



Cisco AnyConnect VPN Client Administrator Guide

Release 2.4

Updated: May 10, 2010

Americas Headquarters

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

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

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.



CONTENTS

About this Guide ix

Audience ix

Conventions ix

Related Documents x

Obtaining Documentation and Submitting a Service Request x

CHAPTER 1

Introduction to AnyConnect 1-1

Remote User Interface 1-1

AnyConnect License Options 1-6

AnyConnect Standalone and WebLaunch Options 1-6

AnyConnect Files and Components 1-7

Installing Start Before Logon Components (Windows Only) 1-7

AnyConnect Files Installed on the VPN Client Computer 1-9

Configuration and Deployment Overview 1-9

AnyConnect API 1-10

CHAPTER 2

Configuring the Security Appliance to Deploy the AnyConnect Client 2-1

How the Security Appliance Deploys the AnyConnect Client 2-1

Before You Install the AnyConnect Client 2-2

Ensuring Automatic Installation of AnyConnect Clients 2-2

Adding a Security Appliance to the List of Trusted Sites (IE) 2-3

Adding a Security Certificate in Response to Browser Alert Windows 2-4

Ensuring Fast Connection Time when Loading Multiple AnyConnect Client Images 2-5

Configuring the Security Appliance to Download the AnyConnect Client 2-5

Prompting Remote Users for AnyConnect Client Download 2-9

Enabling Modules for Additional AnyConnect Features 2-10

Configuring Certificate-only Authentication 2-11

CHAPTER 3

Configuring AnyConnect Client Features 3-1

Configuring and Deploying the AnyConnect Client Profile 3-2

Default Client Profile 3-3

Editing the Client Profile 3-4

Validating the XML in the Profile 3-5

Deploying the Client Profile to AnyConnect Clients	3-6
Configuring the AnyConnect Local Policy	3-8
AnyConnect Local Policy File Example	3-9
Changing Parameters for Windows Clients using our MST File	3-9
Changing Parameters Manually in the AnyConnect Local Policy File	3-10
Configuring Start Before Logon	3-10
Installing Start Before Logon Components (Windows Only)	3-12
Differences Between Windows-Vista and Pre-Vista Start Before Logon	3-12
Profile Parameters for Enabling SBL	3-12
Making SBL User-Controllable	3-13
Enabling SBL on the Security Appliance	3-13
Using the Manifest File	3-14
Troubleshooting SBL	3-15
Configuring Start Before Logon (PLAP) on Windows 7 and Vista Systems	3-15
Start Before Logon Differences in Windows OSs	3-16
Installing PLAP	3-16
Logging on to a Windows Vista or Windows 7 PC using PLAP	3-17
Disconnecting from the AnyConnect Client Using PLAP	3-19
Enabling FIPS and Additional Security	3-20
AnyConnect Local Policy File Parameters and Values	3-20
AnyConnect Local Policy File Example	3-23
Enabling FIPS with our MST File	3-23
Changing any Local Policy Parameter with your own MST File	3-23
Changing Parameters for all Operating Systems using our Enable FIPS Tool	3-24
Changing Parameters Manually in the AnyConnect Local Policy File	3-25
Enabling Trusted Network Detection	3-25
Users with Multiple Profiles Connecting to Multiple Security Appliances	3-27
Configuring a Certificate Store	3-27
Controlling the Certificate Store on Windows	3-28
Examples of <CertificateStore> and <CertificateStoreOverride> Usage	3-29
Creating a PEM Certificate Store for Mac and Linux	3-29
Restrictions for PEM File Filenames	3-30
Storing User Certificates	3-30
Restricting Certificate Store Use	3-31
Configuring Simplified Certificate Enrollment Protocol	3-31
Provisioning and Renewing Certificates Automatically or Manually	3-32
Automatic Certificate Requests	3-32
Manual Certificate Retrieval	3-32
Windows Certificate Warning	3-33

Configuring SCEP Protocol to Provision and Renew Certificates	3-33
Certificate Storage after SCEP Request	3-38
Configuring the ASA to Support SCEP Protocol for AnyConnect	3-38
Configuring Certificate Only Authentication on the ASA	3-38
Configuring Certificate Matching	3-38
Certificate Key Usage Matching	3-39
Extended Certificate Key Usage Matching	3-39
Certificate Distinguished Name Mapping	3-40
Certificate Matching Example	3-41
Prompting Users to Select Authentication Certificate	3-45
Configuring the Client Profile with AutomaticCertSelection	3-45
Users Configuring Automatic Certificate Selection in AnyConnect Preferences	3-46
Configuring Backup Server List Parameters	3-47
Installing AnyConnect on a Windows Mobile Device	3-47
Configuring a Windows Mobile Policy	3-48
Installing AnyConnect on 64-bit Linux	3-51
Using the Manual Install Option on Mac OS if the Java Installer Fails	3-51
Configuring Auto Connect On Start	3-52
Configuring Auto Reconnect	3-53
Installing Host Scan	3-54
Configuring a Server List	3-54
Split DNS Fallback	3-57
Scripting	3-57
Scripting Requirements and Limitations	3-58
Writing, Testing, and Deploying Scripts	3-58
Configuring the AnyConnect Profile for Scripting	3-59
Troubleshooting Scripts	3-61
Proxy Support	3-61
Ignore Proxy	3-61
Private Proxy	3-62
Private Proxy Requirements	3-62
Configuring a Group Policy to Download a Private Proxy	3-62
Internet Explorer Connections Tab Lockdown	3-62
Proxy Auto-Configuration File Generation for Clientless Support	3-62
Allow AnyConnect Session from an RDP Session for Windows Users	3-63
AnyConnect over L2TP or PPTP	3-64
Configuring AnyConnect over L2TP or PPTP	3-65
Instructing Users to Override PPP Exclusion	3-66

Configuring Other AnyConnect Profile Settings 3-67

CHAPTER 4

Fulfilling Other Administrative Requirements for AnyConnect 4-1

Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users 4-1

Configuring CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop 4-2

CHAPTER 5

Managing Authentication 5-1

SDI Token (SoftID) Integration 5-1

Comparing Native SDI with RADIUS SDI 5-1

Using SDI Authentication 5-2

Categories of SDI Authentication Exchanges 5-4

Normal SDI Authentication Login 5-4

New User, Clear PIN, and New PIN Modes 5-4

Getting a New PIN 5-5

“Next Passcode” and “Next Token Code” Challenges 5-6

Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client 5-6

AnyConnect Client and RADIUS/SDI Server Interaction 5-6

Configuring the Security Appliance to Support RADIUS/SDI Messages 5-7

CHAPTER 6

Customizing and Localizing the AnyConnect Client and Installer 6-1

Customizing the AnyConnect Client 6-1

Replacing Individual GUI Components with your Custom Components 6-2

Deploying Executables That Use the Client API 6-3

Customizing the GUI with a Transform 6-5

Sample Transform 6-7

Information for Creating your Custom Icons and Logos 6-8

Changing the Default AnyConnect English Messages 6-12

Localizing the AnyConnect Client GUI and Installer 6-14

Localizing the AnyConnect GUI 6-14

Translating using the ASDM Translation Table Editor 6-15

Translating by Exporting the Translation Table for Editing 6-19

Localizing the AnyConnect Installer Screens 6-22

Using Tools to Create Message Catalogs for Enterprise Deployment 6-25

Merging a Newer Translation Template with your Translation Table 6-25

CHAPTER 7

Communicating User Guidelines 7-1

Using the AnyConnect CLI Commands to Connect (Standalone Mode) 7-1

Logging Out	7-3
Setting the Secure Connection (Lock) Icon	7-3

CHAPTER 8
Managing, Monitoring, and Troubleshooting AnyConnect Sessions 8-1

Disconnecting All VPN Sessions	8-1
Disconnecting Individual VPN Sessions	8-1
Viewing Detailed Statistical Information	8-2
Viewing Statistics on a Windows Mobile Device	8-3
Resolving VPN Connection Issues	8-4
Adjusting the MTU Size	8-4
Eliminating Compression to Improve VPN Performance and Accommodate Windows Mobile Connections	8-5
Using DART to Gather Troubleshooting Information	8-5
Getting the DART Software	8-6
Installing DART	8-6
Installing DART with AnyConnect	8-6
Manually Installing DART on the Host	8-7
Running DART on a Windows PC	8-7

APPENDIX A
Open Software License Notices A-1

OpenSSL/Open SSL Project	A-1
License Issues	A-1



About this Guide

This guide describes how to install the Cisco AnyConnect VPN Client image onto the central-site security appliance, configure the client for deployment to remote user computers, configure connection profiles and group policies on ASDM for AnyConnect, install the client onto mobile devices, and monitor and troubleshoot AnyConnect VPN connections.

Throughout this guide, the term “security appliance” applies to all models in the Cisco ASA 5500 series (ASA 5505 and higher).

Audience

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

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

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{ x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	Nonprinting characters such as passwords are in angle brackets.

[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Note**

Means *reader take note*.

**Tip**

Means *the following information will help you solve a problem*.

**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Related Documents

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>.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.



CHAPTER 1

Introduction to AnyConnect

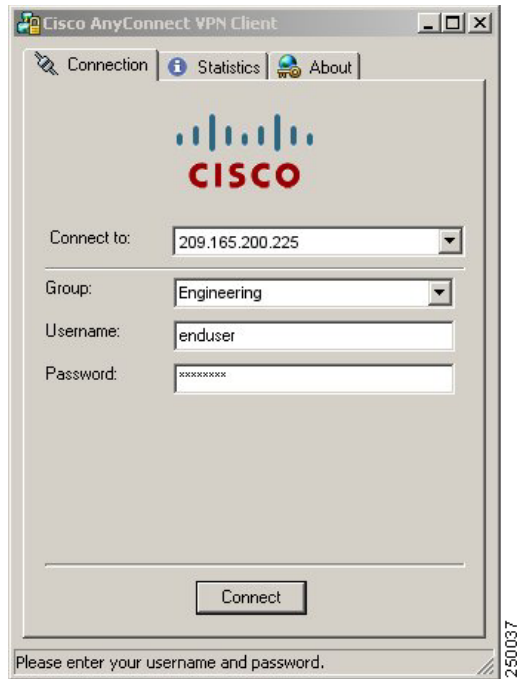
The Cisco AnyConnect VPN Client is the next-generation VPN client, providing remote users with secure VPN connections to the Cisco 5500 Series Adaptive Security Appliance running ASA version 8.0 and higher or ASDM 6.0 and higher.

This chapter includes the following sections:

- [Remote User Interface, page 1-1](#)
- [AnyConnect License Options, page 1-6](#)
- [AnyConnect Standalone and WebLaunch Options, page 1-6](#)
- [AnyConnect Files and Components, page 1-7](#)
- [Configuration and Deployment Overview, page 1-9](#)
- [AnyConnect API, page 1-10](#)

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

If you do not have certificates set up, you might see the dialog box shown in [Figure 1-2](#).

Figure 1-2 Security Alert Dialog Box**Note**

This dialog box opens only if the correct certificate is not deployed. You can click Yes to bypass the certificate requirement.

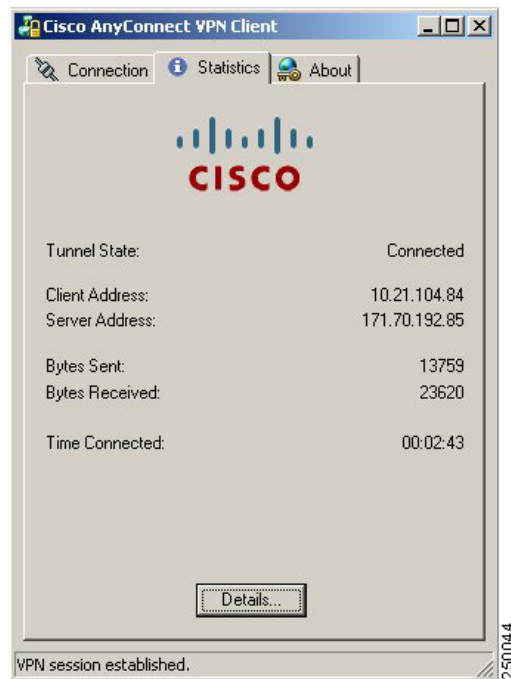
The Security Alert dialog box appears only on the first connection attempt to a given security appliance. After the connection is successfully established, the “thumbprint” of the server certificate is saved in the preferences file, so the user is not prompted on subsequent connections to the same security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

[Table 1-1](#) shows the circumstances and results when the Security Alert dialog box appears.

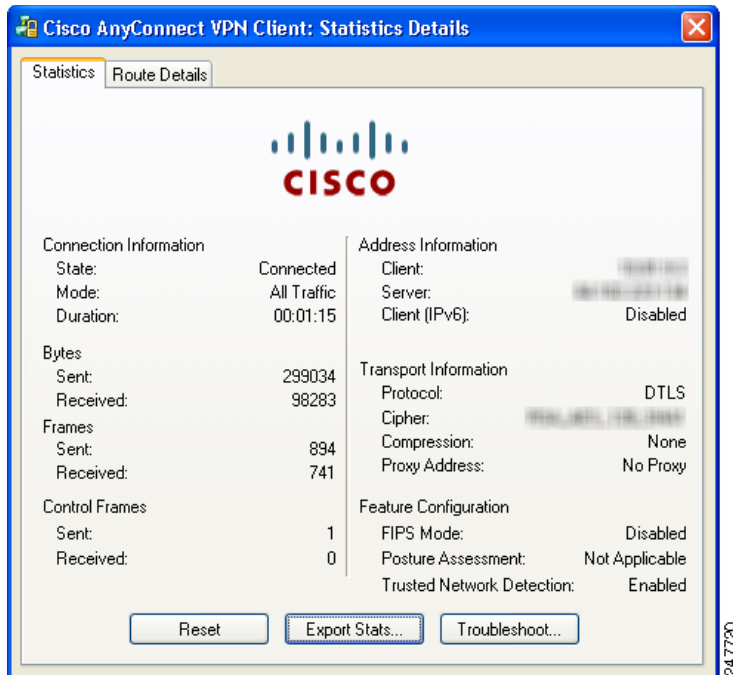
Table 1-1 Certificate, Security Alert, and Connection Status

Certificate Status	Does Security Alert Appear?	Client Connection Status
Server certificate sent to the client from the security appliance is independently verifiable <i>and</i> the certificate has no serious errors.	No	Success
Server certificate sent to the client from the security appliance is <i>not</i> independently verifiable <i>and</i> the certificate contains serious errors.	No	Failure
Server certificate sent to the client from the security appliance is <i>not</i> independently verifiable <i>and</i> the certificate does <i>not</i> 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.

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

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

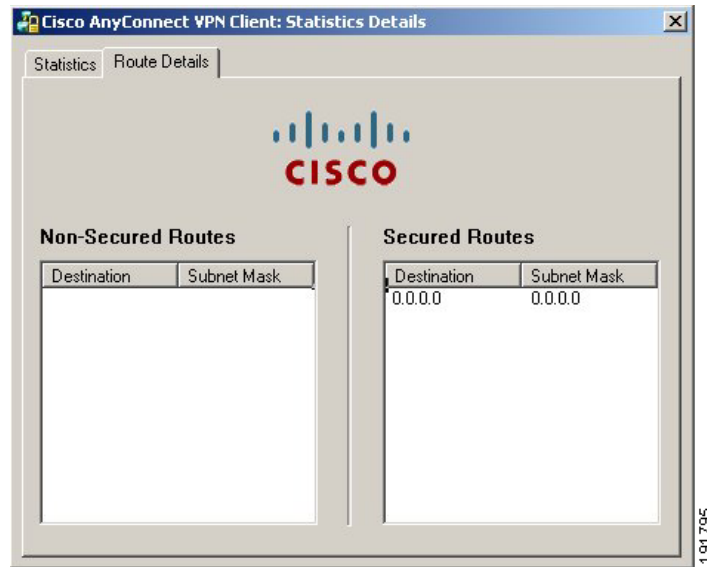
Clicking the Details button opens the Statistics Details window (Figure 1-4).

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

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:

- Clicking **Reset** resets the connection information to zero. AnyConnect immediately begins collecting new data.
- Clicking **Export Stats...** saves the connection statistics to a text file for later analysis and debugging.
- Clicking **Troubleshoot...** Launches the DART (Diagnostic AnyConnect Reporting Tool) wizard which bundles specified log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connection. See [Using DART to Gather Troubleshooting Information, page 8-5](#) for information about the DART package.

The Route Details tab ([Figure 1-5](#)) shows the secured and non-secured routes for this connection.

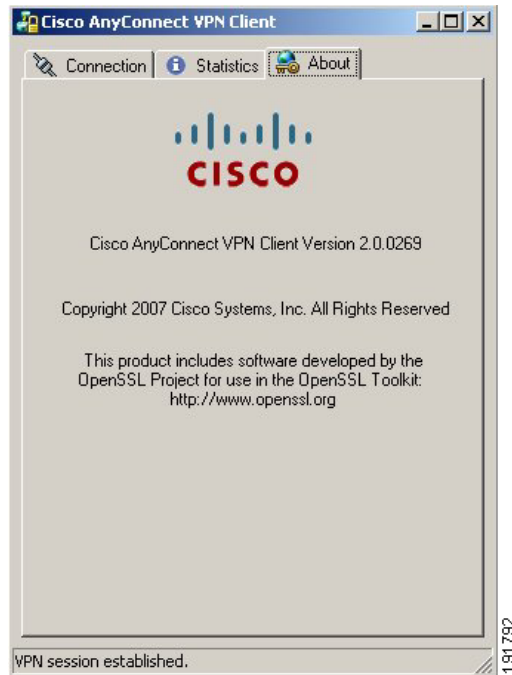
Figure 1-5 Cisco AnyConnect VPN Client User Interface, Statistics Tab, Route Details Tab**Note**

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.

See [Viewing Detailed Statistical Information, page 8-2](#) for information about using the Export and View Log buttons for connection monitoring.

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



AnyConnect License Options

The following options support full AnyConnect client functionality while specifying the number of SSL VPN sessions supported:

- Cisco AnyConnect Essentials license
- Cisco AnyConnect Premium Clientless SSL VPN Edition license
- Cisco AnyConnect Premium Clientless SSL VPN Edition shared license
- Cisco FLEX license

The first three licenses are mutually exclusive per device (that is, per security appliance), but you can configure a mixed network.

AnyConnect Standalone and WebLaunch Options

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 how 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.

Whether connecting via standalone mode or WebLaunch mode, the AnyConnect client package must be installed on the security appliance in order for the client to connect. This ensures that the security appliance is the single point of enforcement as to which versions of the client can establish a session, even if you deploy the client with an enterprise software deployment system. When you load a client package on the security appliance, you enforce a policy that only versions as new as the one loaded can connect. AnyConnect users must upgrade their clients by loading the latest version of the client with the latest security features on the security appliance.

AnyConnect Files and Components

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 computer. 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 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.

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

Installing Start Before Logon Components (Windows Only)

Table 1-2 Files Available for Download on the Cisco AnyConnect VPN Client Download Software Site

AnyConnectProfileEditor.zip	Zip file containing AnyConnect Profile Editor.
anyconnect-all-packages-AnyConnectRelease_Number-k9.zip	Zip file containing all client install packages for this release version. Does not include API.
anyconnect-dart-win-AnyConnectRelease_Number-k9.msi	Standalone MSI package with DART for Windows platforms.
anyconnect-gina-win-AnyConnectRelease_Number-pre-deploy-k9-lang.zip	Language localization transform files for Windows Start Before Login.
anyconnect-gina-win-AnyConnectRelease_Number-pre-deploy-k9.msi	Start Before Login GINA module for Windows 2k/XP/Vista.
anyconnect-gina-win-AnyConnectRelease_Number-web-deploy-k9-lang.zip	Language localization transform files for web-deploy for Windows Start Before
anyconnect-linux-AnyConnectRelease_Number-k9.pkg	Web deployment package for Linux platforms.

Table 1-2 Files Available for Download on the Cisco AnyConnect VPN Client Download Software Site (continued)

AnyConnectProfileEditor.zip	Zip file containing AnyConnect Profile Editor.
anyconnect-linux-AnyConnectRelease_Number-k9.tar.gz	Standalone tarball package for Linux platforms.
anyconnect-macosx-i386-AnyConnectRelease_Number-k9.dmg	Standalone DMG package for Mac OS X Intel platforms.
anyconnect-macosx-i386-AnyConnectRelease_Number-k9.pkg	Web deployment package for Mac OS X Intel platforms.
anyconnect-macosx-powerpc-AnyConnectRelease_Number-k9.dmg	Standalone DMG package for Mac OS X PowerPC platforms.
anyconnect-macosx-powerpc-AnyConnectRelease_Number-k9.pkg	Web deployment package for Mac OS X PowerPC platforms.
anyconnect-no-dart-win-AnyConnectRelease_Number-k9.pkg	Web deployment package without DART for Windows platforms.
anyconnect-win-AnyConnectRelease_Number-k9.pkg	Web deployment package for Windows platforms.
anyconnect-win-AnyConnectRelease_Number-pre-deploy-k9-lang.zip	Language localization transform files for pre-deploy package for Windows platforms.
anyconnect-win-AnyConnectRelease_Number-pre-deploy-k9.msi	Standalone MSI package for Windows platforms.
anyconnect-win-AnyConnectRelease_Number-web-deploy-k9-lang.zip	Language localization transform files for web-deploy package for Windows platforms.
anyconnect-wince-ARMv4I-AnyConnectRelease_Number-k9.cab	Standalone CAB package (signed) for Windows Mobile platforms.
anyconnect-wince-ARMv4I-AnyConnectRelease_Number-k9.pkg	Web deployment package for Windows Mobile platforms.
anyconnect-wince-ARMv4I-activesync-AnyConnectRelease_Number-k9.msi	ActiveSync MSI package for Windows Mobile platforms.

If you configure a security appliance for WebLaunch of AnyConnect, AnyConnect orders the component sequence automatically. Otherwise, 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.), you must specify the components in the correct sequence.

AnyConnect Files Installed on the VPN Client Computer

AnyConnect Client downloads the following files on the local computer:

Table 1-3 *AnyConnect Files on the Endpoint*

File	Description
<i>anyfilename.xml</i>	AnyConnect Client profile. This file specifies the features and attribute values configured for a particular user type.
AnyConnectProfile.tmpl	Example AnyConnect Client Profile provided with the AnyConnect Client software.
AnyConnectProfile.xsd	Defines the XML schema format. AnyConnect uses this file to validate the profile.

AnyConnect downloads these three files to the same directory, as follows:

Table 1-4 *Paths to the Profile Files on the Endpoint*

OS	Directory Path
Windows 7 and Vista	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile\
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\
Mac OS X and Linux	/opt/cisco/vpn/profile/

Configuration and Deployment Overview

Use the AnyConnect Profile editor to configure the client features in the preferences file; then configure the security appliance to upload this file along with the client automatically when users use a web browser to connect to the VPN. The preference file drives the display in the user interface and defines the names and addresses of host computers. By creating and assigning different preferences files to group profiles configured on the security appliance, you can differentiate access to these features. Following assignment to the respective group profiles, the security appliance automatically pushes the one assigned to the user's group profile upon 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.

Alternatively, you can install or let users install the preferences file and client as an application on computers for later access. This alternative method is the only method supported for Windows Mobile devices.

AnyConnect API

Use the Application Programming Interface (API) if you 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 the client on Windows, Linux and Mac OS X. The API package includes project files (Makefiles) for the Windows platform. For other platforms, a platform-specific script shows how to compile the example code. You can link your application (GUI, CLI, or embedded application) with these files and libraries.



CHAPTER 2

Configuring the Security Appliance to Deploy the AnyConnect Client

This chapter describes how to use ASDM to configure the security appliance to deploy the AnyConnect client. To use CLI to configure the security appliance, see the *Cisco 5500 Series Adaptive Security Appliance CLI Configuration Guide*.

This chapter includes the following sections:

- [How the Security Appliance Deploys the AnyConnect Client, page 2-1](#)
- [Before You Install the AnyConnect Client, page 2-2](#)
- [Configuring the Security Appliance to Download the AnyConnect Client, page 2-5](#)
- [Prompting Remote Users for AnyConnect Client Download, page 2-9](#)
- [Enabling Modules for Additional AnyConnect Features, page 2-10](#)
- [Configuring Certificate-only Authentication, page 2-11](#)

How the Security Appliance Deploys the AnyConnect Client

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

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

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

When the client negotiates an SSL VPN connection with the security appliance, it attempts to connect using Datagram Transport Layer Security (DTLS). 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 it cannot establish a DTLS connection, it falls back to Transport Layer Security (TLS).

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

Before You Install the AnyConnect Client

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

- [Ensuring Automatic Installation of AnyConnect Clients, page 2-2](#)
- [Adding a Security Appliance to the List of Trusted Sites \(IE\), page 2-3](#)
- [Adding a Security Certificate in Response to Browser Alert Windows, page 2-4](#)

Ensuring Automatic Installation of AnyConnect Clients

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

- To minimize user prompts during AnyConnect client setup, make sure certificate data on client PCs and on the security appliance match:
 - If you are using a Certificate Authority (CA) for certificates on the security appliance, choose one that is already configured as a trusted CA on client machines.
 - If you are using a self-signed certificate on the security appliance, be sure to install it as a trusted root certificate on clients.

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

- Make sure the Common Name (CN) in security appliance certificates matches the name clients use to connect to it. By default, the security appliance certificate CN field is its IP address. If clients use a DNS name, change the CN field on the security appliance certificate to that name.

If the certificate has a SAN (Subject Alternate Name) then the browser will ignore the CN value in the Subject field and look for a DNS Name entry in the SAN field.

If users connect to the ASA using its hostname, the SAN should contain the hostname and domain name of the ASA. For example, the SAN field would contain

`DNS Name=hostname.domain.com.`

If users connect to the ASA using its IP address, the SAN should contain the IP address of the ASA. For example, the SAN field would contain `DNS Name=209.165.200.254.`

- The Cisco Security Agent (CSA) might display warnings during the AnyConnect client installation.

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

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

Priority Allow, no Log, Description: “Cisco Secure Tunneling Browsers, read/write vpnweb.ocx”

Applications in the following class: "Cisco Secure Tunneling Client - Controlled Web Browsers"
 Attempt: Read file, Write File

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

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

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

We recommend that Microsoft Internet Explorer (MSIE) users add the security appliance to the list of trusted sites, or install Java. The latter enables the ActiveX control to install with minimal interaction from the user. This is particularly important for users of Windows XP SP2 with enhanced security. Windows Vista users *must* add the security appliance to the list of trusted sites in order to use the dynamic deployment feature. For more information, see [Adding a Security Appliance to the List of Trusted Sites \(IE\)](#), page 2-3 .

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.
 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.
-

Ensuring Fast Connection Time when Loading Multiple AnyConnect Client Images

When you load multiple AnyConnect client images on the security appliance, you should order the images in a manner that ensures the fastest connection times for greatest number of remote users.

The security appliance downloads portions of the client images to the remote computer until it achieves a match with the operating system. It downloads the image at the top of the ordered list first. Therefore, you should assign the image that matches the most commonly-encountered operating system used on remote computers to the top of the list.

