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

First Published: 2023-07-27

Last Modified: 2024-08-14

Release Notes for Cisco Secure Client , Release 5.0

Download the Latest Version of Cisco Secure Client

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
macOS	cisco-secure-client-macos-*version*-webdeploy-k9.pkg

OS	Cisco Secure Client Web-Deploy Package Names
Linux (64-bit)*	cisco-secure-client-linux64-*version*-webdeploy-k9.pkg

* Web deployment for RPM&DEB installation is not currently supported.

Cisco Secure Client Package Filenames for Predeployment

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

*Modules provided with RPM and DEB installers: VPN, DART

Other files, which help you add additional features to Cisco Secure Client, can also be downloaded.

Cisco Secure Client 5.0.05040 New Features

This maintenance release includes the following features and resolves the defects described in Cisco Secure Client 5.0.05040, on page 35:

- Addition of Cisco Secure Client ThousandEyes Endpoint Agent Module for macOS—A ThousandEyes macOS installer is now available in the predeploy package: Cisco Secure Client - ThousandEyes Endpoint Agent-x64-<vers>.pkg. Additions have also been made to the DART logs for the ThousandEyes Endpoint Agent Module. Refer to the Thousand Eyes Integration in the *Cisco Secure Client Administrator Guide* for additional details. Refer to the Cisco Secure Client - ThousandEyes Endpoint Agent Module Integration Guide for detailed information on how to collect network- and application-layer performance data when users access specific websites from within monitored networks.
- Addition of collection parameters for the Network Visibility Module around timestamps, Secure Endpoint IDs, and process flows.
- (CSCwf96510) An enhancement which automatically creates a DART bundle in Secure Firewall Posture (Formerly HostScan) when an error occurs in the OPSWAT module

Cisco Secure Client 5.0.04032 New Features

This maintenance release includes the following features and support updates and resolves the defects described in Cisco Secure Client 5.0.04032, on page 36:

- Introduction of Cisco Secure Client ThousandEyes Endpoint Agent Module—We now offer a ThousandEyes Windows installer (.msi) in the predeploy package. Upon installation, Secure Client can detect the installation of the ThousandEyes Module and displays the version in the About box, although

no UI tile is present. This integration enhances a customers' ability to get a complete picture of their application health, allowing them to make better-informed decisions and to resolve issues quicker. Refer to the Thousand Eyes Integration in the *Cisco Secure Client Administrator Guide* for additional details. Refer to the Cisco Secure Client - ThousandEyes Endpoint Agent Module Integration Guide for detailed information on how to collect network- and application-layer performance data when users access specific websites from within monitored networks.

- Integration with Secure Cloud Analytics (Windows Only)—Network Visibility Module data can now additionally be viewed in the NVM Flow tab of Secure Cloud Analytics. With its default deployment and profile, Network Visibility Module sends its data to the Cisco XDR. Refer to the Network Visibility Module in Cisco XDR for additional information. Their documentation is available here.
- ISE Posture for ARM64 Windows 10 and 11—(Both web deploy from ISE NSA and predeploy packages on Windows ARM64 endpoints) ISE can perform posture checks to verify compliance status before giving those endpoints access to the network. USB remediation is unsupported. The detailed support levels are as follows:
  - Built-in[Microsoft Windows Defender] Antimalware detection and remediation
  - Built-in[Microsoft Windows Firewall] detection and remediation
  - Built-in[Microsoft Bit-locker Drive Encryption] Disk Encryption detection
  - Built-in[Microsoft Windows Update Agent] Patch management detection and up-to-date enable checks
  - Standard Application visibility and monitoring
  - Hardware visibility and external drive detection
  - Non-OPSWAT posture assessments like Services/Registry key checks/Application by Process Name/File Detection and Script Condition/Remediation checks are supported.
  - Pre-deployment of Cisco Secure Client 5.0MR1 ARM64 bit ISE Posture and Compliance Modules are supported
  - Uninstallation of Cisco Secure Client/Compliance Module supported
- SWG logging enhancements. Refer to SWG Debug Logging in the *Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5*.

Cisco Secure Client 5.0.03076 New Features

This is a Cisco Secure Client maintenance release that resolves a defect found in Windows (Intel) only. The defect is specific to Network Access Manager, which is a Windows only feature. Refer to Cisco Secure Client 5.0.03076, on page 37 for details on the resolved caveat, which is not applicable to macOS and Linux users.

Cisco Secure Client 5.0.03072 New Features

This is a maintenance release that includes the following features and support updates, and that resolves the defects described in Cisco Secure Client 5.0.03072, on page 37:

- Specific accessibility changes—We addressed specific Voluntary Product Accessibility Template (VPAT) compliance standards to benefit those who are disadvantaged and to drive productivity through digital transformation:
  - High contrast themes, which fixed invisible hyperlinks in the About dialog and tile title
  - Minimum contrast ratio, which increased contrast by adjusting the text colors of the tile submenu and DART menu description
  - Keyboard navigation with Windows common shortcut keys (Tab, Enter, Spacebar)
  - Navigation and selection of Advanced Window with Menu buttons(using Up/Down and Left/Right arrow keys)
  - Keyboard access to Preference/About/DART windows from the Advanced Window
  - Keyboard navigation with PgUp/PgDn to expand/collapse the statistics group
  - Navigation and selection focus visibility for DART and Cisco Secure Client UIs
  - Mismatch between screen reader of log settings and JAWS announcement was adjusted
  - Mismatch between screen reader of DART encryption menu and JAWS announcement was adjusted
  - Appropriate JAWS announcement for label in name
- Dual-Home Detection (for Linux)—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.

  The following limitations are known for dual-home detection (both Linux and macOS) and are currently being addressed:
  - CSCwf51800—Linux, macOS: "On a trusted network" UI msg missing after dual-home detection takes effect in some scenarios
  - CSCwf52884—Linux, macOS: Intermittent issues in Secure TND probing
  - CSCwf52878—Linux, macOS: Dual-home detection timing issue when network configuration is not available quickly enough
- Bypass Connect Upon VPN Session Timeout—Allows you to bypass the connection retry that automatically occurs if a VPN session times out, while either Trusted Network Policy or Untrusted Network Policy are set to connect. This checkbox is added to the VPN Profile Editor (Preferences Part 2).

Known Issue— (CSCwf63877) Trusted Network Detection is not functioning as expected on Red Hat 9.2 due to incorrect DNS server information from *NetworkManager* component on the operating system.

