



## CHAPTER 3

# Configuring AnyConnect Client Features

---

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

### AnyConnect Client Profile

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

You can configure the security appliance to deploy profiles globally for all AnyConnect client users, or based on the group policy of the user. Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and additional settings as needed. In some cases, you might want to provide more than one profile for a given user. For example, someone who works from multiple locations might need more than one profile. Be aware that some of the profile settings, such as Start Before Login, control the connection experience at a global level. Other settings, such as those unique to a particular host, depend on the host selected.

### AnyConnect Local Policy

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

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

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

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

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

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

## Configuring and Deploying the AnyConnect Client Profile

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

You can create and save XML profiles using a text editor. The client installation contains one profile template (AnyConnectProfile.tpl) you can copy, rename, and save as an XML file, then edit and use as a basis to create other profile files.

The profile file is downloaded from the security appliance to the remote user's PC, in the directory: C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile. The location for Windows Vista is slightly different: C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile. You must first import the profile(s) into the security appliance in preparation for downloading to the remote PC. You can import a profile using either ASDM or the command-line interface. The AnyConnectProfile.tpl file automatically downloaded with the AnyConnect client is an example AnyConnect profile.



### Note

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

This section covers the following topics:

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

## Default Client Profile

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

The following example shows a sample AnyConnect Profile file. The bold type identifies the values you can modify to customize the profile. In this example, blank lines separate the major groupings for legibility. Do not include these blank lines in your profile.



### Caution

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

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

<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">

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

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

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

```

<ServerList>
  <HostEntry>
    <HostName>CVC-ASA-01</HostName>
    <HostAddress>CVC-ASA-01.example.com</HostAddress>
    <UserGroup>StandardUser</UserGroup>
    <BackupServerList>
      <HostAddress>cvc-asa-02.example.com</HostAddress>
      <HostAddress>cvc-asa-03.example.com</HostAddress>
    </BackupServerList>
  </HostEntry>
</ServerList>

</AnyConnectProfile>

```

## Editing the Client Profile

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

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

```

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

  The file needs to be renamed to CiscoAnyConnectProfile.xml.

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

```

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

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

**Note**

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

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

## Validating the XML in the Profile

It is important to validate the XML in the AnyConnect client profile you create. Use an online validation tool or the profile import feature in ASDM. For validation, you can use the AnyConnectProfile.xsd found in the same directory as the profile template. This .xsd file is the XML schema definition for the client profile, and is intended to be maintained by a Secure Gateway administrator and then distributed with the client software.

**Note**

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

The XML file based on this schema can be distributed to clients at any time, either as a bundled file with the software distribution or as part of the automatic download mechanism. The automatic download mechanism is available only with certain Cisco Secure Gateway products.

In Microsoft Windows with MSXML 6.0, the AnyConnect client validates the XML profile against the profile XSD schema and logs any validation failures. MSXML 6.0 ships with Windows 7 and Vista. It is available for download from Microsoft for Windows XP from the following link:

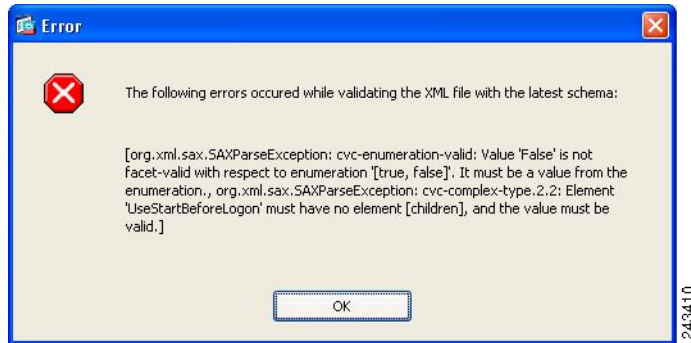
<http://www.microsoft.com/downloads/details.aspx?FamilyID=d21c292c-368b-4ce1-9dab-3e9827b70604&displaylang=en>

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

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

results in the following error message:

Figure 3-1 XML Validation Error



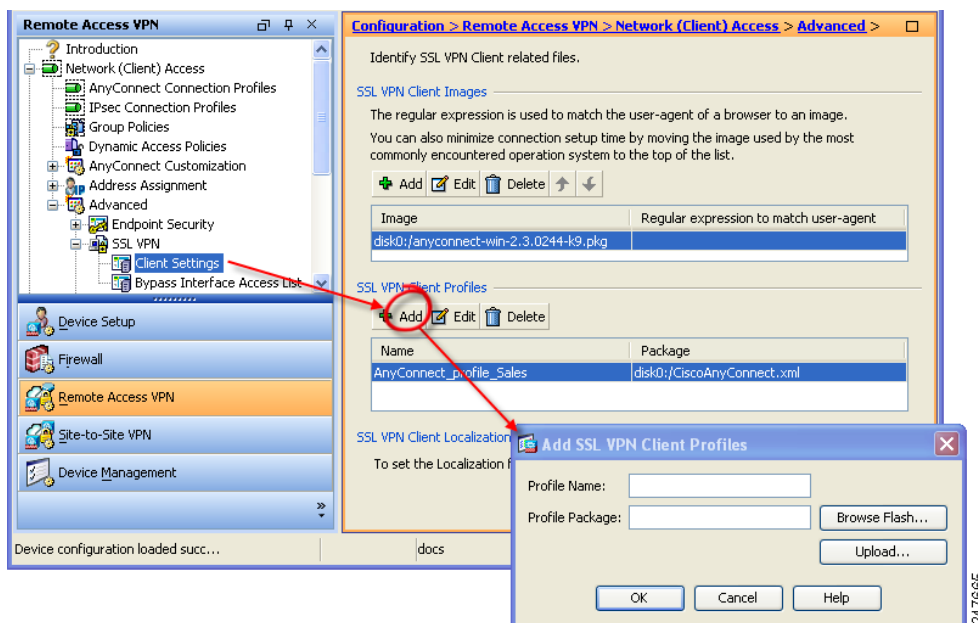
In this example, the value **False** (initial letter capitalized) should have been **false** (all lowercase), and the error indicates this.

