Release Notes for Cisco AnyConnect Secure Mobility Client, Release 2.5

Updated: August 10, 2012

This document includes the following sections:

- Caveats
- Notices/Licensing
- Related Documentation

Introduction

These release notes are for all Cisco AnyConnect Secure Mobility Client, Release 2.5 versions.

Note We removed Releases 2.5.2001 and 2.5.1025 from the AnyConnect Software Download page because they have a regression issue with VPN load balancing (CSCtk01166). If you are running one of these releases in a VPN load balancing environment, we strongly recommend upgrading.

We changed the name of the Cisco AnyConnect VPN Client to the *Cisco AnyConnect Secure Mobility Client*; the product name change is in transition, and may not be complete in all places.

The Cisco AnyConnect Secure Mobility client provides remote users with secure VPN connections to the Cisco ASA 5500 Series Adaptive Security Appliance using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol.

AnyConnect provides remote end users with the benefits of a Cisco SSL VPN client, and supports applications and functions unavailable to a clientless, browser-based SSL VPN connection. It runs on Microsoft Windows, Windows Mobile, Linux, and Mac OS X, and supports connections to IPv6 resources over an IPv4 network tunnel. You can upload the client to the ASA to automatically download to remote users when they log in, or you can download and install it on the endpoint. You can configure the ASA to uninstall AnyConnect from the endpoint after the connection terminates, or it can remain on the remote PC for future SSL VPN connections.

In addition to the Cisco Adaptive Security Appliance 5500 Series, Cisco IOS Release 15.1(2)T supports the AnyConnect Secure Mobility client. For more information, see the Cisco IOS SSL VPN Data Sheet.

Downloading the Latest Version

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

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 Login to Cisco.com.

Step 3 Click **Download Software**.

Step 4 Expand the **Latest Releases** folder and click **2.5.6005.**

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, Configuring the Security Appliance to Deploy AnyConnect in *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5* to install the packages onto an ASA or to deploy AnyConnect using your enterprise software management system.

Important AnyConnect, CSD, and Host Scan Interoperability Information

AnyConnect 2.5.6005 is compatible with Host Scan 3.0.08057 or later versions and CSD 3.6.6020 or later versions. AnyConnect 2.5.6005 is not compatible with earlier versions of Host Scan or CSD.

⚠
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 1   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 2   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

Changes in AnyConnect 2.5.6005

AnyConnect 2.5.6005 specifies new compatibility requirements between AnyConnect, Host Scan, and CSD as described in Important AnyConnect, CSD, and Host Scan Interoperability Information on page page 3 and resolves the caveats in Table 1.

Changes in AnyConnect 2.5.3055

AnyConnect Release 2.5.3055 is a maintenance release that resolves the caveats in Table 2.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.3054

AnyConnect Release 2.5.3054 is a maintenance release that resolves the caveat in Table 4.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.3051

Compatibility with Global Site Selector Devices

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. 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.

LZS Compression

Cisco now supports compression for DTLS and TLS on AnyConnect 3.0.3047 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.x or later for support of the LZS compression feature.

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.

Lion Support

AnyConnect 2.5.3051 provides support for Lion OS X 10.7.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 doing Hostscan or Weblaunch with Safari on OS X 10.7.

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.

Changes in AnyConnect 2.5.3046

AnyConnect Release 2.5.3046 is a maintenance release that resolves the caveat in Table 8. The fix resolves a certificate-based installation issue on Mac OS X and Linux only.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.3041

Network Location Awareness for Windows

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.

Changes in AnyConnect 2.5.2019

AnyConnect Release 2.5.2019 is a maintenance release that resolves the caveat in Table 11.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.2018

AnyConnect Release 2.5.2018 is a maintenance release for Cisco I.T. use only.

Changes in AnyConnect 2.5.2017

AnyConnect Release 2.5.2017 is a maintenance release that resolves the caveat in Table 13.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.2014

AnyConnect Release 2.5.2014 is a maintenance release that resolves the caveat in Table 14.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.2011

AnyConnect Release 2.5.2010 is a maintenance release that resolves the caveat in Table 15.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.2010

AnyConnect Release 2.5.2010 is a maintenance release that resolves the caveats in Table 17.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.2006

AnyConnect Release 2.5.2006 is a maintenance release that resolves the caveats in Table 18.

No new features have been introduced with this release.

Changes in AnyConnect 2.5.2001

AnyConnect Release 2.5.2001 is a maintenance release that resolves the caveats in Table 19.

No new features have been introduced with this release.

Changes Introduced in AnyConnect 2.5.1025

AnyConnect Release 2.5.1025 supports the following new features.

Local Proxy Connection Support

By default, AnyConnect now lets users establish a VPN session through a transparent or non-transparent proxy on the local PC.

Some examples of elements that provide a transparent proxy service include:

- Acceleration software provided by some wireless data cards
- Network component on some antivirus software, such as Kaspersky.

AnyConnect supports this feature on the following Microsoft OSs:

- Windows 7 (32-bit and 64-bit)
- Windows Vista (32-bit and 64-bit)—SP2 or Vista Service Pack 1 with KB952876.
- Windows XP SP2 and SP3.

Support for this feature requires either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.

To use the ASDM AnyConnect Profile Editor to disable this feature, open the Preferences (cont) window and uncheck **Allow Local Proxy Connections** near the top of the panel.

Alternatively, you can use a text editor to insert the XML tag `<AllowLocalProxyConnections>` into the AnyConnect profile. The options are true and false. For example:

```
<ClientInitialization>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
</ClientInitialization>
```

Pause and Resume Support for the Trusted Network Policy

If you set the trusted network policy to pause, and a user then establishes a VPN session outside the network, then enters a network configured as trusted, AnyConnect suspends the VPN session instead of disconnecting it. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.

The ASA idle timer starts when the user's session becomes inactive as a result of leaving the untrusted network and stops when the session resumes in the untrusted network. Before configuring this feature, adjust both the Maximum Connect Time and Idle Timeout values on the ASDM Group Policy General panel.

AnyConnect supports this feature on the following OSs:

- Windows 7 (32-bit and 64-bit)
- Windows Vista (32-bit and 64-bit)—SP2 or Vista Service Pack 1 with KB952876.
- Windows XP SP2 and SP3.
- Mac OS 10.5 and 10.6.x

Support for this feature requires either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.

To use the Profile Editor to set the trusted network policy to pause, open the Preferences (cont) window and choose **Pause** next to the **Trusted Network Policy** parameter.

Alternatively, you can use a text editor to change value of the XML tag `<TrustedNetworkPolicy>` in the AnyConnect profile. The following example shows a complete trusted network policy configuration:

```
<ClientInitialization>
<AutomaticVPNPolicy>true
    <TrustedDNSDomains>*.cisco.com</TrustedDNSDomains>
    <TrustedDNSServers>161.44.124.*,64.102.6.247</TrustedDNSServers>
    <TrustedNetworkPolicy>Pause</TrustedNetworkPolicy>
    <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
</AutomaticVPNPolicy>
</ClientInitialization>
```

Authentication Timeout Control

By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out.

The AnyConnect profile now lets you specify the authentication timeout value. Specify the number of seconds in the range 10–120.

AnyConnect supports this feature on all OSs supported by AnyConnect.

Support for this feature requires either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.

To use the Profile Editor to change the authentication timer, open the Preferences (cont) window and enter the number of seconds into the **Authentication Timeout Values** field.

Alternatively, you can use a text editor to add the XML tag `<AuthenticationTimeout>` to the AnyConnect profile. The following example sets the authentication timeout to 20 seconds:

```
<ClientInitialization>
    <AuthenticationTimeout>20</AuthenticationTimeout>
</ClientInitialization>
```

Microsoft Internet Explorer Proxy Lockdown Control

By default, AnyConnect hides the Connections tab in Microsoft Internet Explorer for the duration of the AnyConnect VPN session. AnyConnect 2.5.1 supports the ASA group policy configuration of the Microsoft Internet Explorer Proxy Lockdown Control feature introduced in ASA Releases 8.2.3, 8.3.2, and later. This feature lets you disable the default behavior.

