Cisco Secure Client release 4.0 and later. Older releases of Cisco Secure Client must be web deployed from an ASA, predeployed with an SMS, or manually deployed.
- If you are installing or updating the Cisco Secure Client ISE Posture module, the package and modules configured on ASA must be the same as the ones configured on ISE. VPN is always upgraded when other modules are upgraded, and a VPN module upgrade is not allowed from ISE when the tunnel is active.

ISE Licensing Requirements

To deploy Cisco Secure Client from an ISE headend and use the ISE Posture module, a Cisco ISE Premier License is required on the ISE Administration node. For detailed ISE license information, see the *Cisco ISE Licenses* chapter of the Cisco Identity Services Engine Admin Guide.

Secure Firewall ASA Requirements for Cisco Secure Client

Minimum ASA/ASDM Release Requirements for Specified Features

- You must upgrade to Secure Firewall ASA 9.17.x (or later) and ASDM 7.17.x (or later) to use Cisco Secure Client VPN SAML External Browser. With that version and Cisco Secure Client version 5, you can configure VPN SAML external browser to enable additional authentication choices, such as passwordless authentication, WebAuthN, FIDO2, SSO, U2F, and an improved SAML experience due to the persistence of cookies. When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the Secure Client use the client's local browser instead of the Secure Client embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication and Yubikeys, which cannot be performed in the embedded browser.
- You must upgrade to Secure Firewall ASA 9.10.1 (or later) and ASDM 7.10.1 (or later) to use DTLSv1.2.

Note DTLSv1.2 is supported on all Secure Firewall ASA models except the 5506-X, 5508-X, and 5516-X and applies when the ASA is acting as a server only, not a client. DTLS 1.2 supports additional ciphers, as well as all current TLS/DTLS ciphers and a larger cookie size.

- You must upgrade to ASDM 7.10.1 to use management VPN tunnel.
- You must upgrade to ASDM 7.5.1 to use Network Visibility Module.
- You must upgrade to ASDM 7.4.2 to use AMP Enabler.

Note AMP Enabler is not part of Cisco Secure Client release 5.0.

- You must upgrade to Secure Firewall ASA 9.3(2) to use TLS 1.2.
- You must upgrade to Secure Firewall ASA 9.2(1) if you want to use the following features:
  - ISE Posture over VPN
  - ISE Deployment of Cisco Secure Client
  - Change of Authorization (CoA) on ASA is supported from this version onwards
- You must upgrade to Secure Firewall ASA 9.0 if you want to use the following features:
  - IPv6 support
  - Cisco Next Generation Encryption “Suite-B” security
  - Dynamic Split Tunneling(Custom Attributes)
  - Cisco Secure Client deferred upgrades
  - Management VPN Tunnel (Custom Attributes)
- You must use Secure Firewall ASA 8.4(1) or later if you want to do the following:
  - Use IKEv2.
  - Use the ASDM to edit non-VPN client profiles (such as Network Access Manager).
  - Deploy firewall rules. If you deploy always-on VPN, you might want to enable split tunneling and configure firewall rules to restrict network access to local printing and tethered mobile devices.
  - Configure dynamic access policies or group policies to exempt qualified VPN users from an always-on VPN deployment.
  - Configure dynamic access policies to display a message on the Cisco Secure Client GUI when an Cisco Secure Client session is in quarantine.
- To perform the Secure Firewall Posture migration from 4.3x to 4.6.x, ASDM 7.9.2 or later is required.

Secure Firewall ASA Memory Requirements

Caution The minimum flash memory recommended for all Secure Firewall ASA models using Cisco Secure Client is 512MB. This will allow hosting of multiple endpoint operating systems, and logging and debugging to be enabled on the ASA.

Due to flash size limitations on the Secure Firewall ASA (maximum of 128 MB), not all permutations of the Cisco Secure Client package will be able to be loaded onto this model. To successfully load Cisco Secure Client, you will need to reduce the size of your packages (such as fewer OSs, no Secure Firewall Posture, and so on) until they fit on the available flash.

Check for the available space before proceeding with the Cisco Secure Client install or upgrade. You can use one of the following methods to do so:

- CLI—Enter the **show memory** command.

```
asa3# show memory
Free memory:       304701712 bytes (57%)
Used memory:       232169200 bytes (43%)
-------------     ----------------
Total memory:      536870912 bytes (100%)
```

- ASDM—Choose Tools > File Management. The File Management window displays flash space.

If your Secure Firewall ASA has only the default internal flash memory size or the default DRAM size (for cache memory), you could have problems storing and loading multiple Cisco Secure Client packages on the ASA. Even if you have enough space on the flash to hold the package files, the Secure Firewall ASA could run out of cache memory when it unzips and loads the client images. For additional information about the ASA memory requirements and upgrading ASA memory, see the latest release notes for the Cisco ASA.

Secure Firewall Posture

Cisco Secure Client 5.0.x **must** use Secure Firewall Posture 5.0.x (or later).

Note Cisco Secure Client 5.0.x will not establish a VPN connection when used with an incompatible version of HostScan; therefore, using HostScan 4.x with Cisco Secure Client 5.0.x endpoints is not supported.

If you are currently using **HostScan 4.3.x or earlier**, a one-time HostScan migration **must** be performed prior to upgrading to any newer version of HostScan. Refer to the AnyConnect HostScan Migration 4.3.x to 4.6.x and Later documentation for the specifics of how to do this migration.

Also, Cisco does not recommend the combined use of Secure Firewall Posture and ISE posture. Unexpected results occur when the two different posture agents are run.

The Secure Firewall Posture Module, formerly HostScan provides Cisco Secure Client the ability to identify the operating system, antimalware, and firewall software installed on the host to the Secure Firewall ASA.

When using Start Before Login (SBL) and Secure Firewall Posture, you must install the Cisco Secure Client predeploy module on the endpoints to achieve full Secure Firewall Posture functionality, since SBL is pre-login.

Secure Firewall Posture, available as its own software package, is periodically updated with new operating system, antimalware, and firewall software information. We recommend that you run the most recent version of Secure Firewall Posture (which is the same as the version of Cisco Secure Client).

The Secure Firewall Posture Antimalware and Firewall Support Charts are available on cisco.com.

ISE Posture Compliance Module

(CSCwa91572) For compatibility and ease of deployment, you must use the following Compliance Modules with Cisco Secure Client version 5.0.01242 and later: Windows version 4.3.2755, macOS version 4.3.2379, and Linux version 4.3.2063. Also, already released Compliance Modules are not supported for Cisco Secure Client version 5.0.01242 (and later) builds.

(CSCvy53730-Windows only) As of AnyConnect 4.9.06037, the Compliance Modules from ISE cannot be updated. Due to this change, Compliance Module version 4.3.1634.6145 or later are required for AnyConnect 4.9.06037 (and above) and Cisco Secure Client 5 (up to 5.0.01242).

The ISE Posture compliance module contains the list of supported antimalware and firewall for ISE posture. While the Secure Firewall Posture list is organized by vendor, the ISE posture list organizes by product type. When the version number on the headend (ISE or Secure Firewall ASA) is greater than the version on the endpoint, the OPSWAT gets updated. These upgrades are mandatory and happen automatically without end user intervention.

The individual files within the library (a zip file) are digitally signed by OPSWAT, Inc., and the library itself is packaged as a single, self-extracting executable which is code signed by a Cisco certificate. Refer to the ISE compliance modules for details.

IOS Support of Cisco Secure Client

Cisco supports AnyConnect VPN access to IOS Release 15.1(2)T functioning as the secure gateway; however, IOS Release 15.1(2)T does not currently support the following Cisco Secure Client features:

- Post Log-in Always-on VPN
- Connect Failure Policy
- Client Firewall providing Local Printer and Tethered Device access
- Optimal Gateway Selection
- Quarantine
- Cisco Secure Client Profile Editor
- DTLSv1.2

For additional limitations of IOS support for AnyConnect VPN, please see Features Not Supported on the Cisco IOS SSL VPN.

Refer to http://www.cisco.com/go/fn for additional IOS feature support information.

Cisco Secure Client Supported Operating Systems

The following tables list the minimum versions supported. When specific versions are noted, as opposed to something such as *8.x*, it is because only particular versions are supported. For example, ISE Posture is not supported on Red Hat 8.0, but it is supported on Red Hat 8.1 and later, and noted as such.

Upon release of new Windows or macOS versions, Cisco provides Day Zero support to prevent disruption and to allow immediate leverage of the new OS features. We proactively test our product against the upcoming OS release and ensure that it works without issues, errors, or security vulnerabilities. However, to complete testing on the final shipped product, the announcement of official support may extend beyond the Day Zero release date. For this reason, the tables below may not reflect the latest Windows or macOS versions, until they coincide with our Secure Client release cycles or until testing of the final shipped product is complete.

It is always advised to upgrade to the latest version to benefit from full support of the operating systems and all defect fixes.

Table 1: Windows

Windows Versions	VPN	Network Access Manager	Secure Firewall Posture	ISE Posture	DART	Customer Experience Feedback	Network Visibility Module	AMP Enabler	Umbrella Roaming Security	Duo Endpoint Agent	Zero Trust Access Module
Current Microsoft supported versions of Windows 11 and Windows 10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes*
Microsoft-supported versions of Windows 11 for ARM64-based PCs	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes*
Windows Server 2022	Supported for Network Visibility Module on-prem and XDR										

* Zero Trust Network Access includes Duo Desktop, which requires devices with TPM 2.0

Table 2: macOS

macOS Versions	VPN	Network Access Manager	Secure Firewall Posture	ISE Posture	DART	Customer Experience Feedback	Network Visibility Module	AMP Enabler	Umbrella Roaming Security	Duo Endpoint Agent	Zero Trust Access Module
macOS 27 (Golden Gate): 5.1.20.333, **macOS 26 (Tahoe):** 5.1.12.146+, **macOS 15 (Sequoia):** 5.1.6.103+**macOS 14 (Sonoma):**											
	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes*

* Zero Trust Network Access includes Duo Desktop, which requires devices with Secure Enclave

Table 3: Linux

Linux Versions (for x86_64)	VPN	Secure Firewall Posture	Network Visibility Module	ISE Posture	DART	Zero Trust Access	Customer Experience Feedback
Red Hat 10.x, 9.x, and 8.x	Yes	Yes	Yes	9.x and 8.1 (and later)	Yes	Yes. Only 9.x.	Yes

Linux Versions (for x86_64)	VPN	Secure Firewall Posture	Network Visibility Module	ISE Posture	DART	Zero Trust Access	Customer Experience Feedback
Ubuntu 26.04, 24.04, and 22.04	Yes	Yes	Yes	Yes	Yes	Yes. Only 24.04 (and later)	Yes
SUSE supported versions of SLES 15	Limited support. Used only to install ISE Posture	No	No	Yes	Yes	No	Yes

Linux Versions (for ARM64)	VPN	Secure Firewall Posture	Network Visibility Module	ISE Posture	DART	Zero Trust Access	Customer Experience Feedback
Red Hat 9.x and 8.x	Yes	Yes	Yes	No	Yes	No	Yes
Ubuntu 24.04 and 22.04	Yes	Yes	Yes	No	Yes	No	Yes

Cisco Secure Client Support for Microsoft Windows

Windows Requirements

- Pentium class processor or greater.
- Secure Client software runs on the minimal hardware requirements determined by the Windows vendor specifications for each version we support.
- Microsoft Installer, version 3.1.
- Upgrading to Windows 8.1 from any previous Windows release requires you to uninstall Cisco Secure Client, and reinstall it after your Windows upgrade is complete.
- Upgrading from Windows XP to any later Windows release requires a clean install since the Cisco Secure Client Virtual Adapter is not preserved during the upgrade. Manually uninstall Cisco Secure Client, upgrade Windows, then reinstall Cisco Secure Client manually or via WebLaunch.
- To start Cisco Secure Client with WebLaunch, you must use the 32-bit version of Firefox 3.0+ and enable ActiveX or install Sun JRE 1.4+.
- ASDM version 7.02 or higher is required when using Windows 10 (or later).

Windows Limitations

- Before AnyConnect release 4.10.03104, Windows ADVERTISE installer action was not supported (CSCvw79615). With release 4.10.03104 and later, we provided a fix to successfully upgrade with

Windows ADVERTISE for those with a lower version of AnyConnect. Consider however that future upgrades could still fail if AnyConnect version 4.10.02086 or earlier (as opposed to 4.10.03104 or later) is advertised.

- HP Protect tools do not work with Cisco Secure Client on Windows 10 (and later).
- If you are using Network Access Manager on a system that supports standby, Cisco recommends that the default Windows 10.x (and later) association timer value (5 seconds) is used. If you find the Scanlist in Windows appears shorter than expected, increase the association timer so that the driver can complete a network scan and populate the scanlist.

Windows Guidelines

- Verify that the driver on the client system is supported by your Windows version. Drivers that are not supported may have intermittent connection problems.
- For Network Access Manager, machine authentication using machine password will not work on Windows 10 or 11/ Server 2012 unless a registry fix described in Microsoft KB 2743127 is applied to the client desktop. This fix includes adding a DWORD value LsaAllowReturningUnencryptedSecrets to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa registry key and setting this value to 1.

