



# Release Notes for Cisco AnyConnect VPN Client, Version 2.0

---

Part Number: OL-12482-01

## Introduction

These release notes are for the Cisco AnyConnect VPN Client, Version 2.0, which connects remote users with the Cisco ASA 5500 Series Adaptive Security Appliance using the Secure Socket Layer (SSL) protocol.

The AnyConnect client provides remote end users running Microsoft Vista, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client, and supports applications and functions unavailable to a clientless, browser-based SSL VPN connection. In addition, the AnyConnect client supports IPv6 over an IPv4 network.

The AnyConnect client can be installed manually on the remote PC by the system administrator. It can also be loaded onto the security appliance and made ready for download to remote users. After downloading, it can automatically uninstall itself after the connection terminates, or it can remain on the remote PC for future SSL VPN connections.

This release supports only the SSL protocol. This release does not include IPSec support.

These release notes describe new features, limitations and restrictions, open and resolved caveats, and related documentation. They also include procedures you should follow before loading this release. The section [Usage Notes](#) describes interoperability considerations and other issues you should be aware of when installing and using the AnyConnect client. Read these release notes carefully prior to installing this software.



# Contents

This document includes the following sections:

[System Requirements, page 3](#)

[Upgrading to AnyConnect Release 2.0, page 5](#)

[New Features in Release 2.0, page 6](#)

[Installation Notes, page 8](#)

[Usage Notes, page 30](#)

[Caveats, page 37](#)

[Obtaining Documentation, page 50](#)

[Documentation Feedback, page 51](#)

[Cisco Product Security Overview, page 51](#)

[Obtaining Technical Assistance, page 52](#)

[Obtaining Additional Publications and Information, page 53](#)

# System Requirements

The following table indicates the system requirements to install the Cisco AnyConnect VPN Client on each of the supported platforms.

Operating System	Computer	Requirements
<ul style="list-style-type: none"> <li>Windows 2000 SP4.</li> <li>Windows XP SP2.</li> <li>Windows Vista.</li> </ul>	<p>Computer with a Pentium®-class processor or greater.</p> <p>In addition, x64 or x86 processors are supported for Windows XP and Windows Vista.</p>	<ul style="list-style-type: none"> <li>5 MB hard disk space.</li> <li>RAM:               <ul style="list-style-type: none"> <li>128 MB for Windows 2000.</li> <li>256 MB for Windows XP.</li> <li>512 MB for Windows Vista.</li> </ul> </li> <li>Microsoft Installer, version 3.1.</li> </ul>
<p>The following Linux distributions have been tested and are known to work with the AnyConnect Client, while following the requirements listed in this document:</p> <ul style="list-style-type: none"> <li>Red Hat Enterprise Linux 3.</li> <li>Fedora Core 4 or higher.</li> <li>Slackware 11.</li> <li>SuSE 10.1.</li> </ul>	<ul style="list-style-type: none"> <li>Computer with an Intel i386 or higher processor.</li> <li>32-bit processors are supported.</li> <li>Biarch 64-bit - standalone mode only; web-based install/connect is not supported.</li> </ul>	<ul style="list-style-type: none"> <li>RAM: 32 MB.</li> <li>About 20 MB hard disk space.</li> <li>sudo access for the security appliance to download and install the AnyConnect client, or to update the AnyConnect client.</li> <li>sudo: 1.6.6 or later required.</li> <li>glibc users must have glibc 2.3.2 installed. For example, libc.so.6 or higher.</li> <li>libstdc++ users must have libstdc++ version 3.3.2 (libstdc++.so.5) or higher, but below version 4.</li> <li>Firefox: required 1.0 or later (with libnss3.so installed in /usr/local/lib, /usr/local/firefox/lib, or /usr/lib).</li> <li>libcurl: required 7.10 or later.</li> <li>openssl: required 0.9.7a or later.</li> <li>java: required 1.5 or later.</li> <li>zlib: required 1.2.3 or later.</li> <li>gtk: required 2.0.0, gdk: required 2.0.0, libpango: required 1.0.</li> <li>iptables: 1.2.7a or later.</li> <li>kernel: tun.o loadable module required. The tun module supplied with kernel 2.4.21 or later is required.</li> </ul>
Mac OS X, Version 10.4 or later	Macintosh computer <sup>1</sup>	50 MB hard disk space

1. The AnyConnect VPN Client is not compatible with Parallels Desktop for Mac.

If you are using Internet Explorer, use version 5.0, Service Pack 2 or later.

**Note**

The Vista version of AnyConnect (32- and 64-bit) supports everything that the Windows 2000 and Windows XP versions support, with the exception of Start Before Login. Cisco Secure Desktop, which is a distinct product from AnyConnect, provides 32-bit Vista support for its posture assessment and cache cleaner components. Cisco Secure Desktop does not support secure desktop on Vista at this time.

## Security Appliances and Software Supported

The Cisco AnyConnect VPN Client supports all Cisco Adaptive Security Appliance models. It does not support PIX devices. [Table 1](#) shows the Cisco ASA 5500 Adaptive Security Appliance software images that support the AnyConnect client.

*Table 1 Software Images that Support the AnyConnect Client*

Image Type	Version
ASA Boot image	8.0(2)
Adaptive Security Device Manager (ASDM)	6.0(2)
Cisco AnyConnect VPN Client	Windows, Linux, and Mac OS X: 2.0(1)
Cisco Secure Desktop	3.2(1)

## Interoperability Considerations

This section describes how the AnyConnect VPN Client interoperates with other software. The AnyConnect client can be loaded on the security appliance and automatically deployed to remote users when they log in to the security appliance, or it can be installed as an application on PCs by a network administrator using standard software deployment mechanisms. You can use a text editor to create user profiles as XML files. These profiles drive the display in the user interface and define the names and addresses of host computers.

### AnyConnect Client and Cisco Secure Desktop

[Table 2](#) shows the interoperability of the AnyConnect Client modes with Cisco Secure Desktop modules on remote computers.

*Table 2 AnyConnect Client and Cisco Secure Desktop Interoperability*

AnyConnect Client Mode (SBL must not be enabled) <sup>1</sup>	Operating System <sup>2</sup>	Cisco Secure Desktop Remote Module			
		Prelogin Assessment	Host Scan	Secure Session	Cache Cleaner
Standalone	Microsoft Windows Vista	Yes	Yes	–	–
	Microsoft Windows XP	Yes	Yes	Yes	–
	Microsoft Windows 2000	Yes	Yes	Yes	–
	Apple Macintosh OS X 10.4 (PowerPC or Intel)	–	–	–	–
	Linux	–	–	–	–

Table 2 AnyConnect Client and Cisco Secure Desktop Interoperability (continued)

AnyConnect Client Mode (SBL must not be enabled) <sup>1</sup>	Operating System <sup>2</sup>	Cisco Secure Desktop Remote Module			
		Prelogin Assessment	Host Scan	Secure Session	Cache Cleaner
WebLaunch	Microsoft Windows Vista	Yes	Yes	–	Yes
	Microsoft Windows XP	Yes	Yes	Yes	Yes
	Apple Macintosh OS X 10.4 (PowerPC or Intel)	–	–	–	Yes
	Linux	–	–	–	Yes

1. By default, the Start Before Logon (SBL) feature of AnyConnect Client is disabled. Cisco Secure Desktop modules are not interoperable with AnyConnect Client if SBL is enabled.
2. Includes both English and non-English support of 32-bit Microsoft operating systems. Cisco Secure Desktop does not support the 64-bit versions.

**Caution**

Do not enable the AnyConnect “Start Before Logon” feature if you want to provide AnyConnect Client access to the Cisco Secure Desktop modules.

## AnyConnect and PIX

PIX does not support SSL VPN connections, either clientless or AnyConnect.

## AnyConnect and IOS

Certain features of the Cisco AnyConnect VPN Client are supported in conjunction with IOS routers with SSL VPN support. Please see the *IOS SSL VPN Feature Guide* for specific details.

# Upgrading to AnyConnect Release 2.0

This section contains information about upgrading from the Cisco SSL VPN client to Cisco AnyConnect VPN Client, Release 2.0.

## Before You Begin

Be aware of the considerations listed in the [Usage Notes, page 30](#), section of these Release Notes before you upgrade. These are known product behaviors, and knowing about them at the beginning of the process should expedite the upgrade. Where appropriate, the number of the caveat documenting the issue appears at the end of the item. See the [“Caveats” section on page 37](#) for a list of open and resolved caveats.

## New Features in Release 2.0

The Cisco AnyConnect VPN Client is the next-generation VPN client, providing remote users with secure VPN connections to the Cisco 5500 Series Adaptive Security Appliance. The AnyConnect client supports Windows Vista, Windows XP and Windows 2000, Mac OS X, and Linux.

The client can be loaded on the security appliance and automatically downloaded to remote users when they log in, or it can be manually installed as an application on PCs by a network administrator. The client includes the ability to create user profiles that are displayed in the user interface and define the names and addresses of host computers.

Additional features of the AnyConnect client include:

- Datagram Transport Layer Security (DTLS) with SSL connections—Avoids latency and bandwidth problems associated with some SSL-only connections and improves the performance of real-time applications that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. For detailed information about DTLS, see RFC 4347 (<http://www.ietf.org/rfc/rfc4347.txt>).
- Standalone Mode—Allows a Cisco AnyConnect VPN client to be established as a PC application without the need to use a web browser to establish a connection.
- Command Line Interface (CLI)—Provides direct access to client commands at the command prompt.
- Microsoft Installer (MSI)—Gives Windows users a pre-install package option that provides installation, maintenance, and removal of AnyConnect client software on Windows systems.
- IPv6 VPN access—Allows access to IPv6 resources over a public IPv4 connection (Windows XP SP2, Windows Vista, Mac OSX, and Linux only). See the [Usage Notes](#) section for information about setting up IPv6 access.
- Start Before Logon (SBL)—Allows for login scripts, password caching, drive mapping, and more, for Windows.
- Certificate-only authentication—Allows users to connect with digital certificate and not provide a user ID and password.
- Simultaneous AnyConnect client and clientless, browser-based connections.
- Compression—Increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred. Compression works only for TLS.
- Fallback from DTLS to TLS—Provides a way of falling back from DTLS to TLS if DTLS is no longer working.
- Language Translation (localization)—Provides a way of implementing translation for user messages that appear on the client user interface.
- Dynamic Access Policies feature of the security appliance—Lets you configure authorization that addresses the variables of multiple group membership and endpoint security for VPN connections.
- Cisco Secure Desktop (CSD) support—Validates the security of client computers requesting access to your SSL VPN, helps ensure they remain secure while they are connected, and attempts to remove traces of the session after they disconnect. The Cisco AnyConnect VPN Client supports the Secure Desktop functions of Cisco Secure Desktop for Windows 2000 and Windows XP.
- Rekey—Specifies that SSL renegotiation takes place during rekey.

# Remote User Interface

Figure 1 shows the Cisco AnyConnect VPN Client user interface. The Connection tab provides a drop-down list of profiles for connecting to remote systems.

Figure 1 Cisco AnyConnect VPN Client User Interface, Connection Tab

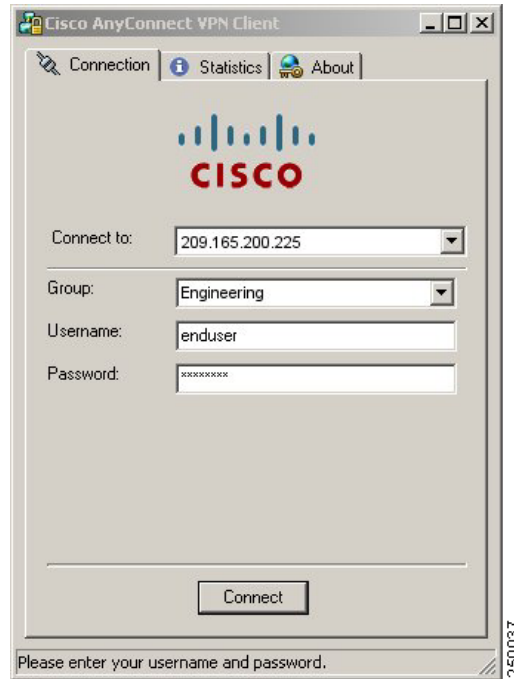
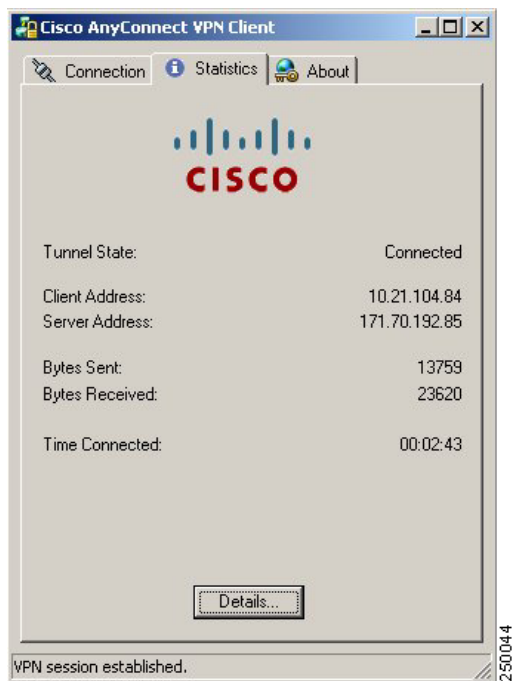


Figure 2 shows the Statistics tab, including current connection information.

Figure 2 Cisco AnyConnect VPN Client User Interface, Statistics Tab



## Installation Notes

This section contains procedures for installing the AnyConnect client software on the ASA5500 using the Adaptive Security Device Manager (ASDM) or the CLI command interface.

Without a previously-installed client, remote users enter the IP address or DNS name in their browser of an interface configured to accept clientless SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.



### Note

A user with a clientless SSL VPN connection can switch to an AnyConnect client SSL vpn connection by clicking the Network Access drawer on the portal and following the instructions on that page.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it uploads the client that matches the operating system of the remote computer. After uploading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously-installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS). The client can also negotiate a simultaneous Datagram Transport Layer Security (DTLS) connection. DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.



The AnyConnect client can be downloaded from the security appliance, or it can be installed manually on the remote PC by the system administrator. For more information about configuring the AnyConnect client, see the *Cisco 5500 Series Adaptive Security Appliance CLI Configuration Guide*.

