Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.1

Last Updated: November 1, 2013

This document includes the following sections:

- Introduction, page 3
- Downloading the Latest Version of AnyConnect, page 3
- Important Security Considerations, page 4
- Important AnyConnect, Host Scan, and CSD Interoperability Information, page 5
- Deprecation of Features: Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection, page 6
- Important AnyConnect 3.1 and ASA 9.0 Interoperability Considerations, page 7
- Installation Overview, page 7
- AnyConnect Support for Windows 8, page 8
- Changes in AnyConnect 3.1.04072 (and 3.1.04074), page 9
- Changes in AnyConnect 3.1.04066, page 10
- Changes in AnyConnect 3.1.04063, page 10
- Changes in AnyConnect 3.1.04059, page 10
- New Features in AnyConnect 3.1.03103, page 10
- Changes in AnyConnect 3.1.02043, page 11
- Changes in AnyConnect 3.1.02040, page 11
- New Features in Release 3.1.02026, page 11
- Changes in AnyConnect 3.1.01065, page 11
- New Features in Release 3.1.00495, page 11
- System Requirements, page 29
- Host Scan Engine Update, 3.1.04075, page 35
- Licensing, page 35

Cisco Systems, Inc.
www.cisco.com

- AnyConnect Support Policy, page 35
- Guidelines and Limitations, page 36
- Application Programming Interface for the AnyConnect Secure Mobility Client, page 46
- AnyConnect Caveats, page 46
- HostScan Engine Caveats, page 70
- Related Documentation, page 73

Introduction

Respecting user values for both seamlessness and simplicity in network access and management while delivering significant enhancements to endpoint security and policy enforcement, AnyConnect supports all capabilities under a single, integrated user interface.

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 3.1.04066**.**

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

Note 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*.

Changes to Server Certificate Verification

The following behavioral changes are being 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, 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*
```

Security Risk for Linux Clients (CSCug31622)

When split tunneling is configured, firewall rules, which allow all traffic, are added to the IPTables. The Linux client may remove these previously defined firewall rules from the IPTable until the clients disconnect from AnyConnect. Windows devices maintain the existing firewall rules, and CSCug31622 was created to maintain the same behavior with Linux. A workaround to configure the client firewall rules on the head-end is listed in CSCug31622.

Important AnyConnect, Host Scan, and CSD Interoperability Information

AnyConnect 3.1.04072 and 3.1.04074 are compatible with Host Scan 3.0.08057 or later versions and CSD 3.6.6020 or later versions.

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
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 will stop developing the Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection (KSL), and Host Emulation Detection features as of November 20, 2012.

Deprecated features, the screens used to configure these features in the Adaptive Security Device Manager (ASDM), and the commands used to configure these features in the Adaptive Security Appliance (ASA) command-line interface will not be removed from the packages in which they are delivered until the end-of-engineering support to address severity 1 and severity 2 defects.

After the features have been deprecated, they 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
- Telemetry
- 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.

AnyConnect 3.1.01065 Installation on Mac OS X Takes Longer than AnyConnect 3.1.00495 Installation on Mac OS X (CSCud17997)

In the AnyConnect 3.1.03103 release, this issue was resolved. However, installation or upgrade from any previous AnyConnect build to AnyConnect 3.1.01065 is expected to take longer on Mac OS X platforms than it did with the AnyConnect 3.1.00495 release. This is due to an AnyConnect installer re-design to support code signing for the Mac OS X Gatekeeper feature.

Those who install AnyConnect 3.1.01065 using the GUI installer will see the delay when the UI shows the messages, "Optimizing system for installed software" and "Registering updated components."

AnyConnect Support for Windows 8

AnyConnect support for Windows 8 32-bit and Windows 8 64-bit operating systems was added in 3.0.11042 and later versions (for 3.0.x versions) and 3.1.02026 and later (for 3.1.x versions), with the following limitations.

Note When upgrading to Windows 8.1, uninstall AnyConnect, and reinstall it after your Windows upgrade is complete.

Requirements

ASDM version 7.02 or higher

Limitations to AnyConnect Support for Windows 8

- 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, written in the Metro design language, that is deployed on Windows 8; however, AnyConnect does run on Windows 8 in desktop mode.
- AnyConnect 3.1.01065 and AnyConnect 3.0.10055, and later AnyConnect 3.0 releases, provide "toast notifications."
- 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.

Changes in AnyConnect 3.1.04072 (and 3.1.04074)

The Mac OS X versions of AnyConnect were updated to 3.1.04074 to resolve the problem of frequent disconnects of the AnyConnect VPN on systems running Mac OS X 10.9 (Mavericks). Apple is aware of this issue and you can reference Apple Bug Report ID 15261749 if you want to open your own case with them. AnyConnect 3.1.0474 also supports Mac OS X 10.8, 10.7 and 10.6.

Once Apple provides a fix for OS X 10.9, we may choose to retract this workaround. At that time, both versions 3.1.04074 and 3.1.04072 of AnyConnect will work reliably with Mac OS X 10.9.

Defect CSCui69769 was fixed by version 3.1.0704.

AnyConnect 3.1.04072 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.04072 and is compatible with Host Scan Engine Update, 3.1.04075.

Note 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.

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

Changes in AnyConnect 3.1.04066

AnyConnect 3.1.04066 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.04066 and is compatible with Host Scan Engine Update, 3.1.04075.

Changes in AnyConnect 3.1.04063

AnyConnect 3.1.04063 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.04063 and is compatible with Host Scan Engine Update, 3.1.04075.

Changes in AnyConnect 3.1.04059

AnyConnect 3.1.04059 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.04059 and is compatible with Host Scan Engine Update, 3.1.04075.

New Features in AnyConnect 3.1.03103

AnyConnect 3.1.03103 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.03103 and is compatible with Host Scan Engine Update, 3.1.04075.

(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.

Although several Linux versions may work with AnyConnect, only the following versions have been qualified for official support: Ubuntu 12.04 and 12.10 (64-bit) and RHEL 6.4 (64-bit). In the AnyConnect 3.2 release, support for Linux 32-bit will be phased out.

(CSCub08319) Added IPv6 public proxy support for Windows (Vista, Windows 7, and Windows 8) and IPv6 private proxy support on platforms already supporting IPv4 private proxy (Windows and Mac OS X).

Changes in AnyConnect 3.1.02043

AnyConnect 3.1.02043 is a maintenance release for Linux that resolves the defects described in Caveats Resolved by AnyConnect 3.1.02043 and is compatible with Host Scan Engine Update, 3.1.04075.

Changes in AnyConnect 3.1.02040

AnyConnect 3.1.02040 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.02040 and is compatible with Host Scan Engine Update, 3.1.04075.

New Features in Release 3.1.02026

- AnyConnect Web Security module
- The VPN feature, Split-DNS.

Changes in AnyConnect 3.1.01065

AnyConnect 3.1.01065 is a maintenance release that resolves the defects described in Caveats Resolved by AnyConnect 3.1.01065 and is compatible with Host Scan Engine Update, 3.1.04075.

Changes to Certificate Verification

AnyConnect release 3.1.01065 requires:

- When a user connects to an ASA that is configured with a server certificate, the checkbox to trust and import that certificate will still display even if there is a problem with the trust chain (Root, Intermediate, etc.) If there are any other certificate problems, that checkbox will not display. The checkbox is shown in Figure 5 on page 28
- For OSX, expired certificates are displayed only when Keychain Access is configured to “Show Expired Certificates.” Expired certificates are hidden by default, which may confuse users.

New Features in Release 3.1.00495

AnyConnect 3.1 makes security improvements and recommendations described in Important Security Considerations on page 4, specifies new compatibility requirements between AnyConnect, Host Scan, and CSD as described in Important AnyConnect, Host Scan, and CSD Interoperability Information on page 5, and introduces the following new features and changes:

- Network Access Manager Profile Converter, page 12
- New Graphical User Interface, page 12
- IPv6 Support for AnyConnect VPN Features, page 14
- Host Scan Engine Updates, page 19
- Next Generation Encryption, page 20

- Network Access Manager Enhancements, page 22
- Web Security Enhancements, page 24
- Deferred Upgrades, page 24
- Customer Experience Feedback, page 25
- Telemetry Module and Customer Experience Feedback Interaction, page 26
- Invalid Certificate Handling, page 26
- Mac OS X Support, page 29
- Additional Translation Tables for AnyConnect Localization, page 29

Network Access Manager Profile Converter

The Network Access Manager module can be configured to convert some existing Windows Vista or Windows 7 or later wireless profiles to Network Access Manager profile format when the module is installed on the client system for the first time.

Restrictions and Limitations

Only infrastructure networks that match the following criteria can be converted:

- Open
- Static WEP
- WPA/WPA2 Personal
- Only non-GPO native Wi-Fi user network profiles are converted.
- WLAN services must be running on the system during profile conversion.
- Conversion will not be done if a Network Access Manager XML configuration file already exists (userConfiguration.xml).

Configuration

To enable network profile conversion, create an MSI transform that sets the **PROFILE_CONVERSION** property value to 1, and apply it to the MSI package. Or change the PROFILE_CONVERSION property to 1 in the command line, and install the MSI package.

For example,

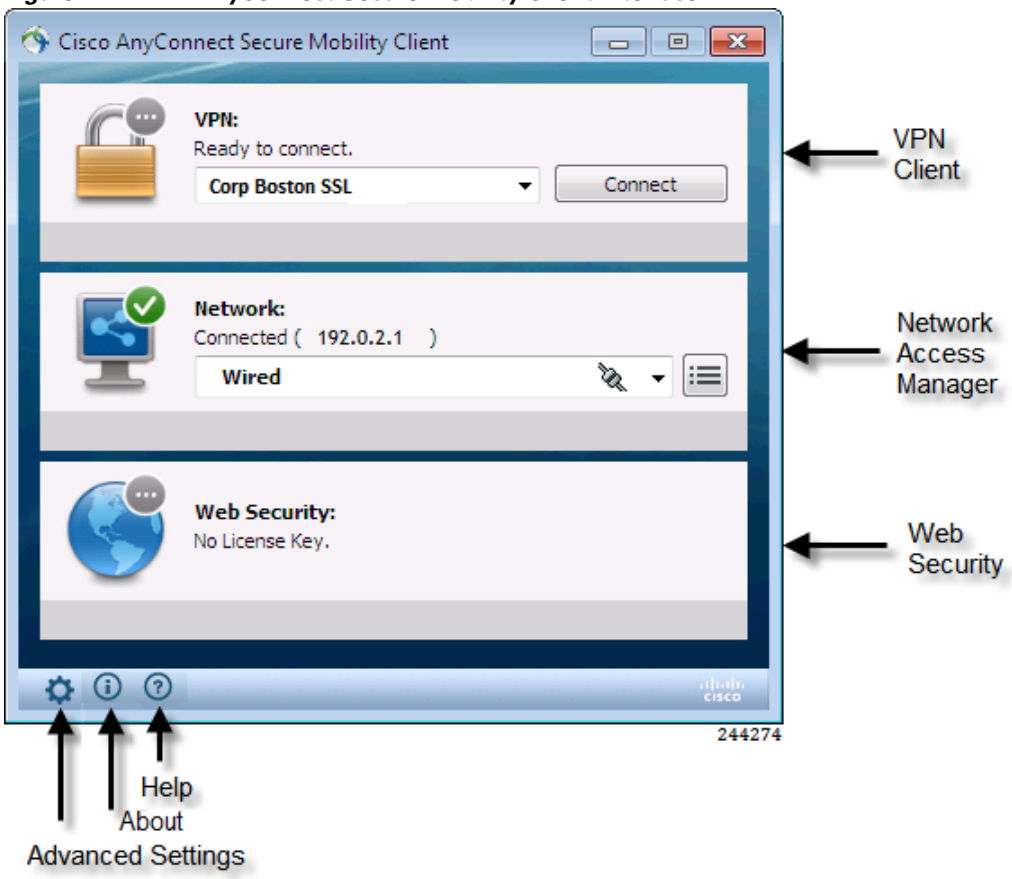
```
msiexec /i anyconnect-nam-win-3.1.xxxxx-k9.msi PROFILE_CONVERSION=1
```

New Graphical User Interface

The new graphical user interface for AnyConnect 3.1 is shown in the following figure.

Note This image shows how the interface looks on a Windows platform. Variances may occur on other operating systems.

Figure 1 AnyConnect Secure Mobility Client Interface



The arrows on the right side of the figure show which AnyConnect modules must be loaded in order to display that block of the user interface.

The arrows on the bottom-left show the icons that open the advanced settings window, and the help.

The help icon only displays if you create and upload a help file on the ASA for the AnyConnect client to download. Instructions for creating and uploading a help file are explained in the next section.

Creating and Uploading a Help File

To provide AnyConnect users with help, create an HTML file with instructions about your site, and load it on the ASA. When users connect with AnyConnect, AnyConnect downloads the help file, and displays the help icon on the AnyConnect user interface. When the user clicks the help icon, the browser opens the help file.

Step 1 Create an HTML file named help_AnyConnect.html.