Cisco Secure Client 5.0.02075 New Features

This maintenance release includes the following features and support updates and resolves the defects described in Cisco Secure Client 5.0.02075, on page 40:

- **UseLocalProfileAsAlternative Custom Attribute**—If you want to distribute a profile out-of-band (using SCCM, MDM, SecureX Cloud Management, or the like) without configuring a Cisco Secure Client Profile (previously known as an AnyConnect profile) on the Secure Firewall ASA, you can use the *UseLocalProfileAsAlternative* custom attribute. When you configure this custom attribute, the client uses the local (on disk) Cisco Secure Client profile for its settings and preferences (rather than the usual defaults). Refer to Predeploying Cisco Secure Client in the administration guide for additional information. Additionally, refer to Configure Secure Client Custom Attributes in an Internal Group Policy for configuration procedures required in ASDM version 7.19 (or later). The Secure Client Custom Attributes section in the *Cisco Secure Firewall ASA Series VPN ASDM Configuration Guide* provides the type and named value for this custom attribute and others.
- **Disable EDR Internet Check**—An ISE Posture Profile Editor option to skip the real-time transfer protocol check, and the definition check of the endpoint and detection response (EDR). If you have EDR products installed, you can use this option during system scan to perform an internet check.
- **Dual-Home Detection (macOS Only)**—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.
- ARM64 support for the Umbrella Module.
- WPA3 Enhanced Open (OWE) and WPA3 Personal (SAE) support added to Network Access Manager.

Known Issue

(CSCwe92223) Windows arm64: SplitDNSV6 tests showing stray DNS queries in pcap outside tunnel

Cisco Secure Client 5.0.01242 New Features

This maintenance release includes the following features and support updates and resolves the defects described in Cisco Secure Client 5.0.01242, on page 43:

- Basic Posture CLI for ISE Posture (CSCwc98263)—For Windows only, added posturecli.exe option so multiple clients can connect to the posture subsystem and send data, instead of just one client and one server communicating, which was all the UI process allowed.
- Support for TLS version 1.3 to encrypt VPN connections, with the following additional cipher suites: TLS_AES_128_GCM_SHA256 and TLS_AES_256_GCM_SHA384

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

DTLS 1.3 is not yet supported.

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

ISE Posture does not yet support TLS 1.3.

- Start Before Login support on Microsoft-supported versions of Windows 10 and Windows 11 for ARM64-based PCs.
- Secure Client Fast User Switching—The GUI will function for multiple users logged into the same device at the same time. This Windows feature is supported only with a Secure Endpoint deployment without the deployment of the AnyConnect VPN module. A VPN deployment interrupts the capability of fast user switching.

Known Issues

CSCwd79171—The Network Access Module client may crash after saving a new configuration file and attempting to parse and validate the xml data of the configuration in the newConfigFiles directory. The administrator may not be aware because the service is configured to restart after a shutdown, and it could result in invalid memory access.

CSCwd68113— Secure Client VPN AAA authentication may fail with a "Login Failed" error, even though the correct username and password are entered. A reboot clears up the issue and allows authentication to work as expected.

Cisco Secure Client 5.0.00556 New Features

This release adds macOS and Linux support to Cisco Secure Client (including AnyConnect), which initially only released with Windows support. It includes the following features and support updates and resolves the defects described in Cisco Secure Client 5.0.00556, on page 46:

- Fixed the known issue of a VPN connection attempt hanging following a post-authentication connection failure (CSCwc56173)
- Linux requirement changes—systemd and libsystemd are now a required package for Linux
- Support for Red Hat 9.0

The following bulleted list highlights key support, naming, and functionality changes that are different from the Cisco AnyConnect Secure Mobility Client 4.x releases. In release 5, Cisco AnyConnect Secure Mobility Client has been renamed to Cisco Secure Client (including AnyConnect).

- Although Network Access Manager is part of Cisco Secure Client 5, the Network Access Manager Profile Editor within SecureX will not be available for release 5.
- AMP Enabler is for macOS only in Cisco Secure Client 5, as Cisco Secure Client for Windows offers full integration with Cisco Secure Endpoint, formerly AMP for Endpoints.
- Some AnyConnect modules also have new names in the Cisco Secure Client 5 release. HostScan (VPN Posture) will be changed to Secure Firewall Posture. In the ASDM UI, you will see it referenced as Posture (for Secure Firewall) in the Remote Access VPN windows. Similarly, the hostscan.pkg download from Cisco.com will be renamed as secure-firewall-posture-*version*-k9.pkg.
- You will notice references in the documentation and in the ASDM UI to AnyConnect. We currently do not intend to change those references to the new Cisco Secure Client name, although ASDM is fully supported to configure Cisco Secure Client 5 profiles. Secure Firewall ASA will be the new ASA name for version 9.18 and later.
- The ability of the Umbrella Roaming Security module to provide automatic updates for all installed AnyConnect modules with the Umbrella Cloud infrastructure has been removed for release 5.

- The Apex and Plus licenses for AnyConnect have been changed to Premier and Advantage licenses for Cisco Secure Client.

Cisco Secure Client 5.0.00529 New Features

This is a major release that includes the following features and support updates, and that resolves the defects described in Cisco Secure Client 5.0.00529, on page 47:

- The initial Cisco Secure Client (including AnyConnect) release 5 is only available for Windows. Although you will find references in the documentation to Cisco Secure Client for macOS and Linux as well, that functionality is not applicable in this initial release. If you are running on macOS or Linux, refer to the AnyConnect 4.x release documentation until Cisco Secure Client is officially released on that platform. Android and iOS have already had a 5.0 release.
- Default localization files for various languages—With Cisco Secure Client installation, default localization files for various languages are included. The locale specified on your device determines the displayed language. Cisco Secure Client uses the language specification, then the region specification, to determine the best match.
- OpenJDK use with profile editor—If you use Oracle Java 8 or higher, you can launch the profile editor without any additional prompt for JRE locations. If you use OpenJDK/JRE (Java 8 or higher), you might be prompted for the JRE path. Some OpenJDK variants require you to manually specify the JRE/JDK path one time upon reinstallation or upgrade of the profile editor.
- ActiveX controls have been removed in Cisco Secure Client, as well as Secure Firewall Posture.

The following bulleted list highlights key support, naming, and functionality changes that are different from the Cisco AnyConnect Secure Mobility Client 4.x releases. In release 5, Cisco AnyConnect Secure Mobility Client has been renamed to Cisco Secure Client (including AnyConnect).

