Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.10

Release Notes for AnyConnect Secure Mobility Client, Release 4.10

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 AnyConnect release 4.10.x will become the maintenance path for any 4.x bugs. AnyConnect 4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, and 4.9 customers must upgrade to AnyConnect 4.10.x to benefit from future defect fixes. Any defects found in AnyConnect 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x, 4.5.x, 4.6.x, 4.7.x, 4.8.x, and 4.9.x will be fixed in the AnyConnect 4.10.x maintenance releases only.

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 Cisco 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**.

Step 8 See the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.x.

AnyConnect 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)	anyconnect-linux64-*version*-predeploy-k9.tar.gz

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

AnyConnect 4.10.00093 New Features

This is a major release that includes the following features and support updates, and that resolves the defects described in AnyConnect 4.10.00093, on page 29:

- Enhanced captive portal remediation now supported in macOS.
- Architecture improvement of downloader to address local platform security concerns.
- Ability to individually allow/disallow scripts, help, resources, or localization updates in Local Policy, while previously they were part of Allow Software Updates.
- CiscoSSL changes: enable EMS for only TLS, and disable EMS for DTLS.
- Operating system support has changed to eliminate older versions. Refer to AnyConnect Supported Operating Systems, on page 6.
- Revision to Linux requirements (due to Linux build toolchain/GTK migration). Refer to AnyConnect Support for Linux, on page 9.

AnyConnect HostScan Engine Update 4.10.00093 New Features

AnyConnect HostScan 4.10.00093 includes updates to the HostScan module and resolves the defects listed in HostScan 4.10.00093, on page 31.

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 Secure Mobility Client 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.

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 NAM 4.7 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.

ISE Licensing Requirements

To deploy AnyConnect from an ISE headend and use the ISE Posture module, a Cisco ISE Apex 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.

ASA Requirements for AnyConnect

Minimum ASA/ASDM Release Requirements for Specified Features

- You must upgrade to ASA 9.10.1 (or later) and ASDM 7.10.1 (or later) to use DTLSv1.2.

Note DTLSv1.2 is supported on all 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 NVM.
- You must upgrade to ASDM 7.4.2 to use AMP Enabler.
- You must upgrade to ASA 9.3(2) to use TLS 1.2.
- You must upgrade to ASA 9.2(1) if you want to use the following features:
  - ISE Posture over VPN
  - ISE Deployment of AnyConnect 4.x
  - Change of Authorization (CoA) on ASA is supported from this version onwards
- You must upgrade to 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 client deferred upgrades
  - Management VPN Tunnel (Custom Attributes)
- You must use 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, Web Security, or Telemetry).
  - Use the services supported by a Cisco IronPort Web Security Appliance. These services let you enforce acceptable use policies and protect endpoints from websites found to be unsafe, by granting or denying all HTTP and HTTPS requests.
  - 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.

ASA Memory Requirements

Caution The minimum flash memory recommended for all ASA 5500 models using AnyConnect 4.0 or later 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 ASA 5505 (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 (i.e. fewer OSs, no HostScan, etc,) 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 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 client packages on the ASA. Even if you have enough space on the flash to hold the package files, the 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 5500 series.

VPN Posture and HostScan Interoperability

The VPN Posture (HostScan) Module provides the Cisco AnyConnect Secure Mobility Client the ability to identify the operating system, antimalware, and firewall software installed on the host to the ASA.

The VPN Posture (HostScan) Module requires HostScan to gather this information. 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 Logon (SBL) and HostScan, you must install the AnyConnect/HostScan posture 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.

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

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 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.

Advanced Notice of End Date for AnyConnect 4.3 HostScan Updates

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.

