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).

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.

The Cisco AnyConnect Secure Mobility client, version 3.0, integrates new modules into the AnyConnect client package. If you are using the ASA to deploy AnyConnect, the ASA can also deploy all the optional modules. When the ASA deploys the AnyConnect client and the various modules, we refer to this as "web deployment."

If you deliver the AnyConnect software to the endpoint using an SMS and install it before the endpoint connects to the ASA, we refer to this as predeployment. You can deploy the core client that provides VPN service and the optional modules using this method, but you must pay special attention to the installation order and other details.

In addition to the core AnyConnect VPN client that provides SSL and IPsec (IKEv2) secure VPN connections to the ASA, version 3.0 has the following modules:

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

This section contains the following sections:

- Predeploying the AnyConnect Client and Optional Modules, page 2-26
- Using Standalone AnyConnect Profile Editor, page 2-40
- Configuring the ASA for WSA Support of the AnyConnect Secure Mobility Solution, page 2-46

Note 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. This limitation is especially true with the AnyConnect 3.0 client with its optional modules. 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.

Introduction to the AnyConnect Client Profiles

You enable Cisco AnyConnect Secure Mobility client features in the AnyConnect profiles—XML files that contain configuration settings for the core client with its 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.

You can configure a profile using the AnyConnect profile editor, a convenient GUI-based configuration tool launched from ASDM. The AnyConnect software package for Windows, version 2.5 and later, includes the editor, which activates when you load the AnyConnect package on the ASA and specify it as an AnyConnect client image.

We also provide a standalone version of the profile editor for Windows that you can use as an alternative to the profile editor integrated with ASDM. If you are predeploying the client, you can use the standalone profile editor to create profiles for the VPN service and other modules that you deploy to computers using your software management system.

Finally, you can manually edit the client profile XML files and import the file to the ASA as a profile.

The two versions of Cisco AnyConnect Profile Editor are different in that there is no “standalone” version of profile editor for configuring a telemetry client profile, and the editors are delivered and launched differently. In all other ways, the two versions of profile editor are the same.

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 host and depend on the host selected.

Note With multiple profiles, AnyConnect merges the server lists in the profiles and displays all servers in the drop-list on the GUI. 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.

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 2-15, 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 2-3
- Using Standalone AnyConnect Profile Editor, page 2-40

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, version 2.5 and later (all operating systems), contains the profile editor. ASDM activates the profile editor when you load the AnyConnect software package on the ASA as an SSL VPN client image.

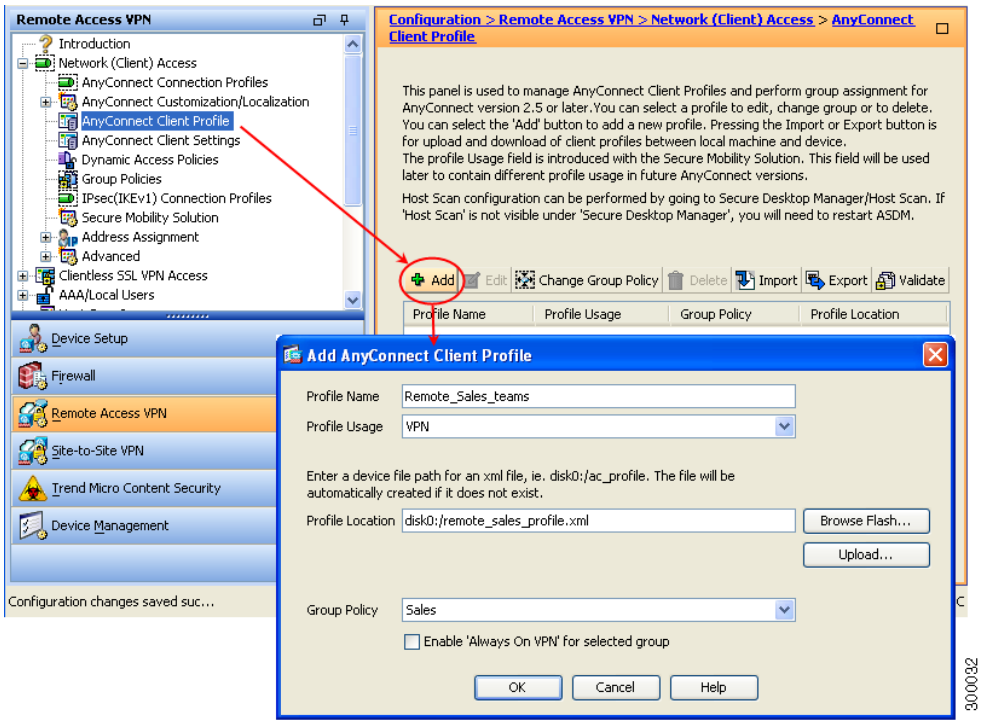
If you load multiple AnyConnect packages, ASDM loads the profile editor from the newest AnyConnect package. This approach ensures that the editor displays the features for the newest AnyConnect loaded, as well as the older clients.

To activate the profile editor in ASDM, follow these steps:

Step 1 Load the AnyConnect software package as an SSL VPN image. If you have not done this already, see Chapter 2, “Configuring the ASA to Download AnyConnect”.

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).

Figure 2-1 Adding an AnyConnect Profile



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: VPN, Network Access Manager, Web Security, or Telemetry.

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

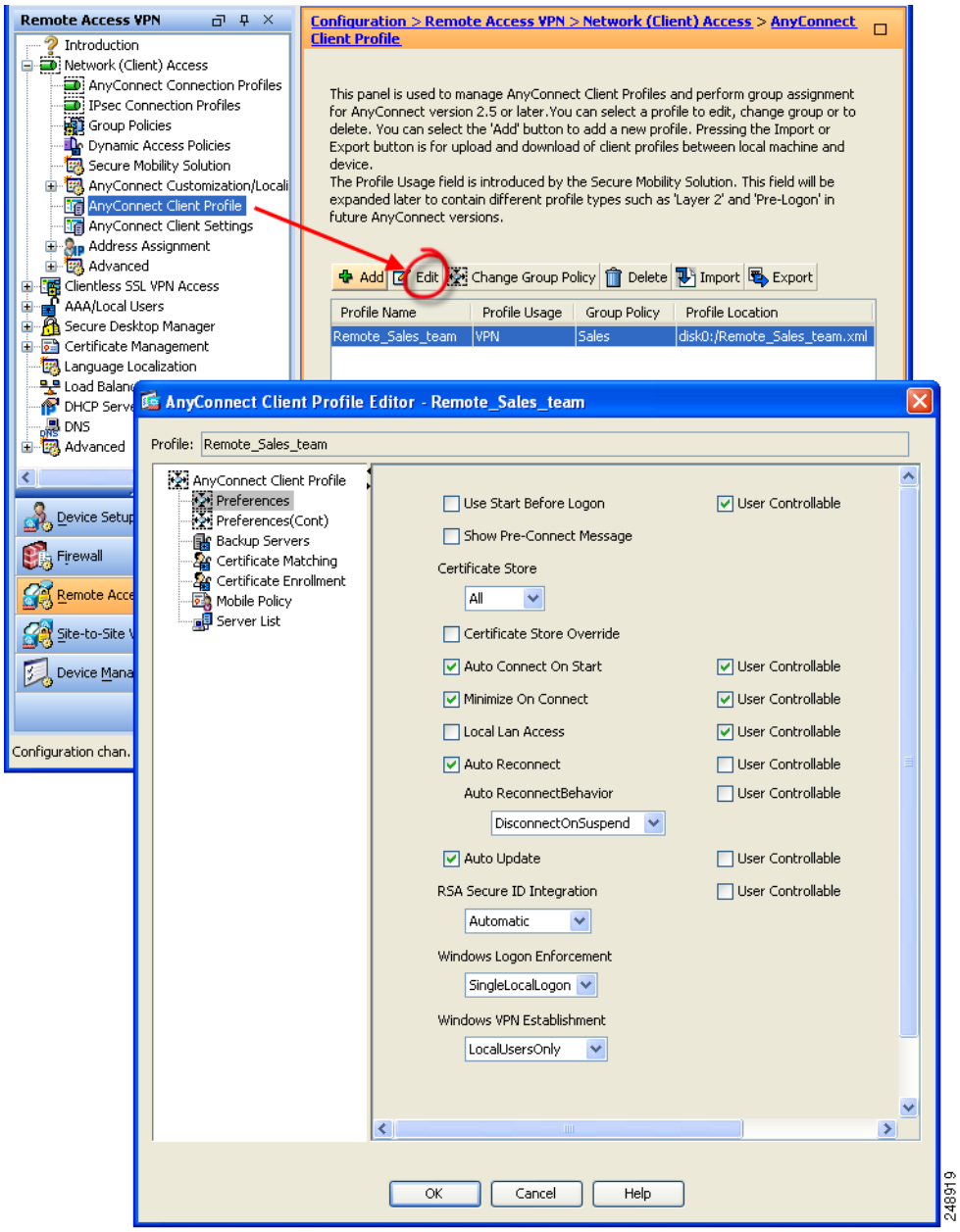
Step 6 Click **OK**. ASDM creates the profile, and the profile appears in the table of profiles.

Step 7 Select the profile you just created from the table of profiles. Click **Edit**. The profile editor displays (Figure 2-2). Enable AnyConnect features in the panes of the profile editor. When you finish, click **OK**.

Step 8 Click **Apply**.

