CHAPTER 4

Configuring and Using AnyConnect Client Operating Modes and User Profiles

Contents

This chapter contains the following major topics:

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 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 4-1 shows the CLI commands.

Table 4-1 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 (IE), page 2-18 and Appendix B, "Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users".

For Windows Mobile users, WebLaunch is supported only using the Pocket Internet Explorer browser. Because Pocket IE cannot load ActiveX components wirelessly, attempts to perform a fresh install of the AnyConnect client using WebLaunch will not succeed and will bring the user to a web page from which he or she must download and install the Mobile installer. After the AnyConnect client has been installed, WebLaunch can be used to initiate tunnels.

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

User profiles are created by an administrator and are automatically delivered to a client machine during connection setup. Profiles provide basic information about connection setup, and users cannot manage or modify them.

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

Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and additional settings as needed. In some cases, you might want to provide more than one profile for a given user. For example, someone who works from multiple locations might need more than one profile. In such cases, the user selects the appropriate profile from a drop-down list. Be aware, however, that some of the profile settings, such as Start Before Login, control the connection experience at a global level. Other settings, such as those unique to a particular host, depend on the host selected.

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 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. See Appendix A, "Sample AnyConnect Profile and XML Schema" for a sample AnyConnect profile.

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. Make a copy and rename that copy with a name meaningful to you. Alternatively, you can modify an existing profile. Table 4-2 shows the installation path for each operating system.

Table 4-2 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:

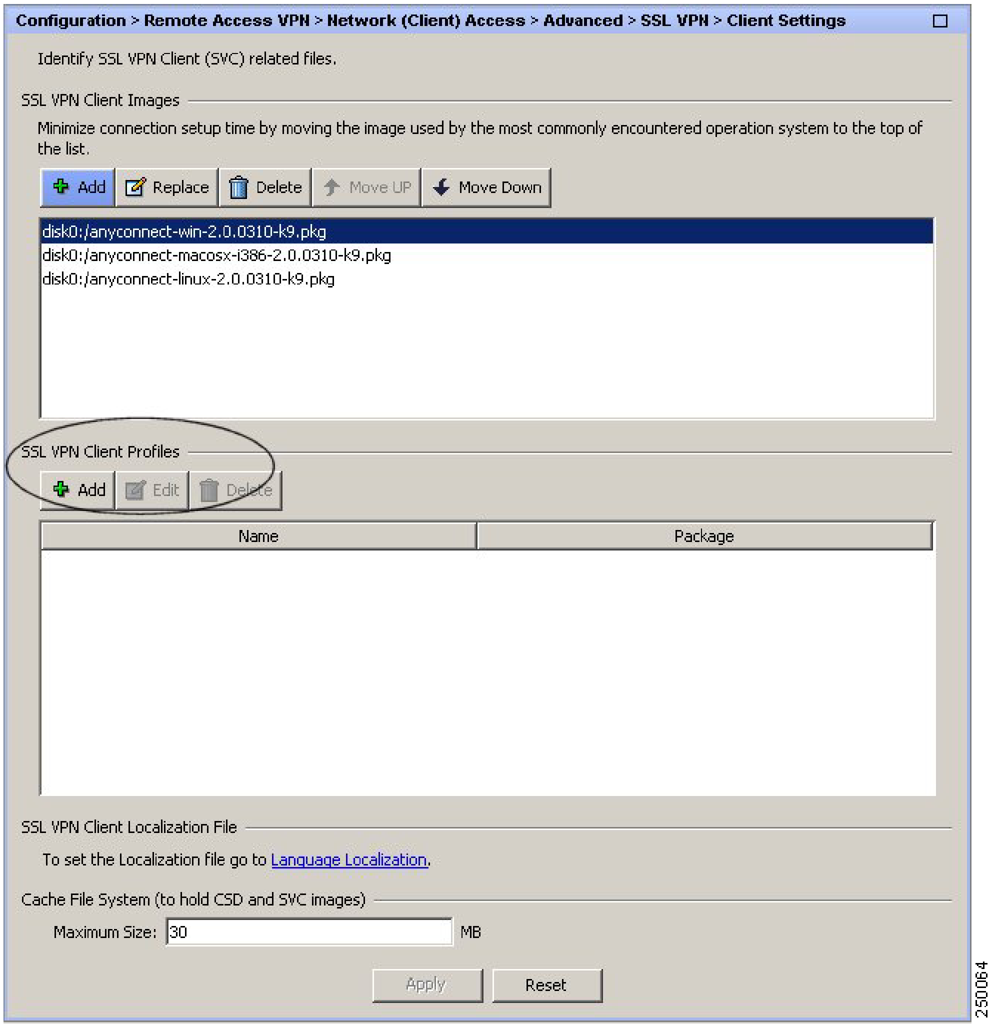
```
    <HostProfile>
        <HostName>Sales_gateway</HostName>
        <HostAddress>209.165.200.225</HostAddress>
    </HostProfile>
```

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

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 4-1).

Figure 4-1 Adding or Editing an AnyConnect VPN Client Profile



Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings

Identify SSL VPN Client (SVC) related files.

SSL VPN Client Images

Minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

disk0:/anyconnect-win-2.0.0310-k9.pkg
disk0:/anyconnect-macosx-i386-2.0.0310-k9.pkg
disk0:/anyconnect-linux-2.0.0310-k9.pkg

SSL VPN Client Profiles

Name	Package

SSL VPN Client Localization File

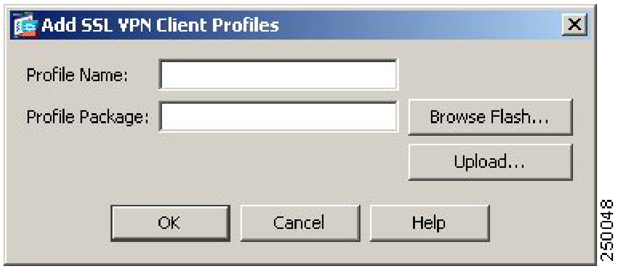
To set the Localization file go to Language Localization.

