Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.0

Last Updated: January 13, 2014

This document includes the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

These release notes are for the following releases:

- Cisco AnyConnect Secure Mobility Client 3.0.10057
- Cisco AnyConnect Secure Mobility Client 3.0.10055
- Cisco AnyConnect Secure Mobility Client 3.0.08066
- Cisco AnyConnect Secure Mobility Client 3.0.08057
- Cisco AnyConnect Secure Mobility Client 3.0.07059
- Cisco AnyConnect Secure Mobility Client 3.0.5080
- Cisco AnyConnect Secure Mobility Client 3.0.5075
- Cisco AnyConnect Secure Mobility Client 3.0.4235
- Cisco AnyConnect Secure Mobility Client 3.0.3054
- Cisco AnyConnect Secure Mobility Client 3.0.3050
- Cisco AnyConnect Secure Mobility Client 3.0.2052
- Cisco AnyConnect Secure Mobility Client 3.0.1047
- Cisco AnyConnect Secure Mobility Client 3.0.0629
- Host Scan Engine Update 3.0.11033

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 version of AnyConnect, you must be a registered user of Cisco.com. Table 1 shows the AnyConnect file package names for ASA deployment.

Table 1 AnyConnect Package Filenames for ASA Deployment

OS	AnyConnect 3.0 Web-Deploy Package Name Loaded onto ASA
Windows	anyconnect-win-<*version*>-k9.pkg
Mac OS X	anyconnect-macosx-i386-<*version*>-k9.pkg
Linux	anyconnect-linux-<*version*>-k9.pkg

Table 2 shows the filenames of the AnyConnect packages for pre-deployment.

Table 2 AnyConnect Package Filenames for Pre-deployment

OS	AnyConnect 3.0 Pre-Deploy Package Name
Windows	anyconnect-win-<*version*>-pre-deploy-k9.iso
Mac OS X	anyconnect-macosx-i386-<*version*>-k9.dmg
Linux	anyconnect-predeploy_linux-<*version*>-k9.tar.gz

There are other files that can be downloaded, which help you add additional features to AnyConnect.

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 on to Cisco.com.

Step 3 Click **Download Software**.

Step 4 Expand the **Latest Releases** folder and click **3.0.010057.**

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**.

What to do Next

See, Chapter 2, "Deploying the AnyConnect Secure Mobility Client" in *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* to install the packages onto an ASA or to deploy AnyConnect using your enterprise software management system.

Installation Overview

AnyConnect Release 3.1 integrates new modules into the AnyConnect client package. 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 3.1 shares the Host Scan component with Cisco Secure Desktop (CSD) version 3.6. The stand-alone Host Scan package for AnyConnect provides the same features as the Host Scan package that is part of CSD. The AnyConnect 3.1 client can co-exist with Cisco Secure DesktopVault, but it cannot be run or deployed from inside the Vault.

For more information about Host Scan and the other new modules in AnyConnect 3.0, see New Features in Release 3.0.08066, page 9.

For more information about deploying the AnyConnect modules, see the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0.*

Upgrading Older AnyConnect Clients and Optional Modules

When you upgrade from an earlier 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.
- If you are upgrading from AnyConnect 3.0.11042 to AnyConnect 3.1, be aware that you must upgrade to AnyConnect 3.1.02026 or higher if you are also upgrading the Network Access Manager module. If you upgrade to an earlier version of AnyConnect 3.1, Network Access Manager upgrade will fail.
- Upgrades any Host Scan files used by AnyConnect.
- ***Does not*** upgrade the Cisco IPsec VPN client (or remove it). However, the AnyConnect 3.0 client can coexist on the computer with the IPsec VPN client.
- ***Does not*** upgrade and cannot coexist with Cisco ScanSafe AnyWhere+. You must uninstall AnyWhere+ before installing the AnyConnect Secure Mobility Client.

Note If you are upgrading from the legacy Cisco VPN client, you should restore the MTU on your physical adapters back to the default (1500). (With IPv6, the interface MTU must be at least 1374.) Use the SetMTU utility that comes with the legacy Cisco VPN clients to restore the default value and reboot for the change to take effect. Some customers reduced their physical LAN and wireless adapter MTU settings to 1300 with legacy Cisco VPN clients, and this negatively impacts the tunneling performance of AnyConnect.

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.

Note Upgrading from AnyConnect 2.2 is not supported using the ASA or Weblaunch. You must uninstall AnyConnect 2.2 then install AnyConnect 3.1 either manually or using an SMS.

Java 7 Issues

Java 7 causes problems with Clienless SSL VPN (WebVPN). A description of the issues and workarounds is provide in the Troubleshooting Technote *Java 7 Issues with AnyConnect, CSD/Hostscan, and WebVPN - Troubleshooting Guide*, which in Cisco documentation under Security > Cisco Hostscan.

Important Security Considerations

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, **Enabling FIPS and Other Parameters with our Enable FIPS Tool** in Chapter 8, "Enabling FIPS and Additional Security in the Local Policy" of the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0.*

Changes to Server Certificate Verification

The following behavioral changes are being made to server certificate verification:

- SSL and IPSec connections from the AnyConnect client to the secure gateway being performed using the FQDN of the secure gateway will 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.
- SSL and IPSec connections from the AnyConnect client to the secure gateway require server certificates to contain Key Usage attributes of Digital Signature and Key Encipherment.
- SSL connections from the AnyConnect client to the secure gateway require server certificates to contain an Enhanced Key Usage attribute of Server Authentication.
- IPSec connections from the AnyConnect client to the secure gateway require server certificates to contain an Enhanced Key Usage attribute of Server Authentication or IKE Intermediate.

Note Note that server certificates not containing a Key Usage will be considered invalid for all Key Usages, and similarly server certificates not containing an Enhanced Key Usage will be considered invalid for all Enhanced Key Usages.

- In this release of AnyConnect, IPSec connections from the AnyConnect client to the secure gateway now perform name verification on server certificates. The following rules will be applied for the purposes of both IPSec and SSL name verification:
  - If a Subject Alternative Name extension is present with relevant attributes, name verification will be 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 will be 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 (far left) subdomain only, and additionally must be the last (far right) character in the subdomain. Any wildcard entry not in compliance will be ignored for the purposes of name verification.

Changes to Client Certificate Verification

AnyConnect releases 3.0.08057 through 3.0.10055 inadvertently required specific values in the EKU field of a client certificate in order for it to be used to establish a VPN connection. Consequently, client certificates issued from an ASA CA were not being used by AnyConnect to establish a VPN connection. This bug, CSCuc07598, was fixed in 3.0.10057.

In releases earlier than 3.0.08057 and in release 3.0 10057 and later, these client certificates can be used to successfully establish a VPN connection.

Important AnyConnect, CSD, and Host Scan Interoperability Information

AnyConnect 3.0.10057 and later is compatible with Host Scan 3.0.08057 or later versions and CSD 3.6.6020 or later versions.

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 your version of Host Scan or CSD fist, then upgrade your version of 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 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."

AnyConnect Support for Windows 8

AnyConnect 3.0.10055 and later versions (including the latest version of AnyConnect, version 3.1.01065), function on Windows 8 32-bit and Windows 8 64-bit operating systems, though there are some limitations.

Requirements

ASDM version 7.0.2 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 logon 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.

Troubleshooting Host Scan Support for Windows 8

Users on Windows 8 and Windows XP fail to connect to an ASA after an upgrade to CSD 3.6.6104 or Host Scan 3.0.08066.

Symptom:

Users on Windows 8 and Windows XP fail to connect to an ASA after an upgrade to CSD 3.6.6104 or Host Scan 3.0.08066. After users fail to connect they receive one of these messages:

"Posture assessment failed: Hostscan Initialize error.."

"HostScan Processing Failed"

Conditions:

Client running Windows 8 or Windows XP.

Workaround:

Upgrade the CSD or Host Scan image on the ASA to CSD 3.6.6210, Host Scan 3.0.10057, or Host Scan 3.1.01065.

New Features in Release 3.0.11046

AnyConnect 3.0.11046 is a maintenance release for Linux that resolves the defects described in New Features in Release 3.0.11046, page 9 and is compatible with Host Scan Engine Update 3.1.02040.

New Features in Release 3.0.11042

The following features are now supported on Windows 8:

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

New Features in Release 3.0.10057

AnyConnect 3.0.10057 is a maintenance release that resolves the list of caveats in AnyConnect 3.0.10055 Caveats, page 52. Cisco recommends that you upgrade to the latest release of AnyConnect.

New Features in Release 3.0.10055

AnyConnect 3.0.10055 is a maintenance release that resolves the list of caveats in Caveats Resolved by Release 3.0.10055, page 52 and incorporates Host Scan engine update 3.0.1055.

New Features in Release 3.0.08066

AnyConnect 3.0.08066 is a maintenance release that resolves the list of caveats in Caveats Resolved by Release 3.0.08057 and incorporates Host Scan Engine Update 3.0.8066.

New Features in Release 3.0.08057

AnyConnect 3.0.08057 makes security improvements and recommendations described in Important Security Considerations on page 5, specifies new compatibility requirements between AnyConnect, Host Scan, and CSD as described in Important AnyConnect, CSD, and Host Scan Interoperability Information on page page 6 and resolves the list of caveats in Table 8.

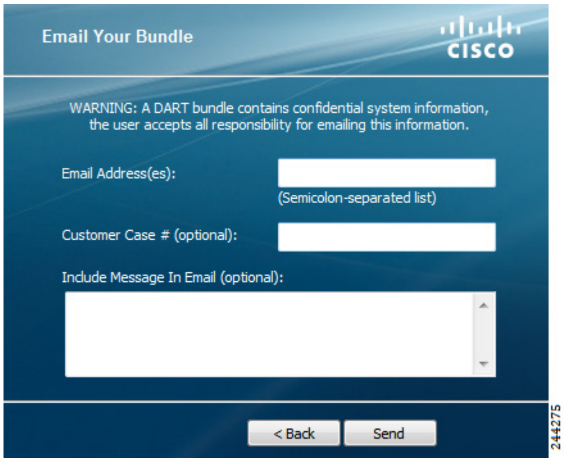
Support for Mac OS X v10.8

AnyConnect 3.0.08057 is the first AnyConnect release to support Mac OS X v10.8.

New Features in Release 3.0.07059

- The number of digits in the release version has increased to support an additional digit, which will be required for future maintenance releases. The extra digit was added to allow Cisco processes to accommodate the change.
- An Email Bundle button has been added to the last screen of the DART wizard, next to the Finish button. When the end-user clicks the Email Bundle button, the Email Your Bundle screen appears, as shown below:

Figure 1 DART Email Send Screen



Email Your Bundle

WARNING: A DART bundle contains confidential system information, the user accepts all responsibility for emailing this information.

Email Address(es):

(Semicolon-separated list)

Customer Case # (optional):

Include Message In Email (optional):

When you instruct your end user to create and email a DART package, tell them what information to add to this screen.

DART Email Requirements

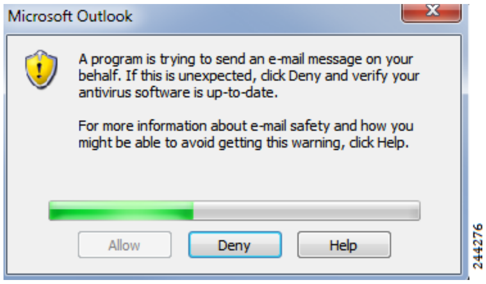
The end user’s system must have a default email client configured that uses the MAPI client. MAPI is only supported on Windows, and uses an Exchange server. The default email client is set in the Windows registry in HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Default.

If the email client does not meet the requirements, then clicking the Send button displays a system message saying that your default email client is not configured.

Email Client Messages

Most email clients display a warning message after the end-user clicks the Send button. The following example shows the error message that Outlook displays:

Figure 2 DART Outlook Warning



Microsoft Outlook

A program is trying to send an e-mail message on your behalf. If this is unexpected, click Deny and verify your antivirus software is up-to-date.

For more information about e-mail safety and how you might be able to avoid getting this warning, click Help.

New Features in Release 3.0.5080

AnyConnect 3.0.5080 is a maintenance release that resolves the list of caveats in Table 12 and incorporates Host Scan engine update 3.0.5080.

AnyConnect 3.0.5080 supports the latest Host Scan Engine Update, 3.0.11033.

New Features in Release 3.0.5075

AnyConnect 3.0.5075 is a maintenance release that incorporates the Host Scan Engine Update, 3.0.5075. This release does not introduce any new features.

New Features in Release 3.0.4235

AnyConnect 3.0.4235 is a maintenance release that resolves the list of caveats in Table 14 and adds support for Mac OS X, ScanCenter Hosted Configuration for the Web Security Hosted Client Profile, enhanced split DNS functionality, and LZS compression.

Mac OS X Support

The Web Security Module now supports these Mac OS X operating systems:

- Mac OS X v10.7 (x86 32-bit and x64 64-bit)
- Mac OS X v10.6 (x86 32-bit and x64 64-bit)
- Mac OS X v10.5 (x86 32-bit)

New Installation Directory Structure for Mac OS X

In previous releases of AnyConnect, AnyConnect components were installed in the **opt/cisco/vpn** path. Now, AnyConnect components are installed in the **/opt/cisco/anyconnect** path.

ScanCenter Hosted Configuration Support for Web Security Client Profile

The ScanCenter Hosted Configuration for the Web Security Hosted Client Profile gives administrators the ability to provide new Web Security client profiles to Web Security clients. Devices with Web Security can download a new client profile from the cloud (hosted configuration files reside on the ScanCenter server). The only prerequisite for this feature is for the device to have Web Security installed with a valid client profile.

Administrators use the Web Security Profile Editor to create the client profile files and then upload the clear text XML file to a ScanCenter server. This XML file must contain a valid license key from ScanSafe. The Hosted Configuration feature uses the license key when retrieving a new client profile file from the Hosted Configuration (ScanCenter) server. Once the new client profile file is on the server, devices with Web Security automatically poll the server and download the new client profile file, provided that the license in the existing Web Security client profile is the same as a license associated with a client profile on the Hosted server. Once a new client profile has been downloaded, Web Security will not download the same file again until the administrator makes a new client profile file available.

Note Web Security client devices must be pre-installed with a valid client profile file containing a ScanSafe license key before it can use the Hosted Configuration feature.

Split DNS Functionality Enhancement

AnyConnect 3.0.4235 supports true split DNS functionality for Windows and Mac OS X platforms, just as found in legacy IPsec clients. If the group policy on the security appliance enables split-include tunneling and if it specifies the DNS names to be tunneled, AnyConnect tunnels any DNS queries that match those names to the private DNS server. True split DNS allows tunnel access to only DNS requests that match the domains pushed down by the ASA. These requests are not sent in the clear. On the other hand, if the DNS requests do not match the domains pushed down by the ASA, AnyConnect lets the DNS resolver on the client operating system submit the host name in the clear for DNS resolution.

Note Split DNS supports standard and update queries (including A, AAAA, NS, TXT, MX, SOA, ANY, SRV, PTR, and CNAME). PTR queries matching any of the tunneled networks are allowed through the tunnel.

AnyConnect tunnels all DNS queries if the group policy does not specify any domains to be tunneled or if Tunnel All Networks is chosen at Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Advanced > Split Tunneling.

In AnyConnect 2.5, split DNS functionality was handled by our best-effort DNS fallback, but the following limitations existed (CSCtq02141):

1. When using split tunneling, the domain name could still be broadcasted to the public DNS servers.

2. When multiple DNS suffices are configured for your company, a risk of hijacking occurs as the DNS query goes out to a public DNS server. For example, assume you have a domain name like mycompany.com and mycompanyproducts.com, and a DNS query such as help.mycompany.com goes out to the public DNS server. The server returns the search page for unfound dns queries before querying the next suffix in the list.
3. In full tunnel mode, a long delay in DNS resolution existed when the DHCP server and the DNS server on the public interface had the same IP address.

For Mac OS X, AnyConnect can use true split-DNS only when not configuring an IPv6 address pool. If an IPv6 address pool is configured, AnyConnect can only enforce DNS fallback for split tunneling.

This 3.0.4235 feature requires that you:

- configure at least one DNS server
- enable split-include tunneling
- specify at least one domain to be tunneled

To configure this feature, establish an ASDM connection to the security appliance and configure the following:

- Split-include tunneling—Choose **Configuration > Remote AccessVPN > Network (Client) Access > Group Policies > Add or Edit > Advanced > Split Tunneling**. From the Policy drop-down menu, choose **Tunnel List Below** and select the relevant network list from the Network List drop-down menu.
- DNS Servers—Choose **Configuration > Remote AccessVPN > Network (Client) Access > Group Policies > Add or Edit > Servers**. Enter one or more private DNS servers in the DNS Servers field.

LZS Compression

Cisco now supports compression for DTLS and TLS on AnyConnect 3.0.3050 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. You enable compression in the webvpn submode of the group policy and username configuration modes. This feature enhances migration from the legacy VPN clients.

You must have ASA release 8.4.2.8 or later for support of the LZS compression feature. Also, to take advantage of TLS/DTLS data compression in a Linux or Mac, your PC must have libz.so or comparable to propose the compression.

Using data compression on high-speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced.

New Features in Release 3.0.3050

The following sections describe the new features in AnyConnect 3.0.3050:

- Global Site Selector
- Mac OS X v10.7 Support

Global Site Selector

The AnyConnect VPN client is now compatible with Global Site Selector (GSS) devices. No client-side configuration is required to take advantage of this capability; however, the end user must have the capability to write to the system Hosts file. When you point the client at the fully qualified domain name (FQDN) answered to the GSS, the devices provide DNS performance improvements through load balancing mechanisms. For GSS support, server certificate verifications must occur at the outset of authentication, including SSL handshakes performed in API, downloader, and agent.

Mac OS X v10.7 Support

AnyConnect 3.0.3050 provides support for Mac OS X v10.7.Without the appropriate Java and Web applet, OS X users may experience CSCtq62860 or CSCto09628. You must install Java and enable the appropriate Applet plug-in and web start applications using these steps:

Step 1 Open the Java Preferences when performing Hostscan or Weblaunch with Safari with Mac OS X v10.7.

Step 2 If Java is not already installed, you are prompted to do so.

Step 3 Check the *Enable applet plug-in and Web Start applications* option.

New Features in Release 3.0.2052

Network Location Awareness for Windows is the new feature delivered with AnyConnect 3.0.2052. With **Network Location Awareness** enabled on the AnyConnect virtual adapter (VA), Windows 7 now applies the proper firewall profile containing a collection of network and security settings to the network connection associated with the VA. The Cisco AnyConnect Secure Mobility Client connection now appears in the Windows Control Panel, Network and Sharing Center, and no additional configuration is required.

New Features in Release 3.0.1047

The following sections describe the new features in AnyConnect 3.0.1047:

- Secure Hash Algorithm SHA-2 Support for IPsec IKEv2 Integrity and PRF, page 15
- Secure Hash Algorithm SHA-2 Support for Digital Signature over IPsec IKEv2, page 15
- Network Access Manager Smart Card Pre Logon support on Windows 7 and Windows Vista, page 15
- MSI Command to Hide AnyConnect from Add/Remove Program List, page 15

Secure Hash Algorithm SHA-2 Support for IPsec IKEv2 Integrity and PRF

This release supports the Secure Hash Algorithm SHA-2 for increased cryptographic hashing security for IPsec IKEv2 connections to the ASA. AnyConnect supports SHA-2 for the integrity and pseudo-random function hash algorithms, with digests of 256, 384, or 512 bits, to meet U.S. government requirements. There are no AnyConnect configuration requirements to enable this feature.

SHA-2 support for IPsec IKEv2 integrity and PRF is supported by the ASA release 8.4(2) and later.

Secure Hash Algorithm SHA-2 Support for Digital Signature over IPsec IKEv2

This release supports the use of SHA-2 compliant signature algorithms to authenticate IPsec IKEv2 VPN connections that use digital certificates, with the hash sizes SHA-256, SHA-384, and SHA-512. There are no AnyConnect configuration requirements to enable this feature.

SHA-2 digital signature for IPsec IKEv2 connections is supported by the ASA release 8.4(2) and later.

Network Access Manager Smart Card Pre Logon support on Windows 7 and Windows Vista

This release adds support for Smart Card Pre Logon for the Network Access Manager on Windows 7 and Windows Vista endpoint computers.

MSI Command to Hide AnyConnect from Add/Remove Program List

This release adds the command-line call ARPSYSTEMCOMPONENT to the AnyConnect installers to hide the installed module from users that view the Windows Add/Remove Programs list. If you launch any installer using ARPSYSTEMCOMPONENT=1, the module does not appear in the Windows Add/Remove Programs list.

We recommend that you use the sample transform we provide to set this property (http://www.cisco.com/cisco/software/release.html?mdfid=283000185&flowid=17001&softwareid=282364313&release=3.0.2052&rellifecycle=&relind=AVAILABLE&reltype=latest), applying the transform to each MSI installer for each module you want to hide.

New Features in Release 3.0.0629

The following sections describe the new features in AnyConnect 3.0.0629:

- New Graphical User Interface, page 16
- Network Access Manager (Replacement for CSSC), page 17
- Telemetry, page 18
- Host Scan, page 19
- Web Security, page 21
- IPsec IKEv2, page 22
- DART Enhancements, page 23

- Windows Services Lockdown, page 23
- Software and Profile Locks, page 24

New Graphical User Interface

The AnyConnect Secure Mobility Client has a new interface for Windows, for an improved user experience.

The illustrations of the tray icons and several example changes to the user interface follow.

We have updated the AnyConnect icons, as shown in the following examples:

System tray icon indicating client components are operating correctly.

System tray icon indicating the VPN is connected.

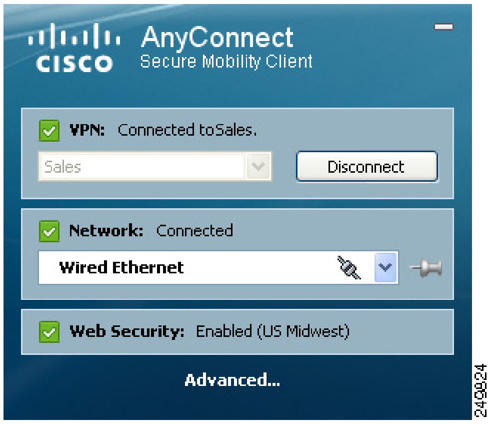
System tray icon alerting the user to a condition requiring attention or interaction. For example, a dialog about the user credentials.

System tray icons that indicate one or more client components are transitioning between states (for example, when the VPN is connecting or when Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right.

AnyConnect does not display more than one icon at a time. The icon with the highest priority takes precedence.

When one clicks the system tray icon, AnyConnect displays the status of only the AnyConnect components installed on the endpoint. (Figure 3).

Figure 3 AnyConnect Flyout



☑ **VPN:** Connected to Sales.

Sales

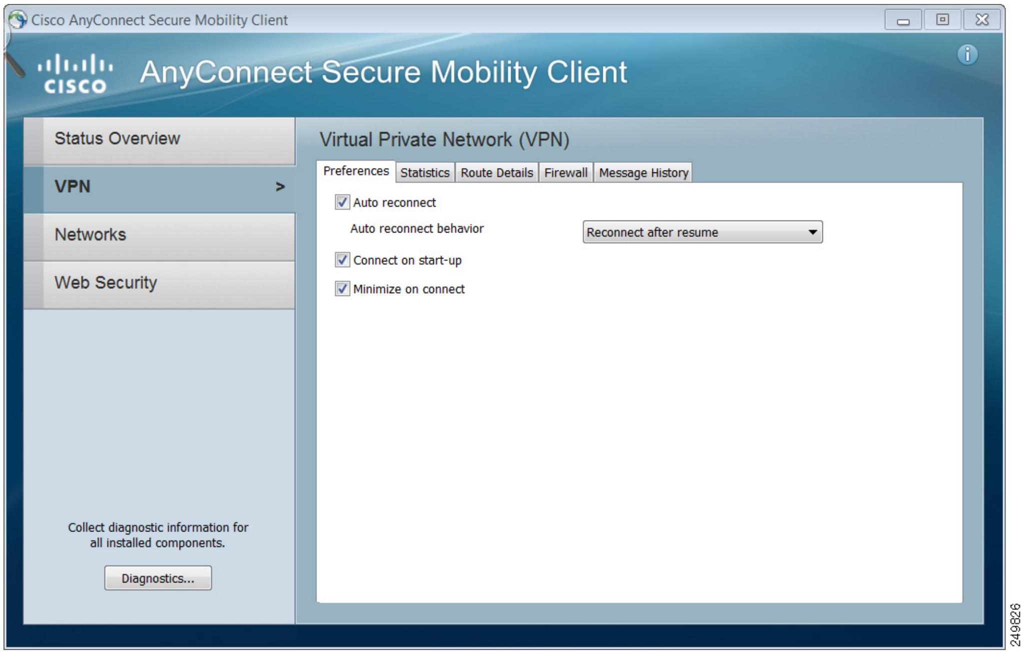
☑ **Network:** Connected

Wired Ethernet

☑ **Web Security:** Enabled (US Midwest)

Clicking **Advanced** provides access to a status overview, and user configuration and details for each installed AnyConnect component. Figure 4 shows an example.

