CHAPTER 2

Deploying the AnyConnect Secure Mobility Client

You can deploy the Cisco AnyConnect Secure Mobility client to remote users from the ASA or by using enterprise software management systems (SMS). These two pre-deploy or web-deploy scenarios are explained in this chapter.

The VPN tunnel is initiated by either the standalone launch, where the AnyConnect client starts the downloader process based on the VPN API components, or the web launch, where the ActiveX/Java components launch the downloader process from a clientless portal through a web browser.

This chapter contains a description of all AnyConnect package filenames:

- For Windows, we provide a standard Windows installer file (.msi) for each module. These files are installed with a Windows utility called msiexec. To reduce the file size of the installer particularly for web-deploy scenarios, we also may offer self-extracting .exe files which contain these .msi files.
- For Mac OS X, we provide disk images that contain OS X standard .pkg (or .mpkg) installers which are installed with the OS X installer utility.
- For Linux, we provide .tgz files which are GZIP compressed tar archive files. The archive contains installation files and an install script that copies files to the proper location.

In addition to the core AnyConnect VPN client that provides SSL and IPsec (IKEv2) secure VPN connections to the ASA, version 3.1 has the following modules:

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

Introduction to the AnyConnect Client Profiles

Cisco AnyConnect Secure Mobility client features are enabled in the AnyConnect profiles. These profiles contain configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, posture, telemetry, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates. Users cannot manage or modify profiles.

Profiles are created using the AnyConnect profile editors, which are GUI-based configuration tools launched from ASDM. There are also a standalone versions of the profile editors for Windows that you can use as an alternative to the profile editors integrated with ASDM. If you are predeploying the client, you can use the standalone profile editors to create profiles for the VPN service and other modules that you deploy to computers using your software management system.

Complete installation of the profile editor also provides standalone editors for Network Access Manager, Web Security, Telemetry, Customer Experience Feedback Module, and the AnyConnect client local policy.

Note Cisco recommends that you use the profile editor rather than manually editing the client profile XML files, for reasons of security.

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

Note When multiple servers are available to a connection profile, AnyConnect merges the server lists in the profiles and displays all servers in a drop-list. When the user chooses a server, AnyConnect uses the profile that server appears in. However, once connected, it uses the profile configured on that ASA.

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

During web deploy, the downloader copies the AnyConnect profiles configured on an ASA to the proper place on the end user’s device. Now during pre-deploy, you can place the profiles in specifically named directories co-located with the .msi files, and the installer automatically copies those to the proper locations when it runs.

The global file has information about user-controllable settings so that you can apply those settings before login (since there is no user). For example, the client needs to know if Start Before Logon and/or AutoConnect On Start are enabled before login. For information about filenames and paths for each operating system, see Table 2-12, Profile Locations for All Operating Systems. For more information about creating client profiles, see these sections:

- Creating and Editing an AnyConnect Client Profile Using the Integrated AnyConnect Profile Editor, page 2-2
- Using Standalone AnyConnect Profile Editor, page 2-35

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

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

The Cisco AnyConnect Secure Mobility client software package contains the profile editor, for all operating systems. ASDM activates the profile editor when you load the AnyConnect client image on the ASA.

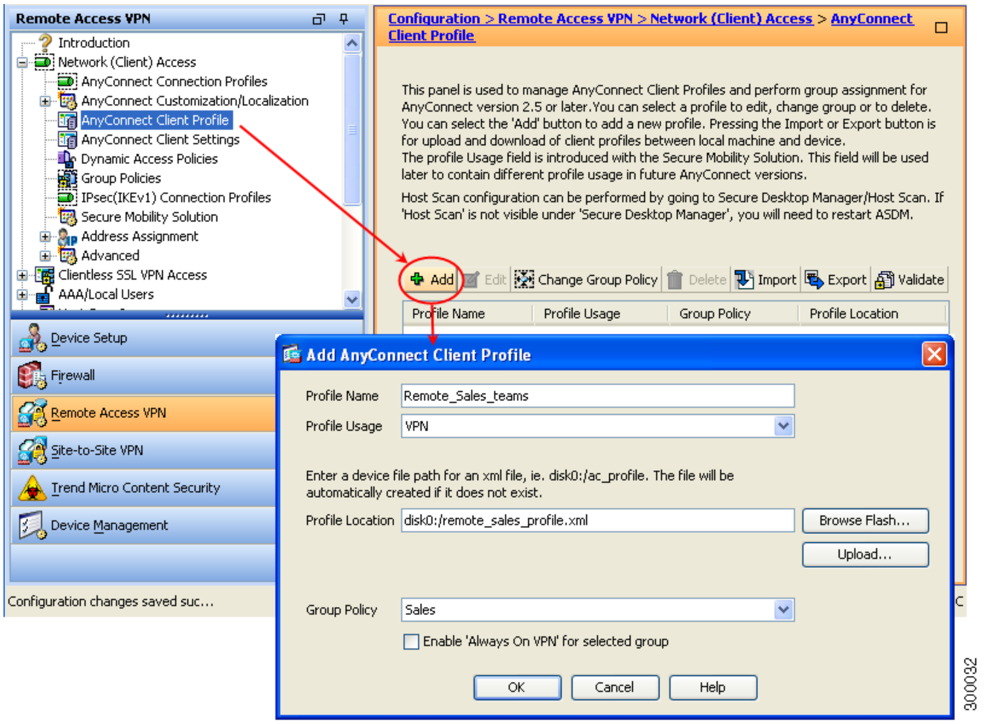
If you load multiple AnyConnect packages, ASDM activates the client profile editor from the newest AnyConnect package. This approach ensures that the editor displays the features for the newest AnyConnect loaded, as well as the older clients.

Step 1 If you have not already done so, load an AnyConnect client image on the ASA.

See Configuring the ASA to Download AnyConnect, page 2-13.

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

Figure 2-1 Adding an AnyConnect Profile



This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field will be used later to contain different profile usage in future AnyConnect versions.

Host Scan configuration can be performed by going to Secure Desktop Manager/Host Scan. If 'Host Scan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Profile Name: Remote_Sales_teams

Profile Usage: VPN

Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.

Profile Location: disk0:/remote_sales_profile.xml

Group Policy: Sales

☐ Enable 'Always On VPN' for selected group

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

Step 4 In the Profile Usage field, identify the type of client profile you are creating: AnyConnect VPN Profile, Network Access Manager Service Profile, Web Security Service Profile, Telemetry Service Profile, or Customer Experience Feedback Profile.

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

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

Step 7 Select the profile you just created from the table of profiles. Click **Edit**. The profile editor displays.

Step 8 Enable AnyConnect features in the panes of the profile editor. When you finish, click **OK**.

Step 9 Click **Apply** and then click **Save**.

Step 10 Close ASDM and relaunch it.

Deploying AnyConnect Client Profiles

- Deploying AnyConnect Client Profiles from the ASA, page 2-4
- Deploying Client Profiles Created by the Standalone Profile Editor, page 2-5

Deploying AnyConnect Client Profiles from the ASA

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

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

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

- Chapter 3, "Configuring VPN Access"

Note You must include the ASA in the VPN profile server list for the client GUI to display all user controllable settings on the first connection. Otherwise, filters are not applied. For example, if you create a certificate match and the certificate properly matches the criteria, but the ASA is not a host entry in that profile, the match is ignored. For more information, see the "Configuring a Server List" section on page 3-57.