Using the default behavior prevents users from specifying a proxy service and changing LAN settings. Preventing user access to these settings enhances endpoint security during the AnyConnect session.

Disabling the default behavior lets users specify the proxy service to use and change LAN settings during the AnyConnect session.

AnyConnect supports this feature on the following Microsoft OSs:

- Windows 7 (32-bit and 64-bit)
- Windows Vista (32-bit and 64-bit)—SP2 or Vista Service Pack 1 with KB952876.
- Windows XP SP2 and SP3.

Support for this feature requires either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.

To prevent AnyConnect from hiding the Connections tab, use the ASA **msie-proxy lockdown disable** command in group-policy configuration mode. The following example does not hide the Connections tab:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy lockdown disable
```

The following example hides the Connections tab for the duration of the AnyConnect session:

```
hostname(config-group-policy)# msie-proxy lockdown enable
```

Changes Introduced in AnyConnect 2.5.0217

AnyConnect Release 2.5.0217 supports the following new features on Windows 7, Vista, and XP; and Mac OS X 10.5 and 10.6.x:

- Post Log-in Always-on VPN
- Connect Failure Policy
- Captive Portal Hotspot Detection
- Captive Portal Remediation
- Client Firewall with Local Printer and Tethered Device Support
- Optimal Gateway Selection
- Quarantine
- AnyConnect Profile Editor

Post Log-in Always-on VPN

As an administrator, you can configure AnyConnect to establish a VPN session automatically after the user logs in to a computer. The VPN session remains open until the user logs out of the computer. If the physical connection is lost, the session remains open, and AnyConnect continually attempts to reestablish the physical connection with the ASA to resume the VPN session.

(Post log-in) always-on VPN enforces corporate policies to protect the computer from security threats by preventing access to Internet resources when it is not in a trusted network.

Always-on VPN requires a valid server certificate configured on the ASA; otherwise, it fails and logs an event indicating the certificate is invalid.

⚠ **Caution** Ensure your server certificates can pass strict mode if you configure always-on VPN.

With always-on enabled, the client does not support connecting through a proxy.

The ASA lets you configure dynamic access policies, group policies, or both to exempt certain individuals from an always-on VPN setting.

If an AnyConnect policy enables always-on VPN and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.

AnyConnect supports a Disconnect button for always-on VPN sessions. If you enable it, AnyConnect displays a Disconnect button upon the establishment of a VPN session. Users of always-on VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as the following:

- Performance issues with the current VPN session.
- Reconnection issues following the interruption of a VPN session.

⚠ **Caution** For the reasons noted above, disabling the Disconnect button can at times hinder or prevent VPN access.

Do not attempt to configure always-on VPN until you have read all of the instructions and understand its requirements and implications, as detailed in the following sections in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*. When using always on, the integrity of your network must be well defined. As such, CRL Distribution Points for the secure gateway's server certificate must be available for verification by a client on a public network.

- Post Log-in Always-on VPN
- Disconnect Button for Always-on VPN

Connect Failure Policy

The connect failure policy determines whether the computer can access the Internet if always-on VPN is enabled and AnyConnect cannot establish a VPN session (for example, when a secure gateway is unreachable). The fail-close policy disables network connectivity–except for VPN access. The fail-open policy permits network connectivity. Regardless of the connect failure policy, AnyConnect continues to try to establish the VPN connection. The following table explains the fail open and fail close policies:

Always-on VPN Connect Policy	Scenario	Advantage	Trade-off
Fail open	AnyConnect fails to establish or reestablish a VPN session. This failure could occur if the secure gateway is unavailable, or if AnyConnect does not detect the presence of a captive portal (often found in airports, coffee shops and hotels).	Grants full network access, letting users continue to perform tasks where access to the Internet or other local network resources is needed.	Security and protection are not available until the VPN session is established. Therefore, the endpoint device may get infected with web-based malware or sensitive data may leak.
Fail close	Same as above except that this option is primarily for exceptionally secure organizations where security persistence is a greater concern than always-available network access.	The endpoint is protected from web-based malware and sensitive data leakage at all times because all network access is prevented except for local resources such as printers and tethered devices permitted by split tunneling.	Until the VPN session is established, this option prevents all network access except for local resources such as printers and tethered devices. It can halt productivity if users require Internet access outside the VPN and a secure gateway is inaccessible.

⚠ **Caution**   A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. AnyConnect detects most captive portals, described in Captive Portal Hotspot Detection and Remediation; however, if it cannot detect a captive portal, a connect failure closed policy prevents all network connectivity.

If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy always-on VPN with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot

program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.

Do not attempt to configure a connect failure policy until you have read all of the instructions and understand the requirements and implications, as detailed in Connect Failure Policy for Always-on VPN in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*.

Captive Portal Hotspot Detection

Many facilities that offer Wi-Fi and wired access, such as airports, coffee shops, and hotels, require the user to pay before obtaining access, agree to abide by an acceptable use policy, or both. These facilities use a technique called *captive portal* to prevent applications from connecting until the user opens a browser and accepts the conditions for access.

AnyConnect displays the `Unable to contact VPN server` message on the GUI if it cannot connect, regardless of the cause. If a captive portal is not present, AnyConnect continues to attempt to connect to the VPN and updates the status message accordingly.

If always-on VPN is enabled, the connect failure policy is closed, captive portal remediation is disabled, and AnyConnect detects the presence of a captive portal, the AnyConnect GUI displays the following message once per connection and once per reconnect:

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

If AnyConnect detects the presence of a captive portal and the AnyConnect configuration differs from that described above, the AnyConnect GUI displays the following message once per connection and once per reconnect:

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

Captive Portal Remediation

Captive portal remediation is the process of satisfying the requirements of a captive portal hotspot to obtain network access. By default, the connect failure policy prevents captive portal remediation because it restricts network access. You can configure AnyConnect to lift restricted access to let the user satisfy the captive portal requirements. You can also specify the duration for which AnyConnect lifts restricted access. For instructions, see Captive Portal Remediation in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*.

Client Firewall with Local Printer and Tethered Device Support

When users connect to the ASA, all traffic is tunneled through the connection and users cannot access resources on their local network. This includes printers, cameras, and Windows Mobile devices (tethered devices) that sync with the local computer. Enabling Local LAN Access in the client profile resolves this problem, however it can introduce a security or policy concern for some enterprises as a result of unrestricted access to the local network. You can use the ASA to deploy endpoint OS firewall capabilities to restrict access to particular types of local resources, such as printers and tethered devices.

To do so, enable client firewall rules for specific ports for printing. The client distinguishes between inbound and outbound rules. For printing capabilities, the client opens ports required for outbound connections, but blocks all incoming traffic. The client firewall is independent of the always-on feature.

Note Be aware that users logged in as administrators have the ability to modify the firewall rules deployed to the client by the ASA. Users with limited privileges cannot modify the rules. For either user, the client reapplies the rules when the connection terminates.

If you configure the client firewall, and the user authenticates to an Active Directory (AD) server, the client still applies the firewall policies from the ASA. However, the rules defined in the AD group policy take precedence over the rules of the client firewall.

Note Host Scan and some third-party firewalls can interfere with the firewall function configured on the ASA group policy. With third-party firewalls, traffic is passed only if both the AnyConnect client firewall and the third-party firewall permit the traffic type. If the third-party firewall blocks a specific traffic type that the AnyConnect client permits, the client blocks the traffic.

Differences in Firewall Behavior between Mac and Windows

For Windows computers, deny rules take precedence over allow rules in Windows Firewall. If the ASA pushes down an allow rule to the AnyConnect client, but the user has created a custom deny rule, the AnyConnect rule is not enforced.

On Mac computers, the AnyConnect client applies rules sequentially in the same order the ASA applies them. Global rules should always be last.

Windows users whose firewall service must be started by the AnyConnect client (not started automatically by the system) may experience a noticeable increase in the time it takes to establish a VPN connection.

Due to limitations of the OS, the client firewall policy on computers running Windows XP is enforced for inbound traffic only. Outbound rules and bidirectional rules are ignored. This would include firewall rules such as **permit ip any any**.

For instructions on how to use the firewall to support local printers and tethered devices, see Client Firewall with Local Printer and Tethered Device Support in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*

Optimal Gateway Selection

Using the Optimal Gateway Selection (OGS) feature, you can minimize latency for Internet traffic without user intervention. With OGS, the AnyConnect client identifies and selects which secure gateway is best for connection or reconnection.

OGS begins upon first connection or upon a reconnection at least four hours after the previous disconnection. Users who travel to distant locations connect to a secure gateway nearer to the new location for better performance. Your home and office will get similar results from the same gateway, so no switch of secure gateways will typically occur in this instance. Connection to another secure gateway occurs rarely and only occurs if the performance improvement is at least 20%.

Note   You can configure these threshold values using the Profile Editor. By optimizing these values for your particular network, you can find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials.

OGS is not a security feature, and it performs no load balancing between secure gateway clusters or within clusters. You can optionally give the end user the ability to enable or disable the feature.

The minimum round trip time (RTT) solution selects the secure gateway with the fastest RTT between the client and all other gateways. The client always reconnects to the last secure gateway if the time elapsed has been less than four hours. Factors such as load and temporary fluctuations of the network connection may affect the selection process, as well as the latency for Internet traffic.

OGS supports computers running:

- Windows 7, Vista, and XP
- Mac OS X 10.5 and 10.6.x

You use the second Preferences menu option of the Profile Editor to control the activation and deactivation of the OGS and to specify whether end users may control the feature themselves.

If OGS is enabled when the AnyConnect client GUI is started, **Automatic Selection** displays in the Connect To drop-down menu on the Cisco AnyConnect Connection tab. You cannot change this selection. OGS automatically chooses the optimal secure gateway and displays the selected gateway on the status bar. You may need to click **Select** to start the connection process.

It contacts only the primary servers to determine the optimal one. Once determined, the connection algorithm is as follows:

1. Attempt connection to the optimal server.
2. If that fails, try the optimal server's backup server list.
3. If that fails, try each remaining server in the OGS selection list, as ordered by its selection results.

If you made the feature user controllable, the user can manually override the selected secure gateway with the following steps:

Step 1   If currently connected, click **Disconnect**.

Step 2   Open the Preferences tab and uncheck **Enable Optimal Gateway Selection**.

Step 3   Choose the desired secure gateway.

Note   If AAA is being used, end users may have to re-enter their credentials when transitioning to a different secure gateway. The use of certificates eliminates this.

For more information about OGS, see Optimal Gateway Selection in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*.

Quarantine

Through the use of quarantine, you can restrict a particular client who already has an established tunnel through a VPN. The ASA applies restricted ACLs to a session to form a restricted group, based on the selected dynamic access policy. When an endpoint is not compliant with an administratively defined policy, the user can still access services for remediation (such as updating the antivirus and so on), but restrictions are placed upon the session. After the remediation occurs, the user can reconnect, which invokes a new posture assessment. If this assessment passes, the user connects.

Note Using the Reconnect button, the user can initiate a disconnect and start a new tunnel after remediation if always-on VPN is enabled.

Quarantine requires an Advanced Endpoint Assessment license specified in the adaptive security license configuration. The advanced endpoint assessment remediates endpoints that do not comply with dynamic policy requirements for antivirus, antispyware, and firewall applications; and any associated application definition file requirements. Advanced endpoint assessment is a Cisco Secure Desktop Host Scan feature, so AnyConnect supports quarantine on the OSs that the version of Cisco Secure Desktop supports. Go to *Supported VPN Platforms* and refer to the "Cisco Secure Desktop" section that identifies the release you are using. The table identifies the OSs that Host Scan supports.

ASA Release 8.3(1) or later features dynamic access policies and group policies that support a user message to display on the AnyConnect UI for the duration of the quarantine state. Quarantine does not require the ASA upgrade; only the user message requires it. If you upgrade the ASA to 8.3(1), we recommend that you also upgrade ASDM to Release 6.3(1) or later so that you can use it to configure the new features.

For instructions, see Using Quarantine to Restrict Non-Compliant Clients in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*.

AnyConnect Profile Editor

The AnyConnect profile editor is a convenient GUI-based configuration tool you can use to configure the AnyConnect client profile—an XML file containing settings that control client features. Previously, you could only change profile settings manually by editing the XML tags in the profile.

The AnyConnect client software package for each operating system, version 2.5 and later, contains the profile editor. You can launch the profile editor from ASDM (version 6.3(1) or later) if the client software package is loaded on the ASA as an SSL VPN client image.

Note If you do not upgrade ASDM to version 6.3(1) or later, use the XML examples in the following sections as a guide to modifying the AnyConnect profile to enable each feature.

If you load multiple client packages, ASDM loads the profile editor from the newest client package. This approach ensures the editor displays the features for the newest client loaded, as well as the older clients.

The Profile Editor supports only Java SE 1.6 on the client computer.

To activate the profile editor in ASDM, load the AnyConnect client software package as an SSL VPN image and go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

For more information about using the profile editor, see the sections beginning with Introduction to the AnyConnect Profile Configuration in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5.*

AnyConnect 2.5 Guidelines

The following sections provide guidelines that are new in AnyConnect 2.5 and guidelines noted in earlier releases that are still in effect.

New Guidelines

The following guidelines are new in AnyConnect 2.5:

- Preventing Other Devices in a LAN from Displaying Hostnames on page 15
- Messages in the Localization File Can Span More than One Line on page 16
- IOS Support on page 16
- Change to AnyConnect Pop-Up Messages on page 16
- Revocation Message on page 17
- MTU Adjustment on Group Policy May Be Required on page 17
- AnyConnect for Mac OS Performance when Behind Certain Routers on page 17
- Preventing Windows Users from Circumventing Always-on on page 17

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. To do so,

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.

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. "
```

