Release Notes for Cisco AnyConnect Secure Mobility Client, Release 2.5

Updated: May 10, 2010

OL-22612-01

This document includes the following sections:

Introduction

These release notes are for the Cisco AnyConnect Secure Mobility Client, Release 2.5.0217.

We have 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

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

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 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 Enter your cisco.com credentials.

Step 3 Click **Download Software**

Step 4 Expand the **Latest Releases** folder and click the 2.5.0217.

Step 5 We provide AnyConnect packages for Windows, Windows Mobile, Mac OS X, and Linux. If you would like to download all of the latest AnyConnect packages, click **Download Now** under anyconnect-all-2.5.0217-k9.zip.

Step 6 Click **Proceed with Download.**

Step 7 Select a download manager option and proceed with the download.

Step 8 Follow the instructions in the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5 to install the packages onto an ASA.

New Features

AnyConnect 2.5 supports the following new features on Windows 7, Vista, and XP; and Mac OS X 10.5 and 10.6:

- 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*:

- 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" section on page 29; 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

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*.

New Guidelines

Please note the following guidelines:

- Change to AnyConnect Pop-Up Messages on page 9
- Revocation Message on page 9
- MTU Adjustment on Group Policy May Be Required for Mac OS on page 9
- AnyConnect for Mac OS X Performance when Behind Certain Routers on page 9
- Preventing Windows Users from Circumventing Always-on on page 10

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.
- You configured the server certificate incorrectly on the ASA. If this happened, and 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) 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.

MTU Adjustment on Group Policy May Be Required for Mac OS

AnyConnect on Mac OS 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 X Performance when Behind Certain Routers

When the AnyConnect client for Mac OS X 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 OS X 10.5 or earlier)

sudo ipconfig utun0 mtu 1200 (For OS X 10.6 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 following guidelines documented for previous releases remain in effect for AnyConnect 2.5:

- Responding to a TUN/TAP Error Message with Mac OS X 10.5 on page 10
- 64-bit Internet Explorer Not Supported on page 11
- Avoid Wireless-Hosted-Network on page 11
- AnyConnect Requires That the ASA Be Configured to Accept TLSv1 Traffic on page 11
- Mac OS X 10.6 Sends All DNS Queries in the Clear on page 11
- Flexibility in Sequence and Method Used to Install Start Before Logon and DART Components on page 11

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.

Mac OS X 10.6 Sends All DNS Queries in the Clear

With split-DNS enabled, Mac OS X 10.6 sends all DNS queries in the clear. It should send DNS queries targeting split-DNS domains over the VPN session. Apple plans to resolve this issue in an upcoming update.

Flexibility in 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

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

AnyConnect does not support virtualization software such as VMWare for any platform or Parallels Desktop for Mac OS.

AnyConnect 2.5 requires the following:

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

We 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.

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

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.

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

AnyConnect supports only standalone installations on Linux. The following sections show the supported Linux distributions and requirements.

Linux Distributions

- Red Hat Enterprise Linux 5 Desktop
- Ubuntu 9.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—standalone mode only; web-based install/connect is not supported.

- 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 or later.
- 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

AnyConnect 2.4 supports the following versions of Mac OS:

- Mac OS X 10.5
- Mac OS X 10.6, 10.6.1, and 10.6.2 (each of these versions on 32-bit and 64-bit).

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. Uninstalling before the upgrade and reinstalling AnyConnect afterwards is necessary because the upgrade does not preserve the Cisco AnyConnect Virtual Adapter.

Windows Mobile

We designed AnyConnect 2.5 for compatibility with Windows Mobile 6.5, 6.1, 6.0 and 5.0 Professional and Classic for touch-screens only. Users have reported success with most touch-screens 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
- Samsung Epix running Windows Mobile 6.1

- Samsung Omnia running Windows Mobile 6.1
- Samsung Saga running Windows Mobile 6.1
- HTC Touch running Windows Mobile 6.0
- HTC TyTN running Windows Mobile 5.0

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 caveats with Severities 2 and 3:

- Open Caveats in AnyConnect 2.5
- Caveats Resolved in AnyConnect 2.5

Open Caveats in AnyConnect 2.5

Table 1 lists the caveats that are unresolved in Cisco AnyConnect Secure Mobility client Release 2.5.

Table 1 Open Caveats in Cisco AnyConnect Secure Mobility client Release 2.5

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
CSCsm76977	Improve content of our logging
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.

Table 1 Open Caveats in Cisco AnyConnect Secure Mobility client Release 2.5 (continued)

ID	Headline
CSCsv49773	Multiple local profiles for SG may result in using wrong settings.
CSCsw28876	AnyConnect: Need to reboot PC to get localization catalog to load.
CSCsw37980	AC needs more certificate matching events.
CSCsw97163	AC should not re-use tg cookie if group-url w/ new tg is being used.
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
CSCsy98882	SD Vault should allow AnyConnect Downloader from any temp folder
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
CSCtd47640	DART: Need additional logging to troubleshoot SBL and TND
CSCtd59583	vpnagent exception in filtering code reported on WER
CSCtd60540	Win 7: autoreconnect attempts after standby affects connectivity
CSCtd63809	ASA: WebVPN Homepage does not launch with correct browser
CSCtd67178	vpnagent BEX-buffer overflow exception in autoproxy code reported to WER
CSCte41997	vpndownloader error appears in CSD Vault
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
CSCte78570	AC needs to be more robust against missing non-essential registry keys
CSCte81696	AnyConnect client remote network host names leak to local network
CSCte85697	AnyConnect install fails with -vpn driver encountered an error- message
CSCte96715	Windows client fails to negotiate AES cipher when available only on gw
CSCte98165	VPNGina crashes due to assumption of chained version of 3rd-party GINA

Table 1 Open Caveats in Cisco AnyConnect Secure Mobility client Release 2.5 (continued)

ID	Headline
CSCtf04766	AnyConnect uses Windows system locale instead of install language
CSCtf06844	AnyConnect SCEP enrollment not working with ASA Per Group Cert Auth
CSCtf09447	Issues seen after power loss with tunnel up
CSCtf19644	With split-exclude, AC LocalLanAccess preference not enabled
CSCtf20119	AnyConnect proxy not removed upon disconnect if SBL configured
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
CSCtf61128	Change AP, client does not get state change events for connected state
CSCtf75772	Anyconnect with SBL. Login prompt is displayed before the service loads.
CSCtf81852	Revocation popup when LDAP CRL on outside is blocked
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
CSCtg25686	AnyConnect fails to launch within a RDP connection with Always-on
CSCtg30439	AnyConnect cannot use certificate from crypto card
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

Caveats Resolved in AnyConnect 2.5

Table 2 shows the caveats that AnyConnect Secure Mobility client Release 2.5 resolves.

Table 2 Caveats Resolved in Cisco AnyConnect Secure Mobility client Release 2.5

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

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:

- *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*