Cisco AnyConnect Secure Mobility Client Administrator Guide

Published: January 13, 2011

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

Cisco AnyConnect Secure Mobility Client Administrator Guide

CONTENTS

About this Guide

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

Throughout this guide, the term “ASA” 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 ASAs
- Configure VPNs

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	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.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	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

- *AnyConnect Secure Mobility Client 2.5 Release Notes*
- *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 2.5*
- Cisco ASA 5500 Series Adaptive Security Appliances Release Notes
- Cisco ASA 5500 Series Adaptive Security Appliances Install and Upgrade Guides
- Cisco ASA 5500 Series Adaptive Security Appliances Configuration Guides
- Cisco ASA 5500 Series Adaptive Security Appliances Command References
- Cisco ASA 5500 Series Adaptive Security Appliances Error and System Messages
- Cisco Adaptive Security Device Manager Release Notes
- Cisco Adaptive Security Device Manager Configuration Guides
- Online help for ASDM
- Cisco Secure Desktop Release Notes
- Cisco Secure Desktop Configuration Guides
- For Open Source License information for this product, go to http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html.

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 the AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility client is the next-generation VPN client, providing remote users with secure IPsec (IKEv2) or SSL VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA). AnyConnect provides end users with a connectivity experience that is intelligent, seamless and always-on, with secure mobility across today's proliferating managed and unmanaged mobile devices.

Deployable from the ASA or from Enterprise Software Deployment Systems

AnyConnect can be deployed to remote users from the ASA or using enterprise software deployment systems. When deployed from the ASA, remote users make an initial SSL connection to the ASA by entering the IP address or DNS name in their browser of an ASA configured to accept clientless SSL VPN connections. The ASA presents a login screen in the browser window, and if the user satisfies the login and authentication, downloads the client that matches the computer operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA.

Customizable and Translatable

You can customize the AnyConnect to display your own corporate image to remote users. You can rebrand AnyConnect by replacing our default GUI components, deploy a transform you create for more extensive rebranding, or deploy your own client GUI that uses the AnyConnect API. You can also translate messages displayed by AnyConnect or the installer program in the language preferred by the remote user.

Easily Configured

Using ASDM, you can easily configure AnyConnect features in the client profile—an XML file that provides basic information about connection setup, as well as advanced features such as Start Before Logon (SBL). For some features, you also need to configure the ASA. The ASA deploys the profile during AnyConnect installation and updates.

Additional Supported Modules

The Cisco AnyConnect Secure Mobility client, Version 3.0, integrates new modules into the AnyConnect client package:

- Network Access Manager (NAM)—Formerly called the Cisco Secure Services Client, this module provides Layer 2 device management and authentication for access to both wired and wireless networks.

- Posture Assessment—The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host prior to creating a remote access connection to the ASA. Based on this prelogin evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance. The Host Scan application is delivered with the posture module and is the application that gathers this information.
- Telemetry—Sends information about the origin of malicious content detected by the antivirus software to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA), which uses this data to provide better URL filtering rules.
- Web Security—Routes HTTP and HTTPS traffic to the ScanSafe Web Security scanning proxy server for content analysis, detection of malware, and administration of acceptable use policies.
- Diagnostic and Reporting Tool (DART)—Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
- Start Before Logon (SBL)—Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.

This chapter includes the following sections:

Standalone and WebLaunch Options

The user can use AnyConnect in the following modes:

- Standalone mode—Lets the user establish an AnyConnect connection without the need to use a web browser. If you have permanently installed AnyConnect on the user's PC, the user can run in standalone mode. In standalone mode, a user opens AnyConnect 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 ASA checks the version of AnyConnect on the user's PC and, if necessary, the client downloads the latest version.
- WebLaunch mode—Lets the user enter the URL of the ASA 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 AnyConnect, 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.

If you configure the ASA to deploy the AnyConnect package, you ensure that the ASA is the single point of enforcement as to which versions of AnyConnect can establish a session, even if you deploy AnyConnect with an enterprise software deployment system. When you load an AnyConnect package

on the ASA, you enforce a policy to which only versions as new as the one loaded on the ASA can connect. AnyConnect upgrades itself when it connects to the ASA. Alternatively, you can deploy a local policy file that specifies the client bypasses the client downloader, eliminating the requirement for the client package file on the ASA. However, other features such as weblaunch and automatic updates are disabled.

AnyConnect Licensing Options

The following sections associate the licensing options with the AnyConnect components.

Network Access Manager

Network Access Manager requires either of the following licenses that specifies the number of supported endpoints:

- AnyConnect Essentials license.
- AnyConnect Premium SSL VPN Edition license.

Web Security

Web security requires a Web Security license that specifies the number of supported endpoints.

VPN Licensing

AnyConnect support for SSL and IKEv2 access requires either of the following licenses to specify the maximum number of remote access sessions supported at a time:

- AnyConnect Essentials license.
- AnyConnect Premium SSL VPN Edition license.

Either license supports the basic AnyConnect features.

Table 1-1 shows the licenses you can combine with the Essentials and Premium licenses.

Table 1-1 Advanced AnyConnect License Options for VPN

Sessions License	License Option	Basic Access	Post Log-in Always-on VPN	Malware Defense, Acceptable Use Policy Enforcement, and Data Leakage Prevention on the Web	Clientless Access	Endpoint Assessment	Endpoint Remediation	Business Continuity
AnyConnect Essentials	(base license)	✓						
	Cisco Secure Mobility for AnyConnect Essentials	✓	✓	✓				
AnyConnect Premium SSL VPN Edition	(base license)	✓	✓		✓	✓		
	Cisco Secure Mobility for AnyConnect Premium	✓	✓	✓	✓	✓		
	Advanced Endpoint Assessment	✓	✓		✓	✓	✓	
	Flex[1]	✓	✓	✓	✓	✓	✓	✓

1. A flex license provides business continuity support for malware defense, acceptable use policy enforcement, data leakage prevention on the web, and endpoint remediation features only if those features are licensed.

The *AnyConnect Essentials*, *AnyConnect Premium SSL VPN Edition*, *Advanced Endpoint Assessment*, and *Flex* licenses require activation on a Cisco adaptive security appliance (ASA) running 8.0(x) or later; however, some features require later versions of the ASA.

The *Cisco Secure Mobility* licenses requires activation on a Cisco IronPort Web Security Appliance (WSA) running 7.0 or later.

The activation of an *AnyConnect Mobile* license on the ASA supports mobile access, but does not provide support for the features in this table. It is available as an option with either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.

For a list of the features available with either an AnyConnect Essentials license or AnyConnect Premium SSL VPN Edition license, see the Basic Features table.

The features enabled by the optional licenses shown in Table 1-1 are as follows:

- *Post Log-in Always-on VPN* establishes a VPN session automatically after the user logs in to a computer. For more information, see Always-on VPN. This feature also includes a Connect Failure Policy for Always-on VPN and Captive Portal Hotspot Detection and Remediation.

- *Malware defense, acceptable use policy enforcement and data leakage prevention for the web* are features provided by the Cisco IronPort Web Security Appliance (WSA). For more information, see the *Cisco IronPort Web Security Appliances Introduction*.
- *Clientless access* lets you use a browser to establish a VPN session and lets specific applications use the browser to access that session.
- *Endpoint assessment* ensures that your choice of antivirus software versions, antispyware versions, associated update definitions, firewall software versions, and corporate property verification checks comply with policies to qualify a session to be granted access to the VPN.
- *Endpoint remediation* attempts to resolve endpoint failures to satisfy corporate requirements for antivirus, antispyware, firewall software, and definitions file requirements.
- *Business continuity* increases the number of licensed remote access VPN sessions to prepare for temporary spikes in usage during cataclysmic events such as pandemics. Each flex license is ASA-specific and provides support for sixty days. The count can consist of both contiguous and noncontiguous days.

Cisco Secure Remote Access: VPN Licensing Overview provides brief descriptions of the AnyConnect license options and example SKUs.

For a detailed list of the AnyConnect features, license and release requirements, and the endpoint OSs supported for each feature, see *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 2.5*.

Configuration and Deployment Overview

Use the AnyConnect Profile editor to configure the AnyConnect features in the profile file; then configure the ASA to download this file along with AnyConnect client automatically when users make a VPN connection to the ASA with a browser. The profile file drives the display in the user interface and defines the names and addresses of host computers. By creating and assigning different profiles to group policies configured on the ASA, you can differentiate access to these features. Following assignment to the respective group policies, the ASA automatically pushes the profile assigned to the user upon connection setup.

Profiles provide basic information about connection setup, and users cannot manage or modify them. The profile is an XML file that lets you identify the secure gateway (ASA) hosts that you want to make accessible. In addition, the profile conveys additional connection attributes and constraints on a user. For some features, you can specify some settings in the profile as user controllable. The AnyConnect GUI displays controls for these settings to the end 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, 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 use an enterprise software deployment system to install the profile file and client as an application on computers for later access.

AnyConnect Secure Mobility Feature Configuration Guidelines

AnyConnect Secure Mobility is a set of features you can configure to optimize the security of the VPN endpoints. To configure all of the AnyConnect secure mobility client options, refer to the following sections:

Step 1 Go to the "Configuring the ASA for WSA Support of the AnyConnect Secure Mobility Solution" section on page 2-43.

Step 2 Use the *Cisco AnyConnect Secure Mobility Solution Guide* as a guide to configuring a WSA to support AnyConnect.

Step 3 Use the AnyConnect Profile Editor to configure the following features:

- Trusted Network Detection, page 3-17
- Always-on VPN, page 3-19
- Disconnect Button for Always-on VPN, page 3-25
- Connect Failure Policy for Always-on VPN, page 3-27
- Captive Portal Hotspot Detection and Remediation, page 3-29
- Configuring Certificate Enrollment using SCEP, page 3-34

API

Use the Application Programming Interface (API) if you want to automate a VPN connection with AnyConnect 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 AnyConnect. There are libraries and example programs that can be used for building AnyConnect 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.

The API supports only the VPN functionality of the client. It does not support the optional AnyConnect modules, such as NAM, Web Security, and telemetry.

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 a VPN session). Host Scan was once only available as a component of Cisco Secure Desktop (CSD). In this release of AnyConnect Secure Mobility Client, host scan is now a separate module which can be installed and updated separately from CSD.

Note Host Scan and some third-party firewalls can interfere with the firewall function optionally deployed by the group policy.

See Chapter 5, “Configuring Host Scan” for more information about installing and managing host scan.

CHAPTER 2

Deploying the AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility client can be deployed to remote users from the ASA or using enterprise software management systems (SMS).

When deployed from the ASA, remote users make an initial SSL connection to the ASA by entering the IP address or DNS name in their browser of an ASA configured to accept clientless SSL VPN connections. The ASA presents a login screen in the browser window, and if the user satisfies the login and authentication, downloads the client that matches their computer's operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA.

The Cisco AnyConnect Secure Mobility client, version 3.0, integrates new modules into the AnyConnect client package. If you are using the ASA to deploy AnyConnect, the ASA can also deploy all the optional modules. When the ASA deploys the AnyConnect client and the various modules, we refer to this as "web deployment."

If you deliver the AnyConnect software to the endpoint using an SMS and install it before the endpoint connects to the ASA, we refer to this as predeployment. You can deploy the core client that provides VPN service and the optional modules using this method but you must pay special attention to the installation order and other details.

In addition to the core AnyConnect VPN client that provides SSL and IPsec (IKEv2) secure VPN connections to the ASA, version 3.0 has the following modules:

- Network Access Manager (NAM)
- Posture Assessment
- Telemetry
- Web Security
- AnyConnect Diagnostic and Reporting Tool (DART)
- Start Before Logon (SBL)

This chapter contains the following sections:

- Enabling IPsec IKEv2 Connections, page 2-22
- Predeploying the AnyConnect Client and Optional Modules, page 2-25
- Configuring the ASA for WSA Support of the AnyConnect Secure Mobility Solution, page 2-43

Note If your ASA has only the default internal flash memory size or the default DRAM size (for cache memory) you could have problems storing and loading multiple AnyConnect client packages on the ASA. This is especially true with the AnyConnect 3.0 client with its optional modules. Even if you have enough space on flash to hold the package files, the ASA could run out of cache memory when it unzips and loads the client images. For more information about the ASA memory requirements when deploying AnyConnect, and possibly upgrading the ASA memory, see the latest release notes for the Cisco ASA 5500 Series.

Introduction to the AnyConnect Client Profiles

You enable Cisco AnyConnect Secure Mobility client features in the AnyConnect profiles—XML files that contain configuration settings for the core client with its VPN functionality and for the optional client modules Network Access Manager (NAM), posture, telemetry, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates. Users cannot manage or modify profiles.

You can configure a profile using the AnyConnect profile editor, a convenient GUI-based configuration tool launched from ASDM. The AnyConnect software package for Windows, version 2.5 and later, includes the editor, which activates when you load the AnyConnect package on the ASA and specify it as an AnyConnect client image.

We also provide a standalone version of the profile editor for Windows that you can use as an alternative to the profile editor integrated with ASDM. If you are predeploying the client, you can use the standalone profile editor to create profiles for the VPN service and other modules that you deploy to computers using your software management system.

Finally, you can manually edit the client profile XML files and import the file to the ASA as a profile.

The two versions of Cisco AnyConnect Profile Editor are different in that there is no “standalone” version of profile editor for configuring a telemetry client profile and that the editors are delivered and launched differently. The profile editor delivered with ASDM is fully supported and the standalone profile is in its Beta release cycle and is not fully supported. In all other ways, the two versions of profile editor are the same.

You can configure the ASA to deploy profiles globally for all AnyConnect users or to users based on their group policy. Usually, a user has a single profile file for each AnyConnect module installed. In some cases, you might want to provide more than one VPN profile for a user. Someone who works from multiple locations might need more than one VPN profile. Be aware that some of the profile settings, such as Start Before Logon, control the connection experience at a global level. Other settings are unique to a particular host and depend on the host selected.

Some profile settings are stored locally on the user’s computer in a user preferences file or a global preferences file. The user file has information the AnyConnect client needs to display user-controllable settings in the Preferences tab of the client GUI and information about the last connection, such as the user, the group, and the host.

The global file has information about user-controllable settings to be able to apply those settings before login (since there is no user). For example, the client needs to know if Start Before Logon and/or AutoConnect On Start are enabled before login. For information about filenames and paths for each operating system, see Table 2-15, Profile Locations for all Operating Systems. For more information about creating client profiles, see these sections:

- Creating and Editing an AnyConnect Client Profile Using the Integrated AnyConnect Profile Editor, page 2-3
- Standalone AnyConnect Profile Editor, page 2-38

Creating and Editing an AnyConnect Client Profile Using the Integrated AnyConnect Profile Editor

This section describes how to launch the profile editor from ASDM and create a new profile.

The Cisco AnyConnect Secure Mobility client software package, version 2.5 and later (all operating systems) contains the profile editor. ASDM activates the profile editor when you load the AnyConnect software package on the ASA as an SSL VPN client image.

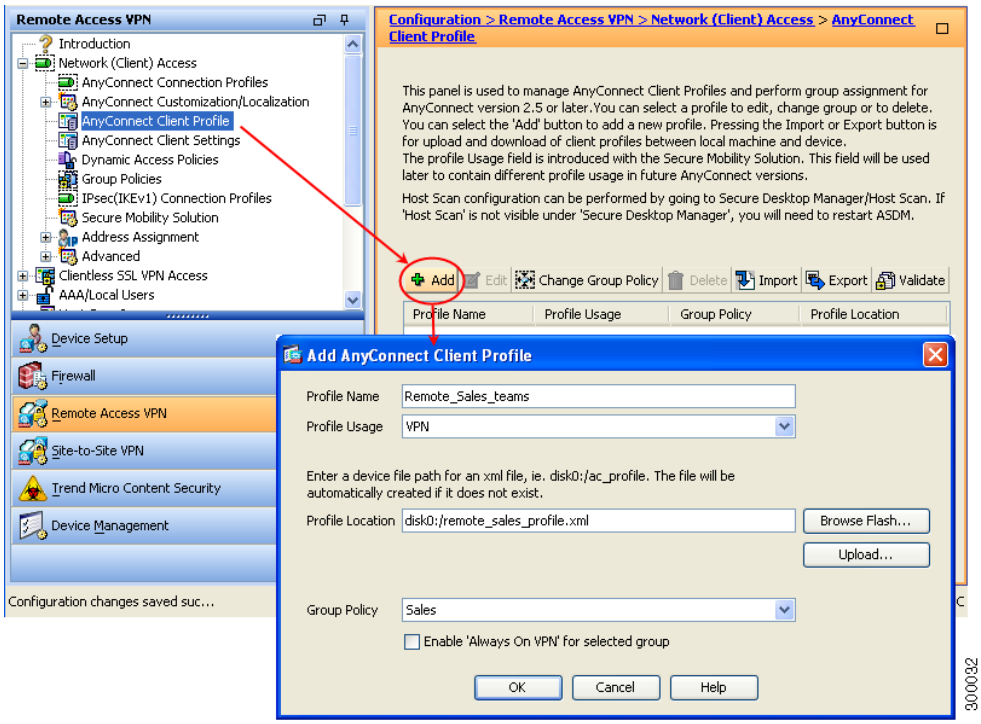
If you load multiple AnyConnect packages, ASDM loads the profile editor from the newest AnyConnect package. This approach ensures that the editor displays the features for the newest AnyConnect loaded, as well as the older clients.

To activate the profile editor in ASDM, follow these steps:

Step 1 Load the AnyConnect software package as an SSL VPN image. If you have not done this already, see Chapter 2, “Configuring the ASA to Download AnyConnect”.

Step 2 Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.** The AnyConnect Client Profile pane opens. Click **Add**. The Add AnyConnect Client Profile window opens (Figure 2-1).

Figure 2-1 Adding an AnyConnect Profile



Step 3 Specify a name for the profile. Unless you specify a different value for Profile Location, ASDM creates the client profile file on the ASA flash memory with the same name.

Step 4 In the Profile Usage field, identify the type of client profile you are creating: VPN, Network Access Manager (NAM), Web Security, or Telemetry.

Step 5 Choose a group policy (optional). The ASA applies this profile to all AnyConnect users in the group policy.

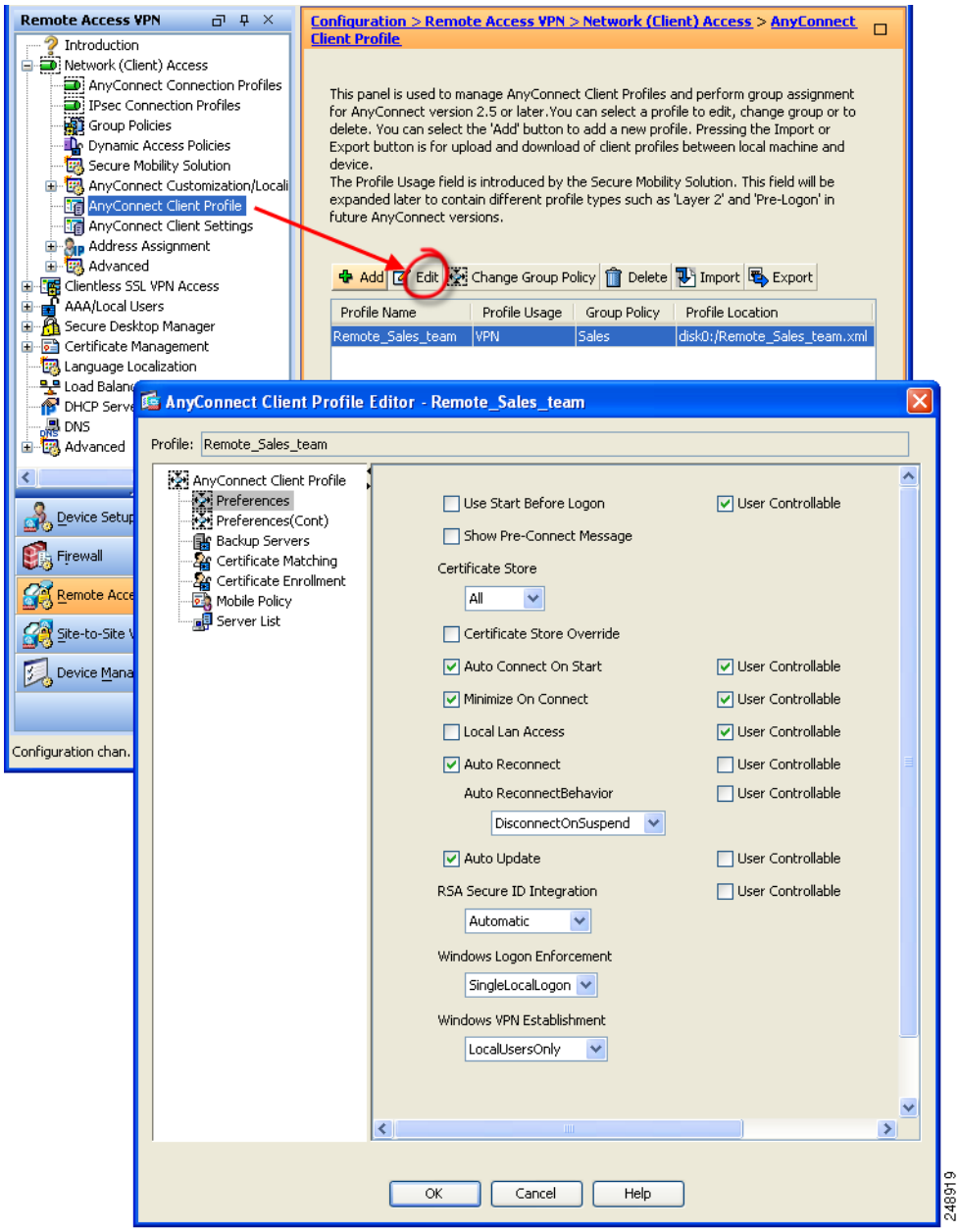
Step 6 Click **OK**. ASDM creates the profile and the profile appears in the table of profiles.

Step 7 Select the profile you just created from the table of profiles. Click **Edit**. The profile editor displays (Figure 2-2). Enable AnyConnect features in the panes of the profile editor. When you finish, click **OK**.

Step 8 Click **Apply**.

Step 9 Close ASDM and relaunch it.

Figure 2-2 Example of Editing a VPN Client Profile



Deploying AnyConnect Client Profiles

You can deploy AnyConnect client profiles using

- Deploying AnyConnect Client Profiles from the ASA, page 2-6
- Deploying Client Profiles Created by the Standalone Profile Editor, page 2-7

Deploying AnyConnect Client Profiles from the ASA

Follow these steps to configure the ASA to deploy a profile with AnyConnect:

Step 1 Create a client profile using "Creating and Editing an AnyConnect Client Profile Using the Integrated AnyConnect Profile Editor" section on page 2-3.

Step 2 Use the profile editor integrated with ASDM to create client profiles for the modules you want to install. See these chapters for instructions on configuring various client profiles:

- Chapter 3, "Configuring VPN Access"

Note You must include the ASA in the host list in the profile so the client GUI displays all the user controllable settings on the initial VPN connection. If you do not add the ASA 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 ASA as a host entry in that profile, the certificate match is ignored. For more information about adding host entries to the profile, see the Chapter 3, "Configuring VPN Access," Configuring a Server List, page 3-46.

- Chapter 4, "Configuring Network Access Manager (NAM)"
- Chapter 6, "Configuring Web Security"
- Chapter 7, "Configuring AnyConnect Telemetry to the WSA"

Step 3 Associate a client profile with a group policy. In ASDM select **Configuration > Remote Access VPN > Network (Client) Access >** AnyConnect Client Profile**.**

Step 4 Select the client profile you want to associate with a group and click **Change Group Policy**.

Step 5 In the **Change Group Policy for Profile** ***policy name*** window, select the group policy from the Available Group Policies field and click the right arrow to move it to the Selected Group Policies field.

Step 6 Click **OK**.

Step 7 In the AnyConnect Client Profile page, click **Apply**.

Step 8 Click **Save**.

Step 9 When you have finished with the configuration, click **OK**.

Deploying Client Profiles Created by the Standalone Profile Editor

See Installing Predeployed AnyConnect Modules, page 2-28 for instructions on deploying the client profiles you created using the standalone profile editor. See Standalone AnyConnect Profile Editor, page 2-38 for instructions on installing and using the Standalone AnyConnect Profile Editor.

Configuring the ASA to Web Deploy AnyConnect

This section addresses the following topics:

AnyConnect File Packages for ASA-Deployment

Table 2-1 shows the AnyConnect file package names for deploying AnyConnect with the ASA:

Table 2-1 AnyConnect Package Filenames for ASA Deployment

OS	AnyConnect 3.0 Web-Deploy Package Name Loaded onto ASA
Windows	anyconnect-win-(ver)-k9.pkg
Mac	anyconnect-macosx-i386-(ver)-k9.pkg
Linux	anyconnect-linux-(ver)-k9.pkg
Linux-64	anyconnect-linux-64-(ver)-k9.pkg **Note** AnyConnect for the 64 bit version of Linux is in its Beta release cycle.

Ensuring Successful AnyConnect Installation

To ensure the AnyConnect Secure Mobility Client installs successfully on user computers, review the following sections:

Minimizing User Prompts about Certificates

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

- If you are using a Certificate Authority (CA) for certificates on the ASA, choose one that is already configured as a trusted CA on client machines.
- If you are using a self-signed certificate on the ASA, 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 ASA certificates matches the name AnyConnect uses to connect to it. By default, the ASA certificate CN field is its IP address. If AnyConnect use a DNS name, change the CN field on the ASA 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`.

Creating a Cisco Security Agent Rule for AnyConnect

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

Current shipping versions of CSA do not have a built-in rule that is compatible with AnyConnect. 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
```

Adding the ASA to the Internet Explorer List of Trusted Sites for Vista and Windows 7

We recommend that Microsoft Internet Explorer (MSIE) users add the ASA to the list of trusted sites, or install Java. The former 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.

For Vista and Windows 7 users, the ASA that deploys the AnyConnect client must be in the list of trusted sites on the user computer. Otherwise, WebLaunch does not occur.

Users can follow this procedure to add an ASA to their list of trusted sites in Microsoft Internet Explorer:

Note This is required on Windows Vista and Windows 7 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 ASA. 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 an ASA 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.

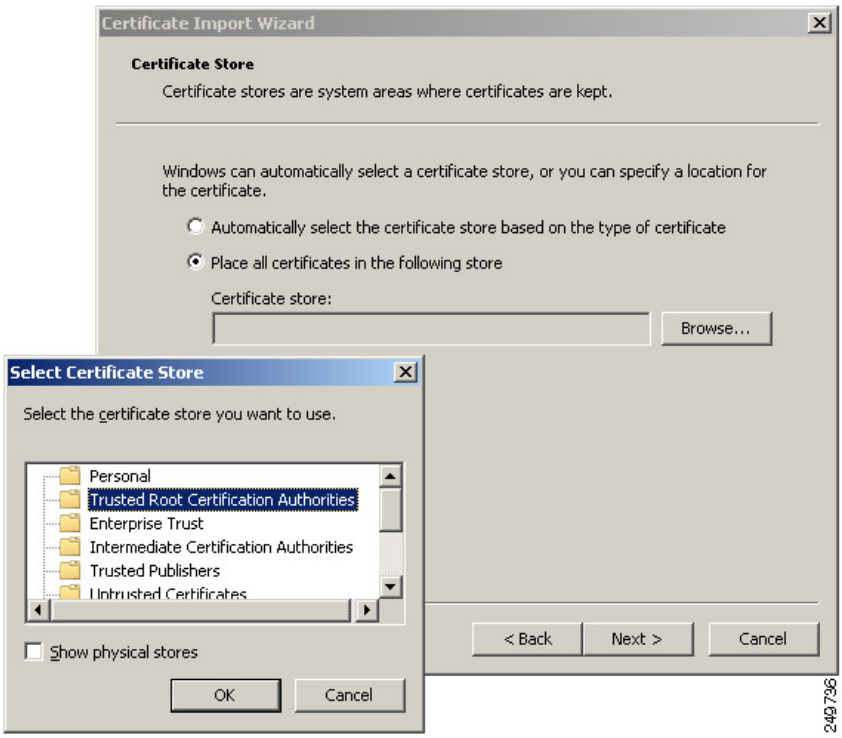
Step 3 Click **Next**. The Certificate Import Wizard – Certificate Store window opens.

Step 4 Select **Place all certificates in the following store**.

Step 5 Click Browse. The Select Certificate Store window opens.

Step 6 In the drop-down list, choose **Trusted Root Certification Authorities** (see Figure 2-3).

Figure 2-3 Importing a Certificate



Step 7 Click **Next**. The Certificate Import Wizard – Completing window opens.

Step 8 Click **Finish**. Another Security Warning window prompts "Do you want to install this certificate?"

Step 9 Click **Yes**. The Certificate Import Wizard window indicates the import is successful.

Step 10 Click **OK** to close this window.

Step 11 Click **OK** to close the Certificate window.

Step 12 Click **Yes** to close the Security Alert window. The ASA 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 an ASA 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 **Examine Certificate** 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 ASA window opens, signifying the certificate is trusted.

Ensuring Fast Connection Time when Loading Multiple AnyConnect Images

When you load multiple AnyConnect images on the ASA, 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 AnyConnect 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 image for Windows Mobile at the top of the list. Alternatively, you can decrease the connection time by specifying the regular expression *Windows CE* to match the user agent on Windows Mobile devices. When the browser on the mobile device connects to the ASA, it includes the User-Agent string in the HTTP header. The ASA, receiving the string, immediately downloads AnyConnect for Windows Mobile without ascertaining whether the other AnyConnect images are appropriate.

To specify a regular expression, in ASDM:

Step 1 Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Settings**.

Step 2 In the list of AnyConnect images, select and image package for Windows Mobile and click **Edit**.

Step 3 Click **Regular expression to match user-agent** and select **Windows CE** in the drop-down list.

Exempting AnyConnect Traffic from Network Address Translation (NAT)

If you have configured your ASA to perform network address translation (NAT), you must exempt your AnyConnect client traffic from being translated so that the AnyConnect clients, internal networks, and corporate resources on a DMZ, can originate network connections to each other. Failing to exempt the AnyConnect client traffic from being translated prevents the AnyConnect clients and other corporate resources from communicating.

"Identity NAT" (also known as "NAT exemption") allows an address to be translated to itself, which effectively bypasses NAT. Identity NAT can be applied between two address pools, an address pool and a subnetwork, or two subnetworks.

This procedure illustrates how you would configure identity NAT between these hypothetical network objects in our example network topology: Engineering VPN address pool, Sales VPN address pool, inside network, a DMZ network, and the Internet. Each Identity NAT configuration requires one NAT rule.

Table 2-2 Network Addressing for Configuring Identity NAT for VPN Clients

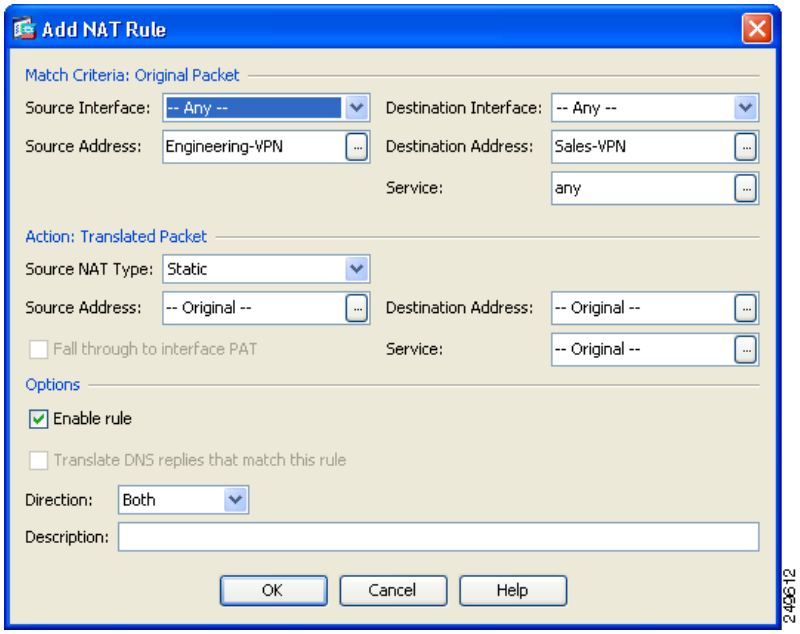
Network or Address Pool	Network or address pool name	Range of addresses
Inside network	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN address pool	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN address pool	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ network	DMZ-network	192.168.1.0 - 192.168.1.255

Step 1 Log into the ASDM and select **Configuration > Firewall > NAT Rules**.

Step 2 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach the hosts in the Sales VPN address pool. In the NAT Rules pane, select **Add > Add NAT Rule Before "Network Object" NAT rules** so that the ASA evaluates this rule before other rules in the Unified NAT table. See Figure 2-4 on page 2-12 for an example of the Add NAT rule dialog box.

Note In ASA software version 8.3, NAT rule evaluation is applied on a top-down, first match basis. Once the ASA matches a packet to a particular NAT rule it does not perform any further evaluation. It is important that you place the most specific NAT rules at the top of the Unified NAT table so that the ASA does not prematurely match them to broader NAT rules.

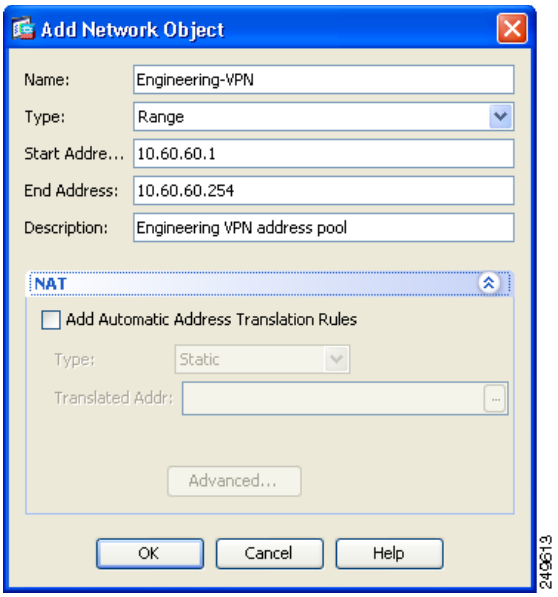
Figure 2-4 Add NAT rule dialog box



a. In the **Match criteria: Original Packet** area, configure these fields:

- Source Interface: Any
- Destination Interface: Any
- Source Address: Click the Source Address browse button and create the network object that represents the Engineering VPN address pool. Define the object type as a **Range** of addresses. Do not add an automatic address translation rule. See Figure 2-5 for an example.
- Destination Address: Click the Destination Address browse button and create the network object that represents the Sales VPN address pool. Define the object type as a **Range** of addresses. Do not add an automatic address translation rule.

Figure 2-5 Create Network Object for a VPN address pool



b. In the **Action Translated Packet** area, configure these fields:
   - Source NAT Type: Static
   - Source Address: Original
   - Destination Address: Original
   - Service: Original

c. In the **Options** area, configure these fields:
   - Check **Enable rule**.
   - Uncheck or leave empty the **Translate DNS replies that match this rule**.
   - Direction: Both
   - Description: Add a Description for this rule.

d. Click **OK**.

e. Click **Apply**. Your rule should look like rule 1 in the Unified NAT table in Figure 2-7 on page 2-16.

   CLI example:

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN
Sales-VPN
```

f. Click **Send**.

Step 3 When the ASA is performing NAT, in order for two hosts in the same VPN pool to connect to each other, or for those hosts to reach the Internet through the VPN tunnel, you must enable the **Enable traffic between two or more hosts connected to the same interface** option. To do this, in ASDM, select **Configuration > Device Setup > Interfaces**. At the bottom of the Interface panel, check **Enable traffic between two or more hosts connected to the same interface** and click **Apply**.

CLI example:

```
same-security-traffic permit inter-interface
```

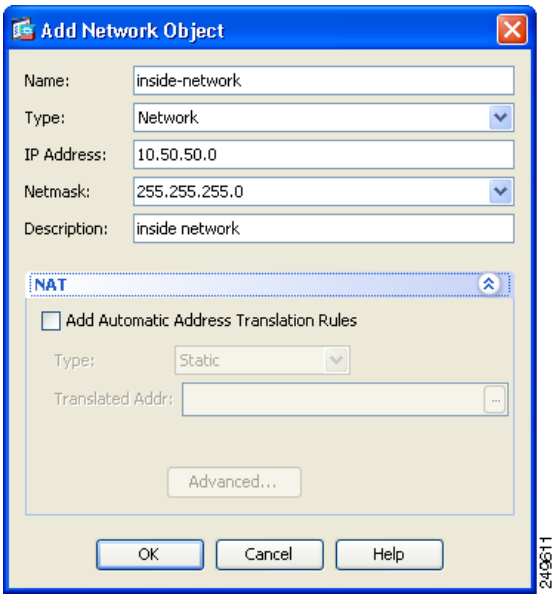
Step 4 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach other hosts in the Engineering VPN address pool. Create this rule just as you created the rule in Step 2 except that you specify the Engineering VPN address pool as both the Source address and the Destination Address in the **Match criteria: Original Packet** area.

Step 5 Create a NAT rule so that the Engineering VPN remote access clients can reach the "inside" network. In the NAT Rules pane, select **Add > Add NAT Rule Before "Network Object" NAT rules** so that this rule will be processed before other rules.

a. In the **Match criteria: Original Packet** area configure these fields:

- Source Interface: Any
- Destination Interface: Any
- Source Address: Click the Source Address browse button and create a network object that represents the inside network. Define the object type as a **Network** of addresses. Do not add an automatic address translation rule.
- Destination Address: Click the Destination Address browse button and select the network object that represents the Engineering VPN address pool.

Figure 2-6 Add inside-network object



b. In the **Action: Translated Packet** area, configure these fields:

- Source NAT Type: Static
- Source Address: Original
- Destination Address: Original
- Service: Original

c. In the **Options** area, configure these fields:

- Check **Enable rule**.
- Uncheck or leave empty the **Translate DNS replies that match this rule**.
- Direction: Both

- Description: Add a Description for this rule.

d. Click **OK**.

e. Click **Apply**. Your rule should look like rule two in the Unified NAT table in Figure 2-7 on page 2-16.

CLI example

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

Step 6 Create a new rule, following the method in Step 5, to configure identity NAT for the connection between the Engineering VPN address pool and the DMZ network. Use the DMZ network as the Source Address and use the Engineering VPN address pool as the Destination address.

Step 7 Create a new NAT rule to allow the Engineering VPN address pool to access the Internet through the tunnel. In this case, you do not want to use identity NAT because you want to change the source address from a private address to an Internet routable address. To create this rule, follow this procedure:

a. In the NAT Rules pane, select **Add > Add NAT Rule Before "Network Object" NAT rules** so that this rule will be processed before other rules.

b. In the **Match criteria: Original Packet** area configure these fields:

- Source Interface: Any
- Destination Interface: Any. This field will be automatically populated with "outside" after you select outside as the Source Address in the **Action: Translated Packet** area.
- Source Address: Click the Source Address browse button and select the network object that represents the Engineering VPN address pool.
- Destination Address: Any.

c. In the **Action: Translated Packet** area, configure these fields:

- Source NAT Type: Dynamic PAT (Hide)
- Source Address: Click the Source Address browse button and select the **outside** interface.
- Destination Address: Original
- Service: Original

d. In the **Options** area, configure these fields:

- Check **Enable rule**.
- Uncheck or leave empty the **Translate DNS replies that match this rule**.
- Direction: Both
- Description: Add a Description for this rule.

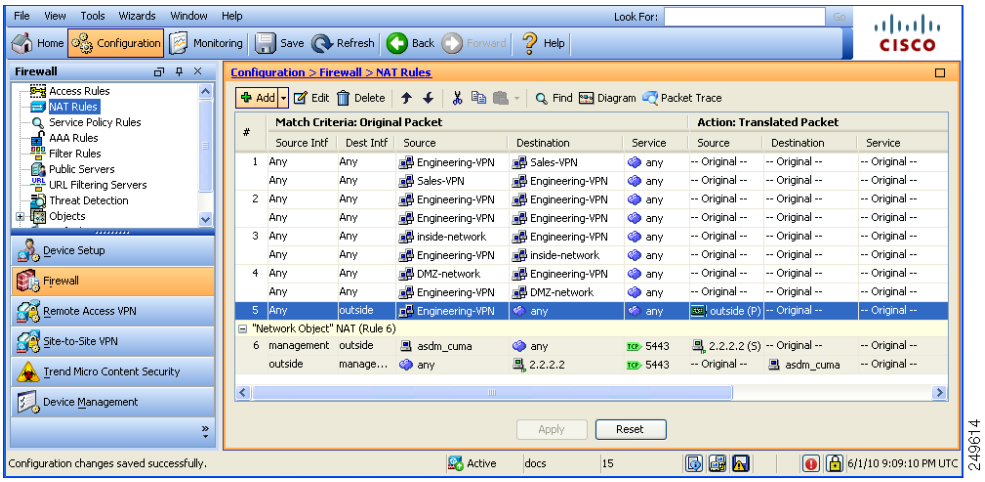
e. Click **OK**.

f. Click **Apply**. Your rule should look like rule five in the Unified NAT table in Figure 2-7 on page 2-16.

CLI example:

```
nat (any,outside) source dynamic Engineering-VPN interface
```

Figure 2-7 Unified NAT table



Step 8 After you have configured the Engineering VPN Address pool to reach itself, the Sales VPN address pool, the inside network, the DMZ network, and the Internet; you must repeat this process for the Sales VPN address pool. Use identity NAT to exempt the Sales VPN address pool traffic from undergoing network address translation between itself, the inside network, the DMZ network, and the Internet.

Step 9 From the **File** menu on the ASA, select **Save Running Configuration to Flash** to implement your identity NAT rules.

Configuring the ASA to Download AnyConnect

To prepare the ASA to web deploy AnyConnect, complete these steps:

Step 1 Review the procedures in the "Ensuring Successful AnyConnect Installation" section on page 2-7 and perform the ones that are applicable to your enterprise.

Step 2 Download the latest Cisco AnyConnect Secure Mobility client package from the Cisco AnyConnect Software Download webpage. See the "AnyConnect File Packages for ASA-Deployment" section on page 2-7 for a list of AnyConnect file packages.

Step 3 Specify the Cisco AnyConnect Secure Mobility client package file as a client image. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Settings**. The AnyConnect Client Settings panel displays, (Figure 2-8), listing client files identified as AnyConnect images. The order in which they appear reflects the order the ASA downloads them to remote computers.

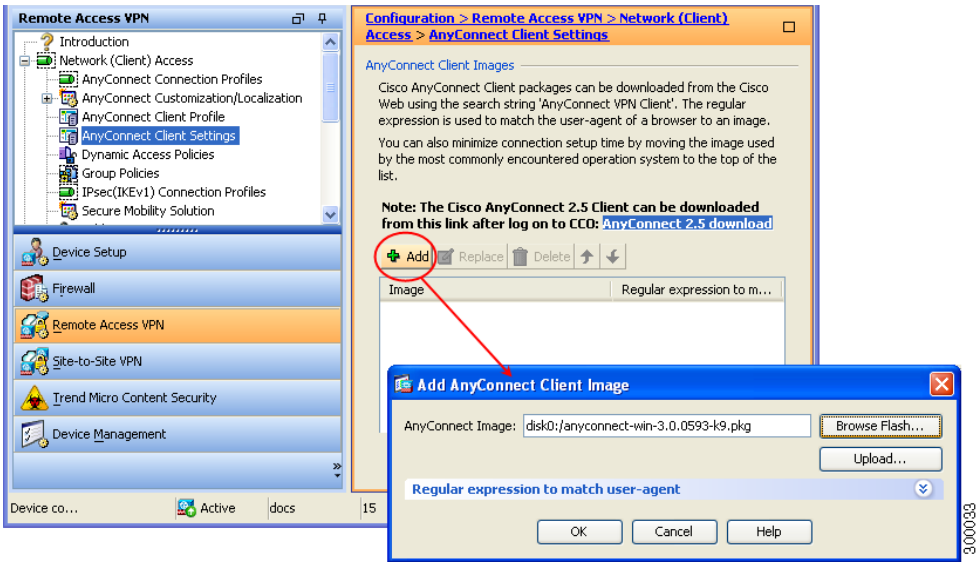
Step 4 To add an AnyConnect image, click **Add** in the AnyConnect Client Images area.

- Click **Browse Flash** to select an AnyConnect image you have already upload to the ASA.
- Click **Upload** to browse to an AnyConnect image you have stored locally on your computer.

Step 5 Click **OK** or **Upload**.

Step 6 Click **Apply**.

Figure 2-8 Specify AnyConnect Images

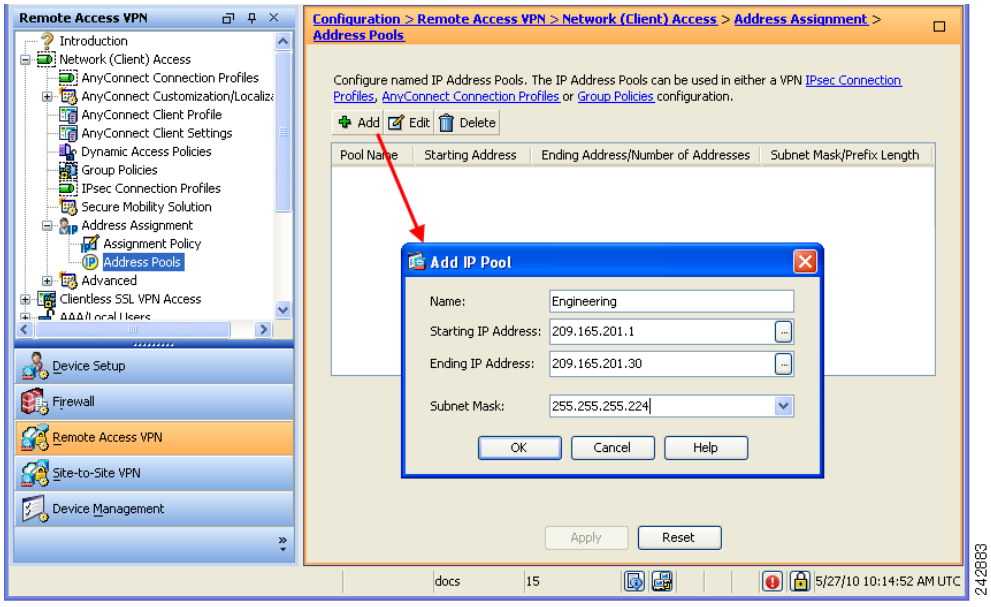


Step 7 Configure a method of address assignment.

You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a connection profile. 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 2-9). Enter address pool information in the Add IP Pool window.

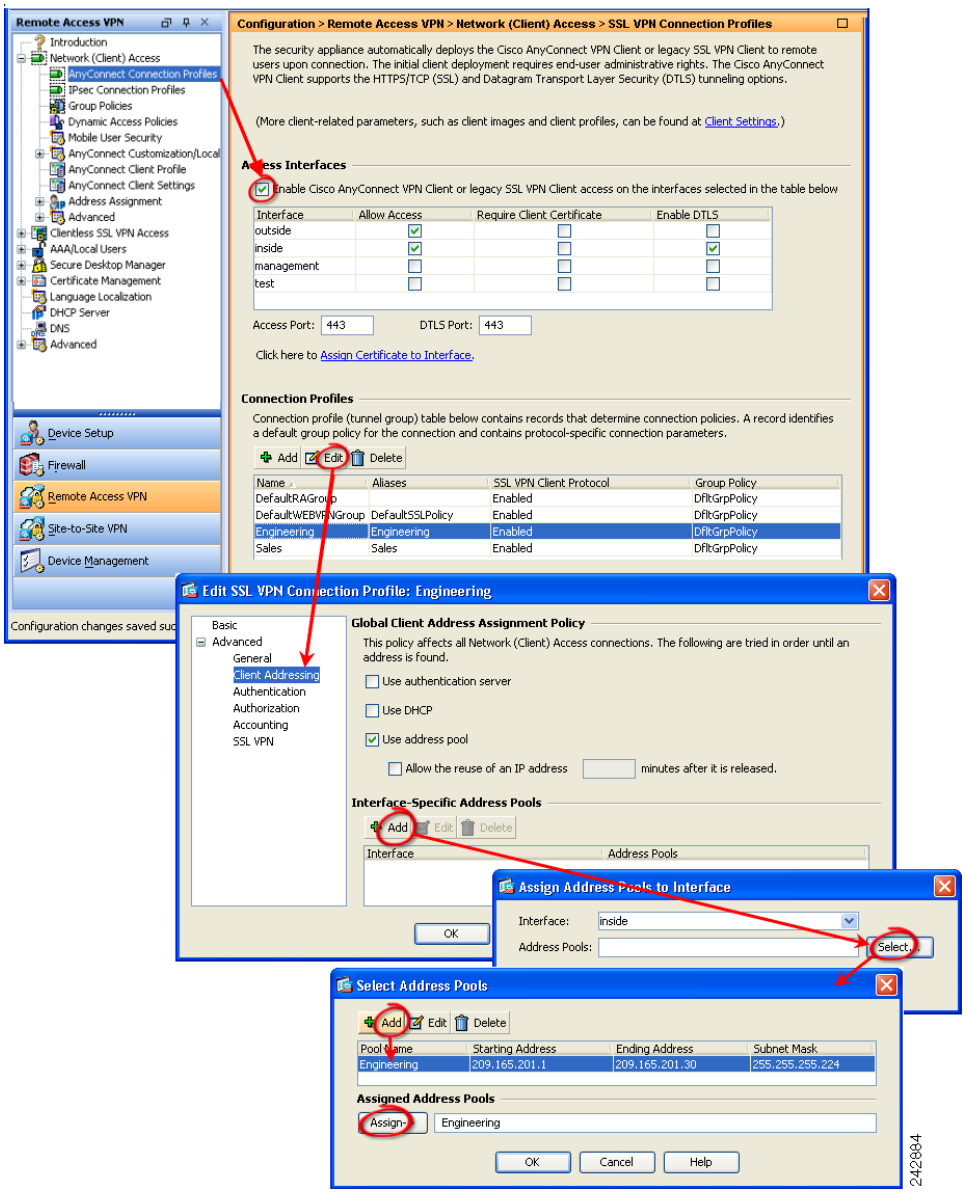
Figure 2-9 Add IP Pool Dialog



Step 8 Enable the AnyConnect 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 2-10) to enable AnyConnect and then assign an address pool.

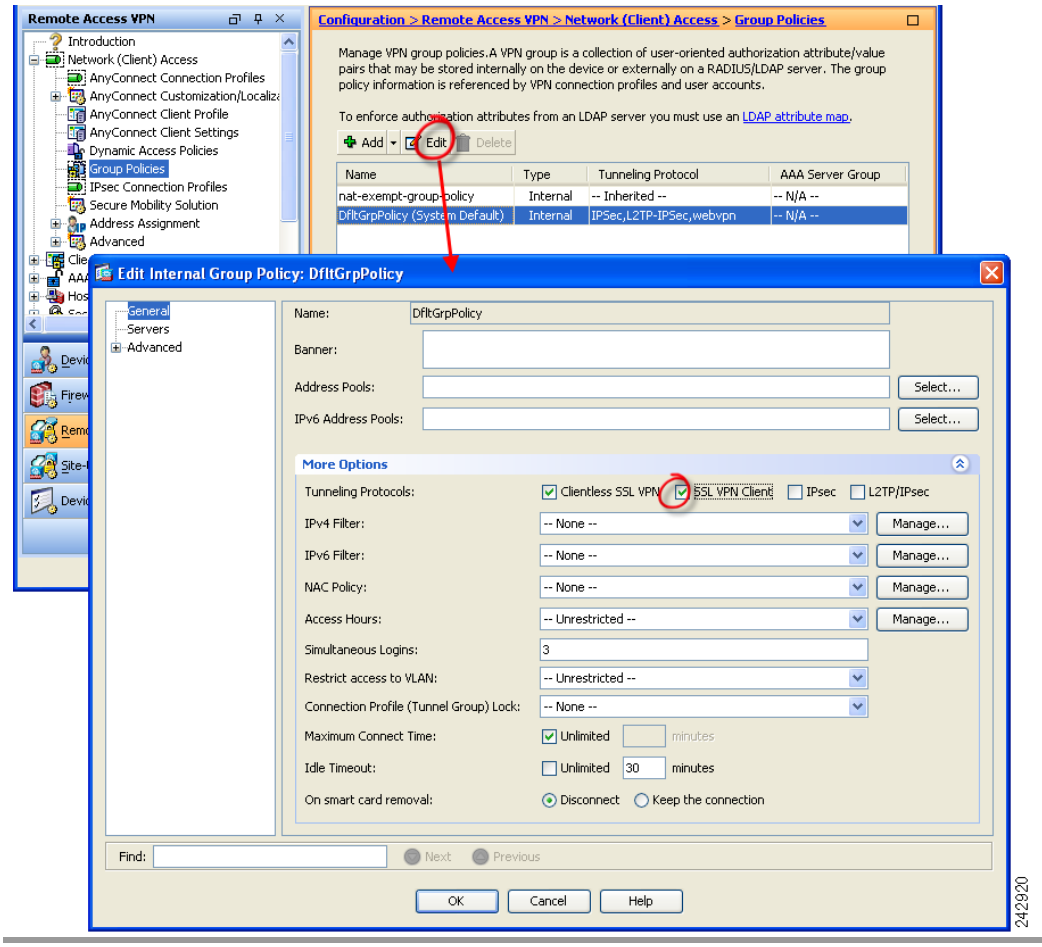
Figure 2-10 Enable AnyConnect Download



Step 9 Specify SSL VPN Client 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 2-11 to enable SSL VPN Client for the group.

Figure 2-11 Specify SSL VPN as a Tunneling Protocol



Prompting Remote Users to Download AnyConnect

By default, the ASA does not download AnyConnect 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 AnyConnect. Alternatively, you can configure the ASA to immediately download AnyConnect without displaying the clientless portal page.

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

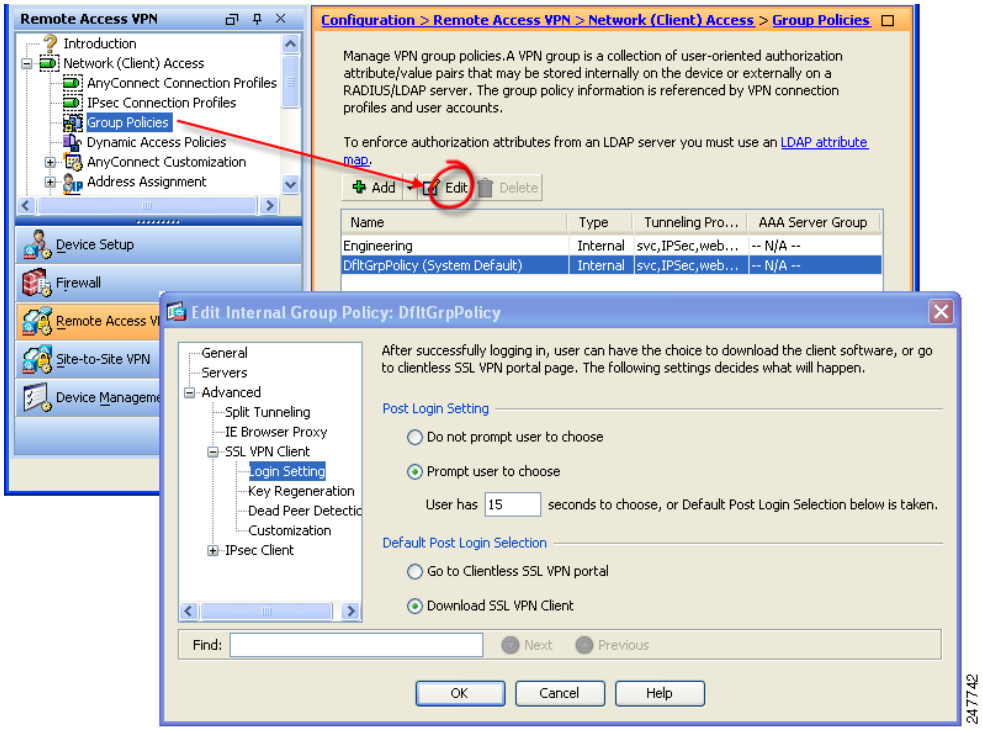
You can configure this feature for a group policy or user. To change these login settings, follow this procedure:

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 2-12).

Step 2 In the navigation pane, choose **Advanced > AnyConnect Client > Login Settings**. The Post Login settings display. Uncheck 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.

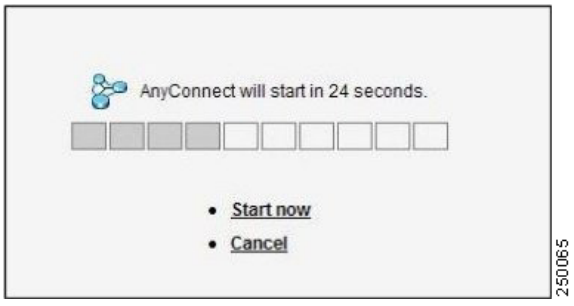
Figure 2-12 Changing Login Settings



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

Figure 2-13 shows the prompt displayed to remote users if you choose **Prompt user to choose** and **Download SSL VPN Client**:

Figure 2-13 Post Login Prompt Displayed to Remote Users



Enabling Modules for Additional Features

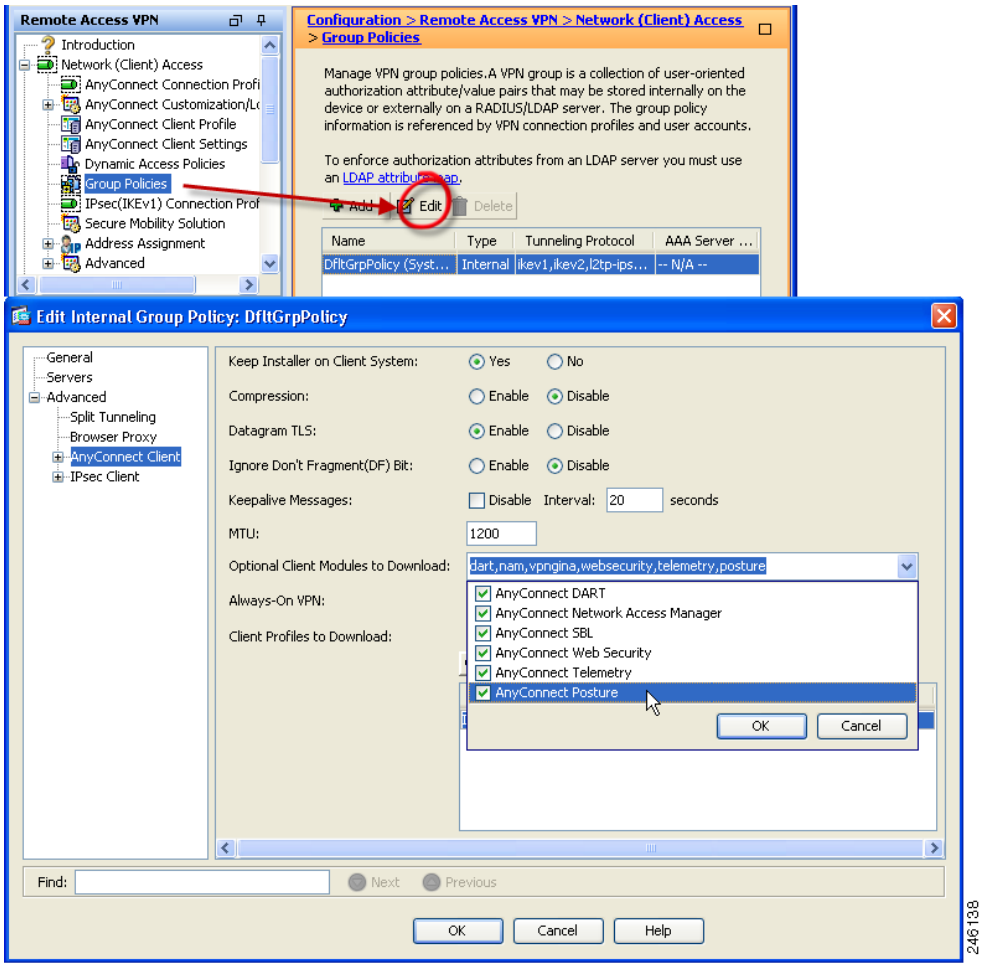
As you enable features on AnyConnect, it must update the modules on the VPN endpoints to use the new features. To minimize download time, AnyConnect requests downloads (from the ASA) only of modules that it needs for each feature that it supports.

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**. Choose a group policy and click **Edit**. The Edit Internal Group Policy window displays (Figure 2-14).

Step 2 In the navigation pane, select **Advanced > AnyConnect Client**. Click the **Optional Client Module to Download** drop-list and choose modules.

Figure 2-14 Specifying an Optional Client Module to Download



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

Note If you choose Start Before Logon, you must also enable this feature in the AnyConnect client profile. See Chapter 3, "Configuring VPN Access" for details.

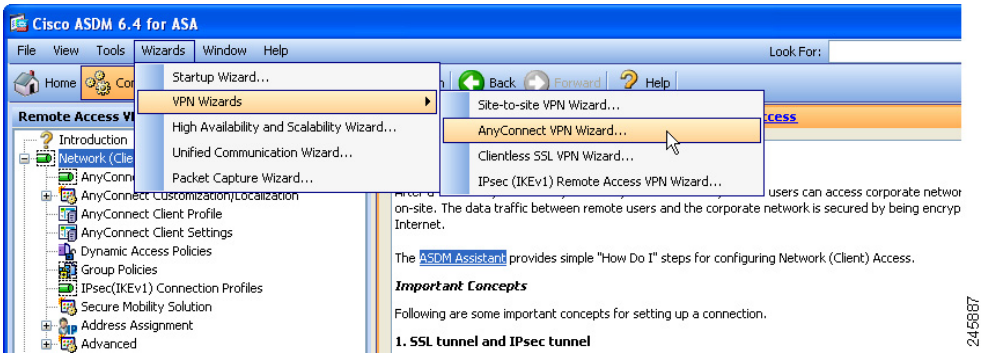
Enabling IPsec IKEv2 Connections

This section provides a procedure for enabling IPsec IKEv2 connections on the ASA.

After loading an AnyConnect client package on the ASA, configure the ASA for IPsec IKEv2 connections by following these steps:

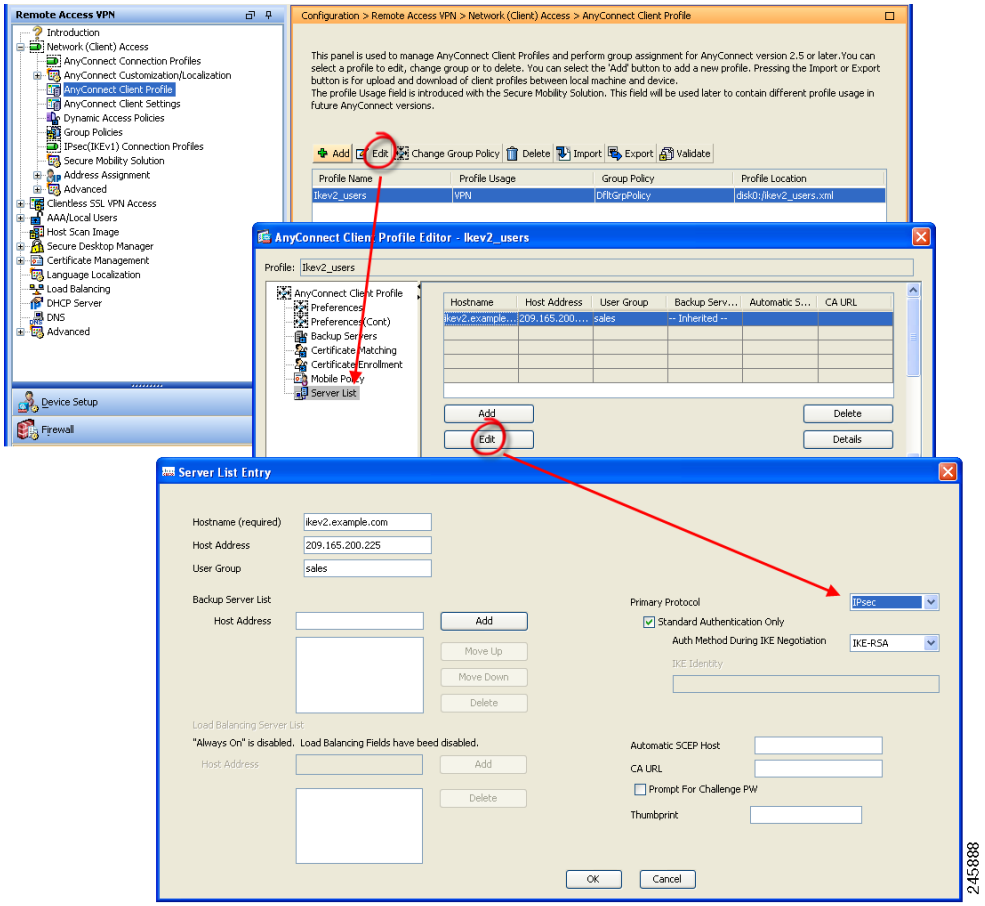
Step 1 Run the AnyConnect VPN Wizard. Choose **Tools >Wizards > AnyConnect VPN Wizard** (Figure 2-15). Follow the wizard steps to create a basic VPN connection for IPsec IKEv2 connections.

Figure 2-15 AnyConnect VPN Wizard



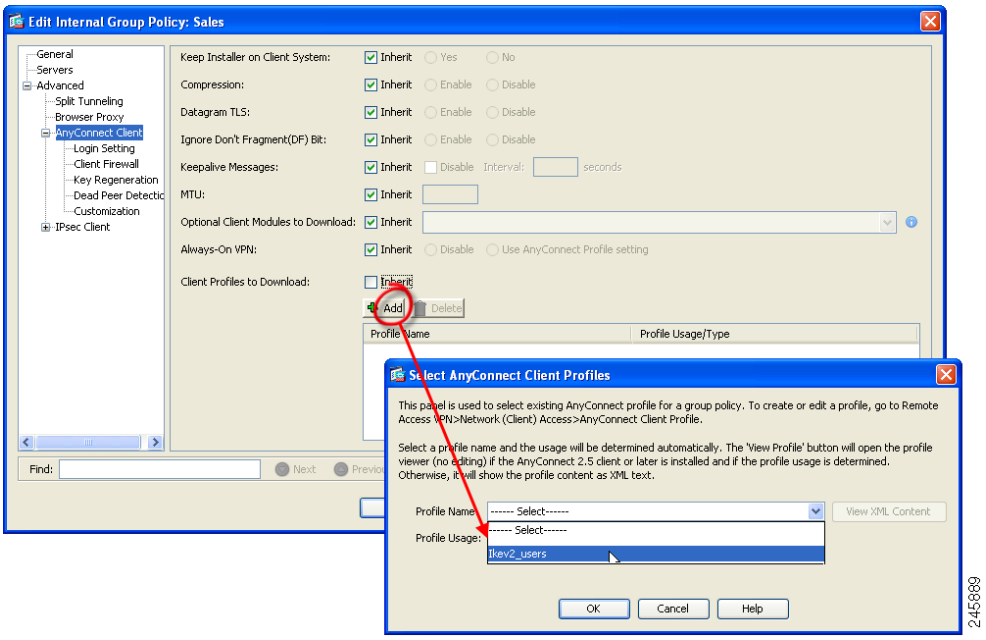
Step 2 Edit the Server List entry of the VPN profile using the profile editor. Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile** (figure).

Figure 2-16 Specifying IKEv2 in an AnyConnect Client Profile



Step 3 Associate the VPN profile with the group policy to be used. Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Edit a group policy and navigate to **Advanced > AnyConnect Client** (Figure 2-17).

Figure 2-17 Associating a Profile with a Group Policy



Predeploying an IKEv2-Enabled Client Profile

If you are predeploying the client using a software management system, you must predeploy the IKEv2-enabled client profile also. Follow these steps:

Step 1 Extract the .ISO using Winzip or 7-zip, or a similar utility.

Step 2 Browse to this folder:

anyconnect-win-3.0.0xxx-pre-deploy-k9\Profiles\vpn

Step 3 Copy the IKEv2/IPSec VPN profile that you created using the profile editor (ASDM version or standalone version) to this folder.

Step 4 Run Setup.exe to run the installer, and uncheck *Select all* and check *AnyConnect VPN Module* only.

Predeploying the Client Profile with a Virtual CD Mount Software

You can also predeploy the client profile using a virtual CD mount software, such as SlySoft or PowerISO. Follow these steps:

Step 1 Mount the .ISO with a virtual CD mount software.

Step 2 After installing the software, deploy the profile to the appropriate folder as show in Table 2-1:

Table 2-3 Paths to Deploy the Client

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

Other Predeployment Tips

If you are using the MSI installer, if you place the client profile with the MSI in the Profiles\vpn folder, the MSI picks the profile and places it in the appropriate folder during installation.

If you are preploying the profile manually after the installation, copy the profile manually or use a SMS, such as Altiris, to deploy the profile to the appropriate folder.

Weblaunching the Client

To Weblaunch the AnyConnect client, instruct users to login and download the AnyConnect client by entering the URL of the ASA in the their browser using the following format:

https://<asa>

Predeploying the AnyConnect Client and Optional Modules

This section describes the process of predeploying the AnyConnect Secure Mobility Client and includes information you need for deploying the client using enterprise software deployment systems.

The following sections describe how to predeploy the AnyConnect client:

- Predeployment ISO Package File Information, page 2-25
- Predeploying to Windows Computers, page 2-26
- Predeploying to Linux and Mac OS X Computers, page 2-32
- Predeploying AnyConnect 2.5 on a Windows Mobile Device, page 2-34
- AnyConnect File Information, page 2-35

Predeployment ISO Package File Information

The core AnyConnect VPN client and the optional modules (such as SBL, AnyConnect Diagnostic Reporting Tool, etc.) are installed and updated by their own installation file or program. For AnyConnect version 3.0, Windows desktop installation files are contained in an ISO image (*.iso). For all other platforms, you can distribute the individual installation files in the same way you did for AnyConnect version 2.5 and earlier, separately at your discretion using your methodology.

Table 2-4 shows the filenames of the AnyConnect packages for predeployment for each OS:

Table 2-4 AnyConnect Package Filenames for Predeployment

OS	AnyConnect 3.0 Predeploy Package Name
Windows	anyconnect-win-<*version*>-k9.iso
Mac OS X	anyconnect-macosx-i386-<*version*>-k9.dmg
Linux	anyconnect-linux-<*version*>-k9.tar.gz
Linux-64	anyconnect-Linux_64-<*version*>-k9.tar.gz **Note** The 64 bit version of Linux is in its Beta release cycle.

Predeploying to Windows Computers

The AnyConnect 3.0 predeploy installation for Windows computers (desktops, not mobile) is distributed in an ISO image. The ISO package file contains the *Install Utility*, a selector menu program to launch the individual component installers, and the MSIs for the core and optional AnyConnect modules.

The following sections describe how to predeploy to Windows computers:

- Deploying the ISO File, page 2-26
- Deploying the Install Utility to Users, page 2-27
- Required Order for Installing or Uninstalling AnyConnect Modules for Windows, page 2-28
- Installing Predeployed AnyConnect Modules, page 2-28
- Instructing Users to Install NAM and Web Security as Stand-Alone Applications, page 2-30
- Packaging the MSI Files for Enterprise Software Deployment Systems, page 2-30
- Upgrading Legacy Clients and Optional Modules, page 2-31
- Customizing and Localizing the Installer, page 2-32

Deploying the ISO File

The predeployment package is bundled in an ISO package file that contains the programs and MSI installer files to deploy to user computers. When you deploy the ISO package file, the setup program (setup.exe) runs and deploys the Install Utility menu, a convenient GUI that lets users choose which AnyConnect modules to install.

If you prefer, you can break out the individual installers from the ISO image and distribute them manually. Each installer in the predeploy package can run individually. The order you deploy the files is very important. See Required Order for Installing or Uninstalling AnyConnect Modules for Windows for more information.

Table 2-5 lists the files contained in the ISO package file and the purpose of each file:

Table 2-5 Contents of the ISO File for Predeployment

File	Purpose
GUI.ico	The AnyConnect icon image.
Setup.exe	Launches the Install Utility (setup.hta).
anyconnect-dart-win-<*version*>-k9.msi	MSI installer file for the DART optional module.

File	Purpose
anyconnect-gina-win-<*version*>-pre-deploy-k9.msi	MSI installer file for the SBL optional module.
anyconnect-nam-win-<*version*>.msi	MSI installer file for the NAM optional module.
anyconnect-posture-win-<*version*>-pre-deploy-k9.msi	MSI installer file for the posture optional module.
anyconnect-telemetry-win-<*version*>-pre-deploy-k9.msi	MSI installer file for the telemetry optional module.
anyconnect-websecurity-win-<*version*>-pre-deploy-k9.msi	MSI installer file for the web security optional module.
anyconnect-win-<*version*>-pre-deploy-k9.msi	MSI installer file for the AnyConnect core client.
autorun.inf	The Setup Information file for setup.exe.
cues_bg.jpg	A background image for the Install Utility GUI.
setup.hta	Install Utility HTML Application (HTA). You can customize this program.
update.txt	A text file listing the AnyConnect version number.

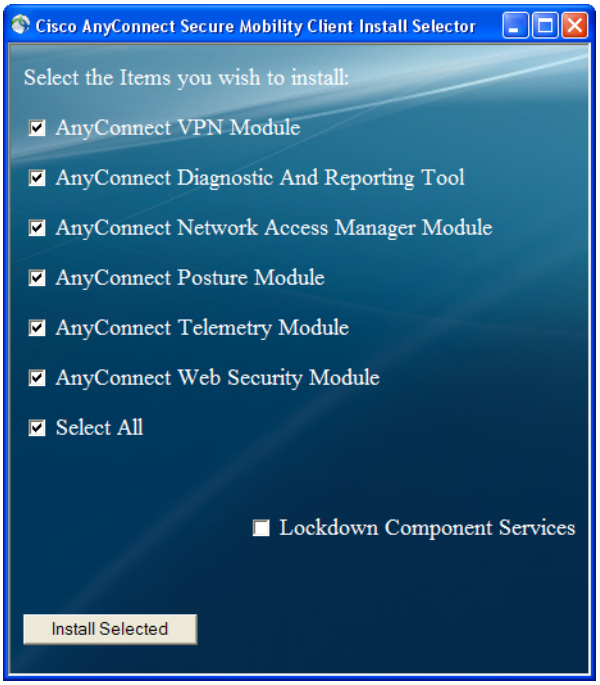
Deploying the Install Utility to Users

With the Install Utility, users select the items they want to install. By default, the check boxes for all the components are checked. If acceptable, the user can click the Install button and agree to the components listed in the Selections To Install dialog box. The program determines what components to install based upon their selection.

The Install Utility is an HTML Application (HTA) named *setup.hta* that is packaged in the ISO package file. You are free to make any changes you want to this program. Customize the utility as you prefer.

Figure 2-18 shows the Install Utility GUI:

Figure 2-18 Install Utility GUI



Each installer runs silently. If an installer requires that the user reboot the computer, the user is informed after the final installer runs. The Install Utility does not initiate the reboot. The user must reboot the computer manually.

Required Order for Installing or Uninstalling AnyConnect Modules for Windows

If you prefer, you can break out the individual installers from the ISO image and distribute them manually. Each installer in the predeploy package can run individually. Use a compressed file utility to view and extract the files in the .iso file.

If you distribute files manually, you must address the dependencies between the selected components. The core client MSI contains all VPN functional components and the common components needed for use by the optional modules. In addition, the installers for the optional modules require that the same version of AnyConnect 3.0 core client be installed as a prerequisite. These installers check for the existence of the same version of the core client before proceeding to install.

Installing Order

The order of installation is important. Install the AnyConnect modules in the following order:

1. Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).
2. Install the AnyConnect Diagnostic and Reporting Tool (DART) module, which provides useful diagnostic information about the AnyConnect core client installation.
3. Install the SBL, NAM, web security, or posture modules in any order.
4. Install the telemetry module, which requires the posture module.

Note Individual installers for optional modules check the version of the installed core VPN client before installing. The versions of the core and optional modules must match. If they do not match, the optional module does not install and the installer notifies the user of the mismatch. If you use the Install Utility, the modules in the package are built and packaged together and the versions always match.

Uninstalling Order

The order of uninstallation is also important. Use the following order for uninstalling the modules:

1. Uninstall the telemetry module.
2. Uninstall NAM, Web Security, Posture, or SBL, in any order.
3. Uninstall the AnyConnect core client.
4. Uninstall DART last. DART information is valuable should the uninstall processes fail.

Installing Predeployed AnyConnect Modules

When predeploying AnyConnect modules, administrators need to copy the predeployment module to the endpoint along with its corresponding client profile, if the module requires one.

Note If you are using NAM, you should choose the **Hide icon and notifications** option to hide the Microsoft *Network* icon when predeploying Windows. By default, the icon is in *Only show notifications* mode, which alerts you to changes and updates.

These modules require an AnyConnect client profile:

- AnyConnect VPN Module
- AnyConnect Telemetry Module
- AnyConnect Network Access Manager Module
- AnyConnect Web Security Module

These features do not require an AnyConnect client profile:

- AnyConnect VPN Start Before Login
- AnyConnect Diagnostic and Reporting Tool
- AnyConnect Posture Module

The predeployment modules need to be installed in the order described in the "Required Order for Installing or Uninstalling AnyConnect Modules for Windows" section on page 2-28.

To predeploy the optional AnyConnect modules along with the VPN module, follow this procedure:

Step 1 Download **anyconnect-win-<*version*>-pre-deploy-k9.iso** from cisco.com.

Step 2 Extract the contents of the .iso file using Winzip or 7-zip, or a similar utility.

Step 3 For those modules that require a client profile, use the profile editor integrated with ASDM or the standalone profile editor to create a client profile for the modules you want to install. See these chapters for instructions on configuring various client profiles:

- Chapter 3, "Configuring VPN Access"
- Chapter 4, "Configuring Network Access Manager (NAM)"
- Chapter 6, "Configuring Web Security"
- Chapter 7, "Configuring AnyConnect Telemetry to the WSA"

Step 4 Once you have created the client profile, copy it to the appropriate directory you extracted from the .iso file:

- Profiles\vpn
- Profiles\nam
- Profiles\websecurity
- Profiles\telemetry

Step 5 Use Table 2-5, "Contents of the ISO File for Predeployment" to identify the packages designed for predeploying your AnyConnect modules.

Step 6 Using a software management system, deploy the predeployment software packages and the **Profiles** directory containing the client profiles to the endpoints.

Step 7 Using the procedures described in "Packaging the MSI Files for Enterprise Software Deployment Systems" section on page 2-30 to install the AnyConnect modules in the order defined in "Required Order for Installing or Uninstalling AnyConnect Modules for Windows" section on page 2-28.

Instructing Users to Install NAM and Web Security as Stand-Alone Applications

You can deploy the AnyConnect modules NAM and Web Security as standalone applications on a user computer. If you deploy the Install Utility to users, instruct them to check:

AnyConnect Network Access Manager **and/or** *AnyConnect Web Security Module*

However, also instruct them to **uncheck** *Cisco AnyConnect VPN Module*. Doing so disables the VPN functionality of the core client, and the Install Utility installs NAM and Web Security as standalone applications with no VPN functionality.

If you do not deploy the Install Utility, you must disable VPN functionality by configuring your software management system (SMS) to set the MSI property PRE_DEPLOY_DISABLE_VPN=1. For example:

```
msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx*
```

By doing this, the MSI copies the VPNDisable_ServiceProfile.xml file embedded in the MSI to the directory specified for profiles for VPN functionality (see Table 2-15 for the file path).

Note The VPNDisable_ServiceProfile.xml file must also be the only AnyConnect profile in VPN client profile directory.

Then you can run the installers for the optional modules, which can use the AnyConnect GUI, but without VPN service.

When the user clicks the **Install Selected** button, the following happens:

Step 1 A pop-up dialog box confirms the selection of the standalone Network Access Manager and/or the standalone Web Security Module.

Step 2 When the user clicks OK, the Install Utility invokes the AnyConnect 3.0 core installer with a setting of PRE_DEPLOY_DISABLE_VPN=1.

Step 3 The Install Utility removes any existing VPN profiles and then installs VPNDisable_ServiceProfile.xml.

Step 4 The Install Utility invokes the NAM installer and/or the Web Security installer.

Step 5 AnyConnect 3.0 Network Access Manager and/or Web Security Module is enabled without VPN service on the computer.

