Cisco AnyConnect VPN Client Administrator Guide

Version 2.0
Updated May 12, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: OL-12950-012

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.

Cisco AnyConnect VPN Client Administrator Guide

CONTENTS

CHAPTER 7

CHAPTER 8

CHAPTER 9

APPENDIX A

About This Guide

OL-12950-012

This preface introduces the *Cisco AnyConnect VPN Client Administrator Guide*, and includes the following sections:

Document Objectives

The purpose of this guide is to help you configure the Cisco AnyConnect VPN Client parameters on the security appliance. This guide does not cover every feature, but describes only the most common configuration scenarios.

You can configure and monitor the security appliance by using either the command-line interface or ASDM, a web-based GUI application. ASDM includes configuration wizards to guide you through some common configuration scenarios, and online Help for less common scenarios. For more information, see: http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm

This guide applies to the Cisco ASA 5500 series security appliances (ASA 5505 and higher). Throughout this guide, the term “security appliance” applies generically to all supported models, unless specified otherwise. The PIX family of security appliances is not supported.

Audience

This guide is for network managers who perform any of the following tasks:

- Manage network security
- Install and configuresecurity appliances
- Configure VPNs

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*
- *Release Notes for Cisco AnyConnect VPN Client, Release 2.0*
- *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.

Document Organization

This guide includes the chapters and appendixes described in Table 1.

Table 1 Document Organization

Chapter/Appendix	Definition
Chapter 1, "Introduction"	Provides a high-level overview of the Cisco Anyconnect VPN Client.
Chapter 2, "Common AnyConnect VPN Client Installation and Configuration Procedures"	Describes how to access the required files and install the Cisco AnyConnect VPN Client on the security appliance and on the remote user PCs.
Chapter 3, "Installing the AnyConnect Client and Configuring the Security Appliance with ASDM"	Describes how to use ASDM to install the Cisco AnyConnect VPN Client on the security appliance.
Chapter 4, "Installing the AnyConnect Client on a Security Appliance Using CLI"	Describes how to use the command-line interface to install the Cisco AnyConnect VPN Client on the security appliance.
Chapter 5, "Configuring AnyConnect Features Using ASDM"	Describes how to use ASDM to configure the various features of the Cisco AnyConnect VPN Client on the security appliance.
Chapter 6, "Configuring AnyConnect Features Using CLI"	Describes how to use ASDM to configure the various features of the Cisco AnyConnect VPN Client on the security appliance.
Chapter 7, "Configuring and Using AnyConnect Client Operating Modes and User Profiles"	Describes how to configure and use AnyConnect client operating modes and XML users profiles.

Table 1 Document Organization (continued)

Chapter/Appendix	Definition
Chapter 8, "Customizing and Localizing the AnyConnect Client"	Describes how to customize and localize the end-user interface of the Cisco AnyConnect VPN Client.
Chapter 9, "Monitoring and Maintaining the AnyConnect Client"	Describes how to monitor and maintain the Cisco AnyConnect VPN Client using the security appliance
Appendix A, "Sample AnyConnect Profile and XML Schema"	Provides a sample AnyConnect user XML profile and an XML schema that you can use to validate the user profiles you create.
Appendix B, "Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users"	Describes in detail how an Active Directory Domain Administrator can push to remote users a group policy that adds the security appliance to the list of trusted sites in Internet Explorer.

Document Conventions

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([ ]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Right-pointing angle brackets (>) indicate a sequence in a path.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen` font.
- Information you need to enter in examples is shown in **`boldface screen`** font.
- Variables for which you must supply a value are shown in *`italic screen`* font.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Licensing

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

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

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

CHAPTER 1

Introduction

This book describes a process for getting the Cisco AnyConnect VPN Client up and running on your central-site security appliance and on your remote users' PCs. In this context, PC refers generically to Windows, Mac, and Linux devices, but the focus in this document is primarily on Windows PC users.

AnyConnect Client Features

The Cisco AnyConnect VPN Client is the next-generation VPN client, providing remote users with secure VPN connections to the Cisco 5500 Series Adaptive Security Appliance running ASA version 8.0 and higher or ASDM 6.0 and higher. It does not connect with a PIX device nor with a VPN 3000 Series Concentrator.

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

The AnyConnect client supports Windows Vista, Windows XP and Windows 2000, Mac OS X (Version 10.4 or later) on either Intel or PowerPC, and Red Hat Linux (Version 9 or later). See the Release Notes for the full set of platform requirements and supported versions.

As the network administrator, you configure the AnyConnect client features on the security appliance. Then, you can load the client on the security appliance and have it automatically download to remote users when they log in, or you can manually install the client as an application on PCs. The client allows user profiles that are displayed in the user interface and define the names and addresses of host computers.

The network administrator can assign particular features to individual users or groups. The AnyConnect client includes the following features:

- 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.

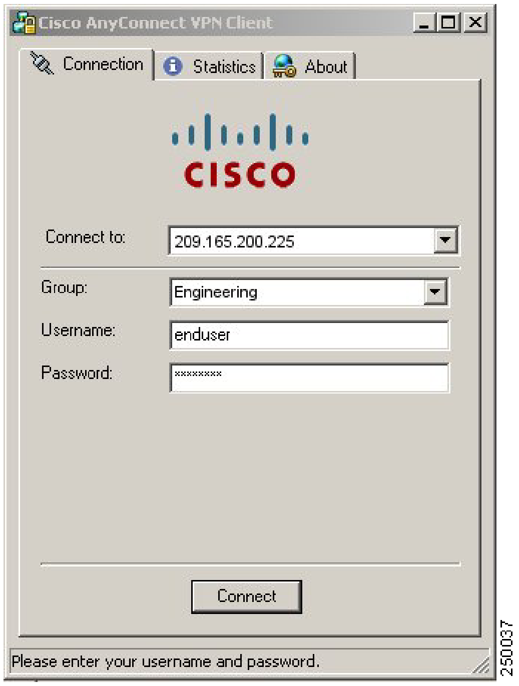
- IPv6 VPN access—Allows access to IPv6 resources over a public IPv4 connection (Windows XP SP2, Windows Vista, Mac OSX, and Linux only).
- Start Before Login (SBL)—Allows for login scripts, password caching, drive mapping, and more, for Windows.
- Certificate-only authentication—Allows users to connect with digital certificate and not provide a user ID and password.
- Simultaneous AnyConnect client and clientless, browser-based connections—Allows a user to have both an AnyConnect (standalone) connection and a Clientless SSL VPN connection (through a browser) at the same time to the same IP address. Each connection has its own tunnel.
- 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 support—Validates the security of client computers requesting access to your SSL VPN, helps ensure they remain secure while they are connected, and attempts to remove traces of the session after they disconnect. The Cisco AnyConnect VPN Client supports the Secure Desktop functions of Cisco Secure Desktop for Windows 2000 and Windows XP.
- Rekey—Specifies that SSL renegotiation takes place during rekey.

Note The Cisco AnyConnect VPN Client can coexist with the IPSec Cisco VPN Client, but they cannot be used simultaneously.

Remote User Interface

Remote users see the Cisco AnyConnect VPN Client user interface (Figure 1-1). The Connection tab provides a drop-down list of profiles for connecting to remote systems. You can optionally configure a banner message to appear on the Connection tab. The status line at the bottom of the interface shows the status of the connection.

Figure 1-1 Cisco AnyConnect VPN Client User Interface, Connection Tab



Connect to: 209.165.200.225

Group: Engineering

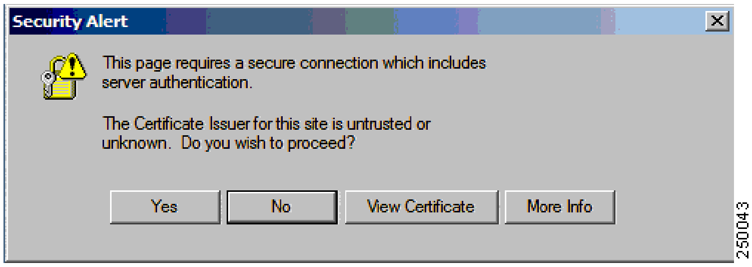
Username: enduser

Password: ********

Please enter your username and password.

If you do not have certificates set up, you might see the dialog box shown in Figure 1-2. When you see this dialog box, click Yes to connect.

Figure 1-2 Security Alert Dialog Box



This page requires a secure connection which includes server authentication.

The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

Note Note: Most users (those with correct certificate deployments) do not see this dialog box.

Table 1-1 shows the circumstances and results when the Security Alert dialog box appears.

Table 1-1 Certificate, Security Alert, and Connection Status

Certificate Status	Does Security Alert Appear?	Client Connection Status
Server certificate sent to the client from the security appliance is independently verifiable *and* the certificate has no serious errors.	No	Success
Server certificate sent to the client from the security appliance is *not* independently verifiable *and* the certificate contains serious errors.	No	Failure
Server certificate sent to the client from the security appliance is *not* independently verifiable *and* the certificate does *not* contain serious errors.	Yes	Because the client cannot verify the certificate, it is still a security concern. The client asks the user whether to continue with the connection attempt.

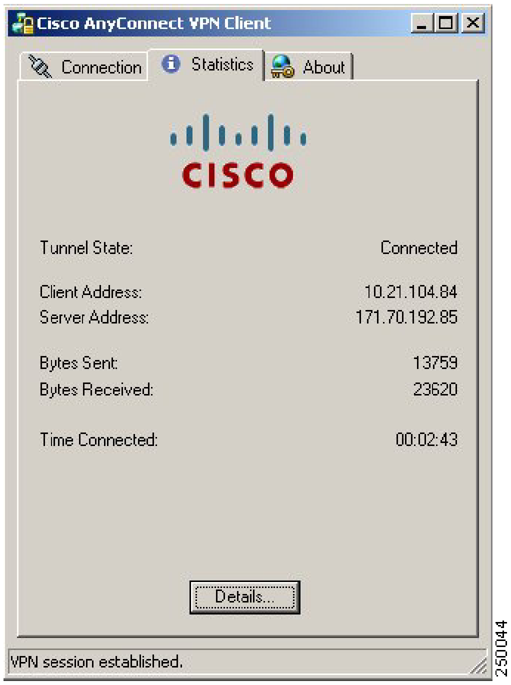
The Security Alert dialog box appears only on the first connection attempt to a given security appliance. After the connection is successfully established, the "thumbprint" of the server certificate is saved in the preferences file, so the user is not prompted on subsequent connections to the same security appliance.

If the user switches to a different security appliance and back, the Security Alert dialog box appears again.

For detailed information and examples of instances in which the remote user does or does not see the Security Alert dialog box, see Adding a Security Certificate in Response to Browser Security Alert Windows, page 2-4.

Figure 1-3 shows the Statistics tab, including current connection information.

Figure 1-3 Cisco AnyConnect VPN Client User Interface, Statistics Tab



Tunnel State: Connected

Client Address: 10.21.104.84
Server Address: 171.70.192.85

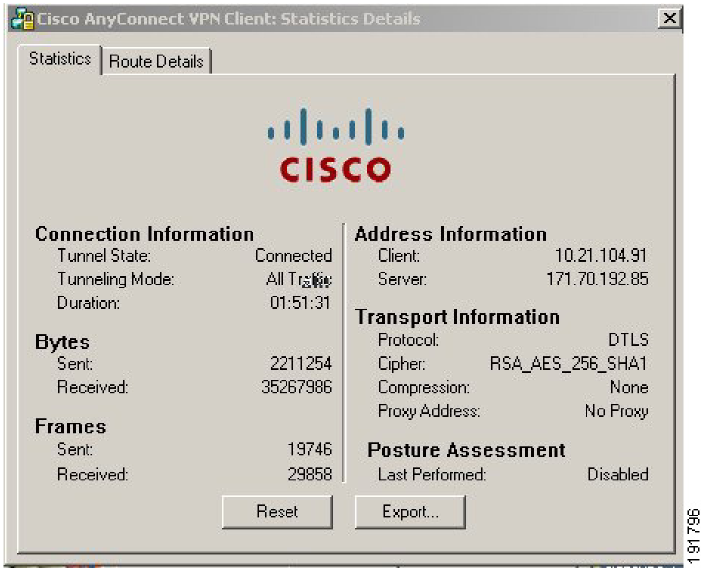
Bytes Sent: 13759
Bytes Received: 23620

Time Connected: 00:02:43

VPN session established.

Clicking the Details tab shows Statistics Details window (Figure 1-4). The Statistics tab in the Statistics Details window has detailed connection statistical information, including the tunnel state and mode, the duration of the connection, the number of bytes and frames sent and received, address information, transport information, and Cisco Secure Desktop posture assessment status. The Reset button on this tab resets the transmission statistics. The Export button lets you export the current statistics, interface, and routing table to a text file. The AnyConnect client prompts you for a name and location for the text file. The default name is AnyConnect-ExportedStats.txt, and the default location is on the desktop.

Figure 1-4 Cisco AnyConnect VPN Client User Interface, Statistics Tab, Statistics Details Tab



Connection Information

Tunnel State:	Connected
Tunneling Mode:	All Traffic
Duration:	01:51:31

Bytes

Sent:	2211254
Received:	35267986

Frames

Sent:	19746
Received:	29858

Address Information

Client:	10.21.104.91
Server:	171.70.192.85

Transport Information

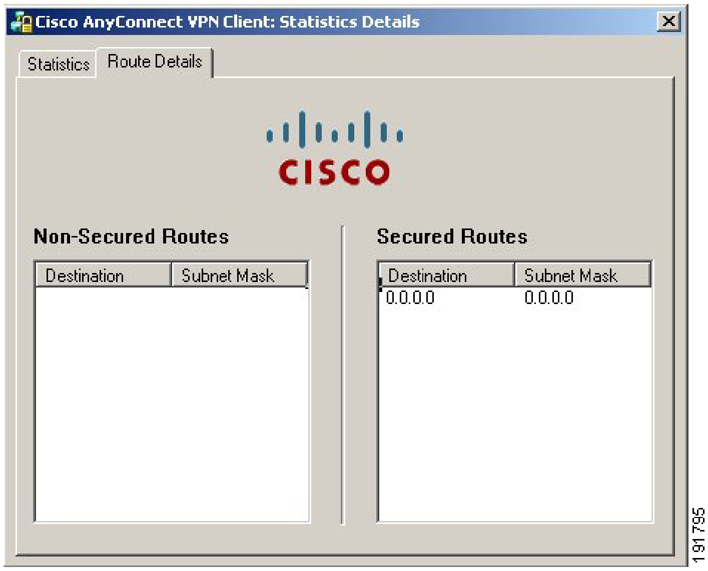
Protocol:	DTLS
Cipher:	RSA_AES_256_SHA1
Compression:	None
Proxy Address:	No Proxy

Posture Assessment

Last Performed:	Disabled

Clicking the Route Details tab (Figure 1-5) shows the secured and non-secured routes for this connection.

Figure 1-5 Cisco AnyConnect VPN Client User Interface, Statistics Tab, Route Details Tab



Non-Secured Routes

Destination	Subnet Mask

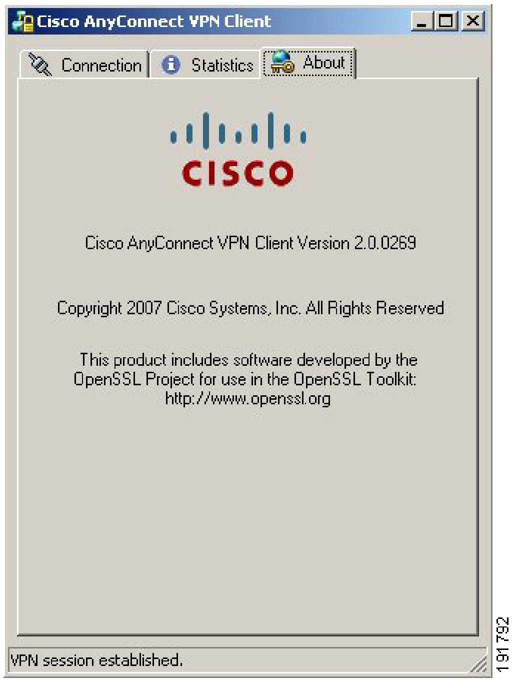
Secured Routes

Destination	Subnet Mask
0.0.0.0	0.0.0.0

Note A Secured Routes entry with the destination 0.0.0.0 and the subnet mask 0.0.0.0 means that all traffic is tunneled.

The About tab (Figure 1-6) shows version, copyright, and documentary information about the Cisco AnyConnect Client.

Figure 1-6 Cisco AnyConnect VPN Client User Interface, About Tab



Cisco AnyConnect VPN Client Version 2.0.0269

Copyright 2007 Cisco Systems, Inc. All Rights Reserved

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

VPN session established.

Getting and Installing the Files You Need

The latest Release Notes document contains the system requirements and detailed instructions for getting and installing the necessary files.Cisco Secure Desktop interoperability with the AnyConnect Client is supported only on Windows 2000 and Windows XP operating systems.

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

The 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.

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*.

CHAPTER 2

Common AnyConnect VPN Client Installation and Configuration Procedures

Installing the AnyConnect Client

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 part of the ASA Release 8.0(1) and later and ASDM Release 6.0 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.

This chapter contains procedures for installing the AnyConnect client software on the ASA5500 using the Adaptive Security Device Manager (ASDM) or the CLI command interface. It also describes how to install the AnyConnect client on a user's PC and how to enable AnyConnect client features after installation.

WebLaunch Mode

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

Note A user with a clientless SSL VPN connection can switch to an AnyConnect client SSL VPN connection by clicking the AnyConnect 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. This document contains information about how to configure the features of the AnyConnect client. 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 download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the portal page.

Note When using Start Before Logon, the VPN Gina (VPN Graphical Identification and Authentication) a cannot be installed dynamically if the AnyConnect client is installed manually. The VPN Gina can be installed either before or after the AnyConnect client, but they must either be both installed manually or both installed dynamically (CSCsh38590).

This section describes installation-specific issues and procedures for the AnyConnect client Release 2.0(1), and contains the following sections:

- Before You Install the AnyConnect Client, page 2-2
- Installing the AnyConnect Client on a User’s PC, page 2-8
- Installing the AnyConnect Client on a User’s PC, page 2-8

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 2-2
- AnyConnect Client and New Windows Installations, page 2-3
- Adding a Security Appliance to the List of Trusted Sites (Internet Explorer), page 2-3
- Adding a Security Certificate in Response to Browser Security Alert Windows, page 2-4

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 the 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 in to a future release of CSA.

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

AnyConnect Client and New Windows Installations

In rare circumstances, if you install the AnyConnect client on a computer that has a new or clean Windows 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 (Internet Explorer)

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

Note Adding a security appliance to the list of trusted sites for Internet Explorer is required for those running Windows Vista who want 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.

Note To use Microsoft Active Directory to add the security appliance to the list of Internet Explorer trusted sites for domain users, see Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users, page B-1.

When a user gets the server certificate for the security appliance from a globally trusted certificate authority—for example, Verisign or Cisco—the user never sees a Security Alert pop-up when connecting to that security appliance.

Adding a Security Certificate in Response to Browser Security 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.

Connecting to this security appliance.

A remote user using standalone mode might see a Security Alert dialog box in several possible login situations. The following examples and scenarios show some instances. After these descriptions, you'll see how to add a security certificate to avoid these situations.

The following examples illustrate sequences of events involving the pop-up Security Alert dialog box.

Example Set 1

1. A user connects to badly configured security appliance #1. As a result, the user sees the pop-up Security Alert dialog box.
2. The user approves the certificate.

3. The user connects successfully to security appliance #1.
4. The user disconnects from security appliance #1.
5. The user reconnects to badly configured security appliance #1.
6. The user does not see the pop-up dialog box, because the certificate is stored in the preferences file. The user connects successfully to security appliance #1.
7. The user disconnects from security appliance #1.
8. The user connects to correctly configured security appliance #2.
9. The user sees no dialog box and connects successfully.
10. The user disconnects from security appliance #2.
11. The user connects to badly configured security appliance #1.
12. The user sees a pop-up Security Alert dialog box prompt.

Example Set 2

The following are examples of non-serious errors that result in a Security Alert dialog box prompting the user.

- Invalid Common Name: The hostname in the certificate sent to us from the security appliance does not match the hostname that the user connected to.

  For example, the user connects to 10.94.147.93, and the certificate received from the security appliance contains cvc-asa06.cisco.com. 10.94.147.93 and cvc-asa06.cisco.com might or might not be the same machine. The Security Alert dialog box prompts the user to approve or disapprove the certificate.
- Invalid Date: The certificate received from the security appliance has expired or is not yet valid. This could be because the date on the customer's machine is incorrect or because the certificate really is invalid. The Security Alert dialog box prompts the user to approve or disapprove the certificate.
- Invalid Certificate Authority: The certificate received from the security appliance has been signed by a Certificate Authority that is not recognized by the AnyConnect client. The AnyConnect client prompts the user for approval/disapproval. Recommendation: The root certificate (certificate of the Certificate Authority) should be imported into the client machine out of band (via E-mail, website, floppy disk, CD, and so on).

Example Set 3

The following are examples of serious errors that result in no Security Alert prompt and no connection.

- Certificate cannot be read.
- Bad password.
- Certificate not sent to the client.
- Bad Usage: Certificate received from the security appliance was not meant to be used as a server certificate.

Scenarios Where a User Might See the Security Alert

- *Scenario A*: The user gets the server certificate for their security appliance from a non-trusted certificate authority; for example, their own certificate authority or cacert.org.

  The user sees the Security Alert pop-up on the first connection attempt but never thereafter until he or she switches to a different security appliance and back.

Recommendation: Administrators should import the root certificate that was used to sign that server certificate (for example, their own certificate authority or cacert.org) into every client machine out of band via E-mail, website, floppy disk, and so on.

- *Scenario B*: The user gets the server certificate for the security appliance from the certificate authority that sits on the security appliance.

  The user sees the Security Alert pop-up on the first connection attempt but never thereafter until he or she switches to a different security appliance and back.

  Recommendation: Administrators should import the root certificate of the certificate authority that sits on the security appliance into every client machine out of band via E-mail, website, floppy disk, and so on.

- *Scenario C*: the security appliance is at default configuration and certificates haven't been configured.

  When at default, the security appliance generates a self-signed server certificate that the AnyConnect client does not trust.

  The user sees the Security Alert pop-up on the first connection attempt but never thereafter until he or she switches to a different security appliance and back.

  Recommendation: Administrators should correctly configure certificates on their security appliance before attempting client connections to them.

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.

Replacing a Digital Certificate with a Trusted Certificate

A trusted Certificate is the most secure option. You can replace the central-site security appliance digital certificate with a trusted certificate by following the procedures in this section. By default, the security appliance has a self-signed Certificate that is regenerated every time the device is rebooted. You can purchase a Certificate from a CA provider like Verisign or Entrust with the name matching the Fully-Qualified Domain Name (FQDN) of your central-site security appliance (for example, vpn.yoursys.com), or you can have the security appliance issue a permanent Certificate for itself by entering the following commands, replacing x.x.x.x with the IP of your security appliance outside or public address:

```
crypto ca trustpoint self
enrollment self
subject-name CN=x.x.x.x,CN=vpn.yoursys.com
crl configure
crypto ca enroll self
ssl trust-point self outside
write
```

When users first connect using AnyConnect, they should click "View Certificate", install this new certificate, then click "Yes" to proceed. The next time they re-connect, they do not see the security alert popup, even if the security appliance is rebooted.

Installing the AnyConnect Client on a User's PC

You can set up a user's PC to run the AnyConnect client in standalone mode by installing the client software for the appropriate operating system directly on the user's PC. In standalone mode, the user starts the AnyConnect client software without first establishing a web connection. The client uses essentially the same authentication mechanisms as the web-enabled (WebLaunch) mode, but the client displays a GUI to the user, asking for the authentication credentials. The following sections describe how to install the client on Windows, Linux, and Mac systems.

