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

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.

Note If you manually deploy the VPN profile, you must also upload the profile to the ASA. When the client system connects, AnyConnect verifies that the profile on the client matches the profile on the ASA.

If you have disabled profile updates, and the profile on the ASA is different from the client, then the manually deployed profile won't work.

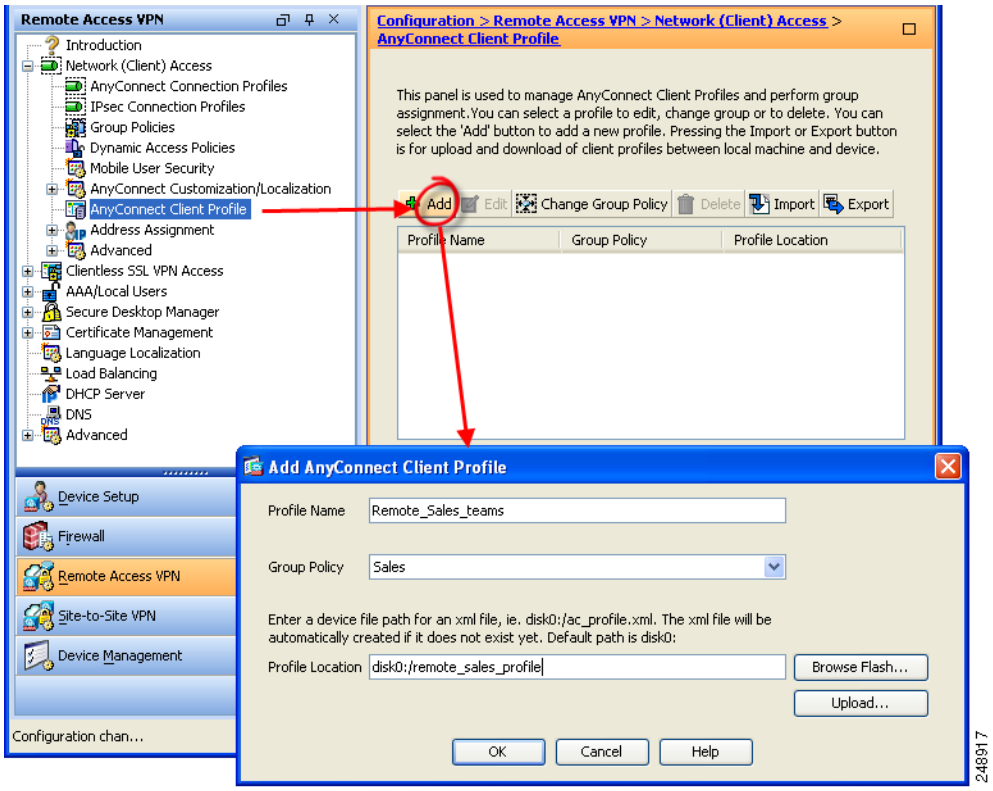
To activate the profile editor, create and edit a profile in ASDM, follow these steps:

Step 1 Load the AnyConnect software package as an AnyConnect Client image, if you have not done so already.

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

Step 3 Click **Add**.

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.

Note When specifying a name, avoid the inclusion of the .xml extension. If you name the profile example.xml, ASDM adds an .xml extension automatically and changes the name to example.xml.xml. Even if you change the name back to example.xml in the Profile Location field on the ASA, the name returns to example.xml.xml when you connect with AnyConnect by remote access. If the profile name is not recognized by AnyConnect (because of the duplicate .xml extension), IKEv2 connections may fail.

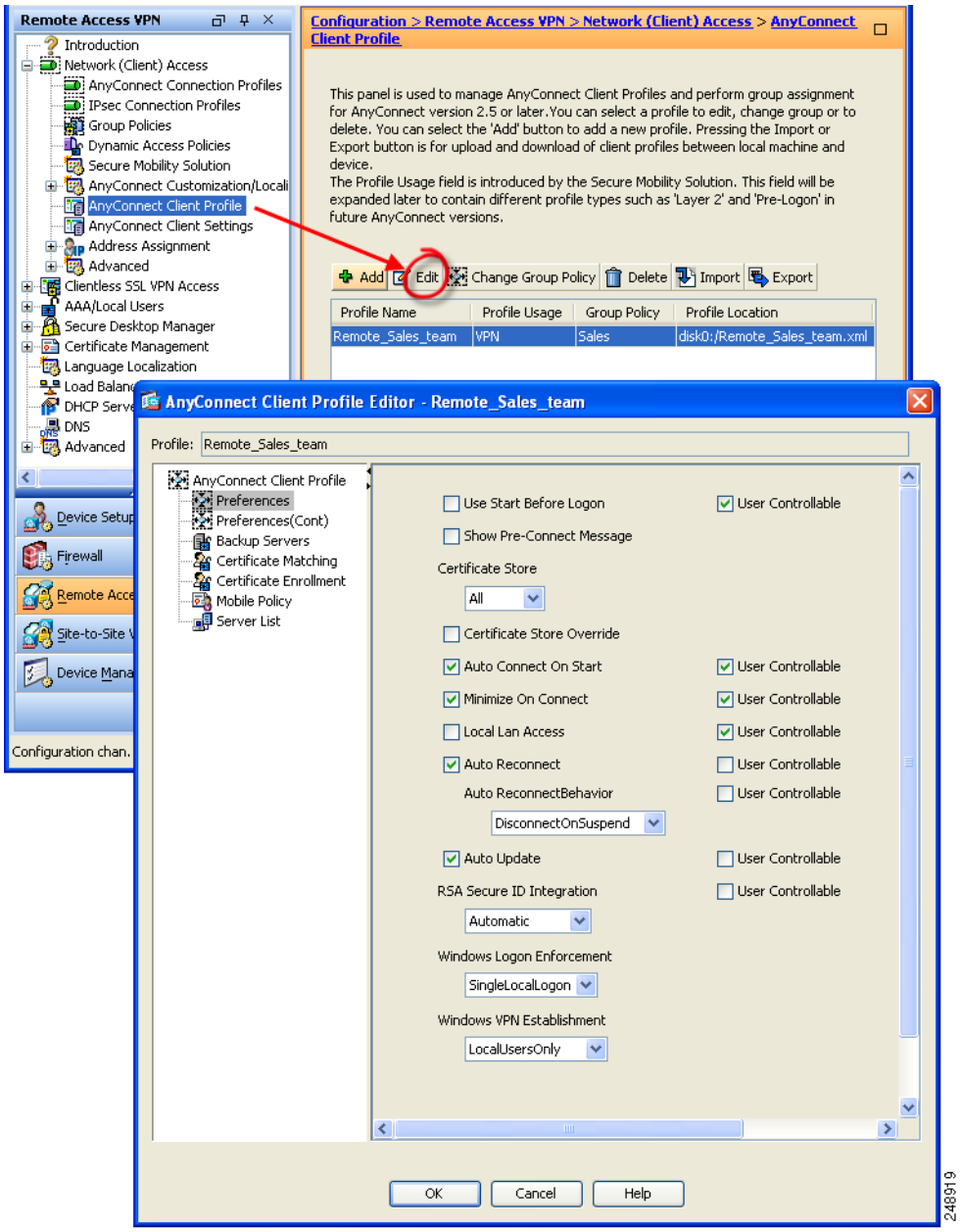
Step 5 Choose a group policy (optional). The ASA applies this profile to all AnyConnect users in the group policy.

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**. Enable AnyConnect features in the panes of the profile editor.

Step 8 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.

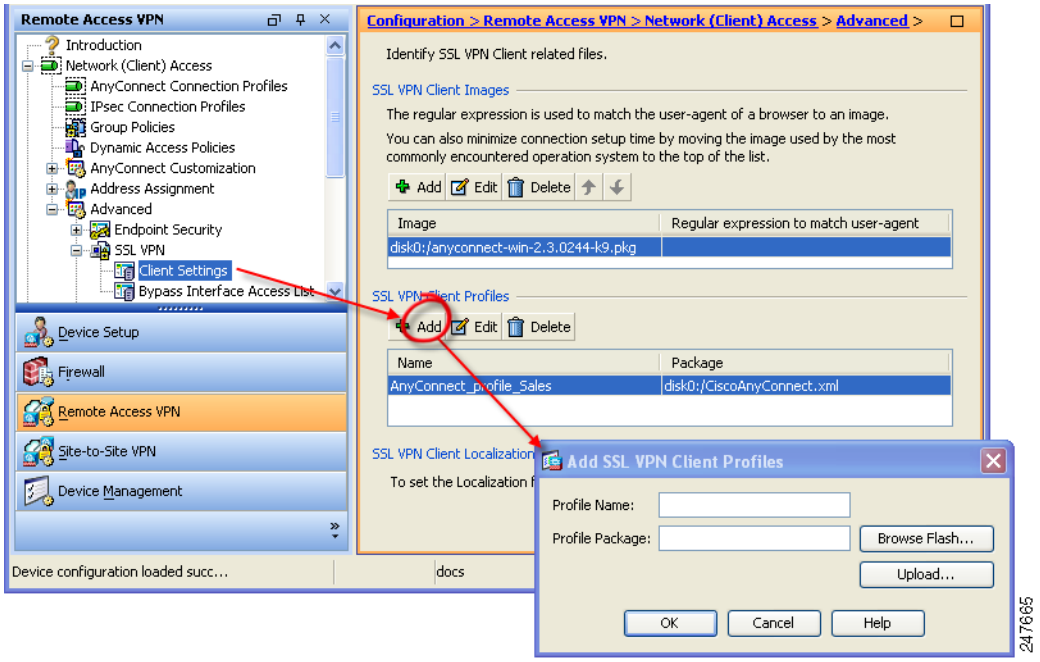
Note You must include the ASA in the host list in the profile so the client GUI displays all the user controllable settings on the initial VPN connection. If you do not add the ASA address or FQDN as a host entry in the profile, then filters do not apply for the session. For example, if you create a 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 the Configuring a Server List, page 3-50.

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**.