Note If a previous installation of NAM did not exist on the computer, the user must reboot the computer to complete the NAM installation. Also, if the installation is an upgrade that required upgrading some of the system files, the user must reboot.

Packaging the MSI Files for Enterprise Software Deployment Systems

This section provides information you need to deploy the AnyConnect client and optional modules using an enterprise software deployment system, including the MSI install command line calls and the locations to deploy profiles:

- MSI Install Command Line Calls, page 2-31
- Locations to Deploy the AnyConnect Profiles, page 2-37
- Installing NAM or Web Security as Standalone Applications, page 2-31

MSI Install Command Line Calls

Table 2-6 shows the MSI install command line calls to use to install individual AnyConnect modules. It also shows the log file produced by the command:

Table 2-6 MSI Install Command Line Calls and Log Files Generated

Module Installed	Command and Log File
AnyConnect core client **No VPN** capability. Use when installing standalone NAM or web security modules.	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-<*version*>-pre-deploy-k9-install-datetimestamp.log
AnyConnect core client **With VPN** capability.	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-win-<*version*>-pre-deploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool (DART)	msiexec /package anyconnect-dart-win-ver-k9.msi /norestart /passive /lvx* anyconnect-dart-<*version*>-pre-deploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-gina-win-ver-k9.msi /norestart /passive /lvx* anyconnect-gina-<*version*>-pre-deploy-k9-install-datetimestamp.log
NAM	msiexec /package anyconnect-nam-win-ver-k9.msi /norestart /passive /lvx* anyconnect-nam-<*version*>-pre-deploy-k9-install-datetimestamp.log
Web security	msiexec /package anyconnect-websecurity-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-websecurity-<*version*>-pre-deploy-k9-install-datetimestamp.log
Posture	msiexec /package anyconnect-posture-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-posture-<*version*>-pre-deploy-k9-install-datetimestamp.log
Telemetry	msiexec /package anyconnect-telemetry-win-ver-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-telemetry-<*version*>-pre-deploy-k9-install-datetimestamp.log

Installing NAM or Web Security as Standalone Applications

To install NAM and/or web security without VPN service, you must run the following command:

msiexec /package anyconnect-win-ver-pre-deloy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1

When the MSI for the core client runs, it installs or updates the core client and deletes any existing profiles and installs VPNDisable_ServiceProfile.xml in the profiles location. Then you can run the installers for the optional modules. The standalone components can then use the AnyConnect GUI, but without VPN service.

Upgrading Legacy Clients and Optional Modules

When upgrading earlier versions, the AnyConnect Secure Mobility Client version 3.0:

- Upgrades all previous versions of the core client and retains all VPN configurations.
- Upgrades Cisco SSC 5.x to the Network Access Manager (NAM) module, retains all SSC configurations for use with NAM, and removes SSC 5.x.

- Upgrades the Host Scan files used by Cisco Secure Desktop. The AnyConnect 3.0 client can co-exist with Secure Desktop.
- ***Does not*** upgrade the Cisco IPsec VPN client (or remove it). However, the AnyConnect 3.0 client can coexist on the computer with the IPsec VPN client.
- ***Does not*** upgrade and cannot coexist with ScanSafe Web Security functionality on the same computer. You must uninstall AnyWhere+.

Customizing and Localizing the Installer

You can customize the AnyConnect core installer for Windows using transforms and you can translate messages displayed by the core installer in the language preferred by the remote user. For more information on customizing and localizing (translating) the AnyConnect client and installer, see Chapter 11, "Customizing and Localizing the AnyConnect Client and Installer."

Predeploying to Linux and Mac OS X Computers

The following sections contain information specific to predeploying to Linux and Mac OS X computers, and contains the following sections:

Recommended Order for Installing or Uninstalling Modules for Linux and MAC OS X

You can break out the individual installers for Linux and Mac and distribute them manually. Each installer in the predeploy package can run individually. Use a compressed file utility to view and extract the files in the tar.gz or .dmg file.

If you distribute files manually, we strongly recommend the following installation order:

1. Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).
2. Install the DART module, which provides useful diagnostic information about the AnyConnect core client installation.
3. Install the posture module.

Uninstalling AnyConnect Modules

The order of uninstallation is also important. Use the following order for uninstalling the modules:

1. Uninstall the posture module.
2. Uninstall the AnyConnect core client.
3. Uninstall DART last. DART information is valuable should the uninstall processes fail.

AnyConnect Requirements for Computers Running Ubuntu 9.x 64-Bit

For the Cisco AnyConnect Secure Mobility client to run on a computer running Ubuntu 9.x 64-Bit, AnyConnect needs the following:

- The 32-bit compatibility library installed on the computer.
- The NSS crypto libraries from the Ubuntu 9.x 32-bit version installed in /usr/local/firefox.
- The profile .mozilla/firefox in the user home directory so it can interact with the Firefox certificate store.

Follow these steps to address these issues:

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.

AnyConnect 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, logged in as the user who will use AnyConnect.

Doing so creates the .mozilla/firefox profile in the user home directory, which is required by AnyConnect to interact with the Firefox certificate store.

Step 5 Install AnyConnect in standalone mode.

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

If users use WebLaunch to start AnyConnect on a Mac and the Java installer fails, a dialog box presents a Manual Install link. Have users follow this procedure when this happens:

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 Secure Mobility Client** to initiate an AnyConnect session.

Predeploying AnyConnect 2.5 on a Windows Mobile Device

AnyConnect 3.0 does not support Windows Mobile devices. However, you can deploy AnyConnect 2.5 to a Windows Mobile device using the ASA in a limited way. Unlike the non-mobile packages, the client for Windows Mobile does not self-install or launch a VPN connection after self-installing. Users make an initial SSL connection to an ASA using their browser, and the ASA downloads the client. Then users must locate the downloaded package and follow the installation wizard directions.

Alternatively, you can predeploy AnyConnect 2.5 to Windows Mobile devices, or users can download and install the client on their device.

Note Some mobile devices have a proxy enabled by default. To ensure AnyConnect can pass data over the SSL connection, remote users may need to configure the mobile device to bypass the proxy.

To ASA-deploy, download anyconnect-wince-ARMv4I-<*version*>-k9.pkg from the Cisco software download page and upload it to the ASA. See Configuring the ASA to Web Deploy AnyConnect, page 2-7 for more information. Instruct users to open the client package file downloaded by the ASA and use the installation wizard to complete the installation.

To predeploy the client, follow these steps:

Step 1 Download one of the following files from the Cisco AnyConnect Download Software site to get the AnyConnect client, version 2.5 for Windows Mobile:

- CAB package signed by Cisco:

  anyconnect-wince-ARMv4I-<*version*>-k9.cab

- ActiveSync MSI package:

  anyconnect-wince-ARMv4I-activesync-<*version*>-k9.msi

Step 2 Transfer the file to a corporate server if you want to provide users with a link to AnyConnect.

Step 3 Make sure the Windows Mobile device meets the system requirements in the latest Cisco AnyConnect Secure Mobility Release Notes.

Step 4 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 5 Use the mobile device to open the file you transferred, and proceed with the installation wizard.

AnyConnect File Information

This section provides information about the location of AnyConnect files on the user computer in the following sections:

Filenames of Modules on the Endpoint Computer

Table 2-7 shows the AnyConnect filenames on the endpoint computer for each operating system type when you predeploy or ASA-deploy the client:

Table 2-7 AnyConnect Core Filenames for ASA or Predeployment

AnyConnect 3.0 Core	Web-Deploy Installer (Downloaded)	Predeploy Installer
Windows	anyconnect-win-(ver)-web-deploy-k9.exe	anyconnect-win-(ver)-pre-deploy-k9.msi
Mac	anyconnectsetup.dmg	anyconnect-macosx-i386-(ver)-k9.dmg
Linux	anyconnectsetup.sh	anyconnect-linux-(ver)-k9.tar.gz
Linux-64	anyconnectsetup.sh	anyconnect-Linux_64-(ver)-k9.tar.gz **Note** The 64 bit version of Linux is in its Beta release cycle.

Table 2-8 shows the DART filenames on the endpoint computer for each operating system type when you predeploy or ASA-deploy the client:

Table 2-8 DART Package Filenames for ASA or Predeployment

DART	Web-Deploy Installer (Downloaded)	Predeploy Installer
Windows	anyconnect-dart-win-(ver)-k9.msi	anyconnect-dart-win-(ver)-k9.msi
Mac	anyconnect-dartsetup.dmg	anyconnect-dart-macosx-i386-(ver)-k9.dmg
Linux	anyconnect-dartsetup.sh	anyconnect-dart-linux-(ver)-k9.tar.gz
Linux-64	anyconnect-dartsetup.sh	anyconnect-dart-linux-64-(ver)-k9.tar.gz **Note** The 64 bit version of Linux is in its Beta release cycle.

Table 2-9 shows the SBL filenames on the endpoint computer when you predeploy or ASA-deploy the client to a Windows computer:

Table 2-9 Start Before Logon Package Filename for ASA or Predeployment

SBL (Gina)	Web-Deploy Installer (Downloaded)	Predeploy Installer
Windows	anyconnect-gina-win-(ver)-web-deploy-k9.exe	anyconnect-gina-win-(ver)-pre-deploy-k9.msi

Table 2-10 shows the NAM filenames on the endpoint computer when you predeploy or ASA-deploy the client to a Windows computer:

Table 2-10 Network Access Manager Filename for ASA or Predeployment

NAM	Web-Deploy Installer (Downloaded)	Predeploy Installer
Windows	anyconnect-nam-win-(ver)-k9.msi	anyconnect-nam-win-(ver)-k9.msi

Table 2-11 shows the posture module filenames on the endpoint computer for each operating system type when you predeploy or ASA-deploy the client:

Table 2-11 Posture Module Filename for ASA or Predeployment

Posture	Web-Deploy Installer (Downloaded)	Predeploy Installer
Windows	anyconnect-posture-win-(ver)-web-deploy-k9.msi	anyconnect-posture-win-(ver)-pre-deploy-k9.msi
Mac	anyconnect-posturesetup.dmg	anyconnect-posture-macosx-i386-(ver)-k9.dmg
Linux	anyconnect-posturesetup.sh	anyconnect-posture-linux-(ver)-k9.tar.gz
Linux-64	anyconnect-posturesetup.sh	anyconnect-posture-linux-(ver)-k9.tar.gz

Table 2-12 shows the telemetry module filenames on the endpoint computer for Windows when you predeploy or ASA-deploy the client:

Table 2-12 Telemetry Filename for ASA or Predeployment

Telemetry	Web-Deploy Installer (Downloaded)	Predeploy Installer
Windows	anyconnect-telemetry-win-(ver)-web-deploy-k9.exe. Dependent upon installation of anyconnect-posture-win-(ver)-web-deploy-k9.msi	anyconnect-telemetry-win-(ver)-pre-deploy-k9.msi. Dependent upon installation of anyconnect-posture-win-(ver)-pre-deploy-k9.msi.

Table 2-13 shows the Web Security module filenames on the endpoint computer for Windows when you predeploy or ASA-deploy the client:

Table 2-13 Web Security Filename for ASA or Predeployment

Web Security	Web-Deploy Installer (Downloaded)	Predeploy Installer
Windows	anyconnect-websecurity-win-(ver)-web-deploy-k9.exe	anyconnect-websecurity-win-(ver)-pre-deploy-k9.msi

Locations to Deploy the AnyConnect Profiles

Table 2-14 shows the profile-related files AnyConnect downloads AnyConnect on the local computer and their purpose:

Table 2-14 Profile Files on the Endpoint

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

Table 2-15 shows the locations of the AnyConnect profiles for all operating systems:

Table 2-15 Profile Locations for all Operating Systems

Operating System	Module	Location
Windows XP	Core client with VPN	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Profile
	NAM	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	Telemetry	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web security	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
Windows Vista	Core client with VPN	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	NAM	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	Telemetry	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web security	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
Windows 7	Core client with VPN	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	NAM	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	Telemetry	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web security	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
Mac OS X	All modules	/opt/cisco/vpn/profile
Linux	All modules	/opt/cisco/vpn/profile

User Preferences Files Installed on the Local Computer

Some profile settings are stored locally on the user computer in a user preferences file or a global preferences file. The user file has information the client needs to display user-controllable settings in the Preferences tab of the client GUI and information about the last connection, such as the user, the group, and the host.

The global file has information about user-controllable settings to be able to apply those settings before login (since there is no user). For example, the client needs to know if Start Before Logon and/or AutoConnect On Start are enabled before login.

Table 2-16 shows the filenames and installed paths for preferences files on the client computer:

Table 2-16 User Preferences Files and Installed Paths

Operating System	Type	File and Path
Windows Vista Windows 7	User	C:\Users*username*\AppData\Local\Cisco\ Cisco AnyConnect VPN Client\preferences.xml
	Global	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\ preferences_global.xml
Windows XP	User	C:\Documents and Settings**username**\Local Settings\ApplicationData\ Cisco\Cisco AnyConnect VPN Client\preferences.xml
	Global	C:\Documents and Settings\AllUsers\Application Data\Cisco\ Cisco AnyConnect VPN Client\preferences_global.xml
Mac OS X	User	/Users/username/.anyconnect
	Global	/opt/cisco/vpn/.anyconnect_global
Linux	User	/home/username/.anyconnect
	Global	/opt/cisco/vpn/.anyconnect_global

Standalone AnyConnect Profile Editor

Note The standalone AnyConnect profile editor allows administrators to configure client profiles for the VPN, Network Access Manager (NAM), and Web Security Modules for the AnyConnect Secure Mobility Client. These profiles can be distributed with predeployment kits for the VPN, NAM and Web Security modules. The standalone AnyConnect profile editor delivered with this release of AnyConnect is in its beta release cycle.

System Requirements for Standalone Profile Editor

Supported Operating Systems

This application has been tested on Windows XP and Windows 7. The MSI only runs on Windows.

Java Requirement

This application requires JRE 1.6. If it is not installed, the MSI installer will automatically install it.

Browser Requirement

The help files in this application are supported by Firefox and Internet Explorer. They have not been tested in other browsers.

Required Hard Drive Space

The Cisco AnyConnect Profile Editor application requires less than five megabytes of hard drive space. JRE 1.6 requires less than 100 megabytes of hard drive space.

Installing the Standalone AnyConnect Profile Editor

The standalone AnyConnect profile editor is distributed as a windows executable file (.exe) separately from the AnyConnect ISO and .pkg files and has this file naming convention: **anyconnect-profileeditor-win-<*version*>-k9.exe**.

To install the standalone profile editor, follow this procedure:

Step 1 Download the **anyconnect-profileeditor-win-<*version*>-k9.exe** from Cisco.com.

Step 2 Double-click **anyconnect-profileeditor-win-<*version*>-k9.exe** to launch the installation wizard.

Step 3 At the Welcome screen, click **Next**.

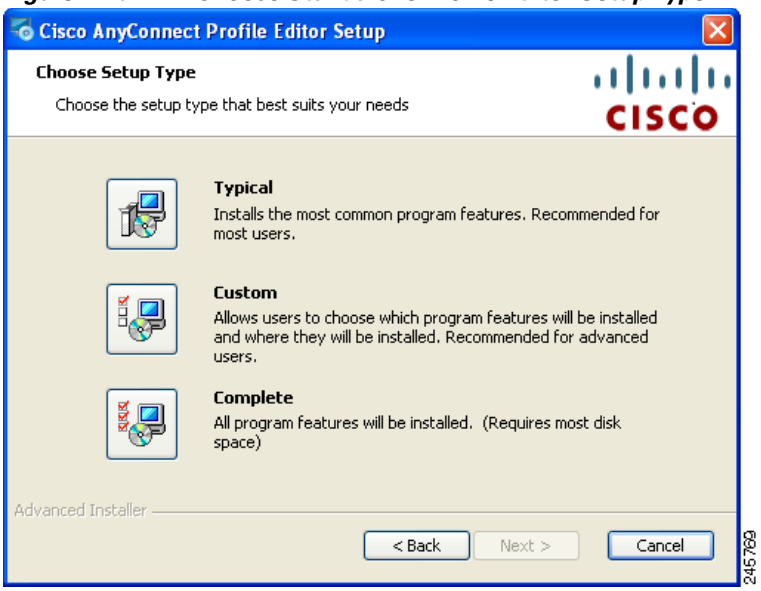
Figure 2-19 Standalone Profile Editor Welcome Screen

Step 4 At the **Choose Setup Type** window click one of these buttons and click **Next**:

- **Typical** - Installs only the Network Access Manager profile editor automatically.

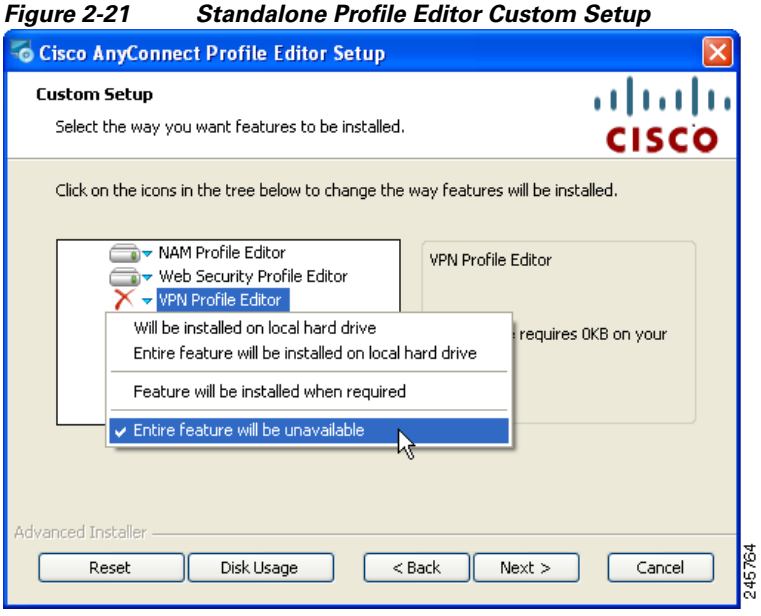
- **Custom** - Allows you to choose any of these profile editors to install: NAM Profile Editor, Web Security Profile Editor, and VPN Profile Editor.
- **Complete** - Automatically installs the NAM Profile Editor, Web Security Profile Editor and VPN Profile Editor.

Figure 2-20 Choose Standalone Profile Editor Setup Type



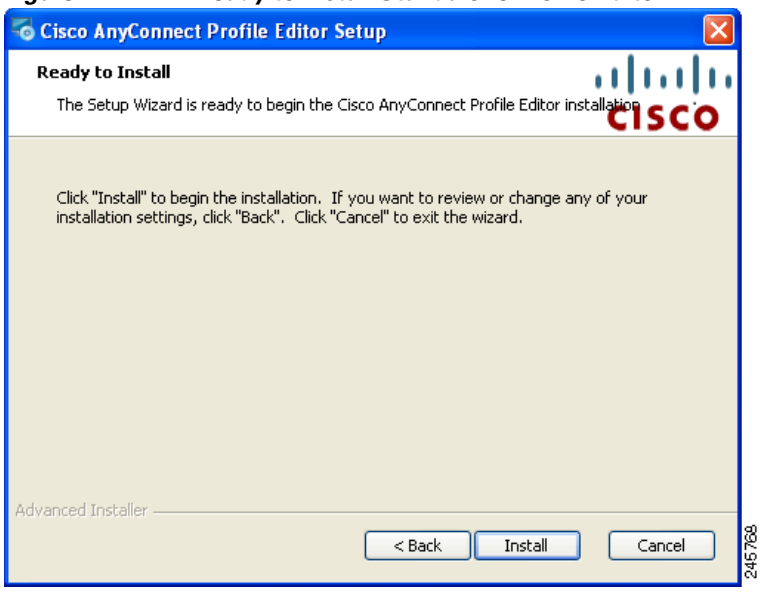
Step 5 If you clicked **Typical** or **Complete** in the previous step, skip to Step 6. If you clicked **Custom** in the previous step, click the icon for the standalone profile editor you want to install and select **Will be installed on local hard drive** or click **Entire Feature will be unavailable** to prevent the standalone profile editor from being installed. Click **Next**.

Figure 2-21 Standalone Profile Editor Custom Setup



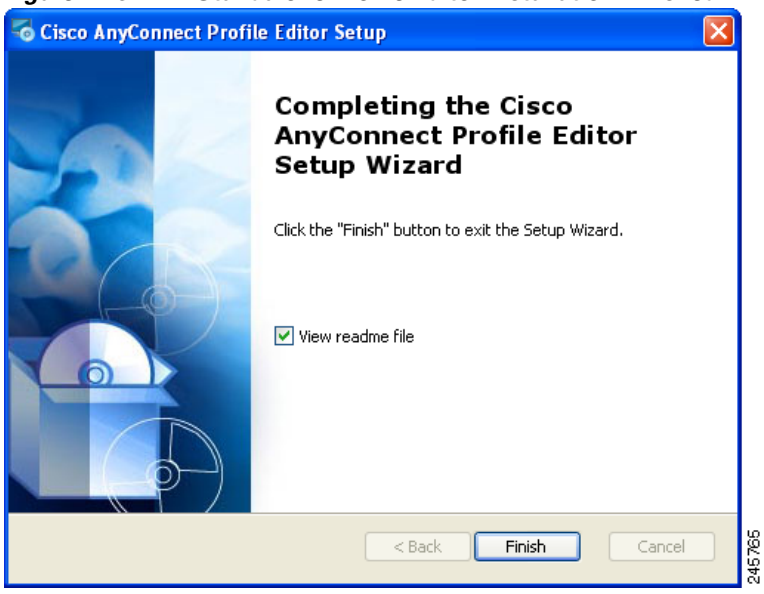
Step 6 At the Ready to Install screen, click **Install**. The Installing Cisco AnyConnect Profile Editor screen displays the progress of the installation.

Figure 2-22 Ready to Install Standalone Profile Editor



Step 7 At the Completing the Cisco AnyConnect Profile Editor Setup Wizard, click **Finish**.

Figure 2-23 Standalone Profile Editor Installation Finished



- The standalone AnyConnect profile editor is installed in the **C:\Program Files\Cisco\Cisco AnyConnect Profile Editor** directory.
- You can launch the VPN, Network Access Manager (NAM), and Web Security profile editors by selecting **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor** and then clicking the standalone profile editor you want from the submenu or by clicking the appropriate profile editor shortcut icon installed on the desktop.

Modifying the Standalone AnyConnect Profile Editor Installation

You can modify the standalone Cisco AnyConnect Profile Editor installation to install or remove the VPN, Network Access Manager (NAM), or Web Security profile editors by following this procedure:

Step 1 Open the Windows control panel and click **Add or Remove Programs**.

Step 2 Select the Cisco AnyConnect Profile Editor and click **Change**.

Step 3 Click **Next**.

Step 4 Click **Modify**.

Step 5 Edit the list of profile editors you want to install or remove and click **Next**.

Step 6 Click **Install**.

Step 7 Click **Finish**.

Uninstalling the Standalone AnyConnect Profile Editor

Step 1 Open the Windows control panel and click **Add or Remove Programs**.

Step 2 Select the Cisco AnyConnect Profile Editor and click **Remove**.

Step 3 Click **Yes** to confirm you want to uninstall Cisco AnyConnect Profile Editor.

Note Note that JRE 1.6 is not uninstalled automatically when uninstalling the standalone profile editor. You will need to uninstall it separately.

Creating a Client Profile Using the Standalone Profile Editor

Step 1 Launch the VPN, NAM, or Web Security profile editor by double-clicking the shortcut icon on the desktop or by navigating **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor** and selecting the VPN, NAM, or Web Security profile editor from the submenu.

Step 2 Follow the instructions for creating client profiles in these chapters of the AnyConnect Administrator Guide.

- Chapter 3, “Configuring VPN Access”
- Chapter 4, “Configuring Network Access Manager (NAM)”
- Chapter 6, “Configuring Web Security”

Step 3 Select **File > Save** to save the client profile. Each panel of the profile editor displays the path and file name of the client profile.

Editing a Client Profile Using the Standalone Profile Editor

Step 1 Launch the VPN, NAM, or Web Security profile editor by double-clicking the shortcut icon on the desktop or by navigating **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor** and selecting the VPN, NAM, or Web Security profile editor from the submenu.

Step 2 Select **File > Open** and navigate to the client profile XML file you want to edit.

Note If you mistakenly try to open a client profile of one kind of feature, such as Web Security, using the profile editor of another feature, such as VPN, you receive a **Schema Validation failed** message and you will not be able to edit the profile.

Step 3 Make your changes to the profile and select **File > Save** to save your changes.

Note If you inadvertently try to edit the same client profile in two instances of the same kind of profile editor, the last edits made to the client profile are saved.

Configuring the ASA for WSA Support of the AnyConnect Secure Mobility Solution

Today, users and their devices are increasingly more mobile, connecting to the Internet from various locations, such as the office, home, airport, and cafés. Traditionally, users insides the network are protected from security threats, and users outside the traditional network have no acceptable use policy enforcement, minimal protection against malware, and a higher risk of data loss.

Employers want to create flexible working environments where employees and partners can work anywhere on any device, but they also want to protect corporate interests and assets from Internet-based threats at all times (always-on security).

Traditional network and content security solutions are great for protecting users and assets behind the network firewall but are useless when users or devices are not connected to the network or when data is not routed through the security solutions.

Cisco offers AnyConnect Secure Mobility to extend the network perimeter to remote endpoints, enabling the seamless integration of web filtering services offered by the Web Security appliance. Cisco AnyConnect Secure Mobility provides an innovative new way to protect mobile users on PC-based or smart-phone platforms, providing a more seamless, always-protected experience for end users and comprehensive policy enforcement for IT administrators.

AnyConnect Secure Mobility is a collection of features across the following Cisco products:

- Cisco IronPort Web Security appliance (WSA)
- Cisco ASA 5500 series adaptive security appliance (ASA)
- Cisco AnyConnect client

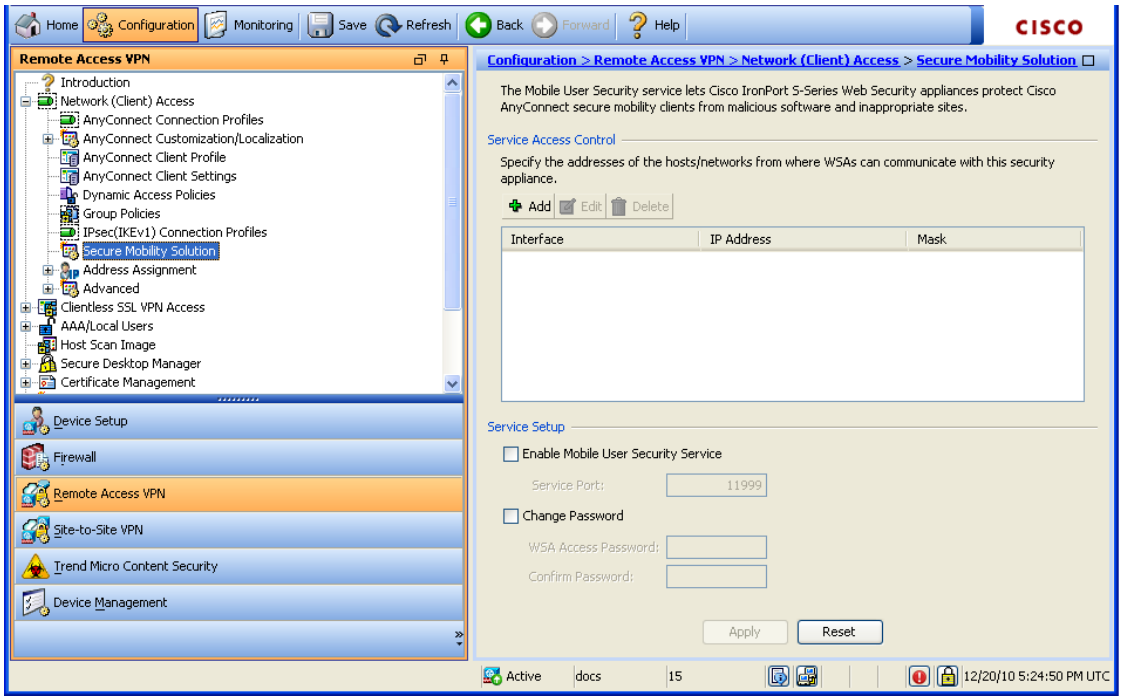
Cisco AnyConnect Secure Mobility addresses the challenges of a mobile workforce by offering the following features:

- **Secure, persistent connectivity**. Cisco AnyConnect (with the adaptive security appliances at the headend) provides the remote access connectivity portion of AnyConnect Secure Mobility. The connection is secure because both the user and device must be authenticated and validated prior to being provided access to the network. The connection is persistent because Cisco AnyConnect is typically configured to be always-on even when roaming between networks. Although Cisco AnyConnect is always-on, it is also flexible enough to apply different policies based on location, allowing users access to the Internet in a "captive portal" situation, when users must accept terms of agreement before accessing the Internet.
- **Persistent security and policy enforcement**. The Web Security appliance applies context-aware policies, including enforcing acceptable use policies and protection from malware for all users, including mobile (remote) users. The Web Security appliance also accepts user authentication information from the AnyConnect client, providing an automatic authentication step for the user to access web content.

Use the Secure Mobility Solution dialog box to configure the ASA portion of this feature. AnyConnect Secure Mobility lets Cisco IronPort S-Series Web Security appliances scan Cisco AnyConnect secure mobility clients to ensure that clients are protected from malicious software and/or inappropriate sites. The client periodically checks to ensure that Cisco IronPort S-Series Web Security appliance protection is enabled.

To configure the ASA for WSA support, launch ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution** panel (see Figure 2-24). Click **Help** for detailed instructions.

Figure 2-24 AnyConnect Secure Mobility Window



Note

- This feature requires a release of the Cisco IronPort Web Security appliance that provides AnyConnect Secure Mobility licensing support for the Cisco AnyConnect secure mobility client. It also requires an AnyConnect release that supports the AnyConnect Secure Mobility feature.
- This feature is available for AnyConnect connections using SSL or IPsec IKEv2 protocols.

Step 1 Specify from which host or network address the WSAs can communicate and identify the remote users using one of the following methods:

- **Associate by IP address**. The Web Security appliance administrator specifies a range of IP addresses that it considers as assigned to remote devices. Typically, the adaptive security appliance assigns these IP addresses to devices that connect using VPN functionality. When the Web Security appliance receives a transaction from one of the configured IP addresses, it considers the user as a remote user. With this configuration, the Web Security appliance does not communicate with any adaptive security appliance.
- **Integrate with a Cisco ASA**. The Web Security appliance administrator configures the Web Security application to communicate with one or more adaptive security appliances. The adaptive security appliance maintains an IP address-to-user mapping and communicates that information to the Web Security appliance. When the Web Proxy receives a transaction, it obtains the IP address and checks the IP address-to-user mapping to determine the user name. When you integrate with an adaptive security appliance, you can enable single sign-on for remote users. With this configuration, the Web Security appliances communicates with the adaptive security appliance.
  - Add—Opens the Add Access Control Configuration dialog box where you can add one or more Web Security appliances that the adaptive security appliance can communicate with.
  - Edit—Opens the Edit Access Control Configuration dialog box for the selected connection.
  - Delete—Removes the selected connection from the table. There is no confirmation or undo.

Step 2 If you choose to enable Mobile User Security Service, it starts the connection with the client through the VPN. When the Web Security appliance is configured to integrate with an adaptive security appliance, it tries to establish an HTTPS connection with all configured adaptive security appliances when it first starts up. When the connection is established, the Web Security appliance authenticates with the adaptive security appliance using the configured ASA access password. After successful authentication, the adaptive security appliance sends the IP address-to-user mapping to the Web Security appliance. If no WSA is present, the status is disabled.

Step 3 If you choose to enable the service, specify which port number for the service to use. The port must be between 1 and 65535 and must match the corresponding value provisioned into the WSA with the management system. The default is 11999.

Step 4 Change the WSA access password, if desired. You can change the Web Security appliance access password that is required for authentication between the adaptive security appliance and the Web Security appliance. This password must match the corresponding password configured on the Web Security appliance.

Step 5 In the WSA Access Password field, specify the shared secret password required for authentication between the ASA and WSA.

Step 6 Re-enter the specified password.

Step 7 Show WSA Sessions allows you to view session information of WSAs connected to the ASA.The host IP address of the WSA that is connected (or has been connected) and the duration of the connection is returned in a dialog box.

Configuring a Proxy Server For Endpoint to WSA Traffic

You must set up a web proxy to redirect web traffic from the endpoint to the WSA. To do this, either set up a transparent proxy using a WCCP router, or, follow these instructions to set up an explicit proxy:

Step 1 Launch ASDM on your ASA, and select **Remote Access VPN > Network (Client) Access > Group Policies.**

Step 2 Select the group policy configured for web vpn and click **Edit**.

Step 3 In the left pane of the Edit Internal Group Policy window, expand the Advanced node and select Browser Proxy.

Step 4 Uncheck **Inherit** in the Proxy Server Policy area.

Step 5 Select **Select proxy server settings from the following** and check **Use proxy server settings given below**.

Step 6 Expand the Proxy Server Settings area and uncheck the Server Address and Port **Inherit** checkbox. Specify the WSA's IP address and port number.

Step 7 Uncheck the Bypass server for local addresses **Inherit** checkbox and select **Yes**.

Step 8 If you want, enter a list of addresses that will not be accessed through a proxy server by unchecking the Exceptions List **Inherit** check box and entering the IP addresses, for which you are making exceptions, in the Exception list area.

Step 9 Click **OK**.

Step 10 Click **Apply**.

CHAPTER 3

Configuring VPN Access

The following sections describe the Cisco AnyConnect Secure Mobility client VPN profile and features, and how to configure them:

Creating and Editing an AnyConnect Profile

This section describes how to launch the profile editor from ASDM and create a new profile.

The Cisco AnyConnect Secure Mobility client software package, version 2.5 and later (all operating systems) contains the profile editor. ASDM activates the profile editor when you load the AnyConnect software package on the ASA as an SSL VPN client image.

If you load multiple AnyConnect packages, ASDM loads the profile editor from the newest AnyConnect package. This approach ensures that the editor displays the features for the newest AnyConnect loaded, as well as the older clients.

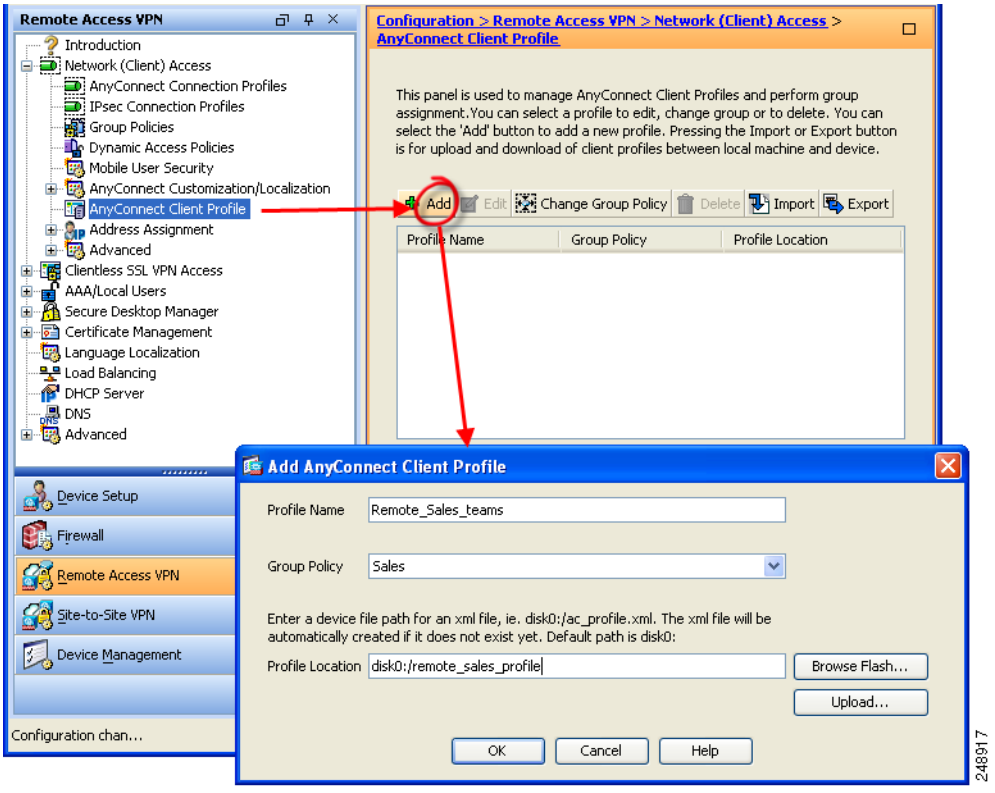
To activate the profile editor in ASDM, follow these steps:

Step 1 Load the AnyConnect software package as an AnyConnect Client image. If you have not done this already, see Chapter 2, "Configuring the ASA to Download AnyConnect".

Step 2 Select **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.** The AnyConnect Client Profile pane opens.

Step 3 Click **Add**. The Add AnyConnect Client Profile window opens (Figure 3-1).

Figure 3-1 Adding an AnyConnect Profile



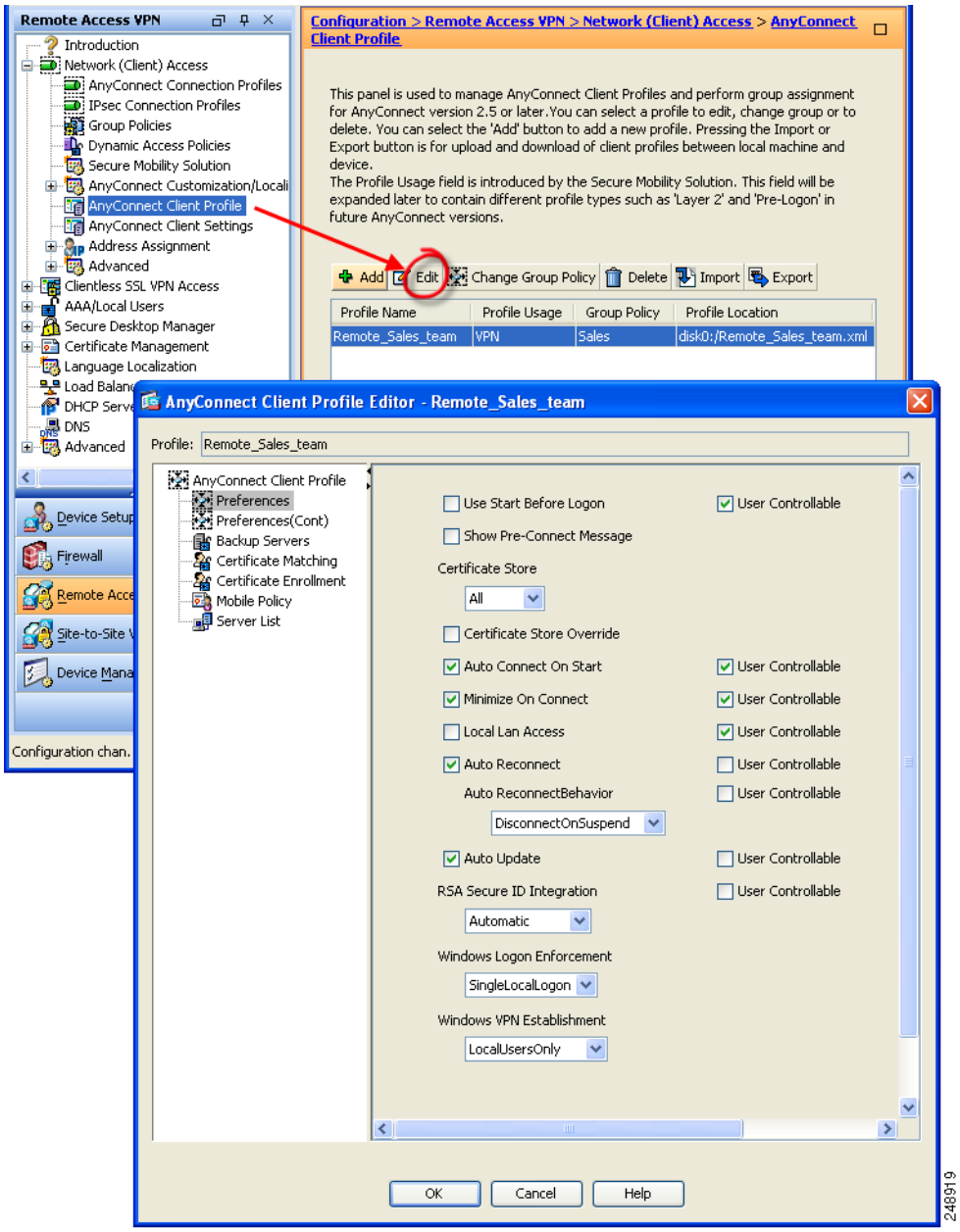
Step 4 Specify a name for the profile. Unless you specify a different value for Profile Location, ASDM creates an XML file on the ASA flash memory with the same name.

Step 5 Choose a group policy (optional). The ASA applies this profile to all AnyConnect users in the group policy.

Step 6 Click **OK**. ASDM creates the profile and the profile appears in the table of profiles.

Step 7 Select the profile you just created from the table of profiles. Click **Edit**. The profile editor displays (Figure 3-2). Enable AnyConnect features in the panes of the profile editor. When you finish, click **OK**.

Figure 3-2 Editing a Profile



Deploying the AnyConnect Profile

You can import a profile using either ASDM or the ASA command-line interface.

Note You must include the ASA in the host list in the profile so the client GUI displays all the user controllable settings on the initial VPN connection. If you do not add the ASA 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 ASA 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" section on page 3-46.

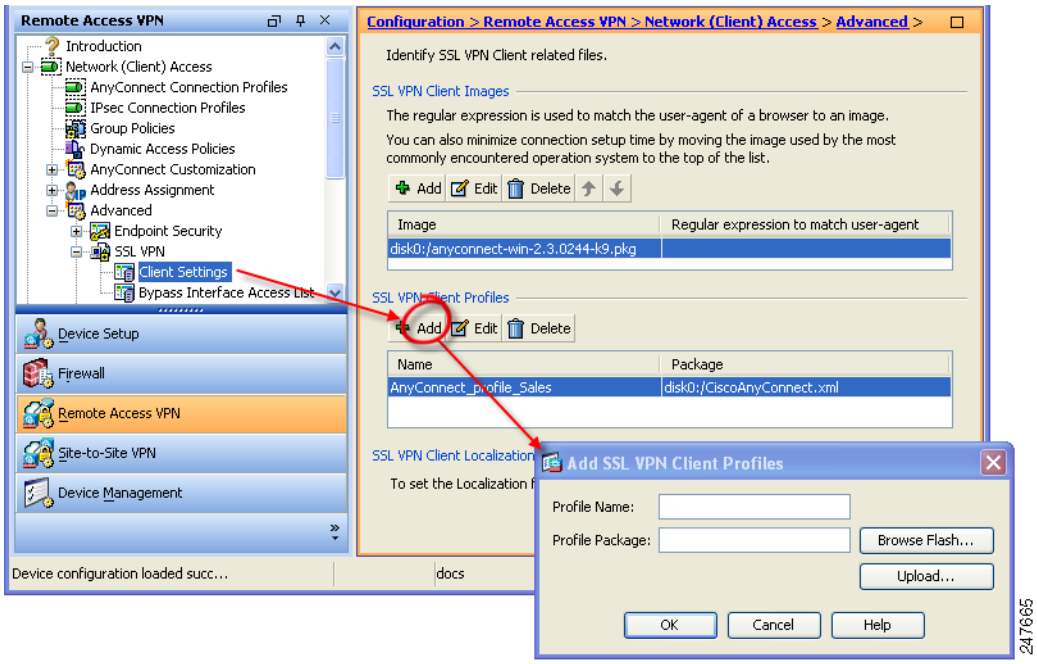
Note In order for the client initialization parameters in a profile to be applied to the AnyConnect configuration, the ASA the user connects to must appear as a host entry in that profile. If you do not add the ASA address or FQDN as a host entry in the profile, then filters do not apply for the session. For example, if you create a certificate match and the certificate properly matches the criteria, but you do not add the ASA as a host entry in that profile, the certificate match is ignored. For more information about adding host entries to the profile, see the "Configuring a Server List" section on page 3-46.

Follow these steps to configure the ASA to deploy a profile with AnyConnect:

Step 1 Identify the AnyConnect profile file to load into cache memory.
Go to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > Client Settings**.

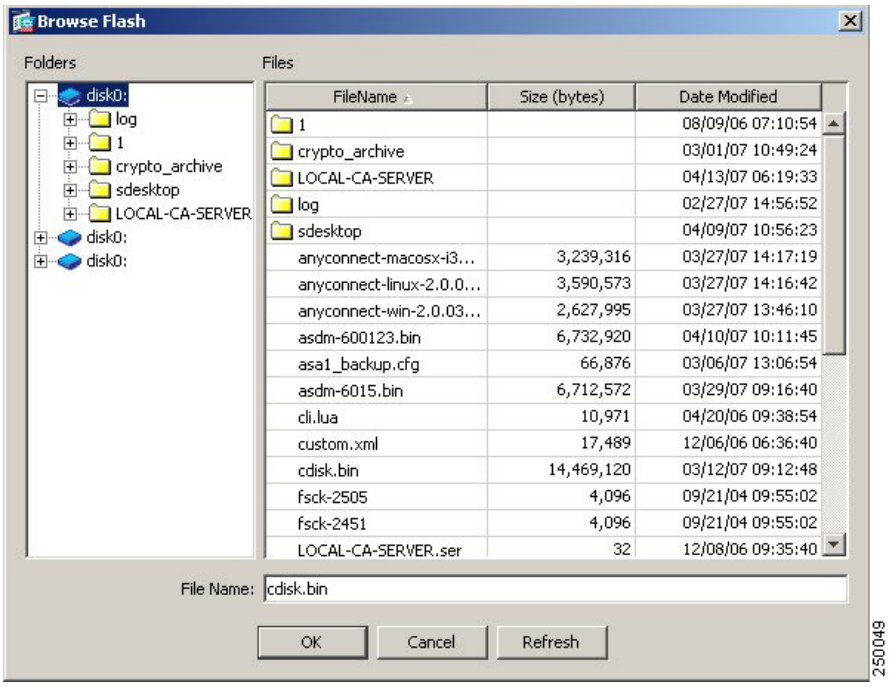
Step 2 In the SSL VPN Client Profiles area, click **Add**. The Add SSL VPN Client Profiles dialog box appears (Figure 3-3).

Figure 3-3 Adding an AnyConnect 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 opens (Figure 3-4).

Figure 3-4 Browse Flash Dialog Box

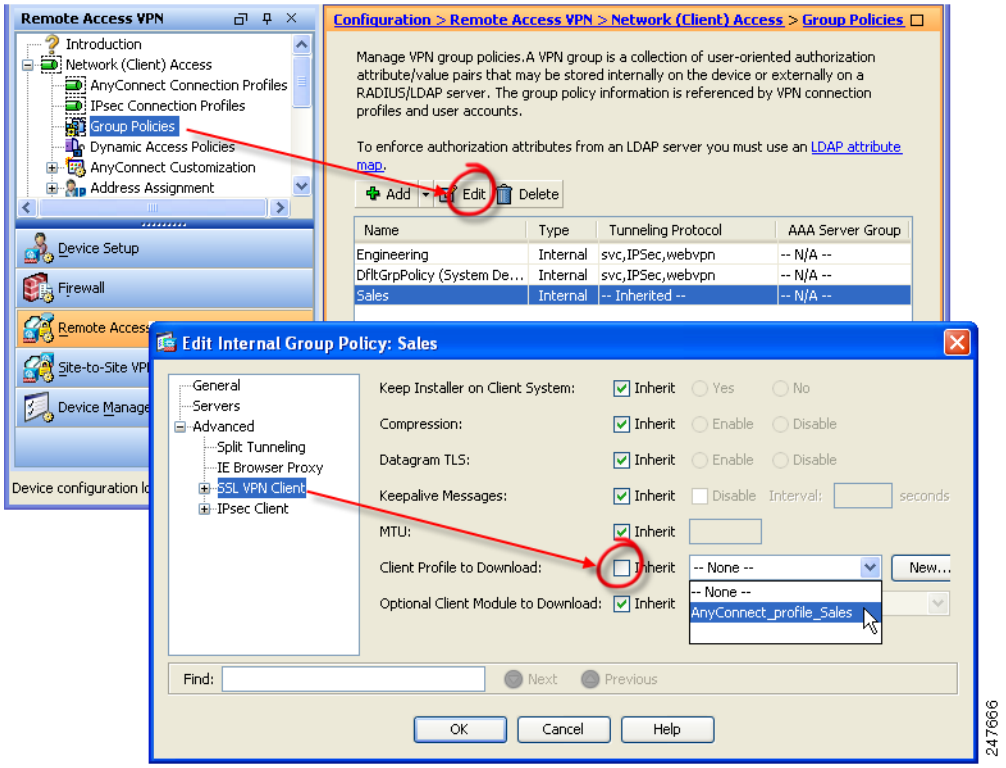


Step 4 Select a file from the table. The file name appears in the File Name field below the table. Click **OK**. The file name you selected appears in the Profile Package field of the Add or Edit SSL VPN Client Profiles dialog box.

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

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

Figure 3-5 Specify the Profile to use in the Group Policy



Step 6 Deselect **Inherit** and select an AnyConnect profile to download from the drop-down list.

Step 7 When you have finished with the configuration, click **OK**.

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 AnyConnect before the Windows login dialog box appears. After authenticating to the ASA, 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 AnyConnect does not support SBL for Windows XP x64 (64-bit) Edition.

Reasons you might consider 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.

To enable the SBL feature, you must make changes to the AnyConnect profile and enable the ASA to download an AnyConnect module for SBL.

The only configuration necessary 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. This includes domain logon scripts, group policy objects and other Active Directory functionality that normally occurs when a user logs on to their system.

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. If NAM is installed, you must deploy machine connection to ensure that an appropriate connection is available. For more information, see Chapter 4, “Configuring Network Access Manager (NAM)”.

AnyConnect is not compatible with fast user switching.

This section covers the following topics:

Installing Start Before Logon Components (Windows Only)

The Start Before Logon components must be installed *after* the core client has been installed. Additionally, the 2.5 Start Before Logon components require that version 2.5, or later, of the core client software be installed. If you are pre-deploying AnyConnect 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.

Start Before Logon Differences Between Windows Versions

The procedures for enabling SBL differ slightly on Windows 7 and Vista systems. Pre-Vista systems use a component called VPNGINA (which stands for virtual private network graphical identification and authentication) to implement SBL. Windows 7 and Vista systems use a component called PLAP to implement SBL.

In AnyConnect, the Windows 7 or Vista SBL 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 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 Windows 7 and 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 7 and Vista systems.

In pre-Vista systems, SBL 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 7 and 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 7 or Vista platform, see the "Configuring Start Before Logon (PLAP) on Windows 7 and Vista Systems" section on page 3-12.

Enabling SBL in the AnyConnect Profile

To enable SBL in the AnyConnect profile, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the Preferences pane and check **Use Start Before Logon**.

Step 3 (Optional) To give the remote user control over using SBL, check **User Controllable**.

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

Enabling SBL on the Security Appliance

To minimize download time, AnyConnect requests downloads (from the ASA) 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 ASA. Follow this procedure:

Step 1 Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

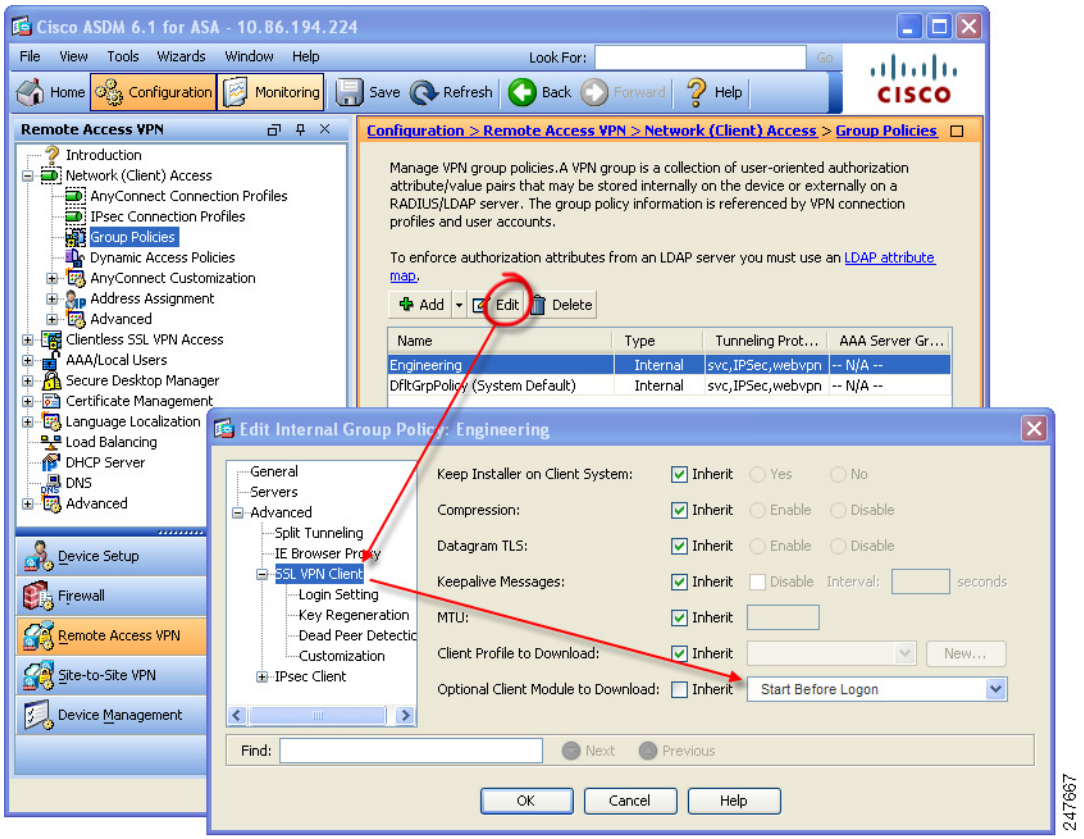
Step 2 Select a group policy and click **Edit**. The Edit Internal Group Policy window displays.

Step 3 Select **Advanced > SSL VPN Client** in the left-hand navigation pane. SSL VPN settings display.

Step 4 Uncheck **Inherit** for the Optional Client Module for Download setting.

Step 5 Select the **Start Before Logon** module in the drop-down list (Figure 3-6).

Figure 3-6 Specifying the SBL Module to Download



Troubleshooting SBL

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

Step 1 Ensure that the AnyConnect profile is loaded on the ASA, ready to be deployed.

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 SBL 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 AnyConnect again.

Step 6 Reboot once. On the next reboot, you should be prompted with the Start Before Logon prompt.

Step 7 Send the event log to Cisco in .evt format

Step 8 If you see the following error, delete the user's AnyConnect profile:

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

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 SBL feature on Windows 7 and Vista uses a different mechanism as well.

The SBL AnyConnect 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, SBL uses a component known as the VPN Graphical Identification and Authentication Dynamic Link Library (vpngina.dll) to provide SBL capabilities. The Windows PLAP component, which is part of Windows 7 and 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 SBL 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 7 and Vista, the installer installs the vpngina.dll component on 32-bit versions of the operating system. On Windows 7 or Vista, or the Windows 2008 server, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component.

Note If you uninstall AnyConnect 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 SBL. See the "Enabling SBL in the AnyConnect Profile" section on page 3-10. 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.

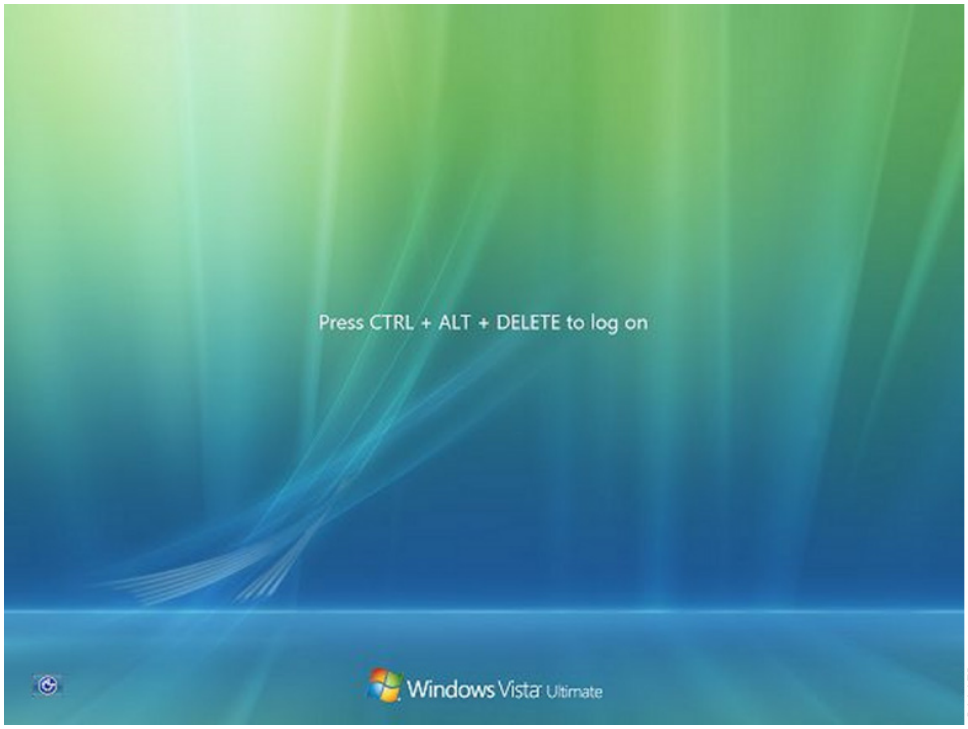
Note If the user mistakenly minimizes the user interface, the user can restore it by pressing the **Alt+Tab** key combination.

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

Users can log on to Windows 7 or Windows Vista with PLAP enabled by following these steps, which are Microsoft requirements. The examples screens are for Windows Vista:

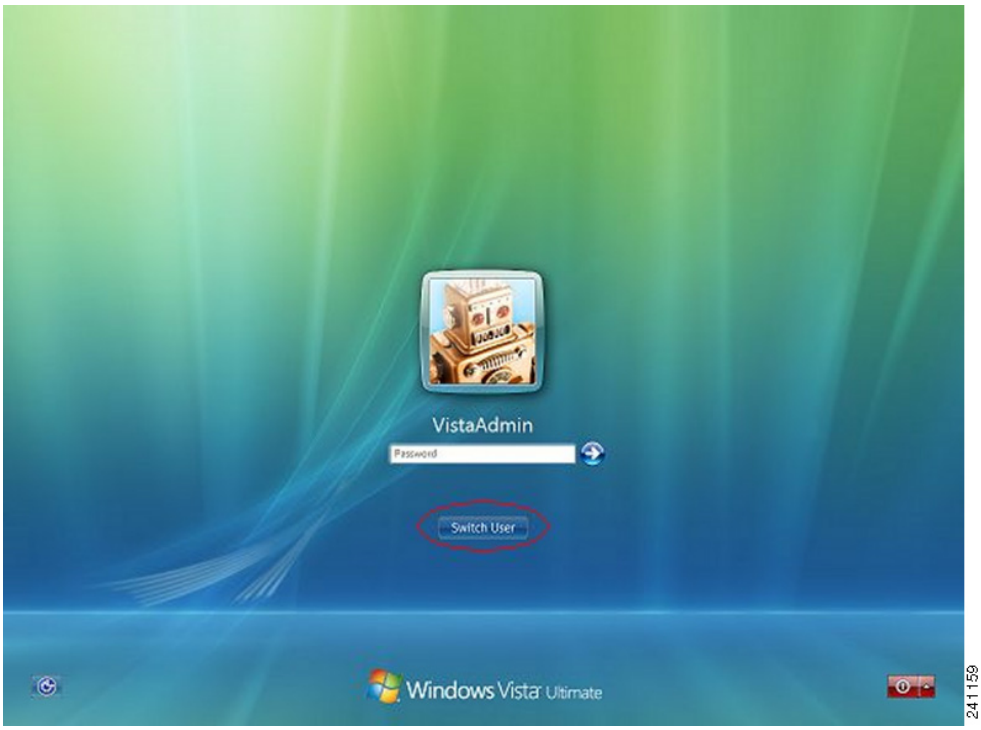
Step 1 At the Windows start window, users press the **Ctrl+Alt+Delete** key combination (Figure 3-7).

Figure 3-7 Example Logon Window Showing the Network Connect Button



This displays the Vista logon window with a Switch User button (Figure 3-8).

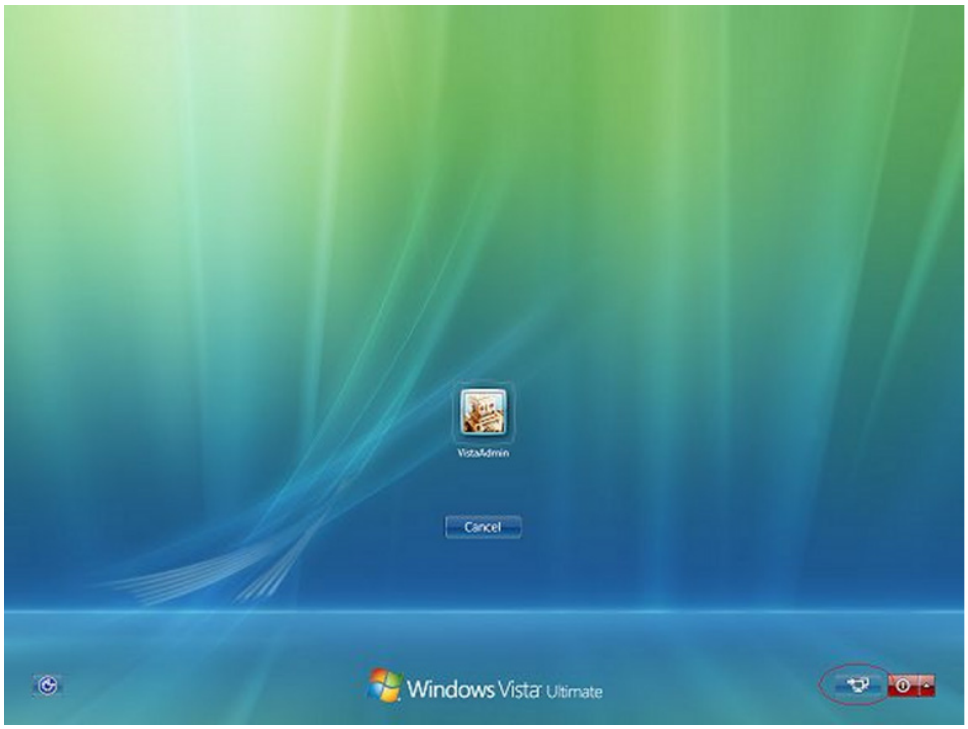
Figure 3-8 Example Logon Window with Switch User Button



Step 2 The user clicks **Switch User** (circled in red in this figure). The Vista Network Connect window displays (Figure 3-9). The network login icon is circled in red in Figure 3-9.

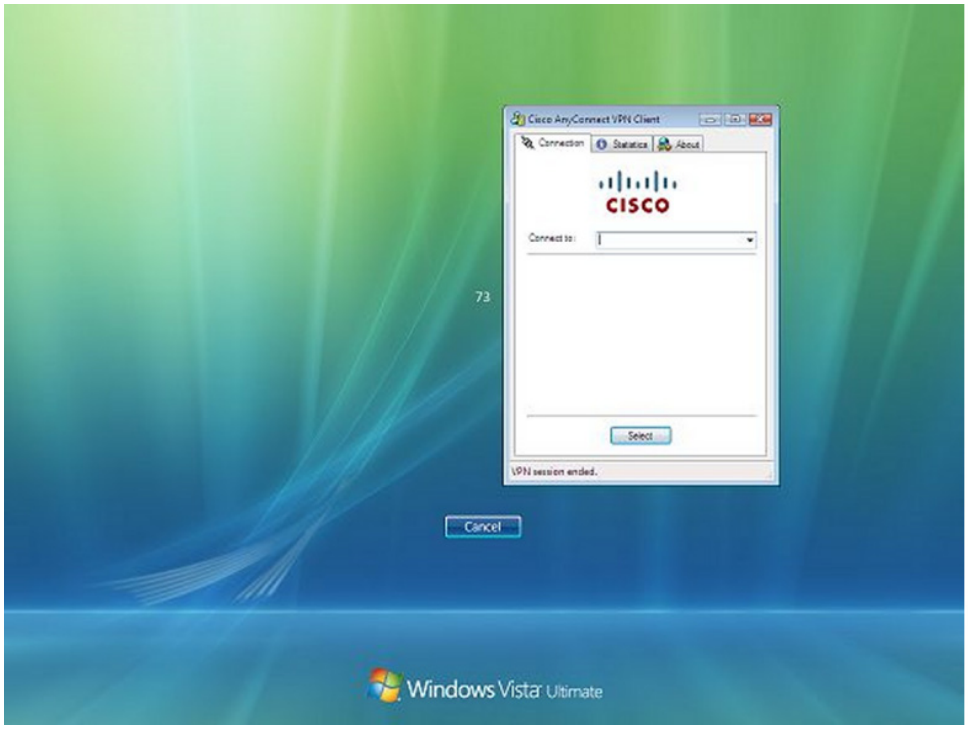
Note If the user is already connected through an AnyConnect connection and clicks **Switch User**, that VPN connection remains. If the user clicks **Network Connect**, the original VPN connection terminates. If the user clicks **Cancel**, the VPN connection terminates.

Figure 3-9 Example Network Connect Window



Step 3 The user clicks the **Network Connect** button in the lower-right corner of the window to launch AnyConnect. The AnyConnect logon window opens (Figure 3-10).

Figure 3-10 Example AnyConnect Logon Window

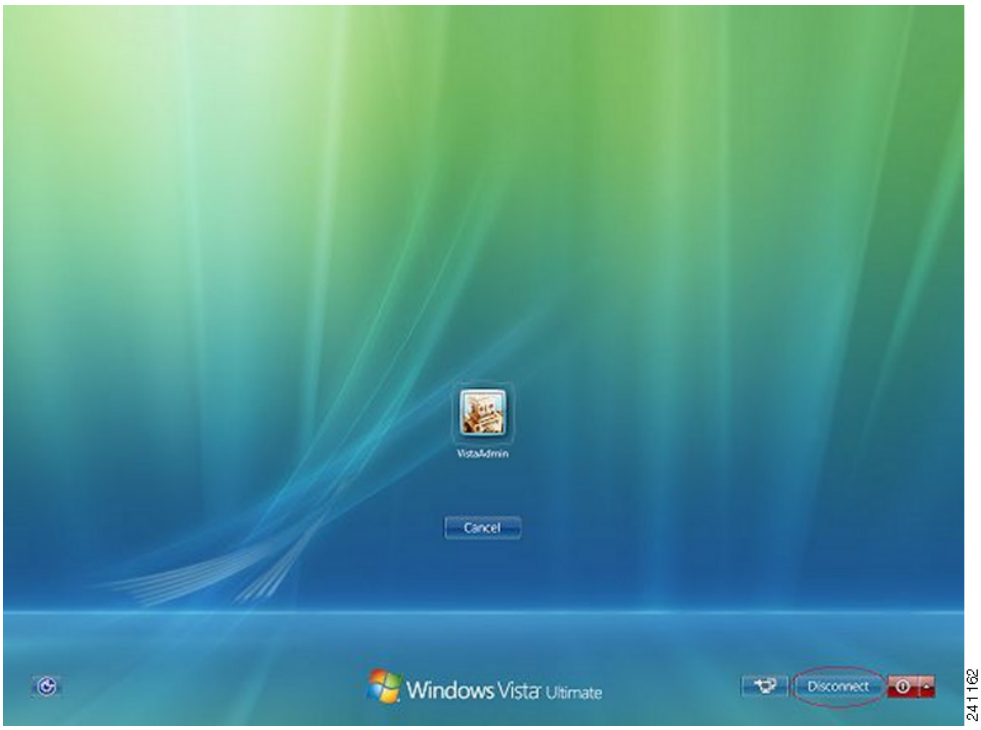


Step 4 The user uses this GUI to log in as usual.

Note This example assumes AnyConnect 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 connects, 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 3-11). This is the only indication the connection is successful.

Figure 3-11 Example Disconnect Window



The user clicks the icon associated with their login. In this example, the user clicks **VistaAdmin** to complete logging onto the computer.

Caution Once the connection is established, the user has an unlimited time to log on. If the user forgets to log on after connecting, the VPN session continues indefinitely.

Disconnecting from AnyConnect Using PLAP

After successfully establishing a VPN session, 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 3-11).

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 AnyConnect.

Trusted Network Detection

Trusted Network Detection (TND) gives you the ability to have AnyConnect 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 AnyConnect 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 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.

You configure TND in the AnyConnect profile. No changes are required to the ASA configuration.

Trusted Network Detection Requirements

TND supports only computers running Microsoft Windows 7, Vista, XP; and Mac OS X 10.5 and 10.6.

Configuring Trusted Network Detection

To configure TND in the client profile, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Preferences (Part 2)** pane.

Step 3 Check **Automatic VPN Policy**.

Note AutomaticVPNPolicy does not prevent users from manually controlling a VPN connection.

Step 4 Select a Trusted Network Policy—the action the client takes when the user is inside the corporate network (the trusted network). The options are:

- Disconnect—The client terminates the VPN connection in the trusted network.
- Connect—The client initiates a VPN connection in the trusted network.
- Do Nothing—The client takes no action in the trusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to *Do Nothing* disables Trusted Network Detection (TND).
- Pause—AnyConnect suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.

Step 5 Select an Untrusted Network Policy—the action the client takes when the user is outside the corporate network. The options are:

- Connect—The client initiates a VPN connection upon the detection of an untrusted network.
  - Do Nothing—The client initiates a VPN connection upon the detection of an untrusted network. This option disables always-on VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.

Step 6 Specify the Trusted DNS Domains—DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *.cisco.com. Wildcards (*) are supported for DNS suffixes. See Table 3-1 for more examples of DNS suffix matching.

Step 7 Specify Trusted DNS Servers—All DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 161.44.124.*,64.102.6.247. Wildcards (*) are supported for DNS server addresses.

Note You must specify all the DNS servers for TND to work. If you configure both the TrustedDNSDomains and TrustedDNSServers, sessions must match both settings to be considered in the trusted network.

Table 3-1 shows examples of DNS suffix matching.

Table 3-1 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

TND and 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 ASA, 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* the ASAs on your corporate network.
- Create *one profile* listing all the ASAs in the host entry section, and load that profile on *all* your ASAs.
- If users do not need to have multiple, different profiles, use the same profiles name for the profiles on *all* the ASAs. Each ASA overrides the existing profile.

Always-on VPN

You can configure AnyConnect to establish a VPN session automatically after the user logs in to a computer. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer expires. The group policy assigned to the session specifies these timer values. If AnyConnect loses the connection with the ASA, the ASA and the client retain the resources assigned to the session until one of these timers expire. AnyConnect continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.

Note If always-on is enabled, but the user does not log on, AnyConnect does not establish the VPN connection. AnyConnect initiates the VPN connection only post-login.

(Post log-in) always-on VPN enforces corporate policies to protect the computer from security threats by preventing access to Internet resources when the computer is not in a trusted network.

Caution Always-on VPN does not currently support connecting though a proxy.

When AnyConnect detects always-on VPN in the profile, it protects the endpoint by deleting all other AnyConnect profiles, and ignores any public proxies configured to connect to the ASA.

To enhance the protection against threats, we recommend the following additional protective measures if you configure always-on VPN:

- Pre-deploy a profile configured with always-on VPN to the endpoints to limit connectivity to the pre-defined ASAs. Predeployment prevents contact with a rogue server.
- Restrict administrator rights so that users cannot terminate processes. A PC user with admin rights can bypass an always-on VPN policy by stopping the agent. If you want to ensure fully-secure always-on VPN, you must deny local admin rights to users.
- Restrict access to the following folders or the Cisco sub-folders on Windows computers:
  - For Windows XP users: C:\Document and Settings\All Users
  - For Windows Vista and Windows 7 users: C:\ProgramData

  Users with limited or standard privileges may sometimes have write access to their program data folders. They could use this access to delete the AnyConnect profile file and thereby circumvent the always-on feature.
- Predeploy a group policy object (GPO) for Windows users to prevent users with limited rights from terminating the GUI. Predeploy equivalent measures for Mac OS users.

Always-on VPN Requirements

Support for always-on VPN requires one of the following licenses:

- AnyConnect Premium (SSL VPN Edition)
- Cisco AnyConnect Secure Mobility

  You can use a Cisco AnyConnect Secure Mobility license to provide support for always-on VPN in combination with either an AnyConnect Essentials or an AnyConnect Premium license.
- Always-on VPN requires a valid server certificate configured on the ASA; otherwise, it fails and logs an event indicating the certificate is invalid.

Ensure your server certificates can pass strict mode if you configure always-on VPN.

Always-on VPN supports only computers running Microsoft Windows 7, Vista, XP; and Mac OS X 10.5 and 10.6.

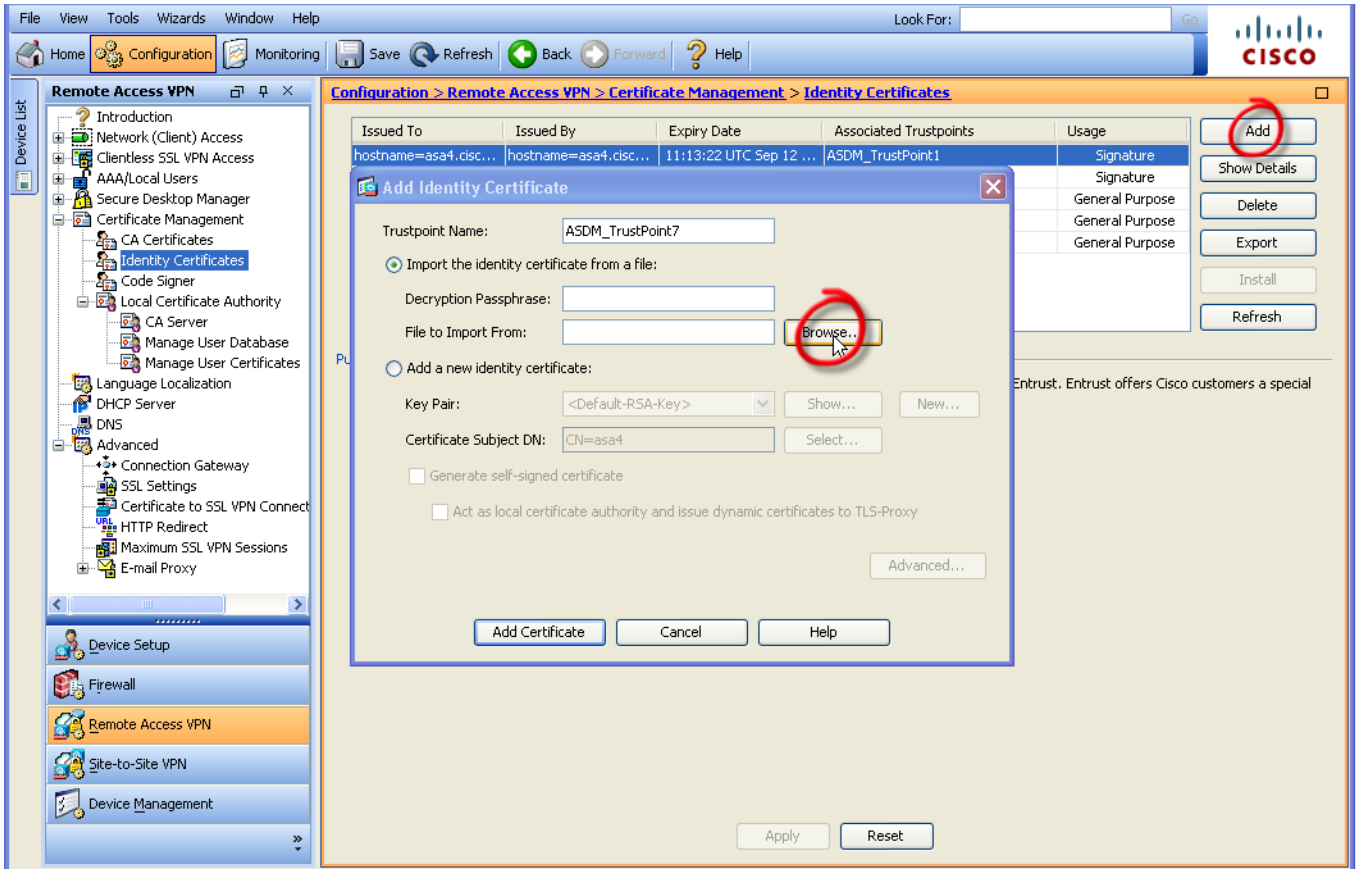
To prevent the download of an always-on VPN profile that locks a VPN connection to a rogue server, the AnyConnect client requires a valid, trusted server certificate to connect to a secure gateway. We strongly recommend purchasing a digital certificate from a certificate authority (CA) and enrolling it on the secure gateways.

If you generate a self-signed certificate, users connecting receive a certificate warning. They can respond by configuring the browser to trust that certificate to avoid subsequent warnings.

Note We do not recommend using a self-signed certificate because of the possibility a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateways.

ASDM provides an **Enroll ASA SSL VPN with Entrust** button on the **Configuration > Remote Access VPN > Certificate Management > Identity Certificates** panel to facilitate enrollment of a public certificate to resolve this issue on an ASA. The **Add** button on this panel lets you import a public certificate from a file or generate a self-signed certificate (Figure 3-12).

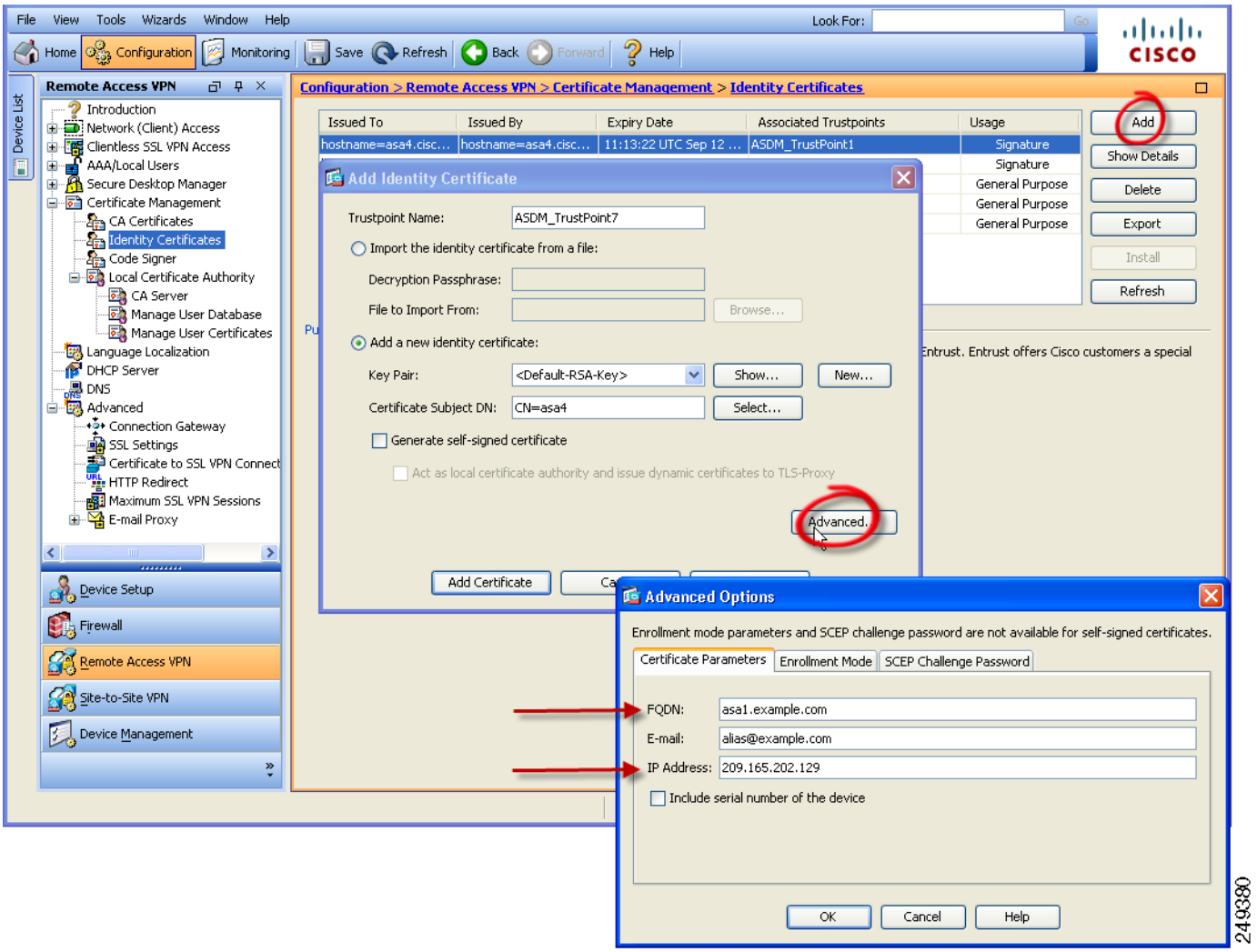
Figure 3-12 Enrolling a Public Certificate (ASDM 6.3 Example)



Note These instructions are intended only as a guideline for configuring certificates. For details, click the ASDM **Help** button, or see the ASDM or CLI guide for the secure gateway you are configuring. For example, *Cisco ASA 5500 Series Configuration Guide using ASDM, 6.3 for ASA 8.3* provides comprehensive instructions in Configuring Digital Certificates.

