# Release Notes for Cisco AnyConnect VPN Client, Release 2.4

**Updated: June 28, 2012**

**OL-20842-11**

This document includes the following sections:



# Introduction

The Cisco AnyConnect VPN 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 security appliance to

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

© 2010 Cisco Systems, Inc. All rights reserved.

automatically download to remote users when they log in, or you can download and install it on the endpoint. You can configure the security appliance 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 AnyConnect. For more information, see the Cisco IOS SSL VPN Data Sheet.

# Retain VPN on Windows Logoff Feature Introduced in AnyConnect 2.4.1012

AnyConnect 2.4.1012 introduces the option to retain the VPN session when a user logs off Windows 7, Vista, or XP. By default, this option is disabled. If you enable this feature, you can specify whether to disconnect the VPN session if a different, local user logs in.

Example use case: With this feature and Remote Desktop enabled, an I.T. administrator can log in from inside the VPN to the user's PC to resolve a problem the user is having.

The following sections provide instructions on configuring and using this feature:

- Configuring Retain VPN on Logoff
- User Experience Note When Using Retain VPN on Logoff

## Configuring Retain VPN on Logoff

To enable this feature, insert the RetainVpnOnLogoff parameter anywhere inside the `ClientInitialization` section of the AnyConnect profile. Table 1 shows the parameters associated with this feature. Examples follow.

*Table 1 RetainVpnOnLogoff and UserEnforcement Client Initialization Tags*

| Tag | Possible Values | User Controllable | OSs Supported |
|---|---|---|---|
| RetainVpnOnLogoff | true—Keeps the VPN session up when the user logs off a Windows OS. **Caution**: If split tunneling is enabled on the group policy and Remote Desktop is enabled on the client PC, users who are not authenticated by the secure gateway and who use RDP to log in to the PC have access to the VPN.<br>false—(Default) Terminates the VPN session when the user logs off a Windows OS. | No | Windows |
| UserEnforcement | If used, this parameter must be embedded within the RetainVpnOnLogoff tag, as shown in Example 2 below this table. This value applies only if the RetainVpnOnLogoff setting is true and the original user logged off Windows when the VPN session was up.<br>The possible values are:<br>• SameUserOnly—(Default) Ends the VPN session if a different user logs on to the PC. AnyConnect ignores this setting if a remote user logs in to the PC as described in the scenario in the "Caution" statement above.<br>• AnyUser—The VPN session remains active after the user logs out and a different user logs in. This value applies only if the RetainVpnOnLogoff is true. **Caution**: With this setting, local users who are not authenticated by the secure gateway and who log in to the PC have access to the VPN. | No | Windows |

### *Example 1*

This example keeps the VPN session up when the user logs off a Windows OS. By default, AnyConnect tears down the session if a different, local user then logs onto the same computer.

```
<ClientInitialization>
    <RetainVpnOnLogoff>true</RetainVpnOnLogoff>
</ClientInitialization>
```

### *Example 2*

This example keeps the VPN session up when the user logs off a Windows OS. AnyConnect retains the VPN session even if a different, local user logs onto the same computer.

```
<ClientInitialization>
    <RetainVpnOnLogoff>true
        <UserEnforcement>AnyUser</UserEnforcement>
    </RetainVpnOnLogoff>
</ClientInitialization>
```

**Note** Be sure to replace the AnyConnect profile assigned to the security appliance group policy.

# User Experience Note When Using Retain VPN on Logoff

If a user who is not logged in to the PC clicks any of the Windows 7 or Vista buttons shown in Figure 1, Retain VPN on Logoff is enabled, and a VPN session is active, Windows terminates the VPN session.

***Figure 1 Example Windows 7 Login Window***


Please ask users not to click these buttons unless they want to terminate the VPN session.