The security appliance uploads the client based on the group policy or username attributes of the user establishing the connection. You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

The installation and configuration consists of two parts: what you have to do on the security appliance, and what you have to do on the remote PC. The AnyConnect client software is built into the ASA Release 8.0(1) and later. You can decide whether to make the AnyConnect client software permanently resident on the remote PC, or whether to have it resident only for the duration of the connection.



#### Note

When using Start Before Logon, the VPN Gina can not be installed dynamically if the AnyConnect client is installed manually. The VPN Gina can be installed either before or after the AnyConnect client, but they must either be both installed manually or both installed dynamically (CSCsh38590).

This section describes installation-specific issues and procedures for AnyConnect client Release 2.0, and contains the following sections:

- [Before You Install the AnyConnect Client, page 9](#)
- [Installing the AnyConnect Client on a System Running Windows, page 12](#)
- [Installing the AnyConnect Client on a System Running Linux, page 13](#)
- [Installing the AnyConnect Client on a System Running MAC OSX, page 13](#)
- [Using the AnyConnect CLI Commands, page 13](#)
- [Loading the AnyConnect Client and Configuring the Security Appliance with ASDM, page 14](#)
- [Loading the AnyConnect Client and Configuring the Security Appliance with CLI, page 22](#)

## Before You Install the AnyConnect Client

The following sections contain recommendations to ensure successful AnyConnect client installation, as well as tips about certificates, Cisco Security Agent (CSA), adding trusted sites, and responding to browser alerts:

- [Ensuring Automatic Installation of AnyConnect Clients, page 9](#)
- [AnyConnect Client and New Windows 2000 Installations, page 10](#)
- [Adding a Security Appliance to the List of Trusted Sites \(IE\), page 10](#)
- [Adding a Security Certificate in Response to Browser Alert Windows, page 11](#)

## Ensuring Automatic Installation of AnyConnect Clients

The following recommendations and caveats apply to the automatic installation of AnyConnect client software on client PCs:

- To minimize user prompts during AnyConnect client setup, make sure certificate data on client PCs and on the security appliance match:

- If you are using a Certificate Authority (CA) for certificates on the security appliance, choose one that is already configured as a trusted CA on client machines.
- If you are using a self-signed certificate on the security appliance, be sure to install it as a trusted root certificate on clients.

The procedure varies by browser. See the procedures that follow this section.

- Make sure the Common Name (CN) in security appliance certificates matches the name clients use to connect to it. By default, the security appliance certificate CN field is its IP address. If clients use a DNS name, change the CN field on the security appliance certificate to that name.
- The Cisco Security Agent (CSA) might display warnings during the AnyConnect client installation.

Current shipping versions of CSA do not have a built-in rule that is compatible with the AnyConnect client. You can create the following rule using CSA version 5.0 or later by following these steps:

---

**Step 1** In Rule Module: “Cisco Secure Tunneling Client Module”, add a FACL:

```
Priority Allow, no Log, Description: "Cisco Secure Tunneling Browsers, read/write
vpnweb.ocx"
Applications in the following class: "Cisco Secure Tunneling Client - Controlled Web
Browsers"
Attempt: Read file, Write File
```

On any of these files: @SYSTEM\vpnweb.ocx

**Step 2** Application Class: “Cisco Secure Tunneling Client - Installation Applications” add the following process names:

```
**\vpndownloader.exe
@program_files\**\Cisco\Cisco AnyConnect VPN Client\vpndownloader.exe
```

This rule will be built into a future version of CSA.

---

- We recommend that Microsoft Internet Explorer (MSIE) users add the security appliance to the list of trusted sites, or install Java. Doing so enables the ActiveX control to install with minimal interaction from the user. This is particularly important for users of Windows XP SP2 with enhanced security. Windows Vista users *must* add the security appliance to the list of trusted sites in order to use the dynamic deployment feature. Refer to the following sections for instructions.

## AnyConnect Client and New Windows 2000 Installations

In rare circumstances, if you install the AnyConnect client on a computer that has a new or clean Windows 2000 installation, the AnyConnect client might fail to connect, and your computer might display the following message:

```
The required system DLL (filename) is not present on the system.
```

This could occur if the computer does not have the file MSVCP60.dll or MSVCRT.dll located in the winnt\system32 directory. For more information about this problem, see the Microsoft Knowledge Base, article 259403, at <http://support.microsoft.com/kb/259403>.

## Adding a Security Appliance to the List of Trusted Sites (IE)

To add a security appliance to the list of trusted sites, use Microsoft Internet Explorer and do the following steps.




---

**Note** This is required on Windows Vista to use WebLaunch.

---

- 
- Step 1** Go to Tools | Internet Options | Trusted Sites.  
The Internet Options window opens.
- Step 2** Click the Security tab.
- Step 3** Click the Trusted Sites icon.
- Step 4** Click Sites.  
The Trusted Sites window opens.
- Step 5** Type the host name or IP address of the security appliance. Use a wildcard such as `https://*.yourcompany.com` to allow all ASA 5500s within the `yourcompany.com` domain to be used to support multiple sites.
- Step 6** Click Add.
- Step 7** Click OK.  
The Trusted Sites window closes.
- Step 8** Click OK in the Internet Options window.
- 

For information on how to use Microsoft Active Directory to add the security appliance to the list of trusted sites for Internet Explorer, see Appendix B of *Cisco AnyConnect VPN Client Administrator Guide*.

## Adding a Security Certificate in Response to Browser Alert Windows

This section explains how to install a self-signed certificate as a trusted root certificate on a client in response to the browser alert windows.

### In Response to a Microsoft Internet Explorer "Security Alert" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a Microsoft Internet Explorer Security Alert window. This window opens when you establish a Microsoft Internet Explorer connection to a security appliance that is not recognized as a trusted site. The upper half of the Security Alert window shows the following text:

```
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate. The security
certificate was issued by a company you have not chosen to trust. View the certificate
to determine whether you want to trust the certifying authority.
```

Install the certificate as a trusted root certificate as follows:

---

- Step 1** Click View Certificate in the Security Alert window.  
The Certificate window opens.
- Step 2** Click Install Certificate.  
The Certificate Import Wizard Welcome opens.
- Step 3** Click Next.

- The Certificate Import Wizard – Certificate Store window opens.
- Step 4** Select “Automatically select the certificate store based on the type of certificate.”
- Step 5** Click Next.
- The Certificate Import Wizard – Completing window opens.
- Step 6** Click Finish.
- Step 7** Another Security Warning window prompts “Do you want to install this certificate?” Click Yes.
- The Certificate Import Wizard window indicates the import is successful.
- Step 8** Click OK to close this window.
- Step 9** Click OK to close the Certificate window.
- Step 10** Click Yes to close the Security Alert window.
- The security appliance window opens, signifying the certificate is trusted.
- 

#### In Response to a Netscape, Mozilla, or Firefox “Certified by an Unknown Authority” Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a “Web Site Certified by an Unknown Authority” window. This window opens when you establish a Netscape, Mozilla, or Firefox connection to a security appliance that is not recognized as a trusted site. This window shows the following text:

Unable to verify the identity of <Hostname\_or\_IP\_address> as a trusted site.

Install the certificate as a trusted root certificate as follows:

---

- Step 1** Click the Examine Certificate button in the “Web Site Certified by an Unknown Authority” window.
- The Certificate Viewer window opens.
- Step 2** Click the “Accept this certificate permanently” option.
- Step 3** Click OK.
- The security appliance window opens, signifying the certificate is trusted.
- 

## Installing the AnyConnect Client on a System Running Windows

To install the AnyConnect client on a PC running Windows, follow these steps. We suggest you accept the defaults unless your system administrator has instructed otherwise.



#### Note

Vista users must add the security appliance to the trusted zone for automatic installation by the security appliance to work (CSCsh23752).

---

- Step 1** Exit all Windows programs, and disable any antivirus software.
- Step 2** Download the AnyConnect client package file from the Cisco site.
- Step 3** Double-click the package file. The welcome screen for the Cisco AnyConnect VPN Client Setup Wizard displays.

- Step 4** Click **Next**. The End-User License Agreement displays. Accept the license agreement and click OK. The Select Installation Folder screen displays.
- Step 5** Accept the default folder or enter a new folder and click **Next**. The Ready to Install screen displays.
- Step 6** Click **Install**. The client installs and displays the status bar during installation. After installing, the Completing the Cisco AnyConnect VPN Client Setup Wizard screen displays.
- Step 7** Click **Next**. The wizard disappears and the installation is complete.

## Installing the AnyConnect Client on a System Running Linux

To install the AnyConnect client on a System Running Linux, follow these steps:

- Step 1** For Linux, the client files are contained in a tar/gz file. Unpack the archive with a **tar** command. For example:

```
tar xvzf AnyConnect-Linux-Release-2.0.0241.tar.gz
```

The files necessary for installation are placed in the folder *ciscovpn*.

- Step 2** Change to the *ciscovpn* folder. As a root user, run the script named *vpn\_install.sh*. For example:

```
[root@linuxhost]# cd ciscovpn
[root@linuxhost]# ./vpn_install.sh
```

The client installs in the directory */opt/cisco/vpn*. This script also installs the daemon *vpnagentd* and sets it up as a service that is automatically started when the system boots.

After installing the client, you can start the client manually with the Linux command */opt/cisco/vpn/bin/vpnui* or with the client CLI command */opt/cisco/vpn/bin/vpn*.

## Installing the AnyConnect Client on a System Running MAC OSX

The AnyConnect client image for MAC OSX is a DMG disk image installation package. To install the AnyConnect client on a System Running MAC OSX, follow these steps:

- Step 1** Transfer the installation package file to the desktop and double-click the file. A window opens showing an icon representing the installation package file.
- Step 2** Double-click the icon to initiate the installation. A dialog window appears asking you to select the device on which to install the client.
- Step 3** Select a device and click **Next**. A dialog to accept the licensing agreement (EULA) appears.
- Step 4** Accept the license agreement and click **Next**.  
The installation is complete.

## Using the AnyConnect CLI Commands

The Cisco AnyConnect VPN Client provides a command line interface (CLI) for users who prefer to issue commands instead of using the graphical user interface. The following sections describe how to launch the CLI command prompt.

### For Windows

To launch the CLI command prompt and issue commands on a Windows system, locate the file *vpncli.exe* in the Windows folder `C:\Program Files\Cisco\Cisco AnyConnect VPN Client`. Double-click the file *vpncli.exe*.

### For Linux

To launch the CLI command prompt and issue commands on a Linux system, locate the file *vpn* in the folder `/opt/cisco/vpn/bin/`. Execute the file *vpn*.

You can run the CLI in interactive mode, in which it provides its own prompt, or you can run it with the commands on the command line. [Table 3](#) shows the CLI commands.

**Table 3** *AnyConnect Client CLI Commands*

Command	Action
<b>connect</b> <i>IP address or alias</i>	Client establishes a connection to a specific security appliance.
<b>disconnect</b>	Client closes a previously established connection.
<b>stats</b>	Displays statistics about an established connection.
<b>quit</b>	Exits the CLI interactive mode.
<b>exit</b>	Exits the CLI interactive mode.

The following examples shows the user establishing and terminating a connection from the command line:

```
/opt/cisco/vpn/bin/vpn connect 1.2.3.4
```

Establishes a connection to a security appliance with the address *1.2.3.4*.

```
/opt/cisco/vpn/bin/vpn connect some_asa_alias
```

Establishes a connection to a security appliance by reading the profile and looking up the alias *some\_asa\_alias* in order to find its address.

```
/opt/cisco/vpn/bin/vpn stats
```

Displays statistics about the vpn connection.

```
/opt/cisco/vpn/bin/vpn disconnect
```

Disconnect the vpn session if it exists.

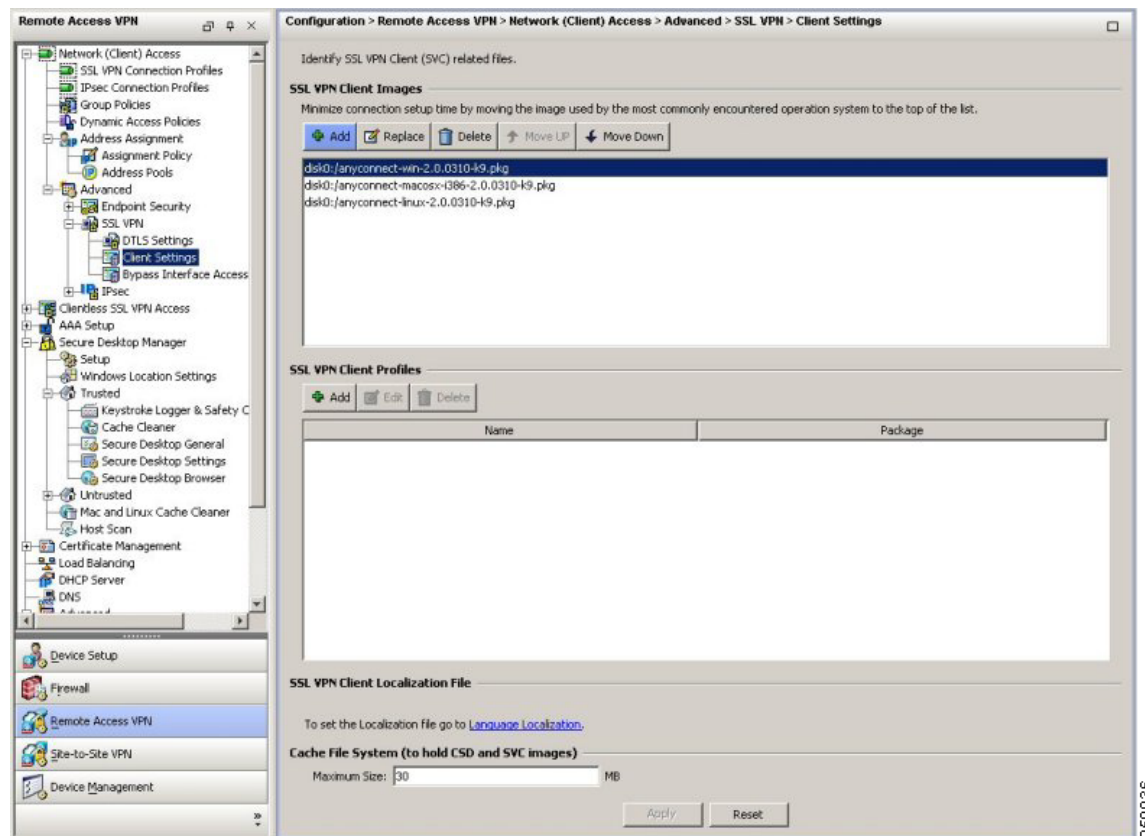
## Loading the AnyConnect Client and Configuring the Security Appliance with ASDM

Loading the client on the security appliance consists of copying a client image to the security appliance and identifying the file to the security appliance as a client image. With multiple clients, you must also assign the order that the security appliance uploads the clients to the remote PC. Perform the following steps to install the client:

- Step 1** Upload the AnyConnect client images to the security appliance. On the ASDM toolbar, click **Configuration**. The navigation pane displays features to configure.
- Step 2** In the navigation pane, click **Remote Access VPN**. The navigation pane displays VPN features.
- Step 3** Choose **Network Access > Advanced > SSL VPN > Client Settings**. The SSL VPN Client Settings panel displays. (Figure 3).