Step 2 Log on to the ASDM, connect to your ASA, and select **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Binary.**

Step 3 Import the help_AnyConnect.html file.

Step 4 On a PC, bring up AnyConnect and connect to your ASA. The help file is downloaded to the client PC.

Step 5 You should see that the help icon was added to the UI automatically.

Step 6 Click the help icon, and the help file opens in the browser.

If the help icon does not appear, check the help directory to see if the AnyConnect downloader was able to retrieve the help file.

The “help_” part of the filename is removed by the downloader, so you should see AnyConnect.html in one of the following directories, depending on the operating system:

- Windows 7 or later and Vista—C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help
- Windows XP—C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Help
- Mac OS—/opt/cisco/anyconnect/help

IPv6 Support for AnyConnect VPN Features

This release of AnyConnect adds support for IPv6 VPN connections to its outside interface using SSL and IKEv2/IPsec protocols and adds support for IPv6 VPN traffic on its inside interface using the SSL protocol. See Supported Network Configurations.

Note These features require ASA 9.0 or later, ASDM 7.0 or later, or both, to be installed on your ASA for them to be effective. ASA 9.0 is under development and is currently scheduled to be released in the fourth quarter of 2012. To be notified automatically when the software is released, create a software notification on Cisco.com.

Public Tunneling

The ASA accepts connections from IPv4, IPv6, or both IPv4 and IPv6 addresses on its outside interface.

IPv6 Transition Technology Support

A variety of transition technologies were developed to support the transition from IPv4 to IPv6. These technologies can be divided into two types: network address translation (NAT) technology and tunneling technologies.

Tunneling technologies can be subdivided into cloud tunneling technologies, where the tunneling is performed in the cloud with no changes to the client, and client-based tunneling technology, where changes are required for the client.

AnyConnect 3.1 supports these NAT technologies:

- NAT IPv6 to IPv4 (NAT64)
- DNS look-ups of IPv6 addresses. (DNS64)Both IPv4 and IPv6 addresses are returned from the DNS server.
- NAT IPv4 to IPv6 (NAT46)
- NAT public IPv6 to private IPv6 (NAT66)
- NAT IPv4 to IPv6 back to IPv4 (NAT464)

AnyConnect 3.1 does not interfere with these technologies:

- IPv6 to IPv4 (6to4)—Enables IPv6 network traffic to be transmitted over an IPv4 network. This is performed over the Internet.

- IPv6 Rapid Deployment (6rd)—Enables IPv6 network traffic to be transmitted over an IPv4 network but this transition mechanism is performed within the client's Internet Service Provider's network.
- IPv6 tunneled in an IPv4 network (6in4)—IPv6 packets are encapsulated in IPv4 packets.

AnyConnect 3.1 **does not support** IPv6 connections originated from virtual tunnel interfaces meant for host-based 6-in-4 tunneling such as Teredo, ISATAP, or 6to4.

Client Protocol Bypass

The Client Protocol Bypass feature allows you to configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

When the AnyConnect client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the AnyConnect connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or "in the clear."

For example, assume that the ASA assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual-stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

The Client Protocol Bypass is configured in group policies on the ASA.

IP Protocol Fallback

For clients assigned both an IPv4 and IPv6 address that attempt to connect to the ASA, AnyConnect needs to determine which Internet Protocol to use to initiate the connection. By default, AnyConnect initially attempts to connect using IPv4. If that is not successful, AnyConnect attempts to initiate the connection using IPv6.

The Internet Protocol used to initiate the VPN connection and order of fallback is configurable in an AnyConnect VPN Client Profile.

IPv6 Address Assignment

You can configure the ASA to assign an IPv4 address, an IPv6 address, or both an IPv4 and an IPv6 address to an AnyConnect client by creating internal pools of addresses on the ASA or by assigning a dedicated address to a local user on the ASA.

The endpoint must have the dual-stack protocol implemented in its operating system to be assigned both types of addresses.

Configuring DNS Servers with IPv6 Address

You can define a DNS server in a Network (Client) Access internal group policy on the ASA. You can specify up to four DNS server addresses including up to two IPv4 addresses and up to two IPv6 addresses.

Split Tunneling for IPv6 Network Traffic

Split tunneling enables you to route some network traffic through the VPN tunnel (encrypted) and to route other network traffic outside the VPN tunnel (unencrypted or "in the clear"). You can now perform split tunneling on IPv6 network traffic by defining an IPv6 policy which specifies a unified access control list.

Unified Access Control Lists for IPv4 and IPv6

ACLs on the ASA now support IPv4 and IPv6 addresses. You can even specify a mix of IPv4 and IPv6 addresses for the source and destination. The IPv4 and IPv6-specific filters located at **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options** have been replaced a single **Filter** field.

Maximum Transmission Unit (MTU) Dynamic Discovery

When AnyConnect is configured to use SSL as its VPN tunneling protocol, the ASA and the AnyConnect client determine the optimal tunnel MTU value which is the maximum tunnel MTU that ensures zero packet loss between the client and ASA.

The minimum tunnel MTU size required for tunneling IPv6 packets is 1280 bytes. If the network adapter used by the client to establish the VPN tunnel has the MTU size set to a value lower than the sum of 1280 bytes plus the VPN tunnel encapsulation overhead, for example 1300 bytes, AnyConnect sets the tunnel MTU to 1280 to allow IPv6 traffic to be tunneled. Reducing the MTU size may cause additional packet fragmentation which could have a performance impact. This implementation is an improvement from AnyConnect 3.0, which would have prevented the tunnel establishment all together. This approach allows tunneling of IPv6 traffic regardless of the network adapter MTU.

If your endpoint has a legacy IPsec VPN client installed, the MTU size of the physical network adapter may have been set lower than the optimal MTU value required by the AnyConnect client to tunnel IPv6 traffic. One way to avoid the performance impact due to a suboptimal tunnel MTU is to set the network interface MTU to the default value (typically 1500).

Trusted Network Detection and Always-On

Trusted Network Detection with or without Always-On configured is supported for IPv6 and IPv4 clients connecting to the ASA over IPv4 and IPv6 networks.

VPN Load Balancing

Clients with IPv6 addresses can make AnyConnect connections through the ASA cluster's public-facing IPv6 address or through a GSS server. Likewise, clients with IPv6 addresses can make AnyConnect VPN connections through the ASA cluster's public-facing IPv4 address or through a GSS server. Either type of connection can be load-balanced within the ASA cluster.

For clients with IPv6 addresses to successfully connect to the ASA's public-facing IPv4 address, a device that can perform network address translation from IPv6 to IPv4 needs to be in the network.

VPN Session Roaming

AnyConnect 3.1 supports roaming between IPv4 and IPv6 networks. The AnyConnect client uses the fully qualified domain name of the ASA to maintain the connection to that secure gateway as AnyConnect moves between the two types of networks.

Host Scan Prelogin Checks for IPv6 Addresses

In AnyConnect 3.1, you can include IPv6 address criteria in a prelogin check performed by Host Scan.

If Host Scan is enabled on the ASA, the ASA downloads Host Scan to the endpoint when users attempt an AnyConnect VPN connection. Host Scan then performs a prelogin assessment of various aspects of the endpoint such as operating system, registry keys, digital certificates and IP addresses. Based on the prelogin check, the ASA defines a prelogin policy.

IPv6 Attributes in Dynamic Access Policies

When using ASA 9.0 or later with ASDM 6.8 or later, you can now specify these attributes as part of a dynamic access policy (DAP):

- IPv6 addresses as a Cisco AAA attribute
- IPv6 TCP and UDP ports as part of a Device endpoint attribute
- Network ACL Filters (client)

Session Management

Session management output displays the IPv6 addresses in Public/Assigned address fields for AnyConnect connections, Site to Site VPN connections, and Clientless SSL VPN connections. New filter keywords have been added to support filtering the output to show only IPv6 (outside or inside) connections. There have been no changes to IPv6 User Filters.

Existing AnyConnect Functionality that Does Not Support IPv6

These AnyConnect features are not supported on IPv6.

- Optimal Gateway Selection—Optimal Gateway Selection (OGS) minimizes latency for Internet traffic without user intervention.
- WINS (Windows Internet Name Service)—You cannot specify WINS servers with IPv6 addresses as we do DNS servers.
- Captive Portal Detection and Remediation
- Bypassing public or private proxies

IPv6 System Requirements

The AnyConnect 3.1 IPv6 feature requires the 32-bit and 64-bit versions of these operating systems:

- Windows Vista
- Windows 7 or later
- Mac OS X 10.6 or greater

The AnyConnect 3.1 IPv6 features are not supported on:

- Windows XP
- Linux
- Mobile Devices

Supported Network Configurations

Table 5 Secure Gateway IP Address Configuration and Client IP Address Configuration Support

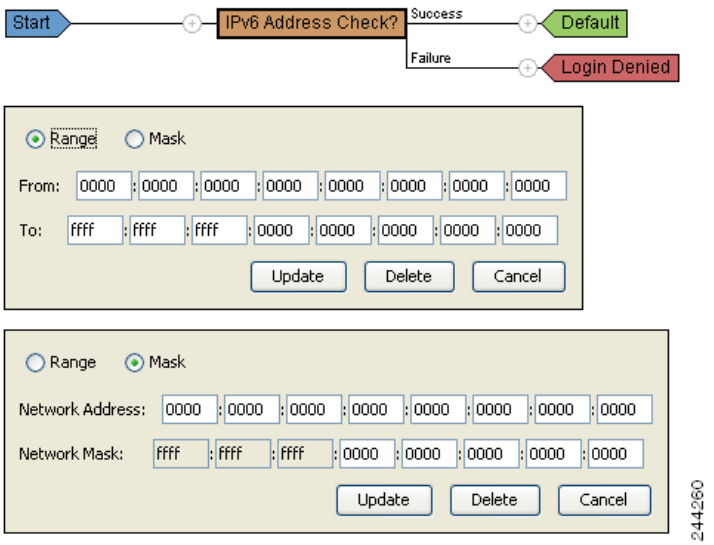
Secure Gateway Configuration		Client Configuration		
Public Address (DMZ or "outside") Interface	**Private Address (MZ or "Inside") Interface***	**IPv4 & IPv6 Dual Stack**	**IPv4 (Dual stack or Single stack)**	**IPv6 (Dual stack or single stack)**
IPv4	IPv4	Exists prior to AC 3.1	Exists prior to AC 3.1	New in AC 3.1 Need a NAT device on edge of network.
IPv4	IPv6 (SSL protocol only)	New in AC 3.1	New in AC 3.1	New in AC 3.1 Need a NAT device on edge of network.
IPv4	Dual Stack (SSL protocol only)	Exists prior to AC 3.1	Exists prior to AC 3.1	New in AC 3.1 Need a NAT device on edge of network.
IPv6	IPv4	New in AC 3.1	New in AC 3.1 Need a NAT device on edge of network.	New in AC 3.1
IPv6	IPv6 (SSL protocol only)	New in AC 3.1	New in AC 3.1 Need a NAT device on edge of network.	New in AC 3.1
IPv6	Dual Stack (SSL protocol only)	New in AC 3.1	New in AC 3.1 Need a NAT device on edge of network.	New in AC 3.1
Dual Stack (Both IPv4 and IPv6)	IPv4 ONLY	Exists prior to AC 3.1	Exists prior to AC 3.1	New in AC 3.1
Dual Stack (Both IPv4 and IPv6)	IPv6 (SSL protocol only)	New in AC 3.1	New in AC 3.1	New in AC 3.1
Dual Stack (Both IPv4 and IPv6)	Dual Stack (SSL protocol only)	Exists prior to AC 3.1	Exists prior to AC 3.1	New in AC 3.1

Host Scan Engine Updates

IPv6 Address Support in Prelogin Policies

Now, prelogin policies can include IPv6 address checks. Administrators can configure prelogin checks for a range of addresses or a single network address with a network mask.

Figure 2 IPv6 Address Check (Default Range and Mask Attributes Displayed)



Updated Host Scan Engine

An updated Host Scan engine, **hostscan_3.1.04059-k9.pkg,** has been incorporated in AnyConnect 3.1.04066.

Host Scan Finds Windows Upgrade Data

Host Scan changed the way it gathers information about Microsoft software updates on a Windows client system. Host Scan previously tracked limited-distribution hotfixes (LDR or QFE). For AnyConnect 3.1, Host Scan tracks service releases (GDR). Although a service release contains hotfixes, those hotfixes are not listed separately.

This change allows you to create DAP rules with endpoint attributes for Microsoft service releases.

Note You will no longer be able to create DAP rules with endpoint attributes for Microsoft hot fixes. If you create an endpoint attribute for a hotfix, that attribute is not found.

Next Generation Encryption

Because the collective set of algorithms defined as National Security Agency (NSA) Suite B are becoming a standard, the AnyConnect IPsec VPN (IKEv2 only), PKI, 802.1X, and EAP now support them. AnyConnect 3.1 uses Cisco SSL 0.9.8r.1.3 FIPS certified implementation of the Suite B ciphers. The next generation encryption (NGE) includes a larger superset of this set adding crypto algorithms for IPsec V3 VPN, Diffie-Hellman Groups 14 and 24 for IKEv2, and RSA certificates with 4096 bit keys for DTLS and IKEv2.