  Machine authentication using machine certificate (rather than machine password) does not require a change and is the more secure option. Because machine password was accessible in an unencrypted format, Microsoft changed the OS so that a special key was required. Network Access Manager cannot know the password established between the operating system and active directory server and can only obtain it by setting the key above. This change permits Local Security Authority (LSA) to provide clients like Cisco Network Access Manager with the machine password.

Note Machine authentication allows a client desktop to be authenticated to the network before the user logs in. During this time the administrator can perform scheduled administrative tasks for this client machine. Machine authentication is also required for the EAP Chaining feature where a RADIUS server can authenticate both the User and Machine for a particular client. This will result in identifying company assets and applying appropriate access policies. For example, if this is a personal asset (PC/laptop/tablet), and corporate credentials are used, the endpoint will fail Machine authentication, but succeed User authentication, and the proper network access restrictions are applied to the user's network connection.

- On Windows 10 (and later), the Export Stats button on the Preferences > VPN > Statistics tab saves the file on the desktop. In other versions of Windows, the user is asked where to save the file.
- AnyConnect VPN is compatible with 3G/4G/5G data cards which interface with Windows via a WWAN adapter.

Cisco Secure Client Support for Linux

Linux Requirements

- Administrator privileges are required for installation

- 64-bit processor
- Secure Client software runs on the minimal hardware requirements determined by the Linux vendor specifications for each version we support.
- tun support in Linux Kernel
- libnss3, only if you are using the NSS Certificate Store
- libstdc++ 6.0.19 (GLIBCXX_3.4.19) or later
- iptables 1.4.21 or later
- NetworkManager 1.0.6 or later
- zlib - to support SSL deflate compression
- glib 2.36 and later
- polkit 0.105 or later, with pkexec (if provided as a separate package; only needed for ISE Posture deployment)
- gtk 3.8 or later
- systemd
- webkitgtk+ 2.10 or later, required only if you are using the Cisco Secure Client embedded browser app
- libnm (libnm.so or libnm-glib.so), required only if you are using Network Visibility Module

Linux Limitations

With the Secure Client for Linux ARM64 support, we have the following limitations:

- Webdeploy on Linux ARM64 is available only through the Chromium browser.
- Linux ARM64 includes all of the same modules as the Linux x86_64 version, except for ISE Posture, which is currently unsupported.

Cisco Secure Client Support for macOS

macOS Requirements

- Secure Client software runs on the minimal hardware requirements determined by the macOS vendor specifications for each version we support.
- To operate correctly with macOS, Cisco Secure Client requires a minimum display resolution of 1024 by 640 pixels.

macOS Guidelines

- Cisco Secure Client 4.8 (and later) for macOS has been notarized, and installer disk images (dmg) have been stapled.
- Because of the introduction of access control in macOS 10.15, you may see additional popups when Secure Firewall Posture (formerly HostScan) or ISE posture are performing a scan on the endpoint. You are required to accept which files and folders can be accessed and scanned.

- Within the ThousandEyes Endpoint Agent (Agent Settings), independent of Secure Client, you are offered separate macOS installer packages for x64 and ARM64. However, the Secure Client predeploy package contains only the ThousandEyes Endpoint Agent x64 installer. The ThousandEyes Endpoint Agent is supported on macOS ARM64 devices only when Rosetta is installed on the endpoint.

Cisco Secure Client Licensing

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.

To deploy Cisco Secure Client from an ISE headend and use the ISE Posture module, a Cisco ISE Premier License is required on the ISE Administration node. For detailed ISE license information, see the *Cisco ISE Licenses* chapter of the Cisco Identity Services Engine.

To deploy Cisco Secure Client from a Secure Firewall ASA headend and use the VPN and Secure Firewall Posture modules, an Advantage or Premier license is required. Trial licenses are available. See the Cisco Secure Client Ordering Guide.

For an overview of the Advantage and Premier licenses and a description of which license the features use, see Cisco Secure Client Features, Licenses, and OSs.

Cisco Secure Client Installation Overview

Deploying Cisco Secure Client refers to installing, configuring, and upgrading the Cisco Secure Client and its related files. The Cisco Secure Client can be deployed to remote users by the following methods:

- Predeploy—New installations and upgrades are done either by the end user, or by using an enterprise software management system (SMS).
- Web Deploy—The Cisco Secure Client package is loaded on the headend, which is either a Secure Firewall ASA or ISE server. When the user connects to a Secure Firewall ASA or to ISE, Cisco Secure Client is deployed to the client.
  - For new installations, the user connects to a headend to download Cisco Secure Client. The client is either installed manually, or automatically (web-launch).
  - Updates are done by Cisco Secure Client running on a system where Secure Client is already installed, or by directing the user to the Secure Firewall ASA clientless portal.
- Cisco Secure Client Cloud Management—Once you have chosen which Cisco Secure Client options you want to enable (such as Start Before Login, Diagnostics and Reporting Tool, Secure Firewall Posture, Network Visibility Module, Secure Umbrella, ISE Posture, Network Access Manager, Secure Endpoint Data Loss Prevention, and so on), click the ellipsis icon for the desired operating system. Choose **Network Installer** or **Full Installer** on the Deployment Management page of the Secure Client Cloud Management UI. This action downloads the csc-deployment.exe file, which then can be executed in a command prompt to install the Cloud Management service and your configured modules onto the endpoints. After you have the XDR Default Deployment installed on your endpoints, you can view the Network Visibility Module data in Secure Cloud Analytics (now part of Cisco XDR). Cisco Secure Client can be used with or without cloud management.

When you deploy Cisco Secure Client, you can include the optional modules that enable extra features, and client profiles that configure the VPN and other features. Keep in mind the following:

- All Cisco Secure Client modules and profiles can be predeployed. When predeploying, you must pay special attention to the module installation sequence and other details.
- The Customer Experience Feedback module and the Secure Firewall Posture package, used by the VPN Posture module, cannot be web deployed from the ISE.
- The Compliance Module, used by the ISE Posture module, cannot be web deployed from the Secure Firewall ASA.



Note Make sure to update the localization MST files with the latest release from CCO whenever you upgrade to a new Cisco Secure Client package.

Cisco Secure Client Support Policy

Cisco only provides fixes and enhancements for 5.x based on the most recent Version 5 release. TAC support is available to any customer with an active Cisco Secure Client Version 5 term/contract running a released version of Cisco Secure Client Version 5. If you experience a problem with an out-of-date software version, you may be asked to validate whether the current maintenance release resolves your issue.

Software Center access is limited to Cisco Secure Client Version 5 versions with current fixes. We recommend that you download all images for your deployment, as we cannot guarantee that the version you are looking to deploy will still be available for download at a future date.

Guidelines and Limitations

Do Not Store Credentials in Config Profiles

Cisco recommends against storing static passwords, tokens, and pre-shared keys in the Network Access Manager configuration profile. The best practice is to share static credentials through secure channels (such as email or a credential management system), rather than embedded directly in configuration profile.

VPN Connection Requires Group Number Not Name

When authenticating through AAA on the ASA and configuring for multiple groups using CLI, you may see something like the following:

```
139) tnd-fpr24-pcloud-pause
140) tnd_cert_donothing-pause
141) zta-enroll
Group: [(AAA)]
```

For the *Group* prompt, you must enter a number and not a name.

SAML Auth Via Embedded Browser Not Supported on RHEL 10

(CSCwp19612) RHEL 10 removed the WebKitGTK web browser engine. As a result, SAML authentication via embedded browser is no longer supported. You can configure to use the external browser instead. Or install the missing WebKitGTK library from a third-party repository like EPEL: https://docs.fedoraproject.org/en-US/epel/.

Some Secure Client Modules Not Working on Windows 11 24H2 Unless Location Permission is Set

Windows 11 (version 24H2) made a change to the API behavior that impacts wireless access and location. Specifically, access to APIs providing Basic Service Set Identifiers (BSSIDs) is now restricted and requires you to configure location services appropriately. You must go to **Windows Settings > Privacy & Security > Location** and set *Location Services* to **On** and then *Let desktop apps access your location* to **On** and then reboot to gain access. The following Secure Client modules that rely on BSSID information are impacted, and you should track the following caveats, as well as Microsoft updates, to ensure continued functionality:

- Network Access Manager: (CSCwm05134) When Network Access Manager is started while running Windows 11 24H2, you are prompted to enable location services. (CSCwn00122) A Network Access Manager uninstall or upgrade will not complete successfully if Windows 11 24H2 (or later) is running without location services being enabled. We corrected uninstalls and upgrades from 5.1.8.x to future releases, but uninstalls and upgrades from versions prior to 5.1.8.x will still fail. Refer to the bug ID for workarounds.
- Network Visibility Module: (CSCwm87018) If the Location feature is disabled in Windows 11 24H2, the Network Visibility Module will not report the SSID details when connected to a wireless network.
- ISE Posture: (CSCwm80714) The discovery process for finding the ISE policy server will not occur in Windows 11 (24H2 and later) unless you enable Location Services as instructed above, or configure an ISE Posture Profile setting. If you set the *Operate on non-802.1X wireless* to **Yes** when the primary interface of the endpoint is wireless, you don't need to enable the Location Services. You will receive a notification in the ISE Posture tile if Location Services are not enabled.
- ThousandEyes: The ability to query information about the current WiFi connection, such as signal strength and noise, is hindered.

Network Access Manager Limitation With Windows Hello for Business

Network Access Manager can use Single Sign On (SSO) credentials for network authentication when a user logs on with a username and password, or a certificate PIN. Microsoft introduced Windows Hello for Business (WHfB) as an additional way to log on, but WHfB SSO credentials cannot be used by Network Access Manager and are not currently supported. Because WHfB SSO credentials are not supported, you will be prompted for 802.1x authentication credentials after WHfB log on.

Deployment on macOS 13 (or Later) Requires Admin Privileges

Due to a new OS requirement, one-time administrator privileges are necessary when performing a fresh install of 5.1.x (or later), or upgrade from 5.0.x (or earlier). Further updates do not need them. You can circumvent this limitation by managing macOS devices via MDM and pre-approving the application. Refer to Managed Login Items for additional information. The VPN and ZTA modules require user approval before they can function.

Embedded Browser Changes After Deprecation of IE11

With the deprecation of IE11, Secure Client embedded browser defaults to WebView2, as long as the runtime is installed. If you need to revert back to the legacy embedded browser control, add a DWORD registry value *UseLegacyEmbeddedBrowser* set to 1 to the following Windows registry key:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client
```

Encrypted DNS Impact and Mitigation

Encrypted Domain Name System (DNS) resolution impacts Secure Client functionality, namely that network flows targeting FQDNs resolved via encrypted DNS either circumvent or are not properly handled by the following Secure Client features: Umbrella DNS protection, Umbrella web protection (when name-based redirect rules are used), AnyConnect VPN (split DNS, dynamic split tunneling and Always On with name-based exceptions), Network Visibility (reporting of peer FQDN) and Zero Trust Access (when name-based rules are applied). To mitigate this impact, you should disable encrypted DNS in browser settings pertaining to Secure Client users.

As an additional mitigation, Cisco Secure Client prohibits DNS over HTTPS (DoH) name resolution for the Windows DNS client via local policy setting **Configure DNS over HTTP (DoH) name resolution** (under Computer Configuration > Administrative Templates > Network > DNS Client). This change is applicable to Windows 11 and later versions and is enforced while any of the following modules is active: VPN, Umbrella Roaming Security, Network Visibility, or Zero Trust Access. Cisco Secure Client does not alter this policy setting if a conflicting setting of higher precedence (for example, domain GPO setting) is detected.

Known Issues With Windows ARM64

The following issues are known with Windows ARM64:

- CSCwd71408—Secure Client customization and localization is missing from ASA on Windows ARM64 platforms
- CSCwh12493—ASDM throws an error unable to load secure client profile editor on ISE Posture profiles on ARM64
- CSCwd81735—When Secure Firewall ASA has Secure Firewall Posture (formerly HostScan) enabled and running the same 5.0 version as Secure Client, a failure could result. However, the Secure Client UI shows no status message or error. The client may still be functioning normally and responds to clicking Connect, but the status message gives no indication.
- CSCwd71408—ASA needs to add support for Cisco Secure Client binary file customization in order for scripting to work.
- CSCwh63153— Failure to launch downloader error if Windows ARM CP is not configured but agent is already installed
- ISE Posture service is unavailable. You can restore the service by manually restarting csc_ise_agent.
- ARM64 version of Java is not supported: only X86 or X64 versions.
- For the Network Visibility Module in ARM64 platforms, Module Name and Module Hash are not reported in flows that are generated for SVCHost processes.

RDP With Wired Connections Not Working

If the Network Access Manager is configured for machine or user authentication while a Windows Remote Desktop Protocol attempt is made from a remote device, the connection may fail. The cause of the failure is an interface change in how Microsoft firewall establishes quarantines for the network. Until we can coordinate a resolution with Microsoft, you can try the workaround documented in CSCvo47467.

Simultaneous VPN Sessions Not Supported

AnyConnect VPN cannot be active at the same time as any other client VPN, either Cisco software like the Cisco Secure Client for Universal Windows Platform or third-party VPNs.

macOS 13 Known Issue

Continuity Camera in macOS 13 is currently not functioning during an active VPN connection.

DNS (Name Resolution) on macOS 12.x May Fail

Those running Cisco Secure Client on macOS 12.x may experience a loss of DNS (name resolution), requiring a reboot for restoration. The cause has been identified as a macOS bug, which has been addressed in macOS 12.3 (FB9803355).

Windows Local Group Policy DNS Settings Ignored

Global DNS settings Searchlist and UseDomainNameDevolution are used by Cisco Secure Client to build the DNS suffix search list for a VPN connection. Any overrides configured via local group policy will be ignored.

Root CA Conflict With Firefox NSS Store (Linux Only)

When a root certificate authority (CA) is public trusted, it is already in the File Certificate Store. However, if the Firefox NSS store is left enabled at the same time, the OCSP check might be bypassed, as we only support OCSP check with File Cert Store. To prevent this bypass, disable Firefox NSS store by setting ExcludeFirefoxNSSCertStore to *true* in the local policy file.

Initiating an Automatic VPN Connection With TND (CSCvz02896)

When using Trusted Network Detection, the automatic VPN connection may not be initiated according to the TND policy, if the system route table does not contain a default route.

Local and Network Proxy Incompatibilities

Local and/or network proxies (such as software/security applications like Fiddler, Charles Proxy, or Third-party Antimalware/Security software that includes Web HTTP/HTTPS inspection and/or decryption capabilities) are not compatible with Cisco Secure Client.

Server Certificate Validation Error

(CSCvu71024) Cisco Secure Client authentication may fail if the Secure Firewall ASA headend or SAML provider uses certificates signed by the AddTrust root (or one of the intermediaries), because they expired in

May 2020. The expired certificate causes Cisco Secure Client to fail and presents as a server certificate validation error, until operating systems make the required updates to accommodate the May 2020 expiration.

Windows DNS Client Optimizations Caveat

Windows DNS Client optimizations present in Windows 10 (and later) may result in failure to resolve certain domain names when split DNS is enabled. The workaround is to disable such optimizations by updating the following registry keys:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

Value:DisableParallelAandAAAA

Data: 1

Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient

Value: DisableSmartNameResolution

Data: 1
```