- Chapter 4, "Configuring Network Access Manager"
- Chapter 6, "Configuring Web Security"
- Chapter 7, "Configuring AnyConnect Telemetry to the WSA"
- Chapter 8, "Using Cisco AnyConnect Customer Experience Feedback Module"
- AnyConnect Local Policy Parameters and Values in Chapter 9, "NGE, FIPS and Additional Security"

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

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

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

Step 6 Click **OK**.

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

Step 8 Click **Save**.

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

Deploying Client Profiles Created by the Standalone Profile Editor

See Using an SMS to Predeploy AnyConnect Modules, page 2-23 for instructions on deploying the client profiles you created using the standalone profile editor. See Using Standalone AnyConnect Profile Editor, page 2-35 for instructions on installing and using the Standalone AnyConnect Profile Editor.

Web Deploying AnyConnect

The Cisco AnyConnect Secure Mobility client, version 3.1, integrates modules into the AnyConnect client package. If you are using the ASA to deploy AnyConnect, the ASA can also deploy all the optional modules. In web deploy scenarios, installs and upgrades are performed automatically by the AnyConnect downloader from packages deployed on ASA headends. In this scenario, the downloader is launched by an already installed AnyConnect client (standalone) or by ActiveX/Java components (web launch).

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

- AnyConnect File Packages for ASA Deployment, page 2-7
- Ensuring Successful AnyConnect Installation, page 2-7
- Configuring the ASA to Download AnyConnect, page 2-13
- Enabling Modules for Additional Features, page 2-17
- Modifying Installer Behavior When Web Deploying, page 2-13

Requirements

Web Deployment uses code-signing for verification. The root certificate for AnyConnect's code signing certificate is issued by VeriSign, and has the Common Name of: “VeriSign Class 3 Public Primary Certification Authority - G5”.

The availability and proper configuration of this certificate varies by the client's operating system.

Windows

The Trusted Root Certification Authorities certificate store must have the VeriSign root CA certificate for AnyConnect's code signing certificate installed and trusted for software makers. This certificate is normally installed by Microsoft's operating system update, and should require no user or administrator action.

OS X

The System Keychain must have the VeriSign root CA certificate for AnyConnect's code signing certificate installed and trusted for software makers. This is normally installed by Apple's operating system update, and should not require user or administrator action.

Linux

The PEM certificate file store must have the Verisign root CA certificate installed and trusted for software makers. The VeriSign root CA certificate is stored in the PEM certificate file store when AnyConnect is installed, starting with AnyConnect version 3.0.3, and is located at /opt/.cisco/certificates/ca.

If the certificate is not in the store, then you must add it:

Step 1 Firefox is installed

Step 2 The trust settings of the VeriSign Class 3 Public Primary Certification Authority - G5 root certificate authority include trust for identifying software makers.

Modern versions of Firefox contain this VeriSign root CA certificate. After the AnyConnect client is installed, no additional user or administrator action is required. This requirement for the Firefox certificate store does not apply to pre-deploy (manual) installation of the 3.1 AnyConnect client on Linux.

If the certificate and trust are not correct, Web Deployment fails to install the client, and the AnyConnect web portal displays a link for users to manually download and install the client. Users can either edit the trust settings in their Firefox browser, and try again, or simply download the client and install it themselves. During installation, the client configures the PEM store with the VeriSign root, verifies the code signing certificate, and configures the VeriSign root. When AnyConnect launches, it uses the VeriSign root in the PEM store for code signing verification.

To set trust in Firefox for Linux web deployment

1. In the Firefox tool bar, select **Edit->Preferences.**
2. Select the **Advance** tab, then choose the **Encryption** sub-tab.
3. Choose **View Certificates**, and then select the **Authorities** tab.
4. Scroll down and select **VeriSign Class 3 Public Primary Certification Authority - G5**.
5. Click **Edit Trust**, and check **This certificate can identify software makers**.

Limitations

- If your ASA has only the default internal flash memory size or the default DRAM size (for cache memory), you could have problems storing and loading multiple AnyConnect client packages on the ASA. Even if you have enough space on flash to hold the package files, the ASA could run out of cache memory when it unzips and loads the client images. For more information about the ASA memory requirements when deploying AnyConnect, and possibly upgrading the ASA memory, see the latest release notes for the Cisco ASA 5500 Series.
- If you are upgrading legacy clients or optional modules, the following occurs:
  - All previous versions of the core client are upgraded and all VPN configurations are retained.
  - Cisco SSC 5.x is upgraded to the Network Access Manager module, retaining all SSC configurations for use with the Network Access Manager and removing SSC 5.x.
  - Host scan files used by Cisco Secure Desktop are upgraded, and the two can coexist.
  - Cisco IPsec VPN client is not upgraded or removed; however, the two can coexist.
  - ScanSafe Web Security functionality is not upgraded and cannot coexist. You must uninstall AnyWhere+.

AnyConnect File Packages for ASA Deployment

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

Table 2-1 AnyConnect Package Filenames for ASA Deployment

OS	AnyConnect 3.1 Web-Deploy Package Name Loaded onto ASA
Windows	anyconnect-win-(ver)-k9.pkg
Mac	anyconnect-macosx-i386-(ver)-k9.pkg
Linux (32-bit)	anyconnect-linux-(ver)-k9.pkg
Linux (64-bit)	anyconnect-linux-64-(ver)-k9.pkg

Ensuring Successful AnyConnect Installation

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

- Exempting AnyConnect Traffic from Network Address Translation (NAT), page 2-7
- Configuring the ASA for DES-Only SSL Encryption Not Recommended, page 2-12
- Connecting with Mobile Broadband Cards, page 2-12
- Disabling Group Policy Settings, page 2-13

Exempting AnyConnect Traffic from Network Address Translation (NAT)

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

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

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

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

Network or Address Pool	Network or address pool name	Range of addresses
Inside network	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN address pool	Engineering-VPN	10.60.60.1 - 10.60.60.254

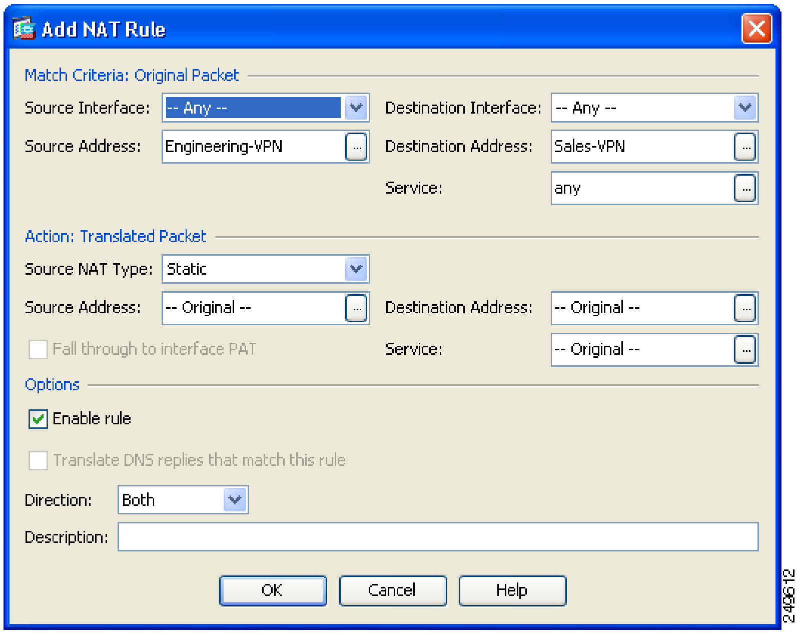
Network or Address Pool	Network or address pool name	Range of addresses
Sales VPN address pool	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ network	DMZ-network	192.168.1.0 - 192.168.1.255

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

Step 2 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach the hosts in the Sales VPN address pool. In the NAT Rules pane, select **Add > Add NAT Rule Before "Network Object" NAT rules** so that the ASA evaluates this rule before other rules in the Unified NAT table. See Figure 2-2 on page 2-8 for an example of the Add NAT rule dialog box.