**Note** Windows shows the Disconnect button only if Start Before Logon is enabled.

# Supported Platforms Introduced in AnyConnect 2.4.0202

AnyConnect Client 2.4 runs on the following new platforms:

- Microsoft Windows 7 (32-bit and 64-bit). See "System Requirements."
- Mac OS X 10.6 and 10.6.1 (both 32-bit and 64-bit)
- Windows Mobile 6.1 Professional on the following additional mobile devices:
  - HTC Touch Pro
  - Samsung Epix SGH-i907
  - Samsung Omnia SCH-i910
  - Samsung Saga SCH-i770

# Features Introduced in AnyConnect 2.4.0202

The following sections describe the new features in Release 2.4.0202:



## In-the-Clear DNS Queries Allowed with Split Tunneling Enabled

If the group policy on the security appliance enables split tunneling and if it specifies the DNS names to be tunneled, AnyConnect tunnels any DNS queries that match those names to the private DNS server. If the private DNS server cannot resolve the host name, AnyConnect lets the DNS resolver on the client OS submit the host name in the clear for DNS resolution.

On the other hand, if a DNS query does not match one of the DNS names specified in the group policy, AnyConnect lets the DNS resolver on the client OS submit the host name in the clear for DNS resolution.

AnyConnect tunnels all DNS queries if the group policy does not specify any domains to be tunneled.

This feature requires that you:

- Configure at least one DNS server
- Enable split-tunneling
- Specify at least one domain to be tunneled

**Note** Mac OS X releases 10.6.0, 10.6.1, and 10.6.2 do not tunnel DNS queries; however, we expect that a fix release will resolve this issue (CSCtc54466).

To configure this feature, establish an ASDM connection to the security appliance, choose Configuration > Remote Access VPN > Network (Client) Access > Group Policies> Add or Edit > Advanced > Split Tunneling, and enter the names of the domains to be tunneled into the DNS Names text box.

# Trusted Network Detection

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

AnyConnect supports TND on Windows XP and later, and Mac OS X.

**Note** If you enable TND with Start Before Logon (SBL), and the user moves into the trusted network, the SBL window displayed on the remote computer automatically closes.

Multiple profiles on a user computer may present problems if the user alternates connecting to a security appliance that has TND enabled and to one that does not. If the user has connected to a TND-enabled security appliance in the past, that user has received a TND-enabled profile. If the user reboots the computer when out of the trusted network, the GUI of the TND-enabled client displays and attempts to connect to the security appliance it was last connected to, which could be the one that does not have TND enabled. If the client connects to the TND-enabled security appliance, and the user wishes to connect to the non-TND security appliance, the user must manually disconnect and then connect to the non-TND security appliance. Please consider these problems before enabling TND when the user may be connecting to security appliances with and without TND.

The following workarounds will help you prevent this problem:

- Enable TND in the client profiles loaded on *all* your security appliances on your corporate network.
- Create *one profile* listing all your security appliances in the host entry section, and load that profile on *all* your security appliances.
- If users do not need to have multiple, different profiles, use the same profiles name for the profiles on *all* your security appliances. The security appliance overrides the existing profile.

**Note** If you enable both TND and FIPS, the AnyConnect GUI Statistics Details window reports FIPS is disabled until the client makes a VPN connection (CSCtc52130).

For a complete description with instructions, go to Configuring AnyConnect Client Features in the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

# Support for Simple Certificate Enrollment Protocol (SCEP)

The AnyConnect 2.4 standalone client can employ the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate used for client authentication. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology whenever possible.

In our implementation of SCEP, AnyConnect sends a certificate request and the certificate authority (CA) automatically accepts or denies the request. (The SCEP protocol also allows for a method where the client requests a certificate and then polls the CA until it receives an accept or deny response. The polling method is not implemented in this release.)

AnyConnect users have one task associated with this feature. If the user profile is configured to have users request a certificate manually, users see a button in the AnyConnect GUI labeled **Get Certificate** or **Enroll.** AnyConnect users do not need to know, and will not know, what method AnyConnect uses to retrieve the certificate.

AnyConnect administers configure the use of SCEP requests in the user profile. For a complete description with instructions, go to Configuring AnyConnect Client Features in the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

**Note** See "CertificateExpirationThreshold Element Not Supported" section on page 11 for additional guidance regarding this feature.

# Prompting Users to Select Authentication Certificate

In previous releases, when users authenticated their AnyConnect session using a certificate, AnyConnect provided the matching certificate without involving the user. Starting in this release, AnyConnect can be configured to present users with a list of valid certificates and allow them to choose the certificate with which they want to authenticate their session.