Cache File System (to hold CSD and SVC images)

Maximum Size: 30 MB

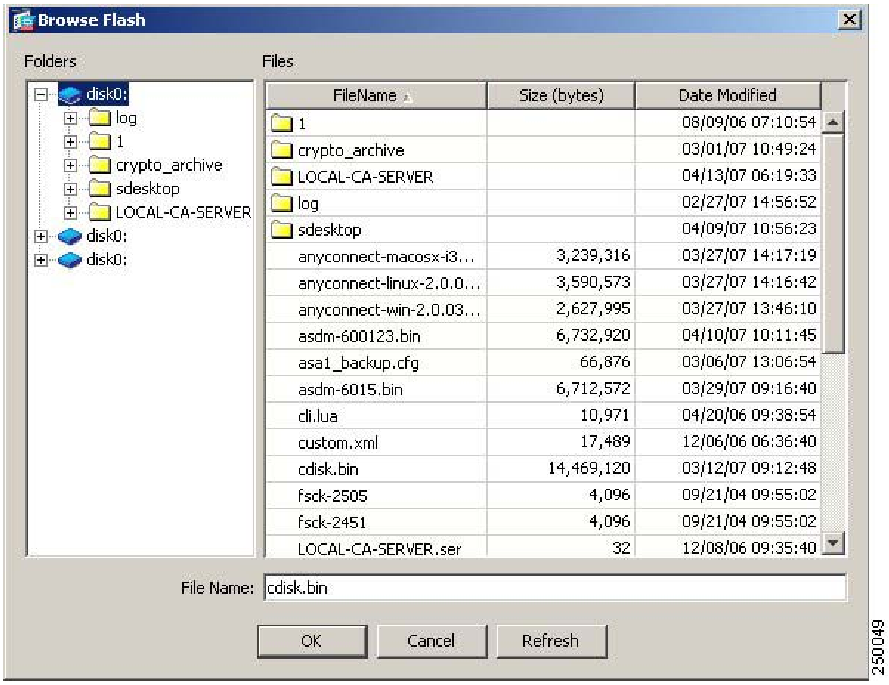
In the SSL VPN Client Profiles area, click Add or Edit. the Add or Edit SSL VPN Client Profiles dialog box appears (Figure 4-2).

Figure 4-2 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 4-3).

Figure 4-3 Browse Flash Dialog Box



FileName	Size (bytes)	Date Modified
1		08/09/06 07:10:54
crypto_archive		03/01/07 10:49:24
LOCAL-CA-SERVER		04/13/07 06:19:33
log		02/27/07 14:56:52
sdesktop		04/09/07 10:56:23
anyconnect-macosx-i3...	3,239,316	03/27/07 14:17:19
anyconnect-linux-2.0.0...	3,590,573	03/27/07 14:16:42
anyconnect-win-2.0.03...	2,627,995	03/27/07 13:46:10
asdm-600123.bin	6,732,920	04/10/07 10:11:45
asa1_backup.cfg	66,876	03/06/07 13:06:54
asdm-6015.bin	6,712,572	03/29/07 09:16:40
cli.lua	10,971	04/20/06 09:38:54
custom.xml	17,489	12/06/06 06:36:40
cdisk.bin	14,469,120	03/12/07 09:12:48
fsck-2505	4,096	09/21/04 09:55:02
fsck-2451	4,096	09/21/04 09:55:02
LOCAL-CA-SERVER.ser	32	12/08/06 09:35:40