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

Figure 2-2 Add NAT Rule Dialog Box



Add NAT Rule

Match Criteria: Original Packet

Source Interface: -- Any --
Destination Interface: -- Any --
Source Address: Engineering-VPN
Destination Address: Sales-VPN
Service: any

Action: Translated Packet

Source NAT Type: Static
Source Address: -- Original --
Destination Address: -- Original --
□ Fall through to interface PAT
Service: -- Original --

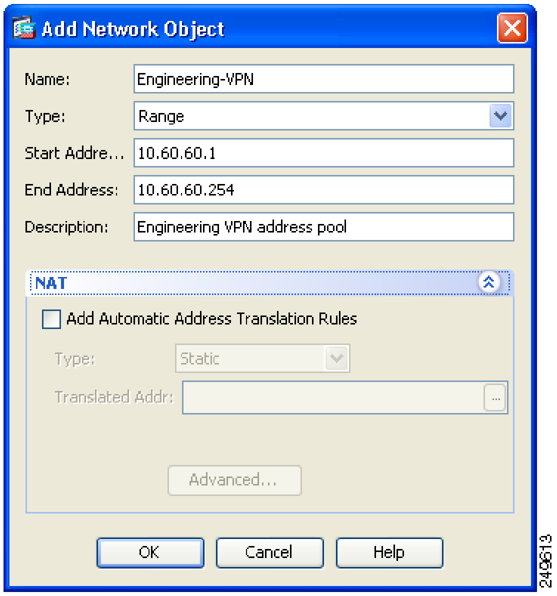
Options

☑ Enable rule
□ Translate DNS replies that match this rule
Direction: Both
Description:

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

- Source Interface: Any
- Destination Interface: Any
- Source Address: Click the Source Address browse button and create the network object that represents the Engineering VPN address pool. Define the object type as a **Range** of addresses. Do not add an automatic address translation rule. See Figure 2-3 for an example.
- Destination Address: Click the Destination Address browse button and create the network object that represents the Sales VPN address pool. Define the object type as a **Range** of addresses. Do not add an automatic address translation rule.

Figure 2-3 Create Network Object for a VPN Address Pool



Add Network Object

Name: Engineering-VPN

Type: Range

Start Addre... 10.60.60.1

End Address: 10.60.60.254

Description: Engineering VPN address pool

NAT

□ Add Automatic Address Translation Rules

Type: Static

Translated Addr:

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

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

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

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

d. Click **OK**.

e. Click **Apply**. Your rule should look like rule 1 in the Unified NAT Table in Figure 2-5 on page 2-12.

CLI example:

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

f. Click **Send**.

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

CLI example:

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

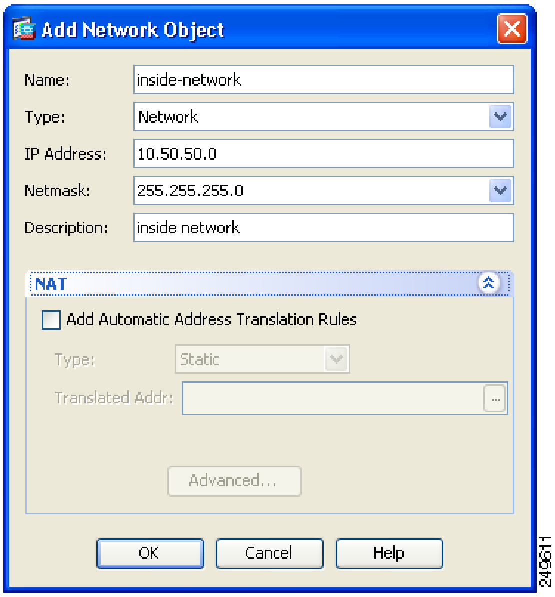
Step 4 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach other hosts in the Engineering VPN address pool. Create this rule just as you created the rule in Step 2 except that you specify the Engineering VPN address pool as both the Source address and the Destination Address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

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

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

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

Figure 2-4 Add inside-network object



Add Network Object

Name: inside-network
Type: Network
IP Address: 10.50.50.0
Netmask: 255.255.255.0
Description: inside network

NAT

□ Add Automatic Address Translation Rules
Type: Static
Translated Addr:

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

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

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

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

- Description: Add a Description for this rule.

d. Click **OK**.

e. Click **Apply**. Your rule should look like rule two in the Unified NAT Table in Figure 2-5 on page 2-12.

CLI example

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

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

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

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

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

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

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

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

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

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

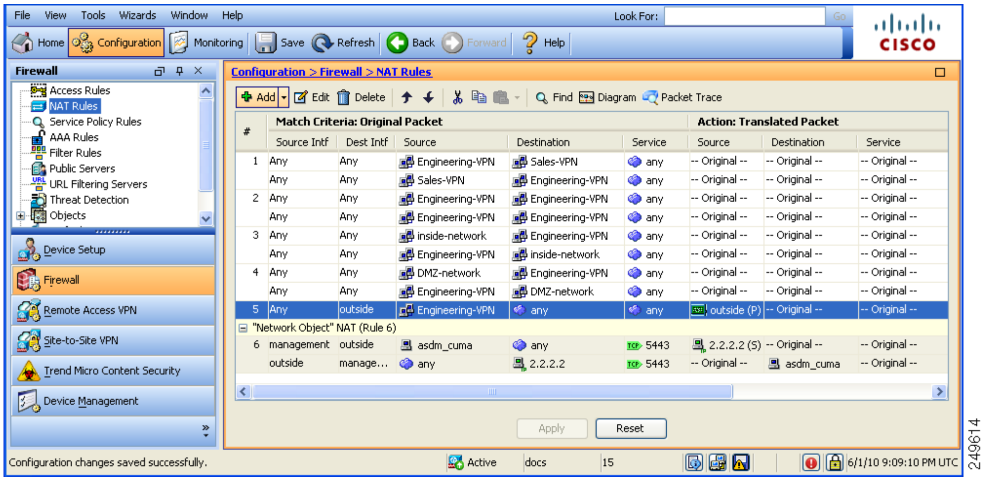
e. Click **OK**.

f. Click **Apply**. Your rule should look like rule five in the Unified NAT Table in Figure 2-5 on page 2-12.