This enhancement is implemented in AnyConnect by configuring the <AutomaticCertSelection> element in the client profile.

This enhancement is available only for the non-mobile Windows operating systems that AnyConnect supports.

For a complete description with instructions, go to Configuring AnyConnect Client Features in the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

# Scripting

AnyConnect Release 2.4 lets you download and run scripts when the following events occur:

- Upon the establishment of a new AnyConnect client VPN session with the security appliance. We refer to a script triggered by this event as an *OnConnect* script because it requires this filename prefix.
- Upon the tear-down of an AnyConnect client VPN session with the security appliance. We refer to a script triggered by this event as an *OnDisconnect* script because it requires this filename prefix.

Thus, the establishment of a new AnyConnect VPN session initiated by Trusted Network Detection triggers the OnConnect script (assuming the requirements are satisfied to run the script). The reconnection of a persistent AnyConnect VPN session after a network disruption does not trigger the OnConnect script.

We assume you know how to write scripts and run them from the command line of the targeted endpoint to test them.

**Note** The AnyConnect software download site provides some example scripts; if you examine them, please remember that they are only examples, they may not satisfy the local computer requirements for running them, and are unlikely to be usable without customizing them for your network and user needs. Cisco does not support example scripts or customer-written scripts.

Requirements and limitations apply. For a complete description with instructions, go to Configuring AnyConnect Client Features in the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

# Proxy Support Enhancement

The proxy support enhancement features the following components new to AnyConnect Release 2.4.

## Mac/Safari Private Proxy

AnyConnect downloads the proxy settings configured in the group policy to the Safari browser after the tunnel is established. The settings return to their original state after the VPN session ends.

To access the proxy settings, establish an ASDM session with the security appliance and choose Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Advanced > IE Browser Proxy. Except for the "Do not use proxy" parameter, the proxy service configured in this window now applies to both Internet Explorer and Safari. The Do not use proxy parameter, if enabled, applies only to Internet Explorer.

## Internet Explorer Connections Tab Lockdown

The Internet Explorer Tools > Internet Options > Connections tab lets the user set proxy information. Hiding this tab during a VPN session prevents the user from intentionally or unintentionally diverting traffic. AnyConnect automatically hides the Connections tab when either of the following occur:

- The security appliance configuration specifies a private-side proxy, and accordingly, AnyConnect specifies the proxy in Internet Explorer upon tunnel establishment.
- AnyConnect uses a public-side proxy defined by Internet Explorer to establish the tunnel. In this case, the split tunneling policy on the security appliance must be set to Tunnel All Networks for lockdown to occur.

Any administrator-defined policies regarding this tab supersede the tab lockdown.

**Note** Windows 7 and Vista support tab lockdown only in Internet Explorer 8 windows opened after the establishment of the VPN session. Thus, Windows 7 and Vista users who open Internet Explorer 8 windows before establishing the VPN session can set a proxy to divert traffic even if the split tunneling policy is set to Tunnel All Networks.

Windows 7 and Vista support tab lockdown in Internet Explorer windows opened before and after the establishment of the VPN session if the version of Internet Explorer is earlier than Version 8. Windows XP supports tab lockdown in all Internet Explorer windows, including Version 8.

Regardless of the Windows or IE version, AnyConnect relinquishes the Connection tab lockdown on disconnect, returning the tab to its previous state.

## Proxy Auto-Configuration File Generation for Clientless Support

Some versions of the security appliance require extra AnyConnect configuration to continue to allow clientless portal access through a proxy server after establishing an AnyConnect session. AnyConnect now uses a proxy auto-configuration (PAC) file to modify the client-side proxy settings to let this occur. AnyConnect generates this file only if the ASA does not specify private-side proxy settings.

# CSD Integration

AnyConnect 2.4 is more tightly integrated with Cisco Secure Desktop (CSD) beginning with CSD 3.5. With this enhancement, the user prompts are displayed as soon as the pre-login scan completes. Typically, this is faster than waiting for the entire hostscan process to run its course. If your site uses AnyConnect 2.4 with CSD 3.4 or earlier, or if your site uses AnyConnect 2.3 with CSD 3.5, you will not receive the benefits of this integration.

