Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.9

First Published: 2022-09-05

Last Modified: 2024-09-04

Release Notes for AnyConnect Secure Mobility Client, Release 4.9

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

Note **CISCO ANYCONNECT 4.X IS CURRENTLY END-OF-LIFE. MOVING FORWARD, ALL ENHANCEMENTS AND BUG FIXES WILL BE PROVIDED AS PART OF THE CISCO SECURE CLIENT 5.1.X VERSION. WITHOUT UPGRADING TO THE CISCO SECURE CLIENT 5.1.X VERSION, YOU CANNOT GET SUPPORT FOR THE EXISTING PRODUCT, ANY NEW FEATURES, ANY COMPLIANCE MODULE UPDATES (HOSTSCAN/SECURE FIREWALL POSTURE/ISE) OR ANY UPDATES ASSOCIATED WITH THE LATEST OPERATING SYSTEMS. ALL CUSTOMERS WITH VALID ANYCONNECT/SECURE CLIENT TERM LICENSES OR PERPETUAL LICENSES WITH ACTIVE SUPPORT CONTRACTS ARE ELIGIBLE TO UPGRADE TO THE CURRENT CISCO SECURE CLIENT 5.1.X VERSION AT NO CHARGE.**

Cisco AnyConnect Users With macOS 10.15 Might Not Be Able To Establish VPN Connection or Might Receive System Pop-up Messages—Software Upgrade Recommended

Cisco AnyConnect and HostScan require updated releases for compatibility with the upcoming macOS Catalina release (10.15). Beginning with macOS Catalina release (10.15), the operating system will no longer support the executing of 32-bit binaries. Additionally, applications must be cryptographically notarized in order to be installed by the operating system. Cisco AnyConnect 4.8.00175 is the first version that officially supports operation on macOS Catalina and contains no 32-bit code.

Download the Latest Version of AnyConnect

Before you begin

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

Procedure

Step 1 Follow this link to the AnyConnect Secure Mobility 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 AnyConnect 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**.

AnyConnect Secure Mobility Client Package Filenames for Web Deployment

OS	AnyConnect Web-Deploy Package Names
Windows	anyconnect-win-*version*-webdeploy-k9.pkg
macOS	anyconnect-macos-*version*-webdeploy-k9.pkg
Linux (64-bit)*	anyconnect-linux64-*version*-webdeploy-k9.pkg

AnyConnect Package Filenames for Predeployment

OS	AnyConnect Predeploy Package Name
Windows	anyconnect-win-*version*-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux (64-bit)	(for script installer) anyconnect-linux64-*version*-predeploy-k9.tar.gz

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

Other files, which help you add additional features to AnyConnect, can also be downloaded.

AnyConnect 4.9.06037 New Features

This AnyConnect 4.9.06037 release introduces the following updates and enhancements, and resolves the defects described in AnyConnect 4.9.06037, on page 35:

- (CSCvy53730-Windows only) AnyConnect 4.9.06037 and above cannot update the Compliance Modules from ISE that are shipped with AnyConnect 4.9MR5 or earlier. Due to this change, Compliance Module version 4.3.1634.6145 or later are required for AnyConnect 4.9.06037 and above.
- (CSCvw92182) Fixed the macOS-only issue of the VPN module reconnecting seconds after initial connection to the ASA SSL gateway or after an interface change. This reconnection impacted TLS-only tunnels. With the fix, the ISE posture module should no longer show "No policy server detected."

- CiscoSSL libraries were updated to address DTLS session failures when connecting to new, unreleased versions of ASA.
- NVM was updated to validate certificates in DTLS mode (Windows only).
- (CSCvw53140) Fixed AnyConnect 4.9.03049 (and later) smartcard issues with VPN modules on Windows. This issue occurred on smartcards that do not support Key Storage Provider (KSP), or that do support legacy Cryptographic Service Provider (CSP), for crypto operations.

AnyConnect 4.9.05042 New Features

This release resolves the defects described in AnyConnect 4.9.05042, on page 36.

AnyConnect 4.9.04053 New Features

This AnyConnect 4.9.4053 release introduces the following enhancement and resolves the defect described in AnyConnect 4.9.04053, on page 37:

Added settings to the VPN Local Policy Editor that allow you to bypass certain downloader functions, while preserving VPN profile updates and software update capabilities. You can disable web deployment of scripts, localization files, help files, or UI customization from ASAs, without impacting other functions of the AnyConnect downloader.

- **Restrict Script Web-deploy Updates**—Prevents administrators from customizing on-connect script updates from the server.
- **Restrict Resource Web-deploy Updates**—Prevents administrators from customizing user interface element updates from the server.
- **Restrict Help Web-deploy Updates**—Prevents administrators from customizing help file updates from the server.
- **Restrict Localization Web-deploy Updates**—Prevents administrators from customizing localization updates from the server.

Setting these four customer web-deploy parameters to bypass **(true)** requires 1) out-of-band updates to the *AnyConnectLocal Policy.xml* file as described below and 2) out-of-band deployment for all future updates to these files:

- <RestrictStrictWebDeploy> controls the download of OnConnect scripts that are located in:
  - Windows—<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\script
  - macOS—/opt/cisco/anyconnect/script
  - Linux—/opt/cisco/anyconnect/script
- <RestrictResourceWebDeploy> controls the download of UI customizations to the directory:
  - Windows—<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\res
  - macOS—/opt/cisco/anyconnect/res
  - Linux—/opt/cisco/anyconnect/res

- <RestrictHelpWebDeploy> controls the download of Help files to the directory:
  - Windows—<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help
  - macOS—/opt/cisco/anyconnect/help
  - Linux—/opt/cisco/anyconnect/help
- <RestrictLocalizationWebDeploy> controls the download of L10N localization files to:
  - Windows—<DriveLetter>\ProgramData\Cisco\Cisco AnyConnect Secure MobilityClient\110n
  - macOS—/opt/cisco/anyconnect/110n
  - Linux—/opt/cisco/anyconnect/110n

AnyConnect 4.9.04043 New Features

This AnyConnect 4.9.04043 release introduces support for macOS 11.x (Big Sur) and compatibility with devices running Apple Silicon. It also resolves the defects described in AnyConnect 4.9.04043, on page 37.

When running on macOS 11, AnyConnect uses a system extension, as opposed to the kernel extension used in previous AnyConnect versions.

Prior AnyConnect versions may still work on macOS 11, but only on MDM-managed devices, since an MDM-based approval of the AnyConnect kernel extension is required starting with macOS 11. Refer to AnyConnect macOS 11 Big Sur Advisory for AnyConnect changes related to macOS 11 (Big Sur).

AnyConnect 4.9.03049 New Features

AnyConnect 4.9.03049 is a Windows-only release that resolves the defect described in AnyConnect 4.9.03049, on page 38.

