CHAPTER 7

Configuring and Using AnyConnect Client Operating Modes and User Profiles

AnyConnect Client Operating Modes

The user can use the AnyConnect Client in the following modes:

- Standalone mode—Lets the user establish a Cisco AnyConnect VPN client connection without the need to use a web browser. If you have permanently installed the AnyConnect client on the user's PC, the user can run in standalone mode. In standalone mode, a user opens the AnyConnect client just like any other application and enters the username and password credentials into the fields of the AnyConnect GUI. Depending on ho w you configure the system, the user might also be required to select a group. When the connection is established, the security appliance checks the version of the client on the user's PC and, if necessary, downloads the latest version.
- WebLaunch mode—Lets the user enter the URL of the security appliance in the Address or Location field of a browser using the https protocol. The user then enters the username and password information on a Logon screen and selects the group and clicks submit. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking Continue.

  The portal window appears. To start the AnyConnect client, the user clicks Start AnyConnect on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities.

Using the AnyConnect CLI Commands to Connect (Standalone Mode)

The Cisco AnyConnect VPN Client provides a command line interface (CLI) for users who prefer to issue commands instead of using the graphical user interface. The following sections describe how to launch the CLI command prompt.

For Windows

To launch the CLI command prompt and issue commands on a Windows system, locate the file *vpncli.exe* in the Windows folder C:\Program Files\Cisco\Cisco AnyConnect VPN Client. Double-click the file *vpncli.exe.*

For Linux and Mac OS X

To launch the CLI command prompt and issue commands on a Linux or Mac OS X system, locate the file *vpn* in the folder /opt/cisco/vpn/bin/. Execute the file *vpn.*

You can run the CLI in interactive mode, in which it provides its own prompt, or you can run it with the commands on the command line. Table 7-1 shows the CLI commands.

Table 7-1 AnyConnect Client CLI Commands

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

The following examples show the user establishing and terminating a connection from the command line:

Windows

connect 209.165.200.224

Establishes a connection to a security appliance with the address 209.165. 200.224. After contacting the requested host, the AnyConnect client displays the group to which the user belongs and asks for the user's username and password. If you have specified that an optional banner be displayed, the user must respond to the banner. The default response is **n**, which terminates the connection attempt. For example:

```
VPN> connect 209.165.200.224
    >>contacting host (209.165.200.224) for login information...
    >>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
    >>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour. The system will not be available during that time.

accept? [y/n] y
    >> notice: Authentication succeeded. Checking for updates...
    >> state: Connecting
    >> notice: Establishing connection to 209.165.200.224.
    >> State: Connected
    >> notice: VPN session established.
VPN>
```

stats

Displays statistics for the current connection; for example:

```
VPN> stats
[ Tunnel Information ]

    Time Connected:01:17:33
    Client Address:192.168.23.45
    Server Address:209.165.200.224

[ Tunnel Details ]

    Tunneling Mode:All Traffic
    Protocol: DTLS
    Protocol Cipher: RSA_AES_256_SHA1
    Protocol Compression: None
```

```
[ Data Transfer ]

    Bytes(sent/received): 1950410/23861719
    Packets (sent/received): 18346/28851
    Bypassed (outbound/inbound): 0/0
    Discarded (outbound/inbound): 0/0

[ Secure Routes ]

    Network     Subnet
    0.0.0.0     0.0.0.0
VPN>
```

disconnect
Closes a previously established connection; for example:

```
VPN> disconnect
    >> state: Disconnecting
    >> state: Disconnected
    >> notice: VPN session ended.
VPN>
```

quit or **exit**

Either command exits the CLI interactive mode; for example:

```
quit
goodbye
    >>state: Disconnected
```

Linux or Mac OS X

/opt/cisco/vpn/bin/vpn connect 1.2.3.4
Establishes a connection to a security appliance with the address *1.2.3.4*.

/opt/cisco/vpn/bin/vpn connect some_asa_alias
Establishes a connection to a security appliance by reading the profile and looking up the alias *some_asa_alias* in order to find its address.

/opt/cisco/vpn/bin/vpn stats
Displays statistics about the vpn connection.

/opt/cisco/vpn/bin/vpn disconnect
Disconnect the vpn session if it exists.

Connecting Using WebLaunch

The Cisco AnyConnect VPN Client provides a browser interface for users who prefer to a graphical user interface. *WebLaunch* mode lets the user enter the URL of the security appliance in the Address or Location field of a browser using the https protocol. For example:

https://209.165.200.225

The user then enters the username and password information on a Logon screen and selects the group and clicks submit. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking Continue.