Permission Popups During Initial Secure Firewall Posture or ISE Posture Launch (CSCvq64942)

macOS 10.15 (and later) requires that applications obtain user permissions for access to Desktop, Documents, Downloads, and Network Volume folders. To grant this access, you may see popups during an initial launch of Secure Firewall Posture, ISE Posture (when ISE posture is enabled on the network), or DART (when ISE posture or Cisco Secure Client is installed). ISE posture and Secure Firewall Posture use OPSWAT for posture assessment on endpoints, and the posture checks access these folders based on the product and policies configured.

At these popups, you must click **OK** to have access to these folders and to continue with the posture flow. If you click **Don't Allow**, the endpoint may not remain compliant, and the posture assessment and remediation may fail without access to these folders.

To Remedy a *Don't Allow* Selection

To see these popups again and grant access to the folders, edit cached settings:

1. Open **System Preferences**.
2. Navigate to **Security & Privacy** > **Privacy > Files and Folders** > **.**
3. Delete folder access related cache details in the Cisco Secure Client folder.

The permission popups will reappear with a subsequent start of posture, and the user can click **OK** to grant access.

GUI Customization on macOS Not Supported

GUI resource customization on macOS is currently not supported.

PMK-Based Roaming Not Supported With Network Access Manager

You cannot use PMK-based roaming (fast transition, pmkid caching, and OKC) with Network Access Manager on Windows.

DART Requires Admin Privileges

Due to system security restrictions, DART now requires administrator privileges on macOS, Ubuntu, and Red Hat to collect logs.

Conflict with Network Access Manager and Group Policy

If your wired or wireless network settings or specific SSIDs are pushed from a Windows group policy, they can conflict with the proper operation of the Network Access Manager. With the Network Access Manager installed, a group policy for wireless settings is not supported.

No Hidden Network Scanlist on Network Access Manager with Windows 10 Version 1703 (CSCvg04014)

Windows 10 version 1703 changed their WLAN behavior, which caused disruptions when the Network Access Manager scans for wireless network SSIDs. Because of a bug with the Windows code that Microsoft is investigating, the Network Access Manager's attempt to access hidden networks is impacted. To provide the best user experience, we have disabled Microsoft's new functionality by setting two registry keys during Network Access Manager installation and removing them during an uninstall.

Impact on Posture When a Power Event or Network Interruption Occurs

If a network change or power event occurs, a posture process that is interrupted will not complete successfully. The network or power change results in the Cisco Secure Client downloader error that must be acknowledged by the user before continuing the process.

Network Access Manager Does Not Automatically Fallback to WWAN/3G/4G/5G

All connections to WWAN/3G/4G/5G must be manually triggered by the user. The Network Access Manager does NOT automatically connect to these networks if no wired or wireless connection is available.

macOS Keychain Prompts During Authentication

On macOS, a keychain authentication prompt may appear after the VPN connection is initiated. The prompt only occurs when access to a client certificate private key is necessary, after a client certificate request from the secure gateway. Even if the tunnel group is not configured with certificate authentication, certificate mapping may be configured on the Secure Firewall ASA, causing the keychain prompts when the access control setting for the client certificate private key is configured as *Confirm Before Allowing Access*.

Configure the Cisco Secure Client profile to restrict Secure Client access strictly to clients certificates from the login keychain (in the ASDM profile editor, choose Login under Preferences (Part 1) - Certificate Store - macOS). You can stop the keychain authentication prompts with one of the following actions:

- Configure the certificate matching criteria in the client profile to exclude well-known system keychain certificates.
- Configure the access control setting for the client certificate private keys in the system keychain to allow access to Cisco Secure Client.

Umbrella Roaming Security Module Changes

The dashboard to retrieve the `OrgInfo.json` file is https://dashboard.umbrella.com. From there you navigate to **Identities** > **Roaming Computers**, click the + (Add icon) in the upper left, and click **Module Profile** from the Cisco Secure Client Umbrella Roaming Security Module section.

Cisco Secure Client Compatibility with Microsoft Windows 10

For best results, we recommend a clean install of Cisco Secure Client on a Windows 10 system and not an upgrade from Windows 7/8/8.1. If you are planning to perform an upgrade from Windows 7/8/8.1 with Cisco Secure Client pre-installed, make sure that you first upgrade Cisco Secure Client prior to uprading the operating system. The Network Access Manager Module **must** be uninstalled prior to upgrading to Windows 10. After the system upgrade is complete, you can re-install Network Access Manager on the system. You may also choose to fully uninstall Cisco Secure Client and re-install one of the supported versions after upgrading to Windows 10.

New Split Include Tunnel Behavior (CSCum90946)

Formerly, if a split-include network was a Supernet of a Local Subnet, the local subnet traffic was *not* tunneled unless a split-include network that exactly matches the Local Subnet was configured. With the resolution of CSCum90946, when a split-include network is a Supernet of a Local Subnet, the Local Subnet traffic is tunneled, unless a split-exclude (deny 0.0.0.0/32 or ::/128) is also configured in the access-list (ACE/ACL).

The following configuration is required when a Supernet is configured in the split-include *and* the desired behavior is to allow LocalLan access:

- access-list (ACE/ACL) must include *both* a permit action for the Supernet and a deny action for 0.0.0.0/32 or ::/128.
- Enable Local LAN Access in the Cisco Secure Client profile (in the Preferences Part 1 menu) of the profile editor. (You also have the option to make it user controllable.)

Using Log Trace in ISE Posture

After a fresh installation, you see ISE posture log trace messages as expected. However, if you go into the ISE Posture Profile Editor and change the Enable Agent Log Trace file to 0 (disable), a service restart of Cisco Secure Client is required to get expected results.

Interoperability With ISE Posture on macOS

If you are using macOS 10.9 or later and want to use ISE posture, you may need to do the following to avoid issues:

- Turn off certificate validation to avoid a "failed to contact policy server" error during posture assessment.
- Disable the captive portal application; otherwise, discovery probes are blocked, and the application remains in pre-posture ACL state.

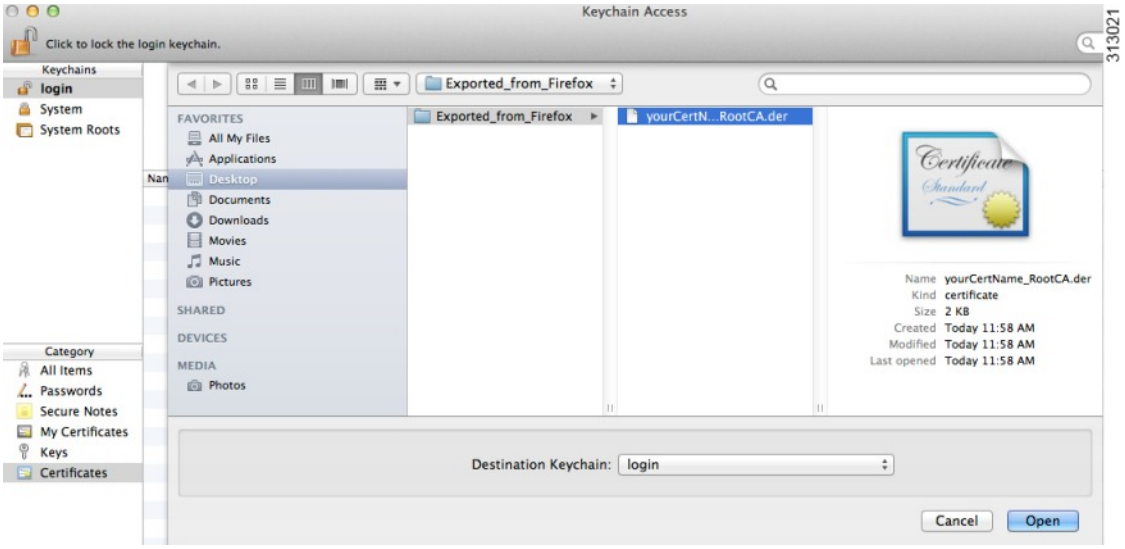
Firefox Certificate Store on macOS is Not Supported

The Firefox certificate store on macOS is stored with permissions that allow any user to alter the contents of the store, which allows unauthorized users or processes to add an illegitimate CA into the trusted root store. Cisco Secure Client no longer utilizes the Firefox store for either server validation or client certificates.

If necessary, instruct your users how to export your Cisco Secure Client certificates from their Firefox certificate stores, and how to import them into the macOS keychain. The following steps are an example of what you may want to tell your Cisco Secure Client users.

1. Navigate to **Firefox > Preferences > Privacy & Security > Advanced**, Certificates tab, click **View Certificates**.
2. Select the Certificate used for Cisco Secure Client, and click **Export**.

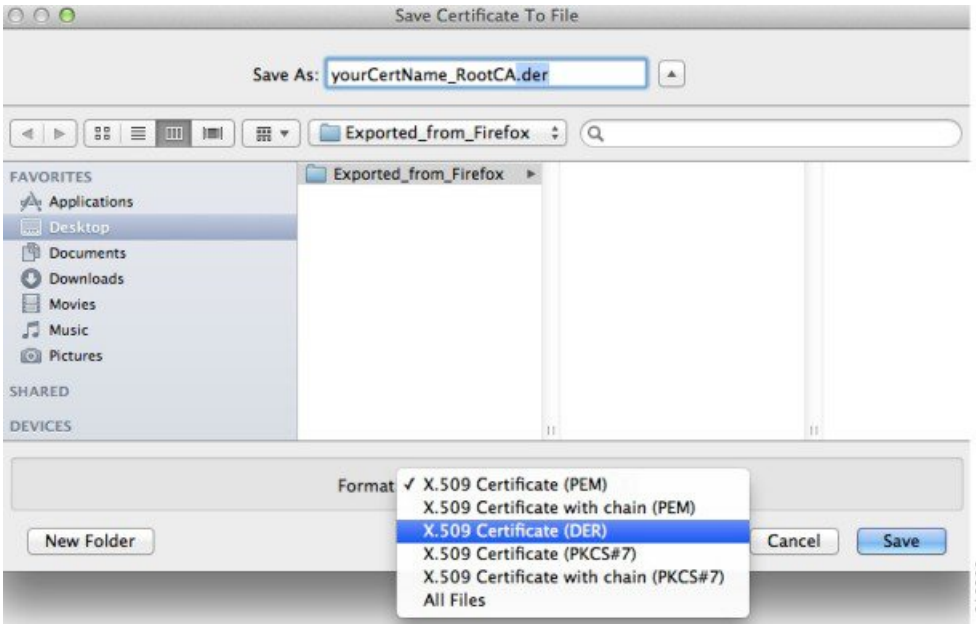
   Your Cisco Secure Client Certificate(s) will most likely be located under the Authorities category. Verify with your Certificate Administrator, as they may be located under a different category (Your Certificates or Servers).
3. Select a location to save the Certificate(s), for example, a folder on your desktop.
4. In the Format pull down menu, select **X.509 Certificate (DER)**. Add the .der extension to the certificate name, if required.