IOS Support

Cisco supports Anyconnect 2.5 VPN access to IOS Release 15.1(2)T functioning as the secure gateway; however, you cannot use the features introduced in AnyConnect 2.5 with IOS.

The new AnyConnect 2.5 features that do not support are IOS are:

- Post Log-in Always-on VPN
- Connect Failure Policy
- Captive Portal Hotspot Detection and Remediation
- Client Firewall with Local Printer and Tethered Device Support
- Optimal Gateway Selection
- Quarantine
- AnyConnect Profile Editor

Refer to http://www.cisco.com/go/fn for additional IOS feature support information.

Change to AnyConnect Pop-Up Messages

For release 2.5, we created this new message displayed to AnyConnect users:

```
AnyConnect cannot confirm it is connected to your secure gateway. The local network may
not be trustworthy. Please try another network.
```

Users receive the new message when the client cannot validate the certificate from the ASA for either of these reasons:

- An entity between the AnyConnect client and the ASA is giving the client an invalid certificate in order to sniff traffic (which could be a *man-in-the-middle* attack). Switching networks could alleviate the problem.
- The server certificate configuration on the ASA is incorrect. If so and if strict-mode is enabled, all users will experience this issue. You can resolve this by putting the proper server certificate on the ASA that can be validated by the AnyConnect client from the certificate authority.

The new message replaces and consolidates the following messages displayed by releases 2.4 and earlier:

- ```
  Connection attempt has failed due to server certificate problem.
  ```
- ```
  Local policy prohibits the acceptance of untrusted server certificates. A VPN
  connection will not be established.
  ```

Revocation Message

An AnyConnect GUI 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) and 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.