## Deploying the Client Profile to AnyConnect Clients

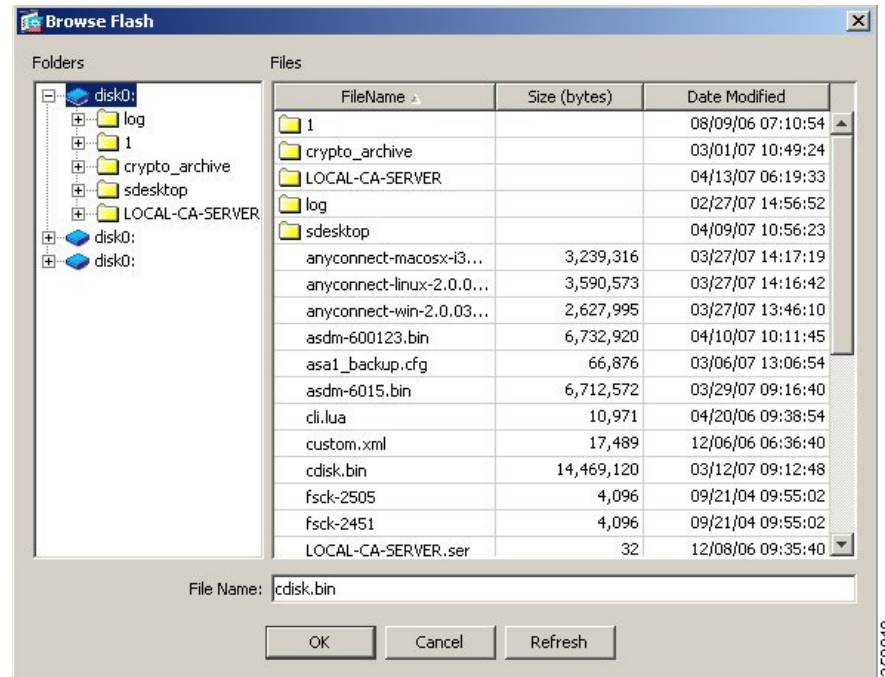
Follow these steps to configure the security appliance to deploy a profile with the AnyConnect client:

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

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



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

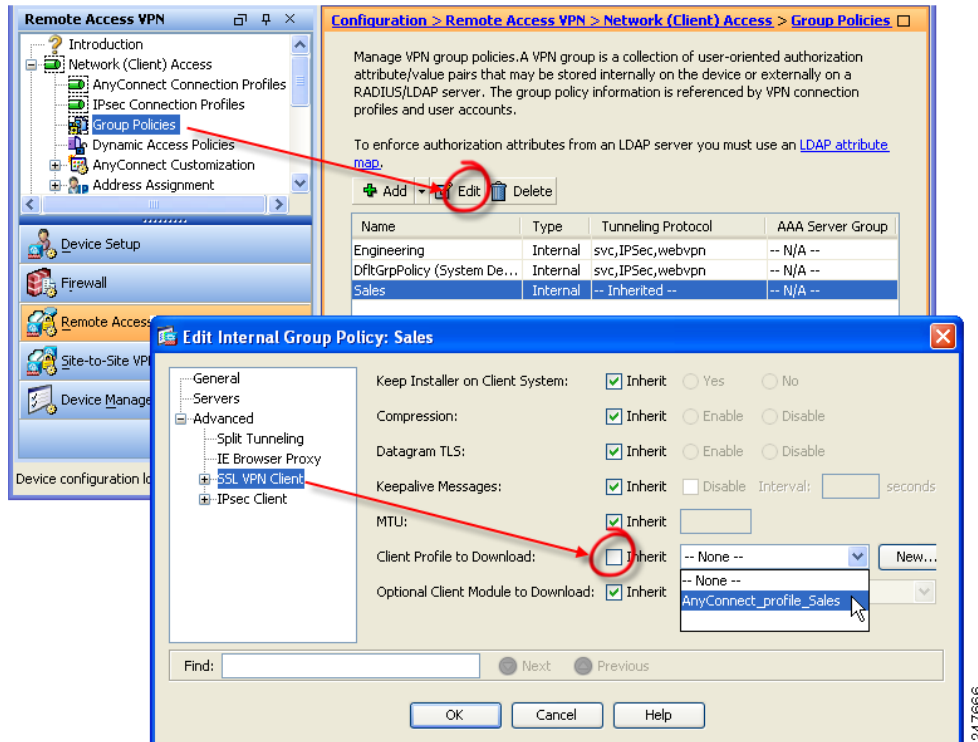
**Figure 3-3 Browse Flash Dialog Box**

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

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

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

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



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

## Configuring the AnyConnect Local Policy

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

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

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

This section covers the following topics:

- [AnyConnect Local Policy File Example, page 3-9](#)



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

## AnyConnect Local Policy File Example

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

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

## Changing Parameters for Windows Clients using our MST File

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

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

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

- LOCAL\_POLICY\_BYPASS\_DOWNLOADER
- LOCAL\_POLICY\_FIPS\_MODE
- LOCAL\_POLICY\_RESTRICT\_PREFERENCE\_CACHING
- LOCAL\_POLICY\_RESTRICT\_TUNNEL\_PROTOCOLS
- LOCAL\_POLICY\_RESTRICT\_WEB\_LAUNCH
- LOCAL\_POLICY\_STRICT\_CERTIFICATE\_TRUST

## Changing Parameters Manually in the AnyConnect Local Policy File

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

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

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

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

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

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

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

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

## Configuring Start Before Logon

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



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

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

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

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

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

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

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

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

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

[http://www.windowsnetworking.com/articles\\_tutorials/wxpplogs.html](http://www.windowsnetworking.com/articles_tutorials/wxpplogs.html)

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

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

AnyConnect is not compatible with fast user switching.

This section covers the following topics:

- [Installing Start Before Logon Components \(Windows Only\), page 3-11](#)
- [Configuring Start Before Logon \(PLAP\) on Windows 7 and Vista Systems, page 3-15](#)

## Installing Start Before Logon Components (Windows Only)

The Start Before Logon components must be installed *after* the core client has been installed. Additionally, the AnyConnect 2.2 Start Before Logon components require that version 2.2, or later, of the core AnyConnect client software be installed. If you are pre-deploying the AnyConnect client and the Start Before Logon components using the MSI files (for example, you are at a big company that has

its own software deployment—Altiris or Active Directory or SMS.) then you must get the order right. The order of the installation is handled automatically when the administrator loads AnyConnect if it is web deployed and/or web updated.