AnyConnect 4.9.03047 New Features

This AnyConnect 4.9.03047 release introduces the following enhancements and resolves the defects described in AnyConnect 4.9.03047, on page 39:

- (CSCvu14970) Allow only one local user to be logged on during the entire VPN connection (with the Logon Enforcement setting in Profile Editor, Preferences (Part 1).
- Allow endpoints to access the configured hosts when VPN is disconnected during Always On (with the Allow Access to the Following Hosts with VPN Disconnected setting in Profile Editor, Preferences (Part 2).
- Add support for Server Name Identification (SNI) for VPN connections (does not include HostScan or other modules).
- Add support for SWG Trusted Network Detection on Umbrella Secure Web Gateway (SWG) Module, based on the AnyConnect client profile's Trusted Domain and Trusted Servers.

- Allow SWG proxy to intercept HTTP and HTTPS traffic coming from non-standard ports, besides the standard 80 and 443 ports.
- Add support to handle multiple requests (for example, 100 or more) sent to SWG proxy URL.
- Determine if you want NVM to securely send data to the collector over DTLS.
- Add support for end-to-end agentless posture flow in ISE posture.

AnyConnect 4.9.03047 functions on macOS 11 (Big Sur) beta 9 (or public beta 5) or newer versions. When running on macOS 11 (Big Sur), AnyConnect uses a system extension, as opposed to the kernel extension used in previous AnyConnect versions.

Prior AnyConnect versions may still work on macOS 11, but only on MDM-managed devices, since an MDM-based approval of the AnyConnect kernel extension is required starting with macOS 11.

Customers are welcome to test now and should always test with the latest Big Sur beta builds.

You can send any Big Sur compatibility issues to **ask-anyconnect@cisco.com**. Refer to AnyConnect macOS 11 Big Sur Advisory for AnyConnect changes related to macOS 11 (Big Sur). Prior to the Big Sur OS release, you cannot open TAC cases for compatibility issues.

AnyConnect 4.9.02028 New Features

This AnyConnect 4.9.02028 release introduces the following enhancements and resolves the defects described in AnyConnect 4.9.02028, on page 41:

AnyConnect 4.9.02028 is a macOS-only release that also functions on macOS 11 (Big Sur) beta 5 (or public beta 2) or newer versions. When running on macOS 11 (Big Sur), AnyConnect uses a system extension, as opposed to the kernel extension used in previous AnyConnect versions.

Prior AnyConnect versions may still work on macOS 11, but only on MDM-managed devices, since an MDM-based approval of the AnyConnect kernel extension is required starting with macOS 11.

AnyConnect 4.9.01095 New Features

This AnyConnect 4.9.01095 release introduces the following enhancements and limitations, and resolves the defects described in AnyConnect 4.9.01095, on page 41 :

- Ability for Linux users to route network traffic on a VM instance/docker container.
- Auto-reconnect unsuccessful after upgrading to AnyConnect 4.9.01095 (Linux Only). See the Client First Auto-Reconnect Unsuccessful After Upgrading to AnyConnect 4.9.01xxx (Linux Only) section for further details.

AnyConnect 4.9.00086 New Features

This is a major release that includes the following features and support updates, and that resolves the defects described in AnyConnect 4.9.00086, on page 44:

- NVM expansion to enrich flow and endpoint data, including new NVM Collector coordinated with Splunk app 3.x and a timestamp for flow information

- For SSL VPN, AnyConnect no longer supports the following cipher suites from both TLS and DTLS: DHE-RSA-AES256-SHA and DES-CBC3-SHA
- For IKEv2/IPsec, AnyConnect no longer supports the following algorithms:
  - Encryption algorithms: DES and 3DES
  - Pseudo Random Function (PRF) algorithm: MD5
  - Integrity algorithm: MD5
  - Diffie-Hellman (DH) groups: 2, 5, 14, 24

  For a list of supported cryptographic algorithms and cipher suites, refer to the AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.9 feature guide.
- Updated OpenSSL (Cisco SSL) library

AnyConnect HostScan Engine Update 4.9.06046 New Features

This AnyConnect HostScan only release includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.9.06046, on page 47.

AnyConnect HostScan Engine Update 4.9.06037 New Features

AnyConnect HostScan 4.9.06037 resolves the defect listed in HostScan 4.9.06037, on page 47.

AnyConnect HostScan Engine Update 4.9.05042 New Features

AnyConnect HostScan 4.9.05042 adds support to detect ARM64 devices. It includes updates to the HostScan module and resolves the defects listed in HostScan 4.9.05042, on page 48.

AnyConnect HostScan Engine Update 4.9.04045 New Features

This AnyConnect HostScan 4.9.04045 release provides official support for macOS 11.x (Big Sur). It includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

If you are using the macOS Big Sur beta or the official macOS Big Sur (version 11.x) release with HostScan, the AnyConnect HostScan Posture Module (if previously installed) on the endpoint and the HostScan PKG on the ASA must be upgraded to 4.9.04045 or later.

AnyConnect HostScan Engine Update 4.9.03047 New Features

AnyConnect HostScan 4.9.03047 supports macOS 11 (Big Sur) beta 9 (or public beta 5) or newer versions and includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

If you are using macOS 11 beta with HostScan, previous versions of HostScan will not function properly. Therefore, the AnyConnect HostScan Posture Module (if previously installed) on the endpoint and the HostScan PKG on the ASA must be upgraded to 4.9.02028 or later.

AnyConnect HostScan Engine Update 4.9.02028 New Features

AnyConnect HostScan 4.9.02028 supports macOS 11 (Big Sur) beta 5 (or public beta 2) or newer versions and includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

This release includes the new macOS 11 support and resolves the defect listed in HostScan 4.9.02028, on page 48.

If you are using macOS 11 beta with HostScan, previously versions of HostScan will not function properly. Therefore, the AnyConnect HostScan Posture Module (if previously installed) on the endpoint and the HostScan PKG on the ASA must be upgraded to 4.9.02028.

AnyConnect HostScan Engine Update 4.9.01095 New Features

AnyConnect HostScan 4.9.01095 includes this update to the HostScan module and resolves the defects listed in HostScan 4.9.01095, on page 49:

Support for Microsoft Defender Advanced Threat Protection (ATP) for Windows 10 endpoints.

AnyConnect HostScan Engine Update 4.9.00086 New Features

AnyConnect HostScan 4.9.00086 includes updates to the HostScan module and resolves the defects listed in HostScan 4.9.00086, on page 49.

System Requirements

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

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

Changes to the AnyConnect Profile Editor

You must install Java, version 6 or higher, before installing the profile editor.

