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

First Published: 2023-07-27

Last Modified: 2023-12-13

Release Notes for Cisco Secure Client, Release 5.1.x.x

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

Note Cisco Secure Client 5.1.x.x will become the maintenance path for any 5.x.x.x bugs. Cisco Secure Client 5.0.x.x customers must upgrade to Cisco Secure Client 5.1.x.x to benefit from future defect fixes. Any defects found in Cisco Secure Client 5.0.x.x will be fixed in the Cisco Secure Client 5.1.x.x maintenance releases only.

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
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 5.1.2.42 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.2.42, on page 31.

- (CSCwh29292) Dynamic split tunneling can now perform both dynamic exclusion from a tunnel and dynamic inclusion into a tunnel for a given configuration, as needed. For example, with enhanced dynamic split exclude tunneling, traffic matching a dynamic include domain may be dynamically included into a tunnel, if necessary to override a static split exclude network. Refer to About Dynamic Split Tunneling in the *Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5* for additional details.
- In the profile editor, wildcards can now be added at the beginning or end of the Host Address in Load Balancing Server List.
- We have implemented a Network Access Manager addition to disable the setting of PMF IGTK until a Windows fix becomes available. Microsoft estimates that fixes for Windows 10 22H2 and Windows 11 21H2 (and later) should be available in the first half of calendar year 2024, which will allow you to set the IGTK from the Network Access Manager. Until then, you can disable the setting of PMF IGTK and allow a connection to a network configured to provide Protection of Management Frames (PMF). If the

Windows fix is not yet available, and you can't avoid connecting to a network with PMF enabled, you need to modify the Windows registry editor by adding the following registry key as a DWORD and setting it as described to disable the use of IGTK by the Network Access Manager:

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

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

- You must have the appropriate AnyConnect VPN version (5.1.1.42) to interoperate with the Zero Trust Access Module (5.1.2.5191).
- Windows 10 ARM64 is no longer supported.

Cisco Secure Client 5.1.1.42 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.1.42, on page 32.

- Fatal error with webdeploy upgrade (CSCwi37384)—ASA or ISE webdeploy only on Windows 11 ARM64 results in a fatal error when upgrading from Cisco Secure Client 5.1.0.x to 5.1.1.x. You will need to uninstall Secure Client 5.1.0.x for a fresh install of 5.1.1.x as a workaround in order for webdeploy to work on Windows 11 ARM64 devices. Alternatively, you can upgrade from Windows 11 ARM64 devices from Secure Client 5.1.0.x to 5.1.1.x using predeploy.
- You must have the appropriate AnyConnect VPN version (5.1.1.42) to interoperate with the Zero Trust Access Module (5.1.1.4867).
- Web Deploy Upgrade on macOS Requires Admin Privileges (CSCwi69393)—Due to a new Apple API change, when using webdeploy to upgrade from Cisco Secure Client 5.0.x (or earlier) to 5.1.x (or later), you must have administrator privileges or manage the macOS devices via MDM to pre-approve the application extension.
- Updates to Network Visibility Module—
  - Added HTTP Host as an additional Collection Parameter for HTTP 1.1 flows from Windows clients running Network Visibility Module.
  - Extended the Collection Parameter Module Name List to include browser plugin information (name and version) for Chrome, Firefox, and MS Edge browser flows from Windows and macOS clients.
  - **Known Issue:**CSCwi48979—The HTTP Host field for macOS is reported as empty instead of providing the proper destination host name for HTTP traffic.
  - **Known Issue:**CSCwi49003—Network Visibility Module is not reporting the Safari Browser plugins for macOS.
- **Known Issue:**CSCwi49850—macOS 12: Hyperlinks not working in AnyConnect Embedded Browser during captive portal remediation

Cisco Secure Client 5.1.0.136 New Features

This release includes the following features and support updates, and resolves the defects described in Cisco Secure Client 5.1.0.136, on page 33.

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

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

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

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

  Current Limitations or Restrictions

  - Zero Trust Access functionality is disabled when multiple users are logged in concurrently to an endpoint.
  - No support for tunneling applications where server sends traffic first (ex:: MySQL).
  - DART will not collect Duo Desktop logs on macOS for 5.1.
  - With a maOS webdeploy, DART does not upgrade. You receive an error and can manually install for the DART collection.
  - ASDM does not show Zero Trust Access as a module in the group-policy (Configuration > Remote Access VPN > Network (Client) Access > Secure Client Connection Profiles Edit Group-Policy, Advanced-Secure Client-Optional Modules to Download) drop-down menu. A defect has been assigned to the ASDM team to address.

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

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

Secure Firewall Posture (Formerly HostScan) 5.1.2.42 New Features

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

Secure Firewall Posture (Formerly HostScan) 5.1.1.42 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.1.42 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defect listed in Secure Firewall Posture (Formerly HostScan) 5.1.1.42, on page 34.

Secure Firewall Posture (Formerly HostScan) 5.1.0.136 New Features

The Secure Firewall Posture (formerly HostScan) 5.1.0.136 release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defect listed in Secure Firewall Posture (Formerly HostScan) 5.1.0.136, on page 35.