CLI example:

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

Figure 2-5 Unified NAT Table



#	Match Criteria: Original Packet					Action: Translated Packet		
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
1	Any	Any	Engineering-VPN	Sales-VPN	any	-- Original --	-- Original --	-- Original --
	Any	Any	Sales-VPN	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
2	Any	Any	Engineering-VPN	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
	Any	Any	Engineering-VPN	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
3	Any	Any	inside-network	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
	Any	Any	Engineering-VPN	inside-network	any	-- Original --	-- Original --	-- Original --
4	Any	Any	DMZ-network	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
	Any	Any	Engineering-VPN	DMZ-network	any	-- Original --	-- Original --	-- Original --
5	Any	outside	Engineering-VPN	any	any	outside (P)	-- Original --	-- Original --
⊟ "Network Object" NAT (Rule 6)								
6	management	outside	asdm_cuma	any	5443	2.2.2.2 (S)	-- Original --	-- Original --
	outside	manage...	any	2.2.2.2	5443	-- Original --	asdm_cuma	-- Original --

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

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

Configuring the ASA for DES-Only SSL Encryption Not Recommended

By default, Windows Vista and Windows 7 do not support DES SSL encryption. If you configure DES-only on the ASA, the AnyConnect connection fails. Because configuring these operating systems for DES is difficult, we do not recommend that you configure the ASA for only DES SSL encryption.

Connecting with Mobile Broadband Cards

Some 3G or 4g cards require configuration steps before connecting to AnyConnect. For example, the Verizon Access Managers has three settings:

- modem manually connect
- modem auto connect except when roaming
- lan adapter auto connect

If you choose **lan adapter auto connect**, you can set the preference to NDIS mode. NDIS is an always on connection where you can stay connected even when the VZAccess Manager is closed. The VZAccess Manager shows an auto-connect LAN adapter as the device connection preference when it is ready for AnyConnect installation. When an AnyConnect interface is detected, the 3G manager drops the interface and allows the AnyConnect connection.

When you move to a higher priority connection, wired networks are the highest priority, followed by wi-fi, and then mobile broadband, AnyConnect will make the new connection before breaking the old one.

Disabling Group Policy Settings

When installing AnyConnect onto Windows 7 or Windows Vista, you must disable either the AlwaysInstallElevated or Windows User Account Control (UAC) group policy setting.

Modifying Installer Behavior When Web Deploying

In Windows, you can modify how the property table is interpreted by the installer utility msiexec using a transform. On the ASA, you upload transform files (.mst), and the downloader applies them to the .msi when it performs the installation (such as msiexec /package vpn.msi TRANSFORMS=hello.mst). Cisco provides sample transforms with instructions in the download area for AnyConnect.

No standard way to customize .pkg behavior is provided for Mac OS X or Linux. To allow customizations, we created an ACTtransforms.xml. which is positioned with the installer, and read when the installer runs. The file has this format:

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

For example, to disable the Customer Experience Feedback Module for Web Deployment with Linux or Mac OS X:

Step 1 Create an ACTransforms.xml file, and add the following element to it:

```
<DisableCustomerExperiencefeedback>true</DisableCustomerExperiencefeedback>
```

Step 2 In ASDM go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms.

Step 3 Upload the ACTransforms.xml file; do not change the name of the file.

Configuring the ASA to Download AnyConnect

Prerequisites

- Review the procedures in the “Ensuring Successful AnyConnect Installation” section on page 2-7 and perform the ones that are applicable to your enterprise.
- As you enable features on AnyConnect, it must update the modules on the VPN endpoints to use the new features. To minimize download time, AnyConnect requests downloads (from the ASA) only of modules that it needs for each feature that it supports. Determine which AnyConnect packages you want to deploy.

Detailed Steps

Step 1 Download the latest Cisco AnyConnect Secure Mobility client package from the Cisco AnyConnect Software Download webpage. See the “AnyConnect File Packages for ASA Deployment” section on page 2-7 for a list of AnyConnect file packages.

Step 2 Specify the Cisco AnyConnect Secure Mobility client package file as a client image. In ASDM, navigate to **Configuration > Remote Access VPN** > **Network (Client) Access > AnyConnect Client Software**. The AnyConnect Client Software panel displays listing client files identified as AnyConnect images.

Step 3 (Optional). The Customer Experience Feedback module is enabled by default. This feedback module provides us with a look at what features and modules customers use and have enabled. The collection of this client information gives us insight into the user experience so that Cisco can continue to improve the quality, reliability, performance, and user experience of AnyConnect. If you want to disable this feature, browse to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms** in ASDM, choose **Import**, and import a transform that sets the DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK property.

Step 4 To add an AnyConnect image, click **Add**.

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

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

Step 6 Click **Apply**.

Configure a Method of Address Assignment

You can use DHCP and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a connection profile. This guide uses the popular address pools method as an example.

Step 1 In ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**. Enter address pool information in the Add window.

Step 2 Navigate to Configuration > Remote Access VPN > Network (Client) Access < AnyConnect Connection Profiles and click the **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** check box.

Step 3 Under Connection Profiles, click **Edit** to assign AnyConnect the address pool in a connection profile.

Step 4 In the Edit AnyConnect Connection Profile window, select from the client or client IPV6 address pools.

Step 5 Click **Add** in the Select Address Pools window to assign address pools to the interface.

Step 6 You must specify which client is permitted as a VPN tunneling protocol for a group policy. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. The Group Policies panel displays.

Step 7 Click **Edit** and choose SSL VPN as the tunneling protocol.

Prompting Remote Users to Download AnyConnect

By default, the ASA does not download AnyConnect when the remote user initially connects using the browser. After users authenticate, the default clientless portal page displays a Start AnyConnect Client drawer that users can select to download AnyConnect. Alternatively, you can configure the ASA to immediately download AnyConnect without displaying the clientless portal page.

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

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

Step 1 In ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Select a group policy and click **Edit**. The Edit Internal Group Policy window displays.

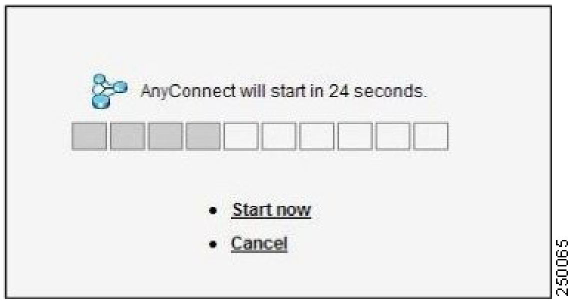
Step 2 In the navigation pane, choose **Advanced > AnyConnect Client > Login Settings**. The Post Login settings display. Uncheck the **Inherit** check box, if necessary, and select a Post Login setting.

If you choose to prompt users, specify a timeout period and select a default action to take when that period expires in the Default Post Login Selection area.

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

Figure 2-6 shows the prompt displayed to remote users if you choose **Prompt user to choose** and **Download AnyConnect Client**:

Figure 2-6 Post Login Prompt Displayed to Remote Users



AnyConnect will start in 24 seconds.

- Start now
- Cancel

Step 4 Click **Save**.

User Control Over Upgrade

You can force the user to accept a client update, or allow them to defer the update until later.

- Auto Update - When enabled on the VPN profile, forces the user to accept the update. You can also configure AutoUpdate so the user can disable it, although this could result in the client never getting any updates.

  Auto Update is described in Chapter 3, “AnyConnect VPN Profile Editor Parameter Descriptions”

- Deferred Update - When a client update is available, AnyConnect opens a dialog asking the user if they would like to update, or to defer the update.

  Deferred Update is enabled by adding all the custom attributes to the ASA, and then referencing and configuring those attributes the group policies. Deferred update is supported by all Windows, Linux and OS X.

Deferred Update Custom Attributes

The following attributes and values configure Deferred Update.