Step 9 Close ASDM and relaunch it.

Figure 2-2 Example of Editing a VPN Client Profile



Deploying AnyConnect Client Profiles

You can deploy AnyConnect client profiles using,

- Deploying AnyConnect Client Profiles from the ASA, page 2-6
- Deploying Client Profiles Created by the Standalone Profile Editor, page 2-6

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 2-3.

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 3-51.

- Chapter 4, "Configuring Network Access Manager"
- Chapter 6, "Configuring Web Security"
- Chapter 7, "Configuring AnyConnect Telemetry to the WSA"

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 Installing Predeployed AnyConnect Modules, page 2-30 for instructions on deploying the client profiles you created using the standalone profile editor. See Using Standalone AnyConnect Profile Editor, page 2-40 for instructions on installing and using the Standalone AnyConnect Profile Editor.

Configuring the ASA to Web Deploy AnyConnect

This section addresses the following topics:

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 3.0 Web-Deploy Package Name Loaded onto ASA
Windows	anyconnect-win-(ver)-k9.pkg
Mac	anyconnect-macosx-i386-(ver)-k9.pkg
Linux	anyconnect-linux-(ver)-k9.pkg

Ensuring Successful AnyConnect Installation

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

Minimizing User Prompts about Certificates

To minimize user prompts during the AnyConnect setup, make sure certificate data on client PCs and on the ASA match:

- If you are using a Certificate Authority (CA) for certificates on the ASA, choose one that is already configured as a trusted CA on client machines.
- If you are using a self-signed certificate on the ASA, or your enterprise uses certificates generated by its own internal certificate server, be sure to install the certificate as a trusted root certificate on clients.

  The procedure varies by browser. See the procedures that follow this section.
- Certificate authorities and internal certificate servers must be reachable by the endpoint prior to the VPN being established.
- Make sure the Common Name (CN) in ASA certificates matches the name AnyConnect uses to connect to it. By default, the ASA certificate CN field is its IP address. If AnyConnect uses a DNS name, change the CN field on the ASA certificate to that name.

  If the certificate has a SAN (Subject Alternate Name), then the browser ignores the CN value in the Subject field and looks for a DNS Name entry in the SAN field.

  If users connect to the ASA using its hostname, the SAN should contain the hostname and domain name of the ASA. For example, the SAN field would contain `DNS Name=hostname.domain.com`.

  If users connect to the ASA using its IP address, the SAN should contain the IP address of the ASA. For example, the SAN field would contain `DNS Name=209.165.200.254`.

Creating a Cisco Security Agent Rule for AnyConnect

The Cisco Security Agent (CSA) might display warnings during the AnyConnect installation.

Current shipping versions of CSA do not have a built-in rule that is compatible with AnyConnect. You can create the following rule using CSA version 5.0 or later by following these steps:

Step 1 In Rule Module: “Cisco Secure Tunneling Client Module”, add a FACL:

```
Priority Allow, no Log, Description: “Cisco Secure Tunneling Browsers, read/write
vpnweb.ocx”
Applications in the following class: “Cisco Secure Tunneling Client - Controlled Web
Browsers”
Attempt: Read file, Write File
```

On any of these files: @SYSTEM\vpnweb.ocx

Step 2 To Application Class: “Cisco Secure Tunneling Client - Installation Applications,” add the following process names:

```
**\vpndownloader.exe
@program_files\**\Cisco\Cisco AnyConnect Secure Mobility Client\vpndownloader.exe
```

Adding the ASA to the Internet Explorer List of Trusted Sites for Vista and Windows 7

We recommend that Microsoft Internet Explorer (MSIE) users add the ASA to the list of trusted sites or install Java. The former enables the ActiveX control to install with minimal interaction from the user. This recommendation is particularly important for users of Windows XP SP2 with enhanced security.

For Vista and Windows 7 users, the ASA that deploys the AnyConnect client must be in the list of trusted sites on the user computer. Otherwise, WebLaunch does not occur.

Users can follow this procedure to add an ASA to their list of trusted sites in Microsoft Internet Explorer:

Note This is required on Windows Vista and Windows 7 to use WebLaunch.

Step 1 Go to **Tools > Internet Options**. The Internet Options window opens.

Step 2 Click the **Security** tab.

Step 3 Click the **Trusted Sites** icon.

Step 4 Click **Sites**. The Trusted Sites window opens.

Step 5 Type the host name or IP address of the ASA. Use a wildcard such as https://*.yourcompany.com to allow all ASA 5500s within the yourcompany.com domain to be used to support multiple sites.

Step 6 Click **Add**.

Step 7 Click **OK**. The Trusted Sites window closes.

Step 8 Click **OK** in the Internet Options window.

Adding a Security Certificate in Response to Browser Alert Windows

This section explains how to install a self-signed certificate as a trusted root certificate on a client in response to the browser alert windows.

In Response to a Microsoft Internet Explorer "Security Alert" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a Microsoft Internet Explorer Security Alert window. This window opens when you establish a Microsoft Internet Explorer connection to an ASA that is not recognized as a trusted site. The upper half of the Security Alert window shows the following text:

```
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate. The security
certificate was issued by a company you have not chosen to trust. View the certificate
to determine whether you want to trust the certifying authority.
```

Install the certificate as a trusted root certificate as follows:

Step 1 Click **View Certificate** in the Security Alert window. The Certificate window opens.

Step 2 Click **Install Certificate**. The Certificate Import Wizard Welcome opens.

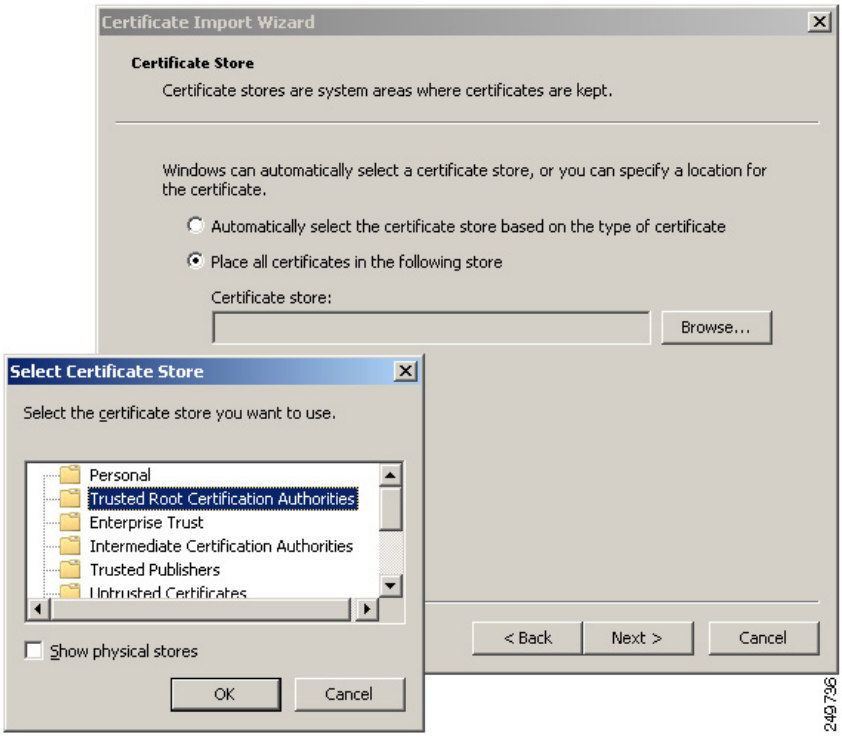
Step 3 Click **Next**. The Certificate Import Wizard – Certificate Store window opens.

Step 4 Select **Place all certificates in the following store**.

Step 5 Click **Browse**. The Select Certificate Store window opens.

Step 6 In the drop-down list, choose **Trusted Root Certification Authorities** (see Figure 2-3).

Figure 2-3 Importing a Certificate



Step 7 Click **Next**. The Certificate Import Wizard – Completing window opens.

Step 8 Click **Finish**. Another Security Warning window prompts "Do you want to install this certificate?"

Step 9 Click **Yes**. The Certificate Import Wizard window indicates the import is successful.

Step 10 Click **OK** to close this window.

Step 11 Click **OK** to close the Certificate window.

Step 12 Click **Yes** to close the Security Alert window. The ASA window opens, signifying the certificate is trusted.

In Response to a Netscape, Mozilla, or Firefox "Certified by an Unknown Authority" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a "Web Site Certified by an Unknown Authority" window. This window opens when you establish a Netscape, Mozilla, or Firefox connection to an ASA that is not recognized as a trusted site. This window shows the following text:

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

Install the certificate as a trusted root certificate as follows:

Step 1 Click **Examine Certificate** in the "Web Site Certified by an Unknown Authority" window. The Certificate Viewer window opens.

Step 2 Click the **Accept this certificate permanently** option.

Step 3 Click **OK**. The ASA window opens, signifying the certificate is trusted.

Ensuring Fast Connection Time when Loading Multiple AnyConnect Images

When you load multiple AnyConnect images on the ASA, you should order the images in a manner that ensures the fastest connection times for greatest number of remote users.

The security appliance downloads portions of the AnyConnect images to the remote computer until it achieves a match with the operating system. It downloads the image at the top of the ordered list first. Therefore, you should assign the image that matches the most commonly-encountered operating system used on remote computers to the top of the list.