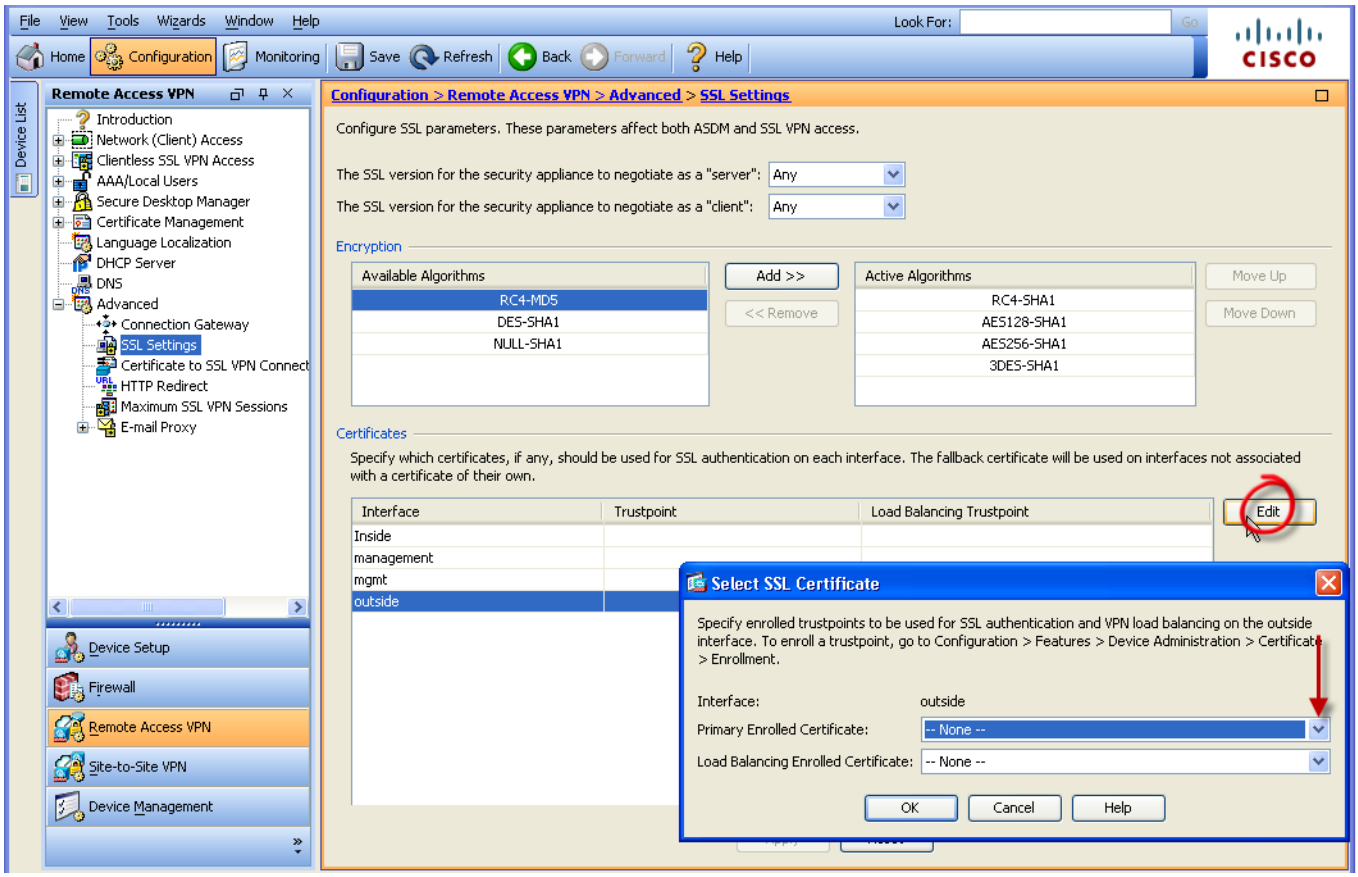
Use the **Advanced** button to specify the domain name and IP address of the outside interface if you are generating a self-signed interface (Figure 3-13).

Figure 3-13 Generating a Self-Signed Certificate (ASDM 6.3 Example)



Following the enrollment of a certificate, assign it to the outside interface. To do so, choose **Configuration > Remote Access VPN > Advanced > SSL Settings**, edit the "outside" entry in the Certificates area, and select the certificate from the Primary Enrolled Certificate drop-down list (Figure 3-14).

Figure 3-14 Assigning a Certificate to the Outside Interface (ASDM 6.3 Example)



Add the certificate to all of the secure gateways and associate it with the IP address of the outside interfaces.

Adding Load-Balancing Backup Cluster Members to the Server List

Always-on VPN affects the load balancing of AnyConnect VPN sessions. With always-on VPN disabled, when the client connects to a master device within a load balancing cluster, the client complies with a redirection from the master device to any of the backup cluster members. With always-on enabled, the client does not comply with a redirection from the master device unless the address of the backup cluster member is specified in the server list of the client profile. Therefore, be sure to add any backup cluster members to the server list.

To specify the addresses of backup cluster members in the client profile, use ASDM to add a load-balancing backup server list by following these steps:

Step 1 Launch the Profile Editor from ASDM (see Creating and Editing an AnyConnect Profile, page 3-2).

Step 2 Go to the **Server List** pane.

Step 3 Choose a server that is a master device of a load-balancing cluster and click **Edit.**

Step 4 Enter an FQDN or IP address of any load-balancing cluster member.

Configuring Always-on VPN

To configure AnyConnect to establish a VPN session automatically only when it detects that the computer is in an untrusted network,

Step 1 Configure TND (see Configuring Trusted Network Detection).

Step 2 Check **Always On**.

Configuring a Policy to Exempt Users from Always-on VPN

By default, always-on VPN is disabled. You can configure exemptions to override an always-on policy. For example, you might want to let certain individuals establish VPN sessions with other companies, or exempt the always-on VPN policy for noncorporate assets.

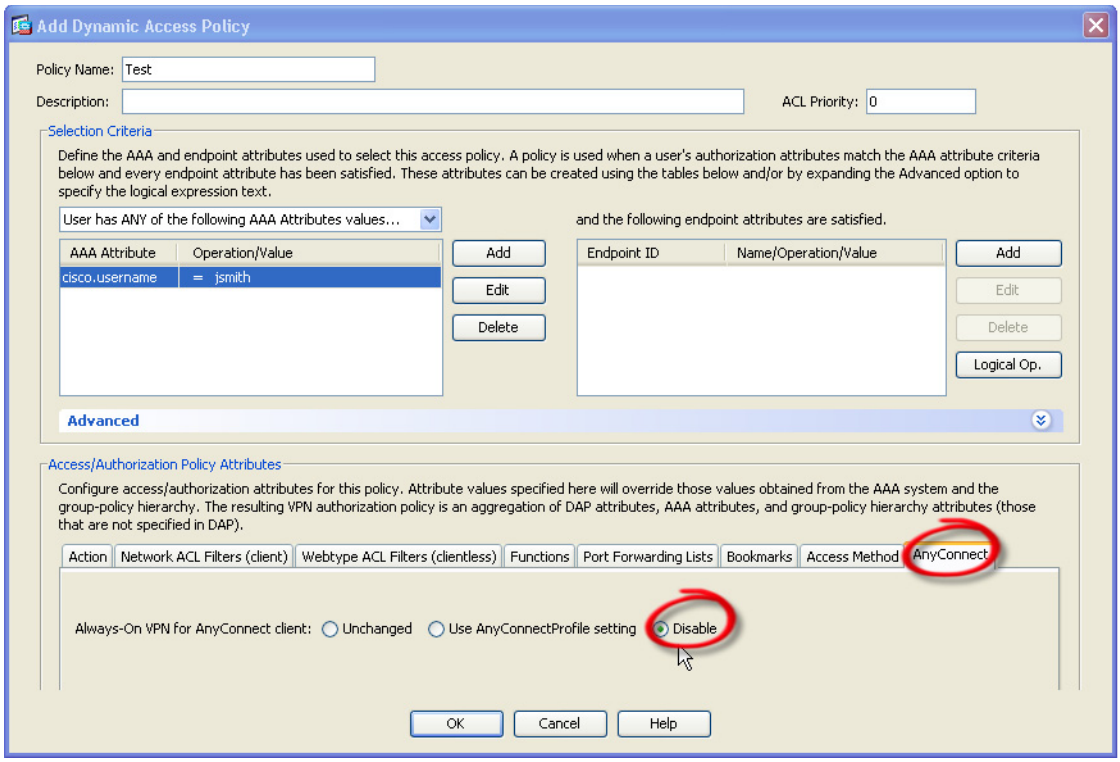
You can set the always-on VPN parameter in group policies and dynamic access policies to override the always-on policy. Doing so lets you specify exceptions according to the matching criteria used to assign the policy. If an AnyConnect policy enables always-on VPN and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.

The following procedure configures a dynamic access policy that uses AAA or endpoint criteria to match sessions to noncorporate assets, as follows:

Step 1 Choose **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add** or **Edit**.

The Add or Edit Dynamic Policy window opens (Figure 3-15).

Figure 3-15 Exempting Users from Always-on VPN



Step 2 Configure criteria to exempt users from always-on VPN. For example, use the Selection Criteria area to specify AAA attributes to match user login IDs.

Step 3 Click the **AnyConnect** tab on the bottom half of the Add or Edit Dynamic Access Policy window.

Step 4 Click **Disable** next to "Always-On for AnyConnect VPN" client.

If a Cisco AnyConnect Secure Mobility client policy enables always-on VPN and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.

Disconnect Button for Always-on VPN

AnyConnect supports a Disconnect button for always-on VPN sessions. If you enable it, AnyConnect displays a Disconnect button upon the establishment of a VPN session. Users of always-on VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as the following:

- Performance issues with the current VPN session.
- Reconnection issues following the interruption of a VPN session.

The Disconnect button locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session.

Caution Disabling the Disconnect button can at times hinder or prevent VPN access.

If the user clicks Disconnect during an always-on VPN session, AnyConnect locks all interfaces to prevent data from leaking out and protects the computer from internet access except for that required to establish a new VPN session. AnyConnect locks all interfaces, regardless of the connect failure policy

Caution The Disconnect locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. For the reasons noted above, disabling the Disconnect button can at times hinder or prevent VPN access.

Disconnect Button Requirements

The requirements for the disconnect option for always-on VPN match the Always-on VPN Requirements.

Enabling and Disabling the Disconnect Button

By default, the profile editor enables the Disconnect button when you enable always-on VPN. You can view and change the Disconnect button setting, as follows:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Preferences (Part 2)** pane.

Step 3 Check or uncheck **Allow VPN Disconnect**.

Connect Failure Policy for Always-on VPN

The connect failure policy determines whether the computer can access the internet if always-on VPN is enabled and AnyConnect cannot establish a VPN session (for example, when a secure gateway is unreachable). The fail-close policy disables network connectivity–except for VPN access. The fail-open policy permits network connectivity. Regardless of the connect failure policy, AnyConnect continues to try to establish the VPN connection. The following table explains the fail open and fail close policies:

Always-on VPN Connect Policy	Scenario	Advantage	Trade-off
Fail open	AnyConnect fails to establish or reestablish a VPN session. This failure could occur if the secure gateway is unavailable, or if AnyConnect does not detect the presence of a captive portal (often found in airports, coffee shops and hotels).	Grants full network access, letting users continue to perform tasks where access to the Internet or other local network resources is needed.	Security and protection are not available until the VPN session is established. Therefore, the endpoint device may get infected with web-based malware or sensitive data may leak.
Fail close	Same as above except that this option is primarily for exceptionally secure organizations where security persistence is a greater concern than always-available network access.	The endpoint is protected from web-based malware and sensitive data leakage at all times because all network access is prevented except for local resources such as printers and tethered devices permitted by split tunneling.	Until the VPN session is established, this option prevents all network access except for local resources such as printers and tethered devices. It can halt productivity if users require Internet access outside the VPN and a secure gateway is inaccessible.

Caution A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. AnyConnect detects most captive portals, described in "Captive Portal Hotspot Detection and Remediation" section on page 3-29; however, if it cannot detect a captive portal, the connect failure closed policy prevents all network connectivity. Use extreme caution when implementing a connect failure closed policy

If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy always-on VPN with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.

Connect Failure Policy Requirements

Support for the connect failure policy feature requires one of the following licenses:

- AnyConnect Premium (SSL VPN Edition)
- Cisco AnyConnect Secure Mobility

  You can use a Cisco AnyConnect Secure Mobility license to provide support for the connect failure policy in combination with either an AnyConnect Essentials or an AnyConnect Premium license.

The connect failure policy supports only computers running Microsoft Windows 7, Vista, XP; and Mac OS X 10.5 and 10.6.

Configuring a Connect Failure Policy

By default, the connect failure policy prevents Internet access if always-on VPN is configured and the VPN is unreachable. To configure a connect failure policy,

Step 1 Configure TND (see Configuring Trusted Network Detection).

Step 2 Check **Always On**.

Step 3 Set the Connect Failure Policy parameter to one of the following settings:

- Closed—(Default) Restricts network access when the VPN is unreachable. The restricted state permits access only to secure gateways to which the computer is allowed to connect. It prevents captive portal remediation (described in the next sections) unless you specifically enable it as part of the fail-closed policy. The restricted state permits the application of the local resource rules imposed by the most recent VPN session if *Apply Last VPN Local Resources* is enabled in the client profile. For example, these rules could determine access to active sync and local printing. The network is unblocked and open during a AnyConnect software upgrade when Always-On is enabled. The purpose of the Closed setting is to help protect corporate assets from network threats when resources in the private network that protect the endpoint are not available.
- Open—Does not restrict network access when the client cannot establish a VPN session (for example, when an ASA is unreachable). This setting permits network access by browsers and other applications when the client cannot connect to the ASA. An open connect failure policy does not apply if you enable the Disconnect button and the user clicks Disconnect.

Note Because the ASA does not support IPv6 addresses for split tunneling, the local print feature does not support IPv6 printers.

Captive Portal Hotspot Detection and Remediation

Many facilities that offer Wi-Fi and wired access, such as airports, coffee shops, and hotels, require the user to pay before obtaining access, agree to abide by an acceptable use policy, or both. These facilities use a technique called *captive portal* to prevent applications from connecting until the user opens a browser and accepts the conditions for access.

The following sections describe the captive portal detection and remediation features.

Captive Portal Hotspot Detection

AnyConnect displays the "Unable to contact *VPN server"* message on the GUI if it cannot connect, regardless of the cause. *VPN server* specifies the secure gateway. If always-on is enabled, and a captive portal is not present, the client continues to attempt to connect to the VPN and updates the status message accordingly.

If always-on VPN is enabled, the connect failure policy is closed, captive portal remediation is disabled, and AnyConnect detects the presence of a captive portal, the AnyConnect GUI displays the following message once per connection and once per reconnect:

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

If AnyConnect detects the presence of a captive portal and the AnyConnect configuration differs from that described above, the AnyConnect GUI displays the following message once per connection and once per reconnect:

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

Captive portal detection is enabled by default, and is non-configurable.

Support for both captive portal detection and remediation requires one of the following licenses:

- AnyConnect Premium (SSL VPN Edition)
- Cisco AnyConnect Secure Mobility

  You can use a Cisco AnyConnect Secure Mobility license to provide support for captive portal detection and remediation in combination with either an AnyConnect Essentials or an AnyConnect Premium license.

Captive portal detection and remediation support only computers running Microsoft Windows 7, Vista, XP; and Mac OS X 10.5 and 10.6.

Captive Portal Remediation

Captive portal remediation is the process of satisfying the requirements of a captive portal hotspot to obtain network access. By default, the connect failure policy prevents captive portal remediation because it restricts network access. You can configure AnyConnect to lift restricted access to let the user satisfy the captive portal requirements. You can also specify the duration for which the client lifts restricted access.

Captive Portal Remediation Requirements

Support for both captive portal detection and remediation requires one of the following licenses:

- AnyConnect Premium (SSL VPN Edition)
- Cisco AnyConnect Secure Mobility

  You can use a Cisco AnyConnect Secure Mobility license to provide support for captive portal detection and remediation in combination with either an AnyConnect Essentials or an AnyConnect Premium license.

Captive portal detection and remediation support only computers running Microsoft Windows 7, Vista, XP; and Mac OS X 10.5 and 10.6.

Configuring Support for Captive Portal Remediation

If the connect failure policy is open, users can remediate captive portal requirements. The captive portal remediation feature applies only if the connect failure policy is closed and a captive portal is present.

By default, support for captive portal remediation is disabled. To enable captive portal remediation,

Step 1 Configure a connect failure policy (see Configuring a Connect Failure Policy).

Step 2 Set the following parameters:

- Allow Captive Portal Remediation—Check to let the Cisco AnyConnect Secure Mobility client lift the network access restrictions imposed by the closed connect failure policy. Doing so lets the user meet the captive portal requirements. By default, this parameter is unchecked to provide the greatest security; however, you must enable it if you want the client to connect to the VPN if a captive portal is preventing it from doing so.
- Remediation Timeout—Enter the number of minutes that AnyConnect lifts the network access restrictions. The user needs enough time to satisfy the captive portal requirements.

  If always-on VPN is enabled, and the user clicks Connect or a reconnect is in progress, a message window indicates the presence of a captive portal. The user can then open a web browser window to remediate the captive portal.

If Users Cannot Access a Captive Portal Page

If users cannot access a captive portal remediation page, ask them to try the following steps successively until they can remediate:

Step 1 Disable and re-enable the network interface. This action triggers a captive portal detection retry.

Step 2 Terminate any applications that use HTTP, such as instant messaging programs, e-mail clients, IP phone clients, and all but one browser to perform the remediation. The captive portal may be actively inhibiting DoS attacks by ignoring repetitive attempts to connect, causing them to time out on the client end. The attempt by many applications to make HTTP connections exacerbates this problem.

Step 3 Retry Step 1.

Step 4 Restart the computer.

Client Firewall with Local Printer and Tethered Device Support

When users connect to the ASA, all traffic is tunneled through the connection and users cannot access resources on their local network. This includes printers, cameras, and Windows Mobile devices (tethered devices) that sync with the local computer. Enabling Local LAN Access in the client profile resolves this problem, however it can introduce a security or policy concern for some enterprises as a result of unrestricted access to the local network. You can use the ASA to deploy endpoint OS firewall capabilities to restrict access to particular types of local resources, such as printers and tethered devices.

To do so, enable client firewall rules for specific ports for printing. The client distinguishes between inbound and outbound rules. For printing capabilities, the client opens ports required for outbound connections, but blocks all incoming traffic. The client firewall is independent of the always-on feature.

Note Be aware that users logged in as administrators have the ability to modify the firewall rules deployed to the client by the ASA. Users with limited privileges cannot modify the rules. For either user, the client reapplies the rules when the connection terminates.

If you configure the client firewall, and the user authenticates to an Active Directory (AD) server, the client still applies the firewall policies from the ASA. However, the rules defined in the AD group policy take precedence over the rules of the client firewall.

Usage Notes about Firewall Behavior

The following notes clarify how the AnyConnect client uses the firewall:

- The source IP is not used for firewall rules. The client ignores the source IP information in the firewall rules sent from the ASA. The client determines the source IP depending on whether the rules are public or private. Public rules are applied to all interfaces on the client. Private rules are applied to the Virtual Adapter.
- The ASA supports many protocols for ACL rules. However, the AnyConnect firewall feature supports only TCP, UDP, ICMP, and IP. If the client receives a rule with a different protocol, it treats it as an invalid firewall rule, and then disables split tunneling and uses full tunneling for security reasons.

Be aware of the following differences in behavior for each operating system:

- For Windows computers, deny rules take precedence over allow rules in Windows Firewall. If the ASA pushes down an allow rule to the AnyConnect client, but the user has created a custom deny rule, the AnyConnect rule is not enforced.
- On Windows Vista, when a firewall rule is created, Vista takes the port number range as a comma-separated string. The port range can be a maximum of 300 ports. For example, from 1-300 or 5000-5300. If you specify a range greater than 300 ports, the firewall rule is applied only to the first 300 ports.
- Windows users whose firewall service must be started by the AnyConnect client (not started automatically by the system) may experience a noticeable increase in the time it takes to establish a VPN connection.
- On Mac computers, the AnyConnect client applies rules sequentially in the same order the ASA applies them. Global rules should always be last.
- For third-party firewalls, traffic is passed only if both the AnyConnect client firewall and the third-party firewall allow that traffic type. If the third-party firewall blocks a specify traffic type that the AnyConnect client allows, the client blocks the traffic.

The following sections describe procedures on how to do this:

- Deploying a Client Firewall for Local Printer Support, page 3-32
- Tethered Devices Support, page 3-33

Deploying a Client Firewall for Local Printer Support

The ASA supports the SSL VPN client firewall feature with ASA version 8.3(1) or later, and ASDM version 6.3(1) or later. This section describes how to configure the client firewall to allow access to local printers, and how to configure the client profile to use the firewall when the VPN connection fails.

Limitations and Restrictions of the Client Firewall

The following limitations and restrictions apply to using the client firewall to restrict local LAN access:

- Due to limitations of the OS, the client firewall policy on computers running Windows XP is enforced for inbound traffic only. Outbound rules and bidirectional rules are ignored. This would include firewall rules such as 'permit ip any any'.
- Host Scan and some third-party firewalls can interfere with the firewall.
- Because the ASA does not support IPv6 addresses for split tunneling, the client firewall does not support IPv6 devices on the local network.

Table 3-2 clarifies what direction of traffic is affected by the source and destination port settings:

Table 3-2 Source and Destination Ports and Traffic Direction Affected

Source Port	Destination Port	Traffic Direction Affected
Specific port number	Specific port number	Inbound and outbound
A range or 'All' (value of 0)	A range or 'All' (value of 0)	Inbound and outbound
Specific port number	A range or 'All' (value of 0)	Inbound only
A range or 'All' (value of 0)	Specific port number	Outbound only

Example ACL Rules for Local Printing

Table 3-3 shows example ACL rules for local printing:

Table 3-3 Example ACL Rules for Local Printing

Description	Permission	Interface	Protocol	Source Port	Destination Address	Destination Port
Deny all	Deny	Public	Any	Default[1]	Any	Default
LPD	Allow	Public	TCP	Default	Any	515
IPP	Allow	Public	TCP	Default	Any	631
Printer	Allow	Public	TCP	Default	Any	9100
mDNS	Allow	Public	UDP	Default	224.0.0.251	5353
LLMNR	Allow	Public	UDP	Default	224.0.0.252	5355
NetBios	Allow	Public	TCP	Default	Any	137
NetBios	Allow	Public	UDP	Default	Any	137

1. The port range is 1 to 65535.

Note To enable local printing, you must enable the **Local LAN Access** feature in the client profile with a defined ACL rule *allow Any Any*.

Configuring Local Print Support

To enable local print support, follow these steps:

Step 1 Enable the SSL VPN client firewall in a group policy. Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 2 Select a group policy and click **Edit**. The Edit Internal Group Policy window displays.

Step 3 Go to **Advanced > SSL VPN Client > Client Firewall**. Click **Manage** for the Private Network Rule.

Step 4 Create an ACL and specify an ACE using the rules in Table 3-3. Add this ACL as a Public Network Rule.

Step 5 If you enabled the Automatic VPN Policy always-on and specified a closed policy, in the event of a VPN failure, users have no access to local resources. You can apply the firewall rules in this scenario by going to **Preferences (Part 2)** in the profile editor and checking **Apply last local VPN resource rules**.

Tethered Devices Support

To support tethered devices and protect the corporate network, create a standard ACL in the group policy, specifying destination addresses in the range that the tethered devices use. Then specify the ACL for split tunneling as a network list to exclude from tunneled VPN traffic. You must also configure the client profile to use the last VPN local resource rules in case of VPN failure.

Note For Windows Mobile devices that need to sync with the computer running AnyConnect, specify the destination address 169.254.0.0 in the ACL.

Follow these steps:

Step 1 In ASDM, go to **Group Policy > Advanced > Split Tunneling**.

Step 2 Next to the Network List field, click **Manage**. The ACL Manager displays.

Step 3 Click the **Standard ACL** tab.

Step 4 Click **Add** and then **Add ACL**. Specify a name for the new ACL.

Step 5 Choose the new ACL in the table and click **Add** and then **Add ACE**. The Edit ACE window displays.

Step 6 For Action, choose the **Permit** radio button. Specify the Destination as *169.254.0.0*. For Service, choose *IP*. Click **OK**.

Step 7 In the Split Tunneling pane, for Policy, choose **Exclude Network List Below**. For Network List, choose the ACL you created. Click **OK**, then **Apply**.

Configuring Certificate Enrollment using SCEP

The secure mobility 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 SCEP, the client sends a certificate request and the certificate authority (CA) automatically accepts or denies the request. (SCEP 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.)

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

This section describes the following topics:

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 the client 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 Automatic SCEP Host settings of their client profile. The client initiates the SCEP certificate request after a VPN, based on the SCEP-enabled group-url, has been established.

The second method for triggering automatic certificate retrieval is the case where the certificate contents are not specified for matching 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, the client searches the client profile, downloaded as part of the VPN activation, to see if the group-url chosen for the connection is in the client profile.

If the client finds the group-url in the Automatic SCEP Host setting of the client profile, this triggers the automatic SCEP retrieval process in the same manner as described in the previous method.

The user may be prompted for a “CA Password”. The CA Password is the challenge password or token to be offered to the certificate authority that identifies the user to the certificate authority. With this password, and the other data in the SCEP section of the profile, the client contacts the certificate authority and continues with the SCEP retrieval process. If the *Prompt For Challenge PW* attribute is enabled in the client profile, the client prompts the user for a CA Certificate.

Manual Certificate Retrieval

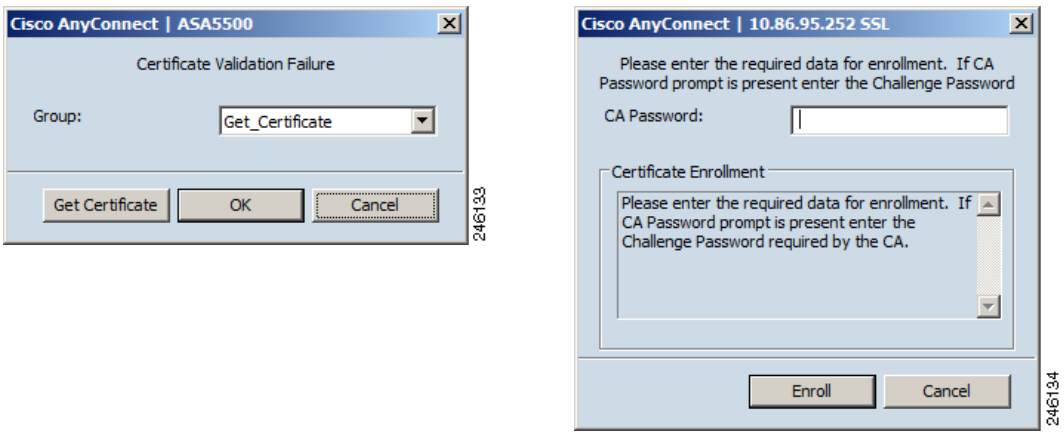
Users initiate requests for new certificates by clicking the **Get Certificate** or **Enroll** button on the client interface. The client presents these buttons to users in any of these circumstances as long as the SCEP feature is enabled in the client profile:

- When the ASA requests a certificate and none of the certificates on the host that are available are accepted.
- When the current certificate used by AnyConnect is set to expire within the number of days defined in the Certificate Expiration Threshold setting in the client profile.
- 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 CA URL field.

Figure 3-16 Get Certificate and Enroll Buttons

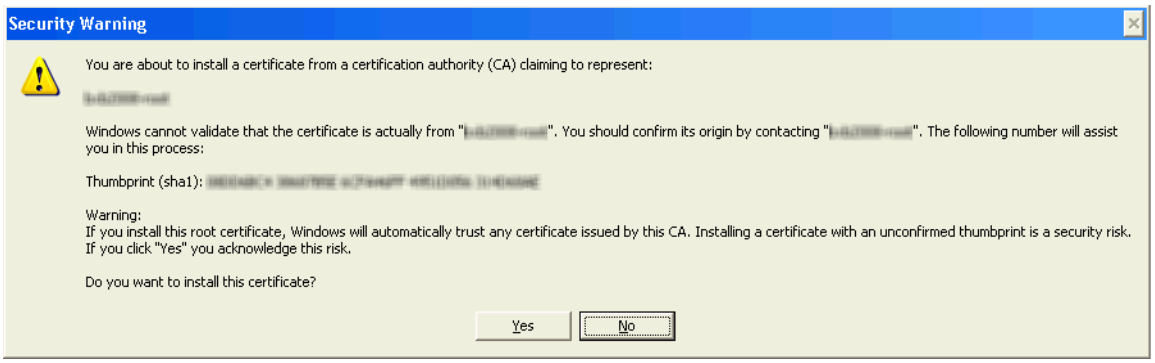


The user may be prompted for a “CA Password”. The CA Password is the challenge password or token to be offered to the certificate authority that identifies the user to the certificate authority. With this password, and the other data in the SCEP section of the profile, the client contacts the certificate authority and continues with the SCEP retrieval process. If the **Prompt For Challenge PW** attribute is enabled in the client profile, the client prompts the user for a CA Certificate.

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 3-17. 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 3-17 Windows Certificate Security Warning



Configuring SCEP to Provision and Renew Certificates

AnyConnect retrieves certificates using SCEP if the SCEP settings are defined in a client profile, the client profile is specified in a group policy, and the group policy is specified in the users' connection profile.

See the "Creating and Editing an AnyConnect Profile" section on page 3-2 for more information about how to configure a client profile.

To enable SCEP, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Click **Add** (or **Edit**) to create (or edit) an AnyConnect Profile and click **Certificate Enrollment** in the AnyConnect Client Profile tree on the left.

Step 3 In the **Certificate Enrollment** pane check **Certificate Enrollment.**

Step 4 Specify an **Automatic SCEP Host** to retrieve the certificate. Enter an FQDN or an IP address. For example: **`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.

Step 5 Specify a CA URL to identify the SCEP CA server. Enter an FQDN or IP Address. For example: **`http://ca01.cisco.com`**

Step 6 (Optional) Check **Prompt For Challenge PW** to prompt the user for their username and one-time password.

Step 7 (Optional) Enter a Thumbprint for the CA certificate. Use SHA1 or MD5 hashes. For example: `8475B661202E3414D4BB223A464E6AAB8CA123AB.`

Note Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a "fingerprint" or "thumbprint" attribute field in a certificate it issued.

Step 8 Check Certificate Contents to be requested. For definitions of the see AnyConnect Profile Editor, Certificate Enrollment, page 3-71

Step 9 Specify a CA Domain. For example: **`cisco.com`**

Step 10 Check **Display Get Certificate Button** to 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. Without this button, users see the **Enroll** button, along with a message box that AnyConnect is contacting the certificate authority to attempt certificate enrollment.

Step 11 (Optional) Enable SCEP for a specific host in the server list. Doing this overrides the SCEP host setting in Step 4. Go to the Server List pane and Edit an existing host entry or create a new one with an SCEP host.

Certificate Storage after SCEP Request

Certificates obtained through a SCEP request are stored in the user's 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 operating systems, 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 for AnyConnect

To provide access to a private Registration Authority (RA), you should create a group-url that has an ACL restricting private side network connectivity to the desired RA. To automatically retrieve a certificate, users 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 CA URL setting of the client profile and initiates certificate enrollment. You 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 Automatic SCEP Host field in the user's client profile.
- Attach the client profile with Certificate Enrollment enabled 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, you 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 Expiration Notice

You can configure the client profile to warn users that their authentication certificate is about to expire. The **Certificate Expiration Threshold** setting specifies the number of days prior to the certificate's expiration date that AnyConnect warns users that their certificate is expiring.

Note The Certificate Expiration Threshold feature cannot be used with SCEP enrollment.

To set the Certificate Expiration Threshold, follow this procedure:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Click **Add** (or **Edit**) to create (or edit) an AnyConnect Profile and click **Certificate Enrollment** in the AnyConnect Client Profile tree on the left.

Step 3 In the **Certificate Enrollment** pane check **Certificate Enrollment.**

Step 4 Specify a Certificate Expiration Threshold—the number of days before the certificate expiration date, that AnyConnect warns users that their certificate is going to expire.

The default is 0 (no warning displayed). The range is 0-180 days.

Step 5 Do not check any **Certificate Content** checkboxes.

Step 6 Click **OK**.

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 which certificate store the client uses for locating 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 search 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 Chapter 8, "Enabling FIPS and Additional Security."

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

- Controlling the Certificate Store on Windows, page 3-39
- Creating a PEM Certificate Store for Mac and Linux, page 3-41

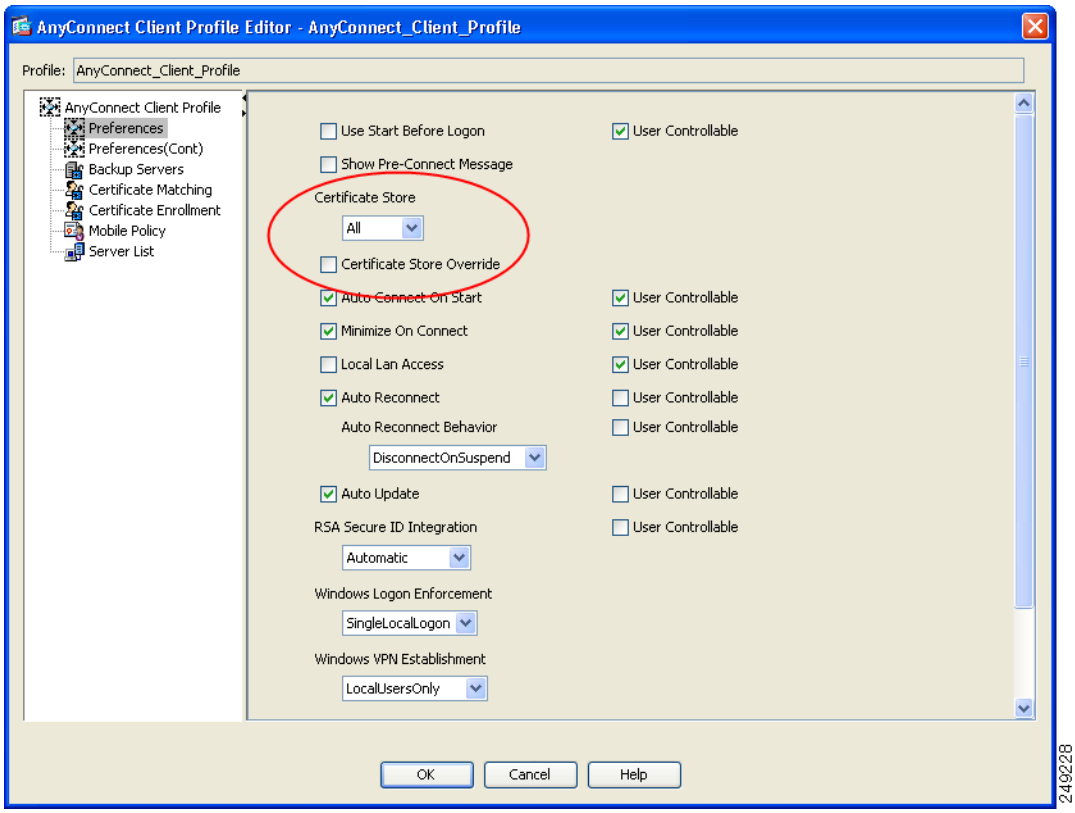
Controlling the Certificate Store on Windows

Windows provides separate certificate stores for the local machine and for the current user. Using Profile Editor you can specify in which certificate store the AnyConnect client searches for certificates.

Users with administrative privileges on the computer have access to both certificate stores. Users without administrative privileges only have access to the user certificate store.

In the Preferences pane of Profile Editor, use the **Certificate Store** list box to configure in which certificate store AnyConnect searches for certificates. Use the **Certificate Store Override** checkbox to allow AnyConnect to search the machine certificate store for users with non-administrative privileges.

Figure 3-18 Certificate Store list box and Certificate Store Override check box



Certificate Store has three possible settings:

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

Certificate Store Override has two possible settings:

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

Table 3-4 shows examples of Certificate Store and Certificate Store Override configurations.

Table 3-4 Examples of Certificate Store and Certificate Store Override Configurations

Certificate Store Setting	Certificate Store Override Setting	AnyConnect Action
All	cleared	AnyConnect searches all certificate stores. AnyConnect is not allowed to access the machine store when the user has non-administrative privileges. This is the default setting. 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	checked	AnyConnect searches all certificate stores. AnyConnect is allowed to access the machine store when the user has non-administrative privileges.
Machine	checked	AnyConnect searches the machine certificate store. AnyConnect is allowed to search the machine store of non-administrative accounts.
Machine	cleared	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.

To specify in which certificate store the AnyConnect client searches for certificates, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Click the **Preferences** pane and choose a Certificate Store type from the drop-down list:

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

Step 3 Check or clear the Certificate Store Override checkbox in order to allow AnyConnect client access to the machine certificate store if the user has a non-administrative account.

Step 4 Click **OK**.

Creating a PEM Certificate Store for Mac and Linux

AnyConnect 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 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 5. Place the appropriate certificates in these folders:

Table 5 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 5 apply.

Configuring Certificate Matching

AnyConnect supports the following certificate match types. Some or all of these may be used for client certificate matching. Certificate matchings 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 the "Certificate Matching Example" section on page 3-44 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 3-6 lists the well known set of constraints with their corresponding object identifiers (OIDs).

Table 3-6 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

Table 3-6 Extended Certificate Key Usage (continued)

Constraint	OID
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.

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 3-7 lists the supported criteria:

Table 3-7 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

Table 3-7 Criteria for Certificate Distinguished Name Mapping (continued)

Identifier	Description
CN	SubjectCommonName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

The profile can contain zero or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. *Distinguished Name* matching offers additional match criteria, including the ability for the administrator to specify that a certificate must or must not have the specified string, as well as whether wild carding for the string should be allowed.

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 Certificate Match criteria that apply to your certificates.

To configure certificate matching in the client profile, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Certificate Matching** pane.

Step 3 Check the Key Usage and Extended Key Usage settings to choose acceptable client certificates. A certificate must match at least one of the specified key to be selected. For descriptions of these usage settings, see the "AnyConnect Profile Editor, Certificate Matching" section on page 3-69

Step 4 Specify any Custom Extended Match Keys. These should be well-known MIB OID values, such as 1.3.6.1.5.5.7.3.11. 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

Step 5 Next to the Distinguished Names table, click **Add** to launch the Distinguished Name Entry window:

- **Name**—A distinguished name.

- **Pattern**—The string to use in the match. The pattern to be matched should include only the portion of the string you want to match. There is no need to include pattern match or regular expression syntax. If entered, this syntax will be considered part of the string to search for.

  For example, if a sample string was abc.cisco.com and the intent is to match on cisco.com, the pattern entered should be cisco.com.
- **Operator**—The operator to be used in performing the match.
  - Equal—Equivalent to ==
  - Not Equal—Equivalent to !=
- **Wildcard**—Include wildcard pattern matching. The pattern can be anywhere in the string.
- **Match Case**—Enable to perform case sensitive match with pattern.

Prompting Users to Select Authentication Certificate

You can configure the AnyConnect to present a list of valid certificates to users and let them choose the certificate with which they want to authenticate the session. This configuration is available only for Windows 7, XP, and Vista. By default, user certificate selection is disabled. To enable certificate selection, follow these steps to enable certificate selection in the AnyConnect profile:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Preferences (Part 2)** pane and uncheck **Disable Cert Selection**. The client now prompts the user to select the authentication certificate.

Users Configuring Automatic Certificate Selection in AnyConnect Preferences

Enabling user certificate selection 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 3-19 shows the Automatic Certificate Selection check box the user sees in the Preferences window:

Figure 3-19 Automatic Certificate Selection check box

Configuring a Server List

One of the main uses of the profile is to let the user list the connection servers. 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. The server list displays a list of server hostnames on the AnyConnect GUI in the *Connect to* drop-down list (Figure 3-20). The user can select a server from this list.

Figure 3-20 User GUI with Host Displayed in Connect to Drop-down List

Initially, the host you configure at the top of the list is the default server and appears in the GUI drop-down list. If the user selects an alternate server from the list, the client records the choice in the user preferences file on the remote computer, and the selected server becomes the new default server.

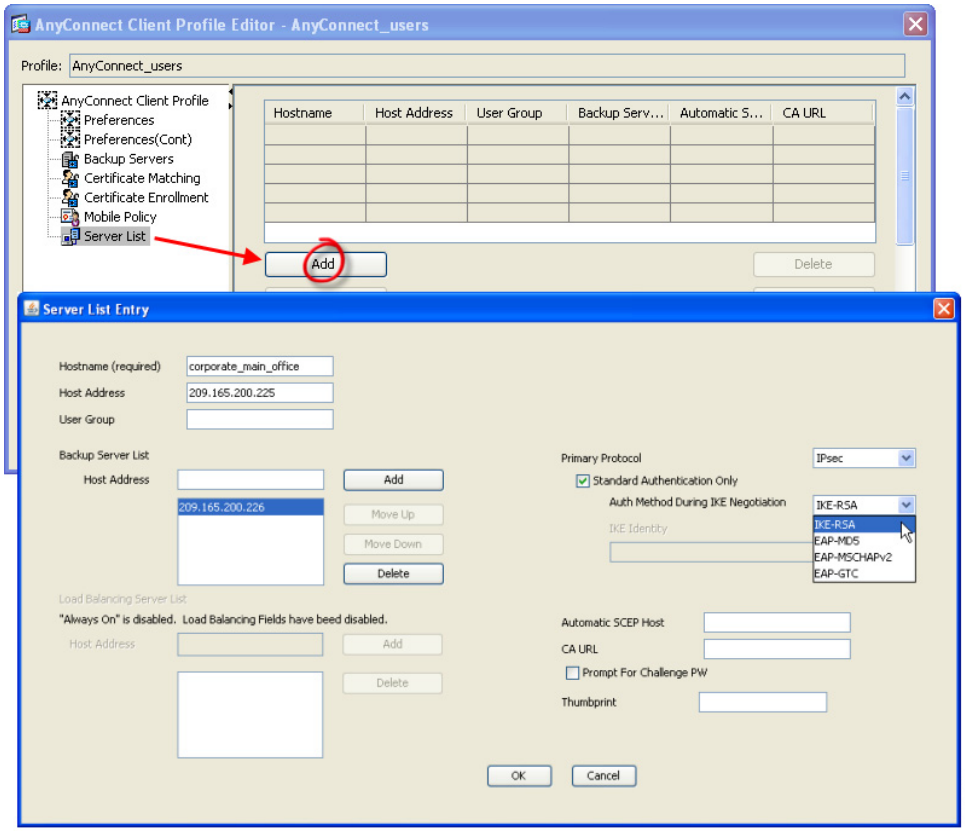
To configure a server list, follow this procedure:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Click **Server List**. The Server List pane opens.

Step 3 Click **Add**. The Server List Entry window opens (Figure 3-21).

Figure 3-21 Adding a Server List



Step 4 Enter a Hostname. You can enter an alias used to refer to the host, an FQDN, or an IP address. If you enter an FQDN or an IP address, you do not need to enter a Host Address.

Step 5 Enter a Host Address, if required.

Step 6 Specify a User Group (optional). The client uses the User Group in conjunction with the Host Address to form a group-based URL.

Note If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile.

Step 7 Add backup servers (optional). If the server in the server list is unavailable, the client attempts to connect to the servers in that server's backup list before resorting to a global backup server list.

Step 8 Add load balancing backup servers (optional). If the host for this server list entry specifies a load balancing cluster of security appliances, and the always-on feature is enabled, specify the backup devices of the cluster in this list. If you do not, the always-on feature blocks access to backup devices in the load balancing cluster.

Step 9 Specify the Primary Protocol (optional) for the client to use for this ASA, either SSL or IPsec using IKEv2. The default is SSL. To disable the default authentication method (the proprietary AnyConnect EAP method), check **Standard Authentication Only**, and choose a method from the drop-down list.

Note Changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.

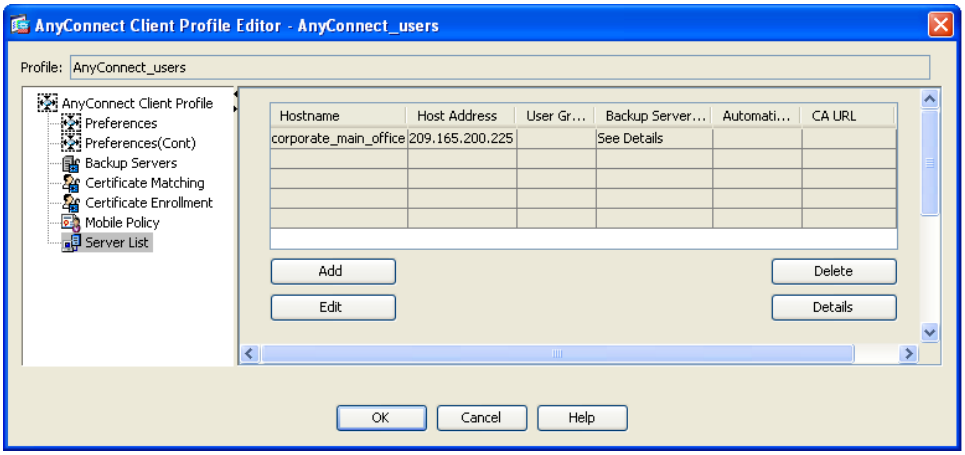
Step 10 Specify the URL of the SCEP CA server (optional). Enter an FQDN or IP Address. For example, http://ca01.cisco.com.

Step 11 Check **Prompt For Challenge PW** (optional) to enable the user to make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.

Step 12 Enter the certificate thumbprint of the CA. Use SHA1 or MD5 hashes. Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.

Step 13 Click **OK**. The new server list entry you configured appears in the server list table (Figure 3-22).

Figure 3-22 A New Server List Entry



Configuring a Backup Server List

You can configure a list of backup servers the client uses in case the user-selected server fails. These servers are specified in the Backup Servers pane of the AnyConnect profile. In some cases, the list might specify host specific overrides. Follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Backup Servers** pane and enter host addresses of the backup servers.

Configuring a Windows Mobile Policy

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

Restrictions and Limitations

Before configuring the Mobile Policy, take note of these restrictions and limitations:

- 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, you 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.
- A Windows Mobile device that uses the Microsoft Local Authentication Plug-ins (LAPs) must be configured with a password or PIN before establishing a VPN connection.
- A Windows Mobile 5 device with the Messaging and Security Feature Pack, delivered as part of Adaptation Kit Upgrade 2 (AKU2), must be synchronized with an Exchange server before the Mobile Policy can be enforced.
- You should remind users to check with their service provider regarding their data plans before using Cisco AnyConnect Secure Mobility client for Windows Mobile. Users might incur additional charges if they exceed the data usage limits of their plans.
- The Mobile Policy merely validates the policy that is already present; it does not change it.

Configuring the Mobile Policy in the Client Profile

To enable the Mobile Device Lock in the client profile, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Mobile Policy** pane and check **Device Lock Required**.

Step 3 In the Maximum Timeout Minutes field, enter the maximum number of minutes before the device lock takes effect.

Step 4 In the Minimum Password Length field, enter the minimum number of characters for the device lock password or PIN.

Step 5 Specify a Password Complexity for the required device lock password:

- alpha—Requires an alphanumeric password.
- pin—Requires a numeric PIN.
- strong—Requires a strong alphanumeric password which must contain at least 7 characters, including a minimum of 3 from the set of uppercase, lowercase, numerals, and punctuation characters.

Configuring Auto Connect On Start

Auto Connect on Start automatically establishes a VPN connection with the secure gateway specified by the VPN client profile. Upon connecting, the client 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.

By default, Auto Connect on Start is **disabled**. When the user launches the AnyConnect client, the 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 GUI and click **Connect**. Upon connecting, the client applies the settings of the client profile provided by the security appliance.

AnyConnect has evolved from having the ability to establish a VPN connection automatically upon the startup of AnyConnect to having that VPN connection be "always-on" by the Post Log-in Always-on feature. The disabled by default configuration of Auto Connect on Startup element reflects that evolution. If your enterprise's deployment uses the Auto Connect on Startup feature, consider using the Trusted Network Detection feature instead.

Trusted Network Detection (TND) gives you the ability to have AnyConnect 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. For information on configuring Trusted Network Detection, see "Trusted Network Detection" section on page 3-17.

By default, Auto Connect on Start is disabled. To enable it, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Choose **Preferences** in the navigation pane.

Step 3 Check **Auto Connect On Start**.

Configuring Auto Reconnect

Unlike the IPsec VPN client, AnyConnect can recover from VPN session disruptions and 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.

You can configure the Auto Reconnect feature to attempt to reestablish a VPN connection if you lose connectivity (the default behavior). You can also define the reconnect behavior during and after *system suspend* or *system resume*. 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, enable the Auto Reconnect Behavior *Reconnect After Resume*.

To configure the Auto Reconnect settings in the client profile, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Choose **Preferences** in the navigation pane.

Step 3 Check **Auto Reconnect**.

Note If you uncheck *Auto Reconnect*, the client does not attempt to reconnect, regardless of the cause of the disconnection.

Step 4 Choose the Auto Reconnect Behavior (not supported for Linux):

- Disconnect On Suspend— AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resume.
- Reconnect After Resume—The client retains resources assigned to the VPN session during a system suspend and attempts to reconnect after the system resume.

Local Proxy Connections

By default, AnyConnect lets users establish a VPN session through a transparent or non-transparent proxy on the local PC.

Some examples of elements that provide a transparent proxy service include:

- Acceleration software provided by some wireless data cards
- Network component on some antivirus software, such as Kaspersky.

Local Proxy Connections Requirements

AnyConnect supports this feature on the following Microsoft OSs:

- Windows 7 (32-bit and 64-bit)
- Windows Vista (32-bit and 64-bit)—SP2 or Vista Service Pack 1 with KB952876.
- Windows XP SP2 and SP3.

Support for this feature requires either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.

Configuring Local Proxy Connections

By default, AnyConnect supports local proxy services to establish a VPN session. To disable AnyConnect support for local proxy services, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Choose **Preferences (Part 2)** in the navigation pane.

Step 3 Uncheck **Allow Local Proxy Connections** near the top of the panel.

Optimal Gateway Selection

Using the Optimal Gateway Selection (OGS) feature, you can minimize latency for Internet traffic without user intervention. With OGS, AnyConnect identifies and selects which secure gateway is best for connection or reconnection. OGS begins upon first connection or upon a reconnection at least four hours after the previous disconnection. Users who travel to distant locations connect to a secure gateway nearer to the new location for better performance. Your home and office will get similar results from the same gateway, so no switch of secure gateways will typically occur in this instance. Connection to another secure gateway occurs rarely and only occurs if the performance improvement is at least 20%.

Note You can configure these threshold values using the Profile Editor. By optimizing these values for your particular network, you can find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials.

OGS is not a security feature, and it performs no load balancing between secure gateway clusters or within clusters. You can optionally give the end user the ability to enable or disable the feature.

The minimum round trip time (RTT) solution selects the secure gateway with the fastest RTT between the client and all other gateways. The client always reconnects to the last secure gateway if the time elapsed has been less than four hours. Factors such as load and temporary fluctuations of the network connection may affect the selection process, as well as the latency for Internet traffic.

It contacts only the primary servers to determine the optimal one. Once determined, the connection algorithm is as follows:

1. Attempt to connect to the optimal server.

2. If that fails, try the optimal server's backup server list.
3. If that fails, try each remaining server in the OGS selection list, ordered by its selection results.

Refer to the "AnyConnect Profile Editor, Backup Servers" section on page 3-68 for additional information on backup servers.

Optimal Gateway Selection Requirements

OGS supports VPN endpoints running:

- Windows 7, Vista, and XP
- Mac OS X 10.5 and 10.6

Configuring Optimal Gateway Selection

You control the activation and deactivation of OGS and specify whether end users may control the feature themselves in the AnyConnect profile. Follow these steps to configure OGS using the Profile Editor:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Check the **Enable Optimal Gateway Selection** check box to activate OGS.

Step 3 Check the **User Controllable** check box to make OGS configurable for the remote user accessing the client GUI.

Note When OGS is enabled, we recommend that you also make the feature user controllable. A user may need the ability to choose a different gateway from the profile if the AnyConnect client is unable to establish a connection to the OGS-selected gateway.

Step 4 At the Suspension Time Threshold parameter, enter the minimum time (in hours) the VPN must have been suspended before invoking a new gateway-selection calculation. The default is 4 hours.

Step 5 At the Performance Improvement Threshold parameter, enter the percentage of performance improvement that is required before triggering the client to re-connect to another secure gateway following a system resume. The default is 20%.

Note If too many transitions are occurring and users have to re-enter credentials quite frequently, you should increase either or both of these thresholds. Adjust these value for your particular network to find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials.

If OGS is enabled when the client GUI starts, **Automatic Selection** displays in the Connect To drop-down menu on the Cisco AnyConnect Connection tab. You cannot change this selection. OGS automatically chooses the optimal secure gateway and displays the selected gateway on the status bar. You may need to click **Select** to start the connection process.

Note

If you made the feature user controllable, the user can manually override the selected secure gateway with the following steps:

Step 1 If currently connected, click **Disconnect**.

Step 2 Open the Preferences tab and uncheck **Enable Optimal Gateway Selection**.

Step 3 Choose the desired secure gateway.

Note If AAA is being used, end users may have to re-enter their credentials when transitioning to a different secure gateway. The use of certificates eliminates this.

Writing and Deploying Scripts

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

- Upon the establishment of a new 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 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 client 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 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.

This section covers the following topics:

Scripting Requirements and Limitations

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

The client 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 the client 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 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, the client does not launch scripts. Use the AnyConnect profile EnableScripting parameter to enable scripts. The client 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 operating system type on which it will run when AnyConnect launches.

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 operating system. If a script cannot run properly from the command line on the native operating system, AnyConnect cannot run it properly.

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

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

Note Microsoft Windows Mobile does not support this option. Use an enterprise software deployment system to deploy scripts for this operating system.

If you use ASDM version 6.3 or later, the ASA 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, you must import the scripts with the following prefixes:

- scripts_OnConnect
- scripts_OnDisconnect

To ensure the scripts run reliably, configure all ASAs 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 ASAs that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- Or use an enterprise software deployment system to deploy scripts manually to the VPN endpoints on which you want to run the scripts.

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

  - OnConnect
  - OnDisconnect

  Install the scripts in the directory shown in Table 3-8.

Table 3-8 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 (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 in the client profile, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Choose **Preferences (Part 2)** in the navigation pane.

Step 3 Check **Enable Scripting**. The client launches scripts on connecting or disconnecting the VPN connection.

Step 4 Check **User Controllable** to let users enable or disable the running of On Connect and OnDisconnect scripts.

Step 5 Check **Terminate Script On Next Event** to enable the client to terminate a running script process if a transition to another scriptable event occurs. For example, the client terminates a running On Connect script if the VPN session ends, and terminates a running OnDisconnect script if AnyConnect starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the On Connect or OnDisconnect script launched, and all their script descendents. On Mac OS and Linux, the client terminates only the On Connect or OnDisconnect script; it does not terminate child scripts.

Step 6 Check **Enable Post SBL On Connect Script** (enabled by default) to let the client launch the On Connect script (if present) if SBL establishes the VPN session.

Note Be sure to add the client profile to the ASA 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 3-8 shows the required scripts directory for each operating system.

Step 2 Try running the script from the command line. The client 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 operating system.

Step 3 Make sure the scripts directory on the VPN endpoint contains only one OnConnect and only one OnDisconnect script. If one ASA downloads one OnConnect script and during a subsequent connection a second ASA downloads an OnConnect script with a different filename suffix, the client might run the unwanted script. If the script path contains more than one OnConnect or OnDisconnect script and you are using the ASA to deploy scripts, remove the contents of the scripts directory and re-establish a 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 a VPN session.

Step 4 If the operating system is Linux, make sure the script file permissions are set to execute.

Step 5 Make sure the client profile has scripting enabled.

Authentication Timeout Control

By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out. Use the instructions in the following sections to change the value of this timer.

Authentication Timeout Control Requirements

AnyConnect supports this feature on all OSs supported by AnyConnect.

Support for this feature requires either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.

Configuring Authentication Timeout

To change the number of seconds AnyConnect waits for an authentication from the secure gateway before terminating the connection attempt, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Choose **Preferences (Part 2)** in the navigation pane.

Step 3 Enter a number of seconds in the range 10–120 into the **Authentication Timeout Values** text box.

Proxy Support

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

Configuring the Client to Ignore Browser Proxy Settings

You can specify a policy in the AnyConnect profile to bypass the Microsoft 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.

Note Connecting through a proxy is not supported with the always-on feature enabled. Therefore, if you enable always-on, configuring the client to ignore proxy settings is unnecessary.

Follow these steps to enable AnyConnect to ignore Internet Explorer proxy settings:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Preferences (Part 2)** pane.

Step 3 In the Proxy Settings drop-down list, choose **Ignore Proxy**.

Note AnyConnect currently supports only the Ignore Proxy setting; it does not support Native and Override.

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 ASA 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 ASA must be set to Tunnel All Networks.

You can configure the ASA to allow or not allow proxy lockdown, in the group policy. To do this using ASDM, follow this procedure:

Step 1 Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 2 Choose a group policy and click **Edit**. The Edit Internal Group Policy window displays.

Step 3 In the navigation pane, go to **Advanced > Browser Proxy**. The Proxy Server Policy pane displays.

Step 4 Click **Proxy Lockdown** to display more proxy settings.

Step 5 Uncheck **Inherit** and select **Yes** to enable proxy lockdown and hide the Internet Explorer Connections tab for the duration of the AnyConnect session or select **No** to disable proxy lockdown and expose the Internet Explorer Connections tab for the duration of the AnyConnect session.

Step 6 Click **OK** to save the Proxy Server Policy changes.

Step 7 Click **Apply** to save the Group Policy changes.

Proxy Auto-Configuration File Generation for Clientless Support

Some versions of the ASA 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 occur. AnyConnect generates this file only if the ASA does not specify private-side proxy settings.

Allowing a Windows RDP Session to Launch a VPN Session

You can allow users to log on, to a computer running the Cisco AnyConnect Secure Mobility client, using Windows Remote Desktop (RDP) and create a VPN connection to a secure gateway from the RDP session. A split tunneling VPN configuration is required for this to function correctly.

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, AnyConnect 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.

You can use the following settings for Windows Logon Enforcement:

- Single Local Logon—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.
- SingleLogon—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.

Note 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.

The Windows VPN Establishment settings in the client profile specify the behavior of the client when a user who is remotely logged on a computer running AnyConnect establishes a VPN connection. The possible values are:

- Local Users Only—Prevents a remotely logged-on user from establishing a VPN connection. AnyConnect client versions 2.3 and earlier operated in this manner.

- Allow Remote Users—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 terminates to allow the remote user to regain access to the client computer. Remote users must wait 90 seconds after VPN establishment if they want to disconnect their RDP session without causing the VPN session to terminate.

Note On Vista, the Windows VPN Establishment profile setting is not currently enforced during Start Before Logon (SBL). AnyConnect 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 Windows VPN Establishment setting is Local Users Only.

To enable an AnyConnect session from a Windows RDP Session, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Preferences** pane.

Step 3 Choose a Windows Logon Enforcement method:

- Single Local Logon—Allows only one local user to be logged on during the entire VPN connection.
- Single Logon—Allows only one user to be logged on during the entire VPN connection.

Step 4 Choose a Windows VPN Establishment method that specifies the behavior of the client when a user who is remotely logged on establishes a VPN connection:

- Local Users Only—Prevents a remotely logged-on user from establishing a VPN connection.
- Allow Remote Users—Allows remote users to establish a VPN connection.

Note On Vista, the Windows VPN Establishment setting is not currently enforced during Start Before Logon (SBL).

AnyConnect over L2TP or PPTP

ISPs in some countries 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, the client 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 PPP Exclusion setting in the AnyConnect profile. 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 in the profile, follow these steps:

Step 1 Launch the Profile Editor from ASDM (see the "Creating and Editing an AnyConnect Profile" section on page 3-2).

Step 2 Go to the **Preferences (Part 2)** pane.

Step 3 Choose a **PPP Exclusion** Method. Checking **User Controllable** for this field lets users view and change these settings:

- 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.

Step 4 In the **PPP Exclusion Server IP field**, enter the IP address of the security gateway used for PPP exclusion. Checking **User Controllable** for this field lets users view and change this IP address.

Instructing Users to Override PPP Exclusion

If automatic detection does not work, and you configured PPP Exclusion as user controllable, the user can override the settings by editing the AnyConnect preferences file on the local computer. The following procedure describes how to do this:

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.

AnyConnect Profile Editor VPN Parameter Descriptions

The following section describes all the settings that appear on the various panes of the profile editor.

Anyconnect Profile Editor, Preferences

Use Start Before Logon (Windows Only)—Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears. After authenticating, the login dialog box appears and the user logs in as usual. SBL also lets you control the use of login scripts, password caching, mapping network drives to local drives, and more.

Show Pre-connect Message—Displays a message to the user before the user makes the first connection attempt. For example, you could remind the user to insert their smartcard into the reader.

Certificate Store—Controls which certificate store AnyConnect uses for locating certificates. 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 stores. The default setting (All) is appropriate for the majority of cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.

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

Certificate Store Override—Allows you to direct AnyConnect to search for certificates in the Windows machine certificate store. This is useful in cases where certificates are located in this store and users do not have administrator privileges on their machine.

Auto Connect On Start—AnyConnect, when started, automatically establishes a VPN connection with the secure gateway specified by the AnyConnect profile, or to the last gateway to which the client connected.

Minimize On Connect—After establishing a VPN connection, the AnyConnect GUI minimizes.

Local LAN Access—Allows the user complete access to the local LAN connected to the remote computer during the VPN session to the ASA.

Note Enabling Local LAN Access can potentially create a security weakness from the public network through the user computer into the corporate network. Alternatively, you can configure the security appliance (version 8.3(1) or later) to deploy an SSL client firewall that uses the new AnyConnect Client Local Print firewall rule (enable *Apply last local VPN resource rules* in the always-on VPN section of the client profile).

Auto Reconnect—AnyConnect attempts to reestablish a VPN connection if you lose connectivity (enabled by default). If you disable Auto Reconnect, it does not attempt to reconnect, regardless of the cause of the disconnection.

Auto Reconnect Behavior:

- DisconnectOnSuspend (default)—AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resumes.
- ReconnectAfterResume—AnyConnect attempts to reestablish a VPN connection if you lose connectivity.

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, choose **ReconnectAfterResume** for the Auto Reconnect Behavior.

Auto Update—Disables the automatic update of the client.

RSA Secure ID Integration (Windows only)—Controls how the user interacts with RSA. By default, AnyConnect determines the correct method of RSA interaction (automatic setting).

- Automatic—Software or Hardware tokens accepted.
- Software Token—Only software tokens accepted.
- Hardware Token—Only hardware tokens accepted.

Windows Logon Enforcement—Allows a VPN session to be established from a Remote Desktop Protocol (RDP) session (A split tunneling VPN configuration is required). AnyConnect 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 terminates.

- Single Local Logon—Allows only one local user to be logged on during the entire VPN connection. A local user can establish a VPN connection while one or more remote users are logged on to the client PC.
- Single Logon—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 terminates. No additional logons are allowed during the VPN connection, so a remote logon over the VPN connection is not possible.

Windows VPN Establishment—Determines the behavior of AnyConnect when a user who is remotely logged on to the client PC establishes a VPN connection. The possible values are:

- Local Users Only—Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of AnyConnect.
- Allow Remote Users—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 terminates to allow the remote user to regain access to the client PC. 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.

Note On Vista, the Windows VPN Establishment setting is not currently enforced during Start Before Logon (SBL). AnyConnect 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 Windows VPN Establishment setting is Local Users Only.

For more detailed configuration information about the client features that appear on this pane, see these sections:

Start Before Logon—Configuring Start Before Logon

Certificate Store and Certificate Override—Configuring a Certificate Store

Auto Reconnect—Configuring Auto Reconnect, page 3-51

Windows Logon Enforcement—Allowing a Windows RDP Session to Launch a VPN Session, page 3-60

Anyconnect Profile Editor, Preferences Cont

Disable Cert Selection—Disables automatic certificate selection by the client and prompts the user to select the authentication certificate.

Allow Local Proxy Connections—By default, AnyConnect lets Windows users establish a VPN session through a transparent or non-transparent proxy service on the local PC. Some examples of elements that provide a transparent proxy service include:

- Acceleration software provided by some wireless data cards
- Network component on some antivirus software

Uncheck this parameter if you want to disable support for local proxy connections.

Proxy Settings—Specifies a policy in the AnyConnect profile to bypass the Microsoft Internet Explorer or Mac Safari proxy settings on the remote computer. This is useful when the proxy configuration prevents the user from establishing a tunnel from outside the corporate network. Use in conjunction with the proxy settings on the ASA.

- Native (not supported)
- Ignore Proxy—AnyConnect bypasses Microsoft Internet Explorer or Mac Safari proxy settings on the user computer.
- Override (not supported)

Enable Optimal Gateway Selection—AnyConnect identifies and selects which secure gateway is best for connection or reconnection based on the round trip time (RTT), minimizing latency for Internet traffic without user intervention. **Automatic Selection** displays in the Connect To drop-down list on the Connection tab of the client GUI.

- Suspension Time Threshold (hours)—The elapsed time from disconnecting to the current secure gateway to reconnecting to another secure gateway. If users experience too many transitions between gateways, increase this time.
- Performance Improvement Threshold (%)—The performance improvement that triggers the client to connect to another secure gateway. The default is 20%.

Note If AAA is used, users may have to re-enter their credentials when transitioning to a different secure gateway. Using certificates eliminates this problem.

Automatic VPN Policy (Windows and Mac only)—Automatically manages when a VPN connection should be started or stopped according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually.

Note Automatic VPN Policy does not prevent users from manually controlling a VPN connection.

- Trusted Network Policy—AnyConnect automatically disconnects a VPN connection when the user is inside the corporate network (the trusted network).
  - Disconnect—Disconnects the VPN connection upon the detection of the trusted network.
  - Connect—Initiates a VPN connection upon the detection of the trusted network.
  - Do Nothing—Takes no action in the trusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
  - Pause—AnyConnect suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.
- Untrusted Network Policy—AnyConnect starts 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.
  - Connect—Initiates the VPN connection upon the detection of an untrusted network.
  - Do Nothing—Initiates the VPN connection upon the detection of an untrusted network. This option disables always-on VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
- Trusted DNS Domains—DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *.cisco.com. Wildcards (*) are supported for DNS suffixes.
- Trusted DNS Servers—DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 161.44.124.*,64.102.6.247. Wildcards (*) are supported for DNS server addresses.
- Always On—Determines whether AnyConnect automatically connects to the VPN when the user logs in to a computer running Windows 7, Vista, or XP; or Mac OS X 10.5 or 10.6. Use this feature to enforce corporate policies to protect the computer from security threats by preventing access to Internet resources when it is not in a trusted network. You can set the always-on VPN parameter in group policies and dynamic access policies to override this setting. Doing so lets you specify exceptions according to the matching criteria used to assign the policy. If an AnyConnect policy enables always-on VPN and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.
- Allow VPN Disconnect—Determines whether AnyConnect displays a Disconnect button for always-on VPN sessions. Users of always-on VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as the following:
  - Performance issues with the current VPN session.
  - Reconnection issues following the interruption of a VPN session.

Caution The Disconnect locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. For the reasons noted above, disabling the Disconnect button can at times hinder or prevent VPN access.

For more information about this feature, see Disconnect Button for Always-on VPN, page 3-25.

- Connect Failure Policy—Determines whether the computer can access the Internet if AnyConnect cannot establish a VPN session (for example, when an ASA is unreachable). This parameter applies only if always-on VPN is enabled.

Caution A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. AnyConnect detects most captive portals; however, if it cannot detect a captive portal, the connect failure closed policy prevents all network connectivity. Be sure to read the "Connect Failure Policy for Always-on VPN" section on page 3-27" before configuring a connect failure policy.

  - Closed—Restricts network access when the VPN is unreachable. The purpose of this setting is to help protect corporate assets from network threats when resources in the private network responsible for protecting the endpoint are unavailable.
  - Open—Permits network access when the VPN is unreachable.
  - Allow Captive Portal Remediation—Lets AnyConnect lift the network access restrictions imposed by the closed connect failure policy when the client detects a captive portal (hotspot). Hotels and airports typically use captive portals to require the user to open a browser and satisfy conditions required to permit Internet access. By default, this parameter is unchecked to provide the greatest security; however, you must enable it if you want the client to connect to the VPN if a captive portal is preventing it from doing so.
  - Remediation Timeout—Number of minutes AnyConnect lifts the network access restrictions. This parameter applies if the Allow Captive Portal Remediation parameter is checked and the client detects a captive portal. Specify enough time to meet typical captive portal requirements (for example, 5 minutes).
  - Apply Last VPN Local Resource Rules—If the VPN is unreachable, the client applies the last client firewall it received from the ASA, which may include ACLs allowing access to resources on the local LAN.

PPP Exclusion —For a VPN tunnel over a PPP connection, specifies whether and how to determine the exclusion route so the client can exclude traffic destined for the secure gateway from the tunneled traffic intended for destinations beyond the secure gateway. The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI. If you make this feature user controllable, users can read and change the PPP exclusion settings.

- 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.
- Disabled—PPP exclusion is not applied.
- Override—Also enables PPP exclusion. If automatic detection fails to get the IP address of the PPP server, and you configured PPP exclusion as user controllable, instruct users to follow the instructions in the "Instructing Users to Override PPP Exclusion" section on page 3-62.

PPP Exclusion Server IP—The IP address of the security gateway used for PPP exclusion.

Enable Scripting—Launches OnConnect and OnDisconnect scripts if present on the security appliance flash memory.

- Terminate Script On Next Event—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 the client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the OnConnect or OnDisconnect script launched, and all their script descendents. On Mac OS and Linux, the client terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts.

- Enable Post SBL On Connect Script—Launches the OnConnect script if present and SBL establishes the VPN session. (Only supported if VPN endpoint is running Microsoft Windows 7, XP, or Vista).

Retain VPN On Logoff—Determines whether to keep the VPN session when the user logs off a Windows OS.

- User Enforcement—Specifies whether to end the VPN session if a different user logs on. This parameter applies only if "Retain VPN On Logoff" is checked and the original user logged off Windows when the VPN session was up.

Authentication Timeout Values—By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out. Enter a number of seconds in the range 10–120.

For more detailed configuration information about the client features that appear on this pane, see these sections:

Allow Local Proxy Connections—Local Proxy Connections, page 3-51

Proxy Settings—Configuring the Client to Ignore Browser Proxy Settings, page 3-58

Optimal Gateway Selection—Optimal Gateway Selection, page 3-52

Automatic VPN Policy and Trusted Network Detection—Configuring Trusted Network Detection, page 3-17

Always-on VPN—Always-on VPN, page 3-19

Connect Failure Policy—Connect Failure Policy for Always-on VPN, page 3-27

Allow Captive Portal Remediation—Captive Portal Hotspot Detection and Remediation, page 3-29

PPP Exclusion—AnyConnect over L2TP or PPTP, page 3-61

Authentication Timeout Values—Authentication Timeout Control, page 3-57

AnyConnect Profile Editor, Backup Servers

You can configure a list of backup servers the client uses in case the user-selected server fails. If the user-selected server fails, the client attempts to connect to the server at the top of the list first, and moves down the list, if necessary.

Host Address—Specifies an IP address or a Full-Qualified Domain Name (FQDN) to include in the backup server list.

Add—Adds the host address to the backup server list.

Move Up—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.

Move Down—Moves the selected backup server down in the list.

Delete—Removes the backup server from the server list.

For more information on configuring backup servers, see the "Configuring a Backup Server List" section on page 3-49.

AnyConnect Profile Editor, Certificate Matching

Enable the definition of various attributes that can be used to refine automatic client certificate selection on this pane.

Key Usage—You can use the following Certificate Key attributes for choosing acceptable client certificates:

- Decipher_Only—Deciphering data, and that no other bit (except Key_Agreement) is set.
- Encipher_Only—Enciphering data, and any other bit (except Key_Agreement) is not set.
- CRL_Sign—Verifying the CA signature on a CRL.
- Key_Cert_Sign—Verifying the CA signature on a certificate.
- Key_Agreement—Key agreement.
- Data_Encipherment—Encrypting data other than Key_Encipherment.
- Key_Encipherment—Encrypting keys.
- Non_Repudiation—Verifying digital signatures protecting against falsely denying some action, other than Key_Cert_sign or CRL_Sign.
- Digital_Signature—Verifying digital signatures other than Non_Repudiation, Key_Cert_Sign or CRL_Sign.

Extended Key Usage—You can use these Extended Key Usage settings. The OIDs are included in parenthesis ():

- 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)

Custom Extended Match Key (Max 10)—Specifies custom extended match keys, if any (maximum 10). A certificate must match all of the specified key(s) you enter. Enter the key in the OID format. For example: 1.3.6.1.5.5.7.3.11

Distinguished Name (Max 10):—Specifies distinguished names (DNs) for exact match criteria in choosing acceptable client certificates.

Name—The distinguished name (DN) to use for matching:

- CN—Subject Common Name
- C—Subject Country
- DC—Domain Component
- DNQ—Subject Dn Qualifier
- EA—Subject Email Address

- GENQ—Subject Gen Qualifier
- GN—Subject Given Name
- I—Subject Initials
- L—Subject City
- N—Subject Unstruct Name
- O—Subject Company
- OU—Subject Department
- SN—Subject Sur Name
- SP—Subject State
- ST—Subject State
- T—Subject Title
- ISSUER-CN—Issuer Common Name
- ISSUER-DC—Issuer Component
- ISSUER-SN—Issuer Sur Name
- ISSUER-GN—Issuer Given Name
- ISSUER-N—Issuer Unstruct Name
- ISSUER-I—Issuer Initials
- ISSUER-GENQ—Issuer Gen Qualifier
- ISSUER-DNQ—Issuer Dn Qualifier
- ISSUER-C—Issuer Country
- ISSUER-L—Issuer City
- ISSUER-SP—Issuer State
- ISSUER-ST—Issuer State
- ISSUER-O—Issuer Company
- ISSUER-OU—Issuer Department
- ISSUER-T—Issuer Title
- ISSUER-EA—Issuer Email Address

Pattern—The string to use in the match. The pattern to be matched should include only the portion of the string you want to match. There is no need to include pattern match or regular expression syntax. If entered, this syntax will be considered part of the string to search for.

For example, if a sample string was abc.cisco.com and the intent is to match cisco.com, the pattern entered should be cisco.com.

Wildcard—Enable to include wildcard pattern matching. With wildcard enabled, the pattern can be anywhere in the string.

Operator—The operator used in performing the match.

- Equal—equivalent to ==
- Not Equal—equivalent to !=

Match Case—Enable to make the pattern matching applied to the pattern case sensitive.

- Selected—Perform case sensitive match with pattern.

- Not Selected—Perform case in-sensitive match with pattern.

For more detailed configuration information about the certificate matching, see the "Configuring Certificate Matching" section on page 3-42.

AnyConnect Profile Editor, Certificate Enrollment

Configure certificate enrollment on this pane.

Certificate Enrollment—Enables AnyConnect to use the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate used for client authentication. The client sends a certificate request, and the certificate authority (CA) automatically accepts or denies the request.

Note The SCEP protocol also allows the client to request a certificate and then poll the CA until it receives a response. However, this polling method is not supported in this release.

Certificate Expiration Threshold—The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported when SCEP is enabled). The default is zero (no warning displayed). The range of values is zero to 180 days.

Automatic SCEP Host—Specifies the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname *asa.cisco.com* and the connection profile name *scep_eng*.

CA URL—Identifies the SCEP CA server. Enter an FQDN or IP Address of the CA server. For example, *http://ca01.cisco.com*.

- **Prompt For Challenge PW**—Enable to let the user make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.
- **Thumbprint**—The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.

Note Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a "fingerprint" or "thumbprint" attribute field in a certificate it issued.

Certificate Contents—defines how the client requests the contents of the certificate:

- Name (CN)—Common Name in the certificate.
- Department (OU)—Department name specified in certificate.
- Company (O)—Company name specified in certificate.
- State (ST)—State identifier named in certificate.
- State (SP)—Another state identifier.
- Country (C)—Country identifier named in certificate.
- Email (EA)—Email address. In the following example, Email (EA) is %USER%@cisco.com. %USER% corresponds to the user's ASA username login credential.
- Domain (DC)—Domain component. In the following example, Domain (DC) is set to cisco.com.
- SurName (SN)—The family name or last name.

- GivenName (GN)—Generally, the first name.
- UnstructName (N)—Undefined name
- Initials (I)—The initials of the user.
- Qualifier (GEN)—The generation qualifier of the user. For example, “Jr.” or “III.”
- Qualifier (DN)—a qualifier for the entire DN.
- City (L)—The city identifier.
- Title (T)—The person's title. For example, Ms., Mrs., Mr.
- CA Domain—Used for the SCEP enrollment and is generally the CA domain.
- Key size—The size of the RSA keys generated for the certificate to be enrolled.

Display Get Cert Button—If enabled, the AnyConnect GUI displays the Get Certificate button. By default, users see an Enroll button and a message that AnyConnect is contacting the certificate authority to attempt certificate enrollment. Displaying Get Certificate may give users a clearer understanding of what they are doing when interacting with the AnyConnect interface.

The button is visible to users if the certificate is set to expire within the period defined by the Certificate Expiration Threshold, after the certificate has expired, or no certificate is present.

Note Enable **Display Get Cert Button** if you permit users to manually request provisioning or renewal of authentication certificates. Typically, these users can reach the certificate authority without first needing to create a VPN tunnel. Otherwise, do not enable this feature.

For more detailed configuration information about Certificate Enrollment, see the “Configuring Certificate Enrollment using SCEP” section on page 3-34.

AnyConnect Profile Editor, Mobile Policy

Set parameters for AnyConnect running on Windows Mobile in this pane:

Device Lock Required—A Windows Mobile device must be configured with a password or PIN before establishing a VPN connection. This only applies to Windows Mobile devices that use the Microsoft Local Authentication Plug-ins (LAPs).

Maximum Timeout Minutes—The maximum number of minutes that must be configured before the device lock takes effect.

Minimum Password Length—Specifies the minimum number of characters for the device lock password or PIN.

Password Complexity—Specifies the complexity for the required device lock password:

- alpha—Requires an alphanumeric password.
- pin—Requires a numeric PIN.
- strong—Requires a strong alphanumeric password which must contain at least 7 characters, including a minimum of 3 from the set of uppercase, lowercase, numerals, and punctuation characters.

For more detailed configuration information about Mobile Policy, see the “Configuring a Windows Mobile Policy” section on page 3-49.

AnyConnect Profile Editor, Server List

You can configure a list of servers that appear in the client GUI. Users can select servers in the list to establish a VPN connection.

Server List Table Columns:

- **Hostname**—The alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- **Host Address**—IP address or FQDN of the server.
- **User Group**—Used in conjunction with Host Address to form a group-based URL.
- **Automatic SCEP Host**—The Simple Certificate Enrollment Protocol specified for provisioning and renewing a certificate used for client authentication.
- **CA URL**—The URL this server uses to connect to certificate authority (CA).