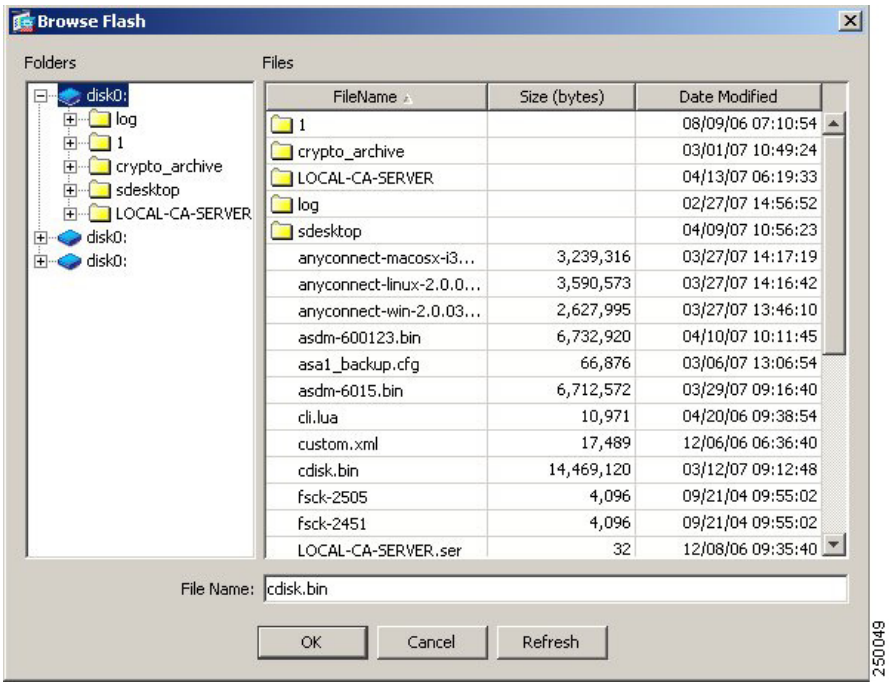
Step 2 In the SSL VPN Client Profiles area, click **Add**.

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**.

Figure 3-4 Browse Flash Dialog Box



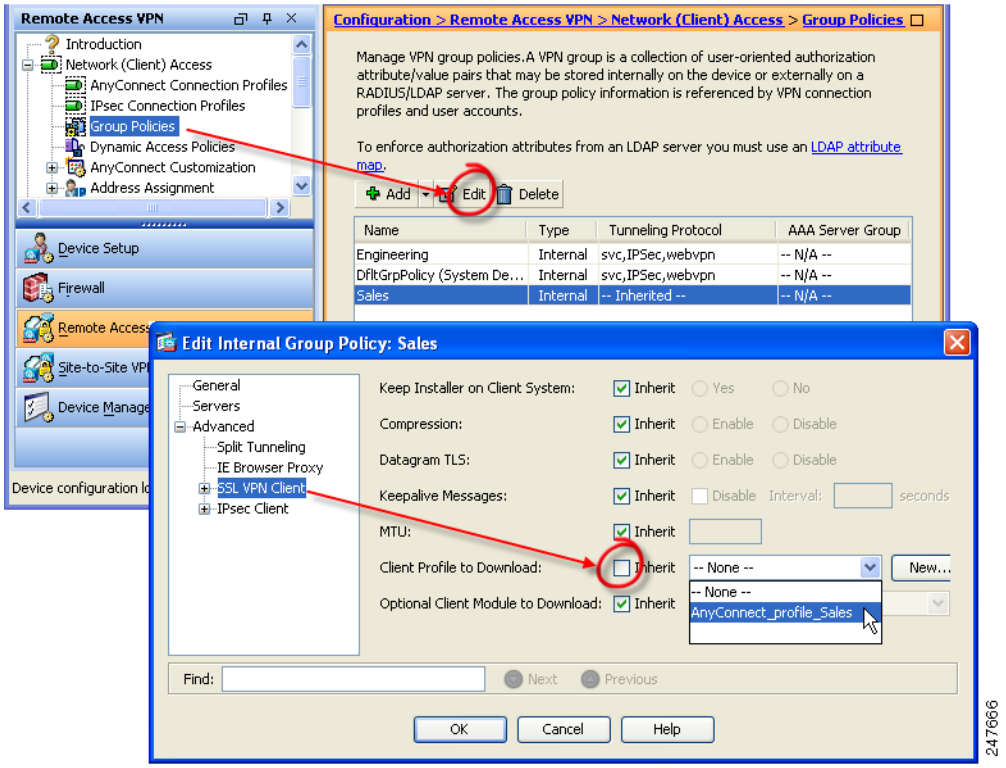
Step 4 Select a file from the table. The file name appears in the File Name field below the table.

Step 5 Click **OK**. The file name you selected appears in the Profile Package field of the Add or Edit SSL VPN Client Profiles dialog box.

Step 6 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 7 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 Specify the Profile to use in the Group Policy



Step 8 Uncheck **Inherit** and select an AnyConnect profile to download from the drop-down list.

Step 9 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 the Network Access Manager 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”.

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, 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.

Note AnyConnect cannot be started by third-party Start Before Logon applications.

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.

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 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**.

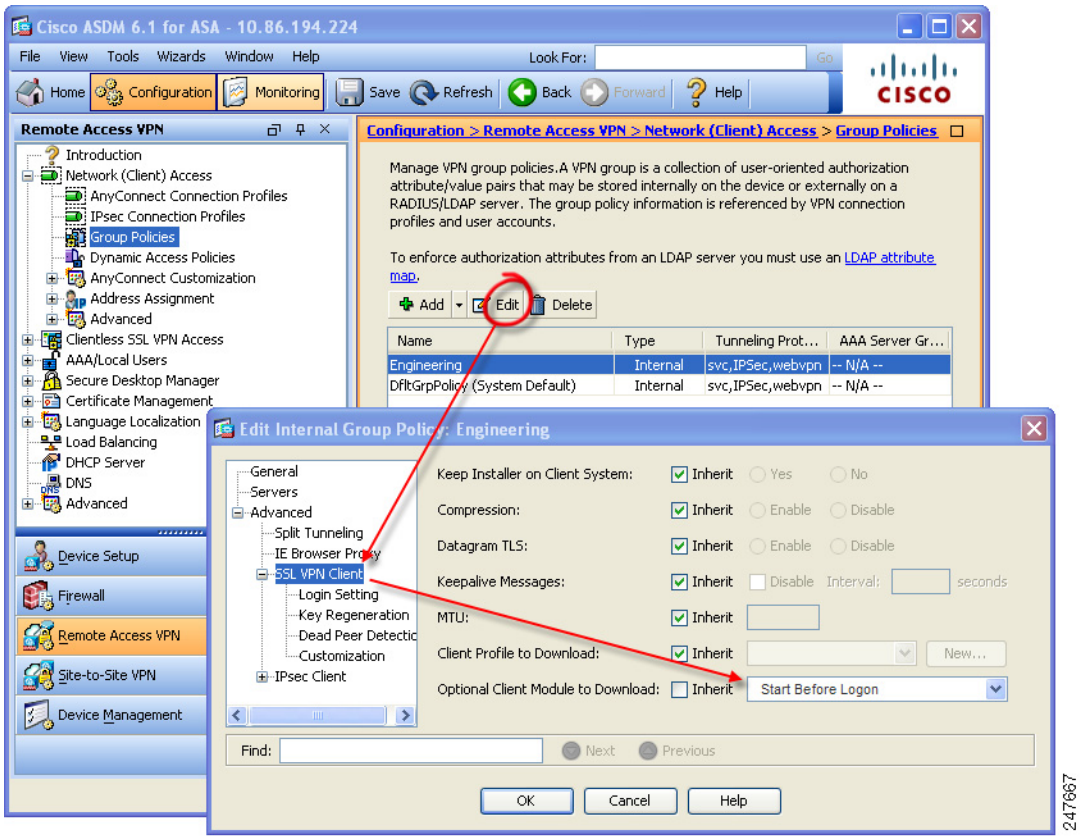
Step 2 Select a group policy and click **Edit**. The Edit Internal Group Policy window displays.

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 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 Secure Mobility
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.

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 "Configuring Start Before Logon (PLAP) on Windows 7 and Vista Systems" section on page 3-12. After activation, the user invokes the Network Connect component by clicking **Switch User**, then the **Network Connect** icon in the lower, right-hand part of the screen.

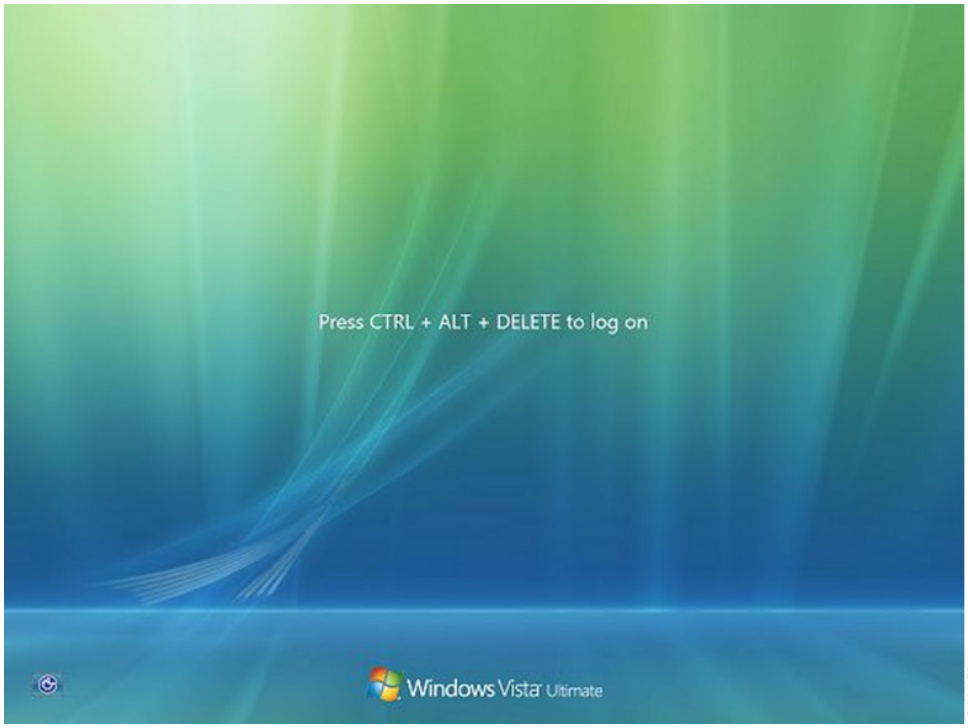
Note If the user mistakenly minimizes the user interface, the user can restore it by pressing the **Alt+Tab** key combination.

