Release Notes for Cisco AnyConnect VPN Client, Version 2.2

Revised: May 24, 2010, OL-16160-08

Introduction

These release notes are for the Cisco AnyConnect VPN Client, Version 2.2, which provides remote users with secure VPN connections to the Cisco ASA 5500 Series Adaptive Security Appliance using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol.

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 connecting to IPv6 resources over an IPv4 network tunnel. This release supports the SSL and DTLS protocol. This release does not include IPsec support.

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. After downloading, it can automatically uninstall itself after the connection terminates, or it can remain on the remote PC for future SSL VPN connections.

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.

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, page 36 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.

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

Contents

This document includes the following sections:

New Features in Cisco AnyConnect VPN Client, Release 2.2, page 2

Feature Overview, page 3

System Requirements, page 4

Upgrading to AnyConnect Release 2.2, page 7

New Features and Enhancements in Release 2.2, page 7

Installation Notes, page 11

Usage Notes, page 36

AnyConnect Support Policy, page 45

Caveats, page 45

Related Documentation, page 48

New Features in Cisco AnyConnect VPN Client, Release 2.2

This release includes the following new features:

- Support for Start Before Logon for Windows Vista systems, in addition to other Windows operating systems.
- Extended customization and localization features—This version of the AnyConnect client includes enhanced customization features and language translation features. In previous versions, you could customize client installations only on an individual PC basis. With this version, the security appliance can customize the client as it downloads and installs the client on the remote PC. You can also translate the client installer. These extended features include the following items:
  - Localized installs using localized MSI transforms (Windows only).
  - Custom MSI transforms (Windows only).
  - User-defined resource files.
  - Third-party GUI/CLI support.
  - Localization for Mac OS X (10.4 and higher).
- System tray in Windows systems now shows an icon when the AnyConnect client is reconnecting after losing connectivity.
- Enhanced Network Mobility—A user can lose connectivity for an extended period of time and still be able to have the client automatically resume the connection, as long as the security appliance has not logged the session off. In addition, a VPN session can now be retained during a hibernate/standby condition. This does not require any configuration changes; it is automatically enabled. The VPN tunnel might be dropped if the hibernation/sleep time exceeds the idle connection timeout or session timeout configured on the security appliance. You can also restrict this feature by setting the idle session timeout to a low value.

  In earlier versions, the tunnel would be automatically torn down when a system entered suspend or hibernate. For Windows Vista, please see the usage note on this topic "Windows Vista Might Become Unresponsive During Sleep/Resume Cycles or Other High-load Conditions (KB-952876)" section on page 37.

- Application Programming Interface (API), for customers who want to automate a VPN connection with the AnyConnect client from another application.

  The API package contains documentation, source files, and library files to support a C++ interface for the Cisco AnyConnect VPN Client.There are libraries and example programs that can be used for building on Windows, Linux and MAC (10.4 or higher) platforms. The Makefiles (or project files) for the Windows platform are also included. For other platforms, there is a platform specific script showing how to compile the example code. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.

Feature Overview

In addition to the new features listed above, the Cisco AnyConnect VPN Client provides remote users with secure VPN connections to the Cisco 5500 Series Adaptive Security Appliance.

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 Host Scan functions for Windows 2000 and Windows XP. Cisco Secure Desktop does not support the AnyConnect client within the Cisco Secure Desktop (Vault) on Windows Vista systems.

- Rekey—Specifies that SSL renegotiation takes place during rekey.

System Requirements

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

Operating System	Computer	Requirements
• Windows 2000 SP4. • Windows XP SP2. • Windows Vista. (*For optimal user experience, we recommend using this product with Vista Service Pack 1.)	Computer with a Pentium®-class processor or greater. In addition, x64 or x86 processors are supported for Windows XP and Windows Vista.	• 5 MB hard disk space. • RAM: – 128 MB for Windows 2000. – 256 MB for Windows XP. – 512 MB for Windows Vista. • Microsoft Installer, version 3.1.

Operating System	Computer	Requirements
AnyConnect supports Linux Kernel releases 2.4 and 2.6 on 32-bit architectures, and 64-bit architectures that support biarch (that is, that run 32-bit code). The tun module is required. All of the distributions we have tested include the tun module by default. The following Linux distributions have been tested and are known to work with the AnyConnect Client, while following the requirements listed in this document: • Ubuntu 7 and 8 (32-bit only). • Red Hat Enterprise Linux 3 or 4. • Fedora Core 4 through 9[1]. • Slackware 11 or 12.1. • openSuSE 10 or SuSE 10.1.	• Computer with an Intel i386 or higher processor. • 32-bit processors or Biarch 64-bit	• RAM: 32 MB. • About 20 MB hard disk space. • sudo access for the security appliance to download and install the AnyConnect client, or to update the AnyConnect client. • sudo: 1.6.6 or later required. • glibc users must have glibc 2.3.2 installed. For example, libc.so.6 or higher. • libstdc++ users must have libstdc++ version 3.3.2 (libstdc++.so.5) or higher, but below version 4. • Firefox: required 1.0 or later (with libnss3.so installed in /usr/local/lib, /usr/local/firefox/lib, or /usr/lib). • libcurl: required 7.10 or later. • openssl: required 0.9.7a or later. • java: required 1.5 or later.[2] • zlib: required 1.2.3 or later. • gtk: required 2.0.0, gdk: required 2.0.0, libpango: required 1.0. • iptables: 1.2.7a or later. • kernel: tun.o loadable module required. The tun module supplied with kernel 2.4.21 or 2.6 is required.
Mac OS X, Version 10.4 or later	Macintosh computer	50 MB hard disk space

[1] To use Fedora 9 with the AnyConnect client, you must first install Sun Microsystems JRE, preferably JRE 6, Update 5 or higher.

[2] The default Java package on Fedora is an open-source GNU version, called Iced Tea on Fedora 8. The only version that works for web installation is Sun Java. You must install Sun Java and configure your browser to use that instead of the default package.

Note The AnyConnect VPN Client is not supported with virtualization software, such as VMWare (any platform) or the Parallels Desktop for Mac.

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

Security Appliances and Software Supported

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

Table 1 shows the minimum Cisco ASA 5500 Adaptive Security Appliance software images that support the AnyConnect client.

Table 1 Software Images that Support the AnyConnect Client, Release 2.2

Image Type	Version
ASA Boot image	8.0(3).1 or later
Adaptive Security Device Manager (ASDM)	6.1(3).1 or later
Cisco AnyConnect VPN Client	Windows, Linux, and Mac OS X: 2.2
Cisco Secure Desktop	3.2(2)[1]

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

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

See the Adaptive Security Appliance VPN Compatibility Reference: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html for a complete list of compatibility requirements.

There is no support of the AnyConnect client within Secure Desktop (Vault) on the Windows Vista platform in Release 3.3 of Cisco Secure Desktop. Do not configure the AnyConnect client and Secure Desktop (Vault) if your users use the Windows Vista platform. This limitation applies only to AnyConnect client users who are using the Windows Vista platform. Users who connect using a clientless connection *can* use the Secure Desktop (Vault).

If you must configure the AnyConnect client and Cisco Secure Desktop secure desktop, but some of your users might be on the Windows Vista platform, consider using Cisco Secure Desktop, Release 3.2.1 to accomplish this. In this case, Secure Desktop (Vault) is started only on non-Vista platforms (otherwise, Cache Cleaner is invoked in its place for the clientless environment).

If you want to enforce Cisco Secure Desktop secure desktop for certain users, and you expect that AnyConnect will also be used for those users who may use Windows Vista or Windows XP, you can, through prelogin policy, configure a policy that starts Cache Cleaner or Hostscan (in place of Secure Desktop) for users on Windows Vista platforms. For example, the policy can key off the registry value:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\CurrentVersion

AnyConnect and PIX

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

AnyConnect and IOS

Several features of the Cisco AnyConnect VPN Client are supported in conjunction with various IOS routers with SSL VPN support. Please see the system requirements listed in the *Cisco IOS SSL VPN Data Sheet* for specific details about supported features for IOS devices and the IOS *SSL VPN* feature guide for configuration details. If you are a remote user, see the IOS *SSL VPN Remote User Guide* for configuration information.

Upgrading to AnyConnect Release 2.2

This section contains information about upgrading from the Cisco SSL VPN Client to Cisco AnyConnect VPN Client, Release 2.2.

Before you begin, be aware of the considerations listed in the Usage Notes, page 36, 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 45 for a list of open and resolved caveats.

New Features and Enhancements in Release 2.2

Cisco AnyConnect VPN Client, Release 2.2, offers the following new features.

