Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.3

First Published: 2016-06-10

Last Modified: 2016-10-07

Release Notes for AnyConnect Secure Mobility Client, Release 4.3

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

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

SUMMARY STEPS

1. Follow this link to the Cisco AnyConnect Secure Mobility Client product support page:
2. Log in to Cisco.com.
3. Click **Download Software**.
4. Expand the **Latest Releases** folder and click the latest release, if it is not already selected.
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.
6. Read and accept the Cisco license agreement when prompted.
7. Select a local directory in which to save the downloads and click **Save**.
8. See the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.x.

DETAILED STEPS

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-*x.x.x*-k9.pkg
Mac OS X	anyconnect-macosx-i386-*x.x.x*-k9.pkg
Linux (64-bit)	anyconnect-linux-64-*x.x.x*-k9.pkg

AnyConnect Package Filenames for Pre-deployment

OS	AnyConnect Pre-Deploy Package Name
Windows	anyconnect-win-<version>-pre-deploy-k9.iso
Mac OS X	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 4.3.03086

AnyConnect 4.3.03086 is a maintenance release that includes enhancements and that resolves the defects described in AnyConnect 4.3.03086, on page 25.

New Features in AnyConnect 4.3.02039

AnyConnect 4.3.02039 is a maintenance release that includes the following feature and enhancements and that resolves the defects described in AnyConnect 4.3.02039, on page 27 .

Hostname Option Added to Static Exception in Profile Editor

You can exclude or include endpoint traffic from Cisco Cloud Web Security Scanning using AnyConnect's Web Security profile editor. With Cisco AnyConnect Secure Mobility Client release 4.3.02039 or later, you can now add hostnames, besides just IP addresses, to exclude from scanning. In the Static Exception field of the profile editor, determine what hostname to exclude from scanning, and Web Security will not forward that HTTP/HTTPS traffic to the Cloud Web Security Proxy for inspection. If you have multiple hostnames with the same IP address but only one of the hostnames is configured in the Static Exceptions list, Web Security exempts the traffic.

If you want to exempt any browser traffic via proxy server, you must list those hostnames in Host Exceptions, so that they are not forwarded. You cannot only configure static exceptions for traffic flowing through proxies not listed in the Proxy Exception list.

New Features in AnyConnect 4.3.01095

AnyConnect 4.3.01095 is a maintenance release that introduces the Cisco Umbrella Roaming Security module and resolves the defects described in AnyConnect 4.3.01095, on page 28.

The Umbrella Roaming Security module requires a subscription to either Cisco Umbrella Roaming service or OpenDNS Umbrella services (Professional, Insights, Platform, or MSP). Cisco Umbrella Roaming provides DNS-layer security when no VPN is active, whereas OpenDNS Umbrella subscriptions add Intelligent Proxy and IP-Layer Enforcement features, both on- and off-network. Additionally, OpenDNS Umbrella subscriptions provide content filtering, multiple policies, robust reporting, active directory integration, and much more. The same Umbrella Roaming Security module is used regardless of the subscription.

The Umbrella Roaming module profile (OrgInfo.json) associates each deployment with the corresponding service, and the corresponding protection features are enabled automatically.

The Umbrella Dashboard provides real-time visibility into all of the Internet activity originating from the Roaming Security module. The level of granularity in policies and reports depends on the Umbrella subscription.

Refer to https://www.opendns.com/enterprise-security/threat-enforcement/packages/ for a detailed comparison of which features are included in which service level subscriptions.

Interoperability Using Both Umbrella Roaming Security and Web Security

To get full functionality when using both the Umbrella Roaming Security and Web Security module, you must configure the host exclusion and exclude static exceptions defined in the Web Security chapter: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect43/administration/guide/b_AnyConnect_Administrator_Guide_4-3/configure-web-security.html. Otherwise, the DNS protection could be completely bypassed.

New Features in AnyConnect 4.3.00748

AnyConnect 4.3.00748 is a major release that includes the following features and enhancements and that resolves the defects described in AnyConnect 4.3.00748, on page 29.