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

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

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



### Note

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

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

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

The sections that immediately follow describe the settings and procedures for both VPNGINA and PLAP SBL. For a complete description of enabling and using the SBL feature (PLAP) on a Windows Vista platform, see [Configuring Start Before Logon \(PLAP\) on Windows 7 and Vista Systems, page 3-15](#).

## Profile Parameters for Enabling SBL

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

You enable SBL by setting the <UseStartBefore Logon> value in the AnyConnect profile to true:

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

To disable SBL, set the same value to false.

The following table shows the settings.

**Table 3-2**      *UseStartBeforeLogon Client Initialization Tag*

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

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

2. Insert the parameter value between the beginning and closing tags; for example, `<UseStartBeforeLogon>true</UseStartBeforeLogon>`.
3. The user controllable attribute is defined inside the preference tags; for example, `<UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>`. Its possible values are "true" or "false", and these determine which preferences are overridden by the preferences\*.xml files. This is an optional attribute, and if not defined, the default value is used. Preferences made `UserControllable="true"` in the profile are visible in the Preferences dialog.

## Making SBL User-Controllable

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

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

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

## Enabling SBL on the Security Appliance

To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of core modules that it needs for each feature that it supports. To enable SBL, you must specify the SBL module name in group policy on the security appliance.

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

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



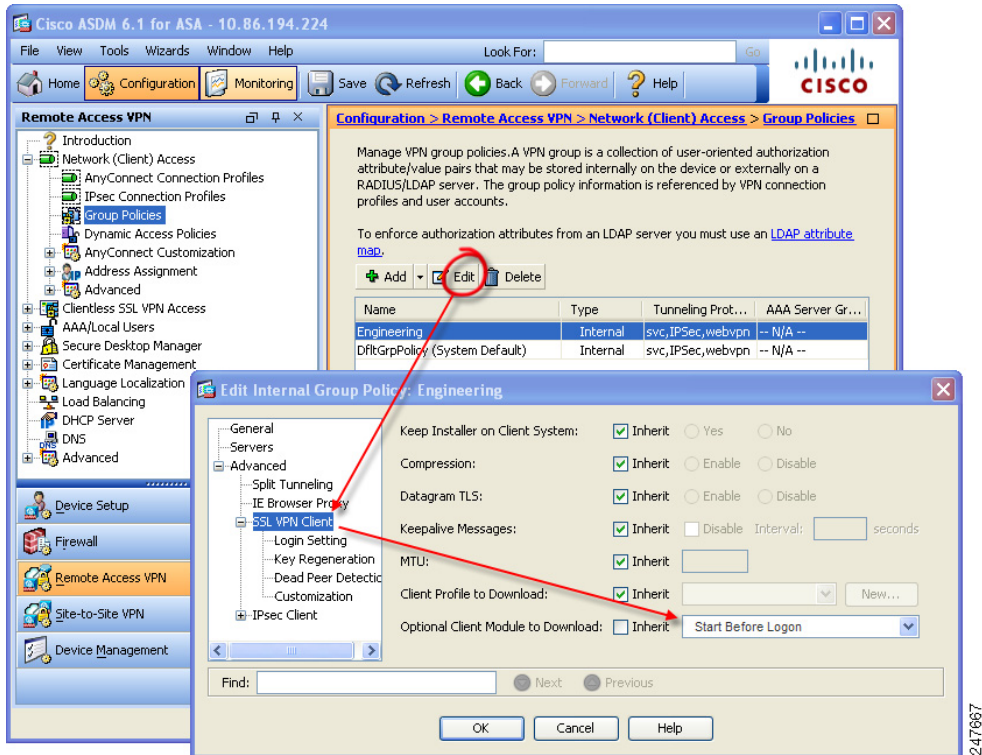
---

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

---

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

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

**Figure 3-5** Specifying the SBL Module to Download

## Using the Manifest File

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

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

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

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

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

When a remote user connects to the security appliance using WebLaunch or an previously-installed client, the downloader is downloaded first and run, and it uses the manifest file to ascertain whether there is a existing client on the remote user's computer that needs to be upgraded, or whether a fresh installation is required. The manifest file also contains information about whether there are any optional modules that must be downloaded and installed—in this case, the VPNGINA. The installation of

VPNGINA is activated if the group-policy of the user specifies SBL as an optional module to download. If it is, the AnyConnect client and VPNGINA are installed, and the user sees the AnyConnect Client at the next reboot, prior to Windows Domain logon.

When the client installs, a sample profile is provided on the client computer at this location:

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

## Troubleshooting SBL

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

- 
- Step 1** Ensure that the profile is being pushed.
  - Step 2** Delete prior profiles (search for them on the hard drive to find the location, \*.xml).
  - Step 3** Using Windows Add/Remove Programs, uninstall the Cisco AnyConnect Client Start Before Login Components. Reboot the computer and retest.
  - Step 4** Clear the user's AnyConnect log in the Event Viewer and retest.
  - Step 5** Web browse back to the security appliance to install the client again.
  - Step 6** Reboot once. On the next reboot, you should be prompted with the Start Before Logon prompt.
  - Step 7** Send the AnyConnect event log to Cisco in .evt format
  - Step 8** If you see the following error, delete the user profile:
 

```
Description: Unable to parse the profile C:\Documents and Settings\All
Users\Application Data\Cisco\AnyConnect VPN Client\Profile\VABaseProfile.xml.
Host data not available.
```
  - Step 9** Go back to the .tmpl file, save a copy as an .xml file, and use that XML file as the default profile.
- 

## Configuring Start Before Logon (PLAP) on Windows 7 and Vista Systems

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

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



### Note

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

## Installing PLAP

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

**Note**

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

Once installed, PLAP is not active until you modify the user profile <profile.xml> file to activate start before logon. See [Profile Parameters for Enabling SBL, page 3-12](#). After activation, the user invokes the Network Connect component by clicking Switch User, then the Network Connect icon in the lower, right-hand part of the screen.