Note If more than one Cisco Secure Client Certificate and/or a Private Key is used/required, repeat the above process for each Certificate).

5. Launch KeyChain. Navigate to File, Import Items…, and select the Certificate that you exported from Firefox.

   In the Destination Keychain:, select the desired Keychain. The login Keychain that is used for this example may not be the one used at your company. Ask your Certificate Administrator to which Keychain your certificate(s) should be imported.
6. In the Destination Keychain:, select the desired Keychain. The login Keychain that is used for this example may not be the one used at your company. Ask your Certificate Administrator to which keychain your certificate(s) should be imported.



7. Repeat the preceding steps for additional Certificates that are used or required for Cisco Secure Client.

Implicit DHCP filter applied when Tunnel All Networks Configured

To allow local DHCP traffic to flow in the clear when Tunnel All Networks is configured, Cisco Secure Client adds a specific route to the local DHCP server when Cisco Secure Client connects. To prevent data leakage on this route, Cisco Secure Client also applies an implicit filter on the LAN adapter of the host machine, blocking all traffic for that route except DHCP traffic.

Cisco Secure Client over Tethered Devices

Network connectivity provided by Bluetooth or USB tethered mobile phones or mobile data devices are not specifically qualified by Cisco and should be verified with Cisco Secure Client before deployment.

Cisco Secure Client Smart Card Support

Cisco Secure Client supports Smartcard provided credentials in the following environments:

- Microsoft CAPI 1.0 and CAPI 2.0 on Windows 10 (and later).
- Keychain on macOS, and CryptoTokenKit on macOS 10.12 and higher.

Note Cisco Secure Client does not support Smart cards on Linux or PKCS #11 devices.

Some smart cards may not support client certificate authentication using KSP (Key Storage Provider) and CSP (Cryptographic Service Provider) settings. Be sure to test the functionality using the latest Secure Client version before deploying them in production, because support may vary by manufacturer.

Cisco Secure Client Virtual Testing Environment

Cisco performs a portion of Cisco Secure Client testing using these virtual machine environments:

- VM Fusion 7.5.x, 10.x, 11.5.x
- ESXi Hypervisor 6.0.0, 6.5.0, and 6.7.x
- VMware Workstation 15.x

We do not support running Cisco Secure Client in virtual environments; however, we expect Cisco Secure Client to function properly in the VMWare environments we test in.

If you encounter any issues with Cisco Secure Client in your virtual environment, report them. We will make our best effort to resolve them.

Disabling Auto Update May Prevent Connectivity Due to a Version Conflict

When Auto Update is disabled for a client running Cisco Secure Client, the Secure Firewall ASA must have the same version of Cisco Secure Client or earlier installed, or the client will fail to connect to the VPN.

To avoid this problem, configure the same version or earlier Cisco Secure Client package on the Secure Firewall ASA, or upgrade the client to the new version by enabling Auto Update.

Interoperability between Network Access Manager and other Connection Managers

When the Network Access Manager operates, it takes exclusive control over the network adapters and blocks attempts by other software connection managers (including the Windows native connection manager) to establish connections. Therefore, if you want Cisco Secure Client users to use other connection managers on their endpoint computers (such as iPassConnect Mobility Manager), they must disable Network Access Manager either through the Disable Client option in the Network Access Manager GUI, or by stopping the Network Access Manager service.

Configuring Antivirus Applications for Cisco Secure Client

Applications like antivirus, antimalware, and Intrusion Prevention System (IPS) can misinterpret the behavior of Cisco Secure Client applications as malicious. You can configure exceptions to avoid such misinterpretation. After installing the Cisco Secure Client modules or packages, configure your antivirus software to allow the Secure Client Installation folder or make security exceptions for the Secure Client applications.

The common directories to exclude are listed below, although the list may not be complete:

- C:\Users\<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Files (x86)\Cisco

Configuring Antivirus Applications for Secure Firewall Posture

Antivirus applications can misinterpret the behavior of some of the applications included in the posture module and the Secure Firewall Posture package as malicious. Before installing the posture module or Secure Firewall Posture package, configure your antivirus software to allow or make security exceptions for these Secure Firewall Posture applications:

- cscan.exe
- ciscod.exe
- cstub.exe

Public Proxy Not Supported by IKEv2

IKEv2 does not support the public-side proxy. If you need support for that feature, use SSL. Private-side proxies are supported by both IKEv2 and SSL as dictated by the configuration sent from the secure gateway. IKEv2 applies the proxy configuration sent from the gateway, and subsequent HTTP traffic is subject to that proxy configuration.

MTU Adjustment on Group Policy May Be Required for IKEv2

Cisco Secure Client sometimes receives and drops packet fragments with some routers, resulting in a failure of some web traffic to pass.

To avoid this, lower the value of the MTU. We recommend 1200. The following example shows how to do this using CLI:

```
hostname# config t
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

To set the MTU using ASDM, go to **Configuration** > **Network (Client) Access** > **Group Policies** > **Add** or **Edit** > **Advanced** > **AnyConnect Client**.

MTU Automatically Adjusted When Using DTLS

If Dead Peer Detection (DPD) is enabled for DTLS, the client automatically determines the path MTU. If you previously reduced the MTU using the Secure Firewall ASA, you should restore the setting to the default (1406). During tunnel establishment, the client auto-tunes the MTU using special DPD packets. If you still have a problem, use the MTU configuration on the Secure Firewall ASA to restrict the MTU as before.

Network Access Manager and Group Policy

Windows Active Directory Wireless Group Policies manage the wireless settings and any wireless networks that are deployed to PCs in a specific Active Directory Domain. When installing the Network Access Manager, administrators must be aware that certain wireless Group Policy Objects (GPOs) can affect the behavior of the Network Access Manager. Administrators should test the GPO policy settings with the Network Access Manager before doing full GPO deployment. GPOs pertaining to wireless networks are not supported.

FreeRADIUS Configuration to Work With Network Access Manager

To use Network Access Manager, you may need to adjust the FreeRADIUS configuration. Any ECDH related ciphers are disabled by default to prevent vulnerability. In /etc/raddb/eap.conf, change the cipher_list value.

Full Authentication Required if Roaming between Access Points

A mobile endpoint running Windows 10 or later must do a full EAP authentication instead of leveraging the quicker PMKID reassociation when the client roams between access points on the same network. Consequently,

in some cases, Cisco Secure Client prompts the user to enter credentials for every full authentication if the active profile requires it.

Preventing Other Devices in a LAN from Displaying Hostnames

After one uses Cisco Secure Client to establish a VPN session with Windows 7 or later on a remote LAN, the network browsers on the other devices in the user's LAN display the names of hosts on the protected remote network. However, the other devices cannot access these hosts.

To ensure the Cisco Secure Client host prevents the hostname leak between subnets, including the name of the Cisco Secure Client endpoint host, configure that endpoint to never become the primary or backup browser.

1. Enter **regedit** in the Search Programs and Files text box.
2. Navigate to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters**
3. Double-click **MaintainServerList**.

The Edit String window opens.

1. Enter **No**.
2. Click **OK**.
3. Close the Registry Editor window.

Revocation Message

The Cisco Secure Client certificate revocation warning popup window opens after authentication if Secure Client attempts to verify a server certificate that specifies the distribution point of an LDAP certificate revocation list (CRL), if the distribution point is only internally accessible.

If you want to avoid the display of this popup window, do one of the following:

- Obtain a certificate without any private CRL requirements.
- Disable server certificate revocation checking in Internet Explorer.



Caution Disabling server certificate revocation checking in Internet Explorer can have severe security ramifications for other uses of the OS.

Messages in the Localization File Can Span More than One Line

If you try to search for messages in the localization file, they can span more than one line, as shown in the example below:

```
msgid ""
"The service provider in your current location is restricting access to the "
"Secure Gateway. "
```

Cisco Secure Client for macOS Performance when Behind Certain Routers

When Cisco Secure Client for macOS attempts to create an SSL connection to a gateway running IOS, or when Cisco Secure Client attempts to create an IPsec connection to a Secure Firewall ASA from behind certain types of routers (such as the Cisco Virtual Office (CVO) router), some web traffic may pass through the connection while other traffic drops. Cisco Secure Client may calculate the MTU incorrectly.

To work around this problem, manually set the MTU for the Cisco Secure Client adaptor to a lower value using the following command from the macOS command line:

```
sudo ifconfig utun0 mtu 1200
```

Preventing Windows Users from Circumventing Always-on

On Windows computers, users with limited or standard privileges may sometimes have write access to their program data folders. These privileges could allow them to delete the Cisco Secure Client profile and thereby circumvent the Always-On feature. To prevent this, configure the computer to restrict access to the `C:\ProgramData` folder, or at least the Cisco sub-folder.

Avoid Wireless-Hosted-Network

Using Windows 10 or later, the Wireless Hosted Network feature can make Cisco Secure Client unstable. When using Cisco Secure Client, we do not recommend enabling this feature or running front-end applications that enable it (such as Connectify or Virtual Router).

Cisco Secure Client Requires That the Secure Firewall ASA Not Be Configured to Require SSLv3 Traffic

Cisco Secure Client requires the Secure Firewall ASA to accept TLSv1 or TLSv1.2 traffic, but not SSLv3 traffic. The SSLv3 key derivation algorithm uses MD5 and SHA-1 in a way that can weaken the key derivation. TLSv1, the successor to SSLv3, resolves this and other security issues present in SSLv3.

Cisco Secure Client cannot establish a connection with the following Secure Firewall ASA settings for “ssl server-version”:

ssl server-version sslv3

ssl server-version sslv3-only

Trend Micro Conflicts with Install

If you have Trend Micro on your device, the Network Access Manager will not install because of a driver conflict. You can uninstall the Trend Micro or uncheck **trend micro common firewall driver** to bypass the issue.

What Secure Firewall Posture Reports

None of the supported antimalware and firewall products report the last scan time information. Secure Firewall Posture reports the following:

- For antimalware
  - Product description
  - Product version

- File system protection status (active scan)
- Data file time (last update and timestamp)

- For firewall
  - Product description
  - Product version
  - Is firewall enabled

Long Reconnects (CSCtx35606)

You may experience long reconnects on Windows if IPv6 is enabled and auto-discovery of proxy setting is either enabled in Internet Explorer or not supported by the current network environment. As a workaround, you can disconnect any physical network adapters not used for VPN connection or disable proxy auto-discovery in IE, if proxy auto-discovery is not supported by the current network environment.

Users with Limited Privileges Cannot Upgrade ActiveX

On Windows clients that support ActiveX controls, user accounts with limited privileges cannot upgrade ActiveX controls and therefore cannot upgrade Cisco Secure Client with the web deploy method. For the most secure option, Cisco recommends that users upgrade the client from within the application by connecting to the headend and upgrading.

Note If the ActiveX control was previously installed on the client using the administrator account, the user can upgrade the ActiveX control.

No Pro-Active Key Caching (PKC) or CCKM Support

Network Access Manager does not support PKC or CCKM caching. Fast roaming is unavailable on all Windows platforms.

Application Programming Interface for the Cisco Secure Client

Cisco Secure Client includes an Application Programming Interface (API) for those who want to write their own client programs.

The API package contains documentation, source files, and library files to support a C++ interface for the Cisco Secure Client. You can use the libraries and example programs for building on Windows, Linux and MAC platforms. The Makefiles (or project files) for the Windows platform are also included. For other platforms, it includes platform specific scripts showing how to compile the example code. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.

You can download the APIs from Cisco.com.

For support issues regarding the Cisco Secure Client API, send e-mail to the following address: anyconnect-api-support@cisco.com.

Cisco Secure Client 5.1.20.333

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwv68963	gui	macOS: Tab key does not move keyboard focus
CSCwt18945	nam	NAM: Authentication Fallback option From User+Machine to Machine
CSCwu59612	nam	Unable to add Certificate Matching Rule Entries in NAM Profile Editor
CSCwv43776	nam	ISE 3.5P3 FIPS: EAP-TLS Auth Failures (DH Errors) with Secure Client 5.1.17.3394+
CSCww04040	opswat-ise	ISE Posture Patch Management condition missing Windows Update Agent 1509.x
CSCww16909	opswat-asa	macOS: Secure Firewall Posture spikes high CPU when running on macOS 15 and macOS 26
CSCwv47385	vpn	Debian client install with ABSOLUTE_INSTALLER_FILE_PATH set does not copy user profiles
CSCwv24739	ztna	ENH: Adjust ZTA DNS Caching Behavior
CSCwv89381	ztna	ZTA: To Extend TTL Duration for Synthetic IP in ZTA Interceptor
CSCww13742	ztna	Apps fail to connect to a named resource after TND deactivates its intercepting ZTA configuration

Cisco Secure Client 5.1.19.1862

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwt63680	core	Multiple certificate authentication may fail if certificates are cached on the client
CSCwt89046	core	ENH: Optimize enabling interceptor debug logging to minimize disruption
CSCwt89139	core	ENH Windows: Use an interceptor logging mechanism that doesn't require an external log collector
CSCwu65181	core	Secure Client installation on Ubuntu 26.x missing libxml2.so.2
CSCws43583	dart	Add option in dartcli to encrypt the bundle
CSCwn45054	nam	Add support for enterprise BIGKT KDE in NAM for 802.1x networks
CSCwr67707	nam	NAM logs no longer transition to networkState event "Connected"
CSCwu72140	nam	Aternity Intel-Riverbed Wi-Fi telemetry upload failure due to IHV interoperability issue with Secure Client NAM
CSCws45813	opswat-ise	ENH: Secure Firewall Posture support for CrowdStrike Falcon Firewall on Linux
CSCwt23310	opswat-ise	To support MS defender ATP automatic remediation
CSCwt90913	opswat-ise	Windows - Need support for Disk encryption Bitlocker 10.x version encryption state check

Identifier	Component	Headline
CSCwu26872	opswat-ise	ENH: Sophos Endpoint Agent 2026.x to be supported on AnyConnect Compliance Module
CSCwf92544	umbrella	Umbrella agent uses TPS component Newtonsoft.Json 6.0.2
CSCwt18374	vpn	Rpm/Deb: Linux ISE CM upgrade/downgrade issues from rpm to script
CSCwu28320	vpn	Linux: switching tunnel-groups it not loading Embedded browser, loads in Ext browser instead
CSCwt77234	ztna	macOS: Chrome connections subject to ZTA interception may fail if re-attempted after enabling interceptor debug logging
CSCwu50030	ztna	Chrome PNA prompt triggered due to ZTA synthetic address on Windows and macOS
CSCwv18649	ztna	ZTA TND IPv6 DNS server matching is case-sensitive and can prevents expected TND match
CSCwv26481	ztna	ZTA Enrollment choice file signing certificate verified against system clock instead of iat claim

Cisco Secure Client 5.1.18.314

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwq99488	core	Secure Client - Always-On Connect Failure Policy Open is cycling internet access in failed state
CSCwu49863	core	Issue with TemplateIdentifier matching in Certificate Match section of XML profile.

Identifier	Component	Headline
CSCwu56802	core	macOS - When SWG is enabled, intermittent to temporary loss of internet connectivity occurs (with potential CPU spikes)
CSCws38664	nam	NAM IHV may not start properly after extended connected standby
CSCwt83015	nam	NAM: Do not display authentication error pop up when user has not entered any credentials
CSCwu42169	nam	NAM fails to load Machine certificates using the MS CNG Key Provider
CSCwt70392	nvm	Linux NVM XDR - "No Proxy discovered" by NVM GRPC
CSCwu53462	nvm	Linux NVM XDR - NVM(On-prem) is not getting uninstalled after the NVM XDR got installed in the Linux
CSCwu53470	nvm	Linux NVM XDR - Downgrade of NVM XDR is not restricted
CSCwt31699	opswat-ise	Unable to see Avast Premium Security 26.x through posture feed update on ISE

Cisco Secure Client 5.1.17.3394

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwu25955	core	SAML authentication using external OS browser fails with "VPN internal server error"

Cisco Secure Client 5.1.17.3382

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwo01396	core	Vulnerabilities in openssl - multiple versions
CSCws60835	core	macOS: Suppress socket filter extension activation attempts during the VPN session if extension not needed
CSCwt71219	nam	SBL is not functioning as expected after upgrading to CSC version 5.1.13 and above
CSCwo03914	nvm	Vulnerabilities in libarchive 3.6.2 CVE-2024-37407 and others
CSCwo04012	nvm	Vulnerabilities in c-ares 1.17.0 CVE-2024-25629
CSCwo05333	nvm	Vulnerabilities in lz4 1.8.1
CSCwo05339	nvm	Vulnerabilities in lz4 - multiple versions
CSCwt56737	nvm	Addition of the 'Unknown' interface state for interface records on NVM-XDR
CSCwt59854	nvm	Sometimes NVM reports source IP as zero
CSCwt70392	nvm	Linux NVM XDR - "No Proxy discovered" by NVM GRPC
CSCwt95795	nvm	NVM-XDR Linux: Delta Fields support is not available
CSCwt97239	nvm	NVM Linux: Transition between On-Prem and NVM-XDR deployments (same version or upgrades) not supported

Identifier	Component	Headline
CSCws44549	opswat-ise	ENH: Support for Trend Micro Deep Security Agent definition check remediation
CSCwt11520	opswat-ise	OPSWAT support for Bitdefender Endpoint Security Tools Version 8.x
CSCwt62294	opswat-ise	Add support for Bitdefender Endpoint Security Tools Version 8.x for MAC OS
CSCws28139	posture-ise	Vulnerabilities in tinyxml-2 9.0.0
CSCwm82530	vpn	Secure Client TLS 1.3 Certificate Based Authentication Failure With Password Protected Certificate
CSCws81927	ztna	macOS: Datagrams from same UDP socket sent to alternate destinations are proxied to initial destination
CSCws81953	ztna	Windows: Initial datagrams from same UDP socket sent to alternate destinations are proxied to initial destination
CSCws97175	ztna	ZTA agent logging unknown_error_60 messages at high rate wth ZTA SIA and NVM enabled
CSCwt52137	ztna	macOS: ZTA enrollment failure with dual stack network
CSCwt69994	ztna	Windows: ZTA service status flap in loop
CSCwt71762	ztna	Null pointer exception when ZTA configuration and enrollment is set
CSCwt77254	ztna	macOS: ZTA proxied flow may target an FQDN resource not intended by the originating app
CSCwt81218	ztna	macOS: Chrome prompts user for local LAN access while accessing a SIA resource

Cisco Secure Client 5.1.16.194

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwq35829	core	Add Always-On support to management tunnel - Secure Client is leaking packets at transition from User Tunnel to Machine Tunnel
CSCws33523	core	AutoConnectOnStart ignores TND TrustedNetworkPolicy Disconnect Policy
CSCws93486	core	Windows: DPC_WATCHDOG_VIOLATION buckgeck in acsock64.sys with ZTA SIA and NVM XDR active
CSCwt20715	gui	Unable to change CSC GUI language macOS
CSCwt24392	vpn	macOS: DNS stops working with ZTA SIA-all and NVM active
CSCws36698	ztna	ZTA Agent timing out Duo requests following system resume
CSCwt10916	ztna	ZTA DNS rule evaluation does not match DNS query names with capital letters
CSCwt17265	ztna	ENH: Support CIDR rule intercept of name-based flows if SIA for all destinations is not configured
CSCwt24008	ztna	Windows: ZTA interceptor fails to initialize after reboot

Cisco Secure Client 5.1.15.287

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwn87687	core	VPN reconnect fails after switching between v4-v6 networks if head end device FQDN is only resolvable via hosts file
CSCwo37416	core	VPN Error: "The VPN Client is unable to configure private-side proxy settings."
CSCwo79290	core	SecureClient 5.1.8.122 does not reflect line breaks in banner
CSCwq35829	core	On support to management tunnel - Secure Client is leaking packets at transition from User Tunnel to Machine Tunnel
CSCws68569	core	ENH: GUI shows stale posture alert even after successful Duo posture reporting
CSCwn72005	nam	NAM shows no adapters available intermittently when random MAC is enabled on Surface 5/6 devices
CSCwr76978	nam	NAM should wait for smart card certificate enumeration before starting auth
CSCws44698	nvm	At times VPN interface marked as TRUSTED when its not
CSCws53547	nvm	Kernel Module Excessive Debug Logging Causes Storage Exhaustion on Linux Hosts
CSCws66616	nvm	NVM agent fails to terminate if stopped during KDF initialization retry loop
CSCws11411	opswat-ise	Inconsistency in definition check for Trend Micro Deep Security Agent AM
CSCws05316	posture-ise	Orphaned csc_iseposture processess causing high CPU usage on Windows

Identifier	Component	Headline
CSCwd13454	vpn	AC is not downloaded to endpoint on NSA flow with IPV6 DNS resolution
CSCwe74972	vpn	ERROR_UNEXPECTED errors logged while in trusted network with Always On FQDN exceptions configured
CSCwo80768	vpn	interface fails to re-enable on Win11-xx after restarting VPN service when Multihoming is enabled
CSCws04131	vpn	ASA/FTD - SAML: SSO logout failure on VPN disconnect with embedded browser based SAML authentication
CSCwr64930	ztna	ZTA TND probes may fail to reach trusted server with only AAAA FQDN in dual stack networks

Cisco Secure Client 5.1.14.145

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwm50768	core	Secure Client UI freezes when quitting the application on Windows
CSCws19101	core	[ui-cosmetic] no minimum size for columns in the stats screen which can result in hiding all stats
CSCws19124	core	[ui-cosmetic] stock Windows icon in the clear browser confirmation dialog
CSCws36722	core	ENH: Modifications to UI messages associated with Duo Desktop posture assessments and various system state conditions

Identifier	Component	Headline
CSCws12260	opswat-ise	Carbon Black Cloud Sensor 4.10+ not detected by ISE Posture
CSCwq97376	posture-ise	Iseagent crash during discovery