- In Network Visibility Module (NVM), adjustments to the rate at which data is sent from the cache to the collector.
- Customization of the NVM timer so that an administrator can define when Cisco nvzFlow exports the data.
- Broadcast and multicast options turned off as a default in NVM, with option to choose data collection methods.
- Creation of anonymization profiles in NVM by including or excluding certain fields to anonymize, and then association of the profiles with a network type or connection scenario.
- Other NVM enhancements such as the ability to know the edition of the operating system (OS), what is running in OS containers, and what interface attributes exist.
- Ability to disable Network Access Manager-originated DHCP requests.
- (Windows only) Detection by posture client of USB mass storage devices and the ability to block or deny access. This feature relies on the OPSWAT v4 compliance module.
- The introduction of OPSWAT version 4, which combined antivirus and antispyware under an anti-malware umbrella. With ISE posture on AnyConnect release 4.3 (or later) or ISE 2.1 (or later), you can choose to use either OPSWAT v3 or v4.
- Upon installation of Start Before Logon, the Network Connection button launches both AnyConnect VPN and Network Access Manager UI.
- A new profile editor Preferences option where the match to certificates with no Extended Key Usage (EKU) can be disallowed.
- More detailed information with certificates in the form of AnyConnect logs to better track certificate handling.
- AnyConnect 4.3 has moved to Visual Studio (VS) 2015 build environment and requires VS redistributable files, which are installed as part of the install package.
- Support for Ubuntu 15.04.

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 1.3 server if NAC Agent is provisioned for the endpoint.
- If the Cisco NAC agent and the AnyConnect ASA Posture 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 1.3 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 1.3 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 1.3 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, Release 2.0.

ASA Requirements for AnyConnect

ASA Release Requirements

- 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
  - 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 host Scan, 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.

ASA Posture and Hostscan Interoperability

The ASA Posture 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 ASA Posture Module requires Cisco Hostscan to gather this information. Cisco Hostscan, available as its own software package, is periodically updated with new operating system, antivirus, antispyware, 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 Antivirus, Antispyware, 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. Ensure that you are running the version of HostScan that is the same version as AnyConnect. Also, Cisco does not recommend the combined use of HostScan and ISE posture. Unexpected results occur when two different posture agents are run.

The Cisco Host Scan package can be pre-deployed or installed on an ASA version 8.4 or later for web-deploy.

ISE Posture Compliance Module

The ISE Posture compliance module contains the list of supported antivirus, antispyware, 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. You can view the charts using Microsoft Excel, Microsoft Excel Viewer, or OpenOffice at this location: .

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 4.3 Supported Operating Systems

Cisco AnyConnect Secure Mobility Client, Release 4.3 supports the following operating systems for its contained modules:

Supported Operating Systems	VPN Client	Network Access Manager	Cloud Web Security	ASA Posture	ISE Posture	DART	Customer Experience Feedback
Windows 7 SP1, 8, 8.1 & 10 x86(32-bit) and x64(64-bit)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mac OS X 10.9, 10.10, 10.11, and 10.12 [1]	Yes	No	Yes	Yes	Yes	Yes	Yes
Linux Red Hat 6, 7 & Ubuntu 12.04 (LTS),14.04 (LTS), and 15.04 (LTS) (64-bit only)	Yes	No	No	Yes	No	Yes	Yes

1 AnyConnect 4.3.3086 and 4.2.6014 are the minimum required releases for 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 (http://support.microsoft.com/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.
- 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 OS X

Mac OS X Requirements

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

Mac OS X 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 see: http://www.apple.com/macosx/mountain-lion/security.html.

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, Release 4.3 .

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, Release 2.1 .

To deploy AnyConnect from an ASA headend and use the VPN and ASA Posture 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, Release 4.3.

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 ASA 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 4.3.

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 Host Scan 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 Host Scan 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 feature 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

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 No Longer Supporting SHA-1

A secure gateway with a SHA-1 certificate or a certificate with SHA-1 intermediate certificates is considered valid by a Windows endpoint until February 14, 2017. After February 14, 2017, Windows endpoints will no

longer consider a secure gateway with a SHA-1 certificate as trusted. Ensure that your secure gateway does not have a SHA-1 identity certificate and that any intermediate certificates are not SHA-1.

