Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.1

Last Updated: April 24 2015

This document includes the following sections:

Cisco Systems, Inc.
www.cisco.com

Downloading the Latest Version of AnyConnect

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

Table 1 AnyConnect Package Filenames for ASA Deployment

OS	AnyConnect Web-Deploy Package Name Loaded onto ASA
Windows	anyconnect-win-<*version*>-k9.pkg
Mac OS X	anyconnect-macosx-i386-<*version*>-k9.pkg
Linux (32-bit)	anyconnect-linux-<*version*>-k9.pkg
Linux (64-bit)	anyconnect-linux-64-<*version*>-k9.pkg

Table 2 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 (32-bit)	anyconnect-predeploy-linux-<*version*>-k9.tar.gz
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.

To obtain the AnyConnect software, follow these steps:

Step 1 Follow this link to the Cisco AnyConnect Secure Mobility Client Introduction 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 “Configuring the ASA to Download AnyConnect” in Chapter 2, Deploying the AnyConnect Secure Mobility Client in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1* to install the packages onto an ASA or to deploy AnyConnect using your enterprise software management system.

Important Security Considerations

- We have removed all AnyConnect software packages prior to AnyConnect 3.1.05182 from Cisco.com because of a security risk found in the OpenSSL software integrated in those releases: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140605-openssl. We recommend that customers running AnyConnect 3.0.X or AnyConnect 3.1.0178 or earlier upgrade to the latest version of AnyConnect 3.1.08009 or AnyConnect 4.0.
- We do not recommend using a self-signed certificate because of the possibility that a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.

Enable Strict Certificate Trust in the AnyConnect Local Policy

We strongly recommend you enable Strict Certificate Trust for the AnyConnect client for the following reasons:

- With the increase in targeted exploits, enabling Strict Certificate Trust in the local policy helps prevent “man in the middle” attacks when users are connecting from untrusted networks such as those in coffee shops and airports.
- Even if you use fully verifiable and trusted certificates, the AnyConnect client, by default, allows end users to accept unverifiable certificates. If your end users were subjected to a man-in-the-middle attack, they may be prompted to accept a malicious certificate. To remove this decision from your end users, enable Strict Certificate Trust.

To configure Strict Certificate Trust see Chapter 9 “Enabling FIPS and Additional Security in the Local Policy” of the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*.

AnyConnect Certificate Requirements

The following behavioral changes have been made to server certificate verification:

- SSL connections being performed via FQDN no longer make a secondary server certificate verification with the FQDN's resolved IP address for name verification if the initial verification using the FQDN fails.
- IPsec and SSL connections require that if a server certificate contains Key Usage, the attributes must contain DigitalSignature AND (KeyAgreement OR KeyEncipherment). If the server certificate contains an EKU: for SSL the attributes must contain serverAuth, and for IPsec the attributes must contain serverAuth OR ikeIntermediate. Note that server certificates are not required to have a KU or an EKU to be accepted.
- IPSec connections perform name verification on server certificates. The following rules are applied for the purposes of IPSec name verification:
  - If a Subject Alternative Name extension is present with relevant attributes, name verification is performed solely against the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates, and additionally include IP address attributes if the connection is being performed to an IP address.
  - If a Subject Alternative Name extension is not present, or is present but contains no relevant attributes, name verification is performed against any Common Name attributes found in the Subject of the certificate.

– If a certificate uses a wildcard for the purposes of name verification, the wildcard must be in the first (left-most) subdomain only, and additionally must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance is ignored for the purposes of name verification.

Increased Security in the AnyConnect Pre-deploy Package

The AnyConnect pre-deploy VPN package previously installed the VPN WebLaunch ActiveX control by default. Starting in AnyConnect 3.1, installation of the VPN ActiveX control is turned off by default. This change was made to favor the most secure configuration as the default behavior.

When pre-deploying the AnyConnect Client and Optional Modules, if you require the VPN ActiveX control to be installed with AnyConnect, you must use the NOINSTALLACTIVEX=0 option with msiexec or a transform. For example, on one line enter:

```
msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive
NOINSTALLACTIVEX=0 /lvx*
```

Important AnyConnect, Host Scan, and CSD Interoperability Information

We always recommend that you upgrade to the latest Host Scan engine version.

Caution AnyConnect will not establish a VPN connection when used with an incompatible version of Host Scan or CSD.

Caution If you cannot upgrade AnyConnect and Host Scan or AnyConnect and CSD at the same time, upgrade Host Scan or CSD first, then upgrade AnyConnect.