AnyConnect components negotiate and use NGE based on how the headend is configured for it. The Statistics panel (within the Transport Information portion) shows the name of the cipher being used.

Note When used with AnyConnect VPN, these features require ASA 9.0 or later, ASDM 7.0 or later, or both, to be installed on your ASA for them to be effective. ASA 9.0 is under development and is currently scheduled to be released in the fourth quarter of 2012. To be notified automatically when the software is released, create a software notification on Cisco.com.

- Information About NGE, page 20
- Requirements, page 21
- Guidelines and Limitations, page 21

Information About NGE

NGE includes the following functionality:

- AES-GCM support (128-, 192-, and 256-bit keys) for symmetric encryption and integrity
  - (Network Access Manager) 802.1AE (MACsec) for wired traffic encryption in software (Windows 7 or later)
  - (VPN) IKEv2 payload encryption and authentication (AES-GCM only)
  - (VPN) ESP packet encryption and authentication
- SHA-2 (SHA with 256/384/bits) support for hashing
  - (Network Access Manager) Ability to use certificates with SHA-2 in TLS-based EAP methods
  - (VPN) IKEv2 payload authentication (Windows Vista or later and Mac OS X 10.6 or later)
  - (VPN) ESP packet authentication (Windows Vista or later and Mac OS X 10.6 or later)
- ECDH support for key exchange
  - (Network Access Manager) Ability to use ECDHE in TLS-based EAP methods (Windows 7 or later and Windows XP)
  - (VPN) Groups 19, 20, and 21 IKEv2 key exchange and IKEv2 PFS
- ECDSA support (256-, 384-, 521-bit elliptic curves) for digital signature, asymmetric encryption, and authentication
  - (Network Access Manager) Ability to use certificates with ECDSA in TLS-based EAP methods (Only Windows 7 or later and Vista is supported for client certificates. Only Windows 7 or later is supported for smart cards.)

  - (VPN) IKEv2 user authentication and server certificate verification

Note On Linux, AnyConnect can use both the Firefox certificate store or the AnyConnect file certificate store. For ECDSA certificates, only the AnyConnect file store is supported. To add certificates to a file store, see Creating a PEM Certificate Store for Mac and Linux.

- New crypto algorithms for IPsecV3 VPN. AnyConnect 3.1 supports the algorithms required by IPsecV3 except for NULL encryption. IPsecV3 also specifies that Extended Sequence Numbers (ESN) must be supported, but AnyConnect 3.1 does not support ESN.
- Other cipher suite dependencies between algorithms promote support for the following in AnyConnect 3.1:
  - Diffie-Hellman Groups 14 and 24 for IKEv2.
  - RSA certificates with 4096 bit keys for DTLS and IKEv2.

Requirements

- Combined-mode encryption algorithms, where both encryption and integrity are performed in one operation, are supported only on SMP ASA gateways with hardware crypto acceleration (such as 5585 and 5515-X).
- NGE requires an AnyConnect premium license for IKEv2 remote access connections using NSA Suite B algorithms. Suite B algorithm usage for other connections or purposes (such as PKI) has no limitations. License checks are performed for remote access connections. If you receive a message that you are attempting to use an NSA Suite B crypto algorithm without an AnyConnect premium license, you have the option to either install the premium license or reconfigure the crypto settings to an appropriate level.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

- Suite B is available only for IKEv2/IPsec.
- No EAP methods support SHA-2 except in TLS-based EAP when validating certificates signed using SHA-2.
- TLS v1.2 handshaking is not supported in AnyConnect 3.1.
- TLS v1.2 certificate authentication is not supported in AnyConnect 3.1.
- ECDSA certificates are supported on Windows Vista or later and Mac OS X 10.6 or later, ECDSA smart cards are supported only on Windows 7 or later.
- ECDSA certificates must have a Digest strength equal or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
- Suite B profiles may require certain policy properties in the certificates; however, these requirements are enforced on the headend and not by AnyConnect.
- When the ASA is configured with a different server certificate for SSL and IPsec, use trusted certificates. A Posture assessment, Weblaunch, or Downloader failure can occur if using Suite B (ECDSA) untrusted certificates having different IPsec and SSL certificates.

- Because ASA does not support ECDSA certificates for SSL VPN, you should not use such certificates for SSL VPN.
- Because AES-GCM is a computationally intensive algorithm, you may experience a lower overall data rate when using it. Some new Intel processors contain special instructions specifically introduced to improve the performance of AES-GCM. AnyConnect 3.1 automatically detects whether the processor on which it is running supports these new instructions. If so, AnyConnect uses the new instructions to significantly improve VPN data rates as compared to those processors that do not have the special instructions. See http://ark.intel.com/search/advanced/?s=t&AESTech=true for a list of processors that support the new instructions. For more information see http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/.
- In order to use NGE with AnyConnect IKEv2 remote access connections, you must have an AnyConnect Premium license installed on the ASA.

Network Access Manager Enhancements

The following features have been added or enhanced in the AnyConnect 3.1 Network Access Manager:

IPv6

Network Access Manager detects IPv6 Network Attachment and indicates autoconfigured IPv6 addresses to the user. AnyConnect functions on systems where the public interface uses static IPv6 address with SLAAC, ICMPv6, DHCPv6.

Suite B and FIPS

AnyConnect Network Access Manager has implemented certain aspects of the collective set of algorithms defined as National Security Agency (NSA) Suite B. Suite B Cryptography provides greater protection from brute force attacks and stronger authentication.

- ACS and ISE do not support Suite B, but FreeRADIUS 2.x + OpenSSL 1.x does. Microsoft NPS 2008 supports Suite-B in part (the NPS's certificate still has to be RSA).
- 802.1X/EAP supports transitional Suite B profile only (as defined in RFC5430); no support for TLS 1.2.
- MACsec is FIPS-compliant on Windows 7 or later.
- Elliptic Curve Diffie-Hellman (ECDH) key exchange for Windows 7 or later and XP.
- ECDSA client certificate is supported on Windows 7 or later and Vista only.
  - ECDSA CA certificates in OS store are supported on Windows 7 or later and Vista only.
  - ECDSA CA certificates in the network profile (PEM encoded) supported on Windows XP/7/Vista.
  - Server's ECDSA certificate chain verification is supported on Windows XP/7/Vista.
- ECDSA Smart Cards are not supported yet.

Mobile Broadband (3G) (Beta)

This release of AnyConnect adds support for Windows 7 or later Mobile Broadband Adapters, using Microsoft Mobile API. This feature requires also requires a WAN adapter that supports the Microsoft Mobile Broadband APIs. See supported adapters.

This support is disabled by default. To enable the feature, check the Manage Mobile Broadband (3G) Media checkbox in the Client Policy page of a Network Access Manager client profile.

Make Before Break

When you move to a higher priority connection, wired networks are the highest priority, followed by Wi-Fi, and then mobile broadband. AnyConnect makes the new connection before breaking the old one.

Corporate Network Updates

- In the Network Access Manager profile, an administrator can designate a Wi-Fi network as a corporate network.
- AnyConnect connects to a corporate network (if it is in range) before other SSIDs, even if the corporate SSIDs are hidden.
- AnyConnect probes for hidden SSIDs, for Windows 7 or later only.
- AnyConnect periodically scans for new networks.

Start Before Logon (SBL)

SBL now includes the Network Access Manager tile and allows connections using user configured home network profiles. Network profiles allowed in SBL mode include all media types employing non-802-1X authentication modes.

Wireless Radio On

AnyConnect detects when the wireless adapter's radio is turned off, and now shows the status change.

TTLS-PAP

- Token based credentials are now supported, which means users can create a EAP-TTLS/PAP network profile using the UI.
- More granular policies for inner methods can be configured for tunneling EAP methods.

Access Point Status

The Access Point name and IP address has been added to the WiFi section of the AnyConnect Statistics tab.

Incorrect PSK Detection

AnyConnect Network Access Manager detects incorrect Pre-shared Key mismatches in WPA/WPA2 4-way handshake and indicates the mismatch to the user.

EAP Chaining

Use combination of machine and user identification (chained) to authorize wireless network connections. Requires ISE 1.1 MnR.

Web Security Enhancements

The following changes have been made to the Cisco Cloud Web Security (Web Security) module in AnyConnect:

- Beacon Server support is dropped with this release. From AnyConnect 3.1.00459 on, Web Security uses a Secure Trusted Network Detection feature to switch off the service when devices are connected to the corporate network. The Secure Trusted Network Detection feature detects when an endpoint is on the corporate LAN, either physically or through a VPN connection.

  The network traffic bypasses scanning proxies only when the Web security client detects that it is on the trusted network. First, you must enable Trusted Network Detection with the https server configured. Then the Web Security client can access and validate the https server certificate. When these steps are taken and Trusted Network Detection is enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than using Cisco Cloud Web Security.
- AnyConnect 3.1.00459 adds the ability to apply profile configuration changes dynamically for configuration elements that do not require a service restart. When this occurs, “New Configuration detected and applied” appears in the Message History of the client.

  Configuration changes that still require a service restart, such as the IPC port change or the KDF port change are indicated as such in the profile editor and, when applied, will display “New Configuration detected, requires restart.”
- In AnyConnect 3.0, when a connection fails to be established, it is reattempted bypassing the proxy servers. This behavior is now referred to as Fail Open and is the default behavior for AnyConnect 3.1. A new configuration element in the Web Security profile directs these failed connections to be terminated: this behavior is referred to as Fail Close. When you configure the policy for Fail Close, the connection is not reattempted, and the user receives a Connection Failure message from the browser.

  In addition, when the policy is configured to Fail Close, the administrator is given the option to configure a captive portal policy in the same way, specifying Fail Open or Fail Close.
- The default list of Cisco Cloud Web Security proxies has been updated to include Canada, Brazil, South Africa, and Switzerland.

Deferred Upgrades

This feature allows the user to defer an AnyConnect 3.1 client upgrade until later, if configured and enabled on the secure gateway. Deferred Update is configured and enabled by adding custom attributes to the ASA, and then referencing those attributes in the group policies.

Note Deferred updates do not apply to Host Scan file upgrades.

When deferred update is enabled and a client update is available, AnyConnect opens a dialog asking the user if they would like to update or to defer the update. This AnyConnect feature is available on Windows, Linux and Mac OS X supported releases.

Note This feature requires ASA 9.0 or later, ASDM 7.0 or later, or both, to be installed on your ASA for it to be effective. ASA 9.0 is under development and is currently scheduled to be released in the fourth quarter of 2012. To be notified automatically when the software is released, create a software notification on Cisco.com.

The following attributes configure Deferred Update:

- DeferredUpdateAllowed: Adding this customer attribute and setting it to true enables deferred update. If set to false, the attributes below are ignored.
- DeferredUpdateMinimumVersion: The minimum version of AnyConnect that must be installed for updates to be deferrable.
- DeferredUpdateDismissTimeout: Number of seconds that the deferred update prompt is displayed before being dismissed automatically.
- DeferredUpdateDismissResponse: Action to take when DeferredUpdateDismissTimeout occurs, defer or update.

See the User Control over Upgrade section in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1* manual for the procedure to add and set these custom attributes.

Customer Experience Feedback

Note Customer feedback is enabled by default. If you do not want to participate, you must disable this feature.

Cisco has created a customer experience feedback module which provides us with a look at what features and modules customers use and have enabled. The collection of this client information gives us insight into the user experience so that Cisco can continue to improve the quality, reliability, performance, and user experience of AnyConnect.

All data is collected anonymously and does not contain personally identifiable data. The data is also securely sent. You can refer to the End User License Agreement or the Privacy Policy from the About Menu for further information. From the Cisco Online Privacy Statement Highlights page you can access the AnyConnect Secure Mobility Client Supplement which details the collection and use of information.

Administrators can disable this service by clearing the check box at any time after installation. End users must abide by the setting established by the administrators. You must browse to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**, open the client profile you created, and change the Customer Experience Feedback component to disable.

Disabling During Installation

You can also remove the customer experience feedback component altogether during installation, although this is not the Cisco preferred method.

- For web-deploy
  - See the "Configuring the ASA to Download AnyConnect" section in Chapter 2 of the *Cisco AnyConnect Secure Mobility Client Administration Guide, Release 3.1*.

- For Windows pre-deploy
  - See the "Using an SMS to Predeploy AnyConnect Modules" section in Chapter 2 of the *Cisco AnyConnect Secure Mobility Client Administration Guide, Release 3.1*.
- For Linux or Mac pre-deploy
  - See the "Predeploying to Linux and Mac OS X Computers" section in Chapter 2 f the *Cisco AnyConnect Secure Mobility Client Administration Guide, Release 3.1*.

Telemetry Module and Customer Experience Feedback Interaction

With the introduction of the Customer Experience Feedback Module, the telemetry module sends its reports in a different way, although telemetry experienced no architectural changes. When the feedback module and the telemetry module are both enabled, the feedback module sends telemetry reports along with its customer feedback data to our customer feedback server. If the feedback module is not enabled, the telemetry module sends its reports to the Cisco IronPort Web Security Appliance (WSA) as it normally does.