"Code Signing Certificates: Windows will no longer trust files with the Mark of the Web attribute that are signed with a SHA-1 code signing certificate and are timestamped after 1/1/2016." Refer to the Microsoft documentation for more details: here

Files signed before January 1st, 2016 will be valid until February 14, 2017.

Note Due to the code signing changes, the current AnyConnect users **must** upgrade to 3.1.13011, 4.2.01035, or AnyConnect 4.3 releases in order to keep their AnyConnect functional on Windows platforms after February 14, 2017.

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.

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.

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.

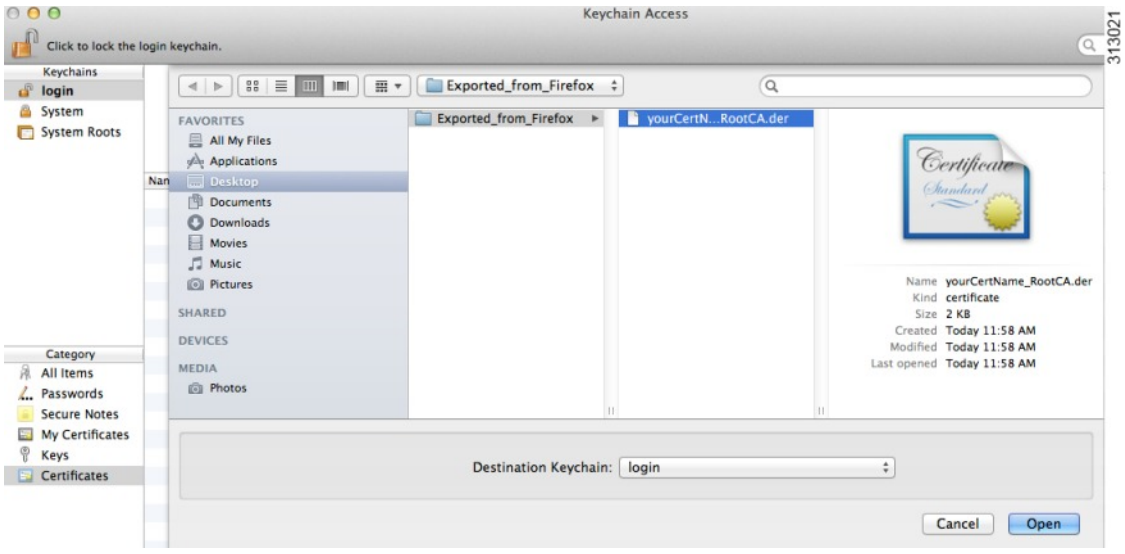
Firefox Certificate Store on Mac OS X is Not Supported

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.

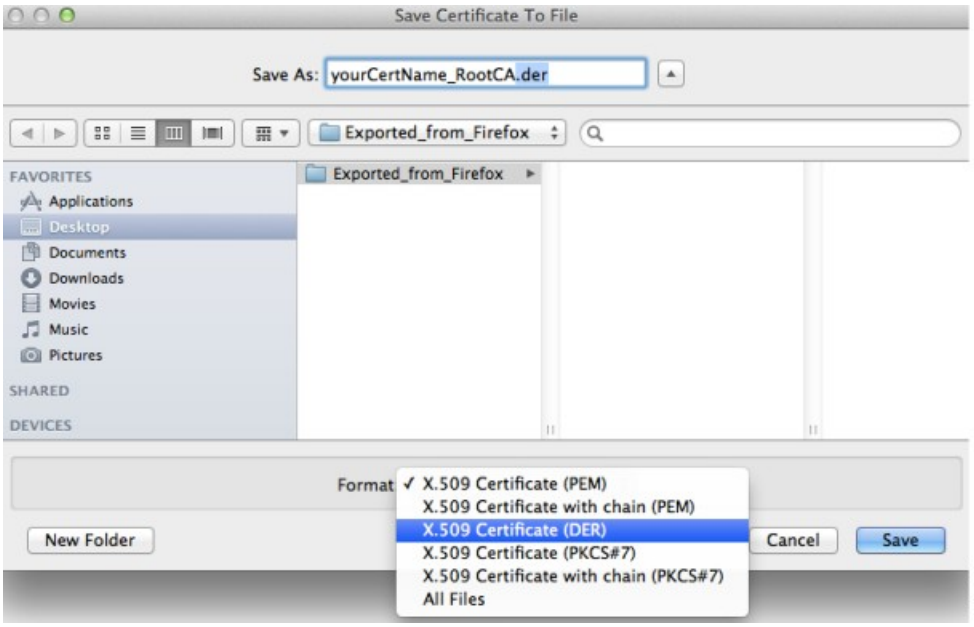


Note If more than one AnyConnect Certificate and/or a Private Key is used/required, repeat the above process for each Certificate).