Requirements

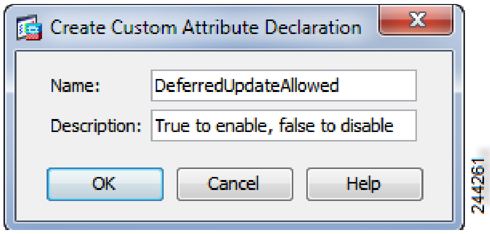
- You must add and configure all custom attributes.
- Custom attribute values are case sensitive.

Custom Attribute *	Valid Values	Default Value	Notes
DeferredUpdateAllowed	true false	false	True enables deferred update. If deferred update is disabled (false), the settings below are ignored.
DeferredUpdateMinimumVersion	x.y.z	0.0.0	Minimum version of AnyConnect that must be installed for updates to be deferrable. The minimum version check applies to all modules enabled on the headend. If any enabled module (including VPN) is not installed or does not meet the minimum version, then the connection is not eligible for deferred update. If this attribute is not specified, then a deferral prompt is displayed (or auto-dismissed) regardless of the version installed on the endpoint.
DeferredUpdateDismissTimeout	0-300 (seconds)	150 seconds	Number of seconds that the deferred upgrade prompt is displayed before being dismissed automatically. This attribute only applies when a deferred update prompt is to be displayed (the minimum version attribute is evaluated first). If this attribute is missing, then the auto-dismiss feature is disabled, and a dialog is displayed (if required) until the user responds. Setting this attribute to zero allows automatic deferral or upgrade to be forced based on: • The installed version and the value of DeferredUpdateMinimumVersion. • The value of DeferredUpdateDismissResponse.
DeferredUpdateDismissResponse	defer update	update	Action to take when DeferredUpdateDismissTimeout occurs.

Step 1 Connect to the ASDM, and select **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes**.

Step 2 Click **Add**, and create a custom attribute for Deferred Update, for example:

Figure 2-7 Adding a Custom Attribute to the ASA


Create Custom Attribute Declaration

Name: DeferredUpdateAllowed

Description: True to enable, false to disable

Step 3 Click **Apply**, and then **Save**. You may want to repeat this step to define the test of the custom attributes.

Step 4 Select **Configuration>Network(Client) Access > Group Policies**.

Step 5 To edit the group policy you want to configure for Deferred Update, select **Advanced > AnyConnect Client > Custom Attributes**.

Step 6 Click **Add**.

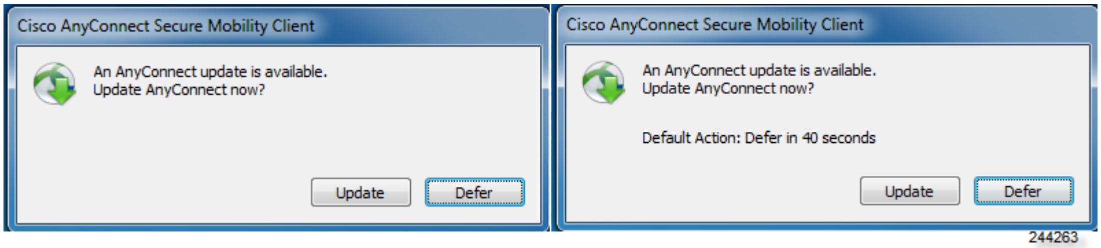
Step 7 Select **Declared Attribute Name**, choose an attribute to configure, and configure it.

Step 8 Add the rest of the Deferred Upgrade custom attributes to the policy, and configure them, using the information in Table 2-2 on page 2-17.

Deferred Update GUI

The following figure shows the UI that the user sees when an update is available, and Deferred Update is configured. The right part of the figure shows the UI when **DeferredUpdateDismissTimeout** is configured.

Figure 2-8 Deferred Update UI


Cisco AnyConnect Secure Mobility Client

An AnyConnect update is available.
Update AnyConnect now?

Cisco AnyConnect Secure Mobility Client

An AnyConnect update is available.
Update AnyConnect now?

Default Action: Defer in 40 seconds

Enabling Modules for Additional Features

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

To enable new features, you must specify the new module names as part of the group-policy or username configuration. To enable module download for a group policy, follow this procedure:

Step 1 In ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Choose a group policy and click **Edit**. The Edit Internal Group Policy window displays.

Step 2 In the navigation pane, select **Advanced > AnyConnect Client**. At **Client Profiles to Download,** click **Add** and choose the desired profiles name which displays the associated profile usage. The profile usages appear as any of the following:

- AnyConnect DART—Downloading DART allows you to collect data useful for troubleshooting AnyConnect installation and collection problems.
- AnyConnect Network Access Manager—This module provides the detection and selection of the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks.
- AnyConnect SBL—The Start Before Logon (SBL) module forces the user to connect to the enterprise infrastructure before logging on to Windows by starting AnyConnect before the Windows login dialog box appears. Refer to the "Configuring Start Before Logon" section on page 3-13 for reasons you might want to enable SBL.
- AnyConnect Web Security—Routes HTTP traffic to the ScanSafe Web Security scanning proxy server for content analysis, detection of malware, and administration of acceptable use policies.
- AnyConnect Telemetry—The telemetry module sends information about the origin of malicious content to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA).
- AnyConnect Posture—Provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host prior to creating a remote access connection to the ASA. Based on this prelogin evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance. The Host Scan application is delivered with the posture module and is the application that gathers this information.
- AnyConnect Customer Experience Feedback—This feature provides us with client information that gives us insight into the user experience statistics, the basis of crash incidents, and so on, so that software quality and user experience are further improved.

Step 3 Click **Apply** and save your changes to the group policy.

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

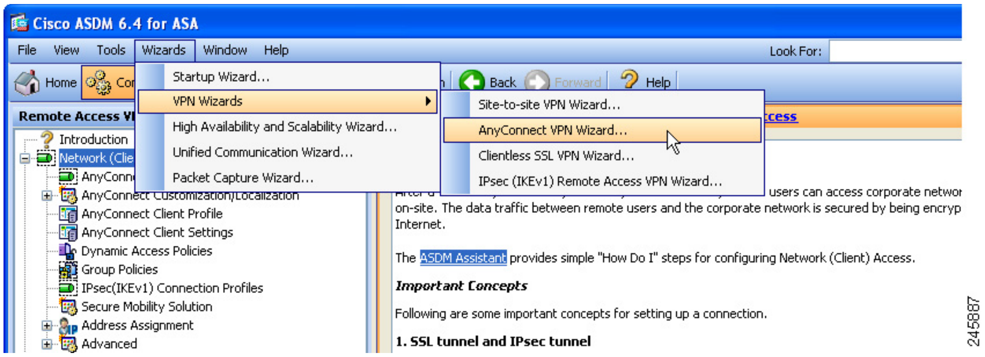
Enabling IPsec IKEv2 Connections

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

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

Step 1 Run the AnyConnect VPN Wizard. Choose **Wizards > VPN Wizards > AnyConnect VPN Wizard** (Figure 2-9). Follow the wizard steps to create a basic VPN connection for IPsec IKEv2 connections.

Figure 2-9 AnyConnect VPN Wizard



users can access corporate networ on-site. The data traffic between remote users and the corporate network is secured by being encryp Internet.

The ASDM Assistant provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

Step 3 Click **Edit** and choose **Server List** from the AnyConnect Client Profile Editor window.