Table 3 AnyConnect and Cisco Secure Desktop Compatibility

AnyConnect Client Version	Cisco Secure Desktop Version	Are these versions compatible?
3.0.08057 or later	3.6.6020 or later	yes
3.0.08057 or later	3.6.5005 or earlier	no
2.5.6005 or later	3.6.6020 or later	yes
2.5.6005 or later	3.6.5005 or earlier	no
2.5.3055 or earlier	Any version of CSD	no

Table 4 AnyConnect and Host Scan Compatibility

AnyConnect Client Version	Host Scan Version	Are these versions compatible?
3.0.08057 or later	3.0.08057 or later	yes
3.0.07059 or earlier	3.0.08057 or later	yes

Table 4 AnyConnect and Host Scan Compatibility

AnyConnect Client Version	Host Scan Version	Are these versions compatible?
2.5.6005 or later	3.0.08057 or later	yes
2.5.6005 or later	3.0.07059 or earlier	no
2.5.3005 and earlier	Any version of Host Scan	no

Deprecation of Features: Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection

Cisco dropped support for the Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection (KSL), and Host Emulation Detection features as of August 20, 2014.

These features will continue to provide the functionality for which they were built, but will eventually be incompatible with future releases of the ASA, ASDM, AnyConnect, or the operating system on which the endpoint runs.

For more information, see the deprecation field notice "Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection Features Are Deprecated."

CSD and AnyConnect Restrictions with Windows

If AnyConnect is running with CSD, then on Windows 7 or later and Vista clients, for non-admin users, DAP policies for registry checks and files can fail.

Important AnyConnect 3.1 and ASA 9.0 Interoperability Considerations

The following AnyConnect features require ASA 9.0 or later, or ASDM 7.0 or later, to be installed on your ASA for them to be effective:

- IPv6 Support for AnyConnect VPN Features
- Next Generation Encryption as it applies to VPN
- Deferred Upgrades

Installation Overview

AnyConnect integrates the following modules into the AnyConnect client package:

- Network Access Manager
- Host Scan

- Web Security
- DART

If you are using the ASA to deploy AnyConnect, the ASA can deploy all the optional modules. If pre-deploying using your SMS, you can deploy all modules, but you must pay special attention to the module installation sequence and other details.

AnyConnect shares its Host Scan component with Cisco Secure Desktop (CSD). The stand-alone Host Scan package for AnyConnect provides the same features as the Host Scan package that is part of CSD. The AnyConnect client can co-exist with Cisco Secure Desktop Vault, but it cannot be run or deployed from inside the Vault.

Every release of AnyConnect includes a localization MST file that administrators can upload to the ASA whenever they upload AnyConnect packages with new software. If you are using our localization MST files, make sure to update them with the latest release from CCO whenever you upload a new AnyConnect package.

For more information about deploying the AnyConnect modules, see the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1.*

Upgrading 3.0 AnyConnect Clients and Optional Modules

When you upgrade from AnyConnect Secure Mobility Client Release 3.0 to AnyConnect Secure Mobility Client Release 3.1, AnyConnect 3.1 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 2.5 and older AnyConnect Clients and Optional Modules

When you upgrade from any 2.5.x version of AnyConnect, the AnyConnect Secure Mobility Client Release 3.1 performs the following:

- Upgrades all previous versions of the core client and retains all VPN configurations.
- If you install Network Access Manager, AnyConnect retains all CSSC 5.x configuration for use with Network Access Manager, then removes CSSC 5.x.
- Upgrades any Host Scan files used by AnyConnect.
- ***Does not*** upgrade the Cisco IPsec VPN client (or remove it). However, the AnyConnect 3.1 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 so as to achieve optimal performance when using AnyConnect.

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.

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.

AnyConnect Support for Windows 8.x

Requirements

ASDM version 7.02 or higher

Limitations to AnyConnect Support for Windows 8.x

- Upgrading to Windows 8.1 requires you to uninstall AnyConnect, and reinstall it after your Windows upgrade is complete.
- AnyConnect is not supported on Windows RT. There are no APIs provided in the operating system to provide this functionality. Cisco has an open request with Microsoft on this topic. Customers 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.
- Verify that the driver on the client system is supported by Windows 8. Drivers that are not supported by Window 8 may have intermittent connection problems.

- For Network Access Manager, machine authentication using machine password will not work on Windows 8 / 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 / 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 server before the user logs in. During this time server can perform scheduled administrative tasks for this client machine. Machine authentication is also required for the EAP Chaining feature where a server can authenticate both User and Machine for a particular client. This will result in identifying company assets and applying appropriate access policy. For example, if this is a personal asset (PC/laptop/tablet), and a company login is used, server will fail Machine authentication, but succeed User authentication and will apply proper access restrictions to this client desktop.