MTU Adjustment on Group Policy May Be Required

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. To access the MTU with ASDM, choose **Configuration > Network (Client) Access > Group Policies > Add** or **Edit > Advanced > SSL VPN Client**.

AnyConnect for Mac OS Performance when Behind Certain Routers

When the AnyConnect client for Mac OS connects to the 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, set the MTU for the AnyConnect adaptor to a lower value using the following command from the OS X command line:

sudo ipconfig cscotun0 mtu 1200 (For Mac OS10.5 or earlier)

sudo ipconfig utun0 mtu 1200 (For Mac OS10.6 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

Guidelines from Previous Releases Still in Effect

The *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*, incorporates most of the guidelines reported in previous releases that remain in effect. The following sections address the remaining guidelines.

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, 10.4 and higher

AnyConnect does not support:

- Smart cards on Linux
- PKCS #11 devices

Responding to a TUN/TAP Error Message with Mac OS X 10.5

During the installation of AnyConnect on Mac OS X 10.5 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 10.6 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, then re-install AnyConnect.

64-bit Internet Explorer Not Supported

AnyConnect installation via WebLaunch does not support 64-bit versions of Internet Explorer. Please instruct users of x64 (64-bit) Windows versions supported by AnyConnect to use the 32-bit version of Internet Explorer or Firefox to install WebLaunch. (At this time, Firefox is available only in a 32-bit version.)

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 (e.g., Connectify or Virtual Router).

AnyConnect Requires That the ASA Be Configured to Accept TLSv1 Traffic

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.

Flexibility in the Sequence and Method Used to Install Start Before Logon and DART Components

Previously, in order to use the Start Before Logon components for Windows, the same installation method was required for both AnyConnect and the Start Before Logon components. Both needed to be pre-deployed or both needed to be web-deployed. AnyConnect Release 2.4 eliminates this requirement. This allows the client to be deployed by one method and, perhaps at a later time, the Start Before Logon components to be installed by the same or another method. The Start Before Logon component still has the requirement that AnyConnect be installed first.

Another new behavior for AnyConnect Release 2.4 is that if SBL or DART is manually uninstalled from an endpoint that then connects, these components will be re-installed. This behavior will only occur if the head-end configuration specifies that these components be installed and the preferences (set on the endpoint) permit upgrades. Previously these components would not be re-installed in this scenario without uninstalling and re-installing AnyConnect.

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, Release 2.5*.

AnyConnect 2.5 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
- Windows Mobile

Security Appliance Software Requirements

For the latest fixes, the ASAs must be running the following:

- ASA Release 8.3(1)
- ASDM 6.3(1)
- Cisco Secure Desktop 3.5.2008

AnyConnect 2.5 requires the following:

- ASA 8.0(2) or later.
- ASDM 6.1(3) or later.

The minimum supported version of Cisco Secure Desktop is 3.2.2 or later.

We also recommend upgrading to ASDM 6.3(1) or later so that you can use the AnyConnect profile editor to configure many of the AnyConnect features. You can use ASDM 6.3(1) in combination with ASA 8.0(2) or later. If you choose not to upgrade ASDM, 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 8.3(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.

Microsoft Windows

For WebLaunch, use Internet Explorer 6.0 or later or Firefox 3.0+, and enable ActiveX or install Sun JRE 1.4+.

Windows Versions

- Windows 7 (32-bit and 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 is compatible with 3G data cards which interface with Windows 7 via a WWAN adapter.

- Windows Vista (32-bit and 64-bit)—SP2 or Vista Service Pack 1 with KB952876.

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

- Windows XP SP2 and SP3.

  > ✎
  > **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.

Windows Requirements

- Pentium class processor or greater.
- x86 (32-bit) or x64 (64-bit) processors.
- 5 MB hard disk space.
- RAM:
  - 256 MB for Windows XP.
  - 512 MB for Windows Vista.
  - 512 MB for Windows 7.
- Microsoft Installer, version 3.1.

Linux

The following sections show the supported Linux distributions and requirements.

Linux Distributions

- Red Hat Enterprise Linux 5 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 or biarch 64-bit processor

- 32 MB RAM.

- 20 MB hard disk space.

- Superuser privileges.

- libstdc++ users must have libstdc++ version 3.3.2 (libstdc++.so.5) or higher, but below version 4.

- Firefox 2.0 or later with libnss3.so installed in /usr/local/lib, /usr/local/firefox/lib, or /usr/lib. Firefox must be installed in /usr/lib or /usr/local, or there must be a symbolic link in /usr/lib or /usr/local called firefox that points to the Firefox installation directory.

- libcurl 7.10 or later.

- openssl 0.9.7a or later.

- 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.

Note AnyConnect SMC 2.5 reportedly runs on 64-bit Linux, although we do not support it.

Mac OS X

AnyConnect 2.5 supports the following versions of Mac OS:

- Mac OS X 10.5

- Mac OS X 10.6.x (32-bit and 64-bit)

• MAC OS X 10.7 (for release 2.5.3051 or later)

AnyConnect requires 50MB of hard disk space.

If you upgrade from one major Mac OS X release to another (for example 10.5 to 10.6), 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.

Windows Mobile

Note End of Life has been announced for all versions of AnyConnect for Windows Mobile.

Refer to the *End-of-Life Announcement for the Cisco AnyConnect Secure Mobility Client on Windows Mobile* for support and availability details.

Although the devices listed below were originally qualified with AnyConnect for Windows Mobile 2.5.02517, these releases were removed from customer availability due to a *security vulnerability*. Please contact your authorized support representative for further details.

AnyConnect 2.5 is compatible with Windows Mobile 6.5, 6.1, 6.0 and 5.0 Professional and Classic for touch-screen devices only. Users have reported success with most touch-screen devices running these versions of Windows Mobile. However, to ensure interoperability, we guarantee compatibility only with the devices we test, as follows:

• HTC Imagio running Windows Mobile 6.5
• HTC Tilt 2 running Windows Mobile 6.5
• HTC Touch running Windows Mobile 6.0
• HTC TyTN running Windows Mobile 5.0
• Samsung Epix running Windows Mobile 6.1
• Samsung Omnia Pro 4 running Windows Mobile 6.5
• Samsung Omnia running Windows Mobile 6.1
• Samsung Saga running Windows Mobile 6.1

AnyConnect Support Policy

We support all 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.

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 the Severities 2 and 3 caveats:

- Caveats Resolved by AnyConnect 2.5.6005
- Caveats Resolved by AnyConnect 2.5.3055
- Open Caveats in Release 2.5.3055
- Caveats Resolved by AnyConnect 2.5.3054
- Open Caveats in Release 2.5.3054
- Caveats Resolved by AnyConnect 2.5.3051
- Open Caveats in Release 2.5.3051
- Caveats Resolved by AnyConnect 2.5.3046
- Open Caveats in AnyConnect 2.5.3041 and 2.5.3046
- Caveats Resolved by AnyConnect 2.5.3041
- Caveat Resolved by AnyConnect 2.5.2019
- Open Caveats in AnyConnect 2.5.2014–2.5.2019
- Caveat Resolved by AnyConnect 2.5.2017
- Caveat Resolved by AnyConnect 2.5.2014
- Caveat Resolved by AnyConnect 2.5.2011
- Open Caveats in AnyConnect 2.5.2001–2.5.2011
- Caveats Resolved by AnyConnect 2.5.2010
- Caveats Resolved by AnyConnect 2.5.2006
- Caveats Resolved by AnyConnect 2.5.2001
- Caveats Resolved by AnyConnect 2.5.1025
- Open Caveats in AnyConnect 2.5.1025
- Caveats Resolved by AnyConnect 2.5.0217
- Caveats Resolved by AnyConnect 2.5.0217

Caveats Resolved by AnyConnect 2.5.6005

Table 1   Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.6005

Component	Identifier	Headline
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
posture-asa	CSCtx74235	CSD: Downloaders/ActiveX to fix validation of downloaded code
vpn	CSCti97331	API not checking file signature on CSD library
vpn	CSCtz94705	Need to disable install on 10.4 OS X

Caveats Resolved by AnyConnect 2.5.3055

Table 2 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.3055 resolves.