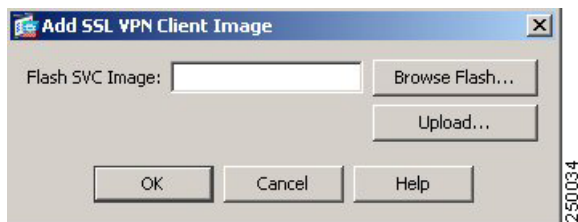
This panel lists any AnyConnect client files that have been identified as AnyConnect client images. The order in which they appear in the table reflects the order that they download to the remote computer.

**Figure 3** *SSL VPN Client Settings Panel*



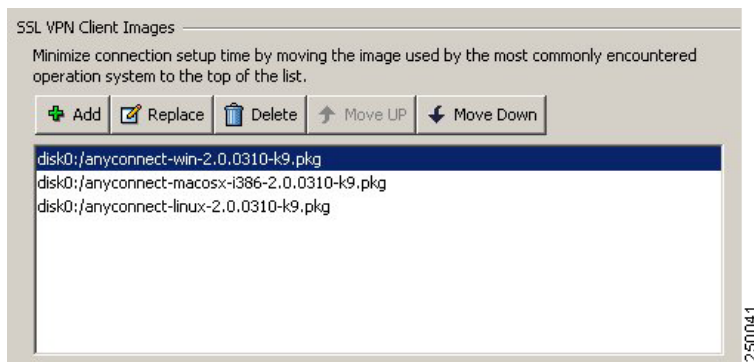
To add an AnyConnect client image, Click **Add** in the SSL VPN Client Images area. The Add SSL VPN Client Image dialog appears (Figure 4).

**Figure 4** Add SSL VPN Client Image Dialog



If you already have an image located in the flash memory of the security appliance, you can enter the name of the image in the Flash SVC Image field, and click **OK**. The SSL VPN Client Images panel now shows the AnyConnect client images you identified (Figure 5).

**Figure 5** SSL VPN Client Panel with AnyConnect Client Images



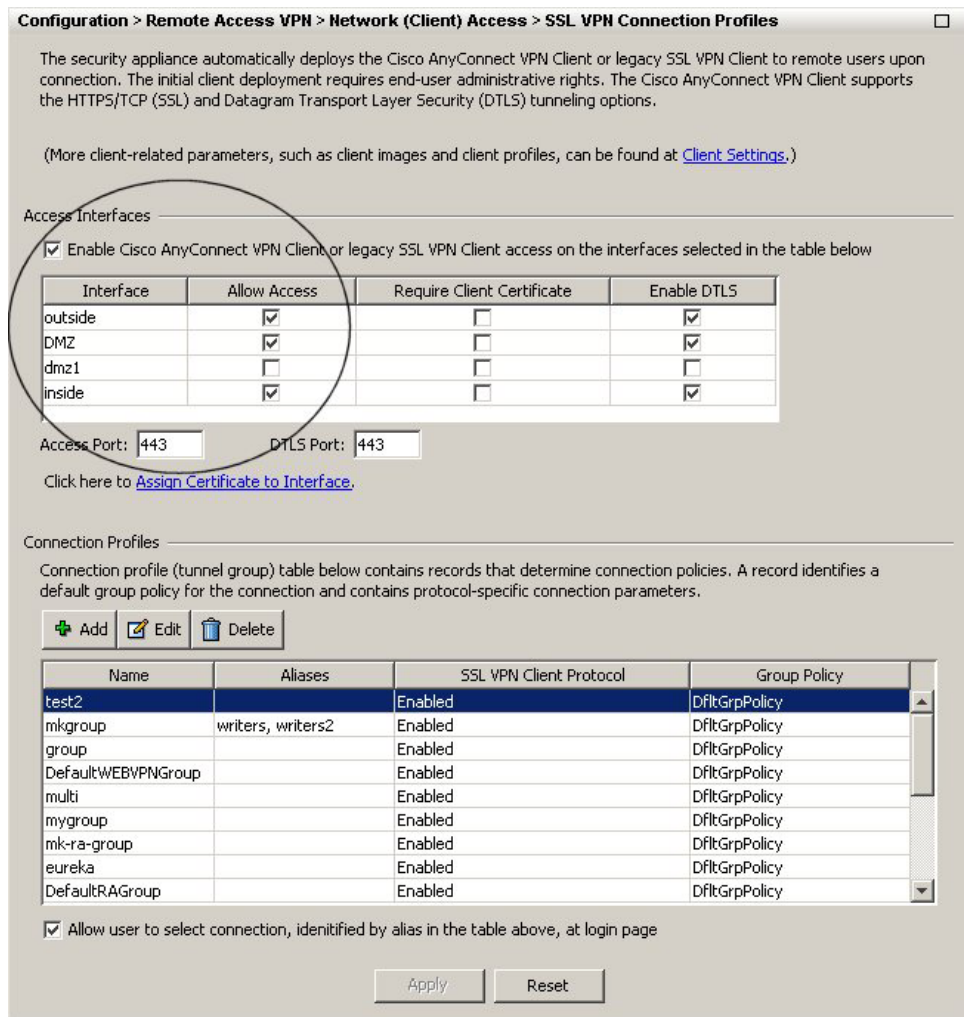
- Step 4** Click on an image name, and use the **Move Down** button to change the position of the image within the list.

This establishes the order in which the security appliance uploads them to the remote computer. It uploads the AnyConnect client image at the top of the list of images first. Therefore, you should move the image used by the most commonly-encountered operating system to the top of the list.

- Step 5** Enable the security appliance to download the AnyConnect client to remote users. Go to **Network Access > SSL VPN Connections**. The SSL VPN Connections panel appears (Figure 6). Check Enable SSL VPN client access for an interface.



**Figure 6 Enable SSL VPN Client Check Box**



- Step 6** Configure a method of address assignment. You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a tunnel group.
- To create an IP address pool, choose **Network Access > Address Management > Address Pools**. Click **Add**. The Add IP Pool dialog appears (Figure 7).

250045

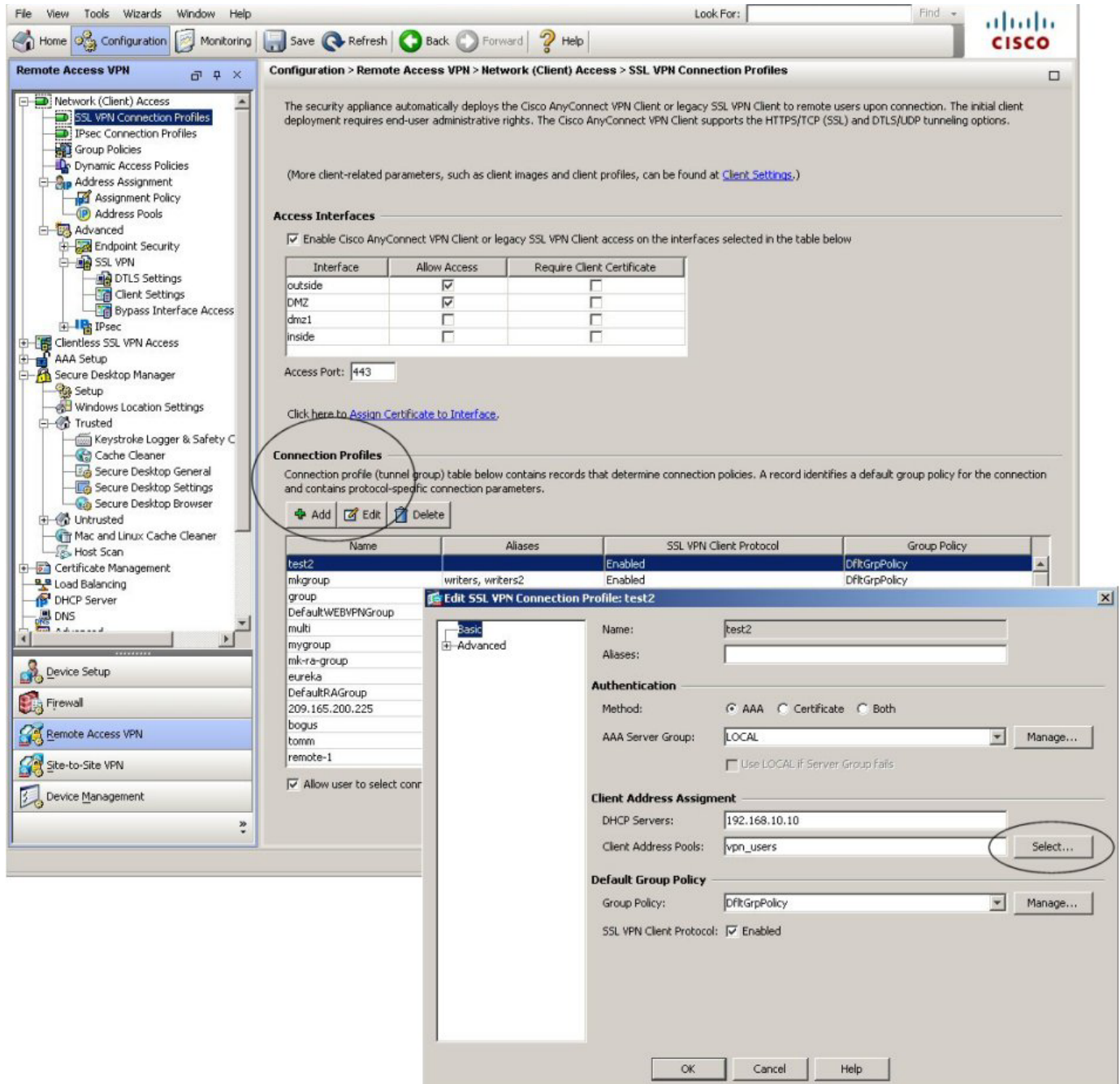
*Figure 7 Add IP Pool Dialog*

The screenshot shows a standard Windows-style dialog box titled "Add IP Pool". It features a title bar with a close button (X) on the right. The main area contains four labeled input fields: "Name:", "Starting IP Address:", "Ending IP Address:", and "Subnet Mask:". The "Subnet Mask" field includes a small downward-pointing arrow on its right side, indicating a dropdown menu. At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help". A vertical number "250033" is printed on the right edge of the dialog box.

Enter the name of the new IP address pool. Enter the starting and ending IP addresses, and enter the subnet mask and click **OK**.

**Step 7** Assign the IP address pool to a Connection (tunnel group). To do this, choose **Network Access > SSL VPN Connections**. The SSL VPN Connections panel appears (Figure 8):

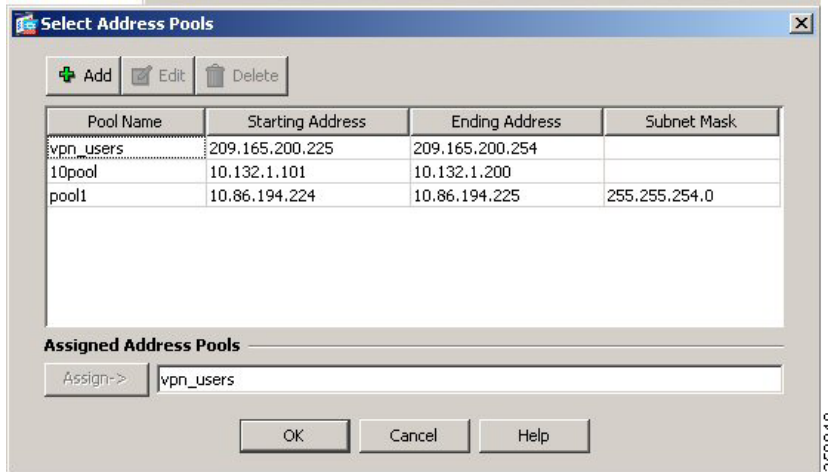
**Figure 8** Connection Address Pool Assignment



Highlight a connection in the table, and click **Edit**. The Edit SSL VPN Connection dialog appears. Click **Select** in the Client Address Assignment area. The Select Address Pool dialog appears (Figure 9), containing available address pools. Select a pool and click **OK**.

