Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.2

First Published: 2015-05-05

Last Modified: 2016-10-07

Release Notes for AnyConnect Secure Mobility Client, Release 4.2

These release notes provide information for AnyConnect Secure Mobility on Windows, Mac OS X and Linux platforms.

Note AnyConnect release 4.4.x will become the maintenance path for any 4.x bugs. AnyConnect 4.0, 4.1, 4.2, and 4.3 customers must upgrade to AnyConnect 4.4.x to benefit from future defect fixes. Any defects found in AnyConnect 4.0.x, 4.1.x, 4.2.x, and 4.3.x will be fixed in the AnyConnect 4.4.x maintenance releases only. However, we are scheduled to provide a 4.3 maintenance release patch that will follow shortly after this 4.4 release.

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*-k9.pkg
macOS	anyconnect-macosx-i386-*version*-k9.pkg
Linux (64-bit)	anyconnect-linux-64-*version*-k9.pkg

AnyConnect Package Filenames for Pre-deployment

OS	AnyConnect Pre-Deploy Package Name
Windows	anyconnect-win-*version*-pre-deploy-k9.iso
macOS	anyconnect-macosx-i386-*version*-k9.dmg
Linux (64-bit)	anyconnect-predeploy-linux-64-*version*-k9.tar.gz

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

New Features in AnyConnect 4.2.06014

AnyConnect 4.2.06014 is a maintenance release that includes enhancements and that resolves the defects described in AnyConnect 4.2.06014, on page 26.

New Features in AnyConnect 4.2.05015

AnyConnect 4.2.05015 is a maintenance release that includes enhancements and that resolves the defects described in AnyConnect 4.2.05015, on page 27.

New Features in AnyConnect 4.2.04039

AnyConnect 4.2.04039 is a maintenance release that includes enhancements and that resolves the defects described in AnyConnect 4.2.04039, on page 28.

New Features in AnyConnect 4.2.04018

AnyConnect 4.2.04018 is a maintenance release that includes enhancements and that resolves the defects described in AnyConnect 4.2.04018, on page 29.

New Features in AnyConnect 4.2.03013

AnyConnect 4.2.03013 is a maintenance release that includes enhancements and that resolves the defects described in AnyConnect 4.2.03013, on page 30.

New Features in AnyConnect 4.2.02075

AnyConnect 4.2.02075 is a maintenance release that includes enhancements and that resolves the defects described in AnyConnect 4.2.02075, on page 31 .

New Features in AnyConnect 4.2.01035

AnyConnect 4.2.01035 is a maintenance release that includes the following features and enhancements and that resolves the defects described in AnyConnect 4.2.01035, on page 33

New Features in AnyConnect 4.2.01022

AnyConnect 4.2.01022 is a maintenance release that includes the following features and enhancements and that resolves the defects described in AnyConnect 4.2.01022, on page 34.

To address users increasingly operating on unmanaged devices, you can choose to enhance protection of AnyConnect by adding the Network Visibility Module (NVM). It provides traffic flow and contextual data regarding users, applications, devices, locations, and destinations. With NVM you can choose whether you want the telemetry targeted as opposed to whole infrastructure deployment.

New Features in AnyConnect 4.2.00096

AnyConnect 4.2.00096 is a major release that includes the following features and enhancements and that resolves the defects described in AnyConnect 4.2.00096, on page 35.

- Reliable access to corporate resources when at a captive portal and the ability to disable when desired

- Last connection entry is no longer displayed in the user's preferences file if the profile is now invalid

- Ability to filter machine certificates based on parameters and to specify appropriate machine certificates for authentication

- ISE posture logging and remediation improvements

- IPv6 VPN network connection support from Linux desktop

- Security and flexibility improvements for Trusted Network Detection (TND)

- DSCP preservation to control Differentiated Services Code Point (DSCP) on Windows or OS X platforms for DTLS connection only

Important Interoperability Considerations

Coexistence of ISE and ASA Headends

- If you are using both ISE and ASA for client posture, the profiles must match on both headends.

- AnyConnect ignores the ISE server if NAC Agent is provisioned for the endpoint.