Table 2   Caveat Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.3055

ID	Headline
CSCtk18952	AnyConnect fails to connect if PtP interface does not have destination address
CSCts44278	AnyConnect fails with SBL and certificates on Windows 7

Open Caveats in Release 2.5.3055

Table 3 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Releases 2.5.3055.

Table 3   Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 2.5.3055

ID	Headline
CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
CSCsv49773	Ability to accommodate multiple head-end profiles
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
CSCta94621	Enable local LAN access not consistent with other split tunnel options
CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
CSCtc03052	SCEP fails in upgrade scenario
CSCtc17266	Private-side proxy on OS X does not support per-protocol proxy
CSCte42921	Get Unresolved Gateway Address when trying to connect

Table 3 **Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 2.5.3055**

ID	Headline
CSCtf20226	Make AnyConnect DNS with split tunnel behavior for Mac same as Windows
CSCtf56830	AC cert popup appears even when not requested by ASA
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
CSCtf90996	OGS selects inaccessible host
CSCtg01525	AnyConnect should have clear description for each error message
CSCtg04881	VPN downloaders always aborts first SSL handshake
CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
CSCtg31729	JPN: JPN message garbled when uninstallation runs without disconnection
CSCtg45505	VPN connection fails from network with unusual captive portal
CSCth85648	GUI: Auth challenge window - Mac is missing text - Windows ignoring CR/LF
CSCtj62029	Cannot establish tunnel with machine cert auth and untrusted server CA
CSCtn84747	Proxy auth problems when proxy offers multiple auth schemes
CSCto53984	pki-crl: crl download fails when always-on enabled
CSCtq02141	AnyConnect DNS issue when ISP DNS is on the same subnet as Public IP
CSCtq75832	AnyConnect does not perform auto route correction on Mac/Linux
CSCtr27865	Observing slow throughput when using AnyConnect Mac client
CSCtr75228	VPN client driver has encountered an error
CSCtr75253	csdlib.dll is corrupted and size of 0K
CSCtr75276	Experiencing frequent disconnects from VPN connection
CSCts46682	AnyConnect Linux init script issues

Caveats Resolved by AnyConnect 2.5.3054

Table 4 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.3054 resolves.

Table 4 **Caveat Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.3054**

ID	Headline
CSCtr20634	AC: Split-exclude route not working when overlapping a link-level route
CSCtr51718	UI exits without an informative message when Captive Portal is detected in SBL mode
CSCtr64798	[Lion] Critical error while connecting to certain head-ends

Open Caveats in Release 2.5.3054

Table 5 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility Client
Releases 2.5.3054.

Table 5   *Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 2.5.3054*

ID	Headline
CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
CSCsv49773	Ability to accommodate multiple head-end profiles
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
CSCta94621	Enable local LAN access not consistent with other split tunnel options
CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
CSCtc03052	SCEP fails in upgrade scenario
CSCtc17266	Private-side proxy on OS X does not support per-protocol proxy
CSCte42921	Get Unresolved Gateway Address when trying to connect
CSCtf20226	Make AnyConnect DNS with split tunnel behavior for Mac same as Windows
CSCtf56830	AC cert popup appears even when not requested by ASA
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
CSCtf90996	OGS selects inaccessible host
CSCtg01525	AnyConnect should have clear description for each error message
CSCtg04881	VPN downloaders always aborts first SSL handshake
CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
CSCtg31729	JPN: JPN message garbled when uninstallation runs without disconnection
CSCtg45505	VPN connection fails from network with unusual captive portal
CSCth85648	GUI: Auth challenge window - Mac is missing text - Windows ignoring CR/LF
CSCtj62029	Cannot establish tunnel with machine cert auth and untrusted server CA
CSCtk75358	AnyConnect compatibility issues with Microsoft Forefront
CSCtl12833	AC certificate prompt after network down with automatic cert selection
CSCtl23155	AnyConnect SBL fails with Novell netware
CSCtn84747	Proxy auth problems when proxy offers multiple auth schemes
CSCto53984	pki-crl: crl download fails when always-on enabled
CSCtq02141	AnyConnect DNS issue when ISP DNS is on the same subnet as Public IP
CSCtq75832	AnyConnect does not perform auto route correction on Mac/Linux
CSCtr27865	Observing slow throughput when using AnyConnect Mac client

Caveats Resolved by AnyConnect 2.5.3051

Table 6 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.3051 resolves.

Table 6   *Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.3051*

ID	Headline
CSCth83069	API fails to launch cached Downloader
CSCtq74504	VPN connection fails with link-local split-exclude network

Table 6   *Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.3051*

ID	Headline
CSCtq84525	AnyConnect 2.5.3041 CertPathValidatorException timestamp check failed
CSCtr19783	AnyConnect Weblaunch ignores proxy server setting

Open Caveats in Release 2.5.3051

Table 7 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Releases 2.5.3051.

Table 7   *Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 2.5.3051*

ID	Headline
CSCsm69213	AnyConnect does not perform auto route correction on Mac/Linux
CSCsv49773	Ability to accommodate multiple head-end profiles
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
CSCta94621	Enable local LAN access not consistent with other split tunnel options
CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
CSCtc03052	SCEP fails in upgrade scenario
CSCtc17266	Private-side proxy on OS X does not support per-protocol proxy
CSCte42921	Get Unresolved Gateway Address when trying to connect
CSCtf20226	Make AnyConnect DNS with split tunnel behavior for Mac same as Windows
CSCtf56830	AC cert popup appears even when not requested by ASA
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
CSCtf90996	OGS selects inaccessible host
CSCtg01525	AnyConnect should have clear description for each error message
CSCtg04881	VPN downloaders always aborts first SSL handshake
CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
CSCtg31729	JPN: JPN message garbled when uninstallation runs without disconnection
CSCtg45505	VPN connection fails from network with unusual captive portal
CSCth85648	GUI: Auth challenge window - Mac is missing text - Windows ignoring CR/LF
CSCtj62029	Cannot establish tunnel with machine cert auth and untrusted server CA
CSCtk75358	AnyConnect compatibility issues with Microsoft Forefront
CSCtl12833	AC certificate prompt after network down with automatic cert selection
CSCtl23155	AnyConnect SBL fails with Novell netware
CSCtn84747	Proxy auth problems when proxy offers multiple auth schemes
CSCto53984	pki-crl: crl download fails when always-on enabled
CSCtq02141	AnyConnect DNS issue when ISP DNS is on the same subnet as Public IP
CSCtq75832	AnyConnect does not perform auto route correction on Mac/Linux
CSCtr27865	Observing slow throughput when using AnyConnect Mac client

Caveats Resolved by AnyConnect 2.5.3046

Table 8 shows the caveat that AnyConnect Secure Mobility Client Release 2.5.3046 resolves.

Table 8   Caveat Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.3046

ID	Headline
CSCtq84525	Anyconnect 2.5.3041 CertPathValidatorException: timestamp check failed

Open Caveats in AnyConnect 2.5.3041 and 2.5.3046

Table 9 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility Client Releases 2.5.3041 and 2.5.3046.