Invalid Certificate Handling

In response to the increase of targeted attacks against mobile users on untrusted networks, we have improved the security protections in the client to help prevent serious security breaches. The default client behavior has been changed to provide an extra layer of defense against Man-in-the-middle attacks.

Updated User Interaction

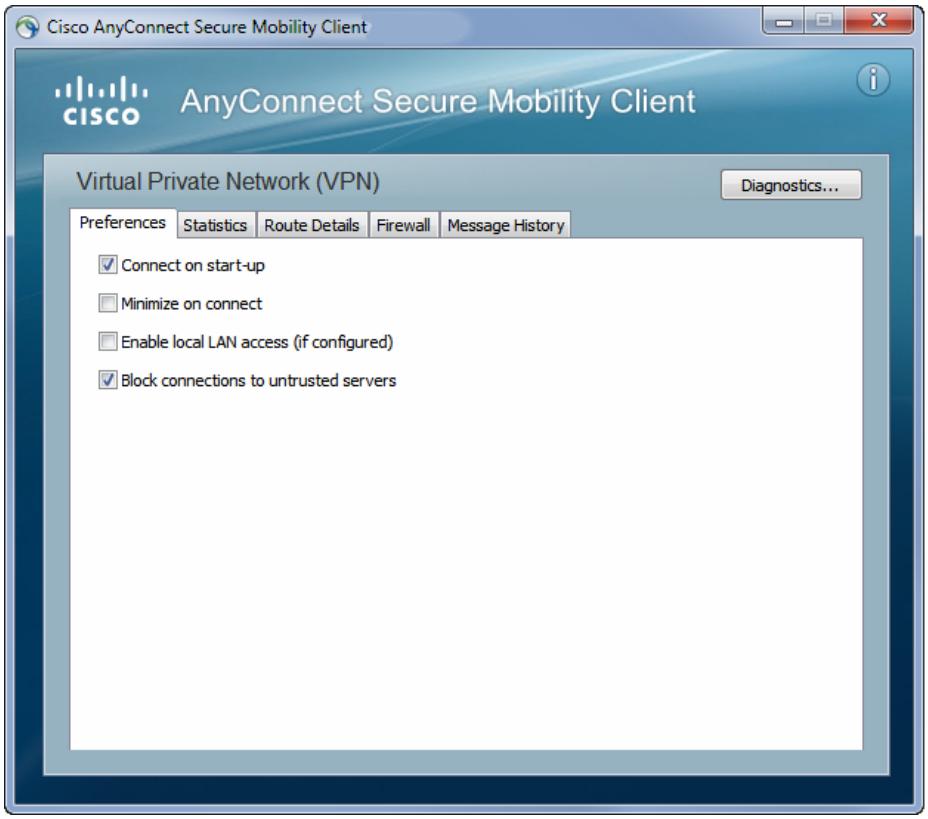
When the user tries to connect to a secure gateway, and there is a certificate error (due to expired, invalid date, wrong key usage, or CN mismatch), the user sees a red-colored dialog with Change Settings and Keep Me Safe buttons.

Note The dialogs for Linux may look different from the ones shown in this document.

Figure 3 Certificate Blocked Error Dialog

- Clicking **Keep Me Safe** cancels the connection.
- Clicking **Change Settings** opens AnyConnect's Advanced > VPN >Preferences dialog, where the user can enable connections to untrusted servers. The current connection attempt is canceled.

Figure 4 AnyConnect Advanced > VPN > Preferences



If the user un-checks **Block connections to untrusted servers**, and (as of 3.1.01065) the only issue with the certificate is that the CA is untrusted, then the next time the user attempts to connect to this secure gateway, the user will not see the Certificate Blocked Error Dialog dialog; they only see the following dialog:

Figure 5 AnyConnect Untrusted Certificate Security Warning

If the user checks **Always trust this VPN server and import the certificate**, then future connections to this secure gateway will not prompt the user to continue.

Note If the user checks **Block connections to untrusted servers** in **AnyConnect Advanced > VPN > Preferences**, or if the user's configuration meets one of the conditions in the list of the modes described under the guidelines and limitations section, then AnyConnect rejects invalid server certificates.

Improved Security Behavior

When the client accepts an invalid server certificate, that certificate is saved in the client's certificate store. Previously, only the thumbprint of the certificate was saved. Note that invalid certificates are saved only when the user has elected to always trust and import invalid server certificates.

There is no administrative override to make the end user less secure automatically. To completely remove the preceding security decisions from your end users, enable **Strict Certificate Trust** in the user's local policy file. When Strict Certificate Trust is enabled, the user sees an error message, and the connection fails; there is no user prompt.

For information about enabling Strict Certificate Trust in the local policy file, see the "AnyConnect Local Policy Parameters and Values" section in Chapter 9 of the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1*.

Guidelines and Limitations

Invalid server certificates are rejected when:

- Always On is enabled in the VPN client profile and is not turned off by an applied group policy or DAP.
- The client has a Local Policy with Strict Certificate Trust enabled.
- AnyConnect is configured to start before logon.
- A client certificate from the machine certificate store is used for authentication.

Mac OS X Support

AnyConnect now supports Mac OS X v10.9 (x86 32-bit and x64 64-bit).

Additional Translation Tables for AnyConnect Localization

The following language translation tables are now available on www.cisco.com:

- Japanese
- French Canadian
- German
- Chinese
- Korean
- Spanish (Latin American)
- Czech
- Polish

See Importing Available Translation Tables for the procedure to make these translations available for AnyConnect localization.

Note AnyConnect 3.1 obtains the client platform's language/locale setting from the specification made in the **Control Panel > Region and Language** dialog box's **Administrative** tab, detailed in Specifying the AnyConnect Client Platform's System Locale. This has changed from previous AnyConnect releases, be sure to set the language/locale as described.

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 6 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 (32-bit) and x64 (64-bit) Windows 7 or later 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
Posture & Host Scan	Core	Yes	Yes
	IPv6	No	Yes
	Keystroke Logger	Yes x86 (32-bit) only	Yes x86 (32-bit) only
Telemetry		Yes	Yes

Table 6 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 (32-bit) and x64 (64-bit) Windows 7 or later x86 (32-bit) and x64 (64-bit)
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.
- 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 7 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 Support Notes

- The AnyConnect 3.1 GUI is not supported on Linux.

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.

- iptables 1.2.7a or later.
- tun module supplied with kernel 2.4.21 or 2.6.

Mac OS X

Table 8 Mac OS X Support the modules and new features in AnyConnect 3.1

AnyConnect Module 3.1	Feature	Mac OS X 10.6, 10.7, 10.8, & 10.9 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 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 10.7 to 10.8) install as expected. Only the pre-deploy installation requires additional configuration as a result of Gatekeeper.

Host Scan Engine Update, 3.1.04075

Caution See Important AnyConnect, Host Scan, and CSD Interoperability Information, page 5, 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_3.1.04075-k9.pkg**, is available for use with AnyConnect 3.1.04072 and higher.

Note Host Scan release 3.1.02016 introduced support for and the ability to check for Windows 8.

The List of Antivirus, Antispyware, and Firewall Applications Supported by Host Scan 3.1.04063 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 5 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 acknowledgements, see Open Source Used In AnyConnect Secure Mobility Client 3.0.

For the latest end-user license agreement, see Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 3.0.

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.

Guidelines and Limitations

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

- OS X 10.9 Safari Can Disable Weblaunch, page 37
- Active X Upgrade Can Disable Weblaunch, page 37
- Internet Explorer, Java 7, and AnyConnect 3.1.1 Interoperability, page 37
- Implicit DHCP filter applied when Tunnel All Networks Configured, page 37
- AnyConnect VPN over Tethered Devices, page 37
- AnyConnect Smart Card Support, page 38
- AnyConnect Virtual Testing Environment, page 38
- UTF-8 Character Support for AnyConnect Passwords, page 38
- Disabling Auto Update May Prevent Connectivity Due to a Version Conflict, page 38
- Interoperability between Network Access Manager and other Connection Managers, page 39
- Network Interface Card Drivers Incompatible with Network Access Manager, page 39
- Network Access Manager Installation and Upgrade Hangs on Windows XP SP2 Systems Running the Cisco NAC Agent, page 39
- Avoiding SHA 2 Certificate Validation Failure (CSCtn59317), page 39
- Configuring Antivirus Applications for Host Scan, page 41
- Windows Mobile Not Supported, page 41
- iPhone Not Supported, page 41
- Microsoft Internet Explorer Proxy Not Supported by IKEv2, page 41
- MTU Adjustment on Group Policy May Be Required for IKEv2, page 41
- MTU Automatically Adjusted When Using DTLS, page 42
- Network Access Manager and Group Policy, page 42
- Full Authentication Required if Roaming between Access Points, page 42
- User Guideline for Cisco Cloud Web Security Behavior with IPv6 Web Traffic, page 42
- Preventing Other Devices in a LAN from Displaying Hostnames, page 43
- Revocation Message, page 43
- Messages in the Localization File Can Span More than One Line, page 43
- AnyConnect for Mac OS X Performance when Behind Certain Routers, page 44
- Preventing Windows Users from Circumventing Always-on, page 44
- Avoid Wireless-Hosted-Network, page 44
- AnyConnect Requires That the ASA Be Configured to Accept TLSv1 Traffic, page 44
- CRL Checking Enabled, page 44
- Trend Micro Conflicts with Install, page 45
- What Host Scan Reports, page 45
- Long Reconnects (CSCtx35606), page 45
- Users with Limited Privileges Cannot Upgrade ActiveX, page 45

- No Pro-Active Key Caching (PKC) or CCKM Support, page 46

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.

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.

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 VPN client connects. To prevent data leakage on this route, AnyConnect also applies an implicit filter on the LAN adaptor 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 XP, Vista, 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.

Network Access Manager Installation and Upgrade Hangs on Windows XP SP2 Systems Running the Cisco NAC Agent

Cisco AnyConnect 3.0 Network Access Manager installation never completes on certain Windows XP SP2 systems due to a deadlock in Microsoft NDIS framework. To work around this issue, install Windows XP Service pack 3 on the endpoint or exit the NAC agent at the point of the Network Access Manager installation.

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 XP—Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)
- For Windows 7 or later and Vista—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

Windows Mobile Not Supported

AnyConnect 3.0+ does not support Microsoft Windows Mobile or Windows Phone. However, you can continue to use the ASA to deploy the AnyConnect 2.5 or earlier client for Windows Mobile even after loading the AnyConnect 3.1 package files to the ASA for web deployment.

See the AnyConnect Secure Mobility Client Administrator Guides from AnyConnect 2.5, and earlier, for information about configuring the ASA to deploy AnyConnect for Windows Mobile devices.

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 2.4, Apple iOS 4.2.

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

Full Authentication Required if Roaming between Access Points

A mobile endpoint running Windows 7 or later or Vista 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 wildcard 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 cscotun0 mtu 1200` (For Mac OS X v10.5 or earlier)

`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 XP users: C:\Document and Settings\All Users
- For Windows Vista and 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

CRL Checking Enabled

On release 3.0.3050, certificate revocation list (CRL) checking for authentication on Windows is enabled and cannot be set to disabled. However, in release 3.0.4235, it is disabled and cannot be enabled. These settings are independent of the Internet Explorer setting.

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 Vista or later platforms 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 XP, Vista, and 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 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.