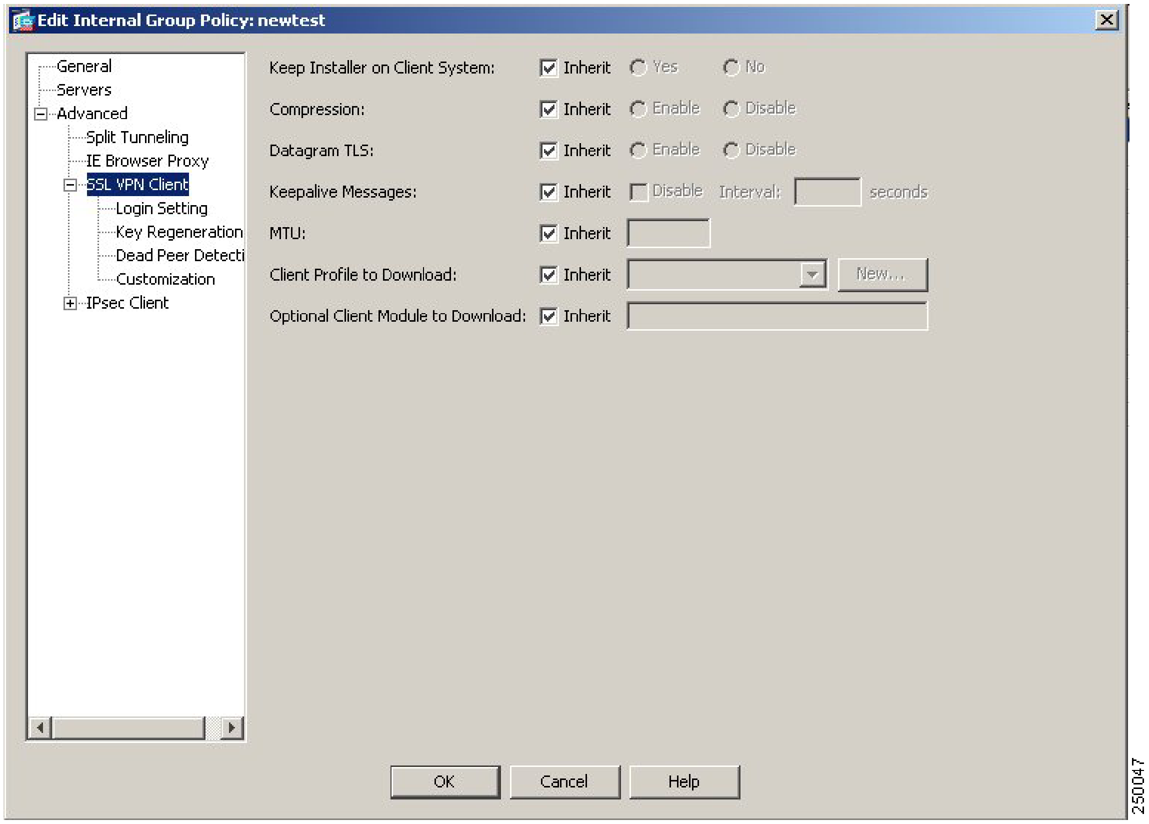
File Name: cdisk.bin

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 4 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 4-4).

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



Edit Internal Group Policy: newtest

- General
- Servers
- Advanced
  - Split Tunneling
  - IE Browser Proxy
  - SSL VPN Client
    - Login Setting
    - Key Regeneration
    - Dead Peer Detecti
    - Customization
  - IPsec Client

Keep Installer on Client System: ☑ Inherit ○ Yes ○ No

Compression: ☑ Inherit ○ Enable ○ Disable

Datagram TLS: ☑ Inherit ○ Enable ○ Disable

Keepalive Messages: ☑ Inherit □ Disable Interval: seconds

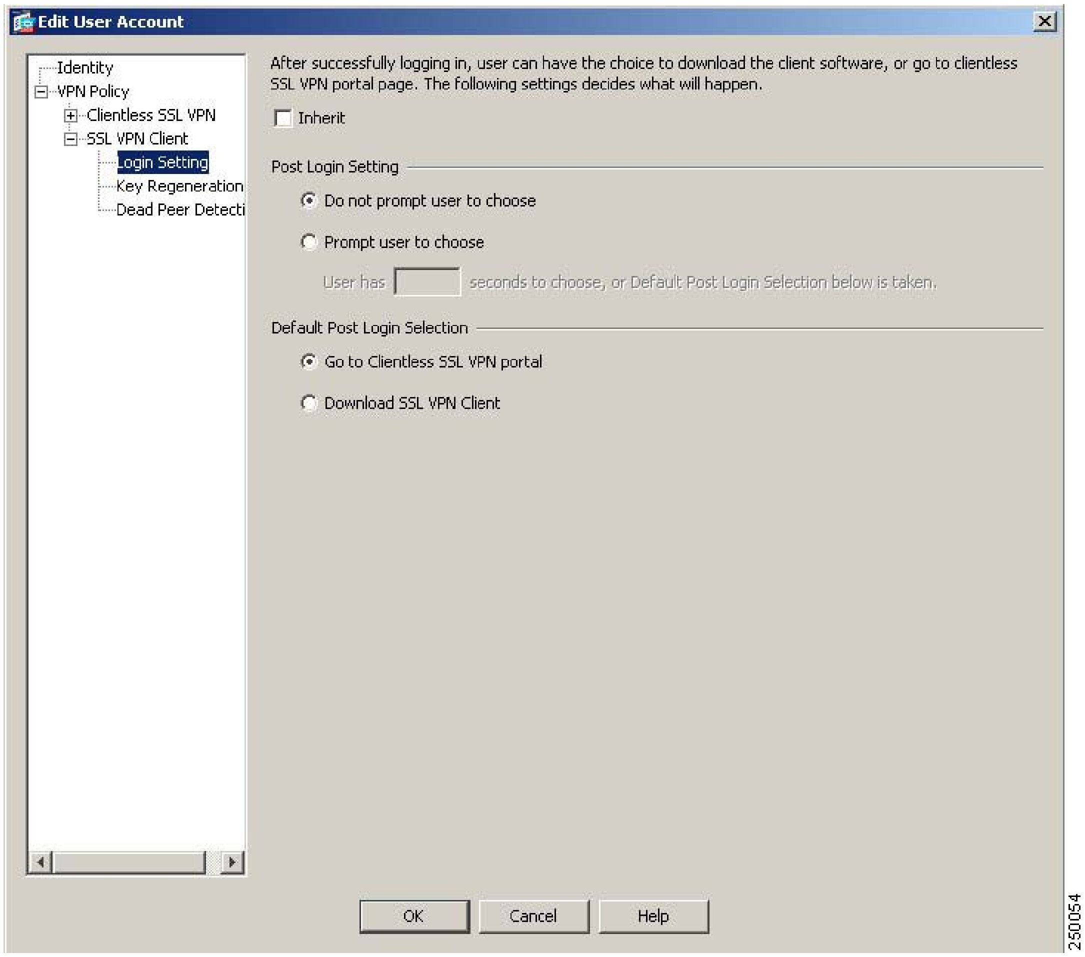
MTU: ☑ Inherit

Client Profile to Download: ☑ Inherit New...

Optional Client Module to Download: ☑ Inherit

Step 5 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. 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 4-5). In the navigation pane, select VPN Policy > SSL VPN Client >Login Setting.