Table 9   Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 2.5.3041 and 2.5.3046

ID	Headline
CSCsm69213	Anyconnect does not perform auto route correction on Mac/Linux
CSCsu52949	GUI pops up certificate warning prompts on every connection attempt
CSCsv49773	Ability to accommodate multiple head-end profiles
CSCsw37980	Needs more certificate matching events
CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
CSCsy34111	SVC MSIE proxy option auto does not work
CSCsy48762	WM: Split tunnel does not work with Anyconnect Mobile
CSCsz56742	Will not use certificates under certain ASA configuration
CSCta94621	Enable local LAN access not consistent with other split tunnel options
CSCtb73073	VPN establishment allowed while multiple local users logged in on MAC
CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
CSCtc03052	SCEP fails in upgrade scenario
CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
CSCte42921	Get Unresolved Gateway Address When Trying to Connect
CSCte73983	bad apple config may cause vpnagentd to fail
CSCtf20226	Make Anyconnect DNS w/ split tunnel behavior for Mac same as windows
CSCtf56830	AC cert popup appears even when not requested by ASA
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
CSCtf90996	OGS selects inaccessible host
CSCtg01525	Anyconnect should have clear description for each error msg
CSCtg04881	VPN Downloader always aborts first SSL handshake
CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection

Table 9   Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 2.5.3041 and 2.5.3046

ID	Headline
CSCtg45505	VPN connection fails from network with unusual captive portal
CSCth32206	Logging is insufficient for troubleshooting
CSCth35315	captive portal reconnect after resume blocks cisco nac agent discovery
CSCth85648	GUI: Auth challenge window - Mac is missing text - Win ignoring CR/LF
CSCtj62029	Can't establish tunnel with machine cert auth and untrusted server CA
CSCtk14009	AnyConnect 2.x/3.x: Public proxy PAC URL fails to connect
CSCtk36448	DOC: Anyconnect for Mac does not check System Keychain for Certificates
CSCtk75358	AnyConnect compatibility issues with Microsoft Forefront
CSCtl12833	AC certificate prompt after network down with automatic cert selection
CSCtl21430	DOC: Anyconnect 2.5 admin guide should include firewall config examples
CSCtl23155	Anyconnect SBL fails with Novell netware
CSCtn46629	DART does not collect files from localized paths
CSCtn84747	proxy auth problems when proxy offers multiple auth schemes
CSCto53984	pki-crl: crl download fails when always-on enabled
CSCtq02141	AnyConnect DNS Issue when ISP DNS is on same subnet as Public IP

Caveats Resolved by AnyConnect 2.5.3041

Table 10 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.3041 resolves.

Table 10   Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.3041

ID	Headline
CSCto76864	Anyconnect fails after few seconds connected on certain 3G cards.
CSCto53112	DNS Cache failure
CSCtj89377	CSD causes client crash on Mac
CSCto05439	Time out setting in the profile editor for websec does not work
CSCtl90819	Random Cert Validation Failures
CSCtf81226	AC Profile Editor: Disable Cert Selection option is not clear
CSCtj51376	IE Proxy setting is not restored after Anyconnect disconnect on Win 7
CSCtn96122	Opening Advanced Window Link While GUI Shutting Down Crashes GUI
CSCtk66387	WPAD doesn't work on Win7 + IE 8
CSCto00117	Tunnel resumption exhibits broken split tunnel (which is not configured)
CSCto08814	Routing Issue Gets Client Stuck Reconnecting
CSCto05492	VPN Connection Stuck Reconnecting and then Disconnecting
CSCtk78458	Anyconnect API crash in attach and detach
CSCtf94284	Anyconnect may show password in clear text in RAM

Table 10   Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.3041

ID	Headline
CSCtn75204	AnyConnect 3.0 VPN Server could not parse request with & or < in passwd
CSCtn89892	signal handling bug causes hostscan to scan twice per minute
CSCtn68171	Add ability for AC to detect wrong client cert CSP and generate event
CSCtn42751	Anyconnect + 'Retain VPN on logoff', case sensitivity not compatible wit
CSCtl79784	Crash from WER Data
CSCtn78403	cscan signature not checked before launch
CSCtk06308	AC failing to perform SCEP proxy enrollment - Profile () not found
CSCto73233	DOC: Anyconnect FIPS package has system-wide consequences.
CSCto73186	DOC Anyconnect FIPS module - details not documented
CSCtl45627	Connection to IPv6 enabled head end fails (Vista/Win7)
CSCtn87093	VPN: WinXP with TND strips DefaultGW and breaks trusted DNS settings
CSCth76124	Retain ASA DNS resolution throughout connection establishment

Caveat Resolved by AnyConnect 2.5.2019

Table 11 shows the caveat that AnyConnect Secure Mobility Client Release 2.5.2019 resolves.

Table 11   Caveat Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.2019

ID	Headline
CSCtn21228	AnyConnect Profile Editor enabling all Extended Key Usages causes error

Open Caveats in AnyConnect 2.5.2014–2.5.2019

Table 12 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility client Releases 2.5.2019, 2.5.2019, 2.5.2017, and 2.5.2014.

Table 12   Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 22.5.2014–2.5.2019

ID	Headline
CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client
CSCsm69213	Anyconnect does not perform auto route correction on Mac/Linux
CSCsu52949	GUI pops up certificate warning prompts on every connection attempt
CSCsu70199	IPv6: Network error: windows has detected and IP address conflict
CSCsv49773	Multiple local profiles for SG may result in using wrong settings
CSCsw37980	AC needs more certificate matching events
CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel

Table 12   *Open Caveats in Cisco AnyConnect Secure Mobility Client*
                Releases 22.5.2014–2.5.2019 (continued)

ID	Headline
CSCsy34111	SVC MSIE proxy option auto does not work
CSCsy48762	AnyConnect: Split tunnel does not work with Anyconnect Mobile
CSCsz56742	Will not use certificates under certain ASA configuration
CSCta94621	Enable local LAN access not consistent with other split tunnel options
CSCtb73073	Mac: VPN establishment allowed while multiple local users logged in
CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
CSCtc03052	SCEP fails in upgrade scenario
CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
CSCtc65842	Mac GUI crash with SCEP in FIPS mode
CSCte42921	Get Unresolved Gateway Address When Trying to Connect
CSCte73983	bad apple config may cause vpnagentd to fail
CSCtf04766	AnyConnect uses Windows system locale instead of install language
CSCtf06844	AnyConnect SCEP enrollment not working with ASA Per Group Cert Auth
CSCtf20226	Make anyconnect DNS w/ split tunnel behavior for Mac same as windows
CSCtf23946	Agent does not restore DNS Suffix search list if VA dies
CSCtf52183	SCEP enrollment on Mac makes private key exportable from keychain
CSCtf56830	AC cert popup appears even when not requested by ASA
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
CSCtf90996	OGS selects inaccessible host
CSCtf94284	Anyconnect may show password in clear text in RAM
CSCtg01304	Split-tunneling: filtering needs to be enforced on the VPN adapter
CSCtg01525	Anyconnect should have clear description for each error msg
CSCtg04881	VPN Downloader always aborts first SSL handshake
CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
CSCtg37737	AnyConnect cannot parse PAC file and does not connect to endpoint
CSCtg45505	VPN connection fails from network with unusual captive portal
CSCtg73736	Captive portal can't be remediated if remediation site in private space
CSCth32206	Logging is insufficient for troubleshooting
CSCth35315	captive portal reconnect after resume blocks cisco nac agent discovery
CSCth61000	Remove GetMUSHostAddr MUS messages when MUS is not enabled
CSCth93690	AnyConnect 2.x on MAC removing e-token will not allow reconnects
CSCti07859	AC reports 'certificate validation failed' with VPN LB intermittently
CSCtj36459	Cannot connect to tunnel groups with CSD enabled
CSCtj62029	Can't establish tunnel with machine cert auth and untrusted server CA

Caveat Resolved by AnyConnect 2.5.2017

Table 13 shows the caveat that AnyConnect Secure Mobility Client Release 2.5.2017 resolves.

Table 13 *Caveat Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.2017*

ID	Headline
CSCtj79104	Multicast traffic should not be tunneled with split-include tunneling config

Caveat Resolved by AnyConnect 2.5.2014

Table 14 shows the caveat that AnyConnect Secure Mobility Client Release 2.5.2014 resolves.