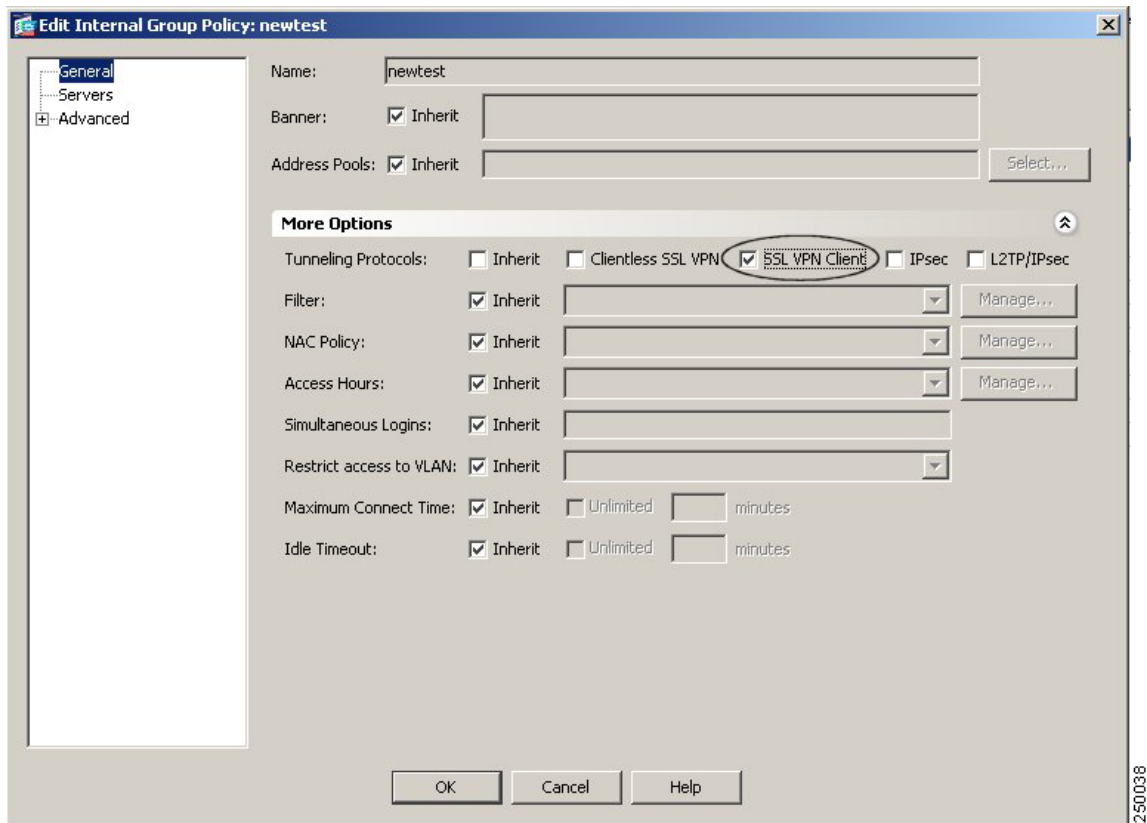
250035

Figure 9 Select Address Pool Dialog



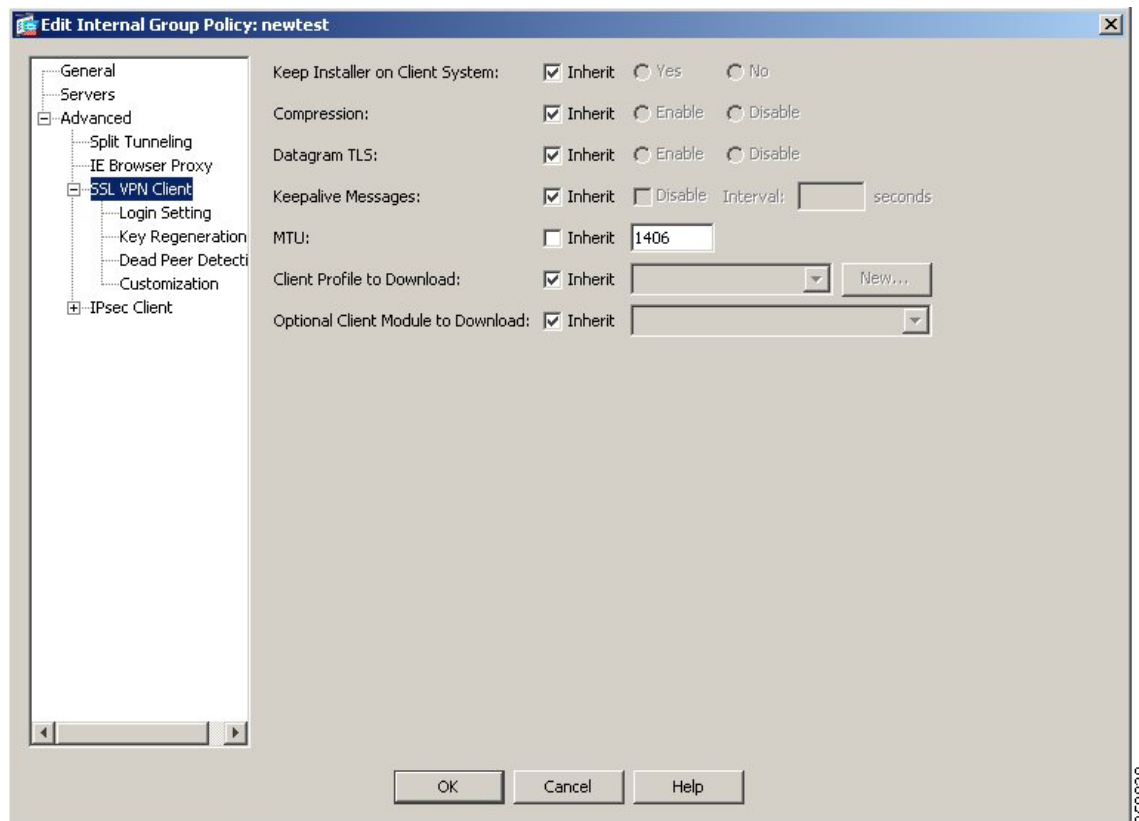
- Step 8** Identify SSL VPN as a permitted VPN tunneling protocol for the group or user.
- Choose **Network Access > Group Policies** from the navigation pane. Highlight the group policy in the Group Policy table, and click **Edit**.
- The Edit Internal Group Policy dialog appears (Figure 10):

Figure 10 Edit Internal Group Policy, General Tab



- Check the **SVC** check box to include SSL VPN as a tunneling protocol.
- Step 9** Configure SSL VPN features for a user or group. To display SSL VPN features for groups, In the navigation pane of the Internal Group Policy dialog, choose **Advanced > SSL VPN Client**. The SSL VPN Client features display [Figure 11](#).

**Figure 11** *SSL VPN Client Features*



Configure the following features on the SSL VPN Client tab:

**Keep Installer on Client System**—Enable to allow permanent client installation on the remote computer. Enabling disables the automatic uninstalling feature of the client. The client remains installed on the remote computer for subsequent connections, reducing the connection time for the remote user.

**Compression**—Compression increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred.

**Datagram TLS**—Datagram Transport Layer Security (DTLS) allows the CVC establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

**Keepalive Messages**—Enter an number, from 15 to 600 seconds, in the Interval field to enable and adjust the interval of keepalive messages to ensure that an connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle. Adjusting the interval also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

**MTU**—Adjust the Maximum Transmission Unit (MTU) in bytes, from 256 to 1410 bytes. This setting affects only the AnyConnect client connections established in SSL, with or without DTLS. By default, the MTU size adjusts automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.

**Client Profile to Download**—Specify a file on flash as a client profile. A profile is a group of configuration parameters that the CVC uses to configure the connection entries that appear in the client user interface, including the names and addresses of host computers.

**Optional Client Module to Download**—Specify any modules that the AnyConnect client needs to download to enable more features, such as Start Before Logon (SBL). To minimize download time, the CVC only requests downloads (from the security appliance) of core modules that it needs for each feature that it supports.

## Loading the AnyConnect Client and Configuring the Security Appliance with CLI

This section covers the following topics:

- [Loading the AnyConnect Client, page 22](#)
- [Enabling SSL VPN Connections, page 23](#)
- [Disabling Permanent Client Installation, page 26](#)
- [Prompting Remote Users, page 26](#)
- [Enabling AnyConnect Client Profile Downloads, page 27](#)
- [Enabling Rekey, page 28](#)
- [Enabling Start Before Logon for the AnyConnect Client, page 29](#)

### Loading the AnyConnect Client

Loading the client on the security appliance consists of copying a client image to the security appliance and identifying the file to the security appliance as a client image. With multiple clients, you must also assign the order that the security appliance uploads the clients to the remote PC. Perform the following steps to install the client:

- 
- Step 1** Copy the client image package to the security appliance using the **copy** command from privileged EXEC mode, or using another method. In this example, the images are copied from a tftp server using the **copy tftp** command:

```
hostname# copy tftp flash
Address or name of remote host []? 209.165.200.226
Source filename []? anyconnect-win-2.0.0.343-k9.pkg
Destination filename []? anyconnect-win-2.0.0.343-k9.pkg
Accessing
tftp://209.165.200.226/anyconnect-win-2.0.0.343-k9.pkg...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file
disk0:/cdisk71...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
319662 bytes copied in 3.695 secs (86511 bytes/sec)
```

- Step 2** Identify a file on flash as a client package file using the **svc image** command from webvpn configuration mode:

**svc image filename order**

The security appliance expands the file in cache memory for downloading to remote PCs. If you have multiple clients, assign an order to the client images with the *order* argument.

The security appliance uploads portions of each client in the order you specify until it matches the operating system of the remote PC. Therefore, assign the lowest number to the image used by the most commonly-encountered operating system. For example:

```
hostname(config-webvpn)# svc image windows.pkg 1
hostname(config-webvpn)# svc image linux.pkg 2
```



#### Note

The security appliance expands SSL VPN client and the CSD images in cache memory. If you receive the error message *ERROR: Unable to load SVC image - extraction failed*, use the **cache-fs limit** command to adjust the size of cache memory:

**Step 3** Check the status of the clients using the **show webvpn svc** command:

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
   CISCO STC win2k+ 1.0.0
   1,0,2,132
   Thu 03/22/2007 21:51:30.43

2. disk0:/linux.pkg 2
   CISCO STC linux 1.0.0
   1,0,0,164
   Thu 03/15/2007 20:09:22.43

2 SSL VPN Client(s) installed
```

## Enabling SSL VPN Connections

After installing the client, enable the security appliance to allow SSL VPN client connections by performing the following steps:

**Step 1** Enable clientless, browser-based connections on an interface using the **enable** command from webvpn configuration mode:

**enable interface**

For example:

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

The following is an example for an IPv6 connection that enables IPv6 on the outside interface:

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

**Step 2** Enable SSL VPN connections globally using the **svc enable** command from webvpn configuration mode.

For example:

```
hostname(config-webvpn)# svc enable
```

**Step 3** Configure a method of address assignment. You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool using the **ip local pool** command from global configuration mode:

**ip local pool poolname startaddr-endaddr mask mask**

The following example assumes the authentication server group is LOCAL. The example creates the local IP address pool *vpn\_users*:

```
hostname(config)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```

- Step 4** Assign IP addresses to a tunnel group. One method you can use to do this is to assign a local IP address pool with the **address-pool** command from general-attributes mode:

**address-pool** *poolname*

To do this, first enter the **tunnel-group** *name* **general-attributes** command to enter general-attributes mode. Then specify the local IP address pool using the **address-pool** command.

In the following example, the user configures the existing tunnel group *telecommuters* to use the address pool *vpn\_users* created in step 3:

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

- Step 5** Assign a default group policy to the tunnel group with the **default-group-policy** command from tunnel group general attributes mode:

**default-group-policy** *name*

In the following example, the user assigns the group policy *sales* to the tunnel group *telecommuters*:

```
hostname(config-tunnel-general)# default-group-policy sales
```

- Step 6** Create and enable a group alias that displays in the group list on the login page using the **group-alias** command from tunnel group webvpn attributes mode:

**group-alias** *name* **enable**

First exit to global configuration mode, and then enter the **tunnel-group** *name* **webvpn-attributes** command to enter tunnel group webvpn attributes mode.

In the following example, the user enters webvpn attributes configuration mode for the tunnel group *telecommuters*, and creates the group alias *sales\_department*:

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

- Step 7** Enable the display of the tunnel-group list on the login page from webvpn mode:

**tunnel-group-list** **enable**

First exit to global configuration mode, and then enter webvpn mode.

In the following example, the user enters webvpn mode, and then enables the tunnel group list:

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

- Step 8** Specify SSL as a permitted VPN tunneling protocol for the group or user with the **vpn-tunnel-protocol** **svc** command in group-policy mode or username mode:

**vpn-tunnel-protocol** **svc**

To do this, first exit to global configuration mode, enter the **group-policy** *name* **attributes** command to enter group-policy mode, or the **username** *name* **attributes** command to enter username mode, and then enter the **webvpn** command to enter webvpn mode and change the settings for the group or user.

The following example identifies SSL as the only permitted tunneling protocol for the group-policy *sales*:

```
hostname(config)# group-policy sales attributes
```



```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol svc
```

For more information about assigning users to group policies, see *Cisco Security Appliance Command Line Configuration Guide*, Chapter 30, “Configuring Tunnel Groups, Group Policies, and Users.”

## Enabling IPv6 Connections

The AnyConnect client allows access to IPv6 resources over a public IPv4 connection (only for Windows XP SP2, Windows Vista, Mac OS X, and Linux). You must use the command line interface to configure IPv6 access. ASDM does not support IPv6.

You enable IPv6 access using the `ipv6 enable` command as part of enabling SSL VPN connections. The following is an example for an IPv6 connection that enables IPv6 on the outside interface:

```
hostname (config)# interface GigabitEthernet0/0
hostname (config-if)# ipv6 enable
```

To enable IPv6 SSL VPN, do the following general actions:

1. Enable IPv6 on the outside interface.
2. Enable IPv6 and an IPv6 address on the inside interface.
3. Configure an IPv6 address local pool for client-assigned IP addresses.
4. Configure an IPv6 tunnel default gateway.

To implement this procedure, do the following steps:

---

### Step 1 Configure Interfaces:

```
interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 192.168.0.1 255.255.255.0
  ipv6 enable ; Needed for IPv6.
!
interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 10.10.0.1 255.255.0.0
  ipv6 address 2001:DB8::1/32 ; Needed for IPv6.
  ipv6 enable ; Needed for IPv6.
```

### Step 2 Configure an 'ipv6 local pool' (used for AnyConnect Client IPv6 address assignment):

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100 ; Use your IPv6 prefix here
```




---

**Note** You still need to configure an IPv4 address pool when using IPv6 (using the `ip local pool` command)

---

### Step 3 Add the ipv6 address pool to your Tunnel group policy (or group-policy):

```
tunnel-group YourTunGrp1 general-attributes ipv6-address-pool ipv6pool
```



**Note** Again, you must also configure an IPv4 address pool here as well (using the 'address-pool' command).

**Step 4** Configure an IPv6 Tunnel Default Gateway:

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

## Disabling Permanent Client Installation

Disabling permanent AnyConnect client installation disables the automatic uninstalling feature of the client. The client remains installed on the remote computer for subsequent connections, reducing the connection time for the remote user.

To disable permanent AnyConnect client installation for a specific group or user, use the **svc keep-installer** command from group-policy or username webvpn modes:

**svc keep-installer none**

The default is that permanent installation of the client is enabled. The client on the remote computer stays installed at the end of every session. The following example configures the existing group-policy *sales* to not keep the client installed on the remote computer:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc keep-installer none
```

## Prompting Remote Users

You can enable the security appliance to prompt remote SSL VPN client users to download the client with the **svc ask** command from group policy webvpn or username webvpn configuration modes:

**[no] svc ask {none | enable [default {webvpn | svc} timeout value]}**

**svc ask enable** prompts the remote user to download the client or go to the portal page for a clientless connection and waits indefinitely for user response.