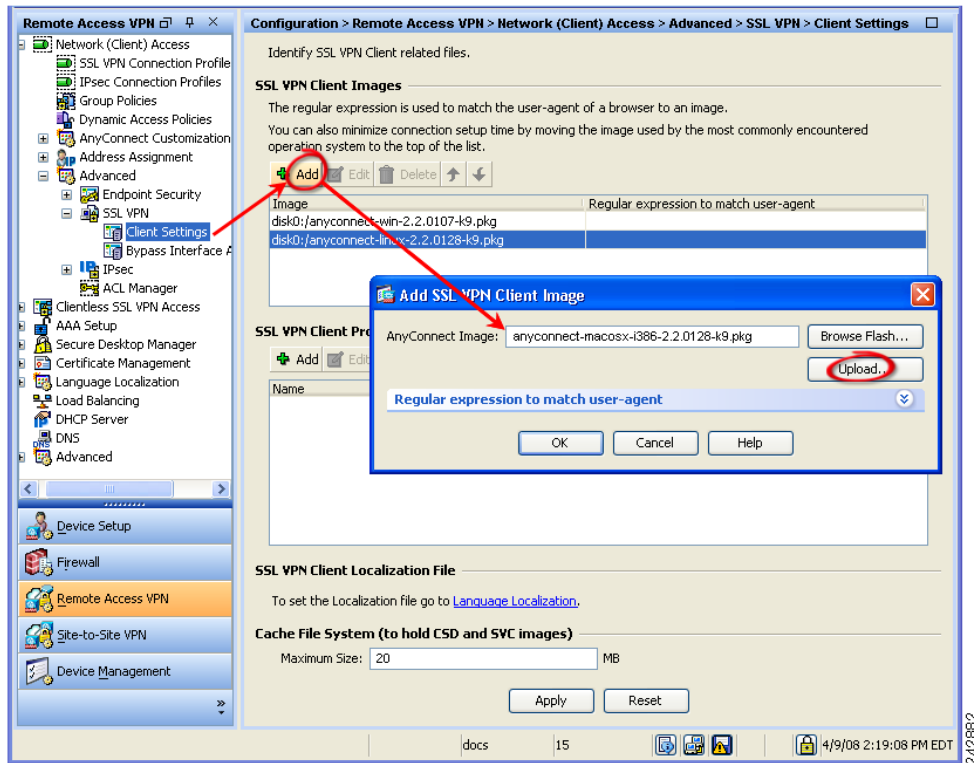
Because mobile users have slower connection speeds, you should load the AnyConnect client image for Windows Mobile at the top of the list.

For mobile users, you can decrease the connection time of the mobile device by using the regex keyword. When the browser connects to the adaptive security appliance, it includes the User-Agent string in the HTTP header. When the adaptive 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.

Configuring the Security Appliance to Download the AnyConnect Client

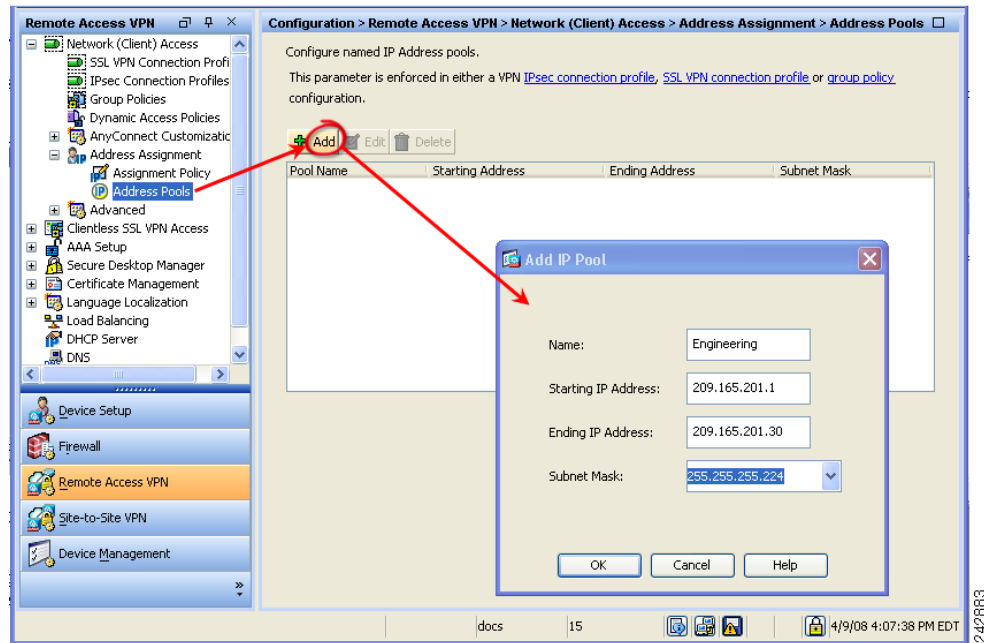
To prepare the security appliance to deploy the AnyConnect client, complete these steps:

-
- Step 1** Download the latest Cisco AnyConnect Secure Mobility client package from the [Cisco AnyConnect Software Download](#) webpage.
- Step 2** Specify the AnyConnect client package file as an SSL VPN client.
- Navigate to **Configuration > Remote Access VPN > Network Access > Advanced > SSL VPN > Client Settings**. The SSL VPN Client Settings panel displays. (Figure 2-1).
- This panel lists AnyConnect client files that have been identified as client images. The order in which they appear in the table reflects the order the security appliance downloads them to the remote computer.
- To add a client image, click **Add** in the SSL VPN Client Images area. Enter the name of the file you downloaded from Cisco.com and click **Upload**. You can also browse your computer for the file.

Figure 2-1 Specify AnyConnect Client Images**Step 3** Configure a method of address assignment.

You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a tunnel group. This guide uses the popular address pools method as an example.

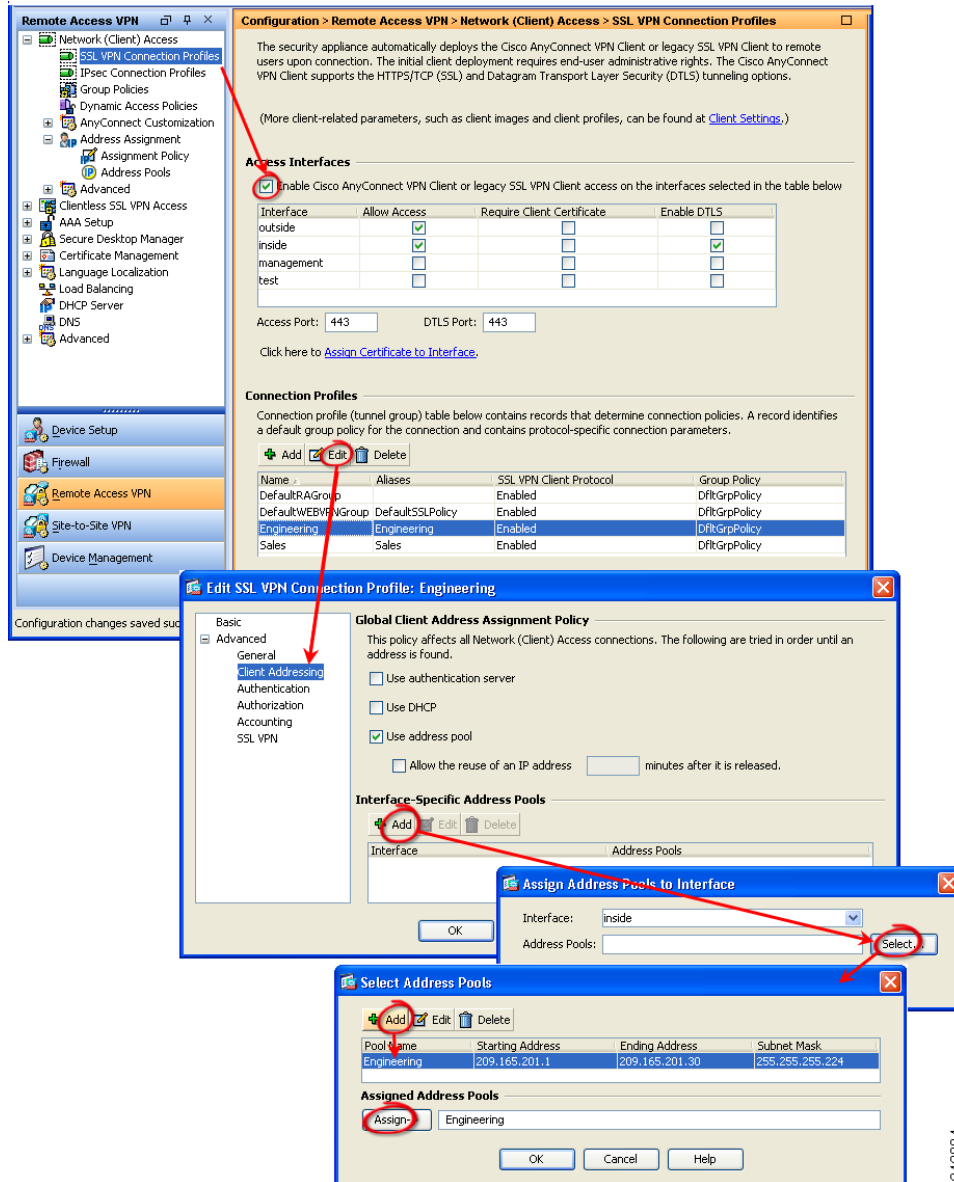
Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools** (Figure 2-2). Enter address pool information in the Add IP Pool window.

Figure 2-2 Add IP Pool Dialog

Step 4 Enable client download and assign the address pool in a connection profile.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. Follow the arrows in (Figure 2-3) to enable the AnyConnect client and then assign an address pool.

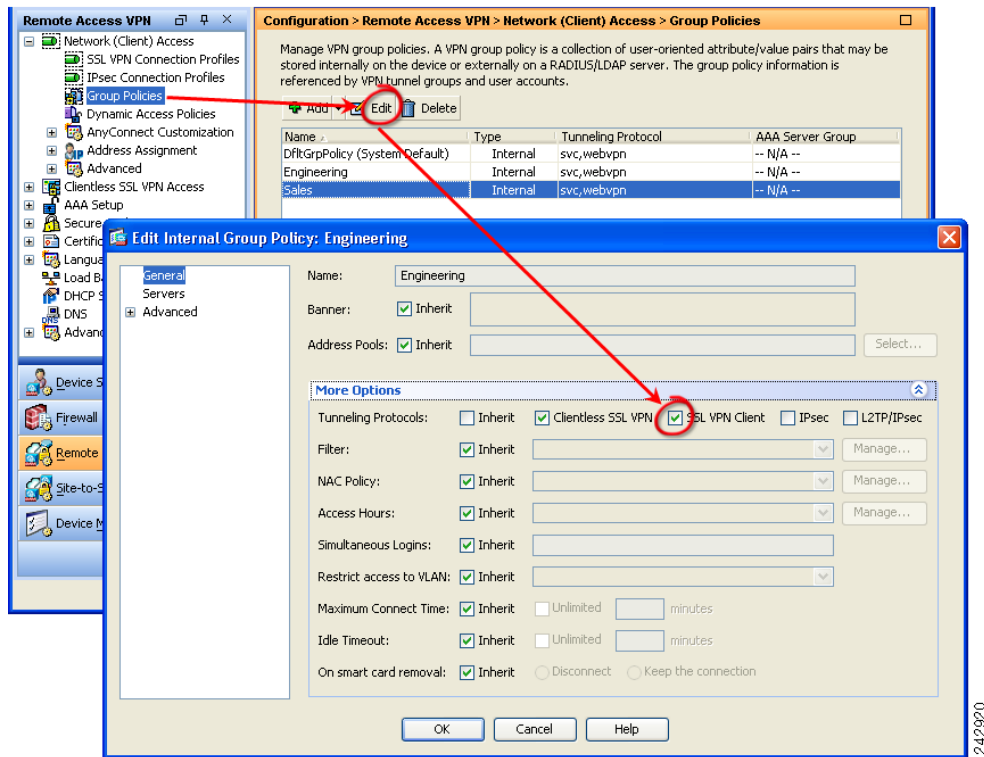
Figure 2-3 Enable SSL VPN Client Download



Step 5 Specify SSL VPN as a permitted VPN tunneling protocol for a group policy.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. The Group Policies panel displays. Follow the arrows in Figure 2-4 to enable SSL VPN for the group.

242884

Figure 2-4 Specify SSL VPN as a Tunneling Protocol

242920

Prompting Remote Users for AnyConnect Client Download

By default, the security appliance does not download the AnyConnect client when the remote user initially connects using the browser. After users authenticate, the default clientless portal page displays a Start AnyConnect Client drawer that users can select to download the client. Alternatively, you can configure the security appliance to immediately download the client without displaying the clientless portal page.

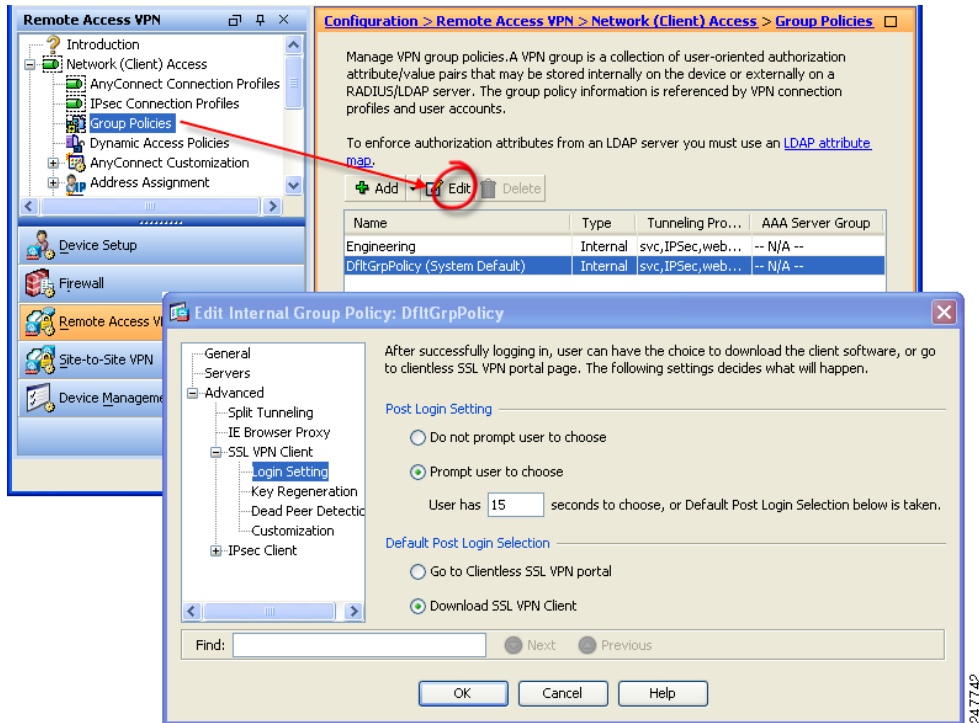
You can also configure the security appliance to prompt remote users, providing a configured time period within which they can choose to download the client or go to the clientless portal page.

You can configure this feature for a group policy or user. To change these login settings, follow this procedure:

- Step 1** Go to Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Select a group policy and click **Edit**. The Edit Internal Group Policy window displays (Figure 2-5).
- Step 2** In the navigation pane, Select Advanced > SSL VPN Client > Login Settings. The Post Login settings display. Deselect the Inherit check box, if necessary, and select a Post Login setting.

If you choose to prompt users, specify a timeout period and select a default action to take when that period expires in the Default Post Login Selection area.

Figure 2-5 Changing Login Settings



Step 3 Click **OK** and be sure to apply your changes to the group policy.

Figure 2-6 shows the prompt displayed to remote users if you choose **Prompt user to choose** and **Download SSL VPN Client**:

Figure 2-6 Post Login Prompt Displayed to Remote Users



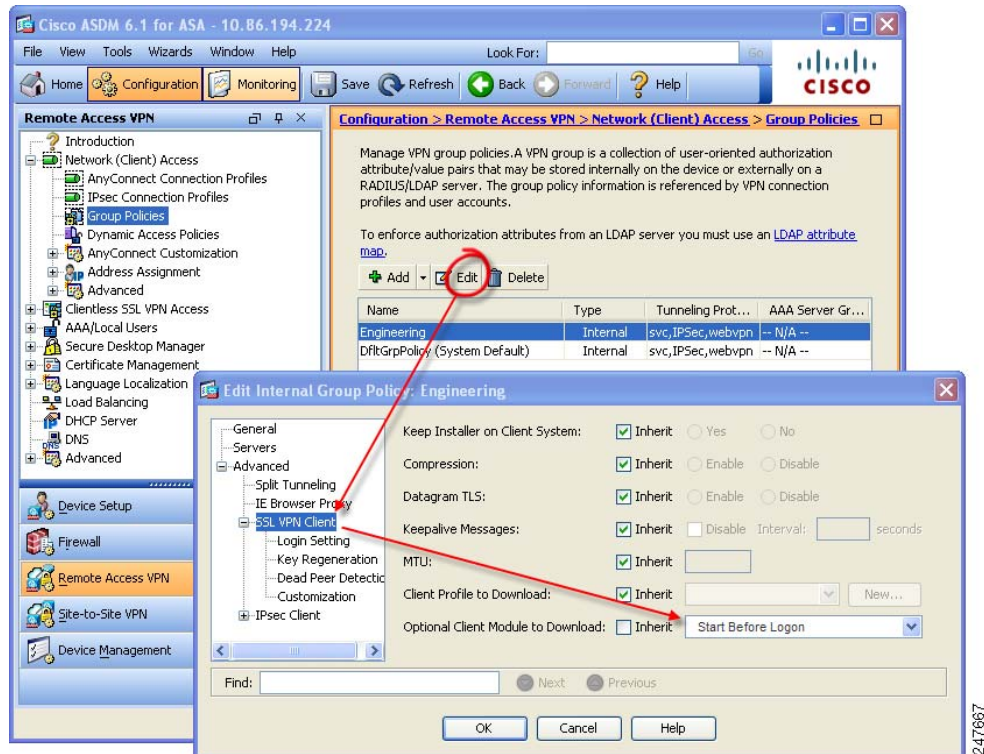
Enabling Modules for Additional AnyConnect Features

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. To enable module download for a group policy, follow this procedure:

- Step 1** Go to Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Select a group policy and click **Edit**. The Edit Internal Group Policy window displays (Figure 2-7).
- Step 2** In the navigation pane, select Advanced > SSL VPN Client. Click the Optional Client Module to Download drop-list and select a module.

Figure 2-7 Specifying an Optional Client Module to Download



- Step 3** Click **OK** and be sure to apply your changes to the group policy.

If you choose Start Before Logon, you must also enable this client feature in the AnyConnect client profile. See [Configuring AnyConnect Client Features](#) for details.

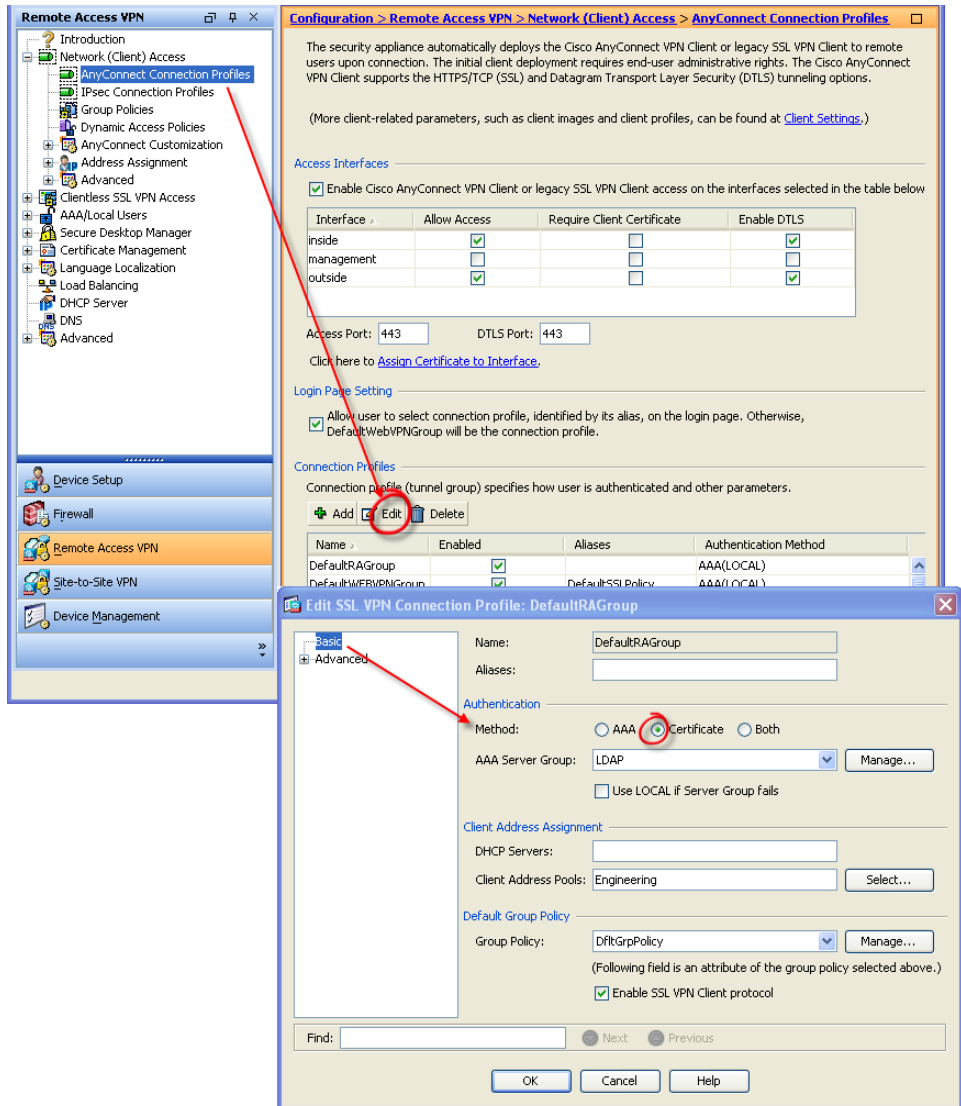
Configuring Certificate-only Authentication

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.

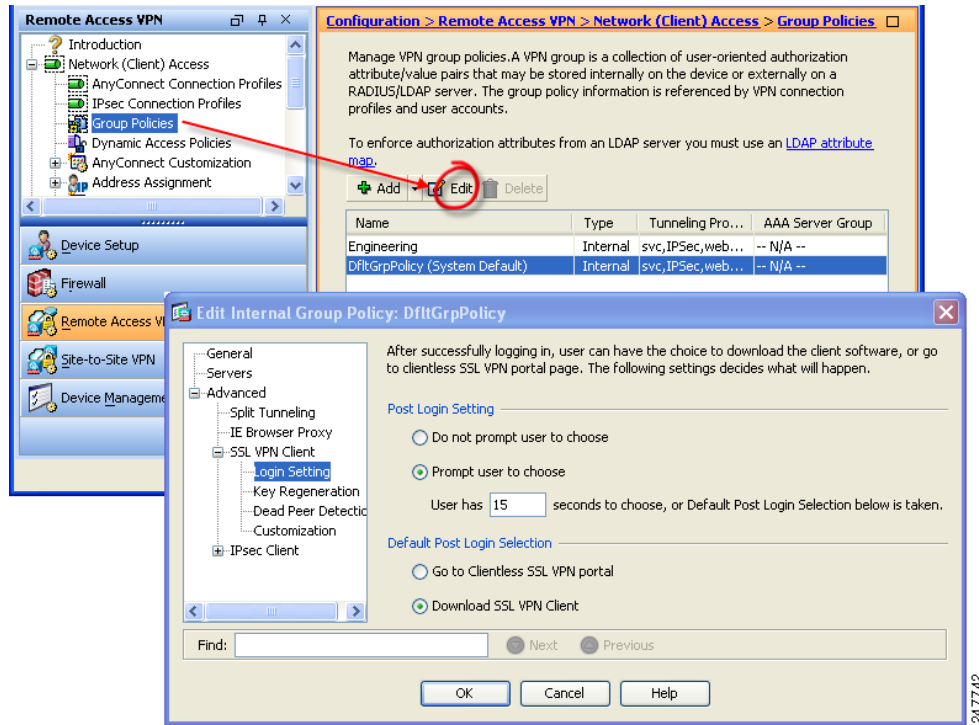
You can configure certificate-only authentication in connection profiles. To enable this setting, follow this procedure:

- Step 1** Go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. Select a connection profile and click **Edit**. The Edit SSL VPN Connection Profile window displays (Figure 2-8).

Figure 2-8 Configuring Certificate-Only Authentication

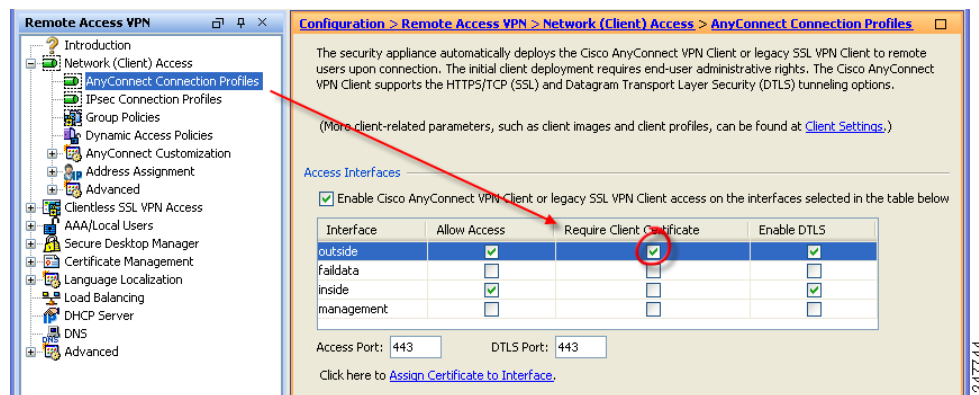


- Step 2** In the Authentication area, enable the method Certificate.
- Step 3** (Optional) You can assign a specific certificate to an interface. Click Require Client Certificate (Figure 2-9).

Figure 2-9 Requiring a Certificate on an Interface

Step 4 (Optional) You can 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.

To do this, go to Configuration > Remote Access VPN > Advanced > SSL Settings. In the Certificates area, select an interface and click **Edit**. The Select SSL Certificate window displays (Figure 2-10). Select a certificate from the drop-list. Click **OK** and apply your changes.

Figure 2-10 Specifying a Certificate for an Interface**Note**

To configure in which certificate store the AnyConnect client searches for the authentication certificate, see [Configuring a Certificate Store](#), page 3-27. You will also find information on configuring certificate restrictions for Linux and Mac OS X operating systems.



CHAPTER 3

Configuring AnyConnect Client Features

The AnyConnect client includes two files that enable and configure client features—the AnyConnect client profile and the AnyConnect local policy. This chapter describes the AnyConnect client features and how to enable them in the profile, the local policy, and on the security appliance.

AnyConnect Client Profile

The AnyConnect profile is an XML file deployed by the security appliance during client installation and updates. This file provides basic information about connection setup, as well as advanced features such as Start Before Logon (SBL). Users cannot manage or modify profiles.

You can configure the security appliance to deploy profiles globally for all AnyConnect client users, or based on the group policy of the 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. Be aware 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.

AnyConnect Local Policy

The AnyConnect local policy specifies additional security parameters for the AnyConnect VPN client, including operating in a mode compliant with Level 1 of the Federal Information Processing Standard (FIPS). Other parameters in the AnyConnect Local Policy increase security by forbidding remote updates to prevent Man-in-the-Middle attacks and by preventing non-administrator or non-root users from modifying client settings. Unlike the client profile, the local policy is not deployed by the security appliance and must be deployed by an enterprise software deployment system.