**Note**

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

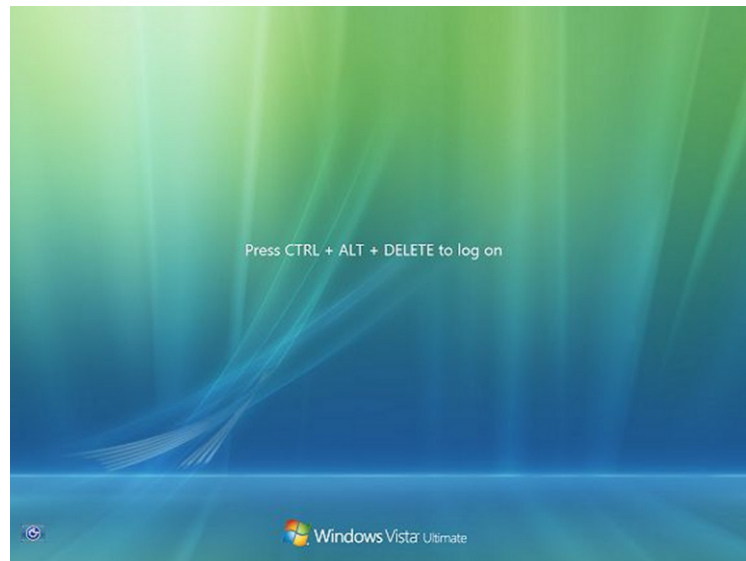


## Logging on to a Windows Vista or Windows 7 PC using PLAP

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

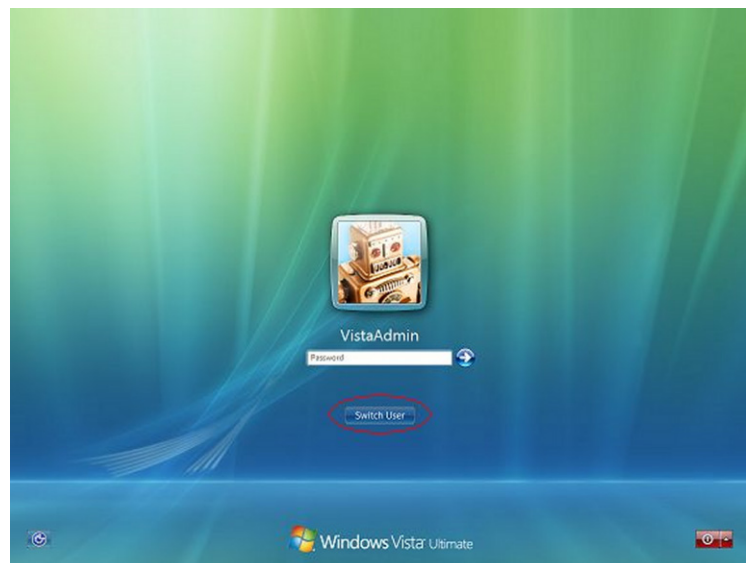
- Step 1** At the Windows Vista start window, press the Ctrl+Alt+Delete key combination (Figure 3-6).

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



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

**Figure 3-7** Vista Logon Window with Switch User Button



- Step 2** Click Switch User (circled in red in this figure). This displays a Vista Network Connect window (Figure 3-8) with the network login icon in the lower-right corner. The network login icon is circled in red in Figure 3-8.

**Note**

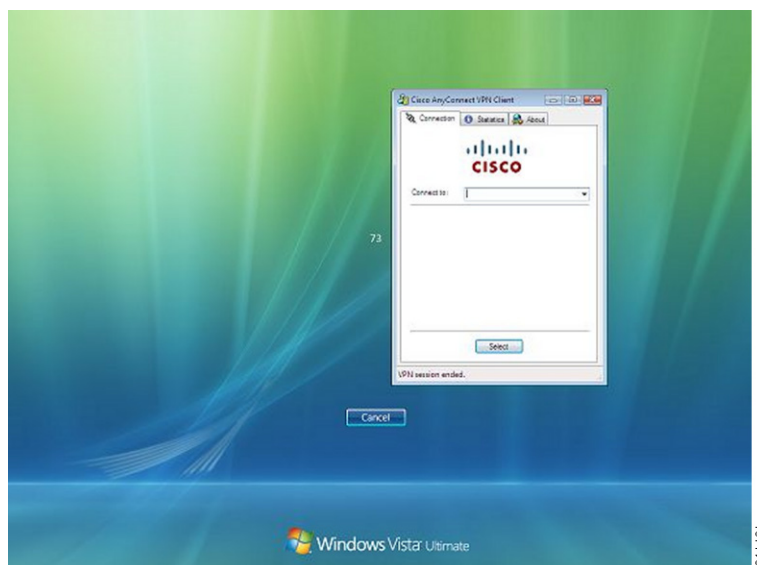
If the user is already connected through an AnyConnect connection and clicks Switch User, that VPN connection remains. If the user clicks Network Connect, the original VPN connection terminates. If the user clicks Cancel, the VPN connection terminates.

**Figure 3-8** Vista Network Connect Window



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

**Figure 3-9** AnyConnect Client Logon Window



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

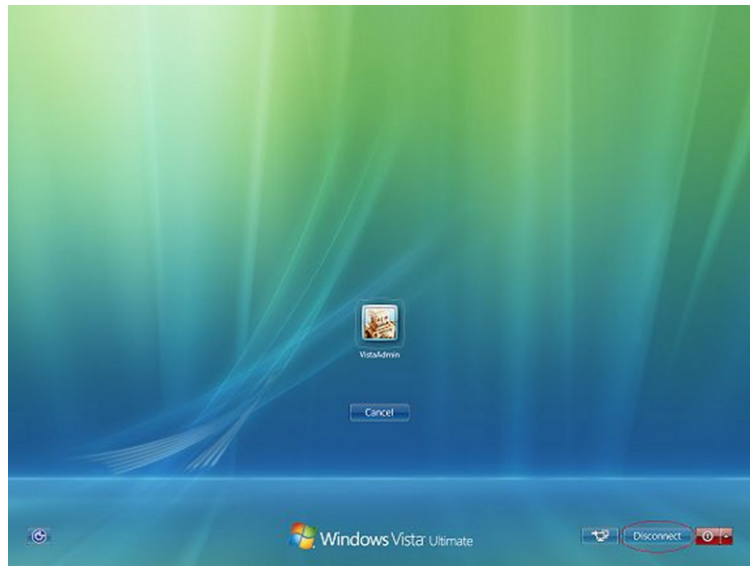


**Note**

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

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

**Figure 3-10** *Disconnect Window*



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



**Caution**

Once the connection is established, the user has an unlimited time in which to log on. If the user forgets to log on after connecting, the tunnel will be up indefinitely.