- 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.
- HP Protect tools do not work with AnyConnect on Windows 8.x.

Changes in AnyConnect 3.1.08009

AnyConnect 3.1.08009 is a maintenance release that resolves defects described in Caveats Resolved by AnyConnect 3.1.08009, page 26.

Changes in AnyConnect 3.1.07021

AnyConnect 3.1.07021 is a maintenance release that resolves the 2015 OpenSSL Vulnerabilities in CSCus42746 and other the defects described in Caveats Resolved by AnyConnect 3.1.07021, page 29. Also, read the section below for issues with Microsoft's February 10, 2015 patch.

Microsoft Permanent Fix for Windows 8.1 AnyConnect Incompatibility

Microsoft's Patch update on February 10, 2015 introduced an OS regression which impacts Windows 8.1 users running AnyConnect. This issue will also impact some Windows 7 users if they have IE11 installed.

To resolve this issue, install the Windows 8.1 March cumulative security update for Internet Explorer (MS15-018) or the Vulnerability in SChannel could allow security feature bypass: March 10, 2015 (MS15-031) update. This update is being distributed by Windows update. After the update is installed, the "fixit" or other workarounds are no longer needed. Go here for more details.

The Cisco Tracking ID is CSCus89729. Further details are available here: https://tools.cisco.com/bugsearch/bug/CSCus89729.

Changes in AnyConnect 3.1.06079

AnyConnect 3.1.06079 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.06079, page 29.

Changes in AnyConnect 3.1.06078

AnyConnect 3.1.06078 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.06078, page 30.

Changes in AnyConnect 3.1.06073

AnyConnect 3.1.06073 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.06073, page 30, and contains Host Scan Engine 3.1.06073. The versions of Antivirus, Antispyware, and Firewall products supported by Hostscan are listed on http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-device-support-tables-list.html.

Changes in AnyConnect 3.1.05187

AnyConnect 3.1.05187 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.05187, page 32, and contains Host Scan Engine 3.1.05183.

AnyConnect 3.1.05187 also adds support for Mac OS X 10.10. Support for Mac OS X 10.7 has been dropped.

Changes in AnyConnect 3.1.05182

AnyConnect 3.1.05182 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.05182, and contains Host Scan Engine 3.1.05182.

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*.

AnyConnect 3.1 installations can coexist with other VPN clients, including IPsec clients, on all supported endpoints; however, we do not support running AnyConnect while other VPN clients are running.

The following sections identify the minimum management and endpoint requirements:

- Adaptive Security Appliance Requirements
- IOS Support by AnyConnect 3.1.x
- Microsoft Windows

- Linux
- Mac OS X

Adaptive Security Appliance Requirements

- 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 license. 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.

Memory Requirements

Caution The minimum flash memory recommended for all ASA 5500 models using AnyConnect 3.1 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 internal memory requirements for each ASA model, see Memory Requirements for the Cisco ASA Adaptive Security Appliances Software Version 8.3 and Later. For additional information about the ASA memory requirements and upgrading ASA memory, see the latest release notes for the Cisco ASA 5500 series.

IOS Support by AnyConnect 3.1.x

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.

Microsoft Windows

Table 5 Microsoft Windows OS Support for the modules and new features in AnyConnect 3.1.

AnyConnect 3.1 Module	Feature	Windows XP SP3 x86 (32-bit) Windows XP SP2 x64 (64-bit)	Windows Vista x86 x86 (32-bit) and x64 (64-bit) Windows 7 x86 (32-bit) and x64 (64-bit) Windows 8, 8.1, and 8.1 Update 1 x86 (32-bit) and x64 (64-bit)
	Customer Feedback	Yes	Yes
VPN	Core	Yes	Yes
	IPv6	No	Yes
	Suite-B (IPsec Only)	No	Yes
Network Access Manager	Core	Yes x86 (32-bit) only	Yes
	IPv6	No	Yes
	Suite-B	No	Yes

Table 5 Microsoft Windows OS Support for the modules and new features in AnyConnect 3.1.

