Cisco AnyConnect VPN Client Administrator Guide

Version 2.3

Revised: June 01, 2009

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-16159-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

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).

Cisco AnyConnect VPN Client Administrator Guide

CONTENTS

CHAPTER 5

CHAPTER 6

APPENDIX A

APPENDIX B

About This Guide

The following sections introduce this guide:

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 configure security 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, "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 3, "Configuring AnyConnect Features Using the CLI"	Describes how to use ASDM to configure the various features of the Cisco AnyConnect VPN Client on the security appliance.
Chapter 4, "Configuring and Using AnyConnect Client Operating Modes and User Profiles"	Describes how to configure and use AnyConnect client operating modes and XML users profiles.
Chapter 5, "Customizing and Localizing the AnyConnect Client and Installer"	Describes how to customize and localize the end-user interface of the Cisco AnyConnect VPN Client.
Chapter 6, "Monitoring and Maintaining the AnyConnect Client"	Describes how to monitor and maintain the Cisco AnyConnect VPN Client using the security appliance

Table 1 Document Organization (continued)

Chapter/Appendix	Definition
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

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

Original SSLeay License:

CHAPTER 1

Introduction

This guide 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.

This chapter introduces the Cisco AnyConnect VPN Client and contains the following sections:

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. See *Release Notes for Cisco Anyconnect VPN Client, Release 2.3* for the latest information about these features:

- Support for Windows Mobile OS touch-screen devices connecting to Cisco Series 5500 Adaptive Security Appliances. For a list of supported devices, see *Release Notes for Cisco Anyconnect VPN Client, Release 2.3.*

Note Windows Mobile requires a special license and must have ASA Release 8.0.3 or higher running on the security appliance.

- Machine certificate access for authentication (standalone mode only). Any logged-in user on the system in standalone mode can have access to available machine certificates, as well as to user certificates, for VPN authentication.
- The AnyConnect client for Windows Mobile requires that a security appliance mobile license be installed. If the correct license is not installed, end user receives an error message.
- Dynamic Updating of the user interface when changing groups.
- Enhancements to the management of user preferences, including a new profile template and more customizable attributes.
- Enhancements to Application Programming Interface (API), for customers who want to automate a VPN connection with the AnyConnect client from another application, including the following:
  - Preferences
  - Set tunnel-group method

  The API package contains documentation, source files, and library files to support a C++ interface for the Cisco AnyConnect VPN Client. There are libraries and example programs that can be used for building on Windows, Linux and MAC (10.4 or higher) platforms. The Makefiles (or project files) for the Windows platform are also included. For other platforms, there is a platform specific script showing how to compile the example code. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.
- Support for the Component Object Module (COM) technology for Microsoft Windows (not Windows Mobile) environments—COM is a metadata-based protocol that allows programming languages—for example, C++, C#, and Visual Basic—to interact with it. Users can write their own applications in C++, C#, or Visual Basic to interact with the AnyConnect client. These applications can include anything from a new user interface to a simple monitoring/statistical application. Source code for three fully functional sample programs, built with Visual Studio 2005 SP 1 or later, are included with the download in the apiDoc examples directory. The documentation for COM is bundled with the package. See *Release Notes for Cisco Anyconnect VPN Client, Release 2.3* for a summary of the examples included with the COM package.
- 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 OS X, and Linux only).

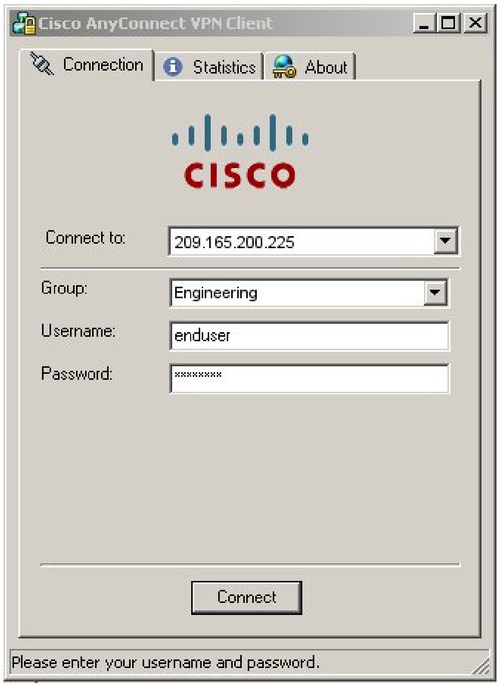
- Start Before Login (SBL)—Allows for login scripts, password caching, drive mapping, and more, for Windows.
- Certificate-only authentication—Allows users to connect with a digital certificate and not provide a user ID and password.
- Simultaneous AnyConnect client and clientless, browser-based connections—Allows 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.
- Support for Start Before Logon for Windows Vista systems, in addition to other Windows operating systems.
- Extended customization and localization features—This version of the AnyConnect client includes enhanced customization features and language translation features. In previous versions, you could customize client installations only on an individual PC basis. With this version, the security appliance can customize the client as it downloads and installs the client on the remote PC. You can also translate the client installer. These extended features include the following items:
  - Localized installs using localized MSI transforms (Windows only).
  - Custom MSI transforms (Windows only).
  - User-defined resource files.
  - Third-party GUI/CLI support.
  - Localization for Mac OS X (10.4 and higher).
- New systray icon—System tray now shows an icon when the AnyConnect client is reconnecting after losing connectivity.
- Application Programming Interface (API)—Lets you create your own GUI and invoke your own programming routines.

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

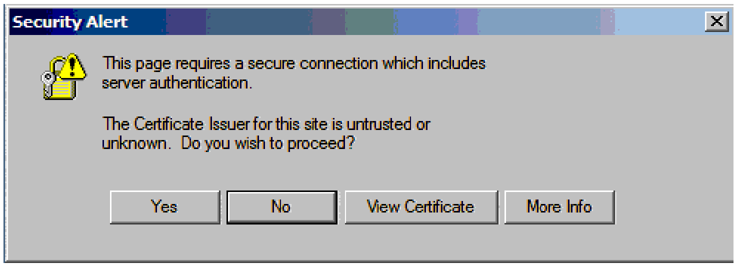


Connect to: 209.165.200.225
Group: Engineering
Username: enduser
Password: ********

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.

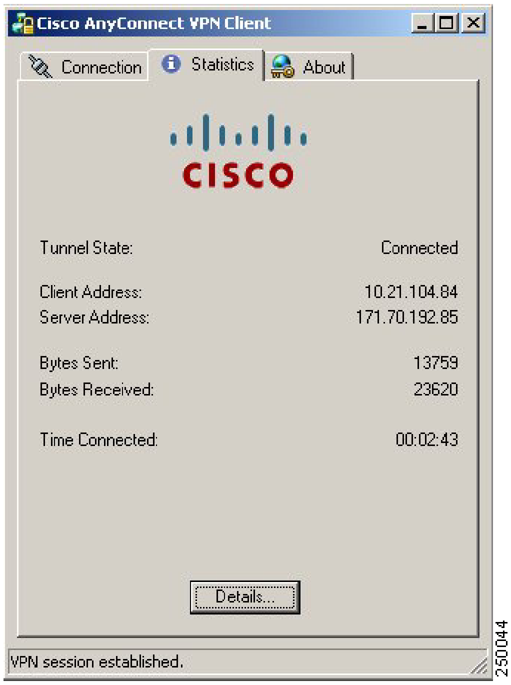
The Security Alert dialog box appears only on the first connection attempt to a given security appliance. After the connection is successfully established, the "thumbprint" of the server certificate is saved in the preferences file, so the user is not prompted on subsequent connections to the same security 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 Configuring and Using User Profiles, page 4-5 and Adding a Security Certificate in Response to Browser Alert Windows, page 2-19.

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

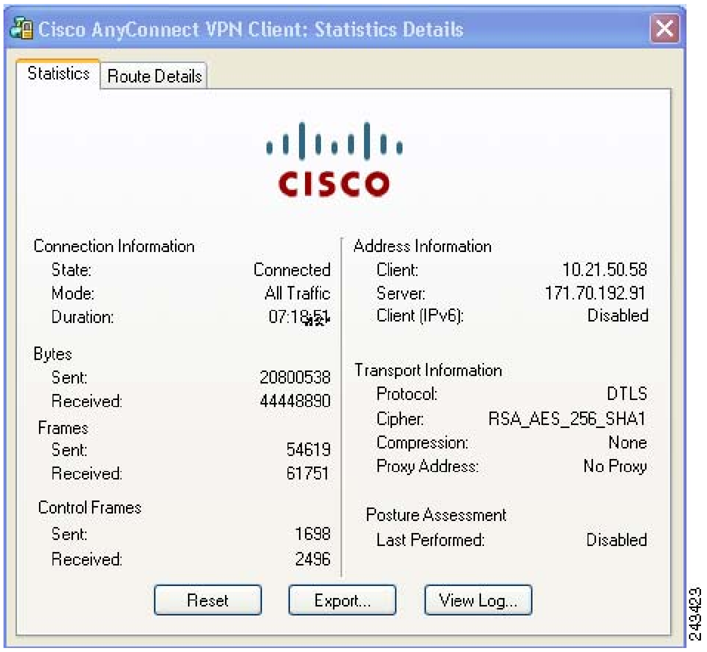
Bytes Sent: 13759
Bytes Received: 23620

Time Connected: 00:02:43

VPN session established.

Clicking the Details button opens the Statistics Details window (Figure 1-4). The Statistics tab connection statistics, 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
State: Connected
Mode: All Traffic
Duration: 07:18:51

Bytes
Sent: 20800538
Received: 44448890

Frames
Sent: 54619
Received: 61751

Control Frames
Sent: 1698
Received: 2496

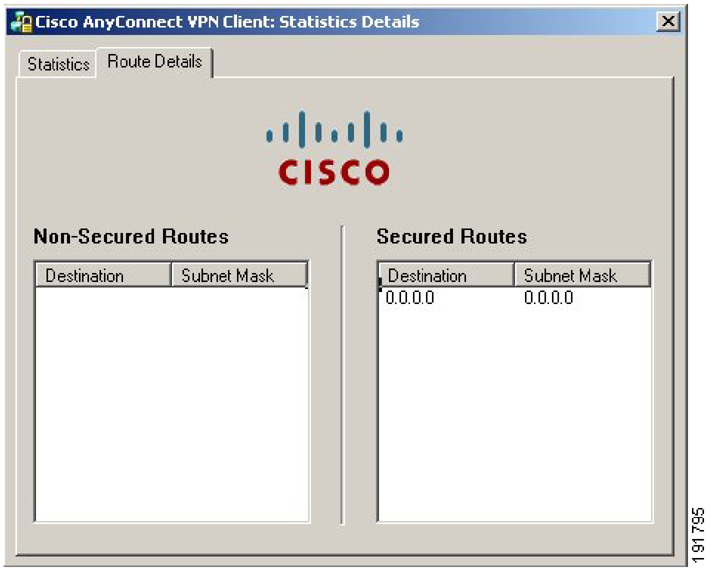
Address Information
Client: 10.21.50.58
Server: 171.70.192.91
Client (IPv6): Disabled

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. See Viewing Detailed Statistical Information, page 6-4 for information about using the Export and View Log buttons for connection monitoring.

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



Non-Secured Routes

Destination	Subnet Mask

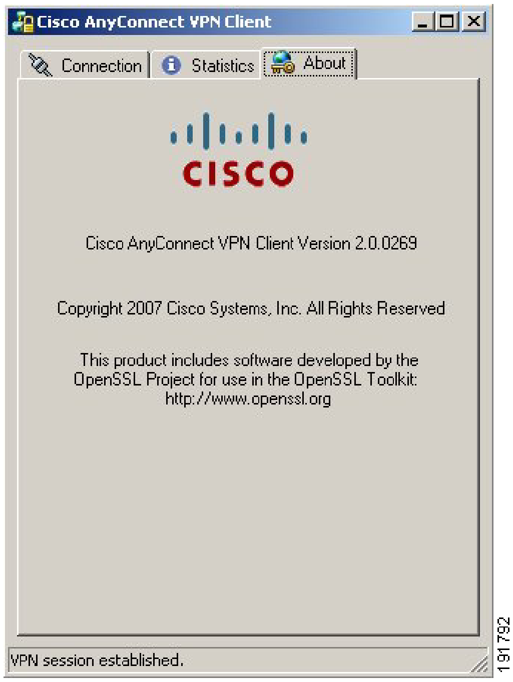
Secured Routes

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

The latest Release Notes document contains the system requirements and detailed instructions for getting and installing the necessary files. The Windows Vista version of AnyConnect (32- and 64-bit) supports everything that the Windows 2000 and Windows XP versions support, including 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. See Appendix A, “Sample AnyConnect Profile” for a sample AnyConnect user profile.

Where to Find the AnyConnect Client Files

To get the AnyConnect client files and API package, go to http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect.

Note The API package contains documentation, source files, library files, and binaries to support a C++ interface for the Cisco AnyConnect VPN Client.There are libraries and example binaries for Windows, Linux, and Mac (10.4 or higher) platforms. The Makefiles (or project files) for these platforms are also included. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.

Installing Start Before Logon Components (Windows Only)

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

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

Configuring AnyConnect Features Using ASDM

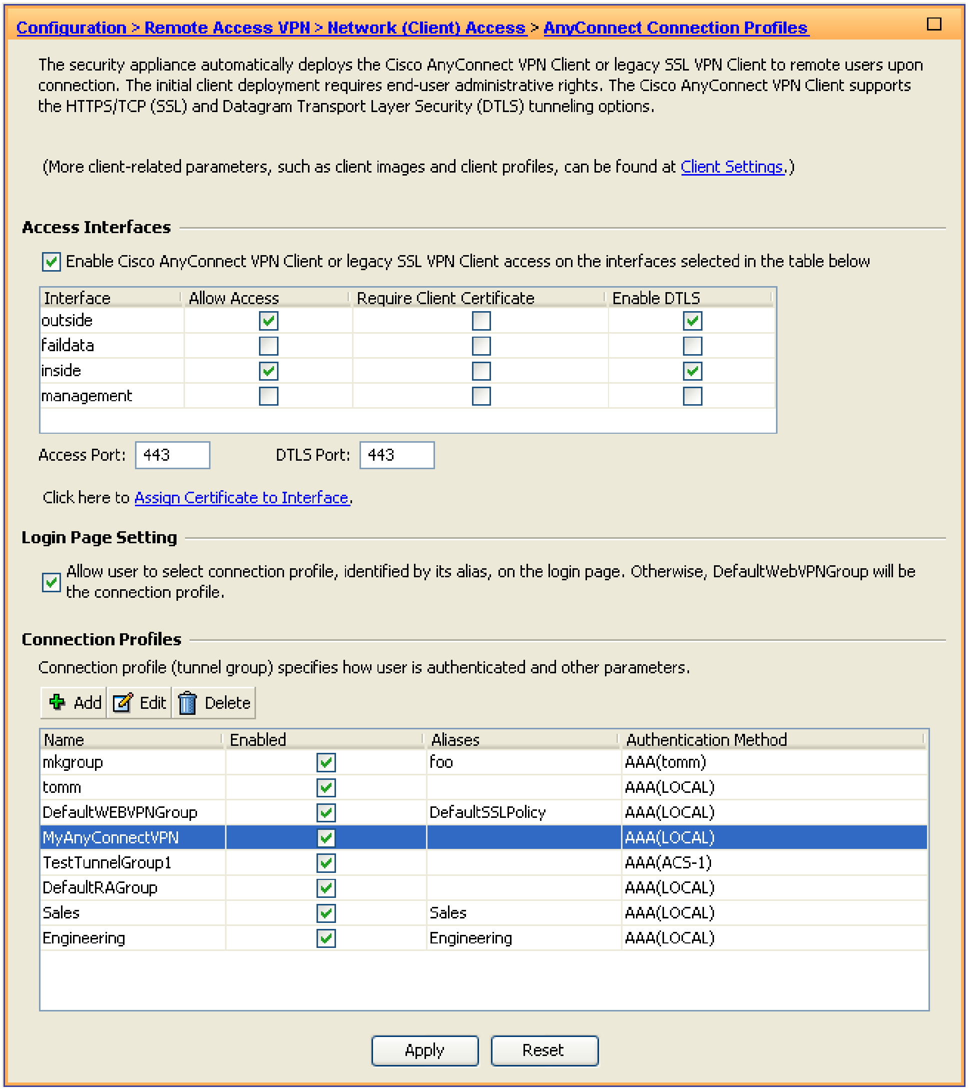
The security appliance automatically deploys the Cisco AnyConnect VPN client to remote users upon connection. The initial client deployment requires end-user administrative rights. The AnyConnect client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Settings (DTLS) tunneling options. This chapter describes how to use ASDM to configure AnyConnect features.

You configure the AnyConnect client features on the security appliance, as described in the following sections:

Enabling the SSL VPN Client Protocol

The AnyConnect client uses the SSL VPN protocol, therefore you must enable the SSL VPN Client protocol as part of the configuration process. To do this, select Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. The AnyConnect Connection Profiles window appears (Figure 2-1).

Figure 2-1 AnyConnect Connection Profiles Window



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect 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	☑	□	☑
faildata	□	□	□
inside	☑	□	☑
management	□	□	□

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

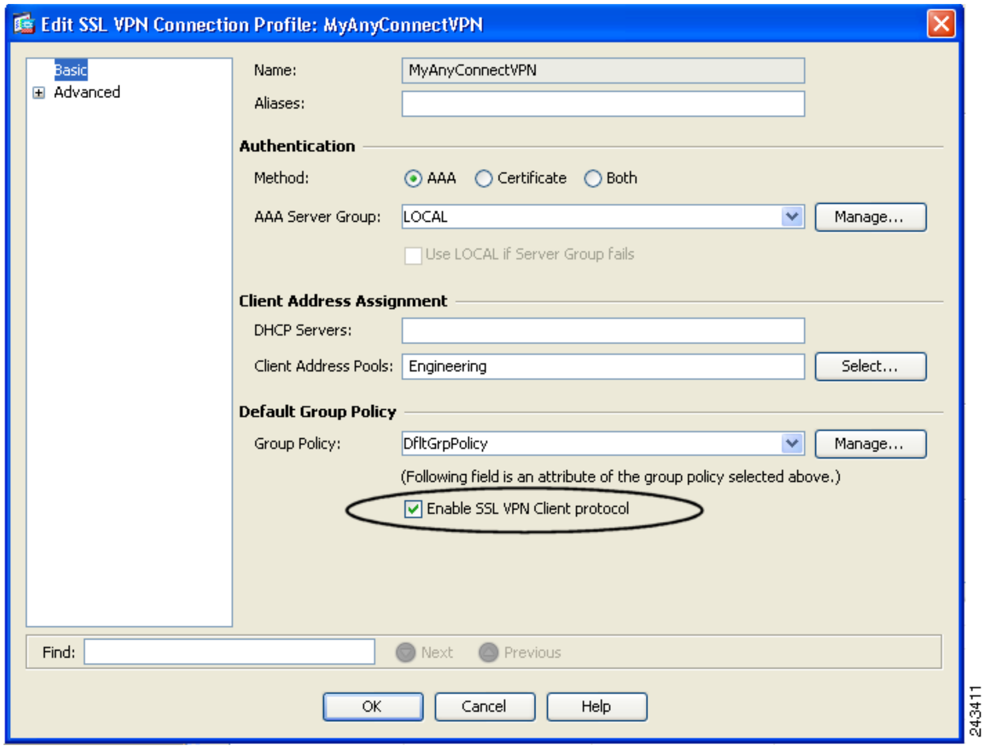
Name	Enabled	Aliases	Authentication Method
mkgroup	☑	foo	AAA(tomm)
tomm	☑		AAA(LOCAL)
DefaultWEBVPNGroup	☑	DefaultSSLPolicy	AAA(LOCAL)
MyAnyConnectVPN	☑		AAA(LOCAL)
TestTunnelGroup1	☑		AAA(ACS-1)
DefaultRAGroup	☑		AAA(LOCAL)
Sales	☑	Sales	AAA(LOCAL)
Engineering	☑	Engineering	AAA(LOCAL)

243412

In the Access Interfaces area, select the check box to enable Cisco AnyConnect VPN Client access on the interfaces selected in the table.

In the Connection Profiles area of the window, select the profile you want to configure, then click Add or Edit. The Add or Edit SSL VPN Connection Profile dialog box appears, with Basic selected in the navigation panel (Figure 2-2). If you are using the Default Group Policy, select the check box for Enable SSL VPN Client Protocol and click OK.

Figure 2-2 Edit SSL VPN Connection Profile Dialog Box



Edit SSL VPN Connection Profile: MyAnyConnectVPN

Basic
⊞ Advanced

Name: MyAnyConnectVPN
Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both
AAA Server Group: LOCAL
□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:
Client Address Pools: Engineering

Default Group Policy

Group Policy: DfltGrpPolicy
(Following field is an attribute of the group policy selected above.)
☑ Enable SSL VPN Client protocol

Find:

Configuring the Login Page Setting

To allow the user to select a connection profile, identified by its alias, on the login page, select the check box in the Login Page Setting area of the AnyConnect Connection Profiles window (Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles). If you do not select this feature, the AnyConnect client uses the DefaultWebVPNGroup profile as the connection profile.

To specify an alias for a connection profile, first select the profile in the AnyConnect Profile window and click Add or Edit, as above. On the Add of Edit SSL VPN Connection profile dialog box, select Advanced > SSL VPN and in the Connection Aliases area, click Add. The Add Connection Alias dialog box appears. Specify an alias to use for this connection profile, and click Enabled, then OK. The alias you specify appears in the Aliases field of the AnyConnect Connection Profiles window.

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).

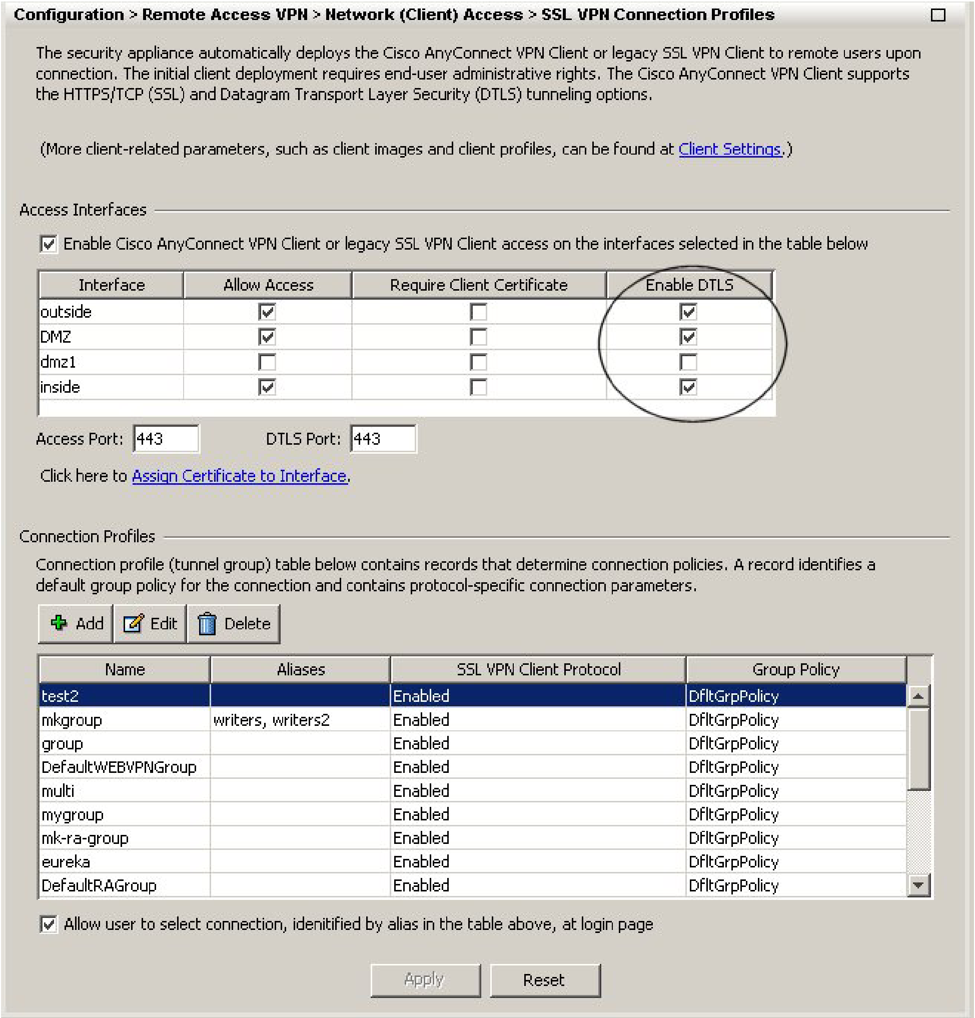
Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications 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 2-3).

Figure 2-3 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.

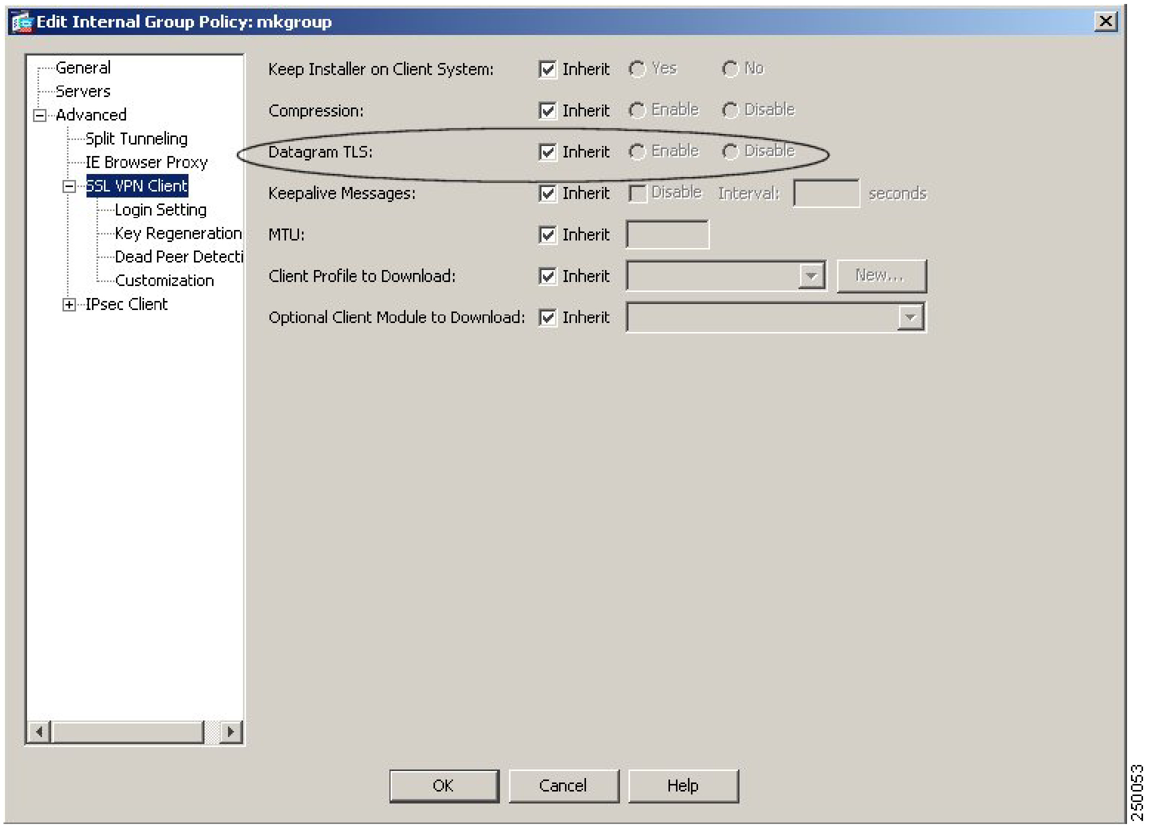
Enabling DTLS allows the AnyConnect client establishing an AnyConnect VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive 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 2-4 shows an example of configuring the DTLS setting for an internal group policy.

Figure 2-4 Enabling or Disabling DTLS



Edit Internal Group Policy: mkgroup

- 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

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 2-5).

Figure 2-5 Edit User Account Dialog Box for Prompt Setting

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.

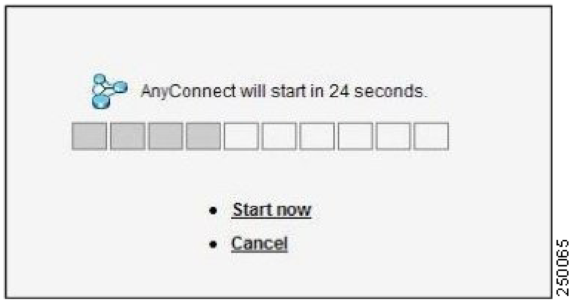
When you enable the prompting option, another field becomes available, asking you to specify the number of seconds the user has to choose before the Default Post Login selection takes effect.

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 2-6 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 2-6 Prompt Displayed to Remote Users for SSL VPN Client Download



AnyConnect will start in 24 seconds.