Add/Edit—Launches the Server List Entry dialog where you can specify the server parameters.

Delete—Removes the server from the server list.

Details—Displays more details about backup servers or CA URL s for the server.

AnyConnect Profile Editor, Add/Edit Server List

Add a server and its backup server and/or load balancing backup device in this pane.

Hostname—Enter an alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).

Host Address—Specify an IP address or an FQDN for the server.

Note

- If you specify an IP address or FQDN in the Host Address Field then the entry in the Host Name field becomes a label for the server in the connection drop-down list in the AnyConnect Client tray fly-out.
- If you only specify an FQDN in the Hostname field, and no IP address in the Host Address field, then the FQDN in the Hostname field will be resolved by a DNS server.

User Group—Specify a user group. The user group is used in conjunction with Host Address to form a group-based URL.

Note If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile.

Backup Server List—You can configure a list of backup servers the client uses in case the user-selected server fails. If the server fails, the client attempts to connect to the server at the top of the list first, and moves down the list, if necessary.

- **Host Address**—Specifies an IP address or an FQDN to include in the backup server list. If the client cannot connect to the host, it attempts to connect to the backup server.
- **Add**—Adds the host address to the backup server list.

- **Move Up**—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.
- **Move Down**—Moves the selected backup server down in the list.
- **Delete**—Removes the backup server from the server list.

Load Balancing Server List—If the host for this server list entry is a load balancing cluster of security appliances, and the always-on feature is enabled, specify the backup devices of the cluster in this list. If you do not, the always-on feature blocks access to backup devices in the load balancing cluster.

- **Host Address**—Specifies an IP address or an FQDN of a backup device in a load-balancing cluster.
- **Add**—Adds the address to the load balancing backup server list.
- **Delete**—Removes the load balancing backup server from the list.

Primary Protocol—Specifies the protocol for connecting to this ASA, either SSL or IPsec with IKEv2. The default is SSL.

Standard Authentication Only—By default, the AnyConnect client uses the proprietary AnyConnect EAP authentication method. Check to configure the client to use a standards-based method. However, doing this limits the dynamic download features of the client and disables some features.

Note Changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.

IKE Identity—If you choose a standards-based EAP authentication method, you can enter a group or domain as the client identity in this field. The client sends the string as the ID_GROUP type IDi payload. By default, the string is *$AnyConnectClient$*.

CA URL—Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, *http://ca01.cisco.com*.

- **Prompt For Challenge PW**—Enable to let the user make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.
- **Thumbprint**—The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.

Note Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.

For more detailed configuration information about creating a server list, see the “Configuring a Server List” section on page 3-46.

CHAPTER 4

Configuring Network Access Manager (NAM)

This chapter provides an overview of the Network Access Manager configuration and provides instructions for adding and configuring user policies and network profiles. This chapter contains these sections:

Introduction

The Network Access Manager (NAM) is client software that provides a secure Layer 2 network in accordance with policies set forth by the enterprise network administrators. NAM detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks. NAM manages user and device identity and the network access protocols required for secure access. It works intelligently to prevent end users from making connections that are in violation of administrator-defined policies.

The NAM component of the AnyConnect Secure Mobility Client supports these main features:

- Wired (802.3) and wireless (802.11) network adapters
- Pre-login authentication using Windows machine credentials
- Single sign-on user authentication using Windows logon credentials

- Simplified and easy-to-use 802.1X configuration
- EAP methods:
  - EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS, and LEAP (EAP-MD5, EAP-GTC, and EAP-MSCHAPv2 for 802.3 wired only)
- Inner EAP methods:
  - PEAP—EAP-GTC, EAP-MSCHAPv2, and EAP-TLS
  - EAP-TTLS—EAP-MD5 and EAP-MSCHAPv2 and legacy methods (PAP, CHAP, MSCHAP, and MSCHAPv2)
  - EAP-FAST—GTC, EAP-MSCHAPv2, and EAP-TLS
- Encryption modes:
  - Static WEP (Open or Shared), dynamic WEP, TKIP, and AES
- Key establishment protocols:
  - WPA, WPA2/802.11i, and CCKM (selectively, depending on the 802.11 NIC card)

Note The only adapter supported for CCKM is the Cisco CB21AG on Windows XP

- Smartcard provided credentials

System Requirements for NAM

The NAM module requires the following:

- ASDM version 6.4(0)104 or later.

Note The standalone NAM editor is an unsupported alternative for configuring a NAM profile. For security reasons, AnyConnect does not accept NAM profiles edited with a standard editor.

- The following operating systems support the NAM:
  - Windows 7 x86 (32-bit) and x64 (64-bit)
  - Windows Vista SP2 x86 (32-bit) and x64 (64-bit)
  - Windows XP x86 SP3 (32-bit)
  - Windows Server 2003 SP2 x86 (32-bit)

Pre-deploying NAM

When you pre-deploy NAM, you install it on the endpoint before the AnyConnect client makes its initial connection to the ASA. You need to install the AnyConnect Secure Mobility Client on the endpoint before you install the NAM modules. See the "Deploying the AnyConnect Secure Mobility Client" section on page 2-1for instructions on installing the AnyConnect Secure Mobility Client and the posture module using web-deployment and pre-deployment methods.

Stopping and Starting NAM

Users with local administrator privileges can start and stop NAM. Users without local administrator privileges cannot start and stop NAM without using the service password defined in the Authentication panel of the NAM profile editor.

NAM Profile Editor

The NAM profile editor is designed for you to create NAM configuration profiles and create pre-configured client profiles. This configuration is deployed on the endpoints so that NAM can enforce administratively defined end user and authentication policies and make the pre-configured network profiles available to end users. To use the profile editor, create settings for a profile, save it, and then place the configurations onto the client. AnyConnect includes the profile editor inside ASDM, but a standalone version is also available. Refer to Chapter 2, "Deploying the AnyConnect Secure Mobility Client" for profile editor requirements and deployment instructions.

Adding a New Profile

Follow these steps to add a new profile for NAM.

Step 1 Click **Configuration** in the ASDM toolbar.

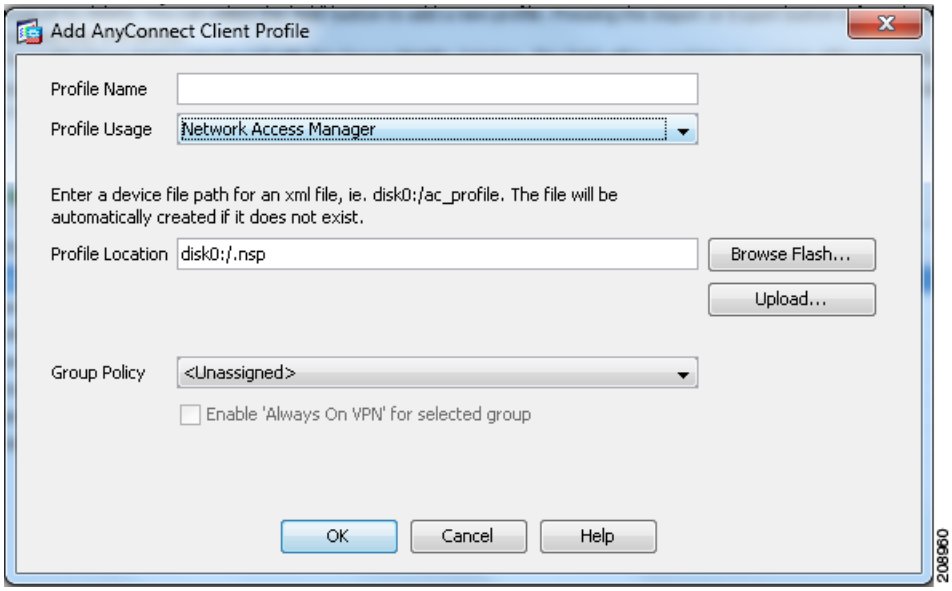
Step 2 Click **Remote Access VPN** in the leftmost navigation area.

Step 3 Click **Network Client Access**.

Step 4 Click **AnyConnect Client Profile**. The profile window appears.

Step 5 Click **Add**. The Add AnyConnect Client Profile window appears (see Figure 4-1).

Figure 4-1 Add AnyConnect Client Profile Window



Step 6 Enter a profile name.

Step 7 From the Profile Usage drop-down list, choose **Network Access Manager** and click **OK**.

Step 8 (Optional) In the Profile Location parameter, establish a device file path for the XML file.

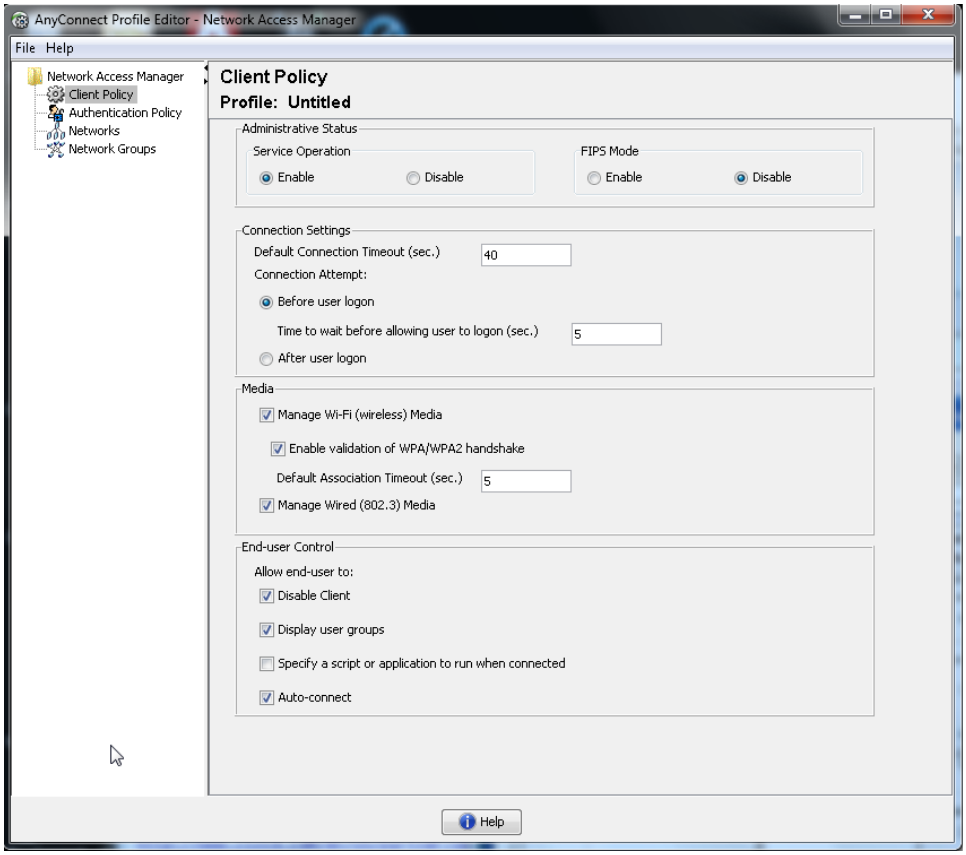
Step 9 (Optional) Choose an AnyConnect group policy from the drop-down list.

Step 10 Click **OK**.

Configuring a Client Policy

The Client Policy window enables you to configure the client policy options (see Figure 4-2).

Figure 4-2 Client Policy Window



Four sections are included:

- Administrative Status
  - You can switch the NAM functionality on or off with the Service Operation parameter. If you choose to disable the service, NAM cannot manage network connections on the client.

  - You can switch FIPS mode on or off. Federal Information Processing Standard (FIPS 104-2) is a U.S. government standard that specifies security requirements for cryptography modules. If you enable FIPS, NAM performs cryptographic operations in a way that meets the government requirements. The normal FIPS mode of operation is disabled. Refer to the "Enabling FIPS and Additional Security" section on page 8-1 for additional information.

- Connection Settings—Allows you to define whether a network with a user connection component is attempted before or after the user logs on.
  - Default Connection Timeout—Specifies the number of seconds to use as the connection timeout parameter for user-created networks. The default value is 40 seconds.
  - Before User Logon—Specifies that you want NAM to attempt the user connection immediately, before Windows user logon procedures take place. Windows logon procedures include user account (kerberos) authentication, loading of user GPOs, and GPO-based logon script execution.
  - Time to Wait Before Allowing User to Logon—Specify the maximum (worst case) number of seconds to wait for NAM to make a complete network connection. If a network connection cannot be established within this time, the Windows logon process continues with user log on. The default is 5 seconds.

    Note If NAM is configured to manage wireless connections, we suggest you use 30 seconds or more because it takes additional time to establish a wireless connection. You must also account for the time required to obtain an IP address via DHCP. If two or more network profiles are configured, you may want to increase the value to cover two or more connection attempts.

  - After User Logon—Specifies that you want NAM to attempt the user connection after a Windows user logon procedure.
- Media—Enables you to choose which types of media are controlled by the NAM client.
  - Manage Wi-Fi (wireless) Media— Enables NAM's management of WiFi media and optionally allows the enabling of WPA/WPA2 handshake validation.

    The IEEE 802.11i Wireless Networking standard specifies the supplicant must validate that the access point's RSN IE sent in the EAPOL Key data during key derivation matches the access point's RSN IE found in the beacon/probe response frame. If you enable the validation of WPA/WPA2 handshake, you must specify the default association timeout. If you uncheck the enable validation of WPA/WPA2 handshake setting, this validation step is skipped.

    Note However, some adapters do not consistently provide the access point's RSN IE, so the authentication attempt fails, and the client will not connect.

  - Manage Wired (802.3) Media—Enables NAM's management of wired media.
- End-user Control—Allows you to determine the following control for users:
  - Disable Client—Allows users to disable and enable NAM's management of wired and wireless media using the AnyConnect UI.
  - Display User Groups—Makes user-created groups (created from CSSC 5.x) visible and capable of a connection, even though they do not correspond to administrator-defined groups.
  - Specify a Script or Application To Run When Connected—Allows users to specify a script or application to run when the network connects.

Note The scripting settings are specific to one user-configured network and allow the user to specify a local file (.exe,.bat, or .cmd) to run when that network gets to a connected state. To avoid conflicts, the scripting feature only permits users to configure a script or application for user-defined networks and not for administrator-defined networks. The feature does not allow users to alter administrator networks regarding the running of scripts; therefore, the interface for administrator networks is not available to the user. Also, if you do not allow users to configure a running script, the feature is not seen in the NAM GUI.

– Auto-connect—If selected, NAM automatically connects to a network without a user needing to choose it. The default is automatic connection.

Configuring an Authentication Policy

This window allows you to define global association and authentication network policies. These policies apply to all networks that the user can create. The policies allows you to limit the type of network a user can create with the GUI. If you do not check any of the association or authentication modes, the user cannot create any networks. If you choose a subset of the modes, the user can create networks for these types and not the unchecked ones. Choose each desired association or authentication mode or choose **Select All**.

When you choose Authentication Policy from the Network Access Manager menu, the window shown in Figure 4-3 appears.

Depending upon the customer requirements, different authentication mechanisms are used in a secure mobility environment, but all of the mechanisms use 802.1X, EAP, and RADIUS as their supporting protocols. These protocols allow the control of access based upon the successful authentication of the wireless LAN client and allow the wireless LAN network to be authenticated by the user.

This system also provides the other elements of AAA, authorization and accounting, through policies communicated through RADIUS and RADIUS accounting.

The mechanism for choosing the authentication protocol is integration with the current client authentication database. A secure wireless LAN deployment should not require the creation of a new authentication system for users.

EAP

EAP is an IEFT RFC that addresses the requirements for an authentication protocol to be decoupled from the transport protocol carrying it. This decoupling allows the transport protocols (such as 802.1X, UDP, or RADIUS) to carry the EAP protocol without changes to the authentication protocol.

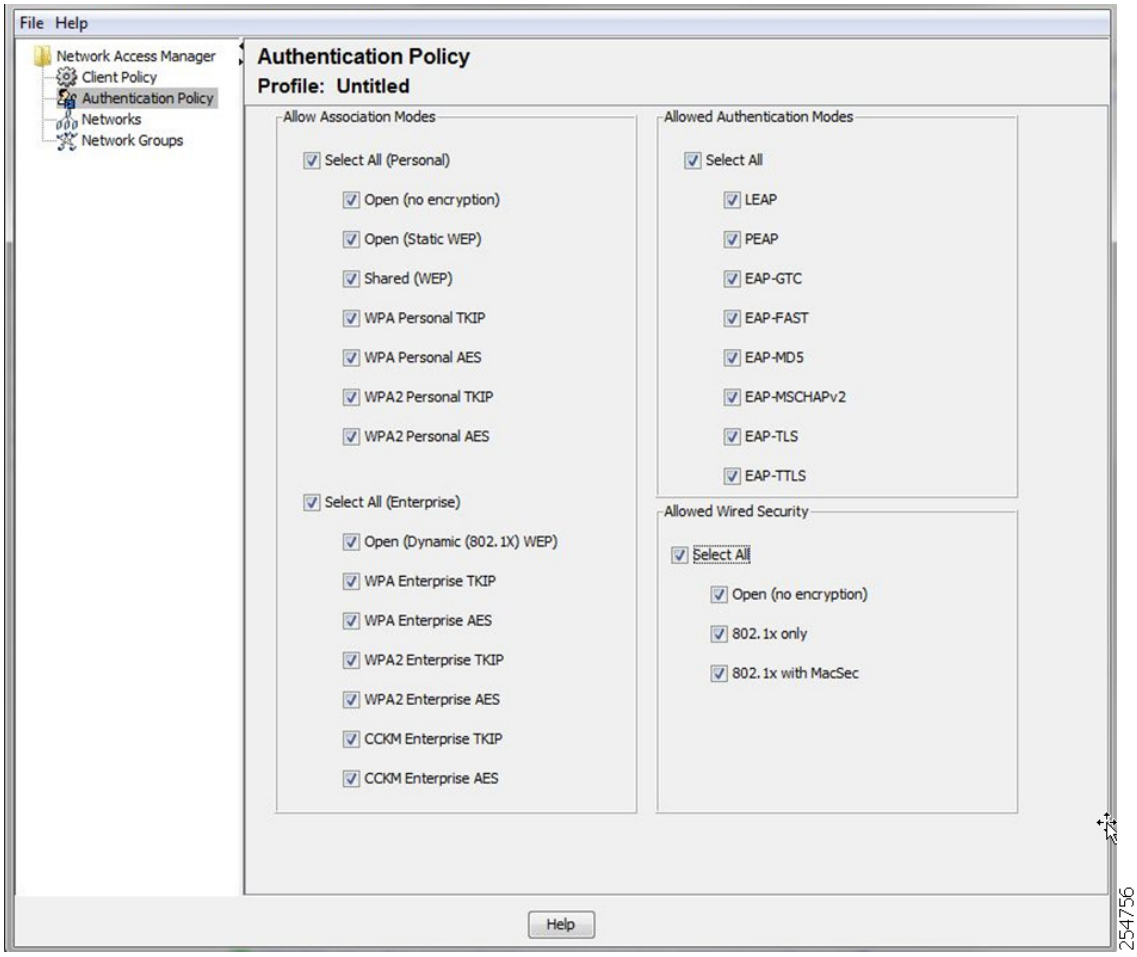
The basic EAP protocol is relatively simple and made up of four packet types:

- EAP request—The authenticator sends the request packet to the supplicant. Each request has a type field that indicates what is being requested, such as the supplicant identity and EAP type to use. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- EAP response—The supplicant sends the response packet to the authenticator and uses a sequence number to match the initiating EAP-request. The type of the EAP response generally matches the EAP request, unless the response is a NAK.

- EAP success—The authenticator sends the success packet upon successful authentication to the supplicant.
- EAP failure—The authenticator sends the failure packet upon successful authentication to the supplicant.

When EAP is in use in an 802.11X system, the access point operates in an EAP pass-through mode. In this mode, the access point checks the code, identifier, and length fields and then forwards the EAP packets received from the supplicant to the AAA server. Packets received from the AAA server at the authenticator are forwarded to the supplicant.

Figure 4-3 Authentication Policy Window



Refer to the following for a description of the options on this page:

- for personal or enterprise association modes—Defining Networks Security Level
- for allowed authentication modes—Defining the Networks Machine or User Authentication
- for allowed wired security—Defining the Networks Connection Type

Configuring Networks

The Networks window allows you to configure networks that are pre-defined for your enterprise user. You can either configure networks that are available to all groups or create groups with specific networks.

A group, fundamentally, is a collection of configured connections (networks). Every configured connection must belong to a group or a member of all groups.

Note For backward compatibility, the administrator-created networks deployed with the Cisco Secure Services Client are treated as hidden networks, which do not broadcast SSIDs. However, user networks are treated as networks which broadcast their SSIDs.

Only administrators can create a new group. If no groups are defined in the configuration, the profile editor creates an auto-generated group. The auto-generated group contains networks that are not assigned to any administrator-defined group. The client attempts to make a network connection using the connections defined in the active group. Depending on the setting of the *Create networks* option in the Network Groups window, end users can add user networks to the active group or delete user networks from the active group.

Networks that are defined are available to all groups at the top of the list. Because you control what networks are in the globalNetworks, you can specify the enterprise networks that an end user can connect to, even in the presence of user-defined networks. An end user cannot remove administrator-configured networks.

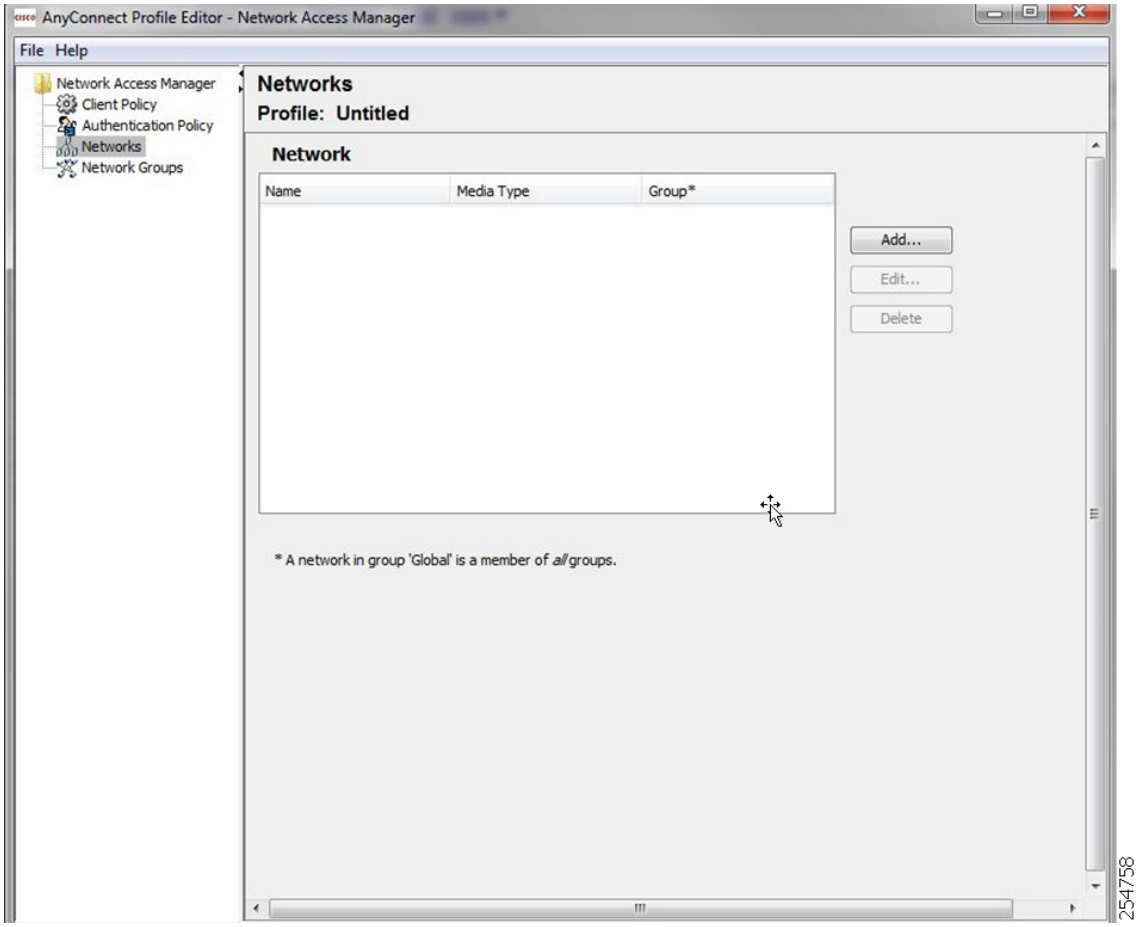
Note End users may add networks to groups, except for networks in the globalNetworks section, because these networks exist in all groups, and you can only create them using the profile editor.

It is important to note that a typical end user of an enterprise network does not need knowledge of groups in order to use this client. The active group is the first group in the configuration, but if only one is available, the client is unaware and does not display the active group. However, if more than one group exists, the UI displays a combo box indicating that the active group is selected. Users can then choose from the active group, and the setting persists across reboots. Depending on the setting of the *Create networks* option in the Network Groups window, end users can add or delete their own networks without using groups.

Note A group selection is maintained across reboots and network repairs (done while right clicking on the tray icon and choosing **Network Repair**). When NAM is repaired or restarted, NAM starts using the previously active group.

When you choose **Networks** from the Network Access Manager menu, the window shown in Figure 4-4 appears.

Figure 4-4 Networks Window



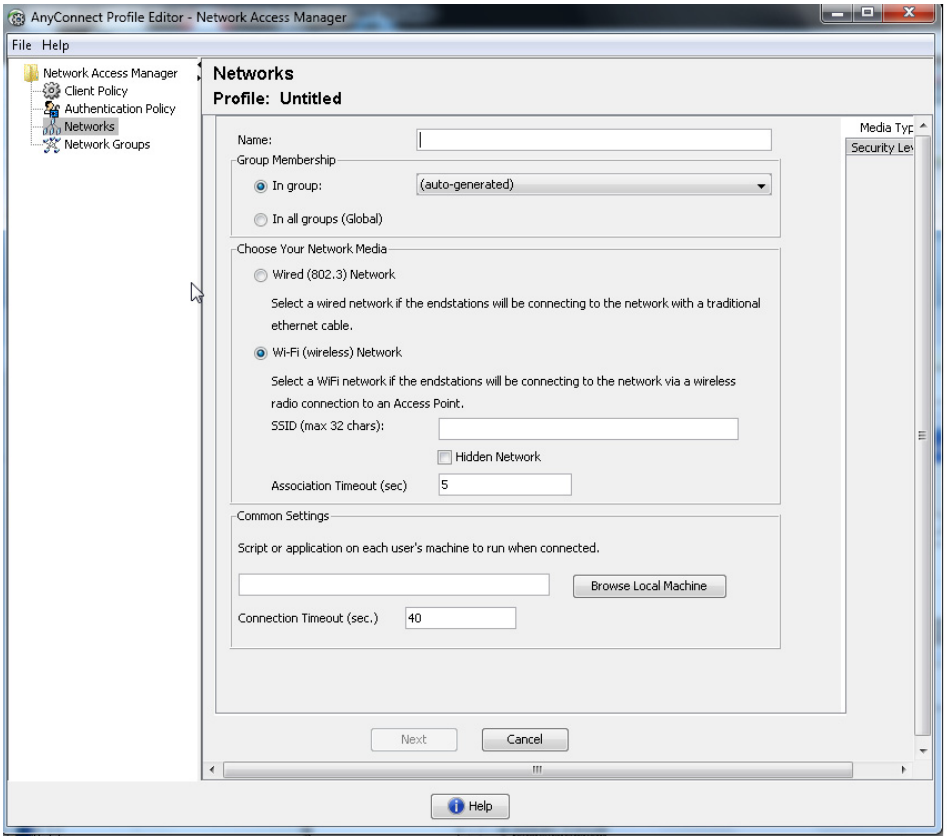
Choose from one of the following actions:

- Click **Add** to create a new network. If you choose to create a new network, follow the steps in the Defining Networks Media Types section below.
- Choose a network you want to change and click **Edit**.
- Choose a network you want to remove and click **Delete**.

Defining Networks Media Types

This window panel enables you to create or edit a wired or a wireless network. The settings vary somewhat depending on whether you choose wired or wireless. Figure 4-5 shows the window that appears if you choose a Wi-Fi network, but this section covers both wired and Wi-Fi options.

Figure 4-5 Media Type Panel



Step 1 In the Name field, enter the name that is displayed for this network.

Step 2 (Wi-Fi Only) At the SSID parameter, enter the SSID of your wireless network.

Step 3 (Wi-Fi only) Choose **Hidden Network** if the network is not broadcasting its SSID.

Note NAM's selection algorithm is optimized to make more use of the network scan list. For networks that broadcast their SSIDs, NAM only attempts connection with these networks when they show up in the network scan list.

Step 4 (Wi-Fi Only) At the Association Timeout parameter, enter the length of time that NAM waits for association with a particular wireless network before it re-evaluates the available networks. The default association timeout is 5 seconds.

Step 5 In the Common Settings section, you can enter the path and filename of the file that you want to run or you can browse to the location and select the file to run.

The following applies to scripts and applications:

- Files with .exe, .bat, or .cmd extensions are accepted.
- Users may not alter the script or application defined in an administrator-created network.

- You may only specify the path and script or application filename using the profile editor. If the script or application does not exist on a user's machine, an error message appears. The user is informed that the script or application does not exist on their machine and that they need to contact their system administrator.
- You must specify the full path of the application that you want to run, unless the application exists in the user's path. If the application exists in the user's path, you can specify only the application or script name.

Step 6 In the Connection Timeout parameter, enter the number of seconds that NAM waits for a network connection to be established before it tries to connect to another network (when the connection mode is automatic) or uses another adapter.

Note Some smartcard authentication systems require almost 60 seconds to complete an authentication. When using a smartcard, you may need to increase the Connection Timeout value.

Step 7 Click **Next**.

Defining Networks Security Level

You can define the type of security level for your wired or wireless network. In the Security Level area, choose the desired network type:

- Defining the Networks Connection Type—Recommended for secure enterprise wired network.
- Using an Open Network—Not recommended but can be used for guest access on a wired network.
- An open network uses no authentication or encryption. Follow these steps if you want to create an open (non-secure) network.—Recommended for wireless networks such as small offices or home offices.
- Using Authenticating WiFi Networks—Recommended for secure enterprise wireless networks.

Using Authenticating Wired Networks

Follow these steps if you want to use 802.1X authentication as your security level.

Step 1 Choose **Authenticating Network**.

Note Make sure you chose Wired (802.3) Network on the Network Media Type panel (shown in Figure 4-5).

Step 2 Adjust the 802.1X settings according to your network configuration:

- authPeriod(sec.)—When authentication begins, this time determines how long the supplicant waits in between authentication messages before it times out and requires the authenticator to initiate authentication again.

- heldPeriod(sec)—When authentication fails, this time defines how long the supplicant waits before another authentication attempt can be made.
- startPeriod(sec)—After sending an EAPoL-Start to initiate an authentication attempt with the authenticator, this timer defines how long the supplicant will wait for the authenticator to respond before initiating authentication again (such as sending the next EAPoL-Start).
- maxStart—The number of times the supplicant will initiate authentication with the authenticator by sending an EAPoL-Start before the supplicant assumes there is no authenticator present. When this happens, the supplicant allows data traffic.

Tip You can configure a single authenticating wired connection to work with both open and authenticating networks by carefully setting the startPeriod and maxStart such that the total time spent trying to initiate authentication is less than the network connection timer (startPeriod x maxStart < Network Connection Timer).

Note: In this scenario, you should increase the network connection timer by (startPeriod x maxStart) seconds to give the client enough time to acquire a DHCP address and finish the network connection.

Conversely, administrators who want to allow data traffic if and only after authentication succeeds should make sure that the startPeriod and maxStart is such that the total time spent trying to initiate authentication is greater than the network connection timer (start Period x maxStart > Network Connection Timer).

Step 3 Choose from the following level of security:

- Key Management—Use the drop-down list to determine which Key Management Protocol you want to use with your wired network.
  - None—No key management protocols are used, and no wired encryption is performed.
  - MKA—The supplicant attempts to negotiate a MACsec key agreement and encryption keys. MACsec is MAC Layer Security, which provides MAC layer encryption over wired networks. The MACsec protocol represents a means to secure MAC level frames with encryption and relies on the MACsec Key Agreement (MKA) Entity to negotiate and distribute the encryption keys.

    Note Refer to IEEE-802.1X-Rev for a detailed definition of MACsec Key Agreement and IEEE 802.1AE-2006 for a detailed definition of the MACsec encryption protocol.

- Encryption
  - None—Data traffic is integrity checked but not encrypted.
  - AES-GCM-128—Data traffic is encrypted using AES-GCM-128.

Step 4 Choose **Port Authentication Exception Policy**. By enabling the Port Authentication Exception Policy, you have the ability to tailor the 802.1X supplicant's behavior during the authentication process. If port exceptions are not enabled, the supplicant continues its existing behavior and only opens the port upon successfully completing the full configuration (or as described earlier in this section, after the maxStarts number of authentications are initiated without a response from the authenticator). Choose from one of the following options:

- Allow data traffic before authentication—When selected, this exception allows data traffic prior to an authentication attempt.
- Allow data traffic after authentication even if

- EAP Fails—When selected, the supplicant attempts authentication. But if authentication fails, the supplicant allows data traffic despite authentication failure.
- EAP succeeds but key management fails—When selected, the supplicant attempts to negotiate keys with the key server but allows data traffic if the key negotiation fails for any reason. This setting is only valid when key management is configured. If key management is set to none, the check box is grayed out.

Note MACsec requires ACS version 5.1 or later and a MACsec capable switch. Refer to the *Catalyst 3750-X and 3560-X Switch Software Configuration Guide* for ACS or switch configuration.

Using an Open Network

An open network uses no authentication or encryption. Follow these steps if you want to create an open (non-secure) network.

Step 1 Choose **Open Network** from the Security Level panel. This choice provides the least secure network and is recommended for guest access wireless networks.

Step 2 Click **Next**.

Step 3 Determine a connection type. Refer to the "Defining the Networks Connection Type" section on page 4-16.

Using a Shared Key

Wi-Fi networks may use a shared key to derive an encryption key for use when encrypting data between end stations and network access points. When the shared key is used in conjunction with WPA or WPA2 Personal, this setting provides a medium level security class that is suitable for small or home offices.

Note This setting is not recommended for enterprise wireless networks.

Follow these steps if you want Shared Key Network as your security level.

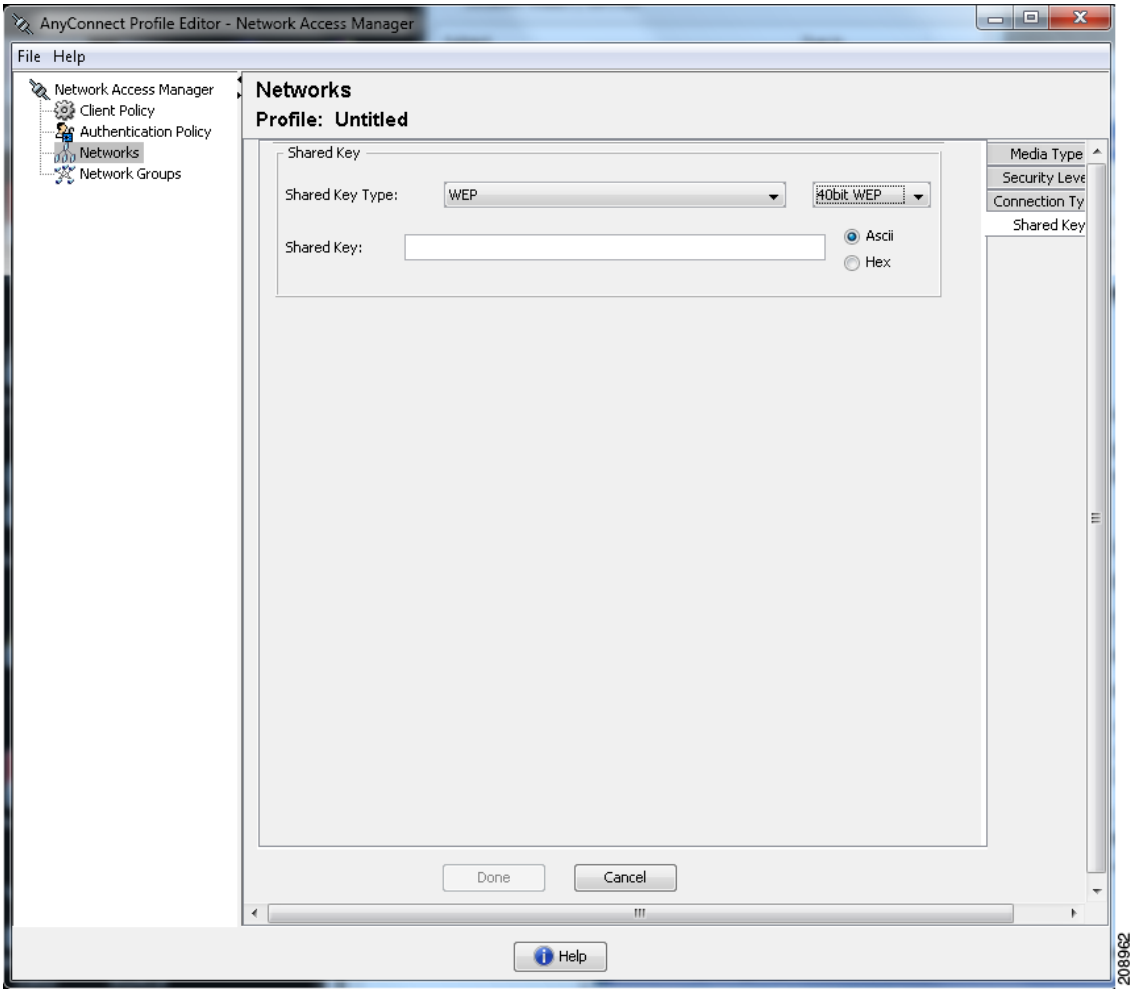
Step 1 Choose **Shared Key Network**.

Step 2 Click **Next** on the Security Level window.

Step 3 Specify **User Connection** or **Machine Connection**. Refer to the "Defining the Networks Connection Type" section on page 4-16 for more information.

Step 4 Click **Next**. The Shared Key panel appears (see Figure 4-6).

Figure 4-6 Shared Key Panel



Step 5 Shared Key Type—Specify the shared key association mode which determines the shared key type. The choices are as follows:

- WEP—Legacy 802.11 open-system association with static WEP encryption.
- Shared—Legacy 802.11 shared-key association.
- WPA/WPA2-Personal—A Wi-Fi security protocol that derives encryption keys from a passphrase pre-shared key (PSK).

Step 6 If you choose Legacy 802.11 WEP or Shared Key, choose 40 bit, 64 bit, 104 bit, or 128 bit. A 40- or 64-bit WEP key must be 5 ASCII characters or 10 hex digits. A 104- or 128-bit WEP key must be 13 ASCII characters or 26 hex digits.

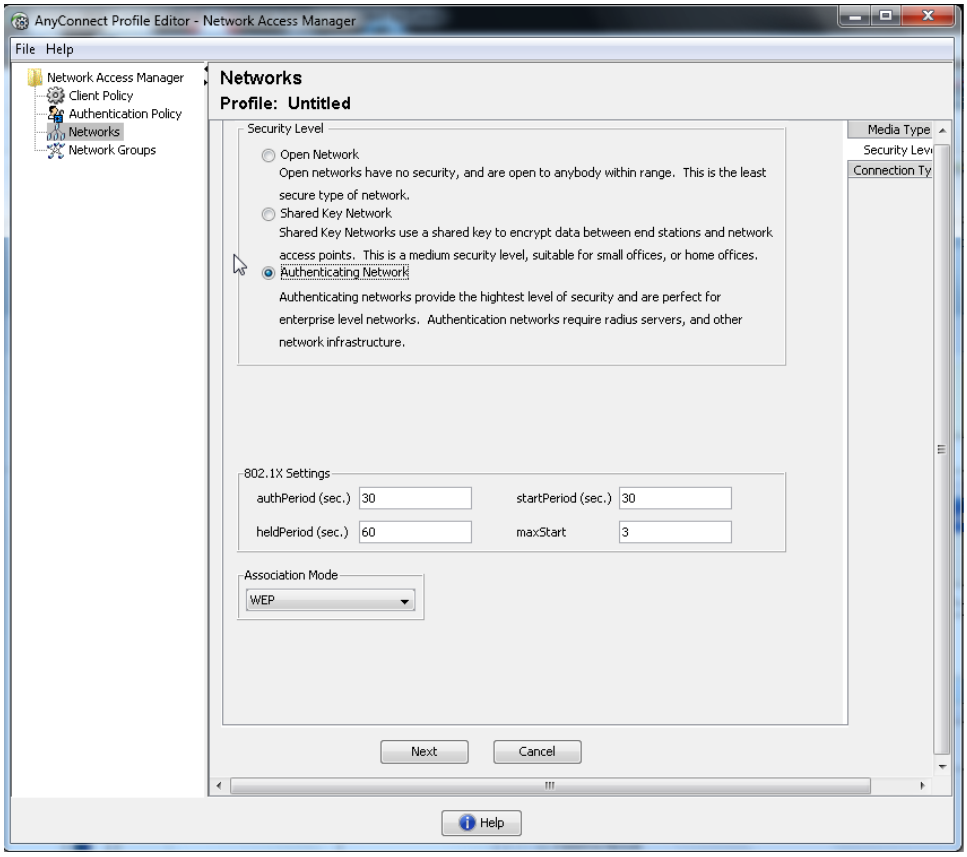
Step 7 If you choose WPA or WPA2 Personal, choose the type of encryption to use (TKIP/AES) and then enter a shared key. The key must be entered as 8 to 63 ASCII characters or exactly 64 hexadecimal digits. Choose **ASCII** if your shared key consists of ASCII characters. Choose **Hexadecimal** if your shared key includes 64 hexadecimal digits.

Using Authenticating WiFi Networks

If you choose Authenticating Network, you can create secure wireless networks based on 802.1X and EAP.

Follow these steps if you want Authenticating Networks as your security level (see Figure 4-7).

Figure 4-7 Authenticating Network Security Level



Step 1 Choose **Authenticating Networks**.

Step 2 Although the default values should work for most networks, you have the option to configure the 802.1X settings to suit your environment, if necessary:

- authPeriod(sec.)—When authentication begins, this time determines how long the supplicant waits in between authentication messages before it times out and requires the authenticator to initiate authentication again. The default is 30 seconds.
- heldPeriod(sec)—When authentication fails, this time defines how long the supplicant waits before another authentication attempt can be made. The default is 60 seconds.
- startPeriod(sec)—After sending an EAPoL-Start to initiate an authentication attempt with the authenticator, this timer defines how long the supplicant will wait for the authenticator to respond before initiating authentication again (such as sending the next EAPoL-Start). The default is 30 seconds.

- maxStart—The number of consecutive times the supplicant will initiate authentication with the authenticator by sending an EAPoL-Start (without receiving a response from the authenticator) before the supplicant assumes there is no authenticator present. When this happens, the supplicant allows data traffic. The default is 3 times.

Note For this section, authentication begins when the authenticator sends the client supplicant an EAP identity request.

Step 3 For Association Mode, specify the type of wireless security to use.

Defining the Networks Connection Type

With the Connection Type panel, you can choose the type of network connection and specify when connection attempts using this network are allowed (see Figure 4-8). The machine connection option defines the connection as a machine connection type. You can use machine connection at any time, but you typically use it whenever user credentials are not required for a connection. The User Connection option defines the connection as a user connection type. The user can make connections only after initiating a logon attempt with the PC. While not required, user connections usually use the logged on user's credentials to establish a connection.

A machine and user network contains a machine part and a user part; however, the machine part is only valid when a user is not logged onto the PC. The configuration is the same for the two parts, but the authentication type and credentials for machine connection can be different from the authentication type and credentials for the user connection.

- Machine Connection—Choose this option if the end station should log onto the network even when a user is logged off and user credentials are unavailable. This option is typically used for connecting to domains and to get GPOs and other updates from the network before the user has access.

Note You should consider that if you want VPN start before login (SBL) to operate as expected, a network connection must exist when the user attempts to start the VPN. If NAM is installed, you must deploy machine connection to ensure that an appropriate connection is available.

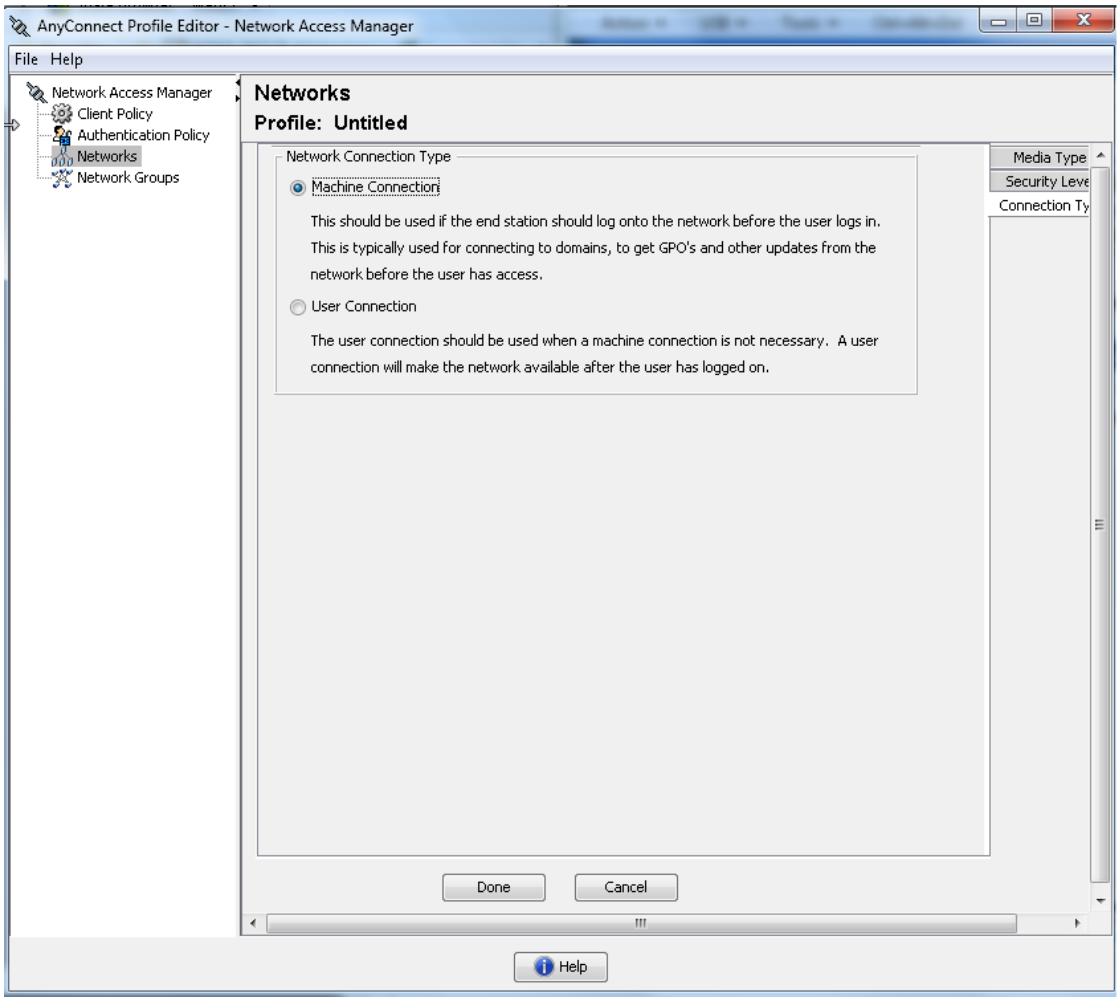
- User Connection—Choose this option when a machine connection is unnecessary. A user connection makes the network available after the user has initiated a logon attempt with the PC. When the user subsequently logs off, the network connection is terminated unless the connection is configured to extend the connection beyond user logoff.

Note The Client Policy Connection settings determine whether a user is considered as logged in by NAM (refer to the "Configuring a Client Policy" section on page 4-4). If Connection Settings are set to *Attempt connection before user logon*, NAM attempts to use the credentials the user entered to make a network connection prior to actual logon. If Connection Settings is set to *Attempt connection after user logon*, NAM waits until user has actually logged in to make a network connection.

- Machine and User Connection—Choose this option to keep the PC connected to the network at all times using the Machine Connection when a user is not logged in and using the User Connection when a user has logged in.

Note For open and shared key networks, the Machine and User Connection option is not available.

Figure 4-8 Network Connection Type Panel

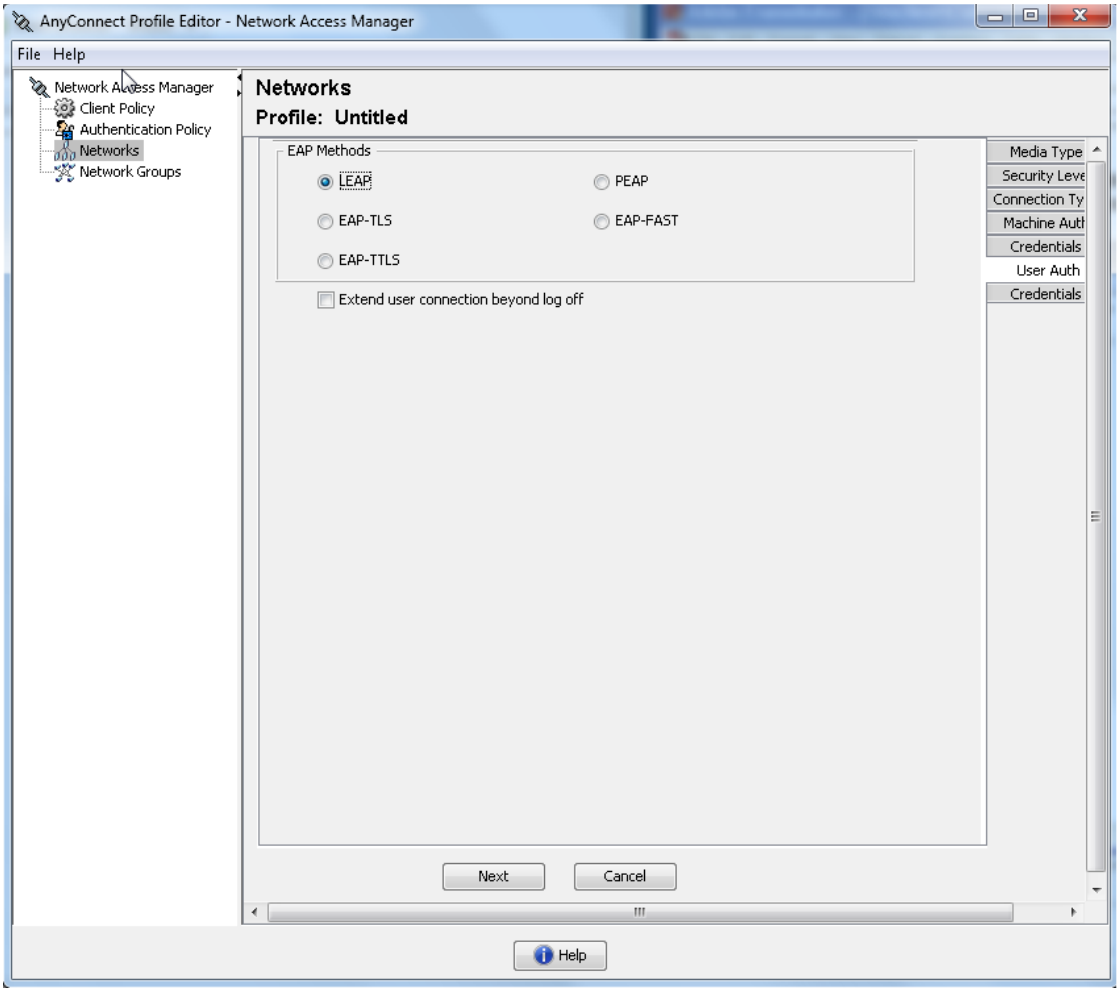


Defining the Networks Machine or User Authentication

With the Machine Authentication or User Authentication panel, you can choose the authentication method for the machine or user (see Figure 4-9). When you specify your authentication method, the center of the window adapts to the method you choose, and you are required to provide additional information for EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, or EAP-GTC.

Refer to the "Using a Windows Remote Desktop" section on page C-5 for information on accessing a network computer remotely while the connection is being managed by NAM on that network computer. It discusses network profiles using machine, user, or machine and user authentication.

Figure 4-9 Machine or User Authentication Panel



You may have additional configuration if you choose an EAP option. For further information on network security fundamentals, refer to http://www.cisco.com/en/US/docs/wireless/wlan_adapter/secure_client/5.1.1/administration/guide/C1_Network_Security.html:

- EAP-GTC—See the "Configuring EAP-GTC" section on page 4-18.EAP TLS—See the "Configuring EAP-TLS" section on page 4-19.
- EAP TTLS—See the "Configuring EAP-TTLS" section on page 4-20.
- PEAP—See the "Configuring PEAP Options" section on page 4-21.
- EAP FAST—See the "Configuring EAP-FAST Settings" section on page 4-22.

Configuring EAP-GTC

EAP-GTC is an EAP authentication method based on simple username and password authentication. Without using the challenge-response method, both username and password are passed in clear text. This method is recommended for either inside a tunneling EAP method (see tunneling EAP methods below) or with a OTP (token).

EAP-GTC does not provide mutual authentication. It only authenticates clients, so a rogue server may potentially obtain users' credentials. If mutual authentication is required, EAP-GTC is used inside tunneling EAP methods, which provide server authentication.

No keying material is provided by EAP-GTC; therefore, you cannot use this method for MACsec. If keying material for further traffic encryption is required, EAP-GTC is used inside tunneling EAP methods, which provides the keying material (and inner and outer EAP methods crytobinding, if necessary).

You have two password source options:

- Authenticate using a Password—Suitable only for well protected wired environments
- Authenticate using a Token—More secure because of the short lifetime (usually about 10 seconds) of a token code or it is a OTP

Note Neither NAM, the authenticator, nor the EAP-GTC protocol can distinguish between password and token code. These options only impact the credential's lifetime within NAM. While a password can be remembered until logout or longer, the token code cannot (because the user is prompted for token code with every authentication).

If a password is used for authentication, you can use this protocol for authentication against the database with hashed (or irreversibly encrypted) passwords since it is passed to the authenticator in clear text. We recommend this method if a possibility of a database leak exists.

Configuring EAP-TLS

EAP-Transport Layer Security (EAP-TLS) is an 802.1X EAP authentication algorithm based on the TLS protocol (RFC 2246). TLS uses mutual authentication based on X.509 digital certificates. The EAP-TLS message exchange provides mutual authentication, cipher suite negotiation, key exchange, verification between the client and the authenticating server, and keying material that can be used for traffic encryption.

The list below provides the main reasons why EAP-TLS client certificates can provide strong authentication for wireless connections:

- Authentication occurs automatically, usually with no intervention by the user.
- No dependency on a user password.
- Digital certificates provide strong authentication protection.
- Message exchange is protected with public key encryption.
- Not susceptible to dictionary attacks.
- The authentication process results in a mutually determined key for data encryption and signing.

EAP-TLS contains two options:

- Validate Server Certificate—Enables server certificate validation.
- Enable Fast Reconnect—Enables TLS session resumption which allows for much faster reauthentication by using abbreviated TLS handshake as long as TLS session data is preserved on both the client and the server.

Note The *Disable when using a Smart Card* option is not available for machine authentication.

Note Before user log on, smart card support is not available on Windows Vista and Windows 7.

Configuring EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) is a two-phase protocol that expands the EAP-TLS functionality. Phase 1 conducts a complete TLS session and derives the session keys used in Phase 2 to securely tunnel attributes between the server and the client. You can use the attributes tunneled during Phase 2 to perform additional authentications using a number of different mechanisms.

NAM does not support the cryptobinding of the inner and outer methods used during EAP-TTLS authentication. If cryptobinding is required, you must use EAP-FAST. Cryptobinding provides protection from a special class of man-in-the-middle attacks where an attacker hijacks the user's connection without knowing the credentials.

The authentication mechanisms that can be used during Phase 2 include these protocols:

- PAP (Password Authentication protocol)—Uses a two-way handshake to provide a simple method for the peer to prove its identity. An ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or failed. If mutual authentication is required, then you must configure EAP-TTLS to validate the server's certificate at Phase 1.

  Because a password is passed to the authenticator, you can use this protocol for authentication against a database with hashed (or irreversibly encrypted) passwords. We recommend this method when a possibility of a database leak exists.

  Note You can use EAP-TTLS PAP for token and OTP-based authentications.

- CHAP (Challenge Handshake Authentication Protocol)—Uses a three-way handshake to verify the identity of the peer. If mutual authentication is required, you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method, you are required to store clear text passwords in the authenticator's database.
- MS-CHAP (Microsoft CHAP)—Uses a three-way handshake to verify the identity of the peer. If mutual authentication is required, you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least NT-hash of the password in the authenticator's database.
- MS-CHAPv2—Provides mutual authentication between peers by including a peer challenge in the response packet and an authenticator response in the success packet. The client is authenticated before the server. If the server needs to be authenticated before the client (to prevent dictionary

attacks), you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least NT-hash of the password in the authenticator's database.

- EAP—Allows use of these EAP methods:
  - EAP-MD5 (EAP-Message Digest 5)—Uses a three-way handshake to verify the peer's identity (similar to CHAP). Using this challenge-response method, you are required to store the clear text password in the authenticator's database.
  - EAP-MSCHAPv2—Uses a three-way handshake to verify the identity of the peer. The client is authenticated before the server. If the server needs to be authenticated before the client (such as for the prevention of a dictionary attack), you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.
- EAP-TTLS Settings
  - Validate Server Identity—Enables server certificate validation.
  - Enable Fast Reconnect—Enables outer TLS session resumption only, regardless of whether the inner authentication is skipped or is controlled by the authenticator.

Note The *Disable when using a Smart Card* option is not available on machine authentication.Before user log on, smart card support is not available on Windows Vista and Windows 7.

- Inner Methods—Specifies the inner methods used after the TLS tunnel is created.

Configuring PEAP Options

EAP-PEAP is a tunneling TLS-based EAP method. It uses TLS for server authentication before the client authentication for the encrypting of inner authentication methods. The inner authentication occurs inside a trusted cryptographically protected tunnel and supports a variety of different inner authentication methods, including certificates, tokens, and passwords. NAM does not support the cryptobinding of the inner and outer methods used during EAP-PEAP authentication. If cryptobinding is required, you must use EAP-FAST. Cryptobinding provides protection from a special class of man-in-the-middle attacks where an attacker hijacks the user's connection without knowing the credentials.

EAP-PEAP protects the EAP methods by providing these services:

- TLS tunnel creation for the EAP packets
- Message authentication
- Message encryption
- Authentication of server to client
- Key exchange to establish encryption keys

You can use these authentication methods:

- Password
  - EAP-MSCHAPv2—Uses a three-way handshake to verify the identity of the peer. The client is authenticated before the server. If the server needs to be authenticated before the client (such as for the prevention of a dictionary attack), you must configure EAP-PEAP to validate the server's

certificate. Using the challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.

  - EAP-GTC (EAP Generic Token Card)—Defines an EAP envelope to carry the username and password. If mutual authentication is required, you must configure EAP-PEAP to validate the server's certificate. Because the password is passed to the authenticator in clear text, you can use this protocol for authentication against the database with hashed (or irreversibly encrypted) passwords. We recommend this method if a possibility of a database leak exists.

- Token
  - EAP-GTC—Defines an EAP envelope to carry a token code or OTP.
- Certificate
  - EAP-TLS—Defines an EAP envelope to carry the user certificate. In order to avoid a man-in-the-middle attack (the hijacking of a valid user's connection), we recommend that you do not mix EAP-PEAP [EAP-TLS] and EAP-TLS profiles meant for authentication against the same authenticator. You should configure the authenticator accordingly (not enabling both plain and tunneled EAP-TLS).
- PEAP settings
  - Validate Server Identity—Enables server certificate validation.
  - Enable Fast Reconnect—Enables outer TLS session resumption only. The authenticator controls whether or not the inner authentication is skipped.
- The *Disable when using a Smart Card* and the *Authenticate using a Token and EAP GTC* options are not available for machine authentication.Inner methods based on Credentials Source—Enables you to choose to authenticate using a password or a certificate.
  - Authenticate using a password for EAP-MSCHAPv2 or EAP-GTC
  - EAP-TLS, using Certificate
  - Authenticate using a Token and EAP-GTC

Note Before user log on, smart card support is not available on Windows Vista and Windows 7.

Configuring EAP-FAST Settings

EAP-FAST is an 802.1X authentication type that offers flexible, easy deployment and management. It supports a variety of user and password database types, server-initiated password expiration and change, and a digital certificate (optional).

EAP-FAST was developed for customers who want to deploy an 802.1X EAP type that does not use certificates and provides protection from dictionary attacks.

EAP-FAST encapsulates TLS messages within EAP and consists of three protocol phases:

1. A provisioning phase that uses Authenticated Diffie-Hellman Protocol (ADHP) to provision the client with a shared secret credential called a Protected Access Credential (PAC).
2. A tunnel establishment phase in which the PAC is used to establish the tunnel.
3. An authentication phase in which the authentication server authenticates the user's credentials (token, username/password, or digital certificate).

Unlike the other two tunneling EAP methods, EAP-FAST provides cryptobinding between inner and outer methods, preventing the special class of the man-in-the-middle attacks where an attacker hijacks a valid user's connection.

The EAP-FAST Settings panel enables you to configure the EAP-FAST settings:

- EAP-FAST Settings
  - Validate Server Identity—Enables server certificate validation. Enabling this introduces two extra dialogs in the management utility and adds additional Certificate panels into the NAM Profile Editor task list.
  - Enable Fast Reconnect—Enables session resumption. The two mechanisms to resume the authentication sessions in EAP-FAST include user authorization PAC, which substitutes the inner authentication, or TLS session resumption, which allows for abbreviated outer TLS handshake. This Enable Fast Reconnect parameter enables or disables both mechanisms. The authenticator decides which one to use.

    Note The machine PAC provides abbreviated TLS handshake and eliminates inner authentication. This control is handled by the enable/disable PAC parameter.

    Note Before user log on, smart card support is not available on Windows Vista and Windows 7.

    Note The *Disable when using a Smart Card* option is not available for machine.

- Inner methods based on Credentials Source—Enables you to authenticate using a password or certificate.
  - Authenticate using a password for EAP-MSCHAPv2 or EAP-GTC. EAP-MSCHAPv2 provides mutual authentication, but it authenticates the client before authenticating the server. If you want mutual authentication with the server being authenticated first, you should configure EAP-FAST for authenticated provisioning only and verify the server's certificate. Using the challenge-response method based on the NT-hash of the password, EAP-MSCHAPv2 requires you to store either the clear text password or at least the NT-hash of the password in the authenticator's database. Since the password is passed to the authenticator in clear text within EAP-GTC, you can use this protocol for authentication against the database with hashed (or irreversibly encrypted) passwords. We recommend this method if a possibility of a database leak exists.

    If you are using password based inner methods, an additional option for using Protected Access Credential (PAC) applies. Choose to allow or disallow unauthenticated PAC provisioning.
  - Authenticate using a certificate—Decide the following criteria for authenticating using a certificate: when requested, send the client certificate in the clear, only send client certificates inside the tunnel, or send client certificate using EAP-TLS in the tunnel.
  - Authenticate Using a Token and EAP-GTC
- Use PACs—You can specify the use of PAC for EAP-FAST authentication. PACs are credentials that are distributed to clients for optimized network authentication.

Note Typically, you use the PAC option because most authentication servers use PACs for EAP-FAST. Before removing this option, verify that your authentication server does not use PACs for EAP-FAST; otherwise, the client's authentication attempts will be unsuccessful. If your authentication server supports authenticated PAC provisioning, we recommend that you disable unauthenticated provisioning. Unauthenticated provisioning does not validate server's certificates, thus allowing rogue authenticators to mount a dictionary attack.

You can manually provide one or more specific PAC files for distribution and authentication by selecting the PAC Files panel and clicking **Add**. You can also highlight a PAC file and click **Remove** to remove a PAC file from the list.

Password protected—If the PAC was exported as password protected, check the **Password Protected** check box and provide the password that matches the one with which PAC is encrypted.

Defining Networks Credentials

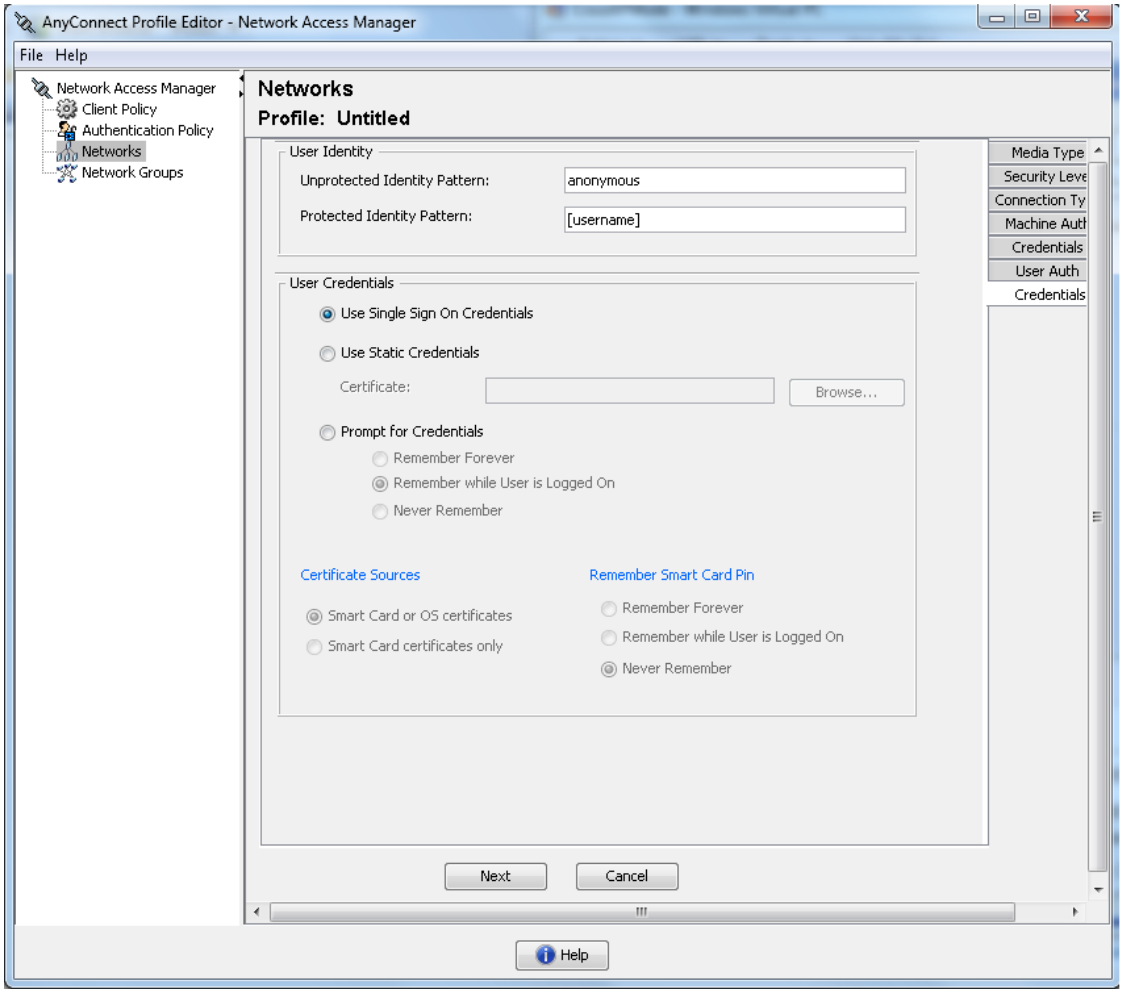
Within Network Credentials, you can establish user or machine credentials and establish trusted server validation rules.

- Configuring User Credentials
- Configuring Machine Credentials
- Configuring Trusted Server Validation Rules

Configuring User Credentials

With the Credentials panel you can specify the desired credentials to use for authenticating the associated network (see Figure 4-10).

Figure 4-10 User Credentials Panel



Step 1 You must identify a User Identity. NAM supports these identity placeholder patterns when you specify user identities:

- [username]—Specifies the username.
- [domain]—Specifies the domain of the user's PC.

For user connections, whenever the [username] and [domain] placeholders are used, these conditions apply:

- If a client certificate is used for authentication, the placeholder values for [username] and [password] are obtained from various X509 certificate properties. The properties are analyzed in the order described below, according to the first match. For example, if the identity is userA@cisco.com (where username=userA and domain=cisco.com) for user authentication and hostA.cisco.com (where username=hostA and domain=cisco.com) for machine authentication, the following properties are analyzed:

  User certificate based authentication:

  - SubjectAlternativeName: UPN = userA@cisco.com
  - Subject = .../CN=userA@cisco.com/...

- Subject = userA@cisco.com
- Subject = .../CN=userA/DC=cisco.com/...
- Subject = userA (no domain)

Machine certificate based authentication:

- SubjectAlternativeName: DNS = hostA.cisco.com
- Subject = .../DC=hostA.cisco.com/...
- Subject = .../CN=hostA.cisco.com/...
- Subject = hostA.cisco.com

- If the credential source is the end user, the placeholder's value is obtained from the information the user enters.
- If the credentials are obtained from the operating system, the placeholder's value is obtained from the logon information.
- If the credentials are static, no placeholders should be used.

Sessions that have yet to be negotiated experience identity request and response in the clear without integrity protection or authentication. These sessions are subject to snooping and packet modification. Typical unprotected identity patterns are as follows:

- anonymous@[domain]—Often used in tunneled methods to hide the user identity when the value is sent in clear text. The real user identity is provided in the inner method as the protected identity.
- [username]@[domain]—For non-tunneled methods

Note Unprotected identity is sent in clear text. If the initial clear text identity request or response is tampered with, the server may discover that it cannot verify the identity once the TLS session is established. For example, the user ID may be invalid or not within the realm handled by the EAP server.

The protected identities present clear text identity in a different way. To protect the userID from snooping, the clear text identity may only provide enough information to enable routing of the authentication request to the correct realm. Typical protected identity patterns are as follows:

- [username]@[domain]
- the actual string to use as the user's identity (no placeholders)

An EAP conversation may involve more than one EAP authentication method, and the identities claimed for each of these authentications may be different (such as machine authentication followed by user authentication). For example, a peer may initially claim the identity of nouser@cisco.com to route the authentication request to the cisco.com EAP server. However, once the TLS session has been negotiated, the peer may claim the identity of johndoe@cisco.com. Thus, even if protection is provided by the user's identity, the destination realm may not necessarily match, unless the conversation terminates at the local authentication server.

Step 2 Provide further user credential information:

- Use Single Sign On Credentials—Obtains the credentials from the operating system's logon information. If logon credentials fail, NAM temporarily (until next logon) switches and prompts the user for credentials with the GUI.
- Use Static Credentials—Obtains the user credentials from the network profiles that this profile editor provides. If static credentials fail, NAM will not use the credentials again until a new configuration is loaded.

- Prompt for Credentials—Obtains the credentials from the end user with the AnyConnect GUI as specified here:
  - Remember Forever—The credentials are remembered forever. If remembered credentials fail, the user is prompted for the credentials again. Credentials are preserved in the file and encrypted using a local machine password.
  - Remember while User is Logged On—The credentials are remembered until the user logs off. If remembered credentials fail, the user is prompted for credentials again.
  - Never Remember—The credentials are never remembered. NAM prompts the user each time it needs credential information for authentication.

Step 3 Determines which certificate source to use for authentication when certificates are required:

- Smart Card or OS certificates—NAM uses certificates found in the OS Certificate Stores or on a Smart Card.
- Smart Card certificates only— NAM only uses certificates found on a Smart Card.

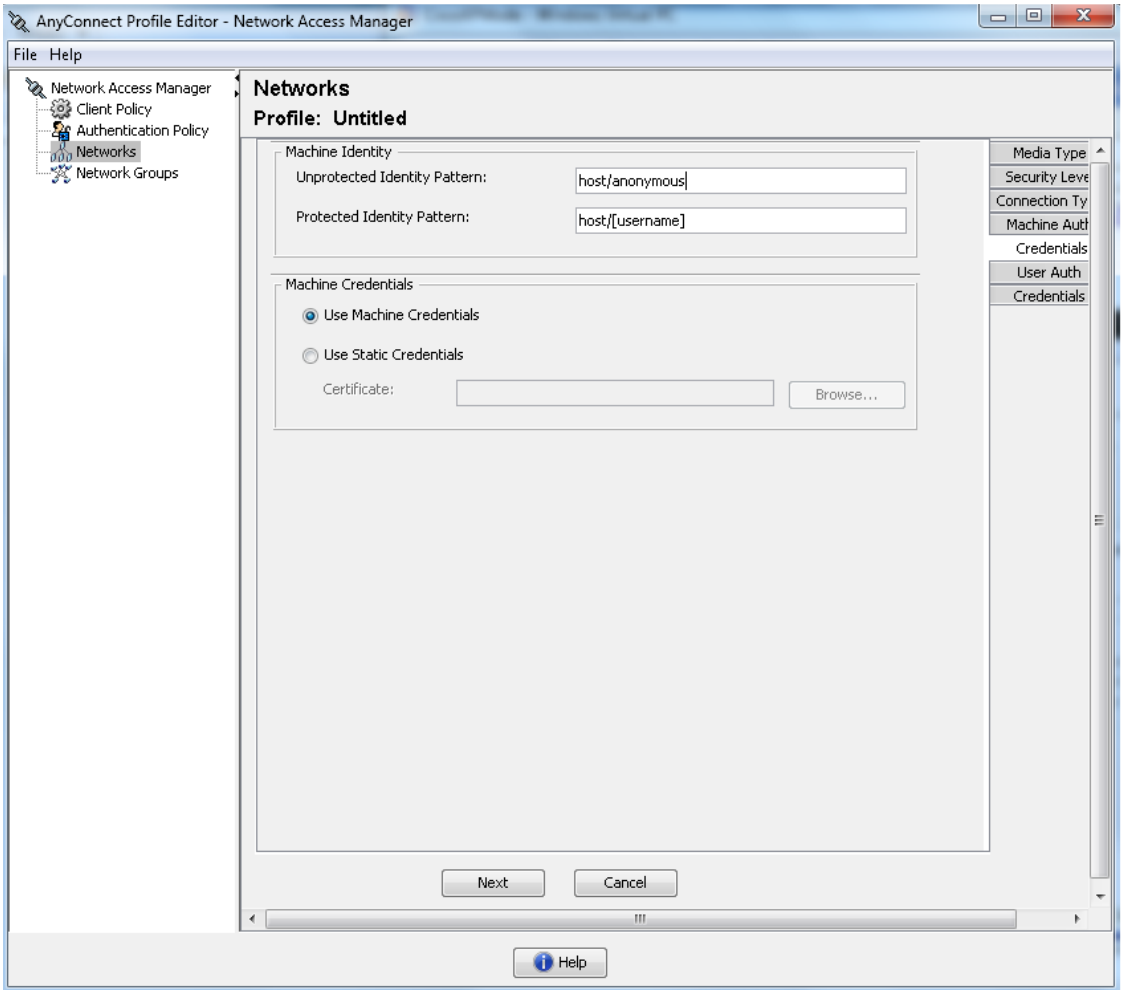
Step 4 At the Remember Smart Card Pin parameter, determine how long NAM remembers the PIN used to retrieve the certificate off a smart card. Refer to Step 2 for the available options.

Note The PIN is never preserved longer than a certificate itself.

Configuring Machine Credentials

With the Credentials panel you can specify the desired machine credentials (see Figure 4-11).

Figure 4-11 Machine Credentials



Step 1 You must identify a Machine Identity. NAM supports these identity placeholder patterns when you specify user identities:

- [username]—Specifies the machine name.
- [domain]—Specifies the domain of the user's PC.

For machine connections, whenever the [username] and [domain] placeholders are used, these conditions apply:

- If a client certificate is used for authentication, the placeholder values for [username] and [password] are obtained from various X509 certificate properties. The properties are analyzed in the order described below, according to the first match. For example, if the identity is userA@cisco.com (where username=userA and domain=cisco.com) for user authentication and hostA.cisco.com (where username=hostA and domain=cisco.com) for machine authentication, the following properties are analyzed:

  User certificate based authentication:

  - SubjectAlternativeName: UPN = userA@cisco.com

- Subject = .../CN=userA@cisco.com/...
- Subject = userA@cisco.com
- Subject = .../CN=userA/DC=cisco.com/...
- Subject = userA (no domain)

Machine certificate based authentication:

- SubjectAlternativeName: DNS = hostA.cisco.com
- Subject = .../DC=hostA.cisco.com/...
- Subject = .../CN=hostA.cisco.com/...
- Subject = hostA.cisco.com

- If a client certificate is not used for authentication, the credentials are obtained from the operating system, and the [username] placeholder represents the assigned machine name.

Sessions that have yet to be negotiated experience identity request and response in the clear without integrity protection or authentication. These sessions are subject to snooping and packet modification. Typical unprotected machine identity patterns are as follows:

- host/anonymous@[domain]
- the actual string to send as the machine's identity (no placeholders)

The protected identities present clear text identity in a different way. To protect the userID from snooping, the clear text identity may only provide enough information to enable routing of the authentication request to the correct realm. Typical protected machine identity patterns are as follows:

- host/[username]@[domain]
- the actual string to use as the machine's identity (no placeholders)

An EAP conversation may involve more than one EAP authentication method, and the identities claimed for each of these authentications may be different (such as machine authentication followed by user authentication). For example, a peer may initially claim the identity of nouser@cisco.com to route the authentication request to the cisco.com EAP server. However, once the TLS session has been negotiated, the peer may claim the identity of johndoe@cisco.com. Thus, even if protection is provided by the user's identity, the destination realm may not necessarily match, unless the conversation terminates at the local authentication server.

Step 2 Provide further Machine Credential information:

- Use Machine Credentials—Obtains the credentials from the operating system.
- Use Static Credentials—If you choose to use static credentials, you can specify an actual static password to send in the deployment file. Static credentials do not apply for certificate-based authentication.

Configuring Trusted Server Validation Rules

When the Validate Server Identity option is configured for the EAP method, the Certificate panel is enabled to allow you to configure validation rules for Certificate Server or Authority. The outcome of the validation determines whether the certificate server or the authority are trusted.

To define certificate server validation rules, follow these steps:

Step 1 When the optional settings appear for the **Certificate Field** and the **Match** columns, click the drop-down arrows and highlight the desired settings.

Step 2 Enter a value in the Value field.

Step 3 Under Rule, click **Add**.

Step 4 In the Certificate Trusted Authority portion, choose one of the following options:

- Trust any Root Certificate Authority (CA) Installed on the OS—If chosen, only the local machine or certificate stores are considered for the server's certificate chain validation.
- Include Root Certificate Authority (CA) Certificates

Note If you choose Include Root Certificate Authority (CA) Certificates, you must click on **Add** to import the CA certificate into the configuration.