The first two sections of this chapter describe how to make changes to the AnyConnect client profile or local policy:

- [Configuring and Deploying the AnyConnect Client Profile, page 3-2](#)
- [Configuring the AnyConnect Local Policy, page 3-8](#)

The following sections describe each client feature and the necessary changes to the AnyConnect client profile, local policy, and/or the security appliance software:

- [Configuring Start Before Logon, page 3-10](#)
- [Enabling FIPS and Additional Security, page 3-20](#)
- [Enabling Trusted Network Detection, page 3-25](#)
- [Configuring a Certificate Store, page 3-27](#)
- [Configuring Simplified Certificate Enrollment Protocol, page 3-31](#)

- [Configuring Certificate Matching, page 3-38](#)
- [Prompting Users to Select Authentication Certificate, page 3-45](#)
- [Configuring Backup Server List Parameters, page 3-47](#)
- [Configuring a Windows Mobile Policy, page 3-48](#)
- [Configuring a Server List, page 3-54](#)
- [Split DNS Fallback, page 3-57](#)
- [Scripting, page 3-57](#)
- [Proxy Support, page 3-62](#)
- [Allow AnyConnect Session from an RDP Session for Windows Users, page 3-63](#)
- [AnyConnect over L2TP or PPTP, page 3-64](#)

Configuring and Deploying the AnyConnect Client Profile

An AnyConnect client profile is an XML file cached to the endpoint file system. The client parameters, represented as XML tags in this file, name the security appliances with which to establish VPN sessions and enable client features.

You can create and save XML profiles using a text editor. The client installation contains one profile template (AnyConnectProfile.tpl) 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. The AnyConnectProfile.tpl file automatically downloaded with the AnyConnect client is an example AnyConnect profile.



Note

In order for the client initialization parameters in a profile to be applied to the client configuration, the security appliance the user connects to must appear as a host entry in that profile. If you do not add the security appliance address or FQDN as a host entry in the profile, then filters do not apply for the session. For example, if you create a certificate match and the certificate properly matches the criteria, but you do not add the security appliance as a host entry in that profile, the certificate match is ignored. For more information about adding host entries to the profile, see [Configuring a Server List, page 3-54](#).

This section covers the following topics:

- [Default Client Profile, page 3-3](#)
- [Editing the Client Profile, page 3-4](#)
- [Validating the XML in the Profile, page 3-5](#)
- [Deploying the Client Profile to AnyConnect Clients, page 3-6](#)

Default Client Profile

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

The following example shows a sample AnyConnect Profile file. The bold type identifies the values you can modify to customize the profile. 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>
    <RSA SecurID Integration UserControllable="false">Automatic</RSA SecurID Integration>

  <CertificateMatch>
    <KeyUsage>
      <MatchKey>Digital_Signature</MatchKey>
    </KeyUsage>
    <ExtendedKeyUsage>
      <ExtendedMatchKey>ClientAuth</ExtendedMatchKey>
    </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>CVC-ASA-01.example.com</HostAddress>
    <UserGroup>StandardUser</UserGroup>
    <BackupServerList>
      <HostAddress>cvc-asa-02.example.com</HostAddress>
      <HostAddress>cvc-asa-03.example.com</HostAddress>
    </BackupServerList>
  </HostEntry>
</ServerList>

</AnyConnectProfile>

```

Editing the Client Profile

Retrieve a copy of the profile file (AnyConnectProfile.xml) from a client installation. Make a copy and rename the copy with a name meaningful to you. Alternatively, you can modify an existing profile. See [Table 1-4, “Paths to the Profile Files on the Endpoint”](#) to identify the profile path for each supported operating system.

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>
  <HostEntry>
    <HostName></HostName>
    <HostAddress></HostAddress>
  </HostEntry>
  <HostEntry>
    <HostName></HostName>
    <HostAddress></HostAddress>
  </HostEntry>
</Configuration>

```

HostName identifies the secure gateway or cluster to the user. It appears on the “Connect to” drop-down list on the Connection tab of the user GUI. It can be any name you want to use. *HostAddress* specifies the actual hostname and domain (e.g., hostname.example.com) of the secure gateway to be reached. (While this value may instead specify an IP address, we do not recommend it.) The value of *HostName* can match the hostname portion of the *HostAddress* value, but matching the name is not a requirement because the parent tag *HostEntry* associates these values. Matching the hostname in both child tags does, however, simplify the association for administrators testing and troubleshooting VPN connectivity.

```
<HostEntry>
  <HostName>Sales_gateway</HostName>
  <HostAddress>Sales_gateway.example.com</HostAddress>
</HostEntry>
```

**Note**

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

Validating the XML in the Profile

It is important to validate the XML in the AnyConnect client 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 client profile, and 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 is available only with certain Cisco Secure Gateway products.

In Microsoft Windows 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 7 and Vista. It is available for download from Microsoft for Windows XP from the following link:

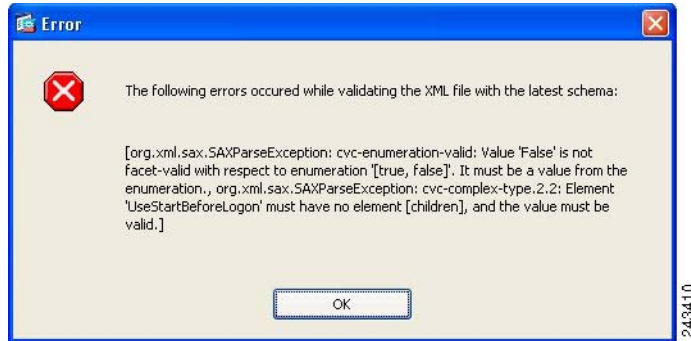
<http://www.microsoft.com/downloads/details.aspx?FamilyID=d21c292c-368b-4ce1-9dab-3e9827b70604&displaylang=en>

When modifying a profile, be sure to check your typing and make sure the capitalization matches the capitalization in the XML tag 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:

Figure 3-1 XML Validation Error



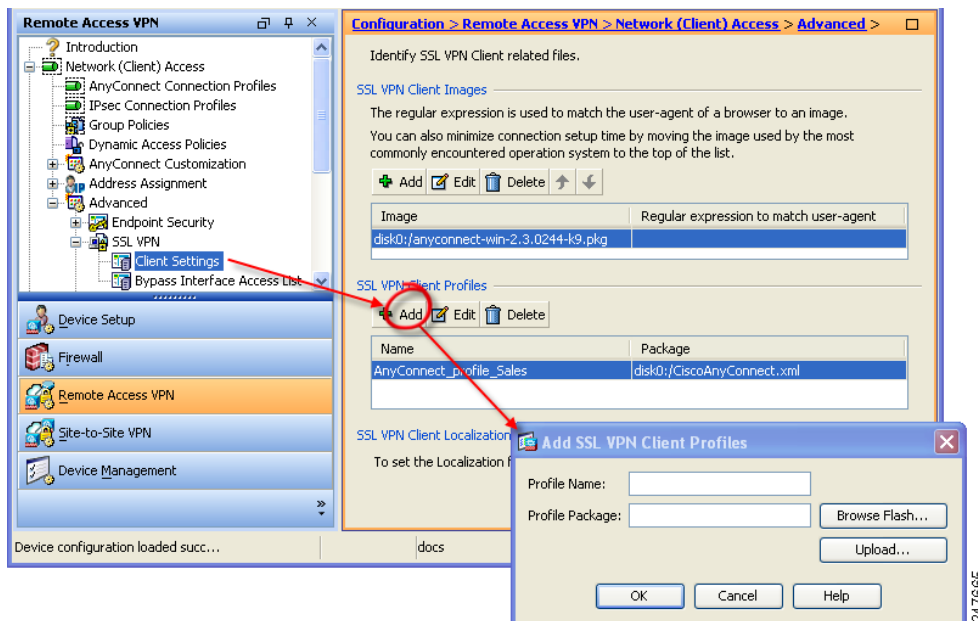
In this example, the value **False** (initial letter capitalized) should have been **false** (all lowercase), and the error indicates this.

Deploying the Client Profile to AnyConnect Clients

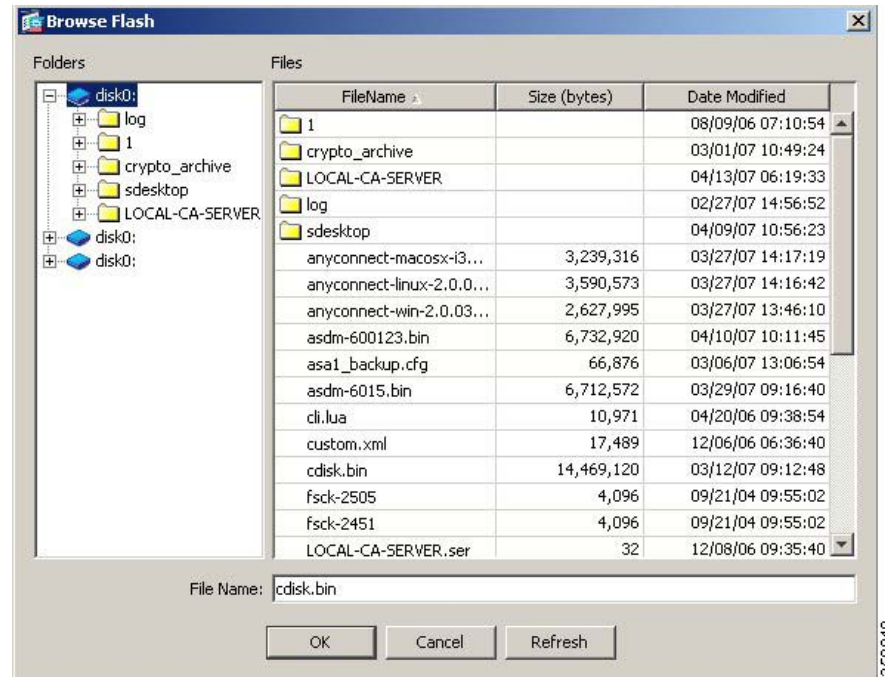
Follow these steps to configure the security appliance to deploy a profile with the AnyConnect client:

- Step 1** Identify to the security appliance the client profiles file to load into cache memory. Go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > Client Settings (Figure 3-2).
- Step 2** In the SSL VPN Client Profiles area, click **Add**. The Add SSL VPN Client Profiles dialog box appears.

Figure 3-2 Adding or Editing an AnyConnect VPN Client Profile



- Step 3** 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 3-3).

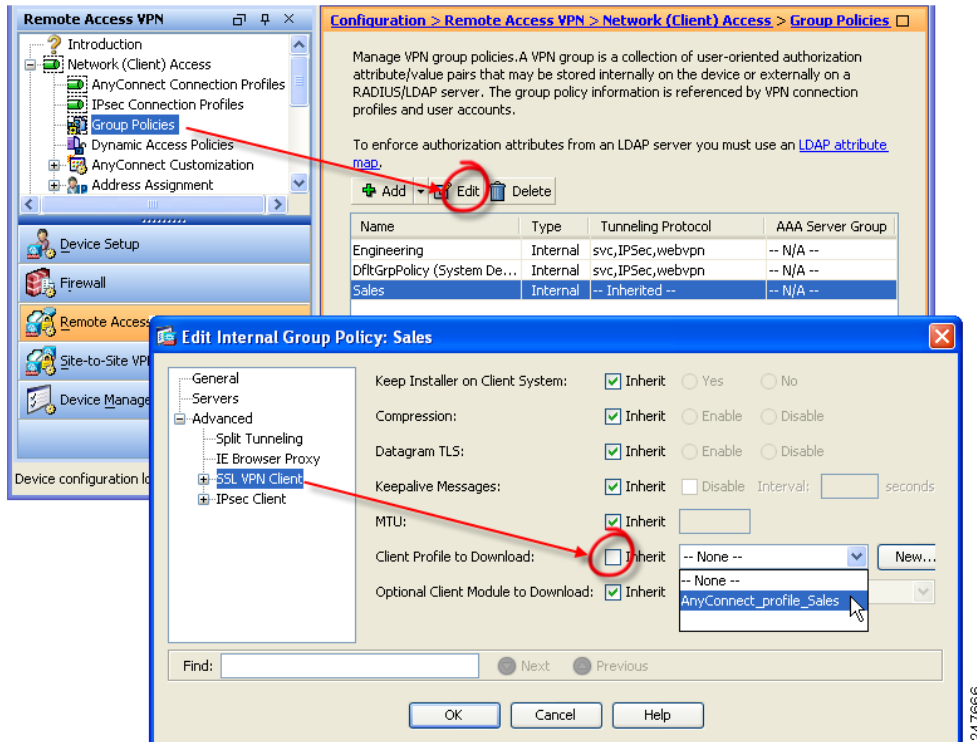
Figure 3-3 Browse Flash Dialog Box

Step 4 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 5** To specify a profile for a group policy, go to Configuration > Remote Access VPN > Network (Client) Access > Group Policies. (Figure 3-4)

Figure 3-4 Specify the Profile to use in the Group Policy



- Step 6** Deselect Inherit and select a Client Profile to Download from the drop-down list.
- Step 7** When you have finished with the configuration, click OK.

Configuring the AnyConnect Local Policy

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

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

AnyConnect Local Policy parameters reside in an XML file called *AnyConnectLocalPolicy.xml*. This file is not deployed by the ASA 5500 Series security appliance. You must deploy this file using corporate software deployment systems or change the file manually on a user computer.

This section covers the following topics:

- AnyConnect Local Policy File Example, page 3-9

- [Changing Parameters for Windows Clients using our MST File, page 3-9](#)
- [Changing Parameters Manually in the AnyConnect Local Policy File, page 3-10](#)

AnyConnect Local Policy File Example

The following is an example of the AnyConnect Local Policy file:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
  xmlns=http://schemas.xmlsoap.org/encoding/
  xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
  xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
  <FipsMode>>false</FipsMode>
  <BypassDownloader>>false</BypassDownloader>
  <RestrictWebLaunch>>false</RestrictWebLaunch>
  <StrictCertificateTrust>>false</StrictCertificateTrust>
  <RestrictPreferenceCaching>>false</RestrictPreferenceCaching>
  <RestrictTunnelProtocols>>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

Changing Parameters for Windows Clients using our MST File

For Windows installations, you can apply the MST file we provide to the standard MSI installation file to change AnyConnect Local Policy parameters, including enabling FIPS mode. The installation generates an AnyConnect Local Policy file with FIPS enabled.

For information about where you can download our MST, see the licensing information you received for the FIPS client.

The MST file contains the following custom rows. The names correspond to the parameters in AnyConnect Local Policy file (AnyConnectLocalPolicy.xml). See [Table 3-3](#) for the descriptions and values you can set for these parameters:

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

Changing Parameters Manually in the AnyConnect Local Policy File

To change AnyConnect Local Policy parameters manually, follow this procedure:

- Step 1** Retrieve a copy of the AnyConnect Local Policy file (AnyConnectLocalPolicy.xml) from a client installation.

Table 3-1 shows the installation path for each operating system.

Table 3-1 Operating System and AnyConnect Local Policy File Installation Path

Operating System	Installation Path
Windows 7	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client
Windows Vista	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client
Windows Mobile	%PROGRAMFILES%\Cisco AnyConnect VPN Client
Linux	/opt/cisco/vpn
Mac OS X	/opt/cisco/vpn

- Step 2** Edit the parameter settings. The example below shows the contents of the AnyConnect Local Policy file for Windows:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
  xmlns=http://schemas.xmlsoap.org/encoding/
  xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
  xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
  <FipsMode>false</FipsMode>
  <BypassDownloader>false</BypassDownloader>
  <RestrictWebLaunch>false</RestrictWebLaunch>
  <StrictCertificateTrust>false</StrictCertificateTrust>
  <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
  <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

- Step 3** Save the file as *AnyConnectLocalPolicy.xml* and deploy the file to remote computers using corporate an IT software deployment system.

Configuring Start Before Logon

Start Before Logon (SBL) forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting the AnyConnect client before the Windows login dialog box appears. After authenticating to the security appliance, the Windows login dialog appears, and the user logs in as usual. SBL is only available for Windows and lets you control the use of login scripts, password caching, mapping network drives to local drives, and more.



Note The AnyConnect client does not support SBL for Windows XP x64 (64-bit) Edition.

To enable the SBL feature, you must make changes to the AnyConnect client profile and enable the security appliance to download a client module for SBL.

Reasons you might consider for enabling SBL for your users include:

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

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 Microsoft Active Directory. As soon as the user logs on, the login script executes.

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 to not allow cached credentials to be used to log on to the computer. In this scenario, 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 computer.

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.

AnyConnect is not compatible with fast user switching.

This section covers the following topics:

- [Installing Start Before Logon Components \(Windows Only\), page 3-12](#)
- [Configuring Start Before Logon \(PLAP\) on Windows 7 and Vista Systems, page 3-15](#)

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.

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

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

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



Note

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

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

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

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 7 and Vista Systems, page 3-15](#).

Profile Parameters 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.

The following table shows the settings.

Table 3-2 UseStartBeforeLogon Client Initialization Tag

Default Value ¹	Possible Values ²	User Controllable	User Controllable by Default ³	OSs Supported
true	true, false	Yes	true	Windows 7, Vista, and XP

1. AnyConnect uses the default value if the profile does not specify one.

2. Insert the parameter value between the beginning and closing tags; for example, `<UseStartBeforeLogon>true</UseStartBeforeLogon>`.
3. The user controllable attribute is defined inside the preference tags; for example, `<UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>`. 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.

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.

Enabling SBL on the Security Appliance

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 SBL, you must specify the SBL module name in group policy on the security appliance.

In addition, you must ensure that the `UseStartBeforeLogon` parameter, within the profile file you specified for the group policy, is set to *true*. For example:

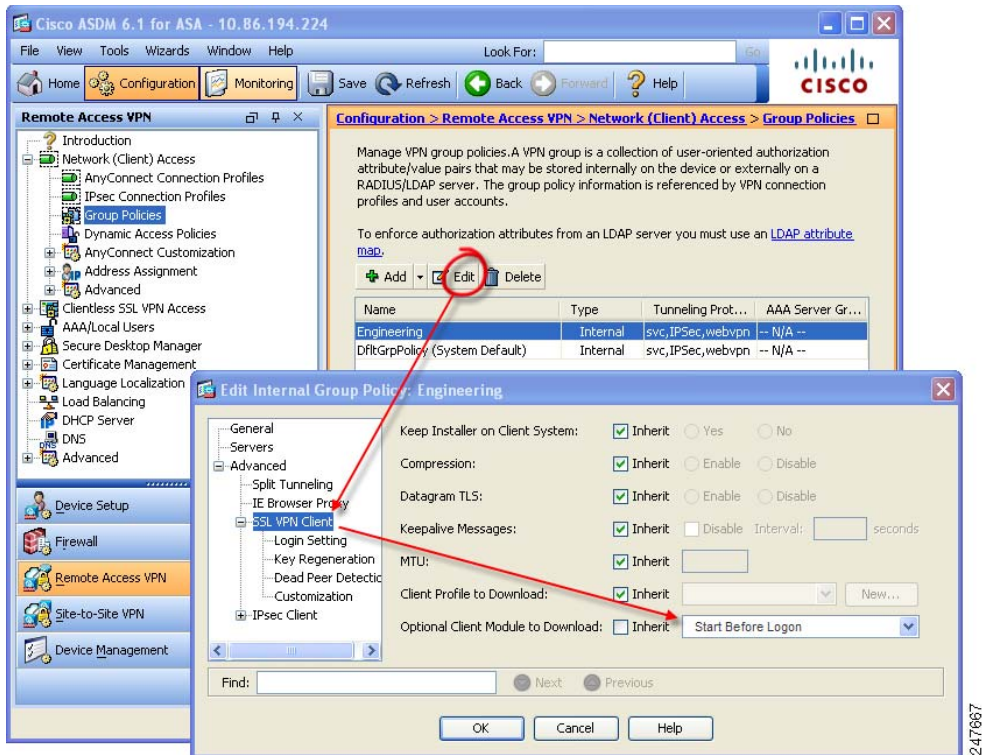
```
<UseStartBeforeLogon UserControllable="false">true</UseStartBeforeLogon>
```



Note The user must reboot the remote computer before SBL takes effect.

To specify the SBL module on the security appliance, follow this procedure:

- Step 1** Go to Configuration > Remote Access VPN > Network (Client) Access > Group Policies ([Figure 3-5](#)).
- Step 2** Select a group policy and click Edit. The Edit Internal Group Policy window displays.
- Step 3** Select Advanced > SSL VPN Client in the left-hand navigation pane. SSL VPN settings display.
- Step 4** Uncheck the Inherit box for the Optional Client Module for Download setting.
- Step 5** Select the Start Before Logon module in the drop-list.

Figure 3-5 Specifying the SBL Module to Download

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 previously-installed 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 computer 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 installation of

VPNGINA is activated if the group-policy of the user specifies SBL as an optional module to download. If it is, 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 client installs, a sample profile is provided on the client computer at this location:

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

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. Reboot the computer and retest. |
| 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 | Reboot once. On the next reboot, you should be prompted with the Start Before Logon prompt. |
| Step 7 | Send the AnyConnect event log to Cisco in .evt format |
| Step 8 | If you see the following error, delete the user profile:

Description: Unable to parse the profile C:\Documents and Settings\All
Users\Application Data\Cisco\AnyConnect VPN Client\Profile\VABaseProfile.xml.
Host data not available. |
| Step 9 | 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 7 and Vista Systems

As on the other Windows platforms, the Start Before Logon (SBL) feature initiates a VPN connection before the user logs in to Windows. This ensures users connect to their corporate infrastructure before logging on to their computers. Microsoft Windows 7 and Vista use different mechanisms than Windows XP, so the AnyConnect client SBL feature on the Windows 7 and Vista uses a different mechanism well.

In the AnyConnect client, the new SBL feature is known as the Pre-Login Access Provider (PLAP), which is a connectable credential provider. This feature lets programmatic network administrators perform specific tasks, such as collecting credentials or connecting to network resources, prior to login. PLAP provides SBL functions on Windows 7 and Vista. PLAP supports 32-bit and 64-bit versions of the operating system with vpnplap.dll and vpnplap64.dll, respectively. The PLAP function supports x86 and x64.



Note

In this section, VPNGINA refers to the Start Before Logon feature for Windows XP, and PLAP refers to the Start Before Logon feature for Windows 7 and Vista.

Start Before Logon Differences in Windows OSs

On Windows XP, 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 Windows XP, 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 you 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, 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 remote user.

Once installed, PLAP is not active until you modify the user profile <profile.xml> file to activate start before logon. See [Profile Parameters for Enabling SBL, page 3-12](#). 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, the user can restore it by pressing the Alt+Tab key combination.

Logging on to a Windows Vista or Windows 7 PC using PLAP

Users can log on to Windows Vista or Windows 7 when PLAP is enabled, by doing the following steps. The examples screens are for Windows Vista. (These steps are Microsoft requirements):

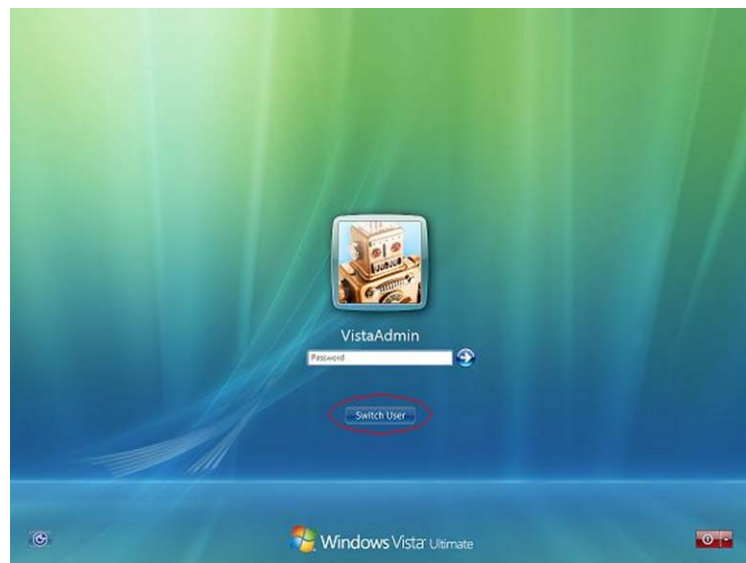
- Step 1** At the Windows Vista start window, press the Ctrl+Alt+Delete key combination (Figure 3-6).

Figure 3-6 Vista Login Window Showing the Network Connect Button



This displays the Vista logon window with a Switch User button (Figure 3-7).

Figure 3-7 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 3-8) with the network login icon in the lower-right corner. The network login icon is circled in red in Figure 3-8.

**Note**

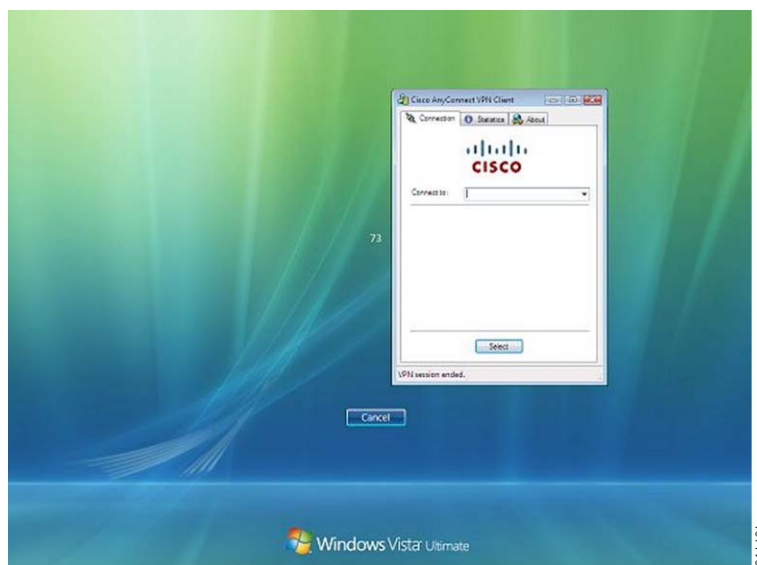
If the user is already connected through an AnyConnect connection and clicks Switch User, that VPN connection remains. If the user clicks Network Connect, the original VPN connection terminates. If the user clicks Cancel, the VPN connection terminates.

Figure 3-8 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 3-9).

Figure 3-9 AnyConnect Client Logon Window



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



Note

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

Step 5 When the user has successfully connected, the user sees a screen similar to the Vista Network Connect window, except that it has the Microsoft Disconnect button in the lower-right corner (Figure 3-10). This is the only indication that the connection is successful.

Figure 3-10 *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, the user has an unlimited time in which to log on. If the user forgets 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 3-10).

When the user clicks 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.

Enabling FIPS and Additional Security

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

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

AnyConnect Local Policy parameters reside in an XML file called *AnyConnectLocalPolicy.xml*. This file is not deployed by the ASA 5500 Series security appliance. You must deploy this file using corporate software deployment systems or change the file manually on a user computer.

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

Alternatively, you can obtain a copy of the AnyConnect Local Policy file from a client installation, manually edit the parameters, and deploy it to user computers.

The following sections describe all these procedures:

- [AnyConnect Local Policy File Parameters and Values, page 3-20](#)
- [AnyConnect Local Policy File Example, page 3-9](#)
- [Changing Parameters for Windows Clients using our MST File, page 3-9](#)
- [Changing Parameters Manually in the AnyConnect Local Policy File, page 3-10](#)
- [Changing Parameters for all Operating Systems using our Enable FIPS Tool, page 3-24](#)

AnyConnect Local Policy File Parameters and Values

**Note**

If you omit a policy parameter in the profile file, the feature resorts to default behavior.

Table 3-3 describes the parameters in the AnyConnect Local Policy file and their values:.