- If the Cisco NAC agent and the VPN Posture (HostScan) module are both installed on a client, the Cisco NAC agent must be at least version 4.9.4.3 or later to prevent posture conflicts.

- The NAC Agent ignores the ISE server if AnyConnect is provisioned for the endpoint in ISE.

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 the 32-bit version of Java, version 6 or higher, before installing the profile editor.

ISE Requirements for AnyConnect

ISE Release Requirements

- 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, pre-deployed 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 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

- 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.

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, antivirus, antispyware, and firewall software installed on the host to the ASA.

The VPN Posture (HostScan) Module requires Cisco Hostscan to gather this information. Cisco Hostscan, available as its own software package, is periodically updated with new operating system, antimalware, and firewall software information. Cisco recommends that you run the most recent version of HostScan, which is the same as the version of AnyConnect.

The List of Antimalware and Firewall Applications is available on cisco.com. The support charts opens most easily using a Firefox browser. If you are using Internet Explorer, download the file to your computer and change the file extension from `.zip` to `.xlsm`. You can open the file in Microsoft Excel, Microsoft Excel viewer, or Open Office.

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.

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 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

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	
Windows 7, 8, 8.1, & 10	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes	
Mac OS X 10.8, 10.9, 10.10, 10.11 Mac OS X 10.9, 10.10, 10.11, and 10.12 [1]	Yes	No	Yes	Yes	Yes	Yes		Yes	Yes	
Linux Red Hat 6, 7 & Ubuntu 12.04 (LTS), and 14.04 (LTS) (64-bit only)	Yes	No	No	Yes	No	Yes	Yes	No	No	

[1] AnyConnect 4.3.3086 and 4.2.6014 are the minimum required releases for Mac OS X 10.12 support.

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. This change permits Local Security Authority (LSA) to provide clients like Cisco Network Access Manager with the Machine password. It is related to the increased default security settings in Windows 8 or 10 / Server 2012. Machine authentication using Machine certificate does not require this change and will work the same as it worked with pre-Windows 8 operating systems.

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

- 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 2.0.0.

- gdk 2.0.0.

- libpango 1.0.

- iptables 1.2.7a or later.

- tun module supplied with kernel 2.4.21 or 2.6.

AnyConnect Support for Mac

Mac Requirements

- AnyConnect requires 50MB of hard disk space.

- To operate correctly with Mac, AnyConnect requires a minimum display resolution of 1024 by 640 pixels.

Mac Guidelines

- Mac OS X 10.8 introduces a new feature called Gatekeeper that restricts which applications are allowed to run on the system. You can choose to permit applications downloaded from:

    - Mac App Store

    - Mac App Store and identified developers

    - Anywhere

    The default setting is Mac App Store and identified developers (signed applications). AnyConnect is a signed application, but it is not signed using an Apple certificate. This means that you must either select the Anywhere setting or use Control-click to bypass the selected setting to install and run AnyConnect from a pre-deploy installation. Users who web deploy or who already have AnyConnect installed are not impacted. For further information, refer to Apple documentation.

    Note   Web launch or OS upgrades (for example 10.7 to 10.8) install as expected. Only the pre-deploy installation requires additional configuration as a result of Gatekeeper.

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:

- Pre-Deploy—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.

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 pre-deployed. When pre-deploying, 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.

For more information about deploying the AnyConnect modules, see the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.6.

For more information about deploying the AnyConnect modules, see the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.5.

For more information about deploying the AnyConnect modules, see the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.3.

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

Upgrading from 3.1 MR10 AnyConnect Clients/Incompatibility Issues

Once AnyConnect 3.1.10010 has been automatically deployed to an endpoint, you cannot connect to a secure gateway configured with AnyConnect versions 4.0, 4.1, 4.1MR2, 4.2, and 4.3 which are incompatible. If you try to upgrade from AnyConnect 3.1 MR10 version to any version other than AnyConnect 4.1MR4 (or later) or 3.1 versions later than 3.1.10010, you will receive a notification that the upgrade is not allowed.

Refer to CSCuv12386 for further information.