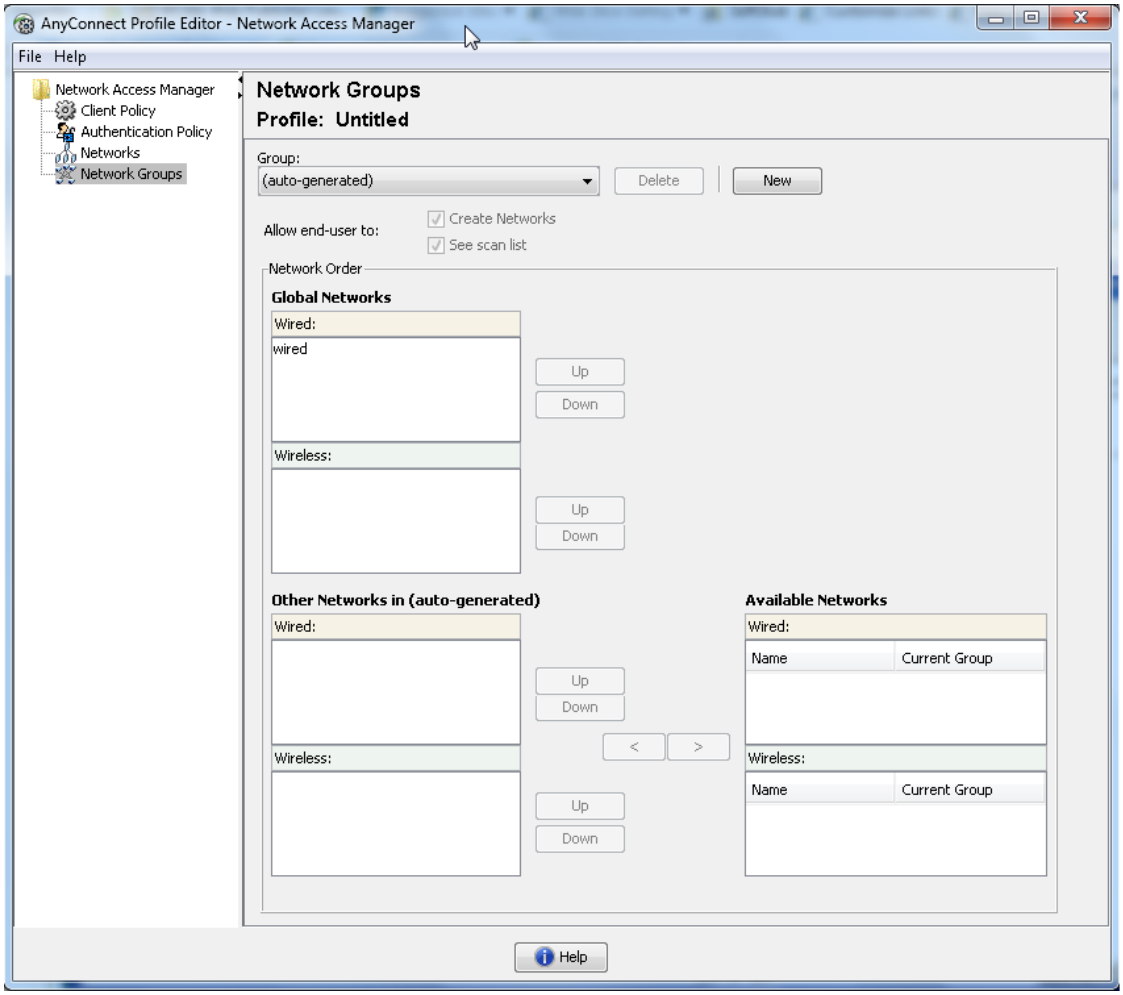
Defining Network Groups

With the Network Groups panel you can assign network connections to a particular group (see Figure 4-12). Classifying connections into groups provides multiple benefits:

- Improved user experience when attempting to make a connection. When multiple hidden networks are configured, the client walks through the list of hidden networks in the order that they are defined until a successful connection is made. In such instances, groups are used to greatly reduce the amount of time needed to make a connection.
- Easier management of configured connections. This benefit allows you to separate administrator networks from user networks if you want and allows users who have multiple roles in a company (or who often visit the same area) to tailor the networks in a group to make the list of selectable networks more manageable.

Networks defined as part of the distribution package are locked, preventing the user from editing the configuration settings or removing the network profiles.

Figure 4-12 Network Groups Window



Step 1 Choose a Group by choosing it in the drop-down list.

Step 2 Choose **Create networks** to allow the end user to create networks in this group. When deployed, if you uncheck this, NAM deletes any user-created networks from this group, which may force the user to re-enter network configuration in another group.

Step 3 Choose **See scan list** to allow end users to view the scanlist when the group is selected as the active group using the AnyConnect GUI. Alternatively, clear the check box to restrict users from viewing the scan list. For instance, if you want to prevent users from accidentally connecting to nearby devices, you should restrict scan list access.

Note These settings are applied on a per group basis.

Step 4 Use the **Right and Left arrows** to insert and remove a network from the group selected in the Group drop-down list.

Note Within a given network, the display name of each network must be unique; therefore, any one group cannot contain two or more networks with the same display name.

Step 5 Use the **Up and Down arrows** to change the priority order of the networks within a group.

CHAPTER 5

Configuring Host Scan

The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host. The Host Scan application, which is among the components delivered by the posture module, is the application that gathers this information.

In the adaptive security appliance (ASA), you can create a prelogin policy that evaluates endpoint attributes such as operating system, IP address, registry entries, local certificates, and filenames. Based on the result of the prelogin policy's evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance.

Starting with AnyConnect 3.0, the Host Scan package becomes a shared component of the AnyConnect Secure Mobility client and Cisco Secure Desktop (CSD). Previously, the Host Scan package was one of several components available only by installing CSD.

The purpose of separating the Host Scan package from CSD is to allow you to update Host Scan support charts more frequently than it was possible when they were delivered as part of CSD. The Host Scan support charts contain the product name and version information of the antivirus, antispyware, and firewall applications you use in your prelogin policies. We deliver the Host Scan application and the Host Scan support charts, as well as other components, in the Host Scan package.

The standalone Host Scan package and the Host Scan package delivered with the posture module provide the same functionality. We provide a separate Host Scan package so that you can update the Host Scan support charts easily.

The Host Scan package can now be delivered in one of three ways: with the AnyConnect Posture Module, with CSD, or as a standalone package. There are two types of AnyConnect posture modules: one version is pushed down by the ASA along with the AnyConnect installation and the other is configured as a pre-deployment module. The pre-deployment module can be installed on endpoints before they make their initial connection to the ASA.

In addition to identifying operating system, antivirus, antispyware, and firewall software installed on the endpoint, the host scan package delivers the components to identify keystroke loggers, detect host emulation and virtual machines running on the endpoint, and clean browser caches. Keystroke logger detection, host emulation and virtual machine detection, and cache cleaner were also features of CSD that are now supported by the Host Scan package.

Still, the Host Scan package is not a replacement for CSD. Customers that want the Secure Vault will need to install and enable CSD in addition to the Host Scan package. See http://www.cisco.com/en/US/products/ps6742/products_installation_and_configuration_guides_list.html to learn about the Secure Vault feature in the CSD Configuration Guides.

You can install, uninstall, enable, and disable Host Scan using the ASA's Adaptive Security Device Manager (ASDM) or command line interface. You can configure prelogin policies using the Secure Desktop Manager tool on the ASDM.

Posture assessment and the AnyConnect telemetry module require Host Scan to be installed on the host.

This chapter contains the following sections:

Host Scan Workflow

Host Scan works with the ASA to protect the corporate network as described in the workflow that follows:

1. The remote device attempts to establish a clientless SSL VPN or AnyConnect Client session with the security appliance.
2. The ASA downloads Host Scan to the client ensuring that the ASA and the client are using the same version of Host Scan.
3. A prelogin assessment checks for the following on the remote computer:

- Operating system
- Presence or absence of any files you specify.
- Presence or absence of any registry keys you specify. This check applies only if the computer is running Microsoft Windows.
- Presence of any digital certificates you specify. This check also applies only if the computer is running Microsoft Windows.
- IP address within a range you specify.

4. At the same time the client is undergoing the prelogin assessment, host scan is performing it's endpoint assessment and gathering up the antivirus, firewall, and antispyware version information; as well as scanning for registry keys, files, and processes that you have specified in dynamic access policies.
5. One of the following events occurs, depending on the result of the prelogin assessment:

- The Login Denied message appears on the remote computer if it runs the prelogin assessment and traverses a sequence that ends with a Login Denied end node. In this case, interaction between the ASA and the remote device stops.
- The prelogin assessment assigns a prelogin policy name to the device and reports the name of the prelogin policy to the ASA.

6. Host Scan checks for keystroke loggers and host emulation on the remote computer, based on the configuration of the prelogin policy the remote computer was assigned after the prelogin assessment.
7. Antivirus, firewall, or antispyware remediation occurs if it is warranted and you have a license for Advanced Endpoint Assessment.
8. The user logs in.
9. The ASA typically uses the authentication data gathered in 3. along with any configured endpoint attribute criteria gathered in 4., which can include such values as the prelogin policy and Host Scan results, to apply a dynamic access policy to the session.
10. Following the termination of the user session, Host Scan terminates, and Cache Cleaner performs its cleanup functions.

Features Enabled with the AnyConnect Posture Module

Prelogin Assessment

The prelogin assessment runs after the user connects to the ASA, but before the user logs in. This assessment can check the remote device for files, digital certificates, the OS, IP address, and Microsoft Windows registry keys.

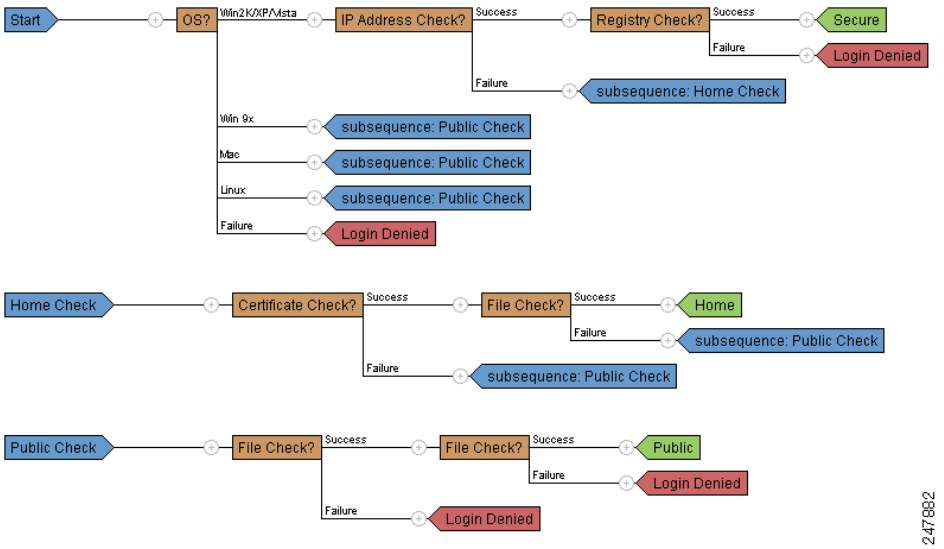
Secure Desktop Manager, the administrator interface to Host Scan, provides a graphical sequence editor to simplify the configuration of the prelogin assessment module.

When configuring the prelogin assessment module, the Host Scan administrator creates branches of nodes called *sequences*. Each sequence begins with the Start node, followed by an endpoint check. The result of the check determines whether to perform another endpoint check or to terminate the sequence with an end node.

The end node determines whether to display a Login Denied message, assign a prelogin policy to the device, or perform a secondary set of checks called a subsequence. A *subsequence* is a continuation of a sequence, typically consisting of more endpoint checks and an end node. This feature is useful to do the following:

- Reuse a sequence of checks in some cases but not others.
- Create a set of conditions that have an overall purpose that you want to document by using the subsequence name.
- Limit the horizontal space occupied by the graphical sequence editor.

Figure 5-1 Example of a Completed Prelogin Assessment

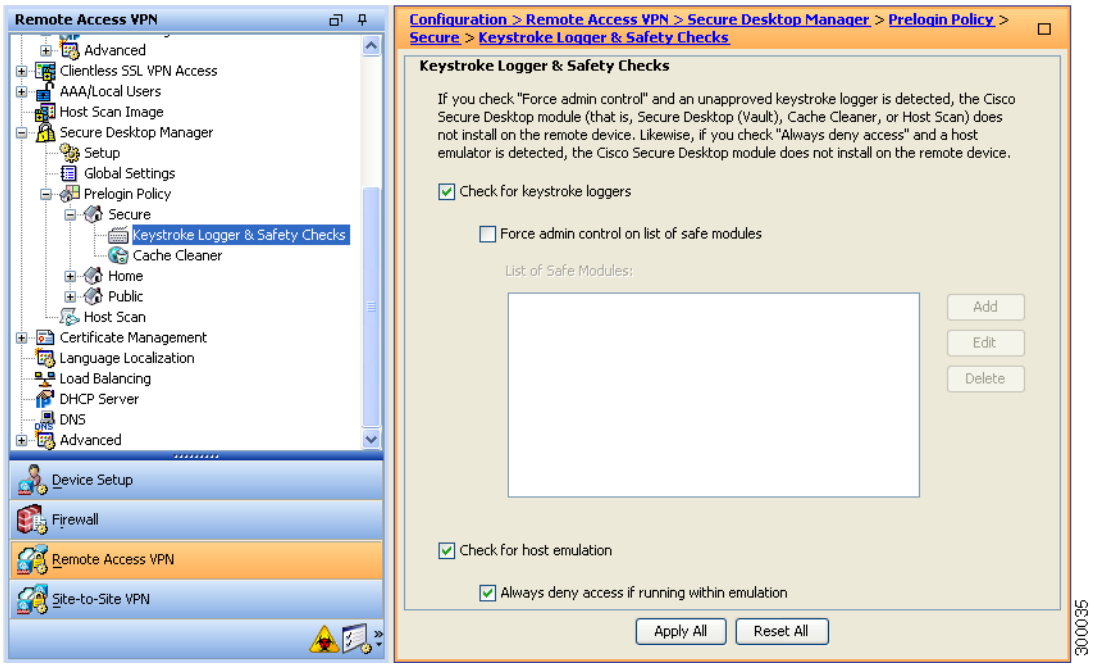


Prelogin Policies

The results of the checks of the prelogin assessment configured in the graphical sequence editor, Figure 5-1, determine whether the prelogin assessment results in the assignment of a particular prelogin policy or a denied remote access connection.

As you create each policy, Secure Desktop Manager adds a menu named after the policy. Each of the policy menus let you assign unique settings to the policy. These settings determine whether Keystroke Logger Detection, Host Emulation Detection, or Cache Cleaner installs on remote devices that match the prelogin criteria assigned to the policy. Administrators typically assign these modules to non-corporate computers to prevent access to corporate data and files after the session is over.

Figure 5-2 Prelogin Policies



Keystroke Logger Detection

You can configure selected prelogin policies to scan for processes or modules that record keystrokes entered by the user, and deny VPN access if a suspected keystroke logging application is present.

By default, keystroke logger detection is disabled for each prelogin policy. You can use Secure Desktop Manager to enable or disable keystroke logger detection. You can specify the keystroke loggers that are safe or let the remote user interactively approve the ones that the scan identifies as a condition for running Cache Cleaner or Host Scan on the remote computer.

If you enable it, keystroke logger detection downloads with Cache Cleaner or Host Scan onto the remote computer. Following the download, keystroke logger detection runs only if the OS is Windows and the user login has administrator privileges.

The associated module runs only if the scan is clear, or only if you assign administrative control to the user and the user approves of the applications the scan identifies.

Note Keystroke logger detection applies to both user mode and kernel mode loggers as long as the end-user is logged in with administrator privileges.

Keystroke logger detection runs only on 32-bit Microsoft Windows OS's. See "Keystroke Logger Detection and Host Emulation Detection Supported Operating Systems" section on page 5-6.

Keystroke logger detection may be unable to detect every potentially malicious keystroke logger. It does not detect hardware keystroke logging devices.

Host Emulation Detection

Host emulation detection, another feature of prelogin policies, determines whether a remote Microsoft Windows operating system is running over virtualization software. You can use Secure Desktop Manager to enable or disable this feature, and deny access if a host emulator is present or report the detection to the user and let the user decide whether to continue or terminate.

By default, host emulation detection is disabled for each prelogin policy. If you enable it, it downloads with Secure Desktop, Cache Cleaner, or Host Scan onto the remote computer. Following the download, host emulation detection runs first, along with keystroke logger detection if it is configured to do so. The associated module then runs if either of the following conditions are true:

- The host is not running over an emulator (or virtualization software).
- You did not configure it to always deny access, and the user approves of the detected host emulator.

See the "Keystroke Logger Detection and Host Emulation Detection Supported Operating Systems" section on page 5-6.

Keystroke Logger Detection and Host Emulation Detection Supported Operating Systems

Keystroke Logger Detection and Host Emulation Detection run on the following operating systems:

- x86 (32-bit) Windows Vista, SP1, and SP2

  KB935855 must be installed on computers running Windows Vista without SP1 or SP2.
- x86 (32-bit) Windows XP SP2 and SP3

Note Secure Desktop, Keystroke Logger Detection and Host Emulation Detection are not supported on Windows 7.

Cache Cleaner

Cache Cleaner, an alternative to Secure Desktop, is functionally more limited, but has the flexibility to support more operating systems. It attempts to eliminate the information from the browser cache at the end of a clientless SSL VPN or AnyConnect Client session. This information includes entered passwords, auto-completed text, files cached by the browser, browser configuration changes made during the session, and cookies.

Cache Cleaner runs on Microsoft Windows, Apple Mac OS, and Linux. For detailed system requirements, see the Cisco Secure Desktop Release Notes.

This is a typical sequence of events when Cache Cleaner has been deployed and the endpoint attempts to create a clientless SSL VPN connection or attempts to launch AnyConnect using web launch:

Step 1 The endpoint connects to the ASA when the user enters its URL in a browser.

Step 2 Hostscan performs the prelogin assessment.

Step 3 Assuming that the endpoint passes the prelogin assessment, AnyConnect authentication begins. The user may enter a password or use a certificate to authenticate.

Step 4 For users running Internet Explorer without **Clean the whole cache in addition to the current session cache (IE only)** enabled, or for users running Safari or Firefox; approximately one minute after the user authenticates, Cache Cleaner takes a snapshot of the browser's cache.

Step 5 As the user works, the browser caches information.

Step 6 When users logout of the VPN session:

- For users running Internet Explorer with **Clean the whole cache in addition to the current session cache (IE only)** enabled, Cache Cleaner attempts to delete the browser's entire cache.
- For users running Internet Explorer without **Clean the whole cache in addition to the current session cache (IE only)** enabled, or running Safari or Firefox, Cache Cleaner attempts to delete all of the browser's cache and then Cache Cleaner restores the snapshot it took of the cache.

  To prevent any sensitive information from being restored on the computer, we recommend that you manually clean the browser's cache after your session and then close the browser.

Note We recommend that Cache Cleaner be configured with the **Clean the whole cache in addition to the current session cache (IE only)** option enabled. See the "Configuring Cache Cleaner" section on page 6-4 for more information.

Host Scan

Host Scan is a component that installs on the remote device after the user connects to the ASA and before the user logs in. Host Scan can perform Basic Host Scan, Endpoint Assessment, and Advanced Endpoint Assessment. Host Scan runs on Microsoft Windows, Apple Mac OS, and Linux. For detailed requirements, see System Requirements, page 5-10.

Basic Host Scan

Basic Host Scan is always performed when Host Scan is enabled and it automatically identifies operating systems and service packs on computers connecting to the adaptive security appliance (ASA). It also lets you configure inspections for specified processes, files, and registry keys. Thus, you can use this feature to configure checks on remote computers to determine whether they are corporate-owned. You can use the results returned by basic Host Scan when configuring different Dynamic Access Policies (DAPs) to distinguish corporate computers, home computers, and public computers.

If Host Scan is enabled on the ASA, basic Host Scan attempts to run on any remote device establishing an AnyConnect Client session. The OS detection qualifies or disqualifies the remote device from running Endpoint Assessment or Advanced Endpoint Assessment. Process name, filename, and registry key checking must be explicitly configured using the Secure Desktop Manager tool in the Adaptive Device Security Manager (ADSM). Basic Host Scan returns the name of the OS and service pack, and the results of any configured posture checks to the ASA.

The ASA evaluates the returned values against the endpoint criteria explicitly configured in the DAPs. Thus, you can assign DAPs to devices based on this data. To view the list of the operating systems and service packs this module detects, choose **Configuration > Remote Access VPN > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies**. Click **Add** or **Edit** next to the endpoint attributes table, select **Operating System** from the Endpoint Attribute Type drop-down list, check **OS Version**, and click the arrow to the right of the adjacent operator.

Basic Host Scan automatically returns the following additional values for evaluation against configured DAP endpoint criteria:

- Microsoft Windows, Mac OS, and Linux builds
- Listening ports active on a connecting host running Microsoft Windows
- Posture Module components installed on the connecting host

- Microsoft Knowledge Base numbers (KBs)

If you want to configure endpoint criteria to match other data, enter the appropriate free-form Lua text into the Advanced Logical Expressions text box. Be aware that doing so requires sophisticated knowledge of the Lua language. For more information, open the Add or Edit Dynamic Access Policies window, click **Advanced** at the bottom of the Selection Criteria area, and click the **Guide** button to the right of the Logical Expressions text box.

Endpoint Assessment

Endpoint Assessment, a Host Scan extension, examines the remote computer for a large collection of antivirus and antispyware applications, associated definitions updates, and firewalls. You can use this feature to combine endpoint criteria to satisfy your requirements before the ASA assigns a specific DAP to the session.

Advanced Endpoint Assessment - Antivirus, Antispyware, and Firewall Remediation

With the purchase of an **Advanced Endpoint Assessment** license installed on the ASA, you can attempt to initiate remediation of various aspects of antivirus, antispyware and personal firewall protection if that software allows a separate application to initiate remediation.

Antivirus —Advanced Endpoint Assessment can attempt to remediate these components of antivirus software:

- Force File System Protection — If the antivirus software is disabled, Advanced Endpoint Assessment can enable it.
- Force Virus Definitions Update — If the antivirus definitions have not been updated in the number of days defined by the Advanced Endpoint Assessment configuration, Advanced Endpoint Assessment can attempt to initiate an update of virus definitions.

Antispyware — If the antispyware definitions have not been updated in the number of days defined by the Advanced Endpoint Assessment configuration, Advanced Endpoint Assessment can attempt to initiate an update of antispyware definitions.

Personal Firewall — The Advanced Endpoint Assessment module can attempt to reconfigure firewall settings and rules if they do not meet the requirements defined in the Advanced Endpoint Assessment configuration.

- The firewall can be enabled or disabled.
- Applications can be prevented from running or allowed to run.
- Ports can be blocked or opened.

Note Not all personal firewalls support this feature.

Host Scan Support Charts

The Host Scan support charts contain the product name and version information for the antivirus, antispyware, and firewall applications you use in your prelogin policies. We deliver Host Scan and the Host Scan support chart in the Host Scan package.

In this release of the AnyConnect Secure Mobility Client, the Host Scan package can be uploaded separately from Cisco Secure Desktop (CSD). This means you can deploy Host Scan functionality without having to install CSD and you are able to update your Host Scan support charts by upgrading the to the latest Host Scan package.

Configuring Antivirus Applications for Host Scan

Antivirus applications can misinterpret the behavior of some of the applications included in the posture module and the Host Scan package as malicious. Before installing the posture module or Host Scan package, configure your antivirus software to "white-list" or make security exceptions for these Host Scan applications:

- cscan.exe
- ciscod.exe
- cstub.exe

Integration with Dynamic Access Policies

The ASA integrates the Host Scan features into dynamic access policies (DAPs). Depending on the configuration, the ASA uses one or more endpoint attribute values in combination with optional, AAA attribute values as conditions for assigning a DAP. The Host Scan features supported by the endpoint attributes of DAPs include OS detection, prelogin policies, basic Host Scan results, and endpoint assessment.

As an administrator, you can specify a single attribute or combine attributes that together form the conditions required to assign a DAP to a session. The DAP provides network access at the level that is appropriate for the endpoint AAA attribute value. The ASA applies a DAP when all of its configured endpoint criteria are satisfied.

Difference Between the Posture Module and the Standalone Host Scan Package

The AnyConnect Posture Module can be deployed by the ASA to the endpoint, or it can be installed on the endpoint using a pre-deployment kit before the endpoint makes its initial connection to the ASA.

The posture module contains the Host Scan package, keystroke logger detection, host emulation detection, and cache cleaner. as well as a few other modules that the Host Scan application requires. Deploying the posture module allows Host Scan to run privileged operations even when the user on the endpoint is not an administrator and it allows other AnyConnect modules to start using Host Scan.

The standalone Host Scan package contains the Host Scan application and Host Scan support charts. The Host Scan support charts contain the product name and version information of the antivirus, antispyware, and firewall applications you use in your prelogin policies.

AnyConnect Posture Module Dependencies and System Requirements

The AnyConnect posture module contains the Host Scan package and other components.

Dependencies

The AnyConnect Secure Mobility Client with the posture module requires these minimum ASA components:

- ASA 8.4
- ASDM 6.4

These AnyConnect features require that you install the posture module.

- Host Scan
- SCEP authentication
- AnyConnect Telemetry Module

Host Scan, CSD, and AnyConnect Secure Mobility Client Interoperability

Caution If you deploy Host Scan with the AnyConnect Secure Mobility Client, version 3.0.x, the AnyConnect Secure Mobility Client requires Host Scan to have the same version number, or a later version number, than itself.

If you have Cisco Secure Desktop (CSD) version 3.5, or earlier, enabled on the ASA and you do not upgrade the Host Scan package to match or exceed the version of AnyConnect Secure Mobility Client 3.0.x you are deploying, prelogin assessments will fail and users will not be able to establish a VPN session. This will happen even if the AnyConnect 3.0.x posture module is pre-deployed to the endpoint because the ASA will automatically downgrade the Host Scan package on the endpoint to match the Host Scan package enabled on the ASA.

Though AnyConnect 3.0.x is not compatible with older versions of Host Scan or CSD, older versions of AnyConnect are compatible with new versions of the Host Scan package. For example, if you are using CSD 3.5 or earlier and AnyConnect 2.5 or earlier and you upgrade just the Host Scan image to 3.0.x or later, prelogin assessments will succeed.

System Requirements

The posture module can be installed on any of these platforms:

- Windows XP (x86 and x86 running on x64)
- Windows Vista (x86 and x86 running on x64)
- Windows 7 (x86 and x86 running on x64)
- Mac OS X 10.5,10.6 (32-bit and 32-bit running on 64-bit)
- Linux (32-bit and 32-bit running on 64-bit)

Note Host Scan is a 32-bit application and requires the core 32-bit libraries to be installed on 64-bit Linux operating systems. Host Scan does not provide these 32-bit libraries at the time it is installed. Customers need to install the 32-bit libraries on the endpoints themselves, if they are not already provisioned.

- Windows Mobile

Licensing

These are the AnyConnect licensing requirements for the posture module:

- AnyConnect Premium for basic Host Scan.
- Advanced Endpoint Assessment license is required for
  - Remediation
  - Mobile Device Management

Entering an Activation Key to Support Advanced Endpoint Assessment

Advanced Endpoint Assessment includes all of the Endpoint Assessment features and lets you configure an attempt to update noncompliant computers to meet version requirements. You can use ASDM to activate a key to support Advanced Endpoint Assessment after acquiring it from Cisco, as follows:

Step 1 Choose **Configuration > Device Management > Licensing > Activation Key**.

Step 2 Enter the key in the **New Activation Key** field.

Step 3 Click **Update Activation Key**.

Step 4 Choose **File > Save Running Configuration to Flash**.

An Advanced Endpoint Assessment entry appears and the Configure button becomes active in the Host Scan Extensions area of the **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan** pane, which is accessible only if CSD is enabled.

Host Scan Packaging

You can load the Host Scan package on to the ASA in one of these ways:

- You can upload it as a standalone package: **hostscan-*version*-**k9**.pkg**
- You can upload it by uploading an AnyConnect Secure Mobility package: **anyconnect-win-*version*-k9.pkg**
- You can upload it by uploading a Cisco Secure Desktop package: **csd_version-k9.pkg**

Table 5-1 Host Scan Packages You Load to the ASA

File	Description
hostscan-*version*-k9.pkg	This file contains the Host Scan image as well as the Host Scan support charts.
anyconnect-win-*version*-k9.pkg	This package contains all the Cisco AnyConnect Secure Mobility Client features including the hostscan-*version*-k9.pkg file.
csd_*version*-k9.pkg	This file contains all Cisco Secure Desktop features including Host Scan software as well as the Host Scan support charts.

Which Host Scan Image Gets Enabled When There is More than One Loaded on the ASA?

The Host Scan image is delivered with the Host Scan package. It can be deployed to the endpoint from the standalone Host Scan package, the full AnyConnect Secure Mobility Client package, and Cisco Secure Desktop. Depending on what licenses you have installed on your ASA, you may have all of these packages loaded on your ASA. In that case, the ASA enables the image that you specified as the Host Scan image first and if you haven't specified one, the ASA enables the Host Scan functionality from Cisco Secure Desktop. See the "Installing or Upgrading Host Scan" section on page 5-14.

If you uninstall the Host Scan package, the ASA cannot enable its Host Scan image.

These scenarios describe which Host Scan package the ASA distributes when it has more than one loaded.

- If you have installed a standalone Host Scan package on the ASA and have designated it as the Host Scan image, and you enable CSD/hostscan, ASA distributes the standalone Host Scan package.
- If you have installed a standalone Host Scan package on the ASA and have designated it as the Host Scan image and you have installed a CSD image on the ASA, and you enable CSD/hostscan, ASA will distribute the standalone Host Scan image.
- If you have installed a Host Scan image on the ASA, but you have not enabled it, and you have installed a CSD image on the ASA and you have enabled CSD/hostscan, the ASA will distribute the standalone Host Scan image because it was not uninstalled.
- If you have installed an AnyConnect Secure Mobility Client package on the ASA and have designated it as the Host Scan image, the ASA will distribute the Host Scan image from that package.
- If you install an AnyConnect Secure Mobility Client package file on the ASA but do not specify it as the Host Scan image, the ASA will not distribute the Host Scan package associated with that AnyConnect package. The ASA will distribute an installed Host Scan package or CSD package, provided CSD is enabled.

Deploying the AnyConnect Posture Module and Host Scan

There are two different deployment scenarios for the posture module and Host Scan.

Pre-deployment. Using the pre-deployment method, you install the AnyConnect client and posture module before the endpoint attempts to make a connection to the ASA. The pre-deployment posture module package contains every component, library, and support chart that could be used to gather posture attributes as well as the applications that provide you with the features described in the "Features Enabled with the AnyConnect Posture Module" section on page 5-3. If you pre-deploy to the endpoint the same version of the AnyConnect client and posture module installed on the ASA, when the endpoint connects to the ASA, there will be no additional posture module files that need to be pushed down from the ASA.

Web-deployment. Using the web-deployment method, when the endpoint connects to the ASA, the ASA pushes the AnyConnect client and posture module down to the endpoint. To make the download as fast and efficient as possible, the ASA only downloads the essential posture module files.

When the endpoint connects again, the essential posture module files determine what other libraries or files it needs from to perform an endpoint assessment and retrieves those files from the ASA. For example, the posture module may retrieve a Host Scan support chart of all Norton anti-virus software because a version of Norton anti-virus is running on the endpoint. After the posture module retrieves the additional files it needs, it performs the endpoint assessment and forwards the attributes to the ASA. Assuming the endpoint attributes are sufficient to satisfy a dynamic access policy (DAP) rule, the ASA allows the endpoint to connect. As a result of satisfying the DAP, the ASA could be configured to push the remainder of the posture module to the endpoint or not.

If you do not want the entire posture module web-deployed to the endpoint, you can perform a limited web-deployment where only one posture file is downloaded to the endpoint and it requests only the Host Scan libraries it needs to perform endpoint assessment. In this scenario, you will have very short downloads times from the ASA to the endpoint but you will lose the ability to perform Advanced Endpoint Assessment and perform such tasks as antivirus, antispyware, or firewall remediation tasks.

Pre-Deploying the AnyConnect Posture Module

When you pre-deploy the posture module, you install it on the endpoint before the AnyConnect client makes its initial connection to the ASA.

You need to install the AnyConnect Secure Mobility Client on the endpoint before you install the posture module. See Chapter 2, "Deploying the AnyConnect Secure Mobility Client" for instructions on installing the AnyConnect Secure Mobility Client and the posture module using web-deployment and pre-deployment methods.

Table 5-2 lists the posture module pre-deployment kits:

Table 5-2 Posture Module Pre-Deployment Kits

File	Description
Windows	anyconnect-posture-win-*version*-pre-deploy-k9.msi
Linux	anyconnect-linux-*version*-posture-k9.tar.gz
Mac OS X	anyconnect-macosx-posture-i386-*version*-i386-k9.dmg

Installing and Enabling Host Scan on the ASA

These tasks describe installing and enabling Host Scan on the ASA:

- Installing or Upgrading Host Scan
- Enabling or Disabling Host Scan on the ASA
- Uninstalling Host Scan
- Assigning AnyConnect Posture Module to a Group Policy

Installing or Upgrading Host Scan

Use this procedure to upload, or upgrade, and enable a new Host Scan image on the ASA. Use the image to enable Host Scan functionality for AnyConnect or upgrade the Host Scan support charts for an existing deployment of Cisco Secure Desktop (CSD).

You can specify a standalone Host Scan package or an AnyConnect Secure Mobility Client version 3.0 or later package in the field.

If you previously uploaded a CSD image to the ASA, the Host Scan image you specify will upgrade or downgrade the existing Host Scan files that were delivered with that CSD package.

You do not need to restart the security appliance after you install or upgrade Host Scan; however, you must exit and restart Adaptive Security Device Manager (ASDM) to access the Secure Desktop Manager tool in ASDM.

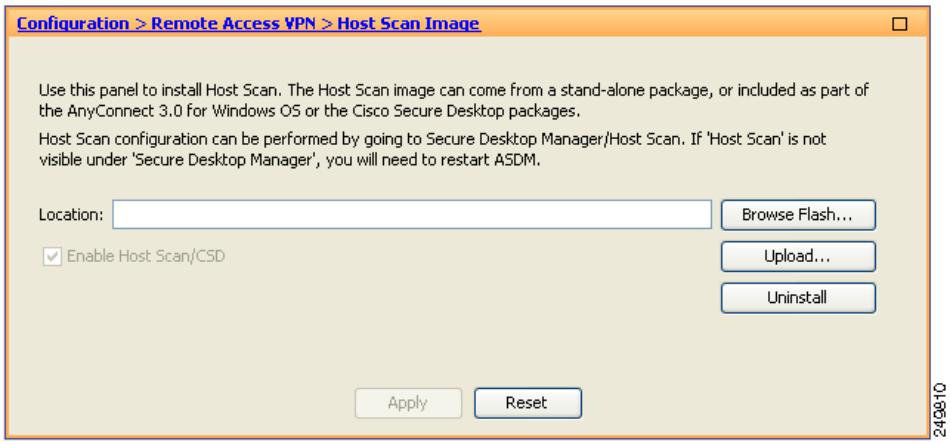
Note Host Scan requires an AnyConnect Secure Mobility Client premium license.

Step 1 Use an Internet browser to download the **hostscan_*version*-k9.pkg** file or **anyconnect-win-*version*-k9.pkg** file from http://www.cisco.com/cisco/software/release.html?mdfid=283000185&softwareid=282364313&i=rm to your computer.

Note You will need to have an account on Cisco.com and be logged in to download the software.

Step 2 Open ASDM and choose **Configuration > Remote Access VPN > Host Scan Image.** ASDM opens the Host Scan Image panel (Figure 5-3).

Figure 5-3 Host Scan Image Panel



Step 3 Click **Upload** to prepare to transfer a copy of the Host Scan package from your computer to a drive on the ASA.

Step 4 In the Upload Image dialog box, click **Browse Local Files** to search for the Host Scan package on your local computer.

Step 5 Select the **hostscan_*version*.pkg** file or **anyconnect-win-*version*-k9.pkg** file you downloaded in Step 1 and click **Select**. The path to the file you selected is in the Local File Path field and the Flash File System Path field reflects the destination path of the Host Scan package. If your ASA has more than one flash drive, you can edit the Flash File System Path to indicate another flash drive.

Step 6 Click **Upload File**. ASDM transfers a copy of the file to the flash card. An Information dialog box displays the following message:

```
File has been uploaded to flash successfully.
```

Step 7 Click **OK**.

Step 8 In the Use Uploaded Image dialog, click **OK** to use the Host Scan package file you just uploaded as the current image.

Step 9 Check **Enable Host Scan/CSD** if it is not already checked.

Step 10 Click **Apply**.

Note If AnyConnect Essentials is enabled on the ASA, you receive a message that Host Scan and CSD will not work with it. You have the choice to **Disable** or **Keep** AnyConnect Essentials.

Step 11 Click **Save**.

Enabling or Disabling Host Scan on the ASA

When you first upload or upgrade a Host Scan image using ASDM, you enable the image as part of that procedure. See "Installing and Enabling Host Scan on the ASA" section on page 5-14.

Otherwise, to enable or disable a Host Scan image using ASDM, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Host Scan Image.** ASDM opens the Host Scan Image panel (Figure 5-3).

Step 2 Check **Enable Host Scan/CSD** to enable Host Scan or uncheck **Enable Host Scan/CSD** to disable Host Scan.

Step 3 Click **Apply**.

Step 4 Click **Save**.

Enabling or Disabling CSD on the ASA

Enabling Cisco Secure Desktop (CSD) loads the CSD configuration file and data.xml, from the flash device to the running configuration. Disabling CSD does not alter the CSD configuration.

Use ASDM to enable or disable CSD as follows:

Step 1 Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.

ASDM opens the Setup pane (Figure 5-3).

Note The Secure Desktop Image field displays the image (and version) that is currently installed. The Enable Secure Desktop check box indicates whether CSD is enabled.

Step 2 Check **Enable Secure Desktop** to enable CSD or uncheck **Enable Secure Desktop** to disable CSD.

Step 3 Close ASDM. A window displays the following message:

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

Step 4 Click **Save**. ASDM saves the configuration and closes.

Host Scan and CSD Upgrades and Downgrades

The ASA automatically distributes the enabled Host Scan package to the endpoint whether that package is the standalone Host Scan package, the package included with AnyConnect Secure Mobility Client, or the package included with Cisco Secure Desktop. If the endpoint has an older version of the Host Scan package installed, the package on the endpoint gets upgraded; if the endpoint has a newer version of the Host Scan package, the endpoint package gets downgraded.

Determining the Host Scan Image Enabled on the ASA

Open ASDM and select **Configuration > Remote Access VPN > Host Scan Image**.

If there is a Host Scan image designated in the Host Scan Image location field, and the Enable HostScan/CSD box is checked, the version of that image is the Host Scan version being used by the ASA.

If the Host Scan Image filed is empty, and the Enable HostScan/CSD box is checked, select **Configuration > Remote Access VPN > Secure Desktop Manager**. The version of CSD in the Secure Desktop Image Location field is the Host Scan version being used by the ASA.

Uninstalling Host Scan

Uninstalling the Host Scan Package

Uninstalling the Host Scan package removes it from view on the ASDM interface and prevents the ASA from deploying it even if Host Scan or CSD is enabled. Uninstalling Host Scan does not delete the Host Scan package from the flash drive.

Use this procedure to uninstall Host Scan on the security appliance:

Step 1 Open ASDM and select **Configuration > Remote Access VPN > Host Scan Image**.

Step 2 In the Host Scan Image pane, click **Uninstall**. ASDM removes the text from the Location text box.

Step 3 Click **Save**.

Uninstalling CSD from the ASA

Uninstalling Cisco Secure Desktop (CSD) **removes the CSD configuration file, data.xml, from the desktop directory on the flash card**. If you want to retain the file, copy it using an alternative name or download it to your workstation before you uninstall CSD.

Use this procedure to uninstall CSD on the security appliance:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.

ASDM opens the Setup pane (Figure 5-3).

Step 2 Click **Uninstall**.

A confirmation window displays the following message:

```
Do you want to delete disk0:/csd_<n>.<n>.*.pkg and all CSD data files?
```

Step 3 Click **Yes**.

ASDM removes the text from the Location text box and removes the Secure Desktop Manager menu options below Setup.

Step 4 Close ASDM. A window displays the following message:

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

Step 5 Click **Save**. ASDM saves the configuration and closes.

Assigning AnyConnect Posture Module to a Group Policy

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies.**

Step 2 In the Group Policies panel, click **Add** to create a new group policy or select the group policy to which you want to assign the Host Scan package and click **Edit**.

Step 3 In the Edit Internal Group Policy panel, expand the **Advanced** navigation tree on the left side of the panel and select **AnyConnect Client**.

Step 4 Uncheck the Optional Client Modules to Download **Inherit** checkbox.

Step 5 In the Optional Client Modules to Download drop down menu, check the AnyConnect Posture Module and click **OK**.

Step 6 Click **OK**.

Host Scan Logging

Host Scan logs to the Event Viewer on Windows platforms, and syslog on non-windows platforms. In the Event Viewer all logs will be in their own “Cisco AnyConnect Secure Mobility Client Posture” folder.

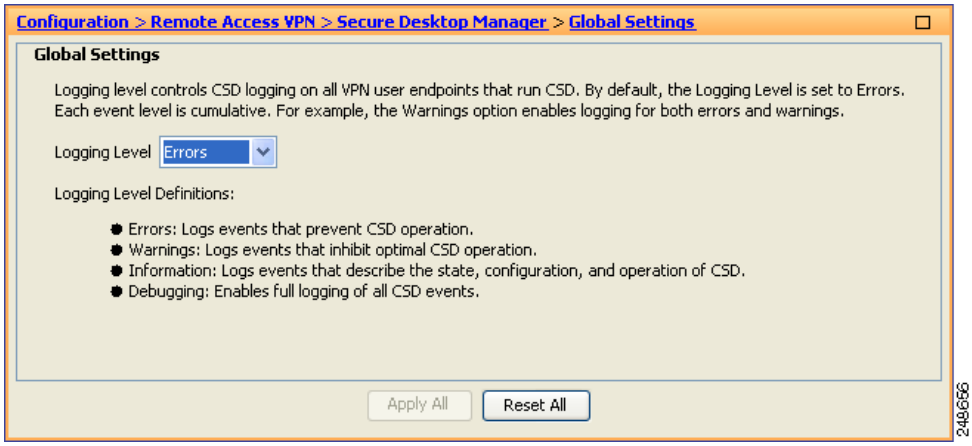
Configuring the Logging Level for All Posture Module Components

By default, components in the posture module log “Error” severity level events. Use these instructions to change the logging severity level for all components of the posture module.

The posture module installs the cscan.log file in the user’s home folder. The cscan.log file shows only the entries from the last VPN session. Each time the user connects to the ASA, Host Scan overwrites the entries in this file with new logging data.

To view or change the posture logging level:

Step 1 From the ASDM interface select **Configuration > Remote Access VPN > Secure Desktop Manager > Global Settings**. The Global Settings panel opens.



Step 2 Set the **Logging Level** using the Logging Level Definitions in the panel as a guide.

Step 3 Click **Apply All** to save the changes to the running configuration.

Note If Host Scan is disabled for a particular connection profile, Host Scan logging does not occur for users of that connection profile.

Posture Module Log Files and Locations

Posture module components output up to three logs based on your operating system, privilege level, and launching mechanism (Web Launch or AnyConnect):

- cstub.log - Captures logging when AnyConnect web launch is used.
- libcsd.log - Created by the AnyConnect thread that uses the Host Scan API. Debugging entries would be made in this log depending on the logging level configuration.
- cscan.log - Created by the scanning executable (cscan.exe) and is the main log for posture and Host Scan. Debugging entries would be made in this log depending on the logging level configuration.

The posture module puts these log files in the user's home folder. The location is dependent on the operating system and VPN method.

Cisco Technical Assistant Center (TAC) uses these log files to debug problems if the need arises. You will not need to review these files. Should Cisco TAC need them, you will be asked to provide them with a DART Bundle. The DART utility will collect all the necessary AnyConnect configuration and log files and store them in a compressed file which you will then send to TAC. See the "Using DART to Gather Troubleshooting Information" section on page 12-4 for more information about DART.

Using a BIOS Serial Number in a Lua Expression

Host Scan can retrieve the BIOS serial number of a host. You can use a Dynamic Access Policy (DAP) to allow or prevent a VPN connection to the ASA based on that BIOS serial number.

Expressing the BIOS in a Lua Expression

This is the Lua logical expression you can use in the **Advanced** field of the **Edit Dynamic Access Policy** screen of ASDM:

endpoint.device.id=***BIOSSerialNumber***

Where ***BIOSSerialNumber*** represents the BIOS serial number of the hardware device attempting to connect to the ASA. This string is a variable length string and is, generally, OS-specific.

Specifying the BIOS as a DAP Endpoint Attribute

Step 1 Log on to ASDM.

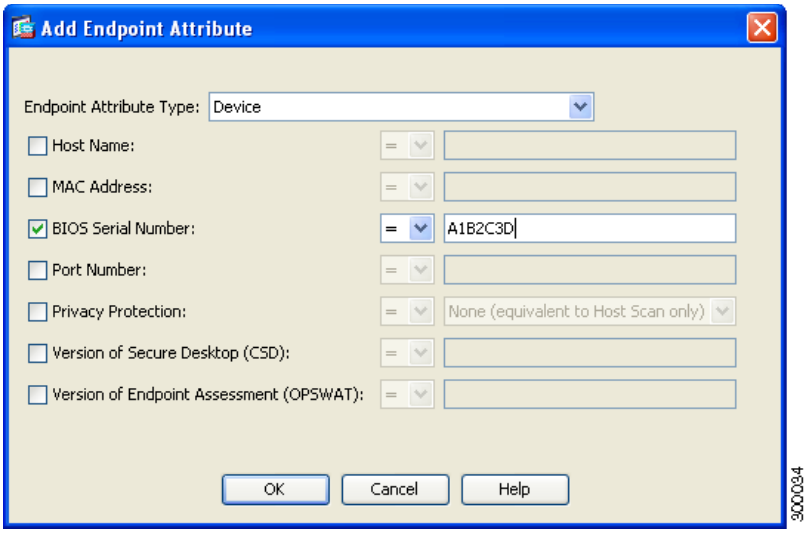
Step 2 Select **Configuration > Remote Access VPN > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies**.

Step 3 In the Configure Dynamic Access Policies panel, click **Add** or **Edit** to configure BIOS as a DAP Endpoint Attribute.

Step 4 To the right of the Endpoint ID table, click **Add**.

Step 5 In the Endpoint Attribute Type field, select **Device**.

Step 6 Check the **BIOS Serial Number** checkbox, select **=** (equals) or **!=** (not equals), and enter the BIOS number in the BIOS Serial Number field.



Step 7 Click **OK** to save changes in the Endpoint Attribute dialog box.

Step 8 Click **OK** to save your changes to the Edit Dynamic Access Policy.

Step 9 Click **Apply** to save your changes to the Dynamic Access Policy.

Step 10 Click **Save**.

How to Obtain BIOS Serial Numbers

These resources explain how to obtain the BIOS Serial number on various endpoints.

- Windows: http://support.microsoft.com/kb/558124
- Mac OS X: http://support.apple.com/kb/ht1529
- Linux: Use this command:

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

Other Important Documentation

Once Host Scan gathers the posture credentials from the endpoint computer, you will need to understand subjects like, configuring prelogin policies, configuring dynamic access policies, and using Lua expressions to make use of the information.

These topics are covered in detail in these documents:

- Cisco Secure Desktop Configuration Guides
- Cisco Adaptive Security Device Manager Configuration Guides

CHAPTER 6

Configuring Web Security

The AnyConnect Web Security module is an endpoint component that routes HTTP and HTTPS traffic to a ScanSafe scanning proxy where the ScanSafe web scanning service evaluates it.

The ScanSafe web scanning service deconstructs the elements of a Web page so that it can analyze each element simultaneously. For example, if a particular Web page combined HTTP, Flash, and Java elements, separate “scanlets” analyze each of these elements in parallel. The ScanSafe web scanning service then lets through benign or acceptable content and drops malicious or unacceptable content based on a security policy defined in the ScanCenter management portal. This prevents “over blocking” where an entire Web page is restricted because a minority of the content is unacceptable or “under blocking” where an entire page is permitted while there is still some unacceptable or possibly harmful content that is being delivered with the page. The ScanSafe web scanning service protects users when they are on or off the corporate network.

With many ScanSafe scanning proxies spread around the world, users taking advantage of AnyConnect Web Security are able to route their traffic to the ScanSafe scanning proxy with the fastest response time to minimize latency.

You can configure one or more instances of Beacon Server to identify endpoints that are on the corporate LAN. This is the “Detect-on-LAN” feature. If the Detect-On-LAN feature is enabled, any network traffic originating from the corporate LAN bypasses ScanSafe scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than the ScanSafe web scanning service. Beacon Server uses a unique public/private key pair for your organization to ensure that only ScanSafe Web Security customers with the correct public key can bypass the ScanSafe scanning proxies while connected to your network. When deploying multiple instances of Beacon Server on your network, each instance must use the same private/public key pair.

AnyConnect Web Security features and functions are configured using the AnyConnect Web Security client profile which you edit using AnyConnect’s profile editor.

ScanCenter is the management portal for ScanSafe web scanning services. Some of the components created or configured using ScanCenter are also incorporated in the AnyConnect Web Security client profile.

You can begin configuring AnyConnect Web Security by Creating an AnyConnect Web Security Client Profile.

System Requirements

AnyConnect Web Security Module

Web Security module is supported on the following client operating systems:

- Windows XP SP 2: x86 (32-bit) and x64 (64-bit) operating systems.
- Windows Vista: x86 (32-bit) and x64 (64-bit) operating systems.
- Windows 7: x86 (32-bit) and x64 (64-bit) operating systems.

ASA and ASDM Requirements

The AnyConnect Secure Mobility Client with the Web security module requires these minimum ASA components:

- ASA 8.4(1)
- ASDM 6.4(0)104

Requirements for Beacon Server

Beacon Server is supported on the following operating systems:

- Windows Server 2003, x86 (32-bit)
- Windows Server 2008, x86 (32-bit)

System Limitations

Users running Web Security cannot also run Anywhere Plus. You will need to uninstall Anywhere Plus before installing Web Security.

Licensing Requirements

AnyConnect License

The Web Security module requires the AnyConnect Essentials or AnyConnect Premium license. There are no AnyConnect licenses specific to Web Security.

ScanCenter License

You need to have a ScanCenter license in order to configure the ScanSafe web scanning service.

User Guideline for Web Security Behavior with IPv6 Web Traffic

Unless an exception for an IPv6 address, domain name, address range, or wildcard is specified, IPv6 web traffic will be sent to the scanning proxy were it will perform a DNS lookup to see if there is an IPv4 address for the URL the user is trying to reach. If the scanning proxy finds an IPv4 address, it will use that for the connection. If it does not find an IPv4 address, the connection will be dropped.

If you want all IPv6 traffic to bypass the scanning proxies, you can add this static exception for all IPv6 traffic **::/0**. Doing this will make all IPv6 traffic bypass all scanning proxies. This means that IPv6 traffic will not be protected by Web Security.

Installing the AnyConnect Web Security Module

The Web Security module requires a client profile when deployed with AnyConnect or when deployed as a standalone module.

Step 1 Create a Web Security client profile by following the Creating an AnyConnect Web Security Client Profile, page 6-3 procedure.

Step 2 Read Chapter 2, "Deploying the AnyConnect Secure Mobility Client" for instructions on installing the Web Security module using web-deployment and pre-deployment methods.

Deploying Web Security Without AnyConnect

You can deploy the Web Security module as a standalone application on user computers without deploying AnyConnect VPN module.

Step 1 Create a Web Security client profile by following the Creating an AnyConnect Web Security Client Profile, page 6-3 procedure.

Step 2 Read and follow the procedures in Predeploying the AnyConnect Client and Optional Modules, page 2-25.

Creating an AnyConnect Web Security Client Profile

To create an AnyConnect Web Security client profile, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Click **Add** to create a client profile.

Step 3 Give the client profile a **name**.

Step 4 Click the **Profile Usage** field and select **Web Security**.

Step 5 Accept the default Profile Location or click **Browse** to specify an alternate file location.

Step 6 (Optional) Select a **Group Policy** to attach the client profile or leave the client profile <Unassigned>.

Step 7 Save the AnyConnect Web Security client profile.

Once you have created the AnyConnect Web Security client profile, you will need to configure these aspects of the profile:

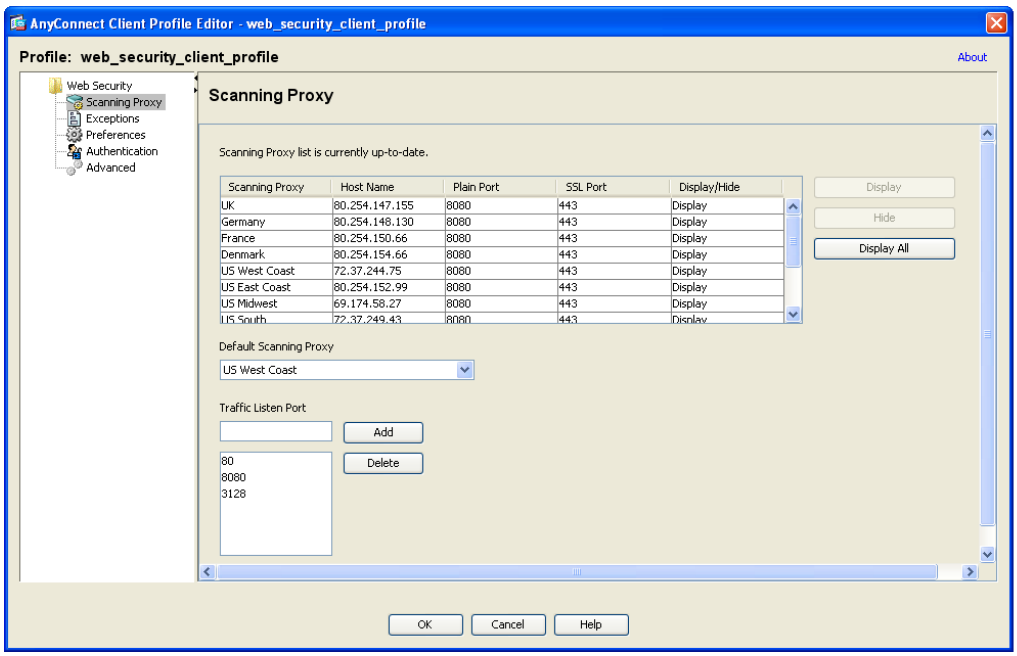
- Configuring ScanSafe Scanning Proxies in the Client Profile, page 6-4
- Excluding Endpoint Traffic from Web Scanning Service, page 6-7
- Configuring User Controls and Calculating Fastest Scanning Proxy Response Time, page 6-10
- Configuring Beacon Server Connections for Detect-On-LAN, page 6-12
- Configuring Authentication to the ScanSafe Scanning Proxy, page 6-15
- Configuring Advanced Web Security Settings, page 6-17

After you create and save the AnyConnect Web Security client profile, ASDM makes two copies of the XML file; one file is obfuscated and the other is in plain text. To learn more about these files see the "Web Security Client Profile Files" section on page 6-20.

Configuring ScanSafe Scanning Proxies in the Client Profile

The ScanSafe web scanning service analyzes Web content; it allows benign content to be delivered to your browser and blocks malicious content based on a security policy. A scanning proxy is a ScanSafe proxy server on which the ScanSafe web scanning service analyzes the Web content. The Scanning Proxy panel in the AnyConnect Web Security profile editor defines to which ScanSafe scanning proxies the AnyConnect Web Security module sends Web network traffic.

Figure 6-1 Web Security Client Profile Scanning Proxy Panel



Use these procedures to define ScanSafe scanning proxies in an AnyConnect Web Security client profile:

Updating the Scanning Proxy List

The Scanning Proxy list in the Web Security profile editor is not editable. You can not add or remove ScanCenter scanning proxies from the table in the Web Security profile editor.

Web Security profile editor updates the scanning proxy list automatically by contacting a ScanCenter website, that maintains the current list of scanning proxies, after you launch Web Security profile editor.

When you add or edit an AnyConnect Web Security client profile, profile editor compares the existing list of ScanSafe scanning proxies to those in the scanning proxy list it downloaded from the ScanSafe website. If the list is out of date, you see a message saying "Scanning Proxy list is out of date" and a command button labeled, Update List. Click the **Update List** button to update the scanning proxy list with the most recent list of ScanSafe scanning proxies.

When you click Update List, profile editor takes care to maintain as much of your existing configuration as possible. Profile editor preserves your default scanning proxy setting and the display/hide settings for the existing ScanSafe scanning proxies.

Default Scanning Proxy Settings in a Web Security Client Profile

By default, the profile you create has these ScanSafe scanning proxy attributes:

- The scanning proxy list is populated with all the ScanSafe scanning proxies your users have access to and they are all marked "Display." See "Displaying or Hiding Scanning Proxies from Users" section on page 6-5 for more information.
- A default ScanSafe scanning proxy is pre-selected. To configure the default ScanSafe scanning proxy see, "Selecting a Default Scanning Proxy" section on page 6-6.
- The list of ports on which the AnyConnect Web Security module listens for HTTP traffic is provisioned with several ports. See "Specifying an HTTP Traffic Listening Port" section on page 6-7 for more information.

Displaying or Hiding Scanning Proxies from Users

After users establish a VPN connection to the ASA, the ASA downloads a client profile to the endpoint. The AnyConnect Web Security client profile determines which ScanSafe scanning proxies are displayed to users.

Users interact with the scanning proxies marked "Display" in the scanning proxy list of the AnyConnect Web Security client profile in these ways:

- The ScanSafe scanning proxies are displayed to users in the Advanced settings of the Web Security panel of their Cisco AnyConnect Secure Mobility Client interface.
- The AnyConnect Web Security module tests ScanSafe scanning proxies marked "Display" when ordering scanning proxies by response time.

- Users can choose which ScanSafe scanning proxy they connect to if their profile allows for user control.
- ScanSafe scanning proxies marked “Hide” in the scanning proxy table of the AnyConnect Web Security client profile are not displayed to users or evaluated when ordering scanning proxies by response time. Users cannot connect to the scanning proxies marked “Hide.”

Note For the maximum benefit to roaming users, we recommend you “Display” all ScanSafe scanning proxies to all users.

To hide or display a ScanSafe scanning proxies to users, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the AnyConnect Web Security client profile you want to edit and click **Edit**. The Web Security profile editor opens and displays the Scanning Proxy panel; see Figure 6-1.

Step 3 To hide or display ScanSafe scanning proxies:

- **To hide a scanning proxy**, select the scanning proxy you want to hide and click **Hide**.
- **To display a scanning proxy,** select the name of scanning proxy you want to display and click **Display**. Displaying all ScanSafe scanning proxies is the recommended configuration.

Step 4 Save the AnyConnect Web Security client profile.

Selecting a Default Scanning Proxy

To define a default ScanSafe scanning proxy, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the AnyConnect Web Security client profile you want to edit and click **Edit**. The Web Security profile editor opens and displays the Scanning Proxy panel; see Figure 6-1.

Step 3 Select a default scanning proxy from the **Default Scanning Proxy** field.

Step 4 Save the AnyConnect Web Security client profile.

How Users Get Connected to Scanning Proxies

1. When users first connect to the network, they are routed to their default scanning proxy.
2. After that, depending on how their profile is configured, users may choose a scanning proxy or the AnyConnect Web Security module connects them to the scanning proxy with the fastest response time.
   - If their client profile allows user control, users will be able to select a scanning proxy from the Settings tab for the Cisco AnyConnect Secure Mobility Client Web Security tray.

- If their client profile has the Automatic Scanning Proxy Selection preference enabled, AnyConnect Web Security orders the scanning proxies from fastest to slowest and connects users to the scanning proxy with the fastest response time.
- If their client profile does not allow for user control but **Automatic Scanning Proxy Selection** is enabled, AnyConnect Web Security will switch users from their default scanning proxy to the scanning proxy with the fastest response time provided that the response time is 25% or more faster than the default scanning proxy to which they originally connected. (25% is the default setting and this value is configurable in the web security client profile.)
- If users start to roam away from their current scanning proxy and **Automatic Scanning Proxy Selection** is configured in their client profile, AnyConnect Web Security could switch users to a new scanning proxy provided that its response time is 25% faster than their current scanning proxy.

Users will know what scanning proxy they are connected to because AnyConnect Web Security displays the enabled scanning proxy name in the expanded AnyConnect tray icon, the Advanced Settings tab, and the Advanced Statistics tab of the AnyConnect GUI.

Specifying an HTTP Traffic Listening Port

The Scan Safe web scanning service analyzes HTTP Web traffic by default and can be configured to filter HTTPS Web traffic. In the Web Security client profile, you can specify the ports on which you want Web Security to "listen" for these types of network traffic.

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the AnyConnect Web Security client profile you want to edit and click **Edit**. The Web Security profile editor opens and displays the Scanning proxy panel; see Figure 6-1.

Step 3 In the **Traffic Listen Port** field enter the logical port number you want Web Security module to "listen" to for HTTP and HTTPS traffic.

Step 4 Save the Web Security client profile.

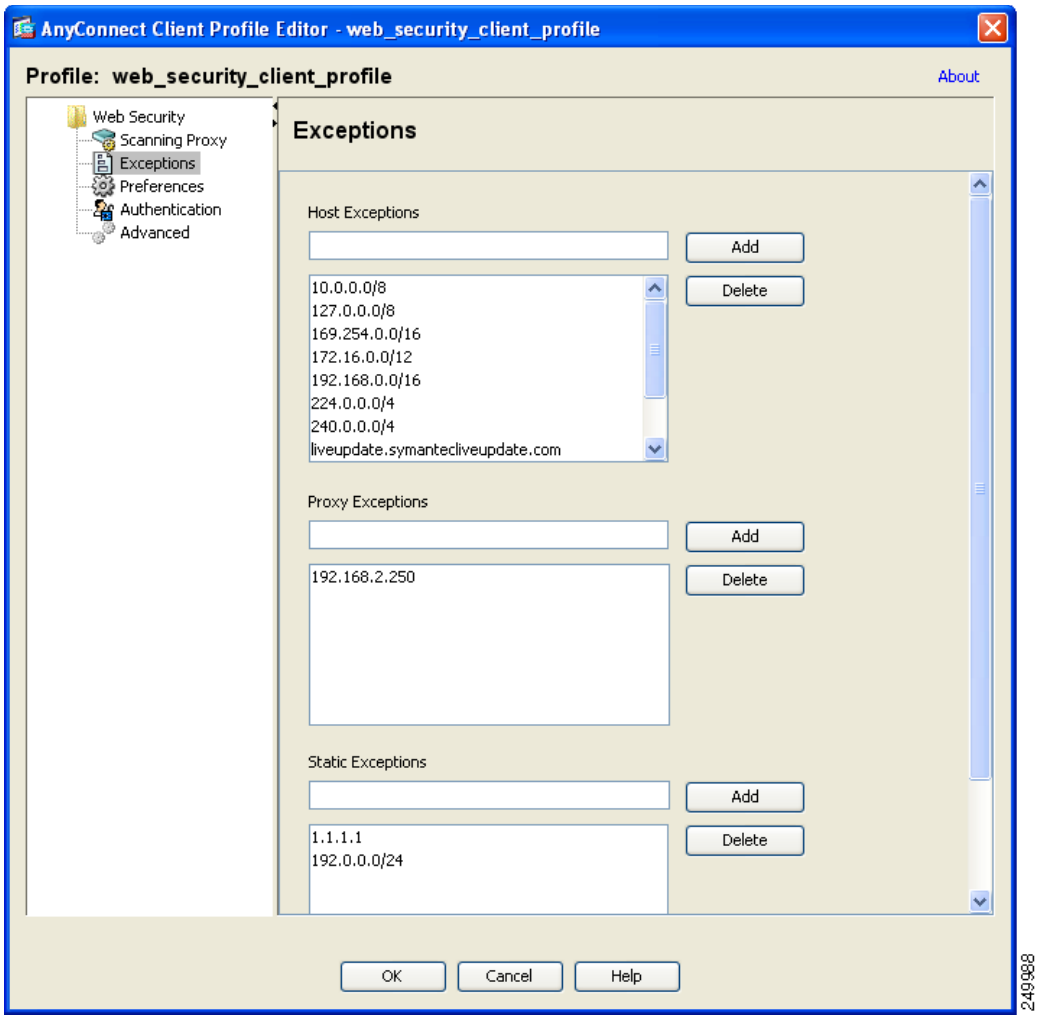
Excluding Endpoint Traffic from Web Scanning Service

If you do not want network traffic, originating from a particular IP address, to be evaluated by the ScanSafe web scanning service, you can configure an exception for that address in one of these categories:

- Host Exceptions
- Proxy Exceptions
- Static Exceptions

These exclusions are configured in the Exceptions panel of the Web Security profile editor. See Figure 6-2.

Figure 6-2 Web Security Profile Editor Exceptions Panel



Host Exceptions

In the Host Exceptions list, add internal subnets and any public websites you want to bypass the ScanSafe web scanning service. See Figure 6-2 for a picture of the Exceptions panel.

You should add any internal subnets you use that are not already included in the default, for example:

```
192.0.2.0/8
```

You should also add any internal or external websites for which you want to enable direct access. For example:

```
update.microsoft.com
*.salesforce.com
*.mycompanydomain.com
```

Also, you must add any public IP addresses you use for intranet services, otherwise you will not be able to access those intranet servers through Web Security.

All private IP addresses described RFC 1918 are included in the host exception list by default.

You can enter subnets and IP addresses using this syntax:

Syntax	Example
Individual IPv4 and IPv6 addresses	80.254.145.118 2001:0000:0234:C1AB:0000:00A0:AABC:003F
Classless Inter-Domain Routing (CIDR) notation	10.0.0.0/8 2001:DB8::/48
Fully Qualified Domain Names	windowsupdate.microsoft.com ipv6.google.com **Note** Partial domains are not supported, for example microsoft.com is not be supported.
Wildcards in fully qualified domain names or IP addresses	127.0.0.* *.cisco.com

Caution Do not use wildcards on both sides of a top level domain, for example *.cisco.*, as this could include phishing sites.

Caution Do not delete or change any of the default host exception entries.

Proxy Exceptions

In the Proxy Exceptions area, enter the IP addresses of authorized internal proxies. For example: `192.168.2.250.` See Figure 6-2 for a picture of the Exceptions panel.

You can specify IPv4 and IPv6 addresses in the field but you cannot specify a port number with them. You can specify IP addresses using CIDR notation.

This will prevent the ScanSafe web scanning service from intercepting Web data bound for these servers and tunneling the data through them using SSL. This allows proxy servers to operate without disruption. If you do not add your proxy servers here, they will see ScanSafe web scanning service traffic as SSL tunnels.

For proxies not on this list, Web Security attempts to tunnel through them using SSL, so if your users are at a different company site that requires a proxy to get out of the network for Internet access, the ScanSafe web scanning service will provide the same level of support as if they were on an open Internet connection.

Static Exceptions

Add a list of individual IP addresses or IP address ranges in Classless Inter-Domain Routing (CIDR) notation for which traffic should bypass the ScanSafe web scanning service. In the list, include the ingress IP addresses of your VPN gateways. See Figure 6-2.

You can specify IPv4 and IPv6 addresses or ranges of addresses using CIDR notation. You cannot specify fully qualified domain names or use wildcards in IP addresses. These are examples of correct syntax:

```
1.1.1.1
192.0.2.0/24
```

Caution Do not change or delete the default IP address entry, 1.1.1.1.

Note Make sure to add the IP addresses of your SSL VPN concentrators to the static exclusion list.

User Guideline for IPv6 Web Traffic

Unless an exception for an IPv6 address, domain name, address range, or wildcard is specified, IPv6 web traffic will be sent to the scanning proxy were it will perform a DNS lookup to see if there is an IPv4 address for the URL the user is trying to reach. If the scanning proxy finds an IPv4 address, it will use that for the connection. If it does not find an IPv4 address, the connection will be dropped.

If you want all IPv6 traffic to bypass the scanning proxies, you can add this static exception for all IPv6 traffic **::/0**. Doing this will make all IPv6 traffic bypass all scanning proxies. This means that IPv6 traffic will not be protected by Web Security.

Configuring Web Scanning Service Preferences

Use this panel to configure these preferences:

- Configuring User Controls and Calculating Fastest Scanning Proxy Response Time, page 6-10
- Configuring Beacon Server Connections for Detect-On-LAN, page 6-12

Configuring User Controls and Calculating Fastest Scanning Proxy Response Time

To allow users to choose the ScanSafe scanning proxy they connect to, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.**

Step 2 Select the Web Security client profile you wish to edit and click **Edit**.

Step 3 Click **Preferences**. See Figure 6-3 for an illustration of the fields you configure in this procedure.

Step 4 Check **User Controllable**. (This is the default setting.) User Controllable determines if the User is allowed to change the Automatic Tower Selection and Order Scanning Proxies by Response Time settings in the AnyConnect interface.

Step 5 If you would like Web Security to automatically select a scanning proxy, check **Automatic Scanning Proxy Selection**. If you do this, **Order Scanning Proxies by Response Time** is checked automatically.

- If you select **Automatic Scanning Proxy Selection**, Web Security determines which scanning proxy has the fastest response time and automatically connects the user to that scanning proxy.

- If you do not select **Automatic Scanning Proxy Selection**, and you still have **Order Scanning Proxies by Response Time** is selected, users will be presented with a list of scanning proxies, to which they can connect, ordered from fastest to slowest response time.

Note When you enable Automatic Scanning Proxy Selection, transient communications interruptions and failures can cause the active scanning proxy selection to change automatically. Changing the scanning proxy can sometimes be undesirable, as it can cause unexpected behavior such as returning search results from a scanning proxy in a different country using a different language.

Step 6 If you checked **Order Scanning Proxies by Response Time,** configure these settings for calculating which scanning proxy has the fastest response time.

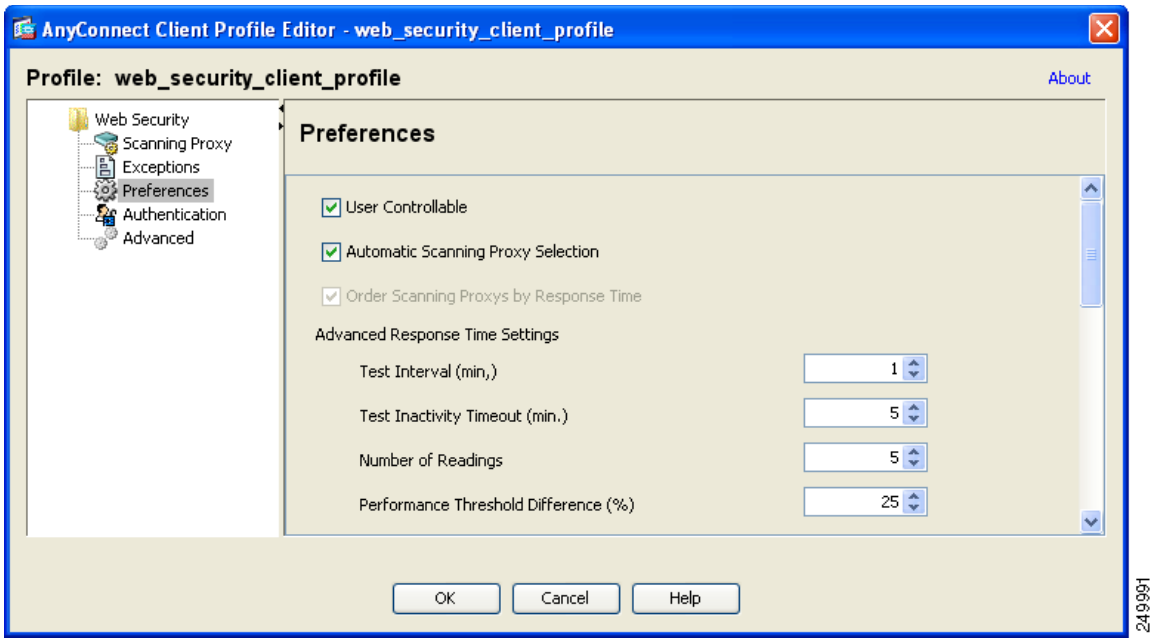
- **Test Interval**: The time, in minutes, between running each performance test. You should not change this setting unless instructed to do so by customer support.
- **Test Inactivity Timeout**: The time, in minutes, after which Web Security suspends the response time test because of user inactivity. Web Security resumes the testing as soon as scanning proxies encounter connection attempts. You should not change this setting unless instructed to do so by customer support.
- **Number of Readings**: The number of tests to perform before switching to a ScanSafe scanning proxy with a faster test response time. You should not change this setting unless instructed to do so by customer support.
- P**erformance Threshold Difference**: The percentage faster than the current scanning proxy that an alternate proxy must be before switching. The default is 25%.

Note The **Ordering Scanning Proxies by Response Time** test runs continuously, based on the Test Interval time, with these exceptions:

- “Detect-On-LAN” is enabled and Beacon Server has detected that the machine is on the Corporate LAN.
- The Web Security license key is missing or invalid.
- The user is inactive for a configured amount of time and, as a result, the Test Inactivity Timeout threshold has been met.

Step 7 Save the Web Security client profile.

Figure 6-3 User Controls and Order Scanning Proxies by Response Time Controls



Configuring Beacon Server Connections for Detect-On-LAN

The Detect-On-LAN feature detects when an endpoint is on the corporate LAN, either physically or by means of a VPN connection. If the Detect-On-LAN feature is enabled, any network traffic originating from the corporate LAN bypasses ScanSafe scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than the ScanSafe web scanning service.

Beacon Server uses a unique public/private key pair for your organization to ensure that only ScanSafe Web Security customers with the correct public key can bypass the ScanSafe scanning proxies while connected to your network. When deploying multiple instances of Beacon Server on your network, each instance must use the same private/public key pair.

Note If you choose not to use Beacon Server and you have any proxies on your network, for example ScanSafe Connector, you must add each proxy to the list of proxy exceptions in the Exceptions panel in profile editor. See Proxy Exceptions, page 6-9.

Follow this procedure to configure Web Security's interaction with Beacon Server:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Edit**.

Step 3 Click **Preferences**. See Figure 6-4 for a picture of the Preferences panel.

Step 4 If you have installed Beacon Server on your network and you have configured it to receive traffic from Web Security users, check **Beacon Check**.

Step 5 In the **Public Key File** field, click **Browse** and select your company's public key certificate. Beacon Server uses RSA public/private key pairs for authentication. Private keys must be a minimum of 512 bits in length; however, Cisco recommends using keys of 1,024 bits.

Step 6 In the **New Beacon Address** field, identify the computer where Beacon Server is installed. Use either a valid IP address or domain name. Here are examples of proper syntax:

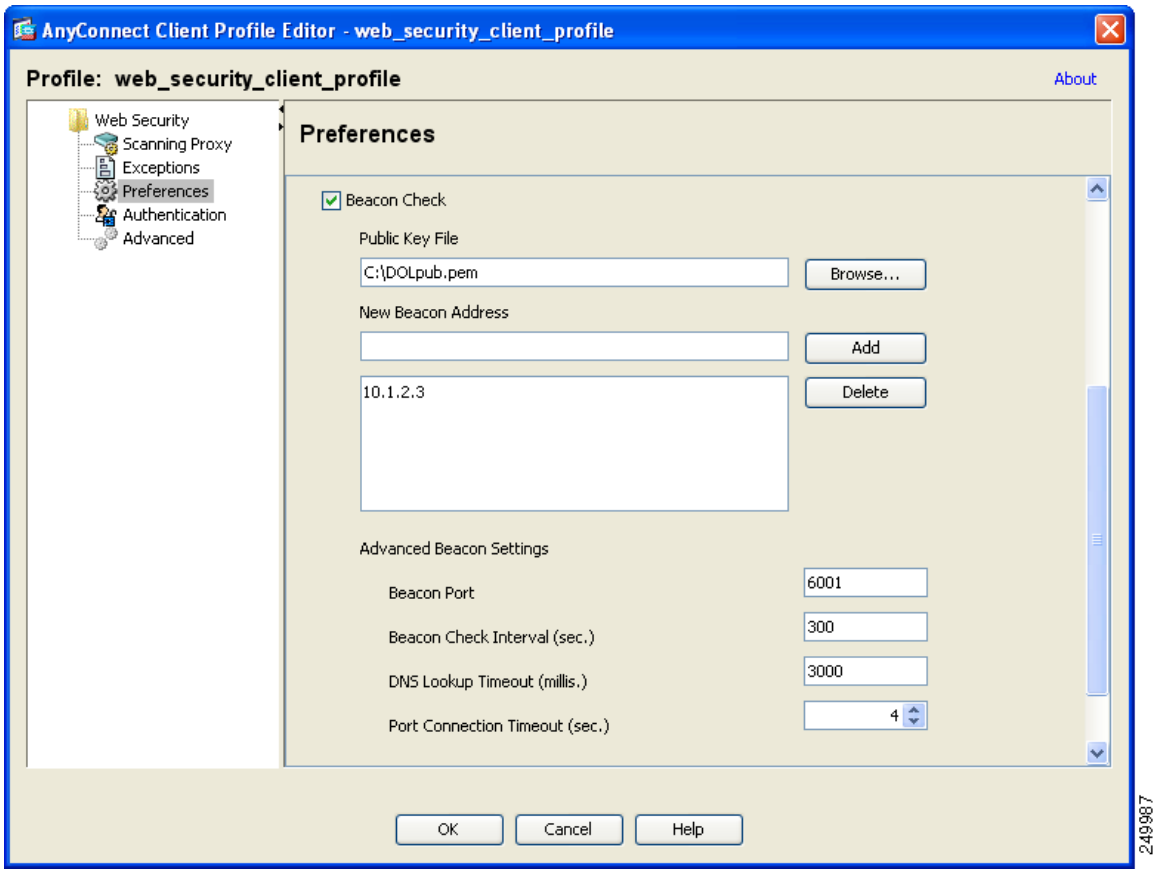
Syntax	Example
Individual IPv4 addresses	`10.10.10.123`
Fully Qualified Domain Names	`beaconserver.cisco.com` **Note** Partial domains are not supported, for example cisco.com would not be supported.

Step 7 Configure these Advanced Beacon Settings

- **Beacon Port**: This element specifies the TCP/IP port used by the service. If you already have a service running on port 6001, you can change this element. You will also need to change the corresponding element in the websecurity.config file on the computer where Beacon Server is installed.
- **Beacon Check Interval:** Web Security will wait this time, specified in seconds, in between attempts to contact Beacon Server and thus determine if it is on a LAN.
- **DNS Lookup Timeout:** Timeout, in milliseconds, for DNS lookups on the hostnames (if any) provided in the <Beacons> setting. You should not change this setting unless instructed to do so by customer support.
- **Port Connection Timeout**: This element specifies the time, in seconds, after which a connection that is not sending any data to Beacon Server will be closed. You should not change this setting unless instructed to do so by customer support.

Step 8 Save the Web Security client profile.

Figure 6-4 Beacon Server Check Configuration



Configuring Detect-On-LAN

The Detect-On-LAN feature detects when an endpoint is on the corporate LAN, either physically or through a VPN connection. If the Detect-On-LAN feature is enabled, any network traffic originating from the corporate LAN bypasses ScanSafe scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than the ScanSafe web scanning service.

Beacon Server uses a unique public/private key pair for your organization to ensure that only Web Security clients with the correct public key can bypass the scanning proxies while connected to your network.You can also deploy multiple copies of Beacon Server if required, providing they use the same private/public key pair. You generate the private/public key pair on the ScanCenter portal.

If you choose not to use Beacon Server and you have any proxies on your network, for example ScanSafe Connector, you must add each proxy to the list of proxy exceptions in the Exceptions panel in profile editor. See Proxy Exceptions, page 6-9 for more information.

Configuring Detect-On-LAN is also required for some third-party solutions, such as data loss prevention (DLP) appliances, that require traffic to be unaffected by Web Security.

To configure the Detect On LAN feature, follow this procedure:

Step 1 Install one or more copies of Beacon Server on your network. Use Chapter 3, "Beacon Server" of the *Anywhere Plus Administrator Guide, Release 1.2* for instructions on how to create your public/private key pair and include that pair with your Beacon Server installation.

Note Beacon Server must be accessible to all Web Security installations that are brought into the corporate LAN physically and to those connected over a full tunnel VPN.

Step 2 Create a Web Security client profile using the "Creating an AnyConnect Web Security Client Profile" section on page 6-3. Ensure that the client profile specifies the group policy you want to deploy to your AnyConnect users.

Step 3 Using the "Configuring Beacon Server Connections for Detect-On-LAN" section on page 6-12, configure these settings in the Preferences Panel of the Web Security client profile:

- Check **Beacon Check** to enable it.
- In the Public Key File field, point to the public key file (DOLpub.pem) you created as part of your public/private key pair.
- Add the IP addresses of each instance of Beacon Server to the **New Beacon Address** field.

Step 4 Configure and save the remainder of the Web Security client profile.

Step 5 To receive this Web Security client profile with the Detect-On-LAN feature configured, users must select the name of this client profile, in the VPN combo box of the AnyConnect Secure Mobility Client, when they attempt to establish a VPN connection to the ASA.

Configuring Authentication to the ScanSafe Scanning Proxy

Follow this procedure to configure authentication to the ScanSafe scanning proxies:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Edit**.

Step 3 Click **Authentication**. See Figure 6-5 for an illustration of the fields you configure in this procedure.