- Although Network Access Manager is part of Cisco Secure Client 5, the Network Access Manager Profile Editor within SecureX will not be available for release 5.
- AMP Enabler is for macOS only in Cisco Secure Client 5, as Cisco Secure Client for Windows offers full integration with Cisco Secure Endpoint, formerly AMP for Endpoints.
- Some AnyConnect modules also have new names in the Cisco Secure Client 5 release. HostScan (VPN Posture) will be changed to Secure Firewall Posture. In the ASDM UI, you will see it referenced as Posture (for Secure Firewall) in the Remote Access VPN windows. Similarly, the hostscan.pkg download from Cisco.com will be renamed as secure-firewall-posture-*version*-k9.pkg.
- You will notice references in the documentation and in the ASDM UI to AnyConnect. We currently do not intend to change those references to the new Cisco Secure Client name, although ASDM is fully supported to configure Cisco Secure Client 5 profiles. Secure Firewall ASA will be the new ASA name for version 9.18 and later.
- The ability of the Umbrella Roaming Security module to provide automatic updates for all installed AnyConnect modules with the Umbrella Cloud infrastructure has been removed for release 5.
- The Apex and Plus licenses for AnyConnect have been changed to Premier and Advantage licenses for Cisco Secure Client.

Known Issue

A VPN connection attempt may hang for up to 3 minutes after a previous post-authentication connection failure (CSCwc56173).

Secure Firewall Posture (Formerly HostScan) 5.0.05040 New Features

The Secure Firewall Posture (formerly HostScan) 5.0.05040 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in Secure Firewall Posture (Formerly HostScan) 5.0.05040, on page 47.

Secure Firewall Posture (Formerly HostScan) 5.0.04032 New Features

Secure Firewall Posture 5.0.04032 includes updated OPSWAT engine versions for Windows, macOS, and Linux and resolves the caveats listed in Secure Firewall Posture (Formerly HostScan) 5.0.04032, on page 48. Refer to the Secure Firewall Posture Support Charts under Release and Compatibility for additional information.

Secure Firewall Posture (Formerly HostScan) 5.0.03072 New Features

The Secure Firewall Posture (formerly HostScan) 5.0.03072 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in Secure Firewall Posture (Formerly HostScan) 5.0.03072, on page 48.

Secure Firewall Posture (Formerly HostScan) 5.0.02075 New Features

The Secure Firewall Posture (formerly HostScan) 5.0.02075 release includes the following feature and resolves the defects provided Secure Firewall Posture (Formerly HostScan) 5.0.02075, on page 49.

Secure Firewall Disk Encryption—Ability to report disk encryption products installed on the endpoint as part of the Secure Firewall Posture (formerly HostScan) feature. The additional checkbox is added to Advanced Endpoint Asssessment on ASDM under Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Settings > Configure.

Secure Firewall Posture (Formerly HostScan) 5.0.01242 New Features

The Secure Firewall Posture, formerly HostScan, 5.0.01242 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects provided Secure Firewall Posture (Formerly HostScan) 5.0.01242, on page 49.

Secure Firewall Posture (Formerly HostScan) 5.0.00556 New Features

The Secure Firewall Posture, formerly HostScan, 5.0.00556 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

Secure Firewall Posture (Formerly HostScan) 5.0.00529 New Features

The Secure Firewall Posture, formerly HostScan, 5.0.00529 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

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.

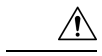
- You must upgrade to ASDM 7.10.1 to use management VPN tunnel.
- You must upgrade to ASDM 7.5.1 to use Network Visibility Module.
- You must upgrade to ASDM 7.4.2 to use AMP Enabler.

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.

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	Thousand Eyes Endpoint Agent	Zero Trust Access Module
Windows 11 (64-bit) and current Microsoft supported versions of Windows 10 x86 (32-bit) and x64 (64-bit)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Microsoft-supported versions of Windows 10 and Windows 11 for ARM64-based PCs	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No

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	Thousand Eyes Endpoint Agent	Zero Trust Access Module
macOS 14 Sonoma, macOS 13 Ventura, macOS 12 Monterey, and macOS 11 Big Sur	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	macOS 10.10 and later	Yes

Table 3: Linux

Linux Versions	VPN	Secure Firewall Posture	Network Visibility Module	ISE Posture	DART	Customer Experience Feedback
Red Hat 9.x and 8.x	Yes	Yes	Yes	9.x and 8.1 (and later)	Yes	Yes
Ubuntu 24.04, 22.04, and 20.04	Yes	Yes	Yes	Yes	Yes	Yes
SUSE supported versions of SLES 15 and 12	Limited support. Used only to install ISE Posture	No	No	Yes	Yes	Yes

Cisco Secure Client Support for Microsoft Windows

Windows Requirements

- Pentium class processor or greater.
- 100 MB hard disk space.
- 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.
- Cisco Secure Client is not supported on Windows RT. There are no APIs provided in the operating system to implement this functionality. Cisco has an open request with Microsoft on this topic. Those who want this functionality should contact Microsoft to express their interest.
- 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

- Using VPN CLI without GUI sessions (for example SSH) is not supported
- Administrator privileges are required for installation
- x86 instruction set
- 64-bit processor
- 100 MB hard disk space
- 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
- 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

Cisco Secure Client Support for macOS

macOS Requirements

- Cisco Secure Client requires 50MB of hard disk space.
- 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.

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.
- SecureX Cloud Management—You can click the **Network Installer** button on the Deployment Management pages of the SecureX UI. It results in the downloading of the installer executable. The Secure Client options that you want to enable (such as Start Before Login, Diagnostics and Reporting Tool, Secure Firewall Posture, Network Visibility Module, Secure Umbrella, ISE Posture, and Network Access Manager) can also be selected.

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.

Web-based Installation May Fail on 64-bit Windows

This issue applies to Internet Explorer versions 10 and 11, on Windows 10 (and later).

When the Windows registry entry HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth is set to 0, Active X has problems during Cisco Secure Client web deployment.

See http://support.microsoft.com/kb/2716529 for more information.

The solution to is to:

- Run a 32-bit version of Internet Explorer.
- Edit the registry entry to a non-zero value, or remove that value from the registry.

Note On Windows 10 (and later), starting Internet Explorer from the Windows start screen runs the 64-bit version. Starting from the desktop runs the 32-bit version.

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

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.

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 requires user approval before they can function.

Encrypted DNS Impact and Mitigation

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

- 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.

VPN Headend DNS Load Balancing Not Supported

AnyConnect supports DNS load balancing using SAML authentication for an embedded browser. Using Secure Firewall ASA, Secure Firewall Threat Defense, or other headends and an external/native browser, VPN headend DNS load balancing is not supported due to operating system limitations, which restrict the ability for Cisco Secure Client to control the necessary underlying conditions.

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.