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

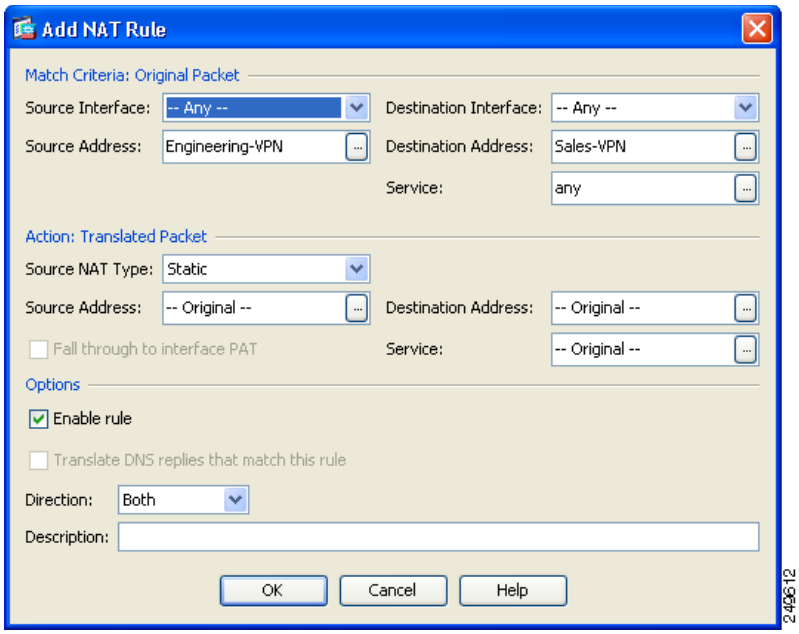
Network or Address Pool	Network or address pool name	Range of addresses
Inside network	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN address pool	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN address pool	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ network	DMZ-network	192.168.1.0 - 192.168.1.255

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 2-4 on page 2-12 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.

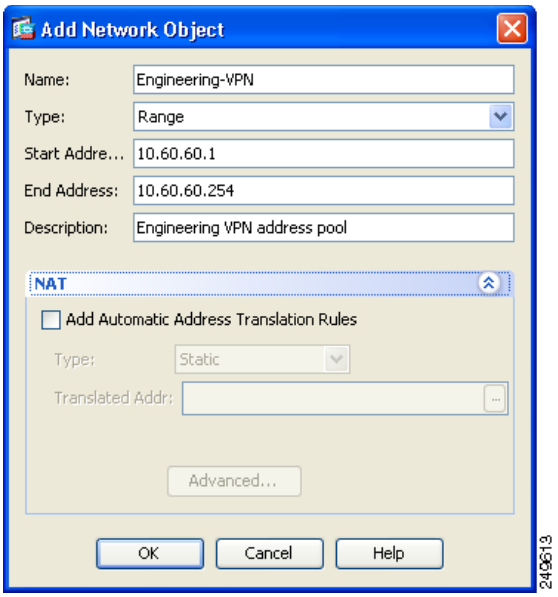
Figure 2-4 Add NAT Rule Dialog Box



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 2-5 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 2-5 Create Network Object for a VPN Address Pool



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 2-7 on page 2-16.