Figure 4 Advanced VPN Preferences Tab



☑ Auto reconnect

Auto reconnect behavior: Reconnect after resume

☑ Connect on start-up

☑ Minimize on connect

Collect diagnostic information for all installed components.

Clicking the **Diagnostics** button opens the AnyConnect Diagnostics and Reporting Tool wizard, which bundles the log files and diagnostic data for analysis of issues.

Network Access Manager (Replacement for CSSC)

The Network Access Manager module is a full replacement for the Cisco Secure Services Client (CSSC).

Like CSSC, the Network Access Manager client software provides a secure Layer 2 network in accordance with policies set forth by the enterprise network administrators. Network Access Manager detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks. Network Access Manager manages user and device identity and the network access protocols required for secure access. It works intelligently to prevent end users from making connections that are in violation of administrator-defined policies on an enterprise wired or wireless network and supports next generation services (such as MACsec).

Network Access Manager client profiles define how end users create and authenticate wired and wireless network connections. The Network Access Manager profile editor is a GUI-based tool that you use to create a Network Access Manager client profile. After you create the profile, you can distribute it along with a pre-deployment AnyConnect Network Access Manager installation package to endpoints using a software management system.

AnyConnect 3.0.0629 delivers a profile editor that gets integrated with ASDM. This profile editor is preferred for creating Network Access Manager client profiles, but for those customers who do not have an ASA or use ASDM, you can use the standalone profile editor, which you can download and use to create these profiles. *Cisco now fully supports all AnyConnect 3.0 profile editors.* For installation instructions, go to "Deploying the AnyConnect Secure Mobility Client" in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0*.

System Requirements for Network Access Manager

Network Access Manager requires the following releases only if you are using ASDM to configure it:

- ASA version 8.4(1)
- ASDM version 6.4(1) or later.

Note *Cisco now fully supports all standalone AnyConnect 3.0 profile editors, including the Network Access Manager profile editor.* AnyConnect does not accept Network Access Manager profiles edited with third-party XML or plain-text editors.

Network Access Manager supports the following operating systems:

- Windows 7 SP1 x86 (32-bit) and x64 (64-bit)
- Windows Vista SP2 x86 and x64
- Windows XP SP3 x86
- Windows Server 2003 SP2 x86

Licensing and Upgrading Requirements for Network Access Manager

The AnyConnect Network Access Manager is licensed without charge for use with Cisco wireless access points, wireless LAN controllers, switches, and RADIUS servers. No AnyConnect Essentials or Premium license is required. A current SMARTnet contract is required on the related Cisco equipment.

Telemetry

The AnyConnect telemetry module for AnyConnect Secure Mobility Client sends information about the origin of malicious content to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA).

AnyConnect may also send personal information in the form of a user ID. If the malware is a web-browser cookie, the information sent to the WSA includes its location (that is, the directory). That directory contains the user ID of the person who downloaded the cookie.

The web filtering infrastructure uses telemetry data to strengthen its web security scanning algorithms, improve the accuracy of the URL categories and web reputation database, and ultimately provide better URL filtering rules.

The AnyConnect telemetry module performs these functions:

- Monitors the arrival of content on the endpoint.
- Identifies and records the origin of any content received by the endpoint whenever possible.
- Reports detection of malicious content, and its origin, of malicious content to Cisco Threat Operations Center.

System Requirements for Telemetry

The telemetry module requires these minimum ASA components:

- ASA 8.4(1)
- ASDM is 6.3.1

The telemetry module supports the following operating systems:

- Windows 7 SP1 x86 (32-bit) and x64 (64-bit)
- Windows Vista SP2 x86 and x64
- Windows XP SP3 x86

The telemetry module can only perform URL origin-tracing for browsers that use **wininet.dll**, such as Internet Explorer 7 and Internet Explorer 8. If you download a file using a browser which does not use **wininet.dll**, such as Firefox or Chrome, we can only identify the browser used to download the file. We cannot identify the URL from which the file was downloaded.

The telemetry module requires that an antivirus application, which the AnyConnect posture module supports, be installed on the endpoint.

The telemetry module is an add-on of AnyConnect Secure Mobility Client and it requires the AnyConnect posture module. The telemetry feature requires these modules to be installed on the endpoint in this order:

1. AnyConnect VPN Module
2. AnyConnect Posture Module
3. AnyConnect Telemetry Module

You can only enable the telemetry feature if you are using the AnyConnect Secure Mobility solution with the Cisco IronPort Web Security Appliance (WSA).

Host Scan

The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host. The module contains host scan, prelogin, and cache cleaner. The Host Scan application is the application that gathers this information. With the download and installation of this module, you gain elevated privileges and more advanced features.

In the adaptive security appliance (ASA), you can create a prelogin policy that evaluates the operating system, antivirus, antispyware, and firewall software Host Scan identifies. Based on the result of the prelogin policy's evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance.

Starting with AnyConnect 3.0, the Host Scan package becomes a shared component of the AnyConnect Secure Mobility client and Cisco Secure Desktop (CSD). Previously, the Host Scan package was one of several components available only by installing CSD.

The purpose of separating the Host Scan package from CSD is to allow Host Scan support charts to be updated more frequently than it was possible when they were delivered as part of CSD. The Host Scan support charts contain the product name and version information of the antivirus, antispyware, and firewall applications you use in your prelogin policies. We deliver the Host Scan application and the Host Scan support charts, as well as other components, in the Host Scan package.

The Host Scan package can now be delivered in one of three ways: with the AnyConnect Posture Module, with CSD, or as a standalone package. There are two types of AnyConnect posture modules: one version is pushed down by the ASA along with the AnyConnect installation and the other is configured as a pre-deployment module. The pre-deployment module can be installed on endpoints before they make their initial connection to the ASA.

System Requirements for Posture Module

The AnyConnect Secure Mobility Client with the posture module requires these minimum ASA components:

- ASA 8.4(1)
- ASDM 6.4(1) or later

The posture module supports the following operating systems:

- Windows XP SP3 (x86 and x86 running on x64)
- Windows Vista SP2 (x86 and x86 running on x64)
- Windows 7 (x86 and x86 running on x64)
- Mac OS X v10.5 and v10.6 (32-bit and 32-bit running on 64-bit)
- Linux (32-bit)

The posture module requires an AnyConnect Premium SSL VPN Edition license.

These AnyConnect features require that you install the posture module.

- SCEP authentication
- AnyConnect Telemetry Module

Host Scan, CSD, and AnyConnect Secure Mobility Client Interoperability

Caution A Host Scan package deployed along with AnyConnect Secure Mobility Client version 3.0.x must have the same or a later version number than the AnyConnect Secure Mobility Client.

- If you have Cisco Secure Desktop (CSD) version 3.5, or earlier, enabled on the ASA and you do not upgrade the Host Scan package to match or exceed the version of AnyConnect Secure Mobility Client 3.0.x you are deploying, prelogin assessments will fail and users will not be able to establish a VPN session. This will happen even if the AnyConnect 3.0.x posture module is pre-deployed to the endpoint because the ASA will automatically downgrade the Host Scan package on the endpoint to match the Host Scan package enabled on the ASA.
- Cisco Secure Desktop versions 3.6 and later are not compatible with AnyConnect version 2.4 and earlier.

Tip See “Chapter 5, Configuring Host Scan” in the *AnyConnect Secure Mobility Client Administrator’s Guide, Release 3.0* for instructions on installing and enabling the Host Scan image.

Web Security

The AnyConnect Web Security module is an endpoint component that routes HTTP traffic to a ScanSafe data center where ScanSafe Web Security service evaluates it.

ScanSafe Web Security service deconstructs the elements of a Web page so that it can analyze each element simultaneously. For example, if a particular Web page combined HTTP, Flash, and Java elements, separate “scanlets” analyze each of these elements in parallel. ScanSafe Web Security service then lets through benign or acceptable content and drops malicious or unacceptable content based on a security policy defined in the ScanCenter management portal. This prevents “over blocking” where an entire Web page is restricted because a minority of the content is unacceptable or “under blocking” where an entire page is permitted while there is still some unacceptable or possibly harmful content that is being delivered with the page. ScanSafe Web Security service protects users when they are on or off the corporate network.

With many ScanSafe data centers spread around the world, users taking advantage of AnyConnect Web Security are able to route their traffic to the ScanSafe data center with the fastest response time to minimize latency.

You can configure one or more Beacon Servers to identify endpoints that are on the corporate LAN. This is the “Detect-on-LAN” feature. If the Detect-On-LAN feature is enabled, any network traffic originating from the corporate LAN bypasses ScanSafe data centers. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than the ScanSafe Web Security service. The Beacon Servers use a unique public/private key pair for your organization to ensure that only ScanSafe Web Security customers with the correct public key can bypass the ScanSafe data centers while connected to your network. When deploying multiple Beacon Servers on your network, all the Beacon Servers must use the same private/public key pair.

AnyConnect Web Security features and functions are configured using the AnyConnect Web Security client profile which you edit using the AnyConnect profile editor.

ScanCenter is the management portal for the ScanSafe Web Security service. Some of the components created or configured using ScanCenter are also incorporated in the AnyConnect Web Security client profile.

Note The most up-to-date documentation for configuring a Web Security client profile using profile editor is in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0*.

System Requirements for Web Security Module

Web Security supports the following operating systems:

- Windows 7 SP1 x86 (x86 32-bit and x64 64-bit)
- Windows Vista SP2 (x86 32-bit and x64 64-bit)
- Windows XP SP 3 (x86 32-bit and x64 64-bit)
- Mac OS X v10.7 (32-bit and 64-bit)
- Mac OS X v10.6 (32-bit and 64-bit)
- Mac OS Xv10.5 (x86 32-bit)

ASA and ASDM Requirements for Web Security

The AnyConnect Secure Mobility Client with the Web security module requires these minimum ASA components:

- ASA 8.4(1)
- ASDM 6.4(1)

Requirements for Beacon Servers

Beacon servers are supported on the following operating systems:

- Windows Server 2008, x86 (32-bit)
- Windows Server 2003, x86 (32-bit)

Licensing Requirements for Web Security

These sections describe the licensing requirements for different deployment methods of the AnyConnect Web Security Module:

- Web Security Deployed as a Standalone Component, page 22
- Web Security Deployed as a Component of AnyConnect, page 22

Web Security Deployed as a Standalone Component

You can deploy the Web Security module and benefit from the ScanSafe web scanning services without having to install an ASA and without enabling the VPN capabilities of the AnyConnect Secure Mobility Client.

You still need a Secure Mobility for ScanSafe license in addition to a ScanSafe Web Filtering and/or ScanSafe Malware Scanning license in order for roaming users to be protected by ScanSafe web scanning services.

Note You **do not** need an AnyConnect Essentials or AnyConnect Premium license to use the AnyConnect Secure Mobility Client with only the Web Security module.

Web Security Deployed as a Component of AnyConnect

AnyConnect License - There are no AnyConnect licenses specific to Web Security. The Web Security module will work with either AnyConnect Essentials or AnyConnect Premium.

ScanCenter License - You need a Secure Mobility for ScanSafe license in addition to a ScanSafe Web Filtering and/or ScanSafe Malware Scanning license in order for roaming users to be protected by ScanSafe web scanning services.

IPsec IKEv2

Internet Key Exchange version 2 (IKEv2) is the latest key exchange protocol used to establish and control Internet Protocol Security (IPsec) tunnels. The AnyConnect Secure Mobility Client now supports IPsec with IKEv2 for all desktop operating systems supported by AnyConnect.

The ASA requires ASA release 8.4(001) and ASDM 6.4(1) or later to support AnyConnect IPsec IKEv2 connections.

On the ASA, you enable IPsec connections for users in the group policy. For the AnyConnect client, you specify the primary protocol (IPsec or SSL) for each ASA in the server list of the client profile.

The AnyConnect client uses a proprietary AnyConnect EAP authentication method with ASA secure gateways. Standards-based EAP authentication methods will soon be available for use with IOS secure gateways. However, using the standards-based method limits the dynamic download features of the client and disables some features. The client supports the following standards-based authentication methods:

- IKEv2 method: RSA
- EAP methods: MD5, GTC, and MSCHAPv2

Note The password change feature of MSCHAPv2 only updates the password on the back-end authentication server, not the local operating system password.

System Requirements for IPsec IKEv2

IPsec IKEv2 requires the following:

- ASA running version 8.4(1)
- ASDM 6.4(1) or later
- AnyConnect Essentials license or an AnyConnect Premium SSL VPN Edition license

DART Enhancements

DART is the AnyConnect Diagnostics and Reporting Tool that you can use to collect data useful for troubleshooting AnyConnect installation and connection problems. The logs now include Web Security, Posture, Telemetry, and Network Access Manager logs.

System Requirements for DART

You can run DART on any of the following OSs:

- Windows 7, Vista SP2, or XP SP3
- Redhat Enterprise Linux 5
- Mac 10.6 and 10.5
- Linux Ubuntu 9.x and 10.x

Note In the Mac environment, you cannot specify which files you want to include in the bundle as you can in Windows and Linux. You only have the default option which includes typical log files and diagnostic information (such as the AnyConnect log files, general information about the computer, and a summary of what DART did and did not do). Also within Mac, you cannot choose to mask the encryption password.

Windows Services Lockdown

Cisco recommends that end users are given limited rights on the device hosting the AnyConnect Secure Mobility client. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from disabling or stopping those Windows services established as locked down on the endpoint.

Each MSI installer supports a common property (LOCKDOWN) which, when set to a non-zero value, prevents the Windows service(s) associated with that installer from being controlled by users or local administrators on the endpoint device. You can enable lockdown by clicking the check box on the ISO installer. We recommend that you use the sample transform provided at the time of install to set this property and apply the transform to each MSI installer that you want to have locked down.

If you deploy the core client plus one or more optional modules, you must apply the lockdown property to each of the installers. This operation is one-way only and cannot be removed unless you re-install the product.

Software and Profile Locks

With software and profile locks, you can restrict the client to obtaining software or client profile updates only from ASAs that you allow. The locks are disabled by default; however, AnyConnect specifies the default domain, preventing the removal of VPN software by an unauthorized security appliance. The AnyConnect client can receive software or client profile updates from any ASA within the default domain.

With the software lock enabled, the client checks that the ASA is on the list of authorized servers before updating the core VPN client and any optional client modules (such as Network Access Manager, Telemetry, Web Security, and so on). If the ASA is not on the list, the client does not connect.

With the profile lock enabled, the client checks the same list before updating the client profiles for VPN or the other modules. If the ASA is not on the list, the client connects to the ASA but does not update the profile(s). You can refer to the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* for more information on the software lock and profile lock, including use cases and example XML in the local policy file.

Host Scan Engine Update, 3.0.11033

Caution See Important AnyConnect, CSD, and Host Scan Interoperability Information, page 6, for important AnyConnect and Host Scan compatibility information.

Tip It is a “best practice” to 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. An updated Host Scan package, **hostscan_3.0.11033-k9.pkg**, is available for use with AnyConnect 3.0.08057 or later.

See the “Host Scan” section on page 19 for a detailed description of Host Scan.

For an explanation of how this independent Host Scan package works in an environment with AnyConnect and CSD, see Host Scan, CSD, and AnyConnect Secure Mobility Client Interoperability, page 20.

The List of Antivirus, Antispyware, and Firewall Applications Supported by Host Scan 3.0.10057 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, CSD, and Host Scan Interoperability Information, page 6 for interoperability information.

Downloading the Host Scan Engine Update

To download the latest Cisco Host Scan Engine Updates, you must be a registered user of Cisco.com.

Step 1 Click this link to reach the software download area for Cisco Host Scan Engine Updates:

http://www.cisco.com/cisco/software/release.html?mdfid=284384091&flowid=33102&softwareid=283929405&release=3.0.11033&relind=AVAILABLE&rellifecycle=&reltype=latest

Step 2 Enter your cisco.com credentials and click **Login**.

Step 3 In the product tree, under **Latest Releases**, select 3.0.11033.

Step 4 In the file information area, select the Host Scan Engine Update 3.0.11033, and click **Download.**

Step 5 Click **Proceed with Download.**

Step 6 Read the End-User License Agreement and click **Agree**.

Step 7 Select a download manager option and click the **download** link to proceed with the download.

Step 8 See “Installing and Enabling Host Scan on the ASA” in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* for instructions on installing and enabling the Host Scan image.

Profile Editors Now Supported

We now support all standalone AnyConnect 3.0 profile editors (that is, those for Network Access Manager, VPN, and Web Security) as well as the local policy editor.

IOS Supported by AnyConnect 3.0.1047

Cisco supports AnyConnect 3.0 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 3.0 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.

UTF-8 Character Support for AnyConnect Passwords

AnyConnect 3.0 used with ASA 8.4(1), supports UTF-8 characters in passwords sent using RADIUS/MSCHAP and LDAP protocols.

Guidelines from Previous Releases Still in Effect

The following guidelines documented for previous releases remain in effect:

- Active X Upgrade Can Disable Weblaunch, page 27
- AnyConnect VPN over Tethered Devices, page 27
- AnyConnect Smart Card Support, page 27
- Disabling Auto Update May Prevent Connectivity Due to a Version Conflict, page 27
- Apple MobileMe Conflicts with AnyConnect, page 27
- Interoperability between Network Access Manager and other Connection Managers, page 28
- Network Interface Card Drivers Incompatible with Network Access Manager, page 28
- Network Access Manager Installation and Upgrade Hangs on Windows XP SP2 Systems Running the Cisco NAC Agent, page 29
- Avoiding SHA 2 Certificate Validation Failure (CSCtn59317), page 29
- Configuring Antivirus Applications for Host Scan, page 30
- Windows Mobile Not Supported, page 30
- iPhone Not Supported, page 31
- Flash and DRAM Requirements for Upgrade, page 31
- Microsoft Internet Explorer Proxy Not Supported by IKEv2, page 31
- MTU Adjustment on Group Policy May Be Required for IKEv2, page 32
- MTU Automatically Adjusted When Using DTLS, page 32
- Network Access Manager and Group Policy, page 32
- Full Authentication Required if Roaming between Access Points, page 32
- Auto Connect on Start Now Disabled By Default, page 33
- User Guideline for Web Security Behavior with IPv6 Web Traffic, page 35
- Preventing Other Devices in a LAN from Displaying Hostnames, page 35
- Revocation Message, page 35
- Messages in the Localization File Can Span More than One Line, page 36
- AnyConnect for Mac OS X Performance when Behind Certain Routers, page 36
- Preventing Windows Users from Circumventing Always-on, page 36
- Responding to a TUN/TAP Error Message with Mac OS X v10.5, page 36
- Avoid Wireless-Hosted-Network, page 37
- AnyConnect Requires the ASA Be Configured to Accept TLSv1 Traffic, page 37
- CRL Checking Enabled, page 37

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.

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 smart cards in the following environments:

- Microsoft CAPI 1.0 and CAPI 2.0 on Windows XP, 7 & Vista
- Keychain via Tokend on Mac OS X, 10.5 and higher

Note AnyConnect does not support Smart cards on Linux or PKCS #11 devices

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.

Apple MobileMe Conflicts with AnyConnect

If users of MobileMe have configured “Back to my Mac,” they will encounter connection problems with AnyConnect. Both AnyConnect and MobileME use the virtual adapter named “utun0.” MobileMe starts before AnyConnect when the computer boots, so it always gets the utun0 interface first, which causes Cisco AnyConnect to fail. Neither application can be configured to use a different interface, such as “utun1.”

Mac users must turn off “Back to my Mac” before connecting to the AnyConnect VPN. Once the VPN has connected, they can re-enable “Back to my Mac.”

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 the following are true:

- One has intentionally pruned root certificates.
- 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 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 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 because of 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 we know work:

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

Caution Do not apply this workaround to SmartCards certificates. The CSP names must not be changed. 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, 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

This release of AnyConnect does not support Microsoft Windows Mobile or Windows Phone. Refer to the *End-of-Life Announcement for the Cisco AnyConnect Secure Mobility Client on Windows Mobile* for support and availability details applicable to earlier releases of AnyConnect.

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 2.4 VPN connections. For ASA setup instructions, see the Release Notes for Cisco AnyConnect Secure Mobility Client 2.4, Apple iOS 4.2.

Flash and DRAM Requirements for Upgrade

Check for the space available before proceeding with the AnyConnect 3.0 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.

Because of the increased size of the AnyConnect package from 4MB in AnyConnect 2.5 to 21 MB in AnyConnect 3.0, you may need to upgrade the ASA flash and memory card first.

Caution The minimum flash memory required is 128MB for an ASA 5505; however, we strongly recommend 256 or preferably 512 MB. To support multiple endpoint operating systems and enable logging and debugging on the ASA, you will most likely need 512 MB of flash memory.

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.

Microsoft Internet Explorer Proxy Not Supported by IKEv2

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

MTU Adjustment on Group Policy May Be Required for IKEv2

AnyConnect sometimes receives and drops packet fragments with some routers. This can result 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 will automatically determine 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 will auto-tune 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 Vista *Only use Group Policy profiles for allowed networks* option
- When deploying XP wireless GPO policy on Windows 7 or Vista

Full Authentication Required if Roaming between Access Points

A mobile endpoint running Windows 7 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 will prompt the user to enter credentials for every full authentication if the active profile requires it.

Auto Connect on Start Now Disabled By Default

In AnyConnect 3.0, the Auto Connect on Start feature connects at logon for Windows. This feature is disabled by default, which is a change from AnyConnect 2.5.2xxx and earlier releases.

The Auto Connect on Start feature is defined in two places: it is hard-coded in AnyConnect and it can be "turned on" or "turned off" in a VPN client profile by using the **Auto Connect on Start** check box in profile editor. In AnyConnect 3.0, both the hard-coded configuration of Auto Connect on Start and the configuration of Auto Connect on Start in a VPN client profile are changed so that they are disabled by default.

Starting the user interface does not trigger Auto Connect on Start.

AnyConnect has evolved from having the ability to establish a VPN connection automatically upon the startup of AnyConnect to having that VPN connection be "always-on" by the Post Log-in Always-on feature. Disabling the Auto Connect on Start element reflects that evolution. If your enterprise's deployment uses the Auto Connect on Start feature, consider using the Trusted Network Detection feature instead.

Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.

If you are a customer running AnyConnect 2.5.xxx or earlier and you are upgrading to AnyConnect 3.0, this change to the Auto Connect on Start feature may affect you.

The Auto Connect on Start feature is enabled or disabled based on an order of precedence:

- The hard-coded value of Auto Connect on Start is used by AnyConnect when you do not distribute a VPN client profile.
- If you distribute a VPN client profile, the value of Auto Connect on Start in the VPN client profile takes precedence over the hard-coded value.
- If you allow users to have control over Auto Connect on Start, their choice to enable it or disable it takes precedence over the value you specified in the VPN client profile.

Table 5 explains how the hard-coded element and VPN client profile element interact.

Table 5 Auto Connect On Start Configuration Change After Upgrade from AnyConnect 2.5.2xxx or earlier to 3.0

AnyConnect 2.5.2xxx and earlier Auto Connect on Start hard-coded value	AnyConnect 2.5.2xxx and earlier Auto Connect on Start VPN client profile value	AnyConnect 3.0 Auto Connect on Start hard-coded value	AnyConnect 3.0 Auto Connect on Start VPN client profile value	Is Auto Connect on Start enabled or disabled by AnyConnect 3.0 user?	Is Auto Connect on Start enabled or disabled in AnyConnect 3.0 deployment?
Enabled	Not specified	Disabled	Not specified	Not specified	Disabled - After upgrade to AnyConnect 3.0
Enabled	Enabled	Disabled	Not specified	Not specified	Enabled - Assuming the AnyConnect 2.5 VPN client profile continues as the AnyConnect 3.0 profile.
Enabled	Enabled	Disabled	Disabled	Not specified	Disabled - Assuming you are distributing an updated AnyConnect 3.0 VPN client profile.
Enabled	Enabled	Disabled	Disabled	Enabled	Enabled - The user's preference takes precedence over all other profiles.

For information on configuring Trusted Network Detection, see "Trusted Network Detection" in "Configuring VPN Access" in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0*.

User Guideline for 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 will be sent to the scanning proxy were it will perform 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 will use that for the connection. If it does not find an IPv4 address, the connection will be 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 will make all IPv6 traffic bypass all scanning proxies. This means that IPv6 traffic will not be protected by Web Security.