Open Caveats in AnyConnect 3.1.04072

Component	Identifier	Headline
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
api	CSCtr18142	GUI Hangs If Launched When Core Service is Still Restarting
api	CSCtz63857	GUI crashes upon exit during CSD prelogin check
api	CSCtz63879	CSD not enforcing IPProtocolSupport preference, VPN connection fails
api	CSCtz67862	"Connection has failed" message shown, but connection is successful
api	CSCtz67951	Connect to ASA URL with incorrect group: fails, but no error shown
api	CSCtz68048	AlwaysOn connection fails, error not shown to user
api	CSCtz68097	API tries to auto-connect to obsolete default host, fails with DNS error
api	CSCtz68114	GUI hangs for 10+ seconds after canceling authentication
api	CSCtz68138	GUI appears to hang for about 10 seconds during authentication
api	CSCtz86519	User interrupted with "reconnecting..." notice for low-level reconnect
api	CSCue14279	VPN API does not display HostScan UI messages
api	CSCuf02473	CSD library signature verification fails with AnyConnect 3.1 on OSX
api	CSCud93231	AC3.1 connecting via RDP does not work when connecting using IKEV2
certificate	CSCtx62491	Revocation shouldn't cause code signing errors
certificate	CSCug46734	Anyconnect Cert Validation Fails if DSA cert present on userstore
cli	CSCua04558	Linux w/Client Cert Auth using CLI - Certificate Validation Failure
core	CSCtz59516	VPN connection has dropped and said login failed after hostscan
core	CSCtz86849	AC not detect Captive Portal
core	CSCtz67049	AlwaysOn: Connection abort due to multiple connection attempts
core	CSCud96246	AC: IKEv2 to IOS and IOS-XE fails with "EVP_VerifyFinal errored" message
core	CSCue48916	Java App(s) Break when using AnyConnect 3.1.00495 or 3.1.02026 & Java v7
dart	CSCty85565	DART Running But Unable to Create a DART Bundle

Component	Identifier	Headline
dart	CSCtz96841	DART: Clear logs option not working
dart	CSCua53113	DART on Red Hat 6 - messages file (syslog) is not collected unless root
dart	CSCuf27250	DART: NAM DART does not collect correct information on x64 systems
download_install	CSCuc53433	Support change for Proxy Auto-Config using local PAC file
ipsecvpn-ike	CSCuf76836	AC: IKEv2 stops decrypting on specific ASA failover condn.
nam	CSCud18077	Memory corrupted when using Shin Kong Bank smart card
nam	CSCug84680	NAM: Password change with SSO and pre-logon does not work
nam	CSCuh00656	NAM: may not send profile matched cert for authentication if EKU exists
nam	CSCuh23463	Anyconnect should never cache machine credentials
nam	CSCua68473	NAM does not work peroperly with Athena on a Win 7 64
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch
posture-asa	CSCtf40994	CSD 3.5 Cache Cleaner termination, long delay in closing browser
posture-asa	CSCua13149	Insecure crypto / Dead-code removal
posture-asa	CSCue56046	HostScan fails to evaluate user/client certificates on Ubuntu 12
posture-asa	CSCui98272	HostScan Java WebLaunch fails due to broken IPC on WIndows 8.1 Preview
posture-asa	CSCti24021	Posture localization PO file needs updated translation
posture-asa	CSCtz73641	UDP ports not detected on Linux and OSX
posture-asa	CSCub32322	cstub should validate server certificates for a ssl connection
profile-editor	CSCug69331	NAM Standalone Profile Editor, allows invalid value
telemetry	CSCtu21924	Telemetry Report was not generated.
telemetry	CSCtu21971	Telemetry Report was generated but send report failed.
telemetry	CSCty29986	Errors post AC installs, service crashes
telemetry	CSCty52956	Telemetry module causing high CPU usage and Page Faults
telemetry	CSCua63117	vpnagent fails to be stopped when Telemetry is installed
vpn	CSCtx21803	Message to user is not clear when Client Cert is expired or revoked
vpn	CSCua24005	Agent not responding to Disconnect button
vpn	CSCua92065	CSSM_SignData - client unable to access private key of a certificate

Component	Identifier	Headline
vpn	CSCuc89210	Can't connect w/Client Cert Auth using Athena smartcard and Athena CSP
vpn	CSCud79055	Anyconnect web deployment unsuccessful & error while connecting to vpn .
vpn	CSCue60100	VPN need to recognize conn. in progress & not exclude current user cert.
vpn	CSCue74449	Browser Proxy Code needs to execute on separate thread
vpn	CSCuf07885	DNS traffic via tunnel is restricted with tunnel-all config (Windows)
vpn	CSCug77980	anyconnect mac crashes after initial launch
vpn	CSCua79567	Unable to pass HTTP traffic after establishing tunnel via IPSec
vpn	CSCug90871	DefaultHostName information lost after SBL connection used
vpn	CSCug04501	VPN Agent need to have crash dumps logged on Linux (Ubuntu & Redhat)
vpn	CSCui69769	Anyconnect Connection Fails When A Not Required Smartcard Is Inserted
vpn	CSCuc28953	After auth '...agent has encountered an error' if Smartcard plugged in
vpn	CSCuf21943	Anyconnect 3.0 WIN7 BSOD in acsock shortly after connecting
vpn	CSCug78530	AC 3.1 stuck in Connecting state after TND, when moving from corp to 3G
web	CSCty54514	VPN Status Message from "Connection Failed" to Captive portal message
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCue07219	ASA IKEv2 rekey to AC with duplicate IPSec proposals brings down tunnel
vpn	CSCuj58009	On Windows 8 and 8.1 with IPV6 with split tunneling enabled, split-include networks are not properly applied.
vpn	CSCuj78043	VPN Agent displays at link speed in the UI that is off by a factor of 100.

Caveats Resolved by AnyConnect 3.1.04072

Component	Identifier	Headline
cli	CSCuc02000	CLI: The 'vpncli.exe --stdin' option does not work in 3.1
core	CSCuj22784	Linux: Anyconnect command does not work after client connects
gui	CSCuj29213	Anyconnect 3.1 MR4 connection hangs with DFS file share mapped
posture-asa	CSCuj53551	Hostscan does not detect detect Kaspersky 14.x, Anyconnect fails
vpn	CSCuj12931	Anyconnect 3.1.04066 - Download breaks through webvpn on Mac OS
vpn	CSCuj17706	Client will not connect - server cert does not comply with FIPS
vpn	CSCuh73010	On OSX 10.9 AnyConnect is occasionally disconnecting and reconnecting in some configurations. Fixed in version 3.1.04074.

Open Caveats in AnyConnect 3.1.04066

Component	Identifier	Headline
api	CSCth28802	Move logic for enabling 'Disconnect' button from GUI to API
api	CSCtr18142	GUI hangs if launched when core service is still restarting
api	CSCtz08641	Pass IP address from AC to hostscan
api	CSCtz63857	GUI crashes upon exit during CSD prelogin check
api	CSCtz63879	CSD not enforcing IPProtocolSupport preference, VPN connection fails
api	CSCtz67862	"Connection has failed" message shown, but connection is successful
api	CSCtz67951	Connect to ASA URL with incorrect group: fails, but no error shown
api	CSCtz68048	AlwaysOn connection fails, error not shown to user
api	CSCtz68097	API tries to auto-connect to obsolete default host, fails with DNS error
api	CSCtz68114	GUI hangs for 10+ seconds after canceling authentication
api	CSCtz68138	GUI appears to hang for about 10 seconds during authentication
api	CSCtz86519	User interrupted with "reconnecting..." notice for low-level reconnect
api	CSCud93231	AC 3.1 connecting via RDP does not work when connecting using IKEv2
api	CSCue14279	VPN API does not display Host Scan UI messages

api	CSCue60112	Posture assessment failed: error locating the Host Scan CSD cache directory
api	CSCuf02473	CSD library signature verification fails with AnyConnect 3.1 on OS X
certificate	CSCtx62491	Revocation should not cause code signing errors
certificate	CSCtz78738	NSS Cert Store: NSS_InitReadWrite fails on Ubuntu 12
certificate	CSCug46734	AnyConnect certficate validation fails if DSA cert present on userstore
cli	CSCua04558	Linux w/client cert auth using CLI - Certificate Validation Failure
cli	CSCuc02000	The 'vpncli.exe --stdin' option does not work in 3.1
core	CSCtz59516	VPN connection has dropped and said login failed after hostscan
core	CSCtz65283	AnyConnect went to infinite loop reconnecting
core	CSCtz67049	AlwaysOn: Connection abort due to multiple connection attempts
core	CSCtz86849	AC cannot detect Captive Portal
core	CSCud96246	IKEv2 to IOS and IOS-XE fails with “EVP_VerifyFinal errored” message
core	CSCue48916	Java app(s) break when using AnyConnect 3.1.00495 or 3.1.02026 and Java v7
core	CSCuf76836	IKEv2 stops decrypting on specific ASA failover condition
dart	CSCty85565	DART running but unable to create a DART bundle
dart	CSCtz96841	Clear logs option not working
dart	CSCua53113	DART on Red Hat 6 - messages file (syslog) is not collected unless root
dart	CSCud03272	Mac system log is missing from DART bundle
dart	CSCuf27250	NAM DART does not collect correct information on x64 systems
download_install	CSCtu07619	.anyconnect file not deleted after uninstall on OS X
download_install	CSCtw59598	Client fails to connect after 3.0.5 to 3.1 upgrade on Rhel6
download_install	CSCtz67898	OS X: Quick timeout of identity certificate popup during Weblaunch
download_install	CSCtz83562	Client prompts for Username/Password after upgrade - should just connect
download_install	CSCuc53433	Support change for proxy auto-config using local PAC file
gui	CSCtx77206	GUI inconsistencies when the VPN component is not (yet) loaded
gui	CSCtz94017	Linux: Password complexity requirement message is truncated
gui	CSCua63561	The "defer update" dialog window does not get focused
gui	CSCua94150	Mac OS GUI: VPN prefs do not load initially with connect on start
gui	CSCua94462	AnyConnect 3.1- Translation strings not translated in PO files

network access manager	CSCuh23463	AnyConnect should never cache machine credentials
network access manager	CSCua68473	NAM does not work properly with Athena on a Win 7 64
network access manager	CSCud18077	Memory corrupted when using Shin Kong Bank smart card
network access manager	CSCug84680	Password change with SSO and pre-login does not work
network access manager	CSCuh00656	May not send profile matched certificate for authentication if EKU exists
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch
posture-asa	CSCtf40994	CSD 3.5 Cache Cleaner termination, long delay in closing browser
posture-asa	CSCtz73641	UDP ports not detected on Linux and OS X
posture-asa	CSCua13149	Insecure crypto / Dead-code removal
posture-asa	CSCua68938	HostScan fails to pick the AV defined as a DAP rule
posture-asa	CSCub32322	cstub should validate server certificates for a ssl connection
posture-asa	CSCue56046	HostScan fails to evaluate user/client certificates on Ubuntu 12
profile editor	CSCug69331	Standalone profile editor allows invalid value
scansafe	CSCtz70539	Websec https filter blocked vpn connection with vpn host in exception
telemetry	CSCtu21924	Telemetry Report was not generated
telemetry	CSCtu21971	Telemetry Report was generated but send report failed
telemetry	CSCty29986	Errors post AC installs, service crashes
telemetry	CSCty52956	Telemetry module causing high CPU usage and Page Faults
telemetry	CSCua63117	vpnagent fails to be stopped when Telemetry is installed
vpn	CSCtx17488	Create IPSec error message tailored to different failure reasons
vpn	CSCtx21803	Message to user is not clear when Client Cert is expired or revoked
vpn	CSCtx42595	Cannot connect SSL with ECDSA Cert when ASA using ECDSA SSL trustpoint
vpn	CSCtx57832	IPv6: Verify input containing brackets in the VPN combobox
vpn	CSCtx74050	IPsec: Private proxy server gets truncated & wrong port - SSL OK
vpn	CSCtx89687	IPv4 address pool exhaustion should cause connection failure
vpn	CSCty16858	Unable to establish an IKEv2 connection when lots of FW rules are pushed
vpn	CSCty33473	OpenSSL Thread crashed on Mac OSX with ECDSA Client Certificate
vpn	CSCty49411	Client getting stuck when trying backup servers
vpn	CSCty67693	VPN Agent IPC problem during connection establishment
vpn	CSCty71027	First auto-connect with AO/TND always fails

vpn	CSCty71126	API: Post-login banner & auth screen appear together, UI then hangs
vpn	CSCty85443	IPsec: Prompt to accept certificate on WebLaunch/upgrade on Mac OS X
vpn	CSCtz00859	When using TND + Client Cert Auth, Mac behaves differently after resume
vpn	CSCtz15198	vpnapi caused GUI crash after ASA reload
vpn	CSCtz18284	Check if IPv6 addresses are assigned in addition to registry check
vpn	CSCtz44356	Reconnects are occurring instead at IPsec rekey interval -affects Telnet
vpn	CSCtz44707	Reconnect issues on OS X when going through a NAT64
vpn	CSCtz59747	Unable to establish a connection when OS X 10.7 has ISATAP setup
vpn	CSCtz63337	VPN connected even when user selected not to accept certificates
vpn	CSCtz63344	VPN gave a pop-up "Error occurred in hostscan. Please connect again."