- Where to Find the AnyConnect Client Files to Install, page 2-8
- Installing the AnyConnect Client Using the Microsoft Windows Installer on a PC Running Windows, page 2-8
- Installing the AnyConnect Client on a PC Running Linux, page 2-9
- Installing the AnyConnect Client on a PC Running MAC OSX, page 2-9

Where to Find the AnyConnect Client Files to Install

All of the AnyConnect clients are located in the same place.

http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect

Installing the AnyConnect Client Using the Microsoft Windows Installer on a PC Running Windows

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

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

Step 1 Exit all Windows programs, and disable any antivirus software (recommended).

Step 2 Download the AnyConnect client MSI file from the Cisco site; for example, anyconnect-win-2.0.xxx.msi, where xxx represents the current build number. See the Release Notes for the current release for the full set of operating-system-specific download sites.

Step 3 Double-click the MSI 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.

You can also use the Microsoft Installer to load the AnyConnect client software on the user's Windows-based PC. MSI gives Windows users a pre-install package option that provides installation, maintenance, and removal of AnyConnect client software on Windows systems.

Installing the AnyConnect Client on a PC Running Linux

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

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

```
tar xvzf AnyConnect-Linux-Release-2.0.0xxx.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 from the user interface 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 PC Running MAC OSX

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

Step 1 Transfer the installation package file to the desktop and double-click the file. Select one of the following files:

- anyconnect-macosx-i386-2.0.xxx.dmg
- anyconnect-macosx-powerpc-2.0.xxx.dmg

This creates a VPN icon representing the installation package file.

Step 2 Double-click the vpn icon to initiate the installation. Follow the sequence of the vpnclient installer, accepting the licensing agreement, selecting the destination volume, and then selecting the "Upgrade" option to perform a basic installation.

Note The installer requires that you authenticate.

The installation is complete.

CHAPTER 3

Installing the AnyConnect Client and Configuring the Security Appliance with ASDM

Installing 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 in which the security appliance loads the clients to the remote PC.

Note The AnyConnect client configuration uses the same parameters as the SSL VPN Client. Many of the file names, panel names, and ASDM navigation elements, as well as most of the CLI commands include the prefix **svc**, indicating this similarity.

Perform the following steps to install the client:

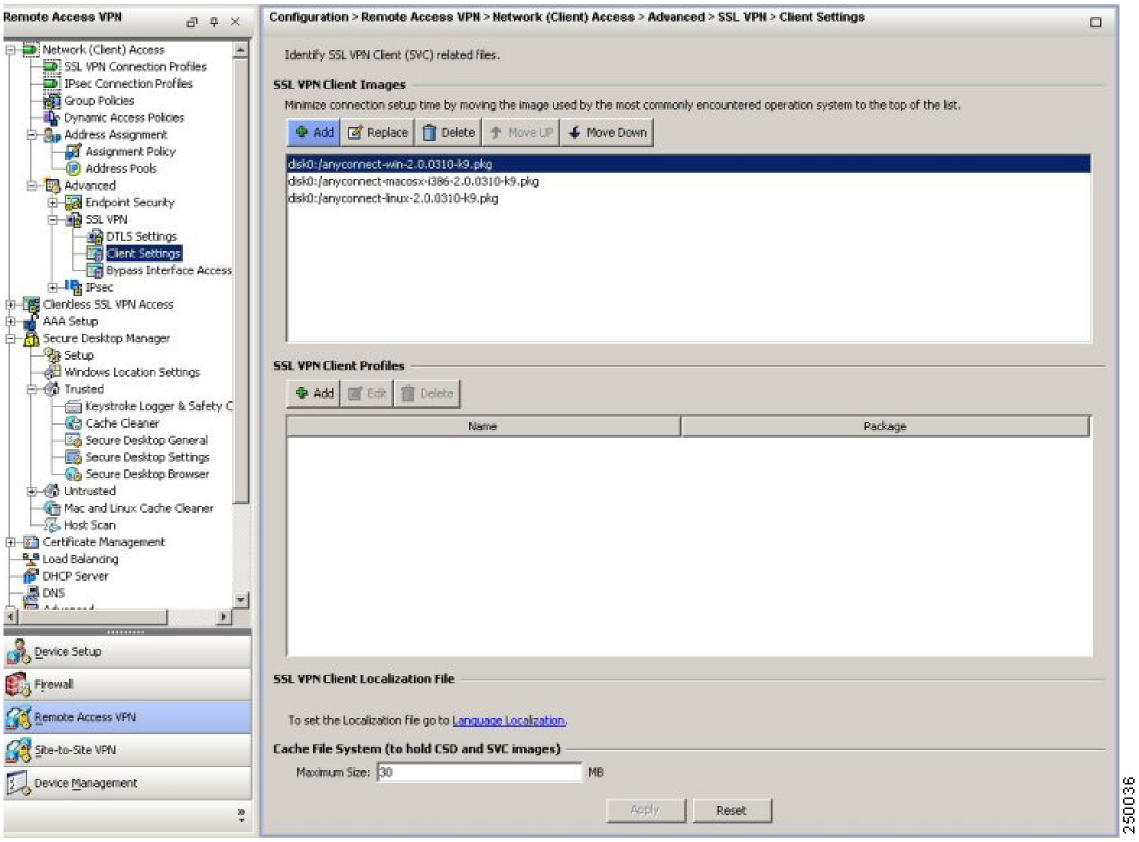
Step 1 Load the AnyConnect client images to the security appliance. On the ASDM toolbar, click **Configuration**. The navigation pane displays features to configure.

Step 2 In the navigation pane, click **Remote Access VPN**. The navigation pane displays VPN features.

Step 3 Choose **Network (Client) Access > Advanced > SSL VPN > Client Settings**. The SSL VPN Client Settings panel displays. (Figure 3-1).

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 in which they download to the remote computer.

Figure 3-1 SSL VPN Client 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

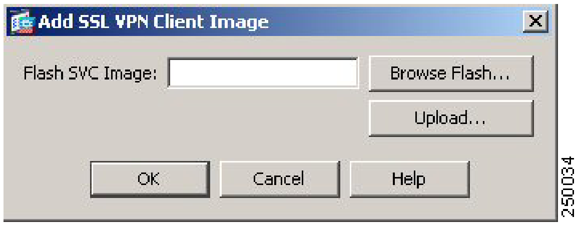
To set the Localization file go to Language Localization.

Cache File System (to hold CSD and SVC images)

Maximum Size: 30 MB

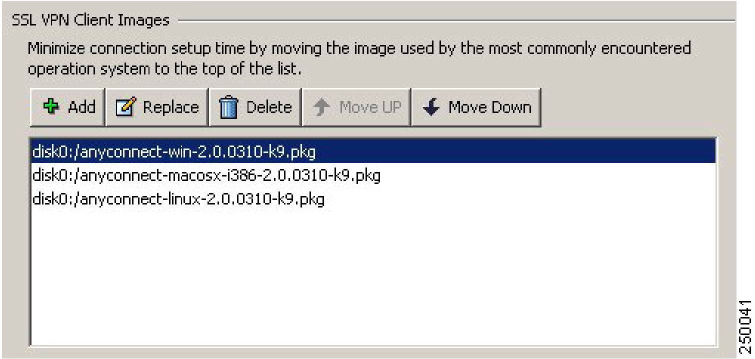
To add an AnyConnect client image, Click **Add** in the SSL VPN Client Images area. The Add SSL VPN Client Image dialog appears (Figure 3-2).

Figure 3-2 Add SSL VPN Client Image Dialog



If you already have an image located in the flash memory of the security appliance, you can enter the name of the image in the Flash SVC Image field, and click **OK**. The SSL VPN Client Settings panel now shows the AnyConnect client images you identified (Figure 3-3).

Figure 3-3 ***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

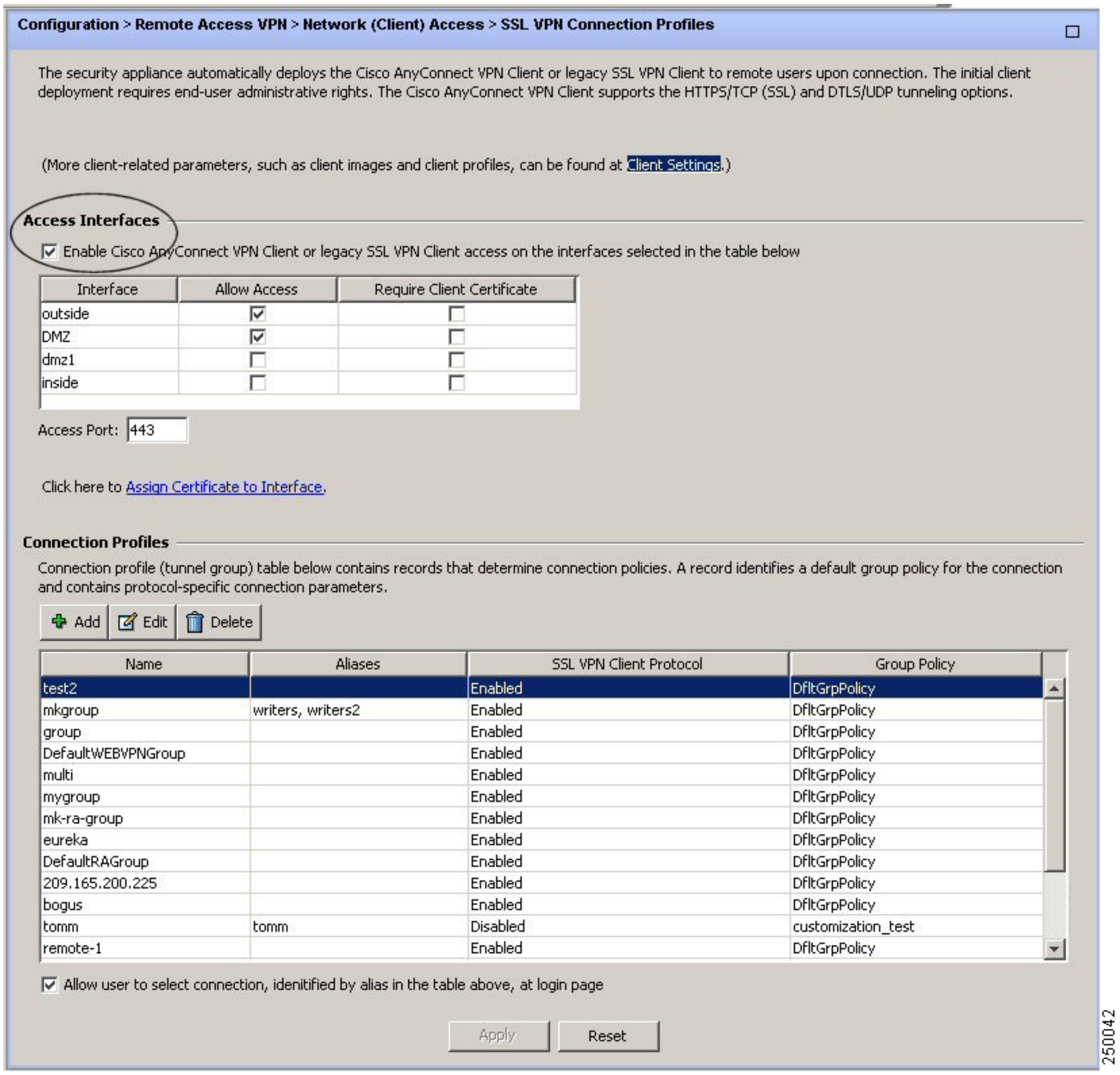
Note The security appliance downloads portions of each client in the order you specify until it matches the operating system of the remote PC. Therefore, assign the topmost position to the image used by the most commonly-encountered operating system.

Step 4 Click on an image name, and use the **Move Up** or **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. The security appliance 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 (Client) Access > SSL VPN Connection Profiles**. The SSL VPN Connection Profiles panel appears (Figure 3-4). Check Enable Cisco AnyConnect VPN Client or legacy SSL VPN client access on the interfaces selected in the table below.

Figure 3-4 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 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.

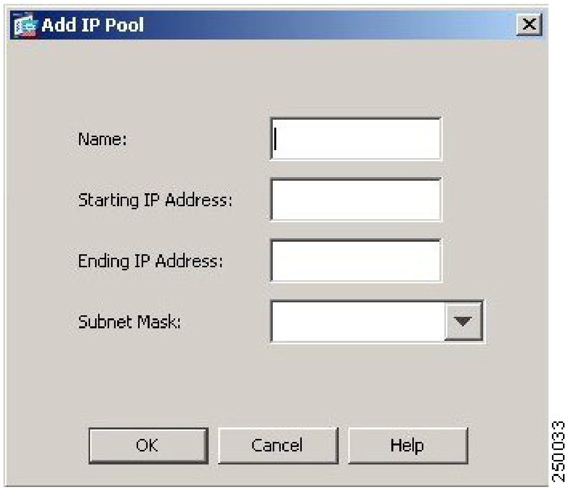
Name	Aliases	SSL VPN Client Protocol	Group Policy
test2		Enabled	DfltGrpPolicy
mkgroup	writers, writers2	Enabled	DfltGrpPolicy
group		Enabled	DfltGrpPolicy
DefaultWEBVPNGroup		Enabled	DfltGrpPolicy
multi		Enabled	DfltGrpPolicy
mygroup		Enabled	DfltGrpPolicy
mk-ra-group		Enabled	DfltGrpPolicy
eureka		Enabled	DfltGrpPolicy
DefaultRAGroup		Enabled	DfltGrpPolicy
209.165.200.225		Enabled	DfltGrpPolicy
bogus		Enabled	DfltGrpPolicy
tomm	tomm	Disabled	customization_test
remote-1		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 (Client) Access > Address Management > Address Pools**. Click **Add**. The Add IP Pool dialog appears (Figure 3-5).

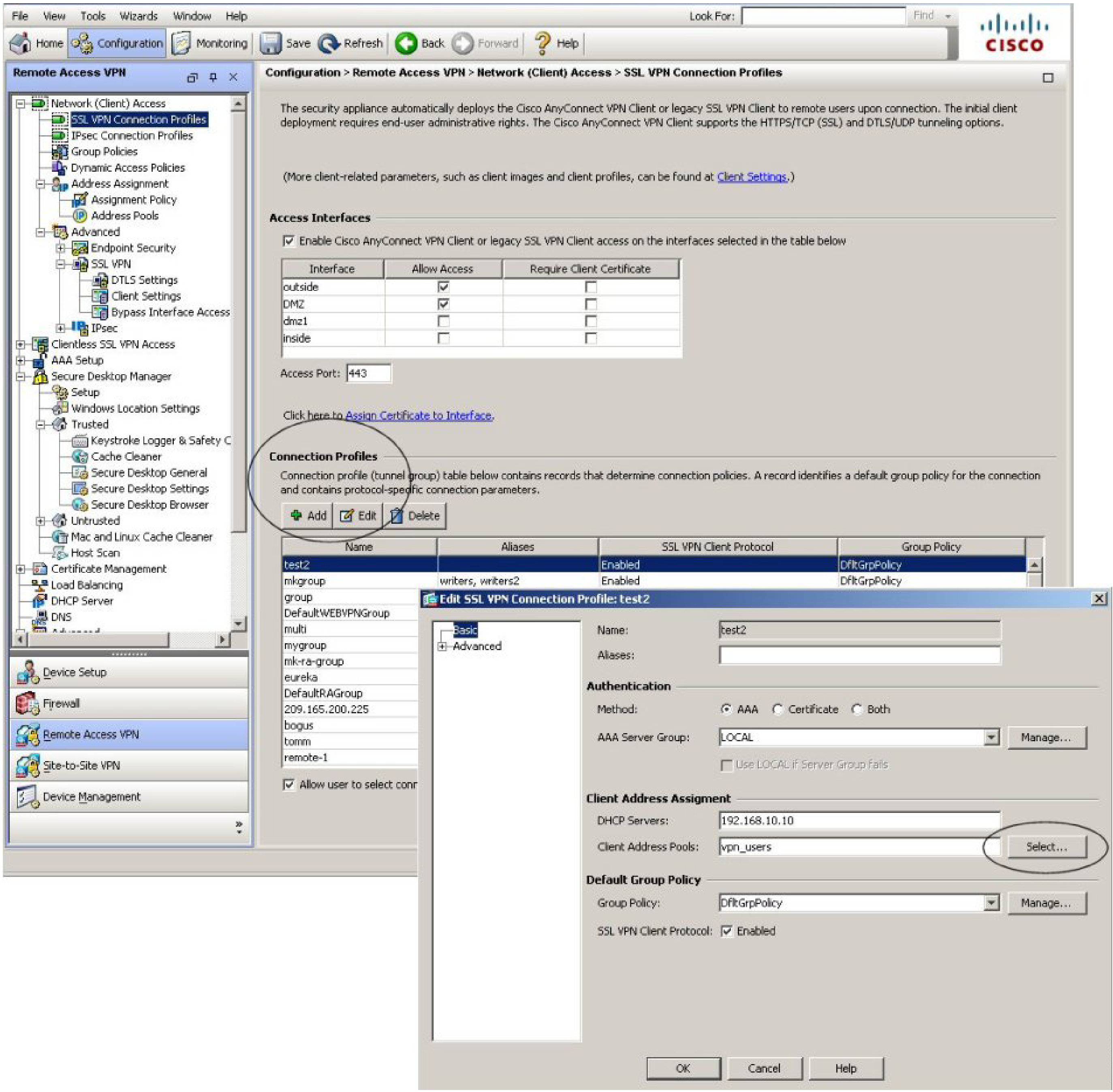
Figure 3-5 Add IP Pool Dialog



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

Step 7 Assign the IP address pool to a Connection (tunnel group). To do this, choose **Network (Client) Access > SSL VPN Connection Profiles**. The SSL VPN Connection Profiles panel appears (Figure 3-6):

Figure 3-6 Client 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

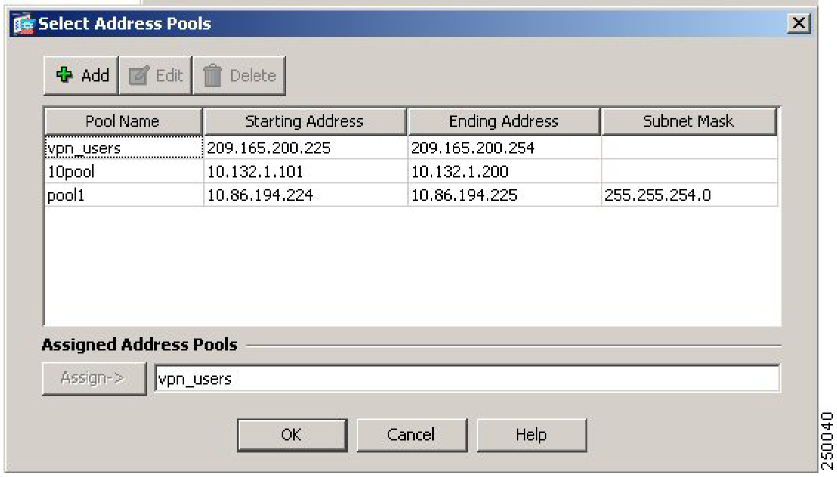
Group Policy: DfltGrpPolicy

SSL VPN Client Protocol: ☑ Enabled

To edit an existing connection profile, highlight a connection in the table, and click **Edit.** The Edit SSL VPN Connection > Basic dialog box appears. To add a new connection profile, click Add. The Add SSL VPN Connection > Basic dialog box appears, which is identical to the Edit dialog box, except that you must supply a name for the connection profile. Then proceed as follows.

Click **Select** in the Client Address Assignment area. The Select Address Pool dialog box appears (Figure 3-7), containing available address pools. Select a pool The pool you select appears in the Assign field in the Assigned Address pools area. Click **OK**.

Figure 3-7 Select Address Pool Dialog



Pool Name	Starting Address	Ending Address	Subnet Mask
vpn_users	209.165.200.225	209.165.200.254	
10pool	10.132.1.101	10.132.1.200	
pool1	10.86.194.224	10.86.194.225	255.255.254.0

Assigned Address Pools

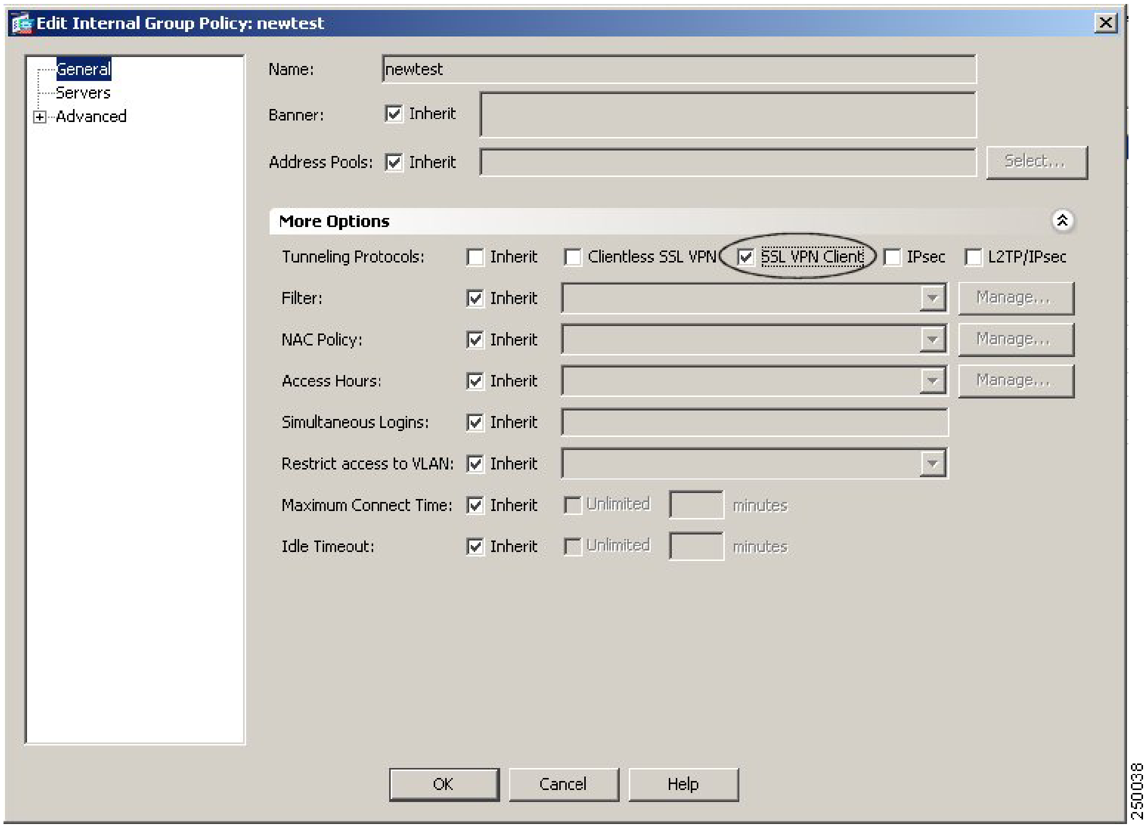
vpn_users

Step 8 Identify SSL VPN as a permitted VPN tunneling protocol for the group or user.

Choose **Network (Client) 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 3-8):

Figure 3-8 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

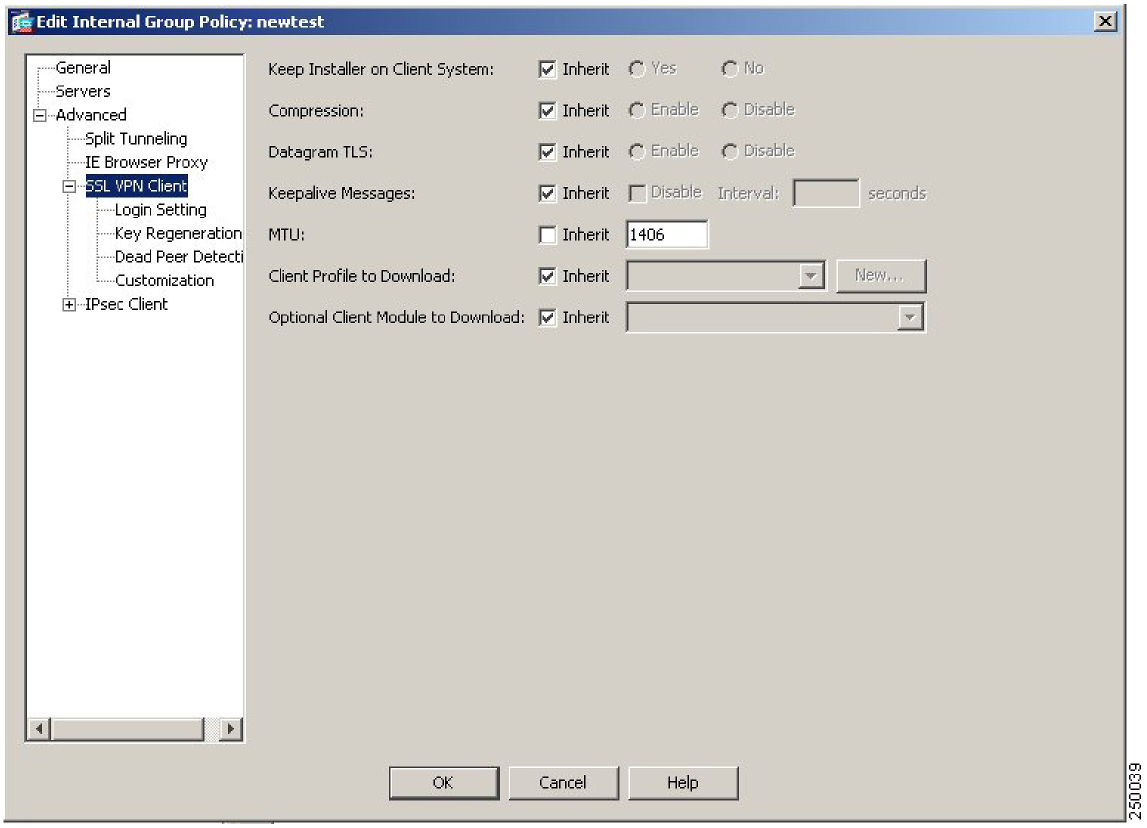
Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

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

Step 9 Configure SSL VPN attributes 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 3-9.

Figure 3-9 SSL VPN Client Features



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 on low-bandwidth links between the security appliance and the client by reducing the size of the packets being transferred. On broadband connections, compression might degrade performance.
- **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 SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Note Compression and DTLS are mutually exclusive. If you enable both, DTLS is inactive for the client connection.

- **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 1406 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 AnyConnect Client 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 AnyConnect Client requests downloads (from the security appliance) only of core modules that it needs for each feature that it supports.

The attributes you configure on the Group Policies > Advanced > SSL VPN Client dialog box set the profile for the AnyConnect Client.

CHAPTER 4

Installing the AnyConnect Client on a Security Appliance Using CLI

Installing the AnyConnect client on the security appliance consists of copying a client image to the security appliance and identifying the file as a client image. With multiple clients, you must also assign the order that the security appliance downloads the clients to the remote PC.

Note The AnyConnect client configuration uses the same parameters as the SSL VPN Client. Most of the CLI commands and many of the file names include the prefix **svc**, indicating this similarity.

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. This example copies the images from a tftp server using the **copy tftp** command:

```
hostname# copy tftp flash
Address or name of remote host []? 209.165.200.226
Source filename []? anyconnect-win-2.0.0.0343.pkg
Destination filename []? anyconnect-win-2.0.0.0343.pkg
Accessing
tftp://209.165.200.226/anyconnect-win-2.0.0.0343.pkg...!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file
disk0:/cdisk71...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
319662 bytes copied in 3.695 secs (86511 bytes/sec)
```

Step 2 Identify a file on flash as an SSL VPN 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 downloads 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 anyconnect-win-2.0.0343-k9.pkg 1
hostname(config-webvpn)# svc image anyconnect-macosx-i386-2.0.0343-k9.pkg 2
hostname(config-webvpn)# svc image anyconnect-linux-2.0.0343-k9.pkg 3
```

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 - increase disk space via the 'cache-fs' command*, 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:/anyconnect-win-2.0.0343-k9.pkg 1
  CISCO STC win2k+
  2,0,0343
  Tue 03/27/2007  4:16:21.09

2. disk0:/anyconnect-macosx-i386-2.0.0343-k9.pkg 2
  CISCO STC Darwin_i386
  2,0,0
  Tue Mar 27 05:09:16 MDT 2007

3. disk0:/anyconnect-linux-2.0.0343-k9.pkg 3
  CISCO STC Linux
  2,0,0
  Tue Mar 27 04:06:53 MST 2007

3 SSL VPN Client(s) installed
```

Enabling AnyConnect Client SSL VPN Connections Using CLI

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

Step 1 Enable WebVPN on an interface using the **enable** command from webvpn mode:

enable *interface*

For example:

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

You must enable WebVPN on the interface before enabling DTLS.

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 Enable DTLS on an interface, using the **dtls enable** command in webvpn mode. For example:

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

To enable DTLS globally for a specific port, use the dtls port command in webvpn mode. The following example enters webvpn configuration mode and specifies port 444 for DTLS:

```
hostname(config)# webvp4
hostname(config-webvpn)# dtls port 445
```

Step 4 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 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 5 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 6 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 7 Create and enable a group alias that displays in the group list on the WebVPN 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 8 Enable the display of the tunnel-group list on the WebVPN 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 9 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

You can also specify other protocols to permit by adding the names of those protocols to this command. For more information about the vpn-tunnel-protocol command, see the command description in *Cisco Security Appliance Command Reference*.

To specify SSL as a permitted tunneling protocol, 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 WebVPN 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 "Configuring Tunnel Groups, Group Policies, and Users" in *Cisco Security Appliance Command Line Configuration Guide*.

Disabling Permanent Client Installation

Disabling permanent AnyConnect client installation enables the automatic uninstalling feature of the client. The client on the remote computer uninstalls at the end of every session.

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 remains installed on the remote computer at the end of every session, reducing the connection time for subsequent connections. The following example configures the existing group-policy *sales* to *not* keep the client installed on the remote computer when the session terminates:

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

CHAPTER 5

Configuring AnyConnect Features Using ASDM

The AnyConnect client includes the following features, which you configure on the security appliance:

Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections

Datagram Transport Layer Security avoids latency and bandwidth problems associated with some SSL-only connections, including AnyConnect 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).

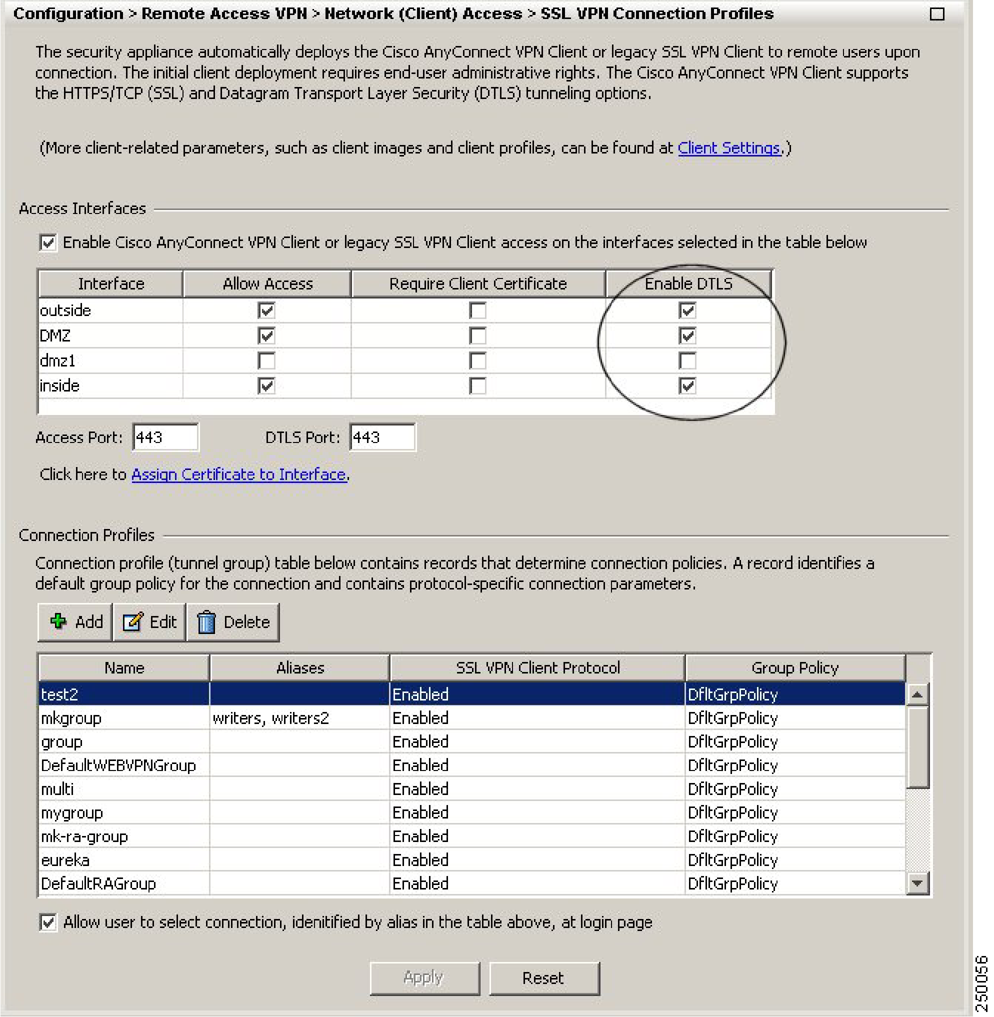
Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications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

If you do not enable DTLS, AnyConnect/SSL VPN connections connect with an SSL VPN tunnel only.

You cannot enable DTLS globally with ASDM. The following section describes how to enable DTLS for any specific interface.

To enable DTLS for a specific interface, select Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN Connection profiles. The SSL VPN Connection Profiles dialog box opens (Figure 5-1).

Figure 5-1 Enable DTLS 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

To enable DTLS on an interface, select the check box in its row. To specify a separate UDP port to use for AnyConnect, enter the port number in the UDP Port field. The default value is port 443.

Configuring DTLS

If DTLS is configured and UDP is interrupted, the remote user's connection automatically falls back from DTLS to TLS. The default is enabled; however, DTLS is not enabled by default on any individual interface.

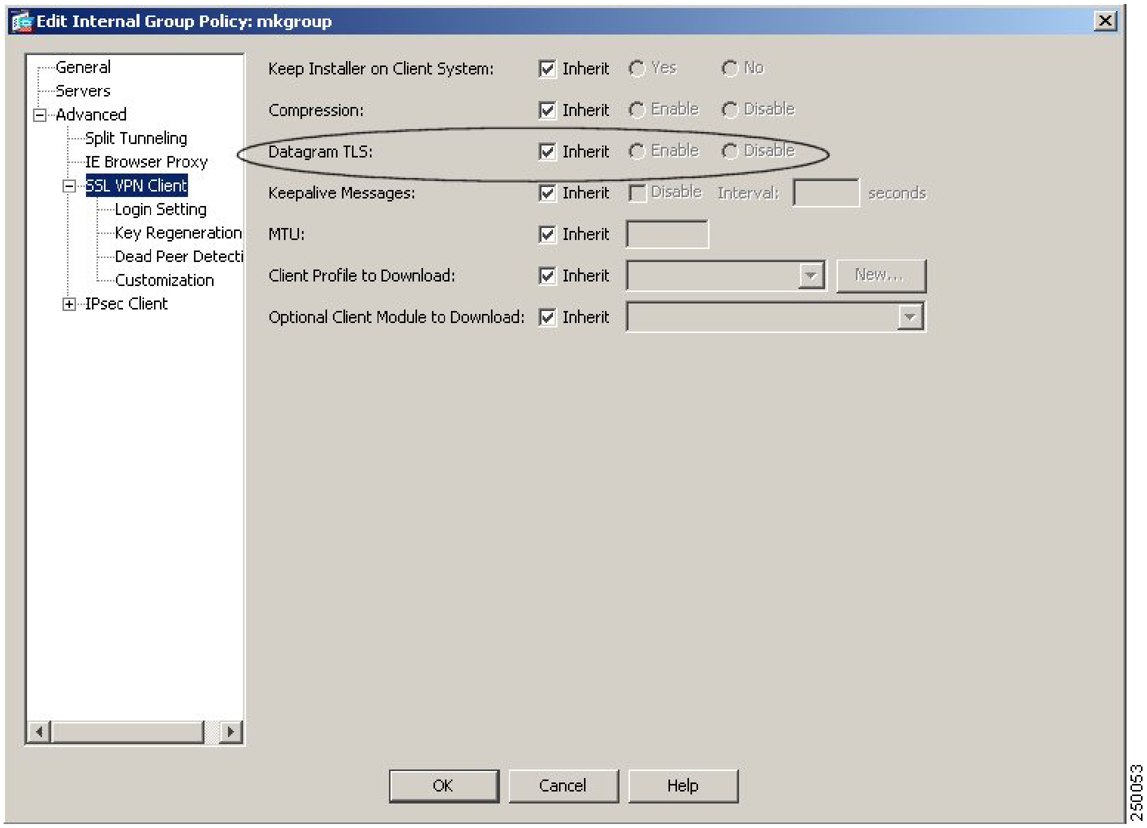
Enabling DTLS allows the AnyConnect client establishing an AnyConnect VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect only with an SSL VPN tunnel. To enable DTLS, use the Datagram TLS setting in either Group Policy or Username. The paths to this setting are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

Figure 5-2 shows an example of configuring the DTLS setting for an internal group policy.

Figure 5-2 Enabling or Disabling DTLS



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

Client Profile to Download: ☑ Inherit New...

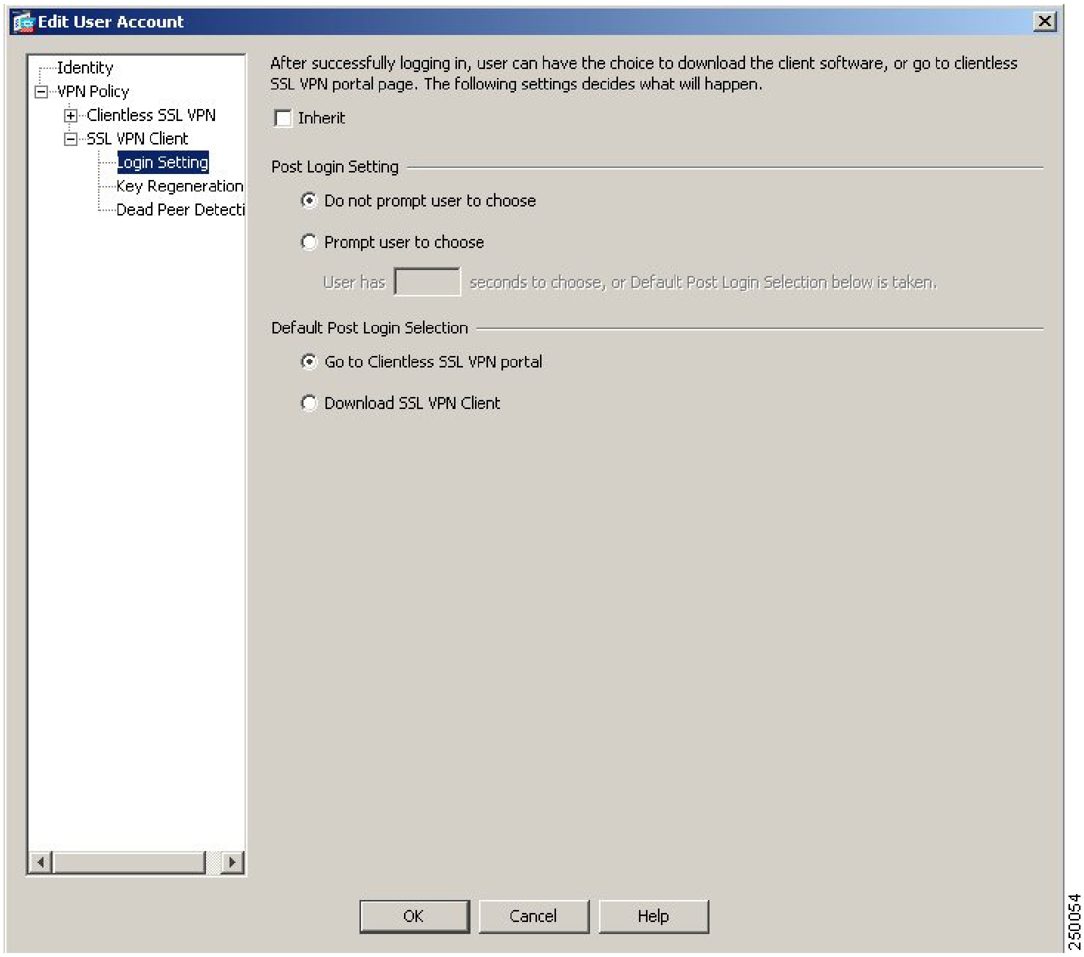
Optional Client Module to Download: ☑ Inherit

Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection must be enabled in the group policy on the security appliance 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 UPD/DTLS session, and the DPD mechanism is necessary for fallback to occur.

Prompting Remote Users

To enable the security appliance to prompt remote AnyConnect VPN client users to download the client, select Configuration > Device Management > Users/AAA > User Accounts > Add or Edit. The Add or Edit dialog box appears. In the navigation panel on the left, select VPN Policy > SSL VPN Client > Login Setting (Figure 5-3).

Figure 5-3 Edit User Account Dialog Box for Prompt Setting



Edit User Account

After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN portal page. The following settings decides what will happen.

□ Inherit

Post Login Setting

● Do not prompt user to choose

○ Prompt user to choose

User has [ ] seconds to choose, or Default Post Login Selection below is taken.

Default Post Login Selection

● Go to Clientless SSL VPN portal

○ Download SSL VPN Client

Deselect the Inherit check box, if necessary, and in the Post Login Setting area, select the option Prompt user to choose. To disable this option, select Do not prompt user to choose.

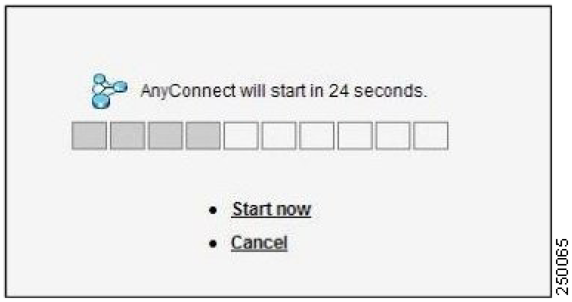
When you enable the prompting option, another field becomes available, asking you to specify the number of seconds the user has to choose before the Default Post Login selection takes effect.

Select the Default Post Login selection to specify the action that the AnyConnect client takes if the user does not make a selection before the timer specified in the prompting option expires. The options are:

- Go to Clientless SSL VPN Portal—Immediately displays the portal page for Clientless SSL VPN. The user can still invoke the AnyConnect client from the portal by clicking Start AnyConnect Client.
- Download SSL VPN Client—Immediately starts downloading the AnyConnect client to the remote user’s PC.

Figure 5-4 shows the prompt displayed to remote users when either the default svc timeout value or the default webvpn timeout value is configured (in this case, the timeout was set to 35 seconds):

Figure 5-4 Prompt Displayed to Remote Users for SSL VPN Client Download



AnyConnect will start in 24 seconds.

- Start now
- Cancel

Enabling IPv6 VPN Access

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

For more information about enabling IPv6, see Chapter 6, "Configuring AnyConnect Features Using CLI."

Enabling Modules for Additional AnyConnect Features

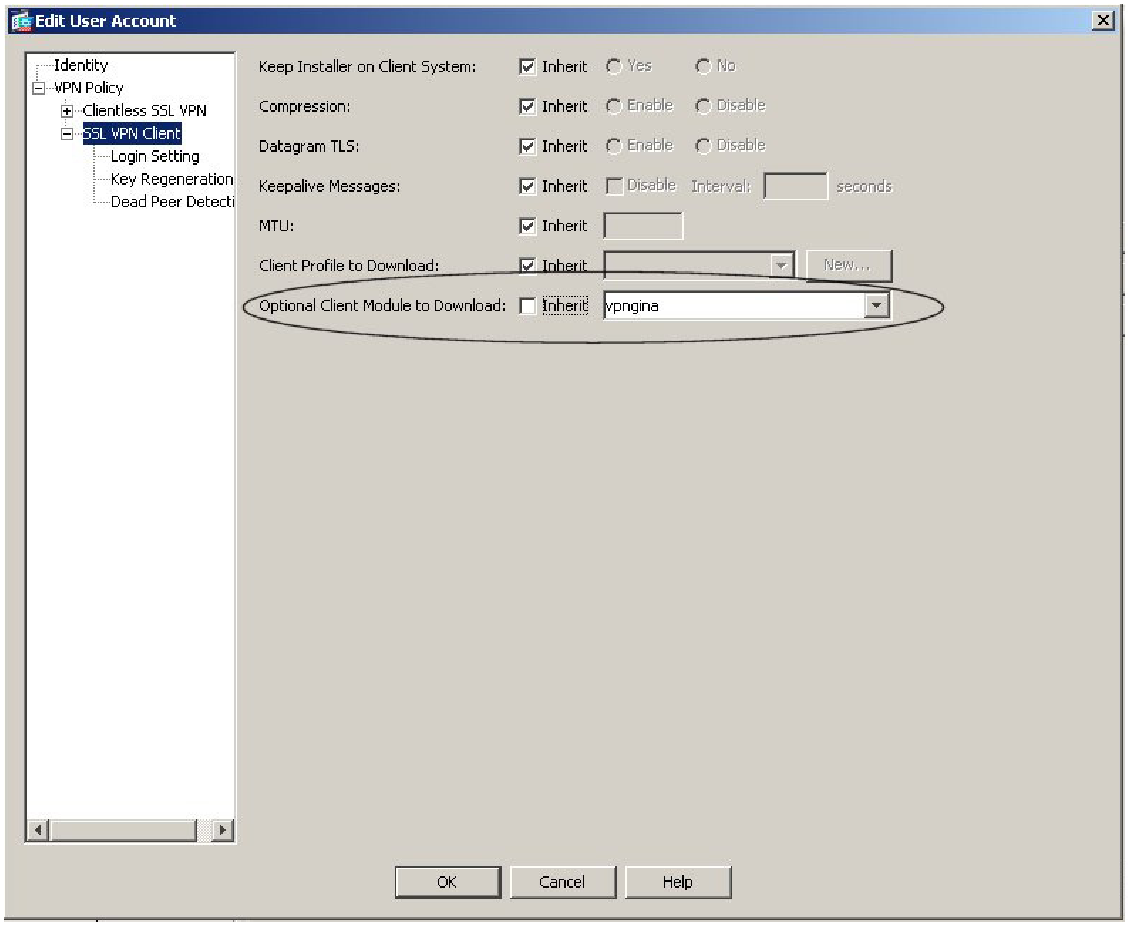
As new features are released for the AnyConnect client, you must update the AnyConnect clients of your remote users for them to use the new features. To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of modules that it needs for each feature that it supports.

To enable new features, you must specify the new module names as part of the group-policy or username configuration. Possible paths to the dialog box where you can specify these modules are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- Device management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client.

Specify the module name, for example, **sbl** for the Start Before Logon feature, in the Optional Client Module to Download field. Separate multiple strings with commas. Figure 5-5 shows an example.

Figure 5-5 Optional Client Module to Download



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

Client Profile to Download: ☑ Inherit New...

Optional Client Module to Download: □ Inherit vpngina

In the case of Start Before Logon, you must also enable the feature in the XML profile.

For a list of values to enter for each AnyConnect client feature, see the Release Notes for the Cisco AnyConnect VPN Client.

Configuring, Enabling, and Using Other AnyConnect Features

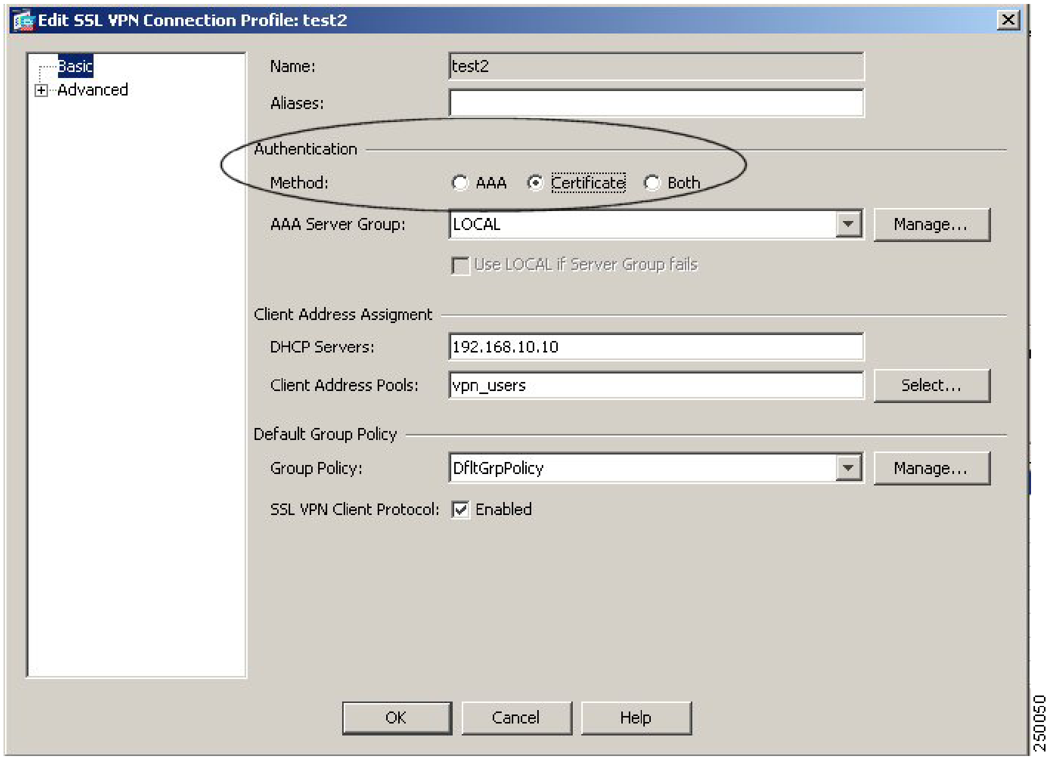
The following sections describe how to configure other AnyConnect features. Some features, such as Secure Desktop and dynamic access policies, do not require that you specifically configure the AnyConnect client to interact with that feature. Rather, all configuration for those features occurs on the security appliance or within the respective software packages.

Configuring Certificate-only Authentication

You can specify whether you want users to authenticate using AAA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with digital certificate and are not required to provide a user ID and password.

To configure certificate-only authentication using ASDM, select Configuration > Remote Access > Network (Client) Access > SSL VPN Connection Profiles, and in the Connection Profiles area, select Add or Edit. This displays the Add or Edit SSL VPN Connect Profile dialog box with the Basic option selected. In the Authentication area, select only Certificate as the Method.

Figure 5-6 Configuring Certificate-Only Authentication, Edit SSL VPN Dialog Box



Edit SSL VPN Connection Profile: test2

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

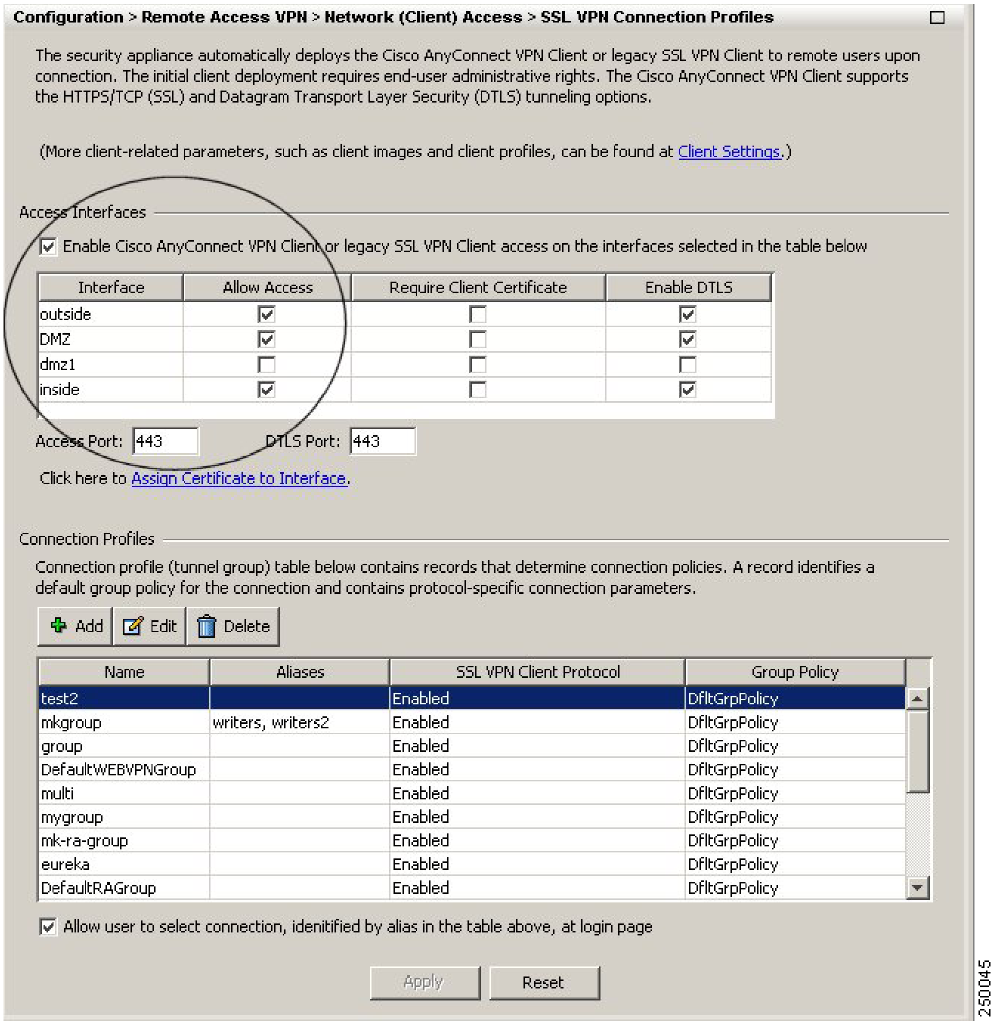
Default Group Policy

Group Policy: DfltGrpPolicy

SSL VPN Client Protocol: ☑ Enabled

To make this feature take effect, you must also enable AnyConnect client access on particular interfaces and ports, as needed. To do this, select Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles. The SSL VPN Connection Profiles dialog box (Figure 5-7) appears.

Figure 5-7 SSL VPN Connection Profiles Dialog 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.

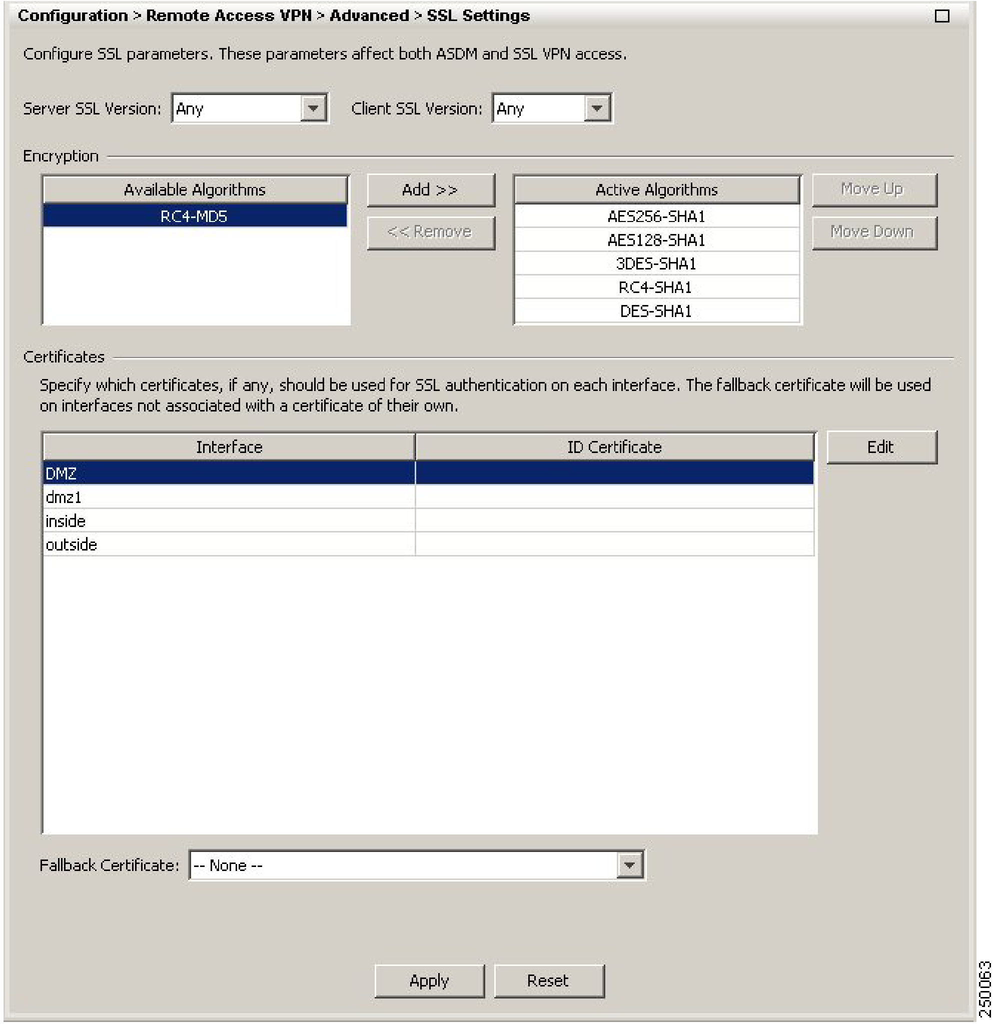
Name	Aliases	SSL VPN Client Protocol	Group Policy
test2		Enabled	DfltGrpPolicy
mkgroup	writers, writers2	Enabled	DfltGrpPolicy
group		Enabled	DfltGrpPolicy
DefaultWEBVPNGroup		Enabled	DfltGrpPolicy
multi		Enabled	DfltGrpPolicy
mygroup		Enabled	DfltGrpPolicy
mk-ra-group		Enabled	DfltGrpPolicy
eureka	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

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

In the Access Interfaces area, select the check box Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below. Then select the check boxes for the interfaces on which you want to enable access. Specify the Access Port. The default access port is 443.

If you want to assign a specific certificate to an interface, click Assign Certificate to Interface. This opens the SSL Settings dialog box (Figure 5-8).

Figure 5-8 SSL Settings Dialog Box



Configuration > Remote Access VPN > Advanced > SSL Settings

Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

Server SSL Version: Any Client SSL Version: Any

Encryption

Available Algorithms	Active Algorithms
RC4-MD5	AES256-SHA1
	AES128-SHA1
	3DES-SHA1
	RC4-SHA1
	DES-SHA1

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	ID Certificate
DMZ	
dmz1	
inside	
outside	

Fallback Certificate: -- None --

In the Certificates area, specify which certificates, if any, you want to use for SSL authentication on each interface. If you do not specify a certificate for a particular interface, the fallback certificate will be used. In the Fallback Certificate field, select a certificate from the drop-down list. The default is --None--.

Using Compression

On low-bandwidth connections, compression increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred. By default, compression for all SSL VPN connections is enabled on the security appliance, both at the global level and for specific groups or users. For broadband connections, compression might result in poorer performance.

By default, if you have not changed the compression setting globally, compression is enabled. You can configure compression globally using the CLI command **compression svc** command from global configuration mode.

Changing Compression Globally

To change the global compression settings, use the **compression svc** command from global configuration mode:

compression svc

no compression svc

To remove the command from the configuration, use the **no** form of the command.

In the following example, compression is disabled for all SSL VPN connections globally:

```
hostname(config)# no compression svc
```

Changing Compression for Groups and Users

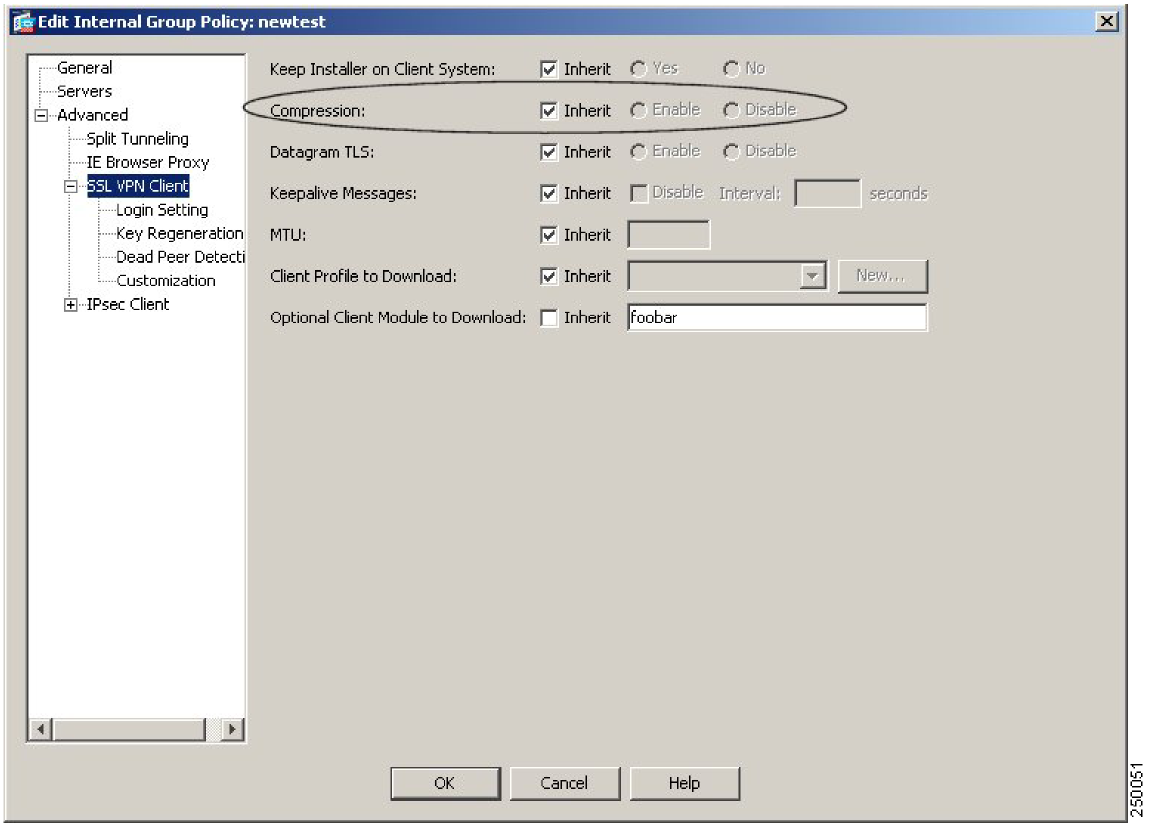
You can also configure compression for specific groups or users using ASDM with the **svc compression** command in group-policy and username webvpn modes. The global setting overrides the group-policy and username settings.

To change compression for a specific group or user, use the Compression setting in either Group Policy or Username. You can get to this setting through any of the following paths:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

Figure 5-9 shows an example of configuring the compression setting for an internal group policy.

Figure 5-9 Compression Setting



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

Client Profile to Download: ☑ Inherit New...

Optional Client Module to Download: □ Inherit foobar

By default, for groups and users, SSL compression is set to Inherit. If you deselect Inherit, the default is enabled (equivalent to *deflate* in the CLI).

Note For compression to work, it must be enabled both globally (by the **compression svc** command configured from global configuration mode) and for the specific group policy or username. If *either* is set to disable (or to the **none** or the **no** form of the command), compression is disabled.

Enabling AnyConnect Keepalives

You can adjust the frequency of keepalive messages to ensure that an AnyConnect client or SSL VPN 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 frequency 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.

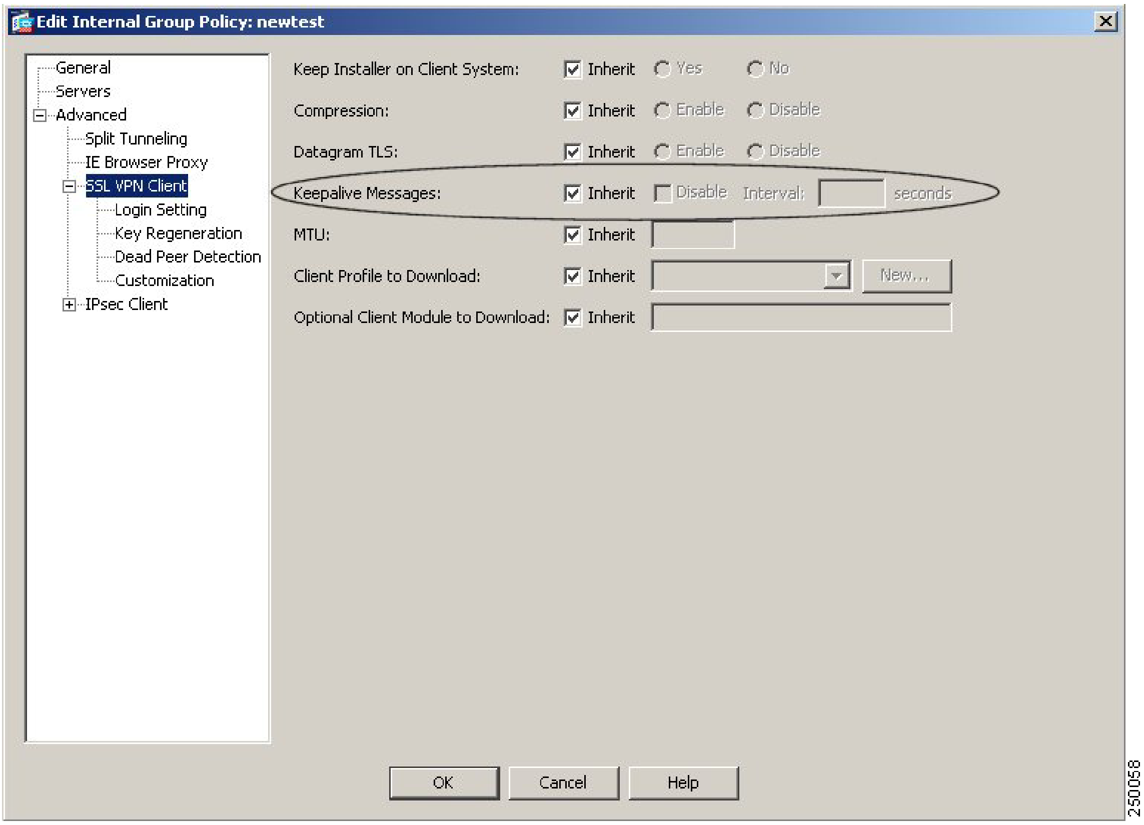
To set the frequency of keepalive messages, use the Keepalive Messages setting in either Group Policy or Username. The paths to this setting are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

Figure 5-10 shows an example of configuring the keepalive messages setting for an internal group policy.

Figure 5-10 Configuring Keepalive Messages



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

Client Profile to Download: ☑ Inherit

Optional Client Module to Download: ☑ Inherit

Configure the Keepalive Messages field for this attributeby deselecting Inherit and entering a 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.

Enabling AnyConnect Rekey

Configuring AnyConnect Rekey specifies that SSL renegotiation takes place during rekey. When the security appliance and the SSL VPN client perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

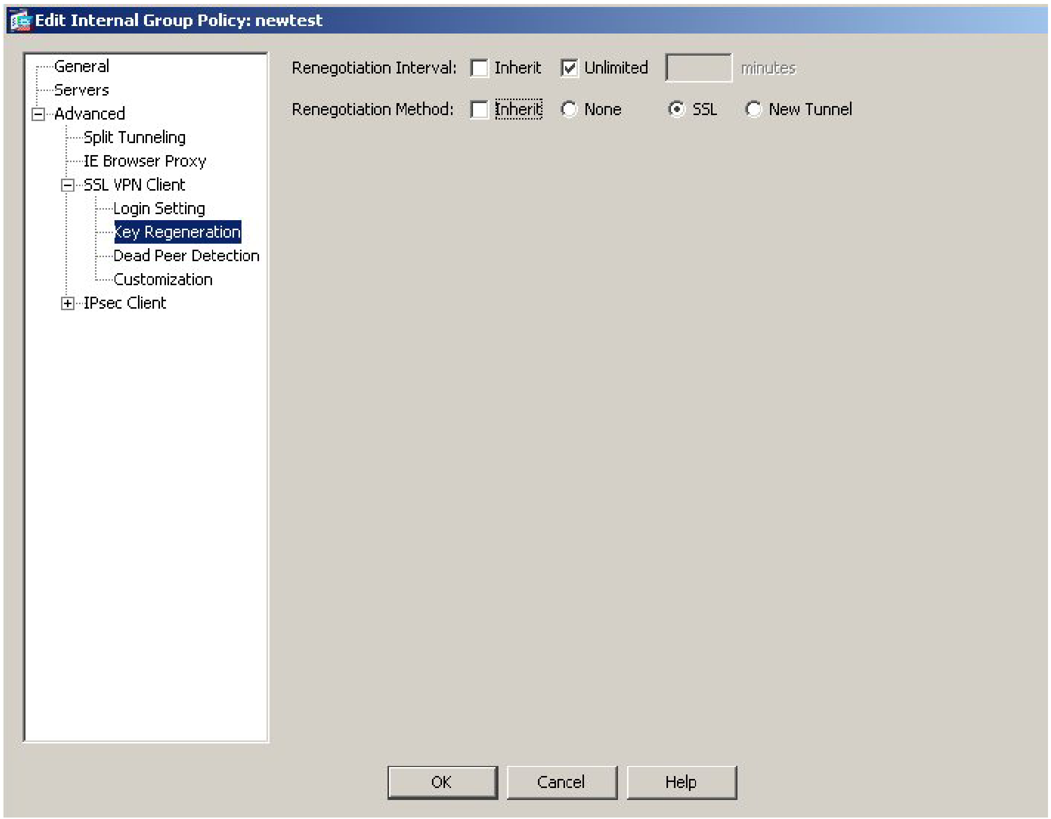
To enable Rekey, use the Key Regeneration dialog box in either Group Policy or Username. The paths to this setting are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client > Key Regeneration

- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client > Key Regeneration
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client > Key Regeneration

Figure 5-11 shows an example of configuring the Rekey setting for an internal group policy.

Figure 5-11 Configuring Rekey Attributes



Edit Internal Group Policy: newtest

Renegotiation Interval: □ Inherit ☑ Unlimited minutes

Renegotiation Method: □ Inherit ○ None ● SSL ○ New Tunnel

Key renegotiation occurs when the security appliance and the client perform a rekey and they renegotiate the crypto keys and initialization vectors, increasing the security of the connection. The fields on this dialog box are as follows:

- Renegotiation Interval—Clear the Unlimited check box to specify the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).
- Renegotiation Method—Check the None check box to disable rekey, check the SSL check box to specify SSL renegotiation during a rekey, or check the New Tunnel check box to establish a new tunnel during rekey.

Note The security appliance does not currently support inline DTLS rekey. The AnyConnect client, therefore, treats all DTLS rekey events as though they were of the new tunnel method instead of the inline ssl type (CSCsh93610).

Enabling and Adjusting Dead Peer Detection

Dead Peer Detection (DPD) ensures that the security appliance (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed.

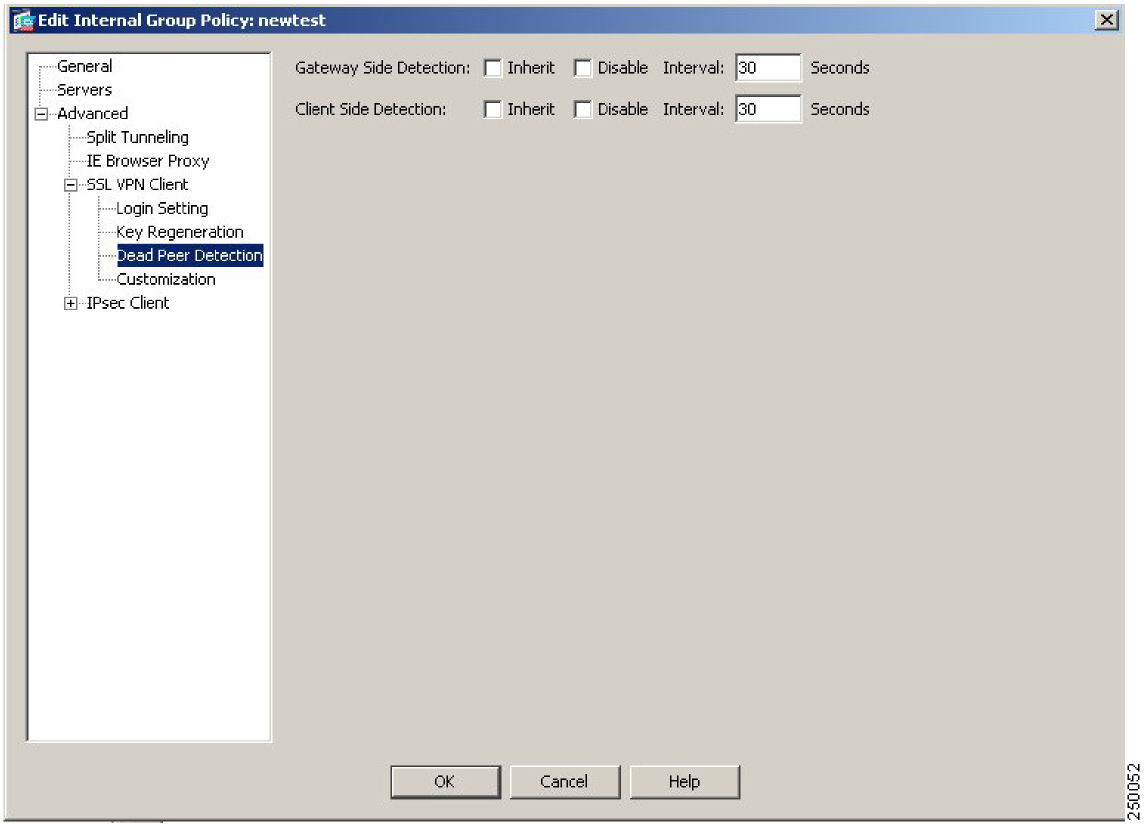
Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection must be enabled in the group policy on the security appliance to allow the AnyConnect client to fall back to TLS, if necessary. Fallback to TLS occurs if the AnyConnect client cannot send data over the UPD/DTLS session, and the DPD mechanism is necessary for fallback to occur.

To enable DPD on the security appliance or client for a specific group or user, and to set the frequency with which either the security appliance or client performs dead-peer detection, use the Dead Peer Detection dialog box for either group-policy or username. The paths to this setting are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client > Dead Peer Detection
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client > Dead Peer Detection
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client > Dead Peer Detection

Figure 5-12 shows an example of configuring the Dead Peer Detection setting for an internal group policy.

Figure 5-12 Enabling or Disabling Dead Peer Detection



Edit Internal Group Policy: newtest

Gateway Side Detection: □ Inherit □ Disable Interval: 30 Seconds

Client Side Detection: □ Inherit □ Disable Interval: 30 Seconds

In this dialog box, you can set the following attributes:

- Gateway Side Detection—Deselect the Disable check box to specify that dead-peer detection is performed by the *security appliance* (gateway). Enter the interval, from 30 to 3600 seconds, with which the security appliance performs dead-peer detection.
- Client Side Detection—Deselect the Disable check box to specify that dead-peer detection is performed by the *client*. Enter the interval, from 30 to 3600 seconds, with which the client performs dead-peer detection.

Configuring the Dynamic Access Policies Feature of the Security Appliance

On the security appliance, you can configure authorization that addresses the variables of multiple group membership and endpoint security for VPN connections. There is no specific configuration of AnyConnect required to use dynamic access policies. For detailed information about configuring dynamic access policies, see *Cisco ASDM User Guide, Cisco Security Appliance Command Line Configuration Guide,* or *Cisco Security Appliance Command Reference.*

Cisco Secure Desktop Support

Cisco Secure Desktop validates the security of client computers requesting access to your SSL VPN, helps ensure they remain secure while they are connected, and attempts to remove traces of the session after they disconnect. The Cisco AnyConnect VPN Client supports the Secure Desktop functions of

Cisco Secure Desktop for Windows 2000 and Windows XP. There is no specific configuration of AnyConnect required to use Secure Desktop. For detailed information about configuring Cisco Secure Desktop, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators (Software Release 3.2)*.

CHAPTER 6

Configuring AnyConnect Features Using CLI

The AnyConnect client includes the following features, which you configure on the security appliance:

Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections

Datagram Transport Layer Security avoids latency and bandwidth problems associated with some SSL-only connections, including AnyConnect 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).

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.

If you do not enable DTLS, SSL VPN connections connect with an SSL VPN tunnel only.

Enabling DTLS Globally for a Specific Port

To enable DTLS globally for a particular port, use the **dtls port** command:

[no] dtls port *port_number*

For example:

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

Enabling DTLS for Specific Groups or Users

To enable DTLS for specific groups or users, use the **svc dtls enable** command in group policy webvpn or username webvpn configuration mode:

[**no**] **svc dtls enable**

If DTLS is configured and UDP is interrupted, the remote user's connection automatically falls back from DTLS to TLS. The default is enabled; however, DTLS is not enabled by default on any individual interface.

Enabling DTLS allows the AnyConnect client establishing an AnyConnect 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.

If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect only with an SSL VPN tunnel.

The following example enters group policy webvpn configuration mode for the group policy *sales* and enables DTLS:

```
hostname(config)# enable inside
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dtls enable
```

Prompting Remote Users

You can enable the security appliance to prompt remote AnyConnect 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 WebVPN portal page and waits indefinitely for user response.

svc ask enable default svc immediately downloads the client.

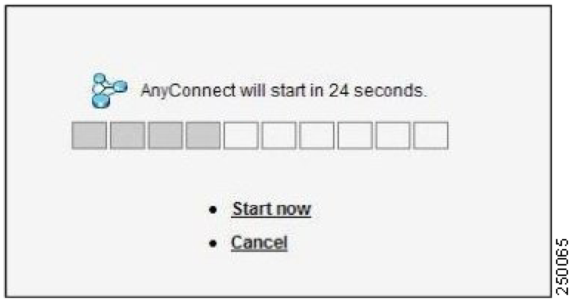
svc ask enable default webvpn immediately goes to the portal page.

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

Figure 6-1 shows the prompt displayed to remote users when either **default svc timeout** *value* or **default webvpn timeout** *value* is configured:

Figure 6-1 Prompt Displayed to Remote Users for SSL VPN Client Download



AnyConnect will start in 24 seconds.

- Start now
- Cancel

The following example configures the security appliance to prompt the remote user to download the client or go to the WebVPN 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 IPv6 VPN Access

The AnyConnect client allows access to IPv6 resources over a public IPv4 connection (Windows XP SP2, Windows Vista, Mac OSX, and Linux only). You must use the command-line interface to configure IPv6; 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
```

Enabling Modules for Additional AnyConnect Features

As new features are released for the AnyConnect client, you must update the AnyConnect clients of your remote users for them to use the new features. To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of modules that it needs for each feature that it supports. To enable new features, you must specify the new module names using the **svc modules** command from group policy webvpn or username webvpn configuration mode:

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

Separate multiple strings with commas.

For a list of values to enter for each AnyConnect client feature, see the release notes for the Cisco AnyConnect VPN Client.

In the following example, the network administrator 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 the AnyConnect client feature Start Before Login:

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

Configuring, Enabling, and Using Other AnyConnect Features

The following sections describe how to configure other AnyConnect features. Some features, such as Secure Desktop and dynamic access policies, do not require that you specifically configure the AnyConnect client to interact with that feature. Rather, all configuration for those features occurs on the security appliance or within the software package itself.

Configuring Certificate-only Authentication

You can specify whether you want users to authenticate using AAA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with digital certificate and are not required to provide a user ID and password. To configure certificate-only authentication using CLI, use the **authentication** command with the keyword **certificate** in tunnel-group webvpn mode. For example:

```
hostname(config)# tunnel-group testgroup webvpn-attributes
asa2(config-tunnel-webvpn)# authentication ?
asa2(config-tunnel-webvpn)# authentication certificate
```

Note You must configure **ssl certificate-authentication interface** <*interface*> **port** <*port*> for this option to take effect.

To configure certificate-only authentication using ASDM, select Configuration > Remote Access > Network (Client) Access > SSL VPN Connection Profiles, and in the Connection Profiles area, select Add or Edit. This displays the Add or Edit SSL VPN Connect Profile dialog box with the Basic option selected. In the Authentication area, specify only Certificate as the Method.

Using Compression

On low-bandwidth connections, compression increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred. By default, compression for all SSL VPN connections is enabled on the security appliance, both at the global level and for specific groups or users. For broadband connections, compression might result in poorer performance.

You can configure compression globally using the **compression svc** command from global configuration mode. You can also configure compression for specific groups or users with the **svc compression** command in group-policy and username webvpn modes. The global setting overrides the group-policy and username settings.

Changing Compression Globally

To change the global compression settings, use the **compression svc** command from global configuration mode:

compression svc

no compression svc

To remove the command from the configuration, use the **no** form of the command.

In the following example, compression is disabled for all SSL VPN connections globally:

```
hostname(config)# no compression svc
```

Changing Compression for Groups and Users

To change compression for a specific group or user, use the **svc compression** command in the group-policy and username webvpn modes:

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

By default, for groups and users, SSL compression is set to *deflate* (enabled).

To remove the **svc compression** command from the configuration and cause the value to be inherited from the global setting, use the **no** form of the command:

The following example disables compression for the group-policy sales:

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

Note For compression to work, both the **compression svc** command (configured from global configuration mode) and the **svc compression** command (configured in group-policy and username webvpn modes) must be enabled. If *either* command is set to **none** or to the **no** form, compression is disabled.

Configuring the Dynamic Access Policies Feature of the Security Appliance

On the security appliance, you can configure authorization that addresses the variables of multiple group membership and endpoint security for VPN connections. There is no specific configuration of AnyConnect required to use dynamic access policies. For detailed information about configuring dynamic access policies, see *Cisco ASDM User Guide, Cisco Security Appliance Command Line Configuration Guide,* or *Cisco Security Appliance Command Reference.*

Cisco Secure Desktop Support

Cisco Secure Desktop validates the security of client computers requesting access to your SSL VPN, helps ensure they remain secure while they are connected, and attempts to remove traces of the session after they disconnect. The Cisco AnyConnect VPN Client supports the Secure Desktop functions of Cisco Secure Desktop for Windows 2000 and Windows XP. There is no specific configuration of AnyConnect required to use Secure Desktop. For detailed information about configuring Cisco Secure Desktop, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators (Software Release 3.2).*

Enabling AnyConnect Rekey

Configuring AnyConnect Rekey specifies that SSL renegotiation takes place during rekey.

When the security appliance and the SSL VPN 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 or from the last rekey until the next 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
```

Note The security appliance does not currently support inline DTLS rekey. The AnyConnect client, therefore, treats all DTLS rekey events as though they were of the new tunnel method instead of the inline ssl type (CSC93610).

Enabling and Adjusting Dead Peer Detection

Dead Peer Detection (DPD) ensures that the security appliance (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed.

Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection 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 UPD/DTLS session, and the DPD mechanism is necessary for fallback to occur.

To enable DPD on the security appliance or client for a specific group or user, and to set the frequency with which either the security appliance or client performs DPD, use the **svc dpd-interval** command from group-policy or username webvpn mode:

svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

Where:

gateway seconds enables DPD performed by the security appliance (gateway) and specifies the frequency, from 30 to 3600 seconds, with which the security appliance (gateway) performs DPD.

gateway none disables DPD performed by the security appliance.

client *seconds* enable DPD performed by the client, and specifies the frequency, from 30 to 3600 seconds, with which the client performs DPD.

client none disables DPD performed by the client.

To remove the **svc dpd-interval** command from the configuration, use the **no** form of the command:

The following example sets the frequency of DPD performed by the security appliance to 30 seconds, and the frequency of DPD performed by the client set to 10 seconds for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc dpd-interval gateway 30
hostname(config-group-policy)# svc dpd-interval client 10
```

Enabling AnyConnect Keepalives

You can adjust the frequency of keepalive messages to ensure that an AnyConnect client or SSL VPN 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 frequency 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.

To set the frequency of keepalive messages, use the **svc keepalive** command from group-policy webvpn or username webvpn configuration mode:

[**no**] **svc keepalive {none |** *seconds***}**

none disables client keepalive messages.

seconds enables the client to send keepalive messages, and specifies the frequency of the messages in the range of 15 to 600 seconds.

The default is keepalive messages are disabled.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

In the following example, the security appliance is configured to enable the client to send keepalive messages with a frequency of 300 seconds (5 minutes), for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

CHAPTER 7

Configuring and Using AnyConnect Client Operating Modes and User Profiles

AnyConnect Client Operating Modes

The user can use the AnyConnect Client in the following modes:

- Standalone mode—Lets the user establish a Cisco AnyConnect VPN client connection without the need to use a web browser. If you have permanently installed the AnyConnect client on the user's PC, the user can run in standalone mode. In standalone mode, a user opens the AnyConnect client just like any other application and enters the username and password credentials into the fields of the AnyConnect GUI. Depending on ho w you configure the system, the user might also be required to select a group. When the connection is established, the security appliance checks the version of the client on the user's PC and, if necessary, downloads the latest version.
- WebLaunch mode—Lets the user enter the URL of the security appliance in the Address or Location field of a browser using the https protocol. The user then enters the username and password information on a Logon screen and selects the group and clicks submit. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking Continue.

  The portal window appears. To start the AnyConnect client, the user clicks Start AnyConnect on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities.

Using the AnyConnect CLI Commands to Connect (Standalone Mode)

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 and Mac OS X

To launch the CLI command prompt and issue commands on a Linux or Mac OS X 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 7-1 shows the CLI commands.

Table 7-1 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.
stats	Displays statistics about an established connection.
quit	Exits the CLI interactive mode.
exit	Exits the CLI interactive mode.

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

Windows

connect 209.165.200.224

Establishes a connection to a security appliance with the address 209.165. 200.224. After contacting the requested host, the AnyConnect client displays the group to which the user belongs and asks for the user's username and password. If you have specified that an optional banner be displayed, the user must respond to the banner. The default response is **n**, which terminates the connection attempt. For example:

```
VPN> connect 209.165.200.224
    >>contacting host (209.165.200.224) for login information...
    >>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
    >>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour. The system will not be available during that time.

accept? [y/n] y
    >> notice: Authentication succeeded. Checking for updates...
    >> state: Connecting
    >> notice: Establishing connection to 209.165.200.224.
    >> State: Connected
    >> notice: VPN session established.
VPN>
```

stats

Displays statistics for the current connection; for example:

```
VPN> stats
[ Tunnel Information ]

    Time Connected:01:17:33
    Client Address:192.168.23.45
    Server Address:209.165.200.224

[ Tunnel Details ]

    Tunneling Mode:All Traffic
    Protocol: DTLS
    Protocol Cipher: RSA_AES_256_SHA1
    Protocol Compression: None
```

```
[ Data Transfer ]

    Bytes(sent/received): 1950410/23861719
    Packets (sent/received): 18346/28851
    Bypassed (outbound/inbound): 0/0
    Discarded (outbound/inbound): 0/0

[ Secure Routes ]

    Network     Subnet
    0.0.0.0     0.0.0.0
VPN>
```

disconnect
Closes a previously established connection; for example:

```
VPN> disconnect
    >> state: Disconnecting
    >> state: Disconnected
    >> notice: VPN session ended.
VPN>
```

quit or **exit**

Either command exits the CLI interactive mode; for example:

```
quit
goodbye
    >>state: Disconnected
```

Linux or Mac OS X

/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.

Connecting Using WebLaunch

The Cisco AnyConnect VPN Client provides a browser interface for users who prefer to a graphical user interface. *WebLaunch* mode lets the user enter the URL of the security appliance in the Address or Location field of a browser using the https protocol. For example:

https://209.165.200.225

The user then enters the username and password information on a Logon screen and selects the group and clicks submit. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking Continue.

The portal window appears. To start the AnyConnect client, the user clicks Start AnyConnect on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities.

Note For Windows Vista users who use the Internet Explorer browser, you must add the security appliance to the list of trusted sites, as described in Adding a Security Appliance to the List of Trusted Sites (Internet Explorer), page 2-3.

User Log In and Log Out

You might find it useful to provide the following instructions to your remote users.

Logging In

Your system administrator has assigned you a remote access username and password. Before you log in, you must get this information from your system administrator.

Step 1 Enter your remote access username in the Username field.

Step 2 Enter your remote access password in the Password field.

Step 3 Click Login.

Step 4 If you receive a certificate warning, install the certificate.

Your remote access home page appears.

Logging Out

To end your remote access session, click the "Close Window" (X) icon in the toolbar or click the Logout link. The Logout page appears, confirming that your session has been terminated and offering you the opportunity to log in again.

Quitting the browser also logs out the session.

Caution *Security note:* Always log out when you finish your session. Logging out is especially important when you are using a public computer such as in a library or Internet cafe. If you do not log out, someone who uses the computer next could access your files. Don't risk the security of your organization! Always log out.

Configuring and Using User Profiles

An AnyConnect client user profile is an XML file that lets you identify the secure gateway (security appliance) hosts that you want to expose to the user community. In addition, the profile conveys additional connection attributes and constraints on a user.

Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and additional settings as needed. In some cases, you might want to provide more than one profile for a given user. For example, someone who works from multiple locations might need more than one profile. In such cases, the user selects the appropriate profile from a drop-down list. Be aware, however, that some of the profile settings, such as Start Before Login, control the connection experience at a global level. Other settings, such as those unique to a particular host, depend on the host selected.

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 users's PC, so you must first import the profile(s) into the security appliance in preparation for downloading to the remote PC. You can import a profile using either ASDM or the command-line interface. See Appendix A, "Sample AnyConnect Profile and XML Schema" 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>\Local Settings\Application Data\Cisco\Cisco AnyConnect VPN Client.

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

You can place a copy of your profile (for example, CiscoAnyConnectProfile.xml) in the directory: C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile The location for Windows Vista is slightly different: C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile The host that appears in the Connect to combo box is the first one listed in the profile or the last host you successfully connected with.

Caution Do not cut and paste the examples from this document. Doing so introduces line breaks that can break your XML. Instead, open the profile template file in a text editor such as notepad or wordpad.

Use the template that appears after installing AnyConnect on a workstation:
\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\AnyConnectProfile.tmpl

Follow these steps to edit profiles and use ASDM to enable the security appliance to download them to remote clients:

Step 1 Retrieve a copy of the profiles file (AnyConnectProfile.xml) from a client installation. Table 7-2 shows the installation path for each operating system.

Table 7-2 Operating System and Profile File Installation Path

Operating System	Installation Path
Windows	%PROGRAMFILES%\Cisco\Cisco AnyConnect VPN Client\[1]
Linux	/opt/cisco/vpn/profile
Mac OS X	/opt/cisco/vpn/profile

[1] %PROGRAMFILES% refers to the environmental variable by the same name. In most Windows installation, this is C:\Program Files.

Step 2 Edit the profiles file. The example below shows the contents of the profiles file (AnyConnectProfile.xml) for Windows:

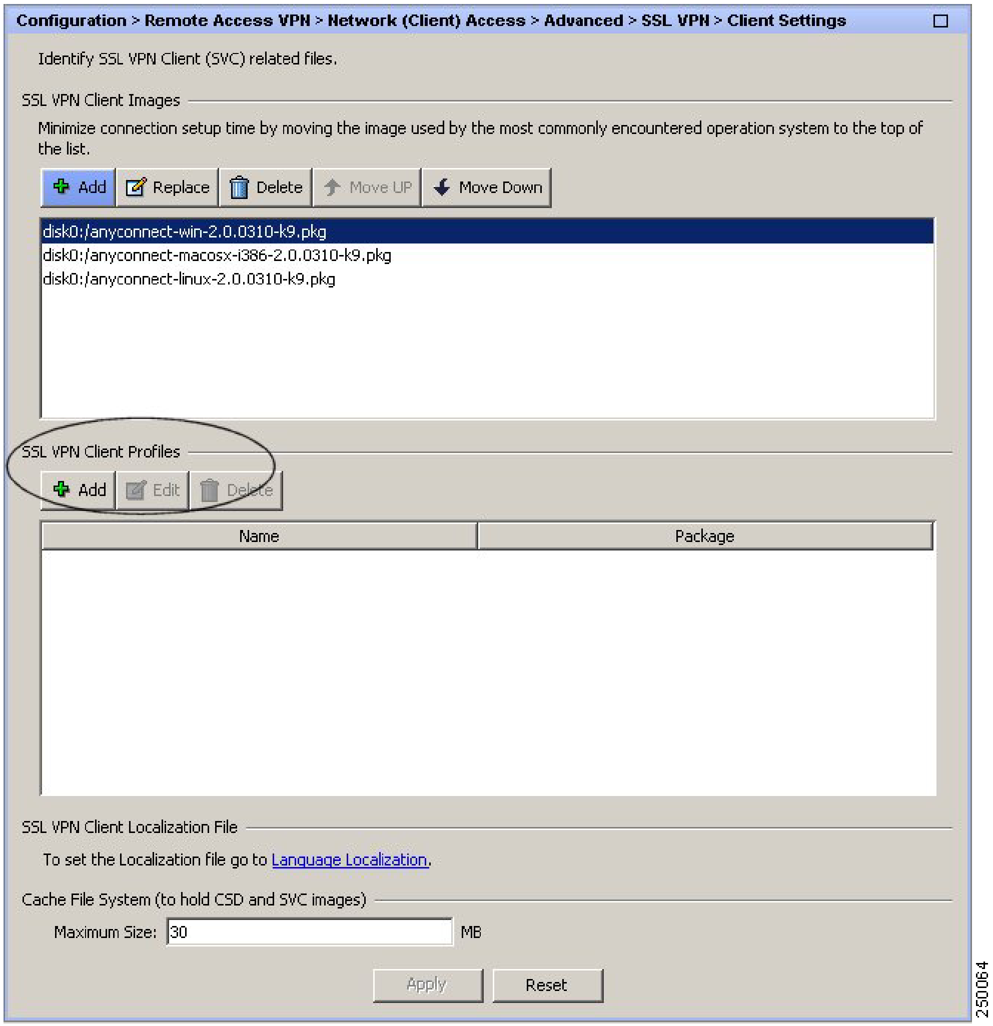
```
<?xml version="1.0" encoding="UTF-8"?>
<!--
    This is a template file that can be configured to support the
    identification of secure hosts in your network.

    The file needs to be renamed to CiscoAnyConnectProfile.xml.

    The svc profiles command imports updated profiles for downloading to
    client machines.
-->
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
    </ClientInitialization>
    <HostProfile>
        <HostName></HostName>
        <HostAddress></HostAddress>
    </HostProfile>
    <HostProfile>
        <HostName></HostName>
        <HostAddress></HostAddress>
    </HostProfile>
</Configuration>
```

The <HostProfile> tags are frequently edited so that the AnyConnect client displays the names and addresses of host computers for remote users. The following example shows the <HostName> and <HostAddress> tags, with the name and address of a host computer inserted:

```
    <HostProfile>
        <HostName>Sales_gateway</HostName>
        <HostAddress>209.165.200.225</HostAddress>
    </HostProfile>
```

Step 3 To identify to the security appliance the client profiles file to load into cache memory, select Configuration > Remote Access VPN > Network (Client) Access > Advanced > Client Settings (Figure 7-1).