Improved User Experience During Download and Installation

AnyConnect 2.2 is optimized to shorten the time required for download and installation. This effect is most noticeable on lower-speed connections.

Localization for Mac OS X Systems

Localization capability is now available on Mac OS X systems, as well as on Windows systems.

Customization and Translations Features

The AnyConnect client includes enhanced customization features and language translation features. In previous versions, you could customize client installations only on an individual PC basis. With this version, the security appliance can customize the client as it downloads and installs the client on the remote PC. You can also translate the client installer. The following sections summarize these features.

Customizing the Client or Installer

You can customize the AnyConnect VPN client to display your own corporate image to remote users. There are different approaches to customizing the AnyConnect VPN client depending on the way you deploy the client to user PCs:

- **Individual PC**—You can manually replace files of logos and icons in the folders of the installed client. To do this, you need administrator privileges on the PC.
- **IT deployment**—If you are deploying the client via a corporate software deployment agent, such as Altris, you can create a transform that customizes the client and deploys with the AnyConnect client and installer program.
- **Security Appliance deployment**—If you deploy the client using the security appliance, you can use one of three methods to customize:
  - Import rebranding components, such as the corporate logo and icons, to the security appliance which deploys them to remote PCs with the installer.
  - Import a transform that you create for more extensive rebranding. The security appliance deploys it with installer.
  - Import your own program that uses the AnyConnect API and customizes the GUI or CLI.

Translating the Client or Installer

You can display messages displayed by the AnyConnect VPN Client or the client installer program in the language preferred by the remote user. Language translation (localization) methods are also different, depending on the way you deploy the client to user PCs:

- **IT deployment**—For installer translation, you download a pre-deploy version of a language translation package from the software download page of cisco.com, and you import transforms from the package to the security appliance. You deploy the transforms with the client installer, applying the transform when the .msi is installed.

  Note If you are using IT deployment, you can only translate the installer. You cannot translate the client. Client translation is only available through ASA deployment.

- **Security Appliance deployment**—You download web-deploy versions of language translation packages from the software download page for the client and the installer. For client translation, you you import the applicable translation tables to the security appliance. For installer translation, you import translation transforms. Both are downloaded by the security appliance to the remote PC with the client.

Start Before Logon for Windows Vista

The AnyConnect client, Release 2.2 and higher, includes support for Start Before Logon for Windows Vista systems, in addition to other Windows operating systems. This feature allows the establishment of a VPN tunnel before the user logs on to the Windows system. This is useful for a number of deployment scenarios in which a user might be outside the physical corporate network and cannot access resources until the user's PC has joined the corporate network. See the description of Start Before Logon in the Cisco AnyConnect VPN Client Administrator Guide for more information about configuring and using the Start Before Logon feature on all Windows systems.

Systray Balloon Shows Reconnect Status

The system tray on Windows systems changes while a client is either disconnected and waiting to resume connectivity or while reconnecting. The systray now shows a balloon when the AnyConnect client is reconnecting after losing connectivity. If the reconnect does not complete within 30 seconds, a balloon informs the user that the client is reconnecting. If this balloon appears, then another balloon pops up once the reconnect succeeds to inform the user of that.

Application Programming Interface Available for AnyConnect Client

The AnyConnect client, Release 2.2, includes an Application Programming Interface (API), for customers who want to write their own client programs.

The API package contains documentation, source files, and library files to support a C++ interface for the Cisco AnyConnect VPN Client.There are libraries and example programs that can be used for building on Windows, Linux and MAC (10.4 or higher) platforms. The Makefiles (or project files) for the Windows platform are also included. For other platforms, there is a platform specific script showing how to compile the example code. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.

You can download the AnyConnect API at http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect

The current download bundle is: AnyConnect_API_2.2.0133.zip.

See the AnyConnect administrator guide (Anyconnect Client Features section) for some discussion on supported platforms:

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect22/administration/guide/22admin1.html

For support issues regarding the AnyConnect API, send e-mail to the following address: anyconnect-api-support@cisco.com

AnyConnect Client Support for Smartcards

Starting with the AnyConnect client Release 2.1, the Cisco AnyConnect VPN Client supports Smartcards on Windows operating systems, via the Windows Crypto API (CAPI) interface, and on Mac OS X, version 10.4 or higher. On the Mac, the Smartcard must be able to work with Keychain. While Cisco can validate compatibility with only a subset of the available cards, readers, and drivers on the market, testing has shown to be compatible with Smartcards that meet these requirements. If a particular combination is not functioning with AnyConnect but meets the above specifications, we recommend contacting your Smartcard manufacturer to determine whether there are known defects in the product implementation.

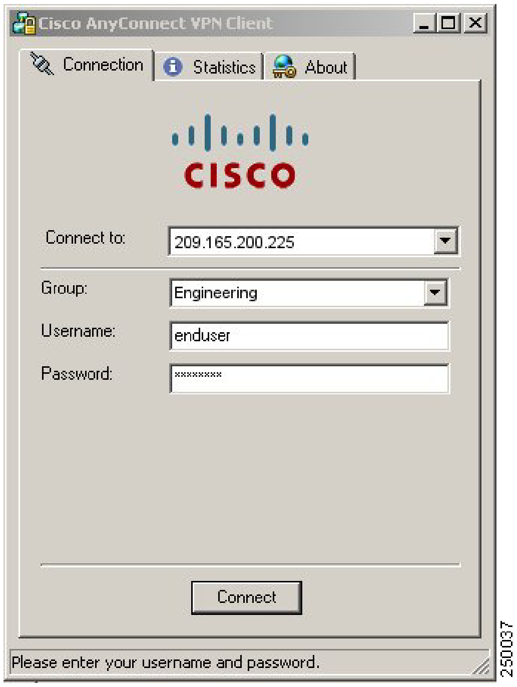
Support for RSA SecurID Software Token Client Software

Cisco AnyConnect VPN Client, Release 2.1 and higher, supports integration of SDI token software on Windows 2000 and Windows XP systems. AnyConnect does not support token selection from multiple tokens imported into the RSA Secure ID Software Token client software, the default token is always used, and AnyConnect does not support SofToken II, by Secure Computing Corporation. For a fuller description, see the *Cisco AnyConnect VPN Client Administrator Guide*.

End 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



Connect to: 209.165.200.225

Group: Engineering

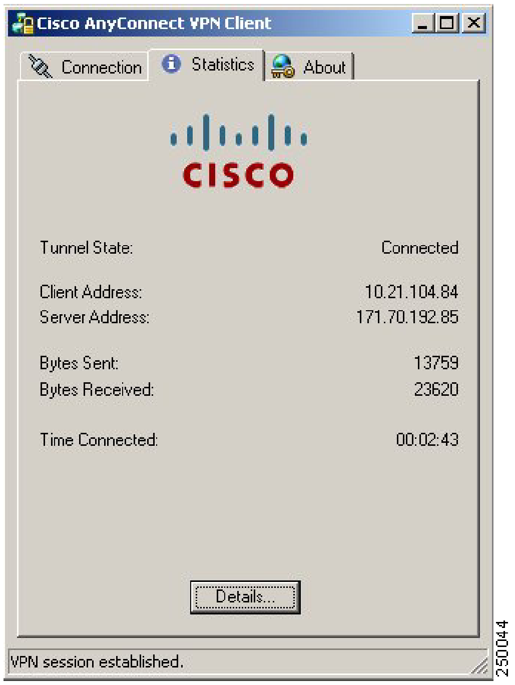
Username: enduser

Password: ********

Please enter your username and password.

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

Figure 2 Cisco AnyConnect VPN Client User Interface, Statistics Tab



Tunnel State: Connected

Client Address: 10.21.104.84
Server Address: 171.70.192.85

Bytes Sent: 13759
Bytes Received: 23620

Time Connected: 00:02:43

VPN session established.

AnyConnect Client Disconnect Behavior

If you click Disconnect, the AnyConnect client, starting with Release 2.2, terminates the connection, as shown in the status bar at the bottom of the dialog box, and the AnyConnect GUI displays a login dialog box with a “Connect to” combo box and a Select button. To reconnect, the remote user must select a new host server to connect to or click Select. At that point, the appropriate authentication prompts are displayed.

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.

WebLaunch Mode

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. Local system admin privileges are required if the client is not already installed. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>. Weblaunch mode can also be used even when the client is already installed.

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

After the user enters 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 loads the client that matches the operating system of the remote computer. After loading, 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.