Table 3-3 AnyConnect Local Policy File and their Values


Parameter and Description	Values and Value Formats
acversion Specifies the minimum version of the AnyConnect client capable of interpreting all of the parameters in the file. If a client older than the version specified reads the file, it issues an event log warning.	The format is <code>acversion="<version number>"</code> .
xmlns The XML namespace specifier. Most administrators do not change this parameter.	The format is a URL, for example: <code>xmlns=http://schemas.xmlsoap.org/encoding/</code>
xsi:schemaLocation The XML specifier for the schema location. Most administrators do not change this parameter.	The format is a URL, for example: <code>xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectLocalPolicy.xsd"></code>
xmlns:xsi The XML schema instance specifier. Most administrators do not change this parameter	The format is a URL, for example: <code>xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance</code>
FipsMode Enables FIPS mode for the client. The client uses only algorithms and protocols approved by the FIPS standard.	<code>true</code> —Enables FIPS mode. <code>false</code> —Disables FIPS mode (default).
BypassDownloader Disables the launch of the VPNDownloader.exe module, which is responsible for detecting the presence of and updating the local versions of the dynamic content.	<code>true</code> —The client does not check for any dynamic content present on the security appliance, including profile updates, translations, customization, optional modules, and core software updates. <code>false</code> —The client checks for dynamic content present on the security appliance (default).  <p>Note If you configure client profiles on the security appliance, they must be installed on the client prior to the client connecting to the security appliance with BypassDownloader set to <code>true</code>. Because the profile can contain administrator defined policy, the BypassDownloader <code>true</code> setting is only recommended if you do not rely on the security appliance to centrally manage client profiles.</p>
RestrictWebLaunch Prevents users from using a non-FIPS-compliant browser to obtain the security cookie used to initiate an AnyConnect tunnel by forbidding the use of WebLaunch and forcing users to connect using the AnyConnect FIPS-compliant stand-alone connection mode.	<code>true</code> —WebLaunch attempts fail and the client displays an informative message to the user. <code>false</code> —Permits WebLaunch (default—behavior consistent with AnyConnect 2.3 and earlier).

Table 3-3 AnyConnect Local Policy File and their Values (continued)


Parameter and Description	Values and Value Formats
StrictCertificateTrust When authenticating remote security gateways, the AnyConnect client disallows any certificate that it cannot verify. Instead of prompting the user to accept these certificates, the client fails to connect to security gateways using self signed certificates.	<i>true</i> —The client fails to connect to security gateways that use invalid, mismatched, or untrusted certificates which require user interaction. <i>false</i> —The client prompts the user to accept the certificate (default—behavior consistent with AnyConnect 2.3 and earlier).
RestrictPreferenceCaching By design, the AnyConnect client does not cache sensitive information to disk. Enabling this parameter extends this policy to any type of user information stored in the AnyConnect preferences.	<i>Credentials</i> —The user name and second user name are not cached. <i>Thumbprints</i> —The client and server certificate thumbprints are not cached. <i>CredentialsAndThumbprints</i> —certificate thumbprints and user names are not cached. <i>All</i> —No automatic preferences are cached. <i>false</i> —All preferences are written to disk (default—behavior consistent with AnyConnect 2.3 and earlier).
RestrictTunnelProtocols (currently not supported) Forbids the use of certain tunnel protocol families to establish a connection to the security appliance.	<i>TLS</i> —The client only uses IKEv2 and ESP to establish the tunnel, and will not use TLS/DTLS to communicate information to the secure gateway. <i>IPSec</i> —The client only uses TLS/DTLS for authentication and tunneling. <i>false</i> —Any encrypted protocol may be used in connection establishment (default).  Note If you forbid the use of TLS or other protocols, certain advanced features, such as the automatic upgrading of Secure Desktop, may not work.
ExcludeFirefoxNSSCertStore (Linux and Mac) Permits or excludes the client from using the Firefox NSS certificate store to verify server certificates. The store has information about where to obtain certificates for client certificate authentication.	<i>true</i> —Excludes the Firefox NSS certificate store. <i>false</i> —Permits the Firefox NSS certificate store (default).
ExcludePemFileCertStore (Linux and Mac) Permits or excludes the client from using the PEM file certificate store to verify server certificates. The store uses FIPS-capable OpenSSL and has information about where to obtain certificates for client certificate authentication. Permitting the PEM file certificate store ensures remote users are using a FIPS-compliant certificate store.	<i>true</i> —Excludes the PEM file certificate store. <i>false</i> —Permits the PEM file certificate store (default).

Table 3-3 AnyConnect Local Policy File and their Values (continued)

Parameter and Description	Values and Value Formats
ExcludeMacNativeCertStore (Mac only) Permits or excludes the client from using the Mac native (keychain) certificate store to verify server certificates.	<i>true</i> —Excludes the Mac native certificate store. <i>false</i> —Permits the Mac native certificate store (default).
ExcludeWinNativeCertStore (Windows only, currently not supported) Permits or excludes the client from using the Windows Internet Explorer native certificate store to verify server certificates.	<i>true</i> —Excludes the Windows Internet Explorer certificate store. <i>false</i> —Permits the Windows Internet Explorer certificate store (default).

AnyConnect Local Policy File Example

The following is an example of the AnyConnect Local Policy file:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
  xmlns=http://schemas.xmlsoap.org/encoding/
  xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
  xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
  <FipsMode>>false</FipsMode>
  <BypassDownloader>>false</BypassDownloader>
  <RestrictWebLaunch>>false</RestrictWebLaunch>
  <StrictCertificateTrust>>false</StrictCertificateTrust>
  <RestrictPreferenceCaching>>false</RestrictPreferenceCaching>
  <RestrictTunnelProtocols>>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

Enabling FIPS with our MST File

For Windows installations, you can apply the MST file we provide to the standard MSI installation file to enable FIPS in the AnyConnect Local Policy. The MST only enables FIPS and does not change other parameters. The installation generates an AnyConnect Local Policy file with FIPS enabled.

For information about where you can download our MST, see the licensing information you received for the FIPS client.

Changing any Local Policy Parameter with your own MST File

You can create your own MST file to change any local policy parameters. Create your own MST file using the following custom rows. The names correspond to the parameters in AnyConnect Local Policy file (AnyConnectLocalPolicy.xml). See [Table 3-3](#) for the descriptions and values you can set for these parameters:

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS

- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

**Note**

The AnyConnect client installation does not automatically overwrite an existing local policy file on the user computer. You must delete the existing policy file on user computers first, then the client installer can create the new policy file.

Changing Parameters for all Operating Systems using our Enable FIPS Tool

For all operating systems, you can use our Enable FIPS tool to create an AnyConnect Local Policy file with FIPS enabled. The Enable FIPS tool is a command line tool that can only be run on Windows using administrator privileges or as a root user for Linux and Mac.

For information about where you can download the Enable FIPS tool, see the licensing information you received for the FIPS client.

Table 3-4 shows the policy settings you can specify and the arguments and syntax to use. The behavior for the argument values is the same behavior specified for the parameters in the AnyConnect Local Policy file in Table 3-3.

You run the Enable FIPS tool by entering the command **EnableFIPS** <arguments> from the command line of the computer. The following usage notes apply to the Enable FIPS tool:

- If you do not supply any arguments, the tool enables FIPS and restarts the vpnagent service (Windows) or the vpnagent daemon (Mac and Linux).
- Separate multiple arguments with spaces.

The following example shows the Enable FIPS tool command, run on a Windows computer:

```
EnableFIPS rwl=false sct=true bd=true fm=false
```

The next example shows the command, run on a Linux or Mac computer:

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

Table 3-4 shows the policy settings and the arguments for the Enable FIPS tool.

Table 3-4 Policy Settings and Arguments for the Enable FIPS Tool

Policy Setting	Argument and Syntax
FIPS mode	fm=[true false]
Bypass downloader	bd=[true false]
Restrict weblaunch	rwl=[true false]
Strict certificate trust	sct=[true false]
Restrict preferences caching	rpc=[Credentials Thumbprints CredentialsAndThumbprints All false]
Exclude FireFox NSS certificate store (Linux and Mac)	efn=[true false]
Exclude PEM file certificate store (Linux and Mac)	epf=[true false]
Exclude Mac native certificate store (Mac only)	emn=[true false]

Changing Parameters Manually in the AnyConnect Local Policy File

To change AnyConnect Local Policy parameters manually, follow this procedure:

- Step 1** Retrieve a copy of the AnyConnect Local Policy file (AnyConnectLocalPolicy.xml) from a client installation.

Table 3-5 shows the installation path for each operating system.

Table 3-5 Operating System and AnyConnect Local Policy File Installation Path

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

1. %APPDATA% refers to the environmental variable by the same name.
This is C:\Documents and Settings\All Users on most Win XP systems and C:\ProgramData on Windows Vista.

- Step 2** Edit the parameter settings. The example below shows the contents of the AnyConnect Local Policy file for Windows:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
  xmlns=http://schemas.xmlsoap.org/encoding/
  xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
  xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
  <FipsMode>>false</FipsMode>
  <BypassDownloader>>false</BypassDownloader>
  <RestrictWebLaunch>>false</RestrictWebLaunch>
  <StrictCertificateTrust>>false</StrictCertificateTrust>
  <RestrictPreferenceCaching>>false</RestrictPreferenceCaching>
  <RestrictTunnelProtocols>>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

- Step 3** Save the file as *AnyConnectLocalPolicy.xml* and deploy the file to remote computers using corporate an IT software deployment system.

Enabling Trusted Network Detection

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

If a client is also running Start Before Logon (SBL), and the user moves into the trusted network, the SBL window displayed on the computer automatically closes.



TND does not interfere with the ability of the user to manually establish a VPN connection. It does not disconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects the VPN session if the user first connects in an untrusted network and moves into a trusted network. For example, TND disconnects the VPN session if the user makes a VPN connection at home and then moves into the corporate office.

Because the TND feature controls the AnyConnect client GUI and automatically initiates connections, the GUI should run at all times. If the user exits the GUI, TND does not automatically start the VPN connection.

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

You configure TND in the AnyConnect profile (AnyConnectProfile.xml). No changes are required to the security appliance configuration. [Table 3-6](#) shows the profile parameters to configure TND and their values:

Table 3-6 Trusted Network Detection Parameters

Name	Possible Values and Descriptions
AutomaticVPNPolicy	<p><i>true</i>—Enables TND. Automatically manages when a VPN connection should be started or stopped according to the <i>TrustedNetworkPolicy</i> and <i>UntrustedNetworkPolicy</i> parameters.</p> <p><i>false</i>—Disables TND. VPN connections can only be started and stopped manually.</p> <p> Note AutomaticVPNPolicy does not prevent users from manually controlling a VPN connection.</p>
TrustedNetworkPolicy	<p><i>Disconnect</i>—Disconnects the VPN connection in the trusted network.</p> <p><i>DoNothing</i>—Takes no action in the trusted network.</p>
UntrustedNetworkPolicy	<p><i>Connect</i>—Initiates the VPN connection (if none exists) in the untrusted network.</p> <p><i>DoNothing</i>—Takes no action in the untrusted network.</p> <p> Note Setting both TrustedNetworkPolicy and UntrustedNetworkPolicy to <i>DoNothing</i> disables TND.</p>
TrustedDNSDomains	<p>A list of DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. The following is an example of a TrustedDNSDomain string:</p> <p>*.cisco.com</p> <p>Wildcards (*) are supported for DNS suffixes.</p>
TrustedDNSServers	<p>A list of DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. The following is an example of a TrustedDNSServers string:</p> <p>161.44.124.*,64.102.6.247</p> <p>Wildcards (*) are supported for DNS server addresses.</p>



Note

If you configure both TrustedDNSDomains and TrustedDNSServers, users must match both settings to be considered in the trusted network.

The following text shows the ClientInitialization section of the profile file with the TND parameters configured. In the example, the client is configured to automatically disconnect the VPN connection when in the trusted network, and to initiate the VPN connection in the untrusted network:

```
<AutomaticVPNPolicy>true
  <TrustedDNSDomains>*.cisco.com</TrustedDNSDomains>
  <TrustedDNSServers>161.44.124.*,64.102.6.247</TrustedDNSServers>
  <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
  <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
</AutomaticVPNPolicy>
```

Table 3-7 shows examples of DNS suffix matching.

Table 3-7 DNS Suffix Matching Examples

To Match this DNS Suffix:	Use this Value for TrustedDNSDomains:
cisco.com (only)	cisco.com
cisco.com AND anyconnect.cisco.com	*cisco.com OR cisco.com, anyconnect.cisco.com
asa.cisco.com AND anyconnect.cisco.com	*.cisco.com OR asa.cisco.com, anyconnect.cisco.com

Users with Multiple Profiles Connecting to Multiple Security Appliances

Multiple profiles on a user computer may present problems if the user alternates connecting to a security appliance that has TND enabled and to one that does not. If the user has connected to a TND-enabled security appliance in the past, that user has received a TND-enabled profile. If the user reboots the computer when out of the trusted network, the GUI of the TND-enabled client displays and attempts to connect to the security appliance it was last connected to, which could be the one that does not have TND enabled.

If the client connects to the TND-enabled security appliance, and the user wishes to connect to the non-TND security appliance, the user must manually disconnect and then connect to the non-TND security appliance. Please consider these problems before enabling TND when the user may be connecting to security appliances with and without TND.

The following workarounds will help you prevent this problem:

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

Configuring a Certificate Store

You can configure how AnyConnect locates and handles certificate stores on the local host. Depending on the platform, this may involve limiting access to a particular store or allowing the use of files instead of browser based stores. The purpose is to direct AnyConnect to the desired location for Client certificate usage as well as Server certificate verification.

For Windows, you can control in which certificate store the AnyConnect client searches for certificates. You may want to configure the client to restrict certificate searches to only the user store or only the machine store. For Mac and Linux, you can create a certificate store for PEM-format certificate files. These certificate store configurations are stored in the AnyConnect client profile.

**Note**

You can also configure more certificate store restrictions in the AnyConnect local policy. The AnyConnect local policy is an XML file you deploy using enterprise software deployment systems and it is separate from the AnyConnect client profile. The settings in the file restrict the use of the Firefox NSS (Linux and Mac), PEM file, Mac native (keychain) and Windows Internet Explorer native certificate stores. For more information, see [Enabling FIPS and Additional Security, page 3-20](#).

The following sections describe the procedures for configuring certificate stores and controlling their use:

- [Controlling the Certificate Store on Windows, page 3-28](#)
- [Examples of <CertificateStore> and <CertificateStoreOverride> Usage, page 3-29](#)
- [Creating a PEM Certificate Store for Mac and Linux, page 3-29](#)
- [Restricting Certificate Store Use, page 3-31](#)

Controlling the Certificate Store on Windows

Windows provides separate certificate stores for the local machine and for the current user. Users with administrative privileges on the computer have access to both certificate stores. You can specify in which certificate store the AnyConnect client searches for certificates.

You can configure certificate store lookups by adding <CertificateStore> as a child element of the <ClientInitialization> element in the AnyConnect client profile.

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

The <CertificateStore> element has three possible values, these values are case-sensitive:

- All—(default) Search all certificate stores.
- Machine—Search the machine certificate store (the certificate identified with the computer).
- User—Search the user certificate store.

If users do not have administrative privileges on their computers, the only certificate store their account has access to is the user store. You can configure an additional element <CertificateStoreOverride>, also as a child of <ClientInitialization>, which grants those users access to the machine certificate store, allowing AnyConnect to search that store as well.

<CertificateStoreOverride> has two possible settings, these values are case-sensitive:

- true—Allows AnyConnect to search a computer's machine certificate store even when the user does not have administrative privileges.
- false—(default) Does not allow AnyConnect to search the machine certificate store of a user without administrative privileges.

Examples of <CertificateStore> and <CertificateStoreOverride> Usage

<CertificateStore> and <CertificateStoreOverride> are both children of <ClientInitialization>. The following example shows these elements in the correct format and illustrates the default values explained in [Table 3-8](#).

```
<ClientInitialization>
  <CertificateStore>All</CertificateStore>
  <CertificateStoreOverride>false</CertificateStoreOverride>
</ClientInitialization>
```

Table 3-8 Examples of Certificate Store and Certificate Store Override Configurations

<CertificateStore> Value	<CertificateStoreOverride> Value	AnyConnect Action
All	false	AnyConnect searches all certificate stores. AnyConnect is not allowed to access the machine store when the user has non-administrative privileges. These are the default values. This setting is appropriate for the majority of cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.
All	true	AnyConnect searches all certificate stores. AnyConnect is allowed to access the machine store when the user has non-administrative privileges.
Machine	true	AnyConnect searches the machine certificate store. AnyConnect is allowed to search the machine store when the user has non-administrative privileges.
Machine	false	AnyConnect searches the machine certificate store. AnyConnect is not allowed to search the machine store when the user has non-administrative privileges. Note This configuration might be used when only a limited group of users are allowed to authenticate using a certificate.
User	not applicable	AnyConnect searches in the user certificate store only. The certificate store override is not applicable because non-administrative accounts have access to this certificate store.

Creating a PEM Certificate Store for Mac and Linux

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

Restrictions for PEM File Filenames

In order for the AnyConnect client to acquire the appropriate certificates under all circumstances, ensure that your files meet the following requirements:

- All certificate files must end with the extension **.pem**.
- All private key files must end with the extension **.key**.
- A client certificate and its corresponding private key must have the same filename.
For example: client.pem and client.key



Note Instead of keeping copies of the PEM files, you can use soft links to PEM files.

Storing User Certificates

To create the PEM file certificate store, create the paths and folders listed in [Table 9](#). Place the appropriate certificates in these folders:

Table 9 *PEM File Certificate Store Folders and Types of Certificates Stored*

PEM File Certificate Store Folders	Type of Certificates Stored
~/.cisco/certificates/ca ¹	Trusted CA and root certificates
~/.cisco/certificates/client	Client certificates
~/.cisco/certificates/client/private	Private keys

1. ~ is the home directory.



Note The requirements for machine certificates are the same as for PEM file certificates, with the exception of the root directory. For machine certificates, substitute /opt/.cisco for ~/.cisco. Otherwise, the paths, folders, and types of certificates listed in [Table 9](#) apply.

Restricting Certificate Store Use

You can configure additional restrictions on the client using certificate stores by setting parameters in the AnyConnect local policy that restrict the use of the Firefox NSS (Linux and Mac), PEM file, Mac native (keychain) and Windows Internet Explorer native certificate stores. [Table 3-10](#) shows the parameters that control these restrictions:

Table 3-10 Certificate Store Parameters in the AnyConnect Local Policy

Parameter and Description	Values and Value Formats
ExcludeFirefoxNSSCertStore (Linux and Mac) Permits or excludes the client from using the Firefox NSS certificate store to verify server certificates. The store has information about where to obtain certificates for client certificate authentication.	<i>true</i> —Excludes the Firefox NSS certificate store. <i>false</i> —Permits the Firefox NSS certificate store (default).
ExcludePemFileCertStore (Linux and Mac) Permits or excludes the client from using the PEM file certificate store to verify server certificates. The store uses FIPS-capable OpenSSL and has information about where to obtain certificates for client certificate authentication. Permitting the PEM file certificate store ensures remote users are using a FIPS-compliant certificate store.	<i>true</i> —Excludes the PEM file certificate store. <i>false</i> —Permits the PEM file certificate store (default).
ExcludeMacNativeCertStore (Mac only) Permits or excludes the client from using the Mac native (keychain) certificate store to verify server certificates.	<i>true</i> —Excludes the Mac native certificate store. <i>false</i> —Permits the Mac native certificate store (default).
ExcludeWinNativeCertStore (Windows only, currently not supported) Permits or excludes the client from using the Windows Internet Explorer native certificate store to verify server certificates.	<i>true</i> —Excludes the Windows Internet Explorer certificate store. <i>false</i> —Permits the Windows Internet Explorer certificate store (default).

Configuring Simplified Certificate Enrollment Protocol

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

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

AnyConnect administrators configure the use of SCEP requests in the client profile file. This file is an XML file downloaded with the client that contains settings that affect client behavior. [Table 3-11](#) describes the profile elements used to configure the SCEP feature.

Use of the SCEP protocol is supported on all operating systems that support the AnyConnect client.

This section describes the following topics:

- [Provisioning and Renewing Certificates Automatically or Manually, page 3-32](#)
- [Configuring SCEP Protocol to Provision and Renew Certificates, page 3-33](#)
- [Certificate Storage after SCEP Request, page 3-38](#)
- [Configuring the ASA to Support SCEP Protocol for AnyConnect, page 3-38](#)

Provisioning and Renewing Certificates Automatically or Manually

You can configure SCEP requests so that either AnyConnect initiates certificate requests automatically or users initiate certificate requests manually.

Automatic Certificate Requests

AnyConnect attempts to automatically retrieve new certificates in two cases. For both cases, client certificate authentication must fail before AnyConnect tries to automatically retrieve the new certificates.

The first case is when users attempt to connect to a group-url which is identified in the <AutomaticSCEPHost> element of their client profile. AnyConnect initiates the SCEP certificate request after a VPN, based on the SCEP-enabled group-url, has been established.

The user may be prompted for a Certificate ID. The Certificate ID is the challenge password or token to be offered to the certificate authority that identifies the user to the certificate authority. With this ID and the other data in the SCEP section of the profile, AnyConnect contacts the certificate authority and continues with the SCEP retrieval process. If the **PromptForChallengePW** attribute of the <CAURL> element is enabled in the client profile, AnyConnect prompts users for a Certificate ID.

The second method for triggering automatic certificate retrieval is the case where the <CertificateSCEP> element is not defined in the client profile. In this case, the user attempts to connect using a connection profile that has been setup to support access to a certificate authority. Once the VPN has been activated, AnyConnect searches the client profile, downloaded as part of the VPN activation, to see if the group-url chosen for the connection is found in the client profile.

If AnyConnect finds the group-url in the <AutomaticSCEPHost> element of the client profile, this triggers the automatic SCEP retrieval process in the same manner as described in the previous method.

Manual Certificate Retrieval

Users initiate requests for new certificates by clicking the **Get Certificate** or **Enroll** button on the AnyConnect interface. AnyConnect presents these buttons to users in either of these circumstances, as long as the SCEP section of the AnyConnect profile is configured:

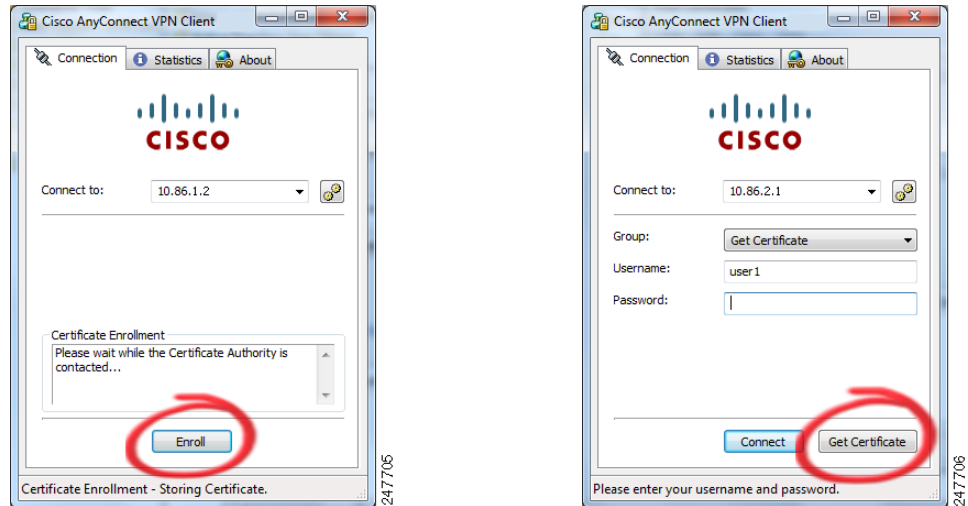
- When the ASA requests a certificate and none of the certificates on the host are available are accepted
- When the current certificate used by AnyConnect has expired

Users will only be able to initiate the certificate request in one of the following instances:

- The host has direct access to the certificate authority
- The certificate authority is publicly available
- The host already has an established VPN tunnel which gives it access to the certificate authority

- The URL of the certificate authority is defined in the client profile in the <CAURL> element

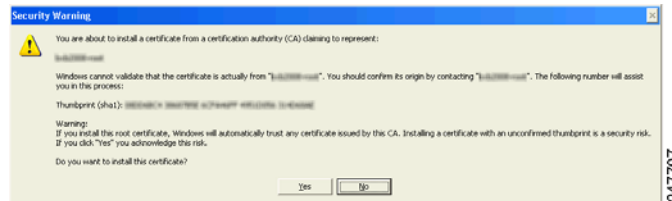
Figure 3-11 *Get Certificate and Enroll Buttons*



Windows Certificate Warning

When Windows clients first attempt to retrieve a certificate from the certificate authority, either manually or automatically, they may see a warning like the one in [Figure 3-12](#). When prompted, users must click **Yes**. This allows them to receive the user certificate and the root certificate. Clicking No will only allow them to receive the user certificate and they may not be able to authenticate.

Figure 3-12 *Windows Certificate Security Warning*



Configuring SCEP Protocol to Provision and Renew Certificates

The AnyConnect client retrieves certificates using the SCEP protocol if the <CertificateSCEP> element is defined in a client profile, the client profile is specified in a group policy, and the group policy is specified in users' connection profile.

[Table 3-11](#) describes the elements in the client profile used to configure SCEP. [Example 3-1](#) shows a sample of the SCEP elements in a client profile.

See [Configuring and Deploying the AnyConnect Client Profile, page 3-2](#) for more information about how to configure a client profile.

Table 3-11 Elements in the client profile file used to configure SCEP

Element name	Child of	Description
CertificateEnrollment	ClientInitialization	Starting tag for certificate enrollment.
CertificateExpirationThreshold	CertificateEnrollment	<p>Note This parameter is not supported in Anyconnect 2.4.</p> <p>Specifies the number of days prior to the certificate's expiration date, that AnyConnect warns users that their certificate is going to expire.</p> <p>Default: 0</p> <p>Range of Values: 0-180</p> <p>The default value for this element is 0 which means no warning will be displayed. The maximum value is 180 days prior to the certificate expiring.</p> <p>In the following example, CertificateExpirationThreshold is set to 14 days.</p> <p>Note CertificateExpirationThreshold is only supported when SCEP is disabled. SCEP is disabled when there is no <CertificateSCEP> element defined in the client profile.</p>
AutomaticSCEPHost	CertificateEnrollment	<p>The host will attempt automatic certificate retrieval if this attribute specifies the ASA host name and connection profile (tunnel group) for which SCEP certificate retrieval is configured.</p> <p>Permitted values:</p> <ul style="list-style-type: none"> Fully qualified domain name of the ASA\connection profile name IP Address of the ASA\connection profile name <p>In the following example, the AutomaticSCEPHost field specifies, asa.cisco.com as the host name of the ASA and scep_eng as the name of the connection profile (tunnel group) configured for SCEP certificate retrieval.</p>

Table 3-11 Elements in the client profile file used to configure SCEP

Element name	Child of	Description
CAURL	CertificateEnrollment	<p>Identifies the SCEP CA server.</p> <p>Permitted values: Fully qualified domain name or IP Address of CA server.</p> <p>In the following example, the CAURL field identifies http://ca01.cisco.com as the name of the SCEP CA server.</p> <p>Attributes of CAURL:</p> <p>PromptForChallengePW: Used for manual get certificate requests. After the user clicks Get Certificate, they will be prompted for their username and one time password.</p> <p>Permitted values: true, false</p> <p>The PromptForChallengePW attribute in the example below is configured “true.”</p> <p>Thumbprint: The CA’s certificate thumbprint. Use SHA1 or MD5 hashes. The Thumbprint attribute in the example below is 8475B661202E3414D4BB223A464E6AAB8CA123AB.</p> <p>Note Obtain the CA URL and thumbprint, from your CA server administrator. The CA server administrator should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.</p>
CertificateSCEP	CertificateEnrollment	<p>Section that defines how the contents of the certificate will be requested. See the CertificateSCEP element in the following example.</p>
CADomain	CertificateSCEP	<p>Domain of the certificate authority.</p> <p>In the following example, the CADomain is cisco.com.</p>
Name_CN	CertificateSCEP	<p>Common Name in the certificate.</p> <p>In the following example, Name_CN is %USER% which corresponds to the user’s ASA username login credential.</p>
Department_OU	CertificateSCEP	<p>Department name specified in certificate.</p>
Company_O	CertificateSCEP	<p>Company name specified in certificate.</p>
State_ST	CertificateSCEP	<p>State identifier named in certificate.</p>
Country_C	CertificateSCEP	<p>Country identifier named in certificate.</p>
Email_EA	CertificateSCEP	<p>Email address.</p> <p>In the following example, Email_EA is %USER%@cisco.com. %USER% corresponds to the user’s ASA username login credential.</p>
Domain_DC	CertificateSCEP	<p>Domain component. In the following example, Domain_DC is set to cisco.com.</p>

Table 3-11 Elements in the client profile file used to configure SCEP

Element name	Child of	Description
DisplayGetCertButton	CertificateSCEP	<p>Determines if the AnyConnect GUI displays the Get Certificate button. Administrators may choose to configure this button if they think it will give their users a clearer understanding of what they are doing when interacting with the AnyConnect interface. Without this button, users see a button labeled “Enroll” along with a message box that AnyConnect is contacting the certificate authority to attempt certificate enrollment.</p> <p>Default value: false</p> <p>Range of Values: true, false</p> <p>If the DisplayGetCertButton attribute is set to false, the Get Certificate button will not be visible in the AnyConnect GUI. Choose false if you do not permit users to manually request provisioning or renewal of authentication certificates.</p> <p>If the DisplayGetCertButton attribute is set to true, the Get Certificate button will be visible to users after the certificate has expired or if no certificate is present. Choose true if you permit users to manually request provisioning or renewal of authentication certificates. Typically, these users will be able to reach the certificate authority without first needing to create a VPN tunnel.</p> <p>In the following example, DisplayGetCertButton is set to false.</p>
ServerList	AnyConnectProfile	Starting tag for the server list. The server list is presented to users when they first launch AnyConnect. Users can choose which ASA to login to. See ServerList in the following example.
HostEntry	ServerList	Starting tag for configuring an ASA. Look at the second HostEntry element in the following example.
HostName	HostEntry	Host name of the ASA. In the second HostEntry element in the following example, the HostName element is Certificate Enroll .
HostAddress	HostEntry	Fully qualified domain name of the ASA. In the second HostEntry element in the following example, the HostAddress element is set to ourasa.cisco.com .