AnyConnect 3.1 Module	Feature	Windows XP SP3 x86 (32-bit) Windows XP SP2 x64 (64-bit)	Windows Vista x86 x86 (32-bit) and x64 (64-bit) Windows 7 x86 (32-bit) and x64 (64-bit) Windows 8, 8.1, and 8.1 Update 1 x86 (32-bit) and x64 (64-bit)
Posture & Host Scan	Core	Yes	Yes
	IPv6	No	Yes
	Keystroke Logger	Yes x86 (32-bit) only	Yes x86 (32-bit) only
Telemetry		Yes	Yes
Web Security		Yes x86 (32-bit) only	Yes
DART		Yes	Yes

Windows Support Notes

- After April 8, 2014, Microsoft will no longer provide new security updates, non-security hotfixes, free or paid assisted support options, or online technical content updates for Windows XP (http://www.microsoft.com/en-us/windows/endofsupport.aspx). On the same date, Cisco will stop providing customer support for AnyConnect releases running on Windows XP, and we will not offer Windows XP as a supported operation system for future AnyConnect releases.
- When Windows XP is configured with a secondary IP address, starting an AnyConnect connection starts the IpFilterDriver, which blocks traffic over the secondary IP. To prevent this, disable the ipFilterDriver with the following command:

  ```
  sc config IpFilterDriver start= disabled
  ```

  Make sure you enter the whitespace between “start=” and “disabled”.
- Upgrading from Windows XP to Windows Vista or Windows 7 or later 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.
- Windows 2003 Server (32 bit) is supported for Network Access Manager only.
- Windows 2008 is not supported; however, we do not prevent the installation of AnyConnect 3.1 on this OS.
- 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+.

Note Internet Explorer 6.0 is no longer supported.

- AnyConnect VPN is compatible with 3G data cards which interface with Windows 7 or later via a WWAN adapter.
- On Windows XP, schannel.dll supports only 3DES and not AES encryption; therefore, an ASA on which XP clients terminate must have 3DES enabled with the ssl encryption **aes128-sha1 aes256-sha1 3des-sha1** command.

Windows Requirements

- Pentium class processor or greater.
- 100 MB hard disk space.
- Microsoft Installer, version 3.1.

Linux

Table 6 Linux OS Support for the modules and new features in AnyConnect 3.1

AnyConnect Module 3.1	Feature	Red Hat Enterprise Linux 6.x (32-bit) and 6.4 (64-bit)	Ubuntu 9.x, 10.x, and 11.x (32-bit) and Ubuntu 12.04 & 12.10 (64-bit)
	Customer Feedback	No	No
VPN	Core	Yes	Yes
	IPv6	No	No
	Suite-B (IPsec only)	Yes	Yes
Network Access Manager	Core	No	No
	IPv6	No	No
	Suite-B	No	No
Posture & Host Scan	Core	Yes	Yes
	IPv6	No	No
	Keystroke Logger	Yes	Yes
Telemetry		No	No
Web Security		No	No
DART		Yes	Yes

Linux Requirements

- x86 instruction set.
- 32-bit or 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 or a compatible build such as package pangox-compat-0.0.2-2.el7.x86_64.rpm or pangox-compat-0.0.2-3.fc20.x86_64.rpm
- iptables 1.2.7a or later.
- tun module supplied with kernel 2.4.21 or 2.6.

Linux Support Notes

The AnyConnect GUI is not supported on all Linux distributions. When the GUI is supported, it's appearance is the same as the AnyConnect version 2.5 GUI.

Mac OS X

Table 7 Mac OS X Support the modules and new features in AnyConnect 3.1

AnyConnect Module 3.1	Feature	Mac OS X 10.8, 10.9, & 10.10 x86 (32-bit) or x64 (64-bit)
	Customer Feedback	Yes
VPN	Core	Yes
	IPv6	Yes
	Suite-B (IPsec only)	Yes
Network Access Manager	Core	No
	IPv6	No
	Suite-B	No
Posture & Host Scan	Core	Yes
	IPv6	Yes
	Keystroke Logger	Yes x86 (32-bit) only
Web Security		Yes
DART		Yes

Max OS X Support Notes

- Mac OS X 10.5 is no longer supported. AnyConnect 3.1 will not install on this platform.
- Mac OS X 10.6, and 10.7 are no longer supported.

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 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 release 3.1 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 10.9 to 10.10) install as expected. Only the pre-deploy installation requires additional configuration as a result of Gatekeeper.

Host Scan Engine

Caution See Important AnyConnect, Host Scan, and CSD Interoperability Information, page 4, for important AnyConnect and Host Scan compatibility information.

Tip You should always upgrade to the latest Host Scan engine.

The Host Scan engine, which is among the components delivered by AnyConnect Secure Mobility Client, identifies endpoint posture attributes of the host. Host Scan package, **hostscan_3.1.08009-k9.pkg**, is available for use with AnyConnect 3.1.08009 and higher.

The List of Antivirus, Antispyware, and Firewall Applications Supported by Host Scan is available on cisco.com. The support chart 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.

System Requirements

This Host Scan package can be installed on ASA version 8.4 or later. See Important AnyConnect, Host Scan, and CSD Interoperability Information, page 4 for interoperability information.