Enabling Modules for Additional AnyConnect Features

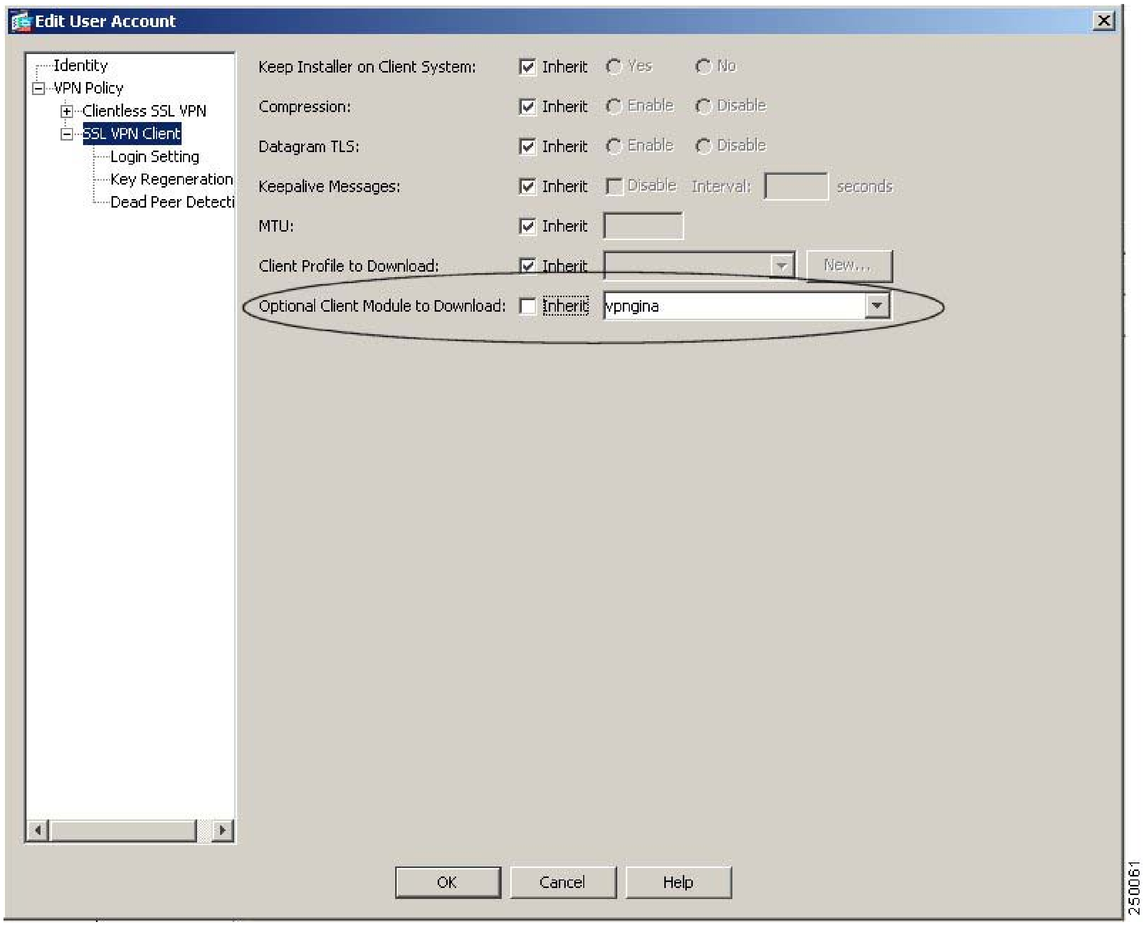
As new features are released for the AnyConnect client, you must update the AnyConnect clients of your remote users for them to use the new features. To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of modules that it needs for each feature that it 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, **vpngina** for the Start Before Logon feature—in the Optional Client Module to Download field. Separate multiple strings with commas. Figure 2-7 shows an example.

Figure 2-7 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 file. See Configuring Profile Attributes, page 4-10 for details.

Note For Release 2.3, you can select **vpngina** from the drop-down list or manually enter the keyword into the field. This enables Start Before Logon for Windows Vista, Windows XP, and Windows 2000. If you have downloaded the Beta software for DART (Diagnostic Analysis and Reporting Tool), you can also enter the keyword **dart** into this field, either alone or in combination with **vpngina**, as long as these values are separated by a comma.

Configuring, Enabling, and Using Other AnyConnect Features

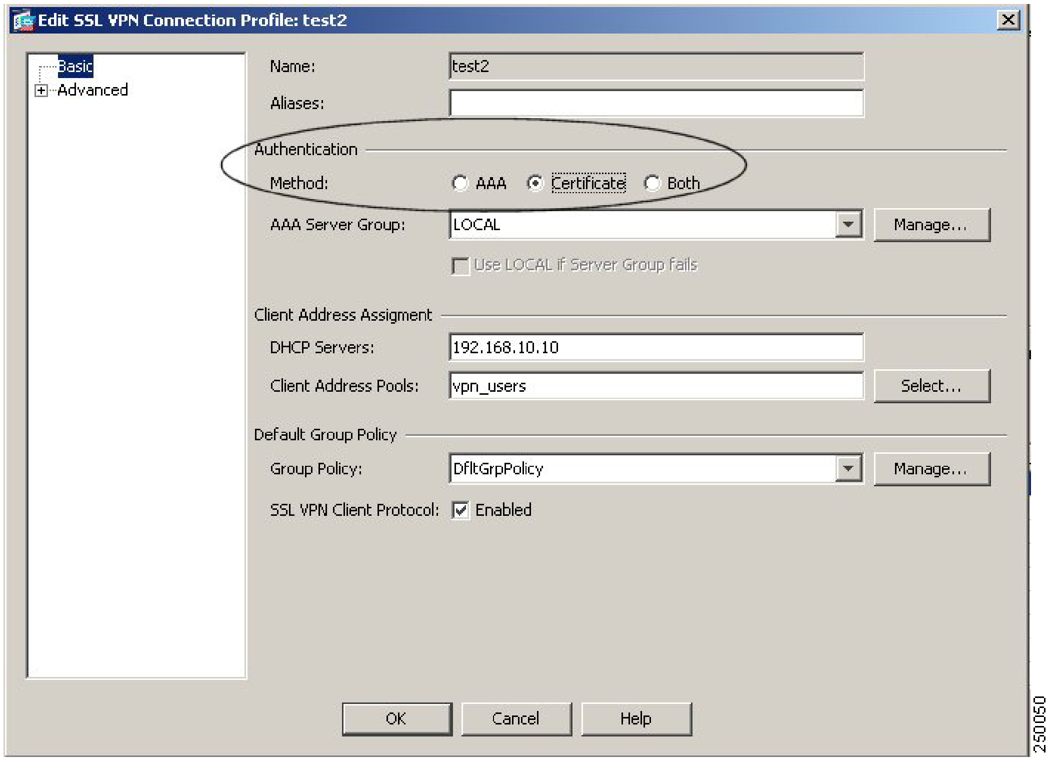
The following sections describe how to configure other AnyConnect features. Some features, such as Secure Desktop and dynamic access policies, do not require that you specifically configure the AnyConnect client to interact with that feature. Rather, all configuration for those features occurs on the 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 a 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 2-8 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

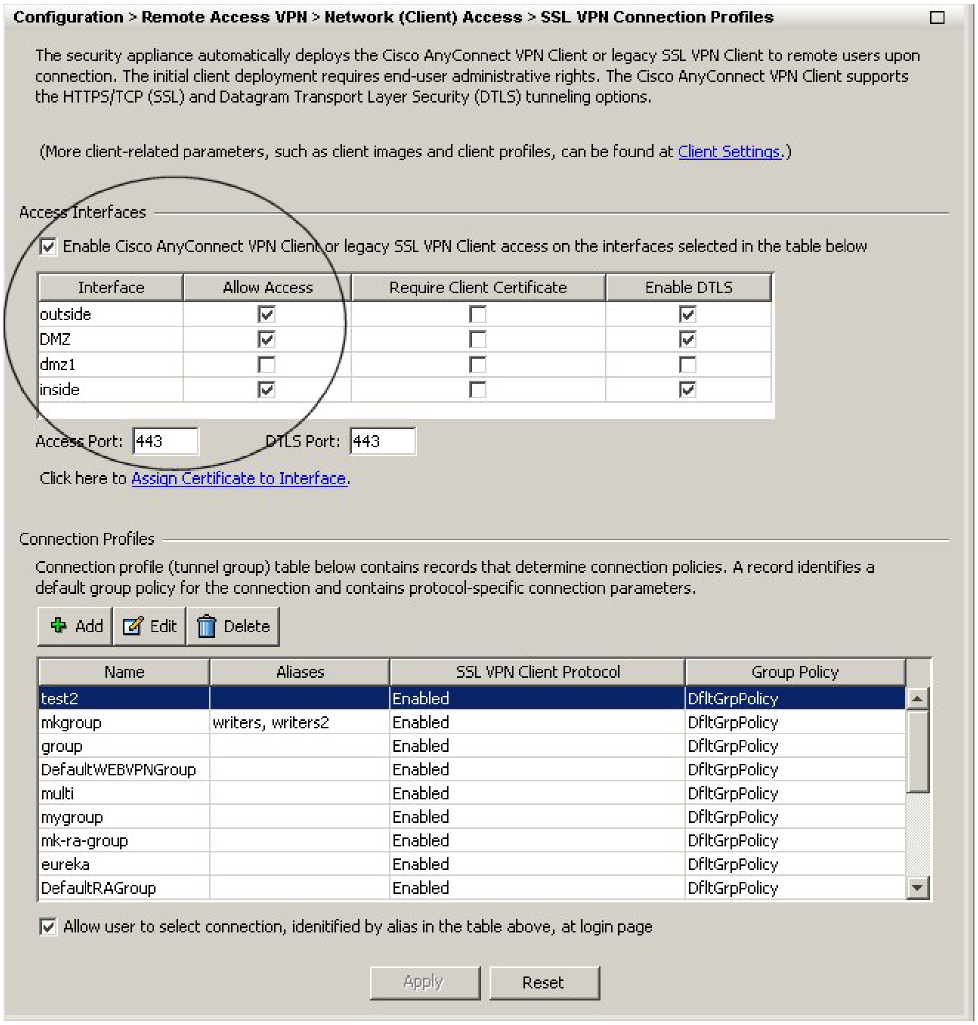
Default Group Policy

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 2-9) appears.

Figure 2-9 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.

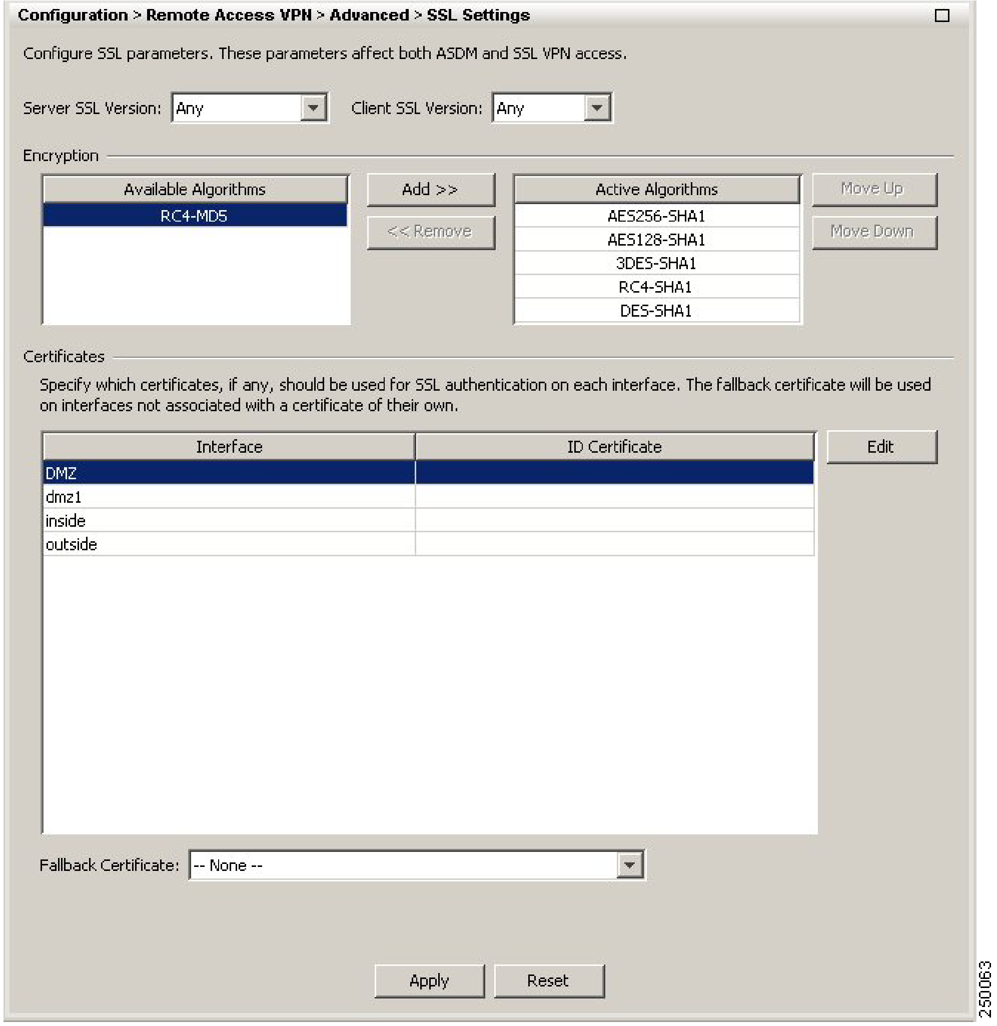
Name	Aliases	SSL VPN Client Protocol	Group Policy
test2		Enabled	DfltGrpPolicy
mkgroup	writers, writers2	Enabled	DfltGrpPolicy
group		Enabled	DfltGrpPolicy
DefaultWEBVPNGroup		Enabled	DfltGrpPolicy
multi		Enabled	DfltGrpPolicy
mygroup		Enabled	DfltGrpPolicy
mk-ra-group		Enabled	DfltGrpPolicy
eureka		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 2-10).

Figure 2-10 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
RC4-MD5

Active Algorithms
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.

Note The AnyConnect client for Windows Mobile does not support compression.

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

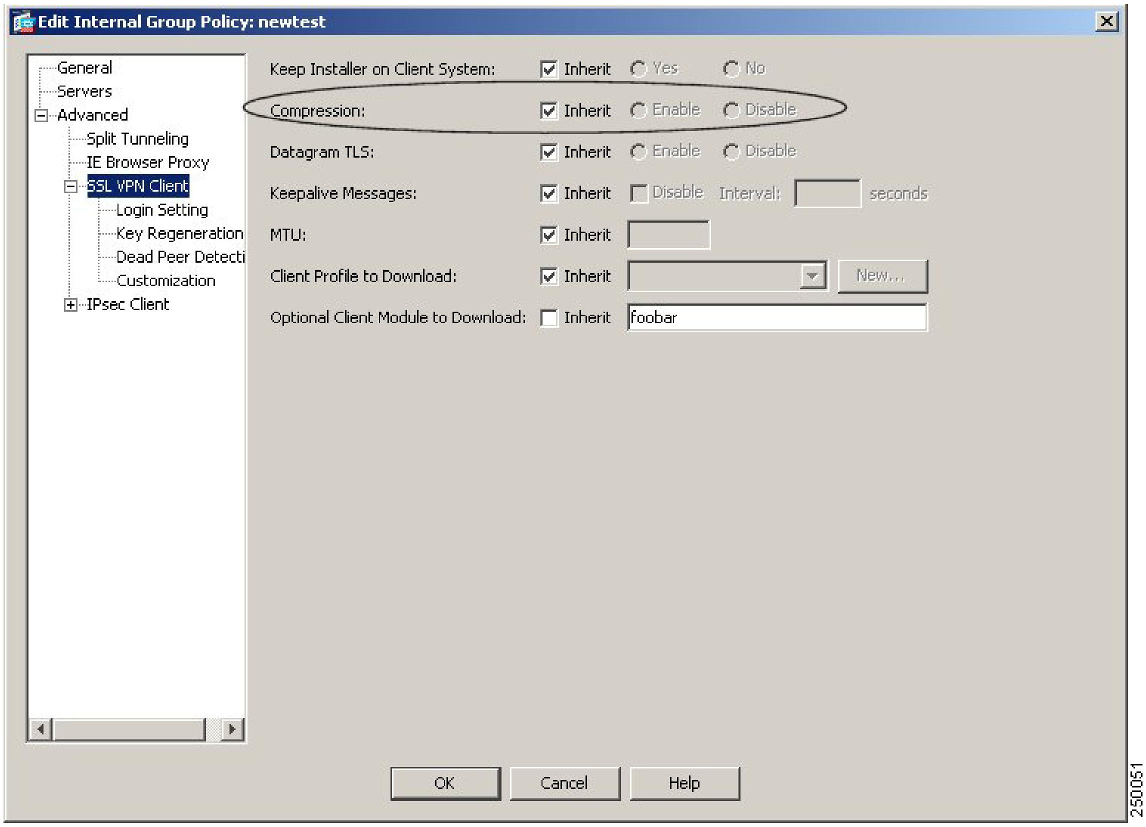
You can also configure compression for specific groups or users using ASDM with the **svc compression** command in group-policy and username webvpn modes. The global setting overrides the group-policy and username settings.

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 2-11 shows an example of configuring the compression setting for an internal group policy.

Figure 2-11 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.

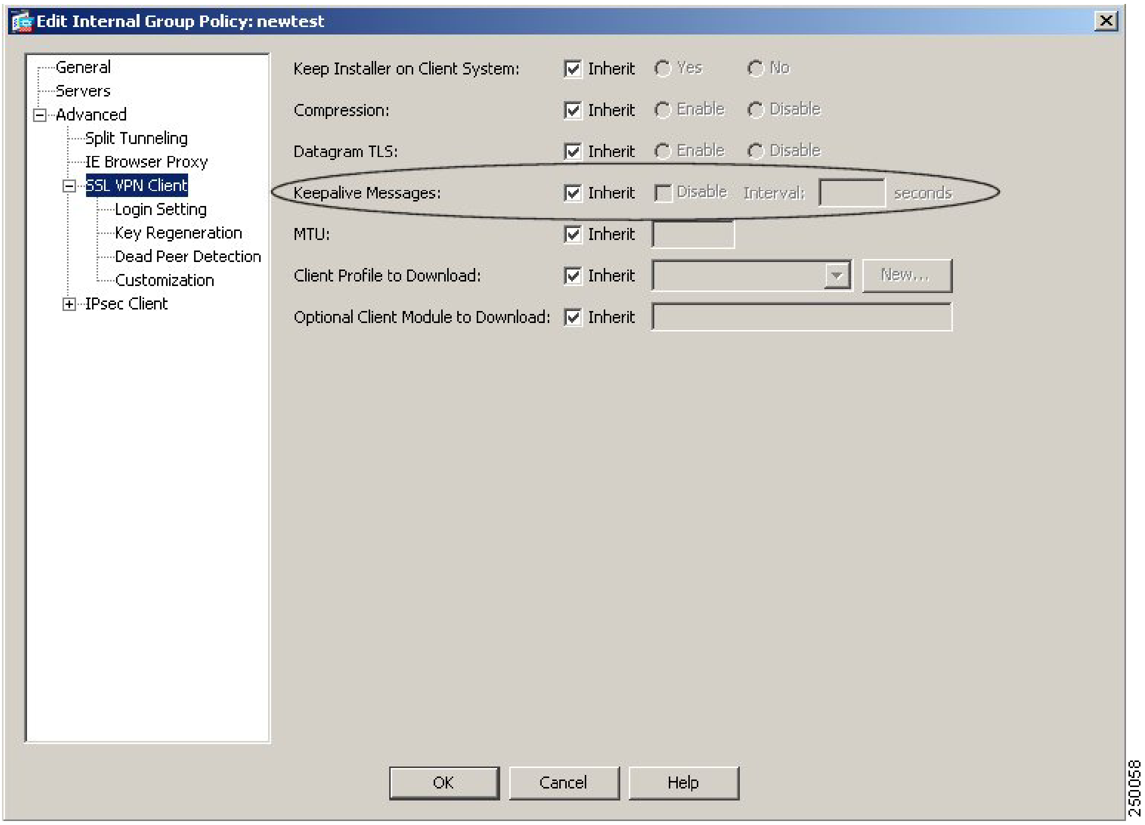
To set the frequency of keepalive messages, use the Keepalive Messages setting in either Group Policy or Username. The paths to this setting are:

- 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 2-12 shows an example of configuring the keepalive messages setting for an internal group policy.

Figure 2-12 Configuring Keepalive Messages



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.

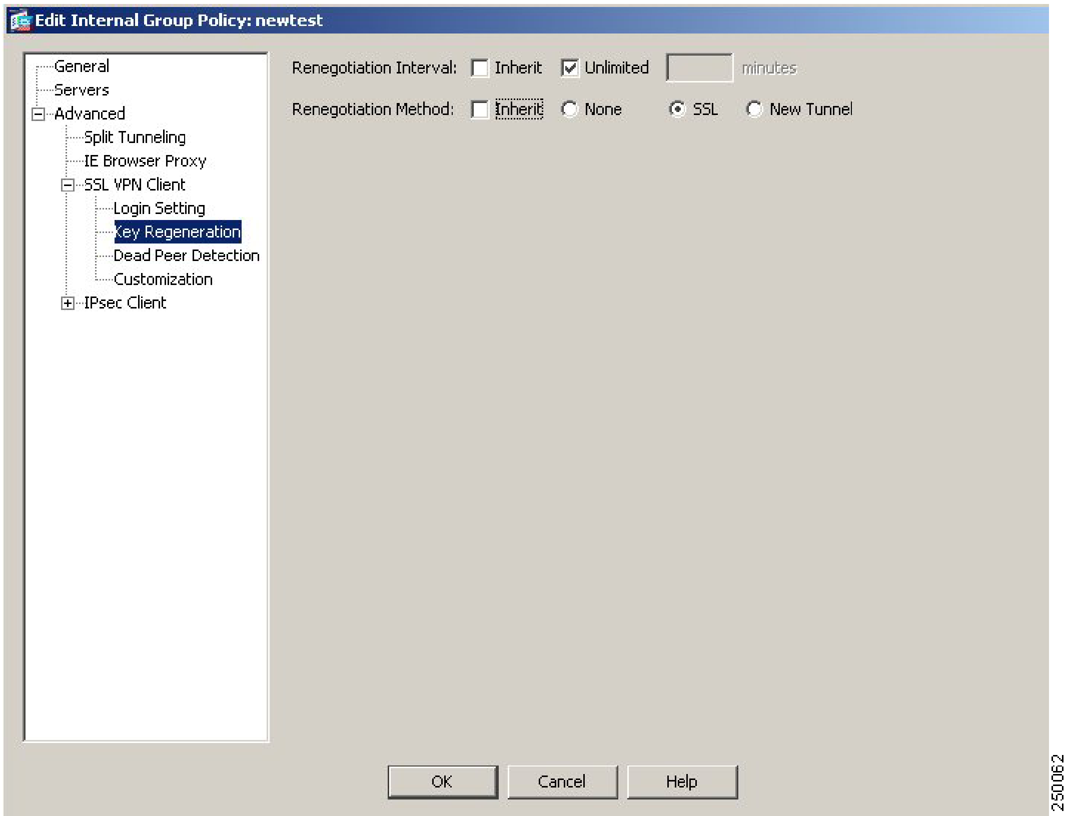
To enable Rekey, use the Key Regeneration dialog box in either Group Policy or Username. The paths to this setting are:

- 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 2-13 shows an example of configuring the Rekey setting for an internal group policy.

Figure 2-13 Configuring Rekey Attributes



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.

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.

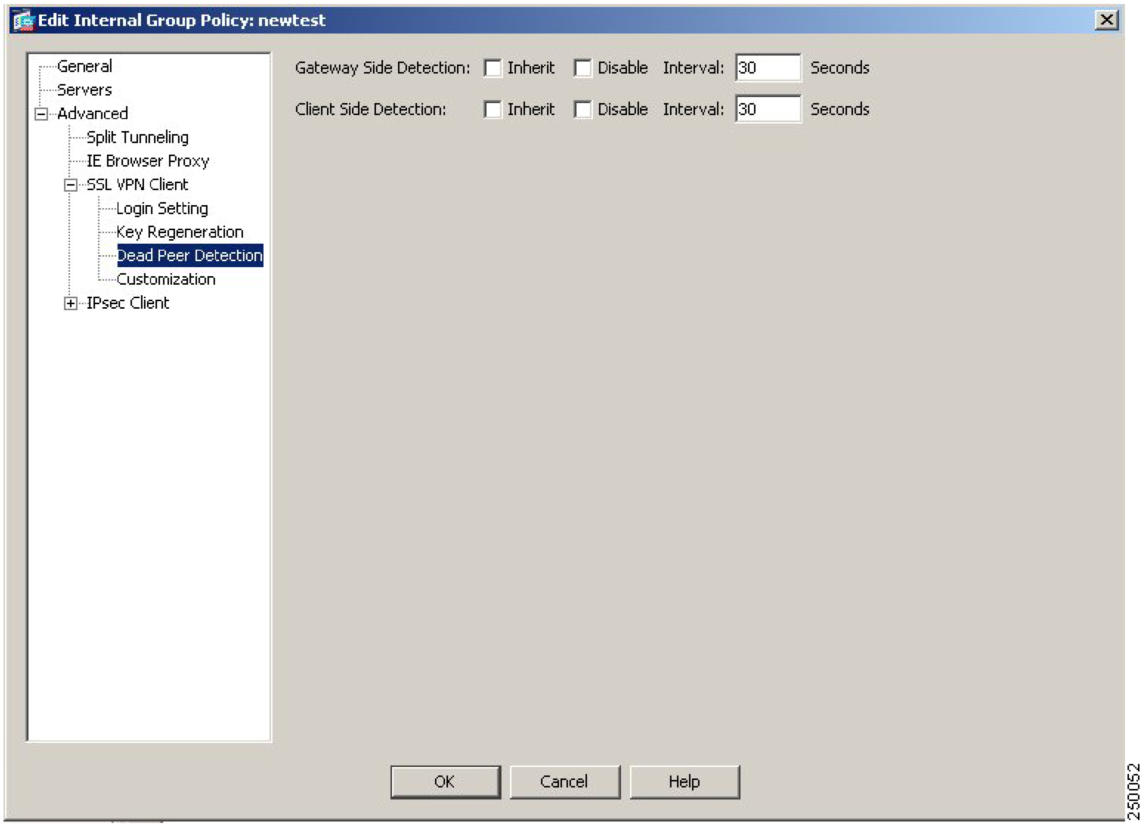
Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection must be enabled in the group policy on the security appliance to allow the AnyConnect client to fall back to TLS, if necessary. Fallback to TLS occurs if the AnyConnect client cannot send data over the UPD/DTLS 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 2-14 shows an example of configuring the Dead Peer Detection setting for an internal group policy.

Figure 2-14 ***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.*

Configuring 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 3.4)*.

Configuring Windows Mobile Support Using ASDM

You configure AnyConnect client Windows Mobile support just as you would any other Windows platform, with the following considerations:

- Windows Mobile connections require a special license, which you install just as you would any other AnyConnect client license. If you do not have this licensed installed, Windows Mobile connections do not work.
- See the latest version of *Release Notes for Cisco AnyConnect VPN Client* for detailed, current information about Windows Mobile device support.
- AnyConnect client Windows Mobile connections do not support compression.
- Windows Mobile connections can use the default profile values, but you can configure a profile that specifies mobile policy device lock parameters. See Configuring Windows Mobile Policy, page 4-22 for details on configuring the Windows Mobile parameters.

Note The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, 5.0AKU2, and 6.0, but not on Windows Mobile 6.1.

- If you have configured a profile specifically for Windows Mobile, then under Group Policy, select a client profile to download that has Windows Mobile support enabled. Select Configuration > Remote Access VPN > Network (Client) Access > Group Policies, then click Add or Edit to either add a group policy or edit an existing one. The Add or Edit Group Policy dialog box appears. Select Advanced > SSL VPN Client and specify a client profile to download.

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

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

Note This is required on Windows Vista to use WebLaunch.

Step 1 Go to Tools | Internet Options | Trusted Sites.

The Internet Options window opens.

Step 2 Click the Security tab.

Step 3 Click the Trusted Sites icon.

Step 4 Click Sites.

The Trusted Sites window opens.

Step 5 Type the host name or IP address of the security appliance. Use a wildcard such as https://*.yourcompany.com to allow all ASA 5500s within the yourcompany.com domain to be used to support multiple sites.

Step 6 Click Add.

Step 7 Click OK.

The Trusted Sites window closes.

Step 8 Click OK in the Internet Options window.

Adding a Security Certificate in Response to Browser Alert Windows

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

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

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

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

Install the certificate as a trusted root certificate as follows:

Step 1 Click View Certificate in the Security Alert window.

The Certificate window opens.

Step 2 Click Install Certificate.

The Certificate Import Wizard Welcome opens.

Step 3 Click Next.

The Certificate Import Wizard – Certificate Store window opens.

Step 4 Select "Automatically select the certificate store based on the type of certificate."

Step 5 Click Next.

The Certificate Import Wizard – Completing window opens.

Step 6 Click Finish.

Step 7 Another Security Warning window prompts "Do you want to install this certificate?" Click Yes.