ISE Posture Compliance Module

The ISE Posture compliance module contains the list of supported antimalware and firewall for ISE posture. While the HostScan list organized by vendor, the ISE posture list organizes by product type. When the version number on the headend (ISE or 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 modulesfor 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

Cisco AnyConnect Secure Mobility Client supports the following operating systems for its contained modules:

Supported Operating Systems	VPN Client	Network Access Manager	Cloud Web Security	VPN Posture (HostScan)	ISE Posture	DART	Customer Experience Feedback	Network Visibility Module	AMP Enabler	Umbrella Roaming Security
Microsoft-supported versions of Windows 10 for ARM64-based PCs	Yes	No	No	No	No	Yes	Yes	No	No	No
Windows 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	Yes
macOS 11.2 (or later), 10.15, and 10.14 (all 64-bit)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Linux Red Hat 8 and 7 & Ubuntu 20.04, 18.04, and 16.04 (all x64)	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No

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 Cisco 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

- 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.
- Windows 2008 is not supported; however, we do not prevent the installation of AnyConnect on this OS. Also, Windows Server 2008 R2 requires the optional SysWow64 component
- 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 Windows 7 or 8. Drivers that are not supported may have intermittent connection problems.
- For Network Access Manager, machine authentication using machine password will not work on Windows 8 or 10 / Server 2012 unless a registry fix described in Microsoft KB 2743127 is applied to the client desktop. This fix includes adding a DWORD value LsaAllowReturningUnencryptedSecrets to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa registry key and setting this value to 1.

  Machine authentication using machine certificate (rather than machine password) does not require a change and is the more secure option. Because machine password was accessible in an unencrypted format, Microsoft changed the OS so that a special key was required. NAM 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 a 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 data cards which interface with Windows 7 or later 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
- Administrator privileges are required for installation
- x86 instruction set
- 64-bit processor
- 100 MB hard disk space
- tun support in Linux Kernel
- libstdc++ 6.0.19 (GLIBCXX_3.4.19) or later
- iptables 1.4.21 or later
- NetworkManager 1.0.6 or later
- zlib - to support SSL deflate compression
- glib 2.36 and later
- polkit 0.105 or later
- gtk 3.8 or later
- webkitgtk+ 2.10 or later, required only if you are using the AnyConnect embedded browser app
- libnm (libnm.so or libnm-glib.so), required only if you are using Network Visibility Module

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 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, Release 4.x .

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 Apex 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 an ASA headend and use the VPN and VPN Posture (HostScan) modules, an AnyConnect 4.X Plus or Apex license is required, trial licenses are available, see the Cisco AnyConnect Ordering Guide.

For an overview of the AnyConnect 4.X Plus and Apex 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 client and its related files. The Cisco AnyConnect Secure Mobility Client can be deployed to remote users by the following methods:

- Predeploy—New installations and upgrades are done either by the end user, or by using an enterprise software management system (SMS).
- Web Deploy—The AnyConnect package is loaded on the headend, which is either an ASA or ISE server. When the user connects to an ASA or to ISE, AnyConnect is deployed to the client.
  - For new installations, the user connects to a headend to download the AnyConnect client. 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 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 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 versions 7 and 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 4.x release. TAC support is available to any customer with an active AnyConnect 4.x term/contract running a released version of AnyConnect 4.x. 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 4.x 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

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

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

NVM Installation Fails With Ubuntu 20

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

Local and Network Proxy Incompatibilities

Local and/or network proxies (such as software/security applications like Fiddler, Charles Proxy, or Third-party Antimwalware/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. Xhostc ontrols the access of a remote host running a terminal on the endpoint, which is restricted by default. Without disabling access control, AnyConnect web deployment will fail.

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 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 an 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 Cisco 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

A macOS fix is pending to correct 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 CSCvo18938 ended up revealing another OS issue, causing the nslookup problematic behavior.

Apple has requested that customers escalate the underlying OS issue directly to them. When escalating to Apple, please reference macOS defect FB7670484. As a workaround, 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 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. For the best user experience, we recommend upgrading to AnyConnect 4.8, because it is the first version that officially supports operation on macOS 10.15 and contains no 32-bit code.

Otherwise, make note of these limitations:

- AnyConnect versions prior to 4.7.03052 may require an active internet connection to upgrade.
- AnyConnect HostScan versions prior to 4.8.x will not function on macOS 10.15. Refer to HostScan Will Not Function With macOS 10.15 Without Upgrade (CSCvq11813), on page 14.