vpn	CSCtz64897	AC error while trying to connect to VPN in SBL mode
vpn	CSCtz65289	VPN does not show connected status in SBL mode
vpn	CSCtz70019	IPSec connection to ASA fails because 'VPN Server Could Not Parse Response'
vpn	CSCtz79125	Split-DNS not handling PTR DNS queries when DNS-Based Service Discovery
vpn	CSCtz84414	Two different server names get displayed in the vpn window
vpn	CSCtz89354	AnyConnect VPN causes the MS adapter to show false "No Network" status
vpn	CSCtz94029	Delay in detecting captive portal
vpn	CSCtz96871	OGS Feature- AC is not trying other servers in OGS list when using OSX
vpn	CSCua02552	On XP with OGS and Auto reconnect enable, stays in reconnect after sleep
vpn	CSCua24005	Agent not responding to Disconnect button
vpn	CSCua60935	GSS w/IPsec + Proxy: file integrity check error - new profile available
vpn	CSCua63334	VPN connection failed, followed immediately by successful connection
vpn	CSCua65784	Unable to connect to the alpha headends due to the CSSM_SignData
vpn	CSCua79567	Unable to pass HTTP traffic after establishing tunnel via IPSec
vpn	CSCua81750	Gray out connect button when there is no network connectivity
vpn	CSCua86943	No credential prompt when attempting to connect with IPsec after wake up

vpn	CSCua92065	cert validation failure with clean 3.1 build when using cec tunnel group
vpn	CSCub18654	'Certificate Validation Failure' with Goldkey ECDSA smartcard-eventually OK
vpn	CSCub34491	Mac is showing previous ASA in AC dialog and Message History
vpn	CSCub40846	Client very slow to react to logon/logoff notifications
vpn	CSCuc28953	After auth '...agent has encountered an error' if Smartcard plugged in
vpn	CSCuc89210	Cannot connect w/client auth using Athena smartcard and Athena CSP
vpn	CSCud79055	AnyConnect web deployment unsuccessful & error while connecting to vpn
vpn	CSCue60100	VPN needs to recognize connection in progress and not exclude current user cert
vpn	CSCue74449	Browser proxy code needs to execute on separate thread
vpn	CSCuf07885	DNS traffic via tunnel is restricted with tunnel-all config (Windows)
vpn	CSCuf21943	AnyConnect 3.0 WIN7 BSOD in acsock shortly after connecting
vpn	CSCug04501	VPN agent needs to have crash dumps logged on Linux
vpn	CSCug77980	AnyConnect Mac creashed after initial launch
vpn	CSCug78530	AC 3.1 stuck in *connecting* state after moving to 3G network
vpn	CSCug90871	DefaultHostName information lost after SBL connection used
vpn	CSCui69769	AnyConnect connection fails when a not required smartcard is inserted
web	CSCty54514	VPN status message from "Connection Failed" to captive portal message

Caveats Resolved by AnyConnect 3.1.04066

Component	Identifier	Headline
certificate	CSCug13458	Certificate Authority(s) not “trusted” in Mac “System Roots” keychain
core	CSCui17578	AC v3.1.04059: Weblaunch Java component unsigned
nam	CSCui09155	NAM authen failed if multi intermediate certification authorities certs
nam	CSCui86188	acnamagent crash caused by PMKID list corruption
posture-asa	CSCui20393	HostScan does not detect product ID for McAfee EPM 2.0
posture-asa	CSCui57801	AC v3.1.04059: Weblaunch Java component unsigned
posture-asa	CSCui78430	HostScan Weblaunch fails on Mac OS X 10.9 Mavericks: libcurl failure

vpn	CSCuh96638	AnyConnect VPN fail to modify IE proxy during disconnect
vpn	CSCui22687	Captive portal on non-default port may not work due to DNS failure
vpn	CSCui31137	AnyConnect Russian “GOST” certificate algorithm cause cert auth failure

Caveats Resolved by AnyConnect 3.1.04063

Component	Identifier	Headline
anyconnect	CSCug59404	RSA Software Token Integration fails in 3.1.03103 - worked in 3.0.4235
anyconnect	CSCue30862	AC 3.1.02026 fails connecting w/certstores errors and term. code 12
anyconnect	CSCue74292	VPN: ActiveX control should not be re-versioned at each release
hostscan	CSCui04556	[HostScan]: OPSWAT Upgrade to v3.6.7198.2
posture-asa	CSCtf70014	Hostscan reports incorrect time since last AV update
posture-asa	CSCuh25647	Hostscan does not return lastupdate for AVG AntiVirus Free 2013

Caveats Resolved by AnyConnect 3.1.04059

Component	Identifier	Headline
certificate	CSCtz23746	AC VPN: PKS12 import should not include Root certs
certificate	CSCtz89042	AnyConnect ‘Certificate Validation Failure’ on Mac/Linux and Firefox 12+
core	CSCua31665	Status command does not work on Ubuntu
core	CSCue25805	AC: Win XP default gateway changes after connection is established
core	CSCue97630	Windows 8 crash due to AnyConnect VA
core	CSCuf51767	AC v3.1.02043: Weblaunch code signing cert expired 2/7/13
download_install	CSCug35505	Java web deployment for AC raises a mixed mode code warning dialog
gui	CSCtz89480	AnyConnect icon does not show up on the task bar on ubuntu 11.10 & 12.04
network access manager	CSCtq60224	Crash in acnamagent.exe:c0000005 in acnamauth.dll - dot11iPmkRemoveEntry

network access manager	CSCua41458	AC password change: two conversations, 1st is dropped
network access manager	CSCub74790	Client incorrectly ignores credential response
network access manager	CSCud93686	Change password fails with AC on Windows 8 and 7
network access manager	CSCue27166	Need to reauth if username is changed in Retry Password dialog
network access manager	CSCue41101	Installing NAM on Windows 8 modifies login screen for local user
network access manager	CSCue53261	NAM does not work with Belgium e-ID smart cards
network access manager	CSCue62658	NAM causing system crash on Windows 8 Surface Pro
network access manager	CSCue98855	UserConfiguration file deleted after creating TTLS-token network
network access manager	CSCuf01515	NAM delayed reconnection to wireless network if PC sleeps with HVN allow
network access manager	CSCug82577	NAM unable to make wireless connection on Surface Pro
network access manager	CSCug92418	NAM crashing at Assertion ‘IM_isTicking’
network access manager	CSCuh45068	NAM throws an exception if unable to read from Certificate store
posture-asa	CSCuc42358	HostScan fails to install on 32bit Ubuntu with native libcurl
posture-asa	CSCud14153	Cisco HostScan elevation of privileges vulnerability
posture-asa	CSCue41045	HostScan does not correctly detect state of Agnitum Firewall 7.0.4
posture-asa	CSCue44500	Hostscan - warnings and errors are not sent to event viewer through AC
posture-asa	CSCue57439	CSD/HostScan does not detect hotfix KB2761226
posture-asa	CSCue70557	CSD/HostScan detects hotfix even though this hotfix was uninstalled
posture-asa	CSCue89850	HostScan activescan returns internalerror for Norton 360 20.x
posture-asa	CSCue97528	CSD/Hostscan does not detect check point endpoint security firewall 8.1
posture-asa	CSCuf03057	HostScan reports “elevationrequired” with Panda Endpoint Protection
posture-asa	CSCuf61143	avast! Pro Antivirus 8.0.1482 support in HostScan
posture-asa	CSCuf66425	HostScan: McAfee total protection 6.0 lastupdate detection error
posture-asa	CSCuf86352	AnyConnect error messages are written to the Win application log

posture-asa	CSCuh22990	Java changes require JNLP applet deployment
profile-editor	CSCud98396	TND AnyConnect profile editor
profile-editor	CSCue93347	Web Security PE: not computing certificate hash with ASA as TND host
scansafe	CSCuf75503	Group lookup fail with 2 similar group name
scansafe	CSCug16996	Websec service fails to stop when xp machine is trying to hibernate
scansafe	CSCug62676	Websec client fails with split tunnel exclude on Windows 8
vpn	CSCua73690	ICH: 'Always Connect' (Import the Cert) fails with an error on Ubuntu 11
vpn	CSCuc23873	AnyConnect 3.0 WIN7 bugcode NDIS BSOD
vpn	CSCue20479	DTLS does not work with AnyConnect 3.1.0.01065 or later and IOS router
vpn	CSCue25743	AC 3.1 fails to connect with IPv6 disabled on VA
vpn	CSCue30862	AC 3.1.02026 fails connecting w/ certstores errors and term. code 12
vpn	CSCue58490	Linux changes made in /etc/hosts between connection start and end lost
vpn	CSCuf20560	Unable to connect on non-default port when no profile is pushed
vpn	CSCuf75228	Variable MTU size causes VPN connection to fail on Windows 8
vpn	CSCug40158	AnyConnect VPN drops routes matching split-exclude network
vpn	CSCug54392	Remove use of Smart Card GUID provider parameter
vpn	CSCug59901	AnyConnect fails to reconnect when moving from trusted network
vpn	CSCug65475	Corrupted proxy.keep file causes crash on disconnect or Agent startup
vpn	CSCug78720	VPN driver failed to load on Windows 8

Caveats Resolved by AnyConnect 3.1.03103

Component	Identifier	Headline
api	CSCub75468	SBL: AnyConnect GINA/PLAP always default to port 443
api	CSCuc48997	AnyConnect Unable to find SSL server certificate Thumbprint
api	CSCud05514	COM API not invoking CertWarningCB
api	CSCud93978	Incorrect error about CSD signature
api	CSCue94762	Posture Assess failed "unable to find SSL server certificate thumbprint"
certificate	CSCtz89042	AnyConnect 'Certificate Validation Failure' on Mac/Linux and Firefox 12+

certificate	CSCud16526	Tunnel establishment fails using Entrust security store login software
core	CSCua31665	Status command does not work on Ubuntu
core	CSCuc03448	AC 3.0.8 LLA blocks WS-Discovery protocol for HP printers when connected
core	CSCuc88563	AC client firewall rules cause return traffic to be dropped on Mac OS X
core	CSCue25805	AC: Win XP default gateway changes after connection is established
dart	CSCuc28631	Correct the summary to report what is included in DART properly
download_install	CSCuc62955	Mac OSX: Installation takes longer on 3.1.1 when compared to 3.1
download_install	CSCuc66065	VPN: OSX install fails during postscript execution
download_install	CSCuc78786	SBL/PLAP components of AnyConnect slow down boot times on Windows
download_install	CSCud17997	AnyConnect DART module installation on Mac OS X changes/opt permissions
download_install	CSCud24558	Mac: Fails to connect when update is available on ASA (cert issue)
download_install	CSCud28176	AnyConnect upgrade from 2.5 to 3.1 does not work with ASA 8.2
gui	CSCtz89480	AnyConnect icon does not show up on the task bar or ubuntu 11.10 & 12.04
gui	CSCuc04807	AC localization: long strings in .po file getting truncated
gui	CSCuc23976	The font size is different in the status bar menu
network access manager	CSCtz62974	Lost all my user networks in NAM after switching networks
network access manager	CSCtz63983	Allow admin to specify cert criteria to be used for cert selection
network access manager	CSCua36146	NAM client interoperability issue with Smart Card authentication
network access manager	CSCuc13862	Windows 8 Machine Auth not working
posture-asa	CSCts13230	Hostscan on Mac not returning definition date for Trend Micro Sec
posture-asa	CSCub08265	Posture - potential issue with locks
posture-asa	CSCub72898	CSD: “Critical failure. Prelogin failed.” with IE9 ActiveX
posture-asa	CSCuc23613	[msvcrt!strcmp+10] cscan.exe: c0000005 (INVALID_POINTER_REA
posture-asa	CSCuc42358	Hostscan fails to install on 32bit Ubuntu with native libcurl
posture-asa	CSCuc42875	Hostscan Weblaunch fails on upgrade when using ActiveX
posture-asa	CSCuc56437	Cache Cleaner removes Firefox profiles.ini file on Ubuntu

posture-asa	CSCud05367	HostScan: cscan process crashes when detecting KSL on WinXP
posture-asa	CSCud26605	CSD: Hostscan does not report Mac address of WiFi adapter to ASA
posture-asa	CSCud39326	Hostscan CSD prelogin error with TLSv1 on OSX and Linux systems
posture-asa	CSCud39455	Hostscan pre-login assessment fails when computer uses proxy server
posture-asa	CSCue89980	Non-admin users may not have access to Posture ActiveX control
profile-ed	CSCtz77888	NAM PE text cut-off on certain systems
scansafe	CSCue06421	Websec crashes during failover
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCtz86314	Mac: DNS queries incorrectly not sent via the tunnel with split-DNS
vpn	CSCua73690	ICH: ‘Always Connect’ (Import the Cert) fails with an error on Ubuntu 11
vpn	CSCub48431	Duplicate messages seen on GUI on DTLS tunnel
vpn	CSCuc11477	Weblaunch ignores proxy server setting from PAC file
vpn	CSCuc16678	AnyConnect 3.1: ‘Invalid host entry’ with group-url and non-443 port
vpn	CSCuc24389	Infinite reconnect loop after connecting to SG with IPv6 site-local addr
vpn	CSCuc26333	Windows: VPN connection fails via some tethered devices (regression)
vpn	CSCuc42019	Bogus error message when SBL is enabled about having to wait to restart
vpn	CSCud17825	Captive portal incorrectly detected on anyconnect 3.1 IKEv2
vpn	CSCud43082	Linux: client in infinite reconnect loop after ARP request from router
vpn	CSCud69846	AC changes profile hostname after reconnecting to a LB environment
vpn	CSCud73928	Failed to establish tunnel on Japanese XP with IPv6 enabled
vpn	CSCue43390	vpnagentd wants to connect to 202.x.x.x - false positive alarming msg
vpn	CSCue58490	Linux changes made in /etc/hosts between connection start and end lost

Caveats Resolved by AnyConnect 3.1.02043

Component	Identifier	Headline
posture-asa	CSCue49663	Signature verification fails on linux with error-certificate has expired

Caveats Resolved by AnyConnect 3.1.02040

Component	Identifier	Headline
api	CSCud70576	AC VPN should increase overall processing timeouts to support Dialup
certificate	CSCud10648	Revert the EKU/KU requirement changes
certificate	CSCud16526	Tunnel establishment fails using Entrust security store login software
posture-asa	CSCud15337	Host scan takes a long time to report information with 360 AV installed
posture-asa	CSCud29674	Host scan takes a long time to report with Enigma AS installed
posture-asa	CSCud38850	Host scan 3.0.10055 does not correctly detect McAfee AntiVirus Enterprise 8.8.0.777 on Windows 7 64-bit machines.