Step 4 In the **Proxy Authentication License Key** field, enter the license key that corresponds to the company key, group key, or user key you created in ScanCenter. If you are going to authenticate users based on their Enterprise domain, enter the company key you created. If you are going to authenticate users based on their ScanCenter or Active Directory group, enter the group key you created. By default the tag is empty. If it is left empty, Web Security operates in pass-through mode.

Step 5 Enter a **Service Password**. The default password for Web Security is **websecurity**. You can change this password when customizing the profile. The password must contain only alphanumeric characters (a-z, A-Z, 0-9) as other characters may be mistaken for control characters by the Windows command shell or may have special meaning in XML. With this password a user with non-administrator privileges can start and stop the Web Security service. Users with administrator privileges can start and stop the Web Security service without this password. See the "Stopping and Starting the Cisco AnyConnect Web Security Agent" section on page 6-22 for more information.

Step 6 Choose to authenticate users by domain names, groups and users, groups, or user name specified in ScanCenter or Active Directory.

- Click the **Use Enterprise Domains** radio button to enter the domain names from which HTTP and HTTPS traffic is going to be sent to the ScanSafe web scanning service. If the domain to which the user belongs is found in this list, AnyConnect Web Security module determines the user and group information to include in the headers when passing traffic up to the scanning proxies.

  Enter the domain names in NetBIOS format. For example the NetBIOS format of **sanjose.cisco.com** is **cisco**. Do not enter domain names using the DNS format: **abc.def.com**.

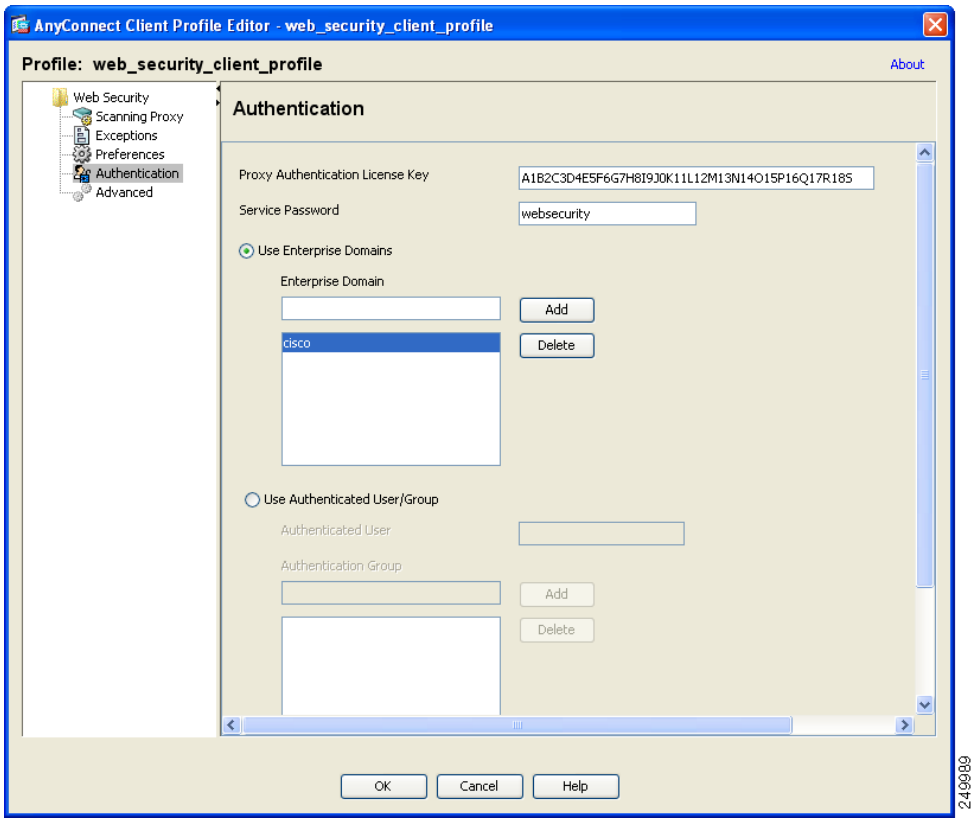
  If you specify a domain name in the Enterprise Domain name field, then ScanCenter identifies the currently logged-in Active Directory user and enumerates that user's Active Directory groups and that information gets sent to the scanning proxy with every request.

- Click the **Use Authenticated User/Group** radio button to authenticate users by username, group, or username and group.
  - In the **Authenticated User** field, enter the ScanCenter or Active Directory domain user name. The syntax for adding users from active directory is as follows: WinNT://[domain-name]\[user-name].
  - In the **Authentication Group** field, enter a group name of up to 256 alphanumeric characters.

Note Performing authentication using a company key and enterprise domains is useful for a web security client profiles you intend to deploy to many users throughout your organization. Performing authentication using username or username and group is useful when testing a new web security client profile on a small group of users.

Step 7 Save the Web Security client profile.

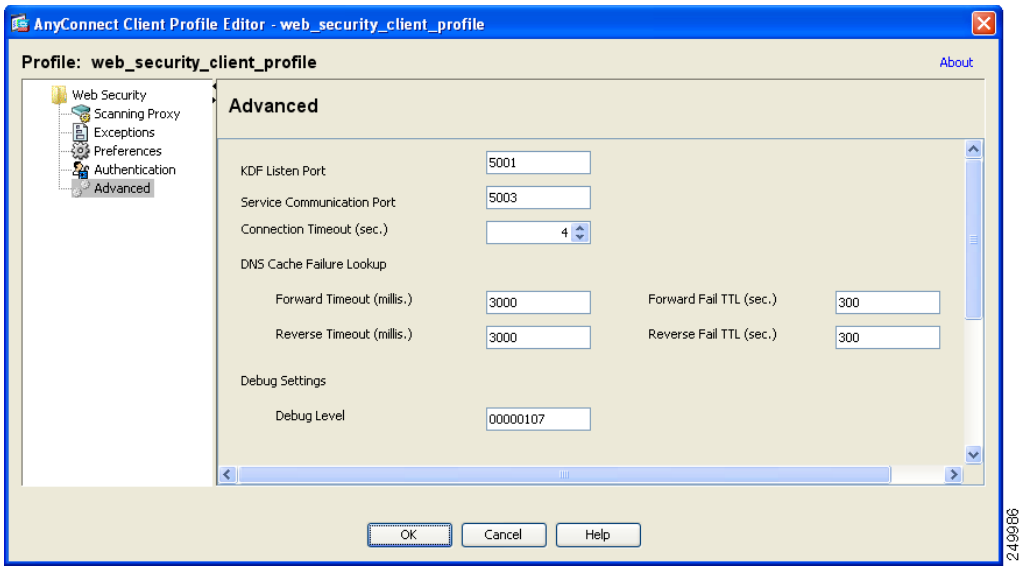
Figure 6-5 Configuring ScanSafe Scanning Proxy Authentication



Configuring Advanced Web Security Settings

The Advanced panel of a web security client profile exposes several settings that may help Cisco customer support engineers troubleshoot problems. You should not change the setting on this panel unless you are instructed to do so by customer support.

Figure 6-6 Web Security Client Profile Advanced Panel



From the Advanced panel in profile editor, you can perform these tasks:

- Configuring KDF Listening Port, page 6-18
- Configuring Service Communication Port, page 6-19
- Configuring Connection Timeout, page 6-19
- Configuring DNS Cache Failure Lookup, page 6-19
- Configuring Debug Settings, page 6-19

Configuring KDF Listening Port

The Kernel Driver Framework (KDF) intercepts all connections which use one of the Traffic Listening Ports as their destination port and forwards the traffic to the KDF Listening Port. The web scanning service analyzes all the traffic forwarded to the KDF Listening Port.

You should not change this setting unless instructed to do so by customer support.

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Edit**. Click **Advanced** in the Web Security tree pane. See Figure 6-6 for an illustration of the **Advanced** panel in the Web Security profile editor.

Step 3 Specify the KDF Listen Port in the **KDF Listen Port** field.

Step 4 Save the Web Security client profile.

Configuring Service Communication Port

The Service Communication Port is the port on which the web scanning service listens for incoming connections from the AnyConnect GUI component, and some other utility components. You should not change this setting unless instructed to do so by customer support.

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Edit**. Click **Advanced** in the Web Security tree pane. See Figure 6-6 for an illustration of the **Advanced** panel in the Web Security profile editor.

Step 3 Edit the **Service Communication Port** field.

Step 4 Save the Web Security client profile.

Configuring Connection Timeout

The connection timeout setting enables you to set the time-out before Web Security tries to go direct to the Internet without using the scanning proxies. If left blank, it will use the default value of four seconds. This allows users to get access to paid network services faster as they will not have to wait so long for the time-out to happen before retrying.

Follow this procedure to configure the Connection Timeout field:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Edit**. Click **Advanced** in the Web Security tree pane. See Figure 6-6 for an illustration of the **Advanced** panel in the Web Security profile editor.

Step 3 Change the **Connection Timeout** field.

Step 4 Save the Web Security client profile.

Configuring DNS Cache Failure Lookup

In the Advanced panel of profile editor you will see several fields for managing Domain Name Server lookups. These settings have been configured with optimal values for DNS lookups. You should not change this setting unless instructed to do so by customer support.

Configuring Debug Settings

The Debug Level is a configurable field; however, you should not change this setting unless instructed to do so by customer support.

Web Security Logging

All Web Security messages are recorded in the Windows Event Viewer in the **Event Viewer (Local)\Cisco AnyConect Web Security Module** directory. The events Web Security records in the event viewer are intended to be analyzed by Cisco Technical Assistance Center engineers.

Web Security Client Profile Files

After you create and save the Web Security client profile using the profile editor bundled with AnyConnect, profile editor makes two copies of the XML file; one file is obfuscated and has the file naming convention *filename*.wso; the other is in plain text and has the file naming convention *filename*.wsp.

After you create and save the Web Security client profile using the standalone profile editor, the plain text version of the client profile has the file naming convention *filename*.xml and the obfuscated file naming convention is *filename*.wso.

Having these two formats allows administrators to perform this special processing if needed:

- Administrators can export the obfuscated Web Security client profile from the ASA and can distribute it to endpoint devices.
- Administrators can edit the plain text Web Security client profile and perform edits that are not supported by the AnyConnect Web Security profile editor. You should not change the plain text version of the Web Security client profile unless instructed to do so by customer support.

Exporting the Plain Text Web Security Client Profile File

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Export**.

Step 3 Browse to a local directory in which to save the file. Editing the file name in the Local Path field will save the Web Security client profile with that new file name.

Step 4 Click **Export**. ASDM exports the plain text *filename*.wsp version of the web security client profile.

Exporting the Plain Text Web Security Client Profile File for DART Bundle

If you need to send a Diagnostic AnyConnect Reporting Tool (DART) bundle to Cisco customer service, you need to send the plain text version of the Web Security client profile file, *filename*.wsp or *filename*.xml, along with the DART bundle. Cisco Customer service will not be able to read the obfuscated version.

To gather the plain text version of the Web Security client profile created by the profile editor on ASDM, use the Exporting the Plain Text Web Security Client Profile File procedure.

The standalone version of Profile editor creates two versions of the Web Security profile file; one file is obfuscated and has the file naming convention *filename*.wso and the other is in plain text and has the file naming convention *filename*.xml. Gather the plain text version of the file, *filename*.xml.

Before sending the DART bundle to Cisco customer service, add the plain text version of your Web Security client profile to the DART bundle.

Editing and Importing Plain Text Web Security Client Profile Files from ASDM

Once you have exported the plain text Web Security client profile file, you can edit it on your local computer using any plain text or XML editor. Use this procedure to import it.

Caution Importing the file **overwrites** the contents of the Web Security client profile you selected.

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Export**.

Step 3 After making the changes to the *filename*.wsp file, return to the AnyConnect Client Profile page and select the Profile Name of the file that you edited.

Step 4 Click **Import**.

Step 5 Browse to the edited version of the Web Security client profile and click **Import**.

Exporting the Obfuscated Web Security Client Profile File

Step 1 Open ASDM and choose **Tools > File Management**.

Step 2 In the File Management screen click **File Transfer > Between Local PC and Flash** and use the File Transfer dialog to transfer the obfuscated *filename*.wso client profile file to your local computer.

Installing a Standalone Web Security Client Profile

Use the standalone profile editor to create a Web Security client profile when you do not have an ASA.

Step 1 Open the Web Security Standalone Profile Editor by choosing **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.

Step 2 Create a Web Security client profile using the "Creating an AnyConnect Web Security Client Profile" section on page 6-3.

Step 3 Save the Web Security client profile by choosing **File > Save**. The standalone profile editor makes two copies of the XML file; one file is obfuscated and has the file naming convention *filename*.wso; the other is in plain text and has the file naming convention *filename*.xml.

Step 4 Rename or save the obfuscated *filename*.wso client profile file with the name **WebSecurity_ServiceProfile.xml** to one of these directories:

- For Windows XP users, put the file in this directory: **%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security**

- For Windows Vista and Windows 7 users, put the file in the this directory: **%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security** directory.

Step 5 Restart the Cisco AnyConnect Web Security Agent windows service from the Windows **Services** dialog box or by opening a command prompt and entering **net stop acwebsecagent** and then **net start acwebsecagent**.

Configuring Split-Tunneling for Web Security Traffic

Web Security and VPN can be used simultaneously. For optimal performance in this configuration, it is recommended that the IP address to ScanSafe scanning proxies are excluded from the tunnel.

No other Split Exclusion needs to be configured as all decisions as to what traffic is sent to the ScanSafe scanning proxies is determined by the Web Security configuration.

To obtain a list of ScanSafe Scanning Proxy IP Addresses, please refer to the following live document which contains the list of addresses:

http://80.254.145.118/websecurity-config-v2ip.xml

If you use the Detect On LAN feature and want to ensure that Web Security and VPN are active at the same time, configure your network so that Beacon Server is not reachable over the VPN Tunnel. In this way, the Web Security functionality will go into bypass mode, only when the user is on the corporate LAN.

Stopping and Starting the Cisco AnyConnect Web Security Agent

Users without local administrator privileges cannot start and stop the Cisco AnyConnect Web Security Agent Windows service without using the service password defined in the Authentication panel of the Web Security profile editor.

Lockdown Option

Cisco recommends that end users are given limited rights on the device hosting the AnyConnect Secure Mobility client. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users from disabling or stopping those Windows services established as locked down on the endpoint.

Each MSI installer supports a common property (lockdown) which, when set to a non-zero value, prevents the Windows service(s) associated with that installer from being controlled by users on the endpoint device. We recommend that you use the sample transform provided at the time of install to set this property and apply the transform to each MSI installer that you want to have locked down.

If you deploy the core client plus one or more optional modules, you need to apply the lockdown property to each of the installers. This operation is one way only and cannot be removed unless you re-install the product.

Non-Administrators Stopping and Starting the Web Security Agent Service

The service password used in this procedure is configured in the Authentication panel of the Web Security profile editor.

Step 1 Open a command prompt window.

Step 2 Change to the **%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** directory.

Step 3 Start or stop the Web Security agent:

- To start the Web Security agent, at the prompt enter
  acwebsecagent.exe -enablesvc -*servicepassword*
- To stop the Web Security agent, at the prompt enter
  acwebsecagent.exe -disablesvc -*servicepassword*

CHAPTER 7

Configuring AnyConnect Telemetry to the WSA

The AnyConnect telemetry module for AnyConnect Secure Mobility Client sends information about the origin of malicious content to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA). The web filtering infrastructure uses this data to strengthen its web security scanning algorithms, improve the accuracy of the URL categories and web reputation database, and ultimately provide better URL filtering rules.

The AnyConnect telemetry module performs these functions:

- Monitors the arrival of content on the endpoint.
- Identifies and records the origin of any content received by the endpoint whenever possible.
- Reports detection of malicious content, and its origin, of malicious content to Cisco's Threat Operations Center.
- Checks the ASA every 24 hours for an updated Host Scan image. If there is an updated Host Scan image available it pulls down the image to the endpoint.

These are the topics covered in this chapter:

System Requirements

The AnyConnect telemetry module, hereafter "telemetry module," is available for this release of AnyConnect Secure Mobility Client running on these platforms:

- Windows 7 (x86 (32-bit) and x64 (64-bit))
- Windows Vista with SP2 (x86 (32-bit) and x64 (64-bit))
- Windows XP SP3 (x86 (32-bit) and x64 (64-bit))

The AnyConnect telemetry module, hereafter "telemetry module," is available for this release of AnyConnect Secure Mobility Client running on these x86 (32-bit) and x64 (64-bit) Windows platforms only: Windows XP, Windows Vista, and Windows 7.

The telemetry module can only perform URL origin-tracing for browsers that use **wininit.dll**, such as Internet Explorer 7 and Internet Explorer 8. If you download a file using a browser which does not use **wininit.dll**, such as Firefox or Chrome, we can only identify the browser used to download the file. We cannot identify the URL from which the file was downloaded.

The telemetry module requires that an antivirus application, which the AnyConnect posture module supports, be installed on the endpoint.

Note The AnyConnect posture module contains the same Host Scan image as the one delivered with CSD. The list of antivirus, antispyware, and firewall applications supported by Host Scan is the same for AnyConnect and CSD.

ASA and ASDM Requirements

The AnyConnect Secure Mobility Client with the telemetry module requires these minimum ASA components:

- ASA 8.4
- ASDM is 6.3.1

AnyConnect Secure Mobility Client Module Requirements

The telemetry module is an add-on of AnyConnect Secure Mobility Client and it requires these modules to be installed on the endpoint in this order:

1. AnyConnect VPN Module
2. AnyConnect Posture Module
3. AnyConnect Telemetry Module

Requirements for Cisco IronPort Web Security Appliance Interoperability

You can only enable the telemetry feature if you are using the AnyConnect Secure Mobility solution with the Cisco IronPort Web Security Appliance (WSA) which requires a WSA Secure Mobility Solution license. The minimum required version of the WSA is 7.1.

The AnyConnect Telemetry functionality requires the Secure Mobility Solution to be properly configured. If you have not done so already, please see the "Configuring the ASA for WSA Support of the AnyConnect Secure Mobility Solution" section on page 2-43 and follow the directions to configure the ASA to work properly with the WSA.

Enable SenderBase on Cisco IronPort Web Security Appliance

The telemetry module sends virus attack incident and activity information to the WSA so that it can be forwarded to the Threat Operations Center and aggregated with other threat information. The WSA must have SenderBase network participation enabled in Standard mode for this to happen.

This is an outline of the procedure to enable the SenderBase Security Service. Consult your WSA documentation for a full description of the SenderBase Security Service.

1. Use a web browser to log into the WSA administrator GUI.
2. Select **Security Services > SenderBase.**
3. If SenderBase network participation is disabled, click **Enable**, and then click **Edit Global Settings** to configure the participation level. Cisco recommends Standard (full) participation.

Note For more information on the difference between Limited and Standard participation levels, see the *IronPort AsyncOS for Web User Guide*.

4. Submit and commit your changes.

Installing the AnyConnect Telemetry Module

You need to install the AnyConnect Secure Mobility Client and AnyConnect posture module on the endpoint before you install the telemetry module. See Chapter 2, "Deploying the AnyConnect Secure Mobility Client" for instructions on installing the telemetry module using web-deployment and pre-deployment methods. If you would like to read just the basics about deploying the telemetry module, see Quick-Deploy of the AnyConnect Telemetry Module.

Once you install the telemetry module, it immediately begins to record the actions of any new processes that start; however, the telemetry module cannot record the actions of processes that were running on the computer before you installed it.

After you install the telemetry module, it does not track processes of Windows Explorer (explorer.exe), including file copies and renames, until the user logs out and logs back in. In addition, the telemetry module cannot record the actions of other processes that start before the user logs in until after the user reboots the computer.

Note Though it is not a requirement, we highly recommend that you reboot the endpoint after you install the telemetry module.

Quick-Deploy of the AnyConnect Telemetry Module

Here is a summary of the procedure you need to perform to deploy the telemetry module with AnyConnect. This procedure assumes that you have already configured group policies and connection profiles for your AnyConnect VPN users. To deploy the AnyConnect telemetry module, use the following procedure.

Step 1 Download the AnyConnect Windows package from Cisco.com. The file has this naming convention: anyconnect-win-<*version*>-k9.pkg.

Step 2 Upload the AnyConnect Windows package to the ASA:

a. Lunch ASDM and select - **Configuration > Remote Access VPN > Network(Client) Access > AnyConnect Client Settings**.

b. Click **Add**.

c. **Upload** the AnyConnect Windows package to ASDM. When prompted, click **OK**, to use the AnyConnect package as your new current image.

d. Click **OK**. Click **Apply**.

e. Restart **ASDM**.

Step 3 Designate the AnyConnect package as the Host Scan package and enable Host Scan:

a. In ASDM select **Configuration > Remote Access VPN > Host Scan Image.**

b. Click **Browse Flash** and select the anyconnect-win-<*version*>-k9.pkg you uploaded in the previous step as the Host Scan Image.

c. Check **Enable Host Scan/CSD**.

d. Click **Apply**.

e. Restart **ASDM**.

Note This step also results in enabling Host Scan for Clientless SSL VPN Access.

Step 4 Configure a group policy to deploy telemetry as an optional module:

a. In ASDM select **Configuration > Remote Access VPN > Network(Client) Access > Group Policies**, select the group policy you want to edit and click **Edit**.

b. Select **Advanced > AnyConnect Client**.

c. Uncheck the Optional Client Modules to Download **Inherit** check box. From the drop down box, select **AnyConnect Telemetry** and **AnyConnect Posture**.

d. Click **OK**. Click **Apply**. Click **Save**.

Step 5 Configure a connection profile to specify the group policy you just configured.

a. In ASDM select **Configuration > Remote Access VPN > Network(Client) Access > AnyConnect Connection Profiles** and select the connection profile you want to configure for telemetry. Click **Edit**. The **Basic** configuration panel opens automatically.

b. In the Default Group Policy area, choose the group policy, from the previous step, that you configured to deploy telemetry.

c. Click **OK**. Click **Apply**. Click **Save**.

Step 6 Create a telemetry client profile and enable telemetry:

a. In ASDM select **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profiles**.

b. Click **Add** to create a telemetry profile. Give the profile a name and select Telemetry in the Profile Usage field.

c. In the Group Policy field, select the group policy you created to deploy telemetry as an optional module. Click **OK**.

d. From the list of Profile Names, select the telemetry client profile you just created and click **Edit**.

e. Click **Enable Service** in the Telemetry Policy panel and accept all the default values for the telemetry client profile.

f. Click **OK**. Click **Apply**. Click **Save**.

Step 7 Enable the Secure Mobility Solution:

a. In ASDM select **Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution**.

b. In the Service Setup area, check **Enable Mobile User Security Service**.

c. Click **Apply**. Click **Save**.

AnyConnect Telemetry Module Interoperability

This section describes the telemetry module's interaction with other AnyConnect Secure Mobility client components:

- AnyConnect VPN Module
- AnyConnect Posture Module
- Third-Party Antivirus Software

AnyConnect VPN Module

The AnyConnect VPN module interacts with the telemetry module in these ways:

- AnyConnect's VPN service process loads and initializes the telemetry module at service starting time along with all other plug-in modules.
- The AnyConnect VPN module provides session state and AnyConnect Secure Mobility (ACSM) state information when the states have changed.
- The AnyConnect VPN module provides the XML of the secure mobility service status response from the WSA in order to get the telemetry settings from WSA.

Other than this, the telemetry module has little interaction with the VPN module and runs independently until the VPN module shuts it down or until the VPN process terminates.

AnyConnect Posture Module

The AnyConect posture module, hereafter "posture module," contains the Host Scan image. The Host Scan image passes virus detection information from the Host Scan-compatible antivirus software to the telemetry module. Host Scan can also pass system posture information to the AnyConnect telemetry module if it is needed for the telemetry report.

The telemetry module checks the ASA for an updated Host Scan image every 24 hours. If there is a an updated Host Scan image installed on the ASA, the telemetry module pulls down the image and installs the update to the endpoint automatically.

Third-Party Antivirus Software

The AnyConnect telemetry module needs a Host Scan-compliant antivirus application to detect viruses and malware. Host Scan checks the antivirus application's threat log periodically and forwards the virus detection incidents to the telemetry module.

The threat log of the antivirus application should always be enabled, otherwise Host Scan can not trigger telemetry reporting.

Telemetry Activity History Repository

The telemetry activity history repository is a directory on the endpoint in which the telemetry module stores activity files. This is the location of the activity history repository:

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Telemetry\data\

The telemetry module intercepts system operations, user operations, and API function calls, which it can use to identify the origin of the content coming into the endpoint. It aggregates this information into application activities, such as the download of a file from a URL by Internet Explorer (iexplorer.exe) or the copying of a file from a removable device by Windows Explorer (explorer.exe).

The telemetry module gathers this activity and records it in the activity.dat file. The activity.dat file is the activity history file.

When the activity.dat file reaches the size of approximately 1MB, the telemetry module saves the current activity.dat file as a new file named with the timestamp of when it was saved; for example, 20110114111312430.dat. The telemetry module then creates a new activity.dat file where it continues to store the latest activity history. Figure 7-1 shows the contents of a renamed activity.dat file.

When the activity history repository reaches a certain size, the telemetry module deletes the oldest activity history files. The activity history repository size is governed by the **Maximum History Log** variable configured in the Telemetry Profile. When activity history files reach a certain age, the telemetry module deletes them from the activity history repository. Activity history file age is defined by the **Maximum History (Days)** variable configured in the Telemetry Profile. See **"Configuring the Telemetry Client Profile" section on page 7-12** for instructions on how to configure these variables.

Note The telemetry module receives its activity information from Windows functions such as winnit.dll and Kerel32.dll. If a browser or an email application does not use these functions, the telemetry module does not receive any activity data. This is why the telemetry module does not receive activity history from such browsers as Firefox and Chrome.

Note URLs stored in the activity history repository are considered sensitive information. The telemetry module encrypts these URLs to prevent unauthorized access. See the "URL Encryption" section on page 7-11 for more information.

Telemetry Reports

Telemetry reports contain information about viruses identified by local antivirus software and the action the antivirus software took to protect the endpoint from the virus. The telemetry module encrypts the reports and sends them to the WSA which forwards them to the Cisco Threat Operations Center (TOC). The TOC combines these reports with others and produces new URL filter and malware filter engine updates which it distributes to all WSAs.

Each telemetry report has an incident section followed by one or more activity sections. The incident section contains information about the malware, the local antivirus application, the action it took to defend against the malware, and system information about the endpoint. The activity sections contain information about the activities leading to the incident and possible origins of the virus.

When the endpoint is connected to the ASA through a virtual private network, the telemetry module sends the report to the WSA, by way of the ASA, immediately. After the telemetry module sends the reports to the WSA, it deletes the local copy.

If the endpoint is not connected to the ASA by a VPN, the telemetry module stores the reports on the endpoint here:

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Telemetry\reports\

The Telemetry report filenames use the naming convention: **YYYYMMDDHHSSmmm.trt** which reflects the year, month, day, hour, minute, second, and hundredths of a second at which the report was created.

Note URLs stored in the telemetry reports are considered sensitive information. The telemetry module encrypts these URLs to prevent unauthorized access. See the "URL Encryption" section on page 7-11 for more information.

Possible Transference of Personal Information by Telemetry Module

The Telemetry incident reports contain the name of the malware and also the location of the malware detected on the local system. This location, the directory path, often contains the user ID of the person who downloaded the malware. For example, if Jonathan Doe downloaded "malware.txt," the directory name that could be included in the telemetry report might be "C:\Documents and Settings**jdoe**\Local Settings\Temp\Cookies**jdoe**@malware[1].txt".

Note If you agree to the Cisco End User License Agreement and install the telemetry module, you consent to Cisco's collection, use, processing and storage of personal information and non-personal information. This personal information and non-personal information is transferred to Cisco, including the transfer of such information to the United States and/or another country outside the European Economic Area, so Cisco can determine how users are interacting with our products and for the purpose of providing you technical networking support and improving our products and services. Cisco may share this information with select third parties in an anonymous aggregated form. None of this personal information and non-personal information will be used to identify or contact you, and use of the personal information and non-personal information shall be subject to Cisco's Privacy Statement, available at http://www.cisco.com/web/siteassets/legal/privacy.html. You may withdraw this consent to collection, use, processing and storage of personal information and non-personal information at any time either by turning the telemetry module off or by uninstalling the telemetry module.

Reading Telemetry Reports

The telemetry module generates reports in "bencode" formatting. The best way to read these reports is by using the Telemetry Report Viewer. The Telemetry Report Viewer is a tool created for Cisco's Threat Operations Center. It is not installed on the endpoint.

Each telemetry report has an incident section followed by one or more activity sections. Table 7-1 and Table 7-2 describe the fields that appear in the report. Figure 7-2 provides examples of field values.

Table 7-1 Telemetry Report Incident Information

Field Name	Field Value
Report Time	Time stamp when the report was generated. The time stamp has this format: YYYY-MM-DD HH:MM:SS.mmm.
Sender ID	Unique hash value derived from MAC address and machine name which can uniquely identify the endpoint unit from others. Using a hash value keeps the telemetry report anonymous.
Operating System Information	Name, version, and release number of the operating system.
Antivirus Information	Name, version, and updated number of the antivirus software installed.
Threat Name	Name of the threat provided by the antivirus software.
Action Taken	Actions taken by the antivirus application, like "Deleted" and "Quarantined."
File Name	Path to the file that the antivirus application determined to be malicious.
Incident Type	Threat detected if the report was triggered by the antivirus software.
Application Name	Path of the application which created the malicious file.

Table 7-2 Telemetry Report Activity Information

Field Name	Field Value
ActivityTime	Time stamp when the report was generated. The time stamp has this format: YYYY-MM-DD HH:MM:SS.mmm.
ActivityType	Field could have one of these values: • Download file • Create file • Unpack file • Pack file • Copy file • Move file • Self extract file
Application Name	Path of the application which created the activity.
File Checksum	SHA1 hash checksum in hex of <FileName>, provided if possible.
File Name	Path of the file that has been created by the application.

Field Name	Field Value
Module Name	Module which ultimately created <FileName>. It could be a DLL or the application executable if the file is not created by any DLL module.
Source URL	Encrypted external URL, in format of [Cisco Encrypted symmetric AES key for external URLs]:[Customer Encrypted symmetric AES key for external URLs]:[Encrypted URL].
Source URL Hash	SHA1 hash of the source URL.
Source URL Internal	Encrypted internal URL, in format of [Encrypted symmetric AES key for internal URLs]:[Encrypted internal URL].
SourceFile	Source file name path.
System State	System state when the activity was recorded, including VPN session status (i.e. VPN:on or VPN:off), and other interested service status.

Figure 7-1 shows a telemetry report displayed in a plain text editor. The highlighted portion represents the encrypted entry for the Source URL, the origin of the virus.

Figure 7-1 Telemetry Report Displayed as Plain Text

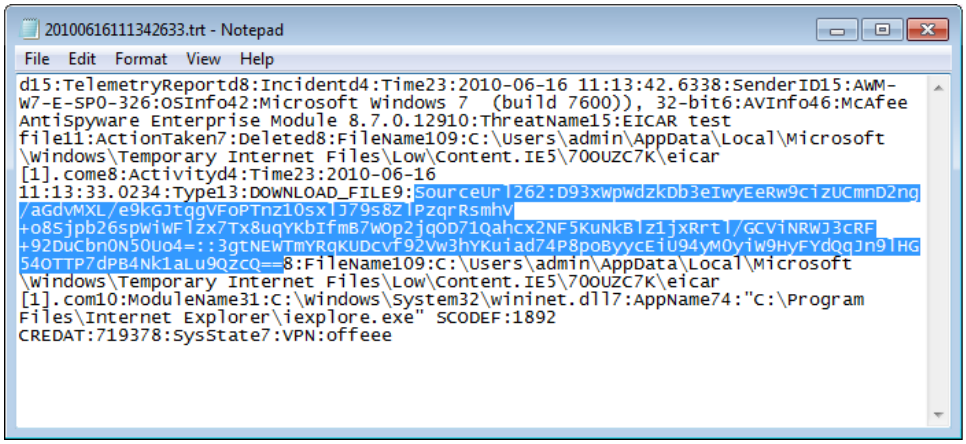
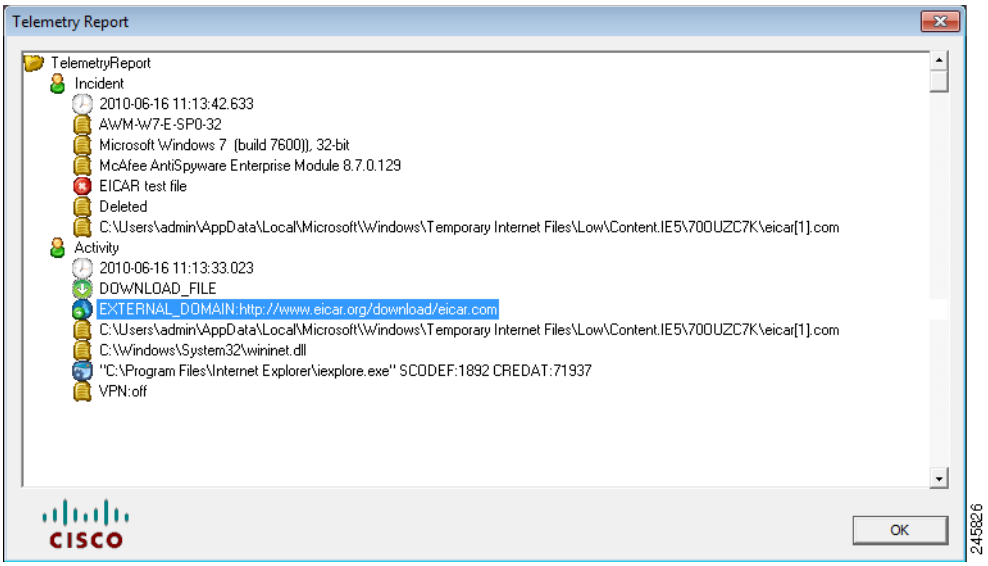


Figure 7-2 shows the same Telemetry report displayed in the Telemetry Report Viewer. The same Source URL is highlighted in the figure.

Figure 7-2 Telemetry Report Displayed in Telemetry Report Viewer



Telemetry Workflow

These steps provide an example of how the telemetry module gathers information and reports it to the WSA.

Step 1 A user visits a web site, **http://www.unabashedevil.com**, and downloads a compressed file, **myriad_evils.zip**. The telemetry module records both activities and stores them in activity.dat.

Step 2 Sometime later, the user extracts the content, **evil_virus.exe**, from the compressed file. The telemetry module records this activity and stores it in activity.dat.

Step 3 A Host Scan-compliant antivirus application identifies a virus in **evil_virus.exe** and deletes the file. The antivirus application activity prompts the telemetry module to create a report on the incident.

Step 4 The telemetry module now works backwards through the information in the activity.dat file to determine the origin of the virus. From the antivirus application incident, the telemetry module determines that **evil_virus.exe** was a virus and it was deleted by the antivirus application. From the activity.dat file, the telemetry module determines that **evil_virus.exe** was extracted from **myriad_evils.zip,** which was downloaded from **http://www.unabashedevil.com**.

All this information is combined in a report.

Step 5 The telemetry module forwards the telemetry report to the WSA.

- If the endpoint is connected to the ASA through a virtual private network, the telemetry module sends the report immediately to the WSA, and it deletes the local copy of the report.
- If the endpoint is not connected to the ASA through a VPN, the telemetry module saves the report in the report repository and sends it to the WSA at its next opportunity.

Step 6 If the WSA enables SenderBase Network Participation, it forwards the report to the Threat Operations Center which analyzes the information along with data from other sources. The WSA receives signature updates to its URL categories and web reputation databases that have incorporated the information from

multiple sources, including the telemetry data. With these new signature updates and depending on the different policies configure on the WSA, users are blocked from accessing **http://www.unabashedevil.com** and prevented from downloading **myriad_evils.zip**.

URL Encryption

URLs stored in the Activity History Repository and Telemetry Report Repository are considered sensitive information. The telemetry module encrypts these URLs to prevent unauthorized access.

The telemetry module treats URLs as either “internal” or “external.” An example of an internal URL might be your company’s intranet home page. An example of an external URL would be any URL that you can access on the Internet.

All domains and IP addresses configured on the WSA to be excluded from SenderBase Network Participation are defined as internal URLs by the telemetry module. If you do not exclude any domains or IP addresses from Senderbase Network Participation, the telemetry module treats all URLs as external.

Both internal and external URLs are included in the telemetry report in encrypted form and sent to the WSA.

All internal URLs specified in Telemetry reports, and in the activity history repository, are encrypted using the symmetric AES key for internal URLs. All external URLs specified in Telemetry reports, and in the activity history repository, are encrypted using the symmetric AES key for external URLs. These symmetric AES keys are randomly generated at the beginning of each VPN session or when the telemetry service starts.

The AES key used for encrypting internal URLs is encrypted with your company’s public key, and sent along with AES encrypted internal URLs in the telemetry report. You can specify your public key in the telemetry profile in the Custom Certificates area. Your public key could be any X.509 public key certificate in PEM-format provided by your company.

The AES key used for encrypting external URLs is encrypted with Cisco’s public key and your company’s public key. Both encrypted versions of the AES key are sent along with AES encrypted external URLs in the telemetry report. Cisco’s public key is one of Cisco’s public certificates and it is delivered with the telemetry module. You are not able to change Cisco’s public key using the ASDM or ASA.

As a result, you can decrypt internal URLs with your company’s private key. You can decrypt external URLs with Cisco’s private key or your company’s private key. This allows the Cisco Threat Operations Center to examine external URLs because it has Cisco’s private key but it cannot decrypt your internal URLs because it does not have your company’s private key.

Finally, the WSA SenderBase Participation Level determines how much of the URL gets encrypted and reported:

- **Standard.** The entire URL is encrypted with Cisco’s public key and reported.
- **Limited.** The URI portion of the URL is encrypted with your private key and then the resulting URL is completely encrypted with Cisco’s public key.

  For example, when telemetry reports on the URL https://www.internetdocs.example.com/Doc?docid=a1b2c3d4e5f6g7h8=en, the **Doc?docid=a1b2c3d4e5f6g7h8=en** portion is encrypted with your private key. Depending on the private key used, the resulting URL might look something like the following string:

  https://www.internetdocs.example.com/93a68d78c787d8f6sa7d09s1455623

This string is encrypted with Cisco's public key and reported. The result is that Cisco's Threat Operations Center would only be able to decrypt the domain name in the URL.

Telemetry Report Encryption

When the telemetry module is ready to send a new telemetry report to the WSA, it encrypts the report based on the configured shared secret between the endpoint, ASA, and WSA. The telemetry module then posts the encrypted report by sending a HTTP POST request to the WSA which aggregates the data and sends it to the Threat Operations Center using SenderBase Network Participation. If the POST request is successful, the telemetry module deletes the report from the local report repository.

Configuring the Telemetry Client Profile

Step 1 Open ASDM and select Configuration > Remote Access VPN > Configuration > Network (Client) Access > AnyConnect Client Profile.

Step 2 Click **Add** to create a client profile.

Step 3 Give the client profile a **name**.

Step 4 Click the **Profile Usage** field and select **Telemetry**.

Step 5 Accept the default Profile Location or click **Browse** to specify an alternate file location.

Step 6 (Optional) Select a **Group Policy** to attach the client profile or leave the client profile <Unassigned>.

Step 7 On the AnyConnect Client Profile page, select the telemetry profile you just created and click **Edit**. You can now edit your telemetry profile in the telemetry profile editor screen.

Step 8 Check the **Enable Service** checkbox to enable telemetry.

Step 9 In the **Maximum History Log (MB)** field, specify the maximum size of activity history repository.

- Range of values: 2-1,000 MB.
- Default value: 100 MB.

Step 10 In the **Maximum History (Days)** field, specify the maximum number of days to retain activity history.

- Range of values: 1-1,000 days.
- Default value: 180 days

Step 11 In the **Antivirus Check Interval (secs)** field, specify the interval at which the telemetry module prompts the posture module to check for new antivirus threat log information.

- Range of values: 5-300 seconds.
- Default value: 60 seconds

Step 12 In the **Retry Send Attempts** field, specify the number of times the telemetry module attempts to send telemetry reports to the WSA if the initial attempt fails.

- Range of values: 0-10
- Default value: 2

Step 13 In the **Administrator Defined Exceptions** field, specify an application's executable file whose behavior you want to exclude from telemetry reports. You can add the executable files in two ways:

- In the **Administration Defined Exceptions** text box, enter the file name, or the full path to the file, that you want to exclude from telemetry reporting and click **Add**. For example:

  trusted.exe

  C:\Program Files\trusted.exe

  If you specify just the file name, the behavior of that file will **not** be tracked in whatever directory it resides. If you add the full directory path and file name, the behavior of the file will **not** be tracked when it is in the directory you specify.
- Click the **Browse** button and select the local file you want to exempt from telemetry reporting. When you browse to add the file, the telemetry profile editor enters the full path to the file. The telemetry module will look for this file, at the end of this path, on all endpoints that use this telemetry profile. The path and filename must be correct for all users of this telemetry profile, not just the administrator.

  In both cases the file is listed in the **Administration Defined Exceptions** list box.

Step 14 In the **Custom Certificate Select from file** field, click **Browse** to locate a Privacy Enhanced Mail (**.pem**) type certificate to generate a profile which includes the your certificate in XML form.

Step 15 Click **OK**.

Step 16 Click **Apply**.

Configuration Profile Hierarchy

There are three client profile resources that govern telemetry behavior. The files act in an order of precedence.

Table 7-3 Telemetry Client Profile Files

File name	Location	Description and Precedence
actsettings.xml	Installed on the endpoint here: %ALLUSERSPROFILE%\Application Data \Cisco\Cisco AnyConnect Secure Mobility Client \Telemetry	File contains the base configuration for Telemetry.
telemetry_profile.tsp The name of this file is specified by the ASA administrator.	Stored on the ASA. Its location is specified on this screen: Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile	Telemetry client profile file. It is created and stored on the ASA. All elements defined in this message overwrite those in the actsettings.xml file.
Telemetry profile message sent by WSA	Not applicable. This is not a file.	There is no XML file on the WSA, but the WSA sends the message in XML format when replying to the status query request. All elements defined in this message overwrite those in the *telemetry_profile*.tsp file.

CHAPTER 8

Enabling FIPS and Additional Security

The Cisco AnyConnect Secure Mobility client VPN functionality and the optional Network Access Manager (NAM) and telemetry modules support 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 ASA on a per-model basis. The following AnyConnect client modules have their own FIPS configuration and requirements:

- AnyConnect core VPN client—FIPS compliance is enabled by a FIPS-mode parameter in the local policy file on the user computer. This file is an XML file containing security settings, and is not deployed by the ASA, but must be installed manually or deployed using an enterprise software deployment system. You must purchase a FIPS license for the ASA the client connects to.
- AnyConnect Network Access Manager (NAM)—Supported on Windows XP computers only, and enabled in the AnyConnect client profile. FIPS support for NAM requires that you deploy a 3eTI FIPS validated Cryptographic Kernel Library (CKL) from 3e Technologies International, with supported drivers that integrate with NAM. Order the FIPS 3eTI CKL supported driver installer from Cisco (shipped on a CD) using part number AIR-SSCFIPS-DRV.

This section contains the following sections:

Enabling FIPS for the AnyConnect Core VPN Client

You enable FIPS compliance for the core AnyConnect Security Mobility Client in the local policy file on the user computer. This file is an XML file containing security settings, and is not deployed by the ASA. The file must be installed manually or deployed to a user computer using an enterprise software deployment system. You must purchase a FIPS license for the ASA the client connects to.

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

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.

This section shows how to enable FIPS mode and additional security for the AnyConnect core VPN client and covers the following topics:

Enabling FIPS 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 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.

Enabling FIPS and other Local Policy Parameters 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 parameters. The names correspond to the parameters in AnyConnect Local Policy file (AnyConnectLocalPolicy.xml). See Table 8-8 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 AnyConnect 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.

Enabling FIPS and Other Parameters with 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 tools is a command line tool that runs 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 8-1 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 8-8.

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 8-1 shows the policy settings and the arguments for the Enable FIPS tool.

Table 8-1 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 Local Policy Parameters Manually in the Local Policy

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 8-2 shows the installation path for each operating system.

Table 8-2 Operating System and AnyConnect Local Policy File Installation Path

Operating System	Installation Path
Windows 7	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows Vista	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client
Windows Mobile	%PROGRAMFILES%\Cisco AnyConnect VPN Client[1]
Linux	/opt/cisco/vpn
Mac OS X	/opt/cisco/vpn

1. AnyConnect 3.0 does not support Windows Mobile. This path for the local policy file for AnyConnect 2.5.

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 a software deployment system.

Enabling Software and Profile Locks

You can restrict the client to obtaining software or client profile updates only from ASAs that you allow by using the software lock or profile lock. By default, the locks are disabled. The AnyConnect client can receive software or client profile updates from any ASA.

With the software lock enabled, the client checks that the ASA is on the list of authorized servers before updating the core VPN client and any optional client modules (such as NAM, telemetry, Web Security, etc.). If the client version loaded on the ASA is newer than the client on the endpoint, but the ASA is not in the list of servers in the software lock, the endpoint client cannot connect. If the client versions are the same, the endpoint client can connect to the ASA.

With the profile lock enabled, the client checks the same list before updating the client profiles for VPN or the other modules. If the ASA is not on the list, the client connects to the ASA but doesn't update the profile(s). If this occurs, the following features are unavailable:

- Service Disable
- Certificate Store Override
- Show Pre-connect Message
- Local LAN Access
- Start Before Logon
- Local proxy connections
- PPP Exclusion
- Automatic VPN Policy
- Trusted Network Policy
- Untrusted Network Policy
- Trusted DNS Domains
- Trusted DNS Servers
- Always-On
- Captive Portal Remediation
- Scripting
- Retain VPN on Logoff
- Device Lock Required
- Automatic Server Selection

AnyConnect Upgrades

When the client connects to the ASA, and a new AnyConnect client package is available, it first determines if the ASA is an authorized server by comparing the ASA name with the server name in the *Authorized Server list* in the local policy file or the *default domain* from the global preferences file. If the ASA is authorized, the client downloads all modules and launches the upgrade of the core VPN client, deleting and recreating the plugins directory, which disables all the optional modules currently installed.

After the core VPN client upgrade, optional modules specified at the ASA are upgraded. Those modules already installed but not specified at the ASA are not upgraded and remain disabled. The client also downloads all the profiles, including the VPN profile and other service profiles supported on the endpoint computer.

If the ASA is not an authorized one, the client checks for the software lock and VPN profile lock. If unauthorized, the only client profile downloaded is the VPN profile. Profiles for the optional modules are not downloaded, irrespective of the lock.

Note If the ASA is not authorized, the NAM, telemetry, and Web Security profiles are not downloaded to the ASA, regardless of the profile lock.

Connecting to an Unauthorized ASA

If the software lock is on, the client does not upgrade anything and disconnects. If the software lock is off, the client ignores the list of optional modules at the ASA and gets the list of all modules currently installed on the system from the *VPNmanifest.dat* file and upgrades only those modules from the ASA. Therefore, any new modules specified at this unauthorized ASA are not installed, and any modules not enabled at the ASA but currently installed on the endpoint computer are not disabled.

The software lock also controls downloading customizations, localizations, scripts and transforms—they are not downloaded from an unauthorized ASA if the software lock is on. Therefore, you must make sure that policy enforcement is not done through scripts for non-corporate assets.

Note If both corporate and non-corporate assets connect to a specific ASA, and that ASA deploys scripts for policy enforcement, those scripts will not run on non-corporate assets that have the software lock on. To remedy this, separate the users of these non-corporate assets into a different group policy on the ASA.

If VPN profile lock is off, the client fetches only the VPN profile and saves it. If on, the VPN profile is not downloaded. The client continues to connect without the profile, resulting in many features being unavailable.

Same Version With Different Modules Enabled

When the client connects to an authorized ASA and determines the modules have changed, it downloads and installs any new modules specified on the ASA. In the case where the core VPN client is not updated, the plugins directory is not deleted. Therefore, modules that have been installed but not specified at the ASA remain enabled.

In case of an unauthorized ASA, the client does not install any new modules or disable any modules not specified at the ASA.

Uninstalling the Core VPN Client

If you uninstall the core VPN client manually (using Windows Add or Remove Programs) all optional client modules also uninstall regardless of the version of the installed core VPN client.

Default Authorized Domain

When the client connects for the first time to a ASA, the global preferences file does not have a value for the default domain. Without a value, if the authorized server list is empty, the current ASA domain name (the ASA name minus the host name) is added as a default domain in the global preferences file. For example, if the ASA is vpn.newyork.example.com, the following lines are added to the global preferences file:

```
<DefaultDomain>example.com</DefaultDomain>
```

The default domain is treated as an authorized ASA, as if it appeared in the list of authorized servers in the local policy file. Be aware that the settings defined in the local policy take precedence over the default domain. Therefore, if you deploy a new local policy file which contains an authorized server list using a software management system (or some other method), the default domain is ignored.

Connecting to an Unauthorized ASA with the Profile Lock Off

If a client connects to an unauthorized ASA that has the Always-on feature enabled and the VPN profile lock is off in the local policy, the old profiles are deleted and the client cannot reconnect to that ASA. Therefore, if you are using Host Scan to detect corporate assets, or you have the right group partitions enabled, be careful that you do not force the Always-on feature to the non-corporate assets and guests.

Logging

The downloader creates a separate text log (UpdateHistory.log) that records the download history. This log includes the time of the updates, the ASA that updated the client, the modules updated, and what version was installed before and after the upgrade. This log file is stored here:

%AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs directory.

XML Tags for the Software and Profile Locks

The following text is an example local policy file. The XML tags for the software and profile locks appear between the UpdatePolicy tags. These tags appear in bold in this example.

You list the authorized servers between the <AuthorizedServerList> tags. The servers can contain either an FQDN or an IP Address. They can have also contain wild cards. For example: newyork.example.com, *.example.com, or 1.2.3.*

Note If you want remote users to connect using the IP address of the server, be sure so list the IP address in the authorized server list. If the user attempts to connect using the IP address but the server is listed as an FQDN, the attempt is treated as connecting to an unauthorized domain.

The example server names *seattle.example.com* and *newyork.example.com* are FQDNs of authorized servers:

```
<?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>
    <UpdatePolicy>
        <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
        <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
        <AuthorizedServerList>
            <ServerName>seattle.example.com</ServerName>
            <ServerName>newyork.example.com</ServerName>
        </AuthorizedServerList>
    </UpdatePolicy>
</AnyConnectLocalPolicy>
```

Software Lock Use Cases

Table 8-3, Table 8-4, Table 8-5, and Table 8-6 provide use cases for the client connecting to authorized and unauthorized ASAs with client package versions that are the same, and different:

Table 8-3 Connecting to an Authorized ASA Having a Newer AnyConnect Package

Client Modules Initially Installed	ASA with Modules A, B, C, D enabled	ASA with modules A, B, X, Y enabled	ASA with modules A, B enabled
A, B, C installed and enabled	A, B, and C are updated with the version loaded on the ASA. The version of D loaded on the ASA is installed.	A and B are updated with the version loaded on the ASA. The versions of X and Y loaded on the ASA are installed. C is disabled but remains installed and is not upgraded.	A and B are updated with the version loaded on the ASA. C is disabled but remains installed and is not upgraded.
A, B, C installed. C is disabled due to previous update.	A, B, and C are updated. C is enabled. D is installed.	A and B are updated. X and Y are installed. C remains disabled and is not updated.	A and B are updated. C remains disabled and is not updated.

Table 8-4 Connecting to an Unauthorized ASA Having a Newer AnyConnect Package

Client Modules Initially Installed	ASA with Modules A, B, C, D Enabled	ASA with Modules A, B, X, Y Enabled	ASA with Modules A, B Enabled
A, B, C installed and enabled. Software lock OFF.	A, B and C are updated with the version loaded on the ASA. D is not downloaded.	A and B are updated with the version loaded on the ASA. C is updated even though it is not specified at this ASA. X and Y are not downloaded.	A and B are updated with the version loaded on the ASA. C is updated even though it is not specified at this ASA.
A, B, C installed. C is disabled due to previous update. Software lock OFF	A and B are updated with the version loaded on the ASA. C is not updated and remains disabled.	A and B are updated with the version loaded on the ASA. C is not updated and remains disabled.	A and B are updated with the version loaded on the ASA. C is not updated and remains disabled.
A, B, C installed and enabled. Software lock ON	No modules are downloaded or updated, and the client disconnects.	No modules are downloaded or updated, and the client disconnects.	No modules are downloaded or updated, and the client disconnects.
A, B, C installed. C is disabled due to previous update. Software lock ON	No modules are downloaded or updated, and the client disconnects.	No modules are downloaded or updated, and the client disconnects.	No modules are downloaded or updated, and the client disconnects.

Table 8-5 Connecting to an Authorized ASA with the Same Version AnyConnect Package but Different Modules

Client Modules Initially Installed	ASA with Modules A, B, C, D Enabled	ASA with Modules A, B, D Enabled	ASA with Modules A, B Enabled
A, B, C installed and enabled	D is downloaded and installed. A, B, C and D are installed and enabled.	D is downloaded and installed. C is not disabled. A, B, C, and D are installed and enabled.[1]	No modules are downloaded. A, B, and C remain enabled.
A, B, C installed. C is disabled due to previous update.	D is downloaded and installed. A, B, and D are installed and enabled. C remains disabled.[2]	D is downloaded and installed. A, B, and D are installed and enabled. C remains disabled.	No modules are downloaded. A and B remain enabled. C remains disabled.

1. If you want to disable C, you must deploy a client VPN profile with a *Disable Service* enabled.
2. You can only enable C if you load an AnyConnect package that is newer and C is enabled.

Table 8-6 Connecting to an Unauthorized ASA with the Same Version AnyConnect Package but Different Modules

Client Modules Initially Installed	ASA with Modules A, B, C, D Enabled	ASA with Modules A, B, D Enabled	ASA with Modules A, B Enabled
A, B, C installed and enabled. Software lock OFF or ON	No modules are downloaded. A, B, and C remain enabled.	No modules are downloaded or disabled. A, B, and C remain enabled.	No modules are disabled. A, B, and C remain enabled.

Software and Profile Lock Example

The following example scenario describes the client upgrading behavior with differing versions of AnyConnect package on the client PC and the ASA. Table 8-7 lists the AnyConnect package versions for three ASAs:

Table 8-7 Example ASA and AnyConnect Client Information

ASA	AnyConnect Package Loaded	Modules to Download
seattle.example.com	Version 3.0.0350	VPN, NAM, Web Security
newyork.example.com	Version 3.0.0351	VPN, NAM
raleigh.example.com	Version 3.0.0352	VPN, posture, telemetry

Continuing with this example, the local policy XML file has the following contents:

```
<UpdatePolicy>
    <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
    <AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfileUpdatesFromAnyServer>
    <AuthorizedServerList>
        <ServerName>seattle.example.com</ServerName>
        <ServerName>newyork.example.com</ServerName>
    </AuthorizedServerList>
</UpdatePolicy>
```

According to this local policy, the software lock is *off* and the VPN profile lock is *on*.

The AnyConnect client user connects to seattle.example.com first, VPN, NAM and Web Security are installed (all the modules supported by version 3.0.0350). The user then decides to connect to newyork.example.com, an authorized ASA running a newer version (version 3.0.0351). The ASA deletes the plugins directory and VPN and NAM are upgraded to version 3.0.0351. Web Security remains at version 3.0.0350 and disabled.

The user then connects to raleigh.example.com which is not in the authorized server list. Since the software lock is not on, VPN and NAM are upgraded to 3.0.0352. However, the other modules specified (posture, and telemetry) are not installed. Web Security remains at version 3.0.0350 and disabled.

Because the VPN profile lock is on, the VPN client profile is not downloaded. And because raleigh-example.com is not an authorized server, other service profiles are also not downloaded.

AnyConnect Local Policy Parameters and Values

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

Table 8-8 describes the parameters in the AnyConnect Local Policy file and their values:.

Table 8-8 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 acversion="<version number>".
xmlns The XML namespace specifier. Most administrators do not change this parameter.	The format is a URL, for example: xmlns=http://schemas.xmlsoap.org/encoding/
xsi:schemaLocation The XML specifier for the schema location. Most administrators do not change this parameter.	The format is a URL, for example: xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectLocalPolicy.xsd">
xmlns:xsi The XML schema instance specifier. Most administrators do not change this parameter	The format is a URL, for example: xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance

Table 8-8 AnyConnect Local Policy File and their Values (continued)

Parameter and Description	Values and Value Formats
FipsMode Enables FIPS mode for the client. The client uses only algorithms and protocols approved by the FIPS standard.	*true*—Enables FIPS mode. *false*—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.	*true*—The client does not check for any dynamic content present on the ASA, including profile updates, translations, customization, optional modules, and core software updates. *false*—The client checks for dynamic content present on the ASA (default). **Note** If you configure client profiles on the ASA, they must be installed on the client prior to the client connecting to the ASA with BypassDownloader set to *true*. Because the profile can contain administrator defined policy, the BypassDownloader *true* setting is only recommended if you do not rely on the ASA to centrally manage client profiles.
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.	*true*—WebLaunch attempts fail and the client displays an informative message to the user. *false*—Permits WebLaunch (default—behavior consistent with AnyConnect 2.3 and earlier).
StrictCertificateTrust When authenticating remote security gateways, AnyConnect 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	*true*—The client fails to connect to security gateways that use self-signed certificates and displays this message: `Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.` *false*—The client prompts the user to accept the certificate (default—behavior consistent with AnyConnect 2.3 and earlier).
RestrictPreferenceCaching By design, AnyConnect does not cache sensitive information to disk. Enabling this parameter extends this policy to any type of user information stored in the AnyConnect preferences.	*Credentials*—The user name and second user name are not cached. *Thumbprints*—The client and server certificate thumbprints are not cached. *CredentialsAndThumbprints*—certificate thumbprints and user names are not cached. *All*—No automatic preferences are cached. *false*—All preferences are written to disk (default—behavior consistent with AnyConnect 2.3 and earlier).

Table 8-8 AnyConnect Local Policy File and their Values (continued)

Parameter and Description	Values and Value Formats
RestrictTunnelProtocols (currently not supported) Forbids the use of certain tunnel protocol families to establish a connection to the ASA.	*TLS*—The client only uses IKEv2 and ESP to establish the tunnel, and will not use TLS/DTLS to communicate information to the secure gateway. *IPSec*—The client only uses TLS/DTLS for authentication and tunneling. *false*—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.	*true*—Excludes the Firefox NSS certificate store. *false*—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.	*true*—Excludes the PEM file certificate store. *false*—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.	*true*—Excludes the Mac native certificate store. *false*—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.	*true*—Excludes the Windows Internet Explorer certificate store. *false*—Permits the Windows Internet Explorer certificate store (default).
AllowSoftwareUpdateFromAnyServer Allows software updates from any ASA, or restricts the client to obtaining software only from ASAs that you allow.	*true*—Software updates for the AnyConnect client are allowed from any ASA (default). *false*—Software updates for the AnyConnect client are allowed only from ASAs specifed in the AuthorizedServerList section.

Table 8-8 AnyConnect Local Policy File and their Values (continued)

Parameter and Description	Values and Value Formats
AllowVPNPolicyUpdateFromAnyServer Allows updates to the VPN local policy file from any ASA, or restricts the client to obtaining updates only from ASAs that you allow.	*true*—VPN local policy file updates for the AnyConnect client are allowed from any ASA (default). *false*—VPN local policy file updates for the AnyConnect client are allowed only from ASAs specifed in the AuthorizedServerList section.
AuthorizedServerList A list of servers allowed to update the AnyConnect client software or VPN local policy file.	Server names listed with ServerName.
ServerName A server name for the software of local policy lock.	The name of a server that the AnyConnect client can receive software or VPN local policy file updates. ServerName can be an FQDN, IP address, domain name, or wildcard with domain name.

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 for the Network Access Manager

FIPS compliance is supported for Windows XP only and requires that you enable FIPS mode in the AnyConnect client profile and that you deploy the 3eTI FIPS Certified Crypto Kernel Library (CKL) to user computers connecting to FIPS networks.

With NAM configured for FIPS compliance, users can still connect to non-FIPS networks. But when the user chooses to connect to a FIPS-compliant network, NAM uses the 3eTI FIPS CKL and displays the FIPS compliance status in the NAM pane of the AnyConnect GUI.

This chapter describes how to enable FIPS compliance for the Network Access Manager (NAM) and contains these sections:

Note FIPS compliance for NAM is supported on user computers running Windows XP only.

You can allow enterprise employees to only connect to FIPS-compliant networks by restricting the allowed association and encryption modes, and the authentication methods, in the NAM configuration section of the AnyConnect profile.

NAM FIPS compliance supports FIPS approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X). The NAM FIPS support includes EAP methods EAP-TLS, EAP-TTLS, EAP-PEAP, and EAP-FAST. NAM enables you to support both FIPS-compliant WLAN profiles as well as optional non-compliant configurations such as access to Wi-Fi hotspots with client VPN security enabled.

As the administrator, you are responsible for naming the profile appropriately to indicate whether the network is FIPS enabled.

A fully FIPS-compliant solution requires three components:

- NAM
- 3eTI FIPS certified Crypto Kernel Library (CKL) with supported NIC adapter drivers
- A FIPS-compliant network profile configuration

Enforcing FIPS Mode in NAM

Within the NAM Profile Editor, you can enable FIPS mode. Refer to the "Configuring a Client Policy" section on page 4-4 for more information.

3eTI FIPS Certified Crypto Kernel Library (CKL)

These NIC adapter chipsets are supported by the 3eTI FIPS certified CKL:

- Intel 2100, 2200, 2915, and 3945 chipsets
- Broadcom: All BCM 43xx chipsets that support driver version 4.100.27.0 or later
- Atheros PCI chipset based NIC adapters, including Cisco AIR-CB21 wireless client adapter cards
- Atheros: 5001, 5004, 5005, AR5211, and AR5212 chipsets

FIPS Integration

To ensure a FIPS-compliant solution, you must set up network profiles that allow only WPA2 handshakes with AES encryption with FIPS-compliant EAP types or WPA2-Personal (Pre-shared key).

The NAM Log Packager utility collects logs of the 3eTI packets.

3eTI CKL Driver Installer

For instructions on how to install the 3eTI FIPS validated CKL with supported drivers, see the "Installing the 3eTI Driver" section on page 8-15.

Installing the 3eTI Driver

This section provides instructions for installing the 3eTI FIPS validated Cryptographic Kernel Library (CKL) with supported drivers that integrate with NAM to provide a complete FIPS solution.

Important Notes

1. The 3eTI CKL driver installer is designed to allow only one 3eTI wireless driver to be installed on a system at any given time. A previous driver must be un-installed prior to installing a different type of driver. For a driver of the same type, uninstalling the previous driver is not necessary because the next installation just updates the existing driver.
2. When the hardware is present and installed in the system, the installer updates the corresponding OEM wireless NIC adapter driver with the 3eTI modified driver that supports the 3eTI CKL.

3eTI CKL Driver Installer Overview

The 3eTI CKL driver installer can be started using one of these methods:

- Double-clicking the .exe file—can only be used for normal driver installations in which the NIC adapter is installed in the PC before the installer is run.
- Using the installer command without command-line options—can be used only for normal driver installations.
- Using the installer command with command- line options—can be used for normal and pre-installed driver installations.

When you start the driver installer by double-clicking the .exe file or using the run command without command-line options, the installer performs these operations:

- Detects and installs the 3eTI CKL with a supported NIC adapter driver for FIPS operation.
- If multiple NIC adapters are detected that support the 3eTI CKL, the installer prompts the user for adapter selection.
- If a compatible NIC adapter is not found on the PC, the installer aborts the installation and displays this error message:

  The installer cannot auto-detect a NIC chipset to provide FIPS support. To enforce a pre-installation, you are required to run the installer using the command line. For instructions or further assistance, please contact your network administrator.

Note Pre-installation scenarios are best supported with command-line options that allow you to specify specific installation options. Pre-installations are typically preformed by you, the network administrator, and not a novice user.

Installer Command and Command-Line Options

The installer supports the following command and command-line options:

3eTI-drv-installer.exe –s –auto Type= XXXX

–s	Used to perform a silent installation without prompting the user.
–auto	Used to perform an intelligent installation, where the installer determines the supported NIC adapter in the PC and installs the appropriate driver. This causes the installer to perform the same operations as entering the command without command line options.
Type=*XXXX*	Used to specify the NIC adapter chipset for a pre-installation or a normal installation. *Pre-installation* means that the driver is installed before the specified NIC adapter is installed in the PC. *Normal installation* means that the NIC adapter is installed before the driver is installed.

XXXX Value	Description
Intel3945	Specifies drivers for the Intel3945 chipset.
Centrino	Specifies drivers for Intel 2100, l2200, and 2915 chipsets.
Broadcom	Specifies drivers for Broadcom chipsets supported by the Installer.
Atheros	Specifies drivers for the Atheros 5001, 5004, 5005, AR5211, and AR5212 chipsets.
Cisco	Specifies drivers for the Cisco AIR-CB21 card with an Atheros chipset.

Note When using –s for silent installation, you must also specify –auto or Type=XXXX or both –auto and Type=XXXX.

Examples:

- Using *–auto* in conjunction with *–s*:
  - Performs an intelligent installation by automatically detecting the NIC adapter that is installed.
  - Performs a silent installation without prompting the user.
  - If multiple NIC adapters are detected, selects any supported chipset.
- Using *–auto* in conjunction with *Type=XXXX*:
  - Attempts to Install the driver for the NIC adapter chipset specified by Type=XXXX.
  - If the detected NIC adapters do not support the specified chipset, installs a driver for any NIC adapter with a supported chipset.
- Using *3eTI-drv-installer.exe Type=Intel3945 –auto –s*:
  - Attempts to install a driver for the Intel3945 chipset without prompting the user.
  - If a NIC adapter with the Intel3945 chipset is not detected, silently installs a driver for any other detected NIC adapter with a supported chipset.
  - If a NIC adapter with a supported chipset is not detected, does not pre-install any driver.
- Using *3eTI-drv-installer.exe Type=Intel3945 –s*:
  - Attempts to install a driver for the Intel3945 chipset without prompting the user.
  - If a supported NIC adapter chipset is not detected, performs a pre-install by installing the specified chipset driver.

Running the Installer without Using Command-Line Options

To perform a normal installation with the NIC adapter installed in the PC, follow these instructions:

Step 1 Start the installer by following one of these steps:

a. Use Windows Explorer to locate the **3eTI-drv-installer.exe** file on your PC and double-click the filename.

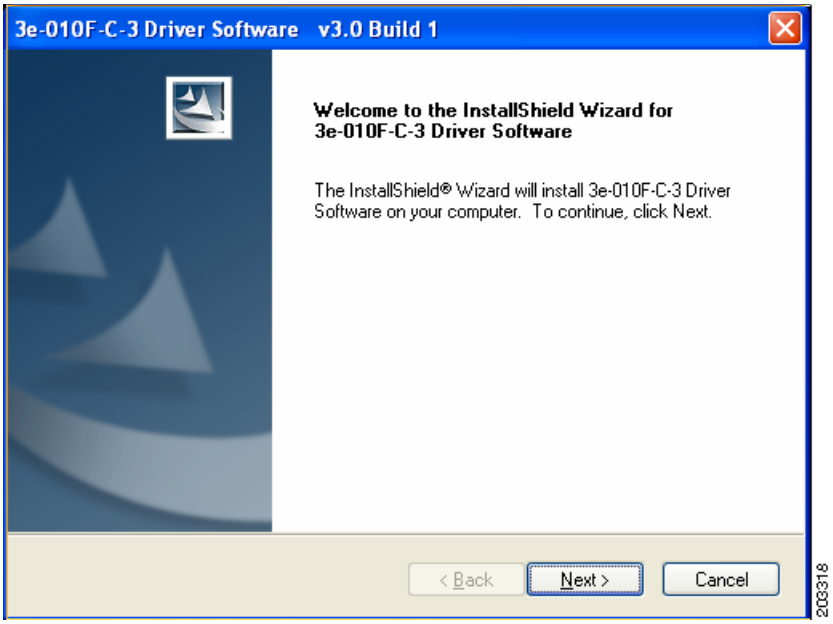
b. Click **Start** > **Run** and enter this installer run command:

path **/ 3eTI-drv-installer.exe**

Where *path* is the directory path to the installer file.

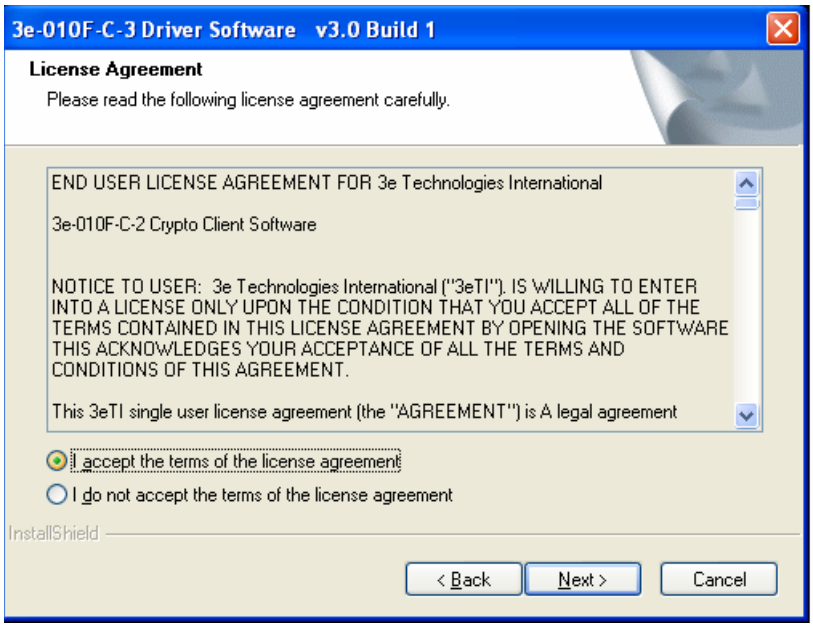
The Driver Welcome window appears (Figure 8-1).

Figure 8-1 Driver Welcome Window



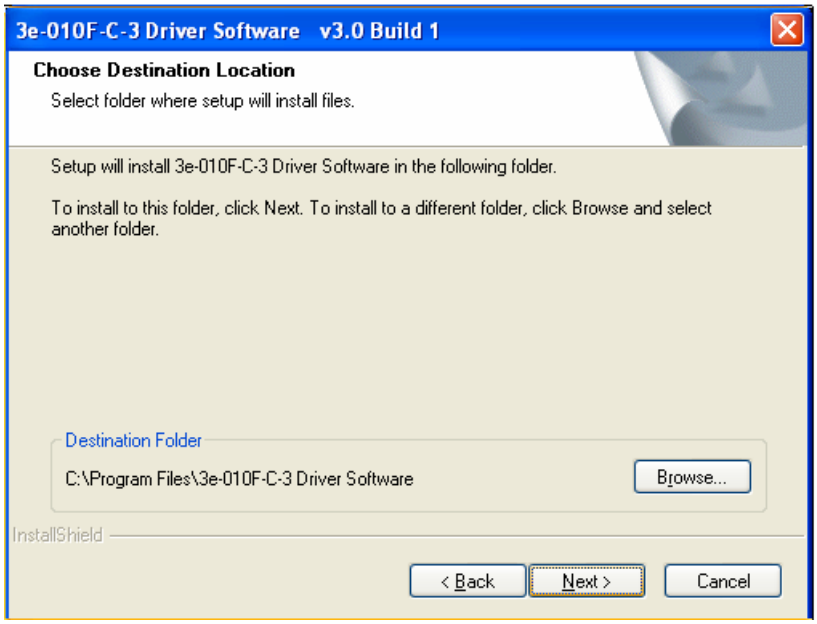
Step 2 Click **Next** and the license agreement appears (see Figure 8-2).

Figure 8-2 License Agreement



Step 3 Read and accept the license agreement and click **Next**. Figure 8-3 appears.

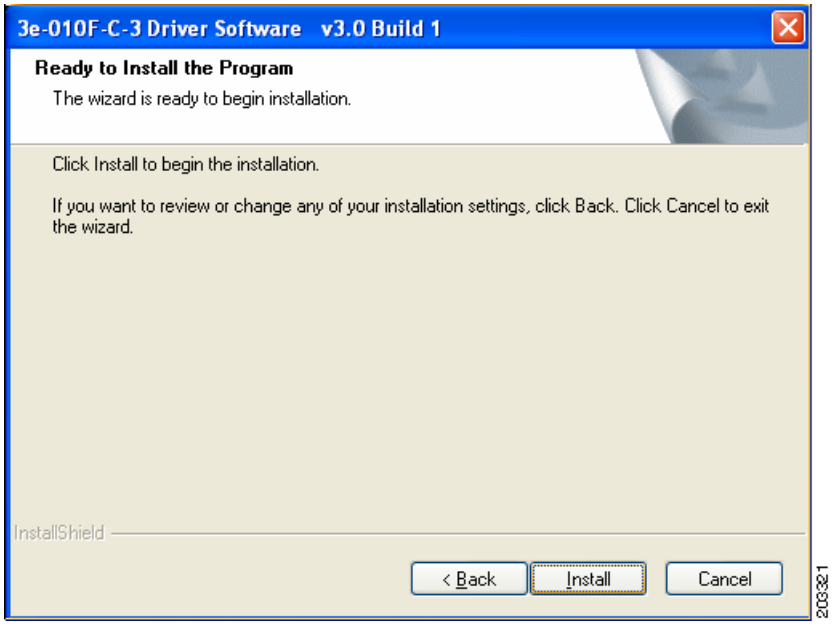
Figure 8-3 Destination Location Window



Step 4 Accept the driver software default destination folder or click **Browse** to locate the desired folder.

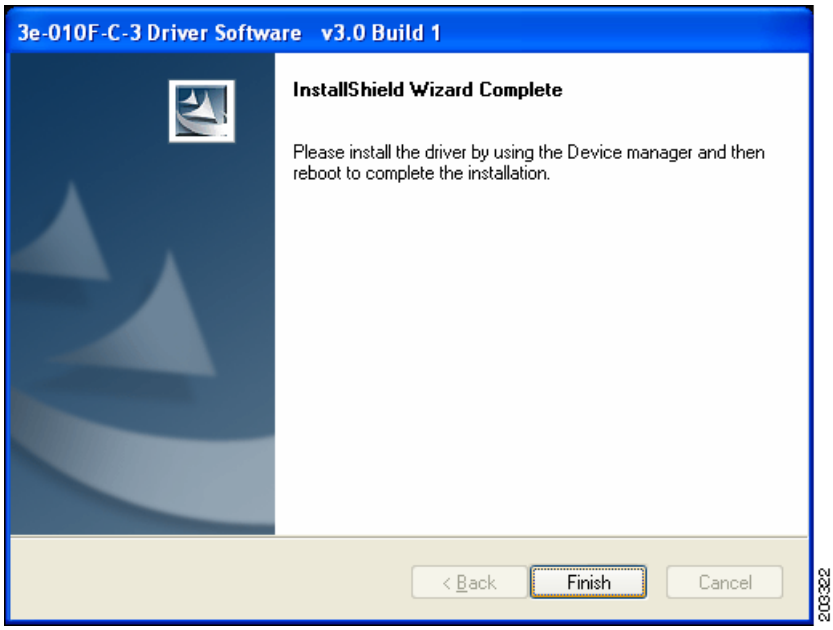
Step 5 Click **Next** and Figure 8-4 appears.

Figure 8-4 Ready to Install Window



Step 6 Click **Install** to start the installation process. When the installation completes, Figure 8-5 appears.

Figure 8-5 Wizard Complete Window



Step 7 Click **Finish**.

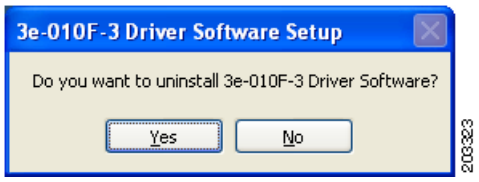
Uninstalling Previous 3eTI Driver Software

To uninstall previous 3eTI driver software, follow these steps:

Step 1 To uninstall the previous 3eTI driver software, click **Start > Settings > Control Panel > Add or Remove Programs**.

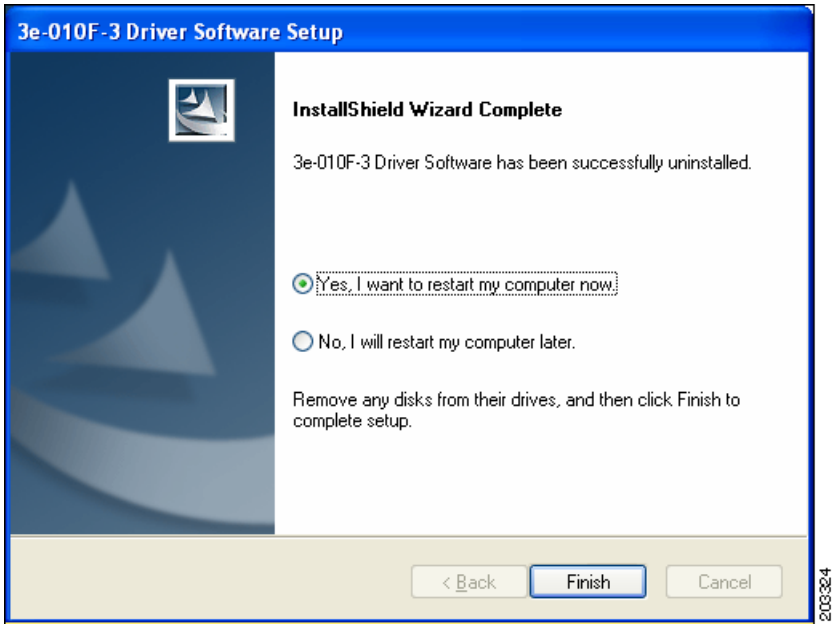
Step 2 Choose the 3eTI driver software, such as 3e-010F-3 and click **Remove**. A pop-up window appears (see Figure 8-6).

Figure 8-6 Uninstall Driver Software Pop-Up



Step 3 Click **Yes** to uninstall the driver software. Figure 8-7 appears.

Figure 8-7 Restart Computer Now Window



Step 4 Check **Yes** to restart your computer.

Step 5 Click **Finish**. Your PC reboots to completely remove the driver software.

Silent Driver Installation for Enterprise Deployment

To run the installer using a silent mode, follow these steps:

Step 1 Run the installer by entering this command:

path **/ 3eTI-drv-installer.exe -s Type=***XXXX*

Where:

path is the directory path to the installer file.

-s indicates silent installation.

Type= *XXXX* specifies the chipset, such as Centrino, Intel3945, or Cisco (see the "Installer Command and Command-Line Options" section on page 8-15).

A pop-up status window appears indicating that the driver installation is in progress and then disappears when the installation completes.

Installing the Driver without a Previously Installed Network Adapter

To install the 3eTI driver on a PC without an installed NIC adapter, follow these steps:

Step 1 Start the installer by clicking **Start > Run** and enter this installer run command:

path **/ 3eTI-drv-installer.exe Type =** *XXXX*

Where:

path is the directory path to the installer file.

Type=*XXXX* specifies the chipset, such as Centrino, Intel3945, or Cisco (see the "Installer Command and Command-Line Options" section on page 8-15).

Figure 8-1 appears.

Step 2 Perform Step 2 through Step 7 in the "Running the Installer without Using Command-Line Options" section on page 8-17.

Step 3 When the driver installation is complete, insert or install the NIC adapter in the PC.

Manually Upgrading the 3eTI Driver Software

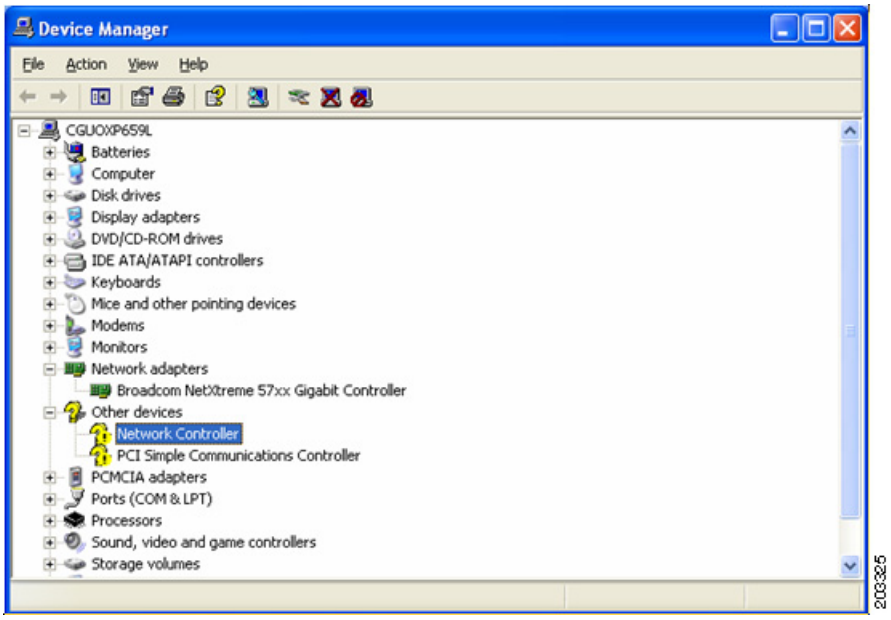
Manual upgrade instructions are provided to help troubleshoot driver installation problems. This is not expected to be a part of an enterprise-wide deployment.