CSCwr86453	posture-ise	Secure Client Posture Module gets restarted when monitoring 3rd party sends Compliance report check
CSCws11636	posture-ise	Windows posture file check fails if file/folder permission is admin read-only
CSCws35955	posture-ise	ISE posture agent stuck in "Initializing" state
CSCwr26996	vpn	Secure Client erroneously adds I flag to local LAN route on VPN disconnect on macOS
CSCwr69007	vpn	AnyConnect Secure Client does not connect due to downloader failing when establishing user tunnel
CSCwr69040	vpn	AnyConnect is unable to connect user tunnel due to machine tunnel reconnecting
CSCwr01204	ztna	ZTA client IPC to the DHA message broker can cause IPC breakdown when Windows pipe send buffers become exhausted
CSCwr74822	ztna	ZTA Agent Enrollment failure due to DHA Posture Client send timeout on Windows Pipc IPC to DUO Trusted Peer Message Broker service
CSCwr90099	ztna	ZTA Certificate based enrollment fails to match certificate when chain certificates are only present in user store
CSCwr95996	ztna	Running iperf UDP over ZTA may may result in unexpected behaviors
CSCws02618	ztna	Ping from non-ZTA device to ZTA-enrolled device fails when on same network

Identifier	Component	Headline
CSCws19128	ztna	ZTA pause timer can be set past max value by manipulating system time
CSCws19140	ztna	Unable to pass ZTA data when QUIC is enabled
CSCws30211	ztna	Upgrading from a release affected by CSCws00283 fails since ZTA service cannot be terminated

Cisco Secure Client 5.1.13.177

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwq29714	core	Enhanced Captive Portal AnyConnect browser unexpectedly reappears when user is directed to "Use a browser" due to intervening profile migration
CCwr21200	core	macOS: Always On FQDN exclusion not enforced for addresses of CNAME resolved via HTTPS DNS query
CSCwr73269	core	Dataplane dynamic posture reporting (to handle stale posture alerts) stops working after a flurry of stale posture alerts arriving during system sleep
CSCwo88234	dart	DART should not email attach@cisco.com
CSCwr60532	dart	XDR Forensics Diagnostics Collection in DART for Mac and Win
CSCwr45253	download_install	Failed to launch downloader issue

Identifier	Component	Headline
CSCwf92550	nam	Cisco Secure Client for Windows NAM Denial of Service Vulnerability
CSCwr51136	nam	Memory Guard corrupts data when re-allocation size is not a multiple of 4 bytes.
CSCwr32812	nvm	Support for L7 metadata in NVM XDR
CSCwr56416	nvm	Memory Leak Affecting Pcgn (NGC_TAG_NVM_APP_FLOW)
CSCwq59674	opswat-ise	Day0-ISE Support need for PM 1450.2507.7012.0 in Win11-25H2
CSCwq72660	opswat-ise	Support to Cisco Secure endpoint ISE posture remediation
CSCwr04951	opswat-ise	Windows 11 PM 1450.2508.x support is missing on Aug'25 ISE_CM
CSCwr27343	posture-ise	Disk encryption check for external USB storage device on Windows and MacOS
CSCwo89666	profile editor	SBL Remains Enabled Regardless of Client Profile Configuration
CSCwr21575	umbrella	Windows: Umbrella DNS proxying fails when the primary DNS server is set to a loopback address
CSCwo89666	vpn	Remove UseStartBeforeLogon preference from VPN and VPN mgmt profiles
CSCwq15440	vpn	DNS queries fail for local domain when using full tunnel VPN on Linux
CSCwr56235	vpn	CSC acwebhelper.exe crashes due to Windows returning null pointer from CreateCoreWebView2Controller API call
CSCwr72705	vpn	CSC Linux Missing mdm-tlv=device-mac & device-public-mac Attributes

Identifier	Component	Headline
CSCvx19289	vpn	UDID values inside a Linux docker might be unique
CSCwq60310	vpn	Secure Client fails to start when FIPS is enabled on Linux ARM64
CSCwq27386	ztna	Windows: ZTA fails to intercept name-based flows when the local DNS server is set to loopback address
CSCws00283	ztna	Zero Trust Access module fails to start when trust bundle signing certificate has expired

Cisco Secure Client 5.1.12.146

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwp64727	opswat-ise	Anti-malware condition Sophos endpoint for Windows OS missing 2025.x
CSCwj43435	vpn	ENH: Enhance Captive Portal (CP) detection logic to interoperate with the various CP implementations
CSCwq74514	vpn	Ubuntu ARM64: NSS cert store not usable
CSCwq79833	ztna	Trigger posture reporting upon user login

Cisco Secure Client 5.1.11.388

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CCwh97991	core	ENH to add support for Linux ARM64 packages
CSCwj43989	core	Captive portal remediation GUI prompt easy to miss during agent/TND initiated connections
CSCwo56648	core	MacOS CSC "The VPN client agent was unable to establish monitoring of VPN profile files"
CSCwp25948	core	Secure Client SCEP enrollment fails due to message header case sensitivity
CSCvw76752	dart	ENH: Linux Anyconnect DART - collect WebKitGTK version from client machine
CSCwp13507	dart	Orbital Diagnostics Collection in DART for Mac and Win
CSCwq13530	dart	Windows: Codesign DART install state tool and system information powershell scripts
CSCwp50994	nvm	NVM.db file size is increasing rapidly beyond expected limits (up to 12 GB)
CSCwp65851	opswat-ise	Add the support on Sophos AM 2025.x for windows
CSCwq47294	opswat-ise	Posture Updates do not contain Windows Update Agent 1350.2506.29012.0
CSCwo67812	posture-ise	ISE 3.4 missing pr_Win10_64_Hotfixes compound condition
CSCwo43323	swg	SWG agent should enhance CP detection to use VPN's Network Environment State
CSCwo04010	umbrella	Vulnerabilities in libevent 2.0.21
CSCwo46950	vpn	After upgrading to Cisco Secure Client 5.1.8, the Start Before Logon (SBL) feature stopped working.

Identifier	Component	Headline
CSCwp19945	vpn	Limit the time taken by vpnagent to determine proxy
CSCwq10613	vpn	macOS 26 beta 2: IPv4 network access disrupted during the AnyConnect VPN session
CSCwq41884	vpn	VPN connections fail after toggling WiFi/wired off and on randomly
CSCwo86040	ztna	Windows ENH: Support intercept of UDP flows created before VPN module install/upgrade
CSCwp61090	ztna	macOS: DNS not working after resume from sleep with public DNS IP covered by ZTA steering rules

Cisco Secure Client 5.1.10.233

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwc82127	core	Linux: VPN traffic leak with full tunnel
CSCwk27900	core	RHEL 8.x/9.x Linux Secure Client installation failure with FIPS enabled
CSCwo00170	core	SC 5.1.7.80 no longer matches base FQDN in XML profile when manually entering group-url to connect
CSCwo25750	core	Windows: Umbrella SWG incompatible with Microsoft GSA
CSCwo13242	core	macOS: Kernel extension failover persists after CSC install
CSCwo32522	core	RAVPN SAML authentication does not work when using Firefox from the Microsoft Application Store

Identifier	Component	Headline
CSCwo38763	core	TND calls for connect but does not complete it; VPN API profile transmigration in progress
CSCwo45337	core	Always on suppress connection retries broken with Secure Client transmigration feature
CSCwp20128	core	NULL pointer dereference in the acsock64.sys kernel driver in Secure Client
CSCux44588	core	ENH: should only report every mismatched adapter name
CSCva24436	core	DART logs should include GW ipaddress when address is not reachable
CSCwn79758	dart	Misleading error message in CollectRegistries_result.txt after collecting DART
CSCwo08874	fireamp	Removing AMP Enabler from Cisco Secure Client Modules installed on macOS
CSCwo33446	gui	Downloader strings are not translated as part of ISE Posture UI improvements
CSCwn76440	nam	NAM GUI does not display correct log settings for IHV and filter driver after a power cycle
CSCwn81065	nam	Manage Networks., from "Network" tile misleading to Zero Trust Access instead of "Network" page
CSCwn84384	nam	Network Access Manager should be more robust when attempting to manage wireless interfaces
CSCwo00049	nam	Encryption key status "NONE" on statistics page
CSCwo01328	nam	Display "Location Services Needed" message only when NAM manages wireless adapters

Identifier	Component	Headline
CSCwo75993	nvm	NVM Tamper Protection on Windows ARM64 devices
CSCwo28302	opswat-ise	Add the support for Windows Avast Premium Security 25.1 & Avast macOS 16.0.0
CSCwo70857	opswat-ise	Osquery upgrade on Linux endpoint
CSCwo04101	posture-ise	Vulnerabilities in rpm 4.1.18.0 CVE-2021-35937
CSCwo75361	posture-ise	ISE posture logs truncate the policy and report if they exceed 4096 bytes
CSCwb86291	swg	Cisco Umbrella Secure Web Gateway filter bypass vulnerability
CSCwo53872	swg	Synchronization issue in SWG KDF code may prevent SWG from intercepting traffic
CSCwp64725	umbrella	Umbrella Module now reports the device serial number for display in the dashboard (Win, macOS)
CSCwp64751	umbrella	Released support for single stack IPv6 networks (Win, macOS)
CSCwp64761	umbrella	Improved network-switching experience by resolving an issue that caused clients to remain in customer trusted network mode during transitions (macOS)
CSCwc70093	vpn	ENH: Optimize tunnel security reinforcement on Linux upon virtual adapter detection
CSCwk64802	vpn	Trusted Network Detection is not case insensitive
CSCwo32975	vpn	macOS: IPv6 connections excluded by dynamic split tunneling timeout with Umbrella SWG active
CSCwo33424	vpn	Incorrect "Untrusted Certificate" pop up when primary VPN gateway in XML is unreachable

Identifier	Component	Headline
CSCwo46950	vpn	After upgrading to Cisco Secure Client 5.1.8, the Start Before Logon (SBL) feature stopped working
CSCwo75251	vpn	Upgrade fails ADVERTISE with Move_PluginReg_vpn_feedback custom action Cisco Secure Client
CSCwp13024	ztna	ZTA has two enrollments/configs with same entries with single ZTE choice file
CSCwp15625	ztna	Web access of private resources times out
CSCwp31165	ztna	ZTA TND/Network Fingerprint DNS domain not matching when letter case is different between config and interface
CSCwr05824	ztna	ENH: Ensure CIDR rules only match IP-based flows

Cisco Secure Client 5.1.9.113

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCvr52867	core	ENH: Support always-on Linux platforms
CSCwf64711	core	Windows multi-homing: cannot connect to split exclude target via secondary interface
CSCwi22704	core	Reconnect does not retry when IP address is present but DNS entry is not
CSCwn19905	core	macOS: VPN tunnel establishment fails (prior to default gateway MAC address provisioning)
CSCwn48390	core	Windows: revisit TCP flow redirect handling in KDF per MS guidelines

Identifier	Component	Headline
CSCwn57079	core	DNS queries sent to configured local DNS resolver instead of Umbrella resolver intermittently
CSCwn76322	core	macOS Intel: ZTA service fails to start upon reboot
CSCwi37344	dart	DART does not collect embedded browser crash dumps
CSCwo40094	download_install	Core module should not upgrade when VPN session is active
CSCwi64320	gui	Stop bringing the UI to foreground after installing and/or uninstalling the Cloud Management
CSCwn15672	nam	NAM support for WPA3 SAE transition disable
CSCwn50681	nam	NAM Enable Wireless in German is not translated well
CSCwn92068	nam	Fast authentication disabled upon smart card removal despite policy settings
CSCwn75887	nvm	Enhancement to exclude HTTP headers by default in Data Collection Policy (DCP)
CSCwn78412	nvm	Support for Linux Browser Plugins
CSCwn91660	nvm	Delay in export of records
CSCwn91729	nvm	Support for EVE records in NVM on-prem
CSCwn96702	nvm	SSIDs with UTF-8 characters not reported properly
CSCwm51430	opswat-ise	Windows Update Agent 1220.2407.15022.0 detected as 1218.2404.17012.0
CSCwn31640	opswat-ise	ISE 3.3 P4 / Trellix Endpoint Security 36.x is not listed under antimalware conditions
CSCwn38100	opswat-ise	Failure in definition check for Microsoft Defender ATP

Identifier	Component	Headline
CSCwn60361	opswat-ise	Add support for ESET Cyber Security version 8.x in MAC Compliance Module
CSCwn93231`	opswat-ise	For macOS Crowdstrike def details are not getting updated
CSCwn56255	posture-ise	Enhancement: VPN disconnection triggers posture "error" instead of "information"
CSCwn59485	posture-ise	Lockdown installer transform is not working for ISE Posture module
CSCwn75759	posture-ise	ISE Posture UI tile improvements - No loader and improved messages
CSCwe39164	swg	ENH: Add IPv4 link-local mapped IPv6 addresses in default exception list
CSCwm90941	swg	ENH: Add IPv4 mapped IPv6 address "::ffff.127.0.0.1" in the default exception list
CSCwf99520	umbrella	Umbrella - DNS state is "unprotected" and not getting back to protected state automatically
CSCwo42715	umbrella	Reduce time to protection on macOS
CSCwn10030	vpn	macOS IPv4 address incompatibilities with iOS hotspot and 464XLAT mobile carrier
CSCwo31872	vpn	Upgrade to Cisco Secure Client 5.1.8 removes VPN address from AnyConnect
CSCwo72082	vpn	Management tunnel ends up disconnected on underpowered client device
CSCwo05365	ztna	Vulnerabilities in nghttp2 1.57.0 CVE-2024-28182
CSCwo32685	ztna	ZTA wildcard steering rule causes synthetic NODATA DNS response on Windows

Identifier	Component	Headline
CSCwo75151	ztna	Fail to access resource when steering FQDN rule has capital letters
CSCwo76652	ztna	ZTA on macOS sometimes fails to detect enrollment after reboot - invalid local user status

Cisco Secure Client 5.1.8.122

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwo09395	gui	UI crashes when load balancer redirects to IP address and Secure Firewall Posture is configured
CSCwo16311	swg	Occasionally, SWG may unsuccessfully redirect a few connections due to incorrect rule match
CSCwo20036	swg	macOS: Changes in connection types (e.g. WiFi to wired) may affect SWG ability to intercept traffic
CSCwo22284	swg	macOS: Occasional KDF disruptions may prevent SWG from intercepting traffic consistently
CSCwo32464	ztna	Intermediate CA cert is deleted when ZTA renews its certificate - ZTA unable to auth to servers

Cisco Secure Client 5.1.8.105

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCvr52867	core	ENH: Support always-on on Linux platforms
CSCwk87458	core	Secure Client doesn't honor UseStartBeforeLogon preference