Preventing Other Devices in a LAN from Displaying Hostnames

After one uses AnyConnect to establish a VPN session with Windows 7 on a remote LAN, the network browsers on the other devices in the user's LAN can 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, please note that 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. This could happen because 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 ipconfig cscotun0 mtu 1200` (For Mac OS X v10.5 or earlier)

`sudo ipconfig 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 users: C:\ProgramData

Responding to a TUN/TAP Error Message with Mac OS X v10.5

During the installation of AnyConnect on Mac OS X v10.5 and earlier versions, the following error message sometimes appears:

```
A version of the TUN virtual network driver is already installed on this system that is
incompatible with the AnyConnect client. This is a known issue with OS X version 10.5 and
prior, and has been resolved in 10.6. Please uninstall any VPN client, speak with your
System Administrator, or reference the AnyConnect Release Notes for assistance in
resolving this issue.
```

Mac OS X v10.6 resolves this issue because it provides the version of the TUN/TAP virtual network driver AnyConnect requires.

Versions of Mac OS X earlier than 10.6 do not include a TUN/TAP virtual network driver, so AnyConnect installs its own on these operating systems. However, some software such as Parallels, software that manages data cards, and some VPN applications install their own TUN/TAP driver. The AnyConnect installation software displays the error message above because the driver is already present, but its version is incompatible with AnyConnect.

To install AnyConnect, you must remove the TUN/TAP virtual network driver.

Note Removing the TUN/TAP virtual network driver can cause issues with the software on your system that installed the driver in the first place.

To remove the TUN/TAP virtual network driver, open the console application and enter the following commands:

```
sudo rm -rf /Library/Extensions/tap.kext
sudo rm -rf /Library/Extensions/tun.kext
sudo rm -rf /Library/StartupItems/tap
sudo rm -rf /Library/StartupItems/tun
sudo rm -rf /System/Library/Extensions/tun.kext
sudo rm -rf /System/Library/Extensions/tap.kext
sudo rm -rf /System/Library/StartupItems/tap
sudo rm -rf /System/Library/StartupItems/tun
```

After entering these commands, restart Mac OS X, then re-install AnyConnect.

Avoid Wireless-Hosted-Network

Using the Windows 7 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 (for example, Connectify or Virtual Router).

AnyConnect Requires 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.

No Prompting for Untrusted Server Certificates

Aligning with the behavior of IPsec, AnyConnect no longer prompts you to accept an untrusted server certificate in always on or start before logon mode for SSL connections. Instead, these connections are terminated.

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.

svc Commands

CLI commands starting with svc are supported only in AnyConnect 2.5 or earlier. Those commands were switched from *svc* to *anyconnect* in AnyConnect 3.0.

System Requirements

This section identifies the general 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 3.0 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:

- Security Appliance Software Requirements
- Microsoft Windows
- Linux
- Mac OS X

Security Appliance Software Requirements

- The VPN portion of the AnyConnect 3.0 client requires ASA 8.0(4).
- If you wish to use the ASDM-integrated Profile Editor to configure any of AnyConnect’s components, you must use ASDM version 6.4(1) or later.

Note If you choose not to upgrade ASDM to 6.4(1) or later, you must use an editor to add the XML tags to the AnyConnect profile if you want to deploy the new AnyConnect features.You must upgrade to ASA 8.4(1) or later if you want to use IKEv2.

- If you wish to use ASDM to edit only VPN profiles, you must use ASA version 8.2 or later.

- If you wish to use ASDM to edit non-VPN profiles (such as Network Access Manager, Web Security, or Telemetry), you must use ASA version 8.4 or later.

You must upgrade to ASA 8.3(1) if you want to do the following:

- 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.

The minimum supported version of Cisco Secure Desktop is 3.2(2) or later.

The minimum supported version of Host Scan is 3.0.0629, which is provided with this release of AnyConnect.

Microsoft Windows

To start AnyConnect with WebLaunch, use Internet Explorer 6.0 or later or Firefox 3.0+, and enable ActiveX or install Sun JRE 1.4+. Users of x64 (64-bit) Windows versions supported by AnyConnect must use the 32-bit version of Internet Explorer or Firefox to use WebLaunch. At this time, Firefox is available only in a 32-bit version.

Windows Versions

- Windows 7 SP1 x86 (32-bit) and x64 (64-bit)

  AnyConnect requires a clean install if you upgrade from Windows XP to Windows 7.

  If you upgrade from Windows Vista to Windows 7, manually uninstall AnyConnect first, then after the upgrade, reinstall it manually or by establishing a web-based connection to a security appliance configured to install it. Uninstalling before the upgrade and reinstalling AnyConnect afterwards is necessary because the upgrade does not preserve the Cisco AnyConnect Virtual Adapter.

  AnyConnect VPN is compatible with 3G data cards which interface with Windows 7 via a WWAN adapter.

- Windows Vista SP2 x86 (32-bit) and x64 (64-bit)

  AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista.

- Windows XP SP3 x86 (32-bit) and x64 (64-bit)

Note 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.

Note The Network Access Manager portion of AnyConnect does not support Windows XP SP3 x64 (64-bit).

Windows Requirements

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

Caution The minimum flash memory required is 128MB for an ASA 5505; however, we strongly recommend 256 or preferably 512 MB. To support multiple endpoint operating systems and enable logging and debugging on the ASA, you will most likely need 512 MB of flash memory.

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.

Linux

The following sections show the supported Linux distributions and requirements.

Linux Distributions

- Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 6 Desktop
- Ubuntu 9.x and 10.x

  We do not validate other Linux distributions. We will consider requests to validate other Linux distributions for which you experience issues, and provide fixes at our discretion.

Linux Requirements

- x86 instruction set.
- 32-bit.
- 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. Iced Tea is the default Java package on Fedora 8. 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.

- 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

AnyConnect 3.0 supports the following versions of Mac OS X:

- Mac OS Xv10.8 (32-bit and 64-bit) Starting with AnyConnect release 3.0.08057.
- Mac OS X v10.7 (32-bit and 64-bit)
- Mac OS X v10.6.x (32-bit and 64-bit)
- Mac OS X v10.5 (32-bit)

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.

If you upgrade from one major Mac OS X release to another (for example, 10.7 to 10.8), manually uninstall AnyConnect first, then after the upgrade, reinstall it manually or by establishing a web-based connection to a security appliance configured to install it.

Gatekeeper

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

- Mac App Store
- Mac App Store and identified developers
- Anywhere

The default setting is **Mac App Store and identified developers** (signed applications). AnyConnect is a signed application and will run normally with this setting or with the **Anywhere** setting. If you select the **Mac App Store** setting, you must use Control-click to install and run AnyConnect. For further information see: http://www.apple.com/macosx/mountain-lion/security.html.

Note This applies only to new stand-alone installs and is not applicable to web launch or OS upgrades (for example 10.7 to 10.8)

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.

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, please report them. We will make our best effort to resolve them.

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 this site:
http://www.cisco.com/cisco/software/release.html?mdfid=283000185&release=3.0.xxxx&relind=AVAILABLE&i=rm&softwareid=282364313&rellifecycle=&reltype=latest.

For support issues with 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.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, select Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

The following sections lists caveats with Severities 1-3:

- AnyConnect 3.0.11046 Caveats
- AnyConnect 3.0.11042 Caveats
- AnyConnect 3.0.10055 Caveats
- AnyConnect 3.0.10055 Caveats
- AnyConnect 3.0.08057 Caveats
- AnyConnect 3.0.07059 Caveats
- AnyConnect 3.0.5080 Caveats

- AnyConnect 3.0.4235 Caveats
- AnyConnect 3.0.3054 Caveats
- AnyConnect 3.0.3050 Caveats
- AnyConnect 3.0.2052 Caveats
- AnyConnect 3.0.1047 Caveats
- AnyConnect 3.0.0629 Caveats
- Host Scan Engine Caveats

AnyConnect 3.0.11046 Caveats

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

AnyConnect 3.0.11042 Caveats

Caveats Resolved by Release 3.0.11042

Component	Identifier	Headline
api	CSCtz92140	Anyconnect 3.x may display incorrect gateway in established to field
api	CSCub59164	Mac Auto Upgrade fails
certificate	CSCtz83719	SCEP enrollment fails if CA doesn't send complete cert chain
certificate	CSCub11994	valid certification error after successful connection
core	CSCtz81595	AnyConnect on Mac 3.0.07059 and later don't work with Cisco IOS Routers
download_install	CSCub46241	AnyConnect weblaunch fails from Internet Explorer with Java 7
gui	CSCub27157	Anyconnect NAM: Unable to pass arguments to scripts
gui	CSCub27170	Ability for admins to specify scripts while preventing users running it
nam	CSCtz21260	NAM: RDP fails on second connection attempt
posture-asa	CSCto40355	Improve HostScan logging: Label non-warning messages as debug
posture-asa	CSCtx45701	HostScan consumes a large amount of CPU time
posture-asa	CSCua64423	HostScan reports Sophos AV Virus Def Last Update incorrectly on MacOSX
posture-asa	CSCub02626	HostScan Engine 3.0.08062 AS support chart should not list 'Eset'
posture-asa	CSCub05542	HostScan Weblaunch does not work on Windows 8
posture-asa	CSCub10948	Hostscan reports "elevationrequired" with Eset AV
posture-asa	CSCub19730	HostScan doesn't report "lastupdate" value for Kaspersky 11.x
posture-asa	CSCub29350	HostScan reports Windows 7 as OS on Windows 8
posture-asa	CSCub40522	HostScan should not report information periodically when not needed
posture-asa	CSCub41486	HostScan must renew ASA token every 10 mins until reporting is complete
posture-asa	CSCub56424	HostScan crashes on Mac OS X 10.5
posture-asa	CSCub59068	HostScan Weblaunch fails when using Java 6
posture-asa	CSCub59103	HostScan Weblaunch when using Internet Explorer with Java 7
posture-asa	CSCub70132	HostScan Weblaunch fails with Internet Explorer 10 and ActiveX
posture-asa	CSCuc42875	HostScan Weblaunch fails on upgrade when using ActiveX
posture-asa	CSCuc48299	IE with Java 7 crashes on HostScan Weblaunch
profile-editor	CSCty01313	NAM: PE does not save config if foreign characters are used in the name

Component	Identifier	Headline
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
vpn	CSCtg10248	UI may start too fast on Windows, throwing "Agent is unresponsive" alert
vpn	CSCty89947	AnyConnect MacOSX connection move Reconnecting state and never come up
vpn	CSCua02849	Use primary ASA in LB cluster for IPSec Always On profile check
vpn	CSCua35433	Anyconnect:IP addr in profile causes Always-On/Connection to fail
vpn	CSCub23470	IKEv2 negotiation fails when there are duplicate IKE_AUTH exchanges
vpn	CSCub45932	"No DNS connectivity" incorrectly reported, slow reconnect/disconnect

Caveats Open in Release 3.0.11042

Component	Identifier	Headline
aaa-ipsec	CSCts29023	AC IKEv2 conn failure message should indicate no IP address assigned
aaa-webvpn	CSCts28999	AC SSL message when no IP address available needs changes
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
certificate	CSCtz78738	NSS Cert Store: NSS_InitReadWrite fails on Ubuntu 12
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, NAM or UI open
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCts96212	AnyConnect Stuck at Reconnecting
core	CSCtv00449	PAC proxy settings not honored by Agent in WebLaunch case
core	CSCua31665	Status command doesn't work on Ubuntu
doc	CSCtr61978	DOC: GSS-DNS TTL should be greater than VPN connect time w/ client proxy
doc	CSCtx70754	AnyConnect 3.0 fails to connect from CSD vault
doc	CSCtz02599	DOC:HostScan: 3rd party client-server products are not supported
doc	CSCua89081	DOC: specific Extended Key Usage rqrd in client certs for some 3.0 vers.
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCts64361	Launch AnyConnect UI automatically for WebSecurity only installs on OS X
download_install	CSCtz84437	Connection fails when upgrading from 3.0 connecting to a 3.1 headend
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtl75601	Incorrect ICON shown when certificate warning displayed,gui not notified
hostscan	CSCsz67469	Hostscan with Secure Vault fails to detect Service Pack on 64-bit Vista
nam	CSCtl54461	NAM: lan OneXEnforced policy interferes with IP acquisition
nam	CSCub87696	Anyconnect Nam -Retain VPN connection not working using secured dot1x
posture-asa	CSCtc12807	"Disable Cancel Button" should not appear in the management plugin
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch

Component	Identifier	Headline
posture-asa	CSCte15402	Session cache created 0~30 secs after logon is not cleaned Mac 10.6.x.
posture-asa	CSCtf40994	CSD 3.5 Cache Cleaner termination, long delay in closing browser
posture-asa	CSCtg68119	CSD: Cache Cleaner fails to clear the FF browser history
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	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
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	CSCub03057	McAfee AS is not picked up as a distinct product
posture-asa	CSCub03057	McAfee AS is not picked up as a distinct product
ssa	CSCti90824	Seamless Secure Access - initial development of library, api and infra
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf60851	Network access not being displayed during reconnects
vpn	CSCtf63783	VPN connection failed because "CSD isn't installed..."
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg58360	Always-On profile is deleted if connecting as a user that has no profile
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth13596	AC30 SCEP - combine similar message dialogs into one
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCti78913	AC displays the Pre-Login error twice
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - can't log in
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays "On a Trusted Network"
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials

Component	Identifier	Headline
vpn	CSCtn74489	Can't WebLaunch/Install on Ubuntu if using Proxy Server & Ignored Hosts
vpn	CSCto31503	OGS calculations are not occuring
vpn	CSCtq29607	Host Scan failures with TND enabled right after an upgrade
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCts29059	AC agent sometimes terminates after failed conn where no IP address avai
vpn	CSCts44842	Use non-windows untrusted cert banner logic for SBL and machine certs
vpn	CSCtu18520	Always-On with Fail Close able to contact the ASA but still locked down
vpn	CSCtx08124	GUI simply closes w/no error when using a proxy server w/Digest Auth
vpn	CSCtx74050	IPsec: Private proxy server gets truncated & wrong port - SSL OK
vpn	CSCty61386	AC cannot modify ip forwarding table when VPN is over 2nd interface
vpn	CSCty77231	Anyconnect ikev2 should ignore http-url cert payload
vpn	CSCua36934	Using Firefox 12.0 and 13.0 throws fatal error on Linux
web	CSCua79260	Anyconnect web-launch fails on Linux OS

AnyConnect 3.0.10057 Caveats

Caveats Resolved by Release 3.0.10057

Component	Identifier	Headline
certificate	CSCuc07598	Sort proper EKU certificates to be first

Caveats Open in Release 3.0.10057

Component	Identifier	Headline
aaa-ipsec	CSCts29023	AC IKEv2 conn failure message should indicate no IP address assigned
aaa-webvpn	CSCts28999	AC SSL message when no IP address available needs changes
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
api	CSCtz92140	Anyconnect 3.x may display incorrect gateway in established to field
certificate	CSCtz78738	NSS Cert Store: NSS_InitReadWrite fails on Ubuntu 12
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, NAM or UI open
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCts96212	AnyConnect Stuck at Reconnecting
core	CSCtv00449	PAC proxy settings not honored by Agent in WebLaunch case
core	CSCua31665	Status command doesn't work on Ubuntu
dart	CSCts69478	DART Doesn't Grab the Latest Windows Events
doc	CSCtr61978	DOC: GSS-DNS TTL should be greater than VPN connect time w/ client proxy
doc	CSCtx70754	AnyConnect 3.0 fails to connect from CSD vault
doc	CSCtz02599	DOC:HostScan: 3rd party client-server products are not supported
doc	CSCua89081	DOC: Anyconnect requires specific Extended Key Usage in client certs
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCts64361	Launch AnyConnect UI automatically for WebSecurity only installs on OS X
download_install	CSCtz84437	Connection fails when upgrading from 3.0 connecting to a 3.1 headend
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection

Component	Identifier	Headline
gui	CSCtl75601	Incorrect ICON shown when certificate warning displayed,gui not notified
hostscan	CSCsz67469	Hostscan with Secure Vault fails to detect Service Pack on 64-bit Vista
nam	CSCtl54461	NAM: lan OneXEnforced policy interferes with IP acquisition
posture-asa	CSCtc12807	“Disable Cancel Button” should not appear in the management plugin
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch
posture-asa	CSCte15402	Session cache created 0~30 secs after logon is not cleaned Mac 10.6.x.
posture-asa	CSCtf40994	CSD 3.5 Cache Cleaner termination, long delay in closing browser
posture-asa	CSCtg68119	CSD: Cache Cleaner fails to clear the FF browser history
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	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
posture-asa	CSCtx45701	HostScan is consumming large amounts of CPU time
posture-asa	CSCtz70911	Pre-login assessment w/ SBL and IKEv2 fails for certain registry checks
posture-asa	CSCua31894	Microsoft Forefront Endpoint Protection 2010 Not Detected By Hostscan
ssa	CSCti90824	Seamless Secure Access - initial development of library, api and infra
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf60851	Network access not being displayed during reconnects
vpn	CSCtf63783	VPN connection failed because “CSD isn't installed...”
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg58360	Always-On profile is deleted if connecting as a user that has no profile
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth13596	AC30 SCEP - combine similar message dialogs into one
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCti78913	AC displays the Pre-Login error twice
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - can't log in
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download

Component	Identifier	Headline
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays "On a Trusted Network"
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn74489	Can't WebLaunch/Install on Ubuntu if using Proxy Server & Ignored Hosts
vpn	CSCto31503	OGS calculations are not occuring
vpn	CSCtq29607	Host Scan failures with TND enabled right after an upgrade
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCtr59999	GSS-DNS: Connected through a Public proxy, wrong Server Address in Stats
vpn	CSCtr75134	After new install -not able to establish a connection- reconnect it's OK
vpn	CSCts29059	AC agent sometimes terminates after failed conn where no IP address avai
vpn	CSCts44842	Use non-windows untrusted cert banner logic for SBL and machine certs
vpn	CSCtu18520	Always-On with Fail Close able to contact the ASA but still locked down
vpn	CSCtx08124	GUI simply closes w/no error when using a proxy server w/Digest Auth
vpn	CSCtx74050	IPsec: Private proxy server gets truncated & wrong port - SSL OK
vpn	CSCty61386	AC cannot modify ip forwarding table when VPN is over 2nd interface
vpn	CSCty77231	Anyconnect ikev2 should ignore http-url cert payload
vpn	CSCtz86407	Receiving unexpected cert behind captive portal, connection not allowed
vpn	CSCua36934	Using Firefox 12.0 and 13.0 throws fatal error on Linux
vpn	CSCub42978	Backup Server list fails using IPSec
web	CSCua79260	Anyconnect web-launch fails on Linux OS

AnyConnect 3.0.10055 Caveats

Caveats Resolved by Release 3.0.10055

Component	Identifier	Headline
api	CSCtg67075	Terminate Reason Displayed as Balloon with Non-cert Authentication
api	CSCti33658	TX/RX to show days in the statistics as opposed hrs
api	CSCts35238	VPN: GUI hangs after certificate enrollment
api	CSCts42926	API: [ntdll!RtlpLowFragHeapFree+31] vpnui.exe: c0000005 (Crash 32bit)
api	CSCtu30777	VPN: Unable to connect over satellite uplink with high latency >700ms
api	CSCty02610	VPN API displays HostScan log messages instead of messages tagged UI
api	CSCty80134	Anyconnect COM API broken on Windows XP platform
api	CSCtz83572	API should delay Hostscan poling until Hostscan has finished scanning
api	CSCtz87786	AC VPN should start polling wait.html on notification from HS
api	CSCtz87792	AC VPN should increase connect timeouts to account for Dialup
api	CSCtz87795	AC VPN should increase overall HS processing timeouts for Dialup
api	CSCua02955	'Export Stats' Doesn't Work With Double Byte Translation
api	CSCua07911	VPN API Logging Not Enabled for 3.0 on Linux/OS X
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCts13436	Connection failed due to code signing CRL being unreachable
certificate	CSCts76302	AC: RHEL 5 base install fails to validate some web server certs
certificate	CSCty94486	IKEV2 certificate failure debugs are not verbose enough
certificate	CSCtz83719	SCEP enrollment fails if CA doesn't send complete cert chain
certificate	CSCua53392	AnyConnect can't find libplc4.so on web-launch install on Redhat6
certificate	CSCua61022	Mac and Linux does not verify chain trust for code signing certificate
certificate	CSCua76140	Expiration checks improperly ignored during code sign verification
certificate	CSCub42773	unnecessarily full server cert verification during IKEv2 reconnects
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCty30281	Anyconnect may consume more than one session slot per connection
core	CSCtz81595	AnyConnect on Mac 3.0.07059 and later don't work with Cisco IOS Routers

Component	Identifier	Headline
dart	CSCtt25721	DART bundle on windows is using backslash as file separators.
dart	CSCtx75004	DART CLI on Linux only works if called from DART directory
dart	CSCty27243	Add back button on dart email screen when email client is not configured
dart	CSCty36816	Dart email field should include semicolon as a email list seperator
dart	CSCty42743	Disable Email Dart Bundle when Dart Bundle fails to be created
dart	CSCty55369	Disable DART email button when email client is not configured
dart	CSCty67889	DART CLI option doesn't take single backslash or forward slash argument
dart	CSCty67976	Dart email field should state semi-colon separated list, not comma
dart	CSCty86818	Garbled text on DART "Email Your Bundle" dialog
dart	CSCtz04919	Mac DARTs are copying the same data multiple times
dart	CSCtz21528	Change display message on DART email UI
dart	CSCtz67595	RW Dart "Enable Bundle Encryption" sets password when disabled
dart	CSCtz67632	RW DART "Enable Bundle Encryption" does not work on Windows
dart	CSCtz96919	Make the dart options more user-friendly
dart	CSCtz97008	DART: acwebsecagent crash report not collected
dart	CSCua27123	DART event log export sometimes does not include vital information
dart	CSCua31730	DART on Linux showing folders as zero bytes inside the Archive manager
dart	CSCua60836	DART to pick up Hostscan core dump file
dart	CSCua71694	DART - Removal of unnecessary General Information page (tech debt)
doc	CSCtz29197	AnyConnect PROMPTS user to allow accepting untrusted certs by default
download_install	CSCts46682	AnyConnect Linux init script issues
download_install	CSCts51839	AnyConnect 3.0 Pre-Deployment fails on Linux machines
download_install	CSCtz41704	VPNLB: IKEv2 connections fails on profile update if SSL cert untrusted
download_install	CSCua60812	Add no display support for Anyconnect Downloader
download_install	CSCua76272	Anyconnect VPN Component Uninstall Forces Reboot w XP
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCty78070	Bypassed (LAN) WebSecurity statistic needs to be removed
gui	CSCua02187	GUI: [GdiPlus!GpAssertShutdownNoMemoryLeaks+1b9] vpnui.exe: c0000420 (FA
gui	CSCub35054	Windows VPN Credentials may not layout properly

Component	Identifier	Headline
gui	CSCub56378	Anyconnect websec module 3.0.8066 show service unavailable after reboot
hostscan	CSCsx78621	Hostscan log does not get overwritten with Secure Vault
nam	CSCto05313	EAP-FAST:user authorization PAC issue
nam	CSCto95207	NAM: password protected certificates do not work
nam	CSCtw47024	NAM: Cert authentication does not work with Entrust Security Store
nam	CSCtx35523	Client certificate is sent in the clear even if configured in tunnel
nam	CSCty10978	AnyConnect can not get the user credentials from windows login (SSO)
nam	CSCty48346	NAM delayed to reconnect to wireless network after PC standby with HVN
nam	CSCty62737	NAM may pick the wrong CA cert if 2 CA certs have the same public key
nam	CSCtz38714	NAM: Unable to connect with DELL Lattitude ST with builtin wifi card
nam	CSCtz59344	Anyconnect NAM: Logon module registers for PRESHUTDOWN notification
nam	CSCtz83979	NAM: WZC cannot connect to EAP-TLS networks when NAM is installed
nam	CSCua10288	NAMLOGONAGENT: Verifier stop 00000300, 00000650
nam	CSCua58106	Unable to logon if SSO registry corrupted
posture-asa	CSCsv58270	CSD:Uploading saved data.xml do not retain the advance hostscan details
posture-asa	CSCtc22654	file version, description, company name missing in few pre-dep-csd dlls
posture-asa	CSCti11151	posture service needs crash dumps
posture-asa	CSCtl45008	Incorporate a new compression algorithm for HS
posture-asa	CSCtn93915	AnyConnect process locks up Firefox lib files while running on Mac
posture-asa	CSCtt17813	Ensure error messages are logged for certain failures.
posture-asa	CSCtw16106	Improve performance with HS enabled
posture-asa	CSCtx81234	POSTURE-ASA: [ntdll!RtlpCoalesceFreeBlocks+47c] cscan.exe: c0000005
posture-asa	CSCtx81270	POSTURE-ASA: [cscan!hs_transport_free+20] cscan.exe: (Crash 32bit)
posture-asa	CSCty46078	HostScan failure prevents the connection to bxb alpha headend
posture-asa	CSCty53098	Hostcan 3.0.5075 fails to detect FW/AV/AS when using AC 2.5 on MAC OS
posture-asa	CSCty54487	CSD: Add Products screen is blank when configuring AdvEndPt from MAC OS

Component	Identifier	Headline
posture-asa	CSCty58124	Hostscan takes too long to perform KB (Hotfix) query the first time.
posture-asa	CSCtz56733	XSS vulnerability within Cisco Host Scan package
posture-asa	CSCtz81113	HS should re-use SSL sessions wherever possible
posture-asa	CSCtz81525	Linux: HS crashes on load of unsigned libcurl.so
posture-asa	CSCtz86875	Posture module has significant performance problems
posture-asa	CSCtz87681	Upgrade to OPSWAT 3.5.1058.2
posture-asa	CSCtz87701	HS should not verify file signatures for system files
posture-asa	CSCtz87869	HS should cache manifest data for the duration of a run.
posture-asa	CSCtz99890	Upgrade OPSWAT version 3.5.1427.2
posture-asa	CSCua05814	HS should remove unnecessary HEAD requests to the ASA.
posture-asa	CSCua09922	HostScan unnecessarily contacts the ASA after login
posture-asa	CSCua33887	cscan.exe crashed
posture-asa	CSCua60981	csdm checkin for CSCty54487
posture-asa	CSCua77558	cscan.exe is leaking memory
posture-asa	CSCub05542	Weblaunch for Hostscan/CSD does not work against windows 8
posture-asa	CSCub09138	Support for MC OSX 10.8
posture-asa	CSCub19055	Host Scan initialization error causes a failure on Windows 8 and Windows XP
posture-asa	CSCub27707	memory leaks in ciscod under certain Hostscan settings
profile-editor	CSCty27139	Update JRE that's shipped inside the PE installer to use the latest
profile-editor	CSCua23822	Preserve some hidden profile entries
scansafe	CSCtn49062	Statistics -Date/Time format should be in Japanese when client OS is JPN
scansafe	CSCtu43008	Automatic tower selection may take 20min to complete
scansafe	CSCtx15790	Websec status not updated for invalid license key when tower unreachable
scansafe	CSCtx35783	Websec stat sh license=unknown w/o license or no.wso and config deleted
scansafe	CSCtz23698	Display TND message even when websec was not able to verify license yet
scansafe	CSCua52925	not able to browse to any website after websec service stop
scansafe	CSCua76311	OSX: WebSecurity agent crash on service stop
scansafe	CSCub21325	upgrade from 3.0.2 to 3.0.8 cause the windows xp screen flickering
vpn	CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says "Configuring IPv6 system..."