The Certificate Import Wizard window indicates the import is successful.

Step 8 Click OK to close this window.

Step 9 Click OK to close the Certificate window.

Step 10 Click Yes to close the Security Alert window.

The security appliance window opens, signifying the certificate is trusted.

In Response to a Netscape, Mozilla, or Firefox "Certified by an Unknown Authority" Window

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

```
    Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

Install the certificate as a trusted root certificate as follows:

Step 1 Click the Examine Certificate button in the "Web Site Certified by an Unknown Authority" window.

The Certificate Viewer window opens.

Step 2 Click the "Accept this certificate permanently" option.

Step 3 Click OK.

The security appliance window opens, signifying the certificate is trusted.

CHAPTER 3

Configuring AnyConnect Features Using the CLI

The security appliance automatically deploys the Cisco AnyConnect VPN client to remote users upon connection. The initial client deployment requires end-user administrative rights. The AnyConnect client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Settings (DTLS) tunneling options. This chapter describes how to use ASDM to configure AnyConnect features.

You configure the AnyConnect client features on the security appliance, as described in the following sections:

Enabling the SSL VPN Client Protocol

The AnyConnect client uses the SSL VPN protocol, therefore you must enable the SSL VPN Client protocol as part of the configuration process. To do this, use the **svc enable** command in webvpn configuration mode.

Configuring the Login Page Setting

To allow the user to select a connection profile, identified by its alias, on the login page, use the **tunnel-group-list enable** command in webvpn configuration mode. If you do not configure this feature, the AnyConnect client uses the DefaultWebVPNGroup profile as the connection profile.

To specify an alias for a connection profile, use the **group-alias enable** in tunnel-group webvpn-attributes configuration mode.

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*

The following example enters group policy webvpn configuration mode and specifies port 444 for DTLS:

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

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.

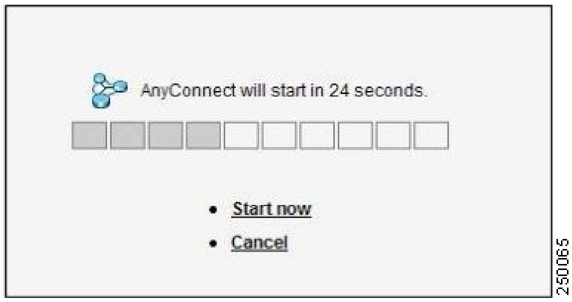
svc ask enable default webvpn immediately goes to the portal page.

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 3-1 shows the prompt displayed to remote users when either **default svc timeout** *value* or **default webvpn timeout** *value* is configured:

Figure 3-1 Prompt Displayed to Remote Users for SSL VPN Client Download



The following example configures the security appliance to prompt the remote user to download the client or go to the 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 OS X, 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 a digital certificate and are not required to provide a user ID and password. To configure certificate-only authentication using the 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.

Note the AnyConnect client for Windows Mobile does not support compression.

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.

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
```

Configuring Windows Mobile Support Using ASDM

You configure AnyConnect client Windows Mobile support just as you would any other Windows platform, with the following considerations:

- Windows Mobile connections require a special license, which you install just as you would any other AnyConnect client license. If you do not have this licensed installed, Windows Mobile connections do not work.
- See the latest version of *Release Notes for Cisco AnyConnect VPN Client* for detailed, current information about Windows Mobile device support.
- AnyConnect client Windows Mobile connections do not support compression.
- Windows Mobile connections can use the default profile values, but you can configure a profile that specifies mobile policy device lock parameters. See Configuring Windows Mobile Policy, page 4-22 for details on configuring the Windows Mobile parameters.

Note The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, 5.0AKU2, and 6.0, but not on Windows Mobile 6.1.

- If you have configured a profile specifically for Windows Mobile, then use the **svc profiles** command in group policy webvpn or username attributes webvpn configuration mode to specify a client profile to download that has Windows Mobile parameters specified. For example, **svc profiles value mymobileprofile** directs the security appliance to download the profile mymobileprofile. If you specify the command **svc profiles none**, the security appliance does not download any profile.
- To specify an SSL VPN client package file that the security appliance expands in cache memory for downloading to remote PCs, use the **svc image** command in webvpn configuration mode. For mobile users, you can decrease the connection time of the mobile device by using the **regex** keyword with this command. When the browser connects to the security appliance, it includes the User-Agent string in the HTTP header. When the security appliance receives the string, if the string matches an expression configured for an image, it immediately downloads that image without testing the other client images.

SDI Token (SoftID) Integration

Cisco AnyConnect VPN Client, Release 2.1 and higher, integrates support for RSA SecurID client software running on Windows XP and Windows 2000 platforms. This support allows IT administrators to make strong authentication a convenient part of doing business. RSA SecurID software authenticators reduce the number of items a user has to manage for safe and secure access to corporate assets. RSA

SecurID Software Tokens residing on a remote device generate a random, one-time-use passcode that changes every 60 seconds. The term SDI stands for Security Dynamics, Inc. technology, which refers to this one-time password generation technology that uses hardware and software tokens.

Note The AnyConnect client is compatible with RSA SecurID software versions 1.1 and higher. At the time of this release, RSA SecurID Software Token client software does not support Windows Vista and 64-bit systems. In addition, the AnyConnect client does not support token selection from multiple tokens imported into the RSA Software Token client software. Instead, the AnyConnect client uses the default selected via the RSA SecurID Software Token GUI.

Comparing Native SDI with RADIUS SDI

The network administrator can configure the secure gateway to allow SDI authentication in either of the following modes:

- *Native SDI* refers to the native ability in the secure gateway to communicate directly with the SDI server for handling SDI authentication.
- *RADIUS SDI* refers to the process of the secure gateway performing SDI authentication using a RADIUS SDI proxy, which communicates with the SDI server.

In Release 2.1 and higher, except for one case, described later, Native SDI and RADIUS SDI appear identical to the remote user. Because the SDI messages are configurable on the SDI server, the message text (see Table 3-1 on page 3-18) on the security appliance must match the message text on the SDI server. Otherwise, the prompts displayed to the remote client user might not be appropriate for the action required during authentication. The AnyConnect client might fail to respond and authentication might fail.

RADIUS SDI challenges, with minor exceptions, essentially mirror native SDI exchanges. Since both ultimately communicate with the SDI server, the information needed from the client and the order in which that information is requested is the same. Except where noted, the remainder of this section deals with native SDI.

When a remote user using RADIUS SDI authentication connects to the security appliance with the AnyConnect VPN client and attempts to authenticate using an RSA SecurID token, the security appliance communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

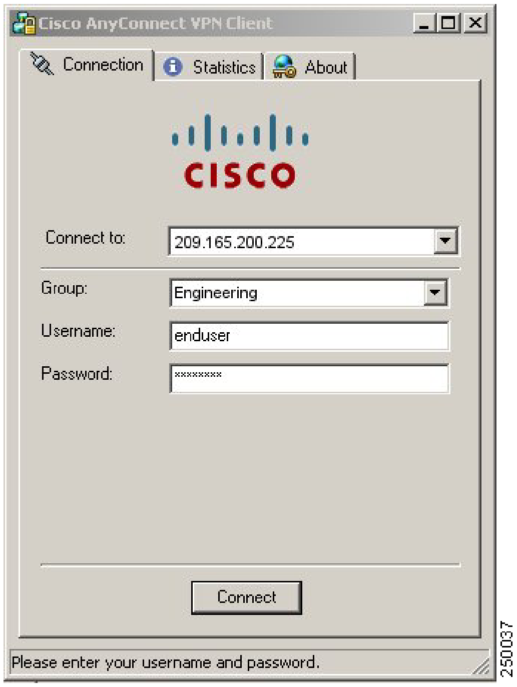
For more information about configuring the ASA to ensure AnyConnect client compatibility, see Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client, page 3-15.

Using SDI Authentication

In releases of the AnyConnect client prior to Release 2.1, a user who wanted to use SecurID had to click Select in the AnyConnect login dialog box to select the server, start the RSA SecurID Software Token GUI, click or type a Personal Identification Number (PIN), click or type Enter, copy the generated passcode, paste the passcode into the password field in the AnyConnect dialog, click Connect in the AnyConnect dialog, and close the RSA SecurID token GUI.

In the AnyConnect client, Release 2.1 and higher, the login (challenge) dialog box changes to match the type of authentication configured for the tunnel group to which the user belongs. The input fields of the login dialog box clearly indicate what kind of input is required for authentication. Users who rely on username/password authentication see a dialog box like that in Figure 3-2.

Figure 3-2 Username/Password Authentication Login Dialog Box



Connect to: 209.165.200.225

Group: Engineering

Username: enduser

Password: ********

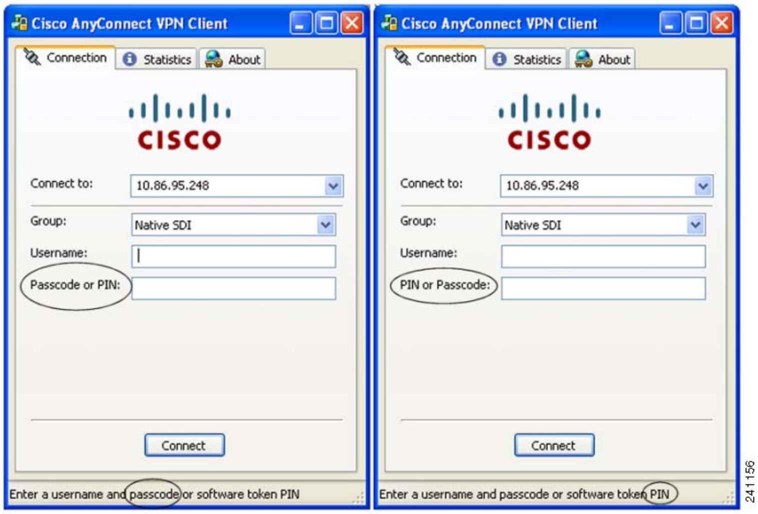
Please enter your username and password.

For SDI authentication, the remote user enters a PIN (Personal Identification Number) into the AnyConnect client software interface and receives an RSA SecurID passcode. After the user enters the passcode into the secured application, RSA Authentication Manager validates the passcode and allows the user to gain access.

In AnyConnect Release 2.0, The field following the username field has the label “Password”.

Users who use RSA SecurID hardware or software tokens see input fields indicating whether the user should enter a passcode or a PIN, and the status line at the bottom of the dialog box provides further information about the requirements. The user enters a software token PIN or passcode directly into the AnyConnect user interface. See Figure 3-3 on page 3-12.

Figure 3-3 PIN and Passcode Dialog Boxes


Connect to: 10.86.95.248
Group: Native SDI
Username:
Passcode or PIN:
Enter a username and passcode or software token PIN

Connect to: 10.86.95.248
Group: Native SDI
Username:
PIN or Passcode:
Enter a username and passcode or software token PIN

The appearance of the initial login dialog box depends on the secure gateway settings: the user can access the secure gateway either through the main login page, the main index URL, or through a tunnel-group login page, a tunnel group URL (URL/tunnel-group). To access the secure gateway via the main login page, the “Allow user to select connection” check box must be set in the secure gateway SSL VPN Connection Profiles. In either case, the secure gateway sends the client a login page. The main login page contains a drop-down box in which the user selects a tunnel group; the tunnel-group login page does not, since the tunnel-group is specified in the URL.

Starting with AnyConnect Release 2.1, in the case of a main login page (with a drop-down tunnel-group list), the authentication type of the default tunnel group determines the initial setting for the password input field label. For example, if the default tunnel group uses SDI authentication, the field label is “Passcode”; but if the default tunnel group uses NTLM authentication, the field label is “Password”. In Release 2.1 and higher, the field label is not dynamically updated with the user selection of a different tunnel group. For a tunnel-group login page, the field label matches the tunnel-group requirements.

Also starting with AnyConnect Release 2.1, the client supports input of RSA SecurID Software Token PINs in the password input field. If the RSA SecurID Software Token software is installed and the tunnel-group authentication type is SDI, the field label is “Passcode” and the status bar states “Enter a username and passcode or software token PIN.” If a PIN is used, subsequent consecutive logins for the same tunnel group and username have the field label “PIN”. The client retrieves the passcode from the RSA SecurID Software Token DLL using the entered PIN. With each successful authentication, the client saves the tunnel group, the username, and authentication type, and the saved tunnel group becomes the new default tunnel group.

The AnyConnect client accepts passcodes for any SDI authentication. Even when the password input label is “PIN”, the user may still enter a passcode as instructed by the status bar. The client sends the passcode to the secure gateway as is. If a passcode is used, subsequent consecutive logins for the same tunnel group and username have the field label “Passcode”.

Categories of SDI Authentication Exchanges

All SDI authentication exchanges fall into one of the following categories:

- Normal SDI Authentication Login

- Normal login challenge
- New user mode
- New PIN mode
- Clear PIN mode
- Next Token Code mode

Normal SDI Authentication Login

A normal login challenge is always the first challenge. The SDI authentication user must provide a user name and token passcode (or PIN, in the case of a software token) in the username and passcode or PIN fields, respectively. The client returns the information to the secure gateway (central-site device), and the secure gateway verifies the authentication with the authentication server (SDI or SDI via RADIUS proxy).

If the authentication server accepts the authentication request, the secure gateway sends a success page back to the client, and the authentication exchange is complete.

If the passcode is not accepted, the authentication fails, and the secure gateway sends a new login challenge page, along with an error message. If the passcode failure threshold on the SDI server has been reached, then the SDI server places the token into next token code mode. See “Next Passcode” and “Next Token Code” Challenges, page 3-15.

New User, Clear PIN, and New PIN Modes

The PIN can be cleared only on the SDI server and only by the network administrator.

In the New User, Clear PIN, and New PIN modes, the AnyConnect client caches the user-created PIN or system-assigned PIN for later use in the “next passcode” login challenge.

Clear PIN mode and New User mode are identical from the point of view of the remote user and are both treated the same by the secure gateway. In both cases, the remote user either must enter a new PIN or be assigned a new PIN by the SDI server. The only difference is in the user response to the initial challenge.

For New PIN mode, the existing PIN is used to generate the passcode, as it would be in any normal challenge. For Clear PIN mode, no PIN is used at all for hardware tokens, with the user entering just a token code. A PIN Of eight consecutive zeros, “00000000”, is used to generate a passcode for RSA software tokens. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Adding a new user to an SDI server has the same result as clearing the PIN of an existing user. In both cases, the user must either provide a new PIN or be assigned a new PIN by the SDI server. In these modes, for hardware tokens, the user enters just a token code from the RSA device. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

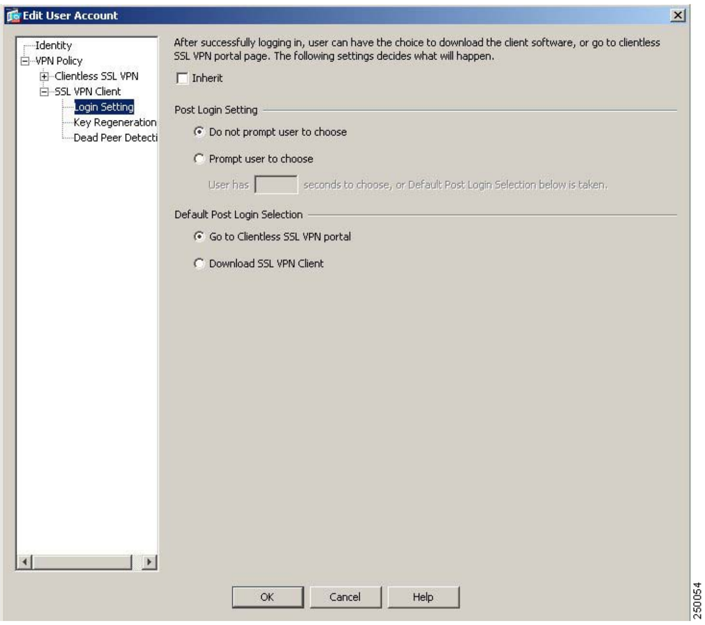
Getting a New PIN

If there is no current PIN, the SDI server requires that one of the following conditions be met, depending on how the system is configured:

- The user can choose whether to create a PIN or have the system assign it.
- The user must create a new PIN.
- The system must assign a new PIN to the user.

By default, the system simply assigns a PIN. If the SDI server is configured to allow the remote user to choose whether to create a PIN or have the system assign a PIN, the login screen presents a drop-down menu showing the options (Figure 3-4).

Figure 3-4 New PIN Creation or Generation Selection Dialog Box



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

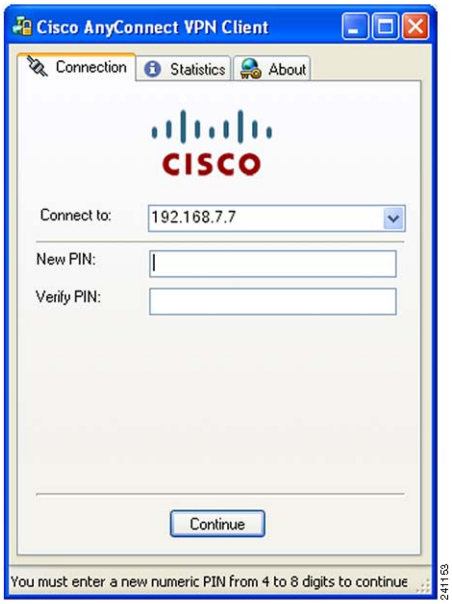
○ Download SSL VPN Client

The status line provides a prompt message. In either case, the user must remember the new PIN for future login authentications.

Creating a New PIN

If the user chooses to create a new PIN and clicks Continue, the AnyConnect client presents a dialog box on which to enter that PIN (Figure 3-5 on page 3-15). The PIN must be a number from 4 to 8 digits long.

Figure 3-5 Creating a New PIN



Connect to: 192.168.7.7

New PIN:

Verify PIN:

You must enter a new numeric PIN from 4 to 8 digits to continue

For a user-created PIN, after entering and confirming the new PIN, the user clicks Continue. Because the PIN is a type of password, anything the user enters into these input fields is displayed as asterisks. With RADIUS proxy, the PIN confirmation is a separate challenge, subsequent to the original dialog box. The client sends the new PIN to the secure gateway, and the secure gateway continues with a "next passcode" challenge.

For a system-assigned PIN, if the SDI server accepts the passcode that the user enters on the login page, then the secure gateway sends the client the system-assigned PIN. The user must click Continue. The client sends a response back to the secure gateway, indicating that the user has seen the new PIN, and the system continues with a "next passcode' challenge.

In both cases, the user must remember the PIN for subsequent login authentications.

"Next Passcode" and "Next Token Code" Challenges

For a "next passcode" challenge, the client uses the PIN value cached during the creation or assignment of a new PIN to retrieve the next passcode from the RSA SecurID Software Token DLL and return it to the secure gateway without prompting the user. Similarly, in the case of a "next Token Code" challenge for a software token, the client retrieves the next Token Code from the RSA SecurID Software Token DLL.

Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client

This section describes procedures to ensure that the AnyConnect client using RSA SecureID Software tokens can properly respond to user prompts delivered to the client through a RADIUS server proxying to an SDI server or servers. This section contains the following topics:

- AnyConnect Client and RADIUS/SDI Server Interaction

- Configuring the Security Appliance to Support RADIUS/SDI Messages

AnyConnect Client and RADIUS/SDI Server Interaction

When a remote user connects to the security appliance with the AnyConnect client and attempts to authenticate using an RSA SecurID token, the security appliance communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

During authentication, the RADIUS server presents access challenge messages to the security appliance. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the security appliance is communicating directly with an SDI server from when communicating through the RADIUS proxy. Therefore, in order to appear as a native SDI server to the AnyConnect client, the security appliance must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the security appliance must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. The AnyConnect client might fail to respond and authentication might fail.

Configuring the Security Appliance to Support RADIUS/SDI Messages

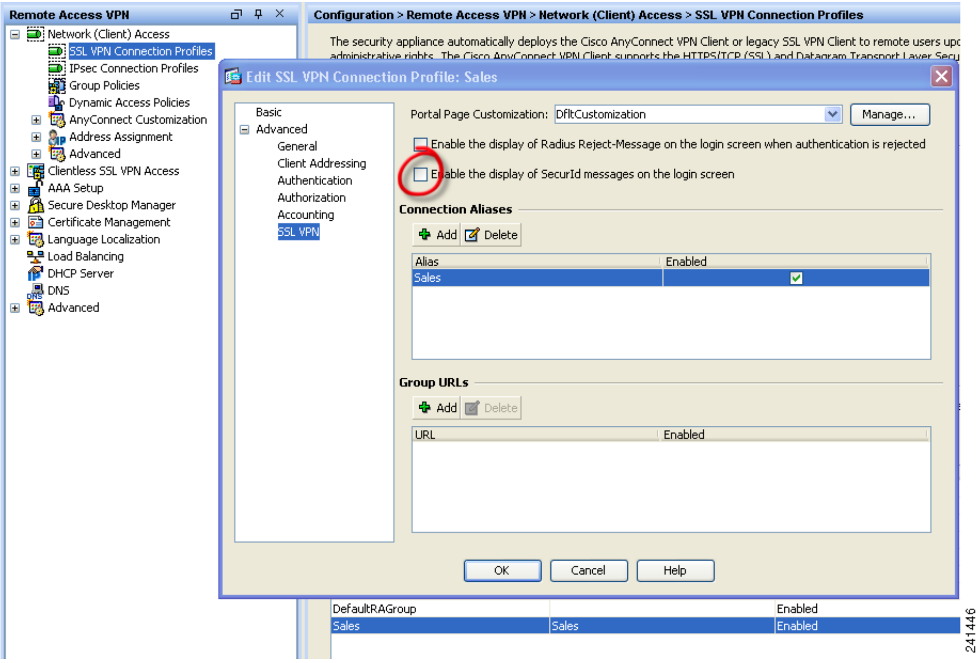
The following section describes the steps to configure the security appliance to interpret SDI-specific RADIUS reply messages and prompt the AnyConnect user for the appropriate action. Each step has information for both ASDM and the CLI.

Step 1 Configure a connection profile (tunnel group) to forward RADIUS reply messages in a manner that simulates direct communication with an SDI server. Users authenticating to the SDI server must connect over this connection profile.

ASDM Procedure

Go to Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles. The Edit SSL VPN Connection Profile window displays (Figure 3-6).

Figure 3-6 Edit SSL VPN Connection Profile Screen



The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upc
administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Secu

Portal Page Customization: DfltCustomization

□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

Alias	Enabled
Sales	✓

Group URLs

URL	Enabled

DefaultRAGroup		Enabled
Sales	Sales	Enabled

Check **Enable the display of SecurID messages on the login screen**.

CLI Procedure

Use the **proxy-auth sdi** command from tunnel-group webvpn configuration mode. For example:

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

Step 2 Configure the RADIUS reply message text on the security appliance to match (in whole or in part) the message text sent by the RADIUS server.

The default message text used by the security appliance is the default message text used by Cisco Secure Access Control Server (ACS). If you are using Cisco Secure ACS, and it is using the default message text, you do not need to configure the message text on the security appliance. Otherwise, configure the messages to ensure the message text matches.

Table 3-1 shows the message code, the default RADIUS reply message text, and the function of each message. Because the security appliance searches for strings in the order in which they appear in the table, you must ensure that the string you use for the message text is not a subset of another string.

For example, “new PIN” is a subset of the default message text for both new-pin-sup and next-ccode-and-reauth. If you configure new-pin-sup as “new PIN”, when the security appliance receives “new PIN with the next card code” from the RADIUS server, it will match the text to the new-pin-sup code instead of the next-ccode-and-reauth code.

Table 3-1 SDI Opcodes, Default Message Text, and Message Function

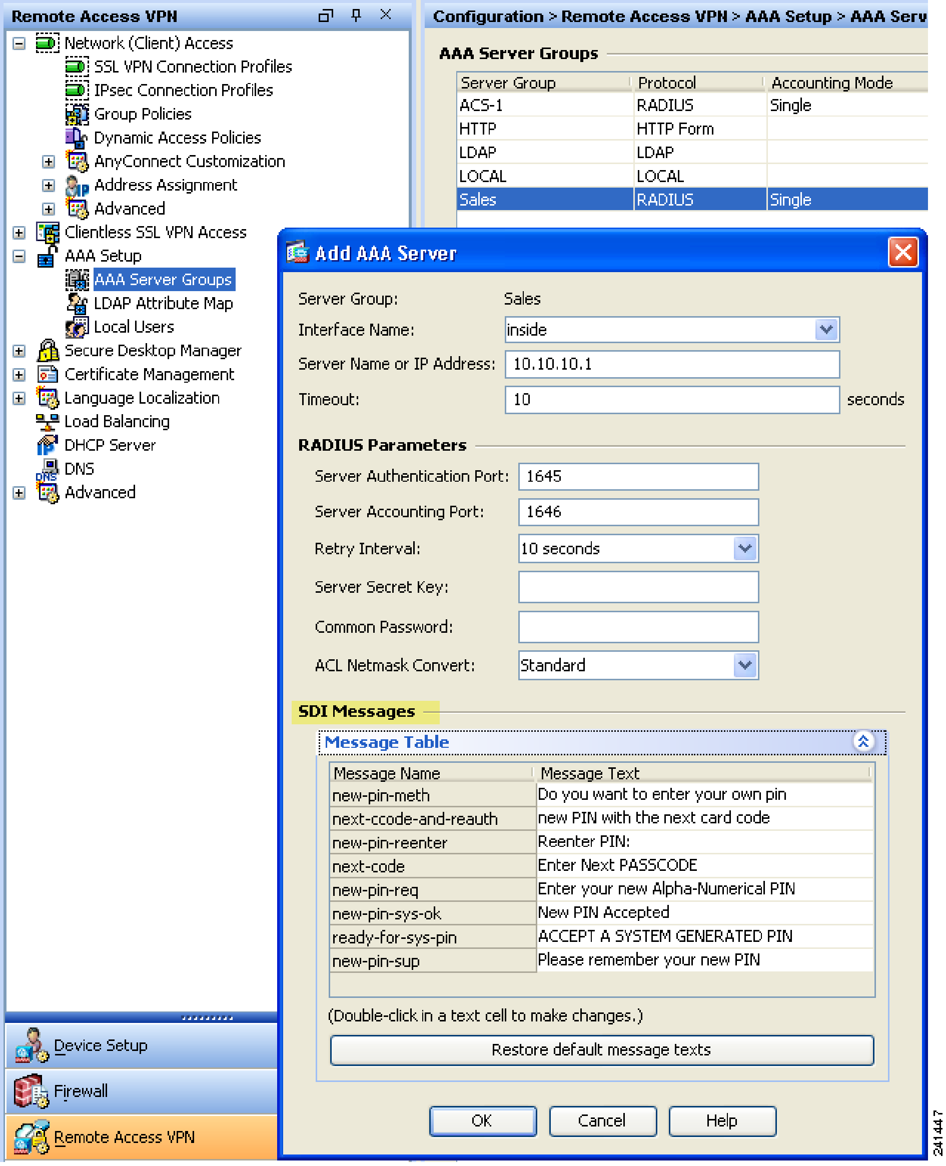
Message Code	Default RADIUS Reply Message Text	Function
next-code	Enter Next PASSCODE	Indicates the user must enter the NEXT tokencode without the PIN.
new-pin-sup	Please remember your new PIN	Indicates the new system PIN has been supplied and displays that PIN for the user.
new-pin-meth	Do you want to enter your own pin	Requests from the user which new PIN method to use to create a new PIN.
new-pin-req	Enter your new Alpha-Numerical PIN	Indicates a user-generated PIN and requests that the user enter the PIN.
new-pin-reenter	Reenter PIN:	Used internally by the security appliance for user-supplied PIN confirmation. The client confirms the PIN without prompting the user.
new-pin-sys-ok	New PIN Accepted	Indicates the user-supplied PIN was accepted.
next-ccode-and-reauth	new PIN with the next card code	Follows a PIN operation and indicates the user must wait for the next tokencode and to enter both the new PIN and next tokencode to authenticate.
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	Used internally by the security appliance to indicate the user is ready for the system-generated PIN.

ASDM Procedure

Go to Configuration > Remote Access VPN > AAA Server Groups. The Add AAA Server window appears (Figure 3-7).

In the SDI Messages area, click Message Table to expand the table and view the messages. Double-click a message text field to edit the message.

Figure 3-7 Configuring RADIUS SDI Messages



AAA Server Groups

Server Group	Protocol	Accounting Mode
ACS-1	RADIUS	Single
HTTP	HTTP Form	
LDAP	LDAP	
LOCAL	LOCAL	
Sales	RADIUS	Single

Server Group: Sales
Interface Name: inside
Server Name or IP Address: 10.10.10.1
Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645
Server Accounting Port: 1646
Retry Interval: 10 seconds
Server Secret Key:
Common Password:
ACL Netmask Convert: Standard

SDI Messages

Message Table

Message Name	Message Text
new-pin-meth	Do you want to enter your own pin
next-ccode-and-reauth	new PIN with the next card code
new-pin-reenter	Reenter PIN:
next-code	Enter Next PASSCODE
new-pin-req	Enter your new Alpha-Numerical PIN
new-pin-sys-ok	New PIN Accepted
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN
new-pin-sup	Please remember your new PIN

(Double-click in a text cell to make changes.)