Figure 4-5 Add or Edit User Account Dialog Box (Username)



After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN portal page. The following settings decides what will happen.

□ Inherit

Post Login Setting

● Do not prompt user to choose

○ Prompt user to choose

User has [ ] seconds to choose, or Default Post Login Selection below is taken.

Default Post Login Selection

● Go to Clientless SSL VPN portal

○ Download SSL VPN Client

Step 6 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 4-2 on page 4-8) appears; follow the procedures that pertain to that figure.

Step 7 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.

Validating the XML Profile

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. This.xsd file is the XML schema definition for the Cisco AnyConnect VPN Client Profile XML file. This file 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.

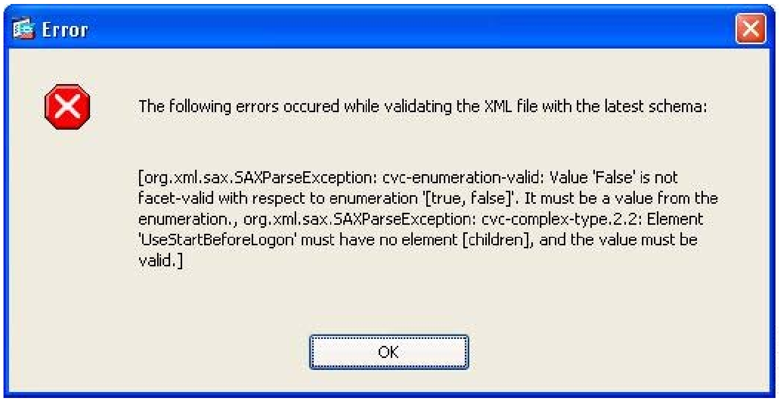
The XML file based on this schema can be distributed to clients at any time, either as a bundled file with the software distribution or as part of the automatic download mechanism. The automatic download mechanism available only with certain Cisco Secure Gateway products. See Appendix A, "Sample AnyConnect Profile and XML Schema" for a hard copy of these files.

For Windows Vista, Windows XP, and Windows 2000 systems 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 Vista and is available for download from Microsoft for Windows XP and Windows 2000 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 that the capitalization matches that in the element 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:



The following errors occured while validating the XML file with the latest schema:

[org.xml.sax.SAXParseException: cvc-enumeration-valid: Value 'False' is not facet-valid with respect to enumeration '[true, false]'. It must be a value from the enumeration., org.xml.sax.SAXParseException: cvc-complex-type.2.2: Element 'UseStartBeforeLogon' must have no element [children], and the value must be valid.]

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

Sample AnyConnect Profile

The following example shows a sample AnyConnect Profile XML file. User-supplied values appear in **bold** type. 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>
    <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>

    <CertificateMatch>
        <KeyUsage>
            <MatchKey>Non_Repudiation</MatchKey>
            <MatchKey>Digital_Signature</MatchKey>
        </KeyUsage>
        <ExtendedKeyUsage>
            <ExtendedMatchKey>ClientAuth</ExtendedMatchKey>
            <ExtendedMatchKey>ServerAuth</ExtendedMatchKey>
            <CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11</CustomExtendedMatchKey>
        </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>10.94.146.172</HostAddress>
        <UserGroup>StandardUser</UserGroup>
        <BackupServerList>
            <HostAddress>cvc-asa-03.cisco.com</HostAddress>
            <HostAddress>10.94.146.173</HostAddress>
            </BackupServerList>
    </HostEntry>
</ServerList>

</AnyConnectProfile>
```

The following sections describe, group by group, each of the AnyConnect Profile Attributes:

- Configuring Client Initialization Attributes, page 4-13
- Configuring the Certificate Match Attributes, page 4-15
- Configuring Backup Server List Parameters, page 4-22
- Configuring Windows Mobile Policy, page 4-22
- Configuring the ServerList Attributes, page 4-24
- Enabling Start Before Logon (SBL) for the AnyConnect Client, page 4-27

These sections summarize the parameters, their possible values, and examples of use.

Configuring Client Initialization Attributes

The VPN Client Initialization section is a repository of information used to manage the Cisco AnyConnect VPN client software. The ClientInitialization section of the AnyConnectProfile file represents global settings for the AnyConnect client. In some cases, for example, BackupServerList, host-specific overrides are possible.

The following example shows a sample of configuring the Client Initialization attributes:

```
<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>
    <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
```

Table 4-3 lists the ClientInitialization parameters. In this table, default values appear in **bold** type.

Table 4-3 ClientInitialization Parameters

Preference Name	Preference Available by Default?[1]	Possible Values (Default appears in bold)[2,3]	User Control Allowed?[4]	Default User Control[5]	OS[6]
UseStartBeforeLogon	false	**true**, false	yes	true	Windows, except Mobile
ShowPreConnectMessage	false	true, **false**	no	n/a	All
CertificateStore	false	**All**, Machine, User	no	n/a	All
CertificateStoreOverride	false	true, **false**	no	n/a	All
AutoConnectOnStart	true	**true**, false	yes	true	All
MinimizeOnConnect	true	**true**, false	yes	true	All
LocalLanAccess	true	true, **false**	yes	true	All
AutoReconnect	false	**true**, false	yes	false	All
AutoReconnectBehavior	false	ReconnectAfterResume **DisconnectOnSuspend**	yes	false	Windows, Mac
AutoUpdate	false	**true**, false	yes	false	all
RSASecurIDIntegration[7]	false	**Automatic**, SoftwareToken, HardwareToken	yes	false	Windows

[1] Preferences available by default are visible to the user and configurable even if there is no profile in the head end.

[2] The default value of a preference is used when its value is not defined in the profile.

[3] The value of a preference is defined in between the preference tags; for example, <AutoUpdate>true</AutoUpdate>.

[4] Preferences that do not allow user control cannot be made UserControllable; that is, even if they are defined as UserControllable=”true” in the profile, this is ignored and the default values are used.

[5] The user controllable attribute is defined inside the preference tags; for example, <AutoUpdate UserControllable=”true”>true</AutoUpdate>. 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.

[6] OS that supports these preferences.

[7] The AnyConnect client is compatible with RSA SecurID software versions 1.1 and higher. At the time of the AnyConnect 2.3 release, RSA SecurID Software Token Client software does not support Windows Vista and 64-bit systems.

Note AutoReconnect is a special type of preference, as it has a child preference. This is configured in the profile as follows:

```
<AutoReconnect UserControllable=“true”>true
    <AutoReconnectBehavior UserControllable=“true”>
     ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

XML Profile Enhancement for Selecting Windows Certificate Store

In the AnyConnect client Release 2.3 and later, administrators can control which certificate store AnyConnect uses for locating certificates. This applies only to the AnyConnect client on Windows.

Windows provides separate certificate stores for the local machine and for the current user. Users with administrative privileges on the computer will have access to both stores. The original AnyConnect behavior was to load certificates from all available certificate stores. An ASA administrator may want to configure AnyConnect via XML profile to restrict certificate lookups to only the user store or only the machine store.

To this end, a new setting called CertificateStore has been added to the ClientInitialization element in the XML profile. It has three possible (case-sensitive) values: All (default), Machine, or User.

Note The default setting (All) is appropriate for the majority of cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.

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

Within the ClientInitialization section of the XML template, you can specify the certificate store that you want to use. Possible values are as follows:

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

Note These attributes are case-sensitive.

Certificate Store Example

The following example shows how to set the CertificateStore attribute within the ClientInitialization element that you can use to change client certificate selection to use a machine certificate:

This setting lets an administrator specify the certificate store that AnyConnect uses for locating certificates. This setting applies only to the Microsoft Windows version of the AnyConnect client and has no effect on other platforms.

```
<CertificateStore>Machine</CertificateStore>
```

This setting lets an administrator direct the AnyConnect client to search for certificates in the Windows machine certificate store. This is useful in cases where certificates are located in this store and users do not have administrator privileges on their machine.

Configuring the Certificate Match Attributes

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 4-18 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 4-4 lists the well known set of constraints with their corresponding object identifiers (OIDs).

Table 4-4 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 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 4-5 lists the supported criteria:

Table 4-5 Criteria for Certificate Distinguished Name Mapping

Identifier	Description
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
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 Appendix A, “Sample AnyConnect Profile and XML Schema,” for an example.

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>ASASecurity</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 4-6 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 4-6 Certificate Match Parameters

Preference 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>
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>

Table 4-6 Certificate Match Parameters (continued)

Preference Name	Possible Values	Description	Example
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 4-6 Certificate Match Parameters (continued)

Preference Name	Possible Values	Description	Example
DistinguishedNameDefinition	Bold text indicates default value. Wildcard: **“Enabled”** “Disabled” Operator: **“Equal”** or **==** “NotEqual”or !== MatchCase: **“Enabled”** “Disabled”	DistinguishedNameDefinition specifies a set of operators used to define a single Distinguished Name attribute to be used in matching. The Operator specifies the operation to use in performing the match. MatchCase specifies whether the pattern matching is case sensitive.	<DistinguishedNameDefinition Operator=”Equal” Wildcard=”Enabled” Matchcase=”Enabled”> <Name>CN</Name> <Pattern>ASASecurity</Pattern> </DistinguishedNameDefinition>
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.	

Configuring Backup Server List Parameters

Within the ClientInitialization section, the BackupServerList section is a collection of one or more backup servers to be used in case the user-selected server fails. 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 4-7 lists these parameters and defines their possible values.

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

Table 4-7 Backup Server Parameters

Name	Possible Values	Description	Examples
BackupServerList	`n/a`	Group identifier	`<BackupServerList>...</BackupServerList>`

HostAddress	`An IP address or a Full-Qualified Domain Name (FQDN)`	Specifies a host address to include in the backup server list.	`<BackupServerList>`
			`<HostAddress>tech.myco.com</HostAddress>`
			`<HostAddress>10.94.146.172</HostAddress>`
			`</BackupServerList>`

Configuring 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 version of *Release Notes for Cisco AnyConnect VPN Client* 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 4-8 shows the MobilePolicy parameters and their values.

Table 4-8 Mobile Policy Parameters

Preference Name	Possible Values	Description	Example
MobilePolicy	`n/a`	Group identifier.	`<MobilePolicy>...</MobilePolicy>`

DeviceLockRequired	n/a	Group identifier. Within the MobilePolicy group, DeviceLockRequired indicates that a Windows Mobile device must be configured with a password or PIN prior to establishing a VPN connection. This configuration is valid only on Windows Mobile devices that use the Microsoft Default Local Authentication Provider (LAP).
		Note The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, WM5AKU2+, and Windows Mobile 6.0, but not on Windows Mobile 6.1.
			`<DeviceLockRequired>`
			`MaximumTimeoutMinutes=”60”`
			`MinimumPasswordLength=”4”`
			`PasswordComplexity=”pin”`
			`</DeviceLockRequired>`

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.	`<DeviceLockRequired>`
			`MaximumTimeoutMinutes=”60”`
			`MinimumPasswordLength=”4”`
			`PasswordComplexity=”pin”`
			`</DeviceLockRequired>`

Table 4-8 Mobile Policy Parameters (continued)