Follow these steps to manually upgrade the 3eTI driver software using the Windows Device Manager:

Step 1 Right-click the **My Computer** icon on your desktop and choose **Properties**.

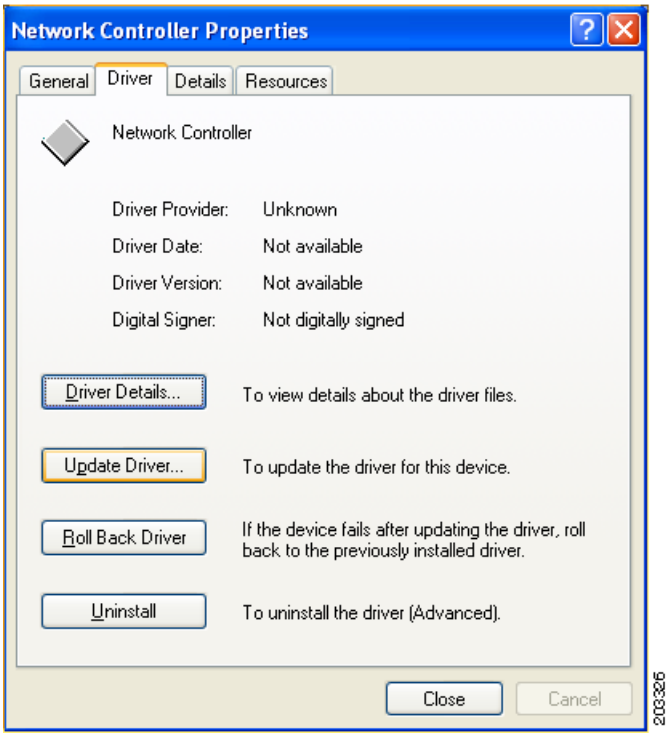
Step 2 Click **Hardware** on the System Properties window, click **Device Manager**. Figure 8-8 appears.

Figure 8-8 Windows Device Manager Window



Step 3 If your Network Adapter is installed or inserted and the driver software is not installed, the device will be listed under Other devices and shown with a yellow question mark. Right-click on your network adapter and choose **Properties**. The Network Controller Properties window appears (see Figure 8-9).

Figure 8-9 Network Controller Properties Window

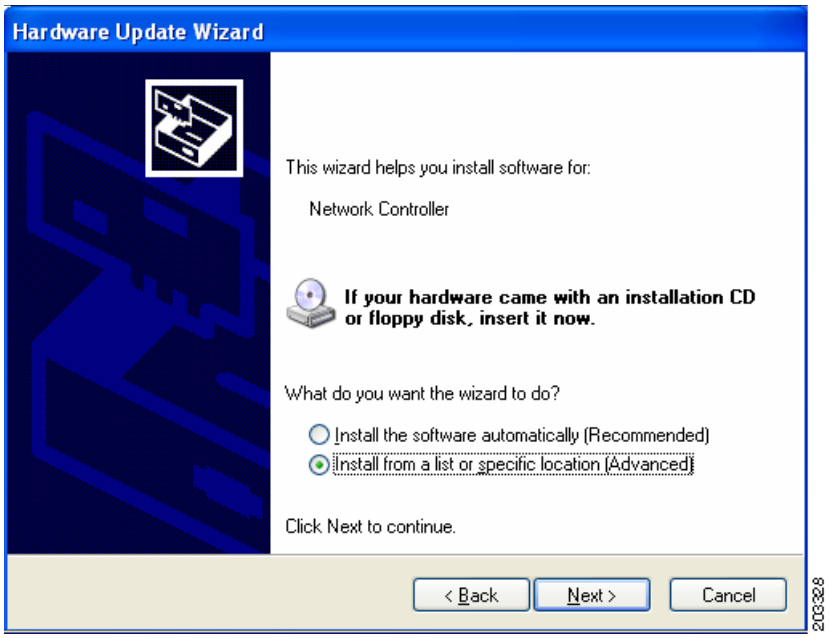


Step 4 Click **Driver > Update Driver** and Figure 8-10 appears.

Figure 8-10 Windows Hardware Update Wizard Window

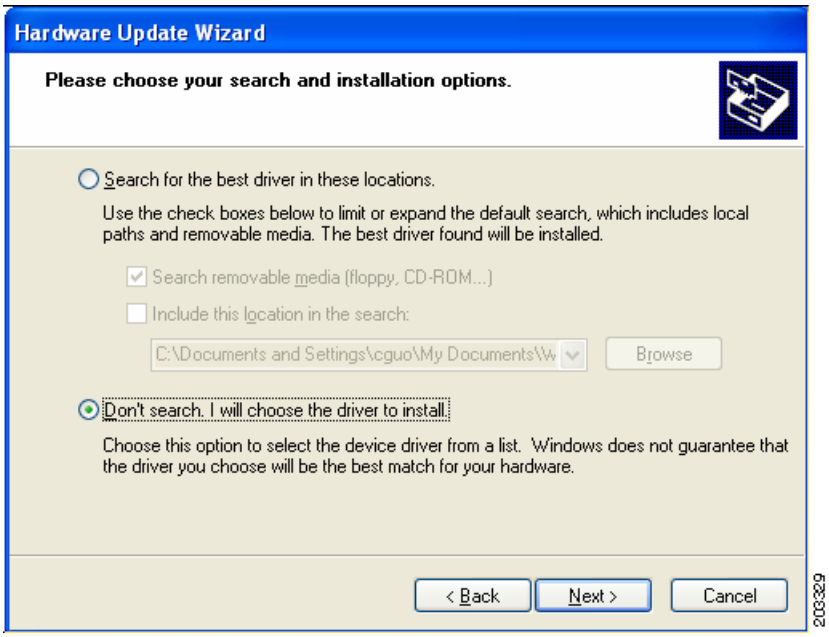
Step 5 Click **No** to prevent Windows from searching for the driver software and click **Next**. Figure 8-11 appears.

Figure 8-11 Installation CD or Floppy Disk Option Window



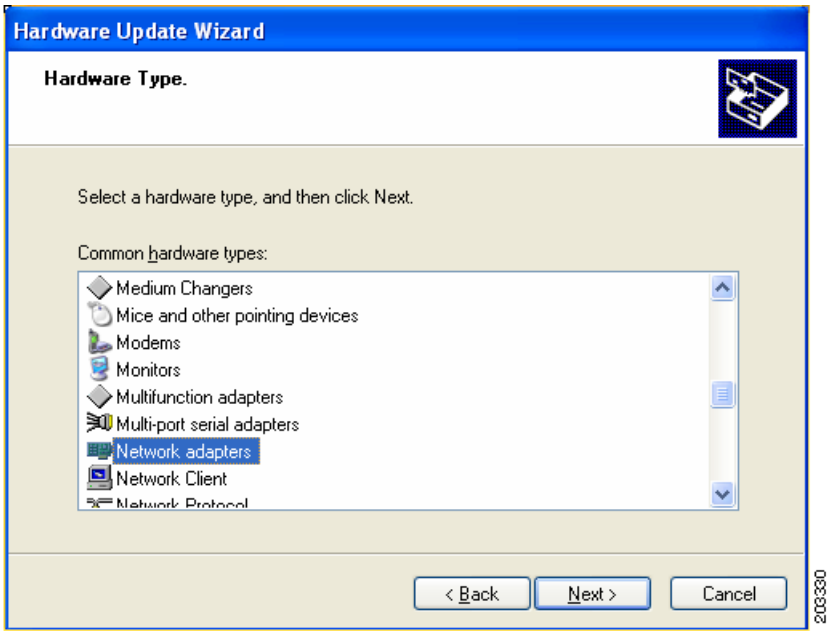
Step 6 Check **Install from a list or specific location (Advanced)** and click **Next**. Figure 8-12 appears.

Figure 8-12 Search and Installation Options Window



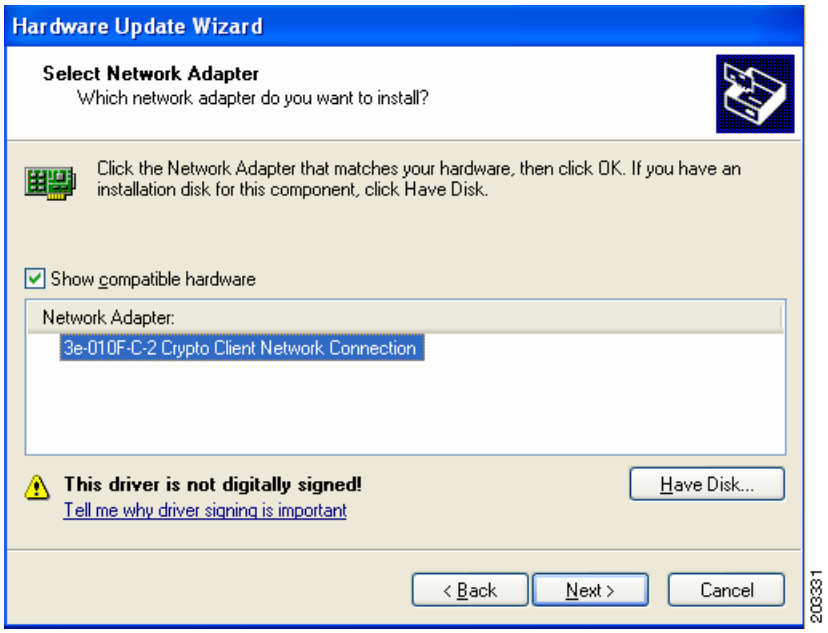
Step 7 Check **Don't search. I will choose the driver to install** and click **Next**. Figure 8-13 appears.

Figure 8-13 Windows Hardware Type Window



Step 8 Choose **Network adapter** and click **Next**. Figure 8-14 appears.

Figure 8-14 Select Network Adapter Window

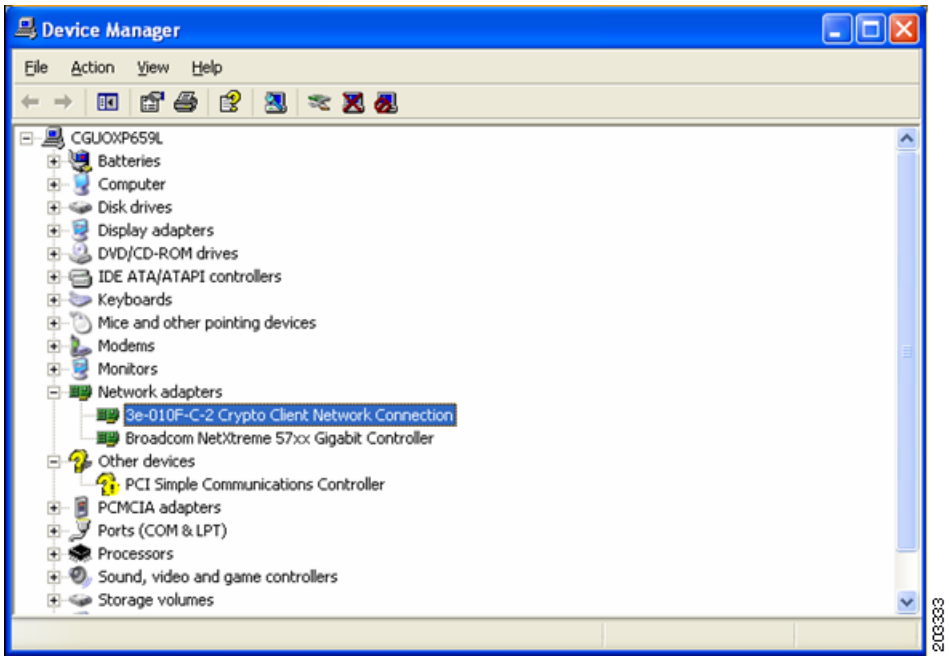


Step 9 Choose the 3eTI network connection and click **Next**. Figure 8-15 appears.

Figure 8-15 Installation Complete Window

Step 10 The hardware driver installation is complete. Click **Finish**. The Device Manager window reappears (see Figure 8-16).

Figure 8-16 Updated Windows Device Manager Window



Step 11 To verify that the driver is installed properly, right click on the 3eTI network connection and choose **Properties**. Ensure that the adapter properties window indicates **This device is working properly** under the Device status.

Obtaining the 3eTI Driver Installer Software

The FIPS 3eTI CKL supported driver installer cannot be downloaded from the Cisco Software Center and must be ordered from Cisco. A non-expiring license for the driver installer can be ordered from Cisco using this product number: AIR-SSCFIPS-DRV

The ordered 3eTI CKL supported driver installer software is shipped to you on a product CD.

CHAPTER 9

Fulfilling Other Administrative Requirements for AnyConnect

This chapter provides the following instructions:

Using Quarantine to Restrict Non-Compliant Clients

Through the use of quarantine, you can restrict a particular client who is attempting to initiate a VPN connection. The ASA applies restricted ACLs to a session to form a restricted group, based on the selected dynamic access policy. When an endpoint is not compliant with an administratively defined policy, the user can still access services for remediation (such as updating an antivirus application), but restrictions are placed upon the user. After the remediation occurs, the user can reconnect, which invokes a new posture assessment. If this assessment passes, the user connects without any restrictions.

Quarantine Requirements

Quarantine requires an advanced endpoint assessment license activated on the adaptive security appliance. The advanced endpoint assessment remediates endpoints that do not comply with dynamic policy requirements for antivirus, antispyware, and firewall applications; and any associated application definition file requirements. Advanced endpoint assessment is a Cisco Secure Desktop Host Scan feature, so AnyConnect supports quarantine on all OSs supported by AnyConnect, including Windows Mobile.

ASA Release 8.3(1) or later features dynamic access policies and group policies that support a user message to display on the AnyConnect GUI when the user is first notified of the quarantine. Other quarantine messages (such as “Quarantined - Remediation Required” and “To attempt a normal connection, please reconnect”) are reported, but these messages cannot be defined by the administrator to show the users. Quarantine does not require the ASA upgrade; only the user message requires it.

If you upgrade the ASA software, we recommend that you also upgrade ASDM to Release 6.3(1) or later so that you can use it to configure the new features.

AnyConnect supports quarantine on all OSs supported by AnyConnect, including Windows Mobile. The client supports the quarantine user message on Windows 7, Vista, XP; and Mac OS and Linux, but not on Windows Mobile.

Configuring Quarantine

To configure quarantine,

Step 1 Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan > Advanced Endpoint Assessment** and configure Host Scan to remediate noncompliant computers.

Step 2 Choose **> Remote Access VPN > Network (Client) Access > Dynamic Access Policies**, click **Add**, create a DAP that uses endpoint attributes that identify noncompliant computers, click the **Action** tab, and click **Quarantine**.

Step 3 (Optional) Enter a message to display for the user in a quarantined session.

Use the ASDM help if you need more information with configuring dynamic access policies.

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 or Windows 7 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).

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 AnyConnect 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 AnyConnect and Cisco Secure Desktop to interoperate with the ASA.

To do this, follow these steps:

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

- The CD shipped with the ASA.
- 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 10

Managing VPN Authentication

This chapter explains how to manage VPN authentication for users using the Cisco AnyConnect Secure Mobility client, and includes these subjects and tasks:

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 AnyConnect Connection Profile window opens.

Step 2 If it is not already, click the **Basic** node of the navigation tree on the left pane of the window. In the right pane of the window, in the **Authentication** area, enable the method **Certificate**.

Step 3 Click **OK**.

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 > AnyConnect Connection Profiles**. In the **Access Interfaces** area in the right pane, select the interface for which you want to specify a certificate, and then click **Device Certificate**.

Step 5 In the Specify Device Certificate dialog, click the **Device Certificate** field to choose a certificate or click **Manage** to add a certificate you want to use for authentication connections to the interface you have chosen.

Step 6 Click **OK** and apply your changes.

Note To configure in which certificate store the AnyConnect client searches for the authentication certificate, see the"Configuring a Certificate Store" section on page 3-38. You will also find information on configuring certificate restrictions for Linux and Mac OS X operating systems.

SDI Token (SoftID) Integration

AnyConnect integrates support for RSA SecurID client software versions 1.1 and later running on Windows 7 x86 (32-bit) and x64 (64-bit), Vista x86 and x64, and XP x86.

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 AnyConnect does not support token selection from multiple tokens imported into the RSA Software Token client software. Instead, the 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 releases 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 10-10) on the ASA 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. AnyConnect 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 ASA with AnyConnect and attempts to authenticate using an RSA SecurID token, the ASA communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

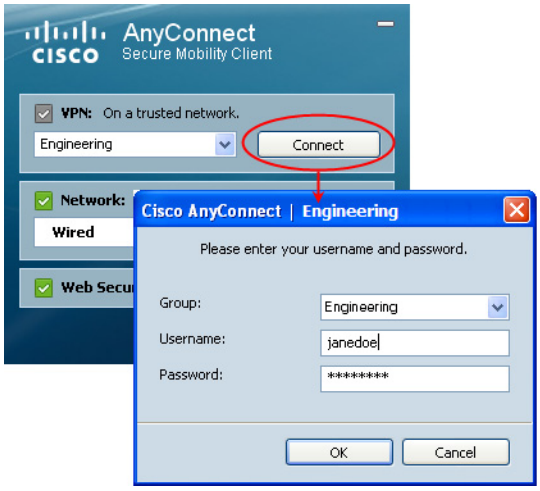
For more information about configuring the ASA to ensure AnyConnect compatibility, see the "Ensuring RADIUS/SDI Proxy Compatibility with AnyConnect" section on page 10-7.

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.

Typically, users make an AnyConnect connection by clicking the AnyConnect icon in the tools tray, selecting the connection profile with which they wish to connect and then entering the appropriate credentials in the authentication dialog box. Users who rely on username/password authentication see a dialog box like that in Figure 10-1.

Figure 10-1 Username/Password Authentication Login Dialog Box



For SDI authentication, the remote user enters a PIN (Personal Identification Number) into the AnyConnect software interface and receives an RSA SecurID passcode. After the user enters the passcode into the secured application, the 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, a PIN, or a passcode 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 10-3, Figure 10-3, and Figure 10-4and

Figure 10-2 Passcode or Pin Dialog Box

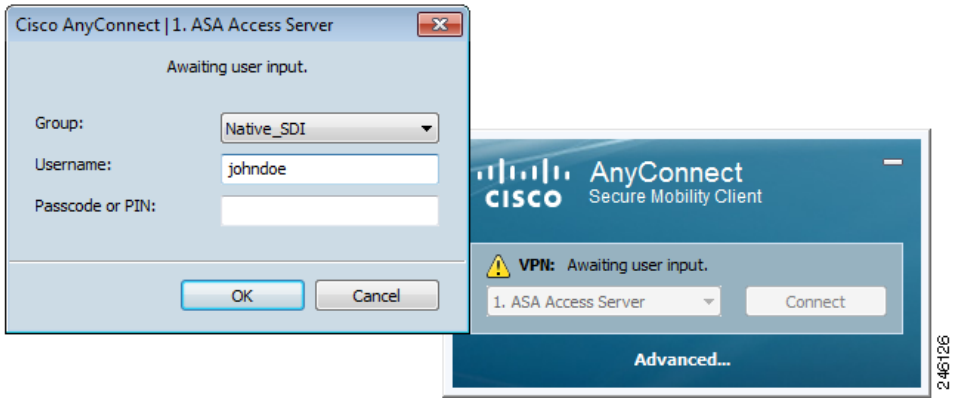


Figure 10-3 PIN Dialog Box

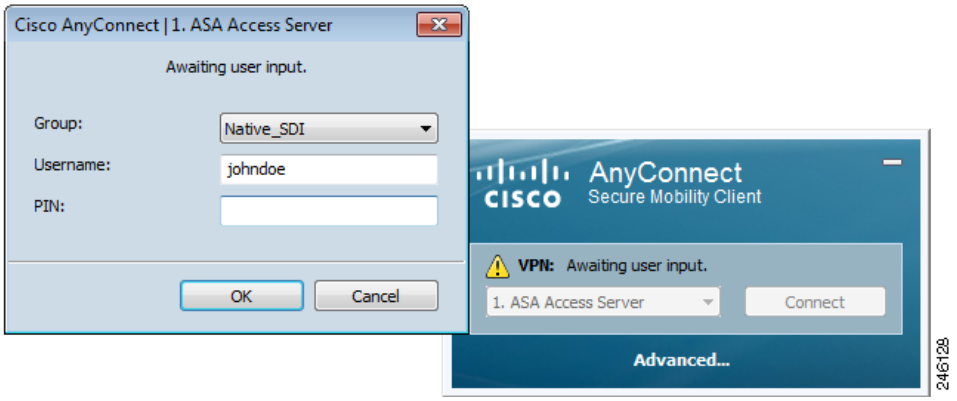
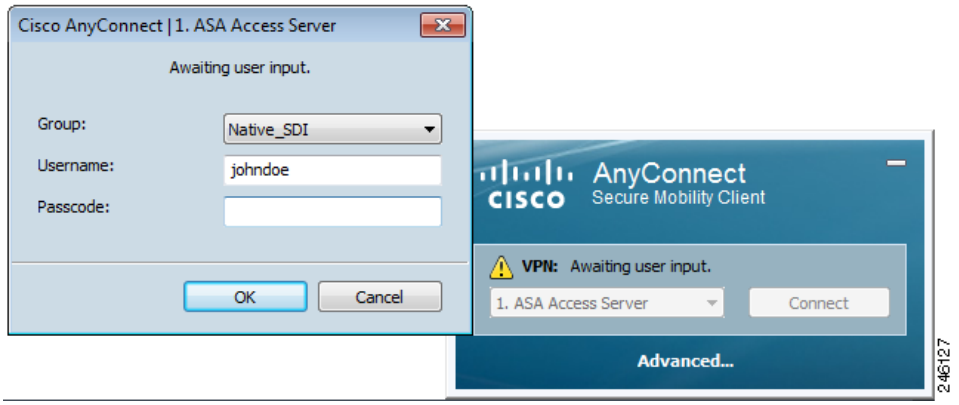


Figure 10-4 Passcode Dialog Box



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, a tunnel-group login page, or 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 Network (Client) Access AnyConnect Connection Profiles page. In either case, the secure gateway sends the client a login page. The main login page contains a drop-down list 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 list of connection profiles or tunnel groups), 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 later, 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.

AnyConnect 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 the ““Next Passcode” and “Next Token Code” Challenges” section on page 10-7.

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, AnyConnect 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 list 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** (Figure 10-5), AnyConnect presents a dialog box on which to enter that PIN (Figure 10-6). The PIN must be a number from 4 to 8 digits long.

Figure 10-5 User Choose to Create a PIN

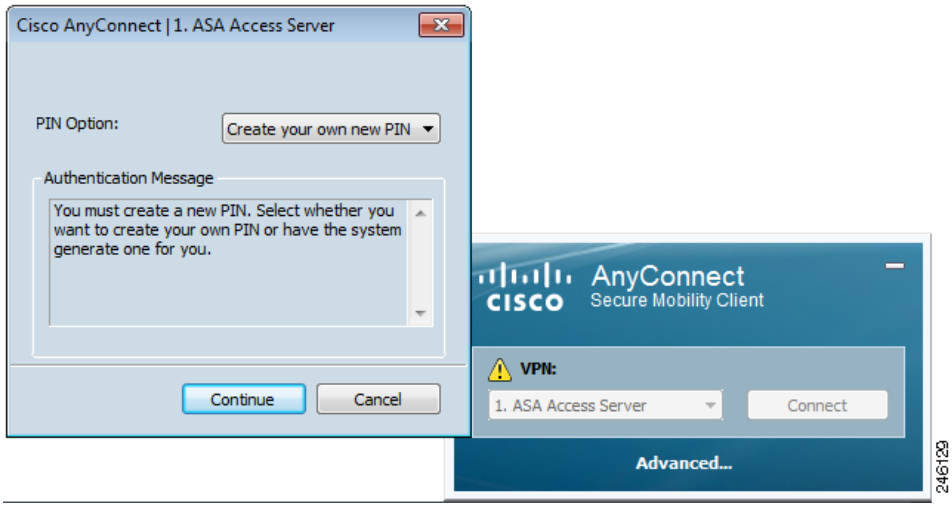
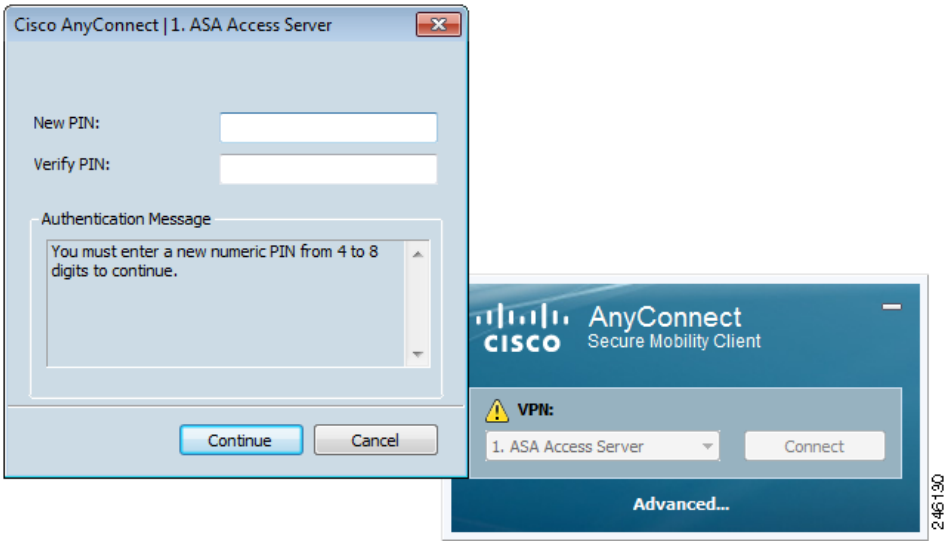


Figure 10-6 Creating a New PIN



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 AnyConnect

This section describes procedures to ensure that AnyConnect 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 and RADIUS/SDI Server Interaction
- Configuring the Security Appliance to Support RADIUS/SDI Messages

AnyConnect and RADIUS/SDI Server Interaction

When a remote user connects to the ASA with AnyConnect and attempts to authenticate using an RSA SecurID token, the ASA 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 ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the ASA 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 AnyConnect, the ASA must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the ASA 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. AnyConnect 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 ASA 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 > AnyConnect Connection Profiles**.

Step 2 Select the connection profile you want to configure to interpret SDI-specific RADIUS reply messages and click **Edit**.

Step 3 In the **Edit AnyConnect Connection Profile** window, expand the Advanced node in the navigation pane on the left and select **Group Alias / Group URL.**

Step 4 Check **Enable the display of SecurID messages on the login screen**.

Step 5 Click **OK**.

Step 6 Choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**.

Step 7 Click **Add** to Add a AAA Server group.

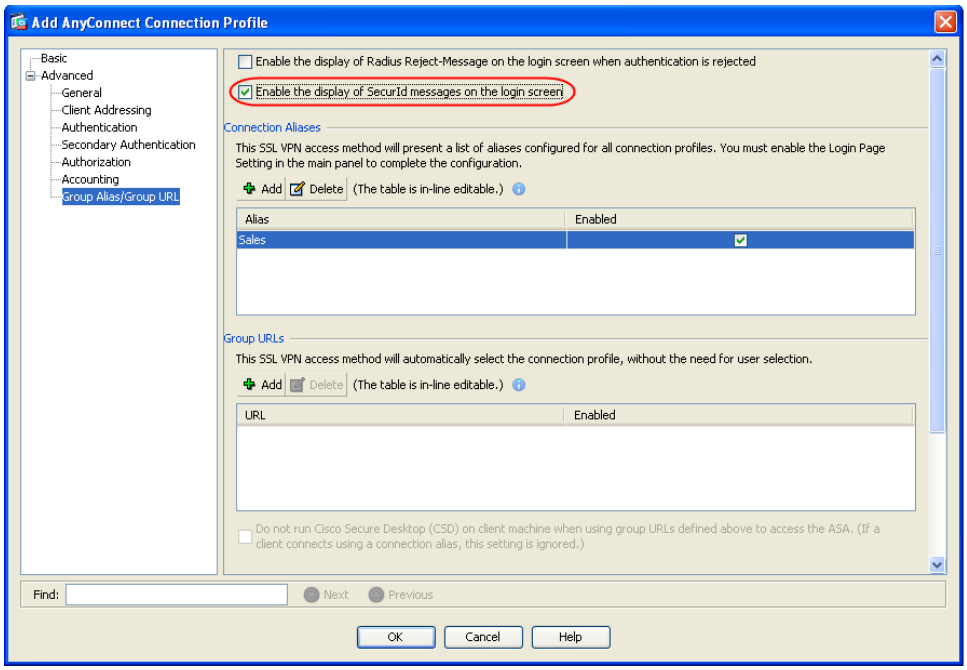
Step 8 Configure the AAA server group in the Edit AAA Server Group dialog and click OK.

Step 9 In the **AAA Server Groups** area, select the AAA server group you just created and then click **Add** in the **Servers in the Selected Group** area.

Step 10 In the SDI Messages area, expand the **Message Table** area. Double-click a message text field to edit the message. Configure the RADIUS reply message text on the ASA to match (in whole or in part) the message text sent by the RADIUS server.

Step 11 Click **OK**. Click **Apply**. Click **Save**.

Figure 10-7 Add/Edit AnyConnect Connection Profile Screen



The default message text used by the ASA 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 ASA. Otherwise, configure the messages to ensure the message text matches.

Table 10-1 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 10-1 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 ASA 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 ASA to indicate the user is ready for the system-generated PIN.

CHAPTER 11

Customizing and Localizing the AnyConnect Client and Installer

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

You can localize (translate) the client and all optional modules for different languages. You can also localize the installer program for the core VPN client.

This chapter contains procedures for customizing and localizing in the following sections:

Customizing the AnyConnect Client

You can customize AnyConnect 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 Cisco AnyConnect Secure Mobility 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 ASA 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.

Note NAM and Web Security do not support the AnyConnect API. If you deploy Web Security or NAM, you must deploy the core AnyConnect client.

- Import a transform (Windows only) that you create for more extensive rebranding. The ASA deploys it with the installer.

The following sections describe procedures for these methods:

Recommended Image Format for AnyConnect 3.0 and Later

For AnyConnect 3.0 and later, we recommend you use Portable Network Graphics (PNG) images with a maximum size of 62x33 pixels for the following reasons:

- PNG images have smaller file sizes than other image formats and use less disk space.
- PNG images support transparency natively.
- The AnyConnect 3.0 and later GUI provides a title adjacent to the logo image in the Advanced window and the tray flyout. Therefore, any title you provided with your image for the earlier client may confuse the user.

Replacing Individual GUI Components with your Custom Components

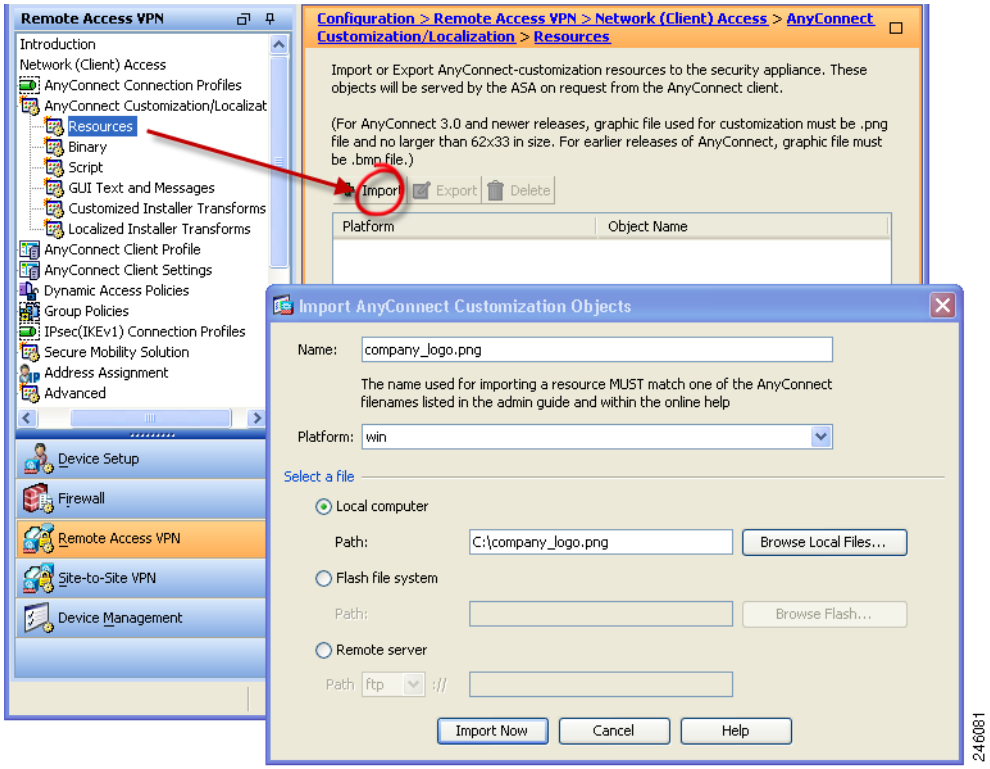
You can customize AnyConnect by importing your own custom files to the security appliance, which deploys the new files with the client. Table 11-2, Table 11-3, and Table 11-4 contain sample images of the original GUI icons and information about their sizes.

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 11-1).

Figure 11-1 Importing a Customization Object

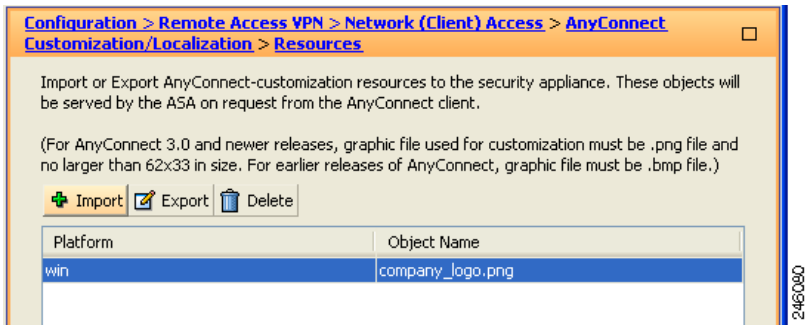


Step 2 Enter the Name of the file to import. See Table 11-2, Table 11-3, and Table 11-4 for the filenames of all the GUI components that you can replace.

Note The filenames of your custom components must match the filenames used by the AnyConnect GUI, which are different for each operating system 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.png*. 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 11-2).

Figure 11-2 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 AnyConnect 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 API. You replace the AnyConnect GUI or the AnyConnect CLI by replacing the client binary files.

Note NAM and Web Security do not support the AnyConnect API. If you deploy Web Security or NAM, you must deploy the core AnyConnect client.

Table 11-1 lists the filenames of the client executable files for the different operating systems.

Table 11-1 Filenames of Client Executables

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

1. Not supported by ASA 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 that you import to the ASA, such as logo images, (See Figure 11-1). Unlike replacing the pre-defined GUI components, when you deploy your own executable, you 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 ASA. A signed binary has a wider range of functionality available to it. If the binaries are not signed, the following functionality is affected:

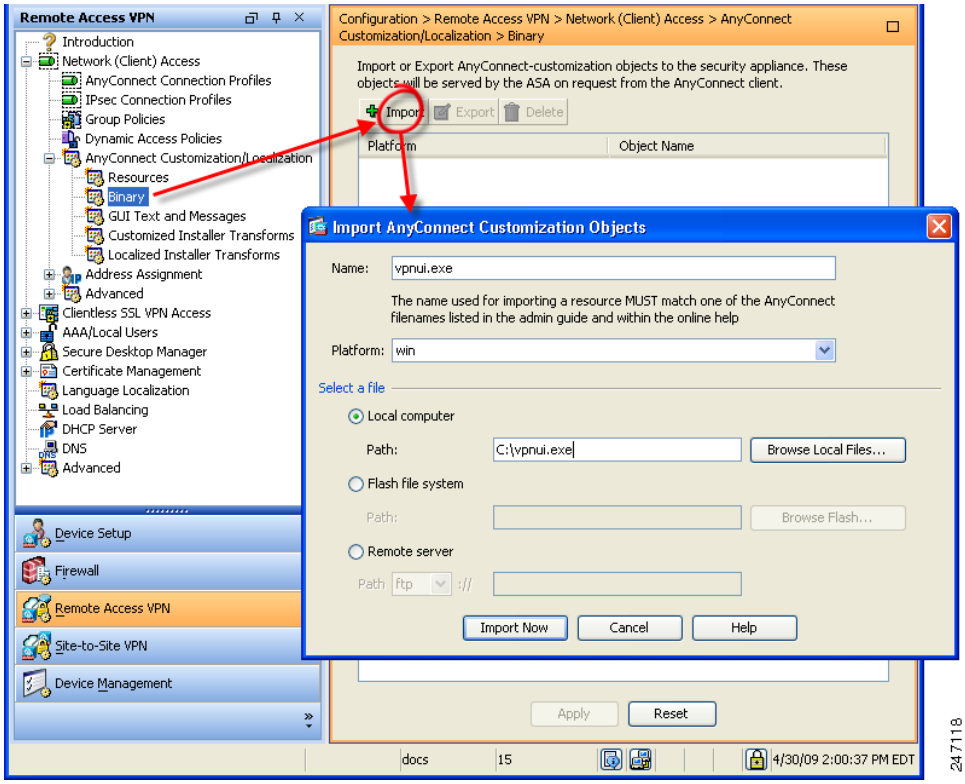
- Web-Launch—The clientless portal is available and the user can authenticate. However, the behavior surrounding tunnel establishment does not work as expected. Having an unsigned GUI on the client results in the client not starting as part of the clientless connection attempt. And once it detects this 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 11-1).

Figure 11-3 Importing an Executable

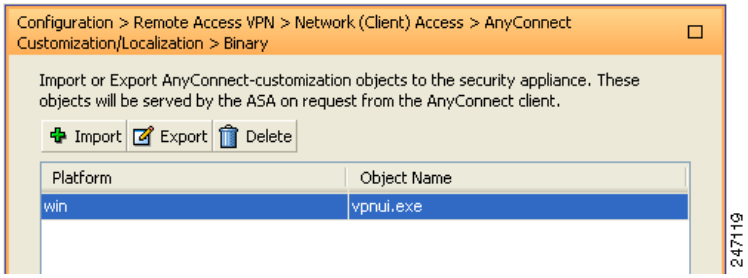


Step 2 Enter the Name of the file to import.

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

Step 3 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table (Figure 11-2).

Figure 11-4 The Imported Executable appears in the table



Customizing the GUI with a Transform

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

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

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

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

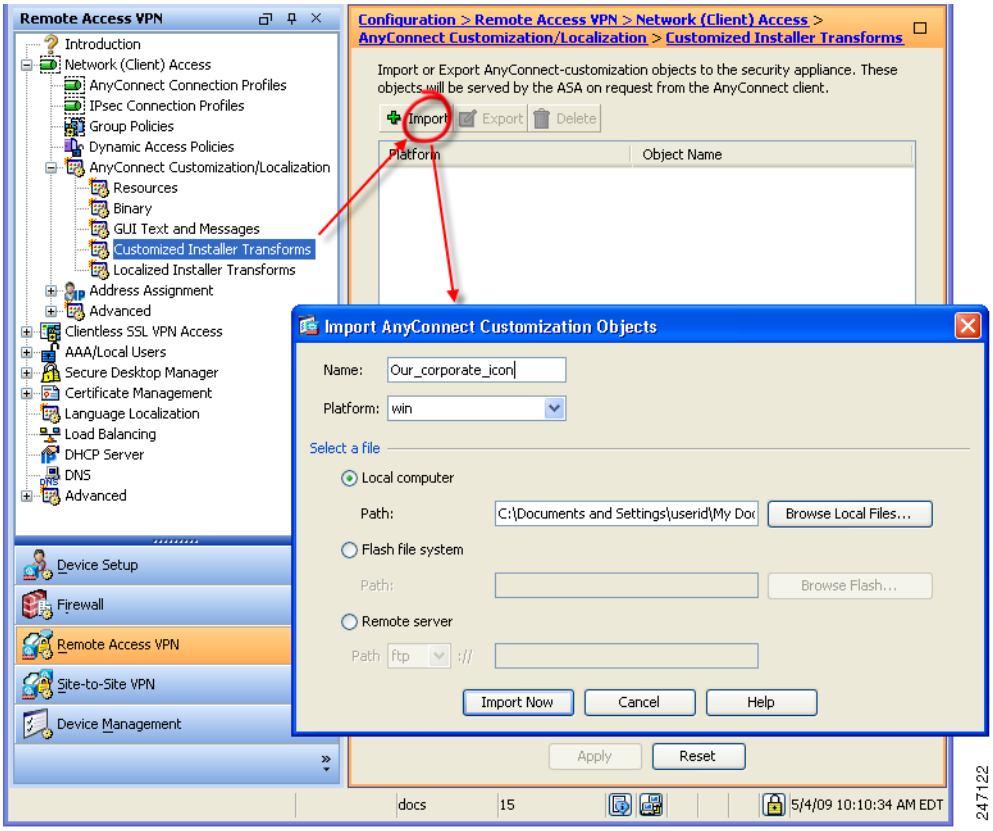
C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi.

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

To import your transform, follow these steps:

Step 1 Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms**. Click **Import**. The Import AnyConnect Customization Objects windows displays (Figure 11-5).

Figure 11-5 Importing a Customizing Transform

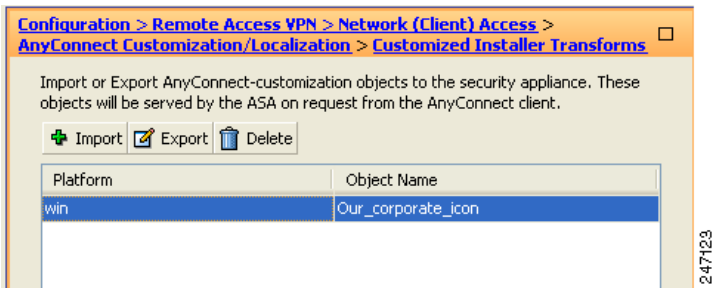


Step 2 Enter the Name of the file to import. Unlike the names of other customizing objects, the name is not significant to the ASA and is for your own convenience.

Step 3 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table (Figure 11-6).

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

Figure 11-6 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 AnyConnect.

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 11-2 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 11-2 AnyConnect for Windows—Icon Files

Filename and Description in Windows Installation	Image Size (pixels, l x h) and Type
about.png The About button in the upper right corner of the Advanced dialog. The size is not adjustable. 	24 x 24 PNG
about_hover.png The About button in the upper right corner of the Advanced dialog. The size is not adjustable. 	24 x 24 PNG
ArrowDown.png The button that allows the user to move networks down in the Networks list of the NAM Advanced window Configuration tab. The size is not adjustable. 	16 x 22 PNG
ArrowDownDisabled.png The disabled button that allows the user to move networks down in the Networks list of the NAM Advanced window Configuration tab. The size is not adjustable. 	16 x 22 PNG
ArrowUp.png The button that allows the user to move networks up in the Networks list of the NAM Advanced window Configuration tab. The size is not adjustable. 	16 x 22 PNG
ArrowUpDisabled.png The disabled button that allows the user to move networks up in the Networks list of the NAM Advanced window Configuration tab. The size is not adjustable. 	16 x 22 PNG

Table 11-2 AnyConnect for Windows—Icon Files (continued)

Filename and Description in Windows Installation	Image Size (pixels, l x h) and Type
company_logo.png The company logo displayed in the top left corner of the tray flyout and Advanced dialog, and bottom right corner of the About dialog. 97x58 is the maximum size. If your custom file is not that size, it is resized to 97x58 in the application. If it is not in the same ratio, it is stretched. 	97 x 58 (maximum) PNG
attention.ico System tray icon alerting the user to a condition requiring attention or interaction. For example, a dialog about the user credentials. The size is not adjustable. 	16 x 16 ICO
error.ico System tray icon alerting the user that something is critically wrong with one or more components. The size is not adjustable. 	16 x 16 ICO
neutral.ico System tray icon indicating client components are operating correctly. The size is not adjustable. 	16 x 16 ICO
vpn_connected.ico System tray icon indicating the VPN is connected. The size is not adjustable. 	16 x 16 ICO

Table 11-2 AnyConnect for Windows—Icon Files (continued)

Filename and Description in Windows Installation	Image Size (pixels, l x h) and Type
cues_bg.jpg The background image for the tray flyout, Advanced window, and About dialog. Because images are not stretched, using a replacement image that is too small results in black space.	1260 x 1024 JPEG
gradient.png The gradient painted behind component titles in the Advanced window. 	1 x 38 PNG
GUI.tif The application and system tray icon. 	
mftogglebtn.png The background of the inactive menu option in the Advanced window. When the AnyConnect installation has multiple components (such as NAM, Web Security, telemetry), the GUI Advanced window displays menu options for each component. This image is used as the background for the menu option when it is inactive. 	300 x 40 PNG

Table 11-2 AnyConnect for Windows—Icon Files (continued)

Filename and Description in Windows Installation	Image Size (pixels, l x h) and Type
mftogglebtn-down.png The background of the Status Overview menu option (when active) in the Advanced window. When the AnyConnect installation has multiple components (such as NAM, Web Security, telemetry), the GUI Advanced window displays menu options for each component. This image is used as the background for the Status Overview when the Advanced window initially opens, and when the user clicks the menu option. 	300 x 40 PNG
mftogglebtn-down-solid.png The background used by Advanced window menu options, other than the Status Overview menu option, when the menu option is activated. When the AnyConnect installation has multiple components (such as NAM, Web Security, telemetry), the GUI Advanced window displays menu options for each component. This image is used as the background for all menu options, other than the Status Overview menu option, when the user clicks the menu option and activates it. 	300 x 40 PNG
minimize.png The minimize button for the tray flyout. The size is not adjustable. 	16 x 16 PNG
minimize-hover.png The minimize button for the tray flyout when the user hovers over it. The size is not adjustable. 	16 x 16 PNG

Table 11-2 AnyConnect for Windows—Icon Files (continued)

Filename and Description in Windows Installation	Image Size (pixels, l x h) and Type
pinned.png The button in the NAM tray flyout tile that allows the user to automatically select a network. The size is not adjustable. 	38 x 30 PNG
pinned_button.png The button in the NAM tray flyout tile, when the user hovers on it, that allows the user to automatically select a network. The size is not adjustable. 	38 x 30 PNG
status_ico_attention.png Attention status icon used by each component in the tray flyout and Advanced window Status Overview pane indicating user attention is required. The size is not adjustable. 	16 x 16 PNG
status_ico_error.png Error status icon used by each component in the tray flyout and Advanced window Status Overview pane indicating a serious error, such as the service being unreachable. The size is not adjustable. 	16 x 16 PNG
status_ico_good.png Good status icon used by each component in the tray flyout and Advanced window Status Overview pane indicating each component is operating properly. The size is not adjustable. 	16 x 16 PNG

Table 11-2 AnyConnect for Windows—Icon Files (continued)

Filename and Description in Windows Installation	Image Size (pixels, l x h) and Type
status_ico_neutral.png Neutral status icon used by each component in the tray flyout and Advanced window Status Overview pane indicating the component is working, but is not necessarily active. The size is not adjustable. 	16 x 16 PNG
status_ico_transition.png Transition status icon used by each component in the tray flyout and Advanced window Status Overview pane indicating the component is between states, such as between connected and disconnected. The size is not adjustable. 	16 x 16 PNG
status_ico_trusted.png Trusted status icon used by each component in the tray flyout and Advanced window Status Overview pane indicating the component is operating properly, but is disabled due to policy, such as set by the Trusted Network Detection (TND) feature. The size is not adjustable. 	16 x 16 PNG
transition_1.ico System tray icon that displays along with transition_2.ico and transition_3.ico indicating one or more client components are in transition between states. For example, when the VPN is connecting or when NAM is connecting. The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 PNG
transition_2.ico System tray icon that displays along with transition_1.ico and transition_3.ico indicating one or more client components are in transition between states. For example, when the VPN is connecting or when NAM is connecting. The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 PNG

Table 11-2 AnyConnect for Windows—Icon Files (continued)

Filename and Description in Windows Installation	Image Size (pixels, l x h) and Type
transition_3.ico System tray icon that displays along with transition_1.ico and transition_2.ico indicating one or more client components are in transition between states. For example, when the VPN is connecting or when NAM is connecting. The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 PNG
unpinned.png The button in the NAM tray flyout tile that allows the user to connect exclusively to the current network. The size is not adjustable. 	38 x 30 PNG
unpinned_button.png The button in the NAM tray flyout tile, when the user hovers on it, that allows the user to connect exclusively to the current network. The size is not adjustable. 	38 x 30 PNG

For Linux

All files for Linux are located in /opt/cisco/vpn/pixmaps/. Table 11-3 lists the files that you can replace and the client GUI area affected.

Table 11-3 AnyConnect for Linux—Icon Files

Filename and Description in Linux Installation	Image Size (pixels, l x h) and Type
company-logo.png Corporate logo that appears on each tab of the user interface. For AnyConnect 3.0 and later, use PNG images no bigger than 62x33 pixels. 	142 x 92 PNG
cvc-about.png Icon that appears on the About tab. 	16 x 16 PNG
cvc-connect.png Icon that appears next to the Connect button, and on the Connection tab. 	16 x 16 PNG
cvc-disconnect.png Icon that appears next to the Disconnect button. 	16 x 16 PNG
cvc-info.png Icon that appears on the Statistics tab. 	16 x 16 PNG
systray_connected.png Tray icon that displays when the client is connected. 	16 x 16 PNG
systray_notconnected.png Tray icon that displays when the client is not connected. 	16 x 16 PNG

Table 11-3 AnyConnect for Linux—Icon Files

Filename and Description in Linux Installation	Image Size (pixels, l x h) and Type
systray_disconnecting.png Tray icon that displays when the client is disconnecting. 	16 x 16 PNG
systray_quarantined.png Tray icon that displays when the client is quarantined 	16x16 PNG
systray_reconnecting.png Tray icon that displays when the client is reconnecting. 	16 x 16 PNG
vpnui48.png Main program icon. 	48 x 48 PNG

For Mac OS X

All files for OS X are located in /Applications/Cisco AnyConnect VPN Client/Contents/Resources. Table 11-4 lists the files that you can replace and the client GUI area affected.

Table 11-4 AnyConnect for Mac OS X—Icon Files

Filename in Mac OS X Installation	Image Size (pixels, l x h)
bubble.png Notification bubble that appears when the client connects or disconnects. 	142 x 92 PNG
connected.png Icon that displays under the disconnect button when the client is connected. 	32 x 32 PNG
logo.png Logo icon that appears on main screen in the top right corner. 	50 x 33 PNG
menu_connected.png Connected state menu bar icon. 	16 x 16 PNG
menu_error.png Error state menu bar icon. 	16 x 16 PNG
menu_idle.png Disconnected idle menu bar icon. 	16 x 16 PNG
menu_quarantined.png Quarantined state menu bar icon 	16 x 16 PNG

Table 11-4 AnyConnect for Mac OS X—Icon Files

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

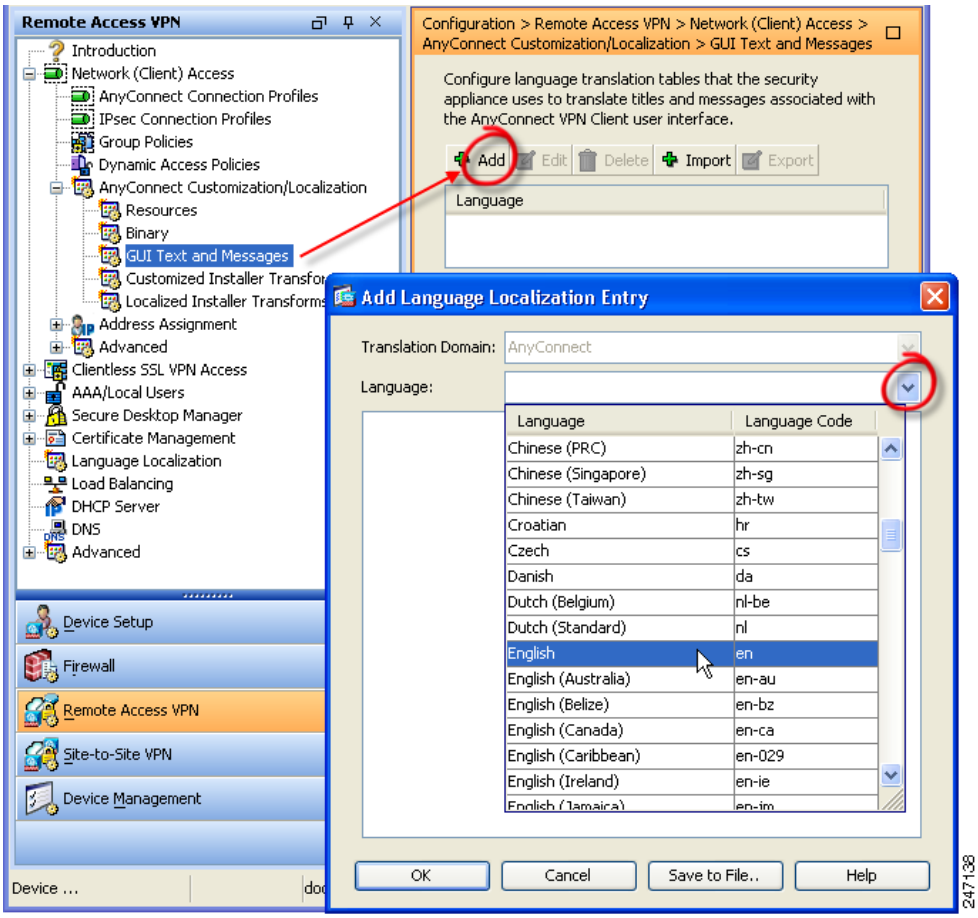
Changing the Default AnyConnect English Messages

You can make changes to the English messages displayed on the AnyConnect 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 11-9).

Figure 11-7 Adding an English Translation Table

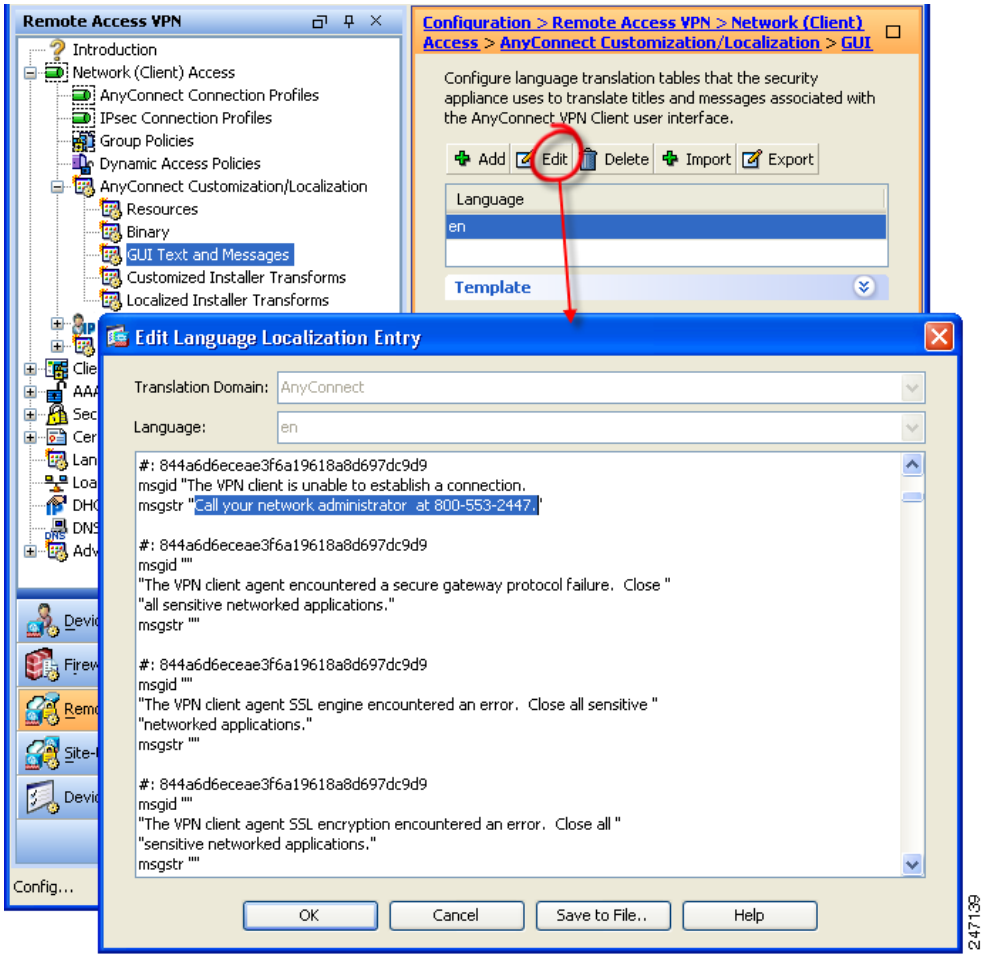


Step 2 Click the Language drop-list and specify the language as *English* (en). The translation table for English displays in the list of languages in the pane.

Step 3 Click **Edit** to begin editing the messages. The Edit Language Localization Entry window displays (Figure 11-8). 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 you own text between the quotes of the msgstr.

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

Figure 11-8 Editing the Message Text



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

Localizing the AnyConnect Client GUI and Installer

You can localize (translate) the client and all optional modules for different languages. You can also localize the installer program for the core VPN client that provides VPN service.

Note If you are deploying AnyConnect 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 ASA deploys the client.

The following sections contain information and procedures for configuring this feature:

Localizing the AnyConnect GUI

The security appliance uses translation tables to translate user messages displayed by AnyConnect. The translation tables are text files with strings to insert translated message text. The AnyConnect package file for Windows contains an English language template for AnyConnect messages. The ASA 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 ASA 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 ASA, 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 ASA, 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 the "Using Tools to Create Message Catalogs for Enterprise Deployment" section on page 11-32 for more information.

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

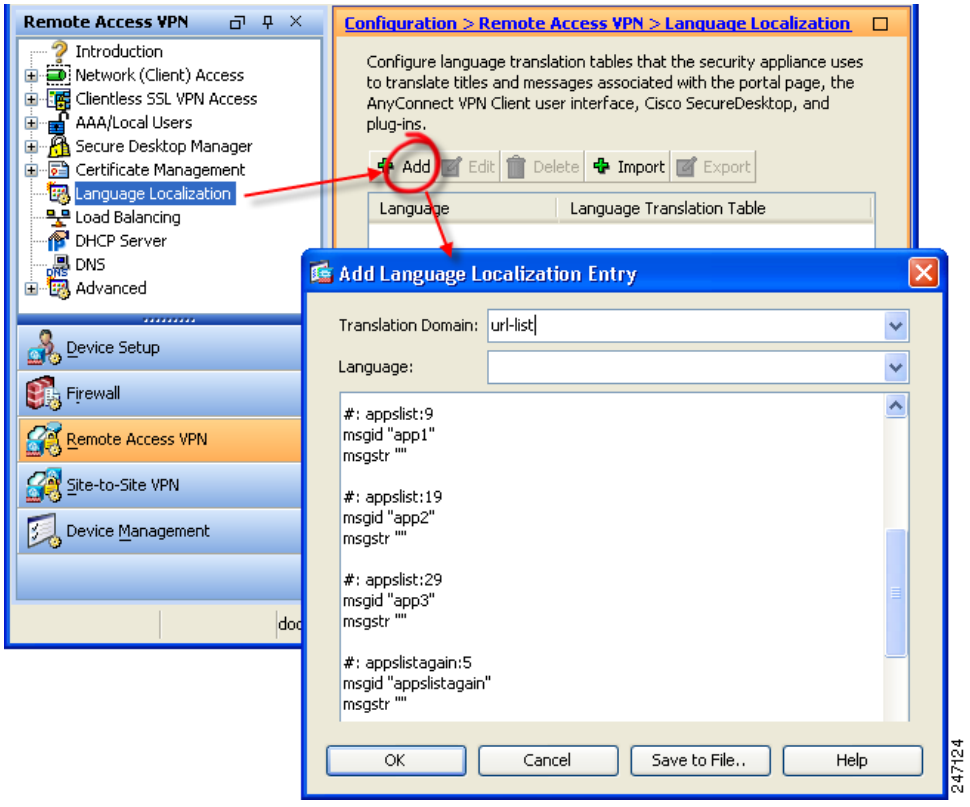
- Translating using the ASDM Translation Table Editor, page 11-23
- Translating by Exporting the Translation Table for Editing, page 11-27

Translating using the ASDM Translation Table Editor

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

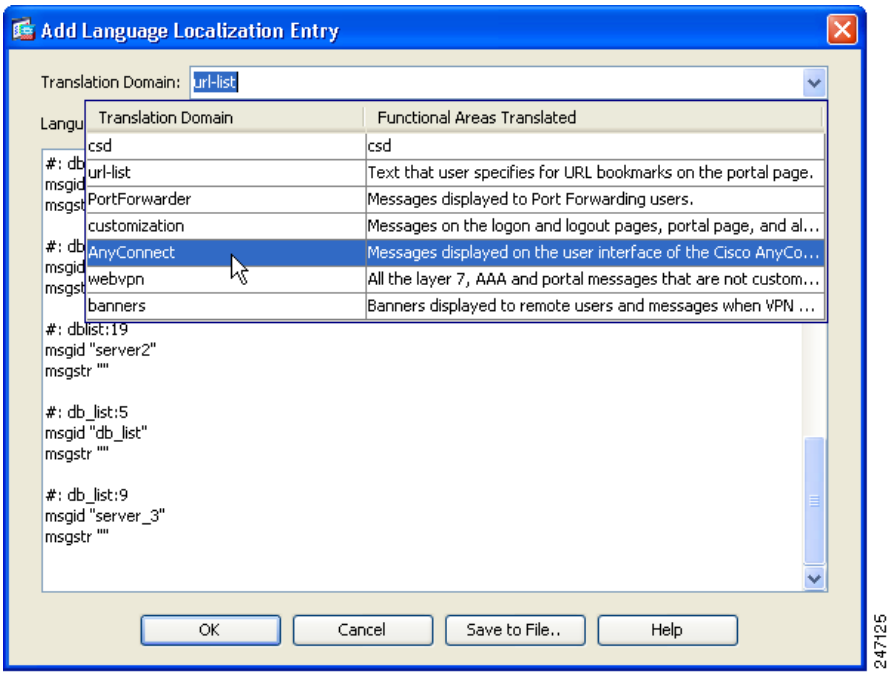
Step 1 Go to **Configuration > Remote Access VPN > Language Localization**. Click **Add**. The Add Language Localization Entry window displays (Figure 11-9).

Figure 11-9 Language Localization Pane



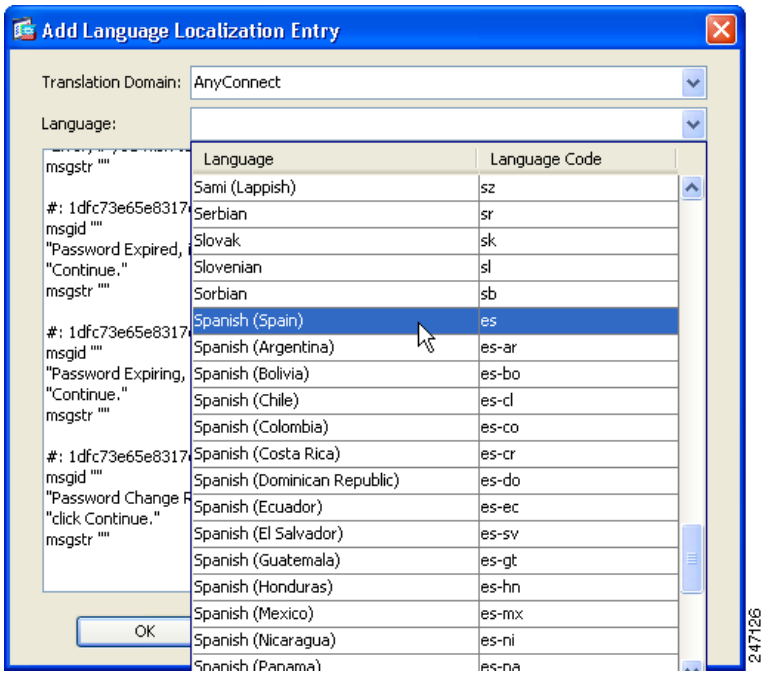
Step 2 Click the **Translation Domain** drop-list and choose **AnyConnect** (Figure 11-10). This ensures only the messages relating to the AnyConnect GUI appear for editing purposes.

Figure 11-10 Translation Domain



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

Figure 11-11 Choosing a Language

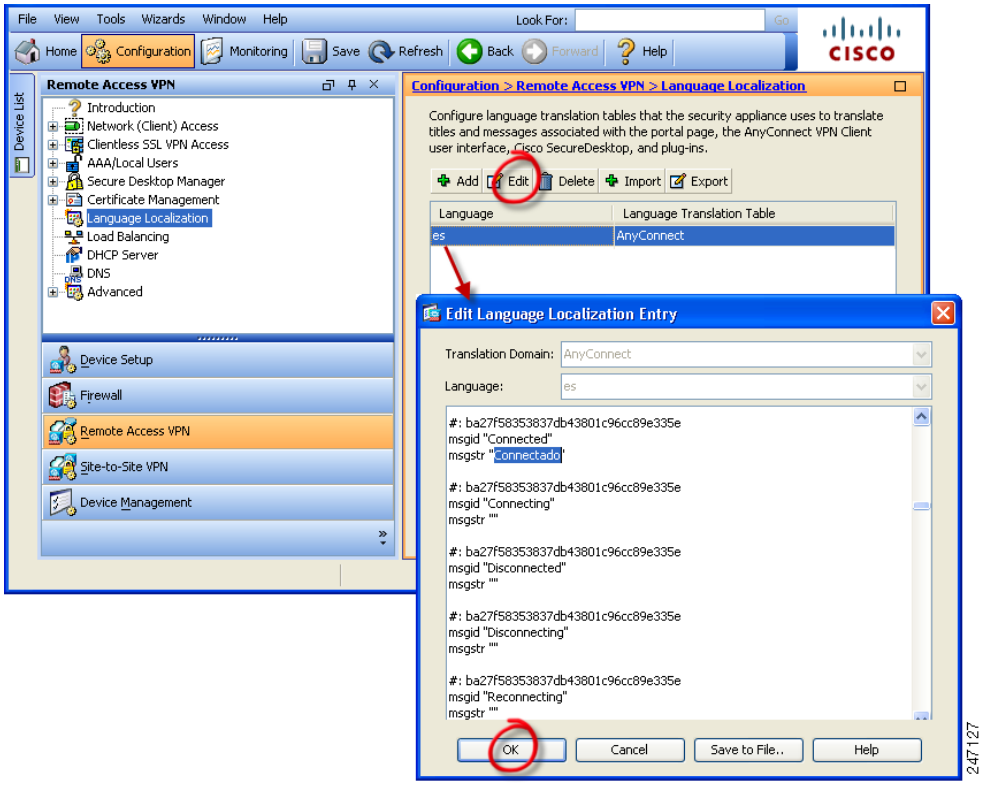


Step 4 The translation table now displays in the list of languages in the pane (*es* in our example). However, it has no translated messages. To begin adding translated text, click **Edit**. The Edit Language Localization Entry window displays (Figure 11-12).

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

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

Figure 11-12 Editing the Translation Table



Translating by Exporting the Translation Table for Editing

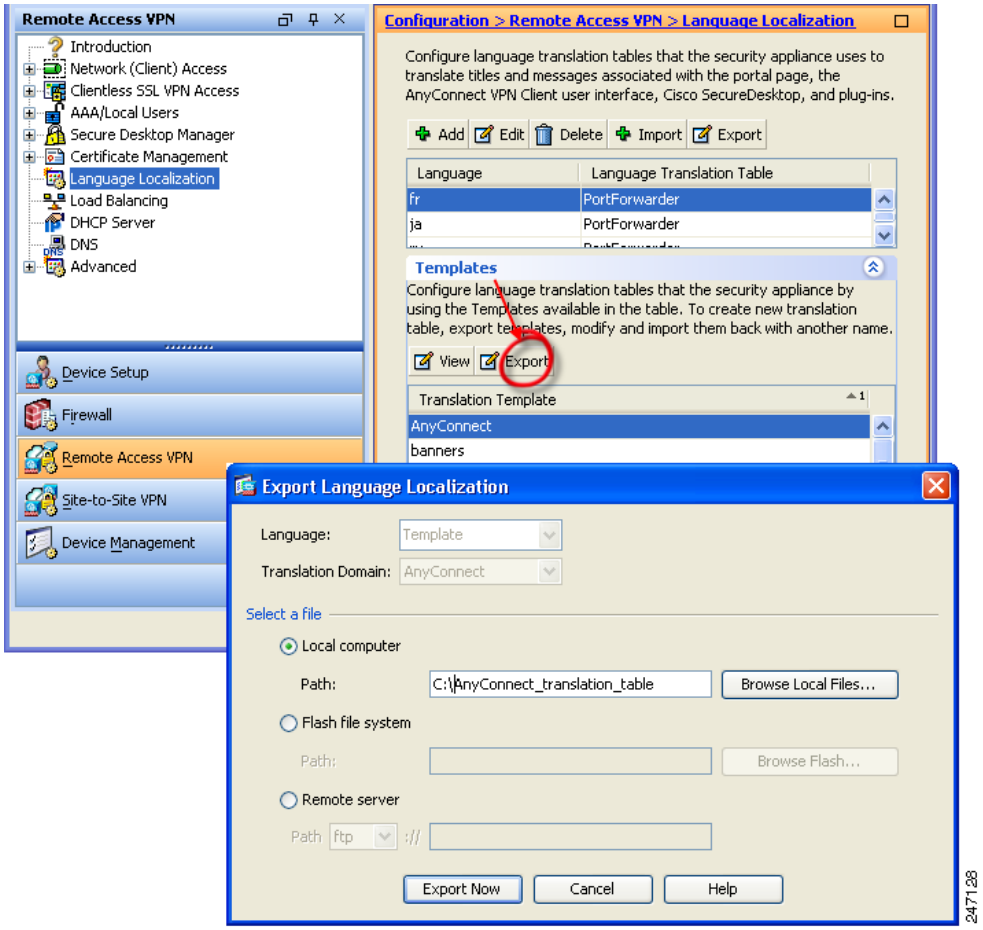
This procedure shows you how to export the AnyConnect translation template to a remote computer, where you can edit the table using an editor or using third party tools such as Gettext or Poedit.

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

Step 1 Export the AnyConnect translation template.

Go to **Configuration > Remote Access VPN > Language Localization**. The language localization pane displays (Figure 11-13). Click the **Templates** link to display a table of available templates. Select the *AnyConnect* template and click **Export**. The Export Language Localization window displays.

Figure 11-13 Exporting a Translation Template



Step 2 Choose a method to export and provide a filename. In Figure 11-13, we export to a local computer with the filename *AnyConnect_translation_table*.

Step 3 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 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 4 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 11-13). Click **Import**. The Import Language Localization window displays.

Step 5 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 6 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 11-13, we specify the language as *Spanish* (es) and import the same file we exported in Step 1 (AnyConnect_translation_table). Figure 11-15 shows the new translation table for Spanish in the list of Languages for AnyConnect.

Figure 11-14 Importing a Translation Template as a new Translation Table

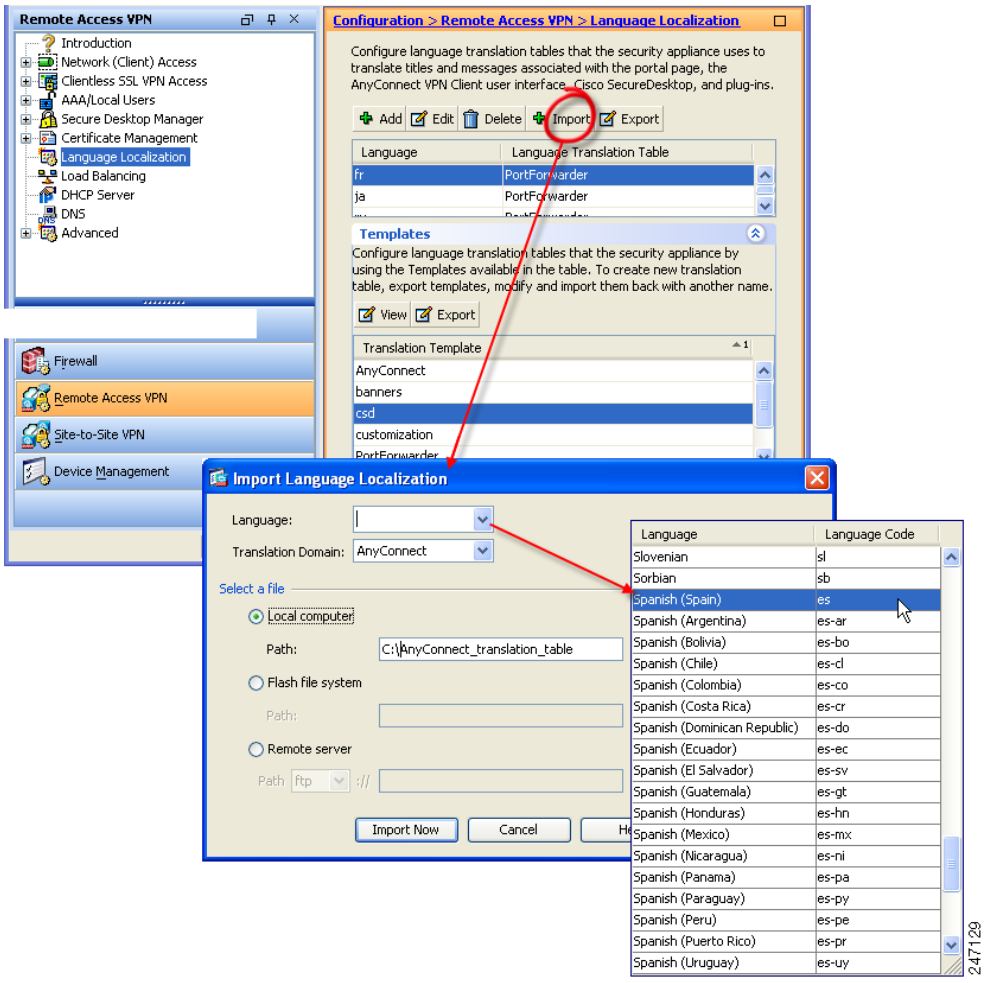
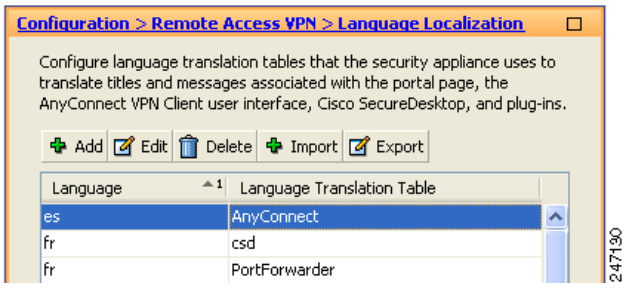


Figure 11-15 New Language Displayed in Language Table



Localizing the AnyConnect Installer Screens

As with the AnyConnect GUI, you can translate messages displayed by the client installer program that installs the VPN service. The ASA uses transform 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.

Note Every release of AnyConnect includes a localized transform that administrators can upload to the ASA whenever they upload AnyConnect packages with new software. If you are using our localization transform, make sure to update them with the latest release from CCO whenever you upload a new AnyConnect package.

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 ASA. 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 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 ASA as a new language. With Orca, the database editor from Microsoft, you can modify existing installations and new files. Orca is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK. The following link leads to the bundle containing the Orca program:

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

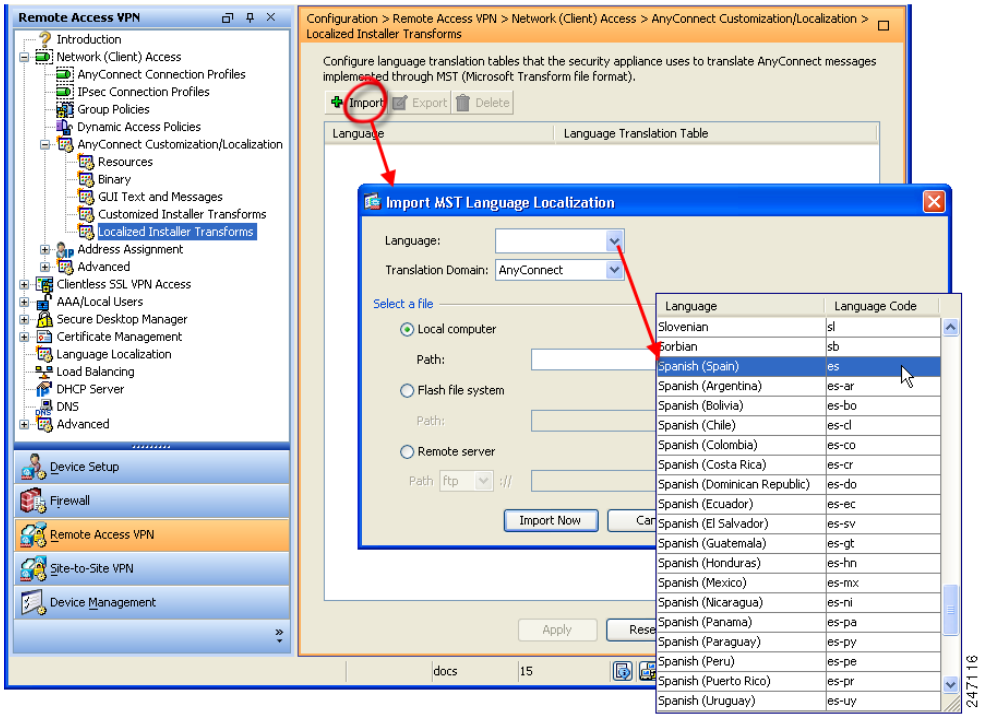
After you install the SDK, the Orca MSI is located here:

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

The following procedure shows how to import a transform to the ASA 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 11-16):

Figure 11-16 Importing a Transform to Translate the Installer Program



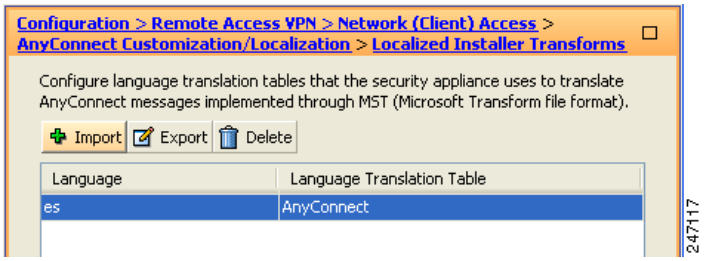
Step 2 Choose a language for this transform. Click the **Language** drop-list to display languages and their industry-recognized abbreviations. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.

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 11-16, we specify the language as *Spanish* (es). Figure 11-17 shows the new transform for Spanish in the list of Languages for AnyConnect.

Figure 11-17 Imported Transform Displays in the Table



Using Tools to Create Message Catalogs for Enterprise Deployment

If you are not deploying the client with the ASA, 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 for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at poedit.net.

The AnyConnect message template is located in these folders:

Windows XP:

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect VPN Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES

Windows Vista:

%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect VPN Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES

Mac OS X and Linux:

/opt/cisco/vpn/l10n/<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 AnyConnect 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 for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at poedit.net. Both methods are covered in the procedure below.

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

Note This step assumes you have already loaded the latest AnyConnect image package to the ASA. 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 12

Managing, Monitoring, and Troubleshooting AnyConnect Sessions

This chapter explains these subjects and tasks:

Disconnecting All VPN Sessions

To log off all SSL VPN sessions, including Cisco AnyConnect Secure Mobility client 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 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.