Table 3-11 Elements in the client profile file used to configure SCEP

Element name	Child of	Description
AutomaticSCEPHost	HostEntry	This element has the same definition and permitted values as the one described earlier in this table. However, if this element is configured, and the user chooses this HostEntry from the server list, this value overrides the value of AutomaticSCEPHost configured earlier in the user profile file. In the following example, for this HostEntry, AutomaticSCEPHost is set to ourasa.cisco.com/scep_eng .
CAURL	HostEntry	This element has the same definition, permitted values, and attributes as the one described earlier in this table. However, if this element is configured, and the user chooses this HostEntry from the server list, this value overrides the value of CAURL configured earlier in the user profile file. In the following example, for this HostEntry, CAURL is set to http://ca02.cisco.com .

Example 3-1 Example of SCEP Elements in User Profile**Note**

The AnyConnect profile fails XML validation if the tags are not presented in the appropriate order. Consult the AnyConnectProfile.xsd which is installed as part of the AnyConnect installation.

```
<AnyConnectProfile>
  <ClientInitialization>
    <CertificateEnrollment>
      <CertificateExpirationThreshold>14</CertificateExpirationThreshold>
      <AutomaticSCEPHost>asa.cisco.com/scep_eng</AutomaticSCEPHost>
      <CAURL PromptForChallengePW="true">
Thumbprint="8475B661202E3414D4BB223A464E6AAB8CA123AB">http://ca01.cisco.com</CAURL>
      <CertificateSCEP>
        <CADomain>cisco.com</CADomain>
        <Name_CN>%USER%</Name_CN>
        <Department_OU>Engineering</Department_OU>
        <Company_O>Cisco Systems</Company_O>
        <State_ST>Colorado</State_ST>
        <Country_C>US</Country_C>
        <Email_EA>%USER%@cisco.com</Email_EA>
        <Domain_DC>cisco.com</Domain_DC>
        <DisplayGetCertButton>>false</DisplayGetCertButton>
      </CertificateSCEP>
    </CertificateEnrollment>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>ABC-ASA</HostName>
      <HostAddress>ABC-asa-cluster.cisco.com</HostAddress>
    </HostEntry>
    <HostEntry>
      <HostName>Certificate Enroll</HostName>
      <HostAddress>ourasa.cisco.com</HostAddress>
      <AutomaticSCEPHost>ourasa.cisco.com/scep_eng</AutomaticSCEPHost>
      <CAURL PromptForChallengePW="false">
Thumbprint="8475B655202E3414D4BB223A464E6AAB8CA123AB">http://ca02.cisco.com</CAURL>
    </HostEntry>
```

```
</ServerList>
</AnyConnectProfile>
```

**Note**

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.

Certificate Storage after SCEP Request

Certificates obtained through a SCEP request are stored in the users personal certificate store. In addition, if the user has sufficient privileges on Windows desktop platforms, the certificate is also saved to the machine store. On MAC platforms, certificates obtained through a SCEP request are only added to the “login” keychain. On Linux, we support the Firefox browser certificate store.

Configuring the ASA to Support SCEP Protocol for AnyConnect

To provide access to a private Registration Authority (RA), the ASA administrator should create a group-url that has an ACL restricting private side network connectivity to the desired RA. To automatically retrieve a certificate, users would then connect and authenticate to this group-url.

Once users have authenticated to this group-url, AnyConnect downloads the client profile assigned to the connection profile. The client profile contains a <CertificateEnrollment> section. With the information in this section, the client automatically connects to the certificate authority specified in the <CAURL> element of the client profile and initiates certificate enrollment. ASA administrators need to perform these configuration tasks:

- Create a group-url on the ASA to point to the specially configured group.
- Specify the group-url in the <AutomaticSCEPHost> element in the user’s client profile.
- Attach the client profile containing the <CertificateEnrollment> section to the specially configured group.
- Set an ACL for the specially configured group to restrict traffic to the private side RA.

To keep the SCEP enabled group from being exposed to the user, it should not be “enabled” on the ASA. With the described implementation it is not necessary to expose the group to users for them to have access to it.

Configuring Certificate Only Authentication on the ASA

To support certificate-only authentication in an environment where multiple groups are used, an administrator may provision more than one group-url. Each group-url would contain a different client profile with some piece of customized data that would allow for a group-specific certificate map to be created. For example, the Department_OU value of Engineering could be provisioned on the ASA to place the user in this group when the certificate from this process is presented to the ASA.

Configuring Certificate Matching

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 3-41](#) 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 3-12](#) lists the well known set of constraints with their corresponding object identifiers (OIDs).

Table 3-12 **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 the example AnyConnect profile named AnyConnectProfile.tmp1, which the AnyConnect client automatically downloads to the endpoint.

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 3-13](#) lists the supported criteria:

Table 3-13 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

Table 3-13 Criteria for Certificate Distinguished Name Mapping (continued)

Identifier	Description
CN	SubjectCommonName
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 the example AnyConnect profile named AnyConnectProfile.tmpl, which the AnyConnect client automatically downloads to the endpoint.

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>ASA_Security</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 3-14](#) 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 3-14 Certificate Match Parameters

XML Tag Name	Possible Values	Description	Example
CertificateMatch	n/a	Group identifier	<pre> <CertificateMatch>... </CertificateMatch> </pre>
KeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to specify acceptable client certificates.	<pre> <KeyUsage> <MatchKey>Non_Repudiation</MatchKey> </KeyUsage> </pre>
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.	<pre> <KeyUsage> <MatchKey>Non_Repudiation</MatchKey> <MatchKey>Digital_Signature</MatchKey> </KeyUsage> </pre>
ExtendedKeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to choose acceptable client certificates.	<pre> <ExtendedKeyUsage> <ExtendedMatchKey>ClientAuth</ExtendedMatchKey> </ExtendedKeyUsage> </pre>

Table 3-14 Certificate Match Parameters (continued)

XML Tag Name	Possible Values	Description	Example
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>
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 3-14 Certificate Match Parameters (continued)

XML Tag Name	Possible Values	Description	Example
DistinguishedNameDefinition	<p>Bold text indicates default value.</p> <p>Wildcard: "Enabled" "Disabled"</p> <p>Operator: "Equal" or == "NotEqual" or !=</p> <p>MatchCase: "Enabled" "Disabled"</p>	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.	<pre><DistinguishedNameDefinition Operator="Equal" Wildcard="Enabled" Matchcase="Enabled"> <Name>CN</Name> <Pattern>ASASecurity</Pattern> </DistinguishedNameDefinition></pre>
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.	

Prompting Users to Select Authentication Certificate

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

This configuration is available only for Windows 7, Vista, and XP.

Configuring the Client Profile with AutomaticCertSelection

To allow users to choose their authentication certificate, AnyConnect Administrators must provide the users with a client profile that has the <AutomaticCertSelection> element set to **false**. See [Configuring and Deploying the AnyConnect Client Profile, page 3-2](#) to learn how to edit and distribute the client profile.

Here is the description of the <AutomaticCertSelection> element and an example of how it appears in the client profile.

Table 3-15 *AutomaticCertSelection element description*

Element name	Child of	Description
AutomaticCertSelection	ClientInitialization	<p>Allows or prevents users from selecting the certificate used to authenticate their AnyConnect session. Presence of this field exposes the Automatic certificate selection checkbox in the AnyConnect Preferences dialog box.</p> <p>Permitted Values:</p> <ul style="list-style-type: none"> • true - Set the value to true to allow AnyConnect to automatically select the authentication certificate. • false - Set the value to false to prompt the user to select the authentication certificate. <p>Default value: true</p>

Figure 3-13 *AutomaticCertSelection element in 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">
```

```
<AnyConnectProfile>
  <ClientInitialization>
    <AutomaticCertSelection>false</AutomaticCertSelection>
  </ClientInitialization>
</AnyConnectProfile>
```



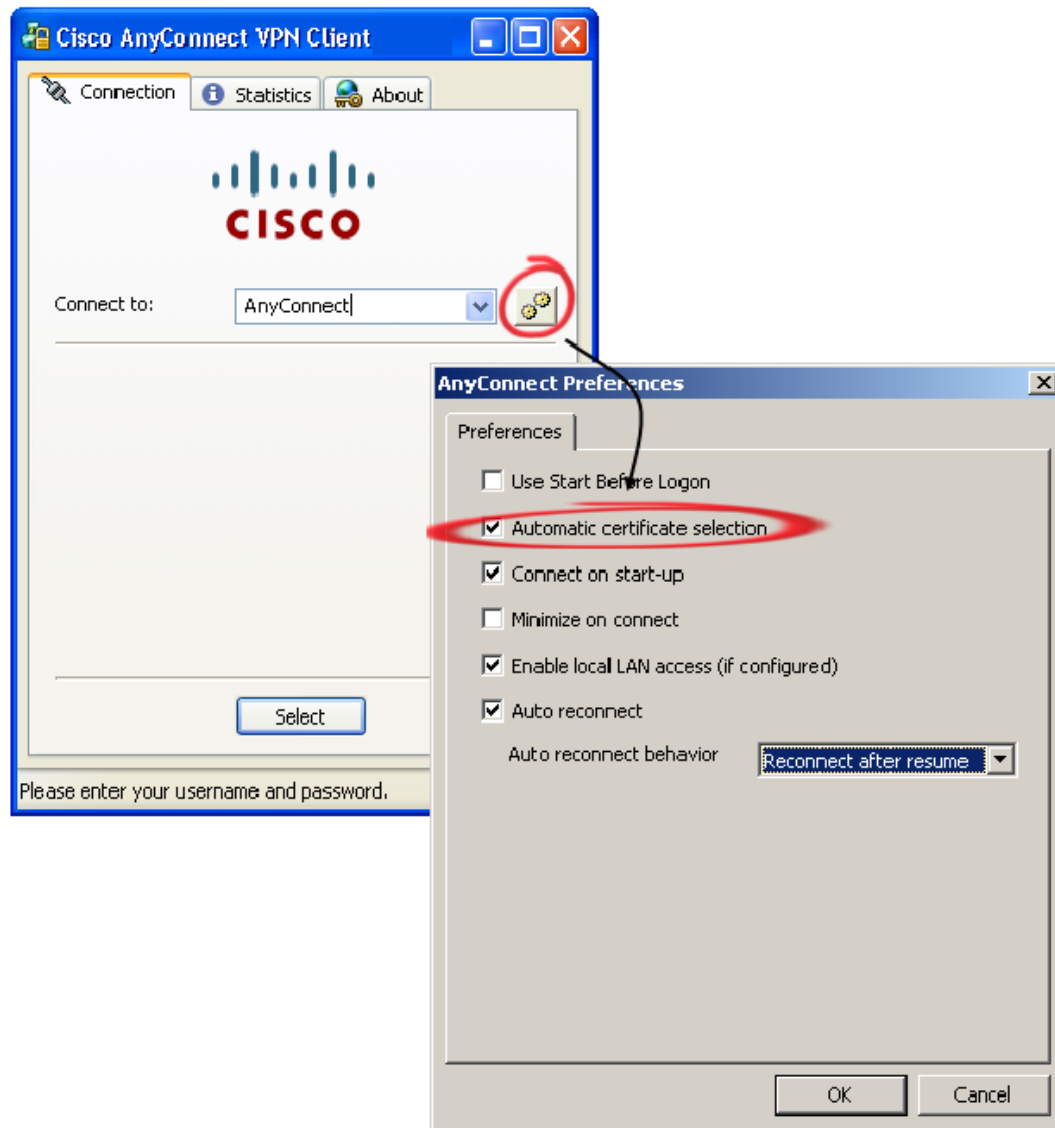
Caution

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.

Users Configuring Automatic Certificate Selection in AnyConnect Preferences

The presence of the <AutomaticCertSelection> element in the client profile, exposes the Automatic certificate selection checkbox in the AnyConnect Preferences dialog box. Users will be able to turn Automatic certificate selection on and off by checking or unchecking Automatic certificate selection.

Figure 3-14 Automatic Certificate Selection check box



Configuring Backup Server List Parameters

You can configure a list of backup servers the client uses in case the user-selected server fails. These servers are specified in the AnyConnect client profile, in the ClientInitialization section. 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 3-16](#) lists these parameters and defines their possible values.

**Note**

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

Table 3-16 Backup Server Parameters

Name	Possible Values	Description	Examples
BackupServerList	n/a	Group identifier	<code><BackupServerList>...</BackupServerList></code>
HostAddress	An IP address or a Full-Qualified Domain Name (FQDN)	Specifies a host address to include in the backup server list.	<code><BackupServerList> <HostAddress>bos</HostAddress> <HostAddress>bos.example.com</HostAddress> </BackupServerList></code>

Installing AnyConnect on a Windows Mobile Device

The security appliance does not support WebLaunch of AnyConnect on mobile devices. Just as you can do so with corporate computers, you can pre-deploy AnyConnect on Windows Mobile devices issued to employees. Otherwise, mobile users must download and install AnyConnect Client for Windows Mobile. Perform the following steps to download and install AnyConnect Client for Windows Mobile.

- Step 1** Download any of the following files from the Cisco AnyConnect VPN Client Download Software site to get the Windows Mobile Client:
 - File containing all client installation packages:
anyconnect-all-packages—*AnyConnectRelease_Number-k9.zip*
 - CAB package signed by Cisco for Windows Mobile devices:
anyconnect-wince-ARMv4I-*AnyConnectRelease_Number-k9.cab*
 - ActiveSync MSI package for Windows Mobile platforms:
anyconnect-wince-ARMv4I-activesync-*AnyConnectRelease_Number-k9.msi*
- Step 2** Unzip the anyconnect-all-packages—*AnyConnectRelease_Number-k9.zip* file if you chose to download that file.
- Step 3** Transfer the file to a corporate server if you want to provide users with a link to the client.
- Step 4** Make sure the Windows Mobile device meets the system requirements in the latest [AnyConnect Release Notes](#).
- Step 5** Use your preferred method to transfer the .cab or .msi file from your intranet server or local computer to the mobile device. Some examples include:
 - Microsoft ActiveSync over radio
 - HTTP, FTP, SSH, or shared files over the LAN or radio

- Bluetooth
- (USB) Cable
- Media card transfer

Step 6 Use the mobile device to open the file you transferred, and proceed with the installation wizard.s

Configuring a 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 [AnyConnect Release Notes](#) 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 3-17](#) shows the MobilePolicy parameters and their values.

Table 3-17 Mobile Policy Parameters

Parameter	Possible Values	Description	Example
MobilePolicy	n/a	Group identifier.	<MobilePolicy>...</MobilePolicy>
DeviceLockRequired	n/a	<p>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).</p> <p>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.</p>	<pre><DeviceLockRequired> MaximumTimeoutMinutes="60" MinimumPasswordLength="4" PasswordComplexity="pin" </DeviceLockRequired></pre>
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.	<pre><DeviceLockRequired> MaximumTimeoutMinutes="60" MinimumPasswordLength="4" PasswordComplexity="pin" </DeviceLockRequired></pre>

Table 3-17 Mobile Policy Parameters (continued)

Parameter	Possible Values	Description	Example
MinimumPasswordLength	Any non-negative integer	<p>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.</p> <p>This setting must be pushed down to the mobile device by syncing with an Exchange server before it can be enforced. (WM5AKU2+)</p>	<pre><DeviceLockRequired> MaximumTimeoutMinutes="60" MinimumPasswordLength="4" PasswordComplexity="pin" </DeviceLockRequired></pre>
PasswordComplexity	<p>"alpha"-Requires an alphanumeric password.</p> <p>"pin"-Requires a numeric PIN.</p> <p>"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.</p>	<p>When present checks for the password subtypes listed in the column to the left.</p> <p>This setting must be pushed down to the mobile device by syncing with an Exchange server before it can be enforced. (WM5AKU2+)</p>	<pre><DeviceLockRequired> MaximumTimeoutMinutes="60" MinimumPasswordLength="4" PasswordComplexity="pin" </DeviceLockRequired></pre>

**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.

Installing AnyConnect on 64-bit Linux

To install AnyConnect on x86_64 versions of Ubuntu 9,

-
- Step 1** Enter the following command to install the 32-bit compatibility library:
- ```
administrator@ubuntu-904-64:/usr/local$ sudo apt-get install ia32-libs lib32nss-mdns
```
- Step 2** Download the 32-bit version of FireFox from <http://www.mozilla.com> and install it on /usr/local/firefox. The client looks in this directory first for the NSS crypto libraries it needs.
- Step 3** Enter the following command to extract the Firefox installation to the directory indicated:
- ```
administrator@ubuntu-904-64:/usr/local$ sudo tar -C /usr/local -xvjf  
~/Desktop/firefox-version.tar.bz2
```
- Step 4** Run Firefox at least once as the user who will use AnyConnect.
- Doing so creates the .mozilla/firefox profile in the user's home directory, which is required by AnyConnect for interacting with the Firefox certificate store.
- Step 5** Install the AnyConnect client in standalone mode.
-

Using the Manual Install Option on Mac OS if the Java Installer Fails

If you use WebLaunch to start AnyConnect on a Mac and the Java installer fails, a dialog box presents a Manual Install link. Proceed as follows:

-
- Step 1** Click **Manual Install**.
- A dialog box presents the option to save the vpnsetup.sh file.
- Step 2** Save the vpnsetup.sh file on the Mac.
- Step 3** Open a Terminal window and use the CD command to navigate to the directory containing the file saved.
- Step 4** Enter the following command:
- ```
sudo /bin/sh vpnsetup.sh
```
- The vpnsetup script starts the AnyConnect installation.
- Step 5** Following the installation, choose Applications > Cisco > Cisco AnyConnect VPN Client to initiate an AnyConnect VPN session.
-

## Configuring Auto Connect On Start

By default, AnyConnect, when started, automatically establishes a VPN connection with the secure gateway specified by the AnyConnect client profile. Upon connecting, AnyConnect replaces the local profile with the one provided by the secure gateway if the two do not match, and applies the settings of that profile.

To modify the default auto connect settings, insert the `<AutoConnectOnStart>` tag into the `<ClientInitialization>` section of the client profile.

If you disable auto connect and the user starts AnyConnect, the AnyConnect GUI displays the settings configured by default as user-controllable. The user must select the name of the secure gateway in the Connect to drop-down list in the AnyConnect GUI and click Connect. Upon connecting, AnyConnect applies the settings of the AnyConnect client profile provided by the security appliance.

Table 3-18 shows the information about the `<AutoConnectOnStart>` tag.

**Table 3-18** *AutoConnectOnStart tag*

| XML Tag Name       | Default Value <sup>1</sup> | Possible Values <sup>2</sup> | User Controllable | User Controllable by Default <sup>3</sup> | OSs Supported |
|--------------------|----------------------------|------------------------------|-------------------|-------------------------------------------|---------------|
| AutoConnectOnStart | true                       | true<br>false                | Yes               | Yes                                       | All           |

1. AnyConnect uses the default value if the profile does not specify one.
2. Insert the parameter value between the beginning and closing tags; for example, `<AutoConnectOnStart>true</AutoConnectOnStart>`.
3. The AnyConnect Preferences dialog box displays the parameter values and lets users change them, depending on the value of the associated user control attribute. The user control attribute is optional. If you do not insert it, AnyConnect uses its default value. To permit or deny user control, insert the user control attribute inside the opening tag; for example, `<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>`.

# Configuring Auto Reconnect

AnyConnect supports two XML tags for configuring auto reconnect behaviors, as follows:

- **AutoReconnect**—By default, AnyConnect attempts to reestablish a VPN connection if you lose connectivity. The default setting of this tag is `true`.
- **AutoReconnectBehavior**—By default, AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resume. The default setting of this tag is `DisconnectOnSuspend`.

A *system suspend* is a low-power standby, Windows “hibernation,” or Mac OS or Linux “sleep.” A *system resume* is a recovery following a system suspend.



## Note

Before AnyConnect 2.3, the default behavior in response to a system suspend was to retain the resources assigned to the VPN session and reestablish the VPN connection after the system resume. To retain that behavior, assign the value `ReconnectAfterResume` to the `AutoReconnectBehavior` tag.

Unlike the IPsec client, AnyConnect can recover from VPN session disruptions. AnyConnect can reestablish a session, regardless of the media used for the initial connection. For example, it can reestablish a session on wired, wireless, or 3G.

To modify the Auto Reconnect setting, insert the `<AutoReconnect>` tag into the `<ClientInitialization>` section of the client profile. The following example shows how to disable the AnyConnect VPN reconnect if it loses connectivity, and makes the behavior user-controllable:

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



## Note

If you disable Auto Reconnect, AnyConnect does not attempt to reconnect, regardless of the cause of the disconnection.

To configure the behavior in response to a system resume, you must enable Auto Reconnect, even though Auto Reconnect is already enabled by default. Insert the `<AutoReconnectBehavior>` tag inside the `<AutoReconnect>` tag. The following example shows how to enable the AnyConnect VPN reconnect behavior after a system resume, and to make both behaviors user-controllable:

```
<AutoReconnect UserControllable="true">true
<AutoReconnectBehavior
UserControllable="true">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

Table 3-19 shows these tags and default values.

**Table 3-19** *AutoReconnect and AutoReconnectBehavior Client Initialization Tags*

| Tag                   | Default Value <sup>1</sup> | Possible Values <sup>2</sup>                                                                                                                                                                                                                                                                                                                  | User Controllable | User Controllable by Default <sup>3</sup> | OSs Supported     |
|-----------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-------------------------------------------|-------------------|
| AutoReconnect         | true                       | true—Client retains resources assigned to the VPN session if it is disrupted, and attempts to reconnect.<br><br>false—Client releases resources assigned to the VPN session if it is interrupted and does not attempt to reconnect.                                                                                                           | Yes               | No                                        | All               |
| AutoReconnectBehavior | DisconnectOnSuspend        | ReconnectAfterResume—Client retains resources assigned to the VPN session during a system suspend. The client attempts to reconnect after the system resume.<br><br>DisconnectOnSuspend—Client <i>releases</i> resources assigned to the VPN session upon a system suspend. The client does not attempt to reconnect after the system resume. | Yes               | No                                        | Windows<br>Mac OS |

**Note:** Applies only if AutoReconnect is true.

1. AnyConnect uses the default value if the profile does not specify one.
2. Insert the parameter value between the beginning and closing tags; for example, <AutoReconnect>true</AutoReconnect>.
3. The AnyConnect Preferences dialog box displays the parameter values and lets users change them, depending on the value of the associated user control attribute. The user control attribute is optional. If you do not insert it, AnyConnect uses its default value. To permit or deny user control, insert the user control attribute inside the opening tag; for example, <AutoReconnect UserControllable="true">true</AutoReconnect>.

## Installing Host Scan

To reduce the chances of intranet infection by hosts establishing VPN connections, you can configure Host Scan to download and check for antivirus, antispyware, and firewall software; and associated definitions file updates as a condition for the establishment of an AnyConnect session. Host Scan is part of Cisco Secure Desktop (CSD). Although CSD works with AnyConnect, it is a different product and is beyond the scope of this document. To learn about and install CSD, see the [Release Notes for Cisco Secure Desktop](#) and the [Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators](#).

## Configuring a Server List

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 the example AnyConnect profile named AnyConnectProfile.tmpl, which the AnyConnect client automatically downloads to the endpoint.

Table 3-20 lists the ServerList parameters and their values. In this table the referenced tag name is in **bold** type. The values in these examples are only for demonstration purposes. Do not use them in your own configuration.

**Table 3-20** Server List Parameters

| XML Tag Name | Possible Values | Description                                                                                                      | Example                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|-----------------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ServerList   | n/a             | Group identifier                                                                                                 | <pre> &lt;ServerList&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-01&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa01.cisco.com   &lt;/HostAddress&gt;   &lt;/HostEntry&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-02&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa02.cisco.com   &lt;/HostAddress&gt;     &lt;UserGroup&gt;StandardUser&lt;/UserGroup&gt;     &lt;BackupServerList&gt;       &lt;HostAddress&gt;cvc-asa03.cisco.com     &lt;/BackupServerList&gt;   &lt;/HostEntry&gt; &lt;/ServerList&gt; </pre> |
| HostEntry    | n/a             | Group identifier, subordinate to ServerList. This is the data needed to attempt a connection to a specific host. | <pre> &lt;ServerList&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-01&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa01.cisco.com   &lt;/HostAddress&gt;   &lt;/HostEntry&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-02&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa02.cisco.com   &lt;/HostAddress&gt;     &lt;UserGroup&gt;StandardUser&lt;/UserGroup&gt;     &lt;BackupServerList&gt;       &lt;HostAddress&gt;cvc-asa03.cisco.com     &lt;/BackupServerList&gt;   &lt;/HostEntry&gt; &lt;/ServerList&gt; </pre> |

Table 3-20 Server List Parameters (continued)

| XML Tag 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.                                                                                                                                                                         | <pre> &lt;ServerList&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-01&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa01.cisco.com   &lt;/HostAddress&gt;   &lt;/HostEntry&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-02&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa02.cisco.com   &lt;/HostAddress&gt;     &lt;UserGroup&gt;StandardUser&lt;/UserGroup&gt;     &lt;BackupServerList&gt;       &lt;HostAddress&gt;cvc-asa03.cisco.com     &lt;/HostAddress&gt;     &lt;/BackupServerList&gt;   &lt;/HostEntry&gt; &lt;/ServerList&gt; </pre> |
| 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.                                                                                                                                                                                                                          | <pre> &lt;ServerList&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-01&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa01.cisco.com   &lt;/HostAddress&gt;   &lt;/HostEntry&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-02&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa02.cisco.com   &lt;/HostAddress&gt;     &lt;UserGroup&gt;StandardUser&lt;/UserGroup&gt;     &lt;BackupServerList&gt;       &lt;HostAddress&gt;cvc-asa03.cisco.com     &lt;/HostAddress&gt;     &lt;/BackupServerList&gt;   &lt;/HostEntry&gt; &lt;/ServerList&gt; </pre> |
| UserGroup    | The tunnel group to use when connecting to the specified host. This parameter is optional.                                                         | <p>Within the ServerList group, the UserGroup, parameter, if present, is used in conjunction with HostAddress to form a Group-based URL. If you use this option in the profile, the corresponding tunnel group must have a group-url defined as well.</p> <p><b>Note</b> Group based URL support requires ASA version 8.0.3, or later.</p> | <pre> &lt;ServerList&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-01&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa01.cisco.com   &lt;/HostAddress&gt;   &lt;/HostEntry&gt;   &lt;HostEntry&gt;     &lt;HostName&gt;ASA-02&lt;/HostName&gt;     &lt;HostAddress&gt;cvc-asa02.cisco.com   &lt;/HostAddress&gt;     &lt;UserGroup&gt;StandardUser&lt;/UserGroup&gt;     &lt;BackupServerList&gt;       &lt;HostAddress&gt;cvc-asa03.cisco.com     &lt;/HostAddress&gt;     &lt;/BackupServerList&gt;   &lt;/HostEntry&gt; &lt;/ServerList&gt; </pre> |

# Split DNS Fallback

If the group policy on the security appliance specifies the names of the domains to be tunneled, AnyConnect Client tunnels only DNS queries that match those domains. It refuses all other DNS queries. The DNS resolver receives the refusal from the client and retries, this time using the public interface instead of AnyConnect Client.