Upgrading from AnyConnect 3.0 or Later

When you upgrade from AnyConnect Secure Mobility Client Release 3.0 or later, AnyConnect performs the following operations:

- Upgrades all previous versions of the core client and retains all VPN configurations.

- Upgrades any HostScan files used by AnyConnect.

Upgrading from AnyConnect 2.5 and earlier

When you upgrade from any 2.5.x version of AnyConnect, the AnyConnect Secure Mobility Client performs the following:

- Upgrades all previous versions of the core client and retains all VPN configurations.

- Upgrades any HostScan files used by AnyConnect.

- If you install Network Access Manager, AnyConnect retains all CSSC 5.x configuration for use with Network Access Manager, then removes CSSC 5.x.

- Does not upgrade or remove the Cisco IPsec VPN client. However, the AnyConnect client can coexist on the computer with the IPsec VPN client.

- Does not upgrade and cannot coexist with Cisco's ScanSafe AnyWhere+. You must uninstall AnyWhere+ before installing the AnyConnect Secure Mobility Client.

Note If you are upgrading from the legacy Cisco VPN client, the MTU value on the physical adapters may have been lowered to 1300. You should restore the MTU back to the default (typically 1500) for each adapter to achieve optimal performance when using AnyConnect.

Upgrading from AnyConnect 2.2 is not supported using the ASA or Weblaunch. You must uninstall AnyConnect 2.2 then install the new verion either manually or using an SMS.

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 supports all non-beta AnyConnect software versions available on the Cisco AnyConnect VPN Software Download site; however, we provide fixes and enhancements only in maintenance or features releases based on the most recently released version.

For information about when releases are no longer supported, see http://www.cisco.com/c/en/us/products/eos-eol-policy.html

Guidelines and Limitations

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-include (deny 0.0.0.0/32 or ::/128) is also configured in the access-list (ACE/ACL).

The new behavior 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.

No Longer Supporting RC4 TLS Cipher Suite

RC4 TLS cipher suites are not supported from AnyConnect release 4.2.01035 and onwards due to security policy enhancements.

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.

Network Visibility Module Incompatible with LittleSnitch Firewall

The Network Visibility Module is incompatible with LittleSnitch firewall on Mac OS X.

AnyConnect Support on Mac OS X El Capitan 10.11

The Cisco AnyConnect Secure Mobility Client is supported on the Mac OS X El Capitan 10.11 operating system.

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 Mac

If you are using Mac OS X 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 Mac OS X is Not Supported

The Firefox certificate store on Mac OS X 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 Mac OS X keychain. The following steps are an example of what you may want to tell your AnyConnect users.

1. Navigate to **Firefox > Preferences > 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.
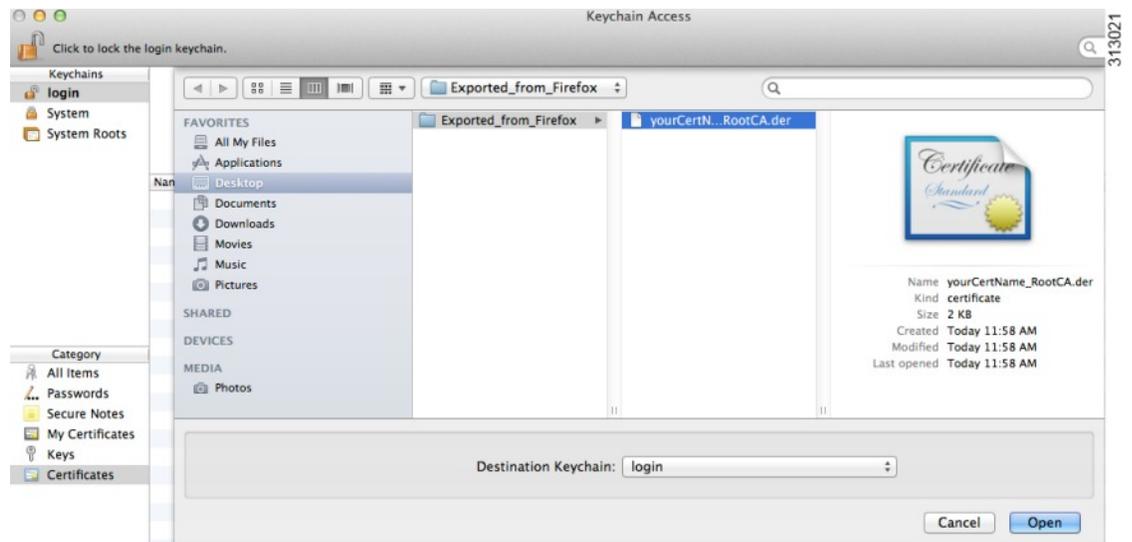
Note If more than one AnyConnect Certificate and/or a Private Key is used/required, repeat the above process for each Certificate).