SAML Requirements

Follow the guidelines below when using SAML:

- For AnyConnect VPN SAML embedded browser

  Safari update 14.1.2 (or later) is required: contains an updated Webkit version, which resolves various behaviors

- For AnyConnect VPN SAML external browser

AnyConnect release 4.10.04065 (or later)

ASA 9.17.1/ASDM 7/7/1 (or later)

FDM 7.1 (or later)

ISE Requirements for AnyConnect

- **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 AnyConnect 4.7MR1 (and later) supports IPv6 non-redirection flows (using stage 2 discovery) on wired and VPN flows.
- AnyConnect 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 AnyConnect software to an endpoint and posturing that endpoint using the new ISE Posture module in AnyConnect 4.0 and later.
- ISE 2.0 can only deploy AnyConnect release 4.0 and later. Older releases of AnyConnect must be web deployed from an ASA, predeployed with an SMS, or manually deployed.
- If you are installing or updating the AnyConnect 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 AnyConnect 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 AnyConnect

Minimum ASA/ASDM Release Requirements for Specified Features

- 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.
- 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 AnyConnect
  - 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)
  - AnyConnect 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 AnyConnect GUI when an AnyConnect session is in quarantine.
- To perform the HostScan 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 AnyConnect 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 AnyConnect package will be able to be loaded onto this model. To successfully load AnyConnect, you will need to reduce the size of your packages (such as fewer OSs, no HostScan, and so on) until they fit on the available flash.

Check for the available space before proceeding with the AnyConnect 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 AnyConnect 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.

HostScan

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

HostScan, available as its own software package, is periodically updated with new operating system, antimalware, and firewall software information. The usual recommendation is to run the most recent version of HostScan (which is the same as the version of AnyConnect).

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

In HostScan 4.4 and later, endpoint data (endpoint attributes) for antivirus, antispyware, and firewall have changed. Antispyware *(endpoint.as)* and antivirus *(endpoint.av)* are both categorized as antimalware *(endpoint.am)*. Firewall *(endpoint.pw)* is categorized as firewall *(endpoint.pfw)*. Refer to the AnyConnect HostScan Migration 4.3.x to 4.6.x and Later documentation for the specifics of this configuration.

Note AnyConnect will not establish a VPN connection when used with an incompatible version of HostScan. Also, Cisco does not recommend the combined use of HostScan and ISE posture. Unexpected results occur when the two different posture agents are run.

With HostScan, macOS Big Sur (version 11.x) is officially supported. Therefore, if you are using macOS Big Sur beta or the official macOS Big Sur (version 11.x) release with HostScan, the HostScan Module (if previously installed) on the endpoint and the HostScan package on the Secure Firewall ASA must be upgraded to 4.9.04045 or later.

Due to this dynamic adoption in supporting Apple Silicon (M1 chip), macOS endpoints using AnyConnect 4.10.02086 or later must also upgrade the HostScan package version to 4.10.02086 or later. The following chart outlines the minimum requirements:

AnyConnect Version	HostScan Engine (.pkg) Minimum Version Supported/Required
4.10.01075 or earlier	All versions posted on CCO are supported. The most recent HostScan.pkg that is posted is always suggested.
4.10.02086 or later	4.10.02086 or later is required. The most recent HostScan .pkg that is posted is always suggested.

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

Notice of End Date for HostScan 4.3.x

HostScan updates for AnyConnect 4.3 and earlier stopped on December 31, 2018. HostScan updates are provided for the HostScan 4.6 (and later) module, which is compatible with AnyConnect 4.4.x (and later) and ASDM 7.9.2 (and later). HostScan migration information is detailed in this migration guide.

End of Support (EOS) for HostScan 4.3.x was announced December 31, 2018. 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.

ISE Posture Compliance Module

(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 HostScan 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 AnyConnect

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 AnyConnect features:

- Post Log-in Always-on VPN
- Connect Failure Policy

- Client Firewall providing Local Printer and Tethered Device access
- Optimal Gateway Selection
- Quarantine
- AnyConnect 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.

AnyConnect Supported Operating Systems

Windows and macOS

Supported Windows and macOS OSs	VPN	Network Access Manager	HostScan	ISE Posture	DART	Customer Experience Feedback	Network Visibility Module	AMP Enabler	Umbrella Roaming Security
Windows 7, 8, 8.1, and current Microsoft supported versions of Windows 10 x86(32-bit) and x64(64-bit)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft-supported versions of Windows 11 for ARM64-based PCs					Yes				No
	Yes	No	Yes	No	Yes	Yes	No	No	No
macOS 11.x, 10.15, 10.14, and 10.13 (only 64-bit is supported from 10.15 and later)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Linux Red Hat 8.2, 7, 6, & Ubuntu 20.04 LTS), 18.04 (LTS), and 16.04 (LTS)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No

Linux

Supported Linux OSs	VPN	HostScan	Network Visibility Module	ISE Posture	DART	Customer Experience Feedback
Red Hat	All 7.x and 8.x	All 7.x and 8.x	All 7.x and 8.x	7.5 (and later) and 8.1 (and later)	Yes	Yes

Supported Linux OSs	VPN	HostScan	Network Visibility Module	ISE Posture	DART	Customer Experience Feedback
Ubuntu	18.04 and 20.04	18.04 and 20.04	18.04 and 20.04	18.04 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

AnyConnect 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 AnyConnect, and reinstall it after your Windows upgrade is complete.
- Upgrading from Windows XP to any later Windows release requires a clean install since the AnyConnect Virtual Adapter is not preserved during the upgrade. Manually uninstall AnyConnect, upgrade Windows, then reinstall AnyConnect manually or via WebLaunch.
- To start AnyConnect 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.
- AnyConnect 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 AnyConnect 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 AnyConnect connection again.

- Outdated wireless cards or wireless card drivers that do not support Windows 8 prevent AnyConnect 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.

- AnyConnect is not integrated with the new UI framework, known as the Metro design language, that is deployed on Windows 8; however, AnyConnect does run on Windows 8 in desktop mode.
- HP Protect tools do not work with AnyConnect 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 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 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.

AnyConnect Support for Linux

Linux Requirements

- Using VPN CLI without GUI sessions (for example SSH) is not supported
- The Snap version of Firefox is not supported by AnyConnect on Linux
- x86 instruction set
- 64-bit processor
- 32 MB RAM
- 20 MB hard disk space
- Superuser privileges are required for installation
- network-manager
- libnm (libnm.so or libnm-glib.so)
- libstdc++ users must have libstdc++.so.6(GLIBCXX_3.4) or higher, but below version 4
- Java 5 (1.5) or later. The only version that works for web installation is Sun Java. You must install Sun Java and configure your browser to use that instead of the default package.
- zlib - to support SSL deflate compression
- xterm - only required if you're doing initial deployment of AnyConnect via Weblaunch from ASA clientless portal
- gtk 2.24
- systemd
- webkitgtk+ 2.10 or later, required only if you are using the AnyConnect embedded browser app
- iptables 1.2.7a or later
- tun module supplied with kernel 2.4.21 or 2.6

AnyConnect Support for macOS

macOS Requirements

- AnyConnect requires 50MB of hard disk space.
- To operate correctly with macOS, AnyConnect requires a minimum display resolution of 1024 by 640 pixels.

macOS Guidelines

- AnyConnect 4.8 (and later) for macOS has been notarized, and installer disk images (dmg) have been stapled.

AnyConnect Licensing

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

For our open source licensing acknowledgments, see Open Source Software Used in AnyConnect Secure Mobility Client.