Step 4 Highlight the server you want to edit, click **Edit**, and choose the primary protocol.

Step 5 Associate the VPN profile with the group policy to be used. Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Edit a group policy and navigate to **Advanced > AnyConnect Client**.

Step 6 At Client Profiles to Download, click **Add** and choose the profile usage.

Predeploying an IKEv2-Enabled Client Profile

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

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

Step 2 Browse to this folder:

anyconnect-win-3.1.0xxx-pre-deploy-k9\Profiles\vpn

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

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

Predeploying the Client Profile with a Virtual CD Mount Software

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

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

Step 2 After installing the software, deploy the profile to the appropriate folder as show in Table 2-3:

Table 2-3 Paths to Deploy the Client

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

Other Predeployment Tips

If you are using the MSI installer, the MSI picks any profile that has been placed in the client profile (Profiles\vpn folder) and places it in the appropriate folder during installation.

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

Weblaunching the Client

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

```
https://<asa>
```

Where <*asa*> is the IP address or FQDN of the ASA. If you use an IP address, use the Public IPv4 or the Global IPv6 address of the secure gateway. Use of the link-local secure gateway address is not supported.

Predeploying AnyConnect

If you use an SMS to deliver and install the AnyConnect software to the endpoint before the endpoint connects to the ASA, we refer to this as “predeployment.” If you use predeployment, you must pay special attention to the installation order and other details.

- Predeployment Package File Information, page 2-21
- Predeploying to Windows Computers, page 2-21
- Predeploying to Linux and Mac OS X Computers, page 2-28
- AnyConnect File Information, page 2-30

Limitations

If you are upgrading legacy clients or optional modules, the following occurs:

- All previous versions of the core client are upgraded and all VPN configurations are retained.
- Cisco SSC 5.x is upgraded to the Network Access Manager module, retaining all SSC configurations for use with the Network Access Manager and removing SSC 5.x.
- Host scan files used by Cisco Secure Desktop are upgraded, and the two can coexist.
- Cisco IPsec VPN client is not upgraded or removed; however, the two can coexist.

- ScanSafe Web Security functionality is not upgraded and cannot coexist. You must uninstall AnyWhere+.

Predeployment Package File Information

The core AnyConnect VPN client and the optional modules (such as SBL, AnyConnect Diagnostic Reporting Tool, and so on) are installed and updated by their own installation file or program. For AnyConnect version 3.1, Windows desktop installation files are contained in an ISO image (*.iso). For all other platforms, you can distribute the individual installation files in the same way you did for AnyConnect version 2.5 and earlier, separately at your discretion using your methodology.

OS	AnyConnect 3.1 Predeploy Package Name
Windows	anyconnect-win-<*version*>-k9.iso
Mac OS X	anyconnect-macosx-i386-<*version*>-k9.dmg
Linux (32-bit)	anyconnect-linux-<*version*>-k9.tar.gz
Linux (64-bit)	anyconnect-linux-64-<*version*>-k9.tar.gz

Predeploying to Windows Computers

The AnyConnect 3.1 predeploy installation for Windows computers (desktops, not mobile) is distributed in an ISO image. The ISO package file contains the *Install Utility*, a selector menu program to launch the individual component installers, and the MSIs for the core and optional AnyConnect modules.

The following sections describe how to predeploy to Windows computers:

- Using the ISO File, page 2-21
- Guidelines and Limitations, page 2-22
- Using the Install Utility for Predeployment, page 2-22
- Using an SMS to Predeploy AnyConnect Modules, page 2-23
- Modifying Installer Behavior During Pre-deploy, page 2-28

Using the ISO File

The predeployment package is bundled in an ISO package file that contains the programs and exec

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

If you prefer, you can break out the individual installers from the ISO image and distribute them manually. Each installer in the predeploy package can run individually. When you start the .msi installer for the AnyConnect core client, the administrator must accept an End User License Agreement (EULA). The order you deploy the files is very important. See Using an SMS to Predeploy AnyConnect Modules for more information.

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

Guidelines and Limitations

Resetting the System MTU

With a Windows installer option, you can choose to reset the MTU of all adapters. Each MSI installer supports a common property (RESET_ADAPTER_MTU) which, when set to 1, causes the installer to reset all Windows network adapter MTU settings to their default value. You must reboot for the changes to take effect. Only the VPN installer has this option. You set the command line parameter as follows: msiexec/package anyconnect-win-ver-pre-deploy-k9.msi/passive RESET_ADAPTER_MTU=1.

Turning on ActiveX Control

The AnyConnect pre-deploy VPN package previously installed the VPN WebLaunch ActiveX control by default. Starting in AnyConnect 3.1, installation of the VPN ActiveX control is turned off by default. This change was made to favor the most secure configuration as the default behavior.

When pre-deploying AnyConnect Client and Optional Modules, if you require the VPN ActiveX control to be installed with AnyConnect, you must use the NOINSTALLACTIVEX=0 option with msiexec or a transform.

Using the Install Utility for Predeployment

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

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

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

If you deploy the core client plus one or more optional modules, you must apply the lockdown property to each of the installers. This operation is one way only and cannot be removed unless you re-install the product.

This option is available for the VPN installer, Network Access Manager installer, and Web Security installer.

Using an SMS to Predeploy AnyConnect Modules

When predeploying AnyConnect modules, administrators need to copy the predeployment module to the endpoint along with its corresponding client profile, if the module requires one. For this type of predeployment, you do not need to have a VPN client installed, and some modules can run in standalone mode.

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

These modules require an AnyConnect client profile:

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

These features do not require an AnyConnect client profile:

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

The predeployment modules need to be installed in the order described in the "Using an SMS to Predeploy AnyConnect Modules" section on page 2-23.

Requirements

:When installing AnyConnect onto Windows 7 or Windows Vista, you must disable either the AlwaysInstallElevated or Windows User Account Control (UAC) group policy setting.

Detailed Steps

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

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

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

- Chapter 3, "Configuring VPN Access"
- Chapter 4, "Configuring Network Access Manager"
- Chapter 6, "Configuring Web Security"
- Chapter 7, "Configuring AnyConnect Telemetry to the WSA"
- Chapter 8, "Using Cisco AnyConnect Customer Experience Feedback Module"
- Chapter 9, "NGE, FIPS and Additional Security"

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

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

Step 5 See "Using the ISO File" section on page 2-21, to identify the packages designed for predeploying your AnyConnect modules.

Note When installing AnyConnect onto Windows 7 or Windows Vista, you must disable either the AlwaysInstallElevated or Windows User Account Control (UAC) group policy setting.

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

Step 7 Use the procedures described in "Packaging the MSI Files for Enterprise Software Deployment Systems" section on page 2-25 to install the AnyConnect modules in the order defined in the "Using an SMS to Predeploy AnyConnect Modules" section on page 2-23.

Installing AnyConnect Modules for Windows (Recommended Order)

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

If you distribute files manually, you must address the dependencies between the selected components. The core client MSI contains all VPN functional components and the common components needed for use by the optional modules. These installers check for the existence of the same version of the core client before proceeding to install.

Prerequisite

The installers for the optional modules require that the same version of AnyConnect 3.1 core client be installed. If they do not match, the optional module does not install, and the installer notifies the user of the mismatch. If you use the Install Utility, the modules in the package are built and packaged together, and the versions always match.

Detailed Steps

Step 1 Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).