   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
```

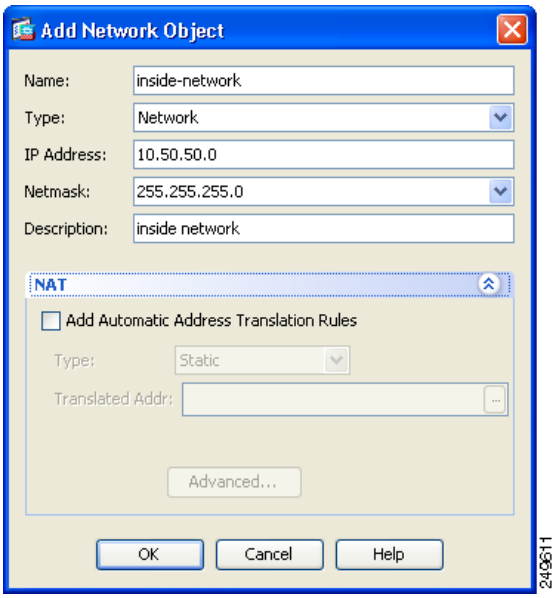
Step 4 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach other hosts in the Engineering VPN address pool. Create this rule just as you created the rule in Step 2 except that you specify the Engineering VPN address pool as both the Source address and the Destination Address 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 2-6 Add inside-network object



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 2-7 on page 2-16.

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.

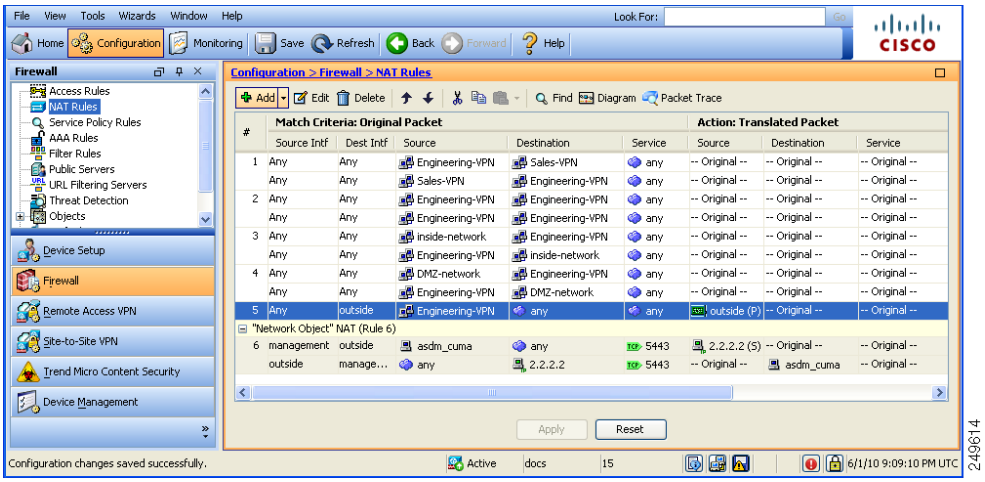
e. Click **OK**.

f. Click **Apply**. Your rule should look like rule five in the Unified NAT Table in Figure 2-7 on page 2-16.

CLI example:

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

Figure 2-7 Unified NAT Table



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 3G Cards

Some 3G 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.

Configuring the ASA to Download AnyConnect

To prepare the ASA to web deploy AnyConnect, complete these steps:

Step 1 Review the procedures in the "Ensuring Successful AnyConnect Installation" section on page 2-7 and perform the ones that are applicable to your enterprise.

Step 2 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 3 Specify the Cisco AnyConnect Secure Mobility client package file as a client image. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Settings**. The AnyConnect Client Settings panel displays, (Figure 2-8), listing client files identified as AnyConnect images. The order in which they appear reflects the order the ASA downloads them to remote computers.

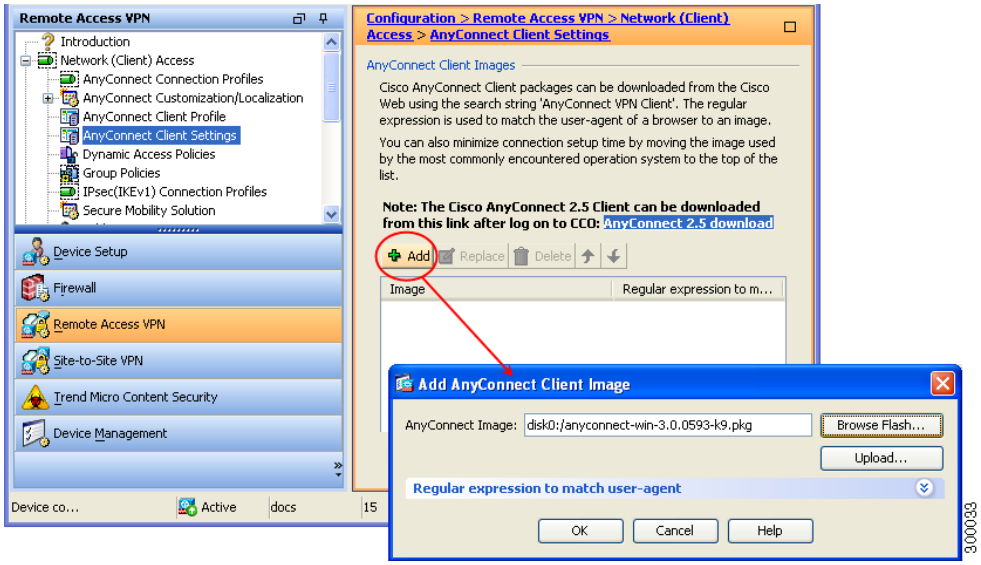
Step 4 To add an AnyConnect image, click **Add** in the AnyConnect Client Images area.

- 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**.

Figure 2-8 Specify AnyConnect Images

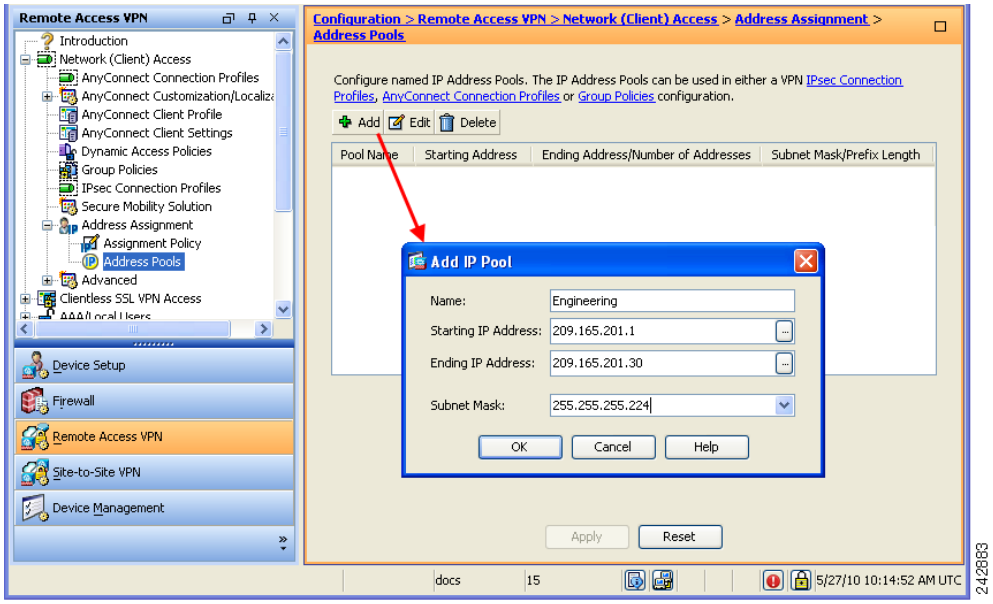


Step 7 Configure a method of address assignment.

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.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools** (Figure 2-9). Enter address pool information in the Add IP Pool window.

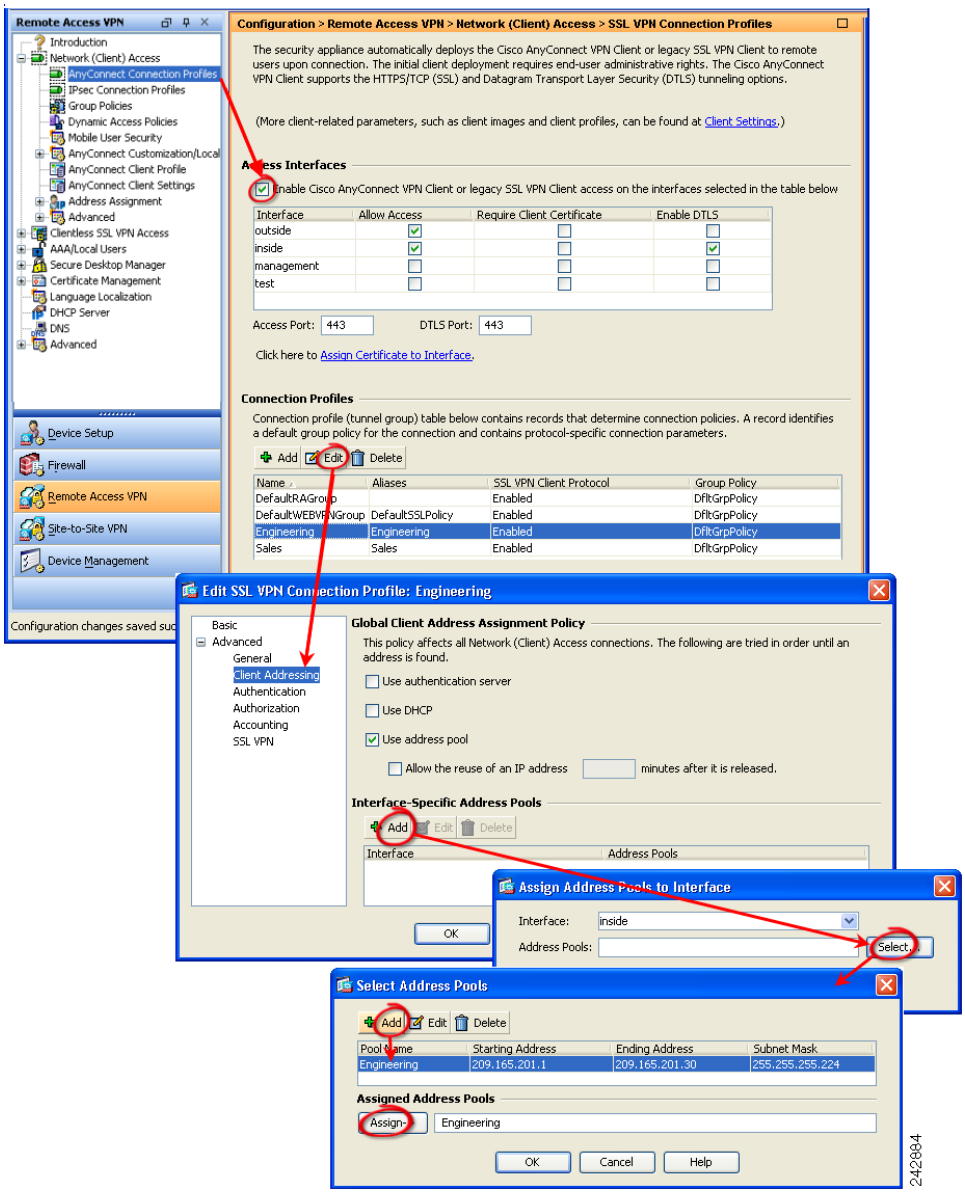
Figure 2-9 Add IP Pool Dialog



Step 8 Enable the AnyConnect download and assign the address pool in a connection profile.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. Follow the arrows in (Figure 2-10) to enable AnyConnect and then assign an address pool.

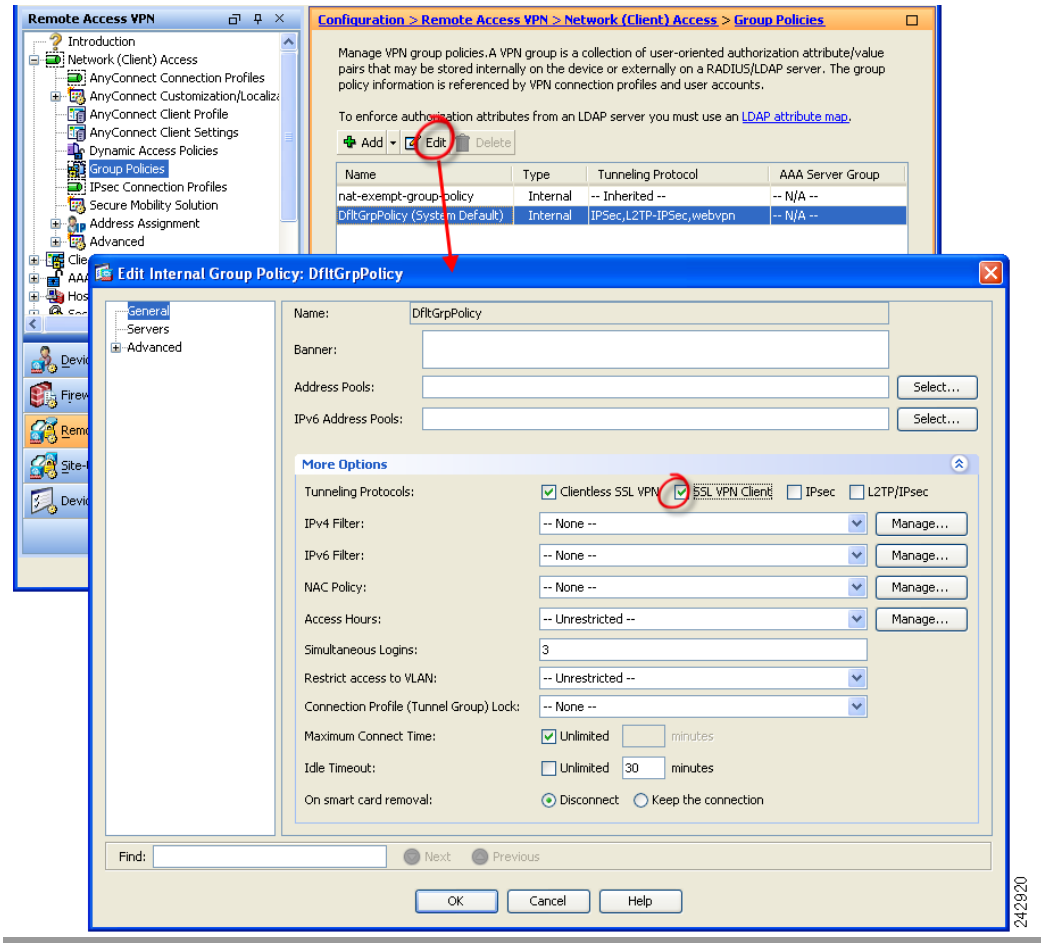
Figure 2-10 Enable AnyConnect Download



Step 9 Specify SSL VPN Client as a permitted VPN tunneling protocol for a group policy.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. The Group Policies panel displays. Follow the arrows in Figure 2-11 to enable SSL VPN Client for the group.

Figure 2-11 Specify SSL VPN as a 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.

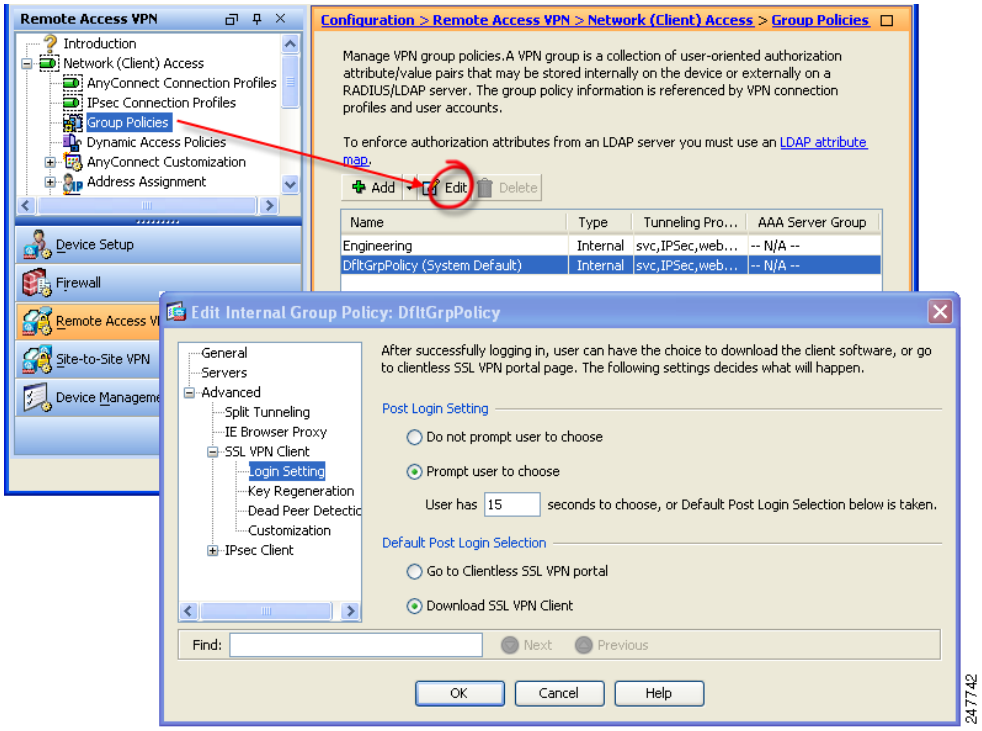
You can configure this feature for a group policy or user. To change these login settings, follow this procedure:

Step 1 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 (Figure 2-12).

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.

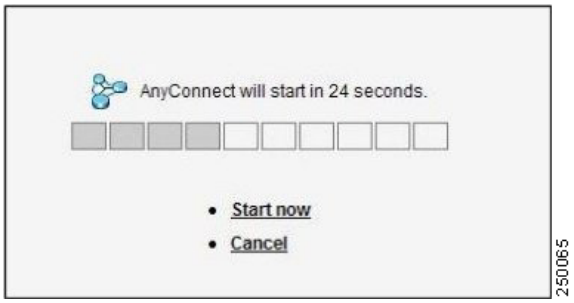
Figure 2-12 Changing Login Settings



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

Figure 2-13 shows the prompt displayed to remote users if you choose **Prompt user to choose** and **Download SSL VPN Client**:

Figure 2-13 Post Login Prompt Displayed to Remote Users