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

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

AnyConnect Installation Overview

Deploying AnyConnect refers to installing, configuring, and upgrading the AnyConnect and its related files. The AnyConnect 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 AnyConnect 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, AnyConnect is deployed to the client.
  - For new installations, the user connects to a headend to download AnyConnect. The client is either installed manually, or automatically (web-launch).
  - Updates are done by AnyConnect running on a system where AnyConnect is already installed, or by directing the user to the Secure Firewall ASA clientless portal.
- Cloud Update—After the Umbrella Roaming Security module is deployed, you can update any AnyConnect modules using one of the above methods, as well as Cloud Update. With Cloud Update, the software upgrades are obtained automatically from the Umbrella cloud infrastructure, and the update track is dependent upon that and not any action of the administrator. By default, automatic updates from Cloud Update are disabled.

When you deploy AnyConnect, 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 AnyConnect 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 HostScan 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 AnyConnect 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 AnyConnect 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.

AnyConnect Support Policy

Cisco only provides fixes and enhancements based on the most recent Version 4.10 release. TAC support is available to any customer with an active AnyConnect Version 4.10 term/contract running a released version of AnyConnect Version 4.10. 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 AnyConnect Version 4.10 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

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 AnyConnect.

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 AnyConnect 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, AnyConnect 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 AnyConnect 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 AnyConnect Network Access Manager service.
2. From the administrator command prompt, enter

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

This removes leftover profiles from previous versions (AnyConnect 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) AnyConnect 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 AnyConnect 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.
- HostScan and System Scan users on macOS 10.15 will experience permission popups during initial launch.

HostScan 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.

To enable successful VPN connections for HostScan users, all DAP and HostScan 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 HostScan packages on their Secure Firewall ASA headends may disable HostScan. If disabled, allHostScan 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 HostScan or System Scan 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 HostScan, System Scan (when ISE posture is enabled on the network), or DART (when ISE posture or AnyConnect is installed). ISE posture and HostScan 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 AnyConnect Secure Mobility 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

AnyConnect 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 AnyConnect 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/anyconnect/bin folder.
4. Enter the password when prompted.
5. Quit Keychain Access and stop the VPN service.
6. Restart.

No Detection of Default Patch Management in ISE Posture (CSCvq64901)

ISE posture failed to detect the default Patch Management while using macOS 10.15. An OPSWAT fix is required to remedy this situation.

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, AnyConnect 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, AnyConnect 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 AnyConnect 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.

AnyConnect 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 AnyConnect is upgraded before a user's system is upgraded to macOS 10.13 and later, the user will automatically have the AnyConnect 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 AnyConnect.

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 AnyConnect 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 AnyConnect 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 AnyConnect profile to restrict AnyConnect 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 AnyConnect.

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 AnyConnect Umbrella Roaming Security Module section.

Microsoft Inadvertently Blocks Updates to Windows 10 When Network Access Manager is Installed

Microsoft intended to block updates to earlier versions of Windows when the Network Access Manager is installed, but Windows 10 and Creators Edition (RS2) were inadvertently blocked as well. Because of the error (Microsoft Sysdev 11911272), you must first uninstall the Network Access Manager module before you can upgrade to the Creators Editor (RS2). You can then reinstall the module after the upgrade. Microsoft's fix for this error is planned for June 2017.

Windows 10 Defender False Positive—Cisco AnyConnect Adapter Issue

When upgrading to Windows 10 Creator Update (April 2017), you may encounter a Windows Defender message that the AnyConnect adapter has an issue. Windows Defender instructs you to enable the adapter under the Device Performance and Health section. In actuality, the adapter should be disabled when not in use, and no manual action should be taken. This false positive error has been reported to Microsoft under Sysdev # 11295710.

AnyConnect 4.4MR1 (or later) and 4.3MR5 are compatible with Windows 10 Creators Edition (RS2).

AnyConnect Compatibility with Microsoft Windows 10

For best results, we recommend a clean install of AnyConnect 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 AnyConnect pre-installed, make sure that you first upgrade AnyConnect 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 AnyConnect 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 AnyConnect profile (in the Preferences Part 1 menu) of the profile editor. (You also have the option to make it user controllable.)

Microsoft Phasing out SHA-1 Support

A secure gateway with a SHA-1 certificate or a certificate with SHA-1 intermediate certificates may no longer be considered valid by a Windows Internet Explorer 11 / Edge browser or a Windows AnyConnect endpoint after February 14, 2017. After February 14, 2017, Windows endpoints may no longer consider a secure gateway with a SHA-1 certificate or intermediate certificate as trusted. We highly recommend that your secure gateway does not have a SHA-1 identity certificate and that any intermediate certificates are not SHA-1.

Microsoft has made modifications to their original plan of record and timing. They have published details for how to test whether your environment will be impacted by their February 2017 changes. Cisco is not able to make any guarantees of correct AnyConnect operation for customers with SHA-1 secure gateway or intermediate certificates or running old versions of AnyConnect.

Cisco highly recommends that customers stay up to date with the current maintenance release of AnyConnect in order to ensure that they have all available fixes in place. The most up-to-date version of AnyConnect 4.x and beyond are available Cisco.com Software Center for customers with active AnyConnect Plus, Apex, and VPN Only terms/contracts. AnyConnect Version 3.x is no longer actively maintained and should no longer be used for any deployments.

Note Cisco has validated that AnyConnect 4.3 and 4.4 (and beyond) releases will continue to operate correctly as Microsoft further phases out SHA-1. Long term, Microsoft intends to distrust SHA-1 throughout Windows in all contexts, but their current advisory does not provide any specifics or timing on this. Depending on the exact date of that deprecation, many earlier versions of AnyConnect may no longer operate at any time. Refer to Microsoft's advisory for further information.

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

OpenSSL Cipher Suites Changes

Because the OpenSSL standards development team marked some cipher suites as compromised, we no long support them beyond AnyConnect 3.1.05187. The unsupported cipher suites include the following: DES-CBC-SHA, RC4-SHA, and RC4-MD5.

Likewise, our crypto toolkit has discontinued support for RC4 ciphers; therefore, our support for them will be dropped with releases 3.1.13011 and 4.2.01035 and beyond.

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 AnyConnect 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.