Preference Name	Possible Values	Description	Example

MinimumPasswordLength	Any non-negative integer	Within the DeviceLockRequired group, when set to a non-negative number, this parameter specifies that any PIN/password used for device locking must have at least the specified number of characters.
		This setting must be pushed down to the mobile device by syncing with an Exchange server before it can be enforced. (WM5AKU2+)
			`<DeviceLockRequired>`
			`MaximumTimeoutMinutes=”60”`
			`MinimumPasswordLength=”4”`
			`PasswordComplexity=”pin”`
			`</DeviceLockRequired>`

PasswordComplexity	`"alpha"-Requires an alphanumeric password.`
	`"pin"-Requires a numeric PIN.`
	`"strong"-Requires a strong alphanumeric password, defined by Microsoft as containing at least 7 characters, including at least 3 from the set of uppercase, lowercase, numerals, and punctuation.`
		When present checks for the password subtypes listed in the column to the left.
		This setting must be pushed down to the mobile device by syncing with an Exchange server before it can be enforced. (WM5AKU2+)
			`<DeviceLockRequired>`
			`MaximumTimeoutMinutes=”60”`
			`MinimumPasswordLength=”4”`
			`PasswordComplexity=”pin”`
			`</DeviceLockRequired>`

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.

Configuring the ServerList Attributes

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 Sample AnyConnect Profile, page 4-12 for an example of the ServerList parameter in a full configuration.

Table 4-9 lists the ServerList parameters and their values. In this table the referenced preference name is in **bold** type. The values in these examples are only for demonstration purposes. Do not use them in your own configuration.

Table 4-9 Server List Parameters

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

Table 4-9 Server List Parameters (continued)

Preference 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.	`<ServerList>`
			`    <HostEntry>`
			`        `**`<HostName>ASA-01</HostName>`**
			`        <HostAddress>cvc-asa01.cisco.com`
			`        </HostAddress>`
			`    </HostEntry>`
			`    <HostEntry>`
			`        `**`<HostName>ASA-02</HostName>`**
			`        <HostAddress>cvc-asa02.cisco.com`
			`        </HostAddress>`
			`        <UserGroup>StandardUser</UserGroup>`
			`        <BackupServerList>`
			`            <HostAddress>cvc-asa03.cisco.com`
			`         </BackupServerList>`
			`    </HostEntry>`
			`</ServerList>`

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.	`<ServerList>`
			`    <HostEntry>`
			`        <HostName>ASA-01</HostName>`
			`        `**`<HostAddress>cvc-asa01.cisco.com`**
			`         `**`</HostAddress>`**
			`    </HostEntry>`
			`    <HostEntry>`
			`        <HostName>ASA-02</HostName>`
			`         `**`<HostAddress>cvc-asa02.cisco.com`**
			`         `**`</HostAddress>`**
			`        <UserGroup>StandardUser</UserGroup>`
			`        <BackupServerList>`
			`            `**`<HostAddress>cvc-asa03.cisco.com`**
			`            `**`</HostAddress>`**
			`         </BackupServerList>`
			`    </HostEntry>`
			`</ServerList>`

UserGroup	`The tunnel group to use when connecting to the specified host. This parameter is optional.`	Within the ServerList group, the UserGroup, parameter, if present, is used in conjunction with HostAddress to form a Group-based URL.
		Note Group based URL support requires ASA version 8.0.3, or later.
			`<ServerList>`
			`    <HostEntry>`
			`        <HostName>ASA-01</HostName>`
			`        <HostAddress>cvc-asa01.cisco.com`
			`         </HostAddress>`
			`    </HostEntry>`
			`    <HostEntry>`
			`        <HostName>ASA-02</HostName>`
			`         <HostAddress>cvc-asa02.cisco.com`
			`         </HostAddress>`
			`        `**`<UserGroup>StandardUser</UserGroup>`**
			`        <BackupServerList>`
			`            <HostAddress>cvc-asa03.cisco.com`
			`            </HostAddress>`
			`         </BackupServerList>`
			`    </HostEntry>`
			`</ServerList>`

The following sections describe how to modify the profiles template to configure the Start Before Logon profile attributes:

- Enabling Start Before Logon (SBL) for the AnyConnect Client, page 4-27.

- Configuring Start Before Logon (PLAP) on Windows Vista Systems, page 4-31

Enabling Start Before Logon (SBL) for the AnyConnect Client

With Start Before Logon 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.

Note 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 Active Directory. As soon as the user logs on, the login script is executed.

The point of SBL is that it connects a remote computer to the company infrastructure prior to logging on to the PC. For example, a user might be outside the physical corporate network, unable to access corporate resources until his or her PC has joined the corporate network.

With SBL enabled, the AnyConnect client connects before the user sees the Microsoft login window. The user must also log in, as usual, to Windows when the Microsoft login window appears.

The reasons that a user might want to use SBL include the following:

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

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

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

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

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

http://www.windowsnetworking.com/articles_tutorials/wxpplogs.html

In another example, a system might be configured not allow cached credentials to be used to log on to the PC. In this scenario, a 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 PC.

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.

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. For complete installation information, see *Release Notes for Cisco AnyConnect VPN Client, Release 2.2*.

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 and the Windows 2008 server. 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 Vista Systems, page 4-31.

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 AnyConnect profile to true:

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

To disable SBL, set the same value to false.

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.

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* value for SBL is **vpngina**.

In the following example, the network administrator 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 (where <profile.xml> is the name that the network administrator has assigned to the 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 2-7 (ASDM) or Enabling Modules for Additional AnyConnect Features, page 3-5 (CLI) for a description of how to do this.