This feature requires that you:

- Configure at least one DNS server
- Enable split-tunneling

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

## Scripting

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

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

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

Some examples that show how you might want to use this feature include:

- Refreshing the group policy upon VPN connection.
- Mapping a network drive upon VPN connection, and un-mapping it after disconnection.
- Logging on to a service upon VPN connection, and logging off after disconnection.

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



### Note

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

## Scripting Requirements and Limitations

AnyConnect runs up to one OnConnect and up to one OnDisconnect script, but these scripts may launch other scripts.

AnyConnect does not require the script to be written in a specific language, but does require an application that can run the script to be installed on the client computer. Thus, for AnyConnect to launch the script, the script must be capable of running from the command line.

AnyConnect supports script launching on all Microsoft Windows, Mac OS X, and Linux platforms supported by AnyConnect. Microsoft Windows Mobile does not provide native support for scripting languages; however, you can create and automatically run an OnConnect application and an OnDisconnect application as long as it complies with the AnyConnect scripting filename prefix and directory requirements.

On Microsoft Windows, AnyConnect can only launch scripts after the user logs onto Windows and establishes a VPN session. Thus, the restrictions imposed by the user's security environment apply to these scripts; scripts can only execute functions that the user has rights to invoke. AnyConnect hides the cmd window during the execution of a script on Windows, so executing a script to display a message in a .bat file for testing purposes does not work.

AnyConnect supports script launching during WebLaunch and standalone launches.

By default, AnyConnect does not launch scripts. Use the AnyConnect profile EnableScripting parameter to enable scripts. AnyConnect does not require the presence of scripts if you do so.

Client GUI termination does not necessarily terminate the VPN session; the OnDisconnect script runs after session termination.

Other requirements apply, as indicated in the next section.

## Writing, Testing, and Deploying Scripts

Deploy AnyConnect scripts as follows:

---

**Step 1** Write and test the script using the OS type on which it will run when AnyConnect launches it.



**Note** Scripts written on Microsoft Windows computers have different line endings than scripts written on Mac OS and Linux. Therefore, you should write and test the script on the targeted OS. If a script cannot run properly from the command line on the native OS, AnyConnect cannot run it properly either.

---

**Step 2** Do one of the following to deploy the scripts:

- Use ASDM to import the script as a binary file to the security appliance. Go to Network (Client) Access > AnyConnect Customization/Localization > Script.



**Note** Microsoft Windows Mobile does not support this option. You must deploy scripts using the manual method for this OS.

---

If you use ASDM version 6.3.1 or later, the security appliance adds the prefix *scripts\_* and the prefix *OnConnect* or *OnDisconnect* to your filename to identify the file as a script. When the client connects, the security appliance downloads the script to the proper target directory on the remote

computer, removing the *scripts\_* prefix and leaving the remaining *OnConnect* or *OnDisconnect* prefix. For example, if you import the script *myscript.bat*, the script appears on the security appliance as *scripts\_OnConnect\_myscript.bat*. On the remote computer, the script appears as *OnConnect\_myscript.bat*.

If you use an ASDM version earlier than 6.3.1, you must import the scripts with the following prefixes:

- *scripts\_OnConnect*
- *scripts\_OnDisconnect*

To ensure the scripts run reliably, configure all security appliances to deploy the same scripts. If you want to modify or replace a script, use the same name as the previous version and assign the replacement script to all of the security appliances that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- Or transfer the scripts manually to the VPN endpoints on which you want to run the them.

If you use this method, use the script filename prefixes below.

- *OnConnect*
- *OnDisconnect*

Install the scripts in the directory shown in [Table 3-21](#).

**Table 3-21 Required Script Locations**

| OS                                                                                     | Directory                                                                   |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Microsoft Windows 7 and Vista                                                          | %ALLUSERSPROFILE%\Cisco\Cisco AnyConnect VPN Client\Script                  |
| Microsoft Windows XP                                                                   | %ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect VPN Client\Script |
| Linux<br>(On Linux, assign execute permissions to the file for User, Group and Other.) | /opt/cisco/vpn/script                                                       |
| Mac OS X                                                                               | /opt/cisco/vpn/script                                                       |
| Windows Mobile                                                                         | %PROGRAMFILES%\Cisco AnyConnect VPN Client\Script                           |

## Configuring the AnyConnect Profile for Scripting

To enable scripting you must insert the `EnableScripting` parameter into the AnyConnect profile.

[Table 3-22](#) describes the scripting parameters you can insert into the AnyConnect profile. Examples follow the table.

**Table 3-22**      *Scripting Parameters*

| Name                         | Possible Values and Descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EnableScripting              | <p>true—Launches OnConnect and OnDisconnect scripts if present.</p> <p>false—(Default) Does not launch scripts.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| UserControllable             | <p><b>Note:</b> If used, this parameter must be embedded within the EnableScripting tag, as shown in the second example below this table.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> <li>• true—Lets users enable or disable the running of OnConnect and OnDisconnect scripts.</li> <li>• false—(Default) Prevents users from controlling the scripting feature.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| TerminateScriptOnNextEvent   | <p>This parameter has meaning only if the EnableScripting is set to true.</p> <p><b>Note:</b> If used, this parameter must be embedded within the EnableScripting tag, as shown in the second example below this table.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> <li>• true—Terminates a running script process if a transition to another scriptable event occurs. For example, AnyConnect terminates a running OnConnect script if the VPN session ends, and terminates a running OnDisconnect script if AnyConnect starts a new VPN session. On Microsoft Windows, AnyConnect also terminates any scripts that the OnConnect or OnDisconnect script launched, and all their script descendents. On Mac OS and Linux, AnyConnect terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts.</li> <li>• false—(Default) Does not terminate a script process if a transition to another scriptable event occurs.</li> </ul> |
| EnablePostSBLOnConnectScript | <p>This parameter has meaning only if the EnableScripting is set to true, and only if the VPN endpoint is running Microsoft Windows 7, XP, or Vista.</p> <p><b>Note:</b> If used, this parameter must be embedded within the EnableScripting tag, as shown in the second example below this table.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> <li>• false—Prevents launching of the OnConnect script if SBL establishes the VPN session.</li> <li>• true—(Default) Launches the OnConnect script if present if SBL establishes the VPN session.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                    |

Insert these parameters anywhere inside the `ClientInitialization` section of the AnyConnect profile. This example enables scripting and uses the default values for the other scripting parameters:

```
<ClientInitialization>
 <EnableScripting>true</EnableScripting>
```

```
</ClientInitialization>
```

This example enables scripting and overrides the default values for the other scripting parameters:

```
<ClientInitialization>

<EnableScripting UserControllable="true">true
 <TerminateScriptOnNextEvent>true</TerminateScriptOnNextEvent>
 <EnablePostSBLOnConnectScript>false</EnablePostSBLOnConnectScript>
</EnableScripting>

</ClientInitialization>
```

**Note**

Be sure to add the AnyConnect profile to the security appliance group policy to download it to the VPN endpoint.

## Troubleshooting Scripts

If a script fails to run, try resolving the problem as follows:

- 
- Step 1** Make sure the script has an `OnConnect` or `OnDisconnect` prefix name. [Table 3-22](#) shows the required scripts directory for each OS.
  - Step 2** Try running the script from the command line. AnyConnect cannot run the script if it cannot run from the command line. If the script fails to run on the command line, make sure the application that runs the script is installed, and try rewriting the script on that OS.
  - Step 3** Make sure the scripts directory on the VPN endpoint contains only one `OnConnect` and only one `OnDisconnect` script. If one security appliance downloads one `OnConnect` script and during a subsequent connection a second security appliance downloads an `OnConnect` script with a different filename suffix, AnyConnect might run the unwanted script. If the script path contains more than one `OnConnect` or `OnDisconnect` script and you are using binary AnyConnect customization to deploy scripts, remove the contents of the scripts directory and re-establish an AnyConnect VPN session. If the script path contains more than one `OnConnect` or `OnDisconnect` script and you are using the manual deployment method, remove the unwanted scripts and re-establish an AnyConnect VPN session.
  - Step 4** If the OS is Linux, make sure the script file permissions are set to execute.
  - Step 5** Make sure the AnyConnect profile includes the `EnableScripting` parameter set to true.
-

# Proxy Support

The following sections describe how to use the proxy support features.

## Ignore Proxy

This feature lets you specify a policy in the AnyConnect profile to bypass the Internet Explorer proxy configuration settings on the user's PC. It is useful when the proxy configuration prevents the user from establishing a tunnel from outside the corporate network.

To enable Ignore Proxy, insert the following line into the <ClientInitialization> section of the AnyConnect profile:

```
<ProxySettings>IgnoreProxy</ProxySettings>
```



### Note

AnyConnect currently supports only the IgnoreProxy setting; it does not support the Native and Override settings in the new ProxySettings section within the <ClientInitialization> section of the XML schema (AnyConnectProfile.xsd).

## Private Proxy

You can configure a group policy to download private proxy settings configured in the group policy to the browser after the tunnel is established. The settings return to their original state after the VPN session ends.

## Private Proxy Requirements

An AnyConnect Essentials license is the minimum ASA license activation requirement for this feature.

AnyConnect supports this feature on computers running:

- Internet Explorer on Windows
- Safari on Mac OS

## Configuring a Group Policy to Download a Private Proxy

To configure the proxy settings, establish an ASDM session with the security appliance and choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Advanced > Browser Proxy**. ASDM versions earlier than 6.3(1) show this option as **IE Browser Proxy**; however, AnyConnect no longer restricts the configuration of the private proxy to Internet Explorer, regardless of the ASDM version you use.

The Do not use proxy parameter, if enabled, removes the proxy settings from the browser for the duration of the session.

## Internet Explorer Connections Tab Lockdown

Under certain conditions, AnyConnect hides the Internet Explorer Tools > Internet Options > Connections tab. When exposed, this tab lets the user set proxy information. Hiding this tab prevents the user from intentionally or unintentionally circumventing the tunnel. The tab lockdown is reversed on disconnect, and it is superseded by any administrator-defined policies regarding that tab. The conditions under which this lockdown occurs are either of the following:

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

## Proxy Auto-Configuration File Generation for Clientless Support

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

## Allow AnyConnect Session from an RDP Session for Windows Users

Some customers require the ability to log on to a client PC using Windows Remote Desktop and create a VPN connection to a secure gateway from within the Remote Desktop (RDP) session. This feature allows a VPN session to be established from an RDP session. A split tunneling VPN configuration is required for this to function correctly. For information about split tunneling, see *Cisco ASDM User Guide* or *Cisco ASA 5500 Series Command Line Configuration Guide Using the CLI*.

By default, a locally logged-in user can establish a VPN connection only when no other local user is logged in. The VPN connection is terminated when the user logs out, and additional local logons during a VPN connection result in the connection being torn down. Remote logons and logoffs during a VPN connection are unrestricted.

**Note**

With this feature, the AnyConnect client disconnects the VPN connection when the user who established the VPN connection logs off. If the connection is established by a remote user, and that remote user logs off, the VPN connection is terminated.

The AnyConnect profile settings determine how Windows logons are treated at connection establishment and during the connection. These preferences are configurable only by the network administrator. They let customers configure the client to allow VPN connection establishment from an RDP session. The end-user does not see any changes in the AnyConnect client GUI as a result of this feature. [Table 3-23](#) shows the preferences.

**Table 3-23** Windows Logon Preferences

XML Tag Name	Possible Values (Defaults in Bold)
WindowsLogonEnforcement	<p><b>SingleLocalLogon</b>—Allows only one local user to be logged on during the entire VPN connection. With this setting, a local user can establish a VPN connection while one or more remote users are logged on to the client PC, but if the VPN connection is configured for all-or-nothing tunneling, then the remote logon is disconnected because of the resulting modifications of the client PC routing table for the VPN connection. If the VPN connection is configured for split-tunneling, the remote logon might or might not be disconnected, depending on the routing configuration for the VPN connection. The SingleLocalLogin setting has no effect on remote user logons from the enterprise network over the VPN connection.</p> <p><b>SingleLogon</b>—Allows only one user to be logged on during the entire VPN connection. If more than one user is logged on, either locally or remotely, when the VPN connection is being established, the connection is not allowed. If a second user logs on, either locally or remotely, during the VPN connection, the VPN connection is terminated.</p> <p>When you select the SingleLogon setting, no additional logons are allowed during the VPN connection, so a remote logon over the VPN connection is not possible.</p>
WindowsVPNEstablishment	<p>Determines the behavior of the AnyConnect client when a user who is remotely logged on to the client PC establishes a VPN connection. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>LocalUsersOnly</b>—Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of the AnyConnect client.</li> <li>• <b>AllowRemoteUsers</b>—Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection is terminated to allow the remote user to regain access to the client PC.</li> </ul> <p>Remote users must wait 90 seconds after VPN establishment if they want to disconnect their remote login session without causing the VPN connection to be terminated.</p> <p>On Vista, the WindowsVPNEstablishment profile setting is not currently enforced during Start Before Logon (SBL). The AnyConnect client does not determine whether the VPN connection is being established by a remote user before logon; therefore, a remote user can establish a VPN connection via SBL even when the WindowsVPNEstablishment setting is LocalUsersOnly.</p>

## AnyConnect over L2TP or PPTP

ISPs in some countries, including Israel, require support of the L2TP and PPTP tunneling protocols.

To send traffic destined for the secure gateway over a PPP connection, AnyConnect uses the point-to-point adapter generated by the external tunnel. When establishing a VPN tunnel over a PPP connection, AnyConnect must exclude traffic destined for the ASA from the tunneled traffic intended for destinations beyond the ASA. To specify whether and how to determine the exclusion route, use the PPPEXclusion configuration option.

The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI.

The following sections describe how to set up PPP exclusion:

- [Configuring AnyConnect over L2TP or PPTP](#)
- [Instructing Users to Override PPP Exclusion](#)

## Configuring AnyConnect over L2TP or PPTP

By default, PPP Exclusion is disabled. To enable PPP exclusion, insert the **PPPEXclusion** line shown below in bold into the `<ClientInitialization>` section of the AnyConnect profile (*anyfilename.xml*):

```
<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>
 <PPPEXclusion UserControllable="true">Automatic</PPPEXclusion>
 </ClientInitialization>
 <ServerList>
 <HostEntry>
 <HostName>DomainNameofASA</HostName>
 <HostAddress>IPaddressOfASA</HostAddress>
 </HostEntry>
 </ServerList>
</AnyConnectProfile>
```

The **PPPEXclusion UserControllable** value **true** lets users read and change the PPP exclusion settings. If you want to prevent users from viewing and changing the PPP exclusion settings, change it to **false**.

AnyConnect supports the following **PPPEXclusion** values:

- **Automatic**—Enables PPP exclusion. AnyConnect automatically uses the IP address of the PPP server. Instruct users to change the value only if automatic detection fails to get the IP address.
- **Override**—Also enables PPP exclusion. If automatic detection fails to get the IP address of the PPP server, and the **PPPEXclusion UserControllable** value is true, instruct users to follow the instructions in the next section to use this setting.
- **Disabled**—PPP exclusion is not applied.

To let users view and change the IP address of the security appliance used for PPP exclusion, add the **PPPEXclusionServerIP** tag with its **UserControllable** value set to true, as shown in bold below:

```
<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>
 <PPPEXclusion UserControllable="true">Automatic</PPPEXclusion>
 <PPPEXclusionServerIP UserControllable="true"></PPPEXclusionServerIP>
 </ClientInitialization>
 <ServerList>
 <HostEntry>
 <HostName>SecureGatewayName</HostName>
 <HostAddress>SecureGatewayName.domain</HostAddress>
 </HostEntry>
 </ServerList>
</AnyConnectProfile>
```

## Instructing Users to Override PPP Exclusion

If automatic detection does not work, and the PPPEXclusion UserControllable value is true, instruct the user to manually override PPP exclusion, as follows:

---

**Step 1** Use an editor such as Notepad to open the preferences XML file.

This file is on one of the following paths on the user's computer:

- Windows: %LOCAL\_APPDATA%\Cisco\Cisco AnyConnect VPN Client\preferences.xml.  
For example,
  - Windows Vista—C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml
  - Windows XP—C:\Documents and Settings\username\Local Settings\Application Data\Cisco\Cisco AnyConnect VPN Client\preferences.xml
- Mac OS X: /Users/username/.anyconnect
- Linux: /home/username/.anyconnect

**Step 2** Insert the PPPEXclusion details under <ControllablePreferences>, while specifying the Override value and the IP address of the PPP server. The address must be a well-formed IPv4 address. For example:

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPEXclusion>Override
<PPPEXclusionServerIP>192.168.22.44</PPPEXclusionServerIP></PPPEXclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

**Step 3** Save the file.

**Step 4** Exit and restart AnyConnect.

---

# Configuring Other AnyConnect Profile Settings

Table 3-24 shows the default values and possible values for other parameters you can insert into the ClientInitialization section of the AnyConnect Client profile (.xml file).

**Table 3-24** Other AnyConnect Client Initialization Tags

XML Tag Name	Default Value <sup>1</sup>	Possible Values <sup>2</sup>	User Controllable <sup>3</sup>	User Controllable by Default <sup>4</sup>	OSs Supported
CertificateStoreOverride	false	true, false	No	n/a	All
ShowPreConnectMessage	false	true, false	No	n/a	All
MinimizeOnConnect	true	true, false	Yes	Yes	All
LocalLanAccess	false	true, false	Yes	Yes	All
AutoUpdate	true	true, false	Yes	No	All
RSASecurIDIntegration <sup>5</sup>	Automatic	Automatic SoftwareToken HardwareToken	Yes	No	Windows

1. AnyConnect uses the default value if the profile does not specify one.
2. Insert the parameter value between the beginning and closing tags; for example, `<CertificateStoreOverride>true</CertificateStoreOverride>`.
3. Anyconnect ignores the `usercontrollable="true"` string if the parameter does not support user control.
4. The AnyConnect Preferences dialog box displays the parameter values and lets users change them, depending on the value of the associated user control attribute. The user control attribute is optional. If you do not insert it, AnyConnect uses its default value. To permit or deny user control, insert the user control attribute inside the opening tag; for example, `<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>`.
5. 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.





## CHAPTER 4

# Fulfilling Other Administrative Requirements for AnyConnect

---

This chapter provides the following instructions:

- [Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users, page 4-1](#)
- [Configuring CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop, page 4-2](#)

## 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. 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 and click New.
  - Step 5** Type a name for the new Group Policy Object and press Enter.
  - Step 6** 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 7** Click Edit and choose User Configuration > Windows Settings > Internet Explorer Maintenance > Security.

- 
- Step 8** Right-click Security Zones and Content Ratings in the right-hand pane, then click Properties.
- Step 9** Select Import the current security zones and privacy settings. If prompted, click Continue.
- Step 10** Click Modify Settings, select Trusted Sites, and click Sites.
- Step 11** 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](https://*.mycompany.com)).
- Step 12** Click Close and click OK continually until all dialog boxes close.
- Step 13** Allow sufficient time for the policy to propagate throughout the domain or forest.
- Step 14** Click OK in the Internet Options window.
- 

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

If your remote users have Cisco Security Agent (CSA) installed, you must import 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 5

# Managing Authentication

---

This chapter explains these subjects and tasks:

- [SDI Token \(SoftID\) Integration, page 5-1](#)
- [Comparing Native SDI with RADIUS SDI, page 5-1](#)
- [Using SDI Authentication, page 5-2](#)
- [Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client, page 5-6](#)

## SDI Token (SoftID) Integration

Cisco AnyConnect VPN Client, Release 2.1 and higher, integrates support for RSA SecurID client software running on Windows XP. 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 [on page 5-9](#)) 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.

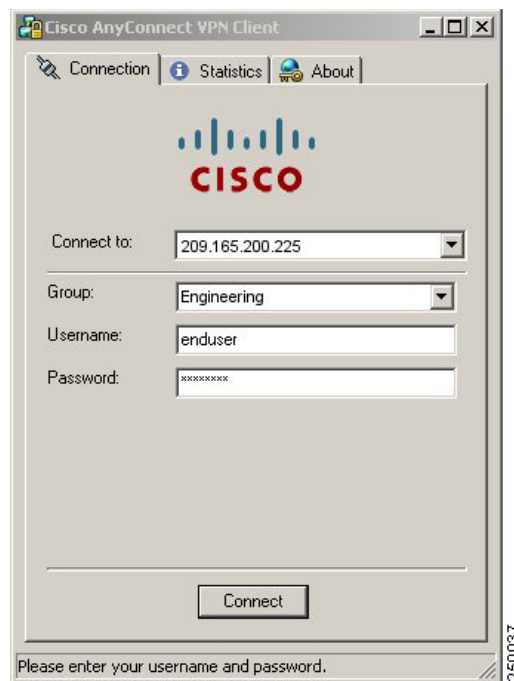
When a remote user using RADIUS SDI authentication connects to the security appliance with the AnyConnect VPN client and attempts to authenticate using an RSA SecurID token, the security appliance communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

For more information about configuring the ASA to ensure AnyConnect client compatibility, see [Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client, page 5-6](#).

## Using SDI Authentication

The login (challenge) dialog box matches 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 5-1](#).

**Figure 5-1** Username/Password Authentication Login Dialog Box



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.

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 5-2 on page 5-3](#).

**Figure 5-2** PIN and Passcode Dialog Boxes



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.

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.

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 5-6.

### 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. 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 5-3 on page 5-5](#)). The PIN must be a number from 4 to 8 digits long.

**Figure 5-3**      **Creating a New PIN**



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.

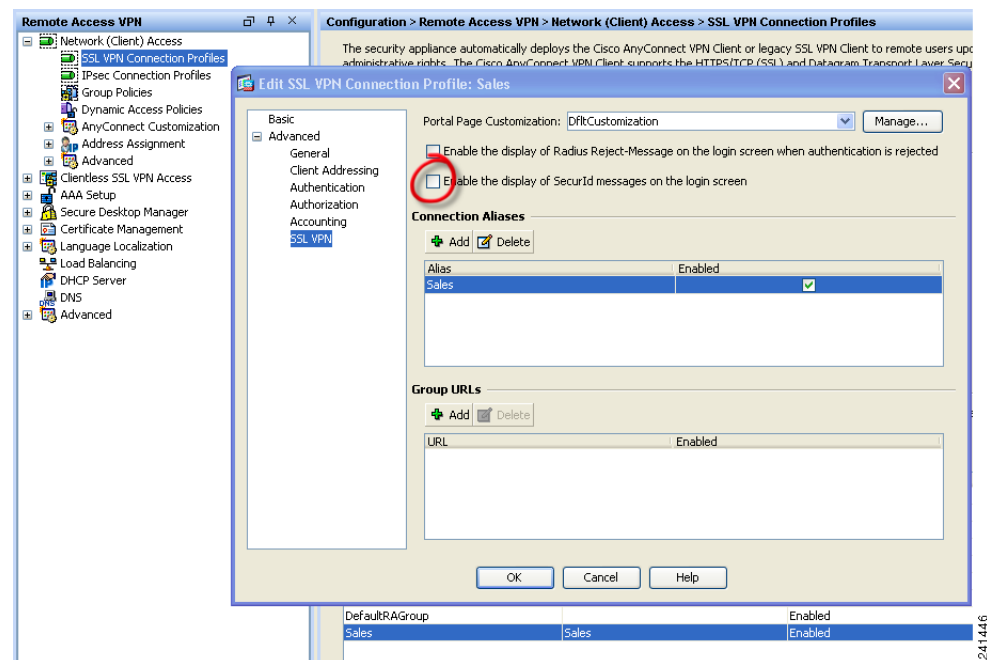
## Configuring the Security Appliance to Support RADIUS/SDI Messages

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.

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.

- Step 1** Go to Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles. The Edit SSL VPN Connection Profile window displays (Figure 5-4).

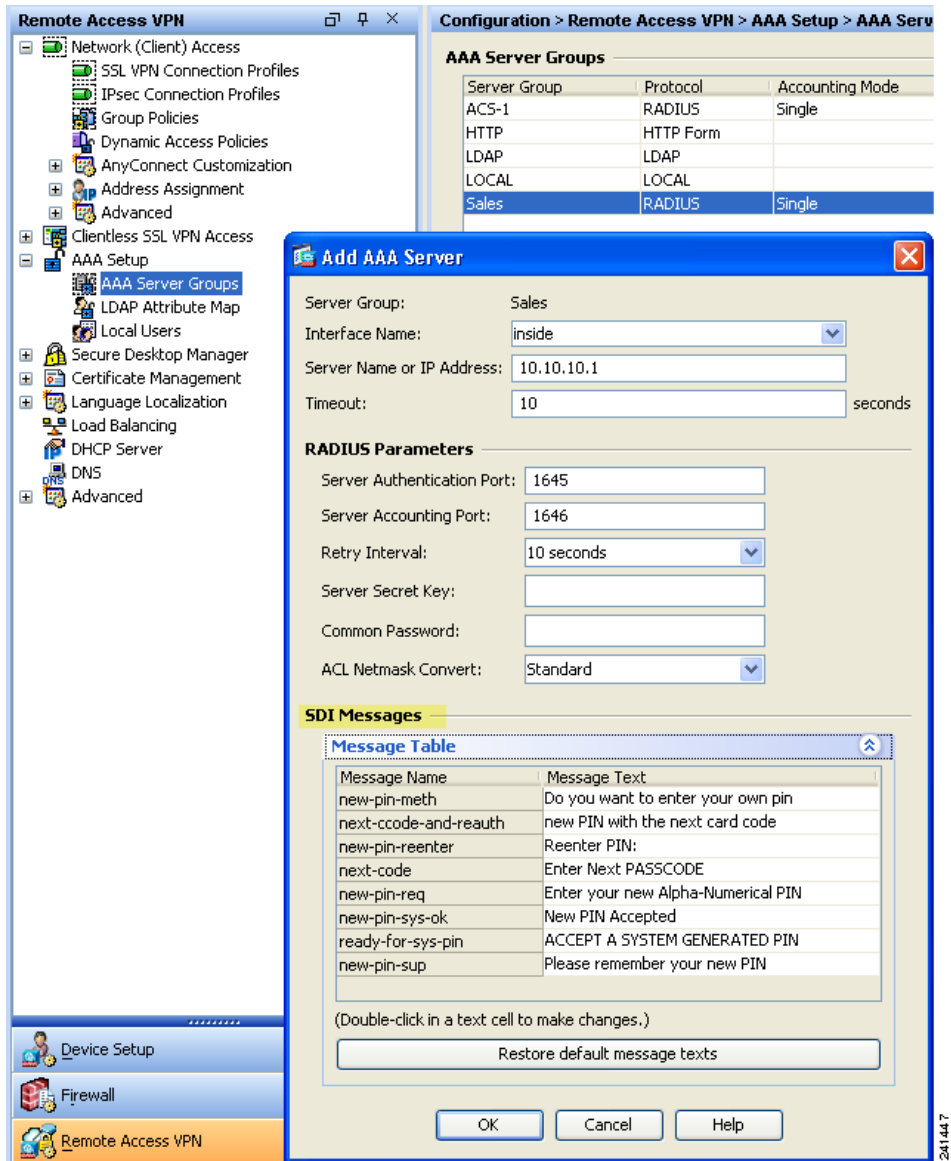
**Figure 5-4** Edit SSL VPN Connection Profile Screen



- Step 2** Check **Enable the display of SecurID messages on the login screen**.