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.

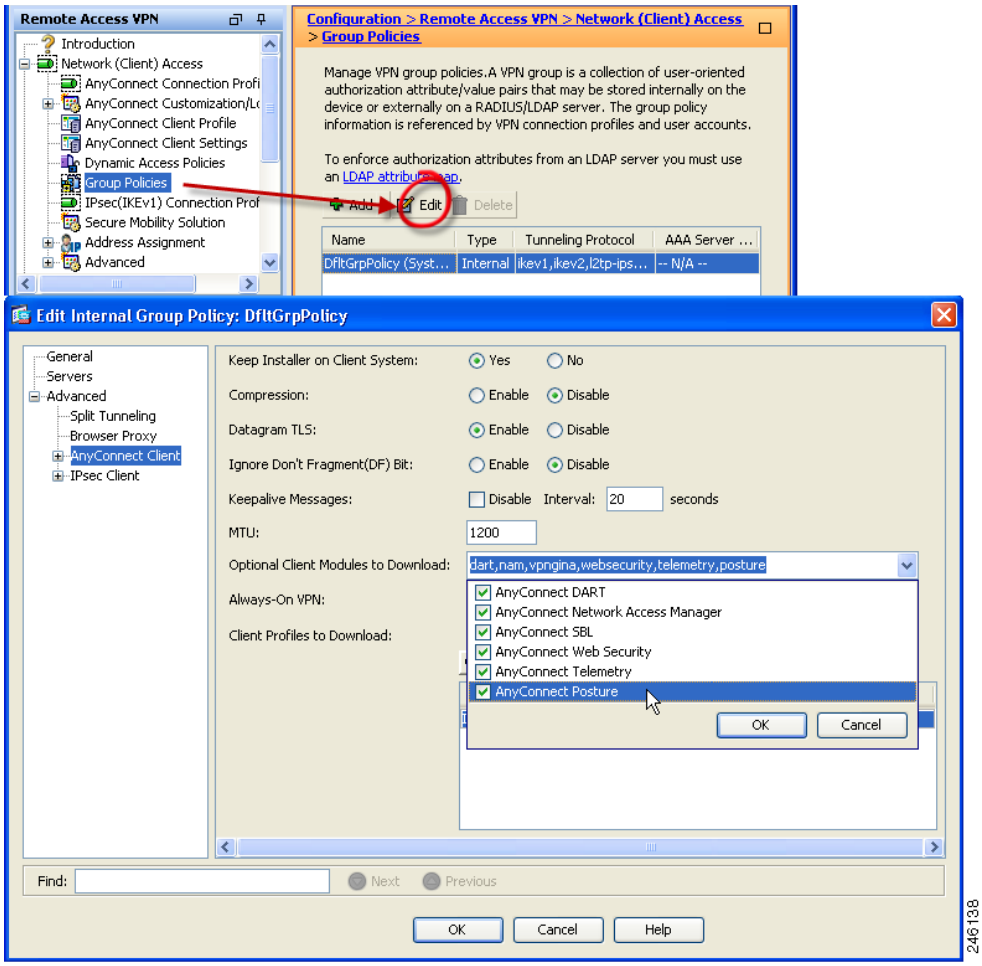
To enable new features, you must specify the new module names as part of the group-policy or username configuration. To enable module download for a group policy, follow this procedure:

Step 1 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 (Figure 2-14).

Step 2 In the navigation pane, select **Advanced > AnyConnect Client**. Click the **Optional Client Module to Download** drop-list and choose modules:

- 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 3-7 for reasons you might want to enable SBL.
- AnyConnect Web Security—Web Security is an endpoint component that routes HTTP traffic to a ScanSafe scanning proxy where the ScanSafe web scanning service evaluates it.
- 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—The posture module provides the client with the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host.

Figure 2-14 Specifying an Optional Client Module to Download



Step 3 Click **OK** and be sure to apply 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.

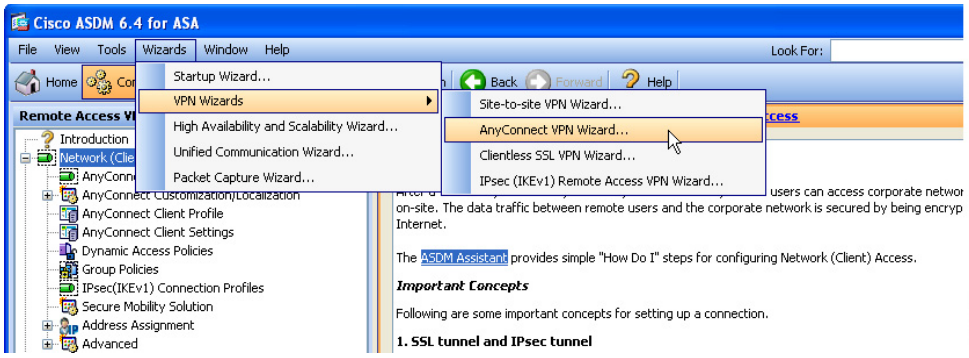
Enabling IPsec IKEv2 Connections

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:

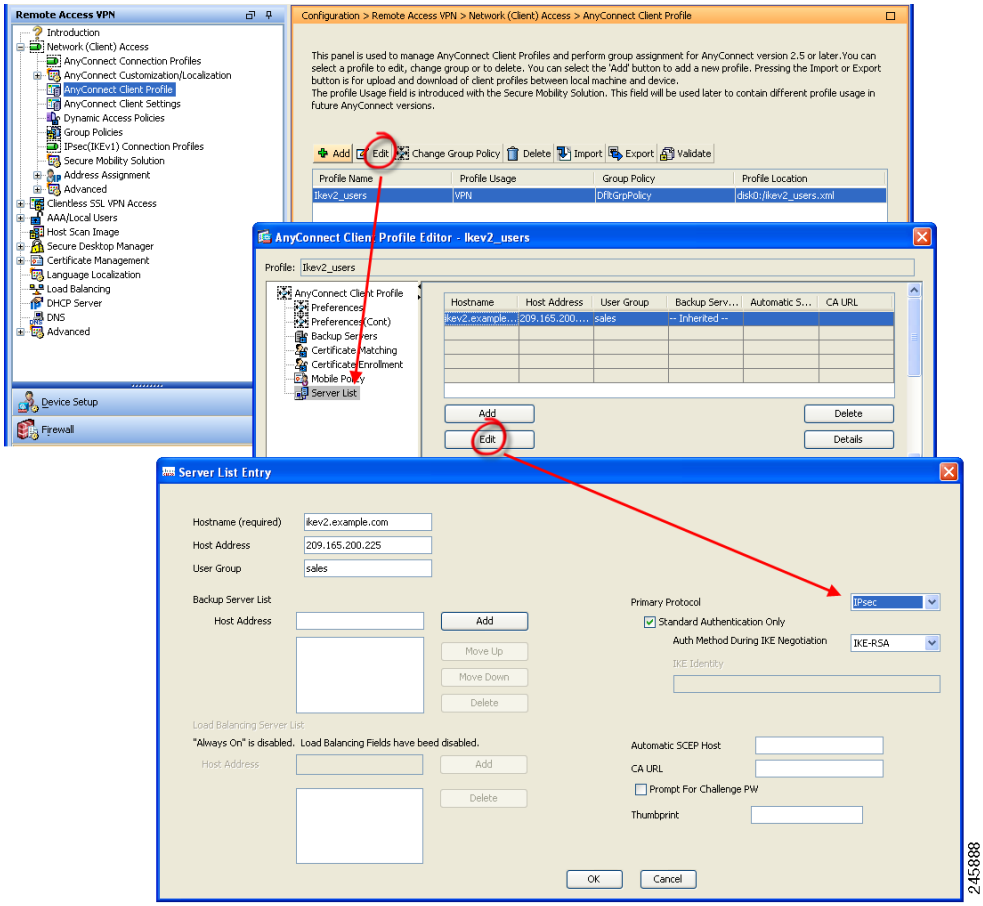
Step 1 Run the AnyConnect VPN Wizard. Choose **Tools >Wizards > AnyConnect VPN Wizard** (Figure 2-15). Follow the wizard steps to create a basic VPN connection for IPsec IKEv2 connections.

Figure 2-15 AnyConnect VPN Wizard



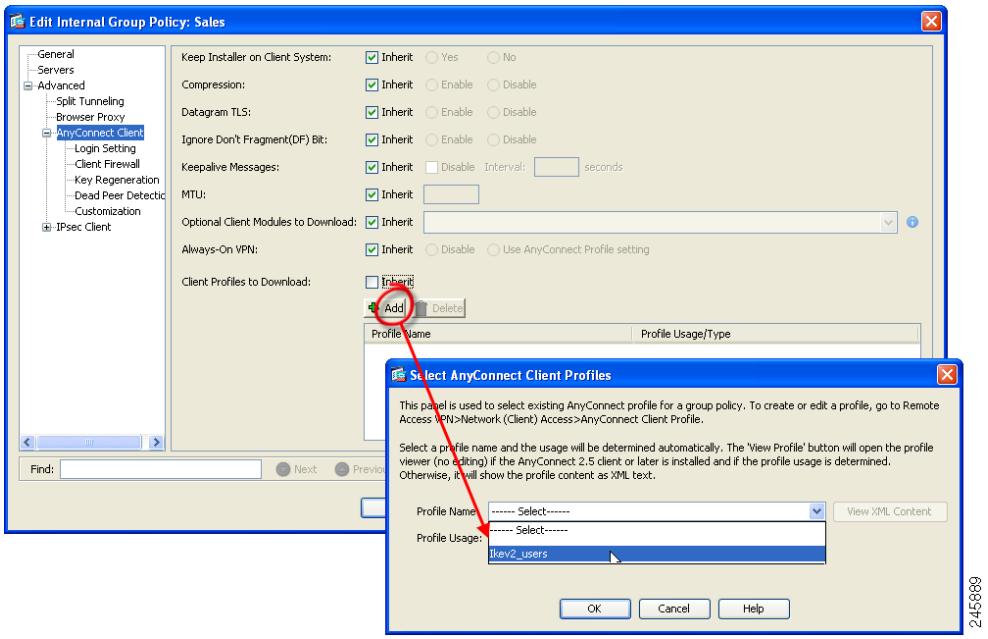
Step 2 Edit the Server List entry of the VPN profile using the profile editor. Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile** (Figure 2-16).

Figure 2-16 Specifying IKEv2 in an AnyConnect Client Profile



Step 3 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** (Figure 2-17).

Figure 2-17 Associating a Profile with a Group Policy



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-3.0.0xxx-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/

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

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>

Predeploying the AnyConnect Client and Optional Modules

This section describes the process of predeploying the AnyConnect Secure Mobility Client and includes information you need for deploying the client using enterprise software deployment systems.

The following sections describe how to predeploy the AnyConnect client:

Predeployment Package File Information

The core AnyConnect VPN client and the optional modules (such as SBL, AnyConnect Diagnostic Reporting Tool, etc.) are installed and updated by their own installation file or program. For AnyConnect version 3.0, 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.

Table 2-4 shows the filenames of the AnyConnect packages for predeployment for each OS:

Table 2-4 AnyConnect Package Filenames for Predeployment

OS	AnyConnect 3.0 Predeploy Package Name
Windows	anyconnect-win-<*version*>-k9.iso
Mac OS X	anyconnect-macosx-i386-<*version*>-k9.dmg
Linux	anyconnect-linux-<*version*>-k9.tar.gz

Predeploying to Windows Computers

The AnyConnect 3.0 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:

- Deploying the ISO File, page 2-27
- Deploying the Install Utility to Users, page 2-28
- Required Order for Installing or Uninstalling AnyConnect Modules for Windows, page 2-29
- Installing Predeployed AnyConnect Modules, page 2-30
- Instructing Users to Install Network Access Manager and Web Security as Stand-Alone Applications, page 2-32