CSD 3.5 is backwards-compatible with earlier versions of AnyConnect and AnyConnect 2.4 is backwards-compatible with earlier versions of CSD. If an AnyConnect user is configured to use CSD, AnyConnect 2.4 will deploy the version of CSD installed on the ASA, even if a later version of CSD is already installed on the host.

AnyConnect 2.4 will display and log descriptive posture assessment messages and installation messages passed to it from CSD 3.5. Other than these messages, AnyConnect users will have no interaction with this enhancement in 2.4.

# PEM File Certificate Store

AnyConnect supports certificate authentication using a file store. Instead of relying on browsers to verify and sign certificates, the client reads Privacy Enhanced Mail (PEM) format certificate files from the file system on the remote computer, and verifies and signs them.

AnyConnect supports the PEM file certificate store for all Linux and Mac OS X platforms currently supported by the client.

Requirements and limitations apply. For a complete description with instructions, go to Configuring AnyConnect Client Features in the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

# FIPS and Additional Security in the New AnyConnect Local Policy

The AnyConnect Local Policy specifies additional security parameters for the AnyConnect VPN client, including operating in a mode compliant with Level 1 of the Federal Information Processing Standard (FIPS), 140-2, a U.S. government standard for specific security requirements for cryptographic modules. The FIPS 140-2 standard applies to all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems.

Other parameters in the AnyConnect Local Policy increase security by forbidding remote updates to prevent Man-in-the-Middle attacks and by preventing non-administrator or non-root users from modifying client settings.

AnyConnect Local Policy parameters reside in an XML file called *AnyConnectLocalPolicy.xml*. This file is not deployed by the security appliance. You must deploy this file using corporate software deployment systems or change the file manually on a user computer.

For Windows, we provide a Microsoft Transform (MST) file that you can apply to the standard MST installation file to enable FIPS. The MST does not change other AnyConnect Local Policy parameters. You can also use our Enable FIPS tool, a command line tool that can only be run on Windows using administrator privileges or as a root user for Linux and Mac.

Alternatively, you can obtain a copy of the AnyConnect Local Policy file from a client installation, manually edit the parameters, and deploy it to user computers. For Mac OS X and Linux, you can only use our Enable FIPS tool.

Requirements and limitations apply. For a complete description with instructions, go to Configuring AnyConnect Client Features in the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

## Licensing Requirements for the FIPS-Compliant VPN Client

The FIPS-compliant AnyConnect VPN client is licensed based on the ASA 5500 Series Adaptive Security Appliance model. Each security appliance model requires a different license. The license does not affect the number of allowed concurrent VPN sessions.

When you purchase the FIPS license, you receive the license and instructions on enabling FIPS, including how to download and use our Enable FIPS tool or our MST file that enables FIPS.

Table 2 shows the Product numbers (also called SKUs) of the licenses for each security appliance model:

***Table 2 FIPS License Product Numbers for each Security Appliance***

| Product Number (also called SKU) | Security Appliance Model | Description |
|---|---|---|
| ASA-FPS-CL-5510= | ASA 5510 | FIPS-compliant VPN Client License |
| ASA-FPS-CL-5520= | ASA 5520 | FIPS-compliant VPN Client License |
| ASA-FPS-CL-5540= | ASA 5540 | FIPS-compliant VPN Client License |
| ASA-FPS-CL-5580= | ASA 5580 | FIPS-compliant VPN Client License |
| ASA-FPS-CL-5505= | ASA 5505 | FIPS-compliant VPN Client License |
| ASA-FPS-CL-5550= | ASA 5550 | FIPS-compliant VPN Client License |

**Note** Each new security appliance model purchased after August 31st, 2009 requires a FIPS-compliant VPN client license. Cisco customers with current SMARTnet contracts who purchased an ASA 5500 Series Adaptive Security Appliance before August 31st, 2009 are not required to purchase a license for these specific appliances and may contact the Cisco federal account team for information on upgrade rights for the FIPS-compliant VPN client.