**svc ask enable default svc** immediately uploads the client.

**svc ask enable default webvpn** immediately goes to the portal page.

**svc ask enable default svc timeout value** prompts the remote user to download the client or go to the portal page and waits the duration of *value* before taking the default action—downloading the client.

**svc ask enable default webvpn timeout value** prompts the remote user to download the client or go to the portal page, and waits the duration of *value* before taking the default action—displaying the portal page.

[Figure 12](#) shows the prompt displayed to remote users when either **default svc timeout value** or **default webvpn timeout value** is configured:

**Figure 12** Prompt Displayed to Remote Users for SSL VPN Client Download



The following example configures the security appliance to prompt the remote user to download the client or go to the portal page and to wait 10 seconds for user response before downloading the client:

```
hostname(config-group-webvpn)# svc ask enable default svc timeout 10
```

## Enabling AnyConnect Client Profile Downloads

An AnyConnect client profile is a group of configuration parameters, stored in an XML file, that the client uses to configure the connection entries that appear in the client user interface. The client parameters (XML tags) include the names and addresses of host computers and settings to enable additional client features.

You can create and save XML profile files using a text editor. The client installation contains one profile template (AnyConnectProfile.tpl) that you can edit and use as a basis to create other profile files.

The profile file is downloaded from the security appliance to the remote users's PC, so you must first import the profile(s) into the security appliance in preparation for downloading to the remote PC. You can import a profile using either ASDM or the command-line interface. See Appendix A of the *Cisco AnyConnect VPN Client Administrator Guide* for a sample AnyConnect profile.

When the AnyConnect client starts, it reads the preferences.xml file in the following directory:

C:\Documents and Settings\\Application Data\Cisco\Cisco AnyConnect VPN Client.

The preferences.xml file contains the username and the security appliance IP address/hostname from the last successful connection. The client then establishes an initial connection to the security appliance to get the list of tunnel groups to display in the GUI. During this initial connection, if the security appliance is no longer accessible or if the hostname cannot be resolved, the user sees the message, "Connection attempt has failed" or "Connection attempt has failed due to unresolvable host entry."

You can place a copy of your profile (for example, CiscoAnyConnectProfile.xml) in the directory:

C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile  
The location for Windows Vista is slightly different: C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile  
The host that appears in the Connect to combo box is the first one listed in the profile or the last host you successfully connected with.

For more information about editing AnyConnect client profiles, see the *Cisco AnyConnect VPN Client Administrator Guide*.

After you create an AnyConnect client profile, follow these steps to enable the security appliance to download them to remote AnyConnect client users:

- Step 1** Identify to the security appliance an AnyConnect client profiles file to load into cache memory using the **svc profile** command from webvpn configuration mode:

```
[no] svc profiles {value profile | none}
```

This command makes profiles available to group policies and username attributes of AnyConnect client users.

In the following example, the user previously created two new profile files (sales\_hosts.xml and engineering\_hosts.xml) from the cvcprofile.xml file and uploaded them to the flash memory.

Now the user specifies these files as AnyConnect client profiles for use by group policies, specifying the names *sales\_hosts* and *engineering\_hosts*:

```
asal(config-webvpn)# svc profiles sales disk0:/sales_hosts.xml
asal(config-webvpn)# svc profiles engineering disk0:/engineering_hosts.xml
```

Entering the **dir cache:stc/profiles** command shows the profiles loaded in cache memory:

```
asal(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774          11:54:41 May 22 2007  engineering.xml
0      ----  774          11:54:29 May 22 2007  sales.xml

2428928 bytes total (18219008 bytes free)
asal(config-webvpn)#
```

- Step 2** Enter group policy webvpn or username attributes webvpn configuration mode and specify a profile for the group or user with the **svc profiles** command:

```
[no] svc profiles {value profile | none}
```

In the following example, the user follows the **svc profiles value** command with a question mark (?) to query the security appliance so see the available profiles. Then the user configures the group policy to use the AnyConnect client profile *sales*:

```
asal(config-group-webvpn)# svc profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
asal(config-group-webvpn)# svc profiles sales
```

## Enabling Rekey

When the security appliance and the AnyConnect client perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

To enable the client to perform a rekey on an SSL VPN connection for a specific group or user, use the **svc rekey** command from group-policy and username webvpn modes.

```
[no] svc rekey {method {new-tunnel | none | ssl} | time minutes}
```

**method new-tunnel** specifies that the client establishes a new tunnel during rekey.

**method none** disables rekey.

**method ssl** specifies that SSL renegotiation takes place during rekey.

**time minutes** specifies the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).

In the following example, the client is configured to renegotiate with SSL during rekey, which takes place 30 minutes after the session begins, for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc rekey method ssl
hostname(config-group-policy)# svc rekey time 30
```

## Enabling or Disabling DTLS

Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL (TLS) tunnel and a DTLS tunnel. DTLS requires the TLS tunnel for a number of reasons, including protocol negotiation and fallback technologies. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

DTLS is enabled implicitly when you enable the interface. If you decide to disable DTLS, SSL VPN connections connect with an SSL VPN tunnel only.

Use the following command options to enable an interface with DTLS or just with TLS:

You can enable DTLS for all AnyConnect client users with the **dtls enable** command in webvpn configuration mode:

```
[no] enable interface | tls-only }
```

For example to enable the outside interface with DTLS, enter the following:

```
hostname(config-webvpn)# enable outside
```

To disable DTLS and allow only TLS, enter the following command instead:

```
hostname(config-webvpn)# enable outside tls-only
```

You can enable DTLS or TLS on a per-user or per-group basis.



### Note

When using the AnyConnect VPN client with DTLS on an ASA device Dead Peer Detection (DPD) must be enabled in the group policy on the ASA to allow the AnyConnect client to fall back to TLS, if necessary. Fallback to TLS occurs if the AnyConnect client cannot send data over the UDP/DTLS session, and DPD is the mechanism necessary for fallback to occur (CSCsh69495).

## Enabling Start Before Logon for the AnyConnect Client

To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of core modules that it needs for each feature that it supports. To enable new features, such as Start Before Logon (SBL), you must specify the module name using the **svc modules** command from group policy webvpn or username webvpn configuration mode:

```
[no] svc modules {none | value string }
```

The *string* for SBL is **vpngina**

In the following example, the user enters group-policy attributes mode for the group policy *telecommuters*, enters webvpn configuration mode for the group policy, and specifies the string *vpngina* to enable SBL:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc modules value vpngina
```

In addition, the administrator must ensure that the AnyConnect profile.xml file has the <UseStartBeforeLogon> statement set to true. For example:

```
<UseStartBeforeLogon UserControllable="false">true</UseStartBeforeLogon>
```

The system must be rebooted before Start Before Logon takes effect.



**Note**

Start Before Logon works only for PCs that are part of a domain and not part of a workgroup or working standalone. Start Before Logon is not compatible with Cisco Secure Desktop.

## CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop

If your remote users have Cisco Security Agent (CSA) installed, you must import new CSA policies to the remote users to enable the AnyConnect VPN Client and Cisco Secure Desktop to interoperate with the security appliance.

To do this, follow these steps:

**Step 1** Retrieve the CSA policies for the AnyConnect client and Cisco Secure Desktop. You can get the files from:

- The CD shipped with the security appliance.
- The software download page for the ASA 5500 Series Adaptive Security Appliance at <http://www.cisco.com/cgi-bin/tablebuild.pl/asa>.

The filenames are AnyConnect-CSA.zip and CSD-for-CSA-updates.zip

**Step 2** Extract the .export files from the .zip package files.

**Step 3** Choose the correct version of the .export file to import. The Version 5.2 export files work for CSA Versions 5.2 and higher. The 5.x export files are for CSA Versions 5.0 and 5.1.

**Step 4** Import the file using the Maintenance > Export/Import tab on the CSA Management Center.

**Step 5** Attach the new rule module to your VPN policy and generate rules.

For more information, see the CSA document *Using Management Center for Cisco Security Agents 5.2*. Specific information about exporting policies is located in the section *Exporting and Importing Configurations*.

## Usage Notes

This section lists known interoperability considerations and other issues to consider before installing and using the Cisco AnyConnect VPN Client, Release 2.0.

### Authenticating Using Digital Certificate Might Fail to Connect

When attempting to use a digital certificate to authenticate using the AnyConnect VPN Client, errors might occur that prevent the user from connecting (CSCsh81014).

## NTLM Authentication

If there is a proxy server between the AnyConnect client (running on a PC) and the security appliance, and the proxy server is expecting NTLM authentication instead of basic authentication, the AnyConnect client must support NTLM Authentication.

## WINS and DNS

The AnyConnect client supports group configured primary and secondary Windows Internet Naming Services (WINS) or Domain Naming Services (DNS). In general, the IPsec Group-based parameters apply to the AnyConnect client. The exception is the Authentication, Authorization, and Accounting configuration, which is always global. [Table 4](#) summarizes the group and global settings that the AnyConnect client supports.

**Table 4** *SVC Group and Global Settings*

Parameter	Group	Global/System-wide
Authentication	No	Yes <sup>1</sup>
Authorization	No	Yes
Accounting	Yes	Yes <sup>2</sup>
DNS and WINS	Yes	N/A
MSIE Proxy Server Setting	Yes	N/A
Default Domain	Yes	N/A
Split DNS	Yes	N/A
Split Tunneling	Yes	N/A
Local LAN	Yes	N/A

1. In this release WebVPN does not support RADIUS with Expiry authentication.
2. If no accounting servers are defined in the group, the system servers apply.

## Internet Explorer Proxy With the AnyConnect Client

If you have Internet Explorer configured with a proxy, you must activate the “Use HTTP 1.1 through proxy connections” setting to use the AnyConnect client. If this option is not set, the AnyConnect client connection does not come up.

In Internet Explorer, choose Internet Options from the Tools menu. Click the Advanced tab, and under the HTTP 1.1 Settings, check “Use HTTP 1.1 through proxy connections.”

## Setting the Secure Connection (Lock) Icon

The Lock icon indicates a secure connection. XP automatically hides this icon among those that have not been recently used. The end user can prevent XP from hiding this icon as follows:

- 
- Step 1** Go to the taskbar where the tray icons are displayed and right click the left angle bracket ( < ).

- Step 2 Select “Customize Notifications...”
  - Step 3 Select “Cisco Systems AnyConnect VPN Client” and set to “Always Show.”
- 

## Cisco Security Agent Version Requirements

Cisco Security Agent (CSA) Version 4.5 and higher is the only version compatible with the AnyConnect client. The appropriate CSA policy ships with CSA and is attached to the group “Remote desktops and laptops.” These policies are not enabled by default; you must select them to prevent the AnyConnect client from failing with CSA version 4.5.

## PC Wireless Client Configurations

If a client wireless adapter profile supports scanning for a better access point, and you use the Cisco AnyConnect VPN Client or Cisco VPN Client (IPSec) with that profile, disable such scanning. These scans can cause disconnections or stall traffic on the tunnel. To support scanning for non-SSL/IPSec connections, create another profile.

## Certificate Revocation List Processing

A Certificate Revocation List (CRL) contains a number of certificate serial numbers that have been revoked. The client downloads this list from a CRL server and looks up the certificate of the security appliance in the list.

The Cisco AnyConnect VPN Client requires a Certificate Revocation key with a value of 1 to enable the checking of the certificate revocation list. The following path shows the Certificate Revocation key and value on the remote PC:

```
My Computer | HKEY_USERS | <Secure ID_of_Logged_User> | Software | Microsoft | Windows |
CurrentVersion | CertificateRevocation REG_DWORD 0x00000001
```

The client attempts to read the value of the flag *CertificateRevocations* shown above to determine whether the client checks for revocation of the security appliance certificate.

To set the Revocation flag, select **Control Panel > Internet Options**. Click the **Advanced** tab, and click the **Restore Defaults** button near the bottom of the window. This option restores all of the options under the Advanced tab to the original settings.

Alternatively, to avoid restoring original settings, you can perform the following:

- 
- Step 1 Check the check-box **Check for server certificate revocation** (requires restart).
  - Step 2 Click Apply.
  - Step 3 Click OK.
  - Step 4 Restart Windows.
- 

If Revocation is enabled, a dialog window prompts the remote user to accept or deny the certificate that has a revocation error.



## Zyxel Modem SSH Incompatibility

The AnyConnect client is not compatible with the Zyxel Prestige 643 V2.50 (AP.3) DSL modem running the Putty SSH protocol.

## Dynamic Install Fails on Windows Vista When Running Low-rights Internet Explorer

Internet Explorer 7 on Windows Vista has a new security feature called Low Rights Internet Explorer. This feature changes the rights of the sandbox that the browser operates from to the lowest level possible. Because Windows Installer service has the ability to elevate all the way to Local System, the Windows Installer refuses to accept calls from Low Rights processes (as IE7 now is).

When using low-rights Internet Explorer to attempt a first-time web installation of the AnyConnect client, the MSI install fails immediately. The MSI log contains the following entry:

```
Failed to connect to server. Error: 0x80070005
```

To avoid this, users on Vista *must* add the Secure Gateway to the Trusted Zone (CSCsh23752).

## AnyConnect Fails to Establish a DTLS Tunnel When Using RC4-MD5 Encryption

When the ASA to which the AnyConnect client is attempting to connect is configured to only do RC4-MD5 encryption, the client is unable to establish a DTLS tunnel (CSCsg73318).

## Linux Client Weblaunch Requires an Account with Sudo Access

Launching the AnyConnect client for Linux from the browser does not work when the user is non-root and when the user does not have sudo access on the machine. To work around this problem, install sudo, adding a line like "someusername ALL = (ALL) ALL" (without the quotes) to /etc/sudoers (CSCsg20843).