Licensing

For brief descriptions and example product numbers (SKUs) of the AnyConnect user license options, see Cisco Secure Remote Access: VPN Licensing Overview.

For our open source licensing acknowledgments, see Open Source Used In AnyConnect Secure Mobility Client 3.1.

For the latest end-user license agreement, see Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 3.1.

AnyConnect Support Policy

We support 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

The following guidelines and limitations for this and previous releases are in effect:

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.

OS X 10.9 Safari Can Disable Weblaunch

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.

Open Safari > Preferences > Security > Manage Website Settings. Click on the ASA and select run in Unsafe Mode.

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 Windows 7 and Windows 8.
- 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 release 2.5.x or 3.0.2, the ASA must have the same version (2.5.x or 3.0.2) 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.

New Certificate Required

AnyConnect 3.0.1047 is signed with the new certificate VeriSign Class 3 Public Primary Certification Authority - G5. Upon installation, Windows XP, Windows Vista, Mac OS X, and Linux users might see a downloader error message, such as the following:

```
An internal certificate chaining error has occurred.
```

This event can occur if one or all of the following are true:

- Root certificates were intentionally pruned.
- Update Root Certificates is disabled.
- The internet is not reachable when an upgrade occurs (for example, you have your ASA in a private network without Internet access).

AnyConnect installations and upgrades might require endpoint users to install the root CA before upgrading or installing AnyConnect. To do so, enable Update Root Certificates and verify that the Internet is reachable before the AnyConnect installation. By default, Update Root Certificates is enabled. Users can also update the root CA manually, as instructed on the VeriSign website.

For more information, see:

- http://technet.microsoft.com/en-us/library/bb457160.aspx
- http://technet.microsoft.com/en-us/library/cc749331%28WS.10%29.aspx

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 for native CSPs that work:

- For Windows 7 or later —Microsoft Enhanced RSA and AES Cryptographic Provider

Caution 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:

Step 1 Open a command window on the endpoint computer.

Step 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
```

Step 3 Identify the <CN> attribute in the certificate. In the example, the CN is *Carol Smith*. You need this information for the next step.

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 Vista and Windows 7 or later, use this command:

```
certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -f -repairstore
-user My <CN> carol smith
```

On Windows XP, use this command:

```
certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)" -f
-repairstore -user My <CN> carol smith
```

Step 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

iPhone Not Supported

This release of AnyConnect does not support Apple iOS. However, you can use the same ASAs to support Apple iOS devices running AnyConnect 3.0 VPN connections. For ASA setup instructions, see the Release Notes for Cisco AnyConnect Secure Mobility Client Release 3.0.x for Apple iOS.

Microsoft Internet Explorer Proxy Not Supported by IKEv2

IKEv2 does not support the Microsoft Internet Explorer proxy. If you need support for that feature, use SSL.

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 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 (CSCtk57290):

- When using the Windows 7 or later *Only use Group Policy profiles for allowed networks* option
- When deploying XP wireless GPO policy on Windows 7 or later

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.

Step 1 Enter **regedit** in the Search Programs and Files text box.

Step 2 Navigate to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters**

Step 3 Double-click **MaintainServerList**.

The Edit String window opens.

Step 4 Enter **No**.

Step 5 Click **OK**.

Step 6 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 v10.6 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 following folders (or at least the Cisco sub-folder):

- For Windows 7 or later users: C:\ProgramData

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. Trend Micro also conflicts with Web Security.

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

ActiveX Controls May Fail During Web-Deployment and Upgrade

Installation of an ActiveX control requires administrative privileges.

AnyConnect web-deployment must install an ActiveX control. If the user can't install that control, then web-deployment fails.

The AnyConnect ActiveX control will change periodically, due to a security fix or the addition of new functionality. Upgrading the ActiveX control will fail during Weblaunch for users with Standard privileges.

To avoid these problems, Administrators can deploy using the AnyConnect pre-installer, SMS, GPO or other administrative deployment methodology.

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

If users use WebLaunch to start AnyConnect on a Mac and the Java installer fails, a dialog box presents a Manual Install link. Users should follow this procedure when this happens:

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

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

Step 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.

Step 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 customers 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 Release Notes for the AnyConnect Secure Mobility Client, Release 3.1 is a living document that we update as we continue to produce maintenance releases and major releases of AnyConnect. As the development of AnyConnect continues, should we find caveats that impact AnyConnect 3.1, or resolve caveats that improve AnyConnect 3.1, we will update these tables and republish this document.

Caveats are fixed for an AnyConnect release until that release reaches end of life. To see Cisco's end of life policy, and which versions are no longer supported, see http://www.cisco.com/c/en/us/products/eos-eol-policy.html.

Caveats Resolved by AnyConnect 3.1.08009

Identifier	Component	Headline
CSCup72548	core	Link level route add for DHCP server fails on Windows 7
CSCut46503	core	Privilege escalation in Cisco AnyConnect client (Linux)
CSCut80840	core	AC v3.1.07021: Weblaunch Code Signing Cert Expired 4/4/15
CSCut52151	download_install	VPN weblaunch and ISE posture fails after AnyConnect customization
CSCut56317	gui	When vpnui.exe is open on the desktop, PC will not shut down.
CSCus79195	gui	AnyConnect Secure Mobility Client Arbitrary Code Execution
CSCut46503	mobile	March 2015 OpenSSL Vulnerabilities
CSCuq89844	posture-asa	DAP does not detect the Sophos AV "lastupdate" values
CSCus05070	posture-asa	ENH: HostScan - add support for Trend Micro Titanium Maximum Security v8
CSCus71120	posture-asa	HostScan: Fails to detect Anti-Virus in Kaspersky Total Security 15.x
CSCus79173	posture-asa	AnyConnect Secure Mobility Client Hostscan path traversal vulnerability
CSCus90159	vpn	MAC: Anyconnect/Homepage functionality broken in Mac OSX
CSCus83057	vpn	AnyConnect on Mac blocks host-only Virtual Machine network communication

Open Caveats in AnyConnect 3.1.08009

Identifier	Component	Headline
CSCum90946	core	Routing Local LAN subnet when Split-include is Supernet of LOCAL subnet
CSCup96999	core	AnyConnect reconnect fails with 3G after screen lock/unlock (sleep mode)
CSCuq37889	core	AnyConnect OGS not working
CSCtz84437	download_install	Connection fails when upgrading from 3.0 connecting to a 3.1 headend

Identifier	Component	Headline
CSCuc53433	download_install	Support change for Proxy Auto-Config using local PAC file
CSCtf20678	gui	Quitting from tray while connection in progress does not stop connection
CSCtx77206	gui	GUI inconsistencies when the VPN component is not (yet) loaded