Step 2 Install the AnyConnect Diagnostic and Reporting Tool (DART) module, which provides useful diagnostic information about the AnyConnect core client installation.

Step 3 Install the SBL, Network Access Manager, Web Security, or posture modules in any order.

Step 4 Install the telemetry module, which requires the posture module.

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

Uninstalling AnyConnect Modules for Windows (Recommended Order)

Detailed Steps

Step 1 Uninstall the telemetry module.

Step 2 Uninstall Network Access Manager, Web Security, Posture, or SBL, in any order.

Step 3 Uninstall the AnyConnect core client.

Step 4 Uninstall DART.

DART information is valuable should the uninstall processes fail.

Note By design, some XML files remain after uninstalling AnyConnect.

Packaging the MSI Files for Enterprise Software Deployment Systems

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

- MSI Install Command Line Calls, page 2-26
- Windows Lockdown Option, page 2-26
- Locations to Deploy the AnyConnect Profiles, page 2-33
- Hiding AnyConnect from Add/Remove Program List, page 2-27

MSI Install Command Line Calls

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

Windows Lockdown Option

Cisco recommends that end users are given limited rights on the device hosting the AnyConnect Secure Mobility client. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from switching off or stopping those Windows services established as locked down on the endpoint. It is still possible to stop the services from the command prompt with the service password.

Each MSI installer supports a common property (LOCKDOWN) which, when set to a non-zero value, prevents the Windows service(s) associated with that installer from being controlled by users or local administrators on the endpoint device. We recommend that you use the sample transform provided at the time of install to set this property and apply the transform to each MSI installer that you want to have locked down. The lockdown option is also a checkbox within the ISO Install Utility.

Hiding AnyConnect from Add/Remove Program List

You can hide the installed AnyConnect modules from users that view the Windows Add/Remove Programs list. If you launch any installer using ARPSYSTEMCOMPONENT=1, the module does not appear in the Windows Add/Remove Programs list.

We recommend that you use the sample transform we provide to set this property, applying the transform to each MSI installer for each module you want to hide.

Instructing Users to Install Network Access Manager and Web Security as Stand-Alone Applications

You can deploy the AnyConnect modules Network Access Manager and Web Security as standalone applications on a user computer using the command in the MSI Install Command Line Calls table above.

Note The client reads all the VPN client profiles. If any of the profiles has <ServiceDisable> set to true, the VPN is disabled.

Detailed Steps

Step 1 If you deploy the Install Utility to users, instruct them to check:

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

Step 2 Instruct users to uncheck Cisco AnyConnect VPN Module.

Doing so disables the VPN functionality of the core client, and the Install Utility installs Network Access Manager and Web Security as standalone applications with no VPN functionality.

Step 3 Run the installers for the optional modules, which can use the AnyConnect GUI without the VPN service.

1. A pop-up dialog box confirms the selection of the standalone Network Access Manager and/or the standalone Web Security Module.
2. When the user clicks OK, the Install Utility invokes the AnyConnect 3.1 core installer with a setting of PRE_DEPLOY_DISABLE_VPN=1.
3. The Install Utility removes any existing VPN profiles and then installs VPNDisable_ServiceProfile.xml.
4. The Install Utility invokes the Network Access Manager installer and/or the Web Security installer.
5. AnyConnect 3.1 Network Access Manager and/or Web Security Module is enabled without VPN service on the computer.

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

Modifying Installer Behavior During Pre-deploy

You can use the command line to specify installer properties and to control normal installation behavior. A command such as msiexec /package vpn.msi SOME_PROPERTY=1 passes the installer parameter to msiexec. You can pass multiple properties on the same command line.

In Windows, you can also modify how the property table is interpreted by the installer utility msiexec using a transform. On the ASA, you upload transform files (.mst), and the downloader applies them to the .msi when it performs the installation (such as msiexec /package vpn.msi TRANSFORMS=hello.mst).

Predeploying to Linux and Mac OS X Computers

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

- Modifying Installer Behavior, page 2-28
- Disabling Installation of Customer Experience Feedback Module for Mac OS X, page 2-29
- Installing Modules for Linux and Mac OS X (Recommended Order), page 2-29
- Uninstalling Modules for Linux and Mac OS X (Recommended Order), page 2-30
- Restricting Applications on System, page 2-30
- Verifying Server Certificates with Firefox, page 2-30

Modifying Installer Behavior

No standard way to customize .pkg behavior is provided for Mac OS X or Linux. To allow implementation of required customizations, we created an ACTtransforms.xml, positioned with the installer and read when the installer runs. You must place the file in a specific location relative to the installer. The installer searches in this order to see if a modification is found:

1. in a “Profile” directory in the same directory as the .pkg installer file
2. in a “Profile” directory in the root of a mounted disk image volume
3. in a “Profile” directory in the same directory as the .dmg file

The XML file has this format:

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

For example, the ACTtransforms.xml property is *DisableVPN* to create a “standalone” deployment of the Network Access Manager or Web Security.

Disabling Installation of Customer Experience Feedback Module for Mac OS X

The Customer Experience Feedback module is enabled by default. This feedback module provides us with a look at what features and modules customers use and have enabled. The collection of this client information gives us insight into the user experience so that Cisco can continue to improve the quality, reliability, performance, and user experience of AnyConnect.

To disable this feature for Mac OS X during predeployment

Step 1 Create an ACTransforms.xml file, and add the following element to it:

```
<DisableCustomerExperiencefeedback>true</DisableCustomerExperiencefeedback>
```

Step 2 Convert the dmg from read-only to read-write using Disk Utility or with the command

```
hdiutil convert anyconnect-macosx-i386-ver-k9.dmg -format UDRW -o
anyconnect-macosx-i386-ver-k9-rw.dmg.
```

Disabling Installation of Customer Experience Feedback Module for Linux

To disable the Customer Experience Feedback Module for Predeployment

Step 1 Create an ACTransforms.xml file, add the following element to it:

```
<DisableCustomerExperiencefeedback>true</DisableCustomerExperiencefeedback>
```

Step 2 Unzip the AnyConnect predeployment file, anyconnect-predeploy-<OS, version>.tar.gz.

Step 3 Create a /profile directory in the expanded directory, and add the edited ACTransforms.xml file to the /profiles directory of the predeployment installation package.

Step 4 Gzip and tar the updated installation package.

Installing Modules for Linux and Mac OS X (Recommended Order)

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

Requirement

To operate correctly with Mac OS X, AnyConnect requires a minimum display resolution of 1024 by 640 pixels.

Detailed Steps

Step 1 Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).

Step 2 Install the DART module, which provides useful diagnostic information about the AnyConnect core client installation.

Step 3 Install the posture module.

Uninstalling Modules for Linux and Mac OS X (Recommended Order)

Detailed Steps

Step 1 Uninstall the posture module.

Step 2 Uninstall the AnyConnect core client.

Step 3 Uninstall DART.

DART information is valuable should the uninstall processes fail.

Restricting Applications on System

Mac OS X 10.8 introduces a new feature called Gatekeeper that restricts which applications are allowed to run on the system. You can choose to permit applications downloaded from:

- Mac App Store
- Mac App Store and identified developers
- Anywhere

The default setting is Mac App Store and identified developers (signed applications). AnyConnect release 3.1 is a signed application, but it is not signed using an Apple certificate. This means that you must either select the Anywhere setting or use Control-click to bypass the selected setting to install and run AnyConnect from a pre-deploy installation. Users who web deploy or who already have AnyConnect installed are not impacted. For further information see:
http://www.apple.com/macosx/mountain-lion/security.html.