Component	Identifier	Headline
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCti35748	AC SCEP enrollment fails over IPv6-in-IPv4 connection-client disconnect
vpn	CSCtn00418	Make the client resilient to network stability issues
vpn	CSCtr00535	Anyconnect fails to disconnect quickly when CAC card removed
vpn	CSCtr15376	GSS-DNS: WebLaunch/WebInstall fails when using the ASA's GSS FQDN
vpn	CSCtr46178	Tech Debt: Rework if statements in NetEnv::analyzeHttpResponse
vpn	CSCtt31972	VPN: AC unable enroll to local CA unless tunnel-group-list is enabled
vpn	CSCtu18520	Always-On with Fail Close able to contact the ASA but still locked down
vpn	CSCtw37962	IKEv2 - take care of smart card removal and tunnel disconnect
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	CSCty30264	VPN Stats in the message log randomly is empty
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	CSCtz13419	AnyConnect keeps trying to connect after failed IPsec connection
vpn	CSCtz28852	IKEv2 connections doing DNS resolution for proxies when not required
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	CSCtz94143	Anyconnect conflicts with Pow causing OS X to lock up after VPN connect
vpn	CSCua02849	Use primary ASA in LB cluster for IPSec Always On profile check
vpn	CSCua16483	VPN connection fails with Novatel 4G card (Win7)

Component	Identifier	Headline
vpn	CSCua21152	base-64 decode routine fails to decode certain sizes of encoded blocks
vpn	CSCua35433	Anyconnect:IP addr in profile causes Always-On/Connection to fail
vpn	CSCua47614	Mac & Linux: IPsec doesn't prompt for 'Untrusted VPN Server' - SSL does
vpn	CSCub16073	Hostscan: CERTIFICATE_ERROR_UNEXPECTED on Ubuntu 10.04
vpn	CSCub40092	AnyConnect cannot handle large messages for IKEv2
win-vpn-client	CSCua28747	Legacy VPN client subject to local priv-escalation DLL load attack

Caveats Open in Release 3.0.10055

Component	Identifier	Headline
aaa-ipsec	CSCts29023	AC IKEv2 conn failure message should indicate no IP address assigned
aaa-webvpn	CSCts28999	AC SSL message when no IP address available needs changes
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
api	CSCtz92140	Anyconnect 3.x may display incorrect gateway in established to field
certificate	CSCtz78738	NSS Cert Store: NSS_InitReadWrite fails on Ubuntu 12
certificate	CSCuc07598	Sort proper EKU certificates to be first
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, NAM or UI open
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCts96212	AnyConnect Stuck at Reconnecting
core	CSCtv00449	PAC proxy settings not honored by Agent in WebLaunch case
core	CSCua31665	Status command doesn't work on Ubuntu
dart	CSCts69478	DART Doesn't Grab the Latest Windows Events
doc	CSCtr61978	DOC: GSS-DNS TTL should be greater than VPN connect time w/ client proxy
doc	CSCtx70754	AnyConnect 3.0 fails to connect from CSD vault
doc	CSCtz02599	DOC:HostScan: 3rd party client-server products are not supported

Component	Identifier	Headline
doc	CSCua89081	DOC: Anyconnect requires specific Extended Key Usage in client certs
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCts64361	Launch AnyConnect UI automatically for WebSecurity only installs on OS X
download_install	CSCtz84437	Connection fails when upgrading from 3.0 connecting to a 3.1 headend
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtl75601	Incorrect ICON shown when certificate warning displayed,gui not notified
hostscan	CSCsz67469	Hostscan with Secure Vault fails to detect Service Pack on 64-bit Vista
network access manager	CSCtl54461	NAM: lan OneXEnforced policy interferes with IP acquisition
network access manager	CSCuc13862	Network Access Manager: Windows 8 Machine Auth not working
posture-asa	CSCtc12807	"Disable Cancel Button" should not appear in the management plugin
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch
posture-asa	CSCte15402	Session cache created 0~30 secs after logon is not cleaned Mac 10.6.x.
posture-asa	CSCtf40994	CSD 3.5 Cache Cleaner termination, long delay in closing browser
posture-asa	CSCtg68119	CSD: Cache Cleaner fails to clear the FF browser history
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	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
posture-asa	CSCtx45701	HostScan is consumming large amounts of CPU time
posture-asa	CSCtz70911	Pre-login assessment w/ SBL and IKEv2 fails for certain registry checks
posture-asa	CSCua31894	Microsoft Forefront Endpoint Protection 2010 Not Detected By Hostscan
ssa	CSCti90824	Seamless Secure Access - initial development of library, api and infra
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf60851	Network access not being displayed during reconnects
vpn	CSCtf63783	VPN connection failed because "CSD isn't installed..."
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal

Component	Identifier	Headline
vpn	CSCtg58360	Always-On profile is deleted if connecting as a user that has no profile
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth13596	AC30 SCEP - combine similar message dialogs into one
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCti78913	AC displays the Pre-Login error twice
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - can't log in
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays "On a Trusted Network"
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn74489	Can't WebLaunch/Install on Ubuntu if using Proxy Server & Ignored Hosts
vpn	CSCto31503	OGS calculations are not occuring
vpn	CSCtq29607	Host Scan failures with TND enabled right after an upgrade
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCtr59999	GSS-DNS: Connected through a Public proxy, wrong Server Address in Stats
vpn	CSCtr75134	After new install -not able to establish a connection- reconnect it's OK
vpn	CSCts29059	AC agent sometimes terminates after failed conn where no IP address avai
vpn	CSCts44842	Use non-windows untrusted cert banner logic for SBL and machine certs
vpn	CSCtu18520	Always-On with Fail Close able to contact the ASA but still locked down
vpn	CSCtx08124	GUI simply closes w/no error when using a proxy server w/Digest Auth
vpn	CSCtx74050	IPsec: Private proxy server gets truncated & wrong port - SSL OK
vpn	CSCty61386	AC cannot modify ip forwarding table when VPN is over 2nd interface
vpn	CSCty77231	Anyconnect ikev2 should ignore http-url cert payload
vpn	CSCtz86407	Recieving unexpected cert behind captive portal, connection not allowed
vpn	CSCua36934	Using Firefox 12.0 and 13.0 throws fatal error on Linux

Component	Identifier	Headline
vpn	CSCub42978	Backup Server list fails using IPSec
web	CSCua79260	Anyconnect web-launch fails on Linux OS
vpn	CSCuc00047	VPN tunnel cannot be established via wireless (Windows 8 Pro)

AnyConnect 3.0.08066 Caveats

Caveats Resolved by Release 3.0.08066

Table 6 Caveats resolved by AnyConnect Release 3.0.08066

Component	Identifier	Headline
certificate	CSCua86863	Certificate verification should use user context first on Windows
core	CSCtn99697	Need to sign AnyConnect shared libraries on Linux, Darwin, etc
gui	CSCua32256	Login prompt shown/closed repeatedly after discarding error popup
hostscan	CSCtz64181	Add support for Microsoft Essentials AV Version 4
posture-hs	CSCua97239	MSE 4.x Data File time is not available (opswat upgrade)

Caveats Open in Release 3.0.08066

Table 7 Caveats open in AnyConnect Release 3.0.08066

Component	Identifier	Headline
aaa-ipsec	CSCts29023	AC IKEv2 conn failure message should indicate no IP address assigned
aaa-webvpn	CSCts28999	AC SSL message when no IP address available needs changes
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
api	CSCtz92140	AnyConnect 3.x may display incorrect gateway in established to field
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCts13436	Connection failed due to code signing CRL being unreachable
certificate	CSCty94486	IKEV2 certificate failure debugs are not verbose enough
certificate	CSCtz78738	NSS Cert Store: NSS_InitReadWrite fails on Ubuntu 12
certificate	CSCtz83719	SCEP enrollment fails if CA doesn't send complete cert chain
certificate	CSCuc07598	Sort proper EKU certificates to be first

Component	Identifier	Headline
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, NAM or UI open
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCtv00449	PAC proxy settings not honored by Agent in WebLaunch case
core	CSCty30281	AnyConnect may consume more than one session slot per connection
core	CSCtz72727	AnyConnect fails to parse PAC correctly with bluecoat proxy
dart	CSCts00164	DART file selection option for “General Information” does not work
dart	CSCua26927	DART creates files w/ wrong information for nonexistent Event logs
dart	CSCua31730	DART on Linux showing folders as zero bytes inside the Archive manager
doc	CSCtr61978	DOC: GSS-DNS TTL should be greater than VPN connect time w/ client proxy
doc	CSCts96212	AnyConnect Stuck at Reconnecting
doc	CSCtx70754	AnyConnect 3.0 fails to connect from CSD vault
doc	CSCtz02599	DOC:HostScan: 3rd party client-server products are not supported
doc	CSCua28747	Legacy VPN client subject to local priv-escalation DLL load attack
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCtk99993	weblaunch deploy UAC displays unknown publisher on Windows 7
download_install	CSCts51839	AnyConnect 3.0 Pre-Deployment fails on Linux machines
download_install	CSCts64361	Launch AnyConnect UI automatically for WebSecurity only installs on OS X
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCtl75601	Incorrect ICON shown when certificate warning displayed,gui not notified
hostscan	CSCsx78621	Hostscan log does not get overwritten with Secure Vault
hostscan	CSCsz67469	Hostscan with Secure Vault fails to detect Service Pack on 64-bit Vista
network access manager	CSCtl54461	NAM: lan OneXEnforced policy interferes with IP acquisition
network access manager	CSCto05313	EAP-FAST:user authorization PAC issue
network access manager	CSCto95207	NAM: password protected certificates do not work

Component	Identifier	Headline
network access manager	CSCtw47024	NAM: Cert authentication does not work with Entrust Security Store
network access manager	CSCty23188	NAM: Does not re-enable MS to manage adapter when no wireless config set
network access manager	CSCty62737	NAM may pick the wrong CA cert if 2 CA certs have the same subject-name
network access manager	CSCtz21260	NAM: RDP fails on second connection attempt
network access manager	CSCtz38831	NAM: After resume no wireless adapters available in NAM with Intel card
posture-asa	CSCtc12807	“Disable Cancel Button” should not appear in the management plugin
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch
posture-asa	CSCte15402	Session cache created 0~30 secs after logon is not cleaned Mac 10.6.x.
posture-asa	CSCtf40994	CSD 3.5 Cache Cleaner termination, long delay in closing browser
posture-asa	CSCtf70014	CSD: Hostscan reports incorrect time since last AV update
posture-asa	CSCtg68119	CSD: Cache Cleaner fails to clear the FF browser history
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	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
posture-asa	CSCtw16106	Improve performance with HS enabled
posture-asa	CSCtx45701	HostScan is consuming large amounts of CPU time
posture-asa	CSCty53098	HostScan 3.0.5075 fails to detect FW/AV/AS when using AC 2.5 on Mac OS X
posture-asa	CSCtz70911	Pre-login assessment w/ SBL and IKEv2 fails for certain registry checks
posture-asa	CSCua31894	Microsoft Forefront Endpoint Protection 2010 Not Detected By Hostscan
ssa	CSCti90824	Seamless Secure Access - initial development of library, api and infra
ssa	CSCtj86498	SSA - Unicoi Network Stack Assertion When Stressed (netperf)
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says "Configuring IPv6 system..."

Component	Identifier	Headline
vpn	CSCtf60851	Network access not being displayed during reconnects
vpn	CSCtf63783	VPN connection failed because "CSD isn't installed..."
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg45671	Implement bidirectional and outbound FW rules for XP
vpn	CSCtg58360	Always-On profile is deleted if connecting as a user that has no profile
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth13596	AC30 SCEP - combine similar message dialogs into one
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCti35748	AC SCEP enrollment fails over IPv6-in-IPv4 connection-client disconnect
vpn	CSCti78913	AC displays the Pre-Login error twice
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - can't log in
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays "On a Trusted Network"
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn00418	Make the client resilient to network stability issues
vpn	CSCtn74489	Can't WebLaunch/Install on Ubuntu if using Proxy Server & Ignored Hosts
vpn	CSCto31503	OGS calculations are not occuring
vpn	CSCtq29607	Host Scan failures with TND enabled right after an upgrade
vpn	CSCtr00535	AnyConnect fails to disconnect quickly when CAC card removed
vpn	CSCtr15376	GSS-DNS: WebLaunch/WebInstall fails when using the ASA's GSS FQDN
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCts29059	AC agent sometimes terminates after failed conn where no IP address avai

Component	Identifier	Headline
vpn	CSCts44842	Use non-windows untrusted cert banner logic for SBL and machine certs
vpn	CSCtu18520	Always-On with Fail Close able to contact the ASA but still locked down
vpn	CSCtw37962	IKEv2 - take care of smart card removal and tunnel disconnect
vpn	CSCtx08124	GUI simply closes w/no error when using a proxy server w/Digest Auth
vpn	CSCtx35616	launching tunnel connection everytime dhcp renews same IP
vpn	CSCty36741	AnyConnect 3.0.4235 on RHEL 5.x and 6.x cannot browse after connecting
vpn	CSCty61386	AC cannot modify ip forwarding table when VPN is over 2nd interface
vpn	CSCty77231	AnyConnect ikev2 should ignore http-url cert payload
vpn	CSCty89947	AnyConnect MacOSX connection move Reconnecting state and never come up
vpn	CSCtz28852	IKEv2 connections doing DNS resolution for proxies when not required
vpn	CSCtz29197	AnyConnect PROMPTS user to allow accepting untrusted certs by default
vpn	CSCtz59756	AlwaysOn Fail Close does not allow user to login behind ATTWifi @ Hilton
vpn	CSCtz79311	OS X Panic - DEPRECATED method ipfw used to set our FW rules
vpn	CSCtz94143	AnyConnect conflicts with Pow causing OS X to lock up after VPN connect
vpn	CSCua35433	AnyConnect IKEv2 :IP addr in profile causes Always-On/Connection to fail
vpn	CSCua36934	Using Firefox 12.0 and 13.0 throws fatal error on Linux

AnyConnect 3.0.08057 Caveats

Caveats Resolved by Release 3.0.08057

Table 8 Caveats resolved by AnyConnect Release 3.0.08057

Component	Identifier	Headline
api	CSCty80134	AnyConnect COM API broken on Windows XP platform
certificate	CSCtz26985	IPsec does not perform certificate Name Checks
certificate	CSCtz29379	Certificate verification using IP when connection uses FQDN

Table 8 Caveats resolved by AnyConnect Release 3.0.08057

Component	Identifier	Headline
certificate	CSCtz29470	WebLaunch of IPsec does not perform certificate Name Checks
download_install	CSCtw47523	Downloader remote code vulnerability: Not Validating Manifest Origin
download_install	CSCtw48681	Downloader remote code vulnerability: ActiveX Not Checking Timestamp
download_install	CSCty45925	One version of the Java applet download does not check signatures
Network Access Manager	CSCtz29041	NAM: Upgrading from CSSC on Vista to NAM breaks WPA-PSK networks
Network Access Manager	CSCtz83979	NAM: WZC cannot connect to EAP-TLS networks when NAM is installed
posture-asa	CSCtx74235	CSD: Downloaders/ActiveX to fix validation of downloaded code
telemetry	CSCty51861	Third-party Microsoft Detours library updated
vpn	CSCty01670	vpnagentd process crashes with specific packet
vpn	CSCtz17774	AnyConnect does not work when a single RA cert is sent with SCEP-Proxy

Caveats Open in Release 3.0.08057

Table 9 Caveats open in AnyConnect Release 3.0.08057

Component	Identifier	Headline
aaa-ipsec	CSCts29023	AC IKEv2 conn failure message should indicate no IP address assigned
aaa-webvpn	CSCts28999	AC SSL message when no IP address available needs changes
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
api	CSCtz92140	AnyConnect 3.x may display incorrect gateway in established to field
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCts13436	Connection failed due to code signing CRL being unreachable
certificate	CSCty94486	IKEV2 certificate failure debugs are not verbose enough
certificate	CSCtz78738	NSS Cert Store: NSS_InitReadWrite fails on Ubuntu 12
certificate	CSCtz83719	SCEP enrollment fails if CA doesn't send complete cert chain
certificate	CSCuc07598	Sort proper EKU certificates to be first

Component	Identifier	Headline
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, NAM or UI open
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCtv00449	PAC proxy settings not honored by Agent in WebLaunch case
core	CSCty30281	AnyConnect may consume more than one session slot per connection
core	CSCtz72727	AnyConnect fails to parse PAC correctly with bluecoat proxy
dart	CSCts00164	DART file selection option for “General Information” does not work
dart	CSCua26927	DART creates files w/ wrong information for nonexistent Event logs
dart	CSCua31730	DART on Linux showing folders as zero bytes inside the Archive manager
doc	CSCtr61978	DOC: GSS-DNS TTL should be greater than VPN connect time w/ client proxy
doc	CSCts96212	AnyConnect Stuck at Reconnecting
doc	CSCtx70754	AnyConnect 3.0 fails to connect from CSD vault
doc	CSCtz02599	DOC:HostScan: 3rd party client-server products are not supported
doc	CSCua28747	Legacy VPN client subject to local priv-escalation DLL load attack
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCtk99993	weblaunch deploy UAC displays unknown publisher on Windows 7
download_install	CSCts51839	AnyConnect 3.0 Pre-Deployment fails on Linux machines
download_install	CSCts64361	Launch AnyConnect UI automatically for WebSecurity only installs on OS X
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCtl75601	Incorrect ICON shown when certificate warning displayed,gui not notified
hostscan	CSCsx78621	Hostscan log does not get overwritten with Secure Vault
hostscan	CSCsz67469	Hostscan with Secure Vault fails to detect Service Pack on 64-bit Vista
network access manager	CSCtl54461	NAM: lan OneXEnforced policy interferes with IP acquisition
network access manager	CSCto05313	EAP-FAST:user authorization PAC issue
network access manager	CSCto95207	NAM: password protected certificates do not work

Component	Identifier	Headline
network access manager	CSCtw47024	NAM: Cert authentication does not work with Entrust Security Store
network access manager	CSCty23188	NAM: Does not re-enable MS to manage adapter when no wireless config set
network access manager	CSCty62737	NAM may pick the wrong CA cert if 2 CA certs have the same subject-name
network access manager	CSCtz21260	NAM: RDP fails on second connection attempt
network access manager	CSCtz38831	NAM: After resume no wireless adapters available in NAM with Intel card
posture-asa	CSCtc12807	“Disable Cancel Button” should not appear in the management plugin
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch
posture-asa	CSCte15402	Session cache created 0~30 secs after logon is not cleaned Mac 10.6.x.
posture-asa	CSCtf40994	CSD 3.5 Cache Cleaner termination, long delay in closing browser
posture-asa	CSCtf70014	CSD: Hostscan reports incorrect time since last AV update
posture-asa	CSCtg68119	CSD: Cache Cleaner fails to clear the FF browser history
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	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
posture-asa	CSCtw16106	Improve performance with HS enabled
posture-asa	CSCtx45701	HostScan is consuming large amounts of CPU time
posture-asa	CSCty53098	Hostscan 3.0.5075 fails to detect FW/AV/AS when using AC 2.5 on Mac OS X
posture-asa	CSCtz70911	Pre-login assessment w/ SBL and IKEv2 fails for certain registry checks
posture-asa	CSCua31894	Microsoft Forefront Endpoint Protection 2010 Not Detected By Hostscan
ssa	CSCti90824	Seamless Secure Access - initial development of library, api and infra
ssa	CSCtj86498	SSA - Unicoi Network Stack Assertion When Stressed (netperf)
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says “Configuring IPv6 system...”

Component	Identifier	Headline
vpn	CSCtf60851	Network access not being displayed during reconnects
vpn	CSCtf63783	VPN connection failed because “CSD isn't installed...”
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg45671	Implement bidirectional and outbound FW rules for XP
vpn	CSCtg58360	Always-On profile is deleted if connecting as a user that has no profile
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth13596	AC30 SCEP - combine similar message dialogs into one
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCti35748	AC SCEP enrollment fails over IPv6-in-IPv4 connection-client disconnect
vpn	CSCti78913	AC displays the Pre-Login error twice
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - can't log in
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays “On a Trusted Network”
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn00418	Make the client resilient to network stability issues
vpn	CSCtn74489	Can't WebLaunch/Install on Ubuntu if using Proxy Server & Ignored Hosts
vpn	CSCto31503	OGS calculations are not occuring
vpn	CSCtq29607	Host Scan failures with TND enabled right after an upgrade
vpn	CSCtr00535	AnyConnect fails to disconnect quickly when CAC card removed
vpn	CSCtr15376	GSS-DNS: WebLaunch/WebInstall fails when using the ASA's GSS FQDN
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCts29059	AC agent sometimes terminates after failed conn where no IP address avai

Component	Identifier	Headline
vpn	CSCts44842	Use non-windows untrusted cert banner logic for SBL and machine certs
vpn	CSCtu18520	Always-On with Fail Close able to contact the ASA but still locked down
vpn	CSCtw37962	IKEv2 - take care of smart card removal and tunnel disconnect
vpn	CSCtx08124	GUI simply closes w/no error when using a proxy server w/Digest Auth
vpn	CSCtx35616	launching tunnel connection everytime dhcp renews same IP
vpn	CSCty36741	AnyConnect 3.0.4235 on RHEL 5.x and 6.x cannot browse after connecting
vpn	CSCty61386	AC cannot modify ip forwarding table when VPN is over 2nd interface
vpn	CSCty77231	AnyConnect ikev2 should ignore http-url cert payload
vpn	CSCty89947	AnyConnect MacOSX connection move Reconnecting state and never come up
vpn	CSCtz28852	IKEv2 connections doing DNS resolution for proxies when not required
vpn	CSCtz29197	AnyConnect PROMPTS user to allow accepting untrusted certs by default
vpn	CSCtz59756	AlwaysOn Fail Close does not allow user to login behind ATTWifi @ Hilton
vpn	CSCtz79311	OS X Panic - DEPRECATED method ipfw used to set our FW rules
vpn	CSCtz94143	AnyConnect conflicts with Pow causing OS X to lock up after VPN connect
vpn	CSCua35433	AnyConnect IKEv2 :IP addr in profile causes Always-On/Connection to fail
vpn	CSCua36934	Using Firefox 12.0 and 13.0 throws fatal error on Linux

AnyConnect 3.0.07059 Caveats

Caveats Resolved by Release 3.0.07059

Table 10 lists the Severity 1–3 caveats that AnyConnect Secure Mobility Client 3.0.07059 resolves. The table sorts the caveats by AnyConnect component, then by identifier.