CSCsq24766	nam	If incorrect old password is supplied during the logon password change.
CSCsq25444	nam	5.1.0.39 password change with local user doesn't update AD
CSCuq62752	nam	AnyConnect cannot connect first time to hidden SSID
CSCuq83437	nam	AnyConnect NAM service needs to be restarted to connect wlan on win 8.1
CSCtw91259	phone-home	PHONEHOME: Documentation bug in SFS
CSCte04839	posture-asa	Feedback is not provided on errors in manual launch
CSCtf40994	posture-asa	CSD 3.5 Cache Cleaner termination, long delay in closing browser
CSCti24021	posture-asa	Posture localization PO file needs updated translation
CSCtk05829	posture-asa	Hostscan does not work when using Google Chrome on a MAC
CSCtq82953	posture-asa	ENH: Allow pre-installed CSD stub to be launched with address parameter
CSCtr39580	posture-asa	JPN CSD: Host Scan Registry MBCS Registry name is not working
CSCtr39606	posture-asa	JPN CSD: Host Scan File MBCS File name is not working
CSCtr39613	posture-asa	JPN CSD: Host Scan MBCS Folder name is not working
CSCtr39630	posture-asa	JPN CSD: Host Scan Process MBCS name is not working
CSCtx06675	posture-asa	ENH: HostScan should provide more granularity in detecting linux flavors
CSCtz73641	posture-asa	UDP ports not detected on Linux and OSX
CSCua68938	posture-asa	HostScan fails to pick the AV defined as a DAP rule
CSCub32322	posture-asa	cstub should validate server certificates for a ssl connection
CSCug08938	posture-asa	HostScan Weblaunch should warn user about Java detection failure on Mac
CSCug19281	posture-asa	HostScan should package published files signed by AnyConnect
CSCui80013	posture-asa	Hostscan “updating software” message is misleading
CSCui80041	posture-asa	Hostscan “waiting for the next scan” message is misleading
CSCua13167	scansafe	ScanSafe Module Host Whitelisting Bypass
CSCui62923	scansafe	AnyConnect web security ignores < SSLPort > option in Websecurity.config
CSCte86255	vpn	TND: Incorrect network type when IPv6 adapters with no gateways present
CSCtf63783	vpn	VPN connection failed because "CSD isn't installed..."
CSCtg45505	vpn	VPN connection fails from network with unusual captive portal

Identifier	Component	Headline
CSCtg97089	vpn	IPsecOverSSL: can't establish VPN connection via data card adapter
CSCti78913	vpn	AC displays the Pre-Login error twice
CSCtk65662	vpn	On my home wifi network VPN incorrectly displays "On a Trusted Network"
CSCtn74489	vpn	Can't WebLaunch/Install on Ubuntu if using Proxy Server & Ignored Hosts
CSCtr38205	vpn	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
CSCts29059	vpn	AC agent sometimes terminates after failed conn where no IP address avai
CSCtx08124	vpn	GUI simply closes w/no error when using a proxy server w/Digest Auth
CSCtx21803	vpn	Message to user is not clear when Client Cert is expired or revoked
CSCty77231	vpn	Anyconnect ikev2 should ignore http-url cert payload
CSCua24005	vpn	Agent not responding to Disconnect button
CSCua92065	vpn	CSSM_SignData - client unable to access private key of a certificate
CSCuc89210	vpn	Can't connect w/Client Cert Auth using Athena smartcard and Athena CSP
CSCud79055	vpn	Anyconnect web deployment unsuccessful & error while connecting to vpn.
CSCue07219	vpn	ASA IKEv2 rekey to AC with duplicate IPSec proposals brings down tunnel
CSCue60100	vpn	VPN need to recognize conn. in progress & not exclude current user cert.
CSCui70300	vpn	Error msg when AC-IKEv2 fails to establish due to IP unavailable/no pkg
CSCuj22359	vpn	IKEv2: Print client error message if anyconnect enable not present on ASA
CSCuj38644	vpn	Scripts are Running even after deleting in the ASA script directory
CSCuj38810	vpn	Proxy Lock down not working when DoNotModify is enabled in ASDM.
CSCul25222	vpn	VPN: AnyConnect should not write the redirected IP to preferences file
CSCuq53322	vpn	AC IKEv2: IKE MTU is set always to 240 hex (576 DEC)
CSCty54514	web	VPN Status Message from "Connection Failed" to Captive portal message
CSCui84433	web	Web-launch needs Admin privilege after pre-install with pre-deploy.iso

Caveats Resolved by AnyConnect 3.1.07021

Identifier	Component	Headline
CSCus71091	certificate	AnyConnect 3.1.06073 PKI card PIN dialogue take up to one minute
CSCur78318	core	AnyConnect 3.1 vpnagent crash with vpncommon module
CSCun08298	download_install	AnyConnect upgrade fails over an active/existing client connection
CSCuq26658	download_install	VPN: Upgrade with setup.exe causes client to get uninstalled
CSCus42726	mobile-android	January 2015 OpenSSL vulnerabilities
CSCur29569	nam	AnyConnect NAM not stable for wireless usb card
CSCur66749	nam	AC NAM 3.1 has periodic high latency and ping timeouts, 3.0 does not
CSCus01288	nam	NAM causes blank login screen page on Windows 10
CSCus15275	nam	AnyConnect NAM scanlist shows zero networks just after hibernation/sleep
CSCuq89844	posture-asa	DAP does not detect the Sophos AV “lastupdate” values
CSCur89372	posture-asa	Unable to upgrade Linux HS from MR5 to MR6 AC version 3.1.5183
CSCus05070	posture-asa	ENH: HostScan - Add support for Trend Micro Titanium Maximum Security v8
CSCus48384	posture-asa	HostScan: Fsecure Standard Client Security firewall 11.51 not detected