AnyConnect 4.10 Upgrade Failure on Linux (Only AnyConnect Versions Prior to 4.9.01095)

If you are using web deploy to upgrade to AnyConnect or HostScan 4.10 from a version prior to 4.9.01095, an error could result. Since AnyConnect versions prior to 4.9.01095 did not have the capacity to parse the system CA store, the result is an upgrade failure, because the correct NSS certificate store path could not be determined in the user's profile directory. If you are upgrading to AnyConnect 4.10 from a release prior to 4.9.01095, copy the root certificate (DigiCertAssuredIDRootCA.pem) to /opt/.cisco/certificates/ca prior to upgrading AnyConnect on the endpoint.

NVM Installation Fails With Ubuntu 20

If you are using Ubuntu 20.04 (which has kernel version 5.4), you must use AnyConnect 4.8 (or later), or Network Visibility Module installation fails.

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.

Web Deployment Workflow Limitations on Linux

Consider these two limitations when doing a web deployment on Linux:

- The Ubuntu NetworkManager Connectivity Checking functionality allows periodic testing, whether the internet can be accessed or not. Because Connectivity Checking has its own prompt, you can receive a network logon window if a network without internet connectivity is detected. To avoid such network prompts, that aren’t tied to a browser window and don't have download capability, you should disable Connectivity Checking in Ubuntu 17 and beyond. By disabling, the user will be able to download a file from the ISE portal using a browser for ISE-based Cisco Secure Client web deployment.
- Before doing a web deploy onto a Linux endpoint, you must disable access control with the xhost+ command. Xhost controls the access of a remote host running a terminal on the endpoint, which is restricted by default. Without disabling access control, Cisco Secure Client web deployment fails.

Client First Auto-Reconnect Unsuccessful After Upgrading to AnyConnect 4.9.01xxx (Linux Only)

With the fix of CSCvu65566 and its device ID computation change, certain deployments of Linux (particularly those that use LVM) experience a one-time connection attempt error immediately after updating from a headend to 4.9.01xxx or later. Linux users running AnyConnect 4.8 (and later) and connecting to a headend to perform an auto update (web-deploy) may receive this error: "The secure gateway has rejected the connection attempt. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication." To successfully connect, you can manually initiate another VPN connection after Cisco Secure Client upgrade. After an initial upgrade to 4.9.01xxx or later, you will no longer hit this issue.

Potential Issues Connecting to a Wireless Network After An Upgrade from AnyConnect 4.7MR4

The Network Access Manager made a revision to write wireless LAN profiles to disk rather than just using temporary profiles in memory. Microsoft requested this change to address an OS bug, but it resulted in a crash of the Wireless LAN Data Usage window and eventual intermittent wireless connectivity issues. To prevent

these issues, we reverted the Network Access Manager to using the original temporary WLAN profiles in memory. The Network Access Manager removes most of the wireless LAN profiles on disk when upgrading to version 4.8MR2 or later. Some hard profiles cannot be removed by the OS WLAN service when directed, but any remaining interfere with the ability for the Network Access Manager to connect to wireless networks. Follow these steps if you experience problems connecting to a wireless network after an upgrade from 4.7MR4 to 4.8MR2:

1. Stop the Secure Client Network Access Manager service.
2. From the administrator command prompt, enter

```
netsh wlan delete profile name=*(AC)
```

This removes leftover profiles from previous versions (Secure Client 4.7MR4 to 4.8MR2). Alternatively, you can look for profiles with **AC** appended to the name and delete them from the native supplicant.

Nslookup Command Needs macOS Fix To Work As Expected

macOS 11 fixed an issue seen in AnyConnect version 4.8.03036 (and later) related to the nslookup command, namely nslookup not sending DNS queries through the VPN tunnel with split-include tunneling configuration. The issue initiated in AnyConnect 4.8.03036 when that version included a fix for defect CSCvo18938. The Apple-suggested changes for that defect ended up revealing another OS issue, causing the nslookup problematic behavior.

As a workaround for macOS 10.x, you can pass the VPN DNS server as a parameter to nslookup: **`nslookup [name] [ip_dnsServer_vpn]`**.