posture-asa	CSCud64869	Opswat update to version 3.6.4900.2

Caveats Resolved by AnyConnect 3.1.02026

Component	Identifier	Headline
aaa-dap	CSCuc64108	ASA:DAP User Messages is truncated when action is terminate
core	CSCts96212	AnyConnect Stuck at Reconnecting
core	CSCty30281	Anyconnect may consume more than one session slot per connection
core	CSCuc03448	AC 3.0.8 LLA blocks WS-Discovery protocol for HP printers when connected
core	CSCuc55720	IE crashes with Java 7 when 3.1.1 package is enabled on the ASA
dart	CSCuc28631	Correct the summary to report what is included in DART properly
doc	CSCtx35606	IPv6: auto-detect proxy can cause long reconnects
doc	CSCua89081	DOC: specific Extended Key Usage rqrd in client certs for some 3.0 vers.
doc	CSCuc02207	Doc: AnyConnect Release Notes Need to indicate where to get API Support

Component	Identifier	Headline
doc	CSCuc61206	DOC: CCO Hostscan Support Chart Version Missing Tabs In Spreadsheet
download_install	CSCtk99993	weblaunch deploy UAC displays unknown publisher on Windows 7
download_install	CSCuc66065	VPN: OSX install fails during postscript execution
download_install	CSCud16838	Cannot disable Customer Experience Feedback on AnyConnect MacOS
download_install	CSCud41231	VPN: Unable to download OSX client with weblaunch link
gui	CSCub66643	Preferences grayed out on Mac in 3.0 UI - works in 3.1
gui	CSCuc04807	AC Localisation: long strings in .po file getting truncated
gui	CSCuc98378	FAST-GTC change pwd issue on AC3.1.0495
gui	CSCud24639	Anyconnect 3.1 on Mac : Banner formatted improperly
gui	CSCud31821	AC is using wrong vaule in 'old password' field for change pwd
nam	CSCtz62974	Lost all my user networks in NAM after switching networks.
nam	CSCua36146	NAM client interoperability issue with Smart Card authentication
nam	CSCub48707	NAM: Windows slow to logon after multiple logon logoff sequences
nam	CSCuc40084	NAM: WEP roaming not working
phone-home	CSCuc31942	Phone Home: Support connectivity through proxies and clean up logs
posture-asa	CSCto87181	HostScan does not detect "lastupdate" of Kaspersky AV 8.x on Mac OS X
posture-asa	CSCtz70911	Pre-login assessment w/ SBL and IKEv2 fails for certain registry checks
posture-asa	CSCua31894	HostScan does not detect Microsoft Forefront Endpoint Protection 2010
posture-asa	CSCua64423	HostScan reports Sophos AV Virus Def Last Update incorrectly on MacOSX
posture-asa	CSCub14760	HostScan reports a negative "lastupdate" value for Kaspersky 12.x
posture-asa	CSCub41486	HostScan must renew ASA token every 10 mins until reporting is complete
posture-asa	CSCuc26695	HostScan 3.0.08066 Not Detecting McAfee 8.7.0.570
posture-asa	CSCuc42875	HostScan Weblaunch fails on upgrade when using ActiveX
posture-asa	CSCuc48299	IE with Java 7 crashes on HostScan Weblaunch
posture-asa	CSCuc56437	Cache Cleaner removes Firefox profiles.ini file on Ubuntu
scansafe	CSCuc16357	Improve behavior when WebSec module is installed but no key is present
scansafe	CSCuc24360	AnyConnect 3.0.5075 - Frequent BSOD on WinXP with Siemens SmartCard

Component	Identifier	Headline
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCtz05075	Multiple DAP User Message popups with 003.001.00264
vpn	CSCtz86314	Mac: DNS queries incorrectly not sent via the tunnel with split-DNS
vpn	CSCub48431	duplicate messages seen on GUI on DTLS tunnel
vpn	CSCub81572	Anyconnect client gives login prompt for certificate authentication
vpn	CSCuc00047	VPN tunnel cannot be established via 802.11 WiFi (Windows 8)
vpn	CSCuc26333	Windows: VPN connection fails via some tethered devices (regression)
vpn	CSCud59407	AC displays French Characters from Group-Policy banner incorrectly

Caveats Resolved by AnyConnect 3.1.01065

Component	Identifier	Headline
api	CSCtz92140	AnyConnect 3.x may display incorrect gateway in established to field
api	CSCua50315	API: Better handling of Expired/Not Yet Valid Cert in AnyConnect 3.1
api	CSCub59164	Mac Auto Upgrade fails
api	CSCub75468	SBL: AnyConnect GINA/PLAP always default to port 443
certificate	CSCub02567	Update CRL cache ourselves instead of relying on the OS
cli	CSCua04464	CLI stats shows 'Not Available' for some fields (XP and Ubuntu)
doc	CSCty61472	DOC: AnyConnect supports specific Extended Key Usage attributes in certs
doc	CSCtz94179	Introducing Mac Gatekeeper
doc	CSCua96091	VPN: SuiteB ECDSA Certs on Linux can only be used from Cert file store
doc	CSCub02539	Support OS upgrade of 10.7 to 10.8 for AnyConnect 3.0.8 and 3.1
doc	CSCub85575	DOC: AnyConnect 3.1 localization behavior change need to be clarified
doc	CSCuc11211	AnyConnect WebSecurity STND documentation is incorrect
download_install	CSCua53348	Re-sizing the installer window on OSX makes the window out of order
download_install	CSCua76272	AnyConnect VPN Component Uninstall Forces Reboot w XP
download_install	CSCub46241	AnyConnect weblaunch fails from Internet Explorer with Java 7

Component	Identifier	Headline
gui	CSCua91851	Mac switches to discrete graphics in the presence of AnyConnect
gui	CSCub24816	AnyConnect GUI truncates authentication challenge grid values
gui	CSCub27157	AnyConnect NAM: Unable to pass arguments to scripts
gui	CSCub27170	Ability for admins to specify scripts while preventing users running it
network access manager	CSCtz21260	Network Access Manager: RDP fails on second connection attempt
posture-asa	CSCtx45701	HostScan is consuming large amounts of CPU time
posture-asa	CSCua04785	CSD Prelogin failed. Denied access.
posture-asa	CSCua97001	CSD: HostScan does not detect Free Avast AV software on MAC OS
posture-asa	CSCub08265	Posture - Potential issue with locks
posture-asa	CSCub10948	HostScan returns "elevationrequired" during DAP
posture-asa	CSCub19055	HostScan initialization error causes a failure on Windows 8 and Windows XP
posture-asa	CSCub19730	CSD/HostScan: doesn't lastupdate value for Kaspersky 11.x
posture-asa	CSCub41486	Renew ASA token every 10 minutes until DAP posting
profile-editor	CSCtz77888	NAM PE Text cut-off on certain systems
profile-editor	CSCub68510	NAM Profile Editor validate server identity should default to true
scansafe	CSCub21325	upgrade from 3.0.2 to 3.0.8 cause the windows xp screen flickering
scansafe	CSCub37547	AnyConnect Web Security Does Not Failover
scansafe	CSCuc16357	Improve behavior when WebSec module is installed but no key is present
vpn	CSCtg10248	UI may start too fast on Windows, throwing "Agent is unresponsive" alert
vpn	CSCth13596	AC30 SCEP - combine similar message dialogs into one
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtw37962	IKEv2 - take care of smart card removal and tunnel disconnect
vpn	CSCty89947	AnyConnect MacOSX connection move Reconnecting state and never come up
vpn	CSCtz29077	Smart Card being removed is not tearing down the SSL tunnel
vpn	CSCtz86314	Mac: DNS queries incorrectly not sent via the tunnel with split-DNS
vpn	CSCua12310	Fail to establish VPN tunnel with machine cert auth (SSL load balancing)
vpn	CSCua35433	AnyConnect:IP addr in profile causes Always-On/Connection to fail

Component	Identifier	Headline
vpn	CSCua49891	Untrusted Cert prompt - does NOT show reason for failure on Mac - Win OK
vpn	CSCua50507	Mac: Untrusted Cert prompt w/CN mismatch says untrusted source for SSL
vpn	CSCub23470	IKEv2 negotiation fails when there are duplicate IKE_AUTH exchanges
vpn	CSCub29128	6-in-4 IPv6 traffic is bypassed with "client bypass protocol" disabled
vpn	CSCub35182	Untrusted server certificate prompt with backup server list
vpn	CSCub40728	IPsec:Untrusted Cert prompt says 'from an untrusted source' when Expired
vpn	CSCub45559	Localization: DAP user messages display French characters incorrectly
vpn	CSCub45932	"No DNS connectivity" incorrectly reported, slow reconnect/disconnect
vpn	CSCub61514	Mac: VPN connection fails when IPv4 address pool has mask /32
vpn	CSCub82633	IKEv2 Encrypt payload is incorrect for AES-GCM
vpn	CSCub87656	VPN Code Signing tests fails due to VPN API MsgType change
vpn	CSCuc28953	After authentication, user may see, “The client agent has encountered an error.” if Smartcard is plugged in.

Resolved Caveats in AnyConnect 3.1.00495

Component	Identifier	Headline
api	CSCtg67075	Terminate Reason Displayed as Balloon with Non-cert Authentication
api	CSCtk83887	Removing Smart Cards at banner does not result in tunnel tear down
api	CSCts35238	VPN: GUI hangs after certificate enrollment
api	CSCtu30777	VPN: Unable to connect over satellite uplink with high latency >700ms
api	CSCtu72336	"Connection is in Progress" - User is Unable to Initiate Connection
api	CSCty02610	VPN API displays HostScan log messages instead of messages tagged UI
api	CSCty80134	AnyConnect COM API broken on Windows XP platform
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCts76302	AC: RHEL 5 base install fails to validate some web server certs
certificate	CSCtx96525	Certificate File Store support of Alt DNS records

Component	Identifier	Headline
certificate	CSCtz26985	IPsec does not perform certificate Name Checks
certificate	CSCtz29379	CSDL: certificate verification using IP when connection uses FQDN
certificate	CSCtz29470	WebLaunch of IPsec does not perform certificate Name Checks
certificate	CSCtz83719	SCEP enrollment fails if CA doesn't send complete cert chain
certificate	CSCua73809	valid server certificates are flagged as untrusted in LB environments
certificate	CSCua86644	IKEv2 does not prompt again for invalid server certificate acceptance
certificate	CSCub11994	valid certification error after successful connection
core	CSCta83106	Routing logic for reconnects needs to ignore invalid routes
core	CSCtw51902	AnyConnect auto-proxy - fails if proxy as FQDN in PAC file
core	CSCty26567	Open SSL error msg and AC is unable to contact the ASA
core	CSCty90659	AC BackupSever(specified by IP) NOT used w/o DNS response
core	CSCtz81595	AnyConnect on Mac 3.0.07059 and later don't work with Cisco IOS Routers
dart	CSCtu73943	anyconnect.txt and other files not being saved to summary.txt in DART
dart	CSCtz78396	Dart Fails on Linux OpenSuse
dart	CSCua31730	DART on Linux showing folders as zero bytes inside the Archive manager
doc	CSCtt22164	HostScan not copying libcsd.dll and libhostscan.dll to proper directory
doc	CSCtu99233	DOC: AnyConnect doc needs to mention Smart Card support per OS
doc	CSCty14734	DOC: Multiple spelling mistakes in AnyConnect Admin Guide 3.0
doc	CSCty52096	IPSec + SSL: must use same untrusted cert
doc	CSCtz04556	Doc that Internet Explorer 6 is not supported anymore for AnyConnect.
doc	CSCtz05169	Connecting for the first time on Linux with Firefox
doc	CSCtz29197	AnyConnect PROMPTS user to allow accepting untrusted certs by default
doc	CSCtz60692	Doc: AC Config Guide /opt/cisco/vpn should be /opt/cisco/anyconnect
doc	CSCtz91317	AnyConnect Installation Fails with a combination of Windows Preferences
doc	CSCua53570	Last scan time not supported for all AV, AS and FW.