Table 14 *Caveat Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.2014*

ID	Headline
CSCte46102	AnyConnect unable to browse websites when connected

Caveat Resolved by AnyConnect 2.5.2011

Table 15 shows the caveat that AnyConnect Secure Mobility Client Release 2.5.2011 resolves.

Table 15 *Caveat Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.2011*

ID	Headline
CSCtk85347	Invalid certs result in connection breakage

Open Caveats in AnyConnect 2.5.2001–2.5.2011

Table 16 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility client Releases 2.5.2011, 2.5.2010, 2.5.2006, and 2.5.2001.

Table 16 *Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 2.5.2001–2.5.2011*

ID	Headline
CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client
CSCsm69213	Anyconnect does not perform auto route correction on Mac/Linux
CSCsu52949	GUI pops up certificate warning prompts on every connection attempt
CSCsu70199	IPv6: Network error: windows has detected and IP address conflict
CSCsv49773	Multiple local profiles for SG may result in using wrong settings
CSCsw37980	AC needs more certificate matching events
CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
CSCsy34111	SVC MSIE proxy option auto does not work

Table 16   Open Caveats in Cisco AnyConnect Secure Mobility Client Releases 2.5.2001–2.5.2011

ID	Headline
CSCsy48762	AnyConnect: Split tunnel does not work with Anyconnect Mobile
CSCsz56742	Will not use certificates under certain ASA configuration
CSCta94621	Enable local LAN access not consistent with other split tunnel options
CSCtb73073	Mac: VPN establishment allowed while multiple local users logged in
CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
CSCtc03052	SCEP fails in upgrade scenario
CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
CSCtc65842	Mac GUI crash with SCEP in FIPS mode
CSCte42921	Get Unresolved Gateway Address When Trying to Connect
CSCte46102	AnyConnect unable to browse websites when connected
CSCte73983	bad apple config may cause vpnagentd to fail
CSCtf06844	AnyConnect SCEP enrollment not working with ASA Per Group Cert Auth
CSCtf20226	Make anyconnect DNS w/ split tunnel behavior for Mac same as windows
CSCtf23946	Agent does not restore DNS Suffix search list if VA dies
CSCtf52183	SCEP enrollment on Mac makes private key exportable from keychain
CSCtf56830	AC cert popup appears even when not requested by ASA
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
CSCtf90996	OGS selects inaccessible host
CSCtf94284	Anyconnect may show password in clear text in RAM
CSCtg01304	Split-tunneling: filtering needs to be enforced on the VPN adapter
CSCtg01525	Anyconnect should have clear description for each error msg
CSCtg04881	VPN Downloader always aborts first SSL handshake
CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
CSCtg37737	AnyConnect cannot parse PAC file and does not connect to endpoint
CSCtg45505	VPN connection fails from network with unusual captive portal
CSCtg73736	Captive portal can't be remediated if remediation site in private space
CSCth32206	Logging is insufficient for troubleshooting
CSCth35315	captive portal reconnect after resume blocks cisco nac agent discovery
CSCth61000	Remove GetMUSHostAddr MUS messages when MUS is not enabled
CSCti07859	AC reports 'certificate validation failed' with VPN LB intermittently
CSCtj36459	Cannot connect to tunnel groups with CSD enabled
CSCtj62029	Can't establish tunnel with machine cert auth and untrusted server CA

Caveats Resolved by AnyConnect 2.5.2010

Table 17 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.2010 resolves.

Table 17   Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.2010

ID	Headline
CSCtk55194	Automatic upgrade fails, downloader unable to stop the agent
CSCtk61455	Fix for OpenSSL cipher renegotiation vulnerability (CVE-2010-4180)

Caveats Resolved by AnyConnect 2.5.2006

Table 18 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.2006 resolves.

Table 18   Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.2006

ID	Headline
CSCtj90974	Headend Selection Cache size causes AnyConnect client to hang
CSCtk01166	Redirects appear to be sent to the client as IP address instead of FQDN

Caveats Resolved by AnyConnect 2.5.2001

Table 19 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.2001 resolves.

Table 19   Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.2001

ID	Headline
CSCti73316	AnyConnect fails to connect with CSD enabled
CSCti96053	AnyConnect fails with "Unable to process response from..." with Auto-Conn
CSCte99278	Infinite prompting during Cert Authentication
CSCtj59741	AnyConnect machine certs cause group mapping to fail if CSD is enabled
CSCtc80017	Doc: StrictCertificate Trust needs to be updated
CSCth40372	Incorrect spelling in Quarantine help

Caveats Resolved by AnyConnect 2.5.1025

Table 20 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.1025 resolves.

Table 20 **Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.1025**

ID	Headline
CSCtb80457	AnyConnect and ASA need to negotiate time-to-wait for authentication
CSCtc43955	Anyconnect stuck in "Contacting Network" and does not timeout
CSCtd59583	vpnagent exception in filtering code reported on WER
CSCtd67178	vpnagent BEX-buffer overflow exception in autoproxy code reported to WER
CSCte77738	MinimizeOnConnect fails with SBL and TND
CSCtf19644	With split-exclude, AC LocalLanAccess preference not enabled
CSCtf98121	Anyconnect fails when client certificate has empty Subject
CSCtg02656	IgnoreProxy does not work with SBL
CSCtg07128	AnyConnect doesn't use IE's exp proxy svr settings telemetry URL req
CSCtg24945	AC Windows: Failure when reconnecting due to caching of the vpn gw IP
CSCtg69281	Allow administrator to configure local proxy support
CSCtg89030	IOS AnyConnect fails when no image is installed for bypassdownloader
CSCtg99019	PPP: VPN connection fails when PPP server name not set in the RAS entry
CSCth03674	AnyConnect SBL Fails when <BypassDownloader> is True in LocalPolicy
CSCth15323	AnyConnect 2.4 on Linux fails to connect if private keys are protected
CSCth87671	AnyConnect: DNS Searchlist Copy Error, Missing Last Entry
CSCti08881	Mac 10.6 AnyConnect Client failing during SSL Rekey
CSCti33633	Unable to reconnect when CP detected and remediation done after 2min

Open Caveats in AnyConnect 2.5.1025

Table 21 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility client in AnyConnect Release 2.5.1025.

Table 21 **Open Caveats in Cisco AnyConnect Secure Mobility Client Release 2.5.1025**

ID	Headline
CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client
CSCsm69213	Anyconnect does not perform auto route correction on Mac/Linux
CSCsu52949	GUI pops up certificate warning prompts on every connection attempt
CSCsu70199	IPv6: Network error: windows has detected and IP address conflict
CSCsv49773	Multiple local profiles for SG may result in using wrong settings
CSCsw37980	AC needs more certificate matching events
CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance

Table 21   *Open Caveats in Cisco AnyConnect Secure Mobility Client Release 2.5.1025*

ID	Headline
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
CSCsy34111	SVC MSIE proxy option auto does not work
CSCsy48762	AnyConnect: Split tunnel does not work with Anyconnect Mobile
CSCsz56742	Will not use certificates under certain ASA configuration
CSCta94621	Enable local LAN access not consistent with other split tunnel options
CSCtb73073	Mac: VPN establishment allowed while multiple local users logged in
CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
CSCtc03052	SCEP fails in upgrade scenario
CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
CSCtc65842	Mac GUI crash with SCEP in FIPS mode
CSCte42921	Get Unresolved Gateway Address When Trying to Connect
CSCte46102	AnyConnect unable to browse websites when connected
CSCte73983	bad apple config may cause vpnagentd to fail
CSCtf04766	AnyConnect uses Windows system locale instead of install language
CSCtf06844	AnyConnect SCEP enrollment not working with ASA Per Group Cert Auth
CSCtf20226	Make anyconnect DNS w/ split tunnel behavior for Mac same as windows
CSCtf23946	Agent does not restore DNS Suffix search list if VA dies
CSCtf52183	SCEP enrollment on Mac makes private key exportable from keychain
CSCtf56830	AC cert popup appears even when not requested by ASA
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
CSCtf90996	OGS selects inaccessible host
CSCtf94284	Anyconnect may show password in clear text in RAM
CSCtg01304	Split-tunneling: filtering needs to be enforced on the VPN adapter
CSCtg01525	Anyconnect should have clear description for each error msg
CSCtg04881	VPN Downloader always aborts first SSL handshake
CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
CSCtg45505	VPN connection fails from network with unusual captive portal
CSCtg52703	AnyConnect fails on Panasonic Toughbook when using wireless
CSCtg73736	Captive portal can't be remediated if remediation site in private space
CSCth32206	Logging is insufficient for troubleshooting
CSCth35315	captive portal reconnect after resume blocks cisco nac agent discovery
CSCth61000	Remove GetMUSHostAddr MUS messages when MUS is not enabled
CSCth93690	AnyConnect 2.x on MAC removing e-token will not allow reconnects
CSCti07859	AC reports 'certificate validation failed' with VPN LB intermittently

Caveats Resolved by AnyConnect 2.5.0217

Table 22 shows the caveats that AnyConnect Secure Mobility Client Release 2.5.0217 resolves.