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
```

Preparation for macOS 10.15 Users

The macOS 10.15 operating system does not support 32-bit binaries. Additionally, Apple verifies that all software installed on 10.15 has been cryptographically notarized via digital signature. From AnyConnect 4.8 and later, operation on macOS 10.15 is supported with no 32-bit code.

Make note of these limitations:

- AnyConnect versions prior to 4.7.03052 may require an active internet connection to upgrade.
- HostScan versions prior to 4.8.x will not function on macOS 10.15.
- Secure Firewall Posture and ISE Posture users on macOS 10.15 will experience permission popups during initial launch.

Secure Firewall Posture Will Not Function With macOS 10.15 Without Upgrade (CSCvq11813)

HostScan packages earlier than 4.8.x will not function with macOS Catalina (10.15). End users who attempt to connect from macOS Catalina to Secure Firewall ASA headends running HostScan packages earlier than 4.8.x will not be able to successfully complete VPN connections, receiving a posture assessment failed message.

AnyConnect 4.10.x clients on macOS Big Sur (11.x) must use HostScan 4.9.04045 or later.

To enable successful VPN connections for Secure Firewall Posture users, all DAP and Secure Firewall Posture policies must be HostScan 4.8.00175 (or later) compatible. Refer to AnyConnect HostScan Migration 4.3.x to 4.6.x and Later for additional information related to policy migration from HostScan 4.3.x to 4.8.x.

As a workaround to restore VPN connectivity, administrators of systems with Secure Firewall Posture packages on their Secure Firewall ASA headends may disable Secure Firewall Posture. If disabled, allSecure Firewall Posture posture functionality, and DAP policies that depend on endpoint information, will be unavailable.

The associated field notice can be found here: https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70445.html.

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.

Incompatibility with SentinelOne

Cisco Secure Client Umbrella module is incompatible with SentinelOne endpoint security software.

macOS Management Tunnel Disconnect After Upgrade to 4.8

If you encounter any of the following scenarios, it is related to security improvements to comply with Apple notarizations:

- You had management tunnel connectivity with AnyConnect 4.7, but the AnyConnect 4.8 version fails in the same environment.
- The VPN statistic window displays "Disconnect (Connect Failed)" as the management tunnel state.
- Console logs indicate "Certificate Validation Failure," signifying a management tunnel disconnect.

If configured to allow access (without prompting) to the Cisco Secure Client app or executables, ACLs must be reconfigured after upgrading to AnyConnect 4.8 (or later), by re-adding the app or executable. You must change the private key access in the system store of the keychain access to include the vpnagentd process:

1. Navigate to **System Keychain** > **System** > **My Certificates** > **Private key**.
2. Remove the vpnagentd process from the access control tab.
3. Add the current vpnagentd into the /opt/cisco/secureclient/bin folder.
4. Enter the password when prompted.
5. Quit Keychain Access and stop the VPN service.
6. Restart.

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.

Restored IPsec Connections in FIPS Mode (CSCvm87884)

AnyConnect releases 4.6.2 and 4.6.3 had IPsec connection issues. With the restoration of the IPsec connection (CSCvm87884) in AnyConnect release 4.7 (and later), Diffie-Hellman groups 2 and 5 in FIPS mode are no longer supported. Therefore, Cisco Secure Client in FIPS mode can no longer connect to Secure Firewall ASA prior to release 9.6 and with configuration dictating DH groups 2 or 5.

Changes with Certificate Store Database (NSS Library Updates) on Firefox58

(Only Impacting users using Firefox prior to 58) Due to the NSS certificate store DB format change starting with Firefox 58, Cisco Secure Client also made the change to use new certificate DB. If using Firefox version

prior to 58, set NSS_DEFAULT_DB_TYPE="sql" environment variable to 58 to ensure Firefox and Cisco Secure Client are accessing the same DB files.

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.

Cisco Secure Client macOS 10.13 (High Sierra) Compatibility

AnyConnect 4.5.02XXX and later has additional functionality and warnings to guide users through the steps needed to leverage complete capabilities, by enabling the Secure Client, formerly AnyConnect, software extension in their macOS Preferences -> Security & Privacy pane. The requirement to manually enable the software extension is a new operating system requirement in macOS 10.13 (High Sierra). Additionally, if Secure Client is upgraded before a user's system is upgraded to macOS 10.13 and later, the user will automatically have the Secure Client software extension enabled.

Users running macOS 10.13 (and later) with a version earlier than 4.5.02XXX must enable the Secure Client, formerly AnyConnect, software extension in their macOS Preferences -> Security & Privacy pane. You may need to manually reboot after enabling the extension.

As described in https://support.apple.com/en-gb/HT208019, macOS system administrators potentially have additional capabilities to disable User Approved Kernel Extension Loading, which would be effective with any currently supported version of Secure Client.

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.

Web Deploy of NAM, DART, ISE Posture, and/or Posture Fails with Signature/File Integrity Verification Error

A "timestamp signature and/or certificate could not be verified or is malformed" error only occurs on Windows during web deploy of AnyConnect 4.4MR2 (or later) from Secure Firewall ASA or ISE. Only the Network

Access Manager, DART, ISE Posture, and Posture modules that are deployed as MSI files are affected. Because of the use of SHA-2 timestamping certificate service, the most up-to-date trusted root certificates are required to properly validate the timestamp certificate chain. You will not have this issue with predeploy or an out-of-the-box Windows system configured to automatically update root certificates. However, if the automatic root certificate update setting has been disabled (not the default), refer to https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx or manually install the timestamping root certificates that we use. You can also use the signtool to verify if the issue is outside of Cisco Secure Client by running the