## Disconnecting from the AnyConnect Client Using PLAP

After successfully connecting the tunnel, the PLAP component returns to the original window, this time with a Disconnect button displayed in the lower-right corner of the window (circled in Figure 3-10).

When the user clicks Disconnect, the VPN tunnel disconnects.

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

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

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

## Enabling FIPS and Additional Security

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

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

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

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

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

The following sections describe all these procedures:

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

## AnyConnect Local Policy File Parameters and Values

**Note**


---

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


---

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

**Table 3-3 AnyConnect Local Policy File and their Values**

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

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

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

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

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

## AnyConnect Local Policy File Example

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

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

## Enabling FIPS with our MST File

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

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

## Changing any Local Policy Parameter with your own MST File

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

- LOCAL\_POLICY\_BYPASS\_DOWNLOADER
- LOCAL\_POLICY\_FIPS\_MODE
- LOCAL\_POLICY\_RESTRICT\_PREFERENCE\_CACHING
- LOCAL\_POLICY\_RESTRICT\_TUNNEL\_PROTOCOLS



- LOCAL\_POLICY\_RESTRICT\_WEB\_LAUNCH
- LOCAL\_POLICY\_STRICT\_CERTIFICATE\_TRUST

**Note**

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

## Changing Parameters for all Operating Systems using our Enable FIPS Tool

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

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

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

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

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

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

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

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

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

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

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

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



## Changing Parameters Manually in the AnyConnect Local Policy File

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

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

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

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

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

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

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

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

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

## Enabling Trusted Network Detection

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

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



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

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

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

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

**Table 3-6**      **Trusted Network Detection Parameters**

Name	Possible Values and Descriptions
AutomaticVPNPolicy	<p><i>true</i>—Enables TND. Automatically manages when a VPN connection should be started or stopped according to the <i>TrustedNetworkPolicy</i> and <i>UntrustedNetworkPolicy</i> parameters.</p> <p><i>false</i>—Disables TND. VPN connections can only be started and stopped manually.</p> <p> <b>Note</b> AutomaticVPNPolicy does not prevent users from manually controlling a VPN connection.</p>
TrustedNetworkPolicy	<p><i>Disconnect</i>—Disconnects the VPN connection in the trusted network.</p> <p><i>DoNothing</i>—Takes no action in the trusted network.</p>
UntrustedNetworkPolicy	<p><i>Connect</i>—Initiates the VPN connection (if none exists) in the untrusted network.</p> <p><i>DoNothing</i>—Takes no action in the untrusted network.</p> <p> <b>Note</b> Setting both TrustedNetworkPolicy and UntrustedNetworkPolicy to <i>DoNothing</i> disables TND.</p>
TrustedDNSDomains	<p>A list of DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. The following is an example of a TrustedDNSDomain string:</p> <p style="padding-left: 40px;">*.cisco.com</p> <p>Wildcards (*) are supported for DNS suffixes.</p>
TrustedDNSServers	<p>A list of DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. The following is an example of a TrustedDNSServers string:</p> <p style="padding-left: 40px;">161.44.124.*,64.102.6.247</p> <p>Wildcards (*) are supported for DNS server addresses.</p>



**Note**

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

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

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

Table 3-7 shows examples of DNS suffix matching.

**Table 3-7** DNS Suffix Matching Examples

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

## Users with Multiple Profiles Connecting to Multiple Security Appliances

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

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

The following workarounds will help you prevent this problem:

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

## Configuring a Certificate Store

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

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

**Note**

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

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

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

## Controlling the Certificate Store on Windows

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

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

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

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

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

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

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

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

## Examples of <CertificateStore> and <CertificateStoreOverride> Usage

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

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

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

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

## Creating a PEM Certificate Store for Mac and Linux

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

## Restrictions for PEM File Filenames

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

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



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

## Storing User Certificates

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

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

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

1. ~ is the home directory.



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

## Restricting Certificate Store Use

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

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

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

## Configuring Simplified Certificate Enrollment Protocol

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

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

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

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

This section describes the following topics:

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

## Provisioning and Renewing Certificates Automatically or Manually

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

### Automatic Certificate Requests

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

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

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

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

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

### Manual Certificate Retrieval

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

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

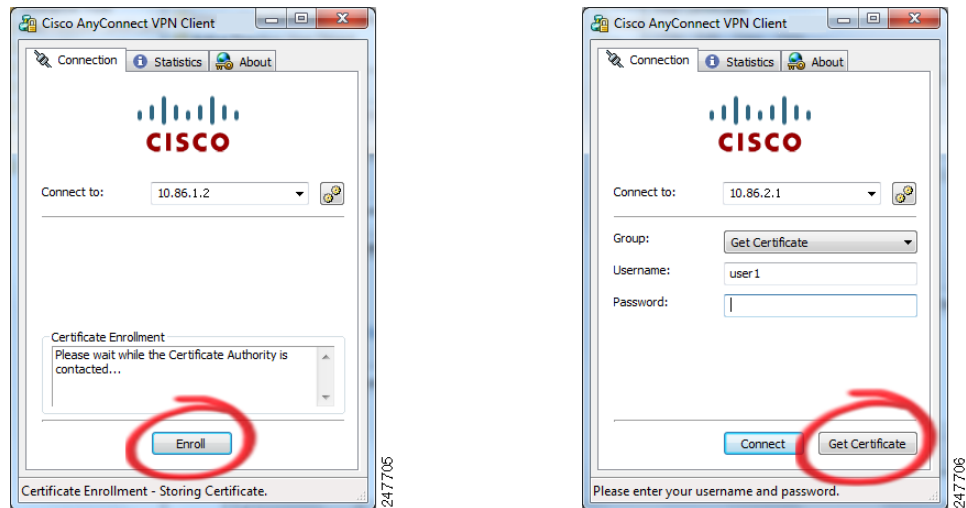
Users will only be able to initiate the certificate request in one of the following instances:

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



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

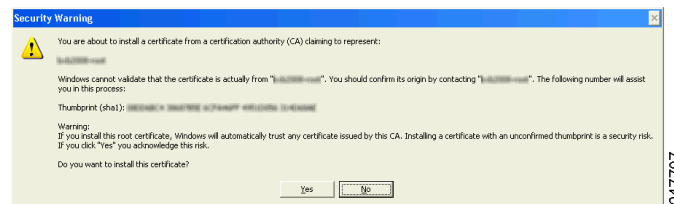
**Figure 3-11** Get Certificate and Enroll Buttons