## msvc60.dll Must Be Available for Installation of the AnyConnect Client

To use the Cisco AnyConnect VPN Client, you must have the file msvc60.dll — c++ runtime located in the winnt\system32 directory on your system. This dll is likely already to be present on most images, since installing other products (such as Office 2000) results in this file being placed on the system.

Because of this common practice, this dll file is excluded to reduce the image size for AnyConnect client dynamic installations. For more information about this problem, see the Microsoft Knowledge Base, article 259403, at <http://support.microsoft.com/kb/259403>. (CSCsg27872).

## Secure VPN Via Windows Remote Desktop Is Not Supported

The AnyConnect VPN Client and the SSL VPN client do not support VPN connection establishment via a Windows Remote Desktop session. If you connect to the PC via Remote Desktop, your VPN connection will not be allowed.

## AnyConnect Start Before Logon GINA Might Not Appear on Login Screen after Reboot

When the AnyConnect Start Before Logon GINA is installed on a user's PC using the standalone installer (WinGinaSetup-xxxx.msi), the GINA does not appear on the login screen after a reboot. This occurs because the AnyConnect GINA requires that the following be installed:

- AnyConnect Client
- An AnyConnect profile (.xml file) in Documents and Settings/All Users/Application Data/Disco/CiscoConnect VPN Client/Profile/ with the following line in it:

```
<UseStartBeforeLogon UserControllable="false">true</UseStartBeforeLogon>
```

Network administrators must push out a profile using their SMS or other software deployment engine along with the MSI files if they want to perform a preinstall of the profile (CSCsh33322).

## When Using a Client-Side Proxy and Full Tunneling, the Proxy Should Be Reset

When a client side proxy is used to connect to the internet, full tunneling cannot not be enforced on the client since users can still connect to the proxy server even when in full tunneling mode. This behavior inherent in the nature of SSL VPN solutions (CSCsh51779).

## Linux-Specific AnyConnect Client Issue

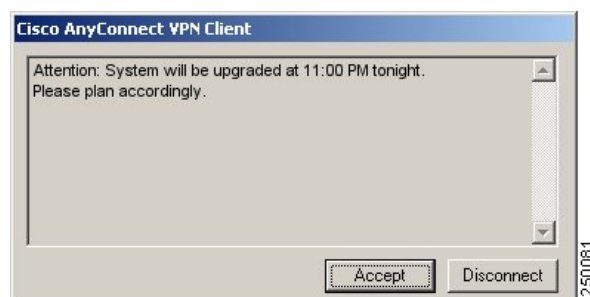
The AnyConnect client might not establish DTLS tunnel in Linux and might revert to TLS.

In addition, the AnyConnect client reports that statistics in the Linux user interface are not available. Closing the user interface without disconnecting and launching another (while the tunnel is still active) seems to fix the problem (CSCsh79391).

## Setting the AnyConnect Pre-Login Banner

The pre-login banner is the optional banner message that appears as a pop-up window in the end-user AnyConnect client interface, as shown in [Figure 13](#).

*Figure 13 Pre-Login Banner*



You can use either of the following methods to configure the banner on the security appliance:

- Import/export the DfltCustomization file <custom> <auth-page>.

```
<copyright-panel>
<mode>enable</mode>
<text>Copyright...</text>
<copyright-panel>
```

The <text> element value is the pre-banner text.

- Select ASDM.Remote Access VPN > Clientless SSL VPN Access > Portal > Customization. On the resulting window, select DfltCustomization, and then Edit. A GUI appears, and you can edit the Copyright text.

## 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 (CSCsh76698).

## Smartcard Support

The AnyConnect client supports Aladdin eTokenPro32k and Axalto Smartcards and readers on Windows Vista Ultimate, Windows XP Professional with SP2 and Windows 2000 Professional with SP4. In Release 2.0, there is no Smartcard support for Mac OS X or Linux.

## Mac OS X and Linux Clients Might Disconnect If a Security Appliance Failover Occurs

When the security appliance is operating in a high-availability Active/Standby configuration and a failover occurs, causing the Standby security appliance to resume current connections, Mac OS X or Linux AnyConnect connections might disconnect. If a MAC OS X or Linux AnyConnect connection disconnects after a failover you must reconnect. (CSCsi44920).

## IPv6 AnyConnect Failover is Not Supported for the Security Appliance

ASA Release 8.0 does not support IPv6 failover, so failover of IPv6 AnyConnect (as well as failover of clientless SSL VPN) sessions is also not supported (CSCsi43708).

## Framed IP Address Is Not Available in a Start Accounting Request

The AnyConnect client does not provide a framed IP address in a START accounting request. The framed IP address is unavailable *only* for this condition. It *is* available in the paired STOP request (CSCsh30754).

## AnyConnect Split-tunneling Does Not Work on Windows Vista

AnyConnect split-tunneling works correctly with Windows XP and Windows 2000 (CSCsi82315).

## Tunneling Mode Value Should Be Split Include, Not Split Tunneling

The Connection Information section of the Statistics Details dialog contains a Tunneling Mode indicator. This indicator can be one of the following values:

- All Traffic for All-or-Nothing tunneling
- Split Include to include the listed networks in the tunnel. This was formerly called “Split Tunneling.”
- Split Exclude to exclude the listed networks from the tunnel.

When Split Include tunneling is configured on the secure gateway, the “Tunneling Mode” value appears as “Split Include,” rather than “Split Tunneling” (CSCsj36826).

## Selecting Crypto Toolkits for AnyConnect on Windows Platforms

To use Windows certificates and proxy support, the AnyConnect client uses the cryptography support present on the operating system to establish an authentication session. The cryptographic cipher used for authentication is bounded by what the host operating system supports and is distinct from the cipher used to encrypt the AnyConnect tunnel data.

This is commonly encountered when an administrator configures “ssl encryption aes128-sha1” on the security appliance. Because older versions of Windows (pre-Vista) do not support AES, neither Internet Explorer nor the AnyConnect client in stand-alone mode can establish clientless or AnyConnect sessions on these platforms when *only* AES is configured.

Since the AnyConnect client always attempts to use the strongest tunnel encryption possible, it is possible to work around this by using “ssl encryption aes128-sha1 3des-sha1”. This causes the initial authentication session to use triple DES, but causes all tunneled data to be encrypted with AES (CSCsi85902).

## First User Message for Double-byte Languages Does Not Translate Correctly

With the Unicode version of the AnyConnect VPN Client—which allows for double-byte languages such as Japanese, Chinese, and so on—the first user message to appear does not correctly translate, because that message is missing from the AnyConnect translation table.

To work around this problem, add the following lines to the translation table file that you are using for translations:

```
msgid "Please enter your username and password."
msgstr ""
```

The message string (msgstr) value should be your translation of the English string in msgid.

## Ensuring Reliable DTLS Connections Through Third-Party Firewalls

A third-party network firewall blocks DTLS (UDP) traffic if traffic is idle for 40 seconds and if DTLS keepalive is not enabled.

When a 3rd party network firewall is located between the client PC and the security appliance, it inspects each DTLS packet and makes a decision whether to pass the packet along to the destination. If there has been an idle period of DTLS traffic, the firewall might stop sending data to the client or security appliance.

A customer has observed that the default behavior of a third party firewall in their network results in the DTLS (UDP) traffic being dropped after an idle period of 40 seconds. This occurs when the DTLS keepalive is not configured, or is configured with a value that is greater than the timeout interval of the third party firewall.

By default, the DTLS keepalive is disabled.

When DTLS traffic is stopped by the firewall, applications such as Microsoft Outlook stop responding while the DTLS tunnel remains active. The time of inactivity is directly related to the interval set for client DTLS DPD. By default, DPD is set to an optimal value of 30 seconds which should work in most cases.

If the client DTLS DPD is too high, failover does not occur quickly enough, and a user notices applications being unresponsive. Once the client DTLS DPD is set correctly, the customer then notices excessive loss and re-establishment of the DTLS channel. This might also be perceived as poor performance of the tunnel.

To correct this problem, do the following steps:

- 
- Step 1** Enable the client DTLS DPD and configure it to be twice the interval of the firewall idle timer.
- For example, set this value to 2 minutes when using the default setting with the third party firewall (40 seconds). The client DTLS DPD value should be no greater than 10 minutes to ensure TLS fallback occurs in a timely manner.
- Step 2** Step 2 Enable the client DTLS keepalive and configure it to be at least 10 seconds less than the firewall idle timer interval.
- For example, set this value to 30 seconds if using the default configuration (40 seconds) of the third party firewall (CSCsj51235).
- 

## Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The open caveats in Release 2.0 appear first in this list.



### 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](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

## Open Caveats in Cisco AnyConnect VPN Client, Release 2.0

Table 5 lists the caveats that are unresolved in the Cisco AnyConnect VPN Client, Release 2.0.

**Table 5** *Open Caveats in Cisco AnyConnect VPN Client, Release 2.0*

Identifier	Headline
CSCsg16910	Mac OS X: hole in routing table for local subnet.
CSCsg16922	Linux/MAC library issues (static/dynamic) for OpenSSL and Curl.
CSCsg17091	Route monitoring for MAC/Linux.
CSCsg17098	File Api - won't work on CE.
CSCsg20141	Create DLL for API, Common, CommonCrypt.
CSCsg20206	Localization message collection tool.
CSCsg20346	Complete Windows Pocket PC 2005 Phone Edition support.
CSCsg20388	performance of data path affected by memory allocations (ipv6).
CSCsg20448	"STATUSCODE error tables are only in Windows' vpnagent. Other OSs ?
CSCsg20456	API & i18n engine do not compile in _UNICODE and/or are not PPC ready.
CSCsg26100	ProcessApiLaunch() should handle platform dependencies.
CSCsg26573	Event for failed connections due to no IPv4 address should be better.
CSCsg29556	Add AnyConnect CLI to AT.
CSCsg40933	GUI statistics should include the assigned IPv6 address.
CSCsg41343	Numerous Routing, Cert, and Socket ERROR Events seen in Event Log.
CSCsg42924	Linux / Mac do not encrypt disk files (Need CDataCrypt).
CSCsg48746	IPv6: XP Anyconnect takes a very long time to complete or disconnect..
CSCsg49179	LocalLAN configuration does not result in prompting to accept/decline.
CSCsg55572	AnyConnect doesn't use 2nd WINS server received from ASA.
CSCsg65937	Need an uniform logging mechanism for all platform.
CSCsg77160	Extract proxy name and port data form firefox and safari.
CSCsg91679	VA does not separate configurable MTU and MRU.
CSCsg93123	IPv6 routing table: Entry for "Auto Tun Pseudo-interf" left after discon.
CSCsg93252	IPv6: Teredo Tun Pseudo-Interface Metric increases with every disconnect.
CSCsg94771	Move ProcessApi cal in standalone api to separate thread.
CSCsg96288	IPv6: Route notification has not been implemented for IPv6.
CSCsg96324	Weblaunch - Replace checkboxes for phase status with image.
CSCsg96758	IPV6 Linux: displaying the IPv6 routing table is very slow after connect.
CSCsg99246	Use "Cisco AnyConnect Mobile" as official name for WM5 client.
CSCsh04359	Linux:ICMP traffic not transmitted to 1 particular device on my network.
CSCsh11163	MSIE Proxy confured msie-proxy method use-pac use-server auto-detect.
CSCsh19245	AnyConnect Client re-branding .mst examples needed & documented.
CSCsh21051	DNS updates can clobber routing changes on Mac OS X.

**Table 5** *Open Caveats in Cisco AnyConnect VPN Client, Release 2.0 (continued)*

Identifier	Headline
CSCsh23440	Linux/MAC: Anyconnect/Homepage functionality does not work.
CSCsh33359	Update usage of CertHelper in standalone API.
CSCsh40306	SBL: AnyConnect GUI doesn't have a way to toggle Start Before Login.
CSCsh40449	AnyConnect standalone on Win2000 takes 45 sec to timeout unavailable con.
CSCsh41494	MAC ipv6 client route is not deleted from routing table on discon.
CSCsh45522	New Tunnel rekey method should establish new tunnel in parallel.
CSCsh46770	SBL: AnyConnect profile param: UserControllable="true" - does not work.
CSCsh46780	SBL: AnyConnect does not have incompatible GINA list or fallback mode.
CSCsh51655	AnyConnect VPN Downloader - The installer has to abort the process.
CSCsh51779	Using a client-side proxy and FULL tunneling, the proxy should be reset.
CSCsh54890	AnyConnect radius password expiry should update win cached credentials.
CSCsh57967	AnyConnect standalone doesn't logout of ASA if error occurs at connect.
CSCsh61062	AnyConnect Agent does not restore routes on start up.
CSCsh61728	cvc: virtual adapter shows as 1 Gbps.
CSCsh62905	SBL: no vpn connection after anyconnect version upgrade using SBL.
CSCsh65683	downloader does not prompt user for validation if cert policy error.
CSCsh66308	Install/Uninstall performance degrades after repeated installation.
CSCsh68236	IPv6: Client should disconnect then restore routing table.
CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client.
CSCsh69793	Mac OS X Cingular broadband card launch2net incompatibility issues.
CSCsh69887	Downloader needs proxy credentials from standalone API.
CSCsh70484	Update CCO title for AnyConnect
CSCsh72839	IPv6: network specific route is not used for XP.
CSCsh73274	While DTLS to SSL fallback powerpc shows no tunnel details on UI.
CSCsh73327	When client falls from DTLS to ssl, the ui never reflects the change.
CSCsh73647	AnyConnect SDI authentication fails.
CSCsh73916	Proxy support in non-windows missing.
CSCsh76671	Rebranding support needs to be documented.
CSCsh76694	IPv4 IPv6 packet filtering needs to be implemented for Vista x86 / x64.
CSCsh77817	CLI: vpncli disconnect - displays unnecessary warning, state, and notice.
CSCsh78808	Mac localization.
CSCsh79410	AnyConnect does an nslookup when an IP Address is used to connect.
CSCsh81003	XP: After failed conn, client reports "Internal Error" and needs restart.
CSCsh81109	non-windows signals need to be handled safely, not inline.
CSCsh81145	Mac OS X link routes need to be programatic, not exec()ed
CSCsh81519	AnyConnect: split-dns - all DNS queries are sent through the tunnel.