Restore default message texts

CLI Procedure

Use the **proxy-auth_map sdi** command from tunnel-group webvpn configuration mode. The following example enters aaa-server-host mode and changes the text for the RADIUS reply message new-pin-sup:

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup "This is your new PIN"
```

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

See Adding a Security Appliance to the List of Trusted Sites (IE), page 2-18 for instructions about how to add a security appliance to the list of trusted sites. This is required on Windows Vista to use WebLaunch.

CHAPTER 4

Configuring and Using AnyConnect Client Operating Modes and User Profiles

Contents

This chapter contains the following major topics:

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 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 4-1 shows the CLI commands.

Table 4-1 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 (IE), page 2-18 and Appendix B, "Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users".

For Windows Mobile users, WebLaunch is supported only using the Pocket Internet Explorer browser. Because Pocket IE cannot load ActiveX components wirelessly, attempts to perform a fresh install of the AnyConnect client using WebLaunch will not succeed and will bring the user to a web page from which he or she must download and install the Mobile installer. After the AnyConnect client has been installed, WebLaunch can be used to initiate tunnels.

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

User profiles are created by an administrator and are automatically delivered to a client machine during connection setup. Profiles provide basic information about connection setup, and users cannot manage or modify them.

An AnyConnect client user profile is an XML file that lets you identify the secure gateway (security appliance) hosts that you want to make accessible. 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 copy, rename, and save as an XML file, then edit and use as a basis to create other profile files.

The profile file is downloaded from the security appliance to the remote user's PC, 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. 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.

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. Make a copy and rename that copy with a name meaningful to you. Alternatively, you can modify an existing profile. Table 4-2 shows the installation path for each operating system.

Table 4-2 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:

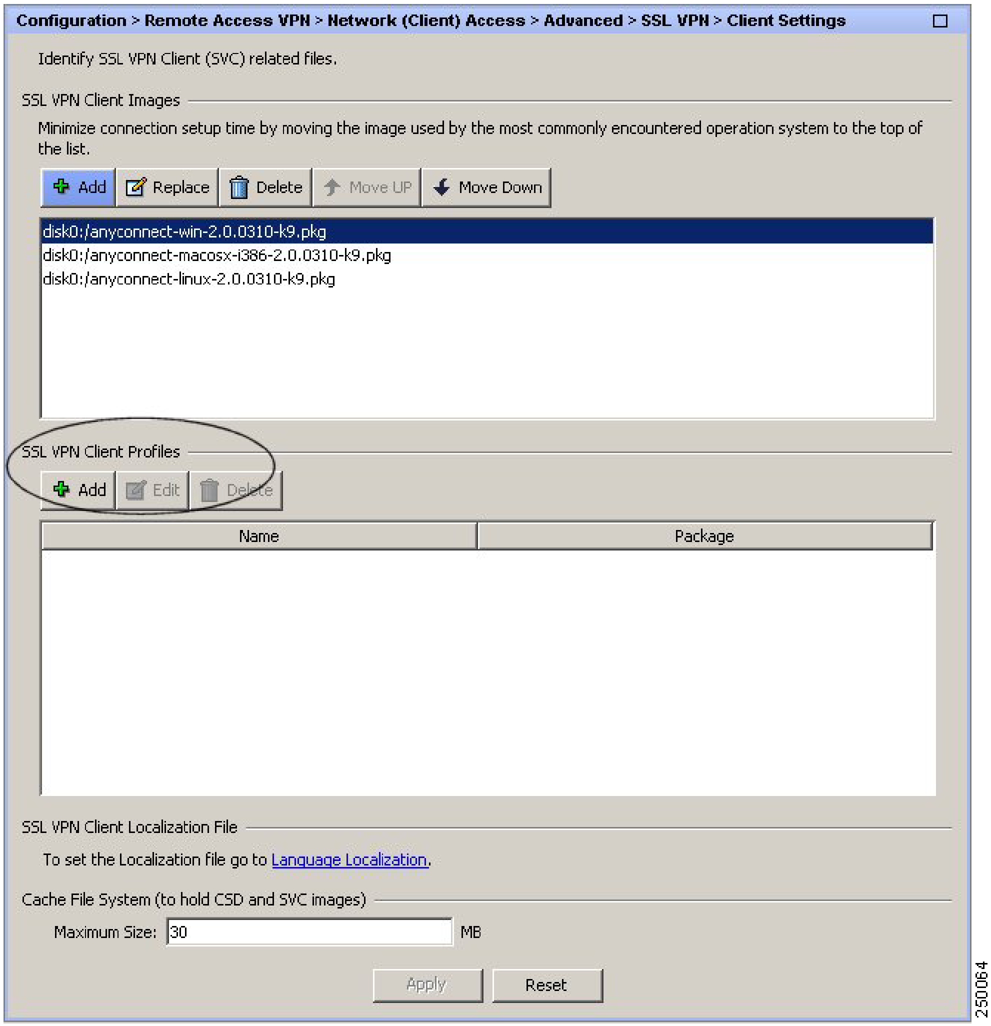
```
    <HostProfile>
        <HostName>Sales_gateway</HostName>
        <HostAddress>209.165.200.225</HostAddress>
    </HostProfile>
```

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

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 4-1).

Figure 4-1 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

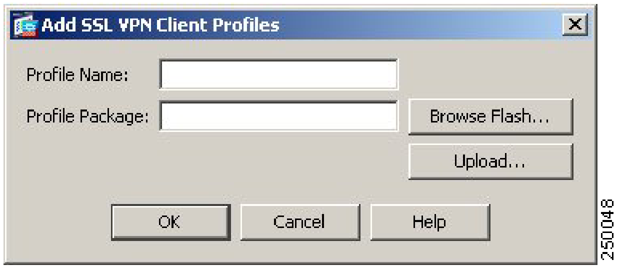
To set the Localization file go to Language Localization.

Cache File System (to hold CSD and SVC images)

Maximum Size: 30 MB

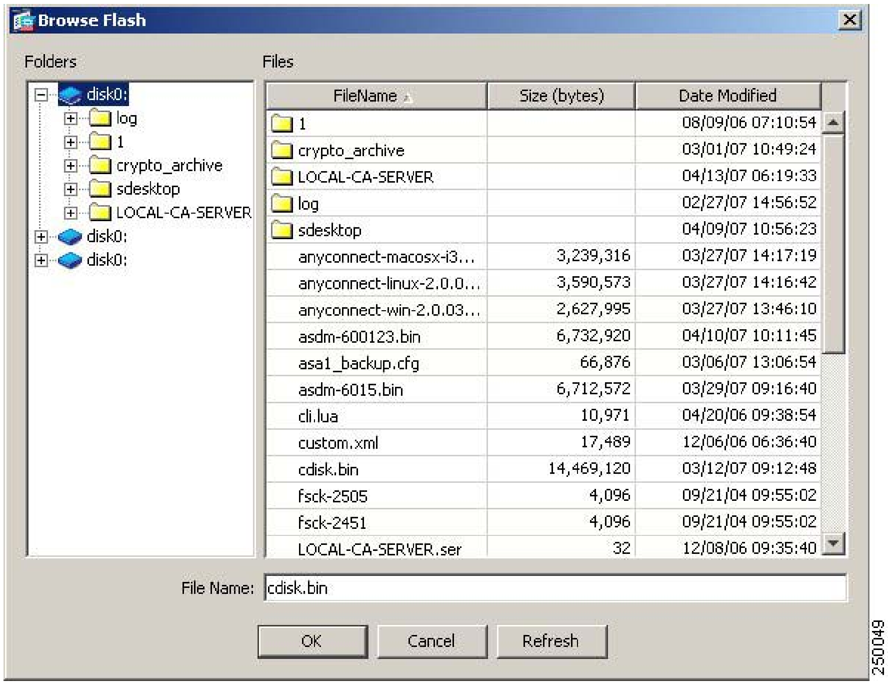
In the SSL VPN Client Profiles area, click Add or Edit. the Add or Edit SSL VPN Client Profiles dialog box appears (Figure 4-2).

Figure 4-2 Add (or Edit) SSL VPN Client Profiles Dialog Box



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 4-3).

Figure 4-3 Browse Flash Dialog Box



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

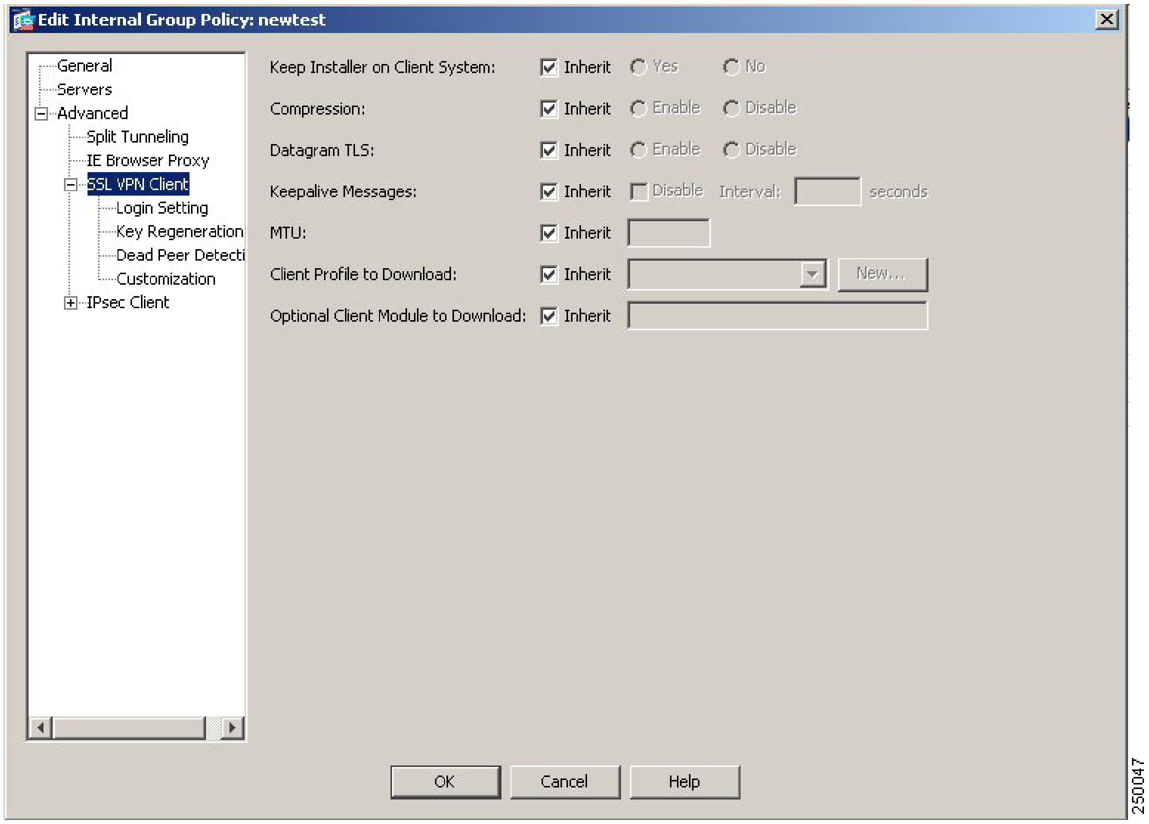
File Name: cdisk.bin

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.

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 4 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 4-4).

Figure 4-4 Add or 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

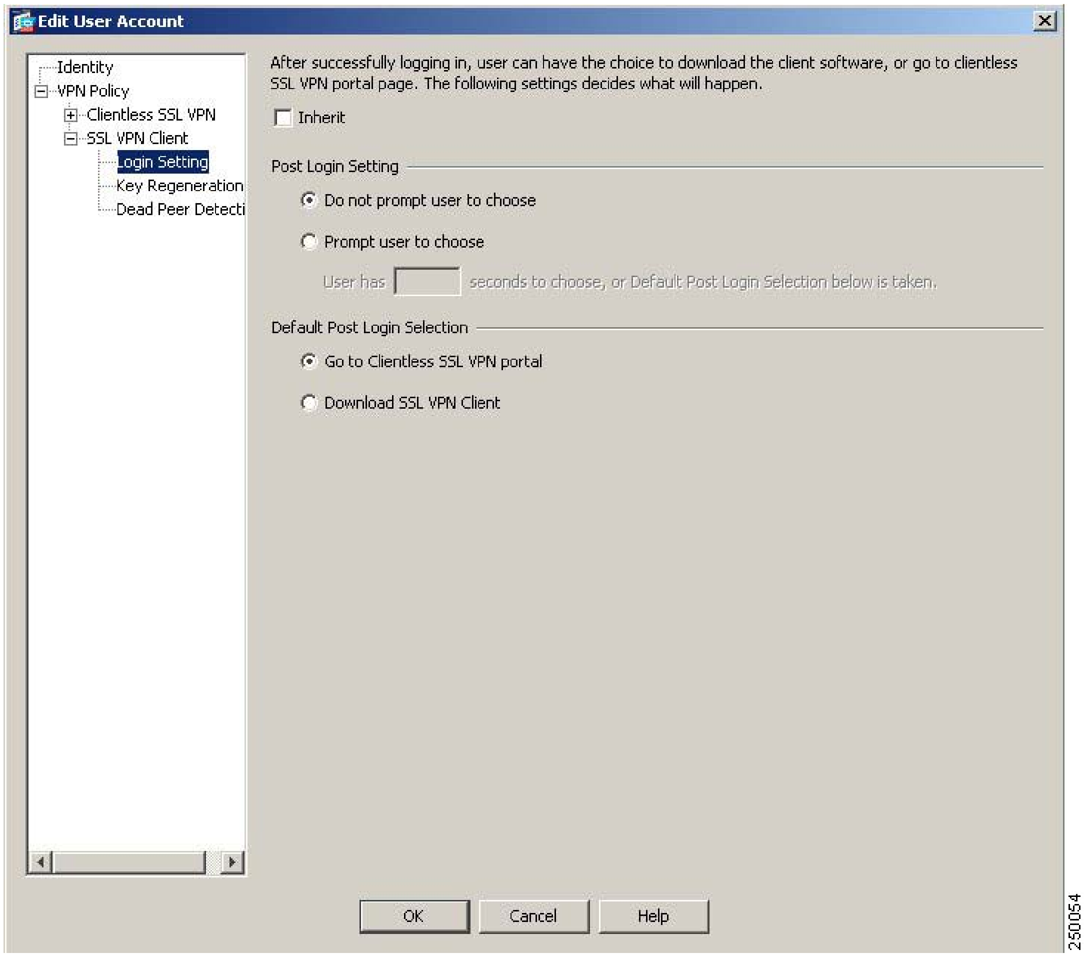
MTU: ☑ Inherit

Client Profile to Download: ☑ Inherit New...

Optional Client Module to Download: ☑ Inherit

Step 5 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. 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 4-5). In the navigation pane, select VPN Policy > SSL VPN Client >Login Setting.

Figure 4-5 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 6 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 4-2 on page 4-8) appears; follow the procedures that pertain to that figure.

Step 7 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.

Validating the XML Profile

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. This.xsd file is the XML schema definition for the 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.

Note Validate the profile before importing it into the security appliance. Doing so makes client-side validation unnecessary.

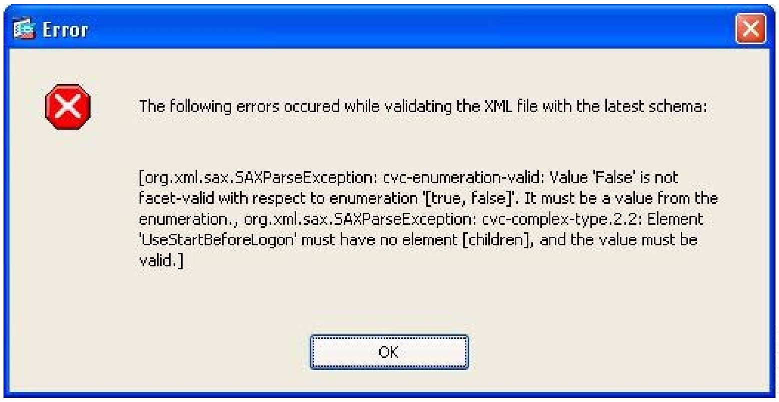
The XML file based on this schema can be distributed to clients at any time, either as a bundled file with the software distribution or as part of the automatic download mechanism. The automatic download mechanism available only with certain Cisco Secure Gateway products. See Appendix A, "Sample AnyConnect Profile and XML Schema" for a hard copy of these files.

For Windows Vista, Windows XP, and Windows 2000 systems with MSXML 6.0, the AnyConnect client validates the XML profile against the profile XSD schema and logs any validation failures. MSXML 6.0 ships with Windows Vista and is available for download from Microsoft for Windows XP and Windows 2000 from the following link: http://www.microsoft.com/downloads/details.aspx?FamilyID=d21c292c-368b-4ce1-9dab-3e9827b70604&displaylang=en

When modifying a profile, be sure to check your typing and make sure that the capitalization matches that in the element names. This is a common error that results in a profile failing validation. For example, attempting to validate a profile that has the following preference entry:

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

results in the following error message:



The following errors occured while validating the XML file with the latest schema:

[org.xml.sax.SAXParseException: cvc-enumeration-valid: Value 'False' is not facet-valid with respect to enumeration '[true, false]'. It must be a value from the enumeration., org.xml.sax.SAXParseException: cvc-complex-type.2.2: Element 'UseStartBeforeLogon' must have no element [children], and the value must be valid.]

In this example, the value **False** (initial cap) should have been **false** (all lowercase), and the error indicates this.

Sample AnyConnect Profile

The following example shows a sample AnyConnect Profile XML file. User-supplied values appear in **bold** type. In this example, blank lines separate the major groupings for legibility. Do not include these blank lines in your profile.

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.

```
<?xml version="1.0" encoding="UTF-8" ?>

<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">

<ClientInitialization>
    <UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreOverride>false</CertificateStoreOverride>
    <AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">true</LocalLanAccess>
    <AutoReconnect UserControllable="true">
    true
        <AutoReconnectBehavior
        UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    </AutoReconnect>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>

    <CertificateMatch>
        <KeyUsage>
            <MatchKey>Non_Repudiation</MatchKey>
            <MatchKey>Digital_Signature</MatchKey>
        </KeyUsage>
        <ExtendedKeyUsage>
            <ExtendedMatchKey>ClientAuth</ExtendedMatchKey>
            <ExtendedMatchKey>ServerAuth</ExtendedMatchKey>
            <CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11</CustomExtendedMatchKey>
        </ExtendedKeyUsage>
        <DistinguishedName>
            <DistinguishedNameDefinition Operator="Equal" Wildcard="Enabled"
             MatchCase="Enabled">
            <Name>CN</Name>
            <Pattern>ASASecurity</Pattern>
        </DistinguishedNameDefinition>
        </DistinguishedName>
    </CertificateMatch>

    <BackupServerList>
        <HostAddress>asa-02.cisco.com</HostAddress>
        <HostAddress>192.168.1.172</HostAddress>
    </BackupServerList>
    <MobilePolicy>
        <DeviceLockRequired MaximumTimeoutMinutes="60" MinimumPasswordLength="4"
        PasswordComplexity="pin" />
    </MobilePolicy>
</ClientInitialization>
```

```
<ServerList>
    <HostEntry>
        <HostName>CVC-ASA-01</HostName>
        <HostAddress>10.94.146.172</HostAddress>
        <UserGroup>StandardUser</UserGroup>
        <BackupServerList>
            <HostAddress>cvc-asa-03.cisco.com</HostAddress>
            <HostAddress>10.94.146.173</HostAddress>
            </BackupServerList>
    </HostEntry>
</ServerList>

</AnyConnectProfile>
```

The following sections describe, group by group, each of the AnyConnect Profile Attributes:

- Configuring Client Initialization Attributes, page 4-13
- Configuring the Certificate Match Attributes, page 4-15
- Configuring Backup Server List Parameters, page 4-22
- Configuring Windows Mobile Policy, page 4-22
- Configuring the ServerList Attributes, page 4-24
- Enabling Start Before Logon (SBL) for the AnyConnect Client, page 4-27

These sections summarize the parameters, their possible values, and examples of use.

Configuring Client Initialization Attributes

The VPN Client Initialization section is a repository of information used to manage the Cisco AnyConnect VPN client software. The ClientInitialization section of the AnyConnectProfile file represents global settings for the AnyConnect client. In some cases, for example, BackupServerList, host-specific overrides are possible.

The following example shows a sample of configuring the Client Initialization attributes:

```
<ClientInitialization>
    <UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreOverride>false</CertificateStoreOverride>
    <AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">true</LocalLanAccess>
    <AutoReconnect UserControllable="true">
    true
        <AutoReconnectBehavior
        UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    </AutoReconnect>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
```

Table 4-3 lists the ClientInitialization parameters. In this table, default values appear in **bold** type.

Table 4-3 ClientInitialization Parameters

Preference Name	Preference Available by Default?[1]	Possible Values (Default appears in bold)[2,3]	User Control Allowed?[4]	Default User Control[5]	OS[6]
UseStartBeforeLogon	false	**true**, false	yes	true	Windows, except Mobile
ShowPreConnectMessage	false	true, **false**	no	n/a	All
CertificateStore	false	**All**, Machine, User	no	n/a	All
CertificateStoreOverride	false	true, **false**	no	n/a	All
AutoConnectOnStart	true	**true**, false	yes	true	All
MinimizeOnConnect	true	**true**, false	yes	true	All
LocalLanAccess	true	true, **false**	yes	true	All
AutoReconnect	false	**true**, false	yes	false	All
AutoReconnectBehavior	false	ReconnectAfterResume **DisconnectOnSuspend**	yes	false	Windows, Mac
AutoUpdate	false	**true**, false	yes	false	all
RSASecurIDIntegration[7]	false	**Automatic**, SoftwareToken, HardwareToken	yes	false	Windows

[1] Preferences available by default are visible to the user and configurable even if there is no profile in the head end.

[2] The default value of a preference is used when its value is not defined in the profile.

[3] The value of a preference is defined in between the preference tags; for example, <AutoUpdate>true</AutoUpdate>.

[4] Preferences that do not allow user control cannot be made UserControllable; that is, even if they are defined as UserControllable=”true” in the profile, this is ignored and the default values are used.

[5] The user controllable attribute is defined inside the preference tags; for example, <AutoUpdate UserControllable=”true”>true</AutoUpdate>. Its possible values are “true” or “false”, and these determine which preferences are overridden by the preferences*.xml files. This is an optional attribute, and if not defined, the default value is used. Preferences made UserControllable=”true” in the profile are visible in the Preferences dialog.

[6] OS that supports these preferences.

[7] The AnyConnect client is compatible with RSA SecurID software versions 1.1 and higher. At the time of the AnyConnect 2.3 release, RSA SecurID Software Token Client software does not support Windows Vista and 64-bit systems.

Note AutoReconnect is a special type of preference, as it has a child preference. This is configured in the profile as follows:

```
<AutoReconnect UserControllable=“true”>true
    <AutoReconnectBehavior UserControllable=“true”>
     ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

XML Profile Enhancement for Selecting Windows Certificate Store

In the AnyConnect client Release 2.3 and later, administrators can control which certificate store AnyConnect uses for locating certificates. This applies only to the AnyConnect client on Windows.

Windows provides separate certificate stores for the local machine and for the current user. Users with administrative privileges on the computer will have access to both stores. The original AnyConnect behavior was to load certificates from all available certificate stores. An ASA administrator may want to configure AnyConnect via XML profile to restrict certificate lookups to only the user store or only the machine store.

To this end, a new setting called CertificateStore has been added to the ClientInitialization element in the XML profile. It has three possible (case-sensitive) values: All (default), Machine, or User.

Note The default setting (All) is appropriate for the majority of cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.

If the CertificateStore setting is not in the profile, AnyConnect uses all available certificate stores. This setting has no effect on non-Windows platforms.

Within the ClientInitialization section of the XML template, you can specify the certificate store that you want to use. Possible values are as follows:

- All—(default) All certificates are acceptable.
- Machine—Use the machine certificate
- User—Use a user-generated certificate.

Note These attributes are case-sensitive.

Certificate Store Example

The following example shows how to set the CertificateStore attribute within the ClientInitialization element that you can use to change client certificate selection to use a machine certificate:

This setting lets an administrator specify the certificate store that AnyConnect uses for locating certificates. This setting applies only to the Microsoft Windows version of the AnyConnect client and has no effect on other platforms.

```
<CertificateStore>Machine</CertificateStore>
```

This setting lets an administrator direct the AnyConnect client to search for certificates in the Windows machine certificate store. This is useful in cases where certificates are located in this store and users do not have administrator privileges on their machine.

Configuring the Certificate Match Attributes

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 4-18 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 4-4 lists the well known set of constraints with their corresponding object identifiers (OIDs).

Table 4-4 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

All other OIDs, such as 1.3.6.1.5.5.7.3.11, used in some examples in this document) are considered “custom.” 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 4-5 lists the supported criteria:

Table 4-5 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
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

The profile can contain zero 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

Note In this and all subsequent examples, the profile values for KeyUsage, ExtendedKeyUsage, and DistinguishedName are just examples. You should configure *only* the CertificateMatch criteria that apply to your certificates.