- Step 3** Choose Configuration > Remote Access VPN > AAA Server Groups. The Add AAA Server window opens (Figure 5-5).

Figure 5-5 Configuring RADIUS SDI Messages



- Step 4** 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. 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 5-1 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 5-1** *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.





## CHAPTER 6

# 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, page 6-1](#)
- [Changing the Default AnyConnect English Messages, page 6-12](#)
- [Localizing the AnyConnect Client GUI and Installer, page 6-14](#)

## 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 computers.



**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 computers 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 6-2](#)
- [Deploying Executables That Use the Client API, page 6-3](#)
- [Customizing the GUI with a Transform, page 6-5](#)
- [Information for Creating your Custom Icons and Logos, page 6-8](#)

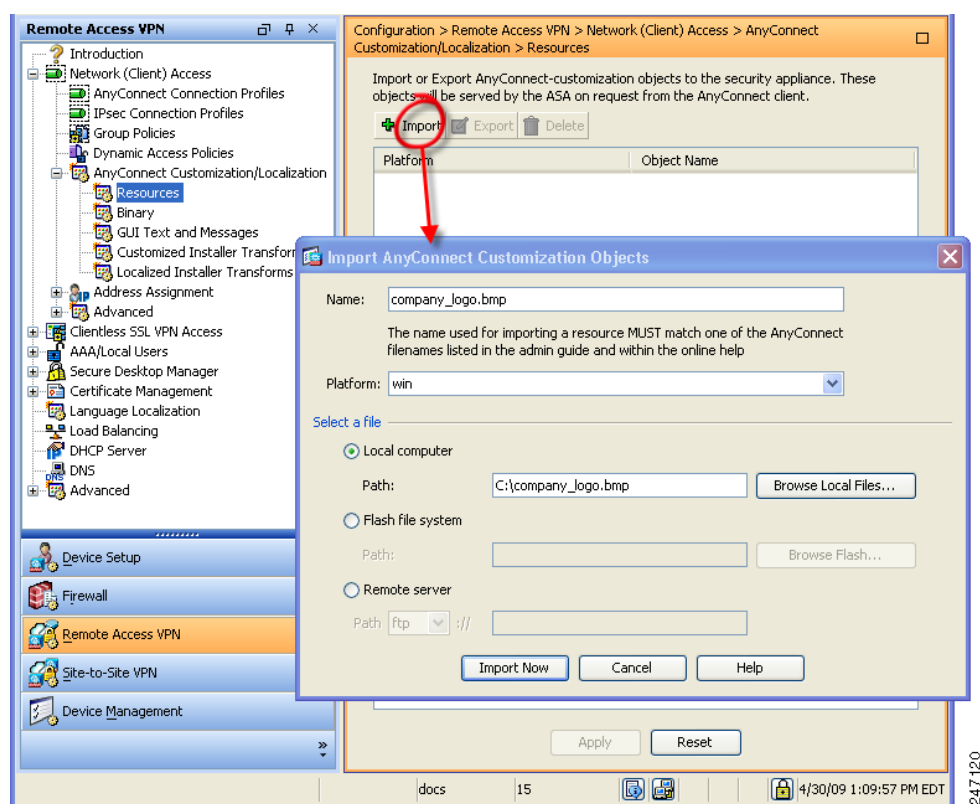
## Replacing Individual GUI Components with your Custom Components

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 6-2, Table 6-3, and Table 6-4 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 6-1).

**Figure 6-1** Importing a Customization Object



- Step 2** Enter the Name of the file to import. See Table 6-2, Table 6-3, and Table 6-4 for the filenames of all the GUI components that you can replace.

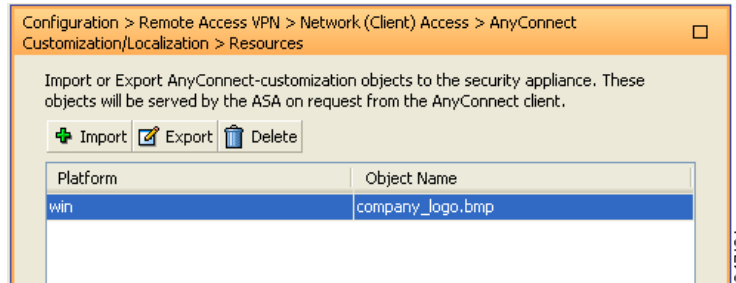


### Note

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. However, if you deploy your own executable to customize the GUI, the executable can call resource files using any filename.

- Step 3** Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table (Figure 6-2).

**Figure 6-2** The Imported file displays in the Table



**Note**

If you import an image as a resource file (such as company\_logo.bmp), the image you import customizes the AnyConnect client until you reimport another image using the same filename. For example, if you replace company\_logo.bmp with a custom image, and then delete the image, the client continues to display your image until you import a new image (or the original Cisco logo image) using the same filename.

## Deploying Executables That Use the Client API

For Windows, Linux, or Mac (PPC or Intel-based) computers, 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 6-1 lists the filenames of the client executable files for the different operating systems.

**Table 6-1** Filenames of Client Executables

Client OS	Client GUI File	Client CLI File
Windows	vpnui.exe	vpnccli.exe
Linux	vpnui	vpn
Mac	Not supported <sup>1</sup>	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.

Your executable can call any resource files, such as logo images, that you import to the security appliance (See Figure 6-1). Unlike replacing the pre-defined GUI components, when you deploy your own executable, can use any filenames for your resource files.

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:

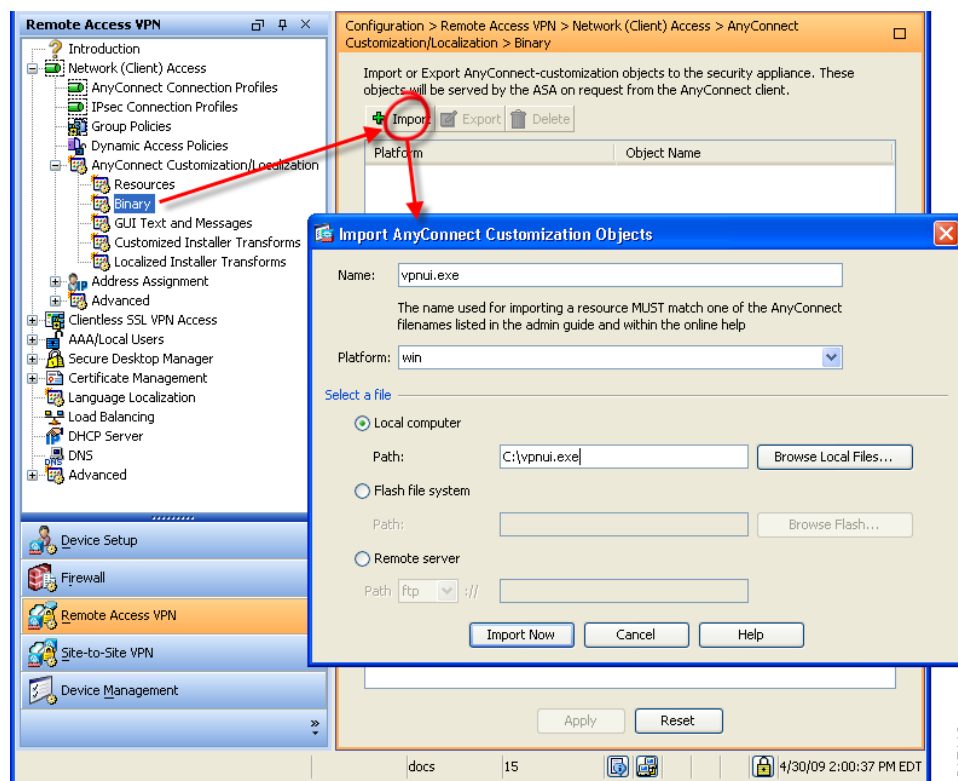
- **Web-Launch**—The clientless portal is available and the user can authenticate. However, the behavior surrounding tunnel establishment does not work as expected. Having an unsigned GUI on the client results in the client not starting as part of the clientless connection attempt. And once it detects 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 6-1).

**Figure 6-3** Importing an Executable

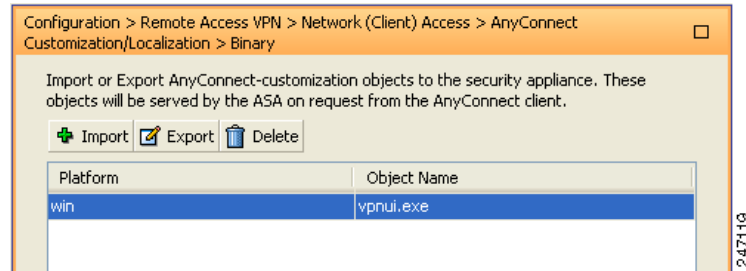


**Step 2** Enter the Name of the file to import.

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 *vpnu.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 6-2).

**Figure 6-4** The Imported Executable appears in the table



## 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](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:

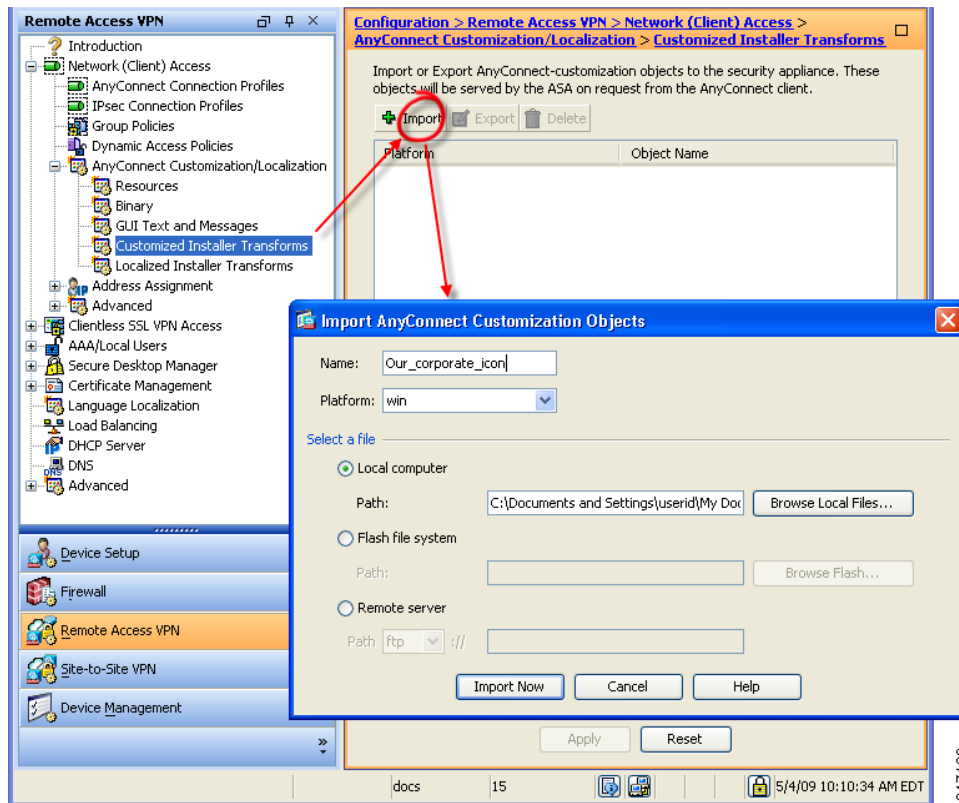
C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi.

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 window displays (Figure 6-5).

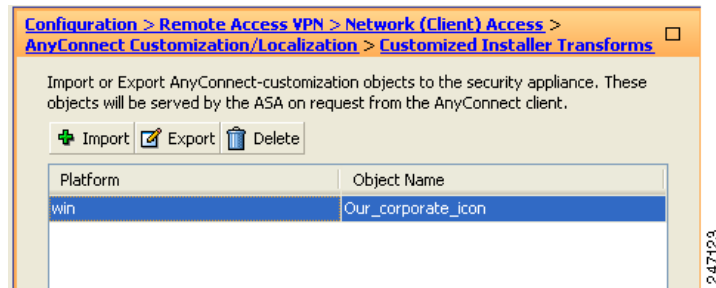
**Figure 6-5** Importing a Customizing Transform



- 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 6-6).



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

**Figure 6-6** The Customizing Transform Appears in the Table

## 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 6-2](#) 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 6-2** *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 6-2** *Icon Files for AnyConnect Client for Windows (continued)*

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 6-3](#) lists the files that you can replace and the client GUI area affected.

**Table 6-3** *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 6-3** *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
vpnuui48.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 6-4](#) lists the files that you can replace and the client GUI area affected.

**Table 6-4** *Icon Files for AnyConnect Client for 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 6-4** *Icon Files for AnyConnect Client for 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

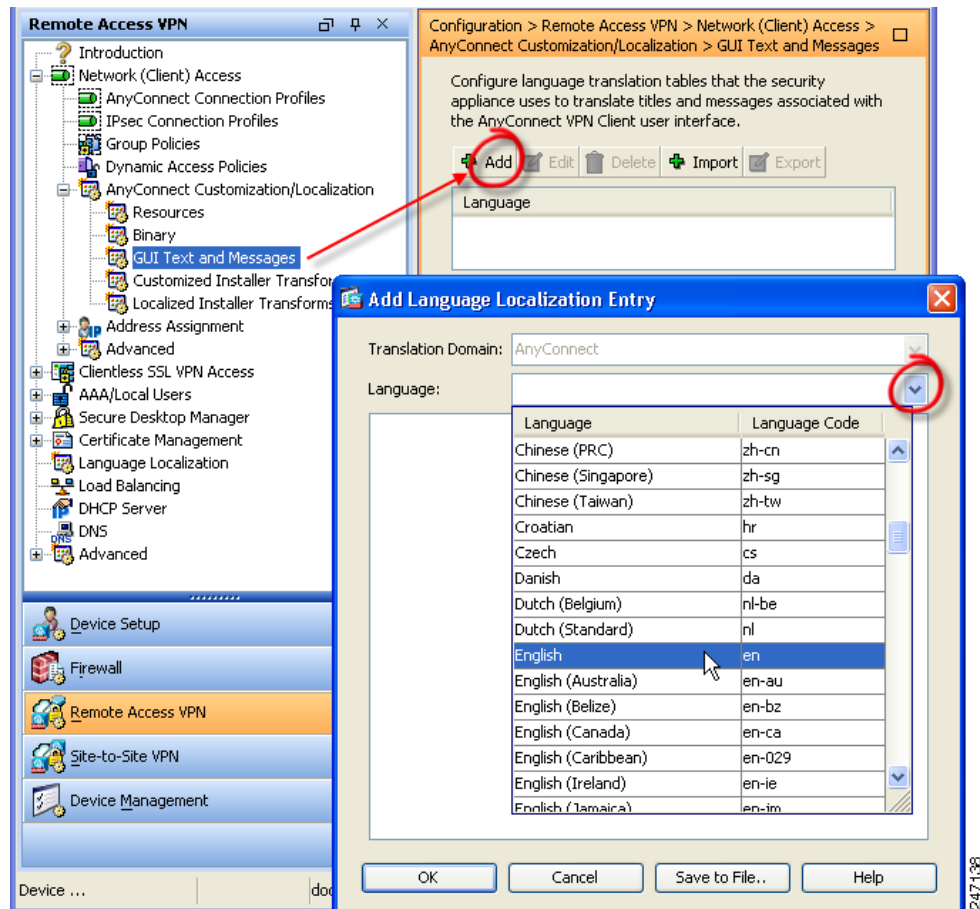
# Changing the Default AnyConnect English Messages

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 6-9).

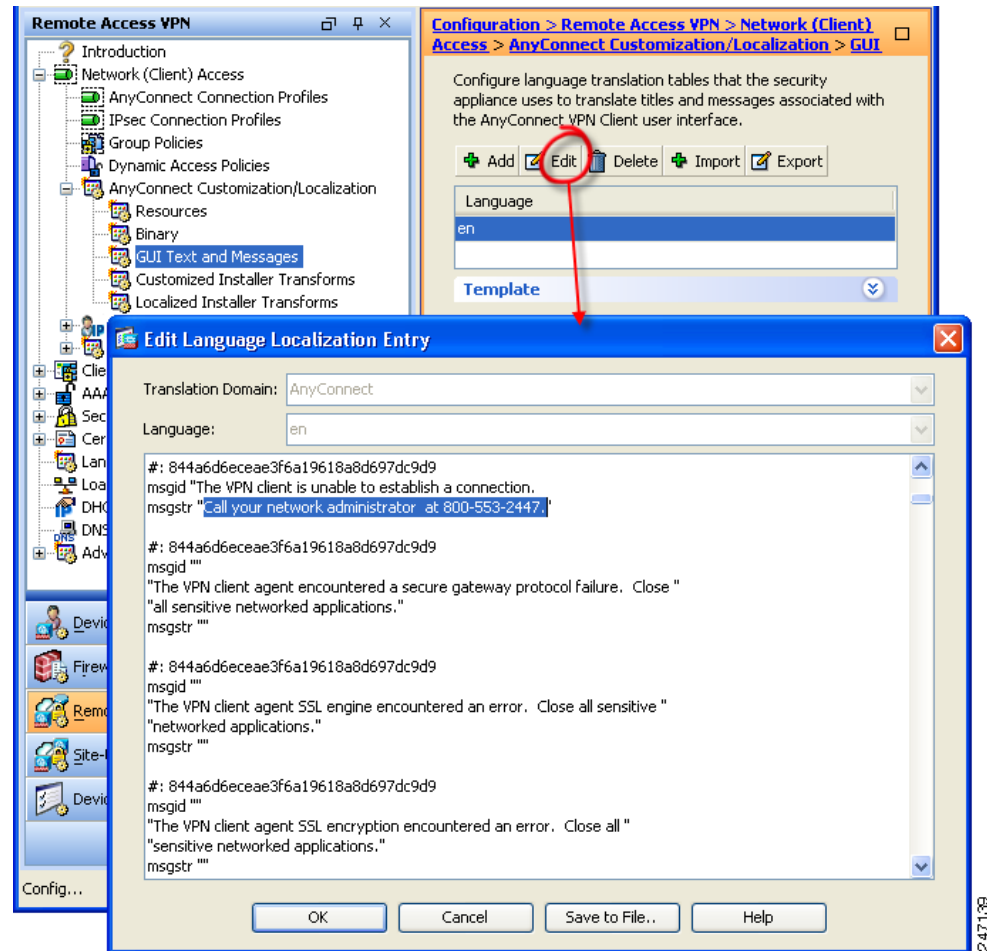
**Figure 6-7 Adding an English Translation Table**



- 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 6-8). 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. Insert your own text between the quotes of the msgstr.

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

**Figure 6-8** Editing the Message Text



- Step 4** Click **Ok**, and then **Apply** in the GUI Text and Messages pane to save your 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:

- [Localizing the AnyConnect GUI, page 6-14](#)
- [Localizing the AnyConnect Installer Screens, page 6-22](#)
- [Using Tools to Create Message Catalogs for Enterprise Deployment, page 6-25](#)
- [Merging a Newer Translation Template with your Translation Table, page 6-25](#)

## 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.

When the remote user connects to the security appliance and downloads the client, the client detects the preferred language of the computer and applies the appropriate translation table. The client detects the locale specified during installation of the operating system. If you update the translation table on the security appliance, the translated messages are not updated until the client is restarted and makes another successful connection.

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 computer. See [Using Tools to Create Message Catalogs for Enterprise Deployment, page 6-25](#) for more information.

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

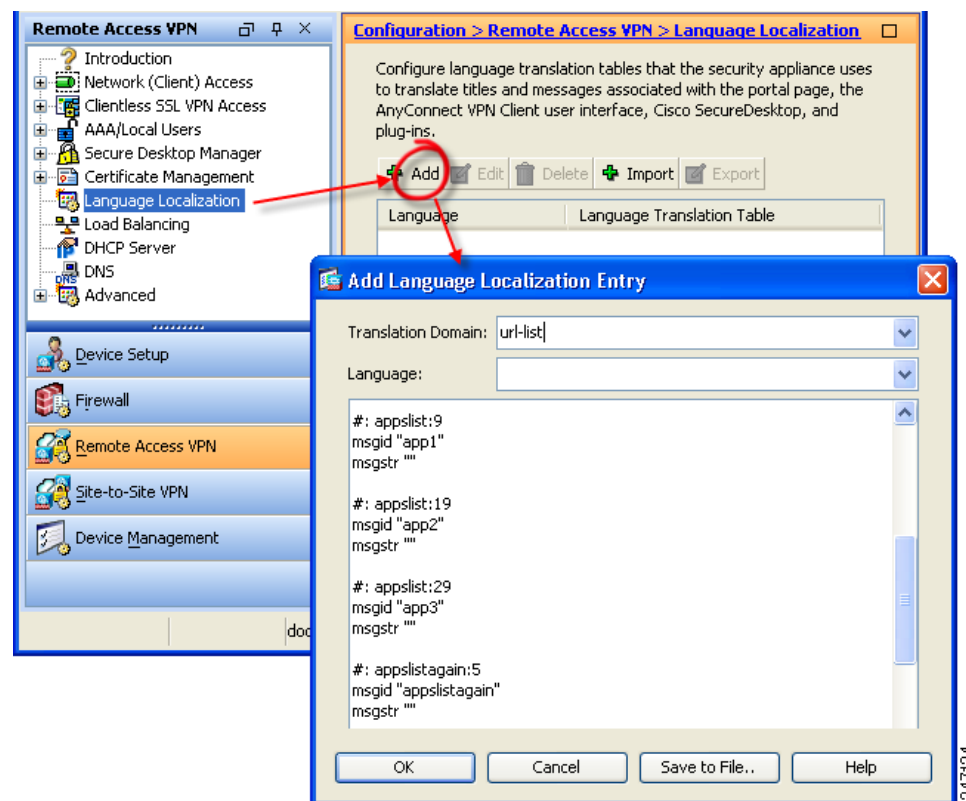
- [Translating using the ASDM Translation Table Editor, page 6-15](#)
- [Translating by Exporting the Translation Table for Editing, page 6-19](#)

## Translating using the ASDM Translation Table Editor

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

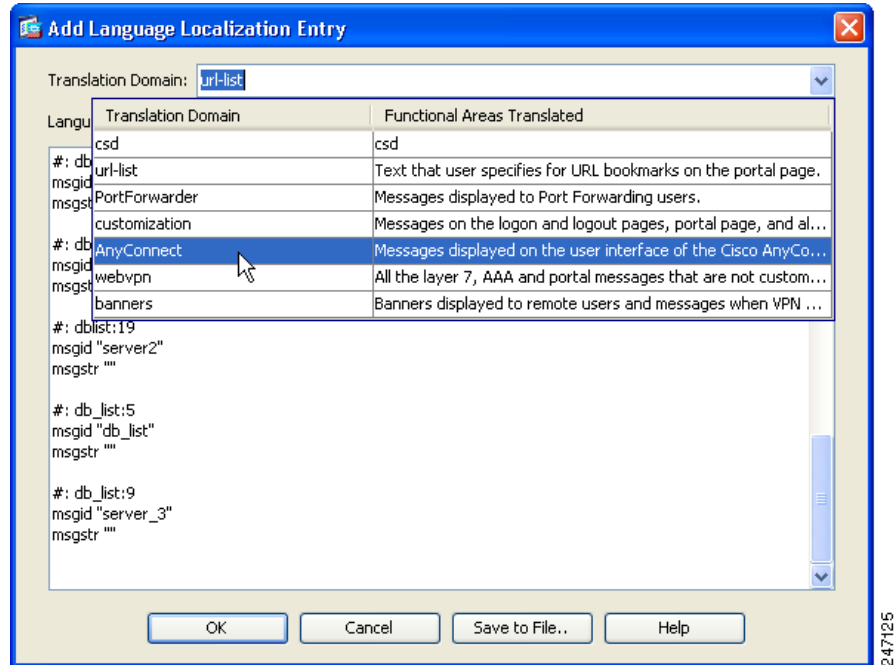
- Step 1** Go to: **Configuration > Remote Access VPN > Language Localization**. Click Add. The Add Language Localization Entry window displays ([Figure 6-9](#)).

**Figure 6-9** Language Localization Pane



- Step 2** Click the Translation Domain drop-list and choose *AnyConnect* (Figure 6-10). This ensures only the messages relating to the AnyConnect GUI appear for editing purposes.

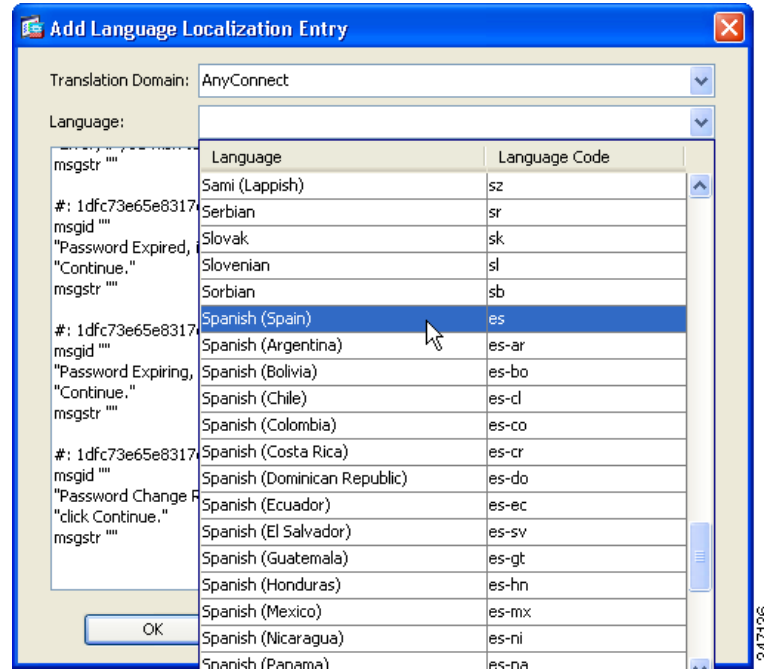
**Figure 6-10** Translation Domain



247125

- Step 3** Specify a language for this translation table (Figure 6-11). ASDM tags this table with the standard abbreviations recognized for languages by Windows and browsers (for example, *es* for Spanish).