Logging on to a Windows 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:

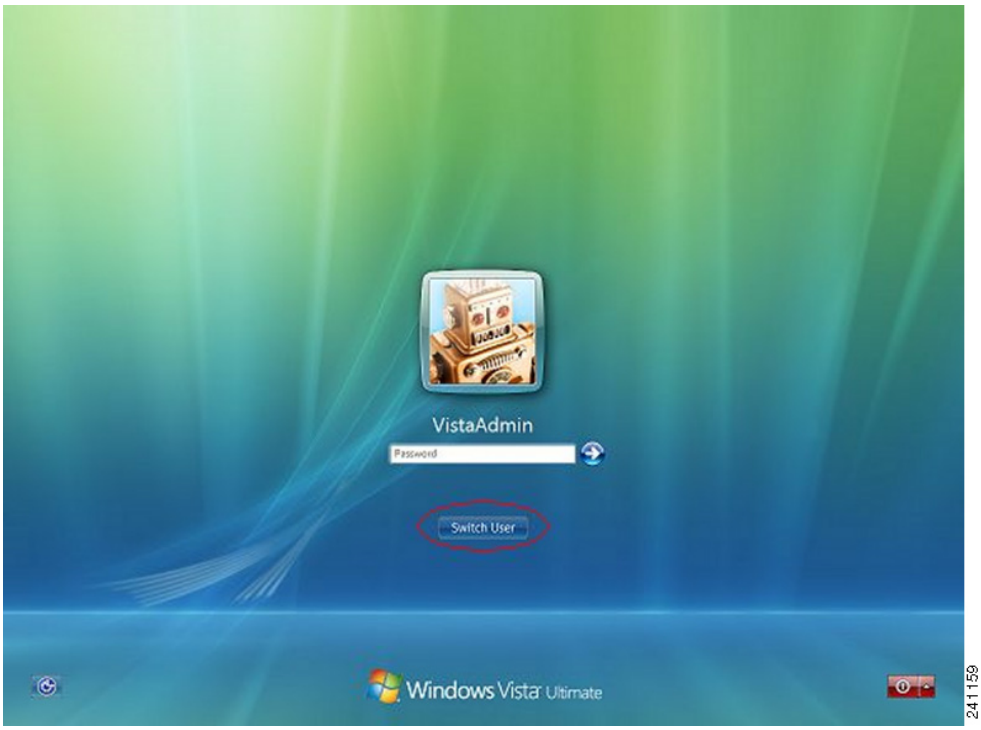
Step 1 At the Windows start window, users press the **Ctrl+Alt+Delete** key combination.

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



The Vista logon window appears with a Switch User button.

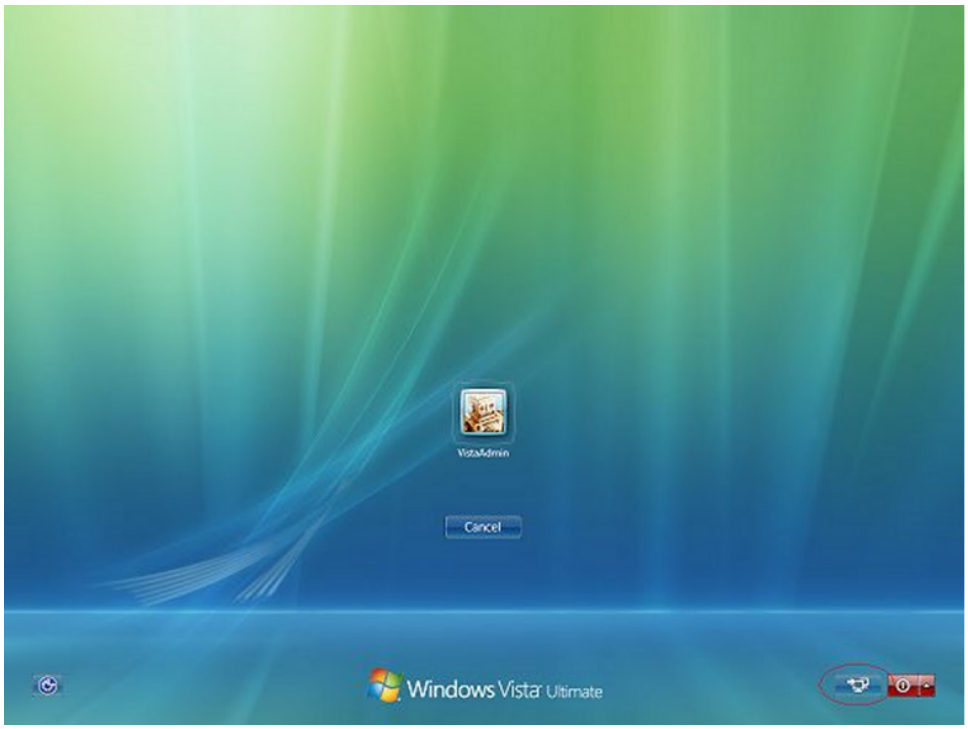
Figure 3-8 Example Logon Window with Switch User Button



Step 2 The user clicks **Switch User** (circled in red in this figure). The Vista Network Connect window displays. The network login icon is circled in red in Figure 3-8.

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

Figure 3-9 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.

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. This button is the only indication that the connection was successful.

Figure 3-10 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 3-10).

When the user clicks **Disconnect**, the VPN tunnel disconnects.

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

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

This behavior is a function of the Windows Vista PLAP architecture, not 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 VPN Client profile. No changes are required to the ASA configuration.

Trusted Network Detection Requirements

TND supports only computers running Microsoft Windows 7, Vista, or XP and Mac OS X 10.5,10.6 and 10.7.

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, page 3-2).

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

Step 3 Check **Automatic VPN Policy**.

Note Automatic VPN Policy 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 DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. You can assign multiple DNS suffixes if you add them to the split-dns list. See Table 3-1 for more examples of DNS suffix matching.

The AnyConnect client builds the DNS suffix list in the following order:

- the domain passed by the head end
- the split-DNS suffix list passed by the head end
- the public interface's DNS suffixes, if configured. If not, the primary and connection specific suffixes, along with the parent suffixes of the primary DNS suffix (if the corresponding box is checked in the Advanced TCP/IP Settings)

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 DNS Suffix Matching Examples

To Match this DNS Suffix:	Use this Value for TrustedDNSDomains:
cisco.com (only)	*cisco.com

Table 3-1 DNS Suffix Matching Examples (continued)

To Match this DNS Suffix:	Use this Value for TrustedDNSDomains:
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

Wildcards (*) are supported for DNS suffixes.

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. 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, 10.6, and 10.7.

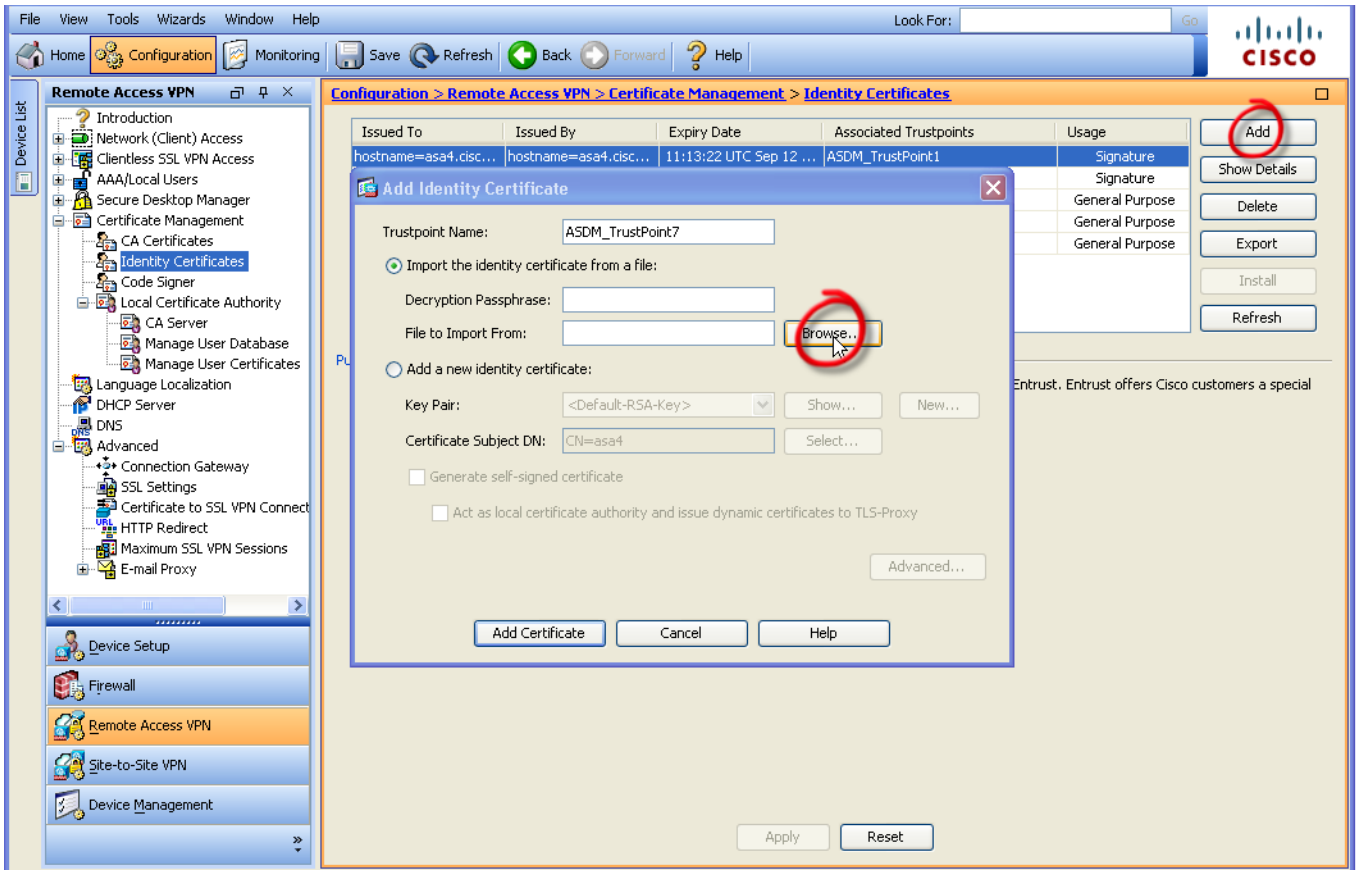
To prevent the download of an always-on VPN profile that locks a VPN connection to a rogue server, the AnyConnect client requires a valid, trusted server certificate to connect to a secure gateway. We strongly recommend purchasing a digital certificate from a certificate authority (CA) and enrolling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