Verifying Server Certificates with Firefox

After you have AnyConnect installed on a Linux device and before you attempt an AnyConnect connection for the first time, open up a Firefox browser. AnyConnect uses Firefox to verify the server certificates. When you open Firefox, the profile is created, and without it, the server certificates cannot be verified as trusted.

If you opt to not use Firefox, you must configure the local policy to exclude the Firefox certificate store, which also requires configuration of the PEM store.

AnyConnect File Information

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

- Filenames of Modules on the Endpoint Computer, page 2-31
- User Preferences Files Installed on the Local Computer, page 2-35

- Locations to Deploy the AnyConnect Profiles, page 2-33

Filenames of Modules on the Endpoint Computer

Table 2-4 shows the AnyConnect filenames on the endpoint computer for each operating system type when you predeploy or ASA-deploy the client:

Table 2-4 AnyConnect Core Filenames for ASA or Predeployment

AnyConnect 3.1 Core	Web-Deploy Installer (Downloaded)	Predeploy Installer
Windows	anyconnect-win-(ver)-web-deploy-k9.exe	anyconnect-win-(ver)-pre-deploy-k9.msi
Mac	anyconnectsetup.dmg	anyconnect-macosx-i386-(ver)-k9.dmg

Linux	anyconnectsetup.sh	anyconnect-linux-(ver)-k9.tar.gz (32-bit)
		anyconnect-linux-64-(ver)-k9.tar.gz (64-bit)

Table 2-5 shows the DART filenames on the endpoint computer for each operating system type when you predeploy or ASA-deploy the client. Before release 3.0.3050, the DART component was a separate download (a .dmg, .sh, or .msi file) for web deploy. With release 3.0.3050 or later, the DART component is included in the .pkg file.

Table 2-5 DART Package Filenames for ASA or Predeployment

DART	Web-Deploy Filenames and Packages (Downloaded)	Pre-Deploy Installer
Windows	*Release 3.0.3050 or later:* anyconnect-win-(ver)-k9.pkg	anyconnect-win-(ver)-pre-deploy-k9.iso
	Before release 3.0.3050: anyconnect-dart-win-(ver)-k9.msi*	anyconnect-dart-win-(ver)-k9.msi*
Mac	*Release 3.0.3050 or later:* anyconnect-macosx-i386-(ver)-k9.pkg	anyconnect-macosx-i386-(ver)-k9.dmg
	Before release 3.0.3.050: anyconnect-dartsetup.dmg	anyconnect-dart-macosx-i386-(ver)-k9.dmg

Linux	*Release 3.0.3050 or later:*
	anyconnect-linux-(ver)-k9.pkg (32-bit)
	anyconnect-linux-64-(ver)-k9.pkg (64-bit)
		anyconnect-predeploy-linux-(ver)-k9.tar.gz (32-bit)
		anyconnect-predeploy-linux-64-(ver)-k9.tar.gz (64-bit)

	Before release 3.0.3050: anyconnect-dartsetup.sh	anyconnect-dart-linux-(ver)-k9.tar.gz

* The web-deploy and predeployment packages are contained in an ISO image (*.iso). The ISO image file contains the programs and MSI installer files to deploy to user computers.

Table 2-6 shows the SBL filenames on the endpoint computer when you predeploy or ASA-deploy the client to a Windows computer:

Table 2-6 Start Before Logon Package Filename for ASA or Predeployment

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

Table 2-7 shows the Network Access Manager filenames on the endpoint computer when you predeploy or ASA-deploy the client to a Windows computer:

Table 2-7 Network Access Manager Filename for ASA or Predeployment

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

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

Table 2-8 Posture Module Filenames for ASA or Predeployment

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

Table 2-9 shows the telemetry module filenames on the endpoint computer for Windows when you predeploy or ASA-deploy the client:

Table 2-9 Telemetry Filename for ASA or Predeployment

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

Table 2-10 shows the Web Security module filenames on the endpoint computer for Windows when you predeploy or ASA-deploy the client:

Table 2-10 Web Security Filename for ASA or Predeployment

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

Locations to Deploy the AnyConnect Profiles

Table 2-11 shows the profile-related files AnyConnect downloads on the local computer and their purpose:

Table 2-11 Profile Files on the Endpoint

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

Table 2-12 shows the locations of the AnyConnect profiles for all operating systems:

Table 2-12 Profile Locations for All Operating Systems

Operating System	Module	Location
Windows XP	Core client with VPN	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Profile
	Network Access Manager	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	Telemetry	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web Security	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
	Customer Experience Feedback	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
Windows Vista	Core client with VPN	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	Network Access Manager	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	Telemetry	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web Security	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
	Customer Experience Feedback	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
Windows 7	Core client with VPN	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	Network Access Manager	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	Telemetry	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web Security	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
	Customer Experience Feedback	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
Mac OS X	All other modules	/opt/cisco/anyconnect/profile

Operating System	Module	Location
	Customer Experience Feedback	/opt/cisco/anyconnect/CustomerExperienceFeedback
Linux	All modules	/opt/cisco/anyconnect/profile

User Preferences Files Installed on the Local Computer

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

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

Table 2-13 shows the filenames and installed paths for preferences files on the client computer:

Table 2-13 User Preferences Files and Installed Paths

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

Using Standalone AnyConnect Profile Editor

The standalone AnyConnect profile editor allows administrators to configure client profiles for the VPN, Network Access Manager, Web Security, Telemetry and Customer Experience Feedback modules for the AnyConnect Secure Mobility Client. These profiles can be distributed with predeployment kits for the VPN, Network Access Manager, Web Security, and Customer Experience Feedback modules.

System Requirements for Standalone Profile Editor

Supported Operating Systems

Standalone Profile Editor is only supported on Windows.

Java Requirement

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

Browser Requirement

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

Required Hard Drive Space

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

Installing the Standalone AnyConnect Profile Editor

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

To install the standalone profile editor, follow this procedure:

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

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

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

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

- **Typical** - Installs only the Network Access Manager profile editor automatically.
- **Custom** - Allows you to choose any of these profile editors to install: Network Access Manager Profile Editor, Web Security Profile Editor, Customer Experience Feedback Profile Editor, and VPN Profile Editor.
- **Complete** - Automatically installs the Network Access Manager Profile Editor, Web Security Profile Editor, Customer Experience Feedback Profile Editor, Telemetry, VPN Local Policy Editor, and VPN Profile Editor.

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

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

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

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

Modifying the Standalone AnyConnect Profile Editor Installation

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

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

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

Step 3 Click **Next**.

Step 4 Click **Modify**.

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

Step 6 Click **Install**.

Step 7 Click **Finish**.

Uninstalling the Standalone AnyConnect Profile Editor

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

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

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

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

Creating a Client Profile Using the Standalone Profile Editor

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

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

- Chapter 3, "Configuring VPN Access"
- Chapter 4, "Configuring Network Access Manager"
- Chapter 6, "Configuring Web Security"
- Chapter 7, "Configuring Telemetry to the WSA"
- Chapter 8, "Using Customer Experience Feedback Module"
- AnyConnect Local Policy Parameters and Values in Chapter 9, "NGE, FIPS and Additional Security"

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

Editing a Client Profile Using the Standalone Profile Editor

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

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

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

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

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