CSCup94707	scansafe	Websecurity profile editor needs to launch as admin to update towers list
CSCus66408	scansafe	User granularity fail to recognize second user
CSCur28884	vpn	AnyConnect should not always advertise EAP-AnyConnect and GRE
CSCur75094	vpn	AnyConnect install fails when using Casper deploy to Mac OS X 10.10
CSCur81302	vpn	AnyConnect leaks DTLS master key in memory

Caveats Resolved by AnyConnect 3.1.06079

Identifier	Component	Headline
CSCus68686	scansafe	AnyConnect upgrade fails to replace WebSecurityCert.cfg file on OS X

Caveats Resolved by AnyConnect 3.1.06078

Identifier	Component	Headline
CSCur97471	mobile	AC fails cert auth to ASA v.9.3.2 Beta (multiple client platforms)
CSCus61295	scansafe	Web Security: CWS root CA certificate expired

Caveats Resolved by AnyConnect 3.1.06073

Identifier	Component	Headline
api	CSCum90663	Certificate expiration warning popup shows up only for last 5 days
certificate	CSCuo14790	AnyConnect IKEv2 and SSL fail if server cert has IKE Intermediate EKU
certificate	CSCuo75389	AnyConnect is sending incorrect auth method for IKEv2 ECDSA based auth
cli	CSCun05525	CLI interactive mode cannot parse multi word phrase as a single argument
core	CSCuo35912	Split-tunnel failing when firewall rules are loaded on localized Windows
core	CSCup01084	AC: Local LAN access not working if SPLIT-ACL has two 0.0.0.0/X networks
core	CSCup47639	Get info version on OS X of “Cisco AnyConnect Secure Mobility Client.app”
core	CSCuq50488	AC MR 5 fails to find Cert in Machine Store - “parse request” error
core	CSCuq54873	AnyConnect with SDI softtoken auth fails against 8.4 ASA
download_install	CSCul57278	Weblaunch - IE 11 on Windows 8.1 - ActiveX not used (called) by default
gui	CSCul71233	AnyConnect UI crashes when unchecking options in preferences tab
gui	CSCup39785	AnyConnect UI crash when connecting to ASA
nam	CSCuf27284	NAM: SSO does not work with windows auto logon
nam	CSCul70064	Network profiles are removed from userConfiguration.xml after reboot
nam	CSCun18851	AnyConnect NAM interoperability with Intel WiDi
nam	CSCuo13939	NAM: Client is unable to obtain DHCP address on Windows 8.1
nam	CSCup69555	NAM does not work on Surface Pro 3, fails to associate
nam	CSCur19425	NAM: Crash when coming out of extended connected standby
scansafe	CSCuo38838	Websec client fail to look up TND when it is entered as a full path
vpn	CSCue74449	Browser Proxy code needs to execute on separate thread

Identifier	Component	Headline
vpn	CSCui56016	Proxy authentication failed after upgrade to anyconnect 3.1.04xxx
vpn	CSCuj33081	AnyConnect agent crashed while trying to connect
vpn	CSCum39848	AnyConnect modify IE proxy setting after VPN disconnection
vpn	CSCun19159	HostScan should use the IP address of the first ASA it connected to
vpn	CSCun54861	AnyConnect long username/password of Basic auth via proxy are trimmed
vpn	CSCun60804	AnyConnect 3.1 Linux fails with non-default Firefox profile name
vpn	CSCuo04920	VPN: Downloader timeout needs to be increased from 3 seconds
vpn	CSCuo06683	VPN session establishment failure through auth required proxy
vpn	CSCuo34570	AC 3.1.05160: tunnel group drop down still there when using group-url
vpn	CSCuo65755	AnyConnect 3.x xml profile name comparison is case sensitive
vpn	CSCuo85318	ASA 9.2.1: AnyConnect weblaunch crashed with URL-list in DAP
vpn	CSCuo93772	VPN connection fails with error “MTU too small”
vpn	CSCup06462	Proxy authentication failed after upgrade to anyconnect 3.1.05xxx
vpn	CSCuq20602	AnyConnect closes IKEv2 connection while waiting for Azure auth response

Caveats Resolved by AnyConnect 3.1.05187

Identifier	Component	Headline
CSCuq54873	core	AnyConnect with SDI softtoken auth fails against 8.4 ASA
CSCuq50488	core	AC MR 5 fails to find Cert in Machine Store - "parse request" error
CSCup52757	posture-asa	ENH: AVG 2014 support in HostScan on Mac OSX
CSCur27617	vpn	AnyConnect vulnerable to POODLE attack (CVE-2014-3566) Win/Mac/Linux

Caveats Resolved by AnyConnect 3.1.05182

Identifier	Component	Headline
CSCup97189	posture-asa	Hostscan doesn't detect Trend Micro OfficeScan Client 11
CSCup54966	nam	AnyConnect NAM prevents Microsoft Store Credential request
CSCup69555	nam	NAM: NAM does not work on Surface Pro 3, fails to associate
CSCuq19848	nam	NAM: Unable to use Smart card if the card name contains a "+" sign
CSCuq31511	vpn	DTLS vulnerabilities in OpenSSL
CSCuq12791	vpn	Update 3rd party libraries
CSCuq24666	vpn	SCEP enrollment broken

Related Documentation

For more information, see the following documents:

- Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1
- Open Source Software Used In AnyConnect Secure Mobility Client, Release 3.1
- Release notes for Cisco ASA 5500
- Release notes for Cisco Adaptive Security Device Manager
- Supported VPN Platforms, Cisco ASA 5500 Series
- Release notes for Cisco Secure Desktop
- AnyConnect and HostScan Antivirus, Antispyware, and Firewall Support Charts
- Navigating the Cisco ASA 5500 Series Documentation
- Cisco AnyConnect Secure Mobility Solution Guide
- IronPort AsyncOS for Web User Guide
- IronPort AsyncOS 7.0 for Web Release Notes