Table 22   Caveats Resolved by Cisco AnyConnect Secure Mobility Client Release 2.5.0217

ID	Headline
CSCsz78112	Long-term fix for Anyconnect with IPv6: non-English Vista
CSCtb11342	Global and user preferences files may get out of sync
CSCtb73046	VPN establishment allowed while multiple local users logged in on Linux
CSCtc25178	Fail to establish tunnel as route table verification fails XP with IPv6
CSCtc35990	Split-DNS: only requests of type A are tunneled in
CSCtc41770	AnyConnect may fail to connect if split-tunnel-list is huge
CSCtc85374	AnyConnect Profile Editor: View Backup Servers can cause ASDM Hang
CSCtd00525	VPN Agent crashes when locale returns NULL string
CSCtd23416	Linux: Disconnect hangs for minutes following resume from sleep
CSCtd34579	CSD: Group-URL Fails w/ Pre-Login Policy & Hostscan
CSCte63458	User impersonation to retrieve proxy settings fails
CSCtf38038	AC on OSX leaks ipv6 traffic that should be tunneled to rogue 6to4 gw
CSCtf16698	MSIE Proxy Lockdown might get stuck after PC reload
CSCtg33029	Schema needs updating for Certs

Open Caveats in AnyConnect 2.5.0217

Table 23 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility client in AnyConnect Release 2.5.0217.

Table 23   Open Caveats in Cisco AnyConnect Secure Mobility Client Release 2.5.0217

ID	Headline
CSCsh51779	Client-side proxy & AoN tunneling: must stop direct access to proxy.
CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client.
CSCsi00491	Standalone can connect to wrong ASA from within Secure Desktop
CSCsm69213	Anyconnect does not perform auto route correction on Mac/Linux
CSCsm92424	Random client DPD disconnects with McAfee HIPS SW.
CSCsq02996	Auto-resume sometimes fails even though head-end not timed out.
CSCtg07128	AnyConnect doesn't use IE's exp proxy svr settings telemetry URL req
CSCsu08798	AnyConnect Linux with certs fails if browser master password defined.
CSCsu52949	GUI pops up certificate warning prompts on every connection attempt.
CSCsu70199	IPv6: Network error: windows has detected and IP address conflict.
CSCsv49773	Multiple local profiles for SG may result in using wrong settings.

Table 23   *Open Caveats in Cisco AnyConnect Secure Mobility Client Release 2.5.0217*

ID	Headline
CSCsw28876	AnyConnect: Need to reboot PC to get localization catalog to load.
CSCsw37980	AC needs more certificate matching events.
CSCsx21485	VPN agent "caches" cert information.
CSCsx25806	XP IPV6: AnyConnect can't ping assigned IPV6 address.
CSCsx48918	RDP+SBL: Unable to retrieve logon information to verify compliance
CSCsx62325	Windows Mobile driver error with SVC rekey new-tunnel
CSCsy34111	SVC MSIE proxy option auto does not work
CSCsy48762	AnyConnect: Split tunnel does not work with Anyconnect Mobile
CSCsz56742	Will not use certificates under certain ASA configuration
CSCta94621	Enable local LAN access not consistent with other split tunnel options
CSCtb73073	Mac: VPN establishment allowed while multiple local users logged in
CSCtb73259	Message "Connection to the proxy server failed" appears during reconnect
CSCtb80457	AnyConnect and ASA need to negotiate time-to-wait for authentication
CSCtc03052	SCEP fails in upgrade scenario
CSCtc17266	Private-side proxy on OS X doesn't support per-protocol proxy
CSCtc43955	Anyconnect stuck in "Contacting Network" and does not timeout
CSCtc65842	Mac GUI crash with SCEP in FIPS mode
CSCtc68735	WM: Long group combo box doesn't have arrows
CSCtd59583	vpnagent exception in filtering code reported on WER
CSCtd60540	Win 7: autoreconnect attempts after standby affects connectivity
CSCtd67178	vpnagent BEX-buffer overflow exception in autoproxy code reported to WER
CSCte42921	Get Unresolved Gateway Address When Trying to Connect
CSCte46102	AnyConnect unable to browse websites when connected
CSCte73957	bad apple config causes session to hang on ASR1k after disconnect
CSCte73983	bad apple config may cause vpnagentd to fail
CSCte85697	AnyConnect install fails with -vpn driver encountered an error- message
CSCte96715	Windows client fails to negotiate AES cipher when available only on gw
CSCtf04766	AnyConnect uses Windows system locale instead of install language
CSCtf06844	AnyConnect SCEP enrollment not working with ASA Per Group Cert Auth
CSCtf19644	With split-exclude, AC LocalLanAccess preference not enabled
CSCtf20226	Make anyconnect DNS w/ split tunnel behavior for Mac same as windows
CSCtf23946	Agent does not restore DNS Suffix search list if VA dies
CSCtf48078	AnyConnect random disconnections
CSCtf52183	SCEP enrollment on Mac makes private key exportable from keychain
CSCtf56830	AC cert popup appears even when not requested by ASA
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked

Table 23   *Open Caveats in Cisco AnyConnect Secure Mobility Client Release 2.5.0217*

ID	Headline
CSCtf90996	OGS selects inaccessible host
CSCtf96386	Anyconnect may fail to connect when launched from iPass
CSCtf98121	Anyconnect fails when client certificate has empty Subject
CSCtg01304	Split-tunneling: filtering needs to be enforced on the VPN adapter
CSCtg01525	Anyconnect should have clear description for each error msg
CSCtg02656	IgnoreProxy does not work with SBL
CSCtg04881	VPN Downloader always aborts first SSL handshake
CSCtg24945	AC Windows: Failure when reconnecting due to caching of the vpn gw IP
CSCtg31720	JPN: Status message appeared at bottom is corrupted when disconnected
CSCtg31729	JPN: JPN message garbled when uninstallation runs w/o disconnection
CSCtg37737	AnyConnect cannot parse PAC file and does not connect to endpoint
CSCtg45505	VPN connection fails from network with unusual captive portal
CSCtg52703	AnyConnect fails on Panasonic Toughbook when using wireless
CSCtg89030	IOS AnyConnect fails when no image is installed for bypassdownloader

Notices/Licensing

See the following sections for Cisco AnyConnect Secure Mobility client license information.

License Options

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

For the latest detailed information about the AnyConnect user license options, see Managing Feature Licenses in the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2*.

End-User License Agreement

For the end-user license agreement, go to:
http://www.cisco.com/univercd/cc/td/doc/es_inpck/eu1jen__.pdf

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

For Open Source License information for this product, please see the following link: http://www.cisco.com/en/US/docs/security/asa/asa80/license/opensrce.html#wp50053.

Related Documentation

For more information, see the following documents:

- *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 3.0*
- *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 2.5*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*