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.
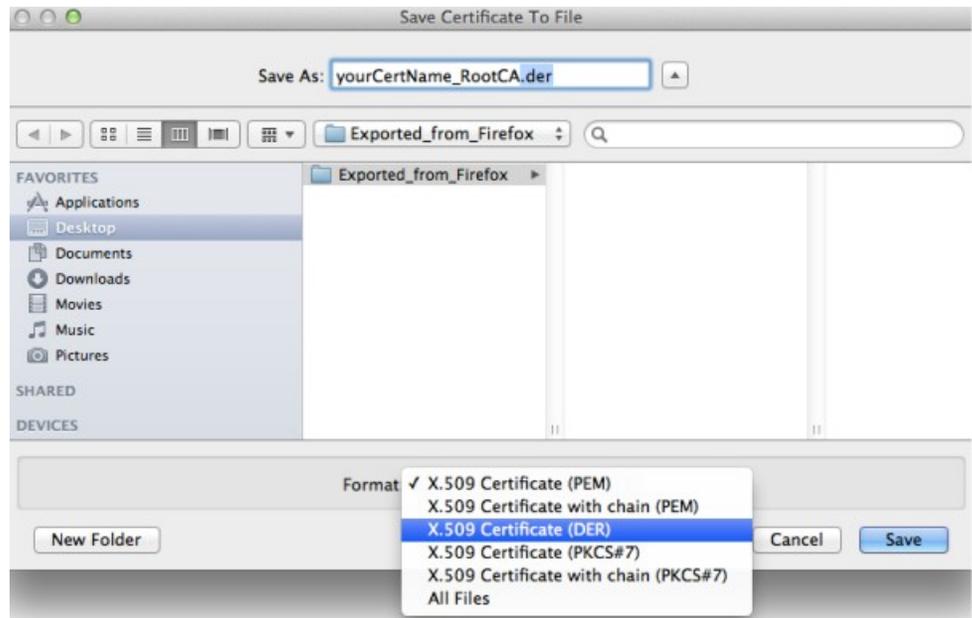
7. Repeat the preceding steps for additional Certificates that are used or required for AnyConnect.

AnyConnect UI Fails Due to Missing Dependency libpangox

On many newer Linux distributions, the AnyConnect UI may fail to start with the error:

```
error while loading shared libraries: libpangox-1.0.so.0: cannot open shared
object file: No such file or directory
```

The missing library is obsolete and is no longer available. This impacts other applications, not just AnyConnect.

Pango has released the source code of a compatible library that has been built by others and is available online. To resolve this problem, find and install either the package
pangox-compat-0.0.2-2.el7.x86_64.rpm or
pangox-compat-0.0.2-3.fc20.x86_64.rpm.

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.

Problems Due to Modified sysctl Network Settings

We have seen instances where Apple's Broadband Tuner application (from 2005) was used with Mac OS X 10.9, That application changes the network settings in sysctl.conf, which can cause connection problems. That application was designed for much older versions of the Mac OS. We suspect that the current default OS settings take broadband networks into consideration, so most users will not need to take any action.