Table 10 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.07059

Component	Identifier	Headline
api	CSCtu72336	"Connection is in Progress" - User is Unable to Initiate Connection
api	CSCtw84179	AC 3.0 removes leading spaces from HostEntry HostName

Table 10 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.07059

Component	Identifier	Headline
api	CSCtx15602	No valid certificates available for authentication due to timeout errors
api	CSCty45409	AC on Win7 GUI minimize call made before the connection is established
automation	CSCtc70565	CSSC client did not resend out its credential after timeout.
core	CSCtu00758	AnyConnect on Mac OS X and Split-include enabled
customer-use	CSCtq24128	Prelogin Certificate Check (Domain Component) fails on Mac OS X
customer-use	CSCtr27865	Observing slow throughput when using AnyConnect Mac client
customer-use	CSCts50389	multiple prompts via standard EAP are not handled correctly
customer-use	CSCtr75253	csdlib.dll is corrupted and size of 0K
customer-use	CSCtq75832	AnyConnect does not perform auto route correction on Mac/Linux
customer-use	CSCtq42832	CSD 3.6 takes noticeably longer to connect than CSD 3.5
customer-use	CSCtr03991	Slower / inconsistent connection times when Posture is enabled
customer-use	CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
customer-use	CSCtq62671	network access manager: fails to retrieve certificates on safenet usb tokens
customer-use	CSCtn56376	AC unable to access the root ca in firefox using Linux
customer-use	CSCto73820	GUI was still showing connected even though was not
customer-use	CSCts42362	Message from ASA is not displayed about password complexity requirements
customer-use	CSCtr21138	AnyConnect counters cannot be reset
customer-use	CSCts48139	DOC: AnyConnect doc for Android should have examples of cert import
customer-use	CSCtr97908	Machine authentication with 2008 AD cert template fails
customer-use	CSCtn11401	AnyConnect failures with connection, yet it is passing data
customer-use	CSCtr80410	Password may be available in clear text in RAM
customer-use	CSCts12090	AnyConnect fails when mutiple IP addr are assigned to single NIC/adapter
development	CSCte42921	Get Unresolved Gateway Address When Trying to Connect
development	CSCtk62756	Some adapters don't update the scanlist without explicit scan request
dev-test	CSCth93459	AC dialog left over after successful SCEP enrollment
dev-test	CSCti34206	AC UI stops after clicking Get Certificate button with Local CA enabled
dev-test	CSCta83106	Routing logic for reconnects needs to ignore invalid routes
func-test	CSCtk68610	AC Get Certificate button not working -Local CA on ASA not usable

Table 10 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.07059

Component	Identifier	Headline
func-test	CSCtr28687	IKEv2-IPSec: Downloader (SSL) isn't using configured public Proxy Server
func-test	CSCts53001	AnyConnect fails EAP-TLS authentication when client certificate is 8k
func-test	CSCtr00334	Always-On: If ASA DNS name can't be resolved, can't select another entry
gui	CSCty55386	AnyConnect 3.0 Credentials Window Hidden
internal-use	CSCtc03052	SCEP fails in upgrade scenario
network access manager	CSCtw72917	network access manager: network access manager should be able to handle unknown/unsupported EAP types
network access manager	CSCtw78555	network access manager: Remove default identity pattern for user created networks
posture-asa	CSCtt17899	Recurring warning message on XP.
posture-asa	CSCtx06647	CSD Host Scan does not recognize RHEL 6.2 on pre-deployment
posture-asa	CSCtx34330	Hostscan 3.0.5075 does not auto-install on windows machine
posture-asa	CSCtx55184	500 MB memory leak with cscan.exe - SEP potential culprit
posture-asa	CSCtz01138	Disable file signature verification for Mac
profile-editor	CSCtx03778	PE: Can't edit Load Balancing Server List even though Always-On enabled
profile-editor	CSCty17245	network access manager PE Schema validation error for send cert using tls in tunnel
qa	CSCtg67075	Terminate Reason Displayed as Balloon with Non-cert Authentication
qa	CSCti93817	Trusted Network not detected when adapter has IPv6 DNS addresses
regression	CSCto96958	Windows 7-64 bit does not fall back to cache Cleaner
scansafe	CSCtu06814	AnyConnect won't accept complex passwords with capital letters
scansafe	CSCtu80517	WebSecApi: UI crash on system resume
scansafe	CSCtw64480	disable websec service only allow in elevated privilege command prompt
scansafe	CSCtx22204	Block site hang with /4 ip range in the static exception field
sol-test	CSCtl51029	IPv6 traffic tunneling success is inconsistent
sys-test	CSCts35238	VPN: GUI hangs after certificate enrollment
sys-test	CSCto83521	DOC: The VPN client driver encountered an error. Please restart your PC
vpn	CSCtk15816	Always On: Web Auth Required message displayed with Network access
vpn	CSCto96645	Bogus AC popup messages about having to wait a minute to restart
vpn	CSCtw61688	IPv6 client address not assigned if IPv6 disabled on tunnel interfaces

Table 10 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.07059

Component	Identifier	Headline
vpn	CSCtw66908	Long delay in boot if prev conn was not disconnected before shutdown
vpn	CSCtw75416	AnyConnect: Unable to connect using Telstra 3G card on Mac OS X
vpn	CSCtw84403	Bogus popup messages about having to wait a minute to restart
vpn	CSCtw86923	VPN: AnyConnect 3.0 ComboxBox changes name after connection
vpn	CSCtx27707	AC: inbound FW policies not working correctly
vpn	CSCtx28970	AC crashes with IE offline
vpn	CSCtx40957	Mac Lion: traffic targeting the local subnet is not tunneled
vpn	CSCtx89672	Cannot establish VPN over PPP if RAS entry's phone number is not set
vpn	CSCty02115	AnyConnect on Mac crashes with Always On and unreachable CDP

Open Caveats in Release 3.0.07059

Table 11 lists the Severity 1–3 caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Release 3.0.07059. The table sorts the caveats by AnyConnect component, then by identifier.

Table 11 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.07059

Component	Identifier	Headline
aaa-ipsec	CSCts29023	AC IKEv2 conn failure message should indicate no IP address assigned
aaa-webvpn	CSCts28999	AC SSL message when no IP address available needs changes
api	CSCtf90996	OGS selects inaccessible host
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
api	CSCtq61680	Hostscan not running with AnyConnect on 64-bit Linux Systems
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, NAM or UI open
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
dart	CSCts00164	Dart file selection option for "General Information" does not work
doc	CSCtr61978	DOC: GSS-DNS TTL should be greater than VPN connect time w/ client proxy
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake

Table 11 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.07059

Component	Identifier	Headline
download_install	CSCts51839	AnyConnect 3.0 Pre-Deployment fails on Linux machines
download_install	CSCts46682	AnyConnect Linux init script issues
download_install	CSCty42674	Wininet - incorrect windows handle passed to InternetErrorDlg
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCtl75601	Incorrect ICON shown when certificate warning displayed,gui not notified
mobile	CSCtj05702	JPN: Windows Mobile Client Status message is garbled in Connection tab
mobile	CSCtj05748	JPN: Windows mobile client Message is garbled in About tab.
mobile	CSCtq33166	Unable to send/recieve MMS messages while connected
mobile	CSCto43931	Symbian: AnyConnectVPN access point is not selectable in the Browser
network access manager	CSCto05313	EAP-FAST:user authorization PAC issue
network access manager	CSCto95207	NAM: password protected certificates do not work
network access manager	CSCtl54461	NAM: lan OneXEnforced policy interferes with IP acquisition
posture-asa	CSCsz67469	Hostscan with Secure Vault fails to detect Service Pack on 64-bit Vista
posture-asa	CSCte04839	Feedback is not provided on errors in manual launch
posture-asa	CSCte15402	Session cache created 0~30 secs after logon is not cleaned Mac 10.6.x.
posture-asa	CSCtg68119	CSD: Cache Cleaner fails to clear the FF browser history
posture-asa	CSCti24021	Posture localization PO file needs updated translation
posture-asa	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
posture-asa	CSCsx78621	Hostscan log does not get overwritten with Secure Vault
vpn	CSCtf60851	Network access not being displayed during reconnects
vpn	CSCth13596	AC30 SCEP - combine similar message dialogs into one
vpn	CSCsx71110	Non-tunneled multicast traffic not passed in split-tunnel
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says "Configuring IPv6 system..."
vpn	CSCtf63783	VPN connection failed because "CSD isn't installed..."

Table 11 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.07059

Component	Identifier	Headline
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg45671	Implement bidirectional and outbound FW rules for XP
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCtj62029	Can't establish tunnel with machine cert auth and untrusted server CA
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays "On a Trusted Network"
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn74489	Can't WebLaunch/Install on Ubuntu if using Proxy Server & Ignored Hosts
vpn	CSCto31503	OGS calculations are not occuring
vpn	CSCtq29607	Host Scan failures with TND enabled right after an upgrade
vpn	CSCts29059	AC agent sometimes terminates after failed conn where no IP address avai
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCtr00535	AnyConnect fails to disconnect quickly when CAC card removed
vpn	CSCth85648	VPN: Auth challenge window - Mac and Win ignoring CR/LF
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled
vpn	CSCsv49773	Ability to accommodate multiple head-end profiles
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCtn00418	Make the client resilient to network stability issues
vpn	CSCtr43275	AnyConnect VPN fails on Mac with MobileMe Back to my Mac enabled

AnyConnect 3.0.5080 Caveats

Caveats Resolved by Release 3.0.5080

Table 12 lists the Severity 1–3 caveats that AnyConnect Secure Mobility Client 3.0.5080 resolves. The table sorts the caveats by AnyConnect component, then by identifier.

Table 12 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
api	CSCtu09841	SCEP Enrollment Fails Due to Race Condition in API
api	CSCtt47507	getState() can cause API state to revert to connecting from connected
build-system	CSCtu39293	ProfileManifest : missing information for WebSec PE
certificate	CSCts44278	AnyConnect fails with SBL and certificates on Windows 7
certificate	CSCts60473	AnyConnect 2.5/3.0 on Linux fails with encrypted private keys
certificate	CSCts67622	AC stuck in loop with invalid cert
certificate	CSCts49178	Indefinite reconnect after RTP head-end cert was changed out
certificate	CSCto91245	AnyConnect: Non-WinX clients not sending entire cert chain
core	CSCtj80031	Reconnects over WiFi will often take upwards of 3 minutes.
core	CSCts48992	AnyConnect 3.0.3 and 3.0.4 fails to connect when AlwaysOn is enabled
core	CSCtu22163	Some Win machines fail to start acsock leading to connection failures
core	CSCts48992	AnyConnect 3.0.3 fails to connect when AlwaysOn is enabled
core	CSCtt42158	time intensive task should not occur in MainThread constructor
core	CSCts41026	Connection fails with SBL and proxies
core	CSCts80077	AnyConnect 3.0.3054 not able to reconnect with RDP session
core	CSCtu21887	Possible memory corruption during signature check
dart	CSCtr64797	DART for Mac to grab install.log
dart	CSCtq15268	DART to capture AnyConnect.mo files
doc	CSCtq41116	NAM fails to install on system with Trend Micro
doc	CSCts00157	DOC: Client is now in new directory “anyconnect” as opposed to "vpn"
doc	CSCts03036	DOC: AnyConnect Profile XML Tags/Options Are Case Sensitive
download_install	CSCts11159	vpn failed to make a connection
download_install	CSCtu37126	Linux DART uninstaller removes manifesttool when its still needed by VPN
download_install	CSCtr43764	Remove reference of 10.4+ from weblaunch installer
download_install	CSCts46419	Add default ACTransforms.xml in OS X installer
download_install	CSCti54776	installers do not check the versions of components that are installed
gui	CSCts89517	crash running vpnui under debugger with heap checks enabled
gui	CSCtr95613	GUI: [vpnui!WTL::CString::CString+2] vpnui.exe: c0000005 (Crash 32bit)
gui	CSCtt22267	AC: pop-up from tray steals application focus

Table 12 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
gui	CSCtt45030	Windows trayflyout UI does not pop to the top under certain conditions
network access manager	CSCtv18565	NAM: Credential Provider does not work with Novell CP
network access manager	CSCtw44295	NAM: CP does not work with Imprivata CP
network access manager	CSCtu10498	NAM: acnmagent.exe uses 99% CPU after reboot
network access manager	CSCts26778	WPA2 Personal AES shows security status of Open
posture	CSCtr14928	CSD: 'Trend Micro Core Protection Module' is not detected correctly
posture	CSCtr41292	CSD : Pre-login Certificate Check fails even if attributes match
posture	CSCtr45076	AntiVirus DAT file age not reported correctly by CSD
posture	CSCts53901	AC 2.5.3051 Posture Assessment Failure With CSD 3.6.185
posture	CSCtt32544	cscan.exe Memory Leak
posture	CSCtw45318	Prelogin Checks for file checks and versions are not working
posture	CSCts32184	HS:clean up persistent HostScan sessions.
posture	CSCts30355	[cscan!restore_ie_history+100] cscan.exe: c0000005 (Crash 32bit)
posture	CSCts62204	AnyConnect Fedora-Linux,hscan fails , /lib/libcurl.so not found
posture	CSCts03224	Error : Please enable Cisco Secure Desktop to configure the parameter
posture	CSCto11223	Upgrade csd from 3.5.x to 3.6.x sets the data.xml file to defaults
posture	CSCtq01504	Crash due to csd_free: Crash 32bit in vpnui.exe: c0000005 in ntdll.dll
posture	CSCtr22170	Posture Crash 32bit in vpnui.exe: in ntdll.dll due to libcsd
posture	CSCtq06895	Crash 32bit in cscan.exe: c0000005 in cscan.exe
posture	CSCtr45076	AntiVirus DAT file age not reported correctly by CSD
posture	CSCti99089	The CSD scan hangs when KSL is enabled
posture	CSCtt01571	CSD: Support for AVG 2012 Anti-virus program
posture	CSCtt35410	Trend Micro OfficeScan - DAP fails to match within Vault.
posture	CSCtr14928	CSD: 'Trend Micro Core Protection Module' is not detected correctly
posture	CSCts29161	ciscod.exe process takes a minute to end once service is stopped
posture	CSCtu10272	HostScan Warning: MD5 not found in manifest
posture	CSCts86184	Hostscan DAP check fails to detect installed Windows Hotfix

Table 12 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
posture	CSCtq02168	Errors in CSD 3.6 prelogin policy panel if reusing data.xml from CSD 3.5
posture	CSCtr00905	CSD: Host scan for processes fails if non-admin
posture	CSCts53901	AC 2.5.3051 Posture Assessment Failure With CSD 3.6.185
posture	CSCtq80972	CSD 3.6 not returning endpoint attributes when logging in with SBL
posture	CSCtr85683	Remove excessive anyconnect logging from application event viewer
posture	CSCtw70984	cscan.exe errors keep popping up modal with 3.0.5MR - CoreUtils.dll
posture-hs	CSCts04619	Hostscan image error while configuring opswat : hostscan_3.0.5003-k9.pkg
posture-hs	CSCts04619	Hostscan image error while configuring opswat : hostscan_3.0.5003-k9.pkg
profile-editor	CSCts55598	[WebSec PE] Do not allow passwords to have a space
profile-editor	CSCts14056	WebSecurity PE - Beacon Server Preferences
scansafe	CSCts86463	KDF on OSX can cause kernel panic() while performing OSMalloc with lock
scansafe	CSCtt29845	AC websec incompatible with Kaspersky AV with Beacon server
vpn	CSCtq71704	AnyConnect 3032 crashes on Mac upon connect-disconnect-connect
vpn	CSCtw44553	VPN Agent crashes with the latest 3.0.5 MR
vpn	CSCtw62208	Mac: Export Stats in the UI fails to work
vpn	CSCtw71005	TND is consistently trying to start connections with the latest 3.0.5
vpn	CSCtu42885	IKEv2 Connections fails due to error 49
vpn	CSCtu13502	Certificate Authentication doesn't work with Entrust Cert Management
vpn	CSCtq75297	Crash 32bit in vpnagent.exe: CNLMgr::SetNlmCategory
vpn	CSCtq75298	Crash 32bit in vpnagent.exe: CTimer::checkExpired
vpn	CSCts83340	An unknown termination has occurred in the client service
vpn	CSCtq71704	AnyConnect 3032 crashes on Mac upon connect-disconnect-connect
vpn	CSCts30169	AnyConnect Profile XML Values Not Being Taken Over Preferences XML
vpn	CSCtw63879	disable impersonation in cwrapper
vpn	CSCto53984	pki-crl: crl download fails when always-on enabled
vpn	CSCtt28991	Ignore expired cert during code signing verification
vpn	CSCtu24589	Mac OS X with AlwaysOn: can't reach ASA after disconnect

Table 12 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
vpn	CSCtt26527	AnyConnect 3.0.4235 password authentication fails w/ CAC Certs cached
vpn	CSCts96105	AC: Client fails to connect if local profile is different from ASA
vpn	CSCtt14822	AnyConnect blocks IPv4 connections to IPv4-mapped IPv6 addresses
vpn	CSCts72767	3.0.4 AnyConnect overwrites hosts file by hosts.ac
vpn	CSCts89212	multiple csd_init when changing tunnel groups
vpn	CSCtt08151	DTLS MTU correction takes too long
vpn	CSCts26503	The secure gateway failed to reply to a connection message & malfunction
vpn	CSCts38500	No network access after disconnect if client FW rules are configured
vpn	CSCtb92777	MSIE proxy not being set in Vista and Windows7 when no port used

Open Caveats in Release 3.0.5080

Table 13 lists the Severity 1–3 caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Release 3.0.5080. The table sorts the caveats by AnyConnect component, then by identifier.

Table 13 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
aaa-webvpn	CSCts42362	Message from ASA is not displayed about password complexity requirements
api	CSCtr75253	csdlib.dll is corrupted and size of 0K
api	CSCtf90996	OGS selects inaccessible host
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCtg67075	Terminate Reason Displayed as Balloon with Non-cert Authentication
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
api	CSCti34206	AC UI stops after clicking Get Certificate button with Local CA enabled
api	CSCtr21138	AnyConnect counters cannot be reset
api	CSCts35238	VPN: GUI hangs after certificate enrollment
api	CSCtq61680	Hostscan not running with AnyConnect on 64-bit Linux Systems
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, NAM or UI open

Table 13 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCta83106	Routing logic for reconnects needs to ignore invalid routes
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCtq75832	AnyConnect does not perform auto route correction on Mac/Linux
dart	CSCts00164	Dart file selection option for "General Information" does not work
doc	CSCto83521	DOC: The VPN client driver encountered an error. Please restart your PC
doc	CSCtr61978	DOC: GSS-DNS TTL should be greater than VPN connect time w/ client proxy
doc	CSCts48139	DOC: AnyConnect doc for Android should have examples of cert import
download_install	CSCts51839	AnyConnect 3.0 Pre-Deployment fails on Linux machines
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCtr28687	IKEv2-IPSec: Downloader (SSL) isn't using configured public Proxy Server
download_install	CSCts46682	AnyConnect Linux init script issues
gui	CSCtc03052	SCEP fails in upgrade scenario
gui	CSCte42921	Get Unresolved Gateway Address When Trying to Connect
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtf60851	Network access not being displayed during reconnects
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCth13596	AC30 SCEP - combine similar message dialogs into one
gui	CSCth93459	AC dialog left over after successful SCEP enrollment
gui	CSCtj05702	JPN: Windows Mobile Client Status message is garbled in Connection tab
gui	CSCtj05748	JPN: Windows mobile client Message is garbled in About tab.
gui	CSCth85648	GUI: Auth challenge window - Mac is missing text - Win ignoring CR/LF
gui	CSCtl75601	Incorrect ICON shown when certificate warning displayed,gui not notified
mobile	CSCtq33166	Unable to send/recieve MMS messages while connected
mobile	CSCto43931	Symbian: AnyConnectVPN access point is not selectable in the Browser
network access manager	CSCto95207	NAM: password protected certificates do not work
network access manager	CSCtc70565	CSSC client did not resend out its credential after timeout.

Table 13 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
nam	CSCtk62756	Some adapters don't update the scanlist without explicit scan request
network access manager	CSCtr97908	Machine authentication with 2008 AD cert template fails
nam	CSCts53001	AnyConnect fails EAP-TLS authentication when client certificate is 8k
network access manager	CSCtq62671	NAM: fails to retrieve certificates on safenet usb tokens
network access manager	CSCto05313	EAP-FAST:user authorization PAC issue
nam	CSCtl54461	network access manager: lan OneXEnforced policy interferes with IP acquisition
posture	CSCto96958	Windows 7-64 bit does not fall back to cache Cleaner
posture	CSCsz67469	Hostscan with Secure Vault fails to detect Service Pack on 64-bit Vista
posture	CSCte04839	Feedback is not provided on errors in manual launch
posture	CSCte15402	Session cache created 0~30 secs after logon is not cleaned Mac 10.6.x.
posture	CSCtg68119	CSD: Cache Cleaner fails to clear the FF browser history
posture	CSCti24021	Posture localization PO file needs updated translation
posture	CSCtq24128	Prelogin Certificate Check (Domain Component) fails on Mac OSX
posture	CSCtq42832	CSD 3.6 takes noticeably longer to connect than CSD 3.5
posture	CSCtr03991	Slower / inconsistent connection times when Posture is enabled
posture	CSCsx78621	Hostscan log does not get overwritten with Secure Vault
posture-hs	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
vpn	CSCtl51029	IPv6 traffic tunneling success is inconsistent
vpn	CSCtn11401	AnyConnect failures with connection, yet it is passing data
vpn	CSCsx71110	Non-tunneled multicast traffic not passed in split-tunnel
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says "Configuring IPv6 system..."
vpn	CSCtf63783	VPN connection failed because "CSD isn't installed..."
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal

Table 13 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
vpn	CSCtg45671	Implement bidirectional and outbound FW rules for XP
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCti93817	Trusted Network not detected when adapter has IPv6 DNS addresses
vpn	CSCtj62029	Can't establish tunnel with machine cert auth and untrusted server CA
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays "On a Trusted Network"
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn74489	Can't WebLaunch/Install on Linux if using Proxy Server & Ignored Hosts
vpn	CSCto31503	OGS calculations are not occuring
vpn	CSCtq29607	Host Scan failures with TND enabled right after an upgrade
vpn	CSCtr00334	Always-On: If ASA DNS name can't be resolved, can't select another entry
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCts28999	AC SSL message when no IP address available needs changes
vpn	CSCts29023	AC IKEv2 conn failure message should indicate no IP address assigned
vpn	CSCts29059	AC agent sometimes terminates after failed conn where no IP address avai
vpn	CSCtk68610	AC Get Certificate button not working -Local CA on ASA not usable
vpn	CSCtr27865	Observing slow throughput when using AnyConnect Mac client
vpn	CSCsv49773	Ability to accommodate multiple head-end profiles
vpn	CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCtn00418	Make the client resilient to network stability issues
vpn	CSCtn56376	AC unable to access the root ca in firefox using Linux
vpn	CSCto73820	GUI was still showing connected even though was not
vpn	CSCtr00535	AnyConnect fails to disconnect quickly when CAC card removed
vpn	CSCtr43275	AnyConnect VPN fails on Mac with MobileMe Back to my Mac enabled

Table 13 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.5080

Component	Identifier	Headline
vpn	CSCtr80410	Password may be available in clear text in RAM
vpn	CSCts12090	AnyConnect fails when mutiple IP addr are assigned to single NIC/adapter
vpn	CSCts50389	multiple prompts via standard EAP are not handled correctly

AnyConnect 3.0.4235 Caveats

Caveats Resolved by Release 3.0.4235

Table 14 lists the Severity 1–3 caveats that AnyConnect Secure Mobility Client 3.0.4235 resolves. The table sorts the caveats by AnyConnect component, then by identifier.