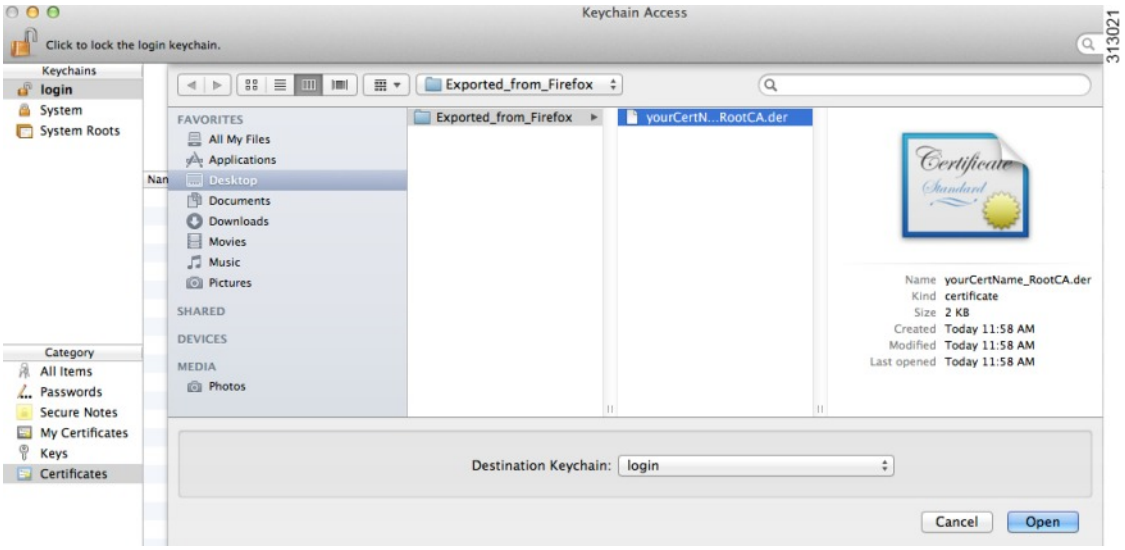
Firefox Certificate Store on macOS is Not Supported

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. AnyConnect no longer utilizes the Firefox store for either server validation or client certificates.

If necessary, instruct your users how to export your AnyConnect 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 AnyConnect users.

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

   Your AnyConnect 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.

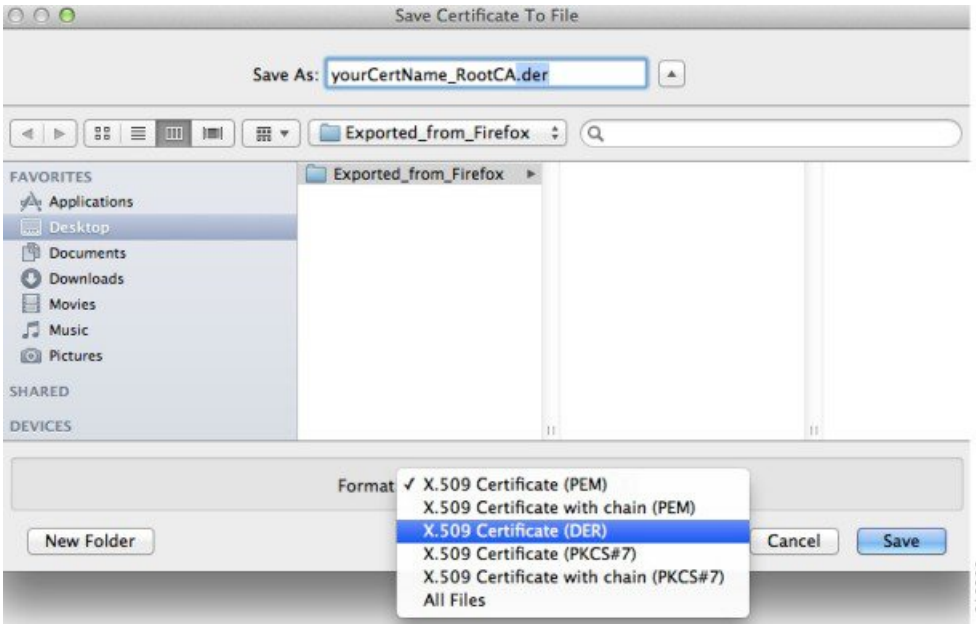


Note If more than one AnyConnect Certificate and/or a Private Key is used/required, repeat the above process for each Certificate).

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 AnyConnect.

SSLv3 Prevents HostScan From Working

(CSCue04930) HostScan does not function when the SSLv3 options SSLv3 only or Negotiate SSL V3 are chosen in ASDM (Configuration > Remote Access VPN > Advanced > SSL Settings > The SSL version for the security appliance to negotiate as a server). A warning message displays in ASDM to alert the administrator.

WebLaunch Issues With Safari

There is an issue with Weblaunch with Safari. The default security settings in the version of Safari that comes with OS X 10.9 (Mavericks) prevents AnyConnect Weblaunch from working. To configure Safari to allow Weblaunch, edit the URL of the ASA to Unsafe Mode, as described below.

Safari 9 (and earlier)

1. Open Safari **Preferences**.
2. Choose **Security** preference.
3. Click **Manage Website Settings...** button.
4. Choose **Java** from the options listed on the left side.
5. Change the option from **Block** to **Allow Always** for the website "Hostname_or_IP_address" that you are trying to connect to.
6. Click **Done**.

Safari 10 (and later)

1. Open Safari **Preferences**.

2. Choose **Security** preference.
3. Check the **Internet plug-ins:** option to **allow plug-ins.**
4. Choose **Plug-in Settings** button.
5. Choose **Java** from the options listed on the left side.
6. Highlight the "Hostname_or_IP_address" that you are trying to connect to.
7. Hold **Alt** (or **Option**) and click the drop-down menu. Make sure that **On** is checked, and **Run in Safe Mode** is unchecked.
8. Click **Done**.

Active X Upgrade Can Disable Weblaunch

Automatic upgrades of AnyConnect 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 AnyConnect pre-installer, SMS, GPO or other administrative deployment methodology.

Java 7 Issues

Java 7 can cause problems with AnyConnect and HostScan. 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 > CiscoHostScan.

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, AnyConnect adds a specific route to the local DHCP server when AnyConnect connects. To prevent data leakage on this route, AnyConnect also applies an implicit filter on the LAN adapter of the host machine, blocking all traffic for that route except DHCP traffic.

AnyConnect 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 AnyConnect before deployment.

AnyConnect Smart Card Support

AnyConnect 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 AnyConnect does not support Smart cards on Linux or PKCS #11 devices.

AnyConnect Virtual Testing Environment

Cisco performs a portion of AnyConnect 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 AnyConnect in virtual environments; however, we expect AnyConnect to function properly in the VMWare environments we test in.

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

UTF-8 Character Support for AnyConnect Passwords

AnyConnect 3.0 or later used with Secure Firewall ASA 8.4(1) or later supports UTF-8 characters in passwords sent using RADIUS/MSCHAP and LDAP protocols.

Disabling Auto Update May Prevent Connectivity Due to a Version Conflict

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

To avoid this problem, configure the same version or earlier AnyConnect 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 AnyConnect 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.

Avoiding SHA 2 Certificate Validation Failure (CSCtn59317)

The AnyConnect client relies on the Windows Cryptographic Service Provider (CSP) of the certificate for hashing and signing of data required during the IKEv2 authentication phase of the IPsec/IKEv2 VPN connection.

If the CSP does not support SHA 2 algorithms, and the ASA is configured for the pseudo-random function (PRF) SHA256, SHA384, or SHA512, and the connection profile (tunnel-group) is configured for certificate or certificate and AAA authentication, certificate authentication fails. The user receives the message Certificate Validation Failure.