Figure 7-1 Adding or Editing an AnyConnect VPN Client Profile



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

Name	Package

SSL VPN Client Localization File

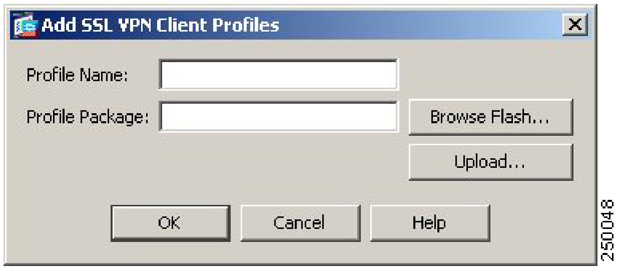
To set the Localization file go to Language Localization.

Cache File System (to hold CSD and SVC images)

Maximum Size: 30 MB

In the SSL VPN Client Profiles area, click Add or Edit. the Add or Edit SSL VPN Client Profiles dialog box appears (Figure 7-2).

Figure 7-2 Add (or Edit) SSL VPN Client Profiles Dialog Box



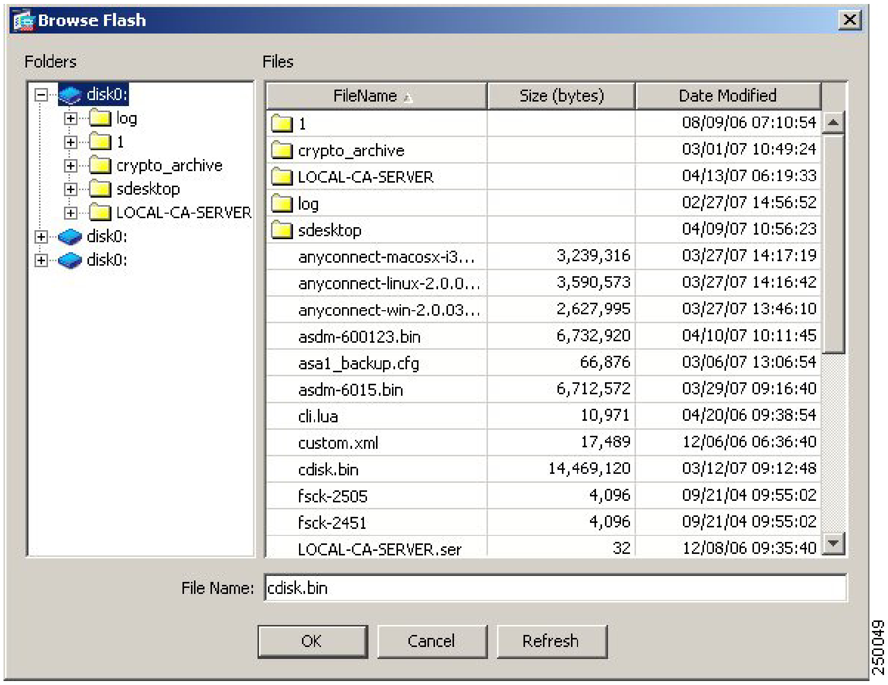
Add SSL VPN Client Profiles

Profile Name:

Profile Package:

Enter the profile name and profile package names in their respective fields. To browse for a profile package name, click Browse Flash. The Browse Flash dialog box appears (Figure 7-3).

Figure 7-3 Browse Flash Dialog Box



- disk0:
  - log
  - 1
  - crypto_archive
  - sdesktop
  - LOCAL-CA-SERVER
- disk0:
- disk0:

FileName	Size (bytes)	Date Modified
1		08/09/06 07:10:54
crypto_archive		03/01/07 10:49:24
LOCAL-CA-SERVER		04/13/07 06:19:33
log		02/27/07 14:56:52
sdesktop		04/09/07 10:56:23
anyconnect-macosx-i3...	3,239,316	03/27/07 14:17:19
anyconnect-linux-2.0.0...	3,590,573	03/27/07 14:16:42
anyconnect-win-2.0.03...	2,627,995	03/27/07 13:46:10
asdm-600123.bin	6,732,920	04/10/07 10:11:45
asa1_backup.cfg	66,876	03/06/07 13:06:54
asdm-6015.bin	6,712,572	03/29/07 09:16:40
cli.lua	10,971	04/20/06 09:38:54
custom.xml	17,489	12/06/06 06:36:40
cdisk.bin	14,469,120	03/12/07 09:12:48
fsck-2505	4,096	09/21/04 09:55:02
fsck-2451	4,096	09/21/04 09:55:02
LOCAL-CA-SERVER.ser	32	12/08/06 09:35:40

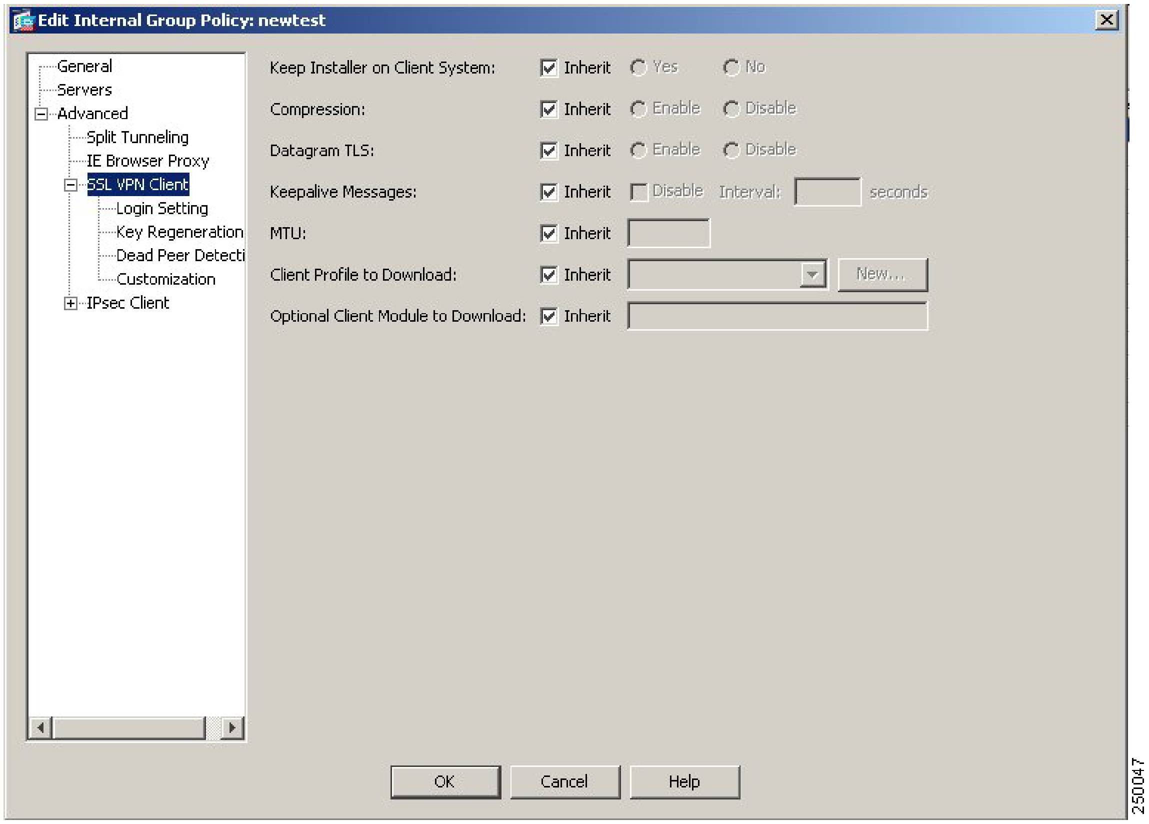
File Name: cdisk.bin

Select a file from the table. The file name appears in the File Name field below the table. Click OK. The file name you selected appears in the Profile Package field of the Add or Edit SSL VPN Client Profiles dialog box.

Step 4 Click OK in the Add or Edit SSL VPN Client dialog box. This makes profiles available to group policies and username attributes of client users.

Step 5 To configure a profile for a group policy, select Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Select an existing group policy and click Edit or click Add to configure a new group policy. In the navigation pane, select Advanced > SSL VPN Client. The Add or Edit Internal Group Policy dialog box appears (Figure 7-4).

Figure 7-4 Add or Edit Internal Group Policy Dialog Box



Edit Internal Group Policy: newtest

- General
- Servers
- Advanced
  - Split Tunneling
  - IE Browser Proxy
  - SSL VPN Client
    - Login Setting
    - Key Regeneration
    - Dead Peer Detecti
    - Customization
  - IPsec Client

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

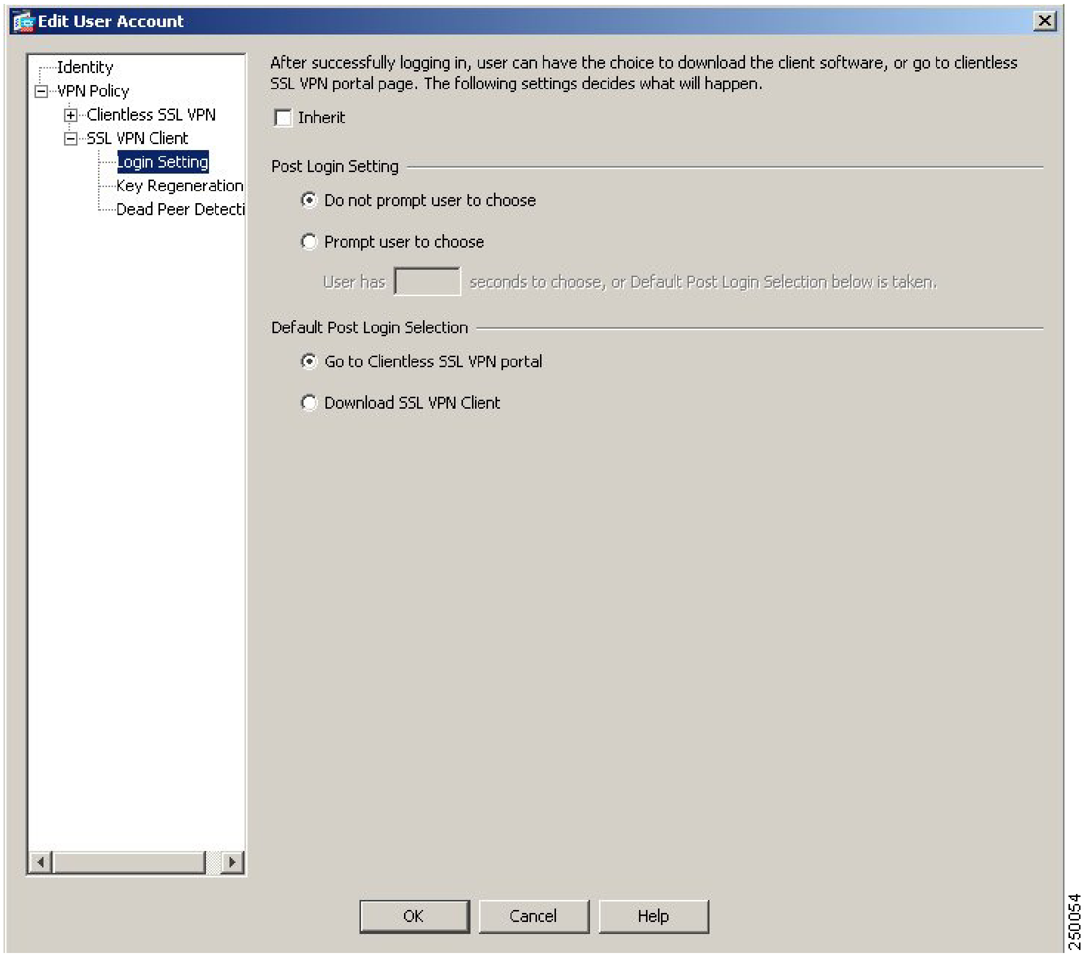
Client Profile to Download: ☑ Inherit New...

Optional Client Module to Download: ☑ Inherit

Continue with Step 7.

Step 6 To configure a profile for a user, select Configuration > Device Management > Users/AAA > User Accounts. Select an existing username and click Edit or click Add to configure a new username. In the navigation pane, select VPN Policy > SSL VPN Client. To modify an existing user's profile, select that user from the table and click Edit. To Add a new user, click Add. The Add or Edit User Account dialog box appears (Figure 7-5).

Figure 7-5 Add or Edit User Account Dialog Box (Username)



After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN portal page. The following settings decides what will happen.

□ Inherit

Post Login Setting

● Do not prompt user to choose

○ Prompt user to choose

User has [ ] seconds to choose, or Default Post Login Selection below is taken.

Default Post Login Selection

● Go to Clientless SSL VPN portal

○ Download SSL VPN Client

Step 7 Deselect Inherit and select a Client Profile to Download from the drop-down list or click New to specify a new client profile. If you click New, the Add SSL VPN Client Profile dialog box (Figure 7-2 on page 7-7) appears; follow the procedures that pertain to that figure.

Step 8 When you have finished with the configuration, click OK.

Configuring Profile Attributes

You configure profile attributes by modifying the XML profile template and saving it with a unique name. You can then distribute the profile XML file to end users at any time. The distribution mechanisms are bundled with the software distribution.

Note It is important to validate the XML profile you create. Use an online validation tool or the profile import feature in ASDM. For validation, you can use the AnyConnectProfile.xsd found in the same directory as the profile template. See Appendix A, “Sample AnyConnect Profile and XML Schema” for a hard copy of these files.

The following sections describe how to modify the profiles template to configure the profile attributes.

Enabling Start Before Logon (SBL) for the AnyConnect Client

With SBL enabled, the user sees the AnyConnect GUI logon dialog before the Windows logon dialog box appears. This establishes the VPN connection first. Available only for Windows platforms, Start Before Logon lets the administrator control the use of login scripts, password caching, mapping network drives to local drives, and more. You can use the SBL feature to activate the VPN as part of the logon sequence. SBL is disabled by default.

XML Settings for Enabling SBL

The element value for UseStartBeforeLogon allows this feature to be turned on (true) or off (false). If the you set this value to true in the profile, additional processing occurs as part of the logon sequence. See the Start Before Logon description for additional details.

You enable SBL by setting the <UseStartBefore Logon> value in the CiscoAnyConnect.xml file to true:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

To disable SBL, set the same value to false.

To enable the UserControllable feature, use the following statement when enabling SBL:

```
<UseStartBeforeLogon userControllable=”false”>true</UseStartBeforeLogon>
```

Any user setting associated with this attribute is stored elsewhere.

CLI Settings for Enabling SBL

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 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.

You must also specify on the security appliance that you want to allow SBL (or any other modules for additional features). See the description in the section Enabling Modules for Additional AnyConnect Features, page 5-5 (ASDM) or Enabling Modules for Additional AnyConnect Features, page 6-4 (CLI) for a description of how to do this.

Configuring the ServerList Attribute

One of the main uses of the profile is to provide a means of supplying a user of the client with a list of hosts to which they can connect. The user then selects the appropriate server. This server list consists of host name and host address pairs. The host name can be an alias used to refer to the host, an FQDN, or an IP address. If an FQDN or IP address is used, a HostAddress element is not required. In establishing a connection, the host address is used as the connection address unless it is not supplied. This allows the host name to be an alias or other name that need not be directly tied to a network addressable host. If no host address is supplied, the connection attempt tries to connect to the host name.

As part of the definition of the server list, a default server can be specified. This default server is identified as such the first time a user attempts a connection using the client. If a user connects with a server other than the default then for this user, the new default is the selected server. The user selection does not alter the contents of the profile.   Instead, the user selection is entered into the user preferences.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ServerList>
    <HostEntry>
        <HostName>MarketingASA01</HostName>
        <HostAddress>209.165.200.224,/HostAddress>
    </HostEntry>
<HostEntry>
        <HostName>EngineeringASA01</HostName>
        <HostAddress>209.165.200.225,/HostAddress>
    </HostEntry>
</ServerList>
```

Configuring the Certificate Match Attribute

The AnyConnect client supports the following certificate match types. Some or all of these may be used for client certificate matching. Certificate matching are global criteria that can be set in an AnyConnect profile. The criteria are:

- Key Usage
- Extended Key Usage
- Distinguished Name

Certificate Key Usage Matching

Certificate key usage offers a set of constraints on the broad types of operations that can be performed with a given certificate. The supported set includes:

- DIGITAL_SIGNATURE
- NON_REPUDIATION
- KEY_ENCIPHERMENT

- DATA_ENCIPHERMENT
- KEY_AGREEMENT
- KEY_CERT_SIGN
- CRL_SIGN
- ENCIPHER_ONLY
- DECIPHER_ONLY

The profile can contain none or more matching criteria. If one or more criteria are specified, a certificate must match at least one to be considered a matching certificate.

The example in Certificate Matching Example, page 7-15 shows how you might configure these attributes.

Extended Certificate Key Usage Matching

This matching allows an administrator to limit the certificates that can be used by the client, based on the *Extended Key Usage* fields. Table 7-3 lists the well known set of constraints with their corresponding object identifiers (OIDs).

Table 7-3 Extended Certificate Key Usage

Constraint	OID
serverAuth	1.3.6.1.5.5.7.3.1
clientAuth	1.3.6.1.5.5.7.3.2
codeSign	1.3.6.1.5.5.7.3.3
emailProtect	1.3.6.1.5.5.7.3.4
ipsecEndSystem	1.3.6.1.5.5.7.3.5
ipsecTunnel	1.3.6.1.5.5.7.3.6
ipsecUser	1.3.6.1.5.5.7.3.7
timeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
dvcs	1.3.6.1.5.5.7.3.10

As an administrator, you can add your own OIDs if the OID you want is not in the well known set. The profile can contain none or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. See profile example in Appendix A, "Sample AnyConnect Profile and XML Schema" for an example.

Certificate Distinguished Name Mapping

The certificate distinguished name mapping capability allows an administrator to limit the certificates that can be used by the client to those matching the specified criteria and criteria match conditions. Table 7-4 lists the supported criteria:

Table 7-4 Criteria for Certificate Distinguished Name Mapping

Identifier	Description
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
"SSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr

The profile can contain none or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. *Distinguished Name* matching offers additional match criteria, including the ability for the administrator to specify that a certificate must or must not have the specified string, as well as whether wild carding for the string should be allowed. See Appendix A, “Sample AnyConnect Profile and XML Schema,” for an example.

Certificate Matching Example

The following example shows how to enable the attributes that you can use to refine client certificate selection.