## Windows Certificate Warning

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

**Figure 3-12** Windows Certificate Security Warning



## Configuring SCEP Protocol to Provision and Renew Certificates

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Note**

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

## Certificate Storage after SCEP Request

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

## Configuring the ASA to Support SCEP Protocol for AnyConnect

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

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

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

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

## Configuring Certificate Only Authentication on the ASA

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

## Configuring Certificate Matching

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

- Key Usage
- Extended Key Usage
- Distinguished Name

## Certificate Key Usage Matching

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

- DIGITAL\_SIGNATURE
- NON\_REPUDIATION
- KEY\_ENCIPHERMENT
- DATA\_ENCIPHERMENT
- KEY\_AGREEMENT
- KEY\_CERT\_SIGN
- CRL\_SIGN
- ENCIPHER\_ONLY
- DECIPHER\_ONLY

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

The example in [Certificate Matching Example, page 3-41](#) shows how you might configure these attributes.

## Extended Certificate Key Usage Matching

This matching allows an administrator to limit the certificates that can be used by the client, based on the *Extended Key Usage* fields. [Table 3-12](#) lists the well known set of constraints with their corresponding object identifiers (OIDs).

**Table 3-12**      **Extended Certificate Key Usage**

Constraint	OID
ServerAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10

All other OIDs, such as 1.3.6.1.5.5.7.3.11, used in some examples in this document) are considered “custom.” As an administrator, you can add your own OIDs if the OID you want is not in the well known set. The profile can contain none or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. See the example AnyConnect profile named AnyConnectProfile.tmp1, which the AnyConnect client automatically downloads to the endpoint.

## Certificate Distinguished Name Mapping

The certificate distinguished name mapping capability allows an administrator to limit the certificates that can be used by the client to those matching the specified criteria and criteria match conditions.

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

**Table 3-13** Criteria for Certificate Distinguished Name Mapping

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



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

Identifier	Description
CN	SubjectCommonName
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

The profile can contain zero or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. *Distinguished Name* matching offers additional match criteria, including the ability for the administrator to specify that a certificate must or must not have the specified string, as well as whether wild carding for the string should be allowed. See the example AnyConnect profile named AnyConnectProfile.tmpl, which the AnyConnect client automatically downloads to the endpoint.

## Certificate Matching Example



### Note

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

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

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

```

        <Name>CN</Name>
        <Pattern>ASA_Security</Pattern>
    </DistinguishedNameDefinition>
    <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
        <Name>L</Name>
        <Pattern>Boulder</Pattern>
    </DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>

```

Within the ClientInitialization section, the CertificateMatch section defines preferences that refine client certificate selection. Except as noted, these parameters do not have default values; that is, if you do not specify a parameter, it is simply not in effect. [Table 3-14](#) summarizes these parameters and defines their possible values.

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

**Table 3-14** Certificate Match Parameters

XML Tag Name	Possible Values	Description	Example
CertificateMatch	n/a	Group identifier	<CertificateMatch>... </CertificateMatch>
KeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to specify acceptable client certificates.	<KeyUsage> <MatchKey>Non_Repudiation</MatchKey> </KeyUsage>
MatchKey	Decipher_Only Encipher_Only CRL_Sign Key_Cert_Sign Key_Agreement Data_Encipherment Key_Encipherment Non_Repudiation Digital_Signature	Within the KeyUsage group, MatchKey attributes specify attributes that can be used for choosing acceptable client certificates. Specify one or more match keys. A certificate must match at least one of the specified key to be selected.	<KeyUsage> <MatchKey>Non_Repudiation</MatchKey> <MatchKey>Digital_Signature</MatchKey> </KeyUsage>
ExtendedKeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to choose acceptable client certificates.	<ExtendedKeyUsage> <ExtendedMatchKey>ClientAuth</ExtendedMatchKey> </ExtendedKeyUsage>

**Table 3-14** Certificate Match Parameters (continued)

XML Tag Name	Possible Values	Description	Example
ExtendedMatchKey	ClientAuth ServerAuth CodeSign EmailProtect IPSecEndSystem IPSecTunnel IPSecUser TimeStamp OCSPSign DVCS	Within the ExtendedKeyUsage group, ExtendedMatchKey specifies attributes that can be used for choosing acceptable client certificates. Specify zero or more extended match keys. A certificate must match all of the specified key(s) to be selected.	<ExtendedMatchKey>ClientAuth</ExtendedMatchKey> <ExtendedMatchKey>ServerAuth</ExtendedMatchKey>
CustomExtendedMatchKey	Well-known MIB OID values, such as 1.3.6.1.5.5.7.3.11	Within the ExtendedKeyUsage group, you can specify zero or more custom extended match keys. A certificate must match all of the specified key(s) to be selected. The key should be in OID form (for example, 1.3.6.1.5.5.7.3.11)	<CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11< <CustomExtendedMatchKey>
DistinguishedName	n/a	Group identifier. Within the DistinguishedName group, Certificate Distinguished Name matching lets you specify match criteria for choosing acceptable client certificates.	<DistinguishedName>...</DistinguishedName>

Table 3-14 Certificate Match Parameters (continued)

XML Tag Name	Possible Values	Description	Example
DistinguishedNameDefinition	<p>Bold text indicates default value.</p> <p>Wildcard:  <b>"Enabled"</b>            "Disabled"</p> <p>Operator:  <b>"Equal"</b> or ==            "NotEqual" or !=</p> <p>MatchCase:  <b>"Enabled"</b>            "Disabled"</p>	DistinguishedNameDefinition specifies a set of operators used to define a single Distinguished Name attribute to be used in matching. The Operator specifies the operation to use in performing the match. MatchCase specifies whether the pattern matching is case sensitive.	<pre>&lt;DistinguishedNameDefinition Operator="Equal" Wildcard="Enabled" Matchcase="Enabled"&gt;   &lt;Name&gt;CN&lt;/Name&gt;   &lt;Pattern&gt;ASASecurity&lt;/Pattern&gt; &lt;/DistinguishedNameDefinition&gt;</pre>
Name	CN DC SN GN N I GENQ DNQ C L SP ST O OU T EA ISSUER-CN ISSUER-DC ISSUER-SN ISSUER-GN ISSUER-N ISSUER-I ISSUER-GENQ ISSUER-DNQ ISSUER-C ISSUER-L ISSUER-SP ISSUER-ST ISSUER-O ISSUER-OU ISSUER-T ISSUER-EA	A DistinguishedName attribute name to be used in matching. You can specify up to 10 attributes.	
Pattern	A string (1-30 characters) enclosed in double quotes. With wildcards enabled, the pattern can be anywhere in the string.	Specifies the string (pattern) to use in the match. Wildcard pattern matching is disabled by default for this definition.	