- AnyConnect HostScan and SystemScan users on macOS 10.15 will experience permission popups during initial launch. Refer to Permission Popups During Initial AnyConnect HostScan or System Scan Launch (CSCvq64942), on page 14.

HostScan Will Not Function With macOS 10.15 Without Upgrade (CSCvq11813)

AnyConnect 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 ASA headends running HostScan packages earlier than 4.8.x will not be able to successfully complete VPN connections, receiving a posture assessment failed message.

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

To enable successful VPN connections for 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 ASA headends may disable HostScan. If disabled, all HostScan 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 AnyConnect 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 HostScan 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 Cisco 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 an AnyConnect app or executables, ACLs must be reconfigured after upgrading to AnyConnect 4.8, 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 from 4.8:

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 18.04, and Red Hat 7 to collect logs.

Restored IPsec Connections in FIPS Mode (CSCvm87884)

AnyConnect customers using release 4.6.2 and 4.6.3 were experiencing 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 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

The recommended version of AnyConnect for macOS 10.13 (High Sierra) is AnyConnect 4.5.02XXX and later.

AnyConnect 4.5.02XXX and above has additional functionality and warnings to guide users through the steps needed to leverage AnyConnect’s complete capabilities, by enabling the 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 to 4.5.02XXX and above 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 of AnyConnect earlier than 4.5.02XXX must enable the AnyConnect software extension in their macOS Preferences -> Security & Privacy pane. Although AnyConnect 4.4.04030 and 4.5.01044 have been tested to work with macOS 10.13 (and later), those users will not have the additional functionality and warning guidance added to AnyConnect 4.5.02XXX. You may need to manually reboot after enabling the extension prior to AnyConnect 4.5.02xxx.

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 an 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

This "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 ASA or ISE. Only the NAM, 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 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 VPN 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 Plugin Changes

The dashboard to retrieve the `OrgInfo.json` file is now 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

AnyConnect 4.1MR4(4.1.04011) and later are compatible with Windows 10 official release. Technical Assistance Center (TAC) support is available beginning on 7/29/2015.

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).

This behavior introduced in AnyConnect release 4.2MR1 requires the following configurations 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 Windws 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) 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.

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), you must do an AnyConnect service restart 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.

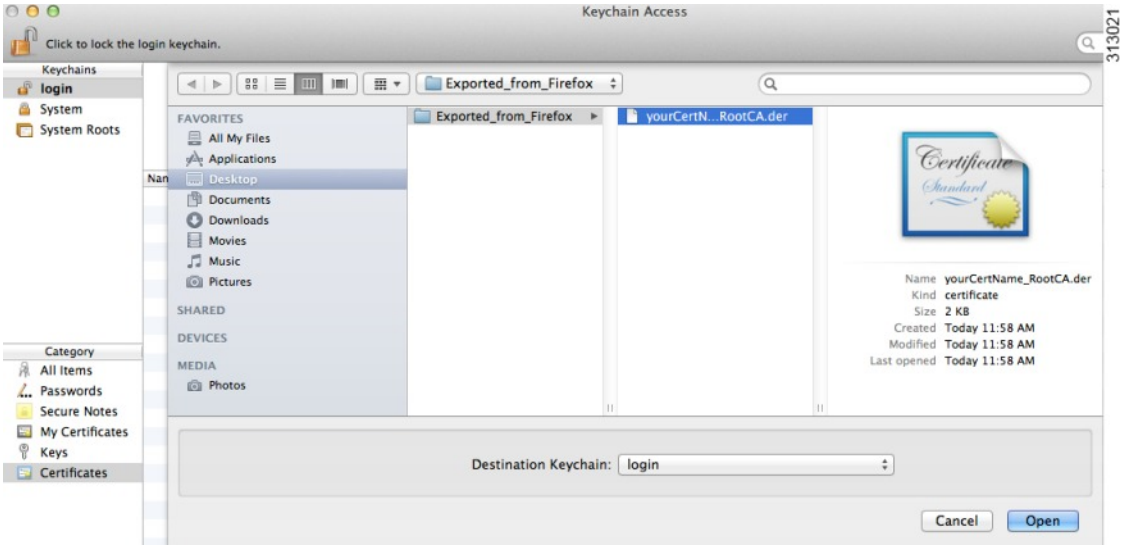
Firefox Certificate Store on macOS is Not Supported

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**.