```
<CertificateMatch>
     <!--
         Specifies Certificate Key attributes that can be used for choosing
         acceptable client certificates.
       -->
    <KeyUsage>
        <MatchKey>Non_Repudiation</MatchKey>
        <MatchKey>Digital_Signature</MatchKey>
    </KeyUsage>
     <!--
         Specifies Certificate Extended Key attributes that can be used for
         choosing acceptable client certificates.
       -->
    <ExtendedKeyUsage>
        <ExtendedMatchKey>ClientAuth</ExtendedMatchKey>
        <ExtendedMatchKey>ServerAuth</ExtendedMatchKey>
        <CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11</CustomExtendedMatchKey>
    </ExtendedKeyUsage>
     <!--
         Certificate Distinguished Name matching allows for exact
         match criteria in the choosing of acceptable client
         certificates.
       -->
    <DistinguishedName>
        <DistinguishedNameDefinition Operator="Equal" Wildcard="Enabled">
            <Name>CN</Name>
            <Pattern>ASASecurity</Pattern>
        </DistinguishedNameDefinition>
        <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
            <Name>L</Name>
            <Pattern>Boulder</Pattern>
        </DistinguishedNameDefinition>
    </DistinguishedName>
</CertificateMatch>
```

CHAPTER 8

Customizing and Localizing the AnyConnect Client

Customizing the End-user Experience

You can customize certain elements, such as the corporate logo, of the AnyConnect client graphical user interface that the remote user sees upon logging in. You customize the AnyConnect Client user interface by replacing files that affect the interface with your own, custom files. For example, with a Windows installation, you can change the company logo from the default Cisco logo by replacing the file *company_logo.bmp* with your own file.

You can also customize the client by translating user messages into other languages.

The sections that follow list the files you can replace for each operating system supported by the AnyConnect client.

Note There is no automated mechanism included with the client to allow customizing the bitmaps and icons. Customizing requires that you manually copy the custom files to the filenames and locations listed in this section.

For Windows

All files for Windows are located in %PROGRAMFILES%\Cisco\Cisco AnyConnect VPN Client\res\. Table 8-1 lists the files that you can replace and the client GUI area affected.

Note %PROGRAMFILES% refers to the environmental variable by the same name. In most Windows installation, this is C:\Program Files.

Table 8-1 Customizing the AnyConnect VPN Client for Windows GUI

Filename in Windows Installation	Client GUI Area Affected
company_logo.bmp	Corporate logo that appears on each tab of the user interface.
ConnectionTab.ico	Icon that appears on the Connection tab.
StatsTab.ico	Icon that appears on the Statistics tab.
AboutTab.ico	Icon that appears on the About tab.

Table 8-1 Customizing the AnyConnect VPN Client for Windows GUI (continued)

Filename in Windows Installation	Client GUI Area Affected
connected.ico	Tray icon that displays when the client is connected.
unconnected.ico	Tray icon that displays when the client is not connected.
disconnecting.ico	Tray icon that displays when the client is in the process of disconnecting.

For Linux

All files for Linux are located in /opt/cisco/vpn/pixmaps/. Table 8-2 lists the files that you can replace and the client GUI area affected.

Table 8-2 Customizing the AnyConnect VPN Client for Linux GIU

Filename in Linux Installation	Client GUI Area Affected
company-logo.png	Corporate logo that appears on each tab of the user interface.
vpnui48.png	Main program icon.
systray_connected.png	Tray icon that displays when the client is connected.
systray_notconnected.png	Tray icon that displays when the client is not connected.
systray_disconnecting.png	Tray icon that displays when the client is in the process of disconnecting.
cvc-info.png	Icon that appears on the Statistics tab.
cvc-disconnect.png	Icon that appears next to the Disconnect button.
cvc-connect.png	Icon that appears next to the Connect button, and on the Connection tab.
cvc-about.png	Icon that appears on the About tab.

For Mac OS X

All files for OS X are located in /Applications/Cisco AnyConnect VPN Client/Contents/Resources. Table 8-3 lists the files that you can replace and the client GUI area affected.

Table 8-3 Customizing the AnyConnect VPN Client for Mac OS X

Filename in Mac OS X Installation	Client GUI Area Affected
bubble.png	Notification bubble that appears when the client connects or disconnects.
logo.png	Logo icon that appears on main screen in the top right corner.
menu_idle.png	Disconnected idle menu bar icon.
menu_connected.png	Connected state menu bar icon.
menu_error.png	Error state menu bar icon.
connected.png	Icon that displays under the disconnect button when the client is connected.
warning.png	Icon that replaces login fields on various authentication/certificate warnings.
vpngui.icns	Mac OS X icon file format that is used for all icon services, such as Dock, Sheets, and Finder.

Language Translation (Localization) for User Messages

Localization provides a way of implementing translation for user messages that appear on the client user interface. The security appliance provides language translation for the portal and screens displayed to users that initiate browser-based, Clientless SSL VPN connections, as well as the interface displayed to Cisco AnyConnect VPN Client users.

This section describes how to configure the security appliance to translate these user messages and includes the following sections:

- Understanding Language Translation, page 8-3
- Creating or Modifying a Translation Table Using CLI, page 8-8
- Referencing the Language in a Customization Object, page 8-10
- Changing a Group Policy or User Attributes to Use the Customization Object, page 8-12

Understanding Language Translation

Functional areas and their messages that are visible to remote users are organized into translation domains. Table 8-4 shows the translation domains and the functional areas translated.

Table 8-4 Translation Domains and Functional Areas Affected

Translation Domain	Functional Areas Translated
AnyConnect	Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	Messages on the logon and logout pages, portal page, and all the messages customizable by the user.
banners	Banners displayed to remote users and messages when VPN access is denied.
PortForwarder	Messages displayed to Port Forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA and portal messages that are not customizable.
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.

The standard software image package for the security appliance includes a translation table template for each domain. The templates for plug-ins are included with the plug-ins and define their own translation domains.

You can export the template for a translation domain, which in some cases creates an XML file of the template at the URL or IP address you provide. The message fields in this file are empty. You can edit the messages and import the template to create a new translation table object that resides in flash memory.

You can also export an existing translation table. The XML file created displays the messages you edited previously. Reimporting this XML file with the same language name creates a new version of the translation table object, overwriting previous messages.

Some templates are static, but some change based on the configuration of the security appliance. Because you can customize the logon and logout pages, portal page, and URL bookmarks for clientless users, the security appliance generates the **customization** and **url-list** translation domain templates dynamically, and the template automatically reflects your changes to these functional areas.

After you create translation tables, they are available to customization objects that you create and apply to group policies or user attributes. With the exception of the AnyConnect translation domain, a translation table has no effect, and messages are not translated on user screens, until you create a customization object, identify a translation table to use in that object, and specify that customization for the group policy or user. Changes to the AnyConnect translations are automatically downloaded to clients the next time they connect to the Secure Gateway.

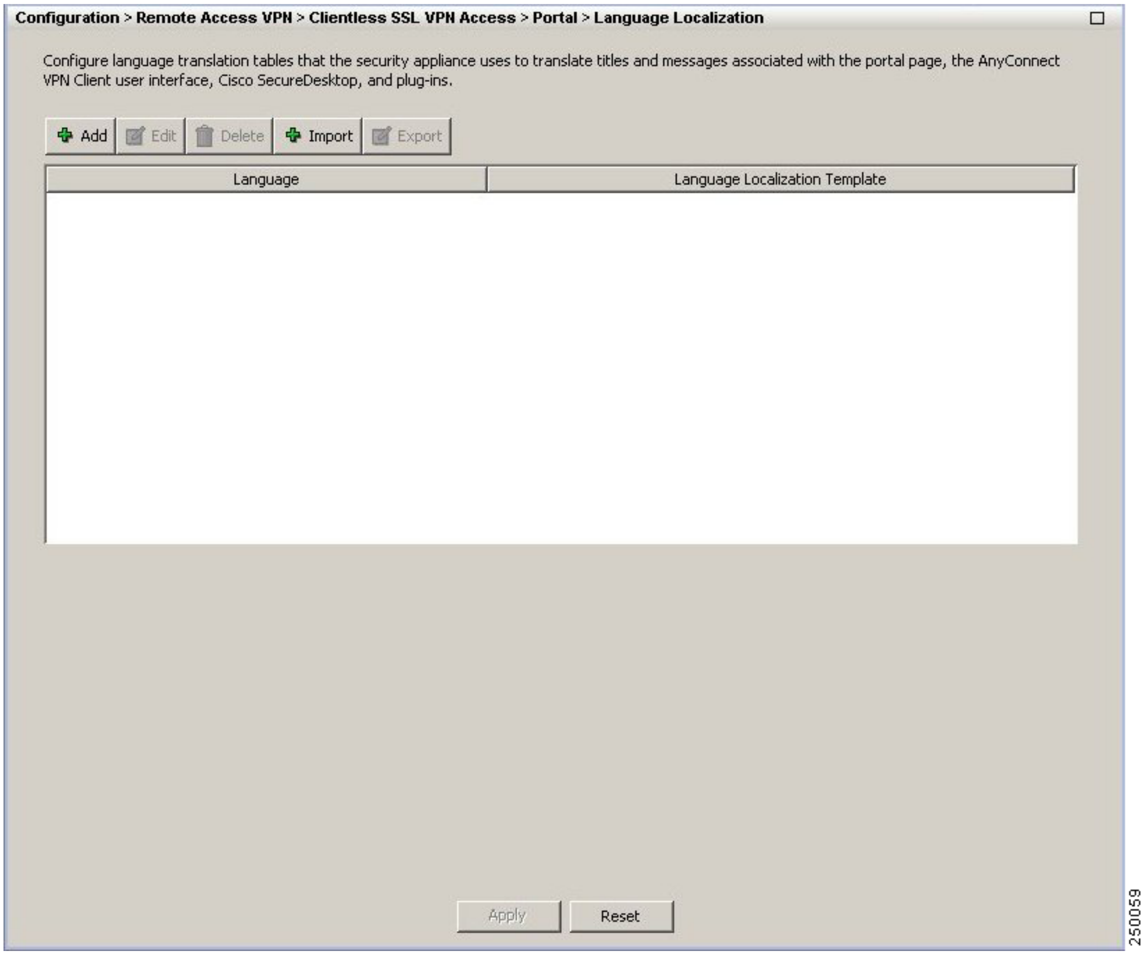
Configuring Language Localization Using ASDM

To use ASDM to configure language localization, select Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Language Localization. This opens the Language Localization pane (Figure 8-1).

Note Both the AnyConnect VPN client and Clientless SSL VPN use the same localization mechanism, and the path merely reflects this.

The language localization pane shows the language of existing language localization tables and the language localization templates the translation tables are based on and lets you add, edit, delete, import, or export language localization templates. Using the buttons on this pane, you can configure language translation tables that the security appliance uses to translate titles and messages associated with the portal page, the AnyConnect VPN client user interface, Cisco Secure Desktop, and plug-ins.

Figure 8-1 Language Localization Pane



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Language Localization

Configure language translation tables that the security appliance uses to translate titles and messages associated with the portal page, the AnyConnect VPN Client user interface, Cisco SecureDesktop, and plug-ins.

Language	Language Localization Template

Fields

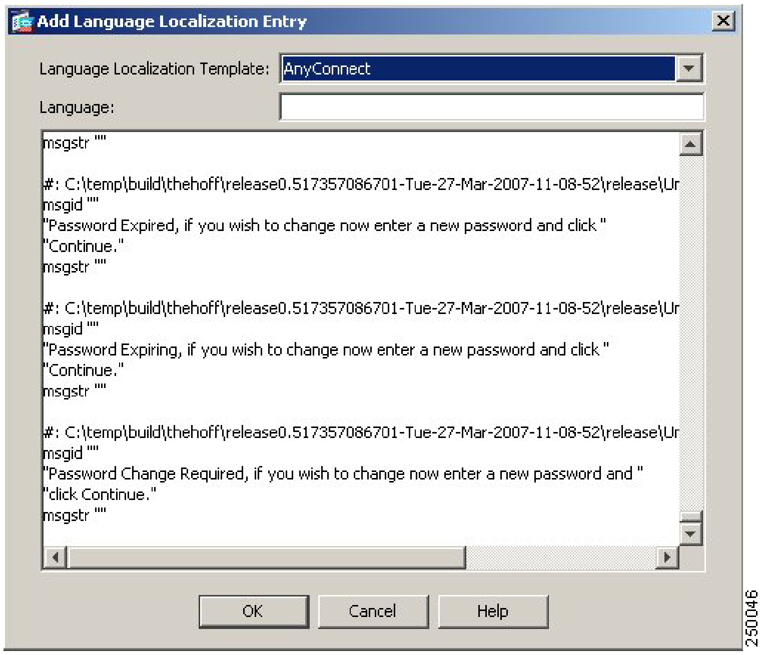
- Add—Launches the Add Localization Entry dialog where you can select a localization template to add and you can edit the contents of the template.
- Edit—Launches the Edit Localization Entry dialog for the selected language in the table, and allows you to edit the previously-imported language localization table.
- Delete—Deletes a selected language localization table.
- Import—Launches the Import Language Localization dialog where you can import a language localization template or table.
- Export—Launches the Export Language Localization dialog where you can export a language localization template or table to a URL or IP address where you can make changes to the table or template.
- Language—The language of existing Language Localization tables.
- Language Localization Template—The template on which the table is based.

Creating or Modifying a Translation Table Using ASDM

To create a translation table, do the following steps:

Step 1 On the Language Localization pane, click Add or Edit. The Add (or Edit) Language Localization dialog box (Figure 8-2) displays. You can add a new translation table, based on a template, or you can modify an already-imported translation table from this pane.

Figure 8-2 Add Language Localization Dialog Box



Language Localization Template: AnyConnect

Language:

```
msgstr ""

#: C:\temp\build\thehoff\release0.517357086701-Tue-27-Mar-2007-11-08-52\release\Ur
msgid ""
"Password Expired, if you wish to change now enter a new password and click "
"Continue."
msgstr ""

#: C:\temp\build\thehoff\release0.517357086701-Tue-27-Mar-2007-11-08-52\release\Ur
msgid ""
"Password Expiring, if you wish to change now enter a new password and click "
"Continue."
msgstr ""

#: C:\temp\build\thehoff\release0.517357086701-Tue-27-Mar-2007-11-08-52\release\Ur
msgid ""
"Password Change Required, if you wish to change now enter a new password and "
"click Continue."
msgstr ""
```

Step 2 Select a Language Localization Template from the drop-down box. The entries in the box correspond to functional areas that are translated. For list of templates and functional areas, see Table 8-4 on page 8-3.

Step 3 Specify a language for the template. The template becomes a translation table in cache memory with the name you specify. Use an abbreviation that is compatible with the language options for your browser. For example, if you are creating a table for the Chinese language, and you are using Internet Explorer, use the abbreviation zh, that is recognized by Internet Explorer.

Note Consult the online help for your specific browser to see what the appropriate language abbreviations are for that browser and make sure that you have added the appropriate languages to your list of languages that you want to use to display web pages in that browser. Adding languages does not ensure that your computer has a font that can display web pages in your preferred language. In addition, most web pages contain information that tells the browser what language encoding (language and character set) to use. Your browser might have a facility to automatically determine the appropriate encoding. See the online help for your browser for specific information about multiple language support.

Step 4 Edit the translation table. For each message represented by the msgid field that you want to translate, enter the translated text between the quotes of the associated msgstr field. The example below shows the message Connected, with the Spanish text in the msgstr field:

```
msgid "Connected"
```

```
msgstr "Conectado"
```

Note With the AnyConnect VPN Client, the first user message to appear does not correctly translate, because that message is missing from the AnyConnect message catalog in the AnyConnect.po template. You retrieve AnyConnect.po from the security appliance using the export procedure. You export the AnyConnect template, AnyConnect.po, add the additional message, and insert the desired translations for the messages currently in the file. When this is complete, you use the import procedure, which specifies the language. You do not reimport the template itself. Only the updated file, which includes the translations, is reloaded.

To ensure that the first user message appears correctly translated, add the following lines to the message catalog file that you are using for translations, before re-importing it with the missing tags:

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

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

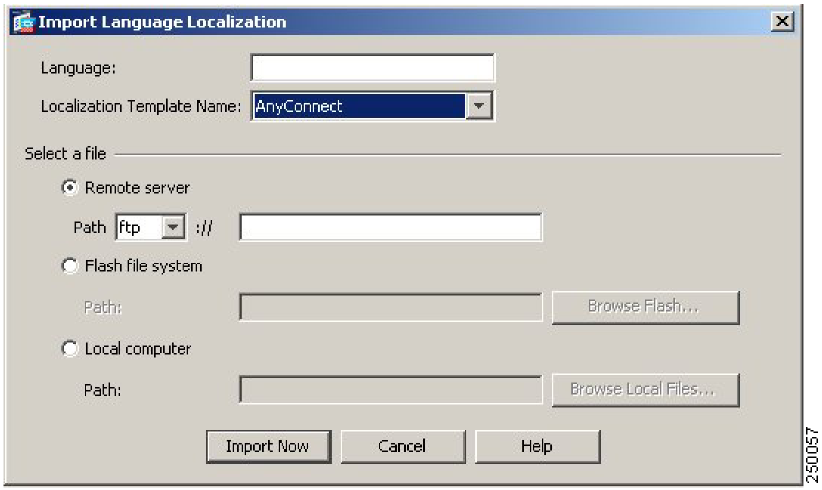
Step 5 Click OK. The new table appears in the list of translation tables.

Import/Export Language Localization

To import or export a translation table, click Import or Export on the Language Localization pane. This opens the Import or Export Language Localization pane (Figure 8-3), on which you can import or export a translation table to the security appliance to provide translation of user messages.

Translation templates are XML files that contain message fields that can be edited with translated messages. You can export a template, edit the message fields, and import the template as a new translation table, or you can export an existing translation table, edit the message fields, and re-import the table to overwrite the previous version.

Figure 8-3 Import Language Localization Pane



Language:
Localization Template Name: AnyConnect
● Remote server
Path ftp ://

Fields

- Language—Enter a name for the language.
- When exporting, it is automatically filled-in with the name from the entry you selected in the table.
- When importing, you enter the language name in the manner that you want it to be identified. The imported translation table then appears in the list with the abbreviation you designated. To ensure that your browser recognizes the language, use language abbreviations that are compatible with the language options of the browser. For example, if you are using IE, use zh as the abbreviation for the Chinese language.
- Localization Template Name—The name of the XML file containing the message fields. The following templates are available:
  - AnyConnect—Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
  - CSD—Messages for the Cisco Secure Desktop (CSD).
  - customization—Messages on the logon and logout pages, portal page, and all the messages customizable by the user.
  - keepout—Message displayed to remote users when VPN access is denied.
  - PortForwarder—Messages displayed to Port Forwarding users.
  - url-list—Text that user specifies for URL bookmarks on the portal page.
  - webvpn—All the layer 7, AAA and portal messages that are not customizable.
  - plugin-ica—Messages for the Citrix plug-in.
  - plugin-rdp—Messages for the Remote Desktop Protocol plug-in.
  - plugin-telnet,ssh—Messages for the TELNET and SSH plug-in.
  - plugin-vnc—Messages for the VNC plug-in.
- Select a file—Choose the method by which you want to import or export the file.
  - Remote server—Select this option to import a customization file that resides on a remote server accessible from the security appliance.
  - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
  - Flash file system—Choose this method to export a file that resides on the security appliance.
  - Path—Provide the path to the file.
  - Browse Flash—Browse to the path for the file.
  - Local computer—Choose this method to import a file that resides on the local PC.
  - Path—Provide the path to the file.
  - Browse Local Files—Browse to the path for the file.
- Import/Export Now—Click to import or export the file.

Creating or Modifying a Translation Table Using CLI

The following procedure describes how to create translation tables:

Step 1 Export a translation table template to a computer with the **export webvpn translation-table** command from privileged EXEC mode.

In the following example, the **show webvpn translation-table** command shows available translation table templates and tables.

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  test                                        customization
hostname#
```

The next example exports the translation table template for the AnyConnect domain, which affects messages displayed to AnyConnect client users. In this example, the filename of the XML file created is *test* (user-specified), and it contains empty message fields:

```
hostname# export webvpn translation-table AnyConnect template tftp://209.165.200.225/test
```

Step 2 Edit the translation table XML file.

The following example shows a portion of the template that was exported as *test*. The end of this output includes a message ID field (msgid) and a message string field (msgstr) for the message *Clientless SSL VPN Service*, which is displayed on the portal page when a Clientless user establishes a VPN connection. The complete template contains many pairs of message fields:

```
# Copyright (C) 2007 by Cisco Systems, Inc.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: ASA\n"
"Report-Msgid-Bugs-To: support@cisco.com\n"
"POT-Creation-Date: 2007-04-23 18:57 GMT\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=UTF-8\n"
"Content-Transfer-Encoding: 8bit\n"

#: DfltCustomization:24 DfltCustomization:64
msgid "Clientless SSL VPN Service"
msgstr ""
```

The message ID field (msgid) contains the default translation. The message string field (msgstr) that follows msgid provides the translation. To create a translation, enter the translated text between the quotes of the msgstr string.

Step 3 Import the translation table using the **import webvpn translation-table** command from privileged EXEC mode.

In the following example, the XML file is imported *es-us*—the abbreviation for Spanish spoken in the United States.

```
hostname# import webvpn translation-table customization language es-us
tftp://209.165.200.225/portal
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder
csd
customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us customization
```

If you import a translation table for the AnyConnect domain, your changes to the AnyConnect translations are automatically downloaded to clients the next time they connect to the Secure Gateway. If you import a translation table for any other domain, you must continue to Step 4, where you create a customization object, identify the translation table to use in that object, and specify that customization object for the group policy or user.

Referencing the Language in a Customization Object

Now that you have created a translation table, you need to refer to this table in a customization object.

Steps 4 through 6 describe how to export the customization template, edit it, and import it as a customization object:

Step 4 Export a customization template to a URL or IP address where you can edit it using the **export webvpn customization template** command from privileged EXEC mode. The example below exports the template and creates the copy *sales* at the URL or IP address specified:

```
hostname# export webvpn customization template tftp://209.165.200.225/sales
```

Step 5 Edit the customization template and reference the previously-imported translation table.

Two areas of XML code in the customization template pertain to translation tables. The first area, shown below, specifies the translation tables to use:

```
<localization>
   <languages>en,ja,zh,ru,fr</languages>
   <default-language>en</default-language>
</localization>
```

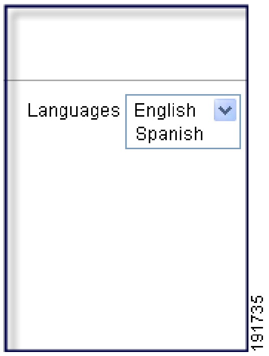
The <languages> tag in the code is followed by the names of the translation tables. In this example code, they are en, ja, zh, ru, and fr (English, Japanese, Chinese, Russian, and French). For the customization object to call these translation tables correctly, the tables must have been previously imported using the exact same names. These names must be compatible with language options of the browser.

Note Consult the online help for your specific browser to see what the appropriate language abbreviations are for that browser and make sure that you have added the appropriate languages to your list of languages that you want to use to display web pages in that browser. Adding languages does not ensure that your computer has a font that can display web pages in your preferred language. In addition, most web pages contain information that tells the browser what language encoding (language and character set) to use. Your browser might have a facility to automatically determine the appropriate encoding. See the online help for your browser for specific information about multiple language support.

The <default-language> tag specifies the language that the remote user first encounters when connecting to the security appliance. In the example code above, the language is English.

Figure 8-4 shows the login page and the Language Selector. This Language Selector gives remote users establishing an SSL VPN connection the ability to select the language of their choice.

Figure 8-4 Language Selector



The following XML code affects the display of the Language Selector, and includes the <language selector> tag and the associated <language> tags that enable and customize the Language Selector:

```
<auth-page>
     ....
         <language-selector>
            <mode>enable</mode>
            <title l10n="yes">Language:</title>
          <language>
             <code>en</code>
             <text>English</text>
          </language>
          <language>
            <code>es-us</code>
            <text>Spanish</text>
          </language>
       </language-selector>
```

The <language-selector> group of tags includes the <mode> tag that enables and disables the displaying of the Language Selector, and the <title> tag that specifies the title of the drop-down box listing the languages.

The <language> group of tags includes the <code> and <text> tags that map the language name displayed in the Language Selector drop-down box to a specific translation table.

Make your changes to this file and save the file.

Step 6 Import the customization template as a new object named sales, using the **import webvpn customization** command from privileged EXEC mode. For example:

```
hostname# import webvpn customization sales tftp://209.165.200.225/sales
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The output of the **show import webvpn customization** command shows the new customization object *sales*:

```
hostname(config)# show import webvpn customization
Template
sales
hostname(config)#
```

Changing a Group Policy or User Attributes to Use the Customization Object

Now that you have created the customization object, you must activate your changes for specific groups or users. Step 7 shows how to enable the customization object in a group policy:

Step 7 Enter the group policy webvpn configuration mode for a group policy and enable the customization object using the **customization** command. The following example shows the customization object *sales* enabled in the group policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# customization value sales
```

Note With the AnyConnect VPN Client, the first user message to appear does not correctly translate, because that message is missing from the AnyConnect message catalog in the AnyConnect.po template. You retrieve AnyConnect.po from the security appliance using the export procedure:

```
export webvpn translation-table AnyConnect template url
```

The variable *url* includes the file name that you supply; for example:

```
https://192.168.200.30/my_anyconnect_translation_template
```

After you export the AnyConnect template, you add the additional message and insert the desired translations for the messages currently in the file. When this is complete, you use the import procedure, which specifies the language. You do not reimport the template itself. Only the updated file, which includes the translations, is reloaded. The import command is:

```
import webvpn translation-table AnyConnect language en url
```

The *url* variable is the address and the filename of the XML file that you edited.

To ensure that the first user message appears correctly translated, add the following lines to the message catalog file that you are using for translations, before re-importing it with the missing tags:

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

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

CHAPTER 9

Monitoring and Maintaining the AnyConnect Client

This chapter describes some common maintenance and monitoring procedures for network administrators dealing with the Cisco AnyConnect Client. You perform these procedures on the security appliance:

Viewing AnyConnect Client and SSL VPN Sessions

You can view information about active sessions using the **show vpn-sessiondb** command in privileged EXEC mode:

show vpn-sessiondb svc

The following example shows the output of the **show vpn-sessiondb svc** command:

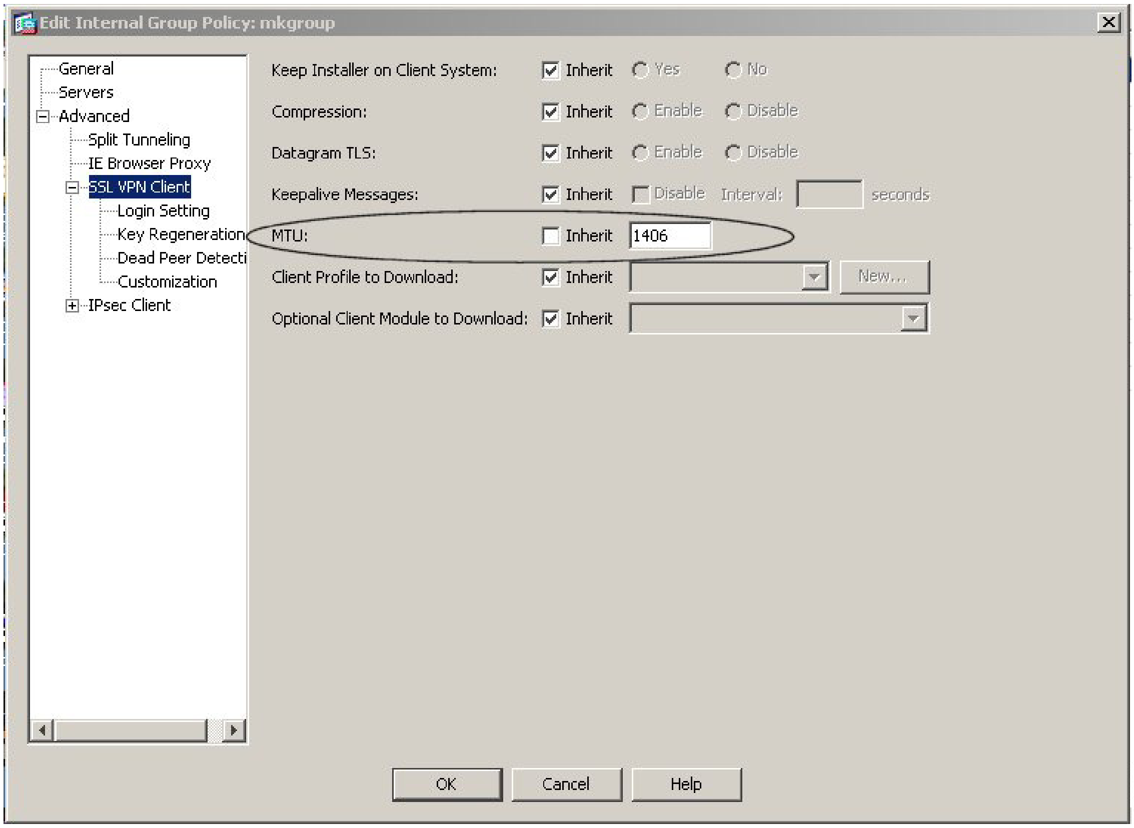
```
hostname# show vpn-sessiondb svc

Session Type: SVC

Username     : testuser               Index        : 17
Assigned IP  : 209.165.200.224        Public IP    : 192.168.23.45
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 17457                  Bytes Rx     : 69502
Group Policy : GroupPolicy            Tunnel Group : CertGroup
Login Time   : 15:19:57 EDT Fri May 25 2007
Duration     : 0h:04m:27s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

To see more detailed information, including the number of AnyConnect (SSL VPN) tunnels, DTLS tunnels, and Clientless tunnels, use the command **show vpn-sessiondb detail svc**.

Adjusting MTU Size Using ASDM

You can adjust the Maximum Transmission Unit size (from 256 to 1406 bytes) for SSL VPN connections established by the AnyConnect Client by selecting Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit. The Edit Internal Group Policy dialog box opens (fig).

Figure 9-1 Edit Internal Group Policy Dialog Box



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

Select Advanced > SSL VPN Client. Uncheck the Inherit check box and specify the appropriate value in the MTU field. The default size for this command in the default group policy is 1406. The MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.

This setting affects only the AnyConnect Client. The Cisco SSL VPN Client (SVC) is not capable of adjusting to different MTU sizes. This setting affects AnyConnect Client connections established in SSL and those established in SSL with DTLS.

Adjusting MTU Size Using CLI

You can adjust the Maximum Transmission Unit size (from 256 to 1406 bytes) for SSL VPN connections established by the AnyConnect Client by using the **svc mtu** command from group policy webvpn or username webvpn configuration mode:

[**no**] **svc mtu** *size*

This command affects only the AnyConnect Client. The Cisco SSL VPN Client (SVC) is not capable of adjusting to different MTU sizes.

The default size for this command in the default group policy is 1406. The MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.

This command affects AnyConnect Client connections established in SSL and those established in SSL with DTLS.

The following example configures the MTU size to 1200 bytes for the group policy *telecommuters*:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc mtu 1200
```

Many consumer-grade end user terminating devices (for example, a home router) do not properly handle the creation or assembly of IP fragments. This is particularly true of UDP. Since DTLS is a UDP-based protocol, it is sometimes necessary to reduce the MTU to prevent fragmentation. The MTU parameter is used by both the client and the security appliance to set the maximum size of the packet to be transmitted over the tunnel. If an end user is experiencing a significant amount of lost packets, or if an application such as Microsoft Outlook is not functioning over the tunnel, it might indicate a fragmentation issue. Lowering the MTU for that user or group of users may address the problem.