# Latest Guidelines

The following guidelines are either new with AnyConnect 2.4.1012 or reported since its release.

## VPN Access through a Tethered Device Not Supported

AnyConnect 2.4 does not support VPN access through a tethered device.

# CertificateExpirationThreshold Element Not Supported

The <CertificateExpirationThreshold> element in the AnyConnect client profile used when Configuring SCEP Protocol to Provision and Renew Certificates is not supported in AnyConnect 2.4. See the Cisco AnyConnect VPN Client Administrator Guide, Release 2.4 for a full description of the SCEP certificate feature.

# 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 Guideline Introduced in AnyConnect 2.4.1012

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).

# Guidelines in AnyConnect 2.4.0202 and Previous Releases

Except for the first, the following guidelines were new in Release 2.40202. For previously documented guidelines that pertain to Release 2.4, go to the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

## 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.

## Changes to OSs Supported

AnyConnect 2.4 now supports Microsoft Windows 7 (32-bit and 64-bit), and Mac OS X 10.6, 10.6.1, and 10.6.2 (each of these versions on 32-bit and 64-bit). AnyConnect 2.4 no longer supports Microsoft Windows 2000 and Mac OS X 10.4, although it may work with these OSs.

Customers running Mac OS X 10.4 must upgrade to 10.5 before upgrading to AnyConnect 2.4. We will continue to support Mac OS X 10.4 users running pre-2.4 versions until we end-of-life those versions.

AnyConnect 2.4 now supports Red Hat Enterprise Linux 5 Desktop and 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.

## 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.

# AnyConnect Tools

Cisco makes the AnyConnect tools described in the following sections available to you for your convenience; however, these tools are in a beta release state.

**Note** Cisco TAC does not provide support for beta releases.

## Profile Editor

The AnyConnect profile is an XML file that drives the display in the user interface and defines the names and addresses of host computers. You can differentiate access to the AnyConnect features by creating and assigning different AnyConnect profiles to group policies configured on the security appliance. Following assignment to the group policies, the security appliance automatically pushes the one assigned to the user's group policy upon connection setup.

The *Cisco AnyConnect VPN Client Administrator Guide, Version 2.4* describes how to add the features to the AnyConnect profile manually. The AnyConnect VPN Software Download site provides access to the Profile Editor to create and edit AnyConnect 2.4 user profiles as an alternative to editing them manually; however, it is in a beta release state. Preliminary testing has been favorable; however, if you choose to use this tool, please observe precautions appropriate for a beta release.

**Caution** If you choose to use the Profile Editor, please back up the AnyConnect client profile before you use the Profile Editor to modify it. After saving the file, use a utility to validate the differences. Test the features before you deploy them.

## Diagnostic AnyConnect Reporting Tool (DART)

DART is the Diagnostic AnyConnect Reporting Tool that you can use to collect data useful for troubleshooting AnyConnect install and connection problems. DART supports Windows 7, Windows Vista, and Windows XP operating systems.

The DART wizard runs on the computer that runs AnyConnect Client. DART assembles the logs, status, and diagnostic information for Cisco Technical Assistance Center (TAC) analysis. DART does not require administrator privileges to run.

DART does not rely on any component of the AnyConnect software to run, though you can launch DART from AnyConnect, and DART collects the AnyConnect log file, if it is available.

Any version of DART works with any version of AnyConnect; the version numbers of each are no longer synchronized. To optimize DART, we recommend downloading the most recent version available on the Cisco AnyConnect VPN Client Software Download site, regardless of the AnyConnect version you are using.

DART is currently available as a standalone installation, or the administrator can push this application to the client PC as part of the AnyConnect dynamic download infrastructure. Once installed, the end user can start the DART wizard from the Cisco folder available through the Start button.

**Note** Cisco has made DART available to its customers so that they may have a convenient method of gathering important troubleshooting information; however, be aware that DART is in the "Beta" phase of its release cycle.

For a complete description with instructions, go to Managing, Monitoring, and Troubleshooting AnyConnect Connections in the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

# System Requirements

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

AnyConnect does not support sessions with a security appliance running on the same subnet as the endpoint.

# Microsoft Windows

For WebLaunch, use Internet Explorer 6.0+ or Firefox 2.0+, 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.