Table 5 Open Caveats in Cisco AnyConnect VPN Client, Release 2.0 (continued)

Identifier	Headline
CSCsh83250	Linux Standalone: auto upgrade does not work until GUI is closed.
CSCsh84315	IPv4 packet filtering for XP x86 and x64.
CSCsh91762	AnyConnect installation problem on win 2k Professional.
CSCsh93889	Apparent GUI hang when svc enable not set for username.
CSCsh96598	AnyConnect cannot start from 64-bit IE - Platform detection: undefined.
CSCsh99297	Anyconnect connection drops when using IM SIP Client advanced features.
CSCsi00491	Standalone can connect to wrong ASA from within SecureDesktop.
CSCsi00707	AnyConnect using SDI -prompts for Password instead of Passcode.
CSCsi00732	AnyConnect stats increase when Client sends DPDs -ASA doesn't count DPDs.
CSCsi02158	Agent need to send new proxy credential request when bad creds received.
CSCsi02702	Mac OS X error notice callback handled inline, when shouldn't be.
CSCsi05333	AnyConnect upgrade on Vista - MSI dialogs don't appear showing progress.
CSCsi08774	Agent contains user displayed strings that are not gettext-ed.
CSCsi11016	MAC: reconnecting with weblaunch will fail.
CSCsi12002	Certificate auth fails under Linux SuSE & MAC with standaolne client.
CSCsi15715	AnyConnect Stats don.t increment after fallback from DTLS to TLS.
CSCsi17247	Mac: Internal Error on GUI if banner is not accepted.
CSCsi17273	Lockup can occur if -Download signed ActiveX- is set to promp
CSCsi20440	AnyConnect GUI fields can sometimes overlap each other - Vista onl
CSCsi29312	Disconnecting tunnel is delayed if cert CN does not match URL.
CSCsi34655	AnyConnect:unable to "quit" the client after "disconnect" (IOS only).
CSCsi35149	Transcend:unable to clear the session from GW after setting MSIE proxy V.
CSCsi44045	Difficult to clear the vpn program after tunnel cleared from GW.
CSCsi44920	Mac OS X and Linux clients may disconnect with an ASA Failover.
CSCsi51176	client behavior when non-admin users try to establish tunnel.
CSCsi52276	Stats   Export: should include routing and interface information.
CSCsi52292	Stats   Export function should be implemented on the MAC.
CSCsi53608	AnyConnect CSCOTUN0 interface does not install under SuSE Linux.
CSCsi55289	AnyConnect does not fail connection when zlib library not present.
CSCsi58457	AnyConnect VPN User Interface sometimes crashes - module msvcrt.dll.
CSCsi63910	Beta: Anyconnect launches w/o GUI, tray icon only appears.
CSCsi65887	AnyConnect vpncli stats - does not display Client / Server addresses.
CSCsi69205	smart card cant be used with MAC AnyConnect client.
CSCsi70729	AnyConnect: Increase default countdown timer from 15 seconds.
CSCsi70995	AnyConnect standalone cannot connect using group-url (ip/tungroup).
CSCsi74237	Error messages / Source (ASA or Client) of error not always clear.



**Table 5** *Open Caveats in Cisco AnyConnect VPN Client, Release 2.0 (continued)*

Identifier	Headline
CSCsi75349	Add VA checks.
CSCsi78868	GUI select button not enabled.
CSCsi82315	AnyConnect split-tunneling does not work on Vista (XP & 2K are OK).
CSCsi83419	JAVA weblaunch component fails NTLM auth on St. Bernard Proxy.
CSCsi86201	AnyConnect/SBL doesn't work if CSD/cache cleaner enabled.
CSCsi87650	Statistics wrap from 2^32 to 0 -- 64-bit counters needed.
CSCsi88191	vpncli cert-only group select - client still prompts for user/pw.
CSCsi89708	Difficult to cancel out at cert popup - click No - more popups.
CSCsi89839	AnyConnect window inside CSD shows ip address and not host name.
CSCsi94721	AnyConnect falsely displays hostname mismatch warning if fqdn exists.
CSCsi98932	Anyconnect need to provide Delete With Reason (DWR) with text to headend.
CSCsj11555	AnyConnect Client bug --split-include route can't go for 20 or above.
CSCsj15170	MAC disconnect message gets truncated.
CSCsj16746	Profile with "Match Case" in cert config generates error.
CSCsj16869	Cert Matching not working with multiple match criteria.
CSCsj20275	Mac OS X UI sometimes truncates netmask information in stats.
CSCsj22315	AnyConnect VPNGINA uninstall does not restore a 3rd party GINA.
CSCsj23813	AnyConnect SBL GUI closes after CSD host scan loads - can't login.
CSCsj24737	API needs to return user error when X-Transcend header is not returned.
CSCsj24764	Downloader needs to support distribution and use of thirdparty gui.
CSCsj25927	Linux installer to check for required client dependencies.
CSCsj27443	AnyConnect MAC client PW management forces user to change PW.
CSCsj27577	Update Linux GUI code generation tool for string references.

## Resolved Caveats

The following sections list the resolved caveats in Cisco AnyConnect VPN Client, Release 2.0:

**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0*

ID	Headline
CSCsg10149	Use new Cisco logo on all dialogs and splash screens.
CSCsg16581	Need a manifest data file update utility.
CSCsg16591	Proxy for standalone not implemented.
CSCsg16594	Proxy for Web launch not implemented.
CSCsg16601	Downloader handling of localization & profile not implemented.
CSCsg16910	Mac OS X: hole in routing table for local subnet.

**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0 (continued)*

ID	Headline
CSCsg17089	CLI minor fixups.
CSCsg17092	MAC install needs cleanup.
CSCsg17100	Convert linux routing code to NETLINK.
CSCsg18576	Sign MSI.
CSCsg20152	General IPC fixes.
CSCsg20159	Statistics cleanup and enhancements.
CSCsg20165	Windows GUI needs functional improvements and aesthetic changes.
CSCsg20175	Profile updates.
CSCsg20220	Certificates - client cert selection should be transparent to user.
CSCsg20222	Profile and Preferences specification not yet available.
CSCsg20242	Certificates - Standalone support of client certificates.
CSCsg20247	Certificates - standalone needs to support certificate enrollment.
CSCsg20325	Recompile the distributed libcurl without zlib.
CSCsg20332	Filtering support missing in Linux.
CSCsg20353	Needs to add IPv6 routing support.
CSCsg20366	Start Before Logon (SBL) feature missing.
CSCsg20402	Import PKCS12 certs on Linux.
CSCsg20414	Import PKCS12 certs on Mac.
CSCsg20429	Key Usage/Extended Key Usage not supported.
CSCsg20439	Cert DN Matching not implemented.
CSCsg20628	Routing change vulnerability - small window.
CSCsg20631	CE crash in CIPV6Packet::ParserIPv6Packet().
CSCsg20711	Agent always tries to launch a 2nd GUI, even when the Stand-Alone one.
CSCsg20843	Linux client weblaunch does not work from an account without sudo access.
CSCsg23338	AnyConnect Client name needs to be added -or changed to- in many areas.
CSCsg23519	AnyConnect GUI can be closed - no indication still connected.
CSCsg23560	IPv4 CVC fails to connect if headend has IPv6 enabled.
CSCsg23594	Old Cvc client stays after connection drops and new svc is installed.
CSCsg24372	vpnui usually crashes when reconnecting the CVC.
CSCsg25159	AnyConnect Client cannot connect when DTLS is configured on the ASA.
CSCsg25188	AnyConnect client drops tunnel when rekey is enabled on headend.
CSCsg25207	AnyConnect cannot connect using CLI when not running xwindows.
CSCsg25313	AnyConnect cli "stats" command non-functional in Linux.
CSCsg25320	AnyConnect clients allows traffic to local net when tunnelall enabled.
CSCsg26111	Uninstall not performed on Mac/Linux implementations.
CSCsg26122	Downloader should not show it's GUI if invoked by stand-alone client.

**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0 (continued)*

ID	Headline
CSCsg26189	ipconfig on CVC client shows ipv6 addresses from earlier conns.
CSCsg26345	vpnui does not report any error messages when connections fail.
CSCsg26399	vpnagent Event ID: 15 should include the IPv6 address in the list.
CSCsg27872	msvc60.dll needs to be available for install of client.
CSCsg27908	Incorrect command line parameters error prevent client install.
CSCsg27953	Linux routes using system().
CSCsg28081	title.gif in Client pkg file needs to be updated with the new Cisco logo.
CSCsg28168	Module doesnt get downloaded with the CLI set on ASA.
CSCsg29663	AnyConnect client is not allowing simultaneous WebVPN portal access.
CSCsg29703	CVC VPN Adapter can't receive packets if monitored using ethereal.
CSCsg29785	AnyConnect client v2.0.0043 does not install via Java - only ActiveX.
CSCsg30234	AnyConnect fails to establish a vpn connection in Mac OSX.
CSCsg30303	AnyConnect Linux GUI tab key fails to change focus to "username" field.
CSCsg31495	AnyConnect linux installer fails to add vpnagentd_init to chkconfig.
CSCsg33025	IPv6: IPv6 header corrupted on some received packets with frag. offsets.
CSCsg33382	AnyConnect linux web-initiated connect doesn't notify user of status.
CSCsg37753	Mac OS X GUI group selection combo not returning correct value.
CSCsg38036	Client connects but GUI displays -VPN Service not available - Windows 2000.
CSCsg39215	IPv6: Pings from on-lan hosts to connected CVC clients fail.
CSCsg39803	Close from AnyConnect GUI should NOT close the GUI when connected.
CSCsg39863	AnyConnect UI can be opened multiple times.
CSCsg42585	Digital signature error on install - virtual adapter needs to be signed.
CSCsg42981	AnyConnect with client cert auth fails to connect - CERT_NOT_FOUND.
CSCsg42999	Mac GUI doesn't show routes.
CSCsg43021	CVC does not support IPv4/6 addresses for msie-proxy-server settings.
CSCsg43920	AnyConnect install does not error when attempted on non admin account.
CSCsg43985	Infinite loop in internalSocketRead logs thousands of syslogs.
CSCsg45647	Localization feature not available.
CSCsg45703	Downloader must store manifest data file in a common directory.
CSCsg47177	Unable to verify routing table mods are correct - client doesnt connect.
CSCsg47559	Mac/Linux agents do not restore routing table and crash on disconnect.
CSCsg47735	Reset button in AnyConnect GUI Statistics   Details - doesn't work.
CSCsg48652	AnyConnect DTLS disconnects when DPD configured on ASA.
CSCsg48699	AnyConnect sees DPD client value from ASA x 1000 (that is, ASA=30 is 30000).
CSCsg51147	AnyConnect client agent crashes on disconnect.
CSCsg53846	AnyConnect VPN Agent fails to start on Windows XP 64-bit (web install).

**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0 (continued)*

ID	Headline
CSCsg54341	Linux iptables support uses system().
CSCsg54344	Mac OS X and Linux filtering is broken.
CSCsg55589	AnyConnect GUI does not show Routes for split-tunneling / local LAN.
CSCsg56203	AnyConnect Linux reinstall fails after manual uninstall.
CSCsg58708	Linux filtering not properly setting up port/protocol filtering.
CSCsg60550	Daemon on Mac OS X is chatty in syslog while idle.
CSCsg60563	Manifest file location a bad choice for Mac OS X and Linux.
CSCsg64798	AnyConnect Linux/Mac group dropdown causes API to hang/crash.
CSCsg64824	vpndownloader causes AnyConnect Linux UI hang when connecting.
CSCsg66558	Any Connect agent crashes on user logoff and system shutdown.
CSCsg67211	Rebootless Client Upgrade.
CSCsg69686	AnyConnect Win client GUI shows incorrect message on standalone connect.
CSCsg69699	AnyConnect Win32: manually stopping vpnagent service results in failure.
CSCsg71528	AnyConnect Linux / Mac client fails to connect after initial web install.
CSCsg72222	AnyConnect Linux/Mac fails to connect with exclude-local-lan configured.
CSCsg73252	“Unable to attach to VPN subsystem” when running GUI/CLI simultaneously.
CSCsg73318	AnyConnect Linux/Mac fails to establish DTLS tunnel when using rc4-md5.
CSCsg73973	AnyConnect Mac cannot connect when DTLS enabled.
CSCsg77199	Gina implementation incorrectly hardcodes path to UI.
CSCsg80040	IPv4 routing support for Windows Vista.
CSCsg80705	cvc: feature, smartcard support for start before logon.
CSCsg81130	AnyConnect Mac dtls connection fails with split-tunnel configured.
CSCsg82454	TerminateTLV is being called during tunnel disconnect.
CSCsg86171	The profile doesnt get installed correctly.
CSCsg86261	AnyConnect Profile folder should be removed - profiles don't go there.
CSCsg86425	AnyConnect error dialogs do not contain AnyConnect in the title bar.
CSCsg86673	vpnui crashes on Windows 2000.
CSCsg88127	AnyConnect Win client GUI crashes when disconnect clicked multiple times.
CSCsg88147	No disconnected state sent to client after clicking disconnect.
CSCsg88161	Agent Crash in IPC code when client sends multiple disconnects.
CSCsg89170	AnyConnect client displays incorrect version number in Linux.
CSCsg89335	AnyConnect client fails to run when you have a cvcprofile.xml with Windows 2000.
CSCsg89369	AnyConnect client fails on library file libstdc .so.5.
CSCsg90253	SVC Client download content needed to be centered in iframe.
CSCsg91133	Window XP: Disconnect button does not work properly.
CSCsg92715	Downloader fails updating localization for limited XP user or Vista.