CSCwi05682	dart	DART should include a copy of the Windows registry in the support bundle by default
CSCwn39981	download_install	Linux: Uninstalling VPN rpm package causes system to hang/freeze
CSCwm89843	nam	Proper management of multiple Smart/SM cards
CSCwn00122	nam	Network Access Manager throws warning onWin 11 24H2 when users try to uninstall without allowing location access
CSCwn15404	nam	NAM wired adapter not available when localization service not enabled on Win11 24H2 and greater
CSCwn22005	nvm	NVM tagging feature for on-prem mode
CSCwn29101	nvm	Support for EVE records in NVM XDR
CSCwn81004	nvm	Support for reporting Windows SID by NVM in process data in XDR
CSCwm12254	opswat-ise	macOS 15.x build in Firewall 15.x enable remediation functionality is not working
CSCwn19567	opswat-ise	ISE Posture support for ESET NOD32 Antivirus 18.x version
CSCwn27942	opswat-ise	ISE Posture to support Kaspersky Plus version 25.x for macOS
CSCvp37180	posture-ise	ENH: Posture on macOS shows "System scan not required on current WiFi"

Identifier	Component	Headline
CSCwi98914	posture-ise	Usb cases are working as expected still system scan is giving noncompliant on Windows 10/11
CSCwn00897	posture-ise	OPSWAT v4Debug log collection without presence of v4Debug.dat
CSCwm66140	swg	Support for inclusion list in SWG
CSCwm99434	swg	Send SWG state change report to umbrella
CSCwm90948	umbrella	Umbrella module intermittently not intercepting DNS flows on Windows 11
CSCwo07105	umbrella	Fixed an issue that causes TCP connections to drop in certain rare instances (Windows)
CSCwo07118	umbrella	Fixed an issue with use of swg_use_kdf.flag (macOS)
CSCwi69392	vpn	Allow PPK credentials for multiple ASAs
CSCwm08025	vpn	IKEv2 Secure Client on Linux not using Cisco Fragmentation for all packet sizes
CSCwm14201	vpn	macOS ENH: Allow admin control over dynamic split tunnel handling of CNAME DNS responses

Cisco Secure Client 5.1.7.80

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwj04407	core	VPN profile not found when "https://" is used in HostName or HostAddress profile fields

Identifier	Component	Headline
CSCwm17973	core	When reconnecting, VPN is not considering switching IP protocols to contact IPv4+IPv6 ASA
CSCwm33282	core	Secure Client unable to connect with Linux Kernel 6.9
CSCwm42192	core	Cisco Secure Client sends encrypted traffic over Virtual Adapter
CSCwm67479	download_install	Cisco Secure Client Windows ARM64 pre-deploy package is missing ZTA module
CSCwh29444	nam	NAM sets adapter state to attached when initialization of the OS WLAN API fails
CSCwk17491	nam	NAM client may send MACsec packets out of order when throughput is high
CSCwm05134	nam	NAM does not work on Windows 11 24H2 without location permission for desktop apps enabled
CSCwm73916	nam	NAM group management cipher 0 not supported
CSCwk21228	nvm	macOS: VPN throughput significantly impacted with NVM flow collection active
CSCwk30374	nvm	Support for Tamper Protection for NVM-XDR on Windows
CSCwm44074	nvm	Support for reporting Process Tree Hierarchy for the flows reported by NVM
CSCwm60665	nvm	mTLS connection fails when there is no matching criteria configured
CSCwm78358	nvm	NVM agent needs to re-resolve the collector name upon handling KDF disruptions
CSCwm83412	nvm	NVM: acnvm crash seen on macOS 15.0 platform

Identifier	Component	Headline
CSCwm42511	opswat-ise	Need support for Firefox 130.x in ISE
CSCwh05294	posture-ise	Osquery Library to execute osqueries
CSCwi65268	posture-ise	ISE Posture - DISA Reporting
CSCwm45685	posture-ise	Application install check fails once after compliance module change on macOS
CSCwm80714	posture-ise	ISE Posture discovery fails on Windows 11 24H2 without location permission for desktop apps enabled
CSCwm26644	swg	Move to HTTP/1.1 from HTTP/1.0
CSCwm60952	swg	Set the SNI field when connecting to a customer trusted server
CSCwm92420	swg	Redirect rules were set during SWG backoff
CSCwm90933	umbrella	Secure Access text changes for SSE
CSCwm66922	vpn	Proxy settings are not being restored when system resumes from sleep

Cisco Secure Client 5.1.6.103

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCvz45813	core	ENH: Add a session ID to the AnyConnect logs in order to group series of related message exchanges
CSCwk81619	core	Cisco Secure Client embedded browser pops-up certificate selection prompt on SAML-based connections

Identifier	Component	Headline
CSCwm13153	core	When Windows display language set to simplified Chinese, CSC crashes
CSCwm41409	core	ISE / 'Check null is not found' when saving posture application condition for Kaspersky AV 17.x
CSCwk20887	dart	Dartcli execution or ISE Posture non-compliant state launches weird pop-ups if DUO app is missing
CSCwm03920	nam	Switch to machine connection upon smart card removal after user logoff
CSCwm56150	nvm	mDTLS (Mutual Authentication / Client Authentication for Network Visibility Module
CSCwk14000	opswat-ise	Cisco Secure Client 5.1.2.42: Compliance Module 4.3.4015.8192 : Trellix endpoint security 10.7
CSCwk19232	opswat-ise	Compliance Module 4.3.4015.8192 cannot detect Trellix Endpoint Security version 10.7.0
CSCwk45967	opswat-ise	Antimalware checks are not working on SUSE 12.5
CSCwk49217	opswat-ise	Latest Definition Date and Latest Definition Version fields blank for macOS
CSCwk74505	opswat-ise	Need support for Windows Update Agent 1219.x in Patch Management posture condition
CSCwk73054	opswat-ise	Sophos Endpoint Agent 2024 to be supported on AnyConnect Compliance Module
CSCwk86071	opswat-ise	MAC Compliance module support for XProtect version 5270
CSCwk90709	opswat-ise	SCCM check fails for standard users on Windows with CM 4.3.4114.8192
CSCwm35873	opswat-ise	Win 11 24H2- ISE support to be added for Windows Update Agent (1308.2408)

Identifier	Component	Headline
CSCwk89143	posture-ise	macOS 15: Secure Client ISE Agent crashes during gatekeeper built-in firewall remediation stage
CSCwk68967	swg	SWG does not detect TND on every network change
CSCwm66026	umbrella	Unprotected state when waking from sleep in certain circumstances
CSCwm54103	umbrella	Umbrella cloud update does not work with macOS using build 5.1.5.65
CSCwm66038	umbrella	SWG proxy URL to be intercepted by KDF in macOS (like Windows)
CSCwf94506	vpn	Cert matching criteria "Certificate Template Information" unavailable causing authentication failures
CSCwj04530	vpn	Captive Portal does not load in embedded browser on macOS in a specific scenario
CSCwj83190	vpn	Cert matching criteria "Certificate Template Information" unavailable causing authentication failure
CSCwm11696	web	Using client hints to differentiate between ARM and Intel packages during web-launch execution
CSCwk53066	ztna	ZTA Module not intercepting all queries from Edge browser

Cisco Secure Client 5.1.5.65

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwd61331	core	AnyConnect Always On AllowedHost using FQDN can result in connectivity failure

Identifier	Component	Headline
CSCwj60270	core	Always-On: add support for suppressing connection retry
CSCwk69124	core	Linux embedded browser stopped on 5xx and 4xx http response codes not allowing login
CSCwk89880	core	Windows: TCP packet with multiple DNS response payloads causes BSOD, with Network Visibility Module or Umbrella SWG active
CSCuw86771	dart	ENH: DART should provide option to upload .zip to service request
CSCwj50019	nam	Transition mode for WPA2/WPA3 personal networks no longer allows selection of WPA3
CSCwk12016	nvm	vpnagent tries to start another instance of Network Visibiliy Module agent when one is already running
CSCwk13032	nvm	NVM XDR: DART is not collecting the NVM Bootstrap profile information in Network Visibility Module logs for macOS
CSCwk40536	nvm	Sending browser plugins' data in Osquery data template
CSCwk45278	nvm	Support for reporting of Zero Trust Access intercepted flows by Network Visibility Module
CSCwf74451	opswat-ise	ISE Posture not accurately detecting FileVault state (On/Off) on M2 Macs
CSCwi79424	opswat-ise	ISE 3.1 Posture Module failing to report definition date for Trellix Endpoint Security for Windows
CSCwj44776	opswat-ise	macOS Sonoma 14.x with hard drives encrypted + FileVault are failing as disk posture condition
CSCwj50577	opswat-ise	AnyConnect Compliance Module can't uninstall Mozilla Firefox

Identifier	Component	Headline
CSCwj55259	opswat-ise	macOS needs support for XProtect version 2191.x
CSCwj96109	opswat-ise	Windows Update Agent 1217.x is not available
CSCwk04245	opswat-ise	Need support for Firefox 126.x in ISE
CSCwk27660	opswat-ise	ISE: Latest Windows Update Agent version 1218.x is not visible in patch management posture condition
CSCwj77424	posture-ise	Missing RTMGRP_LINK in netlink registration on Linux platform
CSCwj82165	posture-ise	ENH: To add cURL debug logs
CSCwk21434	posture-ise	ISE posture stuck when Trust Network Detection terminates a reconnecting VPN
CSCwk46435	posture-ise	Custom Registry reporting capacity similar to application and hardware conditions
CSCwh00386	swg	Browsing slowness is for 25 to 35 sec on macOS when Umbrella + PAC + AnyConnect VPN is running
CSCwj43288	swg	On macOS, SWG back off for noNetwork doesn't change the change the state
CSCwh49588	vpn	Cached certificate is used for authentication followed by SCEP enrollment
CSCwj40176	vpn	Secure Client AlwaysONVPN with ConnectFailurePolicy "Open" does not detect VPN gateway reachability
CSCwj44873	vpn	AnyConnect / Secure Client fails establishing IKEv2/IPsec VPN for first time post upgrade

Identifier	Component	Headline
CSCwk70323	vpn	macOS: Agent crashes when connecting ios devices for debugging
CSCwj48775	ztna	Add support for intercepting connect to IPv4-mapped IPv6
CSCwk08377	ztna	ZTA client not intercepting access to FQDN resource with a superset FQDN rule also configured

Cisco Secure Client 5.1.4.74

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwe48679	core	KDF DNS caching should support DNS requests over TCP
CSCwh56499	core	ENH: Allow the secure client to use a different language other than the local language of the device
CSCwi18018	core	Vulnerabilities in openssl 1.0.2q
CSCwi18072	core	Vulnerabilities in openssl 1.1.1n CVE-2023-4807 and others
CSCwi19138	core	Vulnerabilities in sqlite 3.35.5 CVE-2022-35737
CSCwi37591	core	Windows: SAML auth fails due to embedded browser control failure to set focus
CSCwi58881	core	Vulnerabilities in curl 7.64.0 CVE-2023-46218
CSCwi65764	core	Vulnerabilities in sqlite 3.1.1 CVE-2023-7104
CSCwi65779	core	Vulnerabilities in openssl 1.1.10 CVE-2023-5678

Identifier	Component	Headline
CSCwi66029	core	Vulnerabilities in curl - multiple versions CVE-2023-46219
CSCwj14505	core	Secure Endpoint "start" button display as Record in Japanese language
CSCwj19626	core	The VPN client is unable to configure private-side proxy settings
CSCwj58395	core	TNDv6 when moving to trusted: client spends long time reconnecting instead of applying TND policy
CSCwj58541	core	TND policy not applied with dual stack setup when profile host only resolvable to IPv6 address
CSCwj59856	core	macOS: Local LAN target not reachable after TND VPN disconnect
CSCwj83051	core	libwebkit2gtk-4.0 dependency causing embedded browser launch failure on Ubuntu 24.04
CSCwj83839	core	csc_zta_agent crashes when a private resource is being accessed after ZTA client cert is revoked
CSCwh29307	gui	CSC UI crashing during upgrade from headend due to toolbar PNG corruption
CSCwj34889	gui	Linux Secure Client GUI hangs when selecting or disconnecting SAML based tunnel group
CSCwj43486	gui	macOS CSC GUI app auto start not working reliably with 5.1.x
CSCwh37673	nam	Add NAM support for WPA3 GCMP256
CSCwj77457	nam	NAM cannot connect when PMF is optional and NIC does not support PMF
CSCwj80126	nvm	Day0: NVM installation is failing with latest kernel on ubuntu24.04

Identifier	Component	Headline
CSCwj81971	nvm	Network Visibility Module installation fails on latest Ubuntu22.04.4
CSCwk03480	nvm	HTTP host additionally capture HTTP method and target URL
CSCwk12148	nvm	Added support for link local flows
CSCwj53538	posture-ise	ISE Posture should handle space in Call Home List
CSCwj92612	posture-ise	Service unavailable: ISE Posture not working on non-English Windows OS + 5.1.3.62
CSCwk46435	posture-ise	Custom Registry reporting capability similar to application and hardware conditions
CSCwk09260	umbrella	punycode "xn--" found in mergelocaldomains file causing problems doing local domain resolution
CSCwe06920	vpn	Proxy cannot be changed by macOS users while using "do not modify" proxy setting
CSCwj48522	vpn	Cisco Secure Client for Windows Privilege Escalation Vulnerability
CSCwj88732	vpn	macOS: VPN connect fails when multiple split include networks match a local subnet
CSCwj68515	ztna	ZTA client not accepting configuration with underscore character in domain rule
CSCwj68647	ztna	Windows: ZTA client unable to intercept SMB flows initiated by name
CSCwk06167	ztna	Windows: ZTA service initialization fails with large number of NICs

Cisco Secure Client 5.1.3.62

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwh36395	core	Output of "vpncli.exe stats" doesn't give info of "notice: Connected to IP/FQDN"
CSCwh56499	core	ENH: Allow the Secure Client to use a different language other than the local language of the device
CSCwi37591	core	Windows: SAML auth fails due to embedded browser control failure to set focus
CSCwi66032	core	Vulnerabilities in libressl 3.4.2 CVE-2023-35784
CSCwi66040	core	Vulnerabilities in zlib 1.3 CVE-2023-45853
CSCwi69374	core	macOS: captive portal remediation not possible via AnyConnect browser with PAC file proxy settings
CSCwi69388	core	macOS: AnyConnect browser used only intermittently for captive portal remediation
CSCwi72260	core	macOS: "Too many open files" failures logged, VPN connections failing after a while
CSCwi75848	core	Client Profile Editor cannot be loaded when using the Cisco Secure Client image 5.1