- 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.
- x64 or x86 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
- 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 1.5 or later. The default Java package on Fedora is an open-source GNU version, called Iced Tea 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.

# 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

**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 2.4.x, these releases were removed from customer availability due to a *security vulnerability*. Please contact your authorized support representative for further details.

AnyConnect 2.4 was desgined for compatibility with Windows Mobile 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. Table 3 lists the supported devices with their corresponding service providers and supported operating system versions.

***Table 3 Supported Windows Mobile Devices (Touch-screens Only)***

| Device | OS | Wi-Fi |
|---|---|---|
| ATT Tilt 3.57.502.2 WWE<br>**Note**: TouchFLO must be disabled. | Windows Mobile 6.1 Professional | ✓ |
| Axim X51v with ROM: A03 (23092007 | Windows Mobile 6.0 Classic | ✓ |
| HTC Touch Pro | Windows Mobile 6.1 Professional | ✓ |

*Table 3 Supported Windows Mobile Devices (Touch-screens Only) (continued)*

| Device | OS | Wi-Fi |
|---|---|---|
| iPAQ 2790 | Windows Mobile 5.0 PocketPC | ✓ |
| Palm Treo 700wx–Sprint TREO 700WX-1.15-SPNT | Windows Mobile 5.0+AKU2 PDA Phone | — |
| Palm Treo 750:<br>• AT&T TREO750-2.27-RWE<br>• AT&T TREO 750-2.25-ATT<br>• T-Mobile TREO750-2.27-RWE | Windows Mobile 6.0 Professional | — |
| Palm Treo 800:<br>• Sprint Treo 800w-1.03-SPNT | Windows Mobile 6.1 Professional | ✓ |
| Palm Treo Pro:<br>• AT&T T850UNA-1.01-NAE<br>• Sprint T850EWW-1.03-SPT<br>• T-Mobile T850UNA-1.01-NAE | Windows Mobile 6.1 Professional | ✓ |
| Samsung<br>• Epix SGH-i907<br>• Omnia SCH-i910<br>• Saga SCH-i770 | Windows Mobile 6.1 Professional | ✓ |
| Sprint Touch with ROM: 3.03.651.4<br>**Note**: TouchFLO must be disabled. | Windows Mobile 6.1 Professional | — |
| T-Mobile Wing 4.26.531.1 WWE | Windows Mobile 6.0 Professional | ✓ |
| Verizon XV6800 with ROM: 1.00.00.H:<br>• Verizon 2.09.605.8<br>• Verizon 3.57.605.1 | Windows Mobile 6.0 Professional and Windows Mobile 6.0 Professional | ✓ |

# Security Appliances and Software Supported

The Cisco AnyConnect VPN Client supports all Cisco Adaptive Security Appliance models. It does not support PIX devices. See the Adaptive Security Appliance VPN Compatibility Reference: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html for a complete list of compatibility requirements.

Table 4 shows the minimum Cisco ASA 5500 Adaptive Security Appliance software images that support AnyConnect.

*Table 4 Software Images that Support AnyConnect, Release 2.4*

| Image Type | Version |
|---|---|
| ASA Boot image | 8.0(3).1 or later |
| Adaptive Security Device Manager (ASDM) | 6.1(3).1 or later |
| Cisco Secure Desktop | 3.2(2)[1] or later |

1. Cisco Secure Desktop, Release 3.2(1) is compatible, but it provides more limited functions.

# 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 2.4.1012
- Caveats Resolved in AnyConnect 2.4.1012
- Open Caveats in AnyConnect 2.4.0202
- Caveats Resolved by AnyConnect 2.4.0202

## Open Caveats in AnyConnect 2.4.1012

Table 5 lists the caveats that are unresolved in Cisco AnyConnect VPN Client Release 2.4.1012.