# Prompting Users to Select Authentication Certificate

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

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

## Configuring the Client Profile with AutomaticCertSelection

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

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

**Table 3-15** *AutomaticCertSelection element description*

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

**Figure 3-13** *AutomaticCertSelection element in client profile*

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">

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



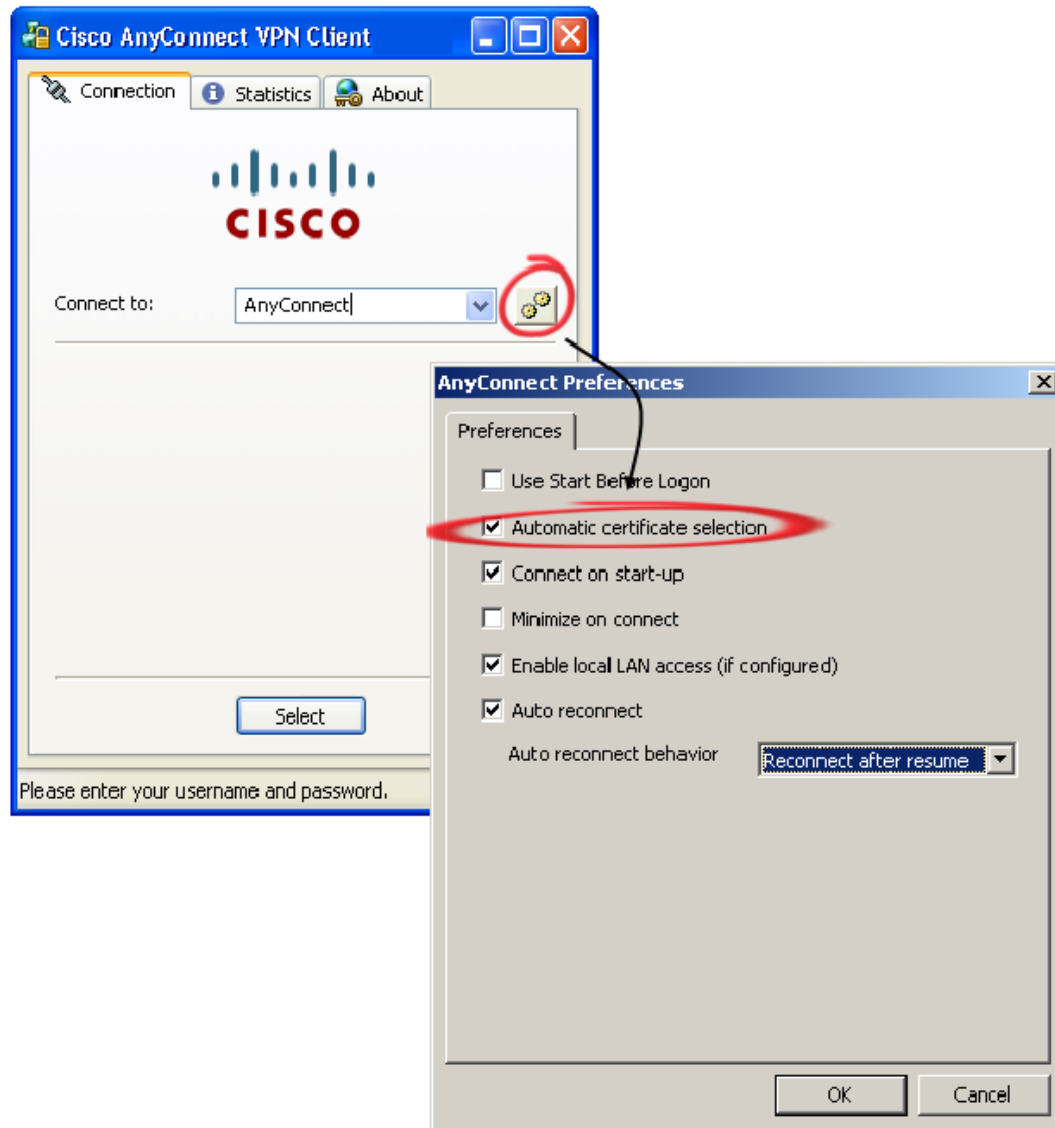
### Caution

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

## Users Configuring Automatic Certificate Selection in AnyConnect Preferences

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

**Figure 3-14** Automatic Certificate Selection check box



# Configuring Backup Server List Parameters

You can configure a list of backup servers the client uses in case the user-selected server fails. These servers are specified in the AnyConnect client profile, in the ClientInitialization section. In some cases, the BackupServerList might specify host specific overrides.

These parameters do not have default values; that is, if you do not specify a parameter, it is simply not in effect. [Table 3-16](#) lists these parameters and defines their possible values.



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

**Table 3-16** Backup Server Parameters

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

## Installing AnyConnect on a Windows Mobile Device

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

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

- Bluetooth
- (USB) Cable
- Media card transfer

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

---

## Configuring a Windows Mobile Policy

To allow end users to connect using Windows Mobile devices, configure the Mobile Policy parameters. These parameters apply only to Windows Mobile devices. Include them only if your end users use Windows Mobile. See the latest [AnyConnect Release Notes](#) for detailed, current information about Windows Mobile device support.



### Note

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

---

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



### Note

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

---

[Table 3-17](#) shows the MobilePolicy parameters and their values.