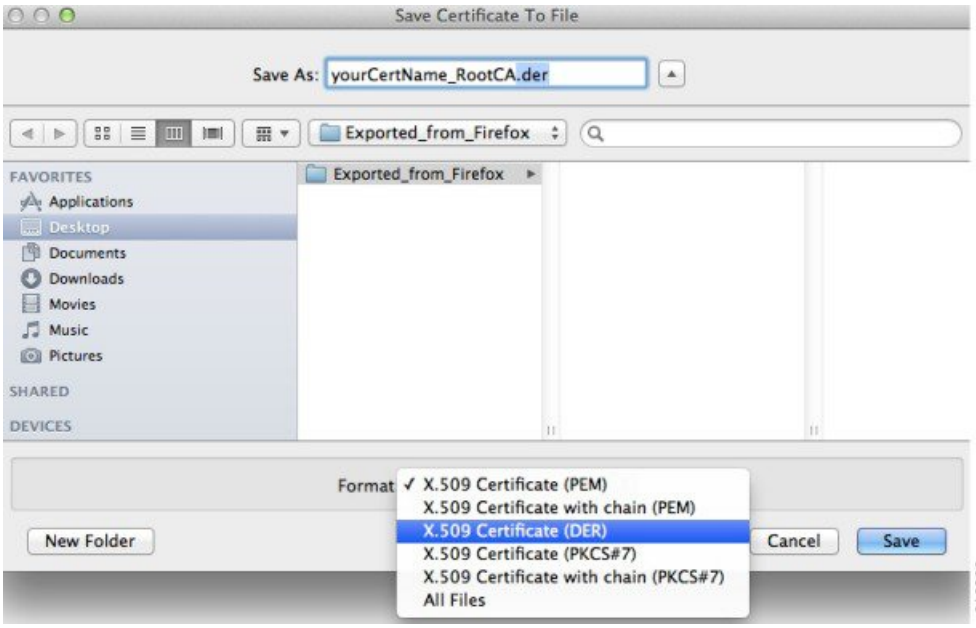
   Your AnyConnect Certificate(s) will most likely be located under the Authorities category. Verify with your Certificate Administrator, as they may be located under a different category (Your Certificates or Servers).
3. Select a location to save the Certificate(s), for example, a folder on your desktop.
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 Secure Mobility Client, Hostscan, CSD and Clientless SSL VPN (WebVPN). A description of the issues and workarounds is provide in the Troubleshooting Technote Java 7 Issues with AnyConnect, CSD/Hostscan, and WebVPN - Troubleshooting Guide, which is in Cisco documentation under Security > Cisco Hostscan.

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 the AnyConnect client 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 VPN over Tethered Devices

Cisco has qualified the AnyConnect VPN client over a bluetooth or USB tethered Apple iPhone only. Network connectivity provided by other tethered devices should be verified with the AnyConnect VPN client 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 client testing using these virtual machine environments:

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

We do not support running 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 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 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 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 Cisco AnyConnect 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 Cisco AnyConnect Installation folder or make security exceptions for the Cisco 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** > **SSL VPN 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 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 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. The following GPO conditions may prevent the Network Access Manager from operating as expected :

- When using the Windows 7 or later,**Only use Group Policy profiles for allowed networks** option.

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

An 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 the AnyConnect client for macOS attempts to create an SSL connection to a gateway running IOS, or when the AnyConnect client attempts to create an IPsec connection to an 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` (For macOS v10.7 and later)

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. This could allow them to delete the AnyConnect profile file 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 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 ASA Not Be Configured to Require SSLv3 Traffic

AnyConnect requires the 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.

Thus, the AnyConnect client cannot establish a connection with the following 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. With release 3.1.03103, those with multi-homed systems may also experience the long reconnects.

Users with Limited Privileges Cannot Upgrade ActiveX

On Windows 7 or later, user accounts with limited privileges cannot upgrade ActiveX controls and therefore cannot upgrade the AnyConnect client with the web deploy method. For the most secure option, Cisco recommends that users upgrade the client from within the application by connecting to the headend and upgrading.