Running AnyConnect 3.1.04074 along with the modified sysctl settings may generate the following message:

```
The VPN client driver encountered an error..please restart
```

To Verify

To verify that the sysctl network setting is the cause of the problem, open a Terminal window and type:

```
sysctl -a | grep maxsockbuf
```

If the results contain a value much lower than the default value of 8388608, for example:

```
kern.ipc.maxsockbuf: 512000
```

Then this value may have been overritten in /etc/sysctl.conf by Apple's Broadband Tuner application

To Fix

Edit /etc/sysctl.conf, comment out the line that sets kern.ipc.maxsockbuf, and reboot the computer.

OR

If you have no other Customization other than the one set by the Broadband Tuner application, rename or delete sysctl.conf.

Apple is aware of this problem, and has opened Bug ID: 15542576.

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.

1. Open **Safari** > **Preferences** > **Security** > **Manage Website Settings**.

2. Click on the ASA and select run in Unsafe Mode.

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.

Internet Explorer, Java 7, and AnyConnect 3.1.1 Interoperability

Supported versions of Internet Explorer stop working when the user attempts to connect to the ASA, when Java 7 is installed on the endpoint, when HostScan is installed and enabled on the ASA, and when AnyConnect 3.1.1 is installed and enabled on the ASA.

This does not happen when Active X or earlier versions of Java 7 are installed. To avoid this, use a supported version of Java on the endpoint that is earlier than Java 7.

Refer to the Bug Toolkit and defect CSCuc48299 to verify.

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.

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:

• VMWare ESXi Hypervisor (vSphere) 4.0.1 and later

• VMWare Fusion 2.x, 3.x, and 4.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 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 "white-list" or make security exceptions for these HostScan applications:

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

Microsoft Internet Explorer Proxy Not Supported by IKEv2

IKEv2 does not support the public-side Microsoft Internet Explorer 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 master 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 Mac OS X Performance when Behind Certain Routers

When the AnyConnect client for Mac OS X 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 Mac OS X command line:

`sudo ifconfig utun0 mtu 1200` (For Mac OS X 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 Be Configured to Accept TLSv1 Traffic

AnyConnect requires the ASA to accept TLSv1 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.

Using the Manual Install Option on Mac OS X if the Java Installer Fails

If users WebLaunch from the ASA headend to start AnyConnect on a Mac, and the Java installer fails, a dialog box presents a **Manual Install** link. Users should do the following when this happens:

1. Click **Manual Install**. A dialog box presents the option to save a `.dmg` file that contains an OS X installer.

2. Mount the disk image (`.dmg`) file by opening it and browsing to the mounted volume using Finder.

3. Open a Terminal window and use the CD command to navigate to the directory containing the file saved. Open the `.dmg` file and run the installer.

4. Following the installation, choose **Applications** > **Cisco** > **Cisco AnyConnect Secure Mobility Client** to initiate an AnyConnect session, or use Launchpad.

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 Caveats

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool, https://tools.cisco.com/bugsearch/, 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.

AnyConnect 4.2.06014

Caveats Resolved and Open

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

Table 1: Resolved

Identifier	Component	Headline
CSCva82166	download_install	Certificate expired on AC build 4.2.5015
CSCux95450	gui	JAWS does not report posture status is compliant
CSCvb01862	gui	Incorrect formatting of customized message in AnyConnect 4.2.x (4.x) GUI
CSCva84287	nam	Windows 10 Anniversary update breaks AnyConnect NAM service
CSCva73262	posture-asa	CSD: HostScan is not detecting some antiviruses

CSCvb05884	posture-asa	Add Avast Free 12.x support in HostScan
CSCvb64718	posture-asa	Mac OS 10.12 (Sierra) FW not detected by HostScan
CSCux03030	vpn	AC OS X using PUBLIC proxy and using load balanced ASA's (VIP) fails
CSCvb02196	vpn	AnyConnect DNS suffix not getting removed from fresh install Windows 10
CSCvb41365	vpn	AnyConnect fails to connect via proxy on Windows 10 (1607) anniversary
CSCvb42478	vpn	Mac OS 10.12 - AnyConnect crash after Connect - cert enumeration
CSCvb62962	vpn	OS X: Deflate compression does not work (can't pass data)