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 Host Scan From Working

(CSCue04930) Host Scan 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 Host Scan 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 via Tokend on Mac OS X, 10.4 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:

- 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 Host Scan

Antivirus applications can misinterpret the behavior of some of the applications included in the posture module and the Host Scan package as malicious. Before installing the posture module or Host Scan package, configure your antivirus software to “white-list” or make security exceptions for these Host Scan 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 Host Scan Reports

None of the supported antivirus, antispyware, and firewall products report the last scan time information. Host scan reports the following:

- For antivirus and antispyware
  - 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 4.3.03086

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

Table 1: Resolved

Identifier	Component	Headline
CSCuy68051	api	Certificate expiration warning not displayed when using IKEv2
CSCva69697	api	Customer API examples migration to Visual Studio 2015
CSCuz27826	core	The DHCP route breaks other services on same server
CSCva28494	core	AC always-on should be disabled by DAP after shutdown

CSCvb43782	core	Upgrade to 4.3MR1 client causes BSOD on Windows 7
CSCva64096	dart	Linux: Posture logs not getting copied in DART
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
CSCva31341	nvm	acnvmagent consumes almost 3% of the CPU on Mac OS X
CSCvb64718	posture-asa	Mac OS 10.12 (Sierra) FW not detected by HostScan
CSCux64789	profile editor	Getting the same error message twice while create Websec Client profile
CSCva44991	umbrella	Incorrect Protection state is displayed with ipv6 enabled AC client
CSCvb34863	umbrella	Umbrella Roaming - Split Tunnel Latency
CSCvb34863	vpn	Umbrella Roaming - Split Tunnel Latency
CSCut70079	vpn	Untrusted Server Certificate when AnyConnect fails over to backup server
CSCux03030	vpn	AC OS X using PUBLIC proxy and using load balanced ASA's (VIP) fails
CSCuz80602	vpn	AnyConnect ESP_ERROR_EXPIRED_SEQ - IPsec engine encountered an error
CSCva55838	vpn	AC probes for mus.cisco.com even if no related component is enabled
CSCvb02196	vpn	AnyConnect DNS suffic not getting removed from fresh install Windows 10
CSCvb05479	vpn	"Apply Last VPN Local Resource Rules" not apply after reboot
CSCvb17874	vpn	AnyConnect SBL fails to detect smart card certificate
CSCvb21345	vpn	AnyConnect stops responding after IOS IKEv2 credential prompt submit
CSCvb36565	vpn	9.7.1 SAML 2.0 AnyConnect - Certificate map breaks SAML authentication

CSCvb36651	vpn	9.7.1 SAML 2.0 AnyConnect - HostScan not working on SAML enabled TG
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
CSCvb50660	vpn	Unable to pass connection-less fragmented traffic (AC 4.3 on Mac)
CSCvb62962	vpn	OS X: Deflate compression does not work (can't pass data)
CSCva44152	web security	ACWebsec crash due to none encrypt .config file
CSCvb29440	web security	AnyConnect Websecurity incompatible with MS Direct Access

Table 2: Open

CSCvb42287	posture-asa	Posture module is missing on upgrade from ISE
CSCvb46561	posture-asa	HostScan not working on XFS filesystem (RHEL 7)

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

AnyConnect 4.3.02039

Caveats Resolved and Open

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

Table 3: Resolved

Identifier	Component	Headline
CSCuz59461	core	AC client does not send "endpoint.anyconnect.devicetype"
CSCva48371	core	AC Websec causes Windows 10 BSOD
CSCva58530	download_install	Ubuntu: Posture fails to install using web deploy
CSCuz80234	gui	AC 4.x customizing "Checking compliance" message