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

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

Network Access Manager does not support PKC or CCKM caching. On Windows 7, fast roaming with a non-Cisco wireless card is unavailable.

Application Programming Interface for the AnyConnect Secure Mobility Client

The 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 Cisco AnyConnect VPN Client. You can use the libraries and example programs for building on Windows, Linux and MAC platforms. The Makefiles (or project files) for the Windows platform are also included. For other platforms, it includes platform specific scripts showing how to compile the example code. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.

You can download the APIs from Cisco.com.

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

AnyConnect 4.10.00093

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://tools.cisco.com/RPF/register/register.do.

Resolved

Identifier	Component	Headline
CSCvx63335	certificate	Windows: AnyConnect randomly throws 'Certificate has expired' error
CSCvx78941	certificate	AnyConnect's code signing certificate needs to be updated due to Symantec Root CAs distrust

Identifier	Component	Headline
CSCvs75542	core	ENH: Support for Enhanced Captive Portal Remediation on macOS
CSCvu14938	core	Cisco AnyConnect Secure Mobility Client for Windows Profile folder modification vulnerability
CSCvu78363	core	AnyConnect Start Before Logon (SBL) displays incorrect name when Native VPN client is configured
CSCvv30103	core	Cisco AnyConnect Secure Mobility Client Arbitrary Code Execution Vulnerability
CSCvw16391	core	UI loses IPC/TCP channel with Agent after keepidle timer is blocked by third-party firewall(s)
CSCvw16601	core	AnyConnect does not fallback to IPv6 when using IPSec/IKEv2
CSCvw29572	core	Cisco AnyConnect Secure Mobility Client Denial of Service Vulnerability
CSCvx04208	core	macOS: WebEx app call interruptions with high rate and/or count of dynamic tunnel inclusions
CSCvx55399	core	When HostScan enable + tunnel-group-list disable, default tunnel group was selected
CSCvw21825	down_install-wer	Cisco AnyConnect Secure Mobility file overwrite vulnerability
CSCvx23656	download_install	Failed to launch downloader due to proxy environment variables
CSCvr54037	nam	Network Access Manager PE not saving user defined EKU for Cert Matching Rule-Machine EAP-TLS
CSCvw63452	nam	NAM bind control DLL deleted during upgrade of Network Access Manager from versions that used DIFxAPI

Identifier	Component	Headline
CSCvx25251	nvm	NVM installation fails with latest kernel version of Ubuntu 20
CSCvw08005	opswat-ise	ISE posture module is not detecting SEP version 14.3.1148.0100
CSCvt26597	posture-ise	ENH: ISE Posture Module support in Linux OS
CSCvu23579	vpn	ENH: Permit 20,000 characters in Dynamic Split Tunnel list
CSCvv61677	vpn	device-mac/device-public-mac ACIDEX attributes are not sent from AnyConnect when using Bluetooth NIC
CSCvw92182	vpn	AnyConnect on macOS connected to the ASA tls-only is reconnecting ~ 20s after connected
CSCvw96331	vpn	Linux: Update Policy, Software and Profile lock feature is broken
CSCvx04190	vpn	anyconnect_global file corrupt after connecting with vpncli on Linux when using OGS
CSCvx20136	vpn	DNS queries are failing for some FQDNs after waking from sleep on macOS Big Sur with AnyConnect 4.9
CSCvx27372	vpn	macOS: Connectivity lost after connected for a while to DST-enabled headend (low TTL DST domains)
CSCvx65570	vpn	AnyConnect UI shows blank "Connect To:" on Linux when no profile is used

HostScan 4.10.00093

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://tools.cisco.com/RPF/register/register.do.

Resolved

Identifier	Component	Headline
CSCvx38993	posture-asa	HostScan unable to retrieve the serial number of macOS Big Sur with Apple M1 chip inserted
CSCvx82055	posture-asa	AnyConnect 4.9.06037 with HostScan 4.9.06046 stuck in "HostScan state idle" on Oracle Linux 7.9

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.