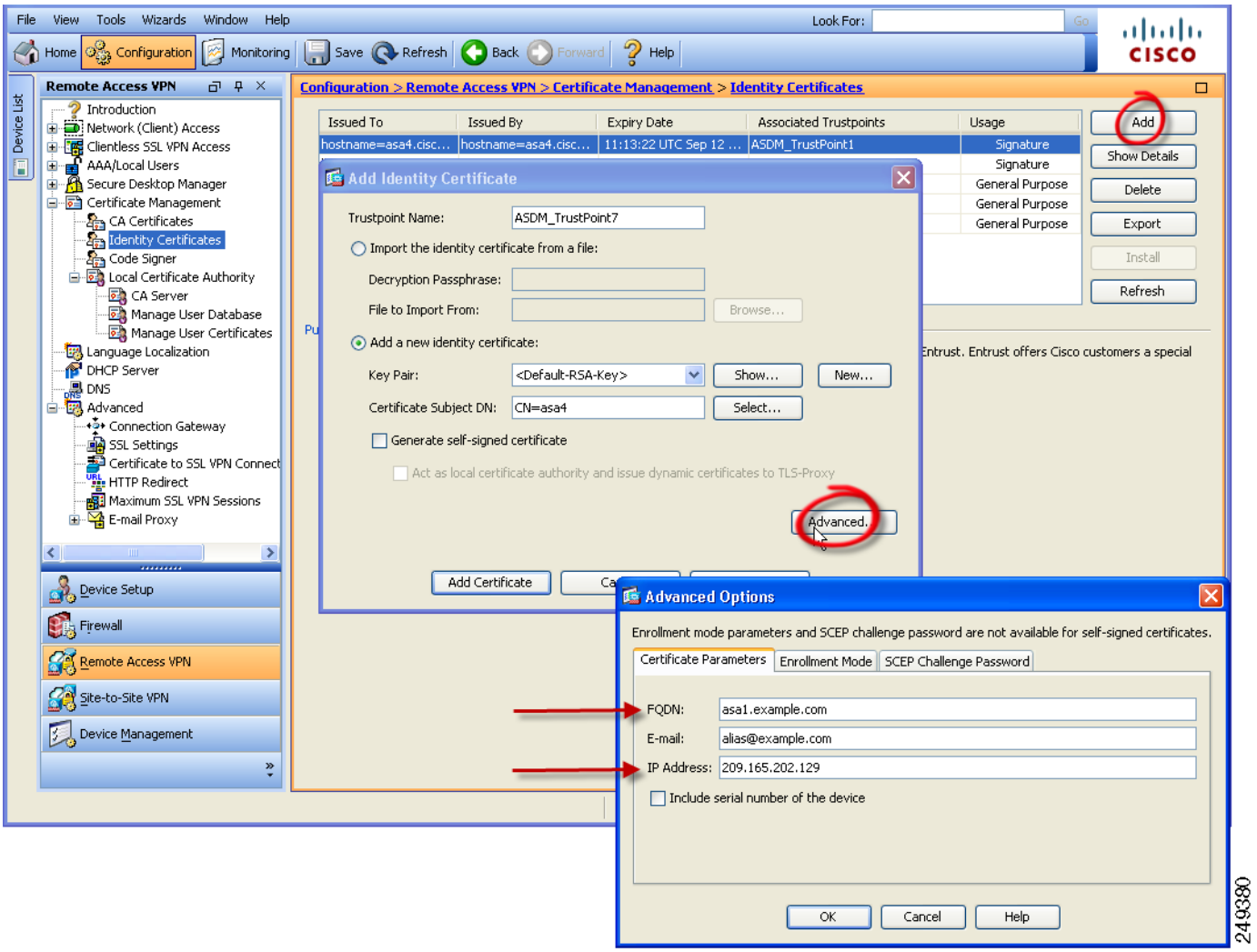
Figure 3-11 Enrolling a Public Certificate (ASDM 6.3 Example)



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.

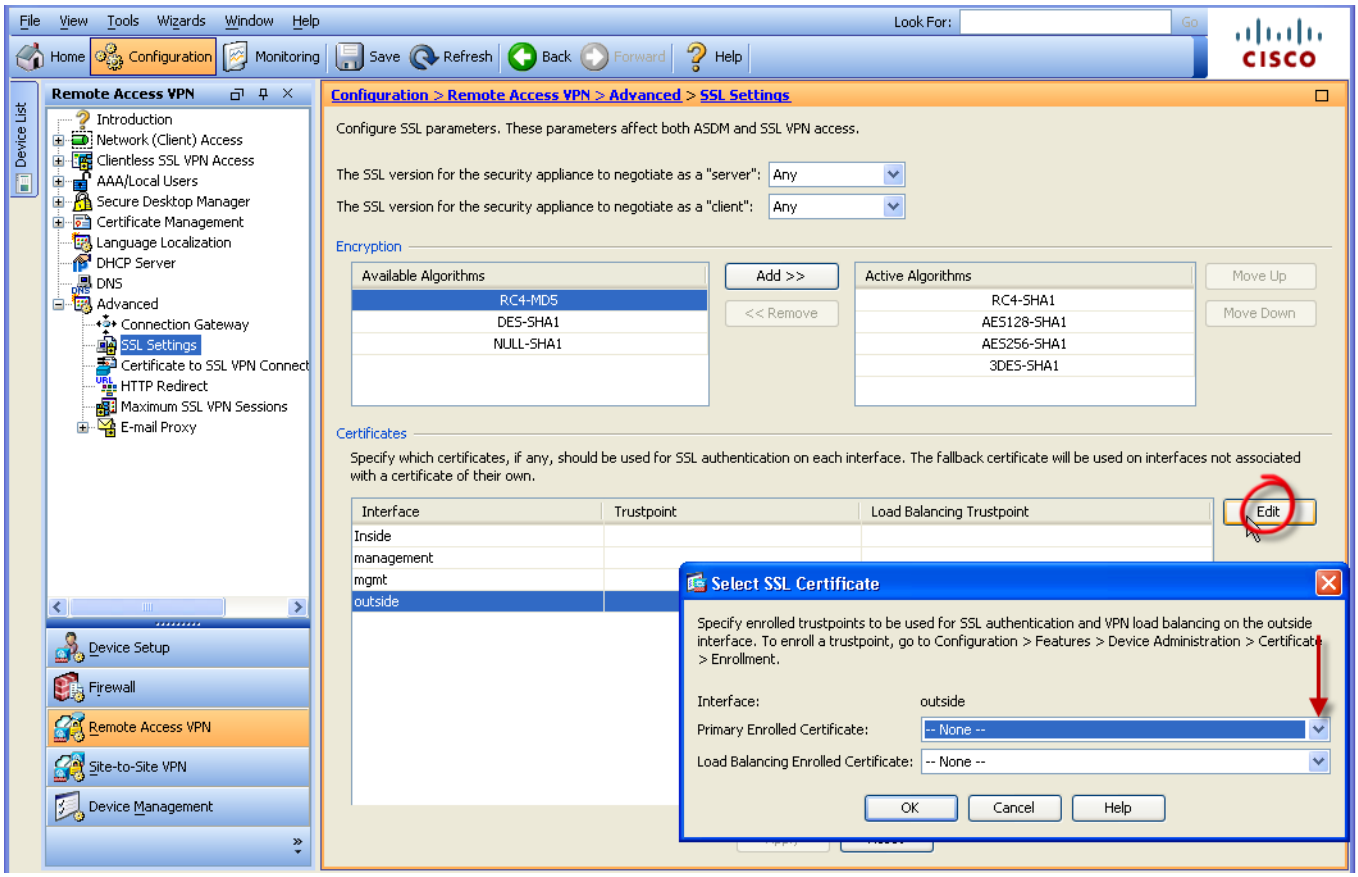
Use the **Advanced** button to specify the domain name and IP address of the outside interface if you are generating a self-signed interface.

Figure 3-12 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 3-13 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 the "Creating and Editing an AnyConnect Profile" section on 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 Trusted Network Detection using Configuring Trusted Network Detection, page 3-17.

Step 2 Check **Always On**.

Configuring a Policy to Exempt Users from Always-on VPN

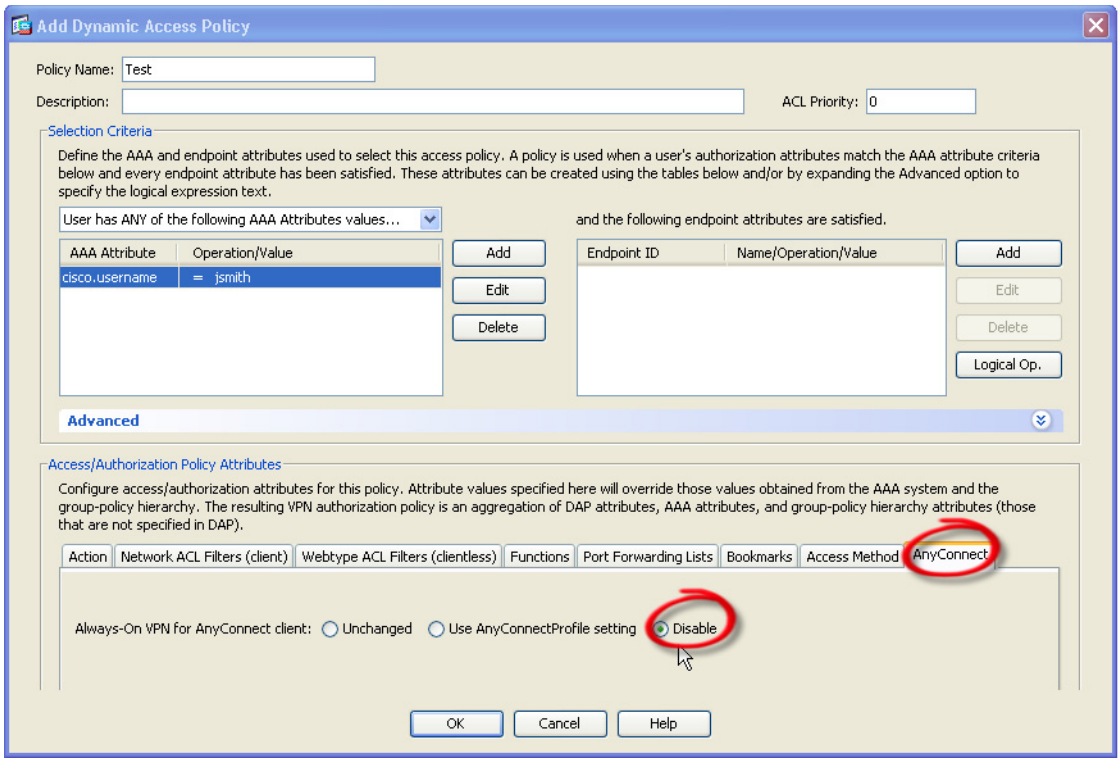
By default, always-on VPN is disabled. You can configure exemptions to override an always-on policy. For example, you might want to let certain individuals establish VPN sessions with other companies or exempt the always-on VPN policy for noncorporate assets.