CSCva64580	gui	AC 4.3.x crashes when using client cert auth using Smart Card
CSCva40868	nam	EAP-TLS is failing for machine authentication on AnyConnect 4.3
CSCux82427	nvm	Revisit DNS cache handling of CNAME DNS requests
CSCuy38610	posture-asa	HostScan initialize error: Windows username with non-English alphabets
CSCuz84937	posture-asa	HostScan timestamp returns -1 for Norton Security
CSCva36699	posture-ise	ISE does not recognize Windows 10 LTSB as a supported operating system
CSCva38809	posture-ise	AC 4.3 posture module sending wrong user agent for Windows 10
CSCud02668	web security	FQDN feature in KDF: Host exception does not honor https site
CSCva67994	web security	ACWS PE is not allowing host names for static exceptions

Open

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

AnyConnect 4.3.01095

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
CSCux46392	core	IPv6 - IPsec split tunneling not working when IPv4 DNS server is config
CSCuy01833	core	split-dns suffixes not added to adapter unless Default Domain defined

CSCuz50259	core	AC w/TND ignores CRL pref setting <EnableCRLCheck>false</EnableCRLCheck>
CSCuw28279	download_install	vpn download fails if username is in Non-English (Japanese or Russian)
CSCuz08974	gui	AnyConnect setup.exe chooser size is not standard on all PCs
CSCva21660	nvm	AnyConnect NVM handles/leak for acnvmagent.exe*32
CSCva05994	posture-ise	ISE AnyConnect configuration issue with compliance module 3.6.10591.2
CSCuy02579	posture-ise	ISE posture module should not rely on NAM
CSCuw99688	vpn	DNS lookups not entering IPsec tunnel on OS X

Table 5: Open

Identifier	Component	Headline
CSCva44991	umbrella	Incorrect Protection state is displayed with ipv6 enabled AC client
CSCva46737	umbrella	"Reserved" state lingering way too long after network/VPN changes

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

AnyConnect 4.3.00748

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
certificate	CSCuy12161	AnyConnect should no longer require KeyAgreement in Server Certificate

core	CSCuy34417	AnyConnect client profile list not in alphabetical order
core	CSCuy88042	Notify user when HostScan posture assessment fails via slow network links
gui	CSCut27870	AnyConnect has exclamation mark on successful connect
nvm	CSCux94887	Mac hostname fetched should be computer name
nvm	CSCuy13416	NVM fails to capture flow information
posture-asa	CSCuz50866	HostScan fails to detect McAfee disk encryption
posture-ise	CSCuw81938	AnyConnect posture module sends illegal character in posture XML report
posture-ise	CSCux01500	PM remediation failing with wrong error message
posture-ise	CSCuz04267	AV/AS and PM remediation does not work on standard users
vpn	CSCuu68856	IKEv2 event log message misleading
vpn	CSCuv74296	SBL does not work on Windows 10
vpn	CSCuw43845	Cert match rule should override all default filtering rules for EKU
vpn	CSCux04097	Implement fails safe mechanism for hosts file
vpn	CSCuy78946	AnyConnect does not connect with PEM store on Linux
web security	CSCux63081	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.

Table 7: Open

Identifier		Headline	
posture-ise		LANdesk "Update Remediation Support" is not supported under CM 4.x	
posture-ise		Posture recycled when initial PDP is down provides no connectivity	
posture-ise		USB remediation does not happen on one of Win 7 client	
posture-ise		CM V4-AVG 2015 definition check is failing on Mac OSX 10.9	
vpn		VPN is initiated before Websec TND is determined and when TND changes	
vpn		After successful Mac upgrade WebSec service is not running	

Related Documentation

Other AnyConnect Documents

- Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.3
- Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.3
- AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.3
- Open Source Software Used in AnyConnect Secure Mobility Client, Release 4.3
- 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
- Host Scan Support Charts

ISE Related Documents

- Release Notes for Cisco Identity Services Engine, Release 2.1
- Cisco Identity Services Engine Admin Guide, Release 2.1

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2016-2016 Cisco Systems, Inc. All rights reserved.