Open

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

AnyConnect 4.2.05015

Caveats Resolved and Open

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

Table 2: Resolved

Identifier	Component	Headline
CSCuz50259	core	AC w/TND ignores CRL pref setting <EnableCRLCheck>false</EnableCRLCheck>
CSCva58530	download_install	Ubuntu: Posture fails to install using web deploy
CSCuz58363	download_install	Ubuntu 16.4: Web-deploy upgrade from 4.2 -> 4.3 fails
CSCuz68672	download_install	SBL module fails to install - web-deploy AC from ISE
CSCuz87832	gui	AnyConnect NAM toast messages not announced with JAWS 16 or 17 on Win7

CSCuy77113	nam	When using two CAC cards in on system, NAM reports no Valid Certificates
CSCuz17009	nam	No smart card certificates available after resume for 2+ minutes
CSCuz84937	posture-asa	HostScan timestamp returns -1 for Norton Security
CSCva69334	posture-asa	Received "accessdenied" error for McAfee HIPS Firewall on Windows 10

Open

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

AnyConnect 4.2.04039

Caveats Resolved and Open

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

Table 3: Resolved

Identifier	Component	Headline
CSCuu35142	core	AnyConnect script: Onconnect script doesn't work with SBL
CSCuz97382	download_install	Clean install failing for 4.x releases using ISE Network Setup Assistant
CSCuz52506	vpn	Evaluation of AnyConnect for OpenSSL May 2016
CSCuz71074	nam	AnyConnect NAM prevents SmartCard services from stopping
CSCuy80927	posture-asa	HostScan fails to get serialNumber from sn in certificate for Linux box
CSCuz34222	posture-asa	Linux: Upgrade to 4.2 MR4 and 4.2 fails with HostScan enabled
CSCuz50866	posture-asa	HostScan fails to detect McAfee disk encryption

CSCux97603	posture-ise	Symantec Altiris 7.6 patch not updated on ISE
CSCuu34998	profile-editor	Unable to install standalone profile editor with JRE 1.8 on the machine
CSCuz52506	vpn	Evaluation of AnyConnect for OpenSSL May 2016

Open

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

AnyConnect 4.2.04018

Caveats Resolved and Open

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

Table 4: Resolved

Identifier	Component	Headline
certificate	CSCuy12161	AnyConnect should no longer require key agreement in server certificate
core	CSCuy88042	Notify user when HostScan posture assessment fails via slow network links
core	CSCuz01066	AnyConnect is setting the public interface to the VA address
gui	CSCuy75474	GUI does not show the connected entry in the drop down control
posture-asa	CSCuy19255	HostScan not detecting 'activescan' for Microsoft AV on Mac
posture-asa	CSCuy43073	HostScan failed to detect ESET Endpoint Security Active scan
posture-asa	CSCuy45662	Add HostScan support for McAfee VirusScan 2.x for Linux
posture-asa	CSCuz01661	HostScan failed to detect ESET Smart Security 7 Active Scan
posture-ise	CSCuy96879	ISE posture agent SCCM remediation fails for non-admin user
profile editor	CSCuu34998	Unable to install standalone profile editor with JRE 1.8 on the machine

| vpn | CSCut09823 | AnyConnect: ICMP6 firewall rule not processed correctly |
| vpn | CSCuy78946 | AnyConnect does not connect with PEM store on Linux |

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

Open

Identity	Component	Headline
CSCuz342222	posture-asa	Linux: Upgrade from 4.2.3013 to 4.2.4018 fails with hostscan enabled

AnyConnect 4.2.03013

Caveats Resolved and Open

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

Table 5: Resolved

Identifier	Component	Headline
CSCuy34417	core	AnyConnect client profile list not in alphabetical order
CSCuw74246	dart	Windows 10 wrongly reported as Windows 8
CSCux95450	gui	JAWS does not report posture status as compliant
CSCuy43409	gui	AnyConnect-Multiple pop ups when using IKEv2 with Always On plus TND
CSCux40858	nam	WWAN APN missing intermittently
CSCuy13416	nvm	NVM fails to capture flow information
CSCuw67168	posture-asa	ENH: HostScan: Add support for Bitdefender Virus Scanner for Mac
CSCux40109	posture-asa	TrendMicro OfficeScan Update to ver 11 is not detected