Table 14 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
api	CSCtj09831	Connect on startup setting user controllable even if disabled in profile
api	CSCtk83887	Removing Smart Cards at banner does not result in tunnel tear down
api	CSCtq46109	AnyConnect Authentication Timeout with machine certificate
api	CSCtq82541	AnyConnect client login delay for domain user login
certificate	CSCtq74054	SCEP is not initiated when using a URL (asa-IP/tunnel-group alias)
certificate	CSCtr64798	[Lion] Critical error while connecting to certain head-ends
core	CSCtr40816	AC3.0 adds route for local DHCP server to def gw w/ split tunneling
dart	CSCtn46629	DART does not collect files from localized paths
dart	CSCtn46629	DART does not collect files from localized paths
doc	CSCtr62706	Doc: AnyConnect 3.0 Release Notes IOS info should be in the IOS section
download_install	CSCtr83229	Mac OS X 10.6 - Cannot Weblaunch AnyConnect - Java : Exception in thread
download_install	CSCts64361	AnyConnect UI should start automatically for WebSecurity-only installs on Mac OS X
network access manager	CSCtr55667	NAM will not associate to network with "&" in SSID
network access manager	CSCtr63595	NAM stuck authenticating when using a wired dot1x configuration
network access manager	CSCts25984	NAM: Unable to lock of logoff of Windows PC
posture	CSCtq31755	CSD: Prelogin Check cannot check for Root certificate on MAcOS X clients

Table 14 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
posture	CSCtq92552	CSD:: HostScan fails to check LastUpdate for Microsoft Forefront AV
profile-editor	CSCtr31629	ASDM AC Profile Editor: Validates NAM profiles incorrectly
scansafe	CSCtk53053	Automatic Tower Selection code improvements
scansafe	CSCtr15005	Websec fail to filter malicious site when used with proxy not excluded
vpn	CSCtk14009	AnyConnect 2.x/3.x: Public proxy PAC URL fails to connect
vpn	CSCtk35111	AlwaysOn: Incorrect message While Reconnecting behind a Captive Portal
vpn	CSCtk48182	Java exceptions installing AC via weblaunch on Ubuntu Linux
vpn	CSCtl74125	IKEv2: Can't install opt modules if client-services has non-default port
vpn	CSCtq02141	AnyConnect DNS Issue when ISP DNS is on same subnet as Public IP
vpn	CSCtq17339	anyconnect 3.0.1047-unable to validate certificate chain when using IKEV2
vpn	CSCtq65063	Infinite reconnect loop with certain data card connection manager
vpn	CSCtq95503	VPN connection fails via data card in 4G mode
vpn	CSCtr20634	AC: Split-exclude route not working when overlapping a link-level route
vpn	CSCtr21400	AnyConnect 3.0 profile selection missing after successful connection
vpn	CSCtr24100	vpnagent crash with split-DNS enabled
vpn	CSCtr48748	AnyConnect 3.0 blocks connection to the tunnel ip with AlwaysOn enabled
vpn	CSCtr59361	Proxy settings not re-determined on reconnect
vpn	CSCts05914	Limited broadcast should be allowed in the clear with split-include
vpn	CSCts11510	AnyConnect doesn't create a default route for IPv6 on Lion
vpn	CSCts35033	server cert CRL check can fail if proxy settings are enabled

Open Caveats in Release 3.0.4235

Table 15 lists the Severity 1–3 caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Release 3.0.4235. The table sorts the caveats by AnyConnect component, then by identifier.

Table 15 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
api	CSCtf73236	AnyConnect constantly checking for localization file.
api	CSCtf90996	OGS selects inaccessible host

Table 15 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCtg67075	Terminate Reason Displayed as Balloon with Non-cert Authentication
api	CSCth28802	Move Logic for Enabling 'Disconnect' Button from GUI to API
api	CSCti34206	AC UI stops after clicking Get Certificate button with Local CA enabled
api	CSCtq26388	API: AC 3.0 GUI shows wrong hostname when connected
api	CSCtq61680	Hostscan not running with AnyConnect on 64-bit Linux Systems
api	CSCtq62860	[Lion] OS X 10.7 Client crashes during connection attempt
api	CSCtr21138	AnyConnect counters cannot be reset
api	CSCtr53998	FoxT/TFS Desktop automatically launching when VPN is initiated
api	CSCtr75253	csdlib.dll is corrupted and size of 0K
api	CSCtr80031	MAC GUI crash
api	CSCts35238	VPN: GUI hangs after certificate enrollment
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCtr00565	AnyConnect 3.0 fails clear PIN for SafeNet Smart Card
certificate	CSCts44278	AnyConnect fails with SBL and certificates on Windows 7
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, NAM or UI open
core	CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCta83106	Routing logic for reconnects needs to ignore invalid routes
core	CSCtj80031	Reconnects over WiFi will often take upwards of 3 minutes.
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCtq75832	AnyConnect does not perform auto route correction on Mac/Linux
core	CSCts48992	AnyConnect 3.0.3 fails to connect when AlwaysOn is enabled
dart	CSCts00164	Dart file selection option for “General Information” does not work
doc	CSCtl21430	DOC: AnyConnect 2.5 admin guide should include firewall config examples

Table 15 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
doc	CSCto83521	DOC: The VPN client driver encountered an error. Please restart your PC
doc	CSCtq41116	NAM fails to install on system with Trend Micro
doc	CSCtr61978	DOC: GSS-DNS Time To Live (TTL) should be greater than VPN connect time
doc	CSCts00157	Client is now in new directory “anyconnect” as opposed to "vpn"
doc	CSCts03036	DOC: AnyConnect Profile XML Tags/Options Are Case Sensitive
doc	CSCts43924	Doc: AnyConnect 2.4 for Android doesn't support “Private-side proxy”
doc	CSCts48139	DOC: AnyConnect doc for Android should have examples of cert import
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCtn53685	Add support for installer to copy profiles over a mapped network drive
download_install	CSCtr28687	IKEv2-IPSec: Downloader (SSL) isn't using configured public Proxy Server
download_install	CSCts46682	AnyConnect Linux init script issues
download_install	CSCts51839	AnyConnect 3.0 Pre-Deployment fails on Linux machines
gui	CSCtc03052	SCEP fails in upgrade scenario
gui	CSCte42921	Get Unresolved Gateway Address When Trying to Connect
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtf60851	Network access not being displayed during reconnects
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCth13596	AC30 SCEP - combine similar message dialogs into one
gui	CSCth85648	GUI: Auth challenge window - Mac is missing text - Win ignoring CR/LF
gui	CSCth93459	AC dialog left over after successful SCEP enrollment
gui	CSCtj05702	JPN: Windows Mobile Client Status message is garbled in Connection tab
gui	CSCtj05748	JPN: Windows mobile client Message is garbled in About tab.
gui	CSCtl75601	Incorrect ICON shown when certificate warning displayed,gui not notified
gui	CSCts28132	2.5 only: AnyConnect localization does not display some characters
gui	CSCts42362	Message from ASA is not displayed about password complexity requirements

Table 15 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
installer	CSCto43931	Symbian: AnyConnectVPN access point is not selectable in the Browser
mobile	CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
mobile	CSCtq33166	Unable to send/receive MMS messages while connected
network access manager	CSCtc70565	CSSC client did not resend out its credential after timeout.
network access manager	CSCtk62756	Some adapters don't update the scanlist without explicit scan request
network access manager	CSCtl54461	NAM: lan OneXEnforced policy interferes with IP acquisition
network access manager	CSCto05313	EAP-FAST:user authorization PAC issue
network access manager	CSCto95207	NAM: password protected certificates do not work
network access manager	CSCtq62671	NAM: fails to retrieve certificates on safenet usb tokens
network access manager	CSCtr97908	Machine authentication with 2008 AD cert template fails
nam	CSCts53001	AnyConnect fails EAP-TLS authentication when client certificate is 8k
posture	CSCsx78621	Hostscan log does not get overwritten with Secure Vault
posture	CSCsz67469	Hostscan with Secure Vault fails to detect Service Pack on 64-bit Vista
posture	CSCte04839	Feedback is not provided on errors in manual launch
posture	CSCte15402	Session cache created 0~30 secs after logon is not cleaned Mac 10.6.x.
posture	CSCtg68119	CSD: Cache Cleaner fails to clear the FF browser history
posture	CSCti24021	Posture localization PO file needs updated translation
posture	CSCto87181	CSD not detecting Last Update of Kaspersky for Mac OS X
posture	CSCto96958	Windows 7-64 bit does not fall back to cache Cleaner
posture	CSCtq24128	Prelogin Certificate Check (Domain Component) fails on Mac OSX
posture	CSCtq42832	CSD 3.6 takes noticeably longer to connect than CSD 3.5
posture	CSCtr03991	Slower / inconsistent connection times when Posture is enabled
posture	CSCtr14928	CSD: 'Trend Micro Core Protection Module' is not detected correctly
posture	CSCtr26427	CSD: Posture assessment fail on certain Win 7 64bit machine
posture	CSCtr39580	JPN CSD: Host Scan Registry MBCS Registry name is not working

Table 15 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
posture	CSCtr39606	JPN CSD: Host Scan File MBCS File name is not working
posture	CSCtr39613	JPN CSD: Host Scan MBCS Folder name is not working
posture	CSCtr39630	JPN CSD: Host Scan Process MBCS name is not working
posture	CSCtr41292	CSD : Pre-login Certificate Check fails even if attributes match
posture	CSCtr45076	AntiVirus DAT file age not reported correctly by CSD
posture	CSCts53901	AC 2.5.3051 Posture Assessment Failure With CSD 3.6.185
posture-hs	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
posture-hs	CSCts04619	Hostscan image error while configuring opswat : hostscan_3.0.5003-k9.pkg
vpn	CSCsv49773	Ability to accommodate multiple head-end profiles
vpn	CSCsx71110	Non-tunneled multicast traffic not passed in split-tunnel
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says “Configuring IPv6 system...”
vpn	CSCtf63783	VPN connection failed because “CSD isn't installed...”
vpn	CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
vpn	CSCtg01525	AnyConnect should have clear description for each error msg
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg45671	Implement bidirectional and outbound FW rules for XP
vpn	CSCtg61388	Unable to Access Captive Portal Login Page While Reconnecting
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCti93817	Trusted Network not detected when adapter has IPv6 DNS addresses
vpn	CSCtj62029	Can't establish tunnel with machine cert auth and untrusted server CA
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download

Table 15 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays “On a Trusted Network”
vpn	CSCtk68610	AC Get Certificate button not working -Local CA on ASA not usable
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23155	AnyConnect SBL fails with Novell netware
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtl51029	IPv6 traffic tunneling success is inconsistent
vpn	CSCtn00418	Make the client resilient to network stability issues
vpn	CSCtn11401	AnyConnect failures with connection, yet it is passing data
vpn	CSCtn56376	AC unable to access the root ca in firefox using Linux
vpn	CSCtn74489	Can't WebLaunch/Install on Linux if using Proxy Server & Ignored Hosts
vpn	CSCto31503	OGS calculations are not occurring
vpn	CSCto73820	GUI was still showing connected even though was not
vpn	CSCtq29607	Host Scan failures with TND enabled right after an upgrade
vpn	CSCtq54703	Many reconnects w DSL / Always-On
vpn	CSCtq71704	AnyConnect 3032 crashes on Mac upon connect-disconnect-connect
vpn	CSCtr00334	Always-On: If ASA DNS name can't be resolved, can't select another entry
vpn	CSCtr00535	AnyConnect fails to disconnect quickly when CAC card removed
vpn	CSCtr00686	Implement Scripting for CP detection
vpn	CSCtr27865	Observing slow throughput when using AnyConnect Mac client
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCtr43275	AnyConnect VPN fails on Mac with MobileMe Back to my Mac enabled
vpn	CSCtr75228	AC: VPN Client Driver has encountered a error
vpn	CSCtr75276	Experiencing frequent disconnects from VPN connection
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	CSCts28999	AC SSL message when no IP address available needs changes
vpn	CSCts29023	AC IKEv2 conn failure message should indicate no IP address assigned

Table 15 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.4235

Component	Id	Headline
vpn	CSCts29059	AC agent sometimes terminates after failed conn where no IP address available
vpn	CSCts34796	AnyConnect: Causes a boot delay of up to 20min on the client PC
vpn	CSCts37932	CRL checks not ignoring proxy when IgnoreProxy is enabled
vpn	CSCts50389	multiple prompts via standard EAP are not handled correctly

AnyConnect 3.0.3054 Caveats

Caveats Resolved by Release 3.0.3054

Table 16 lists the Severity 1–3 caveats that AnyConnect Secure Mobility Client 3.0.3054 resolves. The table sorts the caveats by AnyConnect component, then by identifier.

Table 16 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.3054

Component	Id	Headline
certificate	CSCtr64798	Critical error while connecting to certain headends

Open Caveats in Release 3.0.3054

Table 17 lists the Severity 1–3 caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Release 3.0.3054. The table sorts the caveats by AnyConnect component, then by identifier.

Table 17 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3054

Component	Identifier	Headline
api	CSCtf90996	OGS selects inaccessible host
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs without disconnection
api	CSCtg67075	Terminate reason displayed as balloon with non-cert authentication
api	CSCti34206	AC UI stops after clicking Get Certificate button with Local CA enabled
api	CSCtj09831	Connect on startup setting user controllable even if disabled in profile
api	CSCto03828	GUI status bar states incorrect message about Posture initializing....
api	CSCtq82541	AnyConnect client login delay for domain user login
api	CSCtr21138	AnyConnect counters cannot be reset

Table 17 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3054

Component	Identifier	Headline
api	CSCtr75253	csdlib.dll is corrupted and size of 0K
api	CSCtr80031	Mac GUI crash
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCto91245	AnyConnect: Non-WinX clients not requesting entire cert chain
certificate	CSCtr00565	AnyConnect 3.0 fails clear PIN for SafeNet Smart Card
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, Network Access Manager, or UI open
core	CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect client
core	CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
core	CSCta94621	Enable local LAN access not consistent with other split tunnel options
core	CSCtc17266	Private-side proxy on OS X does not support per-protocol proxy
core	CSCte84061	Quarantined AnyConnect cannot “Reconnect” from within CSD value
core	CSCtf20226	Make AnyConnect DNS w/ split tunnel behavior for Mac same as Windows
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCtq75832	AnyConnect does not perform auto route correction on Mac/Linux
dart	CSCtn46629	DART does not collect files from localized paths
download_ install	CSCtg04881	VPN downloaders always aborts first SSL handshake
download_ install	CSCtl53574	Creating hard link fails on FAT32 systems
download_ install	CSCtr28687	IKEv2-IPsec: Downloader (SSL) is not using configured public Proxy Server
gui	CSCtc03052	SCEP fails in upgrade scenario
gui	CSCte42921	Get unresolved gateway address when trying to connect
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtf60851	Network access not being displayed during reconnects
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCth13596	AC30 SCEP - combine similar message dialogs into one
gui	CSCth93459	AC dialog left over after successful SCEP enrollment
gui	CSCti79049	IKEv2-IPsec: Mac Statistics missing NAT-T from Protocol - Windows has it
gui	CSCtj05702	JPN: Windows Mobile Client Status message is garbled in Connection tab

Table 17 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3054

Component	Identifier	Headline
gui	CSCtj05748	JPN: Windows Mobile Client Message is garbled in About tab
gui	CSCtk35342	SBL interoperability issue with user-created networks
network access manager	CSCtc70565	CSSC client did not resend out its credential after timeout.
network access manager	CSCti17003	No IPv6 support
network access manager	CSCto95207	Password protected certificates do not work
network access manager	CSCtr63595	NAM stuck authenticating when using a wired dot1x configuration
network access manager	CSCtr97908	Machine authentication with 2008 AD certificate template fails
posture	CSCti24021	Posture localization PO file needs updated translation
posture	CSCtj59449	MAC needs to support cert verification
posture	CSCtk05829	Hostscan does not work when using Google Chrome on a Mac
posture	CSCtq80972	CSD 3.6 not returning endpoint attributes when logging in with SBL
posture	CSCtr03991	Slower/inconsistent connection times when Posture is enabled
posture	CSCtr14928	CSD: Trend Micro Core Protection Module is not detected correctly
posture	CSCtr26427	CSD: Posture assessment fail on certain Win 7 64-bit machines
posture	CSCtr85683	Remove excessive AnyConnect logging from application event viewer
posture	CSCts00066	Posture assessment and connection fails with IKEv2 to Load Balance ASA
scansafe	CSCtk53053	Automatic Tower Selection code improvements
scansafe	CSCtr15005	Websec fail to filter malicious site when used with proxy not excluded
vpn	CSCsv49773	Ability to accommodate multiple head-end profiles
vpn	CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
vpn	CSCtb92777	MSIE proxy not being set in Vista and Windows 7 when no port used
vpn	CSCtb92820	Internet Explorer IPv6 address proxy set incorrectly
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-on enabled
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says "Configuring IPv6 system..."
vpn	CSCtf63783	VPN connection failed because "CSD is not installed..."

Table 17 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3054

Component	Identifier	Headline
vpn	CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
vpn	CSCtg01525	AnyConnect should have clear description for each error msg
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg58360	Always-on profile is deleted if connecting as a user that has no profile
vpn	CSCtg61388	Unable to access captive portal login page while reconnecting
vpn	CSCtg97089	IPsecOverSSL: cannot establish VPN connection via data card adapter
vpn	CSCth11271	AC30 deleting certs while GUI loaded causing BIOS ID problems
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCti35748	AC SCEP enrollment fails over IPv6-in-IPv4 connection-client disconnect
vpn	CSCti93817	Trusted network not detected when adapter has IPv6 DNS addresses
vpn	CSCti93996	Get prompted for VPN credentials whenever DHCP lease renewed
vpn	CSCtj62029	Cannot establish tunnel with machine cert auth and untrusted server CA
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtk15816	Always On: Web Auth required message displayed with network access
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - cannot log in
vpn	CSCtk35111	SBL interoperability issue with user-created networks
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays “on a trusted network”
vpn	CSCtk68610	AC Get Certificate button not working - Local CA on ASA not usable
vpn	CSCtk95716	Corrupt Firefox profiles cause AnyConnect to crash
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn00418	Make the client resilient to network stability issues

Table 17 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3054

Component	Identifier	Headline
vpn	CSCtn11401	AnyConnect failures with connection, yet it is passing data
vpn	CSCtn56376	AC unable to access the root ca in Firefox using Linux
vpn	CSCtq17339	AnyConnect 3.0.1047 unable to validate certificate chain when using IKEv2
vpn	CSCtr00334	Always-On: If ASA DNS name cannot be resolved, cannot select another entry
vpn	CSCtr00535	AnyConnect fails to disconnect quickly when CAC card removed
vpn	CSCtr20634	AC: Split-exclude route not working when overlapping a link-level route
vpn	CSCtr24100	vpnagent crash with split-DNS enabled
vpn	CSCtr27865	Observing slow throughput when using AnyConnect Mac client
vpn	CSCtr31163	AnyConnect AlwaysOn fail-close feature broken in Mac OS X v10.6.7
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds
vpn	CSCtr67545	AnyConnect 3.0 Certificate authentication with IOS fails
vpn	CSCtr75228	VPN Client Driver has encountered an error
vpn	CSCtr75276	Experiencing frequent disconnects from VPN connection
vpn	CSCtr80410	Password may be available in clear text in RAM
WebVPN-l3tunnel	CSCtk74949	Reword user message: AC session fails with “CSTP not enabled”

AnyConnect 3.0.3050 Caveats

Caveats Resolved by Release 3.0.3050

Table 18 lists the Severity 1–3 caveats that AnyConnect Secure Mobility Client 3.0.3050 resolves. The table sorts the caveats by AnyConnect component, then by identifier.

Table 18 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.3050

Component	Id	Headline
api	CSCtr07080	OGS does not work when using ports in server list
core	CSCtl97620	Network unreachable after disconnect if wireless active
download_install	CSCtk32971	Translation catalog missing some downloader messages
download_install	CSCtq35035	VPN: Unable to remove 3rd party Active X add-on after pre-deploy of VPN
download_install	CSCtq38732	NAM Install: Repair install (msi) for NAM does not complete successfully

Table 18 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.3050

Component	Id	Headline
network access manager	CSCtn71218	Ping and ARP fails with Ralink 3800PD2 and AnyConnect NAM
network access manager	CSCtn87099	acnamfd crashes when query of OID_GEN_SUPPORTED_LIST fails
network access manager	CSCto05087	AnyConnect 3.0 NAM has problem with Microsoft Forefront TMG Client
network access manager	CSCto68182	Installer rolls back due to INFCACHE.1 file being corrupt
network access manager	CSCtq08317	NAM erroneously allows openStaticWep user networks when policy forbid it
network access manager	CSCtq46501	Remove 64 limit of network lists from NAM
network access manager	CSCtq49274	Saving of active group is broken in 2039
network access manager	CSCtq86528	NAM Status Icon in Flyout Remains in “Transitioning” After L2-Connected
network access manager	CSCtr12963	Activating countermeasures prematurely prevents association
network access manager	CSCtr36013	Activating countermeasures prematurely prevents association
posture	CSCtn93301	CSD 3.5 fails to validate Sophos AV 7.x on Mac OS X
posture	CSCto91503	CSD: PreLogin Device Protection is reported incorrectly
posture	CSCtq00045	Vault login denied when Host Scan incorrectly reports main.exe not running
posture	CSCtq48037	DOC: Need to remove wrong doc on csd Prelogin Cert check for MAC
telemetry	CSCtj74281	Telemetry needs to use log entries from libhostscan
vpn	CSCtl43149	VPN agent hangs on startup (telemetry enabled)
vpn	CSCtl74125	IKEv2: Cannot install opt modules if client-services has non-default port
vpn	CSCto57463	Failing to connect using DNS with GSS in 3.0.2
vpn	CSCto86280	IPSec disconnect with the client is slower than SSL
vpn	CSCtq65063	Infinite reconnect loop with certain data card connection manager
vpn	CSCtq71513	IKEv2-IPsec: Odd reconnect state when ASA behind NAT (w/IPsec rekeys)
vpn	CSCtq74504	VPN connection fails with link-local split-exclude network
vpn	CSCtq77021	Crash when using machine certs in load balanced environment
vpn	CSCtq78841	Proxy Setting is intermittently not restored after AnyConnect disconnect

Table 18 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.3050

Component	Id	Headline
vpn	CSCtq81449	IPsec: Mac:Reconnect after resume -1st time is OK, any after always FAIL
vpn	CSCtq83656	Crash when endpoint has an IPv6 address
vpn	CSCtq95503	VPN connection fails via data card in 4G mode
vpn	CSCtr00262	Host changed: Server communication error wrt GSS
vpn	CSCtr38194	Connection failures with GSS

Open Caveats in Release 3.0.3050

Table 19 lists the Severity 1–3 caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Release 3.0.23050. The table sorts the caveats by AnyConnect component, then by identifier.