Standalone Mode

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*. For more detailed information about configuring the AnyConnect client and other SSL VPN connections on the security appliance, see "Configuring SSL VPN Connections" in *Cisco Security Appliance Command Line Configuration Guide*. For detailed descriptions of the commands referred to in this administrator's guide, see the *Cisco ASA 5500 Command Reference Guide* for version 8.0 or later.

The security appliance loads the client based on the group policy or username attributes of the user establishing the connection. You can configure the security appliance to automatically load 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 either to load the client after a timeout period or to 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. We recommend keeping the client resident on the system, as doing so can speed up subsequent connection attempts.

Note When using Start Before Logon, the VPN Gina (VPN Graphical Identification and Authentication) 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.

This section describes installation-specific issues and procedures for AnyConnect client Release 2.2, and contains the following sections:

- Where to Find the AnyConnect Client Files for Installation, page 13
- Before You Install the AnyConnect Client, page 13
- Installing the AnyConnect Client on a System Running Windows, page 16
- Installing the AnyConnect Client on a System Running Linux, page 17
- Installing the AnyConnect Client on a System Running MAC OS X, page 18
- Loading the AnyConnect Client and Configuring the Security Appliance with ASDM, page 19
- Loading the AnyConnect Client and Configuring the Security Appliance with CLI, page 27

Where to Find the AnyConnect Client Files for Installation

All of the AnyConnect clients are located in the same place:
http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect

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 13
- AnyConnect Client and New Windows 2000 Installations, page 14
- Adding a Security Appliance to the List of Trusted Sites (IE), page 14
- Adding a Security Certificate in Response to Browser Alert Windows, page 15

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. For information about adding a security appliance to the list of trusted sites, see the *Cisco AnyConnect VPN Client Administrator Guide*. For information about 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*.

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.

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.

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 Start Before Logon Components (Windows Only)

The Start Before Logon components must be installed *after* the core client has been installed. Additionally, the AnyConnect 2.2 Start Before Logon components require that version 2.2, or later, of the core AnyConnect client software be installed. If you are pre-deploying the AnyConnect client and the Start Before Logon components using the MSI files (for example, you are at a big company that has its own software deployment—Altiris or Active Directory or SMS.) then you must get the order right. The order of the installation is handled automatically when the administrator loads AnyConnect if it is web deployed and/or web updated.

Both the AnyConnect client and the Start Before Login components must be installed same way, either both manually or both via weblaunch. Therefore:

- If you pre-deploy AnyConnect, you must also pre-deploy the Start Before Logon components.
- If you web-update AnyConnect, you must web-update the Start Before Logon components.
- If you web-deploy AnyConnect, you must web-deploy the Start Before Logon components.
- You cannot pre-deploy AnyConnect, and then web-deploy the Start Before Logon components.

If you manually uninstall either the pre-Vista Start Before Logon component GINA or the Windows Vista Start Before Logon component PLAP, you must manually reinstall it.

You can, for example, pre-deploy both of them... put a new version of both on the head end and web-update them both. The two are joined together in whatever action you perform.

For example, a customer sends out laptops with the software pre-installed. Six months later, Cisco ships a new version of the software and the network administrators want all their users to get the latest version. To do this, the network administrators can put the new software on the security appliance, and all users get the web update.

They could *not* pre-image with just core AnyConnect software and then decide to update via the security appliance both the client and the Start Before Logon software components, since they never pre-installed the Start Before Logon software to begin with.

Differences Between Windows-Vista and Pre-Vista Start Before Logon

The procedures for enabling SBL differ slightly on Windows Vista systems. Pre-Vista systems use a component called VPNGINA (which stands for virtual private network graphical identification and authentication) to implement SBL. Vista systems use a component called PLAP to implement SBL.

In the AnyConnect client, the Windows Vista Start Before Logon feature is known as the Pre-Login Access Provider (PLAP), which is a connectable credential provider. This feature lets network administrators perform specific tasks, such as collecting credentials or connecting to network resources, prior to login. PLAP provides start Before Logon functions on Windows Vista. PLAP supports 32-bit and 64-bit versions of the operating system with vpnplap.dll and vpnplap64.dll, respectively. The PLAP function supports Windows Vista x86 and x64 versions.

Note In this section, VPNGINA refers to the Start Before Logon feature for pre-Vista platforms, and PLAP refers to the Start Before Logon feature for Windows Vista systems.

In pre-Vista systems, Start Before Logon uses a component known as the VPN Graphical Identification and Authentication Dynamic Link Library (vpngina.dll) to provide Start Before Logon capabilities. The Windows PLAP component, which is part of Windows Vista, replaces the Windows GINA component.

A GINA is activated when a user presses the Ctrl+Alt+Del key combination. With PLAP, the Ctrl+Alt+Del key combination opens a window where the user can choose either to log in to the system or to activate any Network Connections (PLAP components) using the Network Connect button in the lower-right corner of the window.

For a complete description of enabling, configuring, and using the Start Before Logon feature (VPNGINA or PLAP) on a Windows platform, see *Cisco AnyConnect VPN Client Administrator Guide, Release 2.2*, Chapter 4.

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-2.2.xxxx.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 OS X

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 2 shows the CLI commands.

Table 2 AnyConnect Client CLI Commands

Command	Action
connect *IP address or alias*	Client establishes a connection to a specific security appliance.
disconnect	Client closes a previously established connection.
exit	Exits the CLI interactive mode.
help or ?	Gets usage information for CLI commands.
hosts	Lists all saved VPN server hosts.
quit	Exits the CLI interactive mode.
state or **status**	Displays current state of the VPN subsystem.
stats	Displays statistics about an established connection.
version	Displays the version of the currently installed Cisco AnyConnect VPN client.

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 loads the clients to the remote PC. Perform the following steps to install the client:

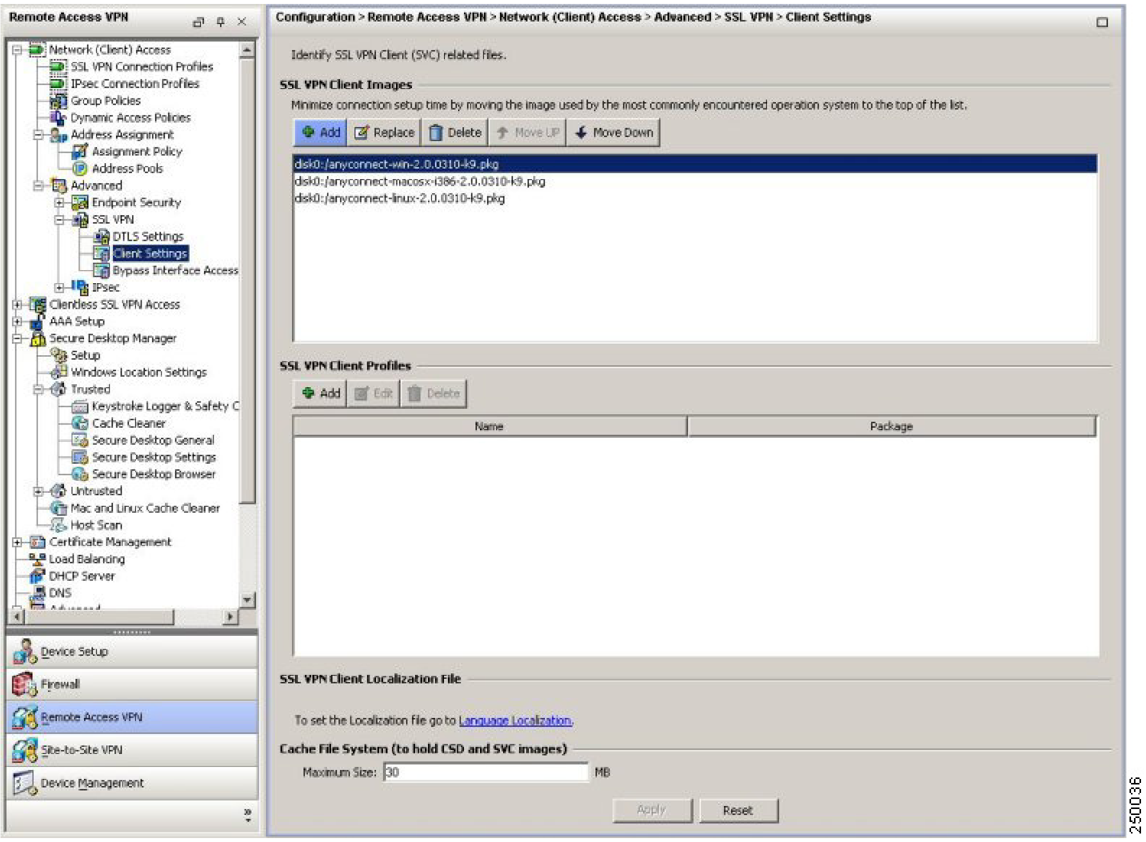
Step 1 Load the AnyConnect client images to the security appliance. On the ASDM toolbar, click **Configuration**. The navigation pane displays features to configure.