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**.

Figure 3-14 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 those in the "Always-on VPN Requirements" section on page 3-20.

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 connectivity to the Internet or other local network resources. 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 they need access to the Internet or other local network resources.	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 the Captive Portal Hotspot Detection and Remediation Requirements, 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, or XP and Mac OS X 10.5,10.6, and 10.7.

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, page 3-17).

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 secure gateway is unreachable. AnyConnect does this by enabling packet filters that block all traffic from the endpoint that is not bound for a secure gateway to which the computer is allowed to connect.

  The fail-closed policy prevents captive portal remediation (described in the next sections) unless you specifically enable it as part of the 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 an 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—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 and 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, Windows Vista, or Windows XP and Mac OS X 10.5,10.6, and 10.7.

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.

AnyConnect does not modify any browser configuration settings during Captive Portal detection.

Captive Portal Hotspot Remediation

Captive portal remediation is the process of satisfying the requirements of a captive portal hotspot to obtain network access.

AnyConnect does not remediate the captive portal, it relies on the end user to perform the remediation.

The end user performs the captive portal remediation by meeting the requirements of the provider of the hostspot. These requirements could be paying a fee to access the network, signing an acceptable use policy, both, or some other requirement defined by the provider.

Captive portal remediation needs to be explicitly allowed in an AnyConnect VPN Client profile if AnyConnect Always-on is enabled and the Connect failure policy is set to **Closed**. If Always-on is enabled and the Connect Failure policy is set to **Open**, you don't need to explicitly allow captive portal remediation in an AnyConnect VPN Clien t profile because the user is not restricted from getting access to the network.

Configuring Support for Captive Portal Hotspot Remediation

You need to enable captive portal remediation in an AnyConnect VPN client policy if the Always-on feature is enabled and the connect failure policy is set to closed. If the connect failure policy is set to open, your users are not restricted from network acces, and so, are capable of remediating a captive portal without any other configuration of the AnyConnect VPN client policy.

By default, support for captive portal remediation is disabled. Use this procedure to enable captive portal remediation:

Step 1 Configure a connect failure policy (see Configuring a Connect Failure Policy, page 3-28).

Step 2 If you set the connect failure policy to closed, configure 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. 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 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 "Denial of Service" 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 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.

The Client Firewall feature is supported on Windows 7, Vista, & XP, Mac OS X 10.5-10.8, Red Hat Enterprise Linux 5 & 6 Desktop, and Ubuntu 9.x & 10.x.

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

The ACL AnyConnect_Client_Local_Print is provided with ASDM to make it easy to configure the client firewall. When you select that ACL for Public Network Rule in the Client Firewall pane of a group policy, that list contains the following ACEs:

Table 3-3 ACL Rules in AnyConnect_Client_Local_Print

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.

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**.

New Installation Directory Structure for Mac OS X

In previous releases of AnyConnect, AnyConnect components were installed in the **opt/cisco/vpn** path. Now, AnyConnect components are installed in the **/opt/cisco/anyconnect** path.

ScanCenter Hosted Configuration Support for Web Security Client Profile

The ScanCenter Hosted Configuration for the Web Security Hosted Client Profile gives administrators the ability to provide new Web Security client profiles to Web Security clients. Devices with Web Security can download a new client profile from the cloud (hosted configuration files reside on the ScanCenter server). The only prerequisite for this feature is for the device to have Web Security installed with a valid client profile.

Administrators use the Web Security Profile Editor to create the client profile files and then upload the clear text XML file to a ScanCenter server. This XML file must contain a valid license key from ScanSafe. The Hosted Configuration feature uses the license key when retrieving a new client profile file from the Hosted Configuration (ScanCenter) server. Once the new client profile file is on the server, devices with Web Security automatically poll the server and download the new client profile file, provided that the license in the existing Web Security client profile is the same as a license associated with a client profile on the Hosted server. Once a new client profile has been downloaded, Web Security will not download the same file again until the administrator makes a new client profile file available.

Note Web Security client devices must be pre-installed with a valid client profile file containing a ScanSafe license key before it can use the Hosted Configuration feature.

Split DNS Functionality Enhancement

AnyConnect supports true split DNS functionality for Windows and Mac OS X platforms, just as found in legacy IPsec clients. If the group policy on the security appliance enables split-include tunneling and if it specifies the DNS names to be tunneled, AnyConnect tunnels any DNS queries that match those names to the private DNS server. True split DNS allows tunnel access to only DNS requests that match the domains pushed down by the ASA. These requests are not sent in the clear. On the other hand, if the DNS requests do not match the domains pushed down by the ASA, AnyConnect lets the DNS resolver on the client operating system submit the host name in the clear for DNS resolution.

Note

- Split DNS supports standard and update queries (including A, AAAA, NS, TXT, MX, SOA, ANY, SRV, PTR, and CNAME). PTR queries matching any of the tunneled networks are allowed through the tunnel.
- Split-DNS does not support the "Exclude Network List Below" split-tunneling policy. You must use the "Tunnel Network List Below" split-tunneling policy to configure split-DNS.

AnyConnect tunnels all DNS queries if the group policy does not specify any domains to be tunneled or if Tunnel All Networks is chosen at Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Advanced > Split Tunneling. You can use any tool or application that relies on the operating system's DNS resolver for domain name resolution. For example, you can use a ping or web browser to test the split DNS solution. Other tools such as nslookup or dig circumvent the OS DNS resolver.

For Mac OS X, AnyConnect can use true split-DNS only when not configuring an IPv6 address pool. If an IPv6 address pool is configured, AnyConnect can only enforce DNS fallback for split tunneling.

This feature requires that you:

- configure at least one DNS server
- enable split-include tunneling
- specify at least one domain to be tunneled
- ensure that the **Send All DNS lookups through tunnel** check box is unchecked. You can find this check box under Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Advanced > Split Tunneling.

Using AnyConnect Logs to Verify

To verify if split-DNS is enabled, search the AnyConnect logs for an entry containing "Received VPN Session Configuration Settings." That entry indicates *Split DNS:enabled* when enabled.

Checking Which Domains Use Split DNS

To use the client to check which domains are used for split DNS, follow these steps:

Step 1 Run **ipconfig/all** and record the domains listed next to DNS Suffix Search List.

Step 2 Establish a VPN connection and again check the domains listed next to DNS Suffix Search List.

Those extra domains added after establishing the tunnel are the domains used for split DNS.

Note This process assumes that the domains pushed from the ASA do not overlap with the ones already configured on the client host.

Configuring Split DNS

To configure this feature, establish an ASDM connection to the security appliance and perform both of the following procedures:

Configure Split-Include Tunneling

Step 1 Choose **Configuration > Remote AccessVPN > Network (Client) Access > Group Policies > Add or Edit > Advanced > Split Tunneling**.

Step 2 From the Policy drop-down menu, choose **Tunnel List Below** and select the relevant network list from the Network List drop-down menu.

In AnyConnect release 3.0.7 and later, if the split-include network is an exact match of a local subnet (such as 192.168.1.0/24), the corresponding traffic is tunneled. If the split-include network is a superset of a local subnet (such as 192.168.0.0/16), the corresponding traffic, except the local subnet traffic, is tunneled. To also tunnel the local subnet traffic, you must add a matching split-include network(specifying both 192.168.1.0/24 and 192.168.0.0/16 as split-include networks).

Configure DNS Servers

Step 1 Choose **Configuration > Remote AccessVPN > Network (Client) Access > Group Policies > Add or Edit > Servers**.

Step 2 Enter one or more private DNS servers in the DNS Servers field.

AnyConnect 3.0.4 and later supports up to 25 DNS server entries in the DNS Servers field, earlier releases only support up to 10 DNS server entries.

Configuring Certificate Enrollment using SCEP

About Certificate Enrollment using SCEP

The AnyConnect Secure Mobility Client can use the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate as part of client authentication. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology.

Certificate enrollment using SCEP is supported by AnyConnect IPsec and SSL VPN connections to the ASA in the following ways:

- SCEP Proxy: The ASA acts as a proxy for SCEP requests and responses between the client and the CA.
  - The CA must be accessible to the ASA, not the AnyConnect client, since the client does not access the CA directly.
  - Enrollment is always initiated automatically by the client. No user involvement is necessary.
  - SCEP Proxy is supported in AnyConnect 3.0 and higher.
- Legacy SCEP: The AnyConnect client communicates with the CA directly to enroll and obtain a certificate.

- The CA must be accessible to the AnyConnect client, not the ASA, through an established VPN tunnel or directly on the same network the client is on.
- Enrollment is initiated automatically by the client and may be initiated manually by the user if configured.
- Legacy SCEP is supported in AnyConnect 2.4 and higher.

SCEP Proxy Enrollment

The following steps describe the process in which a certificate is obtained and a certificate-based connection is made when AnyConnect and the ASA are configured for SCEP Proxy.

1. The user connects to the ASA headend using a connection profile configured for both certificate and AAA authentication. The ASA requests a certificate and AAA credentials for authentication from the client.
2. The user enters their AAA credentials but a valid certificate is not available. This situation triggers the client to send an automatic SCEP enrollment request after the tunnel has been established using the entered AAA credentials.
3. The ASA forwards the enrollment request to the CA and returns the CA's response to the client.
4. If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to an ASA tunnel group.

   If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact their administrator.

SCEP Proxy Notes

- The client automatically renews the certificate before it expires, without user intervention, if the **Certificate Expiration Threshold** field is set in the VPN profile.
- SCEP Proxy enollment requires the use of SSL for both SSL and IPsec tunnel certificate authentication.

Legacy SCEP Enrollment

The following steps describe the process in which a certificate is obtained and a certificate-based connection is made when AnyConnect is configured for Legacy SCEP.

1. The user initiates a connection to the ASA headend using a tunnel group configured for certificate authentication. The ASA requests a certificate for authentication from the client.
2. A valid certificate is not available on the client, the connection can not be established. This certificate failure indicates that SCEP enrollment needs to occur.
3. The user must then initiate a connection to the ASA headend using a tunnel group configured for AAA authentication only whose address matches the **Automatic SCEP Host** configured in the client profile. The ASA requests the AAA credentials from the client.
4. The client presents a dialog box for the user to enter their AAA credentials.