Identifier	Component	Headline
CSCux98114	posture-asa	HostScan fails to get UTF8STRING encoded certificate fields on Mac OS X
CSCuy27569	posture-asa	HostScan fails to get serialNumber from subject name in certificate
CSCuy43901	posture-asa	Linux: ciscod.service fails to load
CSCux94204	posture-ise	ISE 2.0 P2 Posture - Disk encryption not working
CSCuy57519	posture-ise	Too many logs generated for event ID 259
CSCuy51590	profile editor	3.1 higher websec profile editor saves Beacon config in .xml profile
CSCut12260	vpn	VPN url crashes AnyConnect MacOSX client
CSCux04097	vpn	Implement fails safe mechanism for hosts file
CSCuy45271	vpn	Windows 8 and 10 BSOD involving dashost.exe
CSCuy51155	web security	Mac reboot issue: license verification fails
CSCuy51534	web security	AnyConnect web sec 4.2 prompts auth OnTrusted Network

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

AnyConnect 4.2.02075

Caveats Resolved and Open

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

Table 6: Resolved

Identifier	Component	Headline
CSCux86654	download_install	VPN: ISE posture profile not installed by downloader
CSCuw92067	gui	Menu options render % signs around listed options

CSCur85411	nam	Allow connection to user created network before logging into PC
CSCus21060	posture-asa	CScan generates "Fingerprints do not match" Windows log every minute
CSCuw80272	posture-asa	HostScan support for Mac OS X built-in firewall for Mac OS 10.11
CSCuw96489	posture-asa	HostScan 'activescan" returns "internalerror" for ESET antivirus
CSCux07750	posture-asa	HostScan Mac OS X 10 Sophos 9.2 - lastupdate not populated
CSCux52516	posture-asa	Not able to enable Win 8.1 Firewall using Advanced Endpoint Assessment
CSCux53899	posture-asa	Linux: Connecting post disconnect with AC fails with hostscan enabled
CSCuw91192	posture-ise	Unable to detect AVG 2016
CSCus37509	vpn	Linux: AC 3.1 Debian Jessie - vpnagentd.service failed to load
CSCus79211	vpn	AnyConnect preferences parsing issue
CSCuw16498	vpn	AnyConnect SBL missing "Disconnect " button on disabling vpndownloader
CSCuw35003	vpn	AnyConnect stuck in reconnect state with vpncli non-interactive mode
CSCux27277	vpn	AnyConnect reconnect fails with error "MTU too small"
CSCuy01698	vpn	BSOD on Windows 8.1 and Windows 10
CSCux63081	web security	Websec Cert Mgmt :p7b file is not getting downloaded if removed/renamed

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

AnyConnect 4.2.01035

Caveats Resolved and Open

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

Table 7: Resolved

Identifier	Component	Headline
CSCum90946	core	Routing Local LAN subnet when split-include is supernet of Local subnet
CSCuv04516	core	AnyConnect deletes the last entry of host file
CSCuw47430	core	Challenge/Response (challenge messages) not displayed on OS X
CSCuv48563	download install	AnyConnect Secure Mobility Client arbitrary file move vulnerability
CSCux64964	download install	Installation of updated VPN profile fails from ASA
CSCut27870	gui	AnyConnect has exclamation mark on successful connect
CSCux26329	gui	AnyConnect 4.x: GUI does not launch if the User home folder has a space
CSCux41420	mobile	Evaluation of AnyConnect for OpenSSL December 2015 vulnerabilities
CSCuu83807	nam	Need a way to manually configure DHCP functionality in NAM
CSCuv93588	phone home	AnyConnect 4.1 under Mac OS X 10.10.3 to 10.10.5 crashes every few minutes
CSCuv79716	posture-asa	HostScan upgrade from ASA fails if it was pre-deployed via msi package
CSCuw23596	posture-ise	AnyConnect posture module reports wrong OS version