```
signtool.exe verify /v /all/debug/pa<file to verify>
```

command from a Microsoft provided Windows SDK.

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.

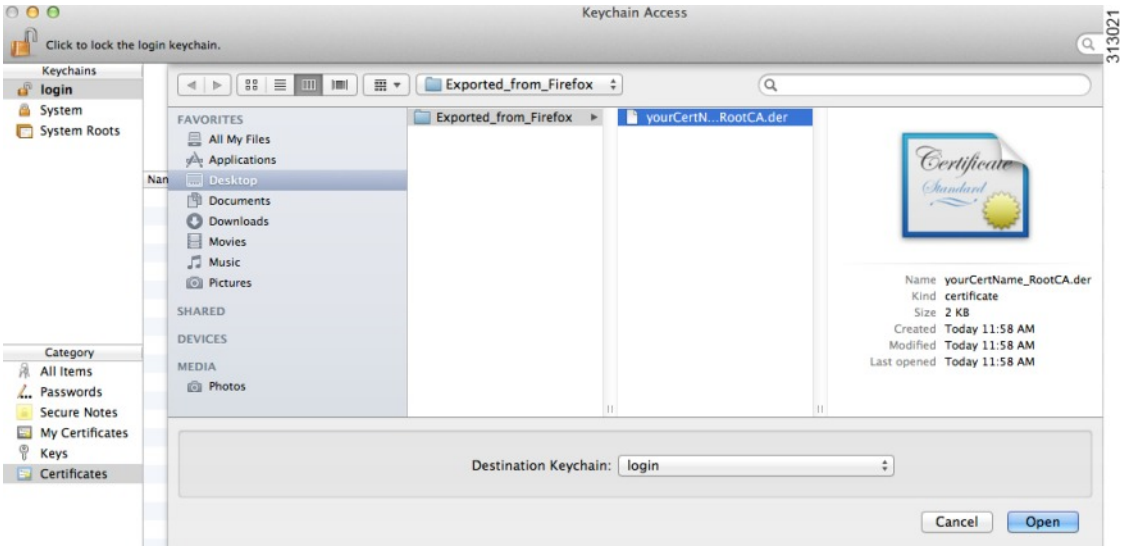
Firefox Certificate Store on macOS is Not Supported

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.

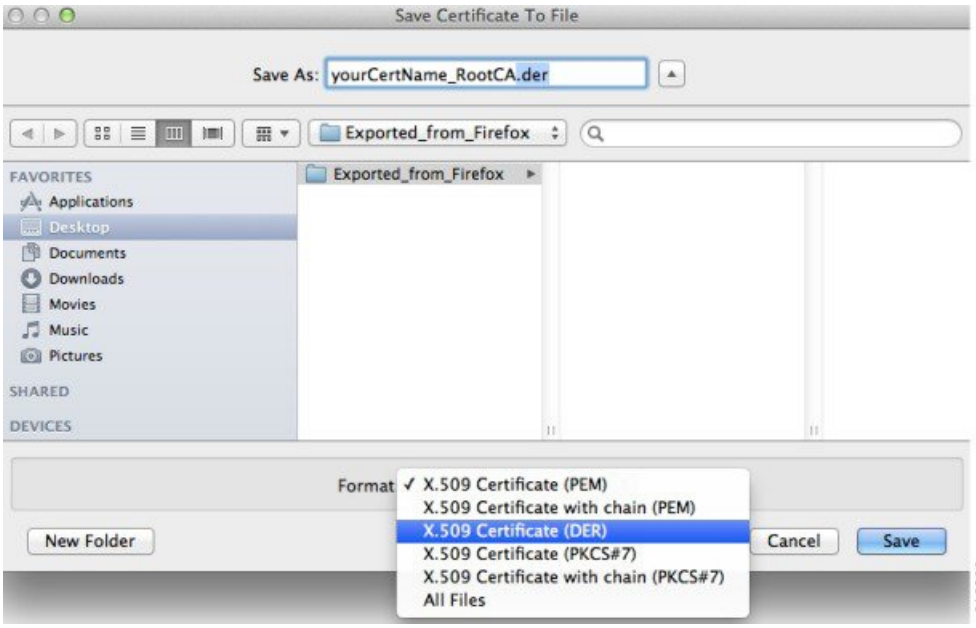


Note If more than one Cisco Secure Client Certificate and/or a Private Key is used/required, repeat the above process for each Certificate).

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.

Active X Upgrade Can Disable Weblaunch

Automatic upgrades of Cisco Secure Client software via WebLaunch will work with limited user accounts as long as there are no changes required for the ActiveX control.

Occasionally, the control will change due to either a security fix or the addition of new functionality.

Should the control require an upgrade when invoked from a limited user account, the administrator must deploy the control using the Cisco Secure Client pre-installer, SMS, GPO or other administrative deployment methodology.

Java 7 Issues

Java 7 can cause problems with Cisco Secure Client and Secure Firewall Posture. A description of the issues and workarounds is provided in the Troubleshooting Technote Java 7 Issues with AnyConnect, CSD/HostScan, and WebVPN - Troubleshooting Guide, which is in Cisco documentation under Security > CiscoSecure Firewall Posture.

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.

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.

Network Interface Card Drivers Incompatible with Network Access Manager

The Intel wireless network interface card driver, version 12.4.4.5, is incompatible with Network Access Manager. If this driver is installed on the same endpoint as the Network Access Manager, it can cause inconsistent network connectivity and an abrupt shutdown of the Windows operating system.

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 5.0.05040

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
CSCvy66557	dart	ENH: DART for Windows should include the Device ID
CSCvu57988	dart	ENH: DART should include a copy of the Windows registry in the support bundle
CSCvy66584	dart	ENH: DART for Mac should include MDM profiles
CSCwb94282	nam	NAM can't connect to WPA2+WPA3/Enterprise SSID
CSCwd26172	nam	AnyConnect NAM fails to display/connect SSID in Unicode characters
CSCwh06886	nam	NAM unable to connect to SSIDs containing curly apostrophes

Identifier	Component	Headline
CSCwf57303	opswat-ise	Sophos Endpoint Point Agent 2023.1.0.73 to be supported on AnyConnect Compliance Module
CSCwf83498	opswat-ise	ISE 3.1 Posture Module support for Trellix Endpoint Security Definition Check for macOS
CSCwh04812	opswat-ise	ENH: Support for Malwarebytes Endpoint Agent v1.7.0
CSCwe60477	posture-ise	Posture scan result for Linux bridged virtual machines being reported incorrectly
CSCwf40722	posture-ise	USB drive getting detected as blocked when its not & USB Block remediation is not getting triggered
CSCwd81612	profile-editor	Unable to save NAM profile when SSID is UNICODE character in PE
CSCwe45817	vpn	Unencoded embedded URL in HTTP redirect prevents captive portal detection
CSCwf33688	vpn	Always On filtering is applied with a slight delay on newly enabled network interface
CSCwf94247	web	QR code may not be properly displayed in External Browser for SAML

Cisco Secure Client 5.0.04032

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
CSCwe67896	core	Vulnerabilities in openssl CVE-2023-0215 and others
CSCwe92223	core	Windows arm64: SplitDNSv6 tests showing stray DNS queries in pcap outside tunnel

Identifier	Component	Headline
CSCwf32105	core	AC agent is crashing after upgrading the AnyConnect from version 4.10.06079 to 4.10.06090
CSCwf58968	download_install	macOS 14 - VPN Notification app failed to launch; KDF deactivation skipped during uninstall
CSCwf08769	nam	Disable Windows RnR on Windows 10 and Windows 11 21H2
CSCvz20270	opswat-ise	ENH: ISE Posture does not support Mozilla Firefox version 87
CSCwd56524	posture-ise	[Document] ISE Posture Limited Support on Windows ARM64 bit platforms
CSCwf37767	swg	Enable SWG max debug log based on the presence of a custom flag file
CSCwe83519	vpn	DTLS MTU DPDs are sent too early and may be dropped by headend

Cisco Secure Client 5.0.03076

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
CSCwf24327	nam	Network Access Manager fails to connect to mixed WPA2/WPA3 Personal network when NAM policy does not allow WPA3

Cisco Secure Client 5.0.03072

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
CSCwe67896	core	Vulnerabilities in openssl CVE-2023-0215 and others
CSCwf32105	core	AC agent is crashing after upgrading AnyConnect from version 4.10.06079 to 4.10.06090
CSCwe17889	download_install	Windows: Desktop shortcut transform is failing to modify VPN core installer property
CSCwc09405	gui	AnyConnect / Secure Client does not fully support internationally accessibility standards
CSCur83728	nam	AnyConnect Network Access Manager doesn't send an EAPol logoff when CAC card is removed
CSCwb45685	nam	Add support for empty PIN when accessing smart card certificates
CSCwe06686	nam	NAM authentication fails after out of band password change and reauth
CSCwe33650	nam	NAM acnamcontrol utility requires GUID to be all caps for restartAdapter
CSCwe38560	nam	NAM unable to connect to networks using AKM 802.1X EAP SHA256
CSCwe40749	nam	File and Product version mismatch for acnamihv.dll
CSCvz20270	opswat-ise	ENH : ISE Posture does not support Mozilla Firefox version 87
CSCwa34429	opswat-ise	file date is wrong for edgehtml.dll after upgrade to KB5007186
CSCwc76493	opswat-ise	Windows 11: Patch Management Check Failure
CSCwd73072	opswat-ise	Carbon Black Cloud no longer supported as of macOS 186.0.0.0 support chart

Identifier	Component	Headline
CSCwe23584	opswat-ise	ENH: Include Trellix Drive Encryption 7.4.0.11 from Trellix to Posture Conditions
CSCwe51629	opswat-ise	Use XProtectPayloads instead of XProtectPlistConfigData to collect definition data of Xprotect AM
CSCwf08773	opswat-ise	Avast Business 23 is not available
CSCwf48234	opswat-ise	ENH: Support for McAfee Total Protection version 16.0 R51
CSCvx49570	posture-ise	ISE posture module not compatible for Windows 10 ARM64-based PCs