**Table 3-17**      *Mobile Policy Parameters*

Parameter	Possible Values	Description	Example
MobilePolicy	n/a	Group identifier.	<MobilePolicy>...</MobilePolicy>
DeviceLockRequired	n/a	<p>Group identifier. Within the MobilePolicy group, DeviceLockRequired indicates that a Windows Mobile device must be configured with a password or PIN prior to establishing a VPN connection. This configuration is valid only on Windows Mobile devices that use the Microsoft Default Local Authentication Provider (LAP).</p> <p><b>Note</b> The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, WM5AKU2+, and Windows Mobile 6.0, but not on Windows Mobile 6.1.</p>	<pre>&lt;DeviceLockRequired&gt;   MaximumTimeoutMinutes="60"   MinimumPasswordLength="4"   PasswordComplexity="pin" &lt;/DeviceLockRequired&gt;</pre>
MaximumTimeoutMinutes	Any non-negative integer	Within the DeviceLockRequired group, this parameter, when set to a non-negative number, specifies the maximum number of minutes that must be configured before device lock takes effect.	<pre>&lt;DeviceLockRequired&gt;   MaximumTimeoutMinutes="60"   MinimumPasswordLength="4"   PasswordComplexity="pin" &lt;/DeviceLockRequired&gt;</pre>

**Table 3-17** Mobile Policy Parameters (continued)

Parameter	Possible Values	Description	Example
MinimumPasswordLength	Any non-negative integer	<p>Within the DeviceLockRequired group, when set to a non-negative number, this parameter specifies that any PIN/password used for device locking must have at least the specified number of characters.</p> <p>This setting must be pushed down to the mobile device by syncing with an Exchange server before it can be enforced. (WM5AKU2+)</p>	<pre>&lt;DeviceLockRequired&gt;   MaximumTimeoutMinutes="60"   MinimumPasswordLength="4"   PasswordComplexity="pin" &lt;/DeviceLockRequired&gt;</pre>
PasswordComplexity	<p>"alpha"-Requires an alphanumeric password.</p> <p>"pin"-Requires a numeric PIN.</p> <p>"strong"-Requires a strong alphanumeric password, defined by Microsoft as containing at least 7 characters, including at least 3 from the set of uppercase, lowercase, numerals, and punctuation.</p>	<p>When present checks for the password subtypes listed in the column to the left.</p> <p>This setting must be pushed down to the mobile device by syncing with an Exchange server before it can be enforced. (WM5AKU2+)</p>	<pre>&lt;DeviceLockRequired&gt;   MaximumTimeoutMinutes="60"   MinimumPasswordLength="4"   PasswordComplexity="pin" &lt;/DeviceLockRequired&gt;</pre>

**Note**

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

## Installing AnyConnect on 64-bit Linux

To install AnyConnect on x86\_64 versions of Ubuntu 9,

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

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

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

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

## Configuring Auto Connect On Start

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

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

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

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

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

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

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

# Configuring Auto Reconnect

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

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

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



## Note

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

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

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

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



## Note

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

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

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

Table 3-19 shows these tags and default values.

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

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

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

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

## Installing Host Scan

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

## Configuring a Server List

One of the main uses of the profile is to let the user list the connection servers. The user then selects the appropriate server. This server list consists of host name and host address pairs. The host name can be an alias used to refer to the host, an FQDN, or an IP address. If an FQDN or IP address is used, a HostAddress element is not required. In establishing a connection, the host address is used as the

connection address unless it is not supplied. This allows the host name to be an alias or other name that need not be directly tied to a network addressable host. If no host address is supplied, the connection attempt tries to connect to the host name.

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

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

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

**Table 3-20** Server List Parameters

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

Table 3-20 Server List Parameters (continued)

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



# Split DNS Fallback

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

This feature requires that you:

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

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

## Scripting

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

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

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

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

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

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



### Note

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

## Scripting Requirements and Limitations

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

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

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

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

AnyConnect supports script launching during WebLaunch and standalone launches.

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

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

Other requirements apply, as indicated in the next section.

## Writing, Testing, and Deploying Scripts

Deploy AnyConnect scripts as follows:

---

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



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

---

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

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



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

---

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

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

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

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

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

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

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

- *OnConnect*
- *OnDisconnect*

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

**Table 3-21 Required Script Locations**

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

## Configuring the AnyConnect Profile for Scripting

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

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

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

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

Insert these parameters anywhere inside the `ClientInitialization` section of the AnyConnect profile.

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

```
<ClientInitialization>
```

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

```
</ClientInitialization>
```

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

```
<ClientInitialization>

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

</ClientInitialization>
```

**Note**

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

## Troubleshooting Scripts

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

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

# Proxy Support

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

## Ignore Proxy

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

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

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



### Note

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

## Private Proxy

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

## Private Proxy Requirements

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

AnyConnect supports this feature on computers running:

- Internet Explorer on Windows
- Safari on Mac OS

## Configuring a Group Policy to Download a Private Proxy

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

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

## Internet Explorer Connections Tab Lockdown

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

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

## Proxy Auto-Configuration File Generation for Clientless Support

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

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

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

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

**Note**

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

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

**Table 3-23** Windows Logon Preferences

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

## AnyConnect over L2TP or PPTP

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

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

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

The following sections describe how to set up PPP exclusion:

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



## Configuring AnyConnect over L2TP or PPTP

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

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
  <ClientInitialization>
    <PPPEXclusion UserControllable="true">Automatic</PPPEXclusion>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>DomainNameofASA</HostName>
      <HostAddress>IPaddressOfASA</HostAddress>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>
```

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

AnyConnect supports the following **PPPEXclusion** values:

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

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

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
  <ClientInitialization>
    <PPPEXclusion UserControllable="true">Automatic</PPPEXclusion>
    <PPPEXclusionServerIP UserControllable="true"></PPPEXclusionServerIP>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>SecureGatewayName</HostName>
      <HostAddress>SecureGatewayName.domain</HostAddress>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>
```

## Instructing Users to Override PPP Exclusion

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

---

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

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

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

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

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

**Step 3** Save the file.

**Step 4** Exit and restart AnyConnect.

---

# Configuring Other AnyConnect Profile Settings

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

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

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

1. AnyConnect uses the default value if the profile does not specify one.
2. Insert the parameter value between the beginning and closing tags; for example, `<CertificateStoreOverride>true</CertificateStoreOverride>`.
3. Anyconnect ignores the `usercontrollable="true"` string if the parameter does not support user control.
4. The AnyConnect Preferences dialog box displays the parameter values and lets users change them, depending on the value of the associated user control attribute. The user control attribute is optional. If you do not insert it, AnyConnect uses its default value. To permit or deny user control, insert the user control attribute inside the opening tag; for example, `<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>`.
5. AnyConnect client is compatible with RSA SecurID software versions 1.1 and higher. At the time of this release, RSA SecurID Software Token client software does not support Windows Vista and 64-bit systems.