The portal window appears. To start the AnyConnect client, the user clicks Start AnyConnect on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities.

Note For Windows Vista users who use the Internet Explorer browser, you must add the security appliance to the list of trusted sites, as described in Adding a Security Appliance to the List of Trusted Sites (Internet Explorer), page 2-3.

User Log In and Log Out

You might find it useful to provide the following instructions to your remote users.

Logging In

Your system administrator has assigned you a remote access username and password. Before you log in, you must get this information from your system administrator.

Step 1 Enter your remote access username in the Username field.

Step 2 Enter your remote access password in the Password field.

Step 3 Click Login.

Step 4 If you receive a certificate warning, install the certificate.

Your remote access home page appears.

Logging Out

To end your remote access session, click the "Close Window" (X) icon in the toolbar or click the Logout link. The Logout page appears, confirming that your session has been terminated and offering you the opportunity to log in again.

Quitting the browser also logs out the session.

Caution *Security note:* Always log out when you finish your session. Logging out is especially important when you are using a public computer such as in a library or Internet cafe. If you do not log out, someone who uses the computer next could access your files. Don't risk the security of your organization! Always log out.

Configuring and Using User Profiles

An AnyConnect client user profile is an XML file that lets you identify the secure gateway (security appliance) hosts that you want to expose to the user community. In addition, the profile conveys additional connection attributes and constraints on a user.

Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and additional settings as needed. In some cases, you might want to provide more than one profile for a given user. For example, someone who works from multiple locations might need more than one profile. In such cases,

the user selects the appropriate profile from a drop-down list. Be aware, however, that some of the profile settings, such as Start Before Login, control the connection experience at a global level. Other settings, such as those unique to a particular host, depend on the host selected.

Enabling AnyConnect Client Profile Downloads

An AnyConnect client profile is a group of configuration parameters, stored in an XML file, that the client uses to configure the connection entries that appear in the client user interface. The client parameters (XML tags) include the names and addresses of host computers and settings to enable additional client features.

You can create and save XML profile files using a text editor. The client installation contains one profile template (AnyConnectProfile.tmpl) that you can edit and use as a basis to create other profile files.

The profile file is downloaded from the security appliance to the remote users's PC, so you must first import the profile(s) into the security appliance in preparation for downloading to the remote PC. You can import a profile using either ASDM or the command-line interface. See Appendix A, "Sample AnyConnect Profile and XML Schema" for a sample AnyConnect profile.

When the AnyConnect client starts, it reads the preferences.xml file in the following directory:

C:\Documents and Settings\<your_username>\Local Settings\Application Data\Cisco\Cisco AnyConnect VPN Client.

The preferences.xml file contains the username and the security appliance IP address/hostname from the last successful connection. The client then establishes an initial connection to the security appliance to get the list of tunnel groups to display in the GUI. during this initial connection, if the security appliance is no longer accessible or if the hostname cannot be resolved, the user sees the message, "Connection attempt has failed" or "Connection attempt has failed due to unresolvable host entry."

You can place a copy of your profile (for example, CiscoAnyConnectProfile.xml) 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 The host that appears in the Connect to combo box is the first one listed in the profile or the last host you successfully connected with.

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

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

Follow these steps to edit profiles and use ASDM to enable the security appliance to download them to remote clients:

Step 1 Retrieve a copy of the profiles file (AnyConnectProfile.xml) from a client installation. Table 7-2 shows the installation path for each operating system.

Table 7-2 Operating System and Profile File Installation Path

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

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

Step 2 Edit the profiles file. The example below shows the contents of the profiles file (AnyConnectProfile.xml) for Windows:

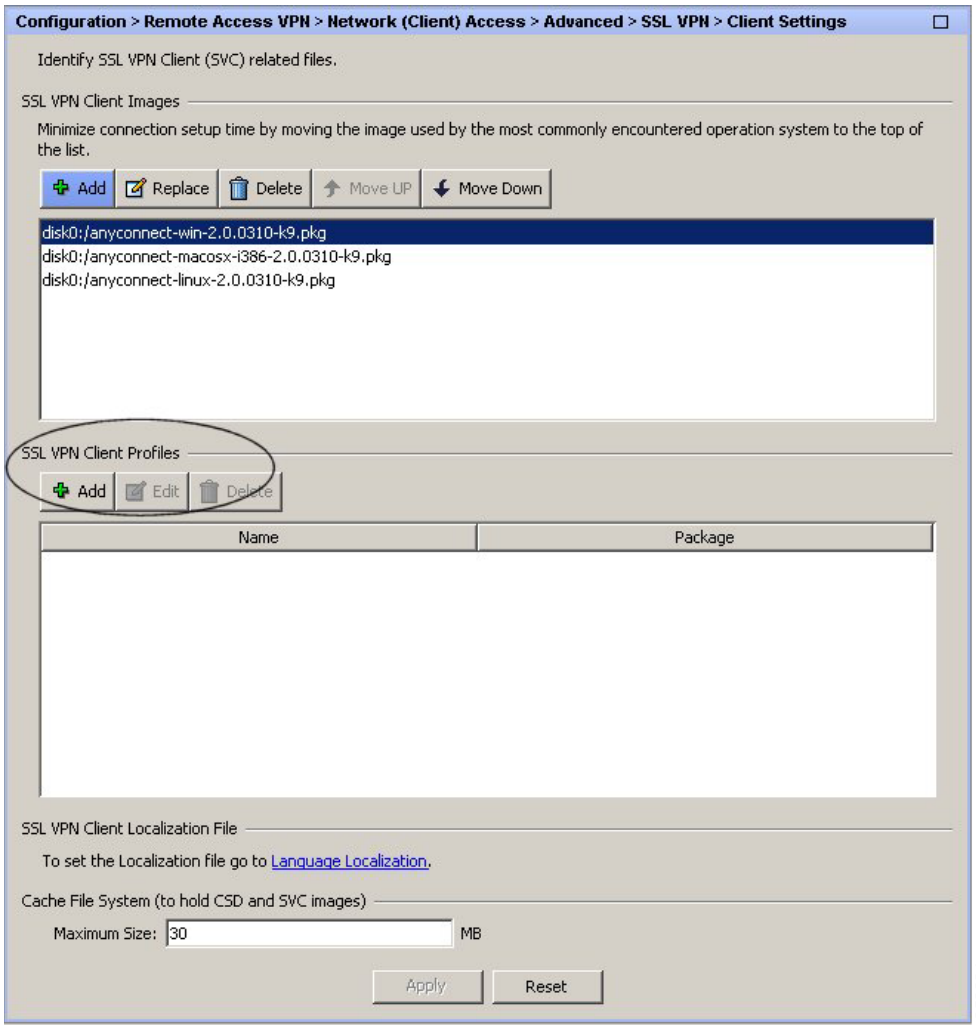
```
<?xml version="1.0" encoding="UTF-8"?>
<!--
    This is a template file that can be configured to support the
    identification of secure hosts in your network.

    The file needs to be renamed to CiscoAnyConnectProfile.xml.

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

The <HostProfile> tags are frequently edited so that the AnyConnect client displays the names and addresses of host computers for remote users. The following example shows the <HostName> and <HostAddress> tags, with the name and address of a host computer inserted:

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

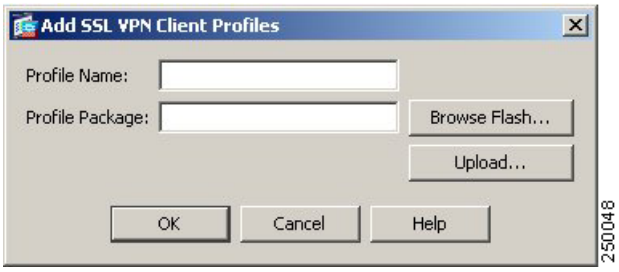
Step 3 To identify to the security appliance the client profiles file to load into cache memory, select Configuration > Remote Access VPN > Network (Client) Access > Advanced > Client Settings (Figure 7-1).

Figure 7-1 Adding or Editing an AnyConnect VPN Client Profile



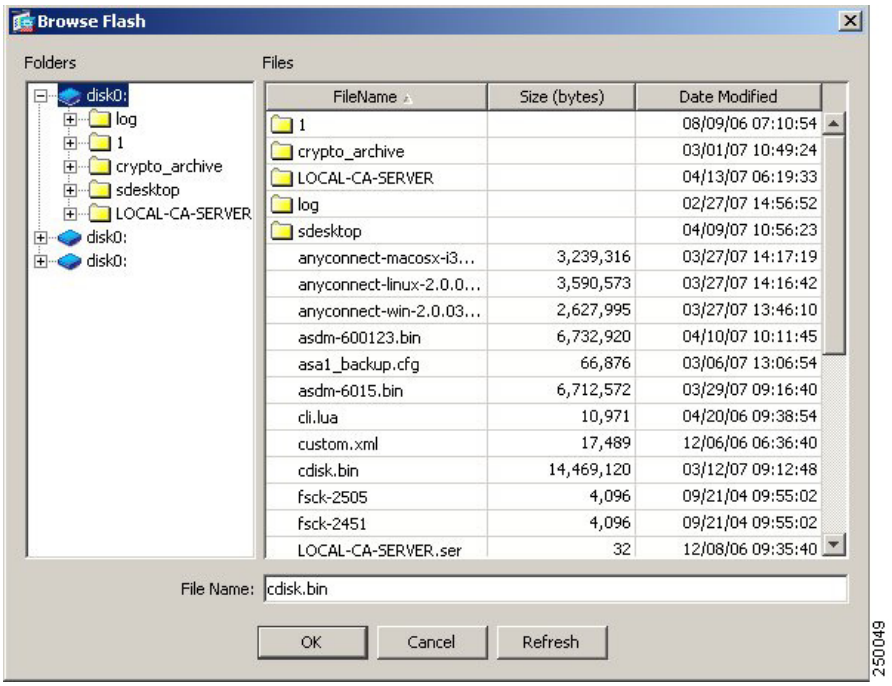
In the SSL VPN Client Profiles area, click Add or Edit. the Add or Edit SSL VPN Client Profiles dialog box appears (Figure 7-2).

Figure 7-2 Add (or Edit) SSL VPN Client Profiles Dialog Box



Enter the profile name and profile package names in their respective fields. To browse for a profile package name, click Browse Flash. The Browse Flash dialog box appears (Figure 7-3).

Figure 7-3 Browse Flash Dialog Box

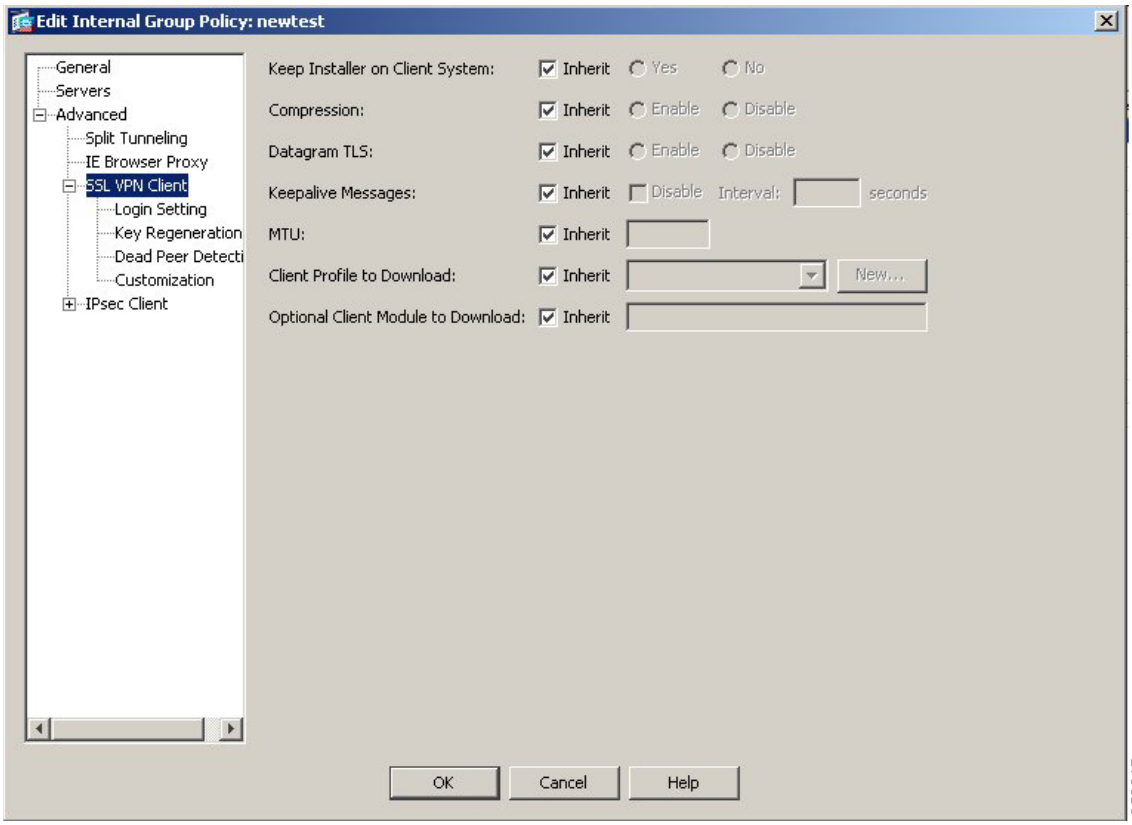


Select a file from the table. The file name appears in the File Name field below the table. Click OK. The file name you selected appears in the Profile Package field of the Add or Edit SSL VPN Client Profiles dialog box.

Step 4 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 configure a profile for a group policy, select Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Select an existing group policy and click Edit or click Add to configure a new group policy. In the navigation pane, select Advanced > SSL VPN Client. The Add or Edit Internal Group Policy dialog box appears (Figure 7-4).