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



Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings

Identify SSL VPN Client (SVC) related files.

SSL VPN Client Images

Minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

disk0:/anyconnect-win-2.0.0310-k9.pkg
disk0:/anyconnect-macosx-i386-2.0.0310-k9.pkg
disk0:/anyconnect-linux-2.0.0310-k9.pkg

SSL VPN Client Profiles

SSL VPN Client Localization File

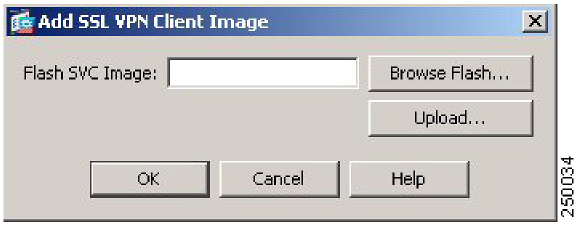
To set the Localization file go to Language Localization.

Cache File System (to hold CSD and SVC images)

Maximum Size: 30 MB

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).

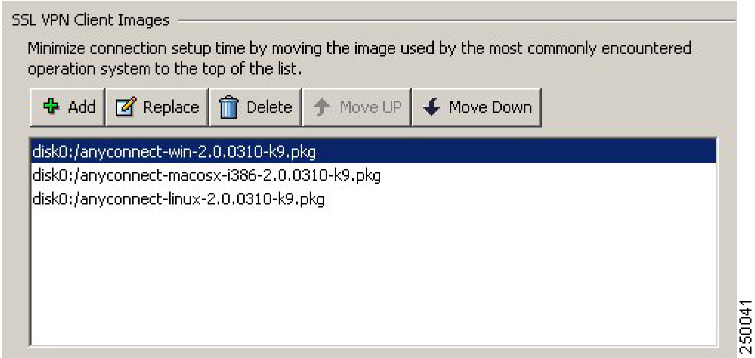
Figure 4 Add SSL VPN Client Image Dialog



Flash SVC Image:

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



SSL VPN Client Images

Minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

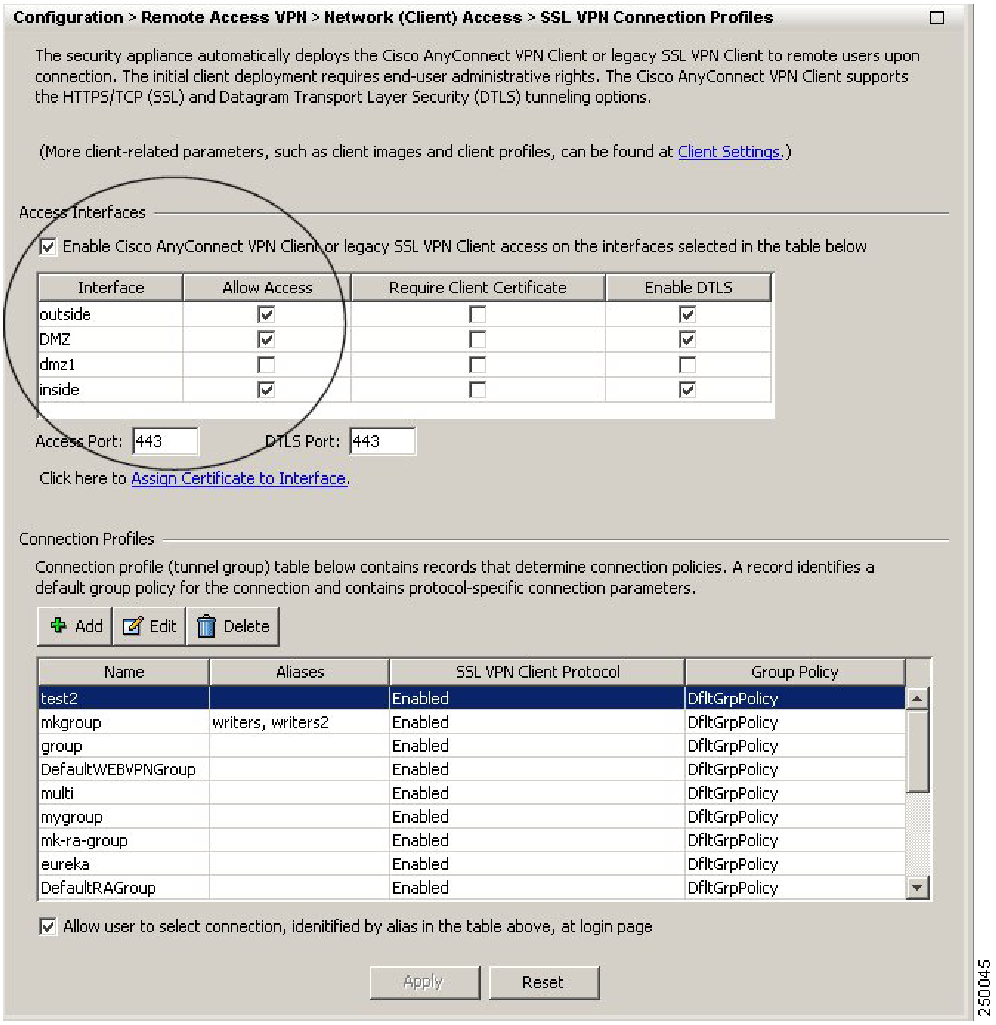
disk0:/anyconnect-win-2.0.0310-k9.pkg
disk0:/anyconnect-macosx-i386-2.0.0310-k9.pkg
disk0:/anyconnect-linux-2.0.0310-k9.pkg

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 loads them to the remote computer. It loads 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



Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at Client Settings.)

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	☑	□	☑
DMZ	☑	□	☑
dmz1	□	□	□
inside	☑	□	☑

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

Connection Profiles

Connection profile (tunnel group) table below contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters.

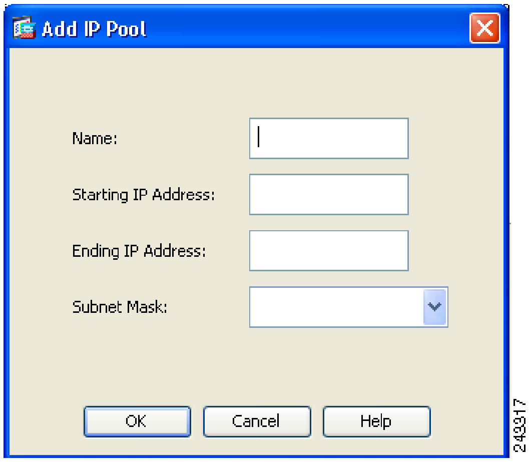
Name	Aliases	SSL VPN Client Protocol	Group Policy
test2		Enabled	DfltGrpPolicy
mkgroup	writers, writers2	Enabled	DfltGrpPolicy
group		Enabled	DfltGrpPolicy
DefaultWEBVPNGroup		Enabled	DfltGrpPolicy
multi		Enabled	DfltGrpPolicy
mygroup		Enabled	DfltGrpPolicy
mk-ra-group		Enabled	DfltGrpPolicy
eureka		Enabled	DfltGrpPolicy
DefaultRAGroup		Enabled	DfltGrpPolicy

☑ Allow user to select connection, idenitified by alias in the table above, at login page

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).