   If the client is configured for manual enrollment and the client knows it needs to initiate SCEP enrollment (see Step 2), a **Get Certificate** button will display on the credentials dialog box. If the client has direct access to the CA on their network, the user will be able to manually obtain a certificate by clicking this button at this time.

Note If access to the CA relies on the VPN tunnel being established, manual enrollment can not be done at this time since there is currently no VPN tunnel established (AAA credentials have not been entered).

5. The user enters their AAA credentials and establishes a VPN connection.
6. The client knows it needs to initiate SCEP enrollment (see Step 2), it initiates an enrollment request to the CA through the established VPN tunnel, and a response is received from the CA.
7. If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to an ASA tunnel group.

   If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact their administrator.
8. If the client is configured for manual enrollment and the **Certificate Expiration Threshold** value is met, a **Get Certificate** button will display on a presented tunnel group selection dialog box. The user will be able to manually renew their certificate by clicking this button.

Legacy SCEP Notes

- If you use manual Legacy SCEP enrollment, we recommend you enable CA Password in the client profile. The CA Password is the challenge password or token that is sent to the certificate authority to identify the user.
- If the certificate expires and the client no longer has a valid certificate, the client repeats the Legacy SCEP enrollment process.

SCEP Guidelines and Limitations

- ASA Load balancing is supported with SCEP enrollment.
- Clientless (browser-based) VPN access to the ASA does not support SCEP proxy, but WebLaunch (clientless-initiated AnyConnect) does.
- The ASA does not indicate why an enrollment failed, although it does log the requests received from the client. Connection problems must be debugged on the CA or the client.
- All SCEP-compliant CAs, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA are supported.
- The CA must be in auto-grant mode; polling for certificates is not supported.
- Some CA's can be configured to email users an enrollment password, this provides an additional layer of security. The password can also be configured in the AnyConnect client profile, which becomes part of SCEP request that the CA verifies before granting the certificate.

Windows Certificate Warning

When Windows clients first attempt to retrieve a certificate from a certificate authority they may see a warning. When prompted, users must click **Yes**. This allows them to import the root certificate. It does not affect their ability to connect with the client certificate.

Identifying Enrollment Connections to Apply Policies

On the ASA, the aaa.cisco.sceprequired attribute can be used to catch the enrollment connections and apply the appropriate policies in the selected DAP record.

Certificate-Only Authentication and Certificate Mapping 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 tunnel group when the certificate from this process is presented to the ASA.

Configuring SCEP Proxy Certificate Enrollment

Configuring a VPN Client Profile for SCEP Proxy Enrollment

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

Step 2 In the ASDM, Click **Add** (or **Edit**) to create (or edit) an AnyConnect Profile. On the stand-alone editor, open an existing profile or continue to create a new one.

Step 3 Click **Certificate Enrollment** in the AnyConnect Client Profile tree on the left.

Step 4 In the **Certificate Enrollment** pane, check **Certificate Enrollment.**

Step 5 Configure the **Certificate Contents** to be requested in the enrollment certificate. For definitions of the certificate fields, see AnyConnect Profile Editor, Certificate Enrollment, page 3-77.

Note
- If you use %machineid%, then Hostscan/Posture must be loaded for the desktop client.
- For mobile clients, at least one certificate field must be specified.

Configuring the ASA to support SCEP Proxy Enrollment

For SCEP Proxy, a single ASA connection profile supports certificate enrollment and the certificate authorized VPN connection.

Prerequisite

Configure a client profile for SCEP Proxy, for example, ac_vpn_scep_proxy. See Configuring a VPN Client Profile for SCEP Proxy Enrollment, page 3-39.

Step 1 Create a group policy, for example, cert_group. Set the following fields:

- On General, enter the URL to the CA in **SCEP Forwarding URL**.
- On the Advanced > AnyConnect Client pane, uncheck **Inherit** for **Client Profiles to Download** and specify the client profile configured for SCEP Proxy. For example, specify the ac_vpn_scep_proxy client profile.

Step 2 Create a connection profile for certificate enrollment and certificate authorized connection, for example, cert_tunnel.

- Authentication: Both (AAA and Certificate)
- Default Group Policy: cert_group
- On Advanced > General, check **Enable SCEP Enrollment for this Connction Profile**.
- On Advanced > GroupAlias/Group URL, create a Group URL containing the group (cert_group) for this connection profile.

Configuring Legacy SCEP Certificate Enrollment

Configuring a VPN Client Profile for Legacy SCEP Enrollment

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

Step 2 In the ASDM, Click **Add** (or **Edit**) to create (or edit) an AnyConnect Profile. On the stand-alone editor, open an existing profile or continue to create a new one.

Step 3 Click **Certificate Enrollment** in the AnyConnect Client Profile tree on the left.

Step 4 In the **Certificate Enrollment** pane, check **Certificate Enrollment.**

Step 5 Specify an **Automatic SCEP Host** to direct the client to retrieve the certificate.

Enter the FQDN or IP address, and the alias of the connection profile (tunnel group) that is configured for SCEP certificate retrieval. For example, if **`asa.cisco.com`** is the host name of the ASA and **`scep_eng`** is the alias of the connection profile, enter **`asa.cisco.com/scep-eng`**.

When the user initiates the connection, the address chosen or specified must match this value exactly for Legacy SCEP enrollment to succeed. For example, if this field is set to an FQDN, but the user specifies an IP address, SCEP enrollment will fail.

Step 6 Configure the Certificate Authority attributes:

Note Your CA server administrator can provide the CA URL and thumbprint. Retrieve the thumbprint directly from the server, not from a “fingerprint” or “thumbprint” attribute field in an issued certificate.

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

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

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

Step 7 Configure the **Certificate Contents** to be requested in the enrollment certificate. For definitions of the certificate fields, see AnyConnect Profile Editor, Certificate Enrollment, page 3-77.

Note If you use %machineid%, then Hostscan/Posture must be loaded on the client.

Step 8 (Optional) Check **Display Get Certificate Button** to permit users to manually request provisioning or renewal of authentication certificates. The button is visible to users if the certificate authentication fails.

Step 9 (Optional) Enable SCEP for a specific host in the server list. Doing this overrides the SCEP settings in the Certificate Enrollment pane described above.

a. Click **Server List** in the AnyConnect Client Profile tree on the left to go to the Server List pane.

b. **Add** or **Edit** a server list entry.

c. Specify the Automatic SCEP Host and Certificate Authority attributes as described in Steps 5 and 6 above.

Configuring the ASA to support Legacy SCEP Enrollment

For Legacy SCEP on the ASA, a connection profile and group policy must be created for certificate enrollment, and a second connection profile and group policy must be created for the certificate authorized VPN connection.

Prerequisite

Configure a client profile for Legacy SCEP, for example, ac_vpn__legacy_scep. See Configuring a VPN Client Profile for Legacy SCEP Enrollment, page 3-40.

Step 1 Create a group policy for enrollment, for example, cert_enroll_group. Set the following fields:

- On the Advanced > AnyConnect Client pane, uncheck **Inherit** for **Client Profiles to Download** and specify the client profile configured for Legacy SCEP. For example, specify the ac_vpn_legacy_scep client profile.

Step 2 Create a second group policy for authorization, for example, cert_auth_group.

Step 3 Create a connection profile for enrollment, for example, cert_enroll_tunnel. Set the following fields:

- On the Basic pane, set the Authentication Method to AAA.
- On the Basic pane, set the Default Group Policy to cert_enroll_group.
- On Advanced > GroupAlias/Group URL, create a Group URL containing the enrollment group (cert_enroll_group) for this connection profile.
- Do not enable the connection profile on the ASA. It is not necessary to expose the group to users in order for them to have access to it.

Step 4 Create a connection profile for authorization, for example, cert_auth_tunnel. Set the following fields.

- On the Basic pane, set the Authentication Method to Certificate.
- On the Basic pane, set the Default Group Policy to cert_auth_group.
- Do not enable this connection profile on the ASA. It is not necessary to expose the group to users in order for them to access it.

Step 5 (Optional) On the General pane of each group policy, set **Connection Profile (Tunnel Group) Lock** to the corresponding SCEP connection profile, which restricts traffic to the SCEP-configured connection profile.

Configuring Certificate Expiration Notice

Configure AnyConnect to warn users that their authentication certificate is about to expire. The **Certificate Expiration Threshold** setting specifies the number of days before the certificate's expiration date that AnyConnect warns users that their certificate is expiring. AnyConnect warns the user upon each connect until the certificate has actually expired or a new certificate has been acquired.

Note The Certificate Expiration Threshold feature cannot be used with RADIUS.

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

Step 2 In the ASDM, Click **Add** (or **Edit**) to create (or edit) an AnyConnect Profile. On the stand-alone editor, open an existing profile or continue to create a new one.

Step 3 Click **Certificate Enrollment** in the AnyConnect Client Profile tree on the left.

Step 4 In the **Certificate Enrollment** pane, check **Certificate Enrollment.**

Step 5 Specify a **Certificate Expiration Threshold**.

This is 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 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 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 3-43
- Creating a PEM Certificate Store for Mac and Linux, page 3-44

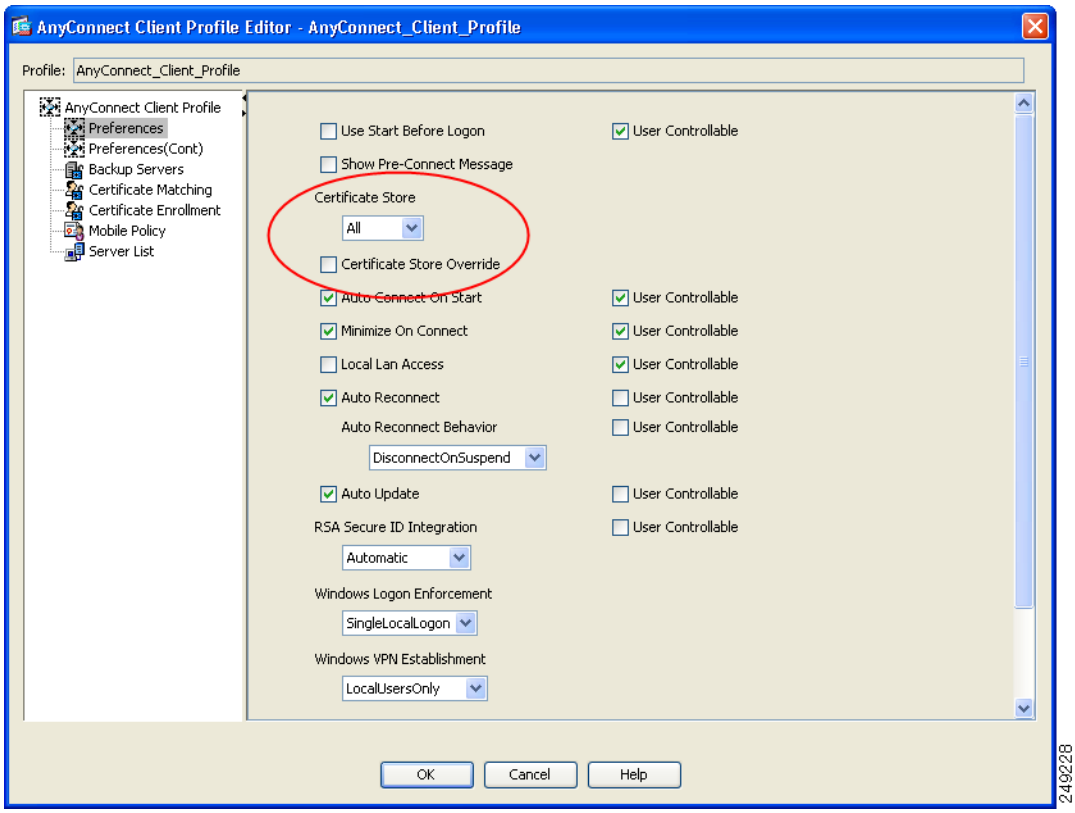
Controlling the Certificate Store on Windows

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 3-15 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.