**Figure 6-11** Choosing a Language

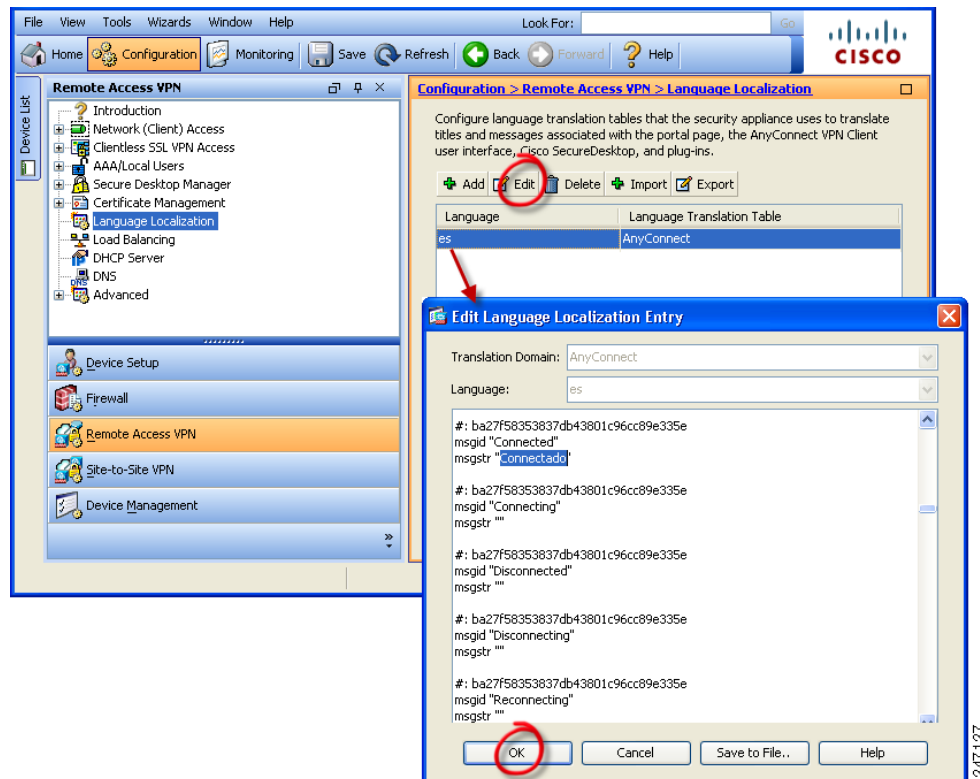


**Step 4** The translation table now displays in the list of languages in the pane (*es* in our example). However, it has no translated messages. To begin adding translated text, click **Edit**. The Edit Language Localization Entry window displays (Figure 6-12).

Add your translated text between the quotes of the message strings (msgstr). In the example below, we insert *Conectado*, 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 6-12** Editing the Translation Table



## Translating by Exporting the Translation Table for Editing

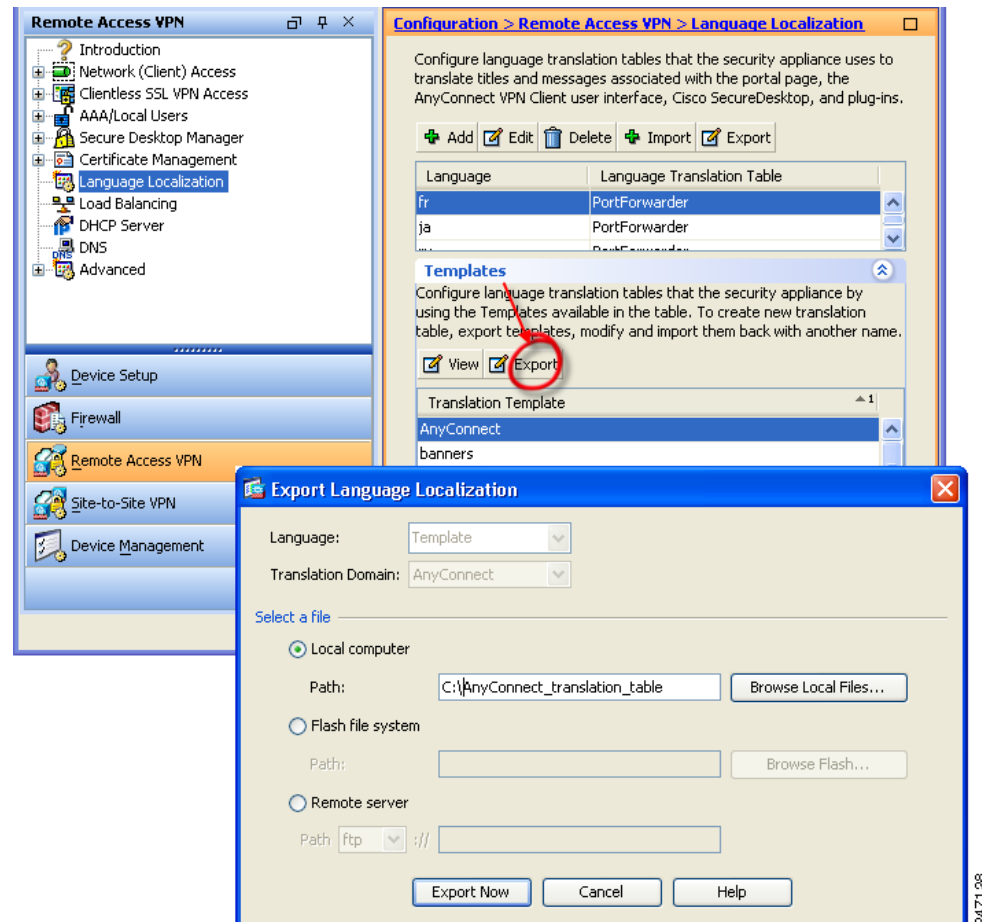
This procedure shows you how to export the AnyConnect translation template to a remote computer, where you can edit the table using an editor or using third party tools such as Gettext or Poedit.

Gettext utilities from The GNU Project is available for Windows and runs in the command window. See the GNU website at [gnu.org](http://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](http://poedit.net).

### Step 1 Export the AnyConnect translation template.

Go to **Configuration > Remote Access VPN > Language Localization**. The language localization pane displays (Figure 6-13). 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 6-13, we export to a local computer with the filename *AnyConnect\_translation\_table*.

**Figure 6-13** Exporting a Translation Template



247128

**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 6-13). Click **Import**. The Import Language Localization window displays.

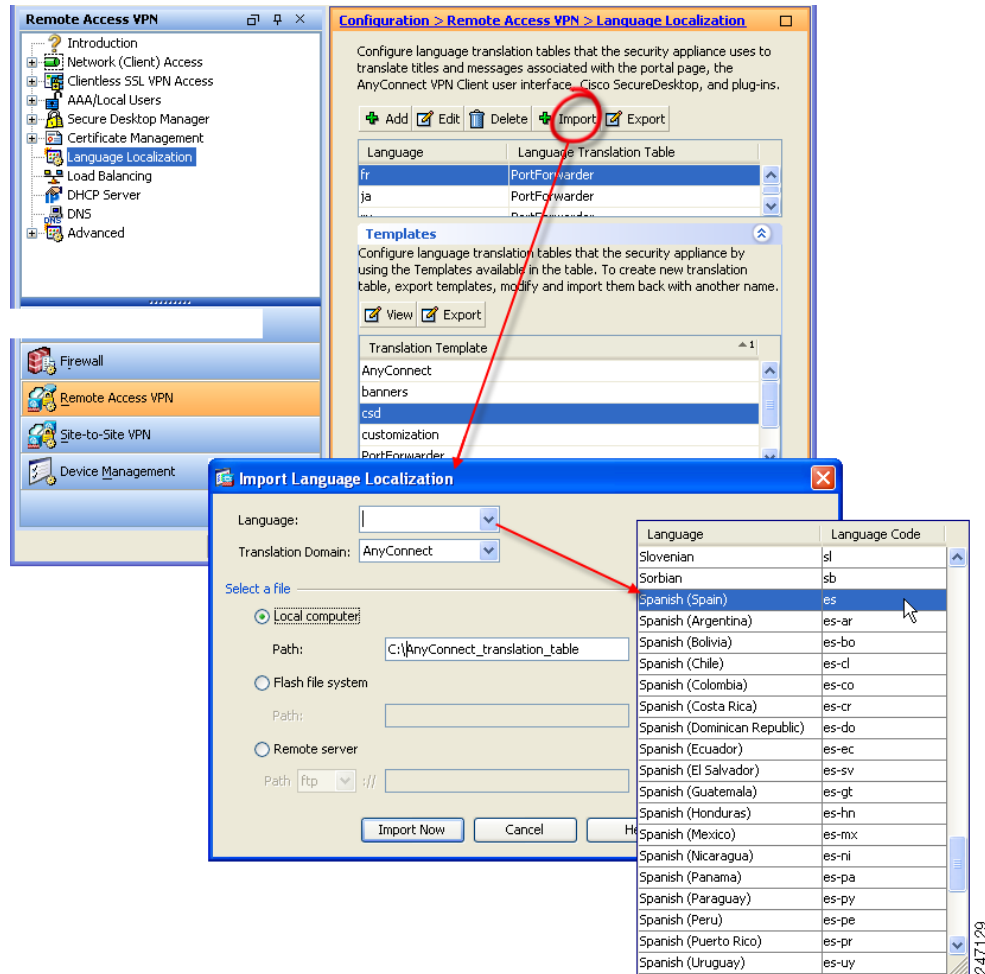
**Step 4** Choose a language for this translation table. Click the Language drop-list to display languages and their industry-recognized abbreviations. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.

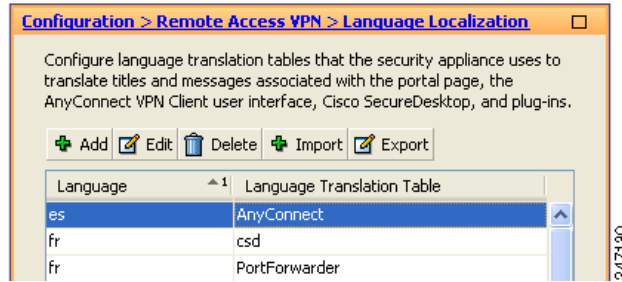
**Step 5** Specify the Translation Domain as *AnyConnect*, choose a method to import, and provide a filename. Click **Import Now**. A message displays saying you successfully imported the table.

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

In [Figure 6-13](#), we specify the language as *Spanish* (es) and import the same file we exported in [Step 1](#) (AnyConnect\_translation\_table). [Figure 6-15](#) shows the new translation table for Spanish in the list of Languages for AnyConnect.

**Figure 6-14** Importing a Translation Template as a new Translation Table



**Figure 6-15** *New Language Displayed in Language Table*

## 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 computer (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](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp).

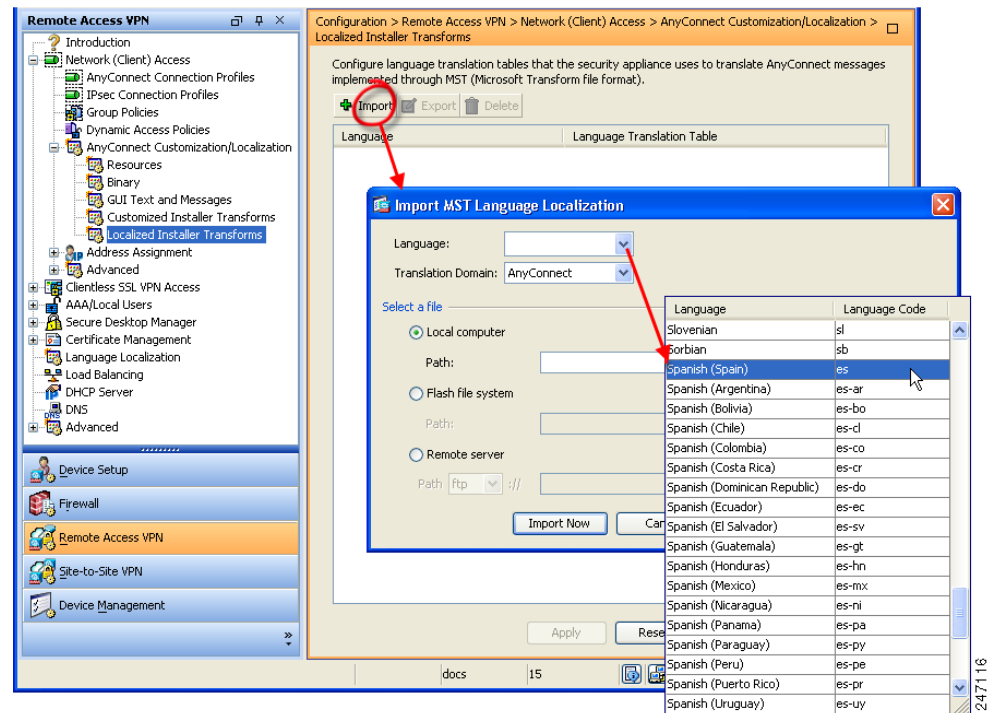
After you install the SDK, the Orca MSI is located here:

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 6-16):

**Figure 6-16** Importing a Transform to Translate the Installer Program

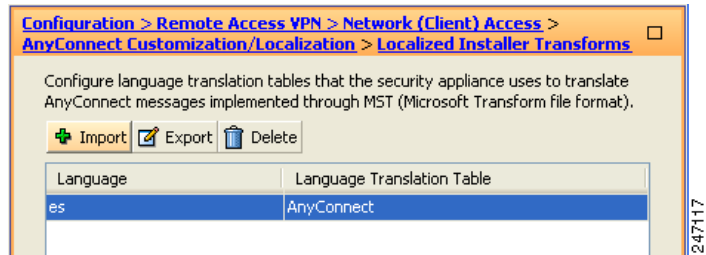


- Step 2** Choose a language for this transform. Click the Language drop-list to display languages and their industry-recognized abbreviations. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.

**Step 3** Click **Import Now**. A message displays saying you successfully imported the table. Be sure to click **Apply** to save your changes.

In Figure 6-16, we specify the language as *Spanish* (es). Figure 6-17 shows the new transform for Spanish in the list of Languages for AnyConnect.

**Figure 6-17** Imported Transform Displays in the Table



## Using Tools to Create Message Catalogs for Enterprise Deployment

If you are not deploying the client with the security appliance, and are using an enterprise software deployment system such as Altiris Agent, you can manually convert the AnyConnect translation table to a message catalog using a utility such as Gettext. After converting the table from a .po file to a .mo file, you then place the file in the proper folder on the client computer.

Gettext is a utility from The GNU Project and runs in the command window. See the GNU website at [gnu.org](http://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](http://poedit.net).

The AnyConnect client message template is located in these folders:

Windows XP:

```
%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect VPN
Client\110n<LANGUAGE-CODE>\LC_MESSAGES
```

Windows Vista:

```
%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect VPN Client\110n\
<LANGUAGE-CODE>\LC_MESSAGES
```

Mac OS X and Linux:

```
/opt/cisco/vpn/110n/<LANGUAGE-CODE>/LC_MESSAGES
```

The following procedure creates a message catalog using Gettext:

- 
- Step 1** Download the Gettext utilities from <http://www.gnu.org/software/gettext/> and install Gettext on a computer you use for administration (not a remote user computer).
  - Step 2** Retrieve a copy of the AnyConnect message template *AnyConnect.po* on a computer with an AnyConnect client installed.
  - Step 3** Edit the AnyConnect.po file (use notepad.exe or any plain text editor) to change strings as desired.
  - Step 4** Run the Gettext message file compiler to create the .mo file from the .po file:  

```
msgfmt -o AnyConnect.mo AnyConnect.po
```
  - Step 5** Place a copy of the .mo file into correct folder on user computer.

## 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](http://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](http://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 7

# Communicating User Guidelines

Please consider selecting from the guidelines for communication with your VPN users, or use this section as a reference when responding to user requests for guidance. The following topics are covered:

- [Using the AnyConnect CLI Commands to Connect \(Standalone Mode\), page 7-1](#)
- [Logging Out, page 7-3](#)
- [Setting the Secure Connection \(Lock\) Icon, page 7-3](#)

## 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 7-1](#) shows the CLI commands.

**Table 7-1**      **AnyConnect Client CLI Commands**

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

The following examples 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.

## Logging Out

*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.

## Setting the Secure Connection (Lock) Icon

The Lock icon indicates a secure connection. Windows XP automatically hides this icon among those that have not been recently used. Users can prevent Windows XP from hiding this icon by following this procedure:

- 
- Step 1** Go to the taskbar where the tray icons are displayed and right click the left angle bracket ( < ).
  - Step 2** Select **Customize Notifications...**
  - Step 3** Select **Cisco Systems AnyConnect VPN Client** and set to **Always Show**.
-





## CHAPTER 8

# Managing, Monitoring, and Troubleshooting AnyConnect Sessions

---

This chapter explains these subjects and tasks:

- [Disconnecting All VPN Sessions, page 8-1](#)
- [Disconnecting Individual VPN Sessions, page 8-1](#)
- [Viewing Detailed Statistical Information, page 8-2](#)
- [Resolving VPN Connection Issues, page 8-4](#)
- [Using DART to Gather Troubleshooting Information, page 8-5](#)

## Disconnecting All VPN 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#
```

## Disconnecting Individual VPN Sessions

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.

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

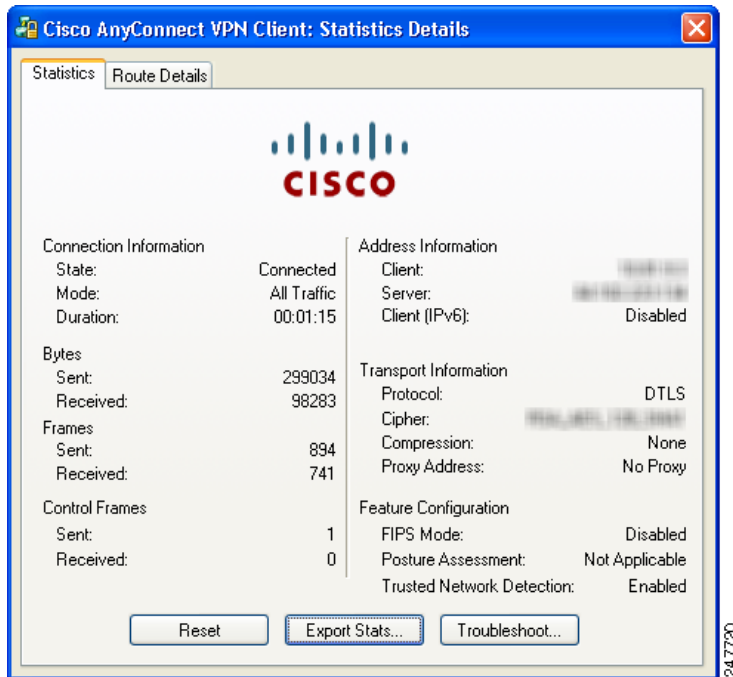
```
hostname# vpn-sessiondb logoff name testuser
INFO: Number of sessions with name "testuser" logged off : 1
```

## Viewing Detailed Statistical Information

You or the user can view statistical information for a current AnyConnect client session by clicking the **Details** button on the user GUI.

This opens the Statistics Details dialog. On the Statistics tab in this window, you can reset the statistics, export the statistics, and gather files for the purpose of troubleshooting.

**Figure 8-1** AnyConnect VPN Client Statistics Details Dialog



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:

- Clicking **Reset** resets the connection information to zero. AnyConnect immediately begins collecting new data.
- Clicking **Export Stats...** saves the connection statistics to a text file for later analysis and debugging.
- Clicking **Troubleshoot...** Launches the DART (Diagnostic AnyConnect Reporting Tool) wizard which bundles specified log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connection. See [Using DART to Gather Troubleshooting Information](#), page 8-5 for information about the DART package.

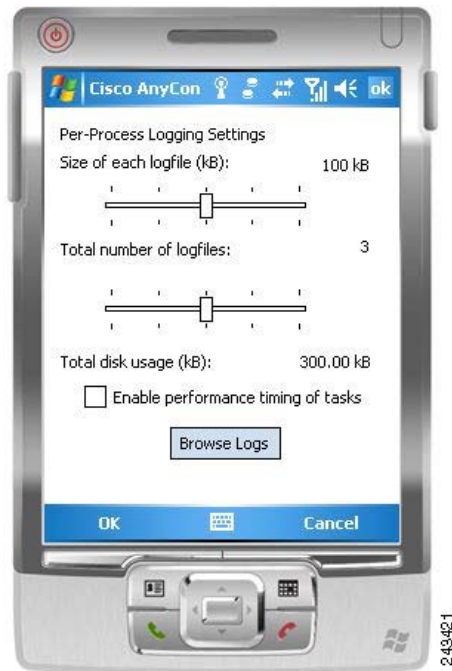
## Viewing Statistics on a Windows Mobile Device

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 8-2).

**Figure 8-2** Windows Mobile Logging Menu



Clicking on Logging opens the logging settings dialog box (Figure 8-3).

**Figure 8-3** Windows Mobile Logging Settings Dialog Box

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.

## Resolving VPN Connection Issues

Use the following sections to resolve VPN connection issues.

### Adjusting the MTU Size

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 sets the maximum size of the packet to be transmitted over the tunnel for the client and security appliance. If a VPN 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 resolve the problem.

To adjust the Maximum Transmission Unit size (from 256 to 1406 bytes) for SSL VPN connections established by the AnyConnect Client,

- 
- Step 1** From the ASDM interface, select Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit.

The Edit Internal Group Policy dialog box opens.

**Step 2** Select Advanced > SSL VPN Client.

**Step 3** 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 AnyConnect Client connections established in SSL and those established in SSL with DTLS.

## Eliminating Compression to Improve VPN Performance and Accommodate Windows Mobile Connections

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 CLI command **compression svc** command from global configuration mode.

## Using DART to Gather Troubleshooting Information

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

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

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

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

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



### Note

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

## Getting the DART Software

DART is available as part of the AnyConnect client download and installation package or as a standalone .msi file.

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

These are the AnyConnect downloads, containing DART, on Cisco.com. Refer to the Release Notes for Cisco AnyConnect VPN Client for the latest version numbers:

- **anyconnect-all-packages-2.4.version-k9.zip** — Contains all AnyConnect packages.
- **anyconnect-dart-win-2.4.version-k9.pkg** — Contains *only* the DART installation package, not the AnyConnect or vpngina software. Use this when installing DART as a standalone application.

## Installing DART

The administrator can include DART as part of the AnyConnect installation, or registered users of Cisco.com can download the file from <http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect>, as described in [Getting the DART Software](#), and install it manually on the PC.

When the user downloads the AnyConnect client, a new version of DART, if available, is also automatically downloaded to the user's PC. When a new version of the AnyConnect client is downloaded as part of an automatic upgrade, that download includes a new version of DART, if there is one.



### Note

If the **dart** keyword is not present in the group-policy configuration (configured through the **svc modules** command or the corresponding ASDM dialog), then the AnyConnect download does not install DART, even if it is present in the package.

## Installing DART with AnyConnect

This procedure downloads DART to the remote-user's machine the next time the user connects.

- Step 1** Load the AnyConnect package containing DART to the security appliance, just as you would any other Cisco software package.
- Step 2** After installing the AnyConnect .pkg file containing DART on the security appliance, you must specify DART in a group policy, in order for it to be installed with AnyConnect. You can do this using ASDM or the CLI, as follows:
  - If using ASDM, begin by clicking **Configuration** and then click **Remote Access VPN > Network (Client) Access > Group Policies**.  
Add a new group policy or edit an existing group policy. In the group policy dialog box, expand **Advanced** and click **SSL VPN Client**.  
In the SSL VPN Client dialog box, uncheck **Inherit** for the **Optional Client Modules to Download** option. Select the **dart** module in the option's drop-down list.  
If the version of ASDM that you are using does not have the DART option checkbox, enter the keyword **dart** in the field. If you want to enable both DART and Start Before Logon, enter both **dart** and **vpngina** in that field, in either order, separated by a comma.

Click **OK** and then click **Apply**.

- If using CLI, use the **svc modules value dart** command.

**Note**

If you later change to **svc modules none** or if you remove the DART selection in the **Optional Client Modules to Download** field, DART remains installed. There is no way for the security appliance to cause DART to be uninstalled. However, you can remove DART by using the Windows Add/Remove Programs in the Control Panel. If you do remove DART in this way, then it is reinstalled automatically when the user reconnects using the AnyConnect client. When the user connects, DART is upgraded automatically when an AnyConnect package with a higher version of DART is uploaded and configured on the security appliance.

To run DART, see [Running DART on a Windows PC, page 8-7](#).

## Manually Installing DART on the Host

- Step 1** Get the DART software from Cisco.com. See, [Getting the DART Software, page 8-6](#), and store **anyconnect-dart-win-2.4.version-k9.pkg** locally.
- Step 2** Using a file compression utility such as WinZip®, extract the contents of the **anyconnect-dart-win-2.4.version-k9.pkg** and maintain the directory structure.
- Step 3** Open the **binaries** directory created from extracting the contents of the **anyconnect-dart-win-2.4.version-k9.pkg** file.
- Step 4** Double-click the **anyconnect-dart-win-2.4.version-k9.msi** file to launch the **DART Setup Wizard**.
- Step 5** Click **Next** at the Welcome screen.
- Step 6** Select **I accept the terms in the License Agreement** to accept the end user license agreement and click **Next**.
- Step 7** Click **Install** to install DART. The installation wizard installs **DartOffline.exe** in the <System Drive>\Program Files\Cisco\Cisco DART directory.
- Step 8** Click **Finish** to complete the installation.

To run DART, see [Running DART on a Windows PC, page 8-7](#).

## Running DART on a Windows PC

To run the DART wizard and create a DART bundle on a Windows PC, follow these steps:

- Step 1** Launch the AnyConnect client GUI.
- Step 2** Click the **Statistics** tab and then click the **Details** button at the bottom of the dialog box. This opens the Statistics Details dialog box.
- Step 3** Click **Troubleshoot** at the bottom of the Statistics Details window.
- Step 4** Click **Next** at the Welcome screen. This brings you to the Bundle Creation Option dialog box.

**Step 5** In the Bundle Creation Options area, select **Default** or **Custom**.

- The **Default** option includes the typical log files and diagnostic information, such as the AnyConnect and Cisco Secure Desktop log files, general information about the computer, and a summary of what DART did and did not do.

By selecting **Default**, and then clicking **Next** at the bottom of the dialog box, DART immediately begins creating the bundle. The default name for the bundle is DARTBundle.zip and it is saved to the local desktop.

- If you choose **Custom**, the DART wizard will present you with more dialog boxes, after you click **Next**, so that you can specify what files you want to include in the bundle and where to store the bundle.



**Tip**

By selecting **Custom**, you could accept the default files to include in the bundle and then only specify a different storage location for the file.

**Step 6** If you want to encrypt the DART bundle, in the **Encryption Option** area check **Enable Bundle Encryption**; then, enter a password in the **Encryption Password** field. Optionally, select **Mask Password** and the password you enter in the **Encryption Password** and **Reenter Password** fields will be masked with astericks (\*).

**Step 7** Click **Next**. If you selected **Default**, DART starts creating the bundle. If you selected **Custom**, the wizard continues to the next step.

**Step 8** In the **Log File Selection** dialog box, select the log files and preference files to include in the bundle. Click **Restore Default** if you want to revert to the default list of files typically collected by DART. Click **Next**.

**Step 9** In the Diagnostic Information Selection dialog box, select the diagnostic information to include in the bundle. Click **Restore Default** if you want to revert to the default list of files typically collected by DART. Click **Next**.

**Step 10** In the Comments and Target Bundle Location dialog box, configure these fields:

- In the **Comments** area, enter any comments you would like to be included with the bundle. DART stores these comments in a comments.txt file included with the bundle.
- In the **Target Bundle Location** field, browse for a location in which to store the bundle.

Click **Next**.

**Step 11** In the Summary dialog box, review your customizations and click **Next** to create the bundle or click **Back** to make customization changes.

**Step 12** Click **Finish** after DART finishes creating the bundle.



**Tip**

In some instances, customers have reported that DART has run for more than a few minutes. If DART seems to be taking a long time to gather the default list of files, click **Cancel** and then re-run the wizard choosing to create a **Custom** DART bundle and only select the files you need.



# APPENDIX A

## Open Software License Notices

---

### 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](mailto:openssl-core@openssl.org).

#### OpenSSL License:

Copyright © 1998-2009 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](mailto: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 LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

#### **Original SSLeay License:**

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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 acknowledgement:

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

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS 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 AUTHOR OR 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 LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