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	Duo Endpoint Agent
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
Microsoft-supported versions of Windows 11 for ARM64-based PCs	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	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	Thousands Endpoint Agent
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

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	9.x and 8.x	9.x and 8.x	9.x and 8.1 (and later)	Yes	Yes
Ubuntu	22.04 and 20.04	22.04 and 20.04	22.04 and 20.04	22.04 and 20.04	Yes	Yes
SUSE (SLES)	Limited support. Used only to install ISE Posture	not supported	not supported	12.3 (and later) and 15.0 (and later)	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 8 or 8.1.

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.
- Other third-party product's incompatibility with Windows 8 prevent Cisco Secure Client from establishing a VPN connection over wireless networks. Here are two examples of this problem:
  - WinPcap service "Remote Packet Capture Protocol v.0 (experimental)" distributed with Wireshark does not support Windows 8.

    To work around this problem, uninstall Wireshark or disable the WinPcap service, reboot your Windows 8 computer, and attempt the Cisco Secure Client connection again.
  - Outdated wireless cards or wireless card drivers that do not support Windows 8 prevent Cisco Secure Client from establishing a VPN connection.

    To work around this problem, make sure you have the latest wireless network cards or drivers that support Windows 8 installed on your Windows 8 computer.
- Cisco Secure Client is not integrated with the new UI framework, known as the Metro design language, that is deployed on Windows 8; however, Cisco Secure Client does run on Windows 8 in desktop mode.
- HP Protect tools do not work with Cisco Secure Client on Windows 8.x.
- If you are using Network Access Manager on a system that supports standby, Cisco recommends that the default Windows 8.x 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 8 or 10 / 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 8, 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 8.

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 8, 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

Web Deploy Upgrade on macOS 13 (or Later) Requires Admin Privileges

Due to a new OS requirement, one-time administrator privileges are necessary when performing a web deploy upgrade from 5.0.x (or earlier) to 5.1.x (or later). Further updates do not need them. You can circumvent this limitation by managing macOS devices via MDM and pre-approving the application.

Embedded Browser Changes After Deprecation of IE11

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

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

Encrypted DNS Impact and Mitigation

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

As an additional mitigation, Cisco Secure Client prohibits DNS over HTTPS (DoH) name resolution for the Windows DNS client via local policy setting **Configure DNS over HTTP (DoH) name resolution** (under Computer Configuration > Administrative Templates > Network > DNS Client). This change is applicable to Windows 11 and later versions and is enforced while any of the following modules is active: VPN, Umbrella Roaming Security, or Network Visibility. 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.
- Installing Cisco Secure Client 5.1.0.136 and later from the XDR portal is not supported on ARM64.

RDP With Wired Connections Not Working

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

Simultaneous VPN Sessions Not Supported

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

macOS 13 Known Issue

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

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

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

Windows Local Group Policy DNS Settings Ignored

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

Root CA Conflict With Firefox NSS Store (Linux Only)

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

Initiating an Automatic VPN Connection With TND (CSCvz02896)

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

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 8 and above 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 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.)

Authentication Failure When Using a SHA512 Certificate for Authentication

(For Windows 7, 8, and 8.1 users running an AnyConnect version prior to 4.9.03047) When the client uses a SHA512 certificate for authentication, authentication fails, even though the client logs show that the certificate is being used. The ASA logs correctly show that no certificate was sent by AnyConnect. These versions of Windows require that you enable support for SHA512 certificates in TLS 1.2, which is not supported by default. Refer to https://support.microsoft.com/en-us/kb/2973337 for information on enabling support for these SHA512 certificates. 4.9.03049

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.

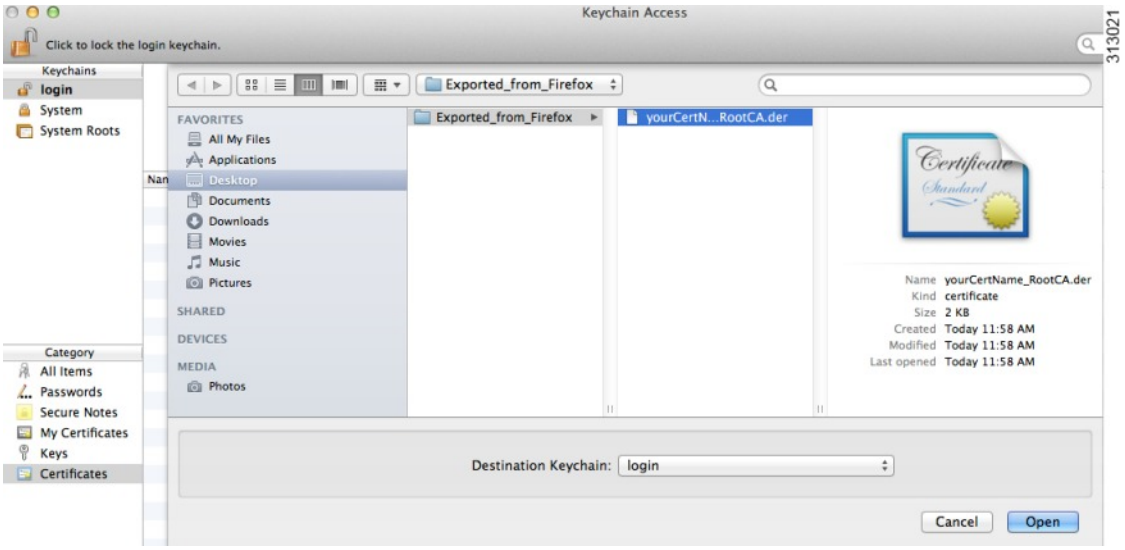
Firefox Certificate Store on macOS is Not Supported

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.