The options available in this window depend on the packages that are loaded on the client PC. If an option is not available, its 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 AnyConnect Diagnostics and Reporting Tool (DART) wizard which bundles specified log files and diagnostic information that can be used for analyzing and debugging the client connection. See Using DART to Gather Troubleshooting Information, page 12-4 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.

Clicking on Logging opens the 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 ASA. 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 AnyConnect,

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 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 ASA and the client by reducing the size of the packets being transferred. By default, compression for all SSL VPN connections is enabled on the ASA, both at the global level and for specific groups or users. For broadband connections, compression might result in poorer performance.

Note The Cisco AnyConnect Secure Mobility 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 AnyConnect Diagnostics and Reporting Tool that you can use to collect data useful for troubleshooting AnyConnect install and connection problems. DART supports Windows 7, Windows Vista, Windows XP. Mac version 10.5 and 10.6, and Linux Redhat.

The DART wizard runs on the computer that runs AnyConnect. 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 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.

Getting the DART Software

DART is available as part of the AnyConnect 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 Client Software Download site, regardless of the AnyConnect version you are using.

Table 12-1 provides the AnyConnect downloads containing DART for both the pre-deploy and web deploy (downloaded) installer:

Table 12-1 DART Package Filenames for ASA or Pre-Deployment

DART	Web-Deploy Installer (Downloaded)	Pre-Deploy Installer
Windows	anyconnect-dart-win-(ver)-k9.msi	anyconnect-dart-win-(ver)-k9.msi
Mac	anyconnect-dartsetup.dmg	anyconnect-dart-macosx-i386-(ver)-k9.dmg
Linux	anyconnect-dartsetup.sh	anyconnect-dart-linux-(ver)-k9.tar.gz
Linux-64	anyconnect-dartsetup.sh	anyconnect-dart-linux-64-(ver)-k9.tar.gz

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 AnyConnect downloads to a PC running Windows, a new version of DART, if available, downloads along with it. When a new version of the AnyConnect downloads as part of an automatic upgrade, it 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 ASA, 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 AnyConnect. When the user connects, DART is upgraded automatically when an AnyConnect package with a higher version of DART is uploaded and configured on the ASA.

To run DART, see Running DART on a Windows PC, page 12-6.

Manually Installing DART on the Host

Note These steps may vary slightly on a Mac or Linux operating system.

Step 1 Get the DART software from Cisco.com. See, Getting the DART Software, page 12-4, and store anyconnect-dart-win-(ver)-k9.msi locally.

Step 2 Double-click the **anyconnect-dart-win-(ver)-k9.msi** file to launch the **DART Setup Wizard**.

Step 3 Click **Next** at the Welcome screen.

Step 4 Select **I accept the terms in the License Agreement** to accept the end user license agreement and click **Next**.

Step 5 Click **Install** to install DART. The installation wizard installs **DartOffline.exe** in the <System Drive>:\Program Files\Cisco\Cisco DART directory.

Step 6 Click **Finish** to complete the installation.

To run DART, see Running DART on a Windows PC, page 12-6.

Running DART on a Windows PC

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

Note These steps may vary slightly on a MAC or Linux operating system.

Step 1 Launch the AnyConnect 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.

  Note Default is the only option for MAC. You cannot customize which files to include in the bundle.

- 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 (*).

Note Masking the password is not an option for MAC operating systems.

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. You have an option to include NAM, Telemetry, Posture, and Web Security logs. 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.

Installing the AnyConnect Client

If you configure the AnyConnect images with the **svc image xyz** command, you must issue the **svc enable** command. Without issuing this command, AnyConnect does not function as expected, and **show webvpn svc** states that the "SSL VPN client is not enabled," instead of listing the installed AnyConnect packages.

Installing the Log Files

The log files are retained in the following files:

- \Windows\setupapi.log — Windows XP and 2K
- \Windows\Inf\setupapi.app.log — Windows Vista
- \Windows\Inf\setupapi.dev.log —Windows Vista

Note In Vista, you must make the hidden files visible.

If registry information is missing from the setupapi.log file, enable verbose logging on a Windows XP-based computer. Follow these steps to enable verbose logging on a Window XP-based computer:

Note Serious problems could result if the registry is modified incorrectly. For added protection, back up the registry before you modify it.

Step 1 Click **Start > Run**.

Step 2 Type **regedit** in the Open field and click **OK**.

Step 3 Locate and double click **LogLevel** in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup registry subkey.

Step 4 Choose **Hexadecimal** on the Base pane of the Edit DWORD Value window.

Step 5 Type **0x2000FFFF** in the Value data box.

Step 6 Click **OK**.

Note When you enable verbose logging, the size of the Setupapi.log file grows to approximately 4 megabytes (MB). Follow these steps again to reset the registry value but instead set the DWORD value (in Step 5) to 0.

Web Install of Log Files

If this is an initial web deployment install, the log file is located in the per-user temp directory:

%TEMP%\anyconnect-win-2.X.xxxx-k9-install-yyyyyyyyyyyyyy.log.

If an upgrade was pushed from the optimal gateway, the log file is in the following location:

%WINDIR%\TEMP\anyconnect-win-2.X.xxxx-k9-install-yyyyyyyyyyyyyy.log.

Obtain the most recent file for the version of the client you want to install. The *xxx* varies depending on the version, and the **yyyyyyyyyyyyyy** specifies the date and time of the install.

Standalone Install of Log Files

To turn on MSI logging and capture logs of the install, run the following:

MSIExec.exe/i anyconnect-win-2.X.xxxx-pre-deploy-k9.msi/lvx* c:\AnyConnect.log

where *anyconnect-win-2.X.xxxx-pre-deplay-k9.msi* is the full name of the actual msi file that you want to install.

The log appears in the following locations:

- \Documents and Settings\<username>\Local Settings\Temp —on Windows XP/Win2K
- \Users\<username>\AppData\Local\Temp —on Vista
- \Windows\Temp —if an automatic upgrade

If you intend to use standalone only (or you do not want ActiveX control installed on your system), perform one of the following:

Note Without these actions, you may receive a Cisco AnyConnect VPN Error 1722 indicating a problem with the Windows Installer package.

- Create an MSI transform to set the ActiveX property to disabled (NOINSTALLACTIVEX=1):

```
MISExec /i anyconnect-win-x.x.xxxx-pre-deploy-k9.msi NOINSTALLACTIVEX=1
```

- Perform a quiet install without a reboot:

```
msiexec /quiet /i "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
msiexec /quiet /norestart /i "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi
```

- Perform a quiet uninstall without a reboot:

```
msiexec /quiet /x "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
```

Note The value of *x.x.xxx* depends on the version being installed.

Problems Disconnecting AnyConnect or Establishing Initial Connection

If you experience problems disconnecting the AnyConnect client or establishing an initial connection, follow these suggestions:

1. Obtain the config file from the ASA to look for signs of a connection failure:
   - From the ASA console, type **write net x.x.x.x:ASA-Config.txt**, where *x.x.x.x* is the IP address of the TFTP server on the network.
   - From the ASA console, type **show running-config**. Cut and paste the config into a text editor and save.

2. View the ASA event logs.
   a. At the ASA console, add the following lines to look at the ssl, webvpn, svc, and auth events:

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

   b. Attempt an AnyConnect client connection, and when the connect error occurs, cut and paste the log information from the console into a text editor and save.
   c. Type **no logging enable** to disable logging.
3. On the client PC, get the Cisco AnyConnect VPN client log from the Windows Event Viewer.
   a. Choose **Start > Run** and type **eventvwr.msc /s**.
   b. Locate the **Cisco AnyConnect VPN Client** in the Applications and Services Logs (of Windows Vista and Win7) and choose **Save Log File As..**.
   c. Assign a filename like AnyConnectClientLog.evt. You must use the .evt file format.
4. Attach the vpnagent.exe process to the Windows Diagnostic Debug Utility if you are having problems with disconnecting or closing the AnyConnect GUI. Refer to the WinDbg documentation for additional information.
5. If a conflict with the IPv6/IPv4 IP address assignment is identified, obtain sniffer traces and add additional routing debugs to the registry of the client PC being used. These conflicts may appear in the AnyConnect event logs as follows:

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

   Route debugging can be enabled on a one-time basis for a connection by adding a specific registry entry (Windows) or file (Mac/Linux) prior to making the VPN connection.

   When a tunnel connection is started and this key or file is found, two route debug text files are created in the system temp directory (usually C:\Windows\Temp on Windows and /tmp on Mac or Linux). The two files (debug_routechangesv4.txt4 and debug_routechangesv6.txt) are overwritten if they already exist.

Problems Passing Traffic

If the AnyConnect client cannot send data to the private network once connected, follow these suggestions:

1. Obtain the output of the show vpn-sessiondb detail svc filter name <username> command. If the output specifies Filter Name: XXXXX, get the output for the show access-list XXXXX command as well. Verify that the ACL is not blocking the intended traffic flow.
2. Obtain the DART file or the output from AnyConnect VPN Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt). Observe the statistics, interfaces, and routing table.

3. Check the ASA config file for NAT statements. If NAT is enabled, you must exempt data returning to the client from network address translation. For example, to NAT exempt the IP addresses from the AnyConnect pool, the following code would be used:

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. Verify whether the tunneled default gateway is enabled for the setup. The traditional default gateway is the gateway of last resort for non-decrypted traffic:

```
route outside 0.0.83.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

   If a VPN client needs to access a resource that is not in the routing table of the VPN gateway, packets are routed by the standard default gateway. The VPN gateway does not need to have the whole internal routing table. If you use a tunneled keyword, the route handles decrypted traffic coming from IPsec/SSL VPN connection. Standard traffic routes to 83.145.50.1 as a last resort, while traffic coming from the VPN routes to 10.0.4.2 and is decrypted.

5. Collect a text dump of ipconfig /all and a route print output before and after establishing a tunnel with AnyConnect.

6. Perform a network packet capture on the client or enable a capture on the ASA.

Note If some applications (such as Microsoft Outlook) do not operate with the tunnel, ping a known device in the network with a scaling set of pings to see what size gets accepted (for example, ping -l 500, ping -l 1000, ping -l 1500, and ping -l 2000). The ping results provide clues to the fragmentation issues in the network. Then you can configure a special group for users who might experience fragmentation and set the svc mtu for this group to 1200. You can also copy the Set MTU.exe utility from the old IPsec client and force the physical adapter MTU to 1300. Upon reboot, see if you notice a difference.

Problems with AnyConnect Crashing

When a crash in the UI occurs, the results are written to the %temp% directory (such as C:\DOCUME~1\jsmith\LOCALS~1\Temp). If you receive a “The System has recovered from a serious error” message after a reboot, gather the .log and .dmp generated files from C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson or a similar application. Either copy them or follow the steps below to back up the files.

Step 1 Run the Microsoft utility called Dr. Watson (Drwtsn32.exe) from the Start > Run menu.

Step 2 Configure the following and click **OK**:

```
Number of Instructions : 25
Number of Errors to Save : 25
Crash Dump Type : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

Step 3 On the client PC, get the Cisco AnyConnect VPN client log from the Windows Event Viewer by entering **eventvwr.msc /s** at the Start > Run menu.

Step 4 Locate the **Cisco AnyConnect VPN Client** in the Applications and Services Logs (of Windows Vista and Win7) and choose **Save Log File As..**. Assign a filename such as AnyConnectClientLog.evt in the .evt file format.

Step 5 If a driver crash occurs in VPNVA.sys, check for any intermediate drivers that are bound to the Cisco AnyConnect Virtual Adapter and uncheck them.

Step 6 If a driver crash occurs in vpnagent.exe, attach the vpnagent.exe process to the debugging tools for Windows. After the tools are installed, perform the following:

a. Create a directory called c:\vpnagent.

b. Look at the Process tab in the Task Manager and determine the PID of the process in vpnagent.exe.

c. Open a command prompt and change to the directory where you installed the debugging tools. By default, the debugging tools for Windows are located in C:\Program Files\Debugging Tools.

d. Type **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst**, where *PID* is the number determined in Step b.

Let the open window run in minimized state. You cannot log off of the system while you are monitoring.

e. When the crash occurs, collect the contents of c:\vpnagent in a zip file.

f. Use **!analyze -v** to further diagnose the crashdmp file.

Problems Connecting to the VPN Service

If you receive an “Unable to Proceed, Cannot Connect to the VPN Service” message, the VPN service for AnyConnect is not running. Most likely, the VPN agent exited unexpectedly. To troubleshoot whether another application conflicted with the service, follow these steps:

Step 1 Check the services under the Windows Administration Tools to ensure that the Cisco AnyConnect VPN Agent is *not* running. If it is running and the error message still appears, another VPN application on the workstation may need disabled or even uninstalled, rebooted, and retested.

Step 2 Try to start the Cisco AnyConnect VPN Agent. This determines if the conflict is with the initialization of the server at boot-up or with another running service (because the service failed to start).

Step 3 Check the AnyConnect logs in the Event Viewer for any messages stating that the service was unable to start. Notice the time stamps of the manual restart from Step 2, as well as when the workstation was booted up.

Step 4 Check the System and Application logs in the Event Viewer for the same general time stamps of any messages of conflict.

Step 5 If the logs indicate a failure starting the service, look for other information messages around the same time stamp which indicate one of the following:

- a missing file—reinstall the AnyConnect client from a standalone MSI installation to rule out a missing file.
- a delay in another dependent service—disable startup activities to speed up the workstation’s boot time
- a conflict with another application or service—determine whether another service is listening on the same port as the port the vpnagent is using or if some HIDS software is blocking our software from listening on a port

If the logs do not point directly to a cause, use the trial and error method to identify the conflict. When the most likely candidates are identified, disable those services (such as VPN products, HIDS software, spybot cleaners, sniffers, antivirus software, and so on) from the Services panel. After rebooting, if the VPN Agent service still fails to start, start turning off services that were not installed by a default installation of the operating system.

Obtaining the PC's System Information

Type the following and wait about two minutes to obtain the PC's system info:

- **winmsd /nfo c:\msinfo.nfo** — on Windows XP or 2K
- **msinfo32 /nfo c:\msinfo.nfo** —on Vista

Obtaining a Systeminfo File Dump

On Windows XP or Vista, type the following at a command prompt to obtain a systeminfo file dump:

systeminfo >> c:\sysinfo.txt

Checking the Registry File

An entry in the SetupAPI log file as below indicates a file cannot be found:

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

Make sure the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce registry key exists. Without this registry key, all inf install packages are forbidden.

Conflicts with Third-Party Applications

Some third-party applications prohibit the installation of AnyConnect's Virtual Adapter drivers. This can result in blue screens and a failure to update the routing table. Using the DART tool (described in the "Using DART to Gather Troubleshooting Information" section on page 12-4), you can gather a customer's operating system environment. Based upon this diagnosis, Cisco has identified the following conflicts with third-party applications and can recommend the following resolutions.

Adobe and Apple—Bonjour Printing Service

- Adobe Creative Suite 3
- BonJour Printing Service
- iTunes

Symptom Unable to successfully verify the IP forwarding table.

Possible Cause The AnyConnect event logs indicate a failure to identify the IP forwarding table and indicate the following entries in the routing table:

```
Destination 169.254.0.0
Netmask 255.255.0.0
Gateway 10.64.128.162
Interface 10.64.128.162
Metric 29
```

Recommended Action Disable the BonJour Printing Service by typing **net stop "bonjour service"** at the command prompt. A new version of mDNSResponder (1.0.5.11) has been produced by Apple. To resolve this issue, a new version of Bonjour is bundled with iTunes and made available as a separate download from the Apple web site.

Recommended Action

AT&T Communications Manager Versions 6.2 and 6.7

Symptom A failure to connect or pass traffic occurs when a customer has an AT&T Sierra Wireless 875 card on several PCs. Versions 6.2 to 6.7 seem to conflict with AnyConnect.

Possible Cause CSTP transport failure indicate that the transport layer is compromised by the AnyConnect Virtual Adapter.

Recommended Action Follow these steps to correct the problem:

1. Disable acceleration on the Aircard.
2. Launch AT&T communication manager > Tools > Settings > Acceleration > Startup.
3. Type **manual**.
4. Click **Stop**.

AT&T Global Dialer

Symptom The client operating system sometimes experiences a blue screen, which causes the creation of a mini dump file.

Possible Cause The AT&T Dialer intermediate driver failed to handle pending packets correctly and caused the operating system to crash. Other NIC card drivers (such as Broadcom) do not exhibit this problem.

Recommended Action Upgrade to the latest 7.6.2 AT&T Global Network Client.

Citrix Advanced Gateway Client Version 2.2.1

Symptom The following error may occur when disconnecting the AnyConnect session:

```
VPN Agent Service has encountered a problem and needs to close. We are sorry for
the inconvenience.
```

Possible Cause During the freeing of memory, the crash occurs as a result of the Citrix CtxLsp.dll, which gets loaded into every process using Winsock.

Recommended Action Remove the Citrix Advanced Gateway Client until Citrix can resolve this generic problem with CtxLsp.dll.

Firewall Conflicts

Third-party firewalls can interfere with the firewall function configured on the ASA group policy.

Juniper Odyssey Client

Symptom When wireless suppression is enabled, the wireless connection drops if a wired connection is introduced. With wireless suppression disabled, the wireless operates as expected.

Possible Cause The Odyssey Client should not manage the network adapter.

Recommended Action Configure the Odyssey Client with the steps below:

1. In Network Connections, copy the name of the adapter as it appears in its connection properties. If you edit the registry, perform a backup before making any changes and use caution as serious problems can occur if modified incorrectly.
2. Open the registry and go to HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual.
3. Create a new string value under virtual. Copy the name of the adapter from Network properties into the registry portion. The additional registry settings, once saved, are ported over when a customer MSI is created and are pushed down to other clients.

Kaspersky AV Workstation 6.x

Symptom When Kaspersky 6.0.3 is installed (even if disabled), AnyConnect connections to the ASA fail right after CSTP state = CONNECTED. The following message appears:

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure
gateway (proxy authentication, handshake, bad cert, etc.).
```

Possible Cause A known incompatibility exists between Kaspersky AV Workstation 6.x and AnyConnect.

Recommended Action Uninstall Kaspersky and refer to their forums for additional updates.

McAfee Firewall 5

Symptom A UDP DTLS connection cannot be established.

Possible Cause McAfee Firewall defaults to blocking incoming IP fragments and thus blocking DTLS if fragmented.

Recommended Action In the McAfee Firewall central console, choose **Advanced Tasks > Advanced options and Logging** and uncheck the **Block incoming fragments automatically** check box in McAfee Firewall.

Microsoft Internet Explorer 8

Symptom You cannot install AnyConnect from the WebVPN portal when using Internet Explorer 8 with Windows XP SP3.

Possible Cause The browser crashes with the installation.

Recommended Action As recommended by Microsoft, remove MSJVM. Refer to Microsoft Knowledge Based Article KB826878.

Microsoft Routing and Remote Access Server

Symptom When AnyConnect attempts to establish a connection to the host device, the following termination error is returned to the event log:

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service "Routing and Remote Access" is incompatible with the Cisco
AnyConnect VPN Client.
```

Possible Cause RRAS and AnyConnect conflict over the routing table. With RRAS, the PC acts as an Ethernet router and therefore modifies the routing table the same way as AnyConnect does. The two cannot run together since AnyConnect depends on the routing table to properly direct traffic.

Recommended Action Disable the RRAS service.

Microsoft Windows Updates

Symptom The following message is encountered when trying to establish a VPN connection:

```
The VPN client driver has encountered an error.
```

Possible Cause A recent Microsoft update to the certclass.inf file has occurred. The following error appears in the C:\WINDOWS\setupapi.log:

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or
invalid. Error 0xffffffbf8: Unknown Error. Assuming all device classes are subject
to driver signing policy.
```

Recommended Action Check which updates have recently been installed by entering **C:\>systeminfo** at the command prompt or checking the C:\WINDOWS\WindowsUpdate.log. To attempt a repair, use the following steps:

1. Open a command prompt as an admin.
2. Enter **net stop CryptSvc**.
3. Analyze the database to verify its validity by entering **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** or rename the following directory: %/WINDIR%\system32\catroot2 to catroot2_old.
4. When prompted, choose **OK** to attempt the repair.Exit the command prompt and reboot.

Even though the steps taken above may indicate that the catalog is not corrupt, they key file(s) may still have been overwritten with an unsigned one. If the failure still occurs, open a case with Microsoft to determine why the driver signing database is being corrupted.

Microsoft Windows XP Service Pack 3

Symptom You cannot install the AnyConnect client. The following error message appears:

```
This application has failed to start because dot3api.dll was not found.
Re-installing the application may fix this problem.
```

Possible Cause The missing dot3api.dll file is a known issue.

Recommended Action Reinstall regsvr32 dot3api.dll and reboot the operating system.

OpenVPN Client

Symptom An error indicates that the version of TUN is already installed on this system and is incompatible with the AnyConnect client.

Possible Cause The MAC OS X Shimo VPN Client can cause this.

Recommended Action Uninstall the Viscosity OpenVPN Client.

Load Balancers

Symptom The connection fails due to lack of credentials.

Possible Cause While the browser may cache the DNS result, additional applications such as the port forwarder and smart tunnels may not. If you log into X.4 and the DNS resolver is set to use x.15, the PF applet or smart tunnel application resolves the DNS and connects to X.15. Since no sessions were established, the connection fails due to lack of credentials.

Recommended Action The third-party load balancer has no insight into the load on the ASA devices. Because the load balance functionality in the ASA is intelligent enough to evenly distribute the VPN load across the devices, we recommend using the internal ASA load balancing.

Ubuntu 8.04 i386

Symptom The AnyConnect client fails to establish a connection to the ASA when using Ubuntu version 8.04. The error message states that the VPN client agent SSL engine encountered an error.

Possible Cause Because the NSS library extensions changed between version 7.04 and 8.04, the AnyConnect client cannot find the Network Security Service Libraries.

Recommended Action Use the following script to correct the links of the NSS libraries:

```
#!/bin/sh
if [ `id | sed -e `s/(.*//' ` != "uid=0" ]; then
    echo "Sorry, you need super user privileges to run this script.
    exit 1
fi
echo Creating Firefox NSS compatible symlinks...
ln -s /usr/lib/libnspr4.so.0d /usr/lib/libnspr4.so || exit 1
ln -s /usr/lib/libnss3.so.1d /usr/lib/libnss3.so || exit 1
ln -s /usr/lib/libplc4.so.0d /usr/lib/libplc4.so || exit 1
ln -s /usr/lib/libsmime3/so/1d /usr/lib/libsmime3.so || exit 1
echo "Success!"
```

You can also check the Ubuntu Forums for discussions on making Ubuntu 64-bit operational with AnyConnect.

Wave EMBASSY Trust Suite

Symptom The AnyConnect client fails to download and produces the following error message:

```
"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to
close."
```

Possible Cause If you gather the mdmp file, the decode of the crash mdmp file indicates that a third-party dll is resident.

Recommended Action Upload the patch update to version 1.2.1.38 to resolve all dll issues.

Layered Service Provider (LSP) Modules and NOD32 AV

Symptom When AnyConnect attempts to establish a connection, it authenticates successfully and builds the ssl session, but then the AnyConnect client crashes in the vpndownloader.

Possible Cause The LSP component imon.dll has incompatibility issues.

Recommended Action Remove the Internet Monitor component in version 2.7 and upgrade to version 3.0 of ESET NOD32 AV.

LSP Symptom 2 Conflict

Symptom If an LSP module is present on the client, a Winsock catalog conflict may occur.

Possible Cause An Intel Mobile Bandwidth LSP Module such as impbw.dll may have caused a fault on the Intel code.

Recommended Action Uninstall the LSP module.

LSP Slow Data Throughput Symptom 3 Conflict

Symptom Slow data throughput may occur with the use of NOD32 V4.0.

Possible Cause The conflict involves Cisco AnyConnect and NOD32 Antivirus 4.0.468 x64 using Windows 7.

Recommended Action Go to **Protocol Filtering > SSL** in the Advanced Setup and enable SSL protocol scanning. Now go to **Web access protection > HTTP, HTTPS** and check **Do not use HTTPS protocol checking**. When the setting is enabled, go back to **Protocol filtering > SSL** and disable **SSL protocol scanning.**

EVDO Wireless Cards and Venturi Driver

Symptom A client disconnect occurred and produced the following in the event log:

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing
connection: DPD failure.
```

Possible Cause Check the Application, System, and AnyConnect event logs for a relating disconnect event and determine if a NIC card reset was applied at the same time.

Recommended Action Ensure that the Venturi driver is up to date. Disable **Use Rules Engine** in the 6.7 version of the AT&T Communications Manager.

DSL Routers Fail to Negotiate

Symptom DTLS traffic was failing even though it was successfully negotiated.

Possible Cause The DSL routers were blocking return DTLS traffic. No settings on the Air Link would allow a stable DTLS connection.

Recommended Action Connecting to a Linksys router with factory settings allowed a stable DTLS session and no interruption in pings. Add a rule to allow DTLS return traffic.

CheckPoint (and other Third-Party Software such as Kaspersky)

Symptom The AnyConnect log indicates a failure to fully establish a connection to the secure gateway.

Possible Cause The client logs indicate multiple occurrences of NETINTERFACE_ERROR_INTERFACE_NOT_AVAILABLE. These errors occur when the client is attempting to retrieve operating system information on the PC's network interface used to make the SSL connection to the secure gateway.

Recommended Action If you are uninstalling the Integrity Agent and then installing AnyConnect, enable TCP/IP. If you disable SmartDefense on Integrity agent installation, TCP/IP is checked. If third-party software is intercepting or otherwise blocking the operating system API calls while retrieving network interface information, check for any suspect AV, FW, AS, and such. Confirm that only one instance of the AnyConnect adapter appears in the Device Manager. If there is only one instance, authenticate with AnyConnect, and after 5 seconds, manually enable the adapter from the Device Manager. If any suspect drivers have been enabled within the AnyConnect adapter, disable them by unchecking them in the Cisco AnyConnect VPN Client Connection window.

Performance Issues with Virtual Machine Network Service Drivers

Symptom When using AnyConnect on some client PCs, performance issues have resulted.

Possible Cause The virtual machine network driver virtualizes a physical network card or connection. When binding other Virtual Machine Network Services to the Cisco AnyConnect VPN Client Connection network adapter, performance issues occurred. The client device became infected with some malware and introduces a delay around SSL_write().

Recommended Action Uncheck the binding for all IM devices within the AnyConnect virtual adapter. The application dsagent.exe resides in C:\Windows\System\dgagent. Although it does not appear in the process list, you can see it by opening sockets with TCPview (sysinternals). When you terminate this process, normal operation of AnyConnect results.

APPENDIX A

VPN XML Reference

Use this appendix only if you are not upgrading ASDM to 6.3(1) or later. AnyConnect 2.5 supports a profile editor that you can access to configure AnyConnect features. However, you can access it only with ASDM 6.3(1) or later. Earlier AnyConnect versions provided a standalone profile editor that you could install on Windows, but it was undocumented and unsupported and is no longer available as a standalone editor. We strongly recommend upgrading to ASDM because it is much easier to create, edit, and manage profiles directly with the AnyConnect profile editor than it is edit them with a conventional editor. The new profile editor is documented and supports and comes with its own online help. The minimum ASA software release supported by ASDM 6.3(1) with AnyConnect 2.5 is ASA 8.0(2). However, we recommend upgrading to ASA 8.3(1) or later to take full advantage of the new client features.

Read *Chapter 3, Configuring AnyConnect Client Features* for familiarity with the AnyConnect profile and features. This appendix provides an alternative to this chapter.

The following sections briefly describe each client feature and provide XML tag names, options, descriptions, and example code. AnyConnect uses the default value if the profile does not specify one.

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.

Local Proxy Connections

Table A-1 shows the tag name, options, and descriptions to configure support for local proxy connections.

Table A-1 Local Proxy Connection Settings

XML Tag Name	Options	Description
AllowLocalProxyConnections	true (default)	Enables local proxy connections.
	false	Disables local proxy connections.

Example:Disable Local Proxy Connections

Refer to the following example to disable AnyConnect support for local proxy connections:

```
<ClientInitialization>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
</ClientInitialization>
```

Optimal Gateway Selection (OGS)

Table A-2 shows the tag names, options, and descriptions to configure OGS.

Table A-2 OGS Settings

XML Tag Name	Options	Description
EnableAutomaticServerSelection	true	Enables OGS by default.
	false	Disables OGS by default.
EnableAutomaticServerSelection UserControllable	true	Allows the user to enable or disable OGS in client preferences.*
	false	Reverts to the default where automatic server selection is not user-controllable.
AutoServerSelectionImprovement	Integer. The default is 20 percent.	Percentage of performance improvement to trigger the client to connect to another secure gateway.
AutoServerSelectionSuspendTime	Integer. The default is 4 hours.	Specifies the elapsed time (in hours) since disconnecting from the current secure gateway and reconnecting to another secure gateway.

* When OGS is enabled, we recommend that you also make the feature user-controllable.

Example:OGS

Refer to the following example to configure OGS:

```
<ClientInitialization>
    <EnableAutomaticServerSelection UserControllable="true">
     true
         <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
         <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
     </EnableAutomaticServerSelection>
</ClientInitialization>
```

Trusted Network Detection

Table A-3 shows the tag names, options, and descriptions to configure trusted network detection.

Table A-3 Trusted Network Detection Settings

XML Tag Name	Options	Description
AutomaticVPNPolicy	true	Enables TND. Automatically manages when a VPN connection should be started or stopped according to the *TrustedNetworkPolicy* and *UntrustedNetworkPolicy* parameters.
	false	Disables TND. VPN connections can only be started and stopped manually.
TrustedNetworkPolicy	Disconnect	Disconnects the VPN connection in the trusted network.
	Connect	Initiates a VPN connection (if none exists) in the trusted network.
	DoNothing	Takes no action in a trusted network.
	Pause	Suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.
UntrustedNetworkPolicy	Connect	Initiates a VPN connection upon the detection of an untrusted network.
	DoNothing	Initiates a VPN connection upon the detection of an untrusted network. This option is incompatible with always-on VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
TrustedDNSDomains	String	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: *.cisco.com Wildcards (*) are supported for DNS suffixes.
TrustedDNSServers	String	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: 161.44.124.*,64.102.6.247 Wildcards (*) are supported for DNS server addresses.

Example:Trusted Network Detection

Refer to the following example to configure trusted network detection. 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>
```

Always-on VPN and Subordinate Features

If you choose always-on VPN, the fail-open policy permits network connectivity, and the fail-close policy disables network connectivity.

Table A-4 shows the tag names, options, and descriptions to configure always-on VPN.

Table A-4 Always-on VPN Settings

XML Tag Name	Options	Description
AutomaticVPNPolicy	true	Enables automatic VPN policy.
	false	Disables automatic VPN policy.
TrustedDNSDomains	string	Specifies possible DNS suffixes that a network interface may have when in a trusted network.
TrustedDNSServers	string	Specifies DNS server addresses that a network interface may have when the client is in a trusted network.
TrustedNetworkPolicy	disconnect	Disconnects from the VPN in upon detection of a trusted network.
	connect	Connects to the VPN upon detection of a trusted network.
	donothing	Do not connect to the VPN or disconnect from the VPN upon detection of a trusted network.
UntrustedNetworkPolicy	connect	Disconnects from the VPN in upon detection of an untrusted network.
	disconnect	Connects to the VPN upon detection of an untrusted network.
	donothing	Do not connect to the VPN or disconnect from the VPN upon detection of an untrusted network.
AlwaysOn	true	Enables always-on VPN.
	false	Disables always-on VPN.
ConnectFailurePolicy	open	Does not restrict network access when AnyConnect cannot establish a VPN session (for example, when an adaptive security appliance is unreachable).
	closed	Restricts network access when the VPN is unreachable. The restricted state permits access only to secure gateways to which the computer is allowed to connect.

Table A-4 Always-on VPN Settings (continued)

XML Tag Name	Options	Description
AllowCaptivePortalRemediation	true	Relaxes the network restrictions imposed by a closed connect failure policy for the number of minutes specified by the CaptivePortalRemediationTimeout tag so that the user can remediate a captive portal.
	false	Enforces the network restrictions imposed by a closed connect failure policy even if AnyConnect detects a captive portal.
CaptivePortalRemediationTimeout	Integer	The number of minutes AnyConnect lifts the network access restrictions.
ApplyLastVPNLocalResourceRules	true	Applies the last client firewall it received from the security appliance, which may include ACLs allowing access to resources on the local LAN.
	false	Does not apply the last client firewall received from the security appliance.
AllowVPNDisconnect	true	Displays a Disconnect button to provide users with the option to disconnect an always-on VPN session. Users might want to do so to select an alternative secure gateway before reconnecting.
	false	Does not display a Disconnect button. This option prevents the use of the AnyConnect GUI to disconnect from the VPN.

Caution A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. It is primarily for exceptionally secure organizations where security persistence is a greater concern than always-available network access. It prevents all network access except for local resources such as printers and tethered devices permitted by split tunneling and limited by ACLs. It can halt productivity if users require Internet access beyond the VPN if a secure gateway is unavailable. AnyConnect detects most captive portals (described in Captive Portal Hotspot Detection, page 3-29). If it cannot detect a captive portal, a connect failure closed policy prevents all network connectivity.

If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy always-on VPN with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.

Always-On VPN—XML Example

If you are using a release of ASDM that is earlier than 6.3(1), use the following example to edit the AnyConnect XML profile manually. This always-on VPN example does the following:

- Enables the Disconnect button (AllowVPNDisconnect) to let users establish a VPN session with another secure gateway.
- Specifies the connect failure policy is closed.
- Relaxes network restrictions imposed by the connect failure policy for five minutes to remediate a captive portal.
- Applies the ACL rules assigned during the last VPN session.

```
<ClientInitialization>
```

```
    <AutomaticVPNPolicy>true
        <TrustedDNSDomains>example.com</TrustedDNSDomains>
        <TrustedDNSServers>1.1.1.1</TrustedDNSServers>
        <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
        <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
        <AlwaysOn>true
            <AllowVPNDisconnect>true</AllowVPNDisconnect>
            <ConnectFailurePolicy>Closed
                <AllowCaptivePortalRemediation>true
                    <CaptivePortalRemediationTimeout>5</CaptivePortalRemediationTimeout>
                </AllowCaptivePortalRemediation>
                <ApplyLastVPNLocalResourceRules>true</ApplyLastVPNLocalResourceRules>
            </ConnectFailurePolicy>
        </AlwaysOn>
    </AutomaticVPNPolicy>
</ClientInitialization>
```

Using Always-on VPN With Load Balancing

Table A-5 shows the tag names, options, and descriptions to configure always-on VPN with load balancing.

Table A-5 Using Always-on VPN With Load Balancing Settings

XML Tag Name	Options	Description
LoadBalancingServerList	FQDN or IP address	Specify the backup devices of the cluster. Without this option, AnyConnect blocks access to backup devices in the load balancing cluster if always-on VPN is enabled.

Example:Always-on VPN With Load Balancing

```
<ServerList>
        <!--
            This is the data needed to attempt a connection to a specific
            host.
          -->
 <HostEntry>
   <HostName>ASA</HostName>
   <HostAddress>10.86.95.249</HostAddress>
  <LoadBalancingServerList>
     <!--
    Can be a FQDN or IP address.
        -->
      <HostAddress>loadbalancing1.domain.com</HostAddress>
      <HostAddress>loadbalancing2.domain.com</HostAddress>
      <HostAddress>11.24.116.172</HostAddress>
</LoadBalancingServerList>
  </HostEntry>
</ServerList>
```

Start Before Logon

Table A-6 shows the tag names, options, and descriptions to configure start before logon.

Table A-6 Start Before Logon Settings

XML Tag Name	Options	Description
UseStartBeforeLogon	true	Enables start before logon.
	false	Disables start before logon.
UseStartBeforeLogon UserControllable	true	Makes SBL user controllable.
	false	Reverts to the default where SBL is not user-controllable.

Example:Start Before Logon

Refer to the following example to configure SBL:

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

AnyConnect Local Policy File Parameters and Values

Table A-7 shows the tag names, options, and descriptions to configure local policy.

Table A-7 AnyConnect Local Policy Settings

XML Tag Name	Options	Description
acversion="<version number>"		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.
xmlns=http://schemas.xmlsoap.org/encoding/	Most administrators do not change this parameter.	The XML namespace specifier.
xsi:schemaLocation="http://schemas.xmlsoap.org/ encoding/AnyConnectLocalPolicy.xsd">	Most administrators do not change this parameter.	The XML specifier for the schema location.
xmlns:xsi=http://www.w3.org/2001/ XMLSchema-instance	Most administrators do not change this parameter.	The XML schema instance specifier.
FipsMode	true	Enables FIPS mode for the client. The client uses only algorithms and protocols approved by the FIPS standard.
	false	Disables FIPS mode for the client.

Table A-7 AnyConnect Local Policy Settings (continued)

XML Tag Name	Options	Description
BypassDownloader	true	The client does not check for any dynamic content present on the ASA, including profile updates, translations, customization, optional modules, and core software updates.
	false	The client checks for dynamic content present on the ASA (default).
RestrictWebLaunch	true	WebLaunch attempts fail, and the client displays an informative message to the user.
	false	Permits WebLaunch (default—behavior consistent with AnyConnect 2.3 and earlier).
StrictCertificateTrust	true	The client fails to connect to security gateways that use invalid, mismatched, or untrusted certificates that require user interaction.
	false	The client prompts the user to accept the certificate (default—behavior consistent with AnyConnect 2.3 and earlier).
RestrictPreferenceCaching	Credentials	The user name and second user name are not cached.
	Thumbprints	The client and server certificate thumbprints are not cached.
	CredentialsAndThumbprints	Certificate thumbprints and user names are not cached.
	all	No automatic preferences are cached.
	false	All preferences are written to disk (default—behavior consistent with AnyConnect 2.3 and earlier).
RestrictTunnelProtocols (currently not supported)	TLS	The client only uses IKEv2 and ESP to establish the tunnel and will not use TLS/DTLS to communicate information to the secure gateway.
	IPSec	The client only uses TLS/DTLS for authentication and tunneling.
	false	Any encrypted protocol may be used in connection establishment (default).
ExcludeFirefoxNSSCertStore (Linux and Mac)	true	Excludes the Firefox NSS certificate store.
	false	Permits the Firefox NSS certificate store (default).

Table A-7 AnyConnect Local Policy Settings (continued)

XML Tag Name	Options	Description
ExcludePemFileCertStore (Linux and Mac)	true	Excludes the PEM file certificate store.
	false	Permits the PEM file certificate store (default).
ExcludeMacNativeCertStore (Mac only)	true	Excludes the Mac native certificate store.
	false	Permits the Mac native certificate store (default).
ExcludeWinNativeCertStore (Windows only, currently not supported)	true	Excludes the Windows Internet Explorer certificate store.
	false	Permits the Windows Internet Explorer certificate store (default).

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

Example:AnyConnect Local Policy

Refer to the following example to configure 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>
```

Certificate Store on Windows

Table A-8 shows the tag name, options, and descriptions to configure certificate store.

Table A-8 Certificate Store Settings

XML Tag Name	Options	Description
CertificateStore	All	(Default) Directs the AnyConnect client to use all certificate stores for locating certificates.
	Machine	Directs the AnyConnect client to restrict certificate lookup to the Windows local machine certificate store.
	User	Directs the AnyConnect client to restrict certificate lookup to the local user certificate stores.

Example:Certificate Store
Refer to the following example to configure certificate store:

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

Restricting Certificate Store Use

Table A-9 shows the tag names, options, and descriptions to restrict certificate store use:

Table A-9 Restricting Certificate Store Settings

XML Tag Name	Options	Description
ExcludeFirefoxNSSCertStore (Linux and Mac)	true	Excludes the Firefox NSS certificate store.
	false	Permits the Firefox NSS certificate store (default).
ExcludePemFileCertStore (Linux and Mac)	true	Excludes the PEM file certificate store.
	false	Permits the PEM file certificate store (default).
ExcludeMacNativeCertStore (Mac only)	true	Excludes the Mac native certificate store.
	false	Permits the Mac native certificate store (default).
ExcludeWinNativeCertStore (Windows only, currently not supported)	true	Excludes the Windows Internet Explorer certificate store.
	false	Permits the Windows Internet Explorer certificate store (default).

SCEP Protocol to Provision and Renew Certificates

Table A-10 shows the tag names, options, and descriptions to configure SCEP protocols to provision and renew certificates.

Table A-10 SCEP Protocol Settings

XML Tag Name	Options	Description
CertificateEnrollment		Starting tag for certificate enrollment.
CertificateExpirationThreshold	number of days	Specifies when AnyConnect should warn users that their certificate is going to expire.
AutomaticSCEPHost	fully qualified domain name of the ASA\connection profile	The host attempts automatic certificate retrieval if this attribute specifies the ASA host name and connection profile (tunnel group) for which SCEP certificate retrieval is configured.
	IP address of the ASA\connection profile name	
CAURL	fully qualified domain name	
	IP address of CA server	
CertificateSCEP		Defines how the contents of the certificate will be requested.
CADomain		Domain of the certificate authority.
Name_CN		Common Name in the certificate.
Department_OU		Department name specified in certificate.

Table A-10 SCEP Protocol Settings (continued)

Company_O		Company name specified in certificate.
State_ST		State identifier named in certificate.
Country_C		Country identifier named in certificate.
Email_EA		Email address.
Domain_DC		Domain component.
DisplayGetCertButton	true	Permits 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.
	false	Does not permit users to manually request provisioning or renewal of authentication certificates.
ServerList		Starting tag for the server list. The server list is presented to users when they first launch AnyConnect. Users can choose which ASA to log into.
HostEntry		Starting tag for configuring an ASA.
HostName		Host name of the ASA.
HostAddress		Fully qualified domain name of the ASA.

Example:SCEP Protocols

Refer to the following example to configure SCEP elements in user profiles:

```
<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>
```

Certificate Matching

Table A-11 shows the tag names, options, and descriptions to configure certificate matching.

Table A-11 Certificate Matching

XML Tag Name	Options	Description
CertificateExpirationThreshold		Specifies the number of days prior to the certificate's expiration date. Users are warned that their certificate is expiring.
CertificateMatch	n/a	Defines preferences that refine client certificate selection. Include 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.
KeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to specify acceptable client certificates.
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.
ExtendedKeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to choose acceptable client certificates
ExtendedMatchKey	ClientAuth ServerAuth CodeSign EmailProtect IPSecEndSystem IPSecUsers Timestamp OCSPSigns 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.

Table A-11 Certificate Matching (continued)

XML Tag Name	Options	Description
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).
DistinguishedName	n/a	Group identifier. Within the DistinguishedName group, Certificate Distinguished Name matching lets you specify match criteria for choosing acceptable client certificates.
DistinguishedNameDefinition	Bold text indicates default value. • Wildcard: **"Enabled"** "Disabled" • Operator: **"Equal"** (**==**) "NotEqual" (!==) • MatchCase: **"Enabled"** "Disabled"	DistinguishedNameDefinition specifies a set of operators used to define a single Distinguished Name attribute to be used in matching. The Operator specifies the operation to use in performing the match. MatchCase specifies whether the pattern matching is case sensitive.

Table A-11 Certificate Matching (continued)

XML Tag Name	Options	Description
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 to be used in matching. You can specify up to 10 attributes.

Table A-11 Certificate Matching (continued)

XML Tag Name	Options	Description
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.

Example:Certificate Matching

Refer to the following example to enable the attributes that you can use to refine client certificate selections:

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

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

Automatic Certificate Selection

Table A-12 shows the tag names, options, and descriptions to configure automatic certificate selection.

Table A-12 Automatic Certificate Selection Settings

XML Tag Name	Options	Description
AutomaticCertSelection	true	Allows AnyConnect to automatically select the authentication certificate.
	false	Prompts the user to select the authentication certificate.

Example:AutomaticCertSelection

Refer to the following example to configure the client profile with AutomaticCertSelection:

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

Backup Server List Parameters

Table A-13 shows the tag names, options, and descriptions to configure backup server list.

Table A-13 Backup Server List Settings

XML Tag Name	Options	Description
BackupServerList	n/a	Determines the group identifier.
HostAddress	An IP address or a Full-Qualified Domain Name (FQDN)	Specifies a host address to include in the backup server list.

Example:Backup Server List

Refer to the following example to configure backup server list parameters:

```
<BackupServerList>
   <HostAddress>bos</HostAddress>
   <HostAddress>bos.example.com</HostAddress>
</BackupServerList>
```

Windows Mobile Policy

Table A-14 shows the tag names, options, and descriptions to configure Windows Mobile policy.

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

Table A-14 Windows Mobile Policy

XML Tag Name	Options	Description
MobilePolicy	n/a	Determines the group identifier.
DeviceLockRequired	n/a	Group identifier. Within the MobilePolicy group, DeviceLockRequired indicates that a Windows Mobile device must be configured with a password or PIN prior to establishing a VPN connection. This configuration is valid only on Windows Mobile devices that use the Microsoft Default Local Authentication Provider (LAP). **Note** The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, WM5AKU2+, and Windows Mobile 6.0, but not on Windows Mobile 6.1.
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.
MinimumPasswordLength	Any non-negative integer	Within the DeviceLockRequired group, when set to a non-negative number, this parameter specifies that any PIN/password used for device locking must have at least the specified number of characters. This setting must be pushed down to the mobile device by synchronizing with an Exchange server before it can be enforced. (WM5AKU2+)
PasswordComplexity	"alpha"-Requires an alphanumeric password. "pin"-Requires a numeric PIN. "strong"-Requires a strong alphanumeric password, defined by Microsoft as containing at least 7 characters, including at least 3 from the set of uppercase, lowercase, numerals, and punctuation.	When present, checks for the password subtypes listed in the column to the left. This setting must be pushed down to the mobile device by synchronizing with an Exchange server before it can be enforced. (WM5AKU2+)

Example:Windows Mobile Policy

Refer to the following example to configure a Windows Mobile policy using XML:

```
<MobilePolicy>
<DeviceLockRequired>
```

```
    MaximumTimeoutMinutes="60"
    MinimumPasswordLength="4"
    PasswordComplexity="pin"
</DeviceLockRequired>
</MobilePolicy>
```

Auto Connect On Start

Table A-15 shows the tag names, options, and descriptions to configure auto connect on start.

Table A-15 Auto Connect On Start Settings

XML Tag Name	Options	Description
AutoConnectOnStart	true	Starts the auto connect settings.
	false	Returns to the default auto connect settings.
AutoConnectOnStart UserControllable	true	Inserts user control attributes.
	false	Removes user control attributes.

Example:Auto Connect On Start
Refer to the following example to configure auto connect on start:

```
<AutoConnectOnStart>
true
</AutoConnectOnStart>
```

Auto Reconnect

Table A-16 shows the tag names, options, and descriptions to configure auto reconnect:

Table A-16 Auto Reconnect Settings

XML Tag Name	Options	Description
AutoReconnect	true	Client retains resources assigned to the VPN session if it is disrupted and attempts to reconnect.
	false	Client releases resources assigned to the VPN session if it is interrupted and does not attempt to reconnect.
AutoReconnectBehavior	DisconnectOnSuspend	AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resume.
	ReconnectAfterResume	Client retains resources assigned to the VPN session during a system suspend. The client attempts to reconnect after the system resume.

Example:Auto Reconnect
Refer to the following example to configure AnyConnect VPN reconnect behavior in the client initialization section:

```
<AutoReconnect>
    true
</AutoReconnect>

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

Server List

Table A-17 shows the tag names, options, and descriptions to configure server list.

Table A-17 Server List Settings

XML Tag Name	Options	Description
ServerList	n/a	Specifies a group identifier.
HostEntry	n/a	Group identifier, subordinate to ServerList. This is the data needed to attempt a connection to a specific host.
HostName	An alias used to refer to the host, 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.
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.
PrimaryProtocol	SSL or IPsec	The encryption protocol for the VPN tunnel, either SSL (default) or IPsec with IKEv2. For IPsec, the client uses the proprietary AnyConnect EAP authentication method by default.
StandardAuthenticationOnly	n/a	Use the StandardAuthenticationOnly parameter to change the authentication method from the default proprietary AnyConnect EAP authentication method to a standards-based method. Be aware that doing this limits the dynamic download features of the client and disables some features and disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.
AuthMethodDuringIKENegotiation	IKE-RSA, EAP-MD5, EAP-MSCHAPv2, EAP-GTC	Specifies the authentication method for standard-based authentication.

Table A-17 Server List Settings

XML Tag Name	Options	Description
IKEIdentity	An alpha-numeric string.	If you choose a standards-based EAP authentication method, you can enter a group or domain as the client identity in this field. The client sends the string as the ID_GROUP type IDi payload. By default, the string is *$AnyConnectClient$*. The string must not contain any terminators (for example, null or CR).
UserGroup	The connection profile (tunnel group) to use when connecting to the specified host. This parameter is optional.	If present, used in conjunction with HostAddress to form a Group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile. **Note** Group-based URL support requires ASA version 8.0.3 or later.

Example:Server List

Refer to the following example to configure a server list:

```
<ServerList>
    <HostEntry>
        <HostName>ASA-01</HostName>
        <HostAddress>cvc-asa01.cisco.com
         </HostAddress>
    </HostEntry>
    <HostEntry>
        <HostName>ASA-02</HostName>
         <HostAddress>cvc-asa02.cisco.com
         </HostAddress>
        <UserGroup>StandardUser</UserGroup>
        <BackupServerList>
            <HostAddress>cvc-asa03.cisco.com
            </HostAddress>
         </BackupServerList>
    </HostEntry>
</ServerList>
```

Scripting

Table A-18 shows the tag names, options, and descriptions to configure scripting.

Table A-18 Scripting Settings

XML Tag Name	Options	Description
EnableScripting	true	Launches OnConnect and OnDisconnect scripts if present.
	false	(Default) Does not launch scripts.
UserControllable	true	Lets users enable or disable the running of OnConnect and OnDisconnect scripts.
	false	(Default) Prevents users from controlling the scripting feature.
TerminateScriptOnNextEvent	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, as well as all their script descendents. On Mac OS and Linux, AnyConnect terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts.
	false	(Default) Does not terminate a script process if a transition to another scriptable event occurs.
EnablePostSBLOnConnectScript	true	Prevents launching of the OnConnect script if SBL establishes the VPN session.
	false	(Default) When SBL establishes the VPN session, launches the OnConnect script, if present.

Example:Scripting

Refer to the following example to configure scripting:

```
<ClientInitialization>

<EnableScripting>true</EnableScripting>

</ClientInitialization>
```

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

```
<ClientInitialization>

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

</ClientInitialization>
```

Authentication Timeout Control

By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out.

Table A-19 shows the tag name, options, and descriptions to change the authentication timer.

Table A-19 Authentication Timeout Control

XML Tag Name	Options	Description
AuthenticationTimeout	Integer in the range 10–120	Enter a number of seconds to change this timer.

Example:Authentication Timeout Control

The following example changes the authentication timeout to 20 seconds:

```
<ClientInitialization>
    <AuthenticationTimeout>20</AuthenticationTimeout>
</ClientInitialization>
```

Ignore Proxy

Table A-20 shows the tag name, options, and descriptions to configure ignore proxy.

Table A-20 Ignore Proxy Settings

XML Tag Name	Options	Description
ProxySettings	IgnoreProxy	Enables ignore proxy.
	native	Not supported.
	override	Not supported.

Example:Ignore Proxy

Refer to the following example to configure ignore proxy in the client initialization section:

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

Allow AnyConnect Session from an RDP Session for Windows Users

Table A-21 shows the tag names, options, and descriptions to configure an RDP session.

Table A-21 Allow AnyConnect Session from an RDP Session

XML Tag Name	Options	Description
WindowsLogonEnforcement	SingleLocalLogon	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. 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.
	SingleLogon	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.
WindowsVPNEstablishment	LocalUsersOnly	Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of the AnyConnect client.
	AllowRemoteUsers	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.

Example:Allow AnyConnect Session from an RDP Session for Windows Users

Refer to the following example to configure AnyConnect sessions from an RDP session:

```
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>

<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
```

AnyConnect over L2TP or PPTP

Table A-22 shows the tag names, options, and descriptions to configure AnyConnect over L2TP or PPTP.

Table A-22 AnyConnect Over L2TP or PPTP

XML Tag Name	Options	Description
PPPExclusion	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, follow the steps in "Instructing Users to Override PPP Exclusion" on page 3-62.
	disabled	PPP exclusion is not applied.
PPPExclusionServerIP	true	Uses the IP address of the PPP server.
	false	Does not use the IP address of the PPP server.
PPPExclusion UserControllable=	true	Lets users read and change the PPP exclusion settings.
	false	Prevents users from viewing and changing the PPP exclusion settings.

Example:AnyConnect Over L2TP or PPTP

Refer to the following example to configure AnyConnect over L2TP or PPTP:

```
<ClientInitialization>
    <PPPExclusion UserControllable="true">Automatic
        <PPPExclusionServerIP UserControllable="true">127.0.0.1</PPPExclusionServerIP>
    </PPPExclusion>
    </ClientInitialization>
        <ServerList>
        <HostEntry>
            <HostName>DomainNameofASA</HostName>
            <HostAddress>IPaddressOfASA</HostAddress>
        </HostEntry>
         </ServerList>
</AnyConnectProfile>
```

Other AnyConnect Profile Settings

Table A-23 shows other parameters you can insert into the ClientInitialization section.

Table A-23 Other AnyConnect Profile Settings

XML Tag Name	Options	Description
CertificateStoreOverride	true	Allows an administrator to direct AnyConnect to search for certificates in the Windows machine certificate store. This tag becomes useful when certificates are located in this store and users do not have administrator privileges on their device.
	false	(Default) AnyConnect will not search for certificates in the Windows machine certificate store.

Table A-23 Other AnyConnect Profile Settings

XML Tag Name	Options	Description
ShowPreConnectMessage	true	Enables an administrator to have a one-time message displayed prior to a users first connection attempt. For example, the message can remind users to insert their smart card into its reader. The message appears in the AnyConnect message catalog and is localized.
	false	(Default) No message displayed prior to a users first connection attempt.
MinimizeOnConnect	true	(Default) Controls AnyConnect GUI behavior when a VPN tunnel is established. By default, the GUI is minimized when the VPN tunnel is established.
	false	No control over AnyConnect GUI behavior.
LocalLanAccess	true	Allows the user to accept or reject Local LAN access when enabled for remote clients on the Secure Gateway.
	false	(Default) Disallows Local LAN access.
AutoUpdate	true	(Default) Allows the administrator to turn off the dynamic update functionality of AnyConnect. A user can also have this functionality.
	false	No ability to turn off the dynamic update functionality of AnyConnect.
RSASecurIDIntegration	automatic	(Default) Allows the administrator to control how the user interacts with RSA. By default, AnyConnect determines the correct method of RSA interaction. An administrator can lock down the RSA or give control to the user.
	software token	
	hardware token	
RetainVPNOnLogoff	true	Keeps the VPN session when the user logs off a Windows operating system.
	false	(Default) Stops the VPN session when the user logs off a Windows operating system.
UserEnforcement	AnyUser	Continues the VPN session even if a different user logs on. This value applies only if the RetainVPNPnLogoff is true and the original users logged off Windows when the VPN session was up.
	SameUserOnly	Ends the VPN session when a different user logs on.

APPENDIX B

Telemetry XML Reference

This appendix describes the XML elements used in a Telemetry client profile. Use this appendix as a reference, if you are troubleshooting a Telemetry client profile, or you have not yet upgraded to ASDM 6.4(1) and do not have use of the AnyConnect profile editor tool.

If you have upgraded to ASDM 6.4(1), we strongly recommend that you use the AnyConnect profile editor to create and maintain AnyConnect client profiles rather than editing the profile files with a plain text or XML editor. The AnyConnect profile editor comes with its own online help.

Read Configuring AnyConnect Telemetry to the WSA, page 7-1 for familiarity with the AnyConnect Telemetry module, client profile, and features. Table B-1 provides XML tag names, options, descriptions, and example code used to configure the AnyConnect telemetry client profile. AnyConnect uses the default value if the profile does not specify one.

The actsettings.xml file provides the default telemetry client profile settings. The parameters in the *telemetry_profile*.tsp file supersede those specified in the actsettings.xml file. See using the "Configuring the Telemetry Client Profile" on page 7-12 for more information about the *telemetry_profile*.tsp file.

The telemetry client profile parameters sent by the WSA in response to the service status request supersede the parameters specified in the *telemetry_profile*.tsp file. The telemetry module stores the WSA settings in the endpoint's registry. The telemetry module updates the registry when it receives new settings from the WSA. This allows the telemetry module to use the same settings when no VPN session is active.

Note The parameters sent by the WSA, in response to the service status request, are configured on WSA releases 7.1 or later.

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.

Table B-1 Telemetry Parameters Defined in XML Configuration Files

Element name	Description	Range	Default Value	Specified by Profile Editor on ASDM	Specified by the WSA
Telemetry	Parent element for all telemetry module elements.				
ServiceDisable	Enables or disables telemetry service	false true	false Telemetry is enabled by default after editing and saving the telemetry profile.	Yes	No
MaxHistLog	Maximum size of the activity history repository.	2-1000 (MB)	100	Yes	No
MaxHistDays	Maximum number of days to retain activity history.	1-1000 (days)	180	Yes	No
AvCheckInterval	Interval for checking new antivirus notification.	5-300 (seconds)	60	Yes	No
PostRetries	Number of retransmitting attempts if report posting or service check fails.	0-10 (times)	2	Yes	No
NewKeyInterval	Interval of changing Internal and External AES keys (0 indicates only changing at service starting time)	0-24 (hours)	0	Yes	No
ExemptFromHooking	Contains a list of <AppName> elements that contain application filenames, or paths to application filenames, that will be exempted from telemetry reporting.	None - unlimited	none	Yes	No
AppName	Contains an application filename, or a path to an application filename, that will be exempted from telemetry reporting. Child element of <ExemptFromHooking>	none-256 (Bytes)	none	No	
CiscoCert	Cisco's certificate with the pubic key to encrypt External AES keys.	None-4 (KB)	None	No	No

Element name	Description	Range	Default Value	Specified by Profile Editor on ASDM	Specified by the WSA
CustCert	Your certificate with the public key to encrypt internal AES keys and also to encrypt external AES keys. This must be a PEM certificate type.	None-4 (KB)	None	Yes	No
MaxPayLoad	Maximum payload length of report posting request	1024 - 65535 (KB)	10240 KB	No	Yes
ServiceHost	Name of AnyConnect Secure Mobility service portal.	None-1 (KB)	mus.cisco.com	No	No
ServiceProxy	Proxy server name and port for posting report with formatting of “proxy:port”	None-1 (KB)	none	No	No
OptIn	AnyConnect Secure Mobility /Telemetry feature enabled.	Yes or No	No	No	Yes
ServiceName	Specifies the AnyConnect Secure Mobility service name.	None-1 (KB)	TelemetryReport	No	No
RelativeURL	Relative URL of AnyConnect Secure Mobility service for report posting.	None-1 (KB)	TelemetryReport	No	Yes
DetailLevel	Level of reporting URL details (**Standard** indicates full URL. **Limited** indicates store hostname and domain name of every path component.)	Standard or Limited	Limited	No	Yes
ExcludedDoamin	Contains a list of <Domain> elements that specify domain names of internal URLs.	None - unlimited	none	No	Yes
Domain	Contains an internal URL that is exempt from telemetry reporting. For example: **cisco.com.** Child element of <ExcludedDomain>	none-1 (KB)	none	No	Yes

Element name	Description	Range	Default Value	Specified by Profile Editor on ASDM	Specified by the WSA
DebugLevel	Log message detail levels 0 – error only 1 – warnings 2 – states 3 – information 4 – debug 5 – all	0-5	1	No	No
ACTuserDebugLevel	Debug levels for hooking DLL (actuser.dll) 0 – No Log 1 – Debug Log	0-1	0	No	no

Example: AnyConnect Telemetry Client Profile

```
Refer to the following example to configure AnyConnect Telemetry:
<?xml version="1.0" encoding="UTF-8"?>
<Telemetry>
        <ServiceDisable>false</ServiceDisable>
        <MaxHistLog>100</MaxHistLog>
        <MaxHistDays>180</MaxHistDays>
        <AvCheckInterval>60</AvCheckInterval>
        <PostRetries>2</PostRetries>
        <ExemptFromHooking>
                <AppName>C:\Program Files\Cisco\CSAgent\bin\okclient.exe</AppName>
        </ExemptFromHooking>
        <CustCert>
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBIQDO5BLlnIfNvuctLkunNIIlNNqB8AYW2X1CQ2UBd0IfJVjquf22
p1UoOUmPx1KqA2zWdqfUzVUqUQUCdZuVw+kWkXOMLVz7lNLpEjmU1PAOoqLeqoUe
NY3IzKInvLIzUQA6oOb8kvCPlN7n7mvjqC6wwvqjJaQCUYbL2/c/4qbIKQIDAQAB
AoIAqIQTjqc7Mlqv2222dOEpQoYtax8ywIqV/q3XQ4U2pOm7wULqLxIU+yIIj/dx
qT6ZIE80jLInUl2W7n1/7vCtylEIqzxKIwJAIOZf+q58KotInzPyIYITAAYU27Tf
qnoICOolwZYiDeXUCA7CWJXLm27oDqF5OlI+ImaUIeqyOUc8cZoUUUXtIQJBAM2J
WlDVI2mxxiIfq2ZtbUdpJzbqtwmEmPEnBEn8PqkqZndY1xdWW3JIuaIl7qQwwO2I
cDbUyM/mtVNvdMDKCjmCQQDTaJUkvB0LED51JIO3KmU8LIQq+4Mamej+qFIZVYiy
cFKfI+U0wqfIo4LILzP78OW4E2OmeaWqmza7VLC4aUUF
-----END RSA PRIVATE KEY-----
        </CustCert>
</Telemetry>
```

APPENDIX C

Communicating User Guidelines

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

Responding to a TUN/TAP Error Message with Mac OS X 10.5

During the installation of AnyConnect on Mac OS X 10.5 and earlier versions, the following error message sometimes appears:

```
A version of the TUN virtual network driver is already installed on this system that is
incompatible with the AnyConnect client. This is a known issue with OS X version 10.5 and
prior, and has been resolved in 10.6. Please uninstall any VPN client, speak with your
System Administrator, or reference the AnyConnect Release Notes for assistance in
resolving this issue.
```

Mac OS X 10.6 resolves this issue because it provides the version of the TUN/TAP virtual network driver AnyConnect requires.

Versions of Mac OS X earlier than 10.6 do not include a TUN/TAP virtual network driver, so AnyConnect installs its own on these operating systems. However, some software such as Parallels, software that manages data cards, and some VPN applications install their own TUN/TAP driver. The AnyConnect installation software displays the error message above because the driver is already present, but its version is incompatible with AnyConnect.

To install AnyConnect, you must remove the TUN/TAP virtual network driver.

Note Removing the TUN/TAP virtual network driver can cause issues with the software on your system that installed the driver in the first place.

To remove the TUN/TAP virtual network driver, open the console application and enter the following commands:

sudo rm -rf /Library/Extensions/tap.kext

sudo rm -rf /Library/Extensions/tun.kext

sudo rm -rf /Library/StartupItems/tap

sudo rm -rf /Library/StartupItems/tun

sudo rm -rf /System/Library/Extensions/tun.kext

sudo rm -rf /System/Library/Extensions/tap.kext

sudo rm -rf /System/Library/StartupItems/tap

sudo rm -rf /System/Library/StartupItems/tun

After entering these commands, restart Mac OS, then re-install AnyConnect.

64-bit Internet Explorer Not Supported

AnyConnect installation via WebLaunch does not support 64-bit versions of Internet Explorer. If using Windows on x64 (64-bit), use the 32-bit version of Internet Explorer or Firefox to install WebLaunch. At this time, Firefox is available only in a 32-bit version.

Avoiding the Wireless Hosted Network

Using the Windows 7 Wireless Hosted Network feature can make AnyConnect unstable. When using AnyConnect, we do not recommend enabling this feature or running front-end applications that enable it (e.g., Connectify or Virtual Router).

Mac OS X 10.6 Sends All DNS Queries in the Clear

With split-DNS enabled, Mac OS X 10.6 sends all DNS queries in the clear. It should send DNS queries targeting split-DNS domains over the VPN session. Apple plans to resolve this issue in an upcoming update.

Start Before Logon and DART Installation

The Start Before Logon component requires that AnyConnect be installed first.

If SBL or DART is manually uninstalled from an endpoint that then connects, these components will be re-installed. This behavior will only occur if the head-end configuration specifies that these components be installed and the preferences (set on the endpoint) permit upgrades.

Responding to a Quarantine State

An endpoint that does not comply with corporate policies for access shows a network status of *Quarantined* on the AnyConnect Connection tab.

An ACL assigned to a dynamic access policy applied to a quarantined session typically grants access only to remediation services such as antivirus and antispyware updates.

A session in a quarantined state must have sufficient time to remediate the endpoint. Following this time period, the user must click **Reconnect** to exit the state and start a new posture assessment.

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*.

If you run the CLI in interactive mode, it provides its own prompt. You can also use the command line. Table 3-1 shows the CLI commands.

Table 3-1 AnyConnect Client CLI Commands

Command	Action
connect *IP address or alias*	Client establishes a connection to a specific ASA.
disconnect	Client closes a previously established connection.
stats	Displays statistics about an established connection.
quit	Exits the CLI interactive mode.
exit	Exits the CLI interactive mode.

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

Windows

```
connect 209.165.200.224
```

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

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

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

stats

Displays statistics for the current connection; for example:

```
VPN> stats
[ Tunnel Information ]

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

[ Tunnel Details ]

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

[ Data Transfer ]

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

[ Secure Routes ]

    Network     Subnet
    0.0.0.0     0.0.0.0
VPN>
```

disconnect

Closes a previously established connection; for example:

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

quit or **exit**

Either command exits the CLI interactive mode; for example:

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

Linux or Mac OS X

`/opt/cisco/vpn/bin/vpn connect 1.2.3.4`
Establishes a connection to an ASA with the address *1.2.3.4*.

`/opt/cisco/vpn/bin/vpn connect some_asa_alias`
Establishes a connection to an ASA 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.

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**.

AnyConnect Hides the Internet Explorer Connections Tab

Under certain conditions, AnyConnect hides the Connections tab located in Internet Explorer Tools, Internet Options. 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 ASA 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 ASA must be set to Tunnel All Networks.

Using a Windows Remote Desktop

Using one of these three methods, you can access a network computer remotely while the connection is being managed by NAM on that network computer:

- Network Profiles with Machine-only Authentication
- Network Profiles with Machine and User Authentication
- Network Profiles with User-only Authentication

Network Profiles with Machine-only Authentication

To use this method, NAM must be configured for machine authentication. When a user logs in remotely, NAM remains authenticated with the machine's credentials. No attempt is made to authenticate with the user's credentials or to reauthenticate with the machine's credentials.

Network Profiles with Machine and User Authentication

To use this method, NAM must be configured for machine authentication plus user authentication. Without any users logged in, NAM authenticates with the machine's credentials.

For Vista or Windows 7, when a user logs in, whether locally or remotely, NAM authenticates only the first user session, ignoring subsequent logon sessions while the first session persists. When the first logon session ends, NAM stops the user connection and reverts to a machine connection. NAM tracks the first succeeding logon attempt after the original session ended as the user session, regardless of whether the secondary sessions were present when the first session ended. Because NAM ignores subsequent logon sessions while the first session is operational, any secondary sessions created after the first session will momentarily lose their network connection when the original session is destroyed or when a subsequent logon attempt is made. If the first user is logged on locally, a remote desktop session will not result in the reauthentication of this user.

Note Only the first logon user session has access to the AnyConnect GUI.

For Windows XP, the number of user sessions are limited to 1, either local or remote; therefore, a new user logon always results in a previous user logoff. If the user is logged on locally, a remote desktop session with the same user will not result in the reauthentication of this user.

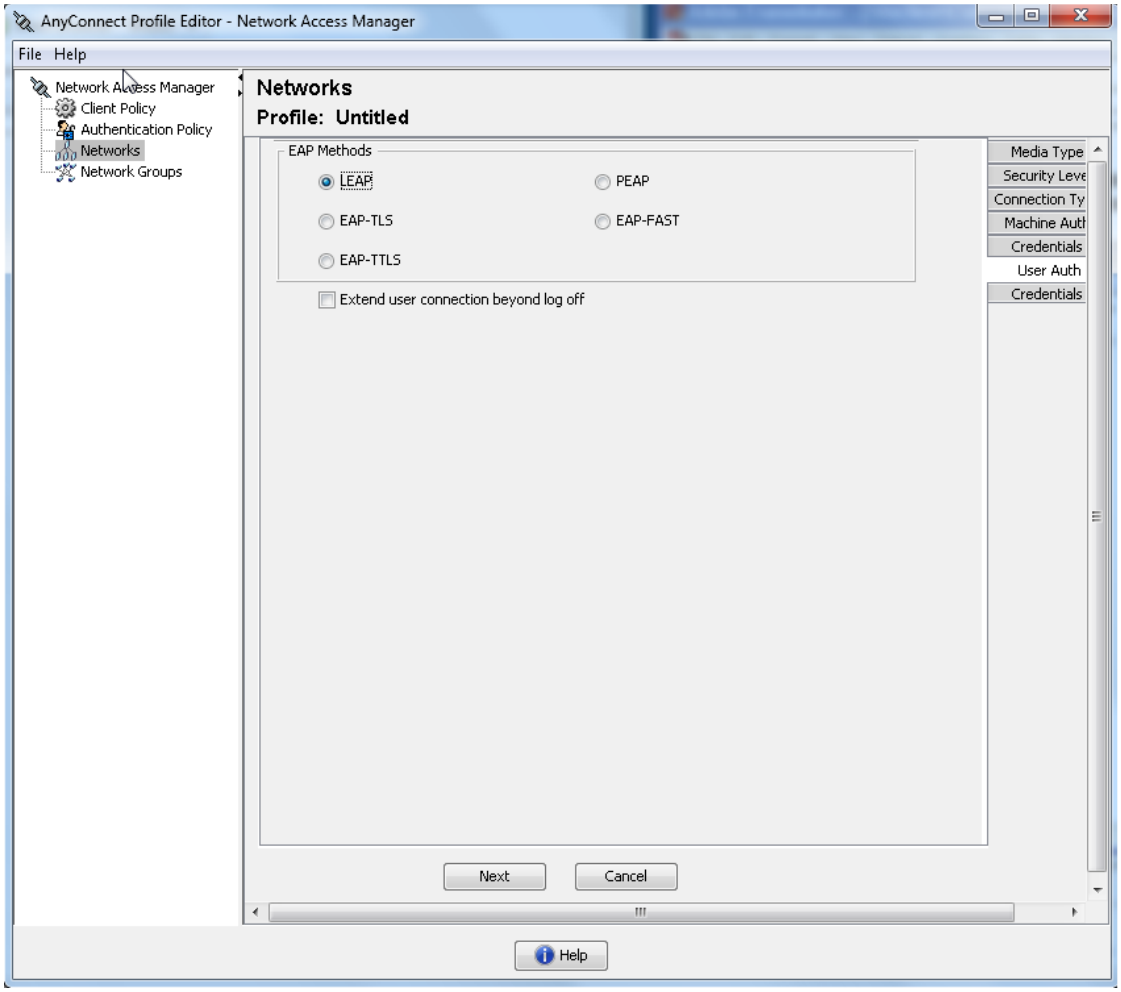
Note When using machine and user authentication, complications may occur. For example, depending on the configuration, the machine and the user profiles may assign the computer to different networks (usually VLANs, referred to here as *user VLAN* and *machine VLAN*). Therefore, if the network computer is connected as a machine on the machine VLAN (user logged off) and later it is accessed remotely, the computer connects as a user VLAN. For that reason, you may need to re-establish the remote desktop session with a different IP address on a different VLAN (the user VLAN).

Network Profiles with User-only Authentication

To use this method, NAM must be configured for user-only authentication. Normally with this configuration and without any users logged in, NAM cannot establish a network connection; therefore, a remote desktop connection is not possible. Now when users log on, they can establish a remote desktop connection. This remote session will not result in the re-authentication of the user.

The extendUserConnectionBeyondLogoff parameter (see Figure C-1) makes it possible to configure a user authentication so that it remains active (connected) even after the local user has logged off. Therefore, you do not need machine authentication solely to support remote desktop functionality.

Figure C-1 GUI Location of Extend User Connection Beyond Logoff Parameter



If a reauthentication that requires credentials occurs while the user is logged out and if NAM no longer has access to the required credentials (such as a user certificate), NAM cannot reauthenticate the connection. Consequently, the authentication attempt times out, and the authenticator eventually disconnects the client. When this occurs, NAM re-evaluates the available connections and attempts to make a network connection from the available machine connections.

For Vista or Windows 7, when a user logs in, whether locally or remotely, NAM authenticates only the first user session, ignoring subsequent logon sessions while the first session persists. When the first logon session ends, NAM stops the user connection and reverts to a machine connection. NAM tracks the first succeeding logon attempt after the original session ended as the user session, regardless of whether the secondary sessions were present when the first session ended. Because NAM ignores subsequent logon sessions while the first session is operational, any secondary sessions created after the first session will momentarily lose their network connection when the original session is destroyed or when a subsequent logon attempt is made. If the first user is logged on locally, a remote desktop session will not result in the reauthentication of this user.

Note Only the first logon user session has access to the AnyConnect GUI.

For Windows XP, the number of user sessions are limited to 1, either local or remote; therefore, a new user logon always results in a previous user logoff. If the user is logged on locally, a remote desktop session with the same user will not result in the reauthentication of this user.

When using machine and user authentication, complications may occur. For example, depending on the configuration, the machine and the user profiles may put the computer on different networks (usually VLANs, referred to here as user VLAN and machine VLAN). Therefore, if the network computer is connected as a machine on the machine VLAN (user logged off) and later it is accessed remotely, the computer connects as a user VLAN. For that reason, you may need to re-establish the remote desktop session with a different IP address on a different VLAN (the user VLAN).

Credential Provider on Microsoft Vista and Win7

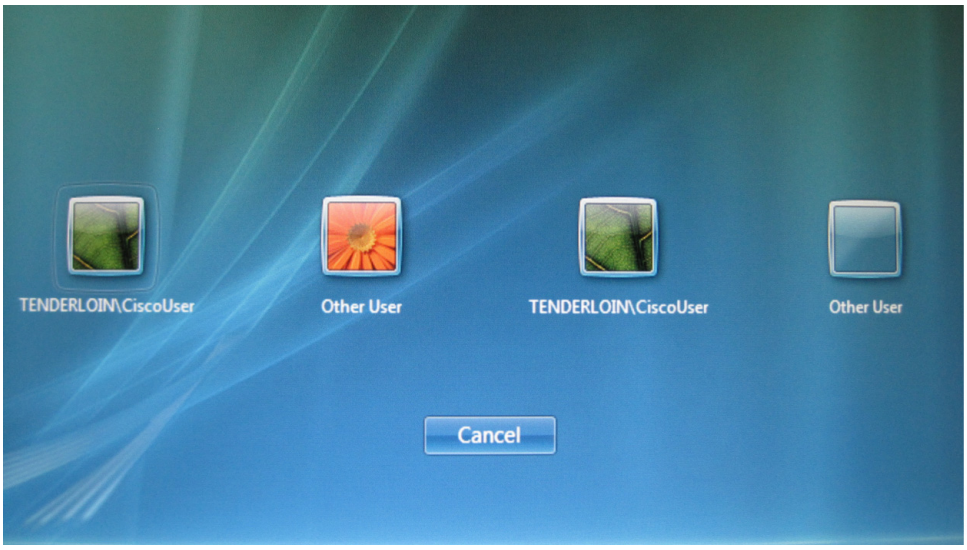
To provide single sign-on (SSO) user authentication using Windows logon credentials on Microsoft Vista and Windows 7, the NAM module implements a password (logon) credential provider. The credential provider (CP) captures the Windows credentials during the logon process and provides notifications when users log in or out of the system to allow the NAM service to switch between machine and user authentication.

For AnyConnect 3.0, the NAM CP is implemented as a wrapper around the Microsoft Password Credential Provider, which is filtered out by the NAM CP to prevent multiple sets of logon tiles from displaying. If this filtering is not done, a logon tile is displayed for each CP.

If a third-party CP is installed on a system, NAM does not detect this, and the user may be presented with multiple sets of logon tiles. If users choose the third-party CP to log on, NAM is unable to obtain the Windows credentials, thus preventing the single sign-on user authentication operation.

Figure C-2 shows the logon screen from a system with both NAM CP and a third-party CP installed.

Figure C-2 AnyConnect Icon Without the Overlay



You have two options for this issue:

1. For the user to distinguish between tiles, the NAM CP provides the option to overlay the AnyConnect icon over the logon tile. A small AnyConnect icon is placed in the lower-right corner of the login tile bitmaps. The user can then see their login tile images and still be aware that AnyConnect is active. Without this Anyconnect icon, a user could not know if login tiles are managed by AnyConnect or not.

   By default, the CP operates as described above. Users can change a value in the registry to disable it, and then the CP will not overlay the AnyConnect icon on login tiles. They would display exactly as they would if AnyConnect was not installed.

   To disable this option, the following registry value is used:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticati
   on\Credential Providers\
   {B12744B8-5BB7-463a-B85E-BB7627E73002}\OverlayIcon]
   ```

   OverLayIcon is a REG_DWORD where a value of 0 disables the overlay icon, and a value of 1 enables the overlay icon. This default value is 1 and is set by the AnyConnect installer. If a registry key is missing or incorrect, the CP assumes the value of 1.

   Sometimes Windows presents a tile labeled “other users” and in some cases, no picture appears in the associated tile. What appears inside the tile frame is whatever happens to be in the background of the window on which the tiles are placed; therefore, the tiles may appear empty or transparent. For technical reasons, the CP is unable to overlay an icon on an empty tile, so the CP must provide its own bitmap when this occurs.

   By default, the CP uses a stock image embedded in the CP executable file. Users may provide a picture to use in place of the stock empty tile by saving the picture in a .bmp file and adding a registry string value that provides the location of the file.

   To set the bitmap file location, the following registry value must be added:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticati
   on\Credential Providers\
   {B12744B8-5BB7-463a-B85E-BB7627E73002}\OverlayEmptyTile]
   ```

   “OverlayEmptyTile” is a REG_SZ value that contains a full path to the bitmap file. Example: "C:\users\jsmith\Pictures\MyEmptyTile.bmp"

   Note The file must be a Windows .bmp file.

   If overlays are disabled (using the overlayicon registry setting), the OverlayEmptyTile option is ignored, and users cannot provide an empty tile bitmap if they disable the icon overlay. The OverlayEmptyTile value is not provided by the AnyConnect installer.

Figure C-3 shows the logon screen from a system with both NAM CP and a third-party CP installed. In this example, the AnyConnect icon is displayed on the logon tile, indicating the NAM CP.

Figure C-3 Anyconnect Icon With Overlay

2. To prevent third-party credential provider's logon tiles from being displayed, the NAM CP can filter these tiles out.

   To set this option, you must add the following registry value:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\ {B12744B8-5BB7-463a-B85E-BB7627E73002}\Filters]
   ```

   Any credential provider that needs to be filtered out is added as a key with its specific GUID in the Filters key.

Note The *Filters* value is not provided by the Anyconnect installer.

When GPO Configured for SSO

When GPO wired or wireless profiles are configured for SSO, winlogon short-circuits the Credential Provider querying process and directly loads the native L2NA credential provider in addition to the NAM CP. This presents the user with two sets of tiles. If GPO profiles that are not configured for SSO, the logon process works as expected, the Microsoft CP is filtered out by the NAM CP, and the user is presented with a single set of tiles.

SmartCard CP

The Microsoft Smartcard Credential Provider is not wrapped by the NAM CP; therefore, prelogon smartcard based certificate authentication is not supported on post XP platforms for AnyConnect 3.0.

NAM CP Pre-logon Status Display

When the Connection Settings value *Before User Logon* is specified as part of the Client Policy, the NAM CP displays a status dialog box to inform the user of the connection status. This dialog box will be displayed after the user credentials are received by the CP and is displayed until the connection is successful, or until the value chosen by the *Time to Wait Before Allowing User to Logon* has expired. You can cancel this dialog box at any time.

Cipher Requirements Running Internet Explorer on Windows XP

With Windows XP, the Internet Explorer browser is not capable of using AES and requires either RC4 or 3DES. If remote users disable RC4 and 3DES in the SSL settings page, the AnyConnect connection fails. For a successful AnyConnect connection using Internet Explorer, remote users must not specify AES as the only cipher in the SSL settings for IE.