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>
```

Within the ClientInitialization section, the CertificateMatch section defines preferences that refine client certificate selection. Except as noted, these parameters do not have default values; that is, if you do not specify a parameter, it is simply not in effect. Table 4-6 summarizes these parameters and defines their possible values.

Include the CertificateMatch section in a profile only if certificates are used as part of authentication. Only those CertificateMatch subsections (KeyUsage, ExtendedKeyUsage and DistinguishedName) that are needed to uniquely identify a user certificate should be included in the profile. The data in any of these sections should be specific to the user certificate to be matched.

Table 4-6 Certificate Match Parameters

Preference Name	Possible Values	Description	Example

CertificateMatch	n/a	Group identifier	`<CertificateMatch>...`
			`</CertificateMatch>`

KeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to specify acceptable client certificates.	`<KeyUsage>`
			`    <MatchKey>Non_Repudiation</MatchKey>`
			`</KeyUsage>`

MatchKey	`Decipher_Only`
	`Encipher_Only`
	`CRL_Sign`
	`Key_Cert_Sign`
	`Key_Agreement`
	`Data_Encipherment`
	`Key_Encipherment`
	`Non_Repudiation`
	`Digital_Signature`
		Within the KeyUsage group, MatchKey attributes specify attributes that can be used for choosing acceptable client certificates. Specify one or more match keys. A certificate must match at least one of the specified key to be selected.	`<KeyUsage>`
			`<MatchKey>Non_Repudiation</MatchKey>`
			`<MatchKey>Digital_Signature</MatchKey>`
			`</KeyUsage>`

ExtendedKeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to choose acceptable client certificates.	`<ExtendedKeyUsage>`
			`<ExtendedMatchKey>ClientAuth</ExtendedMatchKey>`
			`</ExtendedKeyUsage>`

ExtendedMatchKey	`ClientAuth`
	`ServerAuth`
	`CodeSign`
	`EmailProtect`
	`IPSecEndSystem`
	`IPSecTunnel`
	`IPSecUser`
	`TimeStamp`
	`OCSPSign`
	`DVCS`
		Within the ExtendedKeyUsage group, ExtendedMatchKey specifies attributes that can be used for choosing acceptable client certificates. Specify zero or more extended match keys. A certificate must match all of the specified key(s) to be selected.	`<ExtendedMatchKey>ClientAuth</ExtendedMatchKey>`
			`<ExtendedMatchKey>ServerAuth</ExtendedMatchKey>`

Table 4-6 Certificate Match Parameters (continued)

Preference Name	Possible Values	Description	Example
CustomExtendedMatchKey	Well-known MIB OID values, such as 1.3.6.1.5.5.7.3.11	Within the ExtendedKeyUsage group, you can specify zero or more custom extended match keys. A certificate must match all of the specified key(s) to be selected. The key should be in OID form (for example, 1.3.6.1.5.5.7.3.11)	`<CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11< <CustomExtendedMatchKey>`
DistinguishedName	`n/a`	Group identifier. Within the DistinguishedName group, Certificate Distinguished Name matching lets you specify match criteria for choosing acceptable client certificates.	`<DistinguishedName>...</DistinguishedName>`

Table 4-6 Certificate Match Parameters (continued)

Preference Name	Possible Values	Description	Example

DistinguishedNameDefinition	Bold text indicates default value.
	Wildcard:
	“Enabled”
	“Disabled”
	Operator:
	“Equal” or **==**
	“NotEqual”or !==
	MatchCase:
	“Enabled”
	“Disabled”
		DistinguishedNameDefinition specifies a set of operators used to define a single Distinguished Name attribute to be used in matching. The Operator specifies the operation to use in performing the match. MatchCase specifies whether the pattern matching is case sensitive.	<DistinguishedNameDefinition Operator=”Equal” Wildcard=”Enabled” Matchcase=”Enabled”>
			    <Name>CN</Name>
			    <Pattern>ASASecurity</Pattern>
			</DistinguishedNameDefinition>

Name	CN DC SN GN N I GENQ DNQ C L SP ST O OU T EA ISSUER-CN ISSUER-DC ISSUER-SN ISSUER-GN ISSUER-N ISSUER-I ISSUER-GENQ ISSUER-DNQ ISSUER-C ISSUER-L ISSUER-SP ISSUER-ST ISSUER-O ISSUER-OU ISSUER-T ISSUER-EA	A DistinguishedName attribute name to be used in matching. You can specify up to 10 attributes.	
Pattern	A string (1-30 characters) enclosed in double quotes. With wildcards enabled, the pattern can be anywhere in the string.	Specifies the string (pattern) to use in the match. Wildcard pattern matching is disabled by default for this definition.	

Configuring Backup Server List Parameters

Within the ClientInitialization section, the BackupServerList section is a collection of one or more backup servers to be used in case the user-selected server fails. In some cases, the BackupServerList might specify host specific overrides.

These parameters do not have default values; that is, if you do not specify a parameter, it is simply not in effect. Table 4-7 lists these parameters and defines their possible values.

Include the BackupServerList section in a profile only if you want to specify backup servers.

Table 4-7 Backup Server Parameters

Name	Possible Values	Description	Examples
BackupServerList	`n/a`	Group identifier	`<BackupServerList>...</BackupServerList>`

HostAddress	`An IP address or a Full-Qualified Domain Name (FQDN)`	Specifies a host address to include in the backup server list.	`<BackupServerList>`
			`  <HostAddress>tech.myco.com</HostAddress>`
			`  <HostAddress>10.94.146.172</HostAddress>`
			`</BackupServerList>`

Configuring Windows Mobile Policy

To allow end users to connect using Windows Mobile devices, configure the Mobile Policy parameters. These parameters apply only to Windows Mobile devices. Include them only if your end users use Windows Mobile. See the latest version of *Release Notes for Cisco AnyConnect VPN Client* for detailed, current information about Windows Mobile device support.

Note Windows Mobile Policy enforcement is supported only on Windows Mobile 5, Windows Mobile 5+AKU2, and Windows Mobile 6. It is not supported on Windows Mobile 6.1. Attempts to connect to a secure gateway that is configured to require a security policy that cannot be enforced will fail. In environments containing Windows Mobile 6.1 devices, administrators should either create a separate group for Windows Mobile 6.1 users that does not contain Mobile Policy enforcement or disable Mobile Policy enforcement on the secure gateway.

The following attributes can be specified to check additional settings. The platforms for which each additional check is performed are specified with “WM5AKU2+” for Windows Mobile 5 with the Messaging and Security Feature Pack, delivered as part of Adaption Kit Upgrade 2 (AKU2).

Note This configuration merely validates the policy that is already present; it does not change it.

Table 4-8 shows the MobilePolicy parameters and their values.

Table 4-8 Mobile Policy Parameters

Preference Name	Possible Values	Description	Example
MobilePolicy	`n/a`	Group identifier.	`<MobilePolicy>...</MobilePolicy>`

DeviceLockRequired	n/a	Group identifier. Within the MobilePolicy group, DeviceLockRequired indicates that a Windows Mobile device must be configured with a password or PIN prior to establishing a VPN connection. This configuration is valid only on Windows Mobile devices that use the Microsoft Default Local Authentication Provider (LAP).
		Note The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, WM5AKU2+, and Windows Mobile 6.0, but not on Windows Mobile 6.1.
			`<DeviceLockRequired>`
			`MaximumTimeoutMinutes=”60”`
			`MinimumPasswordLength=”4”`
			`PasswordComplexity=”pin”`
			`</DeviceLockRequired>`

MaximumTimeoutMinutes	Any non-negative integer	Within the DeviceLockRequired group, this parameter, when set to a non-negative number, specifies the maximum number of minutes that must be configured before device lock takes effect.	`<DeviceLockRequired>`
			`MaximumTimeoutMinutes=”60”`
			`MinimumPasswordLength=”4”`
			`PasswordComplexity=”pin”`
			`</DeviceLockRequired>`

Table 4-8 Mobile Policy Parameters (continued)

Preference Name	Possible Values	Description	Example

MinimumPasswordLength	Any non-negative integer	Within the DeviceLockRequired group, when set to a non-negative number, this parameter specifies that any PIN/password used for device locking must have at least the specified number of characters.
		This setting must be pushed down to the mobile device by syncing with an Exchange server before it can be enforced. (WM5AKU2+)
			`<DeviceLockRequired>`
			`MaximumTimeoutMinutes=”60”`
			`MinimumPasswordLength=”4”`
			`PasswordComplexity=”pin”`
			`</DeviceLockRequired>`

PasswordComplexity	`"alpha"-Requires an alphanumeric password.`
	`"pin"-Requires a numeric PIN.`
	`"strong"-Requires a strong alphanumeric password, defined by Microsoft as containing at least 7 characters, including at least 3 from the set of uppercase, lowercase, numerals, and punctuation.`
		When present checks for the password subtypes listed in the column to the left.
		This setting must be pushed down to the mobile device by syncing with an Exchange server before it can be enforced. (WM5AKU2+)
			`<DeviceLockRequired>`
			`MaximumTimeoutMinutes=”60”`
			`MinimumPasswordLength=”4”`
			`PasswordComplexity=”pin”`
			`</DeviceLockRequired>`

Note Check with your service provider regarding your data plan before using AnyConnect for Windows Mobile, as you might incur additional charges if you exceed the data usage limits of your plan.

Configuring the ServerList Attributes

One of the main uses of the profile is to let the user list the connection servers. 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, you can specify a default server. 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.

See Sample AnyConnect Profile, page 4-12 for an example of the ServerList parameter in a full configuration.

Table 4-9 lists the ServerList parameters and their values. In this table the referenced preference name is in **bold** type. The values in these examples are only for demonstration purposes. Do not use them in your own configuration.

Table 4-9 Server List Parameters

Preference Name	Possible Values	Description	Example

ServerList	n/a	Group identifier	**<ServerList>**
			    <HostEntry>
			        <HostName>ASA-01</HostName>
			        <HostAddress>cvc-asa01.cisco.com
			        </HostAddress>
			    </HostEntry>
			    <HostEntry>
			        <HostName>ASA-02</HostName>
			        <HostAddress>cvc-asa02.cisco.com
			        </HostAddress>
			        <UserGroup>StandardUser</UserGroup>
			        <BackupServerList>
			            <HostAddress>cvc-asa03.cisco.com
			        </BackupServerList>
			    </HostEntry>
			</ServerList>

HostEntry	n/a	Group identifier, subordinate to ServerList. This is the data needed to attempt a connection to a specific host.	<ServerList>
			    <HostEntry>
			        <HostName>ASA-01</HostName>
			        <HostAddress>cvc-asa01.cisco.com
			        </HostAddress>
			    </HostEntry>
			    <HostEntry>
			        <HostName>ASA-02</HostName>
			        <HostAddress>cvc-asa02.cisco.com
			        </HostAddress>
			        <UserGroup>StandardUser</UserGroup>
			        <BackupServerList>
			            <HostAddress>cvc-asa03.cisco.com
			        </BackupServerList>
			    </HostEntry>
			</ServerList>

Table 4-9 Server List Parameters (continued)

Preference Name	Possible Values	Description	Example
HostName	An alias used to refer to the host or an FQDN or IP address. If this is an FQDN or IP address, a HostAddress is not required.	Within the HostEntry group, the HostName parameter specifies a name of a host in the server list. If an FQDN or IP address is used, a HostAddress is not required.	<ServerList> <HostEntry> **<HostName>ASA-01</HostName>** <HostAddress>cvc-asa01.cisco.com </HostAddress> </HostEntry> <HostEntry> **<HostName>ASA-02</HostName>** <HostAddress>cvc-asa02.cisco.com </HostAddress> <UserGroup>StandardUser</UserGroup> <BackupServerList> <HostAddress>cvc-asa03.cisco.com </BackupServerList> </HostEntry> </ServerList>
HostAddress	An IP address or Full-Qualified Domain Name (FQDN) used to refer to the host. If HostName is an FQDN or IP address, a HostAddress is not required.	Group identifier, subordinate to CertificateMatch. Use these attributes to choose acceptable client certificates.	<ServerList> <HostEntry> <HostName>ASA-01</HostName> **<HostAddress>cvc-asa01.cisco.com** **</HostAddress>** </HostEntry> <HostEntry> <HostName>ASA-02</HostName> **<HostAddress>cvc-asa02.cisco.com** **</HostAddress>** <UserGroup>StandardUser</UserGroup> <BackupServerList> **<HostAddress>cvc-asa03.cisco.com** **</HostAddress>** </BackupServerList> </HostEntry> </ServerList>
UserGroup	The tunnel group to use when connecting to the specified host. This parameter is optional.	Within the ServerList group, the UserGroup, parameter, if present, is used in conjunction with HostAddress to form a Group-based URL. **Note** Group based URL support requires ASA version 8.0.3, or later.	<ServerList> <HostEntry> <HostName>ASA-01</HostName> <HostAddress>cvc-asa01.cisco.com </HostAddress> </HostEntry> <HostEntry> <HostName>ASA-02</HostName> <HostAddress>cvc-asa02.cisco.com </HostAddress> **<UserGroup>StandardUser</UserGroup>** <BackupServerList> <HostAddress>cvc-asa03.cisco.com </HostAddress> </BackupServerList> </HostEntry> </ServerList>

The following sections describe how to modify the profiles template to configure the Start Before Logon profile attributes:

- Enabling Start Before Logon (SBL) for the AnyConnect Client, page 4-27.

- Configuring Start Before Logon (PLAP) on Windows Vista Systems, page 4-31

Enabling Start Before Logon (SBL) for the AnyConnect Client

With Start Before Logon 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.

Note Within the AnyConnect client, the only configuration you do for SBL is enabling the feature. Network administrators handle the processing that goes on before logon based upon the requirements of their situation. Logon scripts can be assigned to a domain or to individual users. Generally, the administrators of the domain have batch files or the like defined with users or groups in Active Directory. As soon as the user logs on, the login script is executed.

The point of SBL is that it connects a remote computer to the company infrastructure prior to logging on to the PC. For example, a user might be outside the physical corporate network, unable to access corporate resources until his or her PC has joined the corporate network.

With SBL enabled, the AnyConnect client connects before the user sees the Microsoft login window. The user must also log in, as usual, to Windows when the Microsoft login window appears.

The reasons that a user might want to use SBL include the following:

- The user's PC itself is joined to an Active Directory infrastructure.
- The user cannot have cached credentials on the PC; that is, if the group policy disallows cached credentials.
- The user must run login scripts that execute from a network resource or that need access to a network resource.
- A user has network-mapped drives that require authentication with the Active Directory infrastructure.
- Networking components (such as MS NAP/CS NAC) exist that might require connection to the infrastructure.

SBL creates a network that is equivalent to being on the local corporate LAN. For example, with SBL enabled, since the user has access to the local infrastructure, the logon scripts that would normally run when a user is in the office would also be available to the remote user.

For information about creating logon scripts, see the following Microsoft TechNet article:

http://technet2.microsoft.com/windowsserver/en/library/8a268d3a-2aa0-4469-8cd2-8f28d6a630801033.mspx?mfr=true

For information about using local logon scripts in Windows XP, see the following Microsoft article:

http://www.windowsnetworking.com/articles_tutorials/wxpplogs.html

In another example, a system might be configured not allow cached credentials to be used to log on to the PC. In this scenario, a users must be able to communicate with a domain controller on the corporate network for their credentials to be validated prior to gaining access to the PC.

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

Installing Start Before Logon Components (Windows Only)

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

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

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

In the AnyConnect client, the Windows Vista Start Before Logon feature is known as the Pre-Login Access Provider (PLAP), which is a connectable credential provider. This feature lets network administrators perform specific tasks, such as collecting credentials or connecting to network resources, prior to login. PLAP provides start Before Logon functions on Windows Vista and the Windows 2008 server. PLAP supports 32-bit and 64-bit versions of the operating system with vpnplap.dll and vpnplap64.dll, respectively. The PLAP function supports Windows Vista x86 and x64 versions.

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

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

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

The sections that immediately follow describe the settings and procedures for both VPNGINA and PLAP SBL. For a complete description of enabling and using the SBL feature (PLAP) on a Windows Vista platform, see Configuring Start Before Logon (PLAP) on Windows Vista Systems, page 4-31.

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 AnyConnect profile to true:

```
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

To disable SBL, set the same value to false.

Making SBL User-Controllable

To make SBL user-controllable, use the following statement when enabling SBL:

```
<UseStartBeforeLogon UserControllable=”true”>true</UseStartBeforeLogon>
```

To revert to the default, in which SBL is not user-controllable, set the UserControllable preference within the UseStartBeforeLogon preference to false.

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* value for SBL is **vpngina**.

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 SBL:

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

In addition, the administrator must ensure that the AnyConnect <profile.xml> file (where <profile.xml> is the name that the network administrator has assigned to the 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 2-7 (ASDM) or Enabling Modules for Additional AnyConnect Features, page 3-5 (CLI) for a description of how to do this.

Scenario: Using Start Before Logon

The following scenario walks you through the process of setting up the XML file and troubleshooting SBL using the CLI. You can also do this setup using ASDM:

Step 1 Create a profile to be pushed down to the Client PCs that looks similar to the one in Sample AnyConnect Profile, page 4-12.

Step 2 Copy the file to the FLASH on the security appliance:

```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```

Step 3 On the security appliance, add the profile as an available profile to the webvpn global section - (assuming everything else is set up correctly for AnyConnect connections):

```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```

Step 4 Edit the group policy you are using and add the 'svc modules' and 'svc profile' commands:

```
hostname(config)# group-policy GroupPolicy internal
    hostname(config)# group-policy GroupPolicy attributes
    hostname(config-group-policy)# webvpn
        hostame(config-group-webvpn)# svc modules value vpngina
        hostame(config-group-webvpn)# svc profiles value ReallyNewProfile
```

Using the Manifest File

The AnyConnect package that is uploaded on the security appliance contains a file called VPNManifest.xml. The following example shows some sample content of this file:

```
<?xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0">

<file version="2.1.0150" id="VPNCore" is_core="yes" type="exe" action="install">
       <uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>

 <file version="2.1.0150" id="gina" is_core="yes" type="exe" action="install"
module="vpngina">
       <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
</vpn>
```

The security appliance has stored on it configured profiles, as explained in Step 1 above, and it also stores one or multiple AnyConnect packages that contain the AnyConnect client itself, downloader utility, manifest file, and any other optional modules or supporting files.

When a remote user connects to the security appliance using WebLaunch or an existing standalone client, the downloader is downloaded first and run, and it uses the manifest file to ascertain whether there is a existing client on the remote user's PC that needs to be upgraded, or whether a fresh installation is required. The manifest file also contains information about whether there are any optional modules that must be downloaded and installed—in this case, the VPNGINA. The client profile also is pushed down from the security appliance. The installation of VPNGINA is activated by the command **svc modules value vpngina** configured under group-policy (webvpn) command mode as explained in Step 4. The AnyConnect client and VPNGINA are installed, and the user sees the AnyConnect Client at the next reboot, prior to Windows Domain logon.

When the users connects, the client and profile are passed down to the user's PC; the client and VPNGINA are installed; and the user sees the AnyConnect client at the next reboot, prior to logging in.

A sample profile is provided on the client PC when AnyConnect is installed:

C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile

Troubleshooting SBL

Use the following procedure if you encounter a problem with SBL:

Step 1 Ensure that the profile is being pushed.

Step 2 Delete prior profiles (search for them on the hard drive to find the location, *.xml).

Step 3 Using Windows Add/Remove Programs, uninstall the Cisco AnyConnect Client Start Before Login Components.

Step 4 Clear the user's AnyConnect log in the Event Viewer and retest.

Step 5 Web browse back to the security appliance to install the client again.

Step 6 Make sure the profile also appeared.

Step 7 Reboot once. On the next reboot, you should be prompted with the Start Before Logon prompt.

Step 8 Send the AnyConnect event log to Cisco in .evt format

Step 9 If you see the following error:

Description: Unable to parse the profile C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml. Host data not available.

delete the user profile.

Step 10 Go back to the .tmpl file, save a copy as an .xml file, and use that XML file as the default profile.

Configuring Start Before Logon (PLAP) on Windows Vista Systems

As on the other Windows platforms, the Start Before Logon feature enables the establishment of a VPN tunnel prior to the user's login on to the Windows system, so that users can connect to their corporate infrastructure before logging on to their PCs. Windows Vista (with Windows Server 2008), Microsoft's next-generation operating system, uses different mechanisms from Windows XP and Windows 2000 (with Windows 2003 server), so the AnyConnect client Start Before Logon feature on the Windows Vista platform uses a different mechanism well.

In the AnyConnect client, the new Start Before Logon feature is known as the Pre-Login Access Provider (PLAP), which is a connectable credential provider. This feature lets network administrators perform specific tasks, such as collecting credentials or connecting to network resources, prior to login. PLAP provides start Before Logon functions on Windows Vista and the Windows 2008 server. PLAP supports 32-bit and 64-bit versions of the operating system with vpnplap.dll and vpnplap64.dll, respectively. The PLAP function supports Windows Vista x86 and x64 versions.

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

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

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

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

Installing PLAP

The vpnplap.dll and vpnplap64.dll components are part of the existing GINA installation package, so the network administrator can load a single, add-on Start Before Logon package on the security appliance, which then installs the appropriate component for the target platform. PLAP is an optional feature. The installer software detects the underlying operating system and places the appropriate DLL in the system directory. For systems prior to Windows Vista, the installer installs the vpngina.dll component on 32-bit versions of the operating system. On Windows Vista or the Windows 2008 server, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component.

Note If you uninstall the AnyConnect client while leaving the VPNGINA or PLAP component installed, the VPNGINA or PLAP component is disabled and not visible to the user.

Once installed, PLAP is not active until the network administrator modifies the user profile <profile.xml> file to activate start before logon. See XML Settings for Enabling SBL, page 4-28. After activation, the user invokes the Network Connect component by clicking Switch User, then the Network Connect icon in the lower, right-hand part of the screen.

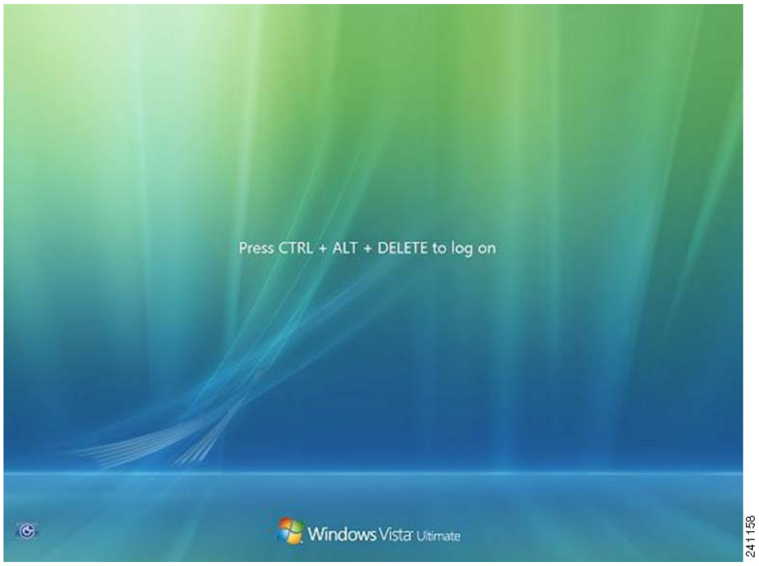
Note If the user mistakenly minimizes the user interface, he or she can restore it by pressing the Alt+Tab key combination.

Logging on to a Windows Vista PC using PLAP

To log on to Windows Vista when PLAP is enabled, do the following steps. (These steps are Microsoft requirements):

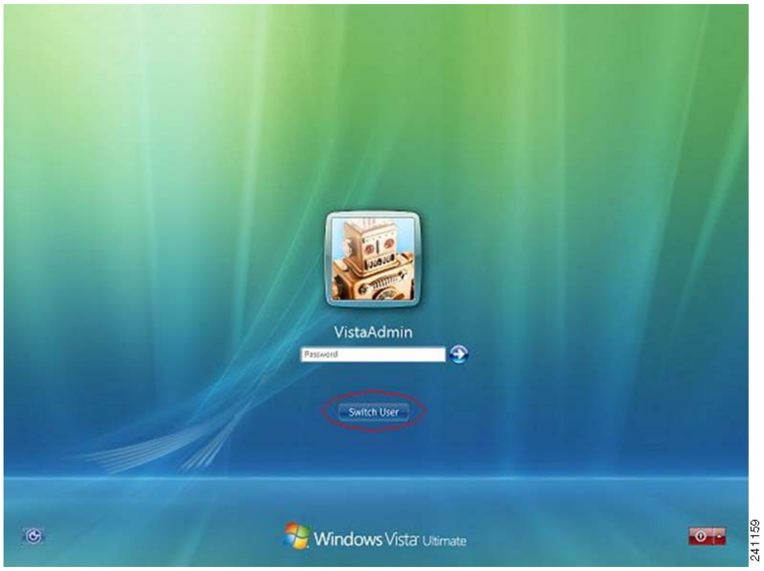
Step 1 At the Windows Vista start window, press the Ctrl+Alt+Delete key combination (Figure 4-6).

Figure 4-6 Vista Login Window Showing the Network Connect Button



This displays the Vista logon window with a Switch User button (Figure 4-7).

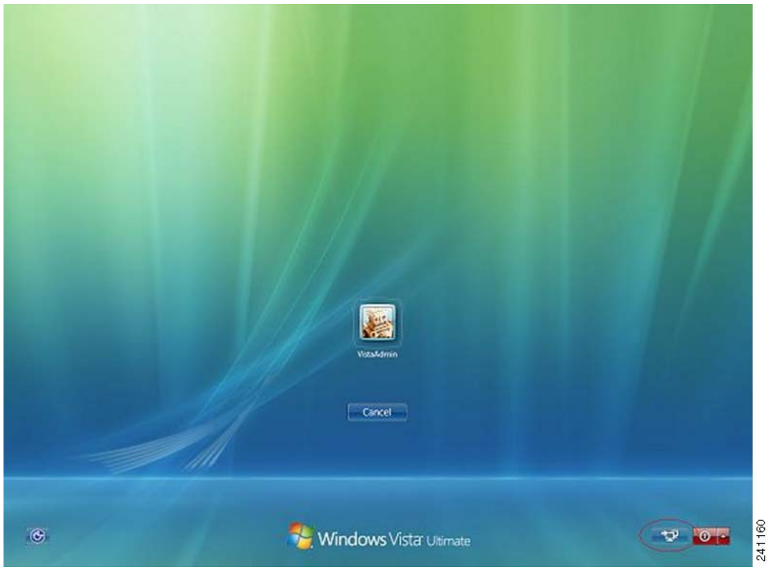
Figure 4-7 Vista Logon Window with Switch User Button



Step 2 Click Switch User (circled in red in this figure). This displays a Vista Network Connect window (Figure 4-8) with the network login icon in the lower-right corner. The network login icon is circled in red in Figure 4-8.

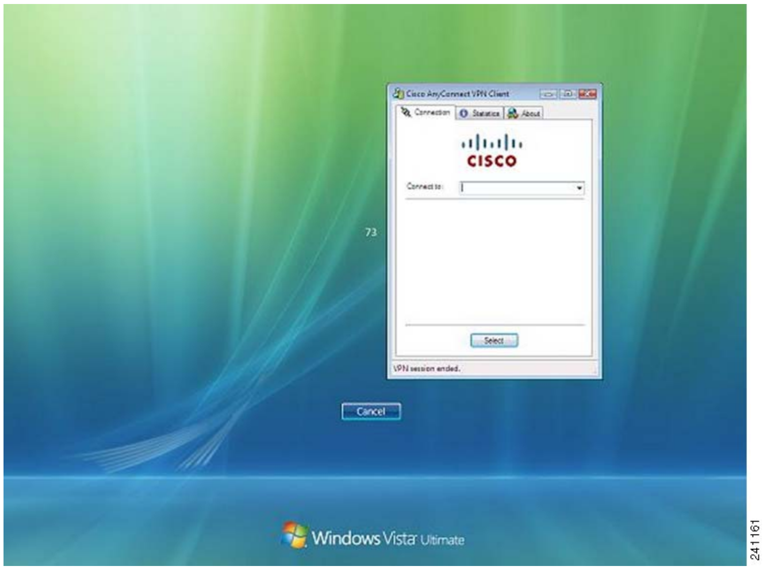
Note If the user is already connected through an AnyConnect tunnel and clicks Switch User, the first tunnel is not disconnected. If the user clicks Network Connect, then the first tunnel is disconnected. If the user clicks Cancel, the tunnel disconnects.

Figure 4-8 Vista Network Connect Window



Step 3 Click the Network Connect button in the lower-right corner of the window to launch the AnyConnect client. This displays the AnyConnect client logon window (Figure 4-9).

Figure 4-9 AnyConnect Client Logon Window



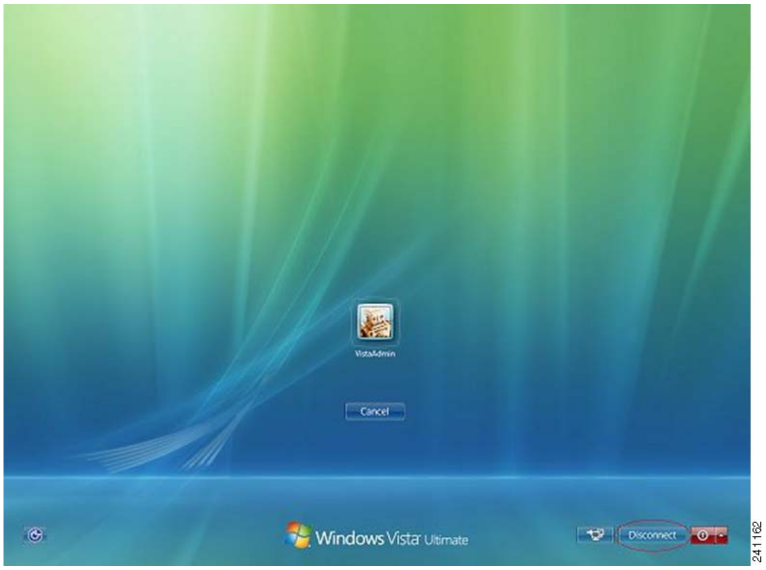
VPN session ended.

Step 4 Use this AnyConnect GUI to log in to the AnyConnect client as usual.

Note This example assumes that AnyConnect is the only installed connection provider. If there are multiple providers installed, you must select the one you want to use from the items displayed on this window.

Step 5 When you have successfully connected, you see a screen similar to the Vista Network Connect window, except that it has the Microsoft Disconnect button in the lower-right corner (Figure 4-10). This is the only indication that the connection is successful.

Figure 4-10 Disconnect Window



Click the icon associated with your login; in this example, click VistaAdmin to complete your logging on to the machine.

Caution Once the connection is established, you have an unlimited time in which to log on. If you forget to log on after connecting, the tunnel will be up indefinitely.

Disconnecting from the AnyConnect Client Using PLAP

After successfully connecting the tunnel, the PLAP component returns to the original window, this time with a Disconnect button displayed in the lower-right corner of the window (circled in Figure 4-10).

When you click Disconnect, the VPN tunnel disconnects.

In addition to explicitly disconnecting in response to the Disconnect button, the tunnel also disconnects in the following situations:

- When a user logs on to a PC using PLAP but then presses Cancel.
- When the PC is shut down before the user logs on to the system.

This behavior is a function of the Windows Vista PLAP architecture, not the AnyConnect client.

CHAPTER 5

Customizing and Localizing the AnyConnect Client and Installer

You can customize the AnyConnect VPN client and you can localize (translate) the client and the installer program for different languages.

This chapter contains the following sections:

Customizing the AnyConnect Client

You can customize the AnyConnect VPN client to display your own corporate image to remote users, including clients running on Windows, Linux, and Mac OS X PCs.

Note Customization is not supported for the AnyConnect client running on a Windows Mobile device.

You can use one of three methods to customize the client:

- Rebrand the client by importing individual client GUI components, such as the corporate logo and icons, to the security appliance which deploys them to remote PCs with the installer.
- Import your own program (Windows and Linux only) that provides its own GUI or CLI and uses the AnyConnect API.
- Import a transform (Windows only) that you create for more extensive rebranding. The security appliance deploys it with installer.