This failure occurs for Windows only, for certificates that belong to CSPs that do not support SHA 2-type algorithms. Other supported OSs do not experience this problem.

To avoid this problem you can configure the PRF in the IKEv2 policy on the ASA to md5 or sha (SHA 1). Alternatively, you can modify the certificate CSP value to native CSPs that work such as Microsoft Enhanced RSA and AES Cryptographic Provider. Do not apply this workaround to SmartCards certificates. You cannot change the CSP names. Instead, contact the SmartCard provider for an updated CSP that supports SHA 2 algorithms.

Caution Performing the following workaround actions could corrupt the user certificate if you perform them incorrectly. Use extra caution when specifying changes to the certificate.

You can use the Microsoft Certutil.exe utility to modify the certificate CSP values. Certutil is a command-line utility for managing a Windows CA, and is available in the Microsoft Windows Server 2003 Administration Tools Pack. You can download the Tools Pack at this URL:

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en

Follow this procedure to run Certutil.exe and change the Certificate CSP values:

1. Open a command window on the endpoint computer.
2. View the certificates in the user store along with their current CSP value using the following command:**`certutil -store -user My`**

   The following example shows the certificate contents displayed by this command:

```
================ Certificate 0 ================
Serial Number: 3b3be91200020000854b
Issuer: CN=cert-issuer, OU=Boston Sales, O=Example Company, L=San Jose,
S=CA, C=US, E=csmith@example.com
NotBefore: 2/16/2011 10:18 AM
NotAfter: 5/20/2024 8:34 AM
Subject: CN=Carol Smith, OU=Sales Department, O=Example Company, L=San Jose, S=C
A, C=US, E=csmith@example.com
Non-root Certificate
Template:
Cert Hash(sha1): 86 27 37 1b e6 77 5f aa 8e ad e6 20 a3 14 73 b4 ee 7f 89 26
  Key Container = {F62E9BE8-B32F-4700-9199-67CCC86455FB}
  Unique container name: 46ab1403b52c6305cb226edd5276360f_c50140b9-ffef-4600-ada
6-d09eb97a30f1
  Provider = Microsoft Enhanced RSA and AES Cryptographic Provider
Signature test passed
```

3. Identify the <CN> attribute in the certificate. In the example, the CN is Carol Smith. You need this information for the next step.
4. Modify the certificate CSP using the following command. The example below uses the subject <CN> value to select the certificate to modify. You can also use other attributes.

   On Windows 7 or later, use this command: **`certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -f -repairstore -user My <CN> carol smith`**

5. Repeat step 2 and verify the new CSP value appears for the certificate.

Configuring Antivirus Applications for AnyConnect

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

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

AnyConnect 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, AnyConnect prompts the user to enter credentials for every full authentication if the active profile requires it.

User Guideline for Cisco Cloud Web Security Behavior with IPv6 Web Traffic

Unless an exception for an IPv6 address, domain name, address range, or wild card is specified, IPv6 web traffic is sent to the scanning proxy where it performs a DNS lookup to see if there is an IPv4 address for the URL the user is trying to reach. If the scanning proxy finds an IPv4 address, it uses that for the connection. If it does not find an IPv4 address, the connection is dropped.

If you want all IPv6 traffic to bypass the scanning proxies, you can add this static exception for all IPv6 traffic ::/0. Doing this makes all IPv6 traffic bypass all scanning proxies. This means that IPv6 traffic is not protected by Cisco Cloud Web Security.