download_install	CSCtr28687	IKEv2-IPSec: Downloader (SSL) isn't using configured public Proxy Server

Component	Identifier	Headline
download_install	CSCts46682	AnyConnect Linux init script issues
download_install	CSCtz41704	VPNLB: IKEv2 connections fails on profile update if SSL cert untrusted
download_install	CSCua11967	CSDL: Dnldr on Linux auto accepts invalid server certs if policies allow
download_install	CSCua60812	Add no display support for AnyConnect Downloader
download_install	CSCua76272	AnyConnect VPN Component Uninstall Forces Reboot w XP
gui	CSCtu21896	GUI Connection Information reports IPv4 mode when connected with IPv6
gui	CSCtu23942	Password complexity requirement message from ASA is truncated
network access manager	CSCtk62756	Some adapters don't update the scanlist without explicit scan request
network access manager	CSCtk75911	Driver does not restore connection state when unbound
network access manager	CSCtn71218	network access manager: Shows limited connectivity with an adapter using a Ralink chipset
network access manager	CSCto33655	Crash 32bit in acnamagent.exe: c0000005 in acnamauth.dll -- (macCopy)
network access manager	CSCtr97908	Machine authentication with 2008 AD cert template fails
network access manager	CSCts53001	AnyConnect fails EAP-TLS authentication when client certificate is 8k
network access manager	CSCtt17221	Any-connect drops conversation on machine auth peap-mschap failure
network access manager	CSCtw47024	Cert authentication does not work with Entrust Security Store
network access manager	CSCtw87576	network access manager reduces MTU size for wireless adapters
network access manager	CSCtx03814	Network access manager should not cache machine passwords
network access manager	CSCty10978	AnyConnect can not get the user credentials from windows login (SSO)
network access manager	CSCty42891	network access manager scanlist does not appear with wired(dot1x) in a use case
network access manager	CSCty48346	network access manager delayed to reconnect to wireless network after PC standby with HVN
network access manager	CSCty55069	Cannot disable wifi when wifi auth fails or timesout
network access manager	CSCty62737	network access manager may pick the wrong CA cert if 2 CA certs have the same public key
network access manager	CSCty94235	AC drops eap chaining conversation: user - mschap, machine - eap-tls

Component	Identifier	Headline
network access manager	CSCtz03204	AC doesn't perform TLS session resume in PEAP
network access manager	CSCtz13556	network access manager does not create packet captures
network access manager	CSCtz17464	AC doesn't perform pac-less EAP-FAST-MSCHAP session resume
network access manager	CSCtz38714	Unable to connect with DELL Latitude ST with builtin wifi card
network access manager	CSCtz59344	AnyConnect network access manager: Logon module registers for PRESHUTDOWN notification
network access manager	CSCtz73281	GUI should remember last username that was used during token auth
network access manager	CSCtz83979	WZC cannot connect to EAP-TLS networks when network access manager is installed
posture-asa	CSCtj59449	MAC needs to support cert verification
posture-asa	CSCtw16106	Improve performance with HS enabled
posture-asa	CSCty54487	CSD: Add Products screen is blank when configuring AdvEndPt from MAC OS
posture-asa	CSCty81366	Re-instate signing for Mac
posture-asa	CSCtz35744	Opswat upgrade to version 3_5_1058_2
posture-asa	CSCtz56733	XSS vulnerability within Cisco HostScan package
posture-asa	CSCua60981	csdm checkin for CSCty54487
posture-asa	CSCua61564	crash : vpn crash on quitting AnyConnect (appverifier)
posture-asa	CSCua97239	MSE 4.x Data File time is not available
posture-asa	CSCub02626	HostScan Engine 3.0.08062 support chart incorrectly list 'Eset Software'
posture-asa	CSCub09138	Support for MC OSX 10.8
profile-editor	CSCtx62540	PE: should not allow bogus characters in TND DNS Servers
profile-editor	CSCty01313	network access manager: PE does not save config if foreign characters are used in the name
scansafe	CSCtz41960	Hard-coded IV in Encrypt()
scansafe	CSCtz67672	AnyConnect can't render images
scansafe	CSCtz70514	websec svc can crash after enable https filter & went to https site
scansafe	CSCua13166	Missing check to find existing ScanSafe headers - AnyConnect
scansafe	CSCua52925	not able to browse to any website after websec service stop
scansafe	CSCub21325	upgrade from 3.0.2 to 3.0.8 cause the windows xp screen flickering
telemetry	CSCtz46052	Third-party Microsoft Detours library updated
vpn	CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux

Component	Identifier	Headline
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says "Configuring IPv6 system..."
vpn	CSCth85648	VPN: Auth challenge window - Mac and Win ignoring CR/LF
vpn	CSCti93817	Trusted Network not detected when adapter has IPv6 DNS addresses
vpn	CSCtl51029	IPv6 traffic tunneling success is inconsistent
vpn	CSCtn11401	AnyConnect failures with connection, yet it is passing data
vpn	CSCtr00334	Always-On: If ASA DNS name can't be resolved, can't select another entry
vpn	CSCtr80410	Password may be available in clear text in RAM
vpn	CSCts12090	AnyConnect fails when multiple IP addr are assigned to single NIC/adapter
vpn	CSCtt15348	Unable to disconnect the client - KPMG
vpn	CSCtt31972	VPN: AC unable enroll to local CA unless tunnel-group-list is enabled
vpn	CSCtw66908	Long delay in boot if prev conn was not disconnected before shutdown
vpn	CSCtx20857	AnyConnect 3.0.x Client Profile filename check is case sensitive
vpn	CSCtx28970	AC crashes with IE offline
vpn	CSCtx35616	launching tunnel connection everytime dhcp renews same IP
vpn	CSCtx95383	AnyConnect does not handle "88" authentication/login failure code
vpn	CSCty01670	vpnagentd process crashes with specific packet
vpn	CSCty43072	IPsec: Posture Assessment Failed -IKEv2 & SSL using different trustpoints
vpn	CSCty89947	AnyConnect MacOSX connection move Reconnecting state and never come up
vpn	CSCty90942	Standalone AnyConnect 3.0.4+ fails to connect on IOS 15.x & 12.4T
vpn	CSCtz12949	Mac: Cannot establish VPN tunnel via 4G card
vpn	CSCtz28852	IKEv2 connections doing DNS resolution for proxies when not required
vpn	CSCtz59756	AlwaysOn Fail Close does not allow user to login behind ATTWifi @ Hilton
vpn	CSCtz75559	Failed to establish VPN tunnel via Sierra 3G card (XP)
vpn	CSCtz94143	AnyConnect conflicts with Pow causing OS X to lock up after VPN connect
vpn	CSCtz94497	VPN Tunnel disrupted for too long when DTLS tunnel can't be established
vpn	CSCua02849	Use primary ASA in LB cluster for IPSec Always On profile check

Component	Identifier	Headline
vpn	CSCua05009	VPN tunnel terminated after loss of public interface
vpn	CSCua16483	VPN connection fails with Novatel 4G card (Win7)
vpn	CSCua35433	AnyConnect:IP addr in profile causes Always-On/Connection to fail
vpn	CSCub45932	"No DNS connectivity" incorrectly reported, tunnel reconnect delayed
win-vpn-client	CSCua28747	Legacy VPN client subject to local priv-escalation DLL load attack

HostScan Engine Caveats

Open Caveats in HostScan Engine 3.1.04060

Component	Identifier	Headline
csdm	CSCud30407	IPv6 : no option to configure ipv6 prelogin policy
csdm	CSCuh08360	ASDM does not show changes made to CSD pre-login policy
hostscan	CSCtb47343	CSDM: AEA lists 13 AVG vendors - only 2 are supported
hostscan	CSCuc86278	CSD: "Critical failure. Prelogin failed!." with IE9 ActiveX
hostscan	CSCuc86284	Posture - Potential issue with locks
java	CSCtt40292	Error in saving the modified settings in CSD
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch
posture-asa	CSCtf40994	CSD 3.5 Cache Cleaner termination, long delay in closing browser
posture-asa	CSCti24021	Posture localization PO file needs updated translation
posture-asa	CSCtk05829	Hostscan does not work when using Google Chrome on a MAC
posture-asa	CSCtr39580	JPN CSD: HostScan Registry MBCS Registry name is not working
posture-asa	CSCtr39606	JPN CSD: HostScan File MBCS File name is not working
posture-asa	CSCtr39613	JPN CSD: HostScan MBCS Folder name is not working
posture-asa	CSCtr39630	JPN CSD: HostScan Process MBCS name is not working
posture-asa	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
posture-asa	CSCts13230	Hostscan on Mac not returning definition date for Trend Micro Sec
posture-asa	CSCtz67975	CSD: Ability to prevent a user from opening data.xml in a browser
posture-asa	CSCtz73641	UDP ports not detected on Linux and OSX
posture-asa	CSCua68938	HostScan fails to pick the AV defined as a DAP rule
posture-asa	CSCub32322	cstub should validate server certificates for a ssl connection
posture-asa	CSCuc92128	Posture pre-deploy msi does not install the ActiveX control
posture-asa	CSCud47132	HS: Computer Associates etrust AV not detected
posture-asa	CSCud54452	ASDM: upgrading hostscan deletes endpoint config
posture-asa	CSCue56046	HostScan fails to evaluate user/client certificates on Ubuntu 12
posture-asa	CSCuf61634	CSD Active Scan returns Internal Error for AVG Free Edition 2013.x
posture-asa	CSCug89590	Hostscan 3.1.03104 does not detect Kaspersky AV 6.0
posture-asa	CSCuh24853	HostScan does not find TrendMicro Products eg: antivrus and antispyware
posture-asa	CSCuh25647	Hostscan does not return lastupdate for AVG AntiVirus Free 2013

Component	Identifier	Headline
posture-asa	CSCuh40088	Hostscan 3.1.03104 Interprets Sophos AntiVirus Last Update Time Wrong
securevault	CSCtr25566	ALL-LANG CSD: file was shared between Local and Secure Desktop

Caveats Resolved by HostScan Engine 3.1.04060

Component	Identifier	Headline
posture-asa	CSCsx54704	Linux OPSWAT Upgrade
posture-asa	CSCsx54706	Mac OS X OPSWAT Upgrade
posture-asa	CSCsx54707	Windows OPSWAT Upgrade
posture-asa	CSCua68733	posture should include/link against published openssl, not system
posture-asa	CSCuc42358	HostScan fails to install on 32bit Ubuntu with native libcurl
posture-asa	CSCuc58777	Posture build dependency Issue
posture-asa	CSCud14153	Cisco HostScan Elevation of Privileges Vulnerability
posture-asa	CSCue17362	Opswat Update to version 3.6.5595.2
posture-asa	CSCue44500	Hostscan - warnings and errors are not sent to event viewer through AC
posture-asa	CSCue57439	CSD/Hostscan does not detect hotfix KB2761226
posture-asa	CSCue70557	CSD/Hostscan detects hotfix even though this hotfix was uninstalled
posture-asa	CSCue70994	"todo" string occurance in libcsd.log and cscan.log
posture-asa	CSCue78541	Crash Dump utility hardcoded version value
posture-asa	CSCue79625	Opswat Upgrade to v3.6.5861.2 for HostScan
posture-asa	CSCue95040	Enable Thread Safely by default in HostScan
posture-asa	CSCuf29909	HostScan reports duplicate Hotfix entries in DAP
posture-asa	CSCug19306	HostScan tries to use OpenSSL as cURL library on linux
posture-asa	CSCug34827	Failed to load libcsd.dll on Windows XP
posture-asa	CSCug77447	CSDJavaInstaller has a Dependency on libcommon
posture-asa	CSCug79771	MSE not detected on endpoint
posture-asa	CSCug84987	OPSWAT Upgrade to version 3.6.6528.2
posture-asa	CSCuh22990	Mixed mode warning seen when running HostScan applet

Caveats Resolved by HostScan Engine Update 3.1.03104

Component	Identifier	Headline
posture-asa	CSCua76702	CSD: Hostscan - Add support for Data File Time attribute for ME AV V4
posture-asa	CSCue25414	ENH:HostScan should detect Microsoft System Endpoint Protection 2012
posture-asa	CSCue41045	Hostscan doesn't correctly detect state of Agnitum Firewall 7.0.4
posture-asa	CSCue89850	HostScan activescan returns internalerror for Norton 360 20.x
posture-asa	CSCue97528	CSD/Hostscan does not detect Check Point Endpoint Security Firewall 8.1
posture-asa	CSCuf03057	Hostscan reports "elevationrequired" with Panda Endpoint Protection
posture-asa	CSCuf07843	HostScan Support for Kaspersky Endpoint Security 10
posture-asa	CSCuf61143	avast! Pro Antivirus 8.0.1482 support in HostScan
posture-asa	CSCuf66425	Hostscan: McAfee Total Protection 6.0 lastupdate detection error
posture-asa	CSCug14179	Opswat upgrade to OESIS framework version 3.6.6259.2

Caveats Resolved by HostScan Engine Update 3.1.02040

Component	Identifier	Headline
posture-asa	CSCud15337	HostScan takes a long time to report information with 360 AV installed
posture-asa	CSCud29674	HostScan takes a long time to report with Enigma AS installed
posture-asa	CSCud38850	HostScan does not detect McAfee AV Ent. 8.8.x
posture-asa	CSCud27369	Hostscan takes a long time due to Opswat's bad request

Caveats Resolved by HostScan Engine Update 3.1.02016

Defect ID	Description
CSCto87181	HostScan does not detect "lastupdate" of Kaspersky AV 8.x on Mac OS X
CSCty89020	ciscod.exe shows excessive spikes and page faults in Task Manager
CSCua31894	HostScan does not detect Microsoft Forefront Endpoint Protection 2010
CSCua64423	HostScan reports Sophos AV Virus Def Last Update incorrectly on MacOSX
CSCub14760	HostScan reports a negative "lastupdate" value for Kaspersky 12.x
CSCuc40304	CSDM: Add support for Windows 8
CSCuc42875	HostScan Weblaunch fails on upgrade when using ActiveX

Defect ID	Description
CSCuc48299	IE with Java 7 crashes on HostScan Weblaunch
CSCuc71750	HostScan does detect state of Windows Defender on Windows 8
CSCuc71886	HostScan fails to detect state of Windows Firewall on Windows 8

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