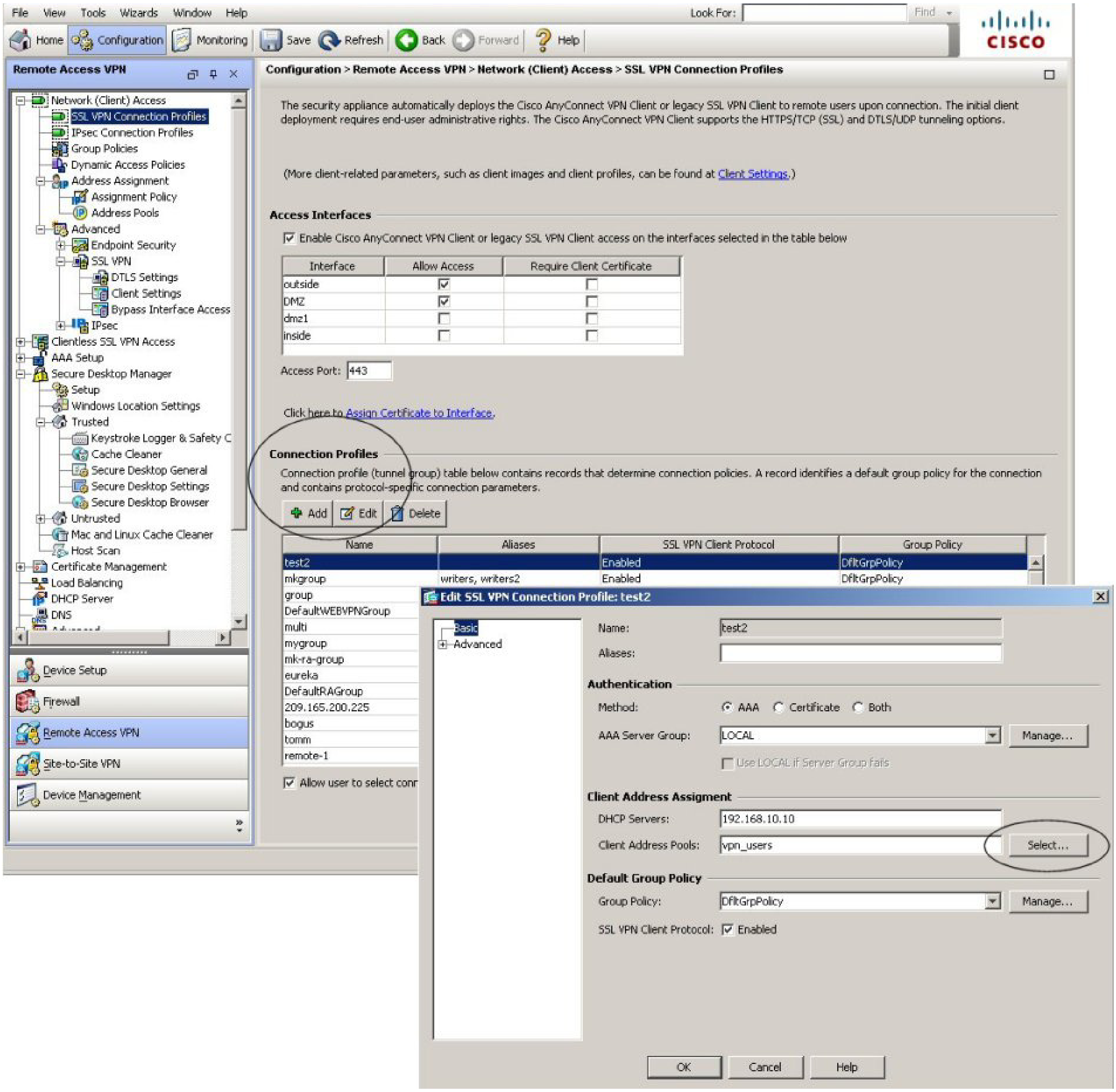
Figure 7 Add IP Pool Dialog



Step 7 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 8 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



The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and DTLS/UDP tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at Client Settings.)

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

Interface	Allow Access	Require Client Certificate
outside	☑	□
DMZ	☑	□
dmz1	□	□
inside	□	□

Access Port: 443

Click here to Assign Certificate to Interface.

Connection Profiles

Connection profile (tunnel group) table below contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters.

Name	Aliases	SSL VPN Client Protocol	Group Policy
test2		Enabled	DfltGrpPolicy
mkgroup	writers, writers2	Enabled	DfltGrpPolicy
group			
DefaultWEBVPNGroup			
multi			
mygroup			
mk-ra-group			
eureka			
DefaultRAGroup			
209.165.200.225			
bogus			
tomm			
remote-1			

☑ Allow user to select conn

Name: test2

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assigment

DHCP Servers: 192.168.10.10

Client Address Pools: vpn_users

Default Group Policy

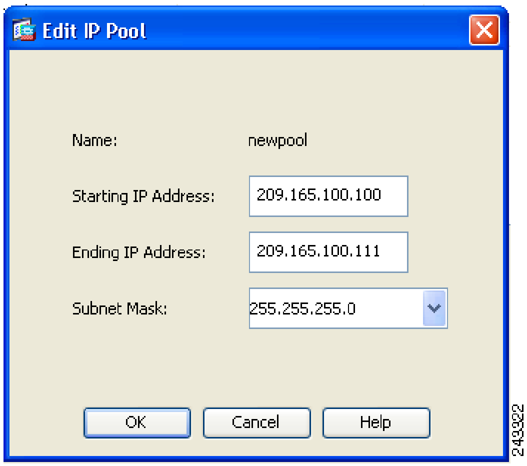
Group Policy: DfltGrpPolicy

SSL VPN Client Protocol: ☑ Enabled

Step 9 Highlight a connection in the table, and click **Edit.** The Edit SSL VPN Connection dialog appears.

Step 10 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**.