Preventing Other Devices in a LAN from Displaying Hostnames

After one uses AnyConnect 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 AnyConnect host prevents the hostname leak between subnets, including the name of the AnyConnect 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 AnyConnect certificate revocation warning popup window opens after authentication if AnyConnect 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. "
```

AnyConnect for macOS Performance when Behind Certain Routers

When AnyConnect for macOS attempts to create an SSL connection to a gateway running IOS, or when AnyConnect 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. AnyConnect may calculate the MTU incorrectly.

To work around this problem, manually set the MTU for the AnyConnect 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 AnyConnect 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 AnyConnect unstable. When using AnyConnect, we do not recommend enabling this feature or running front-end applications that enable it (such as Connectify or Virtual Router).

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

AnyConnect 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.

AnyConnect 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 HostScan Reports

None of the supported antimalware and firewall products report the last scan time information. HostScan 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 AnyConnect 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 AnyConnect Secure Mobility Client

AnyConnect Secure Mobility 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 AnyConnect. 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 AnyConnect API, send e-mail to the following address: anyconnect-api-support@cisco.com.

AnyConnect 4.9.06037

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
CSCvw53140	certificate	Smartcard issues with VPN module on Windows
CSCvw54056	core	Persistent "Cisco System Extensions Blocked" prompt after upgrading AC 4.8 to 4.904043 on Big Sur

Identifier	Component	Headline
CSCvw26076	nam	NAM PE: Add administrative control over defaults for "Allow Connection Before Logon" user setting
CSCvx25251	nvm	NVM installation fails with latest kernel version of Ubuntu 20
CSCvv73666	opswat-ise	ISE posture disk encryption condition fails due to nonstandard characters in a volume name
CSCvt62025	posture-ise	Posture Module should trigger on adapter state change
CSCvw72250	vpn	macOS: DNS queries by short name failing if FQDN matches DNS name other than the default domain
CSCvw92182	vpn	AnyConnect on macOS connected to the ASA TLS-only is reconnecting about 20 seconds after connection

AnyConnect 4.9.05042

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
CSCvw19751	core	macOS dual-NIC: Tunnel cannot be reestablished after disconnecting and reconnecting one of the NICs
CSCvw21846	nam	NAM service crashes when configured to include root CA certs only
CSCvw55271	nam	User network allowed to set "Allow Connect Before Logon" when user control policy does not allow

Identifier	Component	Headline
CSCvw23375	posture-ise	ISE posture not detecting Crowdstrike version 6.x
CSCvw30269	vpn	macOS: Pre-VPN connection, previously allowed by 3rd party filtering, not blocked by AnyConnect

AnyConnect 4.9.04053

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
CSCvw48062	download_install	Restrict optional file web-deploy of custom scripts, help files, UI, & localization via Local Policy

AnyConnect 4.9.04043

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
CSCvu27862	core	Multiple vulnerabilities in jquery 3.2.1
CSCvv68334	core	Calling vpncli for status pre-logon causes post logon tunnel to connect then terminate
CSCvv91510	core	Always on/TND - DHCP-enabled directly connected computers

Identifier	Component	Headline
CSCvv91836	nam	802.11 4 way handshake does not complete when TLS RSA ciphers selected for key exchange
CSCvv35857	opswat-ise	AnyConnect ISE Posture Compliance Module update to support Check Point Endpoint Security 83.x
CSCvv69211	posture-ise	When modern standby is enabled on windows, AnyConnect may receive several internal error popups
CSCvv30401	vpn	macOS network connectivity issues after applying 200+ dynamic tunnel exclusions
CSCvv43515	vpn	Zoom app slowness configured with dynamic split exclude tunneling
CSCvv45271	vpn	VPN tunnel disconnects after ASA upgrade with AutoConnectOnStart is true
CSCvv61677	vpn	device-mac/device-public-mac ACIDEX attributes are not sent from AnyConnect when using Bluetooth NIC
CSCvv68971	vpn	macOS: remove SOCKS protocol when private proxy settings are pushed to make consistent with Windows
CSCvv89360	vpn	AnyConnect ignores the client profile config if the URL in server list has a non-default port number
CSCvv94399	vpn	AC unable to enroll to local CA unless tunnel-group-list is enabled
CSCvw23502	vpn	AnyConnect does not attempt user certificates for authentication on Windows for SSL connections

AnyConnect 4.9.03049

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
CSCvw14118	vpn	VPN - Windows - Authentication fails when username/password has Cyrillic/Unicode characters

AnyConnect 4.9.03047

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
CSCvs28224	core	Flexvpn on router does not work when using default ike-id with EAP auth
CSCvu14970	core	Cisco AnyConnect AllowRemoteUsers bypass
CSCvu77777	core	CIAM: sqlite 3.28.0
CSCvu78363	core	AnyConnect Start Before Logon (SBL) displays incorrect name when Native VPN client is configured
CSCvu83063	core	Multi-homed machine causes AnyConnect reconnect(s) when Dynamic Split Exclude Tunneling is enabled
CSCvv02329	core	AnyConnect 4.8.03052 skips IPv4 when connecting to backup server
CSCvv39691	core	AnyConnect management tunnel failing on Windows startup prior login to PC when using AnyConnect 4.9

Identifier	Component	Headline
CSCvt28992	nam	AnyConnect shows invalid RSSI of -256 when connected to wireless while actually connected just fine
CSCvu26049	nam	NAM crashes with unexpected EAP-FAST PAC provisioning success
CSCvu65082	nam	NAM logs showing incorrect timezone
CSCvv11582	nam	Dot1x NAM EAP chaining error on ISE "Failure reason 12963 received malformed EAP payload TLV"
CSCvv32331	nam	NAM sends multiple EAP start requests before timeout
CSCvv45245	nam	Regression of CSCvs59943 NAM unable to open wireless connection because adapter stuck associating
CSCvv31801	nvm	When upgrade from NVMS to AC+NVM observed that TND state is changed from trusted to untrusted
CSCvq97293	opswat-ise	ENH: Compliance module support for Bitdefender 8.0.0.3 for macOS
CSCvs82258	opswat-ise	Support for LANDesk 11.x Security and Patch Manager
CSCvt07676	opswat-ise	CM 4.3.1053.6145 returning current date/time as Definition date for Sophos Cloud Endpoint
CSCvu65632	opswat-ise	ISE posture module is not detecting Windows firewall status correctly
CSCvt36028	posture-ise	Support for Avast Free 20.1 xxxx in ISE
CSCvu99746	posture-ise	Failure with 'aciseposture' process launch intermittently in macOS
CSCvr70933	vpn	AnyConnect VPN tunnel on macOS interferes with Sidecar feature
CSCvv09906	vpn	IPsec to ISE VPN attribute of type 5 received, which does not meet the minimum requirement of 1

Identifier	Component	Headline
CSCvv10339	vpn	VPNLB: AnyConnect is unable to connect VIP through proxy authentication
CSCvv65303	vpn	macOS 11: DNS resolution broken system-wide after resume from sleep with VPN connected

AnyConnect 4.9.02028

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
CSCvu57985	core	ENH: Support for NetworkExtension on AnyConnect

AnyConnect 4.9.01095

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
CSCvp53403	core	Unexpected (incorrect) <HostName> is displayed in GUI after connecting via SBL
CSCvt08780	core	VM instance/Docker container on Linux cannot route network traffic
CSCvu03376	core	Using 'Auto detect proxy' (Private Proxy set on Group Proxy) causes intermittent browsing failures
CSCvu19710	core	Unable to modify the IP forwarding table error when using WiFi calling (FaceTime calling)

Identifier	Component	Headline
CSCvu82615	core	VPN client agent's DNS component experienced an unexpected error (dynamic split tunneling)
CSCvv15092	core	High memory utlization reported on AnyConnect 4.9.00086 on macOS
CSCvu65566	dart	Linux DART generates same UDID even for non-cloned OS
CSCvu22557	download_install	After upgrading from 4.8.3052 to 4.9.64, AnyConnect fails to establish VPN connection over IPsec
CSCvu03997	gui	macOS embedded SAML browser does not download .dmg files