CSCwe70047	posture-ise	macOS: ISE Posture not accurately detecting FileVault 'state' (On/Off)
CSCwe86806	posture-ise	ENH: Xprotect support for version 2166.x
CSCwd84695	swg	Clear the OS DNS cache when SWG becomes active
CSCwe70156	swg	AnyConnect SWG: DNS Lookup thread exhaustion adding delay in connection establishment
CSCwe86049	swg	Handle non-success HTTP code as connection failure and enhance CP detection logic on slow CP network
CSCwf17017	swg	Timeouts observed while probing to MSFT URL
CSCwf22189	swg	SWG is not getting into protected state occasionally
CSCvv75596	umbrella	Add consistent support for DNS response compression
CSCvy09941	vpn	vpn-session-timeout doesn't work with Untrusted Network Policy and certificate based authentication
CSCwd09989	vpn	AnyConnect - proxy settings are not restored correctly after machine resumes from connected standby

Identifier	Component	Headline
CSCwd68113	vpn	AAA auth failing even when correct password is being entered

Cisco Secure Client 5.0.02075

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
CSCwc55221	core	AnyConnect does not clear SmartCard Pin
CSCwd73497	core	AC is detecting Trusted Network and UI is quitting when there is no network connectivity during SBL
CSCwe00252	core	Cisco AnyConnect Secure Mobility Client and Secure Client for Windows Privilege Esc Vuln
CSCwe43455	core	macOS 13: DNS-related features not working properly with DDR-enabled resolvers
CSCwe17889	download_install	Windows: Desktop shortcut transform is failing to modify VPN core installer property
CSCvp42218	nam	ENH: Allow admin to specify cert criteria to be used for cert selection
CSCwc78325	nam	Support for Certificate Matching Rule Field Certificate Template information
CSCwd79171	nam	libxml2 code may point to a dangling pointer which can result in an invalid memory access
CSCwd87145	nam	NAM Profile Editor: Editing a previously saved network may result in the display becoming corrupted
CSCwd90898	nam	Add support for WPA3 OWE and SAE networks

Identifier	Component	Headline
CSCwe40749	nam	File and Product version mismatch for acnamihv.dll
CSCwa34429	opswat-ise	file date is wrong for edgehtml.dll after upgrade to KB5007186
CSCwa64750	opswat-ise	FireEye agent version 34.x needs to be available in ISE posture conditions
CSCwa81027	opswat-ise	ISE Posture Patch Management Condition - add BMC Client Management Agent 20.x
CSCwc76493	opswat-ise	Windows 11: Patch Management Check Failure
CSCwc77619	opswat-ise	Failed to load CM 4.3.3030.6145 on AC 4.10
CSCwd11788	opswat-ise	OPSWAT unable to detect the FireEye after upgrade to CM version 4.3.2998.6145
CSCwd37792	opswat-ise	USB UpperFilter registry key gets deleted during Compliance Module uninstallation
CSCwd43799	opswat-ise	macOS 12.6 - Xprotect AM install version value detected incorrectly
CSCwd56796	opswat-ise	Wrong Windows Update Agent version is returned on Windows 11 22H2
CSCwd62517	opswat-ise	Adding new "CrowdStrike Windows Sensor" application on AnyConnect Posture ISE
CSCwe11874	opswat-ise	ENH: ISE posture does not support Kaspersky Endpoint Security 12.x
CSCwb64132	posture-ise	[ENH] AnyConnect shows cosmetic error message "Reassessment failed" on clients for session change
CSCwd49714	posture-ise	Translation did not occur in Win, Lin NSA pkg
CSCwd52815	posture-ise	Translation did not occur in MAC NSA pkg

Identifier	Component	Headline
CSCwe30612	posture-ise	ENH: Posture CLI for ISE Posture Module - macOS
CSCwe22036	swg	Backoff SWG protection only in noNetwork, Trusted Network, and VPN cases
CSCvv75596	umbrella	Add consistent support for DNS response compression
CSCwe07816	umbrella	Umbrella agent crash with high rate of socket errors reported by Umbrella plugin
CSCvf70372	vpn	AnyConnect and 'AutoConnectOnStart' feature with Umbrella module causes 'AutoConnectOnStart' to fail
CSCvx93522	vpn	AnyConnect SAML ignoring tunnel-group-list (group-alias)
CSCvz63011	vpn	ENH (desktop): Add support for idle authentication timeout to cancel expired authentication attempts
CSCwd15773	vpn	Sidecar and Continuity Camera video feed not working on macOS 13 with VPN connection active
CSCwd17651	vpn	Management Tunnel goes down after 4-7 days and then stays Disconnected
CSCwd40263	vpn	Proxy settings are not being applied everywhere
CSCwd76149	vpn	SBL/ARM64: SBL icon not appearing after restart - shutdown + reboot works OK
CSCwa31551	web	AnyConnect: Embedded browser not displayed for SAML authentication post upgrade to 4.10.03104

Cisco Secure Client 5.0.01242

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
CSCvz84164	api	RestrictPreferenceCaching credentials still displays username when group-policy has no XMLprofile
CSCwc63454	api	VPN connection fails when Downloader is bypassed in local policy file
CSCwc92975	cli	VPN CLI stuck on disconnecting state
CSCvu77796	core	CIAM: libxml 2.9.10
CSCvx35970	core	AC 4.9MR5 is ignoring Authentication Timeout VPN profile settings
CSCvw31155	core	Multiple Certificate Validation Failure popups when using Always On
CSCwb77035	core	Windows Security 'Credential Required' popup not in focus
CSCwc55221	core	AnyConnect does not clear SmartCard pin
CSCvz68411	dart	DART missing the Umbrella white list file
CSCwb78515	dart	DART does not collect VPN Management Tunnel mini dump crash file
CSCwd06986	dart	AnyConnect DART bundle on Windows 11 in summary reads 'Windows 10' instead of 'Windows 11'
CSCwb74542	download_install	AnyConnect installation failed when changing date format in PC

Identifier	Component	Headline
CSCuw17364	gui	Able to establish vpn without closing the Pre-Connect popup
CSCvz53637	gui	AnyConnect: Users can change preferences while UserControllable is set to false
CSCwc59031	gui	Secure Client: Upgrade to 8.0.1.x with AnyConnect 4.x.x breaks shortcut links in Start Menu [Windows]
CSCwc64861	gui	AnyConnect GUI message update after successful SAML authentication
CSCvo32995	nam	ENH: Add support for "Connect Automatically" feature for individually configured wireless networks
CSCvs29773	nam	ENH: NAM allows users to turn on/off pcap, IHV, fd, credential provider, etc for extended logging
CSCwa91572	posture-ise	Mandate minimum CM version to be downloaded for CSC - Windows, macOS, and Linux
CSCwd62225	posture-ise	Windows: Failed to load Compliance Module
CSCwc73870	profile-editor	AMP Enabler profile editor does not detect or load with OpenJDK