CSCuw81938	posture-ise	AnyConnect posture module sends illegal character in posture XML report
CSCux01500	posture-ise	PM remediation failing with wrong error message
CSCur31786	vpn	DNS suffix list deleted upon AnyConnect client connection
CSCuv74296	vpn	SBL does not work on Windows 10
CSCuw12132	vpn	AnyConnect: ClearSmartcardPin XML tag not working
CSCuw43845	vpn	Cert match should override all default filtering rules for EKU
CSCux13036	vpn	AnyConnect 4.2 ignores the preferences.xml file
CSCuw99991	web security	Client crash due to incompatible MS redistributable package
CSCux24537	web security	Client issuing gprefresh causes cpu spike

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

AnyConnect 4.2.01022

Caveats Resolved and Open

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

Table 8: Resolved

Identifier	Component	Headline
CSCuv56788	web security	Websec client fails to detect TND server

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

Table 9: Open

Identifier	Component	Headline
CSCux20705	download_install	Win10: Intermittently upgrade failing from 4.2.96 > 4.2.1022
CSCuv87103	nvm	Flows records with source IP address as 0.0.0.0 on Mac

| CSCux03932 | nvm | NVM incorrectly reports DNS flows for requests served from AC DNS cache |

AnyConnect 4.2.00096

Caveats Resolved and Open

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

Table 10: Resolved

Identifier	Component	Headline
CSCut83093	build_system	Executables not linked against CiscoSSL in AnyConnect Mac OS X
CSCum90946	core	Routing LOCAL LAN subnet when Split-include is Supernet of LOCAL subnet
CSCur78318	core	AnyConnect 3.1 vpnagent crash with vpncommon module
CSCur82067	core	No DNS query is seen if IPv6 DNS server is configured on PHY interface
CSCuv01279	download_install	AnyConnect client for Windows privilege escalation vulnerability
CSCuv11947	download_install	AnyConnect client for Linux or OS/X privilege escalation vulnerability
CSCum86682	mobile	AnyConnect should not drop DNS request for unqualified host
CSCuu53359	mobile-android	Android: Fix valid fragment issues
CSCuv08412	nam	AnyConnect 4.x login GUI misaligned
CSCuw02322	phone home	Windows 10 wrongly reported as Windows 8
CSCut12524	posture-asa	ASDM: Hostscan cannot be configured after upgrade to 3.1.06073
CSCuu87817	posture-asa	Hostscan fails when Realtime Scanning is checked in Kaspersky 2015

CSCuv24279	posture-asa	HostScan cannot locate "lastupdate" value for AVG 2015
CSCuv82622	posture-asa	Hostscan 3.1.10010 fails to identify Windows 10
CSCut93871	posture-ise	AnyConnect ISE posture module creds in memory longer than necessary
CSCuu04245	posture-ise	Remotely triggerable NULL pointer dereference in ISE
CSCuu88169	posture-ise	Microsoft System Center Endpoint 4.x virus definition check fails
CSCuf07885	vpn	DNS traffic via tunnel is restricted with tunnel-all config (Windows)
CSCuu91515	vpn	DTLS breaks after SSL rekey starting AC 3.1MR7/4.0MR2
CSCuu94601	vpn	AnyConnect fails to connect [IKEv2] if IPProtocolSupport has IPv6 only
CSCuv14020	vpn	SBL creates a delay of 10-15 minutes when VpnDownloader is disabled
CSCuv58340	vpn	Allow ManualHostInput XML tag not working
CSCuw13589	vpn	AnyConnect autoreconnect fails after cable reconnection
CSCuv35713	web security	Suppressing GetHashSHA256 error message
CSCuv42179	web security	Websecurity intercept browser traffic without license key

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

Table 11: Open

Identifier		Headline	
CSCuv46351		AC VPN on OS X Yosemite includes Apple wireless direct link Mac address	
CSCuw28341		Misleading message showing on VPN tile	

Related Documentation

Other AnyConnect Documents

- Open Source Software Used in AnyConnect Secure Mobility Client, Release 4.5*Open Source Software Used In AnyConnect Secure Mobility Client, Release 4.2*

- Cisco End User License Agreement, 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 Services Engine, Release 2.2

- Cisco Identity Services Engine Admin Guide, Release 2.2