CSCwi95666	core	macOS: VPN Agent unable to start when installing CSC 5.1 without a user logged in locally
CSCwj09644	core	Secure Client management tunnel fails to connect with socket error

Identifier	Component	Headline
CSCvu57988	dart	ENH: DART should include a copy of the windows registry in the support bundle
CSCvy66557	dart	ENH: DART for Windows should include the Device ID
CSCwe59992	download_install	SUSE 15.5: Vpndownloader is not working through web-deployment via ISE
CSCwi27071	gui	Secure Client 5 GUI.ico customization failure
CSCwj43486	gui	macOS CSC GUI app auto start not working reliably with 5.1.x
CSCwj85414	nam	Network Access Manager loses connection if a smartcard certificate is used and ISE is not properly configured
CSCwh82810	nvm	Start and intermediate flows are not reporting in Linux
CSCwi17719	nvm	Vulnerabilities in grpc - multiple versions
CSCwi17729	nvm	Vulnerabilities in c-ares - multiple versions
CSCwi49003	nvm	NVM is not reporting the Safari Browser Plugins for macOS
CSCwj27599	nvm	CLI proxy support for NVM XDR on Windows
CSCwh57757	opswat-ise	ENH: Support for IBM BigFix Client 11.x for macOS
CSCwh82964	opswat-ise	ENH: ISE Posture support for Heimdal Thor Agent 3.x
CSCwi96966	opswat-ise	Installation check failure for Trellix Endpoint Security for Linux Threat Prevention
CSCwj05825	opswat-ise	ISE Posture is not detecting Kaspersky Endpoint Security 11.x with CM 4.3.3765.8192

Identifier	Component	Headline
CSCwh96305	posture-ise	ISE Posture intermittently throws "internal system error"
CSCwj02135	posture-ise	[wireless] ISEposture goes to Service Unavailable on SUSE clients
CSCwb40977	swg	Decoupling SWG from URC
CSCwj24659	umbrella	File and Product version for UmbrellaDiagnostic application needs to be updated
CSCwf21427	vpn	Management tunnel connection fails if user tunnel profile has Always On enabled with FQDN exceptions
CSCwf98780	vpn	macOS: Xcode 15 device discovery not working with IPv6 tunnel-all VPN
CSCwi70170	vpn	AnyConnect on Linux: VPN cannot be established after updating libxml2 to version 2.12
CSCwj48522	vpn	Cisco Secure client CODE EXECUTION IN CISCO SECURE CLIENT WITH NAM

Cisco Secure Client 5.1.2.42

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwf21453	core	RetainVpnOnLogoff errors when attempting to validate proxy settings
CSCwh73937	core	ENH: macOS AnyConnect to support Dynamic Split Exclusions based on CNAME DNS responses
CSCwi07144	core	Vulnerabilities in zlib - multiple versions

Identifier	Component	Headline
CSCwi78167	core	Wildcard support to load balancing servers for AO configuration
CSCwi27062	nam	NAM unable to connect to Eero mesh APs
CSCwi27137	nam	NAM does not recognize default PMF IGTK cipher
CSCwi38780	nam	NAM does not complete connection for fast transition wireless network with PMF enabled
CSCwi48979	nvm	NVM HTTP Host support for macOS client
CSCwi49003	nvm	NVM is not reporting the Safari Browser Plugins for macOS
CSCwi50185	posture-ise	ISE Posture: PSN discovery failure
CSCwh29292	vpn	ENH: Allow DSI and DSE configuration together along with static split exclude
CSCwi17408	vpn	ENH: Allow bypassing proxy access hardening for split tunneling via group policy setting
CSCwi33431	vpn	Multiple ZTA versions show as installed after predeploy/webdeploy upgrades

Cisco Secure Client 5.1.1.42

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwf67833	core	(Windows only) - Error: The VPN client is unable to configure private-side proxy settings
CSCwh57935	core	AnyConnect launches the client downloader pop-up outside of core update

Identifier	Component	Headline
CSCwh96410	core	Vulnerabilities in curl - multiple versions
CSCwi20597	core	macOS 14.2 - VPN Agent not started after installation
CSCwi28687	core	Vpnagentd crashes with authenticating proxy on macOS
CSCwf92159	gui	CSC UI crashing after upgrade when the client profile has Automatic Server Selection enabled
CSCwh35676	nvm	ENH: Show the original NVM process and destination host when AnyConnect/Secure Client + SWG are active
CSCwi03257	posture-ise	ISE Posture IPC on macOS breaks when Symantec WSS is connected, leading to posture failure
CSCwe35649	vpn	macOS 13.2: Split include tunneling not working when only enabled for one IP protocol
CSCwe49687	vpn	macOS 12&13: Delay before CP remediation possible, AnyConnect browser not used
CSCwh51369	vpn	SBL not able to restore proxy settings during reconnect
CSCwh75976	vpn	Captive Portal is not loading in WebView2-based embedded browser after upgrade to v117.x
CSCwi24180	ztna	ZTA module continues intercepting traffic after unenrollment

Cisco Secure Client 5.1.0.136

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCvz45813	core	ENH: Add a session ID to the AnyConnect logs in order to group series of related message exchanges
CSCvu57988	dart	ENH: DART should include a copy of the Windows registry in the support bundle
CSCvy66557	dart	ENH: DART for Windows should include the Device ID
CSCvy66584	dart	ENH: DART for macOS should include MDM profiles
CSCvq05530	nam	ENH: NAM - Add support for Management Frame Protection (PMF)
CSCvz20268	opswat-ise	ENH: ISE Posture does not support Google Chrome version 89
CSCvz202709	opswat-ise	ENH: ISE Posture does not support Mozilla Firefox version 87
CSCwc20207	posture-ise	Apex One (MAC) Security Agent [Trend Micro] AM latest definition date/version is not reflected
CSCwd27667	posture-ise	Localization changes on Linux
CSCwd49714	posture-ise	Translation did not occur in Win, Lin NSA package
CSCwd52815	posture-ise	Translation did not occur in MAC NSA package
CSCwd81612	profile-editor	Unable to save NAM profile when SSI is UNICODE character in PE

Secure Firewall Posture (Formerly HostScan) 5.1.20.333

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwu55450	opswat-asa	ENH: Secure Firewall Posture should support latest version of Trend Micro Security
CSCww16909	opswat-asa	macOS: Secure Firewall Posture spikes high CPU when running on macOS 15 and macOS 26
CSCwv38503	posture-asa	ENH: Secure Firewall Posture support for macOS built-in firewall 27.x

Secure Firewall Posture (Formerly HostScan) 5.1.19.1862

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwj96798	posture-asa	Ubuntu26: Secure Firewall Posture module installation fails due to libxml2 dependency error
CSCwn43821	posture-asa	Exclude Poly1305 cipher from proposed cipher list with Secure Firewall Posture
CSCwu67940	posture-asa	Ubuntu26: Secure Firewall Posture module installation fails due to libxml2 dependency error
CSCwv02626	posture-asa	Ubuntu26: Secure Firewall Posture module installation fails due to libxml2 dependency error

Secure Firewall Posture (Formerly HostScan) 5.1.18.314

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwt75634	posture-asa	Secure Firewall Posture process is not terminated after VPN session is disconnected towards Secure Connect headends
CSCwu34187	posture-asa	Secure Firewall Posture enable check fails for Crowdstrike Falcon (Mac) after upgrade to 5.1.14+

Secure Firewall Posture (Formerly HostScan) 5.1.17.3382

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwi959009	opswat-asa	Vulnerabilities in openssl 3.2.0

Secure Firewall Posture (Formerly HostScan) 5.1.16.194

Secure Firewall Posture 5.1.16.194 includes updated OPSWAT engine versions for Windows, macOS, and Linux. Refer to the Secure Firewall Posture Support Charts under Release and Compatibility for additional information.

Secure Firewall Posture (Formerly HostScan) 5.1.15.287

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwr72522	posture-asa	Pen test result found .js files for webvpn where the comments in the code are descriptive

Secure Firewall Posture (Formerly HostScan) 5.1.15.287

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwr72522	posture-asa	Pen test result found .js files for webvpn where the comments in the code are descriptive

Secure Firewall Posture (Formerly HostScan) 5.1.14.145

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCws21678	posture-asa	Zombie processes created by cscan during Secure Firewall Posture operations on macOS

Secure Firewall Posture (Formerly HostScan) 5.1.13.177

Secure Firewall Posture 5.1.13.177 includes updated OPSWAT engine versions for Windows, macOS, and Linux. Refer to the Secure Firewall Posture Support Charts under Release and Compatibility for additional information.

Secure Firewall Posture (Formerly HostScan) 5.1.12.146

Secure Firewall Posture 5.1.12.146 includes updated OPSWAT engine versions for Windows, macOS, and Linux. Refer to the Secure Firewall Posture Support Charts under Release and Compatibility for additional information.

Secure Firewall Posture (Formerly HostScan) 5.1.11.388

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwp62950	posture-asa	ENH: Secure Firewall Posture Linux-arm64 support
CSCwp95367	posture-asa	Built osquery for Linux ARM64 by applying a Cisco patch that supports multipleosqueries and modifies the output format to match with linux x86_64
CSCwq03080	posture-asa	Process checks fail on macOS when Secure Firewall Posture is not pre-installed

Secure Firewall Posture (Formerly HostScan) 5.1.10.295

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwq21355	posture-asa	Incorrect version of Secure Firewall Posture is shown in ASDM

Secure Firewall Posture (Formerly HostScan) 5.1.10.233

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwm83734	opswat-asa	Mac 15: Firewall remediation is failing when SPF upgrade from 5.1.5.65 to 5.1.6.108 on first attempt
CSCwe68232	posture-asa	Secure Client fails SSL handshake with FTD when Secure Firewall Posture and FIPS are enabled

Identifier	Component	Headline
CSCwi65900	posture-asa	An issue in the component luaG_runerror of Lua v5.4.4 and below lead ...
CSCwi65901	posture-asa	singlevar in lparser.c in Lua from (including) 5.4.0 up to (excludin ...
CSCwo59154	posture-asa	Enabling FIPS in Secure Firewall Posture
CSCwo70044	posture-asa	Aggregate privilege ipc calls for firewall checks for Secure Firewall Posture

Secure Firewall Posture (Formerly HostScan) 5.1.9.113

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwn92980	opswat-asa	ENH: Windows Firewall not detected when Management tunnel has connection
CSCwo64644	opswat-asa	ENH: Secure Firewall Posture ver 5.1.x and above support Cortex v8.7
CSCwn90612	posture-asa	Aggregate all priv calls for process check

Secure Firewall Posture (Formerly HostScan) 5.1.8.105

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwk54713	posture-asa	Posture-enabled connection fails due to "slow network" immediately after attempting to connect
CSCwn35616	posture-asa	Enhancement for Secure Firewall Posture to support pure IPv6

Secure Firewall Posture (Formerly HostScan) 5.1.7.80

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwm64103	opswat-asa	Firewall force disable is not working and for fw force enable/disable is showing wrong state in DAP
CSCwk38880	posture-asa	Secure Firewall Posture fails to read data.xml file on Fedora 40, which has libxml v2.12

Secure Firewall Posture (Formerly HostScan) 5.1.6.108

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwm61544	opswat-asa	Secure Firewall Posture detects macOS Firewall as enabled while it is disabled

Secure Firewall Posture (Formerly HostScan) 5.1.6.103

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwc15558	posture-asa	ENH: HostScan to detect unencrypted volumes
CSCwf14818	posture-asa	ENH: HostScan should scan certificates in new NSS DB store on Linux
CSCSwj10295	posture-asa	Disk encryption posture failed to detect FileVault status on macOS (T2/M1chip)

Secure Firewall Posture (Formerly HostScan) 5.1.5.65

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwa10316	opswat-asa	ENH: OPSWAT to verify AntiMalware's last update without having internet access
CSCwj58803	opswat-asa	HostScan slow with Crowdstrike Falcon installed on macOS
CSCwk21134	opswat-asa	HostScan firewall and active scan cause unexpected delays when SentinelOne is installed in macOS
CSCwj05606	posture-asa	ASDM UI to Skip internet check for EDR products before VPN is active

Secure Firewall Posture (Formerly HostScan) 5.1.4.74

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwj60799	opswat-asa	OPSWAT is returning older definition detail for Microsoft Defender ATP
CSCwh87840	posture-asa	ENH: Add support for Shift JIS encoded Windows username
CSCwi57168	posture-asa	Secure Client - HostScan logging issue
CSCwi92616	posture-asa	Vulnerabilities in openssl 1.1.1t CVE-2024-0727

Secure Firewall Posture (Formerly HostScan) 5.1.3.62

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwj15421	opswat-asa	HostScan: Windows Firewall state detection not working if registry key is modified by MDM
CSCwj60799	opswat-asa	OPSWAT is returning older definition details for Microsoft Defender ATP

Secure Firewall Posture (Formerly HostScan) 5.1.2.42

Secure Firewall Posture 5.1.2.42 includes updated OPSWAT engine versions for Windows, macOS, and Linux. Refer to the Secure Firewall Posture Support Charts under Release and Compatibility for additional information.

Secure Firewall Posture (Formerly HostScan) 5.1.1.42

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwh71692	posture-asa	HostScan: Periodic polling adding extra header on every 60 second assessment

Secure Firewall Posture (Formerly HostScan) 5.1.0.136

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats 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.

Resolved

Identifier	Component	Headline
CSCwd44206	opswat-asa	HostScan: firealld prompts for system credentials after upgrade to HostScan version 4.10.05111

Related Documentation

For additional information on Secure Firewall ASA and Secure Client compatibility, see Supported VPN Platforms, Cisco Secure Firewall ASA Series or Release Notes for Cisco ASA Series.

© 2026 Cisco Systems, Inc. All rights reserved.