CSCwb39828	swg	Captive Portal page didn't open when SWG is enabled for both fail open/fail close
CSCwc41729	swg	Reverse DNS lookup in KDF by SWG also accommodates flows targeting IPv4 -mapped IPv6 address
CSCwc53340	swg	macOS: SWG domain bypass fails intermittently for web flows targeting FQDNs with trailing dot
CSCwd02073	swg	Few logs are getting logged in AnyConnect Umbrella path instead of CSC - Umbrella in 5.x

Identifier	Component	Headline
CSCwd83114	umbrella	dcp2 crash fix
CSCvj04741	vpn	AC TND does not check next TrustedHttpsServer if first server hash doesn't match, moves to untrusted
CSCvy99392	vpn	VPN connection via local proxy does not work and fails with "Cannot connect to this gateway"
CSCvz51167	vpn	Chrome browser crashes after external browser authentication on macOS
CSCvz63011	vpn	ENH (desktop): Add support for idle authentication timeout to cancel expired authentication attempts
CSCwa92301	vpn	Defer upgrade prompt not shown when connecting through SBL
CSCwb67733	vpn	AnyConnect increased timeout to 120 seconds for cURL certificate signing operations
CSCwb85473	vpn	Windows: RSAT slow when only virtual subnets are excluded from tunnel (for WSL2 interoperability)
CSCwc15262	vpn	AC 4.10 MR4 or 4.9 MR4 cannot connect VPN using Smartcard Cert auth
CSCwc46323	vpn	Windows integrated authentication failure through SAML flow
CSCwc50423	vpn	AnyConnect client is not able to restore proxy settings when the machine is powered-off
CSCwc64425	vpn	Zenmu Virtual Desktop and AnyConnect SAML external browser compatibility
CSCwc79898	vpn	AnyConnect Ubuntu 22.04 - SAML external browser does not launch
CSCwc81098	vpn	Update AnyConnect LaunchDaemon plist header syntax

Identifier	Component	Headline
CSCwc85871	vpn	ENH: Add Original Address payload for IKEv2 IPv4/IPv6 dual-stack support with public NAT on IOS-XE
CSCwd14401	vpn	Windows Always On: VPN can't connect (DNS error) after VPN disconnect and expected connect failure
CSCwd16706	vpn	Proxy settings are not being restored properly at all places (intermittently)
CSCwd23719	vpn	VPN connection failure due to Session ID caching in cURL
CSCwb22799	web	Embedded browser incorrect windows size

Cisco Secure Client 5.0.00556

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
CSCvx10794	opwat-ise	Windows Update GUI does not open when activate patch management GUI remediation is configured in ISE
CSCwb99183	opswat-ise	Asia Info Office Scan Agent 16.x(16.0.0283) need to add in ISE support condition
CSCwc53490	opswat-ise	Failed to load compliance module
CSCwc59876	opswat-ise	Support for Cisco AMP 8.x and Cisco ISE Posture Compliance Module
CSCwc20207	posture-ise	Apex One (MAC) Security Agent [Trend Micro] AM latest definition date/version is not reflected

Identifier	Component	Headline
CSCwc56173	vpn	VPN connection attempt hangs for up to 3 minutes after a previous post-auth connection failure

Cisco Secure Client 5.0.00529

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
CSCwb41421	core	CiscoSSL CVE-2022-0778
CSCwb78515	dart	DART does not collect VPN Management Tunnel mini dump crash file
CSCvz87690	download_install	AnyConnect CSD Posture assessment failed due to proxy environment variables
CSCvz53637	gui	Users can change preferences while UserControllable is set to False
CSCvr88852	nam	Certificate Selection Policy
CSCwa48531	opswat-ise	OPSWAT 4.3.2443 unable to detect Trendmicro APEXOne agent version 14.0.9601
CSCwb30655	opswat-ise	Fireeye security agent version 34.x is missing in latest ISE posture updates
CSCwc53490	opswat-ise	Failed to load compliance module
CSCwa69058	profile-editor	Standalone VPN Profile Editor for Windows works only with Oracle Java

Secure Firewall Posture (Formerly HostScan) 5.0.05040

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
CSCwf70012	opswat-asa	HostScan getting stuck in definition check for TrendMicro Apex One
CSCwh10607	opswat-asa	Upgrading the HS from 4.10 MR to Secure Firewall Posture to 5.0.x causes VPN timeout or conn delay
CSCwf96510	posture-asa	AutoDART feature in HostScan
CSCwf84160	swg	Fix Network Change Detection in Windows and macOS

Secure Firewall Posture (Formerly HostScan) 5.0.04032

Caveats describe unexpected behavior or defects in Cisco software releases.

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
CSCwf09464	opswat-asa	ENH: Support for McAfee LiveSafe - Internet Security version 16.0 R51
CSCwf44746	opswat-asa	Timeout issue seen on Linux machines with secure firewall posture 5.0.03068

Secure Firewall Posture (Formerly HostScan) 5.0.03072

Caveats describe unexpected behavior or defects in Cisco software releases.

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
CSCvz19204	opswat-asa	ENH: Need to add support of "Sophos Endpoint" Antimalware 10.1.x for macOS on HostScan
CSCwf44746	opswat-asa	Timeout issue seen on Linux machines with Secure Firewall Posture 5.0.03068
CSCwf98852	opswat-asa	Trellix Security Agent incorrectly identified as outdated product McAfee Security Agent

Secure Firewall Posture (Formerly HostScan) 5.0.02075

Caveats describe unexpected behavior or defects in Cisco software releases.

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
CSCwd94368	opswat-asa	ENH: HostScan support for Cisco Secure Endpoint 7.5.5.21061
CSCwd81115	posture-asa	Data .xml file configuration changes due to non availability of csdm.sez for DE feature in ASA/ASDM

Secure Firewall Posture (Formerly HostScan) 5.0.01242

Caveats describe unexpected behavior or defects in Cisco software releases.

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
CSCvw36365	opswat-asa	HostScan support to detect ESET Smart Security 14.x and above

Identifier	Component	Headline
CSCvz01221	opswat-asa	AnyConnect SAML authentication fails due to HostScan delay caused by definition check
CSCwc37138	opswat-asa	Sophos Antimalware remediation causing vpn timeout in RHEL/Ubuntu clients
CSCwd39477	opswat-asa	Sophos Endpoint Agent 2022.2.1.9 fails definition check with Secure Firewall Posture (HostScan) 5.0.00529

Secure Firewall Posture (Formerly HostScan) 5.0.00556

Secure Firewall Posture 5.0.00556 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) 5.0.00529

Secure Firewall Posture 5.0.00529 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.

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.

© 2023 Cisco Systems, Inc. All rights reserved.