Figure 3-15 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, 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 3-5. Place the appropriate certificates in these folders:

Table 3-5 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 3-5 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 3-48 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
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
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

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

Identifier	Description
CN	SubjectCommonName
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.

Default Certificate Matching

The client certificate must be a valid, non-expired certificate, to be matched for use by AnyConnect.

If no certificate matching criteria is specified in the *Certificate Matching* pane, AnyConnect implicitly applies the following certificate matching rules:

- Key Usage: DIGITAL_SIGNATURE
- Extended Key Usage: Client Auth (1.3.6.1.5.5.7.3.2)

If any other Key Usage or Extended Key Usage criteria is specified in the client certificate, then the above specifications must also be specified in the client certificate for it to be matched.

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 3-75

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 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 Certificate 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.

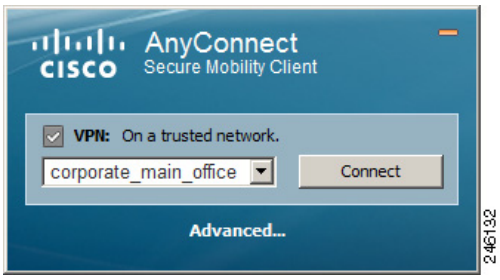
Figure 3-16 shows the Automatic Certificate Selection check box the user sees in the Preferences window:

Figure 3-16 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. The user can select a server from this list.

Figure 3-17 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.

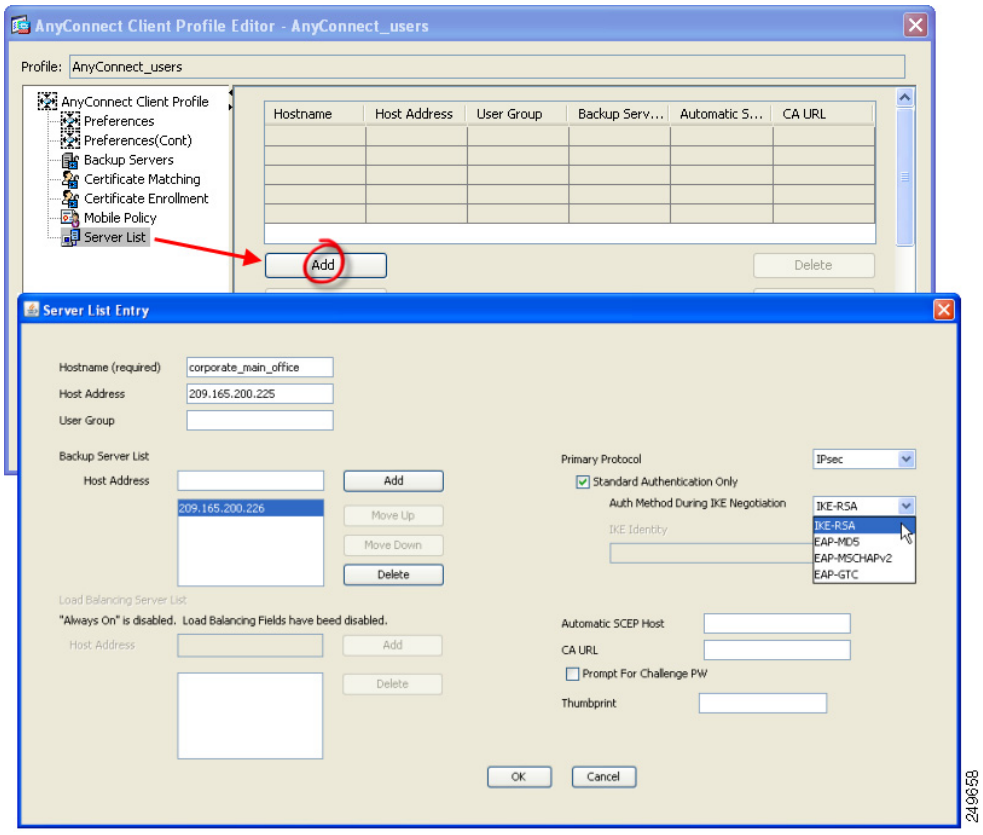
To configure a server list, follow this procedure:

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 3-18 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 (For AnyConnect release 3.0.1047 or later.) To setup server list settings for mobile devices, check the **Additional mobile-only settings** checkbox and click **Edit**. See Configuring Server List Entries for Mobile Devices for more information.

Step 8 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 9 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 10 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.

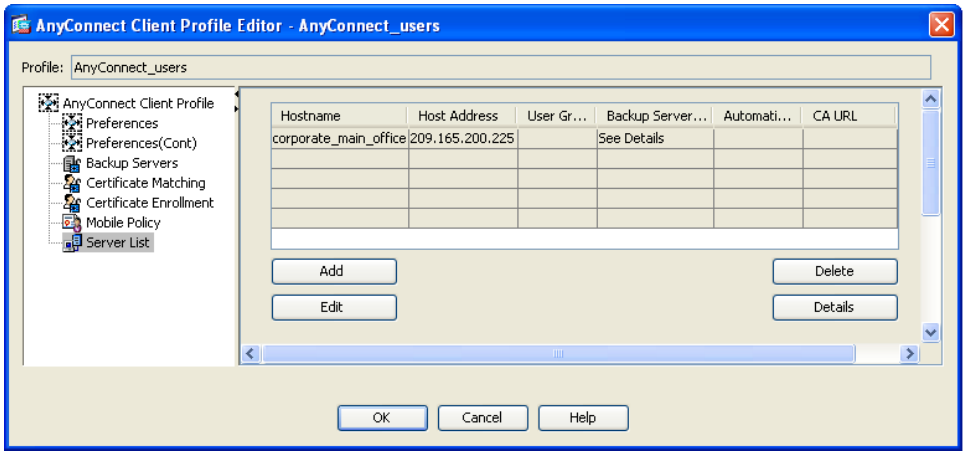
Step 11 Specify the URL of the SCEP CA server (optional). Enter an FQDN or IP Address. For example, http://ca01.cisco.com.

Step 12 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 13 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 14 Click **OK**. The new server list entry you configured appears in the server list table.

Figure 3-19 A New Server List Entry



Configuring Connections for Mobile Devices

Prerequisites

- Perform steps 1-6 of Configuring a Server List, page 3-50.
- You must be using Profile Editor version 3.0.1047 or later.
- Supported on Apple mobile devices, running Apple iOS version 4.1 or later.

Guidelines

AnyConnect VPN client profiles delivered to mobile devices from the ASA, cannot be re-configured or deleted from the mobile device. When users create their own client profiles on their devices for new VPN connections, they will be able to configure, edit, and delete those profiles.

Detailed Steps

Step 1 In the Server List Entry dialog box, check **Additional mobile-only settings** and click **Edit**.

Step 2 In the **Apple iOS / Android Settings** area, you can configure these attributes for devices running Apple iOS or Android operating systems:

a. Choose the Certificate Authentication type:

- **Automatic**—AnyConnect automatically chooses the client certificate with which to authenticate. In this case, AnyConnect views all the installed certificates, disregards those certificates that are out of date, applies the certificate matching criteria defined in VPN client profile, and then authenticates using the certificate that matches the criteria. This happens every time the user attempts to establish a VPN connection.
- **Manual**—AnyConnect searches for the certificate with which to authenticate just as it does with automatic authentication. In the manual certificate authentication type, however, once AnyConnect finds a certificate that matches the certificate matching criteria defined in the VPN client profile, it assigns that certificate to the connection and it will not search for new certificates when users attempt to establish new VPN connections.
- **Disabled**—Client Certificate will never be used for authentication.

b. If you check the **Make this Server List Entry active when profile is imported** check box, you are defining this server list entry as the default connection once the VPN profile has been downloaded to the device. Only one server list entry can have this designation. The default value is unchecked.

Step 3 In the Apple iOS Only Settings area, you can configure these attributes for devices running Apple iOS operating systems only:

a. Configure the **Reconnect when roaming between 3G/Wifi networks** checkbox. The box is checked by default so AnyConnect will attempt to maintain the VPN connection when switching between 3G and Wifi networks. If you uncheck the box, AnyConnect will not attempt to maintain the VPN connection which switching between 3G and Wifi networks.

b. Configure the **Connect on Demand** checkbox.

This area allows you to configure the Connect on Demand functionality provided by Apple iOS. You can create lists of rules that will be checked whenever other applications initiate network connections that are resolved using the Domain Name System (DNS).

Connect on Demand can only be checked if the Certificate Authentication field is set to **Manual** or **Automatic**. If the Certificate Authentication field is set to **Disabled**, this checkbox is grayed out. The Connect on Demand rules, defined by the **Match Domain or Host** and the **On Demand Action** fields, can still be configured and saved when the checkbox is grayed out.

c. In the **Match Domain or Host** field, enter the host names (host.example.com), domain names (.example.com), or partial domains (.internal.example.com) for which you want to create a Connect on Demand rule. Do not enter IP addresses (10.125.84.1) in this field.

d. In the **On Demand Action** field, specify one of these actions when a user attempts to connect to the domain or host defined in the previous step:

- Always connect—iOS will always attempt to initiate a VPN connection when rules in this list are matched.
- Connect if needed—iOS will attempt to initiate a VPN connection when rules in this list are matched only if the system could not resolve the address using DNS.
- Never connect—iOS will never attempt to initiate a VPN connection when rules in this list are matched. Any rules in this list will take precedence over Always connect or Connect if needed rules.