**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0 (continued)*

ID	Headline
CSCsg93626	Windows 2000 does not support “SslEmptyCache” required by API.
CSCsg95388	Crash in HTTP header parsing in ConnectIfc with UNICODE build.
CSCsg95403	Windows CE Weblaunch needs new look and feel.
CSCsg96468	Installer tries 64bit driver on 32-bit machines, fails w/error code 258.
CSCsg97977	WinXP GUI: Misc issues from dogfood week.
CSCsg98209	Client does not use DNS Server value from ASA group-policy.
CSCsg98647	Connection failure: Unknown - when 1st connection entry inaccessible.
CSCsg99018	Agent should not send client cert to the head-end..
CSCsg99032	Downloader should not send client cert to the head-end
CSCsg99773	Weblaunch installation window never closes.
CSCsg99840	Linux/mac all dbrownhi Download fails to start tunnel in standalone on non-windows.
CSCsg99911	Insufficient indication of user connection status at establishment.
CSCsg99937	AnyConnect Stats Details - Crypto Information - shows as Not Available.
CSCsh00010	AnyConnect WebLaunch - there is no installation progress shown to users.
CSCsh00215	AnyConnect standalone wont connect if ASA has tunnel-group-list enable.
CSCsh01349	MSIE Proxy Support configured for no proxy not changing Client setting.
CSCsh01583	Downloader never exits when launched via API.
CSCsh01742	nstaller link for "Download" phase goes to bad url in Release builds.
CSCsh02509	Quitting the AnyConnect GUI does not disconnect the client.
CSCsh02547	UI does is left in bad state when hitting enter with empy cred / pwd.
CSCsh04284	Reconnecting with web install causes “VPN Service not available” error.
CSCsh05087	Default (0.0.0.0) route does not work correctly on Vista.
CSCsh05836	Beta feedback: stats should be greyed out after client disconnect.
CSCsh05869	AnyConnect Mac client fails to connect with GUI.
CSCsh07158	SBL: AnyConnect connection from SBL connects but then restarts the PC.
CSCsh10829	AnyConnect SBL fails to launch after user logout.
CSCsh11131	Delay in getting usernam and password.
CSCsh11142	After Reconnecting using standalone client - disconnect not available.
CSCsh11163	MSIE Proxy configured as “msie-proxy method use-pac use-server auto-detect” fails.
CSCsh11296	CSA complains when GUI/CLI launch the downloader.
CSCsh12710	Attempt to recon connected AnyConnect client should notify user of status.
CSCsh12846	AnyConnect standalone does not display the VPN banner.
CSCsh12855	Cannot enter IP address or DNS name when using profiles.
CSCsh14078	Cannot install AnyConnect Client on MAC.
CSCsh14148	SBL gives connection error.
CSCsh14160	SBL authentication unsuccessful.

**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0 (continued)*

ID	Headline
CSCsh14179	Successful SBL authentication doesn't establish tunnel.
CSCsh14340	AnyConnect Manual Installation does not link to the correct file.
CSCsh14787	CLI & GUI take too long to download the downloader.
CSCsh14967	Downloader fails: "The command line arguments are wrong."
CSCsh14974	Downloader always tries to download localization files.
CSCsh15686	Old GUI is not closed after upgrade/install.
CSCsh16302	Mac OS X GUI connect tab not showing correct connect/disconnect button.
CSCsh17502	Second instance of downloader not on correct desktop.
CSCsh17744	SBL: AnyConnect GINA Events are not being written to new AnyConnect Log.
CSCsh19005	SBL: An unknown reconnect error -occurs after successful Authentication.
CSCsh19165	Downloader installs profiles with wrong permissions.
CSCsh19221	Downloader needs to send TerminateTlv prior to start of install.
CSCsh19616	Agent should only start GUI when IPC ready.
CSCsh19717	Downloader may sometimes set profile permissions to w instead of r/
CSCsh20777	AnyConnect standalone takes too long to timeout unavailable connection.
CSCsh20817	Selecting the Connect menu option from system tray icon does nothing.
CSCsh20863	AnyConnect client should provide option to save username and password.
CSCsh20975	Hitting return on the standalone ui connection tab window doesnt work.
CSCsh21080	MAC: Lock icon always displayed as locked even after disconnecting.
CSCsh22002	AnyConnect Standalone mode:ability to support URL based access.
CSCsh22326	AnyConnect new-tunnel rekey on Win 2000 takes 10-13 sec -apps disconnect.
CSCsh22361	Missing disconnect button on Mac OS X GUI after web-based login.
CSCsh22379	No trayicon when GUI launched before explorer.exe running.
CSCsh22468	Netbt (WINS) setting in VA config does not double NUL terminate strings.
CSCsh23306	Cannot reach local network through tunnel - works with SVC and IPSec.
CSCsh23502	MAC: "Exiting. Upgrade in Progress" message is inaccurate.
CSCsh23604	MAC: Group parameter is not a drop down box.
CSCsh23623	Mac OS X menubar menu not correct in 10.5.
CSCsh23682	MAC: disconnect notification messages are not displayed on MACs.
CSCsh23700	MAC: "AnyConnect Error" when trying to re-connect after physical disconn.
CSCsh23752	Dynamic Install fails on Vista when running low-rights Internet Explorer.
CSCsh24793	Cannot connect to headend if manifest file on remote computer is corrupt.
CSCsh24820	Linux: Can't connect from GUI more than once without reloading GUI.
CSCsh24833	Weblaunch install page does not accurately check off selections.
CSCsh25760	SBL GUI "diminished" when immediately after user logoff.
CSCsh25766	AnyConnect tunnel gets established when manifest on asa is corrupt.

**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0 (continued)*

ID	Headline
CSCsh26702	Web-initiated connect fails with no error message when using FUS.
CSCsh28259	vpnagentd dies after wakeup from sleep.
CSCsh29288	SSL reconnect error message when connection idle times out.
CSCsh29324	AnyConnect fallback from DTLS to TLS fails.
CSCsh29352	SBL: can not connect due to api did not use machine cert store.
CSCsh29386	AnyConnect Client connects then disconnects if DTLS can't be established.
CSCsh29426	Gina uses restrict token to spawn gui.
CSCsh30350	IPv6: IPv6 routing support for Vista needs to be implemented.
CSCsh30593	IPv6: Client should not disconnect until routing table is restored.
CSCsh33291	Failed connection pop-up window can be misleading.
CSCsh33322	SBL: AnyConnect GINA not appearing after MSI (standalone) install.
CSCsh33356	CLI loses original terminal settings on exit error.
CSCsh33389	AnyConnect - rekey using ssl fails with DTLS (OpenSSL:FATAL error).
CSCsh33744	AnyConnect Client stops passing data after a few SSL rekeys.
CSCsh33821	MAC Gui stats do not display client/server IP Addresses.
CSCsh36656	Standalone client does not work if CSD Secure Desktop is enabled.
CSCsh36763	Split tunneling doesn't work through NAT.
CSCsh38128	MAC: uninstaller should remove AnyConnect Icon in Applications folder.
CSCsh38590	VpnGina not dynamically installed after manual install of client.
CSCsh40388	SBL: AnyConnect GINA should not install on Windows XP Home Edition.
CSCsh41386	Certificates fail with AnyConnect client in standalone mode under Linux.
CSCsh41440	Enabling an adapter or mobile phone sync causes AnyConnect disconnect.
CSCsh41536	Mac client while connected shows as disconnected.
CSCsh41678	AnyConnect DTLS connects but fails to pass data using local Proxy server.
CSCsh41682	AnyConnect Win cli does not work with cmd line parameters.
CSCsh43974	CLI doesn't make use of API preferences.
CSCsh45017	MAC: reconn with weblaunch result in multiple icons; cant recon with...
CSCsh45442	Lock icon should unlock with admin reset or popup panel should be on top.
CSCsh45565	MAC: vpn_uninstall.sh does not run when disconnecting; installer=none.
CSCsh46746	SBL: VPNGina doesn't validate vpnu.exe -other apps could be run at boot.
CSCsh46761	AnyConnect fails install under Linux with any user other than root.
CSCsh46937	Wrong msg during uninstall: "Error: Exiting. Upgrade in Progress."
CSCsh47210	CLI disconnect on windows does not work the 1st time - CSD vulnerability.
CSCsh47761	"Unknown Error" when trying to connect while IE set to "Work Offline".
CSCsh48803	"Unknown Error" when trying to connect while IE set to "Work Offline".
CSCsh49282	Linux and mac os x upgrade fails , agent dies.

**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0 (continued)*

ID	Headline
CSCsh49382	Vpn-sessiondb should not display “Trancend 1’ for standalone AnyConnect.
CSCsh50858	SSL channel reconnects when using DPD & DTLS on Mac/Linux.
CSCsh51674	ActiveX control (vpnweb.ocx) should be removed during uninstall.
CSCsh51794	Client disconnect while roaming on 802.11x wireless.
CSCsh52184	AnyConnect Standalone doesn't work with auth challenges like SDI New PIN.
CSCsh52214	New manifest file is not downloaded if the one on remote PC is corrupt.
CSCsh52649	Api not checking the signature of the downloader before launch.
CSCsh53279	VPN downloader window needs to stay in the foreground when connecting.
CSCsh53698	Standalone UI: Focus should be on the password field not username.
CSCsh53794	Standalone UI: when connecting status message never changes.
CSCsh53852	WebLaunch Connection Status page on Win2000 not showing tray icon image.
CSCsh53997	Mac “Quit” should disconnect/quit.
CSCsh54961	Mac OS X client traffic MTU issues.
CSCsh55219	No connection duration info once client disocnects.
CSCsh55280	Progr. Error when restarting vpnui after disconnecting using “quit”.
CSCsh55327	About tab on the ui of client shows version 0.0.0.
CSCsh55438	Linux/MAC: discon notify window should not have Error in the title.
CSCsh55465	AnyConnect fails to reconnect if IP Address of the interface changes.
CSCsh56110	Export button -AnyConnect GUI Statistics   Details -doesn't do anything.
CSCsh56120	WebLaunch -Connection Established page - new icon not in example image.
CSCsh56131	AnyConnect Client   About - Copyright date says 2006 - should be 2007.
CSCsh56164	Help button does not function on AnyConnect UI.
CSCsh56183	Mac OS X intel GUI crash on upgrade.
CSCsh56195	MAC: UI does not Open when selecting from the Dock.
CSCsh56218	MAC: after a failed login the Connect button is no longer functions.
CSCsh56648	AnyConnect client not working with Win Vista.
CSCsh57374	Standalone GUI: Invalid SG can lead to continual error dialogs.
CSCsh58343	CVC:does not support the proxy server list in the auto proxy config.
CSCsh62786	IPv6: When upgrading from Stand Alone, client starts minimized and disco.
CSCsh62803	MAC: About Cisco AnyConnect: missing information.
CSCsh64564	The word "Weblaunch" is incorrect in AnyConnect.
CSCsh66502	Certificate auth fails under Linux when local CA server is used.
CSCsh67985	Update standalone API connection error messages.
CSCsh68135	IPv6-XP: cannot pass data if AnyConnect and ASA share outside interface.
CSCsh68891	Standalone client cannot connect to IOS devices.
CSCsh69717	uninstall needs to remove old icons and shortcuts.



**Table 6** *Resolved Caveats in AnyConnect Client, Release 2.0 (continued)*

ID	Headline
CSCsh70004	AnyConnect install under Linux requires sudo password.
CSCsh70094	MSIE Proxy pac url not sent to client when pac and proxy are used.
CSCsh71015	IPv6 Vista: Cannot est. an AnyConnect session -route verification fails.
CSCsh71022	Vista: Default Gateway for virtual adapter is set to 0.0.0.0.
CSCsh71461	Linux filter implementation is not reliable.
CSCsh71585	Cmemory leak message after connection.
CSCsh71659	The ui doesnt show the complete cipher.
CSCsh72781	vpn-max connect time gives error on mac_powerpc.
CSCsh72867	Disconnecting a ppc based mac AnyConnect client leaves session on ASA.
CSCsh73647	AnyConnect SDI authentication fails.
CSCsh74781	Weblaunch client cannot connect to IOS devices.
CSCsh75314	Client needs to support DTLS failover.
CSCsh76387	Downloader needs additional return code.
CSCsh76676	AnyConnect client cannot login to a vpn load-balancing cluster.
CSCsh76698	ASA must be configured to accept TLSv1 traffic for AnyConnect to work.
CSCsh79391	AnyConnect client cannot establish DTLS tunnel in Linux.
CSCsh81014	Anyconnect client cert auth errors and can not connect.
CSCsh81039	MAC: AnyConnect will hang and require reboot if conn fails due to no IP.
CSCsh81063	IPv6 XP: status bar states "conn establish" before IPv6 routes are added.
CSCsh81187	Linux client iptables location.
CSCsh81485	VPNUI crashes if smart card is pulled out when tunnel connected.
CSCsh81565	Use of "Local LAN" for Tunneling mode is unclear.
CSCsh81620	AnyConnect DTLS reconnect should use a different UDP source port.
CSCsh83118	Standalone client does not work if CSD Posture Assessment is enabled.
CSCsh83136	Stand alone client connect to edit box displays CSD token.
CSCsh83273	AnyConnect URL edit box should be grayed out when in Secure Desktop.
CSCsh84751	AnyConnect Agent crashes after timeout for Proxy creds.
CSCsh86139	Vista: default gateway is removed after disconnecting and rebooting.
CSCsh86494	Can't open SecureDesktop - invalid token.
CSCsh86543	Update release file names.
CSCsh87182	Mac OS X disconnect quit callback not waited for.
CSCsh87966	Mac OS X GUI does not display the host connected to on web based.
CSCsh88894	GUI focus updates needed.
CSCsh89394	With Windows Vista, moving from wireless to docking station crashes agent.
CSCsh89394	Moving from wireless to docking station crashes agent.
CSCsh89509	AnyConnect is not logging out correctly - clientless session still up.

Table 6 Resolved Caveats in AnyConnect Client, Release 2.0 (continued)

ID	Headline
CSCsh89615	Shutting down PC while tunnel is up cause bad VA entries next start...
CSCsh93590	StandAlone fails to connect within Secure Desktop.
CSCsh93610	Workaround for no inline DTLS rekey on ASA.
CSCsh97160	AnyConnect Mac does not work with CSD enabled.
CSCsh97420	AnyConnect can't upgrade to newer version within Secure Desktop.
CSCsi35175	Has some issue in pushing the "auto" option for IE proxy settings.
CSCsj36826	Tunneling Mode value should be Split Include, not Split Tunneling.

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.



### Note

For the Cisco AnyConnect VPN Client, the documentation consist of this set of Release Notes and the *Cisco AnyConnect VPN Client Administrator Guide*. You can find configuration information for the AnyConnect VPN Client in the *Cisco Adaptive Security Appliance 5500 Series CLI Configuration Guide*.

## Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Registered Cisco.com users can order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

---

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. Access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0612R)

© 2007 Cisco Systems, Inc. All rights reserved.