*Table 5 Open Caveats in Cisco AnyConnect VPN Client Release 2.4.2.4.1012*

| 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 SecureDesktop. |
| CSCsm92424 | Random client DPD disconnects with McAfee HIPS SW. |

*Table 5 Open Caveats in Cisco AnyConnect VPN Client Release 2.4.2.4.1012 (continued)*

| ID | Headline |
|---|---|
| CSCsq02996 | Auto-resume sometimes fails even though head-end not timed out. |
| 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. |
| 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 | Split tunnel not working with Anyconnect and Windows Mobile |
| CSCsy73171 | AnyConnect roam from EVDO car to 802.11 never reconnected |
| CSCsy98882 | SD Vault should allow AnyConnect Downloader from any temp folder |
| CSCsz19269 | AnyConnect ignoring exclusion lists and using proxy server |
| CSCsz56742 | Will not use certificates under certain ASA configuration |
| CSCsz97362 | Need to document some 3rd Party inter-operability issues |
| CSCta91617 | Split-DNS: Vista DNS resolver slow in detecting the VA adapter |
| 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 |
| CSCtb11342 | Global and user preferences files may get out of sync |
| CSCtc03052 | SCEP fails in upgrade scenario |
| CSCtc17266 | Private-side proxy on OS X doesn't support per-protocol proxy |
| CSCtc25178 | Fail to establish tunnel as route table verification fails XP with IPv6 |
| CSCtc41770 | AnyConnect may fail to connect if split-tunnel-list is huge |
| CSCtc43844 | GUI hangs if an expected error message is not displayed |
| CSCtc65842 | Mac GUI crash with SCEP in FIPS mode |
| CSCtc68735 | WM: Long group combo box doesn't have arrows |
| CSCtc71437 | AnyConnect Administrator Guide 2.4 script doc needs correction |
| CSCtc85374 | AnyConnect Profile Editor: View Backup Servers can cause ASDM Hang |
| CSCtd23416 | Linux: Disconnect hangs for minutes following resume from sleep |
| CSCtd34579 | CSD: Group-URL Fails w/ Pre-Login Policy & Hostscan |
| CSCtd47432 | Doc: Anyconnect admin guide %ALLUSERSAPPDATA% incorrect |

*Table 5 Open Caveats in Cisco AnyConnect VPN Client Release 2.4.2.4.1012 (continued)*

| ID | Headline |
|---|---|
| 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 |
| CSCtd61185 | AnyConnect fails SSL rekey at configured interval on Mac OS X 10.6 |
| CSCtd67178 | vpnagent BEX-buffer overflow exception in autoproxy code reported to WER |

# Caveats Resolved in AnyConnect 2.4.1012

Table 6 shows the caveats that AnyConnect VPN Client Release 2.4.1012 resolves.

*Table 6 Caveats Resolved in Cisco AnyConnect VPN Client Release 2.4.1012*

| ID | Headline |
|---|---|
| CSCtc76755 | Regression and crash when Mac has no DNS setting pre-tunnel |
| CSCtd59158 | Agent crashes when RRAS is running |
| CSCtd00525 | VPN Agent crashes when locale returns NULL string |
| CSCtd53173 | BEX (Buffer Overrun) error in vpnagent binding code reported to WER |
| CSCtd69424 | AnyConnect 2.4 truncating proxy exception list to 512 chars on connect |
| CSCtc70429 | IPv6 data fails with AnyConnect 2.4 client on Windows XP |
| CSCtc52130 | FIPS Status is not updated until VPN tunnel is established |
| CSCtc25818 | Ability to filter on acceptable SSL certs rather than all |
| CSCtd56554 | Profile downloads sometimes fail |
| CSCsx15036 | Windows Logoff Enforcement preference |

# Open Caveats in AnyConnect 2.4.0202

Table 7 lists the caveats that are unresolved in Cisco AnyConnect VPN Client Release 2.4.0202.