Scenario: Using Start Before Logon

The following scenario walks you through the process of setting up the XML file and troubleshooting SBL using the CLI. You can also do this setup using ASDM:

Step 1 Create a profile to be pushed down to the Client PCs that looks similar to the one in Sample AnyConnect Profile, page 4-12.

Step 2 Copy the file to the FLASH on the security appliance:

```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```

Step 3 On the security appliance, add the profile as an available profile to the webvpn global section - (assuming everything else is set up correctly for AnyConnect connections):

```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```

Step 4 Edit the group policy you are using and add the 'svc modules' and 'svc profile' commands:

```
hostname(config)# group-policy GroupPolicy internal
    hostname(config)# group-policy GroupPolicy attributes
    hostname(config-group-policy)# webvpn
        hostame(config-group-webvpn)# svc modules value vpngina
        hostame(config-group-webvpn)# svc profiles value ReallyNewProfile
```

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 existing standalone 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 PC 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 client profile also is pushed down from the security appliance. The installation of VPNGINA is activated by the command **svc modules value vpngina** configured under group-policy (webvpn) command mode as explained in Step 4. 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 users connects, the client and profile are passed down to the user's PC; the client and VPNGINA are installed; and the user sees the AnyConnect client at the next reboot, prior to logging in.

A sample profile is provided on the client PC when AnyConnect is installed:

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

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.

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 Make sure the profile also appeared.

Step 7 Reboot once. On the next reboot, you should be prompted with the Start Before Logon prompt.

Step 8 Send the AnyConnect event log to Cisco in .evt format

Step 9 If you see the following error:

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

delete the user profile.

Step 10 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 Vista Systems

As on the other Windows platforms, the Start Before Logon feature enables the establishment of a VPN tunnel prior to the user's login on to the Windows system, so that users can connect to their corporate infrastructure before logging on to their PCs. Windows Vista (with Windows Server 2008), Microsoft's next-generation operating system, uses different mechanisms from Windows XP and Windows 2000 (with Windows 2003 server), so the AnyConnect client Start Before Logon feature on the Windows Vista platform uses a different mechanism well.

In the AnyConnect client, the new 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 and the Windows 2008 server. 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.

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

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.

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

Installing PLAP

The vpnplap.dll and vpnplap64.dll components are part of the existing GINA installation package, so the network administrator 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 or the Windows 2008 server, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component.

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

Once installed, PLAP is not active until the network administrator modifies the user profile <profile.xml> file to activate start before logon. See XML Settings for Enabling SBL, page 4-28. 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.

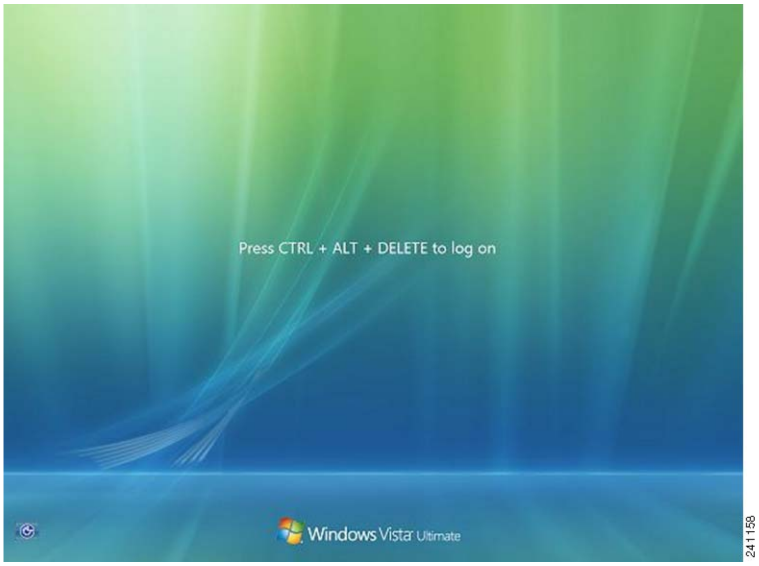
Note If the user mistakenly minimizes the user interface, he or she can restore it by pressing the Alt+Tab key combination.

Logging on to a Windows Vista PC using PLAP

To log on to Windows Vista when PLAP is enabled, do the following steps. (These steps are Microsoft requirements):

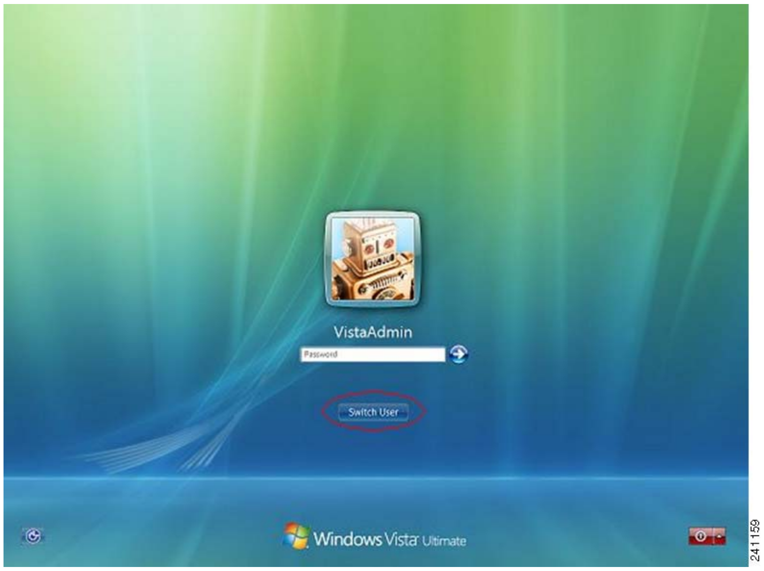
Step 1 At the Windows Vista start window, press the Ctrl+Alt+Delete key combination (Figure 4-6).