  When Connect On Demand is enabled, the application automatically adds the server address to this list. This prevents a VPN connection from being automatically established if you try accessing the server's clientless portal with a web browser. This rule can be removed if you do not want this behavior.

e. Once you have created a rule using the **Match Domain or Host** field and the **On Demand Action** field, click **Add**.

The rule is displayed in the rules list below.

Step 4 Click **OK**.

Step 5 Return to step 8 of Configuring a Server List, page 3-50.

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 Connect On Start-up

Connect on Start-up 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, Connect on Start-up 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 Connect on Start-up element reflects that evolution. If your enterprise's deployment uses the Connect on Start-up 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 the "Trusted Network Detection" section on page 3-17.

By default, Connect on Start-up 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 **Connect On Start-up**.

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.

For best performance, users who travel to distant locations connect to a secure gateway nearest their location. 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%.

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.

OGS maintains a cache of its RTT results in order to minimize the number of measurements it must perform in the future. Upon starting AnyConnect with OGS enabled, OGS determines where the user is located by obtaining network information (such as DNS suffix and DNS server IP).The RTT results, along with this location, are stored in the OGS cache. During the next 14 days, the location is determined with this same method whenever AC restarts, and the cache deciphers whether it already has RTT results. A headend is selected based on the cache without needing to re-RRT the headends. At the end of 14 days, the results for this location are removed from the cache, and restarting AC results in a new set of RTTs.

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 3-74 for additional information on backup servers.

Optimal Gateway Selection Requirements

AnyConnect 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.

Note You can configure this threshold value using the Profile Editor. By optimizing this value in combination with the next configurable parameter (Performance Improvement Threshold), you can find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials.

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 *VPN: Ready to connect* panel next to the Connect button. 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.

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 Click **Advanced**.

Step 3 Open the Preferences tab and uncheck **Enable Optimal Gateway Selection**.

Step 4 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.

OGS and Sleep Mode

AnyConnect must have an established connection at the time the endpoint is put into sleep or hibernation mode. You must enable the AutoReconnect (ReconnectAfterResume) settings on ASDM's profile editor (Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile). If you make it user controllable here, you can configure it on the AnyConnect Secure Mobility Client Preferences tab before the device is put to sleep. When both of these are set, the device comes out of sleep, and AC automatically runs OGS, using the selected headend for its reconnection attempt.

OGS and Proxy Detection

If automatic proxy detection is configured, you cannot perform OGS. It also does not operate with proxy auto-configuration (PAC) files configured.

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 a 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.

AnyConnect supports script launching during WebLaunch and standalone launches.

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, 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

Be aware of the following requirements and limitations for scripts:

Number of Scripts Supported

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

File Formats

AnyConnect identifies the OnConnect and onDisconnect script by the filename. It looks for a file whose name begins with OnConnect or OnDisconnect regardless of file extension. The first script encountered with the matching prefix is executed. It recognizes an interpreted script (such as VBS, Perl, or Bash) or an executable.

Script Language

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.

Restrictions on Scripts by the Windows Security Environment

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.

Enabling the Script

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

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

Running Scripts on 64-bit Windows

The AnyConnect client is a 32-bit application. When running on a 64-bit Windows version, such as Windows 7 x64 and Windows Vista SP2 x64, when it executes a batch script, it uses the 32-bit version of cmd.exe.

Because the 32-bit cmd.exe lacks some commands that the 64-bit cmd.exe supports, some scripts could stop executing when attempting to run an unsupported command, or run partially and stop. For example, the **msg** command, supported by the 64-bit cmd.exe, may not be understood by the 32-bit version of Windows 7 (found in %WINDIR%\SysWOW64).

Therefore, when you create a script, use commands supported by the 32-bit cmd.exe.

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**.

  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.

- 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 Secure Mobility Client\Script
Microsoft Windows XP	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Script
Linux (On Linux, assign execute permissions to the file for User, Group and Other.)	/opt/cisco/anyconnect/script
Mac OS X	/opt/cisco/anyconnect/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 **IgnoreProxy**. Ignore Proxy causes the client to ignore all proxy settings. No action is taken against proxies that reach the ASA.

Note AnyConnect does not support Override as a proxy setting.

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.

Note In a Mac environment, the proxy information that is pushed down from the ASA (upon a VPN connection) is not viewed in the browser until you open up a terminal and issue a "scutil --proxy".

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 Connections tab lockdown.
- The ASA configuration specifies a private-side proxy.
- A Windows group policy previously locked down the Connections tab (overriding the **no lockdown** ASA group policy setting).

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.

Using a Windows RDP Session to Launch a VPN Session

With the Windows Remote Desktop Protocol (RDP), you can allow users to log on to a computer running the Cisco AnyConnect Secure Mobility client 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 and has an established VPN connection, either locally or remotely, the connection is not allowed. If a second user logs on, either locally or remotely, 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 to 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 Start 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, page 3-67
- Instructing Users to Override PPP Exclusion, page 3-68

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 Secure Mobility Client\preferences.xml. For example,
  - Windows Vista—C:\Users*username*\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml
  - Windows XP—C:\Documents and Settings**username**\Local Settings\Application Data\Cisco\Cisco AnyConnect Secure Mobility 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 (Part 1)

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. For information about setting or changing the pre-connect message, see Changing the Default AnyConnect English Messages, page 11-19.

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, page 3-7

Certificate Store and Certificate Override—Configuring a Certificate Store, page 3-42

Auto Reconnect—Configuring Auto Reconnect, page 3-55

Windows Logon Enforcement—Allowing a Windows RDP Session to Launch a VPN Session

AnyConnect Profile Editor, Preferences (Part 2)

Disable Certificate 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—Causes the client to use both the client configured proxy settings and the Internet Explorer configured proxy settings. The native OS proxy settings are used (such as those configured into MSIE in Windows), and proxy settings configured in the global user preferences are pre-pended to these native settings.
- IgnoreProxy—Ignores all Microsoft Internet Explorer or Mac Safari proxy settings on the user computer. No action is taken against proxies that reach the ASA.
- 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 the "Disconnect Button for Always-on VPN" section on 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 Requirements" 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 3-68.

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 Requirements, page 3-56
Proxy Settings	Configuring Local Proxy Connections, page 3-56
Optimal Gateway Selection	Optimal Gateway Selection Requirements, page 3-57
Automatic VPN Policy and Trusted Network Detection	Configuring Trusted Network Detection, page 3-17
Alwayson VPN	Configuring Always-on VPN, page 3-24
Connect Failure Policy	Configuring a Connect Failure Policy, page 3-28
Allow Captive Portal Remediation	Captive Portal Hotspot Remediation, page 3-30
PPP Exclusion	AnyConnect over L2TP or PPTP, page 3-67
Authentication Timeout Values	Configuring Authentication Timeout, page 3-63

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 Fully-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 3-54

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—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—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 3-45.

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 3-36

AnyConnect Profile Editor, Mobile Policy

Set parameters for AnyConnect running on Windows Mobile in this pane:

Note AnyConnect version 3.0 and later does not support Windows Mobile devices. See *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5* for information related to Windows Mobile devices.

- **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.

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 3-50.

Configuring AnyConnect Client Connection Timeouts

Use these procedures to terminate or maintain an idle AnyConnect VPN connection.

You can limit how long the ASA keeps an AnyConnect VPN connection available to the user even with no activity. If a VPN session goes idle, you can terminate the connection or re-negotiate the connection.

Terminating an AnyConnect Connection

Terminating an AnyConnect connection requires the user to re-authenticate their endpoint to the secure gateway and create a new VPN connection.

The following configuration parameters terminate the VPN session based on a simple timeout:

- Default Idle Timeout - Terminates any user's session when the session is inactive for the specified time. The default value is 30 minutes.

  You can only modify default-idle-timeout using the CLI, in webvpn configuration mode. The default is 1800 second. For instructions to configure default-idle-timeout see Configuring Session Timeouts in *Cisco ASA 5500 Series Configuration Guide using the CLI*.

- VPN Idle Timeout - Terminates any user's session when the session is inactive for the specified time. For SSL-VPN only, if vpn-idle-timeout is not configured, then default-idle-timeout is used.

  For instructions to configure VPN idle timeout with the ASDM, see Adding or Editing a Remote Access Internal Group Policy, General Attributes in *Cisco ASA 5500 Series Configuration Guide using ASDM*.

  For instructions to configure VPN idle timeout with the CLI, see Step 4 of Configuring VPN-Specific Attributes in *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Renegotiating and Maintaining the AnyConnect Connection

The following configuration parameters terminate or renegotiate the tunnel, but do not terminate the session:

- Keepalive - The ASA sends keepalive messages at regular intervals. These messages are ignored by the ASA, but are useful in maintaining connections with devices between the client and the ASA.

  For instructions to configure Keepalive with the ASDM, see Configuring AnyConnect VPN Client Connections in *Cisco ASA 5500 Series Configuration Guide using ASDM*.

  For instructions to configure Keepalive with the CLI, see Step 5 of Group-Policy Attributes for AnyConnect Secure Mobility Client Connections in *Cisco ASA 5500 Series Configuration Guide using the CLI*.

- Dead Peer Detection - The ASA and/or AnyConnect client send "R-U-There" messages. These messages are sent less frequently than IPsec's keepalive messages.

  - If the client does not respond to the ASA's DPD messages, the ASA tries three more times before putting the session into "Waiting to Resume" mode. This mode allows the user to roam networks, or enter sleep mode and later recover the connection. If the user does not reconnect before the default idle timeout occurs, the ASA will terminate the tunnel. The recommended gateway DPD interval is 300 seconds.
  - If the ASA does not respond to the client's DPD messages, the client tries three more times before terminating the tunnel. The recommended client DPD interval is 30 seconds.

  You can enable both the ASA (gateway) and the client to send DPD messages, and configure a timeout interval.

  For instructions to configure DPD with the ASDM, see Dead Peer Detection in *Cisco ASA 5500 Series Configuration Guide using ASDM*.

  For instructions to configure DPD with the CLI, see Step 4 of Configuring Group-Policy Attributes for AnyConnect Secure Mobility Client Connections in *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Best Practices

- Set Client DPD to 30 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).
- Set Server DPD to 300 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).
- Set Rekey, for both SSL and IPsec to 1 hour (Group Policy > Advanced > AnyConnect Client > Key Regeneration).