The client proposes an MTU value that is 94 bytes less than the MTU of the physical adapter used for the SSL and DTLS connection to the security appliance. The security appliance accepts the lesser of the configured MTU or the value proposed by the client. Both the client and the security appliance use the value selected by the security appliance.

For example, if the physical adapter on the PC has been changed to use an MTU of 1300, then the client proposes an MTU of 1206 to the security appliance. If the security appliance is set for a value lower than 1206, both the client and the security appliance use the lower value that was set using the MTU configuration command.

Logging Off AnyConnect Client Sessions

To log off all AnyConnect Client and SSL VPN sessions, use the **vpn-sessiondb logoff svc** command in global configuration mode:

vpn-sessiondb logoff svc

In response, the system asks you to confirm that you want to log off the VPN sessions. To confirm press Enter or type y. Entering any other key cancels the logging off.

The following example logs off all SSL VPN sessions:

```
hostname# vpn-sessiondb logoff svc
INFO: Number of sessions of type "svc" logged off : 1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions logged off : 6
hostname#
```

You can log off individual sessions using either the **name** option, or the **index** option:

vpn-sessiondb logoff name *name*

vpn-sessiondb logoff index *index*

For example, to log off the user named tester, enter the following command:

```
hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
```

```
INFO: Number of sessions with name "tester" logged off : 1
hostname#
```

You can find both the username and the index number (established by the order of the client images) in the output of the **show vpn-sessiondb svc** command (see Viewing AnyConnect Client and SSL VPN Sessions, page 9-1).

The following example terminates that session using the **name** option of the **vpn-sessiondb logoff command**:

```
hostname# vpn-sessiondb logoff name testuser
INFO: Number of sessions with name "tesstuser" logged off : 1
```

Updating AnyConnect Client and SSL VPN Client Images

You can update the client images on the security appliance at any time using the following procedure:

Step 1 Copy the new client images to the security appliance using the **copy** command from privileged EXEC mode, or using another method.

Step 2 If the new client image files have the same filenames as the files already loaded, reenter the **svc image** command that is in the configuration. If the new filenames are different, uninstall the old files using the **no svc image** command. Then use the **svc image** command to assign an order to the images and cause the security appliance to load the new images.

APPENDIX A

Sample AnyConnect Profile and XML Schema

This appendix contains a sample AnyConnect profile and a sample AnyConnect profile schema. Both of these are delivered with the client and are present in a client installation in the same directory. The profile defines the attributes configured for a particular user. The schema defines the profile format that is allowed. The schema is suitable for use as a validation mechanism.

- Sample AnyConnect Profile, page A-1
- Sample AnyConnect Profile Schema, page A-3

Caution Do not cut and paste this example from this document. Doing so introduces line breaks that can break your XML. Instead, open the profile template file in a text editor such as notepad or wordpad.

Use the template that appears after installing AnyConnect on a workstation:
\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\AnyConnectProfile.tmpl

Sample AnyConnect Profile

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
    This is a sample of a Cisco AnyConnect VPN Client Profile XML file.

    This file is intended to be maintained by a Secure Gateway administrator
    and then distributed with the client software.  The xml file based on
    this schema can be distributed to clients at any time.  The distribution
    mechanisms supported are as a bundled file with the software distribution
    or as part of the automatic download mechanism.  The automatic download
    mechanism only available with certain Cisco Secure Gateway products.

    NOTE: Administrators are strongly encouraged to validate XML profile they
          create using an online validation tool or via the profile import
          functionality in ASDM.  Validation can be accomplished with the
          AnyConnectProfile.xsd found in this directory.

    AnyConnectProfile is the root element representing the AnyConnect Client
    Profile
  -->
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
    <!--
    The ClientInitialization section represents global settings for the
    client.  In some cases (e.g. BackupServerList) host specific overrides
    are possible.
  -->
<ClientInitialization>
    <!--
        The Start Before Logon feature can be used to activate the VPN as
        part of the logon sequence.

        UserControllable:
        Does the administrator of this profile allow the user to control
        this attribute for their own use.  Any user setting associated
        with this attribute will be stored elsewhere.
      -->
    <UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
    <!--
        If user is importing a certificate using the enrollment feature,
        this attribute will enforce any pin application requirement.
      -->
    <CertEnrollmentPin>pinAllowed</CertEnrollmentPin>
    <!--
        This section enables the definition of various attributes that
        can be used to refine client certificate selection.
      -->
    <CertificateMatch>
        <!--
            Certificate Key attributes that can be used for choosing
            acceptable client certificates.
          -->
        <KeyUsage>
            <MatchKey>Non_Repudiation</MatchKey>
            <MatchKey>Digital_Signature</MatchKey>
        </KeyUsage>
        <!--
            Certificate Extended Key attributes that can be used for
            choosing acceptable client certificates.
          -->
        <ExtendedKeyUsage>
            <ExtendedMatchKey>ClientAuth</ExtendedMatchKey>
            <ExtendedMatchKey>ServerAuth</ExtendedMatchKey>
            <CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11</CustomExtendedMatchKey>
        </ExtendedKeyUsage>
        <!--
            Certificate Distinguished Name matching allows for exact
            match criteria in the choosing of acceptable client
            certificates.
          -->
        <DistinguishedName>
            <DistinguishedNameDefinition Operator="Equal" Wildcard="Enabled">
                <Name>CN</Name>
                <Pattern>ASASecurity</Pattern>
            </DistinguishedNameDefinition>
            <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
                <Name>L</Name>
                <Pattern>Boulder</Pattern>
            </DistinguishedNameDefinition>
        </DistinguishedName>
    </CertificateMatch>
    <!--
        Collection of one or more backup servers to be used in case
        the user selected one fails.
      -->
    <BackupServerList>
        <!--
```

```
                Can be a FQDN or IP address.
              -->
            <HostAddress>cvc-asa-02.cisco.com</HostAddress>
            <HostAddress>10.94.146.172</HostAddress>
        </BackupServerList>
    </ClientInitialization>
    <!--
        This section contains the list of hosts the user will be able to
        select from.
      -->
    <ServerList>
        <!--
            This is the data needed to attempt a connection to a specific
            host.
          -->
        <HostEntry>
            <!--
                Can be an alias used to refer to the host or an  FQDN or
                IP address.  If an FQDN or IP address is used, a
                HostAddress is not required.
              -->
            <HostName>CVC-ASA-02</HostName>
            <HostAddress>cvc-asa-02.cisco.com</HostAddress>
        </HostEntry>
        <HostEntry>
            <HostName>CVC-ASA-01</HostName>
            <HostAddress>10.94.146.172</HostAddress>
            <!--
                This backup server list represents an override to the
                global one defined previously.
              -->
           <BackupServerList>
                <HostAddress>cvc-asa-03.cisco.com</HostAddress>
                <HostAddress>10.94.146.173</HostAddress>
           </BackupServerList>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

Sample AnyConnect Profile Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2006 rel. 3 sp1 (http://www.altova.com) by Chris Fitzgerald
(private) -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns1="http://schemas.xmlsoap.org/encoding/"
targetNamespace="http://schemas.xmlsoap.org/encoding/" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    <xs:annotation>
        <xs:documentation>pwd</xs:documentation>
    </xs:annotation>
    <xs:complexType name="HostEntry">
        <xs:annotation>
            <xs:documentation>This is the data needed to attempt a connection to a
specific host.</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="HostEntry" maxOccurs="unbounded">
                <xs:annotation>
```

```
                    <xs:documentation>A HostEntry comprises the data needed to identify and
connect to a specific host.</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="HostName">
                            <xs:annotation>
                                <xs:documentation>Can be an alias used to refer to the host
or an  FQDN or IP address.  If an FQDN or IP address is used, a HostAddress is not
required.</xs:documentation>
                            </xs:annotation>
                        </xs:element>
                        <xs:element name="HostAddress" minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>Can be a FQDN or IP
address.</xs:documentation>
                            </xs:annotation>
                        </xs:element>
                        <xs:element name="BackupServerList" type="ns1:BackupServerList"
minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>Collection of one or more backup servers
to be used in case the user selected one fails.</xs:documentation>
                            </xs:annotation>
                        </xs:element>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AnyConnectClientProfile">
        <xs:annotation>
            <xs:documentation>This is the XML schema definition for the Cisco AnyConnect
VPN Client Profile XML file.  The VPN Client Initialization is a repository of information
used to manage the Cisco VPN client software.  This file is intended to be maintained by a
Secure Gateway administrator and then distributed with the client software.  The xml file
based on this schema can be distributed to clients at any time.  The distribution
mechanisms supported are as a bundled file with the software distribution or as part of
the automatic download mechanism.  The automatic download mechanism only available with
certain Cisco Secure Gateway products.</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="ClientInitialization" minOccurs="0">
                <xs:annotation>
                    <xs:documentation>The ClientInitialization section represents global
settings for the client.  In some cases (e.g. BackupServerList) host specific overrides
are possible.</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="UseStartBeforeLogon" default="false"
minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>The Start Before Logon feature can be used
to activate the VPN as part of the logon sequence.</xs:documentation>
                            </xs:annotation>
                            <xs:complexType>
                                <xs:simpleContent>
                                    <xs:extension base="ns1:simpleBinary">
                                        <xs:attribute name="UserControllable"
default="false">
                                            <xs:annotation>
```

```
                                                <xs:documentation>Does the administrator of 
this profile allow the user to control this attribute for their own use.  Any user setting 
associated with this attribute will be stored elsewhere.</xs:documentation>
                                            </xs:annotation>
                                            <xs:simpleType>
                                                <xs:restriction base="xs:string">
                                                    <xs:enumeration value="true">
                                                        <xs:annotation>
                                                            <xs:documentation>user is allowed 
to control this setting.</xs:documentation>
                                                        </xs:annotation>
                                                    </xs:enumeration>
                                                    <xs:enumeration value="false">
                                                        <xs:annotation>
                                                            <xs:documentation>user is not 
allowed to control this setting.</xs:documentation>
                                                        </xs:annotation>
                                                    </xs:enumeration>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:attribute>
                                    </xs:extension>
                                </xs:simpleContent>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="CertEnrollmentPin" default="pinAllowed" 
minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>If user is importing a certificate using 
the enrollment feature, this attribute will enforce any pin application 
requirement.</xs:documentation>
                            </xs:annotation>
                            <xs:simpleType>
                                <xs:restriction base="xs:string">
                                    <xs:enumeration value="noPin">
                                        <xs:annotation>
                                            <xs:documentation>user may not enter a pin when 
enrolling a certificate.</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="pinAllowed">
                                        <xs:annotation>
                                            <xs:documentation>user may enter a pin when 
enrolling a certificate.</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="pinRequired">
                                        <xs:annotation>
                                            <xs:documentation>user must enter a pin when 
enrolling a certificate.</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                </xs:restriction>
                            </xs:simpleType>
                        </xs:element>
                        <xs:element name="CertificateMatch" minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>This section enables the definition of 
various attributes that can be used to refine client certificate 
selection.</xs:documentation>
                            </xs:annotation>
                            <xs:complexType>
                                <xs:sequence>
```

```
                                    <xs:element name="KeyUsage" type="ns1:KeyUsage"
minOccurs="0">
                                        <xs:annotation>
                                            <xs:documentation>Certificate Key attributes
that can be used for choosing acceptable client certificates.</xs:documentation>
                                        </xs:annotation>
                                    </xs:element>
                                    <xs:element name="ExtendedKeyUsage"
type="ns1:ExtendedKeyUsage" minOccurs="0">
                                        <xs:annotation>
                                            <xs:documentation>Certificate Extended Key
attributes that can be used for choosing acceptable client
certificates.</xs:documentation>
                                        </xs:annotation>
                                    </xs:element>
                                    <xs:element name="DistinguishedName"
type="ns1:DistinguishedName" minOccurs="0">
                                        <xs:annotation>
                                            <xs:documentation>Certificate Distinguished Name
matching allows for exact match criteria in the choosing of acceptable client
certificates.</xs:documentation>
                                        </xs:annotation>
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="BackupServerList" type="ns1:BackupServerList"
minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>Collection of one or more backup servers
to be used in case the user selected one fails.</xs:documentation>
                            </xs:annotation>
                        </xs:element>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="ServerList" type="ns1:HostEntry" minOccurs="0">
                <xs:annotation>
                    <xs:documentation>This section contains the list of hosts the user will
be able to select from.</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="BackupServerList">
        <xs:annotation>
            <xs:documentation>Collection of one or more backup servers to be used in case
the user selected one fails.</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="HostAddress" maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>Can be a FQDN or IP address.</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="KeyUsage">
        <xs:annotation>
            <xs:documentation>Certificate Key attributes that can be used for choosing
acceptable client certificates.</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="MatchKey" maxOccurs="9">
```

```
                <xs:annotation>
                    <xs:documentation>One or more match key may be specified.  A 
certificate must match at least one of the specified key to be 
selected.</xs:documentation>
                </xs:annotation>
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:enumeration value="Decipher_Only"/>
                        <xs:enumeration value="Encipher_Only"/>
                        <xs:enumeration value="CRL_Sign"/>
                        <xs:enumeration value="Key_Cert_Sign"/>
                        <xs:enumeration value="Key_Agreement"/>
                        <xs:enumeration value="Data_Encipherment"/>
                        <xs:enumeration value="Key_Encipherment"/>
                        <xs:enumeration value="Non_Repudiation"/>
                        <xs:enumeration value="Digital_Signature"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="ExtendedKeyUsage">
        <xs:annotation>
            <xs:documentation>Certificate Extended Key attributes that can be used for 
choosing acceptable client certificates.</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="ExtendedMatchKey" nillable="false" minOccurs="0" 
maxOccurs="10">
                <xs:annotation>
                    <xs:documentation>Zero or more extended match key may be specified.  A 
certificate must match all of the specified key(s) to be selected.</xs:documentation>
                </xs:annotation>
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:whiteSpace value="collapse"/>
                        <xs:enumeration value="ServerAuth">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.1</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="ClientAuth">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.2</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="CodeSign">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.3</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="EmailProtect">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.4</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="IPSecEndSystem">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.5</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="IPSecTunnel">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.6</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="IPSecUser">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.7</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="TimeStamp">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.8</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="OCSPSign">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.9</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="DVCS">
                            <xs:annotation>
                                <xs:documentation>1.3.6.1.5.5.7.3.10</xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="CustomExtendedMatchKey" minOccurs="0" maxOccurs="10">
                <xs:annotation>
                    <xs:documentation>Zero or more custom extended match key may be 
specified.  A certificate must match all of the specified key(s) to be selected.  The key 
should be in OID form (e.g. 1.3.6.1.5.5.7.3.11)</xs:documentation>
                </xs:annotation>
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:whiteSpace value="collapse"/>
                        <xs:minLength value="1"/>
                        <xs:maxLength value="30"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="DistinguishedName">
        <xs:annotation>
            <xs:documentation>Certificate Distinguished Name matching allows for exact 
match criteria in the choosing of acceptable client certificates.</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="DistinguishedNameDefinition" maxOccurs="10">
                <xs:annotation>
                    <xs:documentation>This element represents the set of attributes to 
define a single Distinguished Name mathcing definition.</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Name">
                            <xs:annotation>
                                <xs:documentation>Distinguished attribute name to be used in 
mathcing.</xs:documentation>
                            </xs:annotation>
                            <xs:simpleType>
                                <xs:restriction base="xs:string">
                                    <xs:enumeration value="CN">
                                        <xs:annotation>
```

```
                                          <xs:documentation>Subject Common
Name</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="SN">
                                      <xs:annotation>
                                          <xs:documentation>Subject Sur
Name</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="GN">
                                      <xs:annotation>
                                          <xs:documentation>Subject Given
Name</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="N">
                                      <xs:annotation>
                                          <xs:documentation>Subject Unstruct
Name</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="I">
                                      <xs:annotation>
                                          <xs:documentation>Subject
Initials</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="GENQ">
                                      <xs:annotation>
                                          <xs:documentation>Subject Gen
Qualifier</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="DNQ">
                                      <xs:annotation>
                                          <xs:documentation>Subject Dn
Qualifier</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="C">
                                      <xs:annotation>
                                          <xs:documentation>Subject
Country</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="L">
                                      <xs:annotation>
                                          <xs:documentation>Subject
City</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="SP">
                                      <xs:annotation>
                                          <xs:documentation>Subject
State</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ST">
                                      <xs:annotation>
                                          <xs:documentation>Subject
State</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="O">
                                      <xs:annotation>
                                          <xs:documentation>Subject
Company</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="OU">
                                      <xs:annotation>
                                          <xs:documentation>Subject
Department</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="T">
                                      <xs:annotation>
                                          <xs:documentation>Subject
Title</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="EA">
                                      <xs:annotation>
                                          <xs:documentation>Subject Email
Address</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-CN">
                                      <xs:annotation>
                                          <xs:documentation>Issuer Common
Name</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-SN">
                                      <xs:annotation>
                                          <xs:documentation>Issuer Sur
Name</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-GN">
                                      <xs:annotation>
                                          <xs:documentation>Issuer Given
Name</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-N">
                                      <xs:annotation>
                                          <xs:documentation>Issuer Unstruct
Name</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-I">
                                      <xs:annotation>
                                          <xs:documentation>Issuer
Initials</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-GENQ">
                                      <xs:annotation>
                                          <xs:documentation>Issuer Gen
Qualifier</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-DNQ">
                                      <xs:annotation>
                                          <xs:documentation>Issuer Dn
Qualifier</xs:documentation>
```

```
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-C">
                                      <xs:annotation>
                                          <xs:documentation>Issuer
Country</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-L">
                                      <xs:annotation>
                                          <xs:documentation>Issuer City</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-SP">
                                      <xs:annotation>
                                          <xs:documentation>Issuer
State</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-ST">
                                      <xs:annotation>
                                          <xs:documentation>Issuer
State</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-O">
                                      <xs:annotation>
                                          <xs:documentation>Issuer
Company</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-OU">
                                      <xs:annotation>
                                          <xs:documentation>Issuer
Department</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-T">
                                      <xs:annotation>
                                          <xs:documentation>Issuer
Title</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="ISSUER-EA">
                                      <xs:annotation>
                                          <xs:documentation>Issuer Email
Address</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                              </xs:restriction>
                          </xs:simpleType>
                      </xs:element>
                      <xs:element name="Pattern" nillable="false">
                          <xs:annotation>
                              <xs:documentation>The string to use in the
match.</xs:documentation>
                          </xs:annotation>
                          <xs:simpleType>
                              <xs:restriction base="xs:string">
                                  <xs:minLength value="1"/>
                                  <xs:maxLength value="30"/>
                                  <xs:whiteSpace value="collapse"/>
                              </xs:restriction>
                          </xs:simpleType>
```

```
                        </xs:element>
                    </xs:sequence>
                    <xs:attribute name="Wildcard" default="Disabled">
                        <xs:annotation>
                            <xs:documentation>Should the pattern include wildcard pattern
matching.  With wildcarding enabled, the pattern can be anywhere in the
string.</xs:documentation>
                        </xs:annotation>
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:enumeration value="Disabled">
                                    <xs:annotation>
                                        <xs:documentation>wildcard pattern match is not
enabled for this definition</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="Enabled">
                                    <xs:annotation>
                                        <xs:documentation>wildcard pattern match is enabled
for this definition</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:attribute>
                    <xs:attribute name="Operator" default="Equal">
                        <xs:annotation>
                            <xs:documentation>The operator to be used in performing the
match</xs:documentation>
                        </xs:annotation>
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:enumeration value="Equal">
                                    <xs:annotation>
                                        <xs:documentation>equivalent to
==</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="NotEqual">
                                    <xs:annotation>
                                        <xs:documentation>equivalent to
!=</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:attribute>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="AnyConnectProfile" type="ns1:AnyConnectClientProfile">
        <xs:annotation>
            <xs:documentation>The root element representing the AnyConnect Client
Profile</xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:simpleType name="simpleBinary">
        <xs:restriction base="xs:string">
            <xs:enumeration value="true">
                <xs:annotation>
                    <xs:documentation>enables the Start Before Logon
feature</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="false">
                <xs:annotation>
                    <xs:documentation>disables the Start Before Logon 
feature.</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

APPENDIX B

Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users

An Active Directory Domain Administrator can push a group policy to domain users that adds the security appliance to the list of trusted sites in Internet Explorer. Note that this differs from the procedure to add the security appliance to the list of trusted sites by individual users, described in Adding a Security Appliance to the List of Trusted Sites (Internet Explorer), page 2-3. This procedure applies only to Internet Explorer on Windows machines that are managed by a domain administrator.

Note Adding a security appliance to the list of trusted sites for Internet Explorer is required for those running Windows Vista who want to use WebLaunch.

To create a policy to add the Security Appliance to the Trusted Sites security zone in Internet Explorer by Group Policy using Active Directory, perform the following steps:

Step 1 Log on as a member of the Domain Admins group.

Step 2 Open the Active Directory Users and Computers MMC snap-in.

Step 3 Right-click the Domain or Organizational Unit where you want to create the Group Policy Object and click Properties.

Step 4 Select the Group Policy tab.

Step 5 Click New.

Step 6 Type a name for the new Group Policy Object and press Enter.

Step 7 To prevent this new policy from being applied to some users or groups, click Properties. Select the Security tab. Add the user or group that you want to *prevent* from having this policy, then clear the Read and the Apply Group Policy check boxes in the Allow column. Click OK.

Step 8 Click Edit.

Step 9 Navigate to User Configuration > Windows Settings > Internet Explorer Maintenance > Security.

Step 10 Right-click Security Zones and Content Ratings in the right-hand pane and click Properties.

Step 11 Select Import the current security zones and privacy settings. If prompted, click Continue.

Step 12 Click Modify Settings.

Step 13 Select Trusted Sites and click Sites.

Step 14 Type the URL for the Security Appliance that you want to add to the list of Trusted Sites and click Add. The format can contain a hostname (https://vpn.mycompany.com) or IP address (https://192.168.1.100). It can be an exact match (https://vpn.mycompany.com) or a wildcard (https://*.mycompany.com).

Step 15 Click Close (or OK and OK).

Step 16 Click Close (or OK until all dialog boxes are closed, and close any snap-in window)s.

Step 17 Allow sufficient time for the policy to propagate throughout the domain or forest.

INDEX