The following sections describe procedures for these methods:

- Replacing Individual GUI Components with your Custom Components, page 5-2
- Deploying Executables That Use the Client API, page 5-3
- Customizing the GUI with a Transform, page 5-5
- Information for Creating your Custom Icons and Logos, page 5-7

Replacing Individual GUI Components with your Custom Components

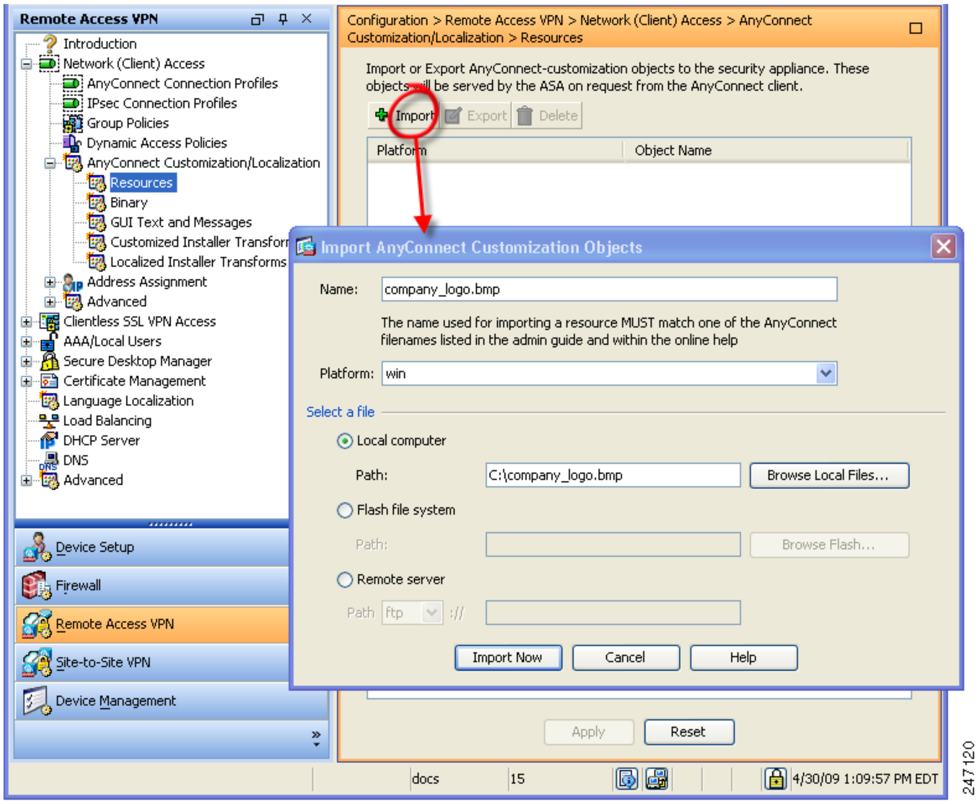
You can customize the AnyConnect client by importing your own custom files to the security appliance, which deploys the new files with the client. Table 5-2, Table 5-3, and Table 5-4 contain sample images of the original GUI icons and information about their sizes. You can use this information to create your custom files.

To import and deploy your custom files with the client, follow this procedure:

Step 1 Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources**.

Click **Import**. The Import AnyConnect Customization Object window displays (Figure 5-1).

Figure 5-1 Importing a Customization Object



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources

Import or Export AnyConnect-customization objects to the security appliance. These objects will be served by the ASA on request from the AnyConnect client.

Import AnyConnect Customization Objects

Name: company_logo.bmp

The name used for importing a resource MUST match one of the AnyConnect filenames listed in the admin guide and within the online help

Platform: win

Select a file

● Local computer

Path: C:\company_logo.bmp

○ Flash file system

Path:

○ Remote server

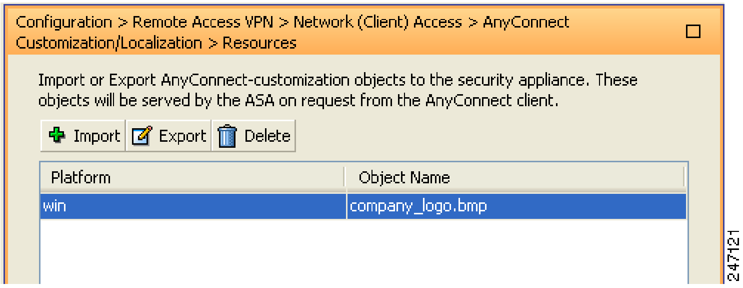
Path ftp ://

Step 2 Enter the Name of the file to import. See Table 5-2, Table 5-3, and Table 5-4 for the filenames of all the GUI components that you can replace.

Note The filenames of your custom components must match the filenames used by the AnyConnect client GUI. The filenames of the GUI components are different for each OS and are case sensitive for Mac and Linux. For example, if you want to replace the corporate logo for Windows clients, you must import your corporate logo as *company_logo.bmp*. If you import it as a different filename, the AnyConnect installer does not change the component.

Step 3 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table (Figure 5-2).

Figure 5-2 The Imported file displays in the Table



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources

Import or Export AnyConnect-customization objects to the security appliance. These objects will be served by the ASA on request from the AnyConnect client.

Platform	Object Name
win	company_logo.bmp

Deploying Executables That Use the Client API

For Windows, Linux, or Mac (PPP or Intel-based) PCs, you can deploy your own client that uses the AnyConnect client API. You replace the AnyConnect GUI or the AnyConnect CLI by replacing the client binary files. Table 5-1 lists the filenames of the client executable files for the different operating systems.

Table 5-1 Filenames of Client Executables

Client OS	Client GUI File	Client CLI File
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
Mac	Not supported[1]	vpn

[1] Not supported by security appliance deployment. However, you can deploy an executable for the Mac that replaces the client GUI using other means, such as Altiris Agent.

We recommend that you sign your custom Windows client binaries (either GUI or CLI version) that you import to the security appliance. A signed binary has a wider range of functionality available to it. If the binaries are not signed the following functionality is affected:

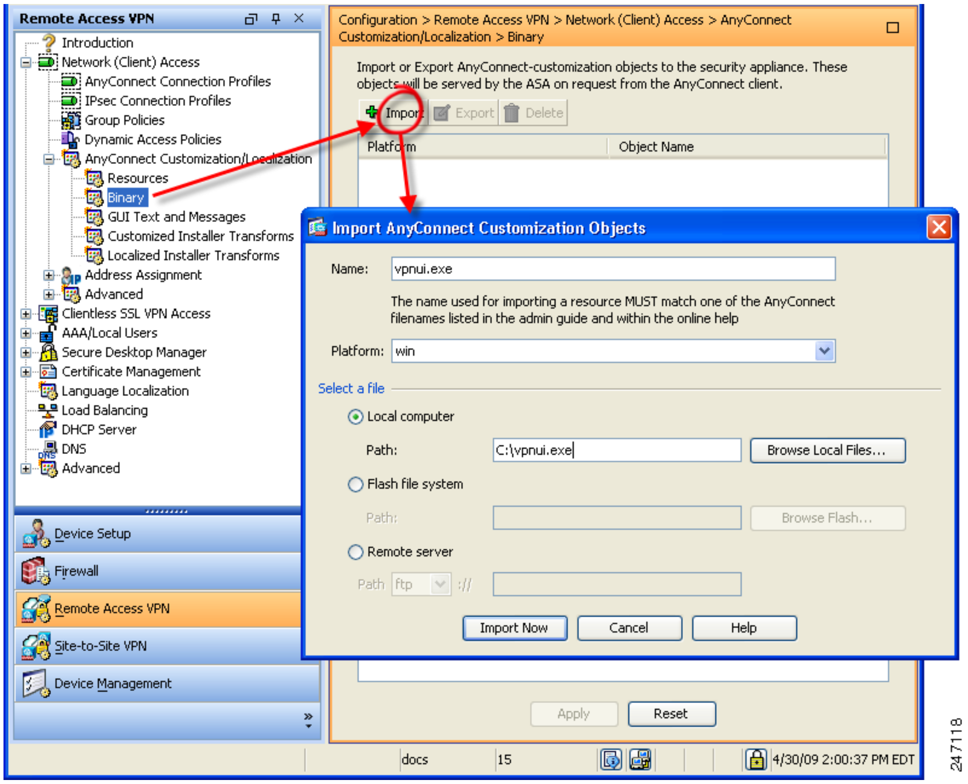
- Web-Launch—The clientless portal is available and the user can authenticate. However, the behavior surrounding tunnel establishment does not work as expected. Having an unsigned GUI on the client results in the client not starting as part of the clientless connection attempt. And once it detects this condition, it aborts the connection attempt.
- SBL—The Start Before Logon feature requires that the client GUI used to prompt for user credentials be signed. If it is not, the GUI does not start. Because SBL is not supported for the CLI program, this affects only the GUI binary file.
- Auto Upgrade—During the upgrade to a newer version of the client, the old GUI exits, and after the new GUI installs, the new GUI starts. The new GUI does not start unless it is signed. As with Web-launch, the VPN connection terminates if the GUI is not signed. However, the upgraded client remains installed.

To import your executable to customize the client GUI, follow these steps:

Step 1 Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Binary**.

Click **Import**. The Import AnyConnect Customization Objects window displays (Table 5-1).

Figure 5-3 Importing an Executable



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Binary

Import or Export AnyConnect-customization objects to the security appliance. These objects will be served by the ASA on request from the AnyConnect client.

Import AnyConnect Customization Objects

Name: vpnui.exe

The name used for importing a resource MUST match one of the AnyConnect filenames listed in the admin guide and within the online help

Platform: win

Select a file

● Local computer

Path: C:\vpnui.exe

○ Flash file system

Path:

○ Remote server

Path ftp ://

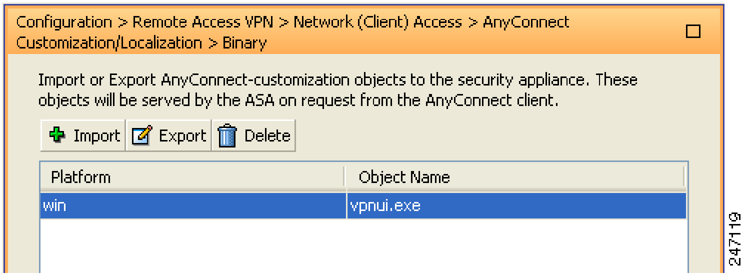
Import Now | Cancel | Help

Step 2 Enter the Name of the file to import.

The filenames of your executable must match the filenames used by the AnyConnect client GUI. For example, if you want to replace the client GUI for Windows clients, you must import your executable as *vpnui.exe*. If you import it as a different filename, the AnyConnect installer does not change the executable.

Step 3 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table (Figure 5-2).

Figure 5-4 The Imported Executable appears in the table



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Binary

Import or Export AnyConnect-customization objects to the security appliance. These objects will be served by the ASA on request from the AnyConnect client.

Platform	Object Name
win	vpnui.exe

Customizing the GUI with a Transform

You can perform more extensive customizing of the AnyConnect client GUI (Windows only) by creating your own transform that deploys with the client installer program. You import the transform to the security appliance, which deploys it with the installer program.

To create an MSI transform, you can download and install the free database editor from Microsoft, named Orca. With this tool, you can modify existing installations and even add new files. The Orca tool is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK. The following link leads to the bundle containing the Orca program:

> http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp.

After you install the SDK, the Orca MSI is located here:

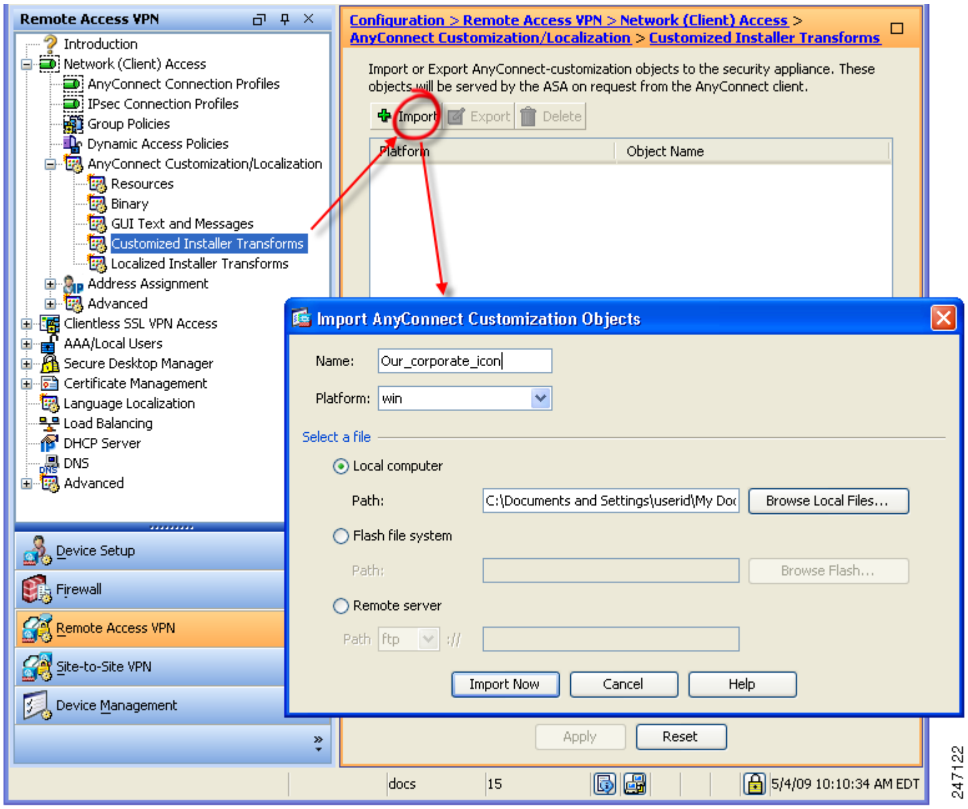
> C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi.

Install the Orca software, then access the Orca program from your Start > All Programs menu.

To import your transform, follow these steps:

Step 1 Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms**. Click **Import**. The Import AnyConnect Customization Objects windows displays (Figure 5-5).

Figure 5-5 Importing a Customizing Transform



Import or Export AnyConnect-customization objects to the security appliance. These objects will be served by the ASA on request from the AnyConnect client.

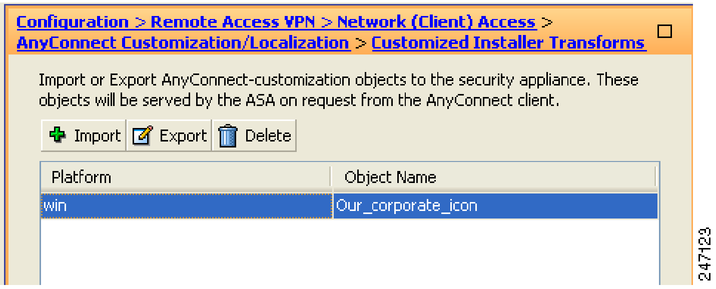
Name: Our_corporate_icon
Platform: win
● Local computer
Path: C:\Documents and Settings\userid\My Doc
○ Flash file system
Path:
○ Remote server
Path ftp ://

Step 2 Enter the Name of the file to import. Unlike the names of other customizing objects, the name is not significant to the security appliance and is for your own convenience.

Step 3 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table (Figure 5-6).

Note Windows is the only valid choice for applying a transform.

Figure 5-6 The Customizing Transform Appears in the Table



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms

Import or Export AnyConnect-customization objects to the security appliance. These objects will be served by the ASA on request from the AnyConnect client.

Platform	Object Name
win	Our_corporate_icon

Sample Transform

While offering a tutorial on creating transforms is beyond the scope of this document, we provide the text below as representative of some entries in a transform. These entries replace *company_logo.bmp* with a local copy and install the custom profile *MyProfile.xml*.

```
DATA CHANGE - Component Component ComponentId
+ MyProfile.xml {39057042-16A2-4034-87C0-8330104D8180}

Directory_ Attributes Condition KeyPath
Profile_DIR 0 MyProfile.xml

DATA CHANGE - FeatureComponents Feature_ Component_
  + MainFeature MyProfile.xml

DATA CHANGE - File File Component_ FileName FileSize Version Language Attributes Sequence
  + MyProfile.xml MyProfile.xml MyProf~1.xml|MyProfile.xml 601 8192 35
 <> company_logo.bmp 37302{39430} 8192{0}

DATA CHANGE - Media DiskId LastSequence DiskPrompt Cabinet VolumeLabel Source
  + 2 35
```

Information for Creating your Custom Icons and Logos

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

Note If you create your own custom images to replace the client icons, your images must be the same size as the original Cisco images.

For Windows

All files for Windows are located in %PROGRAMFILES%\Cisco\Cisco AnyConnect VPN Client\res\. Table 5-2 lists the files that you can replace and the client GUI area affected.

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

Table 5-2 Icon Files for AnyConnect Client for Windows

Filename in Windows Installation	Client GUI Area Affected	Image Size (pixels, l x h)
AboutTab.ico 	Icon that appears on the About tab.	16 x 16
company_logo.bmp 	Corporate logo that appears on each tab of the user interface.	142 x 92
connected.ico 	Tray icon that displays when the client is connected.	16 x 16
ConnectionTab.ico 	Icon that appears on the Connection tab.	16 x 16
disconnecting.ico 	Tray icon that displays when the client is in the process of disconnecting.	16 x 16
GUI.ico 	Icon that appears on the Windows Vista start-before-login screen.	48 x 48 32 x 32 24 x 24 16 x 16

Table 5-2 Icon Files for AnyConnect Client for Windows

Filename in Windows Installation	Client GUI Area Affected	Image Size (pixels, l x h)
reconnecting.ico	Tray icon that displays when the client is in the process of reconnecting.	16 x 16
StatsTab.ico	Icon that appears on the Statistics tab.	16 x 16
unconnected.ico	Tray icon that displays when the client is not connected.	16 x 16

For Linux

All files for Linux are located in /opt/cisco/vpn/pixmaps/. Table 5-3 lists the files that you can replace and the client GUI area affected.

Table 5-3 Icon Files for AnyConnect Client for Linux

Filename in Linux Installation	Client GUI Area Affected	Image Size (pixels, l x h)
company-logo.png	Corporate logo that appears on each tab of the user interface.	142 x 92
cvc-about.png	Icon that appears on the About tab.	16 x 16
cvc-connect.png	Icon that appears next to the Connect button, and on the Connection tab.	16 x 16
cvc-disconnect.png	Icon that appears next to the Disconnect button.	16 x 16
cvc-info.png	Icon that appears on the Statistics tab.	16 x 16
systray_connected.png	Tray icon that displays when the client is connected.	16 x 16

Table 5-3 Icon Files for AnyConnect Client for Linux (continued)

Filename in Linux Installation	Client GUI Area Affected	Image Size (pixels, l x h)
systray_notconnected.png	Tray icon that displays when the client is not connected.	16 x 16
systray_disconnecting.png	Tray icon that displays when the client is disconnecting.	16 x 16
systray_reconnecting.png	Tray icon that displays when the client is reconnecting.	16 x 16
vpnui48.png	Main program icon.	48 x 48

For Mac OS X

All files for OS X are located in /Applications/Cisco AnyConnect VPN Client/Contents/Resources. Table 5-4 lists the files that you can replace and the client GUI area affected.

Table 5-4 Icon Files for AnyConnect Client for Linux Mac OS X

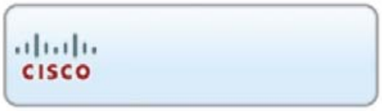
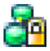
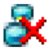
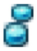
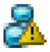
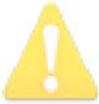
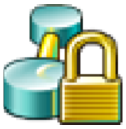
Filename in Mac OS X Installation	Client GUI Area Affected	Image Size (pixels, l x h)
bubble.png 	Notification bubble that appears when the client connects or disconnects.	142 x 92
connected.png	Icon that displays under the disconnect button when the client is connected.	32 x 32
logo.png	Logo icon that appears on main screen in the top right corner.	50 x 33

Table 5-4 Icon Files for AnyConnect Client for Linux Mac OS X (continued)

Filename in Mac OS X Installation	Client GUI Area Affected	Image Size (pixels, l x h)
menu_connected.png 	Connected state menu bar icon.	16 x 16
menu_error.png 	Error state menu bar icon.	16 x 16
menu_idle.png 	Disconnected idle menu bar icon.	16 x 16
menu_reconnecting.png 	Reconnection in process menu bar icon.	16 x 16
warning.png 	Icon that replaces login fields on various authentication/certificate warnings.	40 x 40
vpngui.icns 	Mac OS X icon file format that is used for all icon services, such as Dock, Sheets, and Finder.	128 x 128

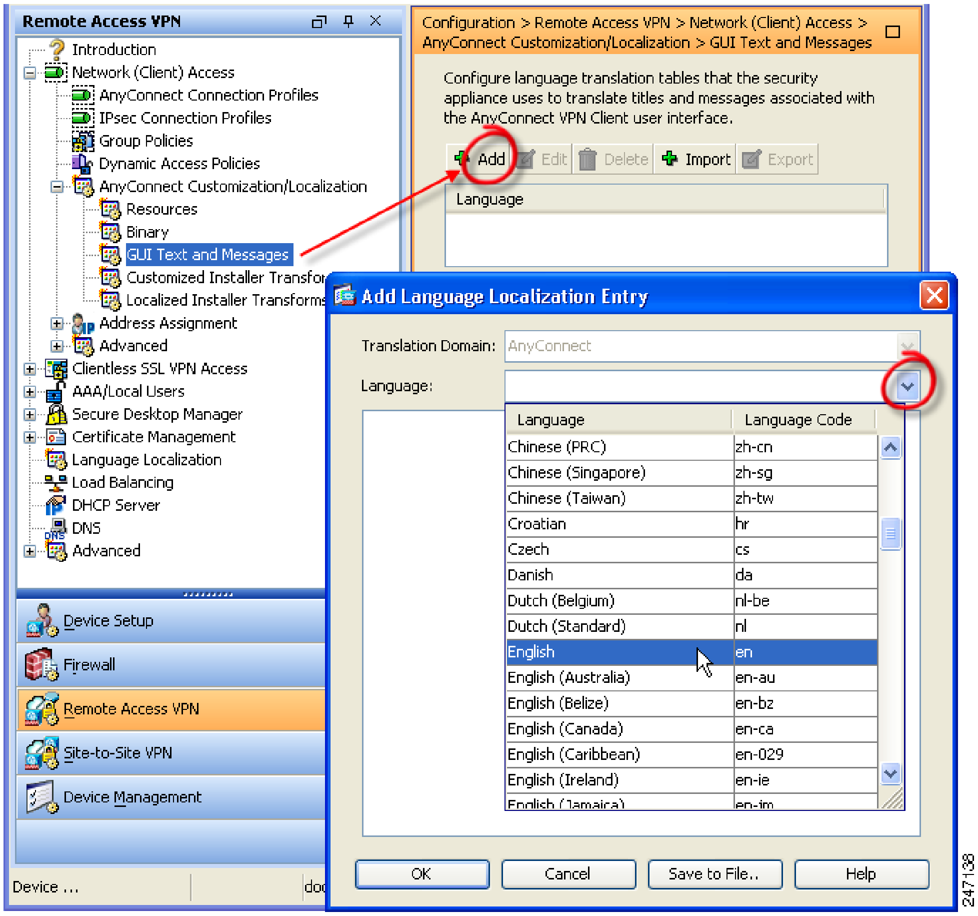
Changing the Default AnyConnect English Messages

You can make changes to the English messages displayed on the AnyConnect client GUI by adding an English translation table and changing message text within an editing window of ASDM.

The following procedure describes how to change the default English messages:

Step 1 Go to: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > GUI Text and Messages**. Click **Add**. The Add Language Localization Entry window displays (Figure 5-9).

Figure 5-7 Adding an English Translation Table



Configure language translation tables that the security appliance uses to translate titles and messages associated with the AnyConnect VPN Client user interface.

Translation Domain: AnyConnect

Language:

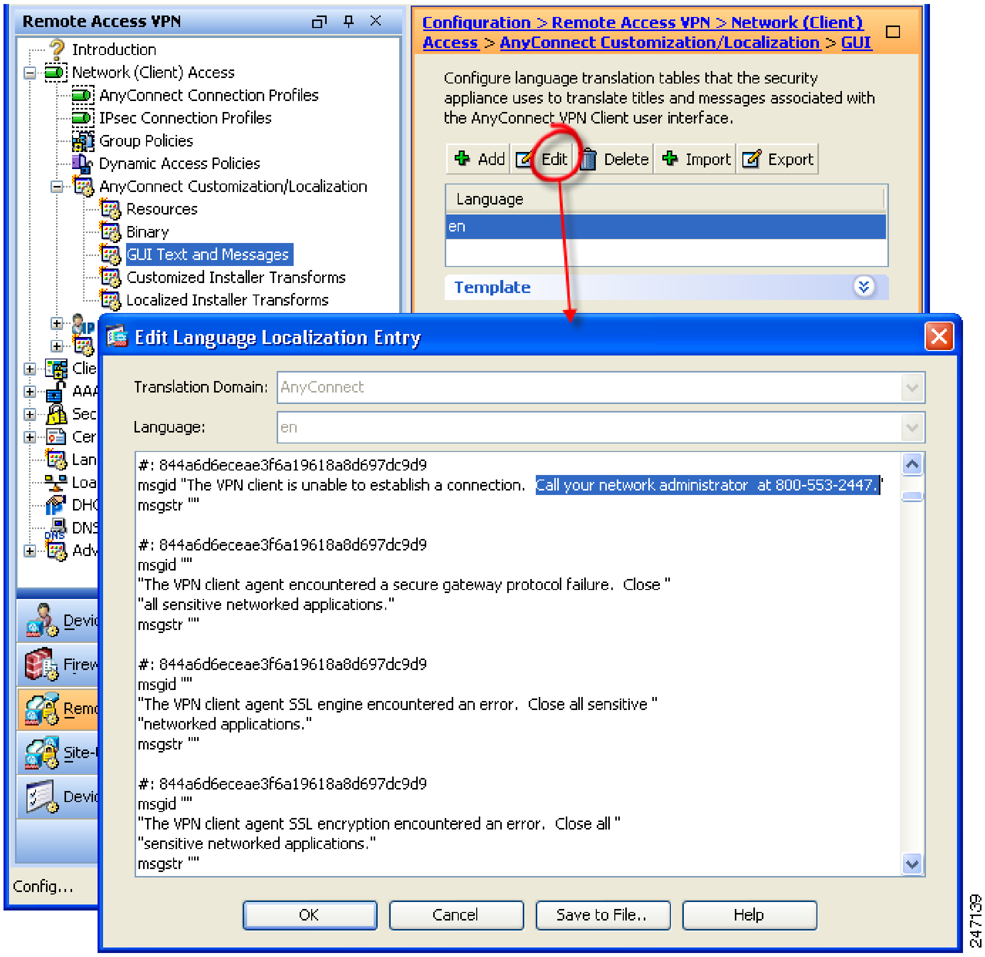
Language	Language Code
Chinese (PRC)	zh-cn
Chinese (Singapore)	zh-sg
Chinese (Taiwan)	zh-tw
Croatian	hr
Czech	cs
Danish	da
Dutch (Belgium)	nl-be
Dutch (Standard)	nl
English	en
English (Australia)	en-au
English (Belize)	en-bz
English (Canada)	en-ca
English (Caribbean)	en-029
English (Ireland)	en-ie
English (Jamaica)	en-jm

Step 2 Click the Language drop-list and specify the language as *English* (en). The translation table for English displays in the list of languages in the pane.

Step 3 Click **Edit** to begin editing the messages. The Edit Language Localization Entry window displays (Figure 5-8). The text between the quotes of msgid is the default English text displayed by the client, and *must not* be changed. The msgstr string contains text the client uses to replace the default text in msgid. You can replace the msgstr text with your own, custom text.

In the example below, we added “Call your network administrator at 800-553-2447”.

Figure 5-8 Editing the Message Text


Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
IPsec Connection Profiles
Group Policies
Dynamic Access Policies
AnyConnect Customization/Localization
Resources
Binary
GUI Text and Messages
Customized Installer Transforms
Localized Installer Transforms
Clie
AAA
Sec
Cer
Lan
Loa
DHC
DNS
Adv
Devic
Firew
Remo
Site-
Devic
Config...
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > GUI
Add
Edit
Delete
Import
Export
Language
Template
Edit Language Localization Entry
OK
Cancel
Save to File..
Help
247139

Configure language translation tables that the security appliance uses to translate titles and messages associated with the AnyConnect VPN Client user interface.

Language: en

Translation Domain: AnyConnect

Language: en

```
#: 844a6d6eceae3f6a19618a8d697dc9d9
msgid "The VPN client is unable to establish a connection.  Call your network administrator  at 800-553-2447."
msgstr ""

#: 844a6d6eceae3f6a19618a8d697dc9d9
msgid ""
"The VPN client agent encountered a secure gateway protocol failure.  Close "
"all sensitive networked applications."
msgstr ""

#: 844a6d6eceae3f6a19618a8d697dc9d9
msgid ""
"The VPN client agent SSL engine encountered an error.  Close all sensitive "
"networked applications."
msgstr ""

#: 844a6d6eceae3f6a19618a8d697dc9d9
msgid ""
"The VPN client agent SSL encryption encountered an error.  Close all "
"sensitive networked applications."
msgstr ""
```

Step 4 Click **Ok**, and then **Apply** in the GUI Text and Messages pane to save you changes.

Localizing the AnyConnect Client GUI and Installer

You can translate messages displayed by the AnyConnect VPN Client or the client installer program in the language preferred by the remote user.

Note If you are deploying the AnyConnect client using a corporate IT deployment software, such as Altiris Agent, you can only translate the installer. You cannot translate the client. Client translation is only available when the security appliance deploys the client.

The following sections contain information and procedures for configuring this feature using the CLI or ASDM:

- Localizing the AnyConnect GUI, page 5-13
- Localizing the AnyConnect Installer Screens, page 5-21
- Merging a Newer Translation Template with your Translation Table, page 5-23

Localizing the AnyConnect GUI

The security appliance uses translation tables to translate user messages displayed by the AnyConnect client. The translation tables are text files with strings to insert translated message text. The AnyConnect client package file for Windows contains an English language template for AnyConnect messages. The security appliance automatically imports this file when you load the client image. The file contains the latest changes to message strings and you can use it to create new translation tables for other languages.