CSCvs78379	nam	Does not stay connected during logon to a WiFi network created using the SBL GUI
CSCvs86736	nam	NAM should allow use of PAC files larger than 1024 bytes
CSCvt06237	nam	Add option for user created networks to connect during machine time to support VPN management tunnel
CSCvt74330	nam	NAM client fails to switch to user-defined network when admin configured hidden network not available
CSCvu24358	nam	Unable to log in locally after closing RDP session on a PC with NAM
CSCvu26262	nam	NAM cred provider does not load Imprivata OneSign Agent cred provider DLL
CSCvq97328	opswat-ise	ENH: Compliance module support for Kaspersky Internet Security 20.x for macOS
CSCvu83305	opswat-ise	AnyConnect AM condition for Cortex 7.x

Identifier	Component	Headline
CSCvc89249	posture-ise	Support for TrendMicro WorryFree 6.x for posture
CSCvm56656	posture-ise	AC compliance module 4.3.x support for ESET Endpoint Security 7.x
CSCvo46838	posture-ise	Kaspersky endpoint security 11.x not present in disk encryption in posture remediation
CSCvp27316	posture-ise	ENH: Compliance module support for Trend Micro Apex One 14.x
CSCvq20688	posture-ise	Posture KES11 support for macOS
CSCvu06725	swg	SWG client crash/freeze
CSCvu63661	umbrella	DNS resolution hangs globally after sending multiple TCP DNS requests with large response
CSCvu68957	umbrella	Umbrella sync and state change delay on macOS
CSCvu73467	umbrella	Umbrella DNS protection disabled after enabling dynamic IPv6 config on NIC (with IPv6 DNS server)
CSCvf65224	vpn	ENH: Allow AnyConnect to search for CA certificates in /etc/ssl/certs directory on Linux machines
CSCvt35162	vpn	AnyConnect SBL icon goes missing because of the Windows feature Automatic Restart Sign-On (ARSO)
CSCvt49314	vpn	AnyConnect reconnects multiple times after an active DTLS session reverts to TLS
CSCvt63861	vpn	AnyConnect installation instructions for Linux platform with Weblaunch is showing incorrect OS image
CSCvt64638	vpn	Windows only: AnyConnect does not support Unicode characters in the interface name

Identifier	Component	Headline
CSCvt85695	vpn	AnyConnect offers Diffie-Hellman group 1 or 2 in initial IKE_SA_INIT
CSCvu95344	vpn	AnyConnect fails to disconnect VPN upon smartcard removal
CSCvv19684	vpn	Cloud upgrade doesn't kick in from 4.9 FCS to 4.9 MR1

AnyConnect 4.9.00086

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
CSCvs60391	core	Multiple vulnerabilities in OpenSSL 1.0.2q
CSCvs60397	core	Multiple vulnerabilities in libxml2 2.9.8
CSCvt31657	core	Umbrella/SWG client does not honor O365 Bypass
CSCvt74385	core	Delay in macOS/pfctl when adding dynamic split exclusions
CSCvt92079	core	macOS - Intermittent OS memory allocation failure leaves IPv6 route table in inconsistent state
CSCvu46279	core	macOS - Delay in passing network traffic due to vpnagent being blocked
CSCvu22557	download_install	After upgrading from 4.8.3052 to 4.9.64 AnyConnect fails to establish VPN connection over IPsec
CSCvt82526	gui	AnyConnect for Windows VPN SAML browser sometimes generates duplicate JavaScript key events

Identifier	Component	Headline
CSCvu03997	gui	macOS embedded SAML browser does not download dmg files
CSCvm85974	nam	AnyConnect NAM does not reprompt for password in case of entering wrong password for SSID with PSK
CSCvt99342	nam	Unauthenticated PAC provisioning no longer supported - 4.9 and later
CSCvu13185	nam	NAM PE: Add config policy option to allow user created networks to connect during machine time
CSCvu06461	nvm	CFlows dropped when the path and args are bigger
CSCvt12850	nvm	Android-NVM: Cashed flows are not sent out immediately when NVM TND is configured as untrusted
CSCvu01704	nvm	NVM collector does not preload nvzFlowV4 templates
CSCvu21676	nvm	Linux: NVMAgent crash while fetching process args
CSCvr21787	opswat-ise	ENH: Support for Trend Micro OfficeScan Client version 14.x
CSCvc89249	posture-ise	Support for TrendMicro WorryFree 6.x for posture
CSCvm56656	posture-ise	AnyConnect Compliance module 4.3.x support for ESET Endpoint Security 7.x
CSCvo46838	posture-ise	Kaspersky endpoint security 11.x not present in disk encryption in posture remediation
CSCvp27316	posture-ise	ENH: Compliance module support for Trend Micro Apex One 14.x
CSCvq20688	posture-ise	Posture KES11 support for macOS
CSCvt72492	umbrella	Umbrella cloud update parameter change not always applied on Windows

Identifier	Component	Headline
CSCvf32537	vpn	ENH: VPN high bandwidth/throughput performance improvements for AnyConnect
CSCvq74726	vpn	ENH: AnyConnect dynamic split tunneling should support scenarios with low TTL
CSCvs78426	vpn	DHCP traffic incorrectly sent over VPN tunnel
CSCvt49314	vpn	AnyConnect reconnects multiple times after an active DTLS session reverts to TLS
CSCvt75904	vpn	macOS: Umbrella stuck in reserved state on macOS
CSCvt81585	vpn	AnyConnect VPN fails to connect with an error HTTP/1.1 401 Unauthorized X-Reason: Other error
CSCvt85695	vpn	AnyConnect should not offer Diffie-Hellman group 1 or 2 in the initial IKE_SA_INIT
CSCvt88461	vpn	AnyConnect VPN fails to connect after upgrade with HTTP/1.1 401 Unauthorized X-Reason: Other error
CSCvt90659	vpn	AC 4.8.3036 macOS: DNS queries by short name not working - macOS resolver not appending default domain
CSCvt95013	vpn	AnyConnect VPN load balancing IKEv2 fails on AC 4.8
CSCvu03917	vpn	AnyConnect connection failure with automatic certificate selection enabled
CSCvu10868	vpn	Dynamic split exclude breaks connectivity if static split exclude is supernet of a dynamic exclusion
CSCvt65103	vpn-wer	ENH: AnyConnect support for non-RDP remote desktop types

Open

To find the latest information about open defects in this release, refer to the Cisco Bug Search Tool:

Identifier	Component	Headline
CSCvo32995	nam	ENH: Add support for "Connect Automatically" feature for individually configured wireless networks
CSCvu51439	nvm	Whenever NVM profile is edited on ASDM, TND config is duplicated and pushed to endpoint

HostScan 4.9.06046

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
CSCvx11008	posture-asa	Cybereason ActiveProbe on macOS not detected by HostScan 4.9.04045 or 4.9.05042
CSCvx38993	posture-asa	HostScan unable to retrieve the serial number of macOS Big Sur with Apple M1 chip inserted

HostScan 4.9.06037

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
CSCvw93595	opswat-asa	Add support for Server Name Identification (SNI)

HostScan 4.9.05042

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
CSCvv79007	opswat-asa	Support to detect MS Defender ATP (Antimalware Client Version 101.01.54 & 101.06.63) with HostScan
CSCvw72925	opswat-asa	HostScan 4.9.04045 unable to detect the CrowdStrike 6.x version

HostScan 4.9.04045

HostScan 4.9.04045 includes updated OPSWAT engine versions for Windows, macOS, and Linux. Refer to the HostScan Support Charts under Release and Compatibility for additional information.

HostScan 4.9.03057

HostScan 4.9.03057 includes updated OPSWAT engine versions for Windows, macOS, and Linux. Refer to HostScan Support Charts under Release and Compatibility for additional information.

HostScan 4.9.02028

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
CSCvu16574	opswat-asa	ENH: AnyConnect HostScan support for Endgame (Elastic) Anti-Malware 3.52.14

HostScan 4.9.01095

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
CSCvr90986	opswat-asa	ENH: HostScan support for Microsoft Defender Advanced Threat Protection (ATP) for Win 10 endpoints
CSCvu14696	opswat-asa	HostScan Ciscod daemon creates multiple codesign/pkgutil processes
CSCvu20458	opswat-asa	HostScan incorrectly reports Windows Defender versions higher than 4.18.1902.5
CSCvt12241	posture-asa	AnyConnect 4.9.x HostScan is stuck in Posture Assessment initiating on Linux

HostScan 4.9.00086

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
CSCvt12241	posture-asa	AC 98.136.00022 (4.9) HostScan is stuck in Posture Assessment initiating on Linux

Related Documentation

Other AnyConnect Documents

- Cisco AnyConnect Secure Mobility Client Administrator Guide
- Cisco AnyConnect Secure Mobility Client Features, Licenses, and OSs
- Open Source Software Used in AnyConnect Secure Mobility Client
- Cisco General Terms, AnyConnect Secure Mobility Client, Release 4.x

ASA Related Documents

- Release Notes for the Cisco ASA Series
- Navigating the Cisco ASA Series Documentation
- Cisco ASA 5500-X Series Next-Generation Firewalls, Configuration Guides
- Supported VPN Platforms, Cisco ASA 5500 Series
- HostScan Support Charts

ISE Related Documents

- Release Notes for Cisco Identity Service Engine