*Table 7 Open Caveats in Cisco AnyConnect VPN Client Release 2.4.0202*

| 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 SecureDesktop. |
| CSCsi35149 | Transcend: unable to clear session from GW after setting MSIE proxy V |
| CSCsi44045 | Difficult to clear the VPN program after tunnel cleared from GW |
| CSCsm92424 | Random client DPD disconnects with McAfee HIPS SW. |
| CSCsq02996 | Auto-resume sometimes fails even though head-end not timed out. |
| CSCsq88383 | AnyConnect user authentication fails in some scenarios. |

*Table 7 Open Caveats in Cisco AnyConnect VPN Client Release 2.4.0202 (continued)*

| ID | Headline |
|---|---|
| CSCsr23029 | Standalone client fails to connect if CSD and Authenticating proxy. |
| 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. |
| CSCsw28876 | AnyConnect: Need to reboot PC to get localization catalog to load. |
| CSCsw30030 | Vista: Unable to process response from using standalone AnyConnect. |
| 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 |
| CSCsy34111 | SVC MSIE proxy option auto does not work |
| CSCsy48762 | Split tunnel not working with Anyconnect and Windows Mobile |
| CSCsy73171 | AnyConnect roam from EVDO car to 802.11 never reconnected |
| CSCsz19269 | AnyConnect ignoring exclusion lists and using proxy server |
| CSCsz95464 | Anyconnect fails to connect with special character password “<>” |
| CSCsz97362 | Need to document some 3rd Party inter-operability issues |
| CSCtb73073 | Mac: VPN establishment allowed while multiple local users logged in |
| CSCtb80457 | AnyConnect and ASA need to negotiate time-to-wait for authentication |
| CSCtb11342 | Global and user preferences files may get out of sync |

# Caveats Resolved by AnyConnect 2.4.0202

Table 8 shows the caveats that AnyConnect VPN Client Release 2.4.0202 resolved.

*Table 8 Caveats Resolved in Cisco AnyConnect VPN Client Release 2.4.0202*

| ID | Headline |
|---|---|
| CSCsq49102 | AnyConnect incompatibility with Citrix advanced gateway client 2.2.1 |
| CSCsx14777 | DART:AC Standalone AnyConnect Client shows AnyConnect 2.3.xx instead of AnyConnect dart 2.3.xx. |
| CSCsx62325 | Windows Mobile driver error with SVC rekey new-tunnel |
| CSCsx79055 | Upgrade during SBL incomplete |
| CSCsy00749 | AnyConnect: Failed to initialize connection to subsystem upon reconnect |
| CSCsy44786 | GUI fails when users log off using SBL |
| CSCsz67246 | Anyconnect SBL: XML parsing prevents concurrent connections |
| CSCsz78112 | Long-term fix for Anyconnect with IPv6: non-English Vista |

*Table 8 Caveats Resolved in Cisco AnyConnect VPN Client Release 2.4.0202 (continued)*

| ID | Headline |
|---|---|
| CSCsz99190 | AnyConnect Mac: Installer leaves vpnclient.dmg in root directory |
| CSCta01109 | file move operation fails |
| CSCta13784 | Post SBL script launch fails on Vista with access denied error |
| CSCta21437 | AnyConnect: Safesign CSP prompts for PIN using AAA |
| CSCta31173 | Allow mDNS through filters with Local LAN |
| CSCta39434 | AC - If CertificateMatch in Profile selects 0 certs, AC will use any |
| CSCta55059 | AnyConnect: Admin unable to use Local Machine certificates |
| CSCta59527 | Anyconnect picks invalid certificate |
| CSCta59878 | DART install gets out-of-sync with local manifest |
| CSCta63379 | Voice mails through an Anyconnect tunnel on a Mac OS is garbled |
| CSCta70161 | HCP renew clobbers DNS settings on Linux AnyConnect |
| CSCta73252 | AnyConnect connection failure due to wrong windows shell registry |
| CSCtb51693 | Installer MST causes Anyconnect install/auto-update to fail |
| CSCtb63734 | UserControllable variable broken for SBL |
| CSCtb70879 | AnyConnect fails to connect if Ignore Proxy is enabled with CSD |
| CSCtb73046 | Linux: Single user at time of connection establishment not enforced |
| CSCtb76577 | Anyconnect connection failure with IPv6 |

# Notices/Licensing

See the following sections for Cisco AnyConnect VPN 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, refer to the following documentation:

- For additional information about the security appliance or ASDM or its platforms, see *Navigating the Cisco ASA 5500 Series Documentation*:

  http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html
- *Cisco AnyConnect VPN Client, Release 2.3, Administrator Guide*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2010 Cisco Systems, Inc. All rights reserved.