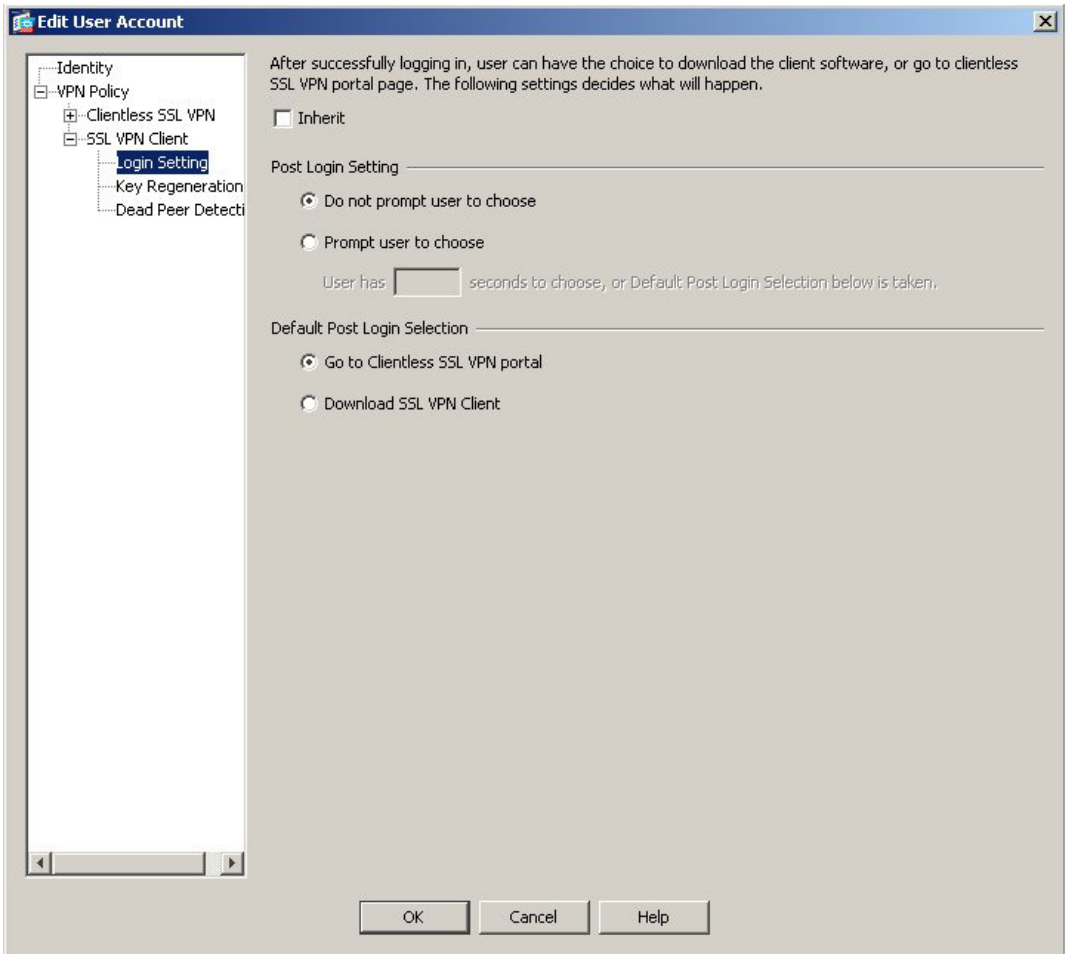
Figure 7-4 Add or Edit Internal Group Policy Dialog Box



Continue with Step 7.

Step 6 To configure a profile for a user, select Configuration > Device Management > Users/AAA > User Accounts. Select an existing username and click Edit or click Add to configure a new username. In the navigation pane, select VPN Policy > SSL VPN Client. To modify an existing user's profile, select that user from the table and click Edit. To Add a new user, click Add. The Add or Edit User Account dialog box appears (Figure 7-5).

Figure 7-5 Add or Edit User Account Dialog Box (Username)



Step 7 Deselect Inherit and select a Client Profile to Download from the drop-down list or click New to specify a new client profile. If you click New, the Add SSL VPN Client Profile dialog box (Figure 7-2 on page 7-7) appears; follow the procedures that pertain to that figure.

Step 8 When you have finished with the configuration, click OK.

Configuring Profile Attributes

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

Note It is important to validate the XML profile you create. Use an online validation tool or the profile import feature in ASDM. For validation, you can use the AnyConnectProfile.xsd found in the same directory as the profile template. See Appendix A, "Sample AnyConnect Profile and XML Schema" for a hard copy of these files.

The following sections describe how to modify the profiles template to configure the profile attributes.

Enabling Start Before Logon (SBL) for the AnyConnect Client

With SBL enabled, the user sees the AnyConnect GUI logon dialog before the Windows logon dialog box appears. This establishes the VPN connection first. Available only for Windows platforms, Start Before Logon lets the administrator control the use of login scripts, password caching, mapping network drives to local drives, and more. You can use the SBL feature to activate the VPN as part of the logon sequence. SBL is disabled by default.