We also provide translation tables for French and Japanese on the software download page for the AnyConnect client. These files may not include the latest messages added by Cisco software engineers, but you can conveniently use them instead of creating new translation tables for these languages from scratch. You can edit these files with a text or translation editor like Poedit and then import them, or you can import them first and then edit them using the translation table editor in ASDM.

When the remote user connects to the security appliance and downloads the client, the client detects the preferred language of the PC and applies the appropriate translation table. The client detects the locale specified during installation of the operating system. For more information about language options for Windows, go to these URLs:

http://www.microsoft.com/windowsxp/using/setup/winxp/yourlanguage.mspx
http://www.microsoft.com/globaldev/reference/win2k/setup/changeUI.mspx

Note If you are not deploying the client with the security appliance, and are using a corporate software deployment system such as Altiris Agent, you can manually convert the AnyConnect translation table (anyconnect.po) to a .mo file using a catalog utility such as Gettext, and install the .mo file to the proper folder on the client PC.

The following sections contain detailed procedures for two different methods of translating GUI text:

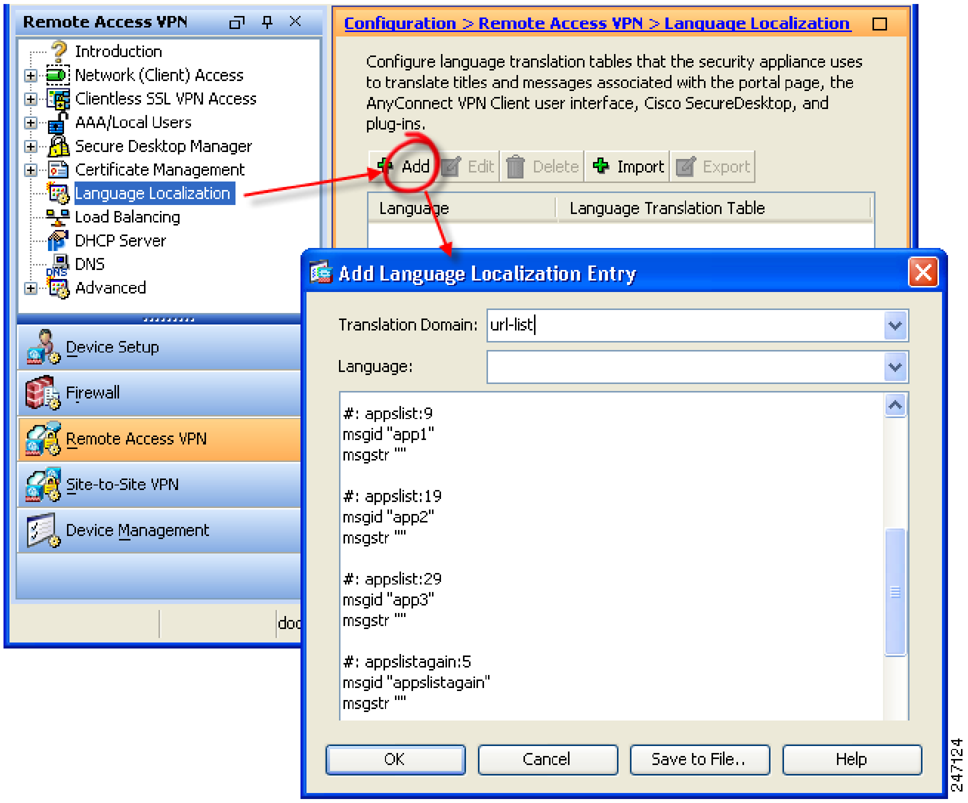
- Translating using the ASDM Translation Table Editor, page 5-14
- Translating by Exporting the Translation Table for Editing, page 5-18

Translating using the ASDM Translation Table Editor

The following procedure describes how to localize the AnyConnect client GUI using ASDM:

Step 5 Go to: **Configuration > Remote Access VPN > Language Localization**. Click Add. The Add Language Localization Entry window displays (Figure 5-9).

Figure 5-9 Language Localization Pane



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.

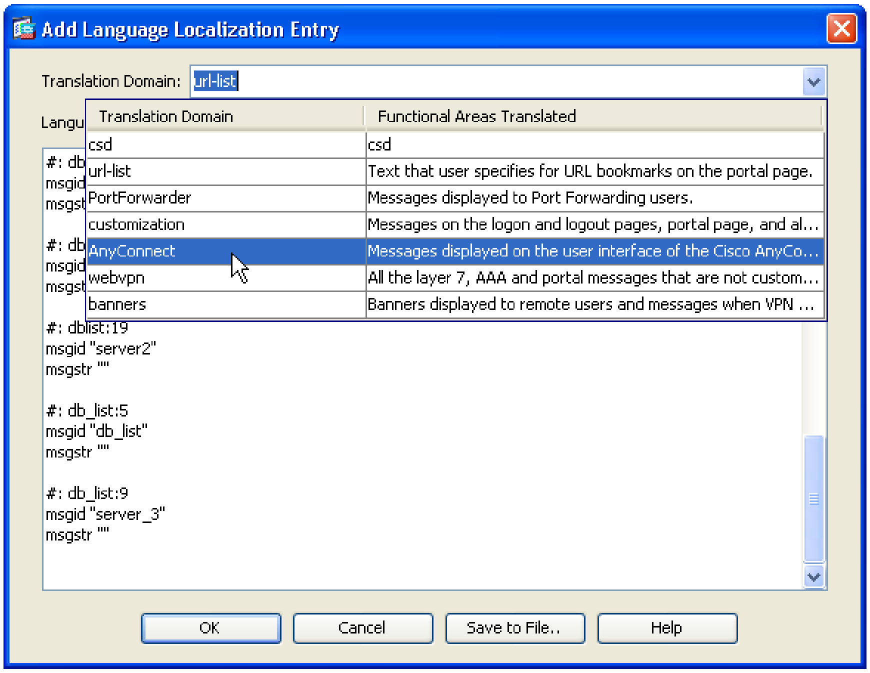
Translation Domain: url-list

Language:

```
#: appslist:9
msgid "app1"
msgstr ""

#: appslist:19
msgid "app2"
msgstr ""

#: appslist:29
msgid "app3"
msgstr ""

#: appslistagain:5
msgid "appslistagain"
msgstr ""
```

Step 6 Click the Translation Domain drop-list and choose *AnyConnect* (Figure 5-10). This ensures only the messages relating to the AnyConnect GUI appear for editing purposes.

Figure 5-10 Translation Domain



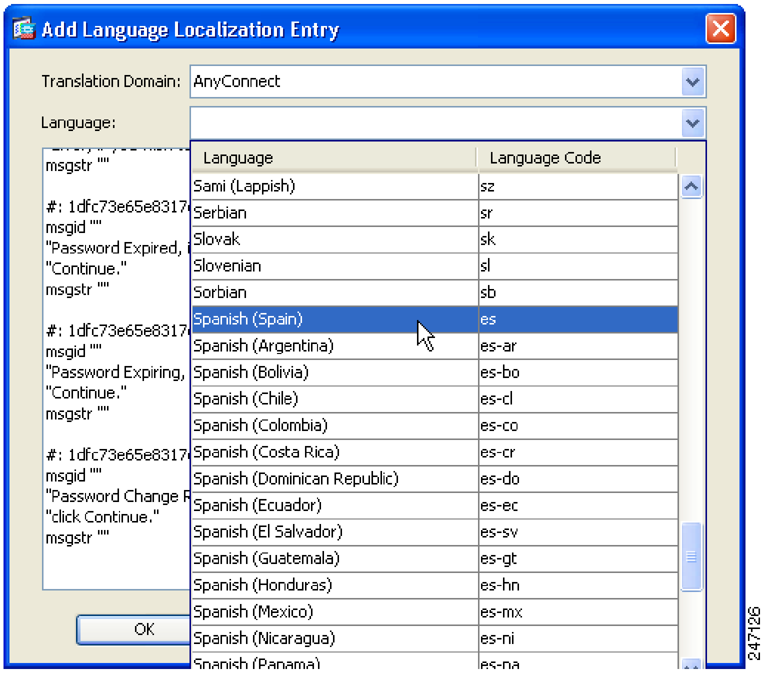
Translation Domain: url-list

Translation Domain	Functional Areas Translated
csd	csd
url-list	Text that user specifies for URL bookmarks on the portal page.
PortForwarder	Messages displayed to Port Forwarding users.
customization	Messages on the logon and logout pages, portal page, and al...
AnyConnect	Messages displayed on the user interface of the Cisco AnyCo...
webvpn	All the layer 7, AAA and portal messages that are not custom...
banners	Banners displayed to remote users and messages when VPN ...

```
#: db
msgid
msgst

#: db
msgid
msgst

#: dblist:19
msgid "server2"
msgstr ""

#: db_list:5
msgid "db_list"
msgstr ""

#: db_list:9
msgid "server_3"
msgstr ""
```

Step 7 Specify a language for this translation table (Figure 5-11). ASDM tags this table with the standard abbreviations recognized for languages by Windows and browsers (for example, *es* for Spanish).

Figure 5-11 Choosing a Language



Translation Domain: AnyConnect

Language:

```
msgstr ""

#: 1dfc73e65e8317
msgid ""
"Password Expired, 
"Continue."
msgstr ""

#: 1dfc73e65e8317
msgid ""
"Password Expiring,
"Continue."
msgstr ""

#: 1dfc73e65e8317
msgid ""
"Password Change R
"click Continue."
msgstr ""
```

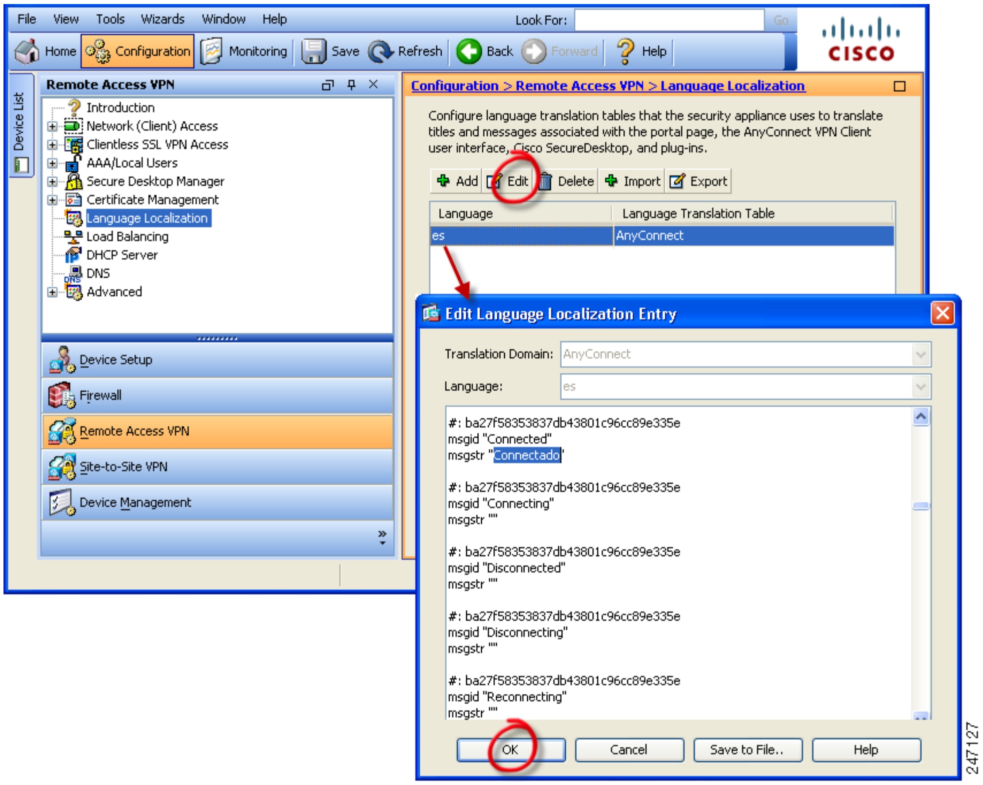
Language	Language Code
Sami (Lappish)	sz
Serbian	sr
Slovak	sk
Slovenian	sl
Sorbian	sb
Spanish (Spain)	es
Spanish (Argentina)	es-ar
Spanish (Bolivia)	es-bo
Spanish (Chile)	es-cl
Spanish (Colombia)	es-co
Spanish (Costa Rica)	es-cr
Spanish (Dominican Republic)	es-do
Spanish (Ecuador)	es-ec
Spanish (El Salvador)	es-sv
Spanish (Guatemala)	es-gt
Spanish (Honduras)	es-hn
Spanish (Mexico)	es-mx
Spanish (Nicaragua)	es-ni
Spanish (Panama)	es-pa

Step 8 The translation table now displays in the list of languages in the pane (*es* in our example). However, it has no translated messages. To begin adding translated text, click **Edit**. The Edit Language Localization Entry window displays (Figure 5-12).

Add your translated text between the quotes of the message strings (msgstr). In the example below, we insert *Connectado*, the Spanish word for *Connected*, between the quotes of its message string.

Be sure to click **Ok**, and then **Apply** in the Language Localization pane to save you changes.

Figure 5-12 *Editing the Translation Table*



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 Translation Table
es	AnyConnect

Translation Domain: AnyConnect

Language: es

```
#: ba27f58353837db43801c96cc89e335e
msgid "Connected"
msgstr "Connectado"

#: ba27f58353837db43801c96cc89e335e
msgid "Connecting"
msgstr ""

#: ba27f58353837db43801c96cc89e335e
msgid "Disconnected"
msgstr ""

#: ba27f58353837db43801c96cc89e335e
msgid "Disconnecting"
msgstr ""

#: ba27f58353837db43801c96cc89e335e
msgid "Reconnecting"
msgstr ""
```

Translating by Exporting the Translation Table for Editing

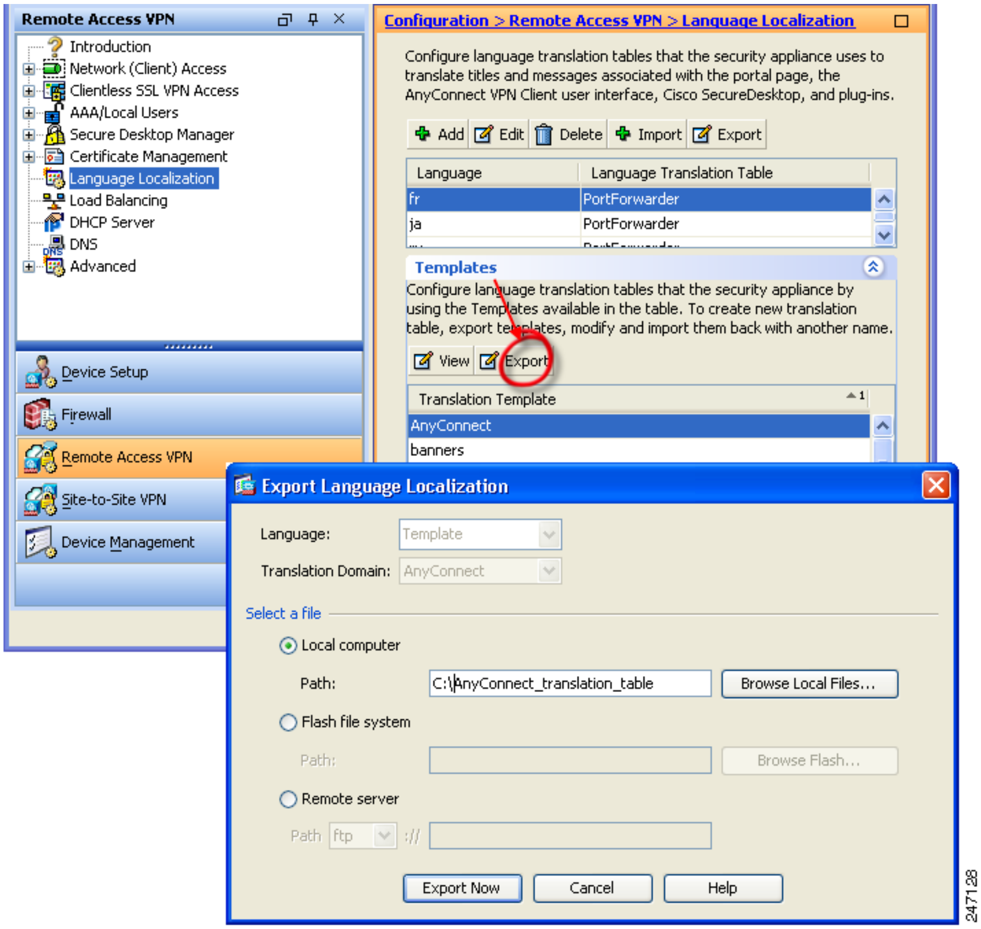
This procedure shows you how to export the AnyConnect translation template to a remote PC, where you can edit the table using an editor or using third party tools such as Gettext or Poedit.

Gettext utilities from The GNU Project is available for Windows and runs in the command window. See the GNU website at gnu.org for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at poedit.net.

Step 1 Export the AnyConnect translation template.

Go to **Configuration > Remote Access VPN > Language Localization**. The language localization pane displays (Figure 5-13). Click the **Templates** link to display a table of available templates. Select the *AnyConnect* template and click **Export**. The Export Language Localization window displays. Choose a method to export and provide a filename. In Figure 5-13, we export to a local PC with the filename *AnyConnect_translation_table*.

Figure 5-13 Exporting a Translation Template



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 Translation Table
fr	PortForwarder
ja	PortForwarder

Configure language translation tables that the security appliance by using the Templates available in the table. To create new translation table, export templates, modify and import them back with another name.

Translation Template
AnyConnect
banners

Language: Template

Translation Domain: AnyConnect

● Local computer

Path: C:\AnyConnect_translation_table

○ Flash file system

Path:

○ Remote server

Path ftp ://

Step 2 Edit the translation table.

The following example shows a portion of the AnyConnect template. The end of this output includes a message ID field (msgid) and a message string field (msgstr) for the message *Connected*, which appears on the AnyConnect client GUI when the client establishes a VPN connection (the complete template contains many pairs of message fields):

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\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=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

msgid "Connected"
msgstr ""
```

The msgid contains the default translation. The msgstr that follows msgid provides the translation. To create a translation, enter the translated text between the quotes of the msgstr string. For example, to translate the message “Connected” with a Spanish translation, insert the Spanish text between the quotes:

```
msgid "Connected"
msgstr "Conectado"
```

Be sure to save the file.

Step 3 Import the translation template as a new translation table for a specific language.

Go to **Configuration > Remote Access VPN > Language Localization**. The language localization pane displays (Figure 5-13). Click **Import**. The Import Language Localization window displays.

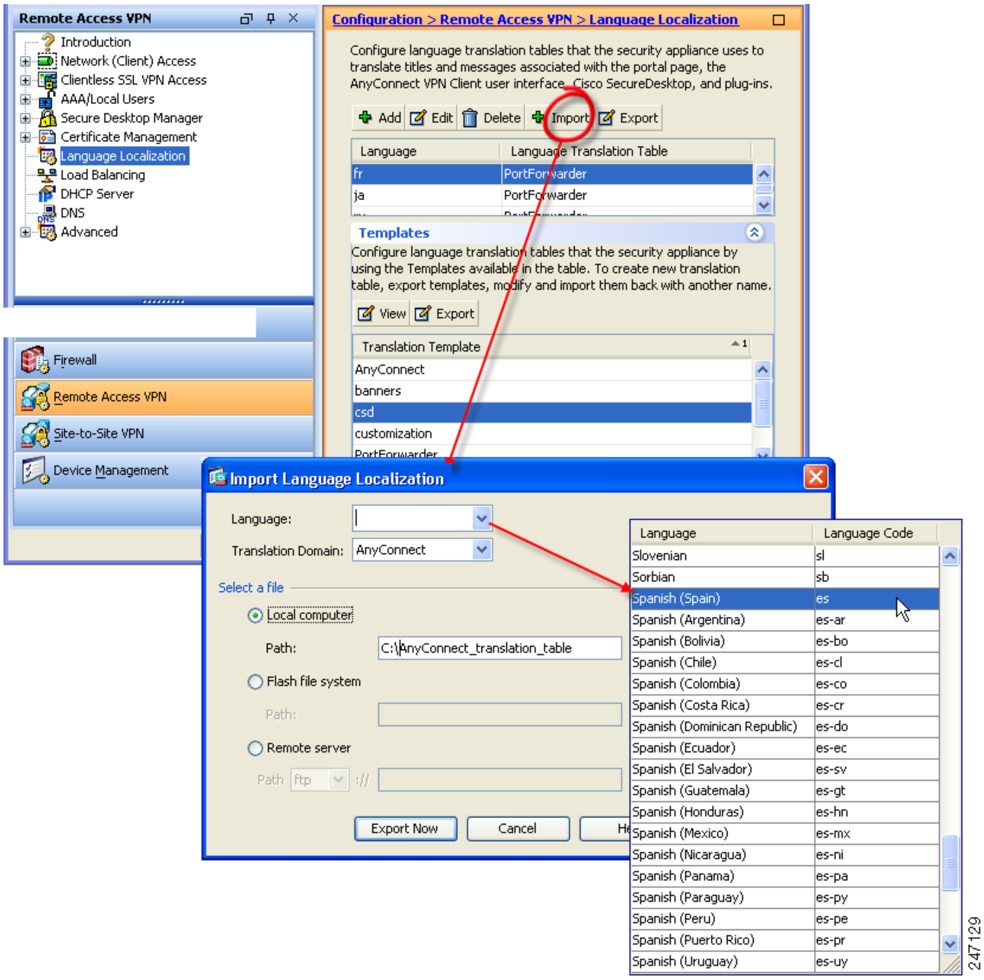
Step 4 Choose a language for this translation table. Click the Language drop-list to display languages and their industry-recognized abbreviations. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.

Step 5 Specify the Translation Domain as *AnyConnect,* choose a method to import, and provide a filename. Click Export Now. A message displays saying you successfully import the table.

Be sure to click **Apply** to save your changes.

In Figure 5-13, we specify the language as *Spanish* (es) and import the same file we exported in Step 1 (AnyConnect_translation_table). Figure 5-15 shows the new translation table for Spanish in the list of Languages for AnyConnect.

Figure 5-14 Importing a Translation Template as a new Translation Table



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 Translation Table
fr	PortForwarder
ja	PortForwarder

Configure language translation tables that the security appliance by using the Templates available in the table. To create new translation table, export templates, modify and import them back with another name.

Translation Template
AnyConnect
banners
csd
customization
PortForwarder

Language:

Translation Domain: AnyConnect

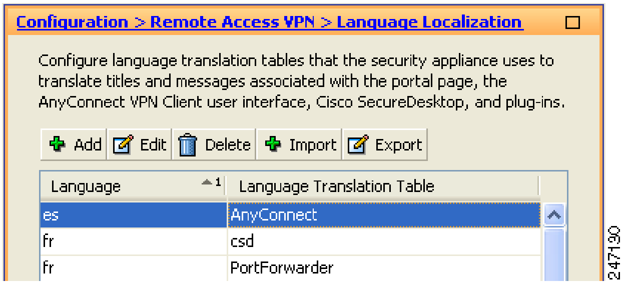
○ Local computer — Path: C:\AnyConnect_translation_table

○ Flash file system — Path:

○ Remote server — Path ftp ://

Language	Language Code
Slovenian	sl
Sorbian	sb
Spanish (Spain)	es
Spanish (Argentina)	es-ar
Spanish (Bolivia)	es-bo
Spanish (Chile)	es-cl
Spanish (Colombia)	es-co
Spanish (Costa Rica)	es-cr
Spanish (Dominican Republic)	es-do
Spanish (Ecuador)	es-ec
Spanish (El Salvador)	es-sv
Spanish (Guatemala)	es-gt
Spanish (Honduras)	es-hn
Spanish (Mexico)	es-mx
Spanish (Nicaragua)	es-ni
Spanish (Panama)	es-pa
Spanish (Paraguay)	es-py
Spanish (Peru)	es-pe
Spanish (Puerto Rico)	es-pr
Spanish (Uruguay)	es-uy

Figure 5-15 New Language Displayed in Language Table



Configuration > Remote Access VPN > 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 Translation Table
es	AnyConnect
fr	csd
fr	PortForwarder

Localizing the AnyConnect Installer Screens

As with the AnyConnect client GUI, you can translate messages displayed by the client installer program. The security appliance uses transforms to translate the messages displayed by the installer. The transform alters the installation, but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.

Each language has its own transform. You can edit a transform with a transform editor such as Orca, and make changes to the message strings. Then you import the transform to the security appliance. When the user downloads the client, the client detects the preferred language of the PC (the locale specified during installation of the operating system) and applies the appropriate transform.

We currently offer transforms for 30 languages. These transforms are available in the following .zip file on the AnyConnect client software download page at cisco.com:

anyconnect-win-<VERSION>-web-deploy-k9-lang.zip

In this file, `<VERSION>` is the version of AnyConnect release (e.g. 2.2.103).

The package contains the transforms (.mst files) for the available translations. If you need to provide a language to remote users that is not one of the 30 languages we provide, you can create your own transform and import it to the security appliance as a new language. With Orca, the database editor from Microsoft, you can modify existing installations and new files. Orca is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK. The following link leads to the bundle containing the Orca program:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp.

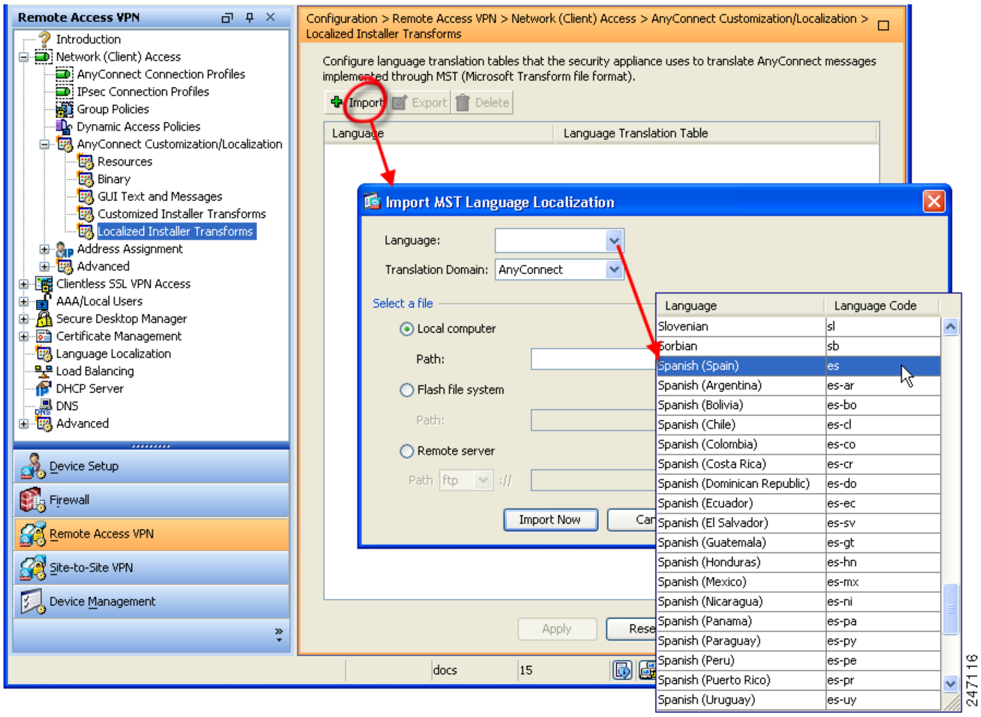
After you install the SDK, the Orca MSI is located here:

C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi.

The following procedure shows how to import a transform to the security appliance using ASDM:

Step 1 Import a Transform. Go to: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Localized Installer Transforms**. Click **Import**. The Import MST Language Localization window opens (Figure 5-16).

Figure 5-16 Importing a Transform to Translate the Installer Program



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Localized Installer Transforms

Configure language translation tables that the security appliance uses to translate AnyConnect messages implemented through MST (Microsoft Transform file format).

Language	Language Translation Table

Import MST Language Localization

Language:

Translation Domain: AnyConnect

Select a file

● Local computer

Path:

○ Flash file system

Path:

○ Remote server

Path ftp ://

Import Now Cancel

Language	Language Code
Slovenian	sl
Sorbian	sb
Spanish (Spain)	es
Spanish (Argentina)	es-ar
Spanish (Bolivia)	es-bo
Spanish (Chile)	es-cl
Spanish (Colombia)	es-co
Spanish (Costa Rica)	es-cr
Spanish (Dominican Republic)	es-do
Spanish (Ecuador)	es-ec
Spanish (El Salvador)	es-sv
Spanish (Guatemala)	es-gt
Spanish (Honduras)	es-hn
Spanish (Mexico)	es-mx
Spanish (Nicaragua)	es-ni
Spanish (Panama)	es-pa
Spanish (Paraguay)	es-py
Spanish (Peru)	es-pe
Spanish (Puerto Rico)	es-pr
Spanish (Uruguay)	es-uy

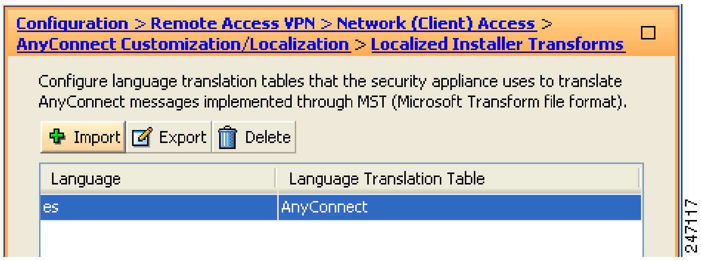
Step 2 Choose a language for this transform. Click the Language drop-list to display languages and their industry-recognized abbreviations. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.

Step 3 Click **Export Now**. A message displays saying you successfully import the table.

Be sure to click **Apply** to save your changes.

In Figure 5-16, we specify the language as *Spanish* (es). Figure 5-17 shows the new transform for Spanish in the list of Languages for AnyConnect.

Figure 5-17 Imported Transform Displays in the Table



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Localized Installer Transforms

Configure language translation tables that the security appliance uses to translate AnyConnect messages implemented through MST (Microsoft Transform file format).

Language	Language Translation Table
es	AnyConnect

Merging a Newer Translation Template with your Translation Table

Occasionally, we add new messages displayed to AnyConnect users that provide helpful information about the client connection. To enable translation of these new messages, we create new message strings and include them in the translation template packaged with the latest client image. Therefore, if you upgrade to the latest available client, you also receive the template with the new messages. However, if you have created translation tables based on the template included with the previous client, the new messages *are not* automatically displayed to remote users. You must merge the latest template with your translation table to ensure your translation table has these new messages.

You can use convenient third party tools to perform the merge. Gettext utilities from The GNU Project is available for Windows and runs in the command window. See the GNU website at gnu.org for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at poedit.net. Both methods are covered in the procedure below.

Step 1 Export the latest AnyConnect Translation Template from **Remote Access VPN > Language Localization > Templates.** Export the template with the filename as *AnyConnect.pot*. This filename ensures that the msgmerge.exe program recognizes the file as a message catalog template.

Note This step assumes you have already loaded the latest AnyConnect image package to the security appliance. The template is not available for export until you do.

Step 2 Merge the AnyConnect Template and Translation Table.

If you are using the Gettext utilities for Windows, open a command prompt window and run the following command. The command merges the AnyConnect translation table (.po) and the template (.pot), creating the new *AnyConnect_merged.po* file:

msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot

The following example shows the results of the command:

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po
AnyConnect.pot
....................................... done.
```

If you are using Poedit, first open the AnyConnect.po file; Go to File > Open > <*AnyConnect.po*>.
Then merge it with the template; go to Catalog > Update from POT file <*AnyConnect.pot*>.
Poedit displays an Update Summary window with both new and obsolete strings. Save the file, which we will import in the next step.