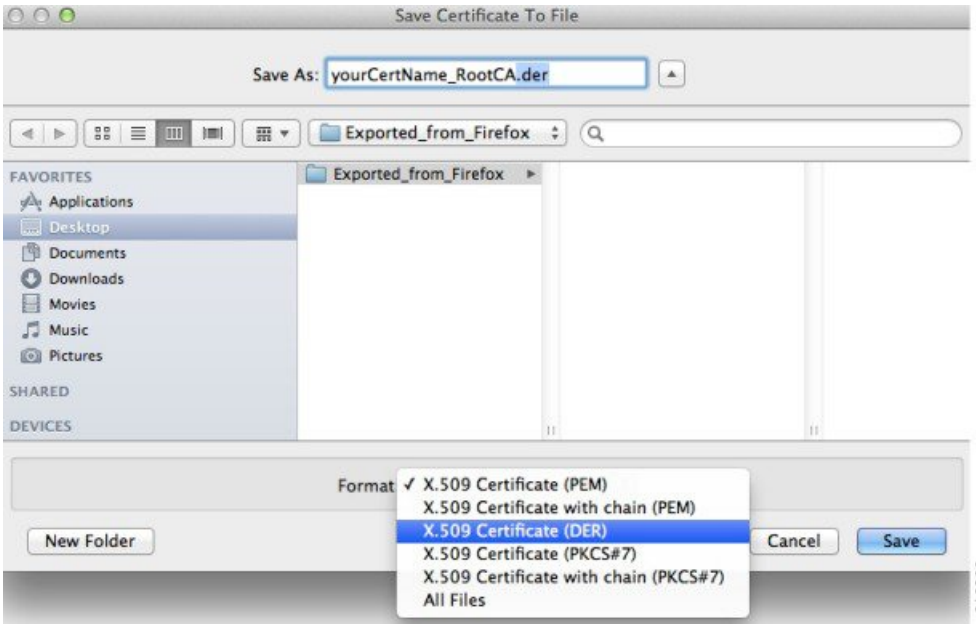


Note If more than one Cisco Secure Client Certificate and/or a Private Key is used/required, repeat the above process for each Certificate).

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 Windows7, Windows 8, and Windows 10.
- 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 7 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 the Windows 7 or later, the Wireless Hosted Network feature can make Cisco Secure Client unstable. When using Cisco Secure Client, we do not recommend enabling this feature or running front-end applications that enable it (such as Connectify or Virtual Router).

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

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

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

ssl server-version sslv3

ssl server-version sslv3-only

Trend Micro Conflicts with Install

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

What Secure Firewall Posture Reports

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

- For antimalware
  - Product description
  - Product version
  - File system protection status (active scan)
  - Data file time (last update and timestamp)
- For firewall
  - Product description
  - Product version
  - Is firewall enabled

Long Reconnects (CSCtx35606)

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

Users with Limited Privileges Cannot Upgrade ActiveX

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

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

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

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

Application Programming Interface for the Cisco Secure Client

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

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

You can download the APIs from Cisco.com.

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

Cisco Secure Client 5.1.2.42

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwf21453	core	RetainVpnOnLogoff errors when attempting to validate proxy settings
CSCwh73937	core	ENH: macOS AnyConnect to support Dynamic Split Exclusions based on CNAME DNS responses
CSCwi07144	core	Vulnerabilities in zlib - multiple versions
CSCwi78167	core	Wildcard support to load balancing servers for AO configuration
CSCwi27062	nam	NAM unable to connect to Eero mesh APs
CSCwi27137	nam	NAM does not recognize default PMF IGTK cipher

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

Cisco Secure Client 5.1.1.42

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwf67833	core	(Windows only) - Error: The VPN client is unable to configure private-side proxy settings
CSCwh57935	core	AnyConnect launches the client downloader pop-up outside of core update
CSCwh96410	core	Vulnerabilities in curl - multiple versions
CSCwi20597	core	macOS 14.2 - VPN Agent not started after installation
CSCwi28687	core	Vpnagentd crashes with authenticating proxy on macOS

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

Cisco Secure Client 5.1.0.136

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvz45813	core	ENH: Add a session ID to the AnyConnect logs in order to group series of related message exchanges
CSCvu57988	dart	ENH: DART should include a copy of the Windows registry in the support bundle

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

Secure Firewall Posture (Formerly HostScan) 5.1.2.42

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

Secure Firewall Posture (Formerly HostScan) 5.1.1.42

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

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

Secure Firewall Posture (Formerly HostScan) 5.1.0.136

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

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

Related Documentation

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