XML Settings for Enabling SBL

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

You enable SBL by setting the <UseStartBefore Logon> value in the CiscoAnyConnect.xml file to true:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

To disable SBL, set the same value to false.

To enable the UserControllable feature, use the following statement when enabling SBL:

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

Any user setting associated with this attribute is stored elsewhere.

CLI Settings for Enabling SBL

To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of core modules that it needs for each feature that it supports. To enable new features, such as Start Before Logon (SBL), you must specify the module name using the **svc modules** command from group policy webvpn or username webvpn configuration mode:

[no] svc modules {**none** | **value** *string*}

The *string* for SBL is **vpngina**

In the following example, the user enters group-policy attributes mode for the group policy *telecommuters*, enters webvpn configuration mode for the group policy, and specifies the string *vpngina* to enable SBL:

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

In addition, the administrator must ensure that the AnyConnect profile.xml file has the <UseStartBeforeLogon> statement set to true. For example:

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

The system must be rebooted before Start Before Logon takes effect.

You must also specify on the security appliance that you want to allow SBL (or any other modules for additional features). See the description in the section Enabling Modules for Additional AnyConnect Features, page 5-5 (ASDM) or Enabling Modules for Additional AnyConnect Features, page 6-4 (CLI) for a description of how to do this.

Configuring the ServerList Attribute

One of the main uses of the profile is to provide a means of supplying a user of the client with a list of hosts to which they can connect. 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, a default server can be specified. 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.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ServerList>
    <HostEntry>
        <HostName>MarketingASA01</HostName>
        <HostAddress>209.165.200.224,/HostAddress>
    </HostEntry>
<HostEntry>
        <HostName>EngineeringASA01</HostName>
        <HostAddress>209.165.200.225,/HostAddress>
    </HostEntry>
</ServerList>
```

Configuring the Certificate Match Attribute

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 7-15 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 7-3 lists the well known set of constraints with their corresponding object identifiers (OIDs).

Table 7-3 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

As an administrator, you can add your own OIDs if the OID you want is not in the well known set. The profile can contain none or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. See profile example in Appendix A, “Sample AnyConnect Profile and XML Schema” for an example.

Certificate Distinguished Name Mapping

The certificate distinguished name mapping capability allows an administrator to limit the certificates that can be used by the client to those matching the specified criteria and criteria match conditions. Table 7-4 lists the supported criteria:

Table 7-4 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
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
"SSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr

The profile can contain none or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. *Distinguished Name* matching offers additional match criteria, including the ability for the administrator to specify that a certificate must or must not have the specified string, as well as whether wild carding for the string should be allowed. See Appendix A, “Sample AnyConnect Profile and XML Schema,” for an example.

Certificate Matching Example

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

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