Table 19 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3050

Component	Identifier	Headline
api	CSCtf90996	OGS selects inaccessible host
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs without disconnection
api	CSCtg67075	Terminate reason displayed as balloon with non-cert authentication
api	CSCti34206	AC UI stops after clicking Get Certificate button with Local CA enabled
api	CSCtj09831	Connect on startup setting user controllable even if disabled in profile
api	CSCto03828	GUI status bar states incorrect message about Posture initializing....
api	CSCtq82541	AnyConnect client login delay for domain user login
api	CSCtr21138	AnyConnect counters cannot be reset
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCto91245	AnyConnect: Non-WinX clients not requesting entire cert chain
certificate	CSCtr00565	AnyConnect 3.0 fails clear PIN for SafeNet Smart Card
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, Network Access Manager, or UI open
core	CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect client
core	CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
core	CSCta94621	Enable local LAN access not consistent with other split tunnel options
core	CSCtb73073	VPN establishment allowed while multiple local users logged in on Mac
core	CSCtc17266	Private-side proxy on OS X does not support per-protocol proxy
core	CSCte84061	Quarantined AnyConnect cannot “Reconnect” from within CSD value

Table 19 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3050

Component	Identifier	Headline
core	CSCtf20226	Make AnyConnect DNS w/ split tunnel behavior for Mac same as Windows
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
core	CSCtq75832	AnyConnect does not perform auto route correction on Mac/Linux
core	CSCsy34111	SVC MSIE proxy option auto does not work
dart	CSCtn46629	DART does not collect files from localized paths
download_ install	CSCtg04881	VPN downloaders always aborts first SSL handshake
download_ install	CSCtl53574	Creating hard link fails on FAT32 systems
download_ install	CSCtr28687	IKEv2-IPsec: Downloader (SSL) is not using configured public Proxy Server
gui	CSCtc03052	SCEP fails in upgrade scenario
gui	CSCte42921	Get unresolved gateway address when trying to connect
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtf60851	Network access not being displayed during reconnects
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCth13596	AC30 SCEP - combine similar message dialogs into one
gui	CSCth93459	AC dialog left over after successful SCEP enrollment
gui	CSCti79049	IKEv2-IPsec: Mac Statistics missing NAT-T from Protocol - Windows has it
gui	CSCtj05702	JPN: Windows Mobile Client Status message is garbled in Connection tab
gui	CSCtj05748	JPN: Windows Mobile Client Message is garbled in About tab
gui	CSCtk35342	SBL interoperability issue with user-created networks
network access manager	CSCtc70565	CSSC client did not resend out its credential after timeout.
network access manager	CSCth21866	Windows 7 system tray icon shows when network access manager installed
network access manager	CSCti17003	No IPv6 support
network access manager	CSCto95207	Password protected certificates do not work
network access manager	CSCtr63595	NAM stuck authenticating when using a wired dot1x configuration

Table 19 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3050

Component	Identifier	Headline
posture	CSCti24021	Posture localization PO file needs updated translation
posture	CSCtj59449	MAC needs to support cert verification
posture	CSCtk05829	Hostscan does not work when using Google Chrome on a Mac
posture	CSCtq80972	CSD 3.6 not returning endpoint attributes when logging in with SBL
posture	CSCtr03991	Slower/inconsistent connection times when Posture is enabled
posture	CSCtr14928	CSD: Trend Micro Core Protection Module is not detected correctly
posture	CSCtr26427	CSD: Posture assessment fail on certain Win 7 64-bit machines
scansafe	CSCtk53053	Automatic Tower Selection code improvements
scansafe	CSCtr15005	Websec fail to filter malicious site when used with proxy not excluded
vpn	CSCsu52949	GUI pops up certificate warning prompts on every connection attempt
vpn	CSCsv49773	Ability to accommodate multiple head-end profiles
vpn	CSCtb73259	Message “Connection to the proxy server failed” appears during reconnect
vpn	CSCtb92777	MSIE proxy not being set in Vista and Windows 7 when no port used
vpn	CSCtb92820	Internet Explorer IPv6 address proxy set incorrectly
vpn	CSCte73983	bad apple config may cause vpnagentd to fail
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-on enabled
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says “Configuring IPv6 system...”
vpn	CSCtf63783	VPN connection failed because “CSD is not installed...”
vpn	CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
vpn	CSCtg01525	AnyConnect should have clear description for each error msg
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg58360	Always-on profile is deleted if connecting as a user that has no profile
vpn	CSCtg61388	Unable to access captive portal login page while reconnecting
vpn	CSCtg97089	IPsecOverSSL: cannot establish VPN connection via data card adapter
vpn	CSCth11271	AC30 deleting certs while GUI loaded causing BIOS ID problems
vpn	CSCth35315	AC captive portal black cisco nac agent discovery/posture communication
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure

Table 19 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3050

Component	Identifier	Headline
vpn	CSCti35748	AC SCEP enrollment fails over IPv6-in-IPv4 connection-client disconnect
vpn	CSCti93817	Trusted network not detected when adapter has IPv6 DNS addresses
vpn	CSCti93996	Get prompted for VPN credentials whenever DHCP lease renewed
vpn	CSCtj61887	Captive portal not detected when previously connected with IPsec
vpn	CSCtj62029	Cannot establish tunnel with machine cert auth and untrusted server CA
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtk15816	Always On: Web Auth required message displayed with network access
vpn	**CSCtk34456**	Always-On & SBL: The VPN agent service is not responding - cannot log in
vpn	CSCtk35111	SBL interoperability issue with user-created networks
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays “on a trusted network”
vpn	CSCtk68610	AC Get Certificate button not working - Local CA on ASA not usable
vpn	CSCtk95716	Corrupt Firefox profiles cause AnyConnect to crash
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn00418	Make the client resilient to network stability issues
vpn	CSCtn11401	AnyConnect failures with connection, yet it is passing data
vpn	CSCtn56376	AC unable to access the root ca in Firefox using Linux
vpn	CSCtq17339	AnyConnect 3.0.1047 unable to validate certificate chain when using IKEv2
vpn	CSCtr00334	Always-On: If ASA DNS name cannot be resolved, cannot select another entry
vpn	CSCtr00535	AnyConnect fails to disconnect quickly when CAC card removed
vpn	CSCtr20634	AC: Split-exclude route not working when overlapping a link-level route
vpn	CSCtr24100	vpnagent crash with split-DNS enabled
vpn	CSCtr27865	Observing slow throughput when using AnyConnect Mac client
vpn	CSCtr31163	AnyConnect AlwaysOn fail-close feature broken in Mac OS X v10.6.7
vpn	CSCtr38205	XP: After Cancel from Auth window, a delay occurs for ~13 seconds

Table 19 Caveats Open by Cisco AnyConnect Secure Mobility Client Release 3.0.3050

Component	Identifier	Headline
vpn	CSCtr38549	AC on Mac does not connect due to ioctl Return code: -1 (0xFFFFFFFF)
WebVPN-l3tunnel	CSCtk74949	Reword user message: AC session fails with “CSTP not enabled”

AnyConnect 3.0.2052 Caveats

Caveats Resolved by Release 3.0.2052

Table 20 lists the caveats that AnyConnect Secure Mobility Client 3.0.2052 resolves. The table sorts the caveats by AnyConnect component, then by identifier.

Table 20 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.2052

Component	Identifier	Headline
api	CSCtj89377	CSD causes client crash on Mac
api	CSCtk78458	AnyConnect API crash in attach and detach
certificate	CSCtn50072	CFileCertificate: SignHash fails in FIPS mode for IKEv2 connections
core	CSCtf94284	AnyConnect may show password in clear text in RAM
core	CSCtl45627	Connection to IPv6 enabled head end fails (Vista/Win7)
core	CSCtn75204	AnyConnect 3.0 VPN Server could not parse request with & or < in passwd
doc	CSCto73186	DOC AnyConnect FIPS module - details not documented
doc	CSCto73233	DOC: AnyConnect FIPS package has system-wide consequences.
gui	CSCtj45111	Network Name is Not Shown in network access manager Credentials With Longer Network Names
gui	CSCtn96122	Opening Advanced Window Link While GUI Shutting Down Crashes GUI
network access manager	CSCtg99206	Network Access Manager service not sending Password Change result event
network access manager	CSCtk75676	Network Access Manager: association takes long time upon system resume.
network access manager	CSCtn18183	Network Access Manager: Connect Exclusively does not work
network access manager	CSCtn66957	Network Access Manager crashes when loading a tunnel PAC from configuration.

Table 20 ***Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.2052***

Component	Identifier	Headline
network access manager	CSCto31142	Network Access Manager: Smart card authentication not working with E-Token
posture	CSCtl79784	Crash from WER Data
posture	CSCtn78403	cscan signature not checked before launch
posture	CSCtn89892	signal handling bug causes hostscan to scan twice per minute
profile-editor	CSCtf81226	AC Profile Editor: Disable Cert Selection option is not clear
profile-editor	CSCto05439	Time out setting in the profile editor for websec does not work
profile-editor	CSCto88404	Network Access Manager PE: Ignores ConnectionBehaviorAtLogon when reading new config
scansafe	CSCto53112	DNS Cache failure
vpn	CSCth76124	Retain ASA DNS resolution throughout connection establishment
vpn	CSCtj51376	IE Proxy setting is not restored after AnyConnect disconnect on Win 7
vpn	CSCtk06308	AC failing to perform SCEP proxy enrollment - Profile () not found
vpn	CSCtk66387	WPAD doesn't work on Win7 + IE 8
vpn	CSCtl47289	IKEv2 browser proxy config fails
vpn	CSCtl90819	Random Cert Validation Failures
vpn	CSCtn39753	Client certs gotten with SCEP Proxy cannot be used for IKEv2 PRF SHA2
vpn	CSCtn42416	SCEP Proxy with IKEv2 PRF SHA2 results in repeated enrollments
vpn	CSCtn42751	AnyConnect + 'Retain VPN on logoff', case sensitivity not compatible wit
vpn	CSCtn68171	Add ability for AC to detect wrong client cert CSP and generate event
vpn	CSCtn87093	VPN: WinXP with TND strips DefaultGW and breaks trusted DNS settings
vpn	CSCto00117	Tunnel resumption exhibits broken split tunnel (which is not configured)
vpn	CSCto05492	VPN Connection Stuck Reconnecting and then Disconnecting
vpn	CSCto08814	Routing Issue Gets Client Stuck Reconnecting
vpn	CSCto76864	AnyConnect fails after few seconds connected on certain 3G cards.
vpn	CSCto83758	UI terminates after cert select during IKEv2 connection attempt
vpn	CSCtr19783	AnyConnect WebLaunch ignores proxy server setting

Open Caveats in Release 3.0.2052

Table 21 lists the Severity 1–3 caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Release 3.0.2052. The table sorts the caveats by AnyConnect component, then by identifier.

Table 21 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.2052

Component	Identifier	Headline
api	CSCtf90996	OGS selects inaccessible host
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCtg67075	Terminate Reason Displayed as Balloon with Non-cert Authentication
api	CSCti34206	AC UI stops after clicking Get Certificate button with Local CA enabled
api	CSCtj09831	Connect on startup setting user controllable even if disabled in profile
api	CSCtk74949	Reword user message: AC session fails with “CSTP not enabled”
api	CSCto03828	GUI status bar states incorrect message about Posture initializing....
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCto91245	AnyConnect: Non-WinX clients not requesting entire cert chain
cli	CSCtk58176	CLI does not establish VPN connection with Web Security, Network Access Manager or UI open
core	CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client.
core	CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
core	CSCsy34111	SVC MSIE proxy option auto does not work
core	CSCta94621	Enable local LAN access not consistent with other split tunnel options
core	CSCtb73073	VPN establishment allowed while multiple local users logged in on MAC
core	CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
core	CSCte84061	Quarantined AnyConnect can't “Reconnect” from within CSD Vault
core	CSCtf20226	Make anyconnect DNS w/ split tunnel behavior for Mac same as windows
core	CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
dart	CSCtn46629	DART does not collect files from localized paths
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCtk32971	Translation catalog missing some downloader messages
download_install	CSCtl53574	Creating hard link fails on FAT32 systems
download_install	CSCtn53685	Installer fails to copy profiles over a mapped network drive

Table 21 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.2052

Component	Identifier	Headline
download_install	CSCtq35035	VPN: Unable to remove 3rd party Active X add-on after pre-deploy of VPN
gui	CSCtc03052	SCEP fails in upgrade scenario
gui	CSCte42921	Get Unresolved Gateway Address When Trying to Connect
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtf60851	Network access not being displayed during reconnects
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCth13596	AC30 SCEP - combine similar message dialogs into one
gui	CSCth93459	AC dialog left over after successful SCEP enrollment
gui	CSCti79049	IKEv2-IPSec: Mac Statistics missing NAT-T from Protocol - Windows has it
gui	CSCtj05702	JPN: Windows Mobile Client Status message is garbled in Connection tab
gui	CSCtj05748	JPN: Windows mobile client Message is garbled in About tab.
gui	CSCtk35342	SBL interoperability issue with user-created networks
network access manager	CSCtc70565	CSSC client did not resend out its credential after timeout.
network access manager	CSCth21866	Windows 7 system tray icon shows when Network Access Manager installed
network access manager	CSCti17003	No IPv6 support
network access manager	CSCti70485	Network Access Manager: Extra step required to unlock Windows PC
network access manager	CSCtn87099	acnamfd crashes when query of OID_GEN_SUPPORTED_LIST fails
network access manager	CSCto45146	Network Access Manager: Interop issue with Hitachi APS password reset software
network access manager	CSCto95207	Network Access Manager: password protected certificates do not work
network access manager	CSCtq09710	AnyConnect 3.0 Network Access Manager randomly fails installation through Microsoft SCCM
posture	CSCti24021	Posture localization PO file needs updated translation
posture	CSCtj59449	MAC needs to support cert verification
posture	CSCtk05829	Hostscan does not work when using Google Chrome on a MAC
sbl	CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance
scansafe	CSCtk53053	Automatic Tower Selection code improvements
telemetry	CSCtj74281	telemetry needs to use log entries from libhostscan

Table 21 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.2052

Component	Identifier	Headline
vpn	CSCsu52949	GUI pops up certificate warning prompts on every connection attempt
vpn	CSCsv49773	Ability to accommodate multiple head-end profiles
vpn	CSCsw37980	Needs more certificate matching events
vpn	CSCsz56742	Will not use certificates under certain ASA configuration
vpn	CSCtb73259	Message “Connection to the proxy server failed” appears during reconnect
vpn	CSCtb92777	MSIE proxy not being set in Vista and Windows7 when no port used
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCte73983	bad apple config may cause vpnagentd to fail
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled
vpn	CSCtf56937	Always-On: After Admin disconnect, GUI says “Configuring IPv6 system...”
vpn	CSCtf63783	VPN connection failed because “CSD isn't installed...”
vpn	CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
vpn	CSCtg01525	AnyConnect should have clear description for each error msg
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg58360	Always-On profile is deleted if connecting as a user that has no profile
vpn	CSCtg61388	Unable to Access Captive Portal Login Page While Reconnecting
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth11271	AC30 deleting certs while GUI loaded causing BIOS ID problems
vpn	CSCth35315	captive portal reconnect after resume blocks cisco nac agent discovery
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCti35748	AC SCEP enrollment fails over IPv6-in-IPv4 connection-client disconnect
vpn	CSCti93817	Trusted Network not detected when adapter has IPv6 DNS addresses
vpn	CSCti93996	Get prompted for VPN credentials whenever DHCP lease renewed
vpn	CSCtj61887	Captive Portal not detected when previously connected with IPsec

Table 21 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.2052

Component	Identifier	Headline
vpn	CSCtj62029	Can't establish tunnel with machine cert auth and untrusted server CA
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtj77505	AC SCEP certenroll using Hostname causing enrollment failure
vpn	CSCtk14009	AnyConnect 2.x/3.x: Public proxy PAC URL fails to connect
vpn	CSCtk15816	Always On: Web Auth Required message displayed with Network access
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - can't log in
vpn	CSCtk35111	AlwaysOn: Incorrect message While Reconnecting behind a Captive Portal
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays “On a Trusted Network”
vpn	CSCtk68610	AC Get Certificate button not working -Local CA on ASA not usable
vpn	CSCtk95716	Corrupt Firefox profiles cause AnyConnect to crash
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtn00418	Make the client resilient to network stability issues
vpn	CSCtn11401	AnyConnect failures with connection, yet it is passing data
vpn	CSCtn56376	AC unable to access the root ca in firefox using Linux
vpn	CSCtq17339	anyconnect 3.0.1047-unable to validate certificate chain when using IKEV2

AnyConnect 3.0.1047 Caveats

Caveats Resolved by Release 3.0.1047

Table 22 lists the caveats that AnyConnect Secure Mobility Client 3.0.1047 resolves. The table sorts the caveats by AnyConnect component, then by identifier.

Table 22 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.1047

Component	Identifier	Headline
api	CSCti19702	TND Pause/Do-Nothing Enhancement
api	CSCtl94063	AnyConnect 3.0.0629 API package for Mac OS X contains zero length files
api	CSCtn34496	AC30: Machine Certs don't work with Hostscan with preference

Table 22 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.1047

Component	Identifier	Headline
certificate	CSCtn21228	CryptSetProvParam can be called with a NULL handle
core	CSCtg14425	AC GUI Fails to launch on Ubuntu when “Assistive Tech is enabled”
core	CSCtj79104	Multicast traffic should be allowed in the clear with split-tunneling
core	CSCtl23144	AnyConnect does not track the VPN adapter default route (Vista/Win7)
core	CSCtl45627	Connection to IPv6 enabled head end fails (Vista/Win7)
gui	CSCtk30342	Win 7 at 125 DPI cuts off user GUI
gui	CSCtk68739	allowRunScriptAfterConnect=false fails to override runScriptAfterConnect
gui	CSCtk69095	UI shows wrong credential type when using 802.1x with an open switch
gui	CSCtl17993	shared/dynamic wep assoc modes are hidden by disabling open static wep
gui	CSCtl97606	GUI goes “bong” (or possibly “bing”) when you press Enter
gui	CSCtn11999	AnyConnect 3 should not display tray flyout unless it is doing something
network access manager	CSCtc49071	Network Access Manager strips xxx\prefix for UPN format for MSCHAP challenge calculation
network access manager	CSCtk60234	Network Access Manager incorrectly reports connected when TCP/IP unbound
network access manager	CSCtk75911	Driver does not restore connection state when unbound
network access manager	CSCtk95912	Network Access Manager has an IP address but stays in the authenticating state
network access manager	CSCtl42814	No PreLogon SmartCard Support for Vista and Windows 7
network access manager	CSCtl43167	Network Access Manager skips prelogon timeout before trying all networks (with 2+ networks)
network access manager	CSCtl55996	IPass connect can't associate while Network Access Manager is running
network access manager	CSCtl74624	Password retry should prompt for both username and password, not just password
network access manager	CSCtn12554	When set, PEAP will now negotiation inner methods MSCHAPv2 or GTC
network access manager	CSCtn21728	Network Access Manager supplicants do not ignore additional authentication attempts in host mode multi-auth.
profile-editor	CSCtn21076	AnyConnect Profile Editor enabling all Extended Key Usages causes error
profile-editor	CSCtn49958	Network Access Manager PE: Double byte UTF-8 formats cause schema validation failure

Table 22 Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.1047

Component	Identifier	Headline
profile-editor	CSCtn59418	Profile Editor Corrupting PAC files
telemetry	CSCtl12304	Unable to install MS SDK on Win7 when Telemetry enabled
vpn	CSCsu70199	IPv6: Network error: windows has detected and IP address conflict
vpn	CSCth33617	No error logged if PrimaryProtocol in the profile is incorrect
vpn	CSCtk13870	When AnyConnect adapter is disabled it prevents future connections
vpn	CSCtk55369	SCEP Enrollment to IOS CA inconsistent
vpn	CSCtk60914	Connect to combo and button disabled when cancelling proxy creds dialog
vpn	CSCtk61494	Connection Attempt to ASA Headend 'Hangs' for Over Ten Minutes
vpn	CSCtl25769	VPN stuck at “Reconnecting” for 30+ minutes (IPv6 enabled head-end)
vpn	CSCtn56658	GUI Run Key Precludes Use of CLI

Open Caveats in Release 3.0.1047

Table 23 lists the Severity 1–3 caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Release 3.0.1047. The table sorts the caveats by AnyConnect component, then by identifier.

Table 23 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.1047

Component	Identifier	Headline
api	CSCtf90996	OGS selects inaccessible host
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCtg67075	Terminate Reason Displayed as Balloon with Non-cert Authentication
api	CSCti34206	AC UI stops after clicking Get Certificate button with Local CA enabled
api	CSCtj09831	Connect on startup setting user controllable even if disabled in profile
api	CSCtk74949	AC session fails with “CSTP not enabled” modify message
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCth93690	AnyConnect 2.x on MAC removing e-token will not allow reconnects.
cli	CSCtk58176	CLI does not establish VPN connection with Web Security or Network Access Manager

Table 23 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.1047

Component	Identifier	Headline
core	CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client
core	CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
core	CSCsy34111	SVC MSIE proxy option auto does not work
core	CSCta94621	Enable local LAN access not consistent with other split tunnel options
core	CSCtb73073	Mac: VPN establishment allowed while multiple local users logged in
core	CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
core	CSCte84061	Quarantined AnyConnect can't "Reconnect" from within CSD Vault
core	CSCtf20226	Make anyconnect DNS w/ split tunnel behavior for Mac same as windows
core	CSCtg25686	AnyConnect fails to launch within a RDP connection with Always-on
dart	CSCtj86495	DART: wrong OS name shown in summary.txt file
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake
download_install	CSCth75313 (reported previously as CSCti06185)	No EULA display before installation of NGC
download_install	CSCtk32971	Translation catalog missing some downloader messages
download_install	CSCtl29351	setup.exe ought to be signed
download_install	CSCtl53574	Creating hard link fails on FAT32 systems
gui	CSCtc03052	SCEP fails in upgrade scenario
gui	CSCte42921	Get Unresolved Gateway Address When Trying to Connect
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtf56937	Always-On: After Admin disconnect, GUI says "Configuring IPv6 system..."
gui	CSCtf60851	Network access not being displayed during reconnects
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCth13596	AC30 SCEP - combine similar message dialogs into one
gui	CSCth93459	AC dialog left over after successful SCEP enrollment
gui	CSCti79049	IKEv2-IPSec: Mac Statistics missing NAT-T from Protocol - Windows has it
gui	CSCtj05702	JPN: Windows mobile client message is garbled in Connection tab
gui	CSCtj05748	JPN: Windows mobile client message is garbled in About tab
gui	CSCtj50653	Get cert button should dismiss credentials dialog

Table 23 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.1047

Component	Identifier	Headline
ipsec-ezvpn	CSCtk76925	AnyConnect ikev2 client doesn’t send periodic DPD at 30 sec interval
network access manager	CSCtc70565	CSSC client did not resend out its credential after timeout.
network access manager	CSCth21866	Windows 7 system tray icon shows when Network Access Manager installed
network access manager	CSCti17003	No IPv6 Support
network access manager	CSCti70485	Extra step required to unlock PC
network access manager	CSCtk35342	SBL interoperability issue with user-created networks
network access manager	CSCtn71218	Network Access Manager: Shows limited connectivity in the UI when using wireless adapters with a Ralink chipset.
posture	CSCti24021	Posture localization PO file needs updated translation
posture	CSCti95975 (reported previously as CSCti96752)	Web Security sends GUI conflicting messages
posture	CSCtj11412	hostscan unable to read firefox 3.6 certificates
posture	CSCtj59449	MAC needs to support cert verification
posture	CSCtk05829	Host Scan does not work when using Google Chrome on a MAC
sbl	CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance
scansafe	CSCtj95601	Third-party security proxy causes recursive redirection loop
scansafe	CSCtk53053	Automatic Tower Selection code improvements
ssl-vpn	CSCti89976	AnyConnect 3.0 doesn't work with existing IOS
telemetry	CSCtj74281	telemetry needs to use log entries from libs
vpn	CSCsu52949	GUI pops up certificate warning prompts on every connection attempt
vpn	CSCsv49773	Ability to accommodate multiple head-end profiles
vpn	CSCsw37980	Needs more certificate matching events
vpn	CSCsz56742	Will not use certificates under certain ASA configuration
vpn	CSCtb34499	Fail to establish tunnel with a locally installed proxy
vpn	CSCtb73259	Message “Connection to the proxy server failed” appears during reconnect
vpn	CSCtb92777	MSIE proxy not being set in Vista and Windows7 when no port used
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCte73983	bad apple config may cause vpnagentd to fail

Table 23 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.1047

Component	Identifier	Headline
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled
vpn	CSCtf63783	VPN connection failed because “CSD isn't installed...”
vpn	CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
vpn	CSCtg01525	AnyConnect should have clear description for each error msg
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg58360	Always-On profile is deleted if connecting as a user that has no profile
vpn	CSCtg61388	Unable to Access Captive Portal Login Page While Reconnecting
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth11271	AC30 deleting certs while GUI loaded causing BIOS ID problems
vpn	CSCth32206	Logging is insufficient for troubleshooting
vpn	CSCth35315	captive portal reconnect after resume blocks cisco nac agent discovery
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCti35748	AC SCEP enrollment fails over IPv6-in-IPv4 connection - client disconnect
vpn	CSCti93817	Trusted Network not detected when adapter has IPv6 DNS addresses
vpn	CSCti93996	Get prompted for VPN credentials whenever DHCP lease renewed
vpn	CSCtj26311	SCEP Proxy enrollment to CA with SCEP challenge enabled fails
vpn	CSCtj28374	SCEP proxy over SSL - success syslog should not say ERROR
vpn	CSCtj50913	AC SSL failing to use certs - SCEP and non SCEP modes
vpn	CSCtj51376	IE Proxy setting is not restored after AnyConnect disconnect on Win 7
vpn	CSCtj61887	Captive Portal not detected when previously connected with IPsec
vpn	CSCtj62029	Can’t establish tunnel with machine cert auth and untrusted server CA
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtj77505	AC SCEP certenroll using Hostname causing enrollment failure
vpn	CSCtk06308	AC failing to perform SCEP proxy enrollment - Profile () not found
vpn	CSCtk15816	Always On: Web Auth Required message displayed with Network access

Table 23 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.1047

Component	Identifier	Headline
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - can't log in
vpn	CSCtk35111	AlwaysOn: Incorrect message While Reconnecting behind a Captive Portal
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays “On a Trusted Network”
vpn	CSCtk68610	AC Get Certificate button not working -Local CA on ASA not usable
vpn	CSCtk95716	Corrupt Firefox profiles cause AnyConnect to crash
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtl43149	VPN agent hangs on startup (telemetry enabled)
vpn	CSCtn56376	AC unable to access the root ca in firefox using Linux
webvpn-lb	CSCti07859	AC reports 'certificate validation failed' with VPN LB intermittently

AnyConnect 3.0.0629 Caveats

Caveats Resolved by Release 3.0.0629

Table 24 lists the CSSC caveats that Network Access Manager resolves.