Step 3 Import the Merged Translation Table from **Remote Access VPN > Language Localization**. Click **Import,** specify a language, and select *AnyConnect* as the Translation Domain. Specify the file to import as *AnyConnect_merged.po*.

CHAPTER 6

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:

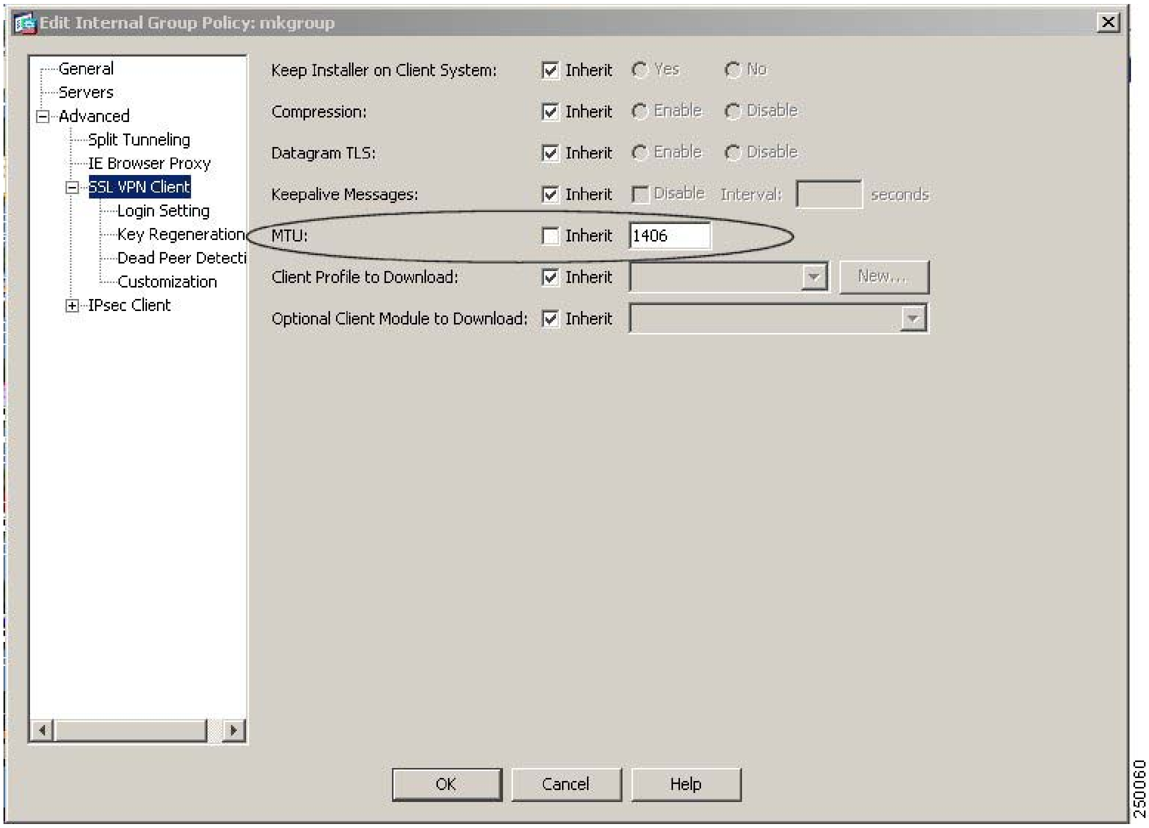
```
hostname# show vpn-sessiondb svc

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 6-1 Edit Internal Group Policy Dialog Box



Edit Internal Group Policy: mkgroup

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 the 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. Because 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 6-1).

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 "testuser" 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.

Viewing Detailed Statistical Information

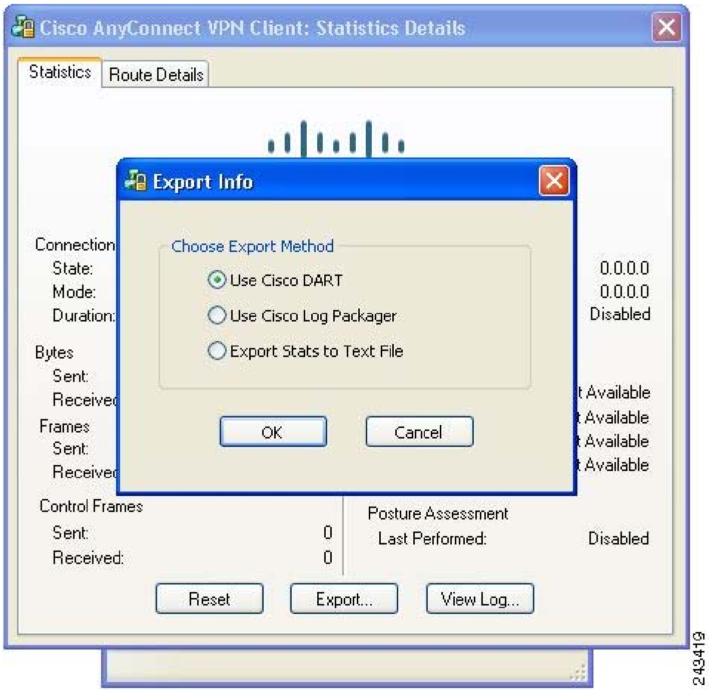
A user can view statistical information for a current AnyConnect client session by clicking the Details button on the GUI (see Figure 1-3).

This opens the Statistics Details window (Figure 1-4). On the Statistics tab in this window, you can reset the statistics, export the statistics, or view an HTML-format log of the statistics for this session. This section describes how to export and view the detailed session statistics.

Exporting Statistics

To export AnyConnect connection statistics to a reporting format, click Export at the bottom of the Statistics Details window. The Export Info dialog box appears (Figure 6-2).

Figure 6-2 Export Info Dialog Box



Choose Export Method
● Use Cisco DART
○ Use Cisco Log Packager
○ Export Stats to Text File

Connection
State:
Mode:
Duration:
Bytes
Sent:
Receivec
Frames
Sent:
Receivec
Control Frames
Sent: 0
Received: 0

0.0.0.0
0.0.0.0
Disabled
t Available
t Available
t Available
t Available
Posture Assessment
Last Performed: Disabled

The options available in this window depend on the packages that are loaded on the client PC. If an option is not available, its radio button is not active and a "(Not Installed)" indicator appears next to the option name in the dialog box. The options are as follows:

- Use Cisco DART—DART (Diagnostic AnyConnect Reporting Tool) bundles specified log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connection. *See Release Notes for Cisco AnyConnect VPN Client, Release 2.3* for information about the DART package.
- Use Cisco Log Packager—Collects log files from compliant Cisco utilities (not just the AnyConnect client) into a particular folder and compresses them into a .zip file. This function is similar to DART, but it uses a different format.
- Export Stats to Text File—Saves the connection statistics to a text file for later analysis and debugging.

Select an option and click OK. The AnyConnect client prompts you for the location to which you want to save the file or bundle. Enter a file name and save the file.

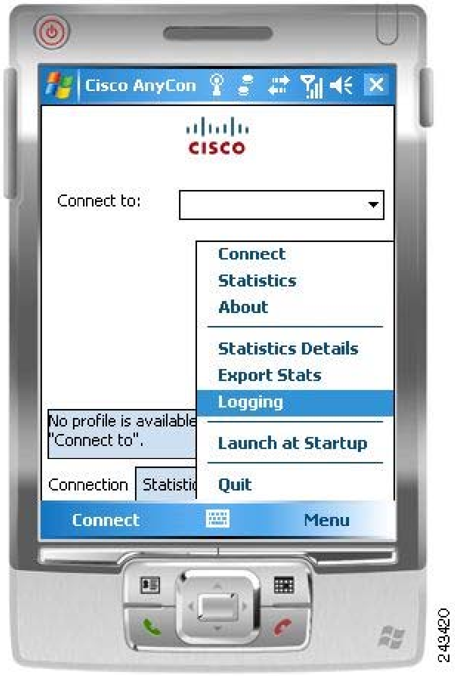
Viewing the Log

To view the log as an HTML file in a browser window, click View Log on the Statistics Detail window. The log information appears in a new browser window, showing the number of message instances, the end-user node name, the event codes and types, the log file name, the event messages, the source of the message, and the time themessage was generated. The browser window might take a short time to appear after you click View Log.

Viewing Statistics on a Windows Mobile Device

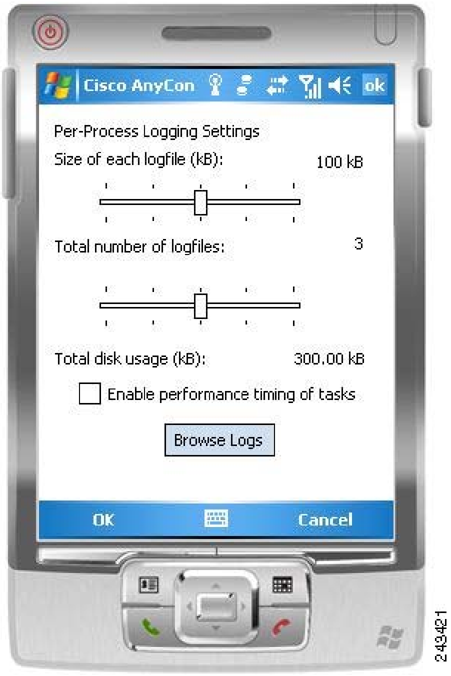
An AnyConnect user with a Windows Mobile device can also use the statistical details export and logging functions by clicking Menu on the lower-right corner of the screen and selecting the desired function from the menu that appears (Figure 6-3).

Figure 6-3 Windows Mobile Logging Menu



Clicking on Logging opens the logging settings dialog box (Figure).

Figure 6-4 Windows Mobile Logging Settings Dialog Box



Per-Process Logging Settings

Size of each logfile (kB): 100 kB

Total number of logfiles: 3

Total disk usage (kB): 300.00 kB

□ Enable performance timing of tasks

Move the sliders on this dialog box to control the total number of log files and the size of each log file and to enable performance timing of tasks.

Click Browse Logs to display an HTML list of the log messages in a separate browser window.

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-5

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

This profile and the profile schema that follows are different from those for earlier AnyConnect client releases.

Caution This example profile contains enterprise-specific values that do not work for other networks. Set the values to those that are consistent with your network.

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

    Please refer to the Cisco AnyConnect VPN Client Administrator Guide
    for information regarding profile management and examples of all
    available options. In short:

      - A Profile should be uniquely named for your Company.  An example is:
        CiscoProfile.xml

      - The profile name should be the same even if different for individual
        group within the company.
    This file is intended to be maintained by a Secure Gateway administrator
    and then distributed with the client software.  The profile based on
    this XML 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>
        <!--
            This control enables an administrator to have a one time message
            displayed prior to a users first connection attempt.  As an example,
            the message could be used to remind a user to insert their smart
            card into it’s reader.

            The message to be used with this control is localizable and can be
            found in the AnyConnect message catalog.
            (default: "This is a pre-connect reminder message.")
          -->
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <!--
            This setting allows an administrator to specify which certificate
            store AnyConnect will use for locating certificates.

            This setting only applies to the Microsoft Windows version of
            AnyConnect and has no effect on other platforms.
          -->
        <CertificateStore>All</CertificateStore>
        <!--
            This setting allows an administrator to direct AnyConnect to search
            for certificates in the Windows machine certificate store.  This is
            useful in cases where certificates are located in this store and
            users do not have administrator privileges on their machine.
          -->
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <!--
            Controls AnyConnect client behavior when started.  By default, the
    client will attempt to contact the last Gateway a user connected
    to or the first one in the list from the AnyConnect profile.  In
    the case of certificate-only authentication, this will result in
    the establishment of a VPN tunnel when the client is started.
  -->
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<!--
    Controls AnyConnect GUI behavior when a VPN tunnel is established.
    By default, the GUI will minimize when the VPN tunnel is
    established.
  -->
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<!--
    If Local LAN access is enabled for remote clients on the Secure
    Gateway, this setting can be used to allow the user to accept or
    reject this access.
  -->
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
<!--
    This setting allows an administrator to control how a client will
    behave when the VPN tunnel is interrupted.  Control can optionally
    be given to the user.
  -->
<AutoReconnect UserControllable="true">true
  <AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<!--
    This setting allows the adminstrator to turn off the dynamic
    update functionality of AnyConnect.  Control of this can also be
    given to the user.
  -->
<AutoUpdate UserControllable="false">true</AutoUpdate>
<!--
    This setting allows the adminstrator to control how the user will
    interact with RSA.  By default, AnyConnect will determine the
    correct method of RSA interaction.  The desired setting can be
    locked down by the administrator or control can be given to the
    user.
  -->
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<!--
    This setting allows the adminstrator to control if more than one
    user may be logged into the client PC during a VPN connection.
  -->
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<!--
    This setting allows the adminstrator to control if a VPN
    connection may be initiated by a remote user.
  -->
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<!--
    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>
        </ExtendedKeyUsage>
    </CertificateMatch>
    <MobilePolicy>
        <!--
        DeviceLockRequired indicates that a Windows Mobile device must
        be configured with a password or PIN prior to establishing a
        VPN connection.  This configuration is only valid on Windows
        Mobile devices that use the Microsoft Default Local
        Authentication Provider (LAP).

        The following attributes can be specified to check additional
        settings.  The platforms for which each additional check is
        performed as specified with "WM5AKU2+" for Windows Mobile 5 with
        the Messaging and Security Feature Pack delivered as part of
        Adaption Kit Upgrade 2 (AKU2).

            MaximumTimeoutMinutes - when set to non-negative
                number, specifies the maximum number of minutes
                that must be configured before device lock takes
                effect.  (WM5/WM5AKU2+)
            MinimumPasswordLength - when set to a non-negative number,
                specifies that any PIN/password used for device lock
                must be equal to or longer than the specified value,
                in characters.  This setting must be pushed down to
                the mobile device by syncing with an Exchange server
                before it can be enforced. (WM5AKU2+)
            PasswordComplexity - when present checks for the following
                password subtypes:
                    "alpha"  - Requires an alphanumeric password
                    "pin"    - Numeric PIN required
                    "strong" - Strong alphanumeric password defined by
                               Microsoft as containing at least 7
                               characters, including at lesst 3 from
                               the set of uppercase, lowercase,
                               numerals, and punctuation.

                This setting must be pushed down to the mobile device
                by syncing with an Exchange server before it can be
                enforced. (WM5AKU2+)

        Note that this configuration setting merely enforces policy -
        it does not actually change local device policy.
      -->
    <DeviceLockRequired
        MaximumTimeoutMinutes="60"
        MinimumPasswordLength="4"
        PasswordComplexity="pin"/>
    </MobilePolicy>
</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>REPLACE_AsaName</HostName>
            <HostAddress>REPLACE_asa.address.com</HostAddress>
        </HostEntry>
        <HostEntry>
            <HostName>REPLACE_AsaName2</HostName>
            <HostAddress>REPLACE_10.94.146.172</HostAddress>
            <!--
                If present, UserGroup will be used in conjunction with
                HostAddress to form a Group based URL.
                NOTE: Group based URL support requires ASA version 8.0.3 or
                      later.
              -->
            <UserGroup>REPLACE_TunnelGroup</UserGroup>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
© 2009 Cisco Systems, Inc. - Internal Use Only
```

Sample AnyConnect Profile Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<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="UserGroup" minOccurs="0">
```

```
                            <xs:annotation>
                                <xs:documentation>The tunnel group to use when connecting to
the specified host.  This field is used in conjunction with the HostAddress value to form
a Group based URL.  NOTE: Group based URL support requires ASA version 8.0.3 or
later.</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:all>
                        <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"
type="ns1:UserControllableValues" default="true">
                                            <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:attribute>
                                    </xs:extension>
                                </xs:simpleContent>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="ShowPreConnectMessage" default="false"
minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>
```

```
                  This control enables an administrator to have a one time message
displayed prior to a users first connection attempt.  As an example, the message could be
used to remind a user to insert their smart card into it’s reader.

                 The message to be used with this control is localizable and can be found
in the AnyConnect message catalog (default: "This is a pre-connect reminder message.").
                </xs:documentation>
                          </xs:annotation>
                          <xs:simpleType>
                              <xs:restriction base="xs:string">
                                  <xs:enumeration value="true">
                                      <xs:annotation>
                                          <xs:documentation>Show a pre-connect message
prior to users first connect attempt.</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="false">
                                      <xs:annotation>
                                          <xs:documentation>Do not show a pre-connect
message prior to users first connect attempt.</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                              </xs:restriction>
                          </xs:simpleType>
                      </xs:element>
                      <xs:element name="CertificateStore" default="All" minOccurs="0">
                          <xs:annotation>
                              <xs:documentation>
                  This setting allows an administrator to specify which certificate store
AnyConnect will use for locating certificates.

                 This setting only applies to the Microsoft Windows version of AnyConnect
and has no effect on other platforms.
                </xs:documentation>
                          </xs:annotation>
                          <xs:simpleType>
                              <xs:restriction base="xs:string">
                                  <xs:enumeration value="All">
                                      <xs:annotation>
                                          <xs:documentation>Use certificates from all
available certificate stores.</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="Machine">
                                      <xs:annotation>
                                          <xs:documentation>Use certificates only from the
Windows machine certificate store.</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                                  <xs:enumeration value="User">
                                      <xs:annotation>
                                          <xs:documentation>Use certificates only from the
Windows user certificate store.</xs:documentation>
                                      </xs:annotation>
                                  </xs:enumeration>
                              </xs:restriction>
                          </xs:simpleType>
                      </xs:element>
                      <xs:element name="CertificateStoreOverride" type="ns1:simpleBinary"
default="false" minOccurs="0">
                          <xs:annotation>
```

```
                              <xs:documentation>This setting allows an administrator to
direct AnyConnect to search for certificates in the Windows machine certificate store.
This is useful in cases where certificates are located in this store and users do not have
administrator privileges on their machine.</xs:documentation>
                          </xs:annotation>
                      </xs:element>
                      <xs:element name="AutoConnectOnStart" default="true" minOccurs="0">
                          <xs:annotation>
                              <xs:documentation>Controls AnyConnect client behavior when
started.  By default, the client will attempt to contact the last Gateway a user connected
to or the first one in the list from the AnyConnect profile.  In the case of
certificate-only authentication, this will result in the establishment of a VPN tunnel
when the client is started.</xs:documentation>
                          </xs:annotation>
                          <xs:complexType>
                              <xs:simpleContent>
                                  <xs:extension base="ns1:simpleBinary">
                                      <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" default="true">
                                          <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:attribute>
                                  </xs:extension>
                              </xs:simpleContent>
                          </xs:complexType>
                      </xs:element>
                      <xs:element name="MinimizeOnConnect" default="true" minOccurs="0">
                          <xs:annotation>
                              <xs:documentation>Controls AnyConnect GUI behavior when a
VPN tunnel is established.  By default, the GUI will minimize when the VPN tunnel is
established.</xs:documentation>
                          </xs:annotation>
                          <xs:complexType>
                              <xs:simpleContent>
                                  <xs:extension base="ns1:simpleBinary">
                                      <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" default="true">
                                          <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:attribute>
                                  </xs:extension>
                              </xs:simpleContent>
                          </xs:complexType>
                      </xs:element>
                      <xs:element name="LocalLanAccess" default="false" minOccurs="0">
                          <xs:annotation>
                              <xs:documentation>If Local LAN access is enabled for remote
clients on the Secure Gateway, this setting can be used to allow the user to accept or
reject this access.</xs:documentation>
                          </xs:annotation>
                          <xs:complexType>
                              <xs:simpleContent>
                                  <xs:extension base="ns1:simpleBinary">
                                      <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" default="true">
                                          <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:attribute>
                                    </xs:extension>
                                </xs:simpleContent>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="AutoReconnect" default="true" minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>This setting allows an administrator to
control how a client will behave when the VPN tunnel is interrupted.  Control can
optionally be given to the user.</xs:documentation>
                            </xs:annotation>
                            <xs:complexType mixed="true">
                                <xs:sequence>
                                    <xs:element name="AutoReconnectBehavior"
default="DisconnectOnSuspend" minOccurs="0">
                                        <xs:complexType>
                                            <xs:simpleContent>
                                                <xs:extension base="ns1:AutoConnectValues">
                                                    <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" 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:attribute>
                                                </xs:extension>
                                            </xs:simpleContent>
                                        </xs:complexType>
                                    </xs:element>
                                </xs:sequence>
                                <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" 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:attribute>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="AutoUpdate" default="true" minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>This setting allows the adminstrator to
turn off the dynamic update functionality of AnyConnect.  Control of this can also be
given to the user.</xs:documentation>
                            </xs:annotation>
                            <xs:complexType>
                                <xs:simpleContent>
                                    <xs:extension base="ns1:simpleBinary">
                                        <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" 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:attribute>
                                    </xs:extension>
                                </xs:simpleContent>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="RSASecurIDIntegration" default="Automatic" 
minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>This setting allows the adminstrator to 
control how the user will interact with RSA.  By default, AnyConnect will determine the 
correct method of RSA interaction.  The desired setting can be locked down by the 
administrator or control can be given to the user.</xs:documentation>
                            </xs:annotation>
                            <xs:complexType>
                                <xs:simpleContent>
                                    <xs:extension base="ns1:RSAIntegrationValues">
                                        <xs:attribute name="UserControllable" 
type="ns1:UserControllableValues" 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:attribute>
                                    </xs:extension>
                                </xs:simpleContent>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="WindowsLogonEnforcement" 
default="SingleLocalLogon" minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>This preference allows an administrator to 
control if more than one user may be logged into the client PC during the VPN connection 
(Windows only).</xs:documentation>
                            </xs:annotation>
                            <xs:complexType>
                                <xs:simpleContent>
                                    <xs:extension base="ns1:WindowsLogonEnforcementValues"/>
                                </xs:simpleContent>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="WindowsVPNEstablishment" default="LocalUsersOnly" 
minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>This preference allows an administrator to 
control whether or not remote users may initiate a VPN connection (Windows 
only).</xs:documentation>
                            </xs:annotation>
                            <xs:complexType>
                                <xs:simpleContent>
                                    <xs:extension base="ns1:WindowsVPNEstablishmentValues"/>
                                </xs:simpleContent>
                            </xs:complexType>
                        </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:element name="MobilePolicy" minOccurs="0">
                          <xs:annotation>
                              <xs:documentation>Collection of policy settings specific to
the Windows Mobile version of AnyConnect that have no effect on other
platforms.</xs:documentation>
                          </xs:annotation>
                          <xs:complexType>
                              <xs:sequence>
                                  <xs:element name="DeviceLockRequired" minOccurs="0">
                                      <xs:annotation>
                                          <xs:documentation>Indicates that a Windows
Mobile device must be configured with a password or PIN prior to establishing a VPN
connection.  This configuration is only valid on Windows Mobile devices that use the
Microsoft Default Local ation Provider (LAP).</xs:documentation>
                                      </xs:annotation>
                                      <xs:complexType>
                                          <xs:attribute name="MaximumTimeoutMinutes"
type="xs:unsignedInt">
                                              <xs:annotation>
                                                  <xs:documentation>When set to
non-negative number, specifies the maximum number of minutes that must be configured
before device lock takes effect.  (WM5/WM5AKU2+)  </xs:documentation>
                                              </xs:annotation>
                                          </xs:attribute>
                                          <xs:attribute name="MinimumPasswordLength"
type="xs:unsignedInt">
                                              <xs:annotation>
                                                  <xs:documentation>When set to a
non-negative number,  specifies that any PIN/password used for device lock must be equal
to or longer than the specified value, in characters. (WM5AKU2+)</xs:documentation>
                                              </xs:annotation>
                                          </xs:attribute>
                                          <xs:attribute name="PasswordComplexity">
                                              <xs:annotation>
```

```
                                                    <xs:documentation>When present checks for 
the following password subtypes:  "alpha"  - Requires an alphanumeic password,  "pin"    - 
Numeric PIN required, "strong" - Strong alphanumeric password defined by Microsoft as 
containing at least 7 characters, including a minimum of 3 from the set of uppercase, 
lowercase,  numerals, and punctuation characters. (WM5AKU2+)</xs:documentation>
                                                </xs:annotation>
                                                <xs:simpleType>
                                                    <xs:restriction base="xs:string">
                                                        <xs:enumeration value="alpha"/>
                                                        <xs:enumeration value="pin"/>
                                                        <xs:enumeration value="strong"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:attribute>
                                        </xs:complexType>
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                    </xs:all>
                </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="DC">
                                        <xs:annotation>
                                            <xs:documentation>Domain 
Component</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-DC">
                                      <xs:annotation>
                                          <xs:documentation>Issuer Domain
Component</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:attribute name="MatchCase" default="Enabled">
                        <xs:annotation>
                            <xs:documentation>Should the pattern matching applied to
"Pattern" be case sensitive?  Default is "Enabled" (case sensitive).</xs:documentation>
                        </xs:annotation>
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:enumeration value="Enabled">
                                    <xs:annotation>
                                        <xs:documentation>perform case sensitive match with
pattern</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="Disabled">
                                    <xs:annotation>
                                        <xs:documentation>perform case in-sensitive match
with pattern</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>
           </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="false">
                <xs:annotation>
                    <xs:documentation>
           </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="AutoConnectValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="DisconnectOnSuspend"/>
            <xs:enumeration value="ReconnectAfterResume"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="RSAIntegrationValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Automatic"/>
            <xs:enumeration value="SoftwareToken"/>
            <xs:enumeration value="HardwareToken"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="UserControllableValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="true">
                <xs:annotation>
                    <xs:documentation source="user is allowed to control this setting."/>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="false">
                <xs:annotation>
                    <xs:documentation source="user is not allowed to control this 
setting."/>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="WindowsLogonEnforcementValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="SingleLogon">
                <xs:annotation>
                    <xs:documentation>Allows only one user during a VPN 
connection</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="SingleLocalLogon">
                <xs:annotation>
                    <xs:documentation>Allows only one local user but many remote users
during a VPN connection</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="WindowsVPNEstablishmentValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="LocalUsersOnly">
                <xs:annotation>
                    <xs:documentation>Only local users may establish a VPN
connection</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="AllowRemoteUsers">
                <xs:annotation>
                    <xs:documentation>Local and remote users may establish a VPN
connection</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:element name="element1">
        <xs:complexType>
            <xs:sequence/>
        </xs:complexType>
    </xs:element>
</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 (IE), page 2-18. 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