Figure 4-6 *Vista Login Window Showing the Network Connect Button*



This displays the Vista logon window with a Switch User button (Figure 4-7).

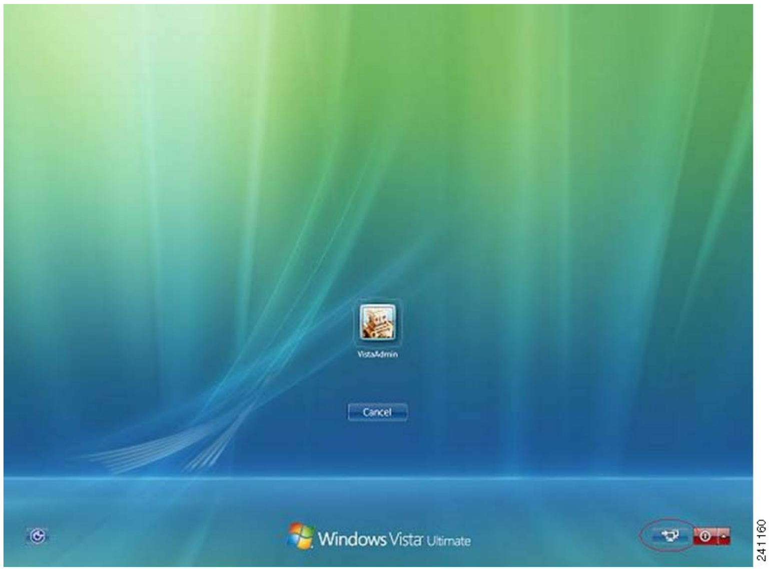
Figure 4-7 *Vista Logon Window with Switch User Button*



Step 2 Click Switch User (circled in red in this figure). This displays a Vista Network Connect window (Figure 4-8) with the network login icon in the lower-right corner. The network login icon is circled in red in Figure 4-8.

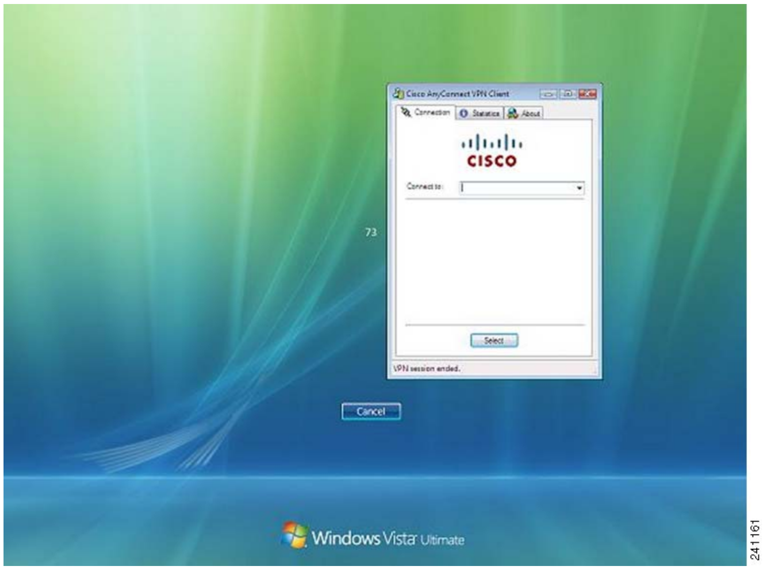
Note If the user is already connected through an AnyConnect tunnel and clicks Switch User, the first tunnel is not disconnected. If the user clicks Network Connect, then the first tunnel is disconnected. If the user clicks Cancel, the tunnel disconnects.

Figure 4-8 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 4-9).

Figure 4-9 AnyConnect Client Logon Window



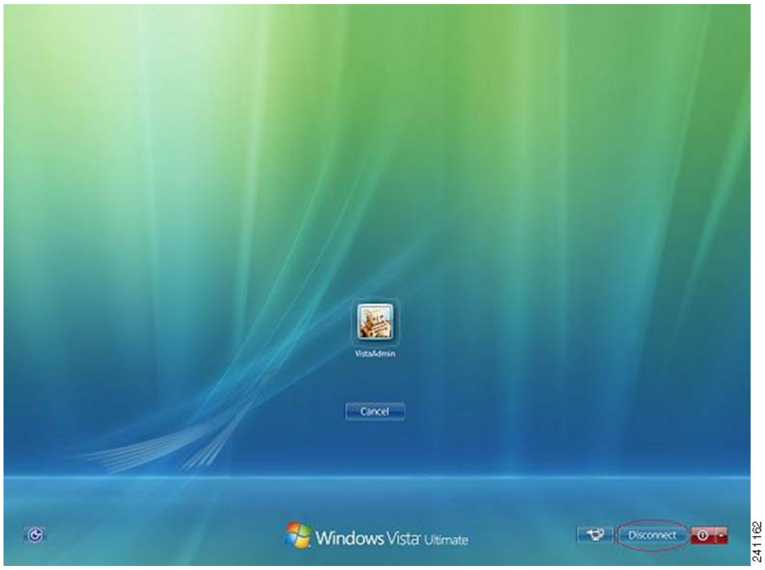
VPN session ended.

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

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

Step 5 When you have successfully connected, you see a screen similar to the Vista Network Connect window, except that it has the Microsoft Disconnect button in the lower-right corner (Figure 4-10). This is the only indication that the connection is successful.

Figure 4-10 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, you have an unlimited time in which to log on. If you forget 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 4-10).

When you click 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.