Figure 9 Select Address Pool Dialog



Edit IP Pool

Name: newpool

Starting IP Address: 209.165.100.100

Ending IP Address: 209.165.100.111

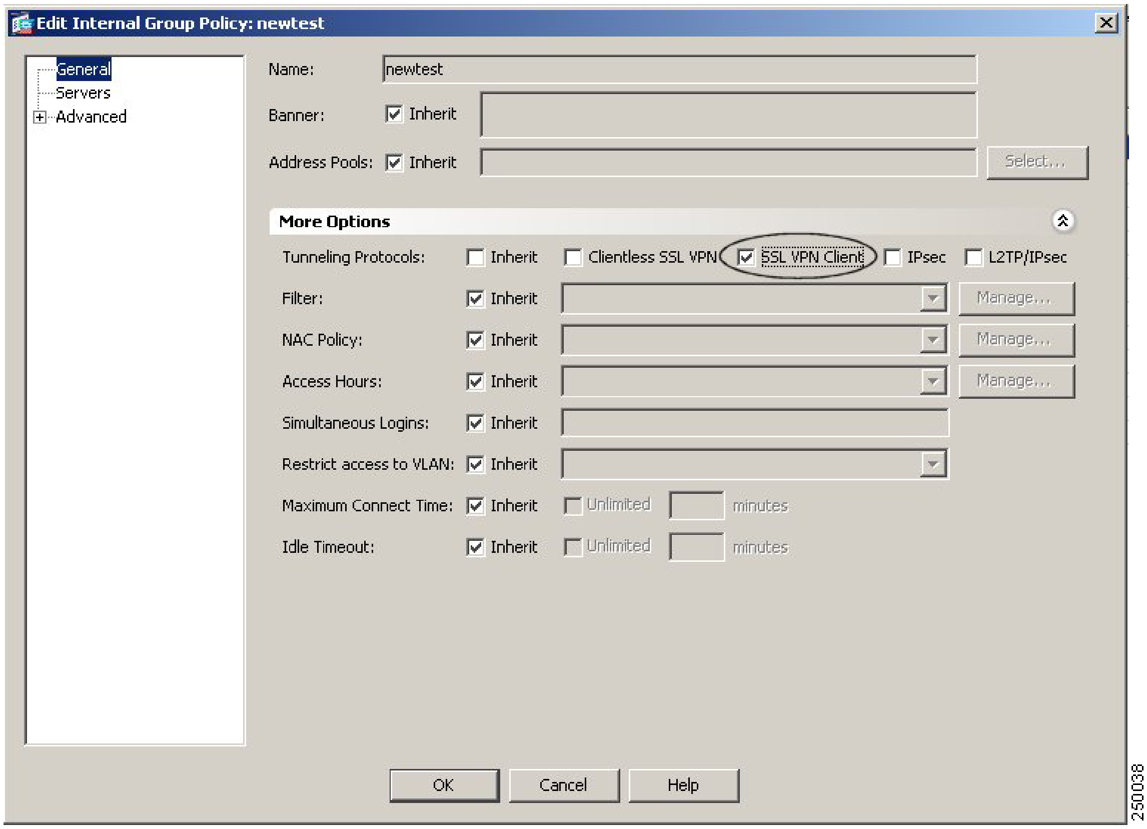
Subnet Mask: 255.255.255.0

Step 11 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



Edit Internal Group Policy: newtest

Name: newtest

Banner: ☑ Inherit

Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec □ L2TP/IPsec

Filter: ☑ Inherit

NAC Policy: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

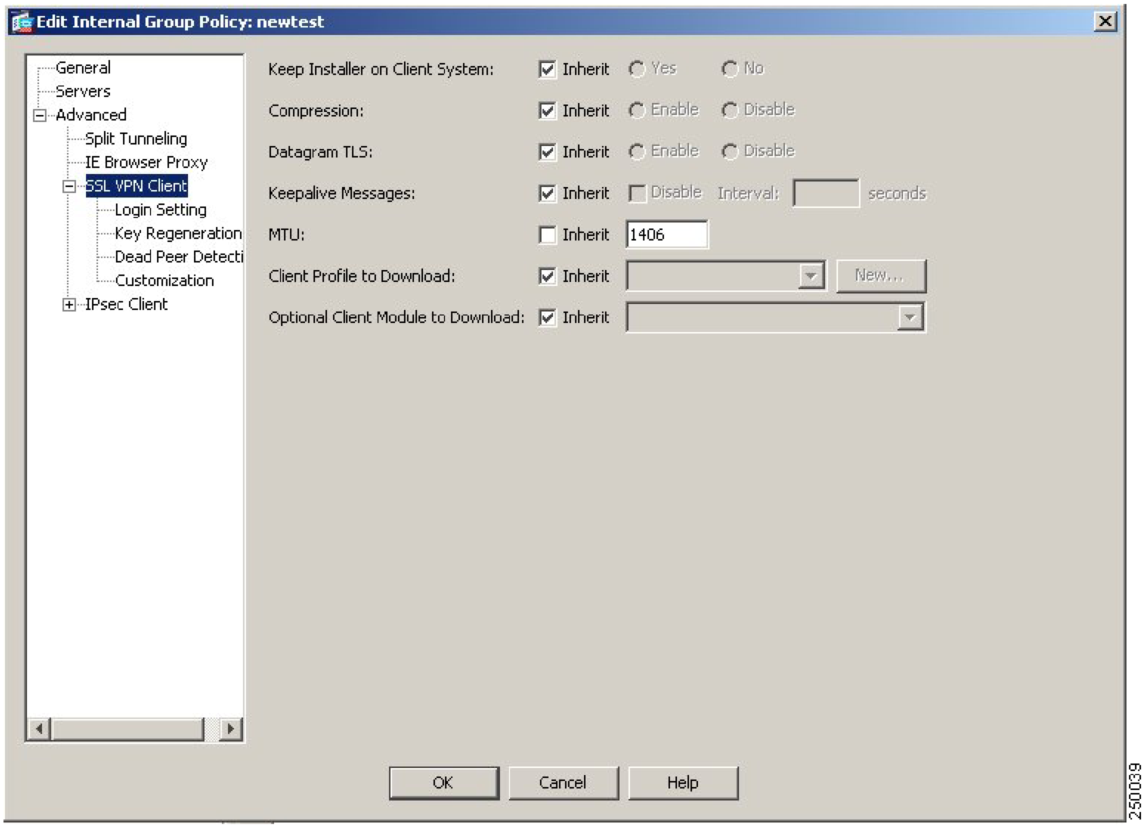
Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

Check the **SSL VPN Client** check box to include SSL VPN as a tunneling protocol.

Step 12 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



Edit Internal Group Policy: newtest

Keep Installer on Client System: ☑ Inherit ○ Yes ○ No

Compression: ☑ Inherit ○ Enable ○ Disable

Datagram TLS: ☑ Inherit ○ Enable ○ Disable

Keepalive Messages: ☑ Inherit □ Disable Interval: seconds

MTU: □ Inherit 1406

Client Profile to Download: ☑ Inherit

Optional Client Module to Download: ☑ Inherit

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 AnyConnect client 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 27
- Enabling SSL VPN Connections, page 28
- Disabling Permanent Client Installation, page 31
- Prompting Remote Users, page 31
- Enabling AnyConnect Client Profile Downloads, page 32
- Enabling Rekey, page 33
- Enabling Start Before Logon for the AnyConnect Client, page 34

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 loads 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-2.2.1.xxx-k9.pkg
Destination filename []? anyconnect-win-2.2.1.xxx-k9.pkg
Accessing
tftp://209.165.200.226/anyconnect-win-2.2.1.xxx-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 loads 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 Cisco Secure Desktop 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 06/22/2008 21:51:30.43

2. disk0:/linux.pkg 2
  CISCO STC linux 1.0.0
  1,0,0,164
  Thu 06/15/2008 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 loads the client.

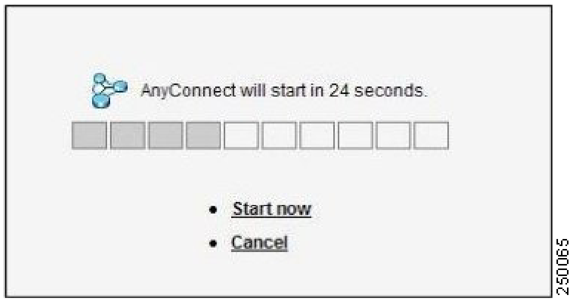
svc ask enable default webvpn immediately goes to the portal page.

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



AnyConnect will start in 24 seconds.

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.tmpl) 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 user'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\<your_username>\Application Data\Cisco\Cisco AnyConnect VPN Client.

The AnyConnect client stores data that the user previously entered, such as 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. This is a way to test a potential client profile.

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 loaded 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*:

```
asa1(config-webvpn)# svc profiles sales disk0:/sales_hosts.xml
asa1(config-webvpn)# svc profiles engineering disk0:/engineering_hosts.xml
```

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

```
asa1(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Jun 22 2008 engineering.xml
0      ----  774         11:54:29 Jun 22 2008 sales.xml

2428928 bytes total (18219008 bytes free)
asa1(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*:

```
asa1(config-group-webvpn)# svc profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
asa1(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.

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
hostame(config-group-webvpn)# svc modules value vpngina
```

In addition, the administrator must ensure that the AnyConnect <profile.xml> file (where <profile> is whatever the users has named the profile) 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.

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

Note On Systems prior to Windows Vista, Start Before Logon works only for PCs that are part of a domain and not part of a workgroup or working standalone.

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*.

Uninstalling the Cisco AnyConnect VPN Client

To manually uninstall the AnyConnect client from a Windows system, use the standard “Add or Remove Programs” Control Panel available from the Start menu.

The procedure for manually uninstalling the AnyConnect client from a Linux or Mac OS X system is the same for both systems. As root, run the following shell script:

```
/opt/cisco/vpn/bin/vpn_uninstall.sh
```

Typically, you would do this via sudo, as follows:

```
$ sudo /opt/cisco/vpn/bin/vpn_uninstall.sh
```

If you do not use sudo, use a root shell:

```
# /opt/cisco/vpn/bin/vpn_uninstall.sh
```

Usage Notes

This section lists known interoperability considerations and other issues to consider before installing and using the Cisco AnyConnect VPN Client, Release 2.2.

Usage Notes for AnyConnect Release 2.2.0136

The following usage notes apply specifically to Release 2.2.0136.

QoS Policing Does Not Apply to AnyConnect Connections

Quality of Service policing does not apply to AnyConnect client connections. Attempting to do this results in an error message from the security appliance.

Network Connections Control Panel Might Show Generic Adapter Name

The name of the adapter that AnyConnect adds to Windows (as shown in the Network Connections control panel) might be marked with the generic name “Local Area Connection *n*”, where *n* is a number (for example, Local Area Connection 6). The Windows operating system sets this generic name when the adapter is installed. The AnyConnect client code attempts to update this name to “Cisco AnyConnect VPN Client Connection” each time a VPN session starts. If an upgrade occurs during Start Before Login (SBL), then the attempt to change the name of the AnyConnect adapter might fail. In this case, the generic name appears in the operating system’s Network Connections control panel. The next time a VPN is established (after the SBL-initiated session disconnects), the name should be properly updated. This is a cosmetic issue (due to a limitation in the operating system) that affects only the name displayed in the Windows Network Connections control panel. An upgrade during SBL is the only known cause for this issue.

Usage Notes for AnyConnect Release 2.2.nnnn

The following usage notes apply to all AnyConnect Release 2.2 versions, including Release 2.2.0133 and earlier versions.

AnyConnect and Citrix Incompatibility

There exists a conflict between AnyConnect and Citrix Advanced Gateway client 2.2.1.

When disconnecting AnyConnect, users can receive this Microsoft Windows error: "VPN Agent Service has encountered a problem and needs to close. We are sorry for the inconvenience." After clicking close on the Microsoft Windows error, users receive this next message from AnyConnect: "Unable to Proceed. Cannot contact the VPN service." Finally, at the bottom of the AnyConnect client window, users receive the message: "The VPN Service has failed. Please restart the application" This indicates the AnyConnect Agent service has crashed.

The Citrix client installs a Layered Service Provider DLL (CtxLsp.dll) that it loads into every process using Windows Sockets (WinSock). As such, this DLL is loaded into the AnyConnect Agent Service. The crash occurs as a result of this DLL being part of the Agent process. The crashes always occur during freeing of memory because of memory heap corruptions caused by this DLL. These same operations work correctly when the DLL is not part of the process. The crashes have been seen to occur in the downloader application as well, and even in the FileZilla FTP Server.

While the crashes occur very frequently, they do not always occur. Also, the crashes occur in different places in the process, but they are always the result of a memory heap corruption. The bug is in the Citrix DLL. Others have reported this issue to Citrix:
http://support.citrix.com/forums/thread.jspa?forumID=60&threadID=80923&tstart=15

The current workaround for this problem is to disable the Citrix client.

Windows Vista Might Become Unresponsive During Sleep/Resume Cycles or Other High-load Conditions (KB-952876)

If you use sleep and resume on Vista, you might find that the tunnel cannot be established due to the AnyConnect driver not being enabled. A reboot is typically required to recover from this condition.

The problem is caused by an issue in the Vista Kernel component as described in KB-952876 (http://support.microsoft.com/kb/952876). When this issue occurs, another core Vista component, TCPIPREG.sys, fails to function. The Cisco AnyConnect VPN Client relies on this service to set the IP address of the Virtual Adapter. If you see an error stating that the Virtual Adapter could not be set up, you might have encountered this issue. We recommend that you apply the patch if you are experiencing issues on Vista where the AnyConnect adapter fails to enable. After applying the patch, you might still see an occasional failure due to a timing issue in the TCPIPREG.sys service. This is rare and should be recoverable by simply trying the tunnel a second time. Cisco is working with Microsoft to correct this remaining issue.

AnyConnect Client over Proxies

AnyConnect supports connections to the security appliance via a proxy server that uses Basic and NTLM authentication. Socks proxies are not supported. DTLS (using UDP) is not supported if the proxy server runs only TCP.

Additionally, on Windows only, you can also use authenticating proxies that use Basic or NTLM for authorization. If you have Internet Explorer configured with a proxy, you must activate the “Use HTTP 1.1 through proxy connections” setting in the advanced Internet Explorer settings 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.”

WINS and DNS

The AnyConnect client supports group-configured primary and secondary Windows Internet Naming Services (WINS) or Domain Naming Services (DNS). Most of the parameters (DNS, WINS, MSIE Proxy setting, split-tunnel lists, and so on) are enforced on a VPN remote access session. A few of the key parameters, specifically Authentication, Authorization, and Accounting configuration, are enforced from the tunnel-group.

SSL VPN Clients Do Not Support DNS Fallback for Split Tunneling

The AnyConnect 2.2 client does not support DNS Fallback for Split Tunneling (also called Split DNS).

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.

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.

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.

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.

msvcp60.dll Must Be Available for Installation of the AnyConnect Client

To use the Cisco AnyConnect VPN Client, you must have the file msvcp60.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.

Secure VPN Via Windows Remote Desktop Is Supported

The AnyConnect VPN Client, Release 2.2, supports VPN connection establishment via a Windows Remote Desktop session. If you connect to the PC via Remote Desktop, your VPN connection will 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/CiscnyConnect 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.

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.

To work around this issue, set the VPN connection MSIE configuration settings on the secure gateway to “no proxy” rather than “do not change proxy settings.” This will cause the client to remove the “public side” proxy settings from MSIE, while the VPN connection is established. Then, browser and other Windows Internet traffic goes over the tunnel.

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.

Setting the AnyConnect Pre-Login Banner

The pre-login banner is the optional banner message that appears in line with the end-user AnyConnect client interface. 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.

Smartcards Supported

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, as well as for Mac OS X (10.4 and higher). In Release 2.2, there is no Smartcard support for Linux.

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.

RADIUS Interim Accounting Update Feature

In conjunction with ASA Release 8.0.3.1 and higher, the AnyConnect client now supports interim accounting for a VPN connection running simultaneous SSL VPN Clientless and AnyConnect sessions.

This is especially important for SSO integration with the NAC appliance, where NAC requires the Accounting Start request to contain the Frame-IP-Address.

Previously, if an AnyConnect session was launched from a browser and not the standalone AnyConnect GUI, the Clientless session (with no concept of Frame-IP) would send the Accounting Start request without it, and NAC-SSO would fail as a result.

To enable this feature, enable the new CLI command **interim-accounting-update** under aaa-server on the security appliance.

Note ASDM has not yet made the change to implement this new command (CSCsm10513) as of the ASDM 6.0.3.51 build.

AnyConnect Split-tunneling Works on Windows Vista

In the AnyConnect client, Release 2.1 and higher, split-tunneling works correctly with Windows XP, Windows 2000, *and* Windows Vista.

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.

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 (UDP) 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 third-party network firewall is located between the client PC and the security appliance, the firewall 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 the firewall stops DTLS traffic, 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 that TLS fallback occurs in a timely manner.

Step 2 Enable the client DTLS keepalive and configure it to be at least 10 seconds less than the firewall idle timer default interval.

For example, set this value to 30 seconds if using the default configuration (40 seconds) of the third-party firewall.

If there has been an idle period of DTLS traffic, the firewall might stop sending data to the client or security appliance. The client attempts to re-establish DTLS each time this occurs up to the limit of the retry counter. The tunnel falls back to TLS during this period if the DTLS DPD is set to a sufficient value. For example, a typical setting for DPD from both the client and security appliance might be 120 seconds. If the DTLS session is blocked by the firewall, a user experiences an outage and then eventually the session falls back to TLS. This outage is directly proportional to the value set for DTLS DPD.

DTLS is a UDP based protocol and is connectionless. There is a flow associated with the DTLS session that is based on the source and destination addresses and ports. Firewalls build a session table based on these values and track this as a unique session. By default, DTLS is enabled when SSL VPN access is enabled on an interface.

No AnyConnect Confirmation Dialog for Cisco Secure Desktop Users

When contacting a central-site security appliance that enforces a Cisco Secure Desktop policy, the AnyConnect client no longer lets the user terminate the connection attempt prior to starting the download and execution of Cisco Secure Desktop. In AnyConnect Release 2.0, the dialog appears for each connection attempt. The AnyConnect client, Release 2.1 and higher, however, removes this dialog for Cisco Secure Desktop users, and Cisco Secure Desktop processing continues without further input from the user.

AnyConnect Client uses OpenSSL Libraries 0.9.8f

The AnyConnect client uses the OpenSSL cryptography libraries to perform encryption and security protocol encapsulation. A new version of OpenSSL has been released that fixes several issues in older versions of OpenSSL. The OpenSSL libraries used by the AnyConnect client have been updated by merging in 0.9.8f changes with custom Cisco changes. For more information see the following URLs:

- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4995
- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5135

Optionally Disable Tearing Down Tunnel Upon Smartcard Removal

A network administrator can optionally disable tearing down a tunnel when the remote user removes the Smartcard. Some companies impose a requirement that a user must remove his/her Smartcard when the laptop is unattended. If the remote user in such a situation is downloading an application or replicating data to the central site and needs to step away from the laptop, the transfer fails and must be restarted because the tunnel has been dropped.

Upgrading Standalone AnyConnect Client for Windows Vista Shows Activity Indication

When Windows Vista users upgrade via standalone AnyConnect client, the client briefly displays a message “Exiting. Update in progress.” and then the client exits. There is no AnyConnect or Installer windows or dialogs visible on the user's desktop for the duration of the upgrade. When the upgrade completes, the AnyConnect icon appears in the system tray.

When Windows Vista users upgrade via the browser launch of AnyConnect, the AnyConnect Downloader window is visible for the duration of the upgrade, but the Installer window is not visible. When the upgrade completes, the Downloader exits and the AnyConnect icon appears in the system tray.

AnyConnect SBL Does Not Support Dialer and Third-Party Application Launchers

Due to the security implications, the dialer and third-party application launchers are not supported in AnyConnect Start Before Login.

Start Before Logon and PLAP Require a Network Connection

Start Before Logon and PLAP require a network connection to be present at the time it is invoked. In some cases, this might not be possible, because a wireless connection might depend on credentials of the user to connect to the wireless infrastructure. Since SBL mode precedes the credential phase of a login, a connection would not be available in this scenario. In this case, for SBL/PLAP to work, the wireless connection must be configured to cache the credentials across login, or another wireless authentication must be configured.

Windows Machine Cannot Be Named localhost

Microsoft allows a user to configure the machine name as “localhost” without any warnings. When a machine has the name of localhost, connections made with the SSL VPN Client or IPSec VPN Client fail.

AnyConnect Client connections fail without logs clearly outlining the issue. The AnyConnect message is “Unable to establish VPN.” IPSec VPN Client connections fail with Reason 442. To work around this issue, rename the PC to something other than localhost.

Synchronizing a Mobile Device to a PC While a Tunnel Is Active

If using ActiveSync or Windows Mobile Device Center to synchronize a mobile device to your PC while the tunnel is active, you must either enable Local LAN in the security appliance configuration or configure your device to use a serial port instead of Remote Network Driver Interface Specification (RNDIS).

When RNDIS is enabled, mobile devices are assigned a link-local address when they are connected to the PC. When Tunnel All is configured on the security appliance, all network traffic, including link-local traffic, is sent to the tunnel interface.

If Tunnel All is a requirement for your deployment, you can try to configure the mobile device to synchronize using a serial port interface, you can synchronize your device while Tunnel All is configured. On the Mobile Device, under Start > Settings > Connections > USB-to-PC, deselect the “Enable advanced network functionality” check box to disable RNDIS.

Obtaining a DHCP Ethernet IP If Connected via Wireless-only First

When roaming between different network interfaces with the Cisco AnyConnect VPN Client, you might be unable to obtain an IP address via DHCP on a new interface, causing an inability to move to the new network without first tearing down the VPN session.

To work around this issue, ensure that Split Tunneling or Local LAN access is enabled. With one of these features enabled, the new local network interface can obtain a DHCP assigned IP address and the user can successfully roam.

AnyConnect Support Policy

We support all AnyConnect software versions available on the Cisco AnyConnect VPN Software Download site; however, we provide fixes and enhancements only in maintenance or feature releases based on the most recently released version.

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The open caveats in Release 2.2 appear first in this list. Only caveats with Severity 2 and 3 are listed.

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.

Open Caveats in Cisco AnyConnect VPN Client, Release 2.2

Table 3 lists the caveats that are unresolved in the Cisco AnyConnect VPN Client, Release 2.2.140.

Table 3 Open Caveats in Cisco AnyConnect VPN Client, Release 2.2

ID	Headline
CSCsh51779	Using a client-side proxy and FULL tunneling, the proxy should be reset.
CSCsh69786	IPv6 link local addresses are not tunneled through AnyConnect Client.
CSCsh81003	XP: After failed conn, client reports “Internal Error” and needs restart.
CSCsi00491	Standalone can connect to wrong ASA from within SecureDesktop.
CSCsi53608	AnyConnect CSCOTUN0 interface does not install under SuSE Linux.
CSCsi69205	Smart card cant be used with MAC anyconnect client.
CSCsk05393	Avoid Multiple Auth requests for every AnyConnect--TPM.
CSCsk74884	Clicking entry in profile drop-down fails on subsequent connections.
CSCsl01485	Client does nothing when <enter> pressed in password input field.
CSCsm26776	Linux/mac downloader does not check connection status.
CSCsm44621	AnyConnect: UI/API crashed in 'connect' method.
CSCsm48367	Cached Downloader is not used when in standalone for both 2.0 and 2.1.
CSCsm60339	Sleep/Resume Cycles on Vista non-responsive tcpipreg.sys - VA failure.
CSCsm95630	Default route missing after disconnect on MAC Power PC.
CSCsm98903	AnyConnect 2.x fails via HTTP Proxy if no DNS lookup configured on user PC.
CSCso31229	AnyConnect standalone fails to connect to Group url on first attempt.
CSCsq49102	Anyconnect incompatibility with Citrix advanced gateway client 2.2.1

Resolved Caveats

AnyConnect VPN Client, Release 2.2 resolves the following caveats. The following tables list which caveats were resolved in each released build

Caveats Resolved in AnyConnect Release 2.2.140

Table 4 lists the caveats resolved in the Cisco AnyConnect VPN Client, Release 2.2.140.

Table 4 Caveats Resolved in Cisco AnyConnect VPN Client, Release 2.2.140

ID	Headline
CSCsk25563	MAC OS X AnyConnect client fails to connect to Load Balancing IP.
CSCso42825	RDP into PC using the same logon that is already logged on fails.
CSCso79661	AnyConnect BSOD (vpnva.sys) after disconnecting session.
CSCsr46257	Need to analyze password lifetime/exposure in UI components.
CSCsr65273	Anyconnect - R6025 -pure virtual function call error when quit.

Caveats Resolved in AnyConnect Release 2.2.136

Table 5 lists the caveats resolved in the Cisco AnyConnect VPN Client, Release 2.2.136.

Table 5 Caveats Resolved in Cisco AnyConnect VPN Client, Release 2.2.136

ID	Headline
CSCsq50583	vpnagent crash on XP after returning from hibernate (tunnel up).
CSCsr07346	AnyConnect uses SSLv3 instead of TLSv1 with Linux/MAC client.
CSCsr56126	DTLS Windowing issue in OpenSSL 0.9.8f.

Caveats Resolved in AnyConnect Release 2.2.133

Table 6 lists the caveats resolved in the Cisco AnyConnect VPN Client, Release 2.2.133. For more information about CSCsq34406, see Network Connections Control Panel Might Show Generic Adapter Name, page 36.

Table 6 Caveats Resolved in Cisco Anyconnect VPN Client, Release 2.2.133

ID	Headline
CSCso57937	Entering Group-URL in “Connect to” doesn't work.
CSCso67063	AnyConnect: Suppress the showing of the message box on reconnect.
CSCso98837	The word “Tunnel” must be replaced with “Connection” for all displays.
CSCsq01605	Limited Users can't connect when customizations applied to AnyConnect.
CSCsq34406	Windows client upgrades fail during SBL connection attempt.

Caveats Resolved in AnyConnect Release 2.2.128

Table 7 lists the caveats resolved in the Cisco AnyConnect VPN Client, Release 2.2.128.

Table 7 Caveats Resolved in Cisco Anyconnect VPN Client, Release 2.2.128

ID	Headline
CSCsi12002	Certificate auth fails under MAC 10.4 with standalone client.
CSCsi44920	Mac OS X and Linux clients may disconnect with an ASA Failover.
CSCsi47777	SSLVPN: IOS: AnyConnect Connection Established msg even though it failed.
CSCsi88191	Vpncli cert-only group select - client still prompts for user/pw.
CSCsi89708	Difficult to cancel out at cert popup - click No - more popups.
CSCsi94721	AnyConnect falsely displays hostname mismatch warning if fqdn exists.
CSCsj16869	Cert Matching not working with multiple match criteria.
CSCsj58515	AnyConnect bad profile or preferences not logged in event log.
CSCsj59065	Connection attempt has failed - if ASA 'svc image' is missing or wrong.
CSCsj62218	Anyconnect Mac freeze crash with gui excluded or split networks.
CSCsj88360	Backup server list in profile not working.

Table 7 Caveats Resolved in Cisco Anyconnect VPN Client, Release 2.2.128 (continued)

ID	Headline
CSCsk35677	AnyConnect gives up reconnect attempts after ~30 seconds.
CSCsk39966	AnyConnect Client pops up Certificate Verification Error upon Disconnect.
CSCsk51997	AnyConnect doesn't connect with proxy PAC file configured in IE.
CSCsk64409	AnyConnect stops passing data after a few rekeys - new-tunnel method.
CSCsk75180	CLI does not show correct tunnel “stats” information.
CSCsl06264	AnyConnect banner should be system modal - always on top.
CSCsl19031	Vista keeps reporting the AnyConnect IP into the DNS Dynamic Update.
CSCsl38401	AnyConnect detects ASA SSL cert as invalid connection fails.
CSCsl39652	Linux init scripts not installed correctly in Ubuntu 7.10.
CSCsl54475	GUI does not display server and realm for proxy creds prompt.
CSCsl77521	Certificate auth fails under Linux SuSE 10.1 with standalone client.
CSCsl90251	AnyConnect/SSLVPN Client Blue Screens with AT&T Global Network installed.
CSCsm24968	Windows machine cannot be named “localhost”.
CSCsm39103	AnyConnect: With CSD enabled, AC will automatically go to last ASA.
CSCso34634	AnyConnect upgrades fail on alternate desktop in Vista.
CSCso43942	Agent crashes after sleep in Mac OS X, leaves network in bad state.

Related Documentation

For more information, refer to the following documentation:

- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Cisco ASDM Online Help*
- *Cisco AnyConnect VPN Client, Release 2.2, Administrator Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco Security Appliance Logging Configuration and System Log Messages*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*
- For Open Source License information for this product, please see the following link: http://www.cisco.com/en/US/docs/security/asa/asa80/license/opensrce.html#wp50053.

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