Table 24 CSSC Caveats Resolved by Network Access Manager, Cisco AnyConnect Secure Mobility Client Release 3.0.0629

Identifier	Headline
CSCsk54277	When a user types an incorrect smartcard PIN, a GUI indication is not given
CSCso23071	The wired open connection shows as open rather than as connected
CSCsq25503	User is not prompted to re-insert smart card if card is removed after entering PIN.
CSCsq39157	SSC deletes all profiles stored in Vista native profile store
CSCsu75164	SSC displays an unsupported option for users who attempt to create 802.1x networks with PEAP and use certificates as the authentication mechanism
CSCsu96058	SSC on Vista supports a single wired network
CSCsu96084	SSC on Vista does not support credential caching “forever”
CSCtd24600	fallback to WebAuth from dot1x(timeout) MAB (uk), client doesn't get ip
CSCtd63236	If CSSC password contains the character “#” authentication will fail

Table 25 lists the caveats in AnyConnect Secure Mobility Client 2.5 and previous releases that AnyConnect Secure Mobility Client 3.0 resolves. The table sorts the caveats by AnyConnect component, then by identifier.

Table 25 AnyConnect Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.0629

Component	Identifier	Headline
api	CSCsz42024	AnyConnect exits before logoff scripts run / roaming profile updated
api	CSCtf04766	AnyConnect uses Windows system locale instead of install language
api	CSCtf61128	Change AP, client does not get state change events for connected state
api	CSCtj36459	Cannot connect to tunnel groups with CSD enabled
api	CSCtj43216	AnyConnect SBL missing 'Disconnect' button in Window 7
api	CSCtj59741	AnyConnect machine certs cause group mapping to fail if CSD is enabled
api	CSCtj90974	Headend Selection Cache size causes AnyConnect client to hang
asdm	CSCti70504	ASDM: Unable to create AnyConnect Profiles on Disk1
certificate	CSCtf06844	AnyConnect SCEP enrollment not working with ASA Per Group Cert Auth
certificate	CSCtf52183	SCEP enrollment on Mac makes private key exportable from keychain
certificate	CSCth93690	AnyConnect 2.x on MAC removing e-token will not allow reconnects
core	CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
core	CSCtb37826	Size of buffer for network bound packets reported incorrectly
core	CSCtb73046	VPN establishment allowed while multiple local users logged in on Linux
core	CSCtf23946	Agent does not restore DNS Suffix search list if VA dies
core	CSCtg01304	Split-tunneling: filtering needs to be enforced on the VPN adapter
core	CSCtg37737	AnyConnect cannot parse PAC file and does not connect to endpoint
core	CSCtg52703	AnyConnect fails on Panasonic Toughbook when using wireless **Note** We cannot reproduce this behavior in AnyConnect 3.0.
core	CSCth11301	XP x64: AnyConnect fails to recreate routes after L2 disruption
core	CSCth22251	Mac split-tunneling: DNS fails if no DNS servers are pushed from ASA
core	CSCth61000	Remove GetMUSHostAddr MUS messages when MUS is not enabled
core	CSCti45554	AnyConnect dropping packets that are close to the MTU when using DTLS

Table 25 AnyConnect Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.0629 (continued)

Component	Identifier	Headline
core	CSCti59666	AnyConnect misconfigures route table on Windows 7 in multi-homed scenario
core	CSCti82286	AnyConnect fails to account for OS-generated route causing failure
core	CSCti88663	AC: Windows 7 pushed proxy settings not cleared after hard boot
core	CSCti96053	AnyConnect fails with "Unable to process response from.." with Auto-Conn
core	CSCtj61695	Split-DNS uses search domains from the public interface
core	CSCtj79104	Multicast traffic should be allowed in the clear with split-tunneling
core	CSCtk32293	Mac: IPsec connection fails after upgrade, no network connectivity
core	CSCtk55194	Automatic upgrade fails, downloader unable to stop the agent
core	CSCtl45627	Connection to IPv6 enabled head end fails (Vista/Win7)
dart	CSCtj74910	DART fails to save to default location if Desktop is not named Desktop
download_install	CSCth35172	Multiple Administrative Domains support
download_install	CSCth66014	Multi Domain: Customizations must be linked with software update lock
download_install	CSCti28319	On Mac OS X and Linux operating systems, we should not be downloading unnecessary modules
download_install	CSCtj23504	Tun extension should not be installed on Mac 10.6
download_install	CSCtk18585	AnyConnect upgrade can fail silently and will not be retried again
downloader	CSCtg76707	Cannot connect when hostname must be resolved via proxy from PAC file
gui	CSCtc65842	Mac GUI crash with SCEP in FIPS mode
gui	CSCtg23845	using shift-tab crashes the GUI.
gui	CSCth28869	Network status messages need to be shortened
gui	CSCth93280	SCEP challenge password dialog has text cutoff at top
gui	CSCti25611	vpnui crash - possible gdi library issue **Note** We cannot reproduce this behavior in AnyConnect 3.0.
gui	CSCti66285	VPN Status Banner Reports Old Headend
gui	CSCtj21326	Auto-connect on startup doesn't occur due to launch mode setting
gui	CSCtj33517	AC failed to start. It is already running in another user's session
gui	CSCtj50653	Get cert button should dismiss credentials dialog
installer	CSCth46760	PAC file does not work across the AnyConnect client.
installer	CSCti52956	AnyConnect install on OS X: permission changes to everything in /opt
installer	CSCtj31380	AnyConnect Installer is mounted Read-Write instead of Read-Only
network access manager	CSCta93976	Server certificate chain invalid - log details inadequate

Table 25 AnyConnect Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.0629 (continued)

Component	Identifier	Headline
network access manager	CSCtc05960	Need notification when no certificate is available for authentication
pki-scep	CSCti38293	SCEP cert renewal not being triggered when connection is SSL
posture	CSCti25624	Host Scan failing when 5 digit csport is used <44999 or 65000>
posture	CSCti28958	AnyConnect UI shows CSD messages / debugs and it should not be.
profile-editor	CSCth23899	AC Profile Editor should allow multiple domain components to be defined
profile-editor	CSCtj75896	Prof Editor: Cert Enrollment panel should show replacable parameters
telemetry	CSCtj33227	Uncompressing a virus file using WinRAR not always trigger report
ui	CSCtf21161	AnyConnect on OSX does not display line breaks in banner
ui	CSCtg61106	AnyConnect does not request translation tables in standalone mode
ui	CSCti22600	AnyConnect: Language Localization fails if translation size over a limit
ui	CSCtj09033	AnyConnect: OGS causes GUI to pop-up in Trusted Network w/ Always-On Cfg
vpn	CSCte46102	AnyConnect unable to browse websites when connected
vpn	CSCtg73736	Captive portal can't be remediated if remediation site in private space
vpn	CSCth09439	AC30 agent stops during SCEP enroll if CA is unavailable
vpn	CSCth13586	AC30 SCEP status dialog has blank button during enrollment
vpn	CSCth19437	AC30 - implement support for SCEP Success/Fail customized messages
vpn	CSCth28675	In preferences.xml, DefaultHost is all lowercase (web deploy w/profile)
vpn	CSCth75201	SCEP cert renewal not working
vpn	CSCth75269	AC does not detect some SCEP enrollment failures - displays positive msg
vpn	CSCth75749	client not initiating SCEP enrollment over SSL connection
vpn	CSCth83969	IPsec:Tunnel disconnected at the time of IPsec rekey with FTP traffic
vpn	CSCth93194	AC agent stops during SCEP enroll with password challenge on CA
vpn	CSCth95010	CA thumbprint check not done during SCEP proxy enrollment
vpn	CSCti22086	VPN reports connected without having any Internet connection **Note** We cannot reproduce this behavior in AnyConnect 3.0.
vpn	CSCti23396	AnyConnect fails with proxy timeout error when port 80 is used
vpn	CSCti30716	Posture assessment failed - AC not starting Host Scan **Note** We cannot reproduce this behavior.

Table 25 AnyConnect Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 3.0.0629 (continued)

Component	Identifier	Headline
vpn	CSCti38254	SCEP proxy cert renewal - AC client not deleting old cert
vpn	CSCti55676	Reconnects fail if connectivity lost right after IPsec VPN connection
vpn	CSCti68193	SCEP Proxy - implement import filtering machine vs. user store
vpn	CSCti73316	AnyConnect fails to connect with CSD enabled.
vpn	CSCti75548	Repeated GUI Crashes As a Result of VPN
vpn	CSCti78869	AC Statistics is not updated during a connection
vpn	CSCti98852	CDP packets get passed down the tunnel
vpn	CSCtj01954	IPv6 over IPv4 is failing on Linux/Mac
vpn	CSCtj04180	Updated profile for host entry is not reflected in the GUI
vpn	CSCtj32259	Weblaunch attempt after standalone connection fails when GUI closed
vpn	CSCtj44795	Can't access remediation site after captive portal detection, DNS fails
vpn	CSCtj65042	IPv6 over IPv4 is not working with localized XP in .411
vpn	CSCtj77460	AC needs error when Host Scan disabled and %MACHINEID% is specified
vpn	CSCtj80478	AnyConnect: Connection timeout doesn't work when a proxy configured
vpn	CSCtk10673	AC selects Basic proxy auth over NTLM auth
vpn	CSCtk13870	When AnyConnect adapter is disabled it prevents future connections
vpn	CSCtk18952	AnyConnect fails to connect if PtP interface doesn't have dest addr
vpn	CSCtk57468	OSX: with split-tunneling IPv6 doesn't get a default gateway
vpn	CSCtk60489	Host Scan prevents the use of Group URLs with prior releases of AnyConnect
vpn	CSCtk60914	Connect to combo and button disabled when cancelling proxy creds dialog
vpn	CSCtl25769	VPN stuck at “Reconnecting” for 30+ minutes (IPv6 enabled head-end)
webvpn-lb	CSCti07859	AC reports 'certificate validation failed' with VPN LB intermittently

Open Caveats in Release 3.0.0629

Table 26 lists the Severity 1–3 caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Release 3.0.0629. The table sorts the caveats by AnyConnect component, then by identifier.

Table 26 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.0629

Component	Identifier	Headline
api	CSCtf90996	OGS selects inaccessible host
api	CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
api	CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
api	CSCtg67075	Terminate Reason Displayed as Balloon with Non-cert Authentication
api	CSCti34206	AC UI stops after clicking Get Certificate button with Local CA enabled
api	CSCtj09831	Connect on startup setting user controllable even if disabled in profile
api	CSCtk74949	AC session fails with "CSTP not enabled" modify message
certificate	CSCtf56830	AC cert popup appears even when not requested by ASA
certificate	CSCth93690	AnyConnect 2.x on MAC removing e-token will not allow reconnects.
cli	CSCtk58176	CLI does not establish VPN connection with Web Security or Network Access Manager
core	CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client
core	CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
core	CSCsy34111	SVC MSIE proxy option auto does not work
core	CSCta94621	Enable local LAN access not consistent with other split tunnel options
core	CSCtb73073	Mac: VPN establishment allowed while multiple local users logged in
core	CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
core	CSCte84061	Quarantined AnyConnect can't "Reconnect" from within CSD Vault
core	CSCtf20226	Make anyconnect DNS w/ split tunnel behavior for Mac same as windows
core	CSCtg25686	AnyConnect fails to launch within a RDP connection with Always-on
dart	CSCtj86495	DART: wrong OS name shown in summary.txt file
download_install	CSCtg04881	VPN Downloader always aborts first SSL handshake

Table 26 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.0629

Component	Identifier	Headline
download_install	CSCth75313 (reported previously as CSCti06185)	No EULA display before installation of NGC
download_install	CSCtk32971	Translation catalog missing some downloader messages
download_install	CSCtl29351	setup.exe ought to be signed
download_install	CSCtl53574	Creating hard link fails on FAT32 systems
gui	CSCtc03052	SCEP fails in upgrade scenario
gui	CSCte42921	Get Unresolved Gateway Address When Trying to Connect
gui	CSCtf20678	Quitting from tray while connection in progress does not stop connection
gui	CSCtf56937	Always-On: After Admin disconnect, GUI says "Configuring IPv6 system..."
gui	CSCtf60851	Network access not being displayed during reconnects
gui	CSCtg18621	Automatic connections are not always indicated in the GUI
gui	CSCth13596	AC30 SCEP - combine similar message dialogs into one
gui	CSCth93459	AC dialog left over after successful SCEP enrollment
gui	CSCti79049	IKEv2-IPSec: Mac Statistics missing NAT-T from Protocol - Windows has it
gui	CSCtj05702	JPN: Windows mobile client message is garbled in Connection tab
gui	CSCtj05748	JPN: Windows mobile client message is garbled in About tab
gui	CSCtj50653	Get cert button should dismiss credentials dialog
gui	CSCtk30342	Win 7 at 125 DPI cuts off user GUI
gui	CSCtk68739	Network Access Manager: allowRunScriptAfterConnect=false fails to override runScriptAfterConnect
gui	CSCtk69095	UI shows wrong credential type when using 802.1x with an open switch
gui	CSCtl17993	shared/dynamic wep assoc modes are hidden by disabling open static wep
ipsec-ezvpn	CSCtk76925	AnyConnect ikev2 client doesn't send periodic DPD at 30 sec interval
network access manager	CSCtc70565	CSSC client did not resend out its credential after timeout.
network access manager	CSCth21866	Windows 7 system tray icon shows when Network Access Manager installed
network access manager	CSCti17003	No IPv6 Support
network access manager	CSCtk35342	SBL interoperability issue with user-created networks

Table 26 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.0629

Component	Identifier	Headline
network access manager	CSCtk60234	Network Access Manager incorrectly reports connected when TCP/IP unbound
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	CSCtk95912	Network Access Manager has an IP address but stays in the authenticating state
network access manager	CSCtl42814	No PreLogon SmartCard Support for Vista and Windows 7
posture	CSCti24021	Posture localization PO file needs updated translation
posture	CSCti95975 (reported previously as CSCti96752)	Web Security sends GUI conflicting messages
posture	CSCtj11412	hostscan unable to read firefox 3.6 certificates
posture	CSCtj59449	MAC needs to support cert verification
posture	CSCtk05829	Host Scan does not work when using Google Chrome on a MAC
sbl	CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance
scansafe	CSCtj95601	Third-party security proxy causes recursive redirection loop
scansafe	CSCtk53053	Automatic Tower Selection code improvements
ssl-vpn	CSCti89976	AnyConnect 3.0 doesn't work with existing IOS
telemetry	CSCtj74281	telemetry needs to use log entries from libs
telemetry	CSCtl12304	Unable to install MS SDK on Win7 when Telemetry enabled
vpn	CSCsu52949	GUI pops up certificate warning prompts on every connection attempt
vpn	CSCsu70199	IPv6: Network error: windows has detected and IP address conflict
vpn	CSCsv49773	Ability to accommodate multiple head-end profiles
vpn	CSCsw37980	Needs more certificate matching events
vpn	CSCsz56742	Will not use certificates under certain ASA configuration
vpn	CSCtb73259	Message “Connection to the proxy server failed” appears during reconnect
vpn	CSCtb92777	MSIE proxy not being set in Vista and Windows7 when no port used
vpn	CSCtb92820	Internet Explorer IPv6 address as proxy set incorrectly
vpn	CSCte73983	bad apple config may cause vpnagentd to fail
vpn	CSCte86255	TND: Incorrect network type when IPv6 adapters with no gateways present
vpn	CSCtf52125	Implement connecting via proxies with Always-On enabled

Table 26 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.0629

Component	Identifier	Headline
vpn	CSCtf63783	VPN connection failed because “CSD isn't installed...”
vpn	CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
vpn	CSCtg01525	AnyConnect should have clear description for each error msg
vpn	CSCtg18553	Message indicating captive portal presence when no network connection
vpn	CSCtg45505	VPN connection fails from network with unusual captive portal
vpn	CSCtg58360	Always-On profile is deleted if connecting as a user that has no profile
vpn	CSCtg61388	Unable to Access Captive Portal Login Page While Reconnecting
vpn	CSCtg97089	IPsecOverSSL: can't establish VPN connection via data card adapter
vpn	CSCth11271	AC30 deleting certs while GUI loaded causing BIOS ID problems
vpn	CSCth32206	Logging is insufficient for troubleshooting
vpn	CSCth33617	No errors in the log if a parameter in the profile is NOT being used
vpn	CSCth35315	captive portal reconnect after resume blocks cisco nac agent discovery
vpn	CSCth70842	No code signing support for Linux 64-bit
vpn	CSCth87793	The IPsec VPN connection was terminated due to an authentication failure
vpn	CSCti35748	AC SCEP enrollment fails over IPv6-in-IPv4 connection - client disconnect
vpn	CSCti93817	Trusted Network not detected when adapter has IPv6 DNS addresses
vpn	CSCti93996	Get prompted for VPN credentials whenever DHCP lease renewed
vpn	CSCtj26311	SCEP Proxy enrollment to CA with SCEP challenge enabled fails
vpn	CSCtj28374	SCEP proxy over SSL - success syslog should not say ERROR
vpn	CSCtj50913	AC SSL failing to use certs - SCEP and non SCEP modes
vpn	CSCtj51376	IE Proxy setting is not restored after AnyConnect disconnect on Win 7
vpn	CSCtj61887	Captive Portal not detected when previously connected with IPsec
vpn	CSCtj62029	Can’t establish tunnel with machine cert auth and untrusted server CA
vpn	CSCtj68067	Sample CLI does not support IPsec connections
vpn	CSCtj77505	AC SCEP certenroll using Hostname causing enrollment failure
vpn	CSCtk06308	AC failing to perform SCEP proxy enrollment - Profile () not found
vpn	CSCtk15816	Always On: Web Auth Required message displayed with Network access
vpn	CSCtk34456	Always-On & SBL: The VPN agent service is not responding - can't log in

Table 26 Open Caveats in Cisco AnyConnect Secure Mobility Client Release 3.0.0629

Component	Identifier	Headline
vpn	CSCtk35111	AlwaysOn: Incorrect message While Reconnecting behind a Captive Portal
vpn	CSCtk55369	SCEP Enrollment to IOS CA inconsistent
vpn	CSCtk61494	Connection Attempt to ASA Headend 'Hangs' for Over Ten Minutes
vpn	CSCtk62606	AC SSL - SCEP enroll not using new profile settings on first download
vpn	CSCtk65662	On my home wifi network VPN incorrectly displays “On a Trusted Network”
vpn	CSCtk68610	AC Get Certificate button not working -Local CA on ASA not usable
vpn	CSCtk95716	Corrupt Firefox profiles cause AnyConnect to crash
vpn	CSCtl06902	Unexpected credentials dialog popup with AnyConnect
vpn	CSCtl23730	Incorrect error message when typing in incorrect SDI credentials
vpn	CSCtl43149	VPN agent hangs on startup (telemetry enabled)
vpn	CSCtn56376	AC unable to access the root ca in firefox using Linux
webvpn-lb	CSCti07859	AC reports 'certificate validation failed' with VPN LB intermittently

Host Scan Engine Caveats

Caveats Reported with Host Scan Engine Update 3.0.11033

Caveats Resolved by Host Scan Engine Update 3.0.11033

Defect ID	Description
CSCtk12042	CSDM: Label "Win7" in prelogin OS check is not clearly visible
CSCto40355	Improve HostScan logging: Label non-warning messages as debug
CSCtx4570	HostScan consumes a large amount of CPU time
CSCty23613	HostScan fails user level process checks on Windows7 64 bit
CSCua31894	HostScan does not detect Microsoft Forefront Endpoint Protection 2010
CSCua64423	HostScan reports Sophos AV Virus Def Last Update incorrectly on MacOSX
CSCua97001	HostScan does not detect Free Avast AV 7.x software on MAC OS
CSCub02626	HostScan Engine 3.0.08062 AS support chart should not list 'Eset'
CSCub05542	HostScan Weblaunch does not work on Windows 8
CSCub10948	Hostscan reports "elevationrequired" with Eset AV

Defect ID	Description
CSCub16606	HostScan does not support Virus Security Zero v12
CSCub19730	HostScan doesn't report "lastupdate" value for Kaspersky 11.x
CSCub29350	HostScan reports Windows 7 as OS on Windows 8
CSCub56424	HostScan crashes on Mac OS X 10.5
CSCub59068	HostScan Weblaunch fails when using Java 6
CSCub59103	HostScan Weblaunch when using Internet Explorer with Java 7
CSCub70132	HostScan Weblaunch fails with Internet Explorer 10 and ActiveX
CSCuc42875	HostScan Weblaunch fails on upgrade when using ActiveX
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

Open Caveats in Host Scan Engine 3.0.11033

Defect ID	Headline
CSCud15337	Host Scan takes a long time to report information with 360 AV

Caveats Resolved by Host Scan Engine Update 3.0.08066

Defect ID	Headline
CSCtz64181	CSD: Hostscan - Add support for Microsoft Essentials AV Version 4
CSCua97239	MSE 4.x Data File time is not available

Caveats Resolved by Host Scan Engine Update 3.0.7042

Defect ID	Headline
CSCtw96017	POSTURE: [libcsd+3661] vpnui.exe: c0000005 (Crash 32bit)
CSCtx22002	POSTURE: [cscan!restore_ie_history+102] cscan.exe: c0000005 (Crash 32bit
CSCtw70984	cscan.exe errors keep popping up modal with 3.0.5MR - CoreUtils.dll
CSCtx01243	HS is failing as of build 3.0.6025 - XML parsing checkin potential
CSCtl00606	CSD Messaging needs to be reworked
CSCts26155	Host Emulation Detection not working on XP-64 bit
CSCtu69657	Un-installation of older predeploy kit not happening automatically.
CSCtu69444	hostscan-win-build-pre-deploy-k9.msi file

Caveats Resolved by Host Scan Engine Update 3.0.5009

Identifier	Headline
CSCts32184	HS:clean up persistent HostScan sessions.

Caveats Resolved by Host Scan Engine Update 3.0.4216

Identifier	Headline
CSCtr35869	Telemetry fails to detect AV(McAfee) is installed
CSCtq31755	CSD: Prelogin Check cannot check for Root certificate on Mac OS X clients

Caveats Resolved by Host Scan Engine Update 3.0.4207

Identifier	Headline
CSCtq48037	DOC: Need to remove wrong doc on csd Prelogin Cert check for MAC
CSCtq68002	CSD: Error 1920 when installing CSD 3.6.181 MSI on French Windows 7
CSCtq86204	Cscan popups taking place every minute
CSCtr20825	libcsd support for input callbacks was lost in 3.6 release

Caveats Resolved by Host Scan Engine Update 3.0.4016

Identifier	Headline
CSCsw17514	CSD: Deny access if emulation message box has blank button
CSCtd26933	CSD: Hostscan returns protection=”vault” with XP 64,should return “secure desktop”
CSCtk99496	Hostscan Prelogin Error on AnyConnect on Red Hat 5.3 when FIPS enabled
CSCtn93301	CSD 3.5 fails to validate Sophos AV 7.x on Mac OSX
CSCto45087	We need a way to roll over logs like AnyConnect VPN RollingLogger CSCtl17920 CSD only logs the last connection attempt
CSCto65864	Improper return value for the Kaspersky Antivirus CSCtn87540 CSD Add support for Avast 6.0
CSCto96682	AnyConnect Hostscan module noisy log warnings
CSCtq00045	Vault login denied when Host Scan incorrectly reports main.exe not running
CSCtq08733	cscan.exe consuming 195MB of memory and climbing
CSCtq18019	CSD weblaunch with ActiveX fails (Java OK) - Fingerprints do not match
CSCtq61788	Expired cert with CSD's Java file....
CSCtq81064	DOC: CSD does not support Symantec Endpoint Protection 12.x antispyware
CSCtq92552	CSD: HostScan fails to check LastUpdate for Microsoft Forefront AV

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.

Related Documentation

For more information, see the following documents:

- *Cisco AnyConnect Secure Mobility Solution Guide*
- *IronPort AsyncOS for Web User Guide*
- *IronPort AsyncOS 7.0 for Web Release Notes*
- *Navigating the Cisco ASA 5500 Series Documentation*
- *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*
- *AnyConnect and Host Scan Antivirus, Antispyware, and Firewall Support Charts*
- *Anywhere Plus Administration Guide, Release 1.2*

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.