- Packaging the MSI Files for Enterprise Software Deployment Systems, page 2-32
- Upgrading Legacy Clients and Optional Modules, page 2-34
- Customizing and Localizing the Installer, page 2-34

Deploying the ISO File

The predeployment package is bundled in an ISO package file that contains the programs and MSI 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. The order you deploy the files is very important. See Required Order for Installing or Uninstalling AnyConnect Modules for Windows for more information.

Table 2-5 lists the files contained in the ISO package file and the purpose of each file:

Table 2-5 Contents of the ISO File for Predeployment

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.

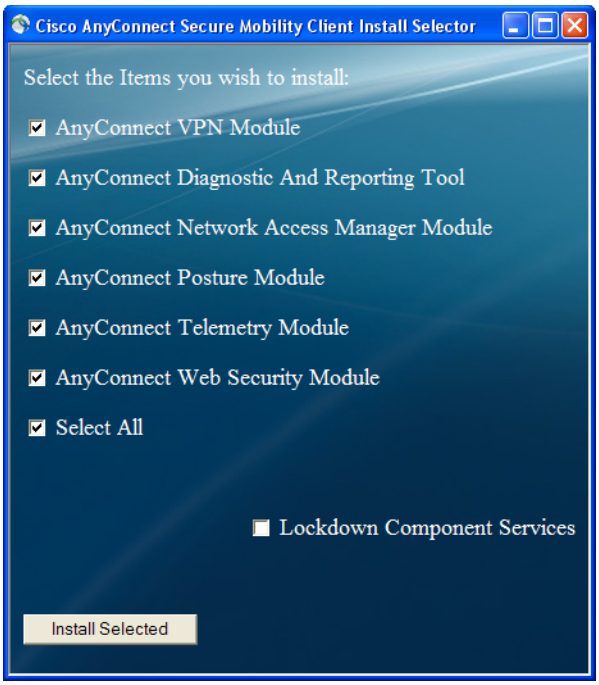
Deploying the Install Utility to Users

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.

Figure 2-18 shows the Install Utility GUI:

Figure 2-18 Install Utility GUI



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. The user must reboot the computer manually.

Required Order for Installing or Uninstalling AnyConnect Modules for Windows

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. In addition, the installers for the optional modules require that the same version of AnyConnect 3.0 core client be installed as a prerequisite. These installers check for the existence of the same version of the core client before proceeding to install.

Installing Order

The order of installation is important. Install the AnyConnect modules in the following order:

1. Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).
2. Install the AnyConnect Diagnostic and Reporting Tool (DART) module, which provides useful diagnostic information about the AnyConnect core client installation.
3. Install the SBL, Network Access Manager, Web Security, or posture modules in any order.
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 Order

The order of uninstallation is also important. Use the following order for uninstalling the modules:

1. Uninstall the telemetry module.
2. Uninstall Network Access Manager, Web Security, Posture, or SBL, in any order.
3. Uninstall the AnyConnect core client.
4. Uninstall DART last. DART information is valuable should the uninstall processes fail.

Installing Predeployed 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.

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

The predeployment modules need to be installed in the order described in the "Required Order for Installing or Uninstalling AnyConnect Modules for Windows" section on page 2-29.

To predeploy the optional AnyConnect modules along with the VPN module, follow this procedure:

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"

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 Use Table 2-5, "Contents of the ISO File for Predeployment" to identify the packages designed for predeploying your AnyConnect modules.

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 2-32 to install the AnyConnect modules in the order defined in the "Required Order for Installing or Uninstalling AnyConnect Modules for Windows" section on page 2-29.

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

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

However, also instruct them 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.

If you do not deploy the Install Utility, you must disable VPN functionality by configuring your software management system (SMS) to set the MSI property PRE_DEPLOY_DISABLE_VPN=1. For example:

```
msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx*
```

By doing this, the MSI copies the VPNDisable_ServiceProfile.xml file embedded in the MSI to the directory specified for profiles for VPN functionality (see Table 2-15 for the file path).

Note The client reads all the VPN client profiles. If ANY of the profiles has <ServiceDisable> set to true, then the VPN will be disabled.

Then you can run the installers for the optional modules, which can use the AnyConnect GUI without the VPN service.

When the user clicks the **Install Selected** button, the following happens:

Step 1 A pop-up dialog box confirms the selection of the standalone Network Access Manager and/or the standalone Web Security Module.

Step 2 When the user clicks OK, the Install Utility invokes the AnyConnect 3.0 core installer with a setting of PRE_DEPLOY_DISABLE_VPN=1.

Step 3 The Install Utility removes any existing VPN profiles and then installs VPNDisable_ServiceProfile.xml.

Step 4 The Install Utility invokes the Network Access Manager installer and/or the Web Security installer.

Step 5 AnyConnect 3.0 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.

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 2-33

- Locations to Deploy the AnyConnect Profiles, page 2-39
- Installing Network Access Manager or Web Security as Standalone Applications, page 2-33
- MSI Command to Hide AnyConnect from Add/Remove Program List, page 2-34

MSI Install Command Line Calls

Table 2-6 shows the MSI install command line calls to use to install individual AnyConnect modules. It also shows the log file produced by the command:

Table 2-6 MSI Install Command Line Calls and Log Files Generated

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
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

Installing Network Access Manager or Web Security as Standalone Applications

To install Network Access Manager and/or Web Security without VPN service, you must run the following command:

msiexec /package anyconnect-win-ver-pre-deloy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1

When the MSI for the core client runs, it installs or updates the core client, deletes any existing profiles, and installs VPNDisable_ServiceProfile.xml in the profiles location. Then you can run the installers for the optional modules. The standalone components can then use the AnyConnect GUI without the VPN service.

MSI Command to Hide 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.

Upgrading Legacy Clients and Optional Modules

When upgrading earlier versions, the AnyConnect Secure Mobility Client version 3.0:

- Upgrades all previous versions of the core client and retains all VPN configurations.
- Upgrades Cisco SSC 5.x to the Network Access Manager module, retains all SSC configurations for use with Network Access Manager, and removes SSC 5.x.
- Upgrades the Host Scan files used by Cisco Secure Desktop. The AnyConnect 3.0 client can co-exist with Secure Desktop.
- ***Does not*** upgrade the Cisco IPsec VPN client (or remove it). However, the AnyConnect 3.0 client can coexist on the computer with the IPsec VPN client.
- ***Does not*** upgrade and cannot coexist with ScanSafe Web Security functionality on the same computer. You must uninstall AnyWhere+.

Customizing and Localizing the Installer

You can customize the AnyConnect core installer for Windows using transforms, and you can translate messages displayed by the core installer in the language preferred by the remote user. For more information on customizing and localizing (translating) the AnyConnect client and installer, see Chapter 11, “Customizing and Localizing the AnyConnect Client and Installer.”

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:

Recommended Order for Installing or Uninstalling Modules for Linux and MAC OS X

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.

If you distribute files manually, we strongly recommend the following installation order:

1. Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).
2. Install the DART module, which provides useful diagnostic information about the AnyConnect core client installation.
3. Install the posture module.

Uninstalling AnyConnect Modules

The order of uninstallation is also important. Use the following order for uninstalling the modules:

1. Uninstall the posture module.
2. Uninstall the AnyConnect core client.
3. Uninstall DART last. DART information is valuable should the uninstall processes fail.

AnyConnect Requirements for Computers Running Ubuntu 9.x 64-Bit

For the Cisco AnyConnect Secure Mobility client to run on a computer running Ubuntu 9.x 64-Bit, AnyConnect needs the following:

- The 32-bit compatibility library installed on the computer.
- The NSS crypto libraries from the Ubuntu 9.x 32-bit version installed in /usr/local/firefox.
- The profile .mozilla/firefox in the user home directory so it can interact with the Firefox certificate store.

Follow these steps to address these issues:

Step 1 Enter the following command to install the 32-bit compatibility library:

```
administrator@ubuntu-904-64:/usr/local$ sudo apt-get install ia32-libs lib32nss-mdns
```

Step 2 Download the 32-bit version of FireFox from http://www.mozilla.com and install it on /usr/local/firefox.

AnyConnect looks in this directory first for the NSS crypto libraries it needs.

Step 3 Enter the following command to extract the Firefox installation to the directory indicated:

```
administrator@ubuntu-904-64:/usr/local$ sudo tar -C /usr/local -xvjf
~/Desktop/firefox-version.tar.bz2
```

Step 4 Run Firefox at least once, logged in as the user who will use AnyConnect.

Doing so creates the .mozilla/firefox profile in the user home directory, which is required by AnyConnect to interact with the Firefox certificate store.

Step 5 Install AnyConnect in standalone mode.

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

If users use WebLaunch to start AnyConnect on a Mac and the Java installer fails, a dialog box presents a Manual Install link. Users should follow this procedure when this happens:

Step 1 Click **Manual Install**. A dialog box presents the option to save the vpnsetup.sh file.

Step 2 Save the vpnsetup.sh file on the Mac.

Step 3 Open a Terminal window and use the CD command to navigate to the directory containing the file saved.

Step 4 Enter the following command:

```
sudo /bin/sh vpnsetup.sh
```

The vpnsetup script starts the AnyConnect installation.

Step 5 Following the installation, choose **Applications > Cisco > Cisco AnyConnect Secure Mobility Client** to initiate an AnyConnect session.

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 is a signed application and will run normally with this setting or with the **Anywhere** setting. If you select the **Mac App Store** setting, you must use Control-click to install and run AnyConnect. For further information see: http://www.apple.com/macosx/mountain-lion/security.html.

Note This applies only to new stand-alone installs and is not applicable to web launch or OS upgrades (for example 10.7 to 10.8)

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

Table 2-7 shows the AnyConnect filenames on the endpoint computer for each operating system type when you predeploy or ASA-deploy the client:

Table 2-7 AnyConnect Core Filenames for ASA or Predeployment

AnyConnect 3.0 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

Table 2-8 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 2-8 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	anyconnect-predeploy-linux-(ver)-k9.tar.gz
	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 2-9 shows the SBL filenames on the endpoint computer when you predeploy or ASA-deploy the client to a Windows computer:

Table 2-9 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 2-10 shows the Network Access Manager filenames on the endpoint computer when you predeploy or ASA-deploy the client to a Windows computer:

Table 2-10 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 2-11 shows the posture module filenames on the endpoint computer for each operating system type when you predeploy or ASA-deploy the client:

Table 2-11 Posture Module Filename 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

Table 2-12 shows the telemetry module filenames on the endpoint computer for Windows when you predeploy or ASA-deploy the client:

Table 2-12 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 2-13 shows the Web Security module filenames on the endpoint computer for Windows when you predeploy or ASA-deploy the client:

Table 2-13 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 2-14 shows the profile-related files AnyConnect downloads on the local computer and their purpose:

Table 2-14 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 2-15 shows the locations of the AnyConnect profiles for all operating systems:

Table 2-15 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
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
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

Table 2-15 Profile Locations for all Operating Systems

Operating System	Module	Location
Mac OS X	All modules	/opt/cisco/anyconnect/profile
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 2-16 shows the filenames and installed paths for preferences files on the client computer:

Table 2-16 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 Secure Mobility Client\preferences.xml
	Global	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ preferences_global.xml
Windows XP	User	C:\Documents and Settings**username**\Local Settings\ApplicationData\ Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml
	Global	C:\Documents and Settings\AllUsers\Application Data\Cisco\ Cisco AnyConnect Secure Mobility 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, and Web Security Modules for the AnyConnect Secure Mobility Client. These profiles can be distributed with predeployment kits for the VPN, Network Access Manager, and Web Security modules.

System Requirements for Standalone Profile Editor

Supported Operating Systems

This application has been tested on Windows XP and Windows 7. The MSI only runs 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.

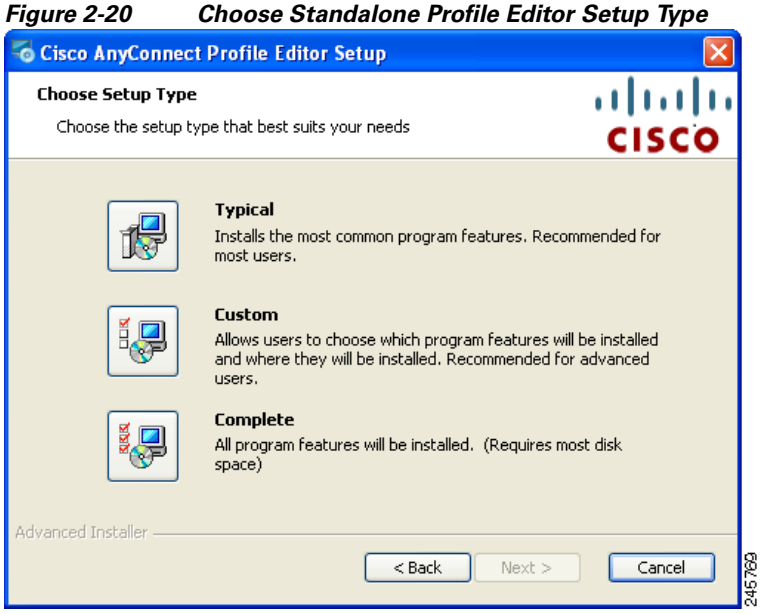
Step 3 At the Welcome screen, click **Next**.

Figure 2-19 Standalone Profile Editor Welcome Screen

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

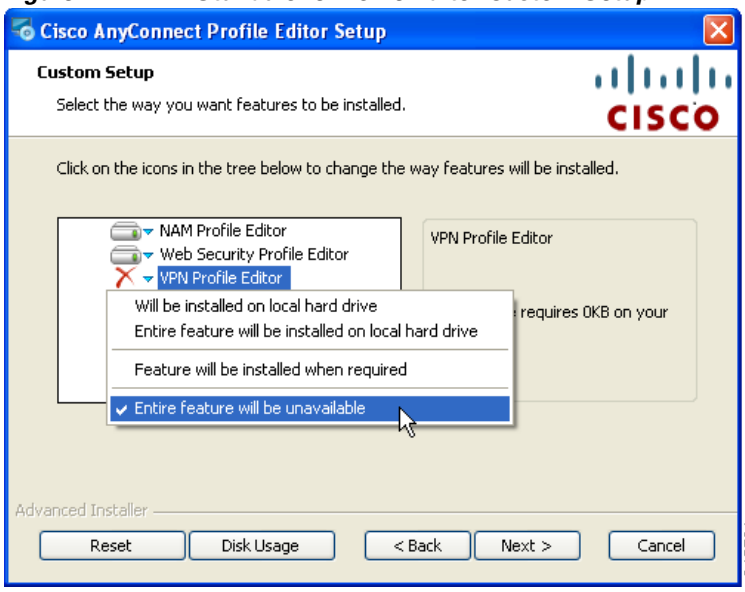
- **Typical** - Installs only the Network Access Manager profile editor automatically.
- **Custom** - Allows you to choose any of these profile editors to install: Network Access Manager Profile Editor, Web Security Profile Editor, and VPN Profile Editor.
- **Complete** - Automatically installs the Network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

Figure 2-20 Choose Standalone Profile Editor Setup Type



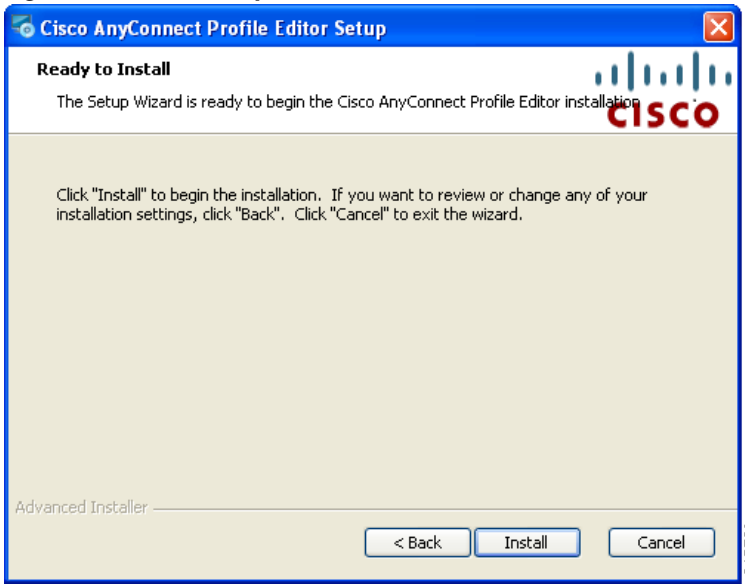
Step 5 If you clicked **Typical** or **Complete** in the previous step, skip to Step 6. If you clicked **Custom** in the previous step, click the icon for the standalone profile editor you want to install and select **Will be installed on local hard drive** or click **Entire Feature will be unavailable**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

Figure 2-21 Standalone Profile Editor Custom Setup



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

Figure 2-22 Ready to Install Standalone Profile Editor



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

Figure 2-23 Standalone Profile Editor Installation Finished

- 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, or Web Security 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, or Web Security 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, or Web Security 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”

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 VPN, Network Access Manager, or Web Security 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, or Web Security 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.

Configuring the ASA for WSA Support of the AnyConnect Secure Mobility Solution

Today, users and their devices are increasingly more mobile, connecting to the Internet from various locations, such as the office, home, airport, and cafés. Traditionally, users inside the network are protected from security threats, and users outside the traditional network have no acceptable use policy enforcement, minimal protection against malware, and a higher risk of data loss.

Employers want to create flexible working environments where employees and partners can work anywhere on any device, but they also want to protect corporate interests and assets from Internet-based threats at all times (always-on security).

Traditional network and content security solutions are great for protecting users and assets behind the network firewall but are useless when users or devices are not connected to the network or when data is not routed through the security solutions.

Cisco offers AnyConnect Secure Mobility to extend the network perimeter to remote endpoints, enabling the seamless integration of web filtering services offered by the Web Security appliance. Cisco AnyConnect Secure Mobility provides an innovative new way to protect mobile users on PC-based or smart-phone platforms, providing a more seamless, always-protected experience for end users and comprehensive policy enforcement for IT administrators.

AnyConnect Secure Mobility is a collection of features across the following Cisco products:

- Cisco IronPort Web Security appliance (WSA)
- Cisco ASA 5500 series adaptive security appliance (ASA)
- Cisco AnyConnect client

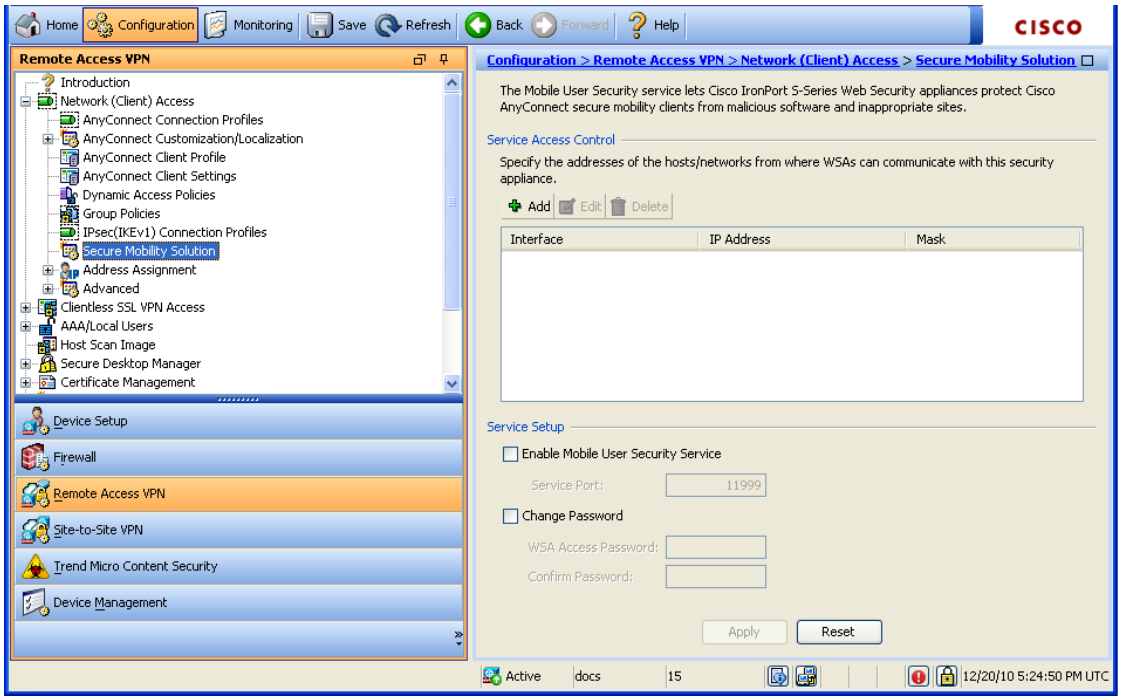
Cisco AnyConnect Secure Mobility addresses the challenges of a mobile workforce by offering the following features:

- **Secure, persistent connectivity**. Cisco AnyConnect (with the adaptive security appliances at the headend) provides the remote access connectivity portion of AnyConnect Secure Mobility. The connection is secure because both the user and device must be authenticated and validated prior to being provided access to the network. The connection is persistent because Cisco AnyConnect is typically configured to be always-on even when roaming between networks. Although Cisco AnyConnect is always-on, it is also flexible enough to apply different policies based on location, allowing users access to the Internet in a “captive portal” situation, when users must accept terms of agreement before accessing the Internet.
- **Persistent security and policy enforcement**. The Web Security appliance applies context-aware policies, including enforcing acceptable use policies and protection from malware for all users, including mobile (remote) users. The Web Security appliance also accepts user authentication information from the AnyConnect client, providing an automatic authentication step for the user to access web content.

Use the Secure Mobility Solution dialog box to configure the ASA portion of this feature. AnyConnect Secure Mobility lets Cisco IronPort S-Series Web Security appliances scan Cisco AnyConnect secure mobility clients to ensure that clients are protected from malicious software and/or inappropriate sites. The client periodically checks to ensure that Cisco IronPort S-Series Web Security appliance protection is enabled.

To configure the ASA for WSA support, launch ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution** panel (see Figure 2-24). Click **Help** for detailed instructions.

Figure 2-24 AnyConnect Secure Mobility Window



Note

- This feature requires a release of the Cisco IronPort Web Security appliance that provides AnyConnect Secure Mobility licensing support for the Cisco AnyConnect secure mobility client. It also requires an AnyConnect release that supports the AnyConnect Secure Mobility feature.
- This feature is available for AnyConnect connections using SSL or IPsec IKEv2 protocols.

Step 1 Specify from which host or network address the WSAs can communicate and identify the remote users using one of the following methods:

- **Associate by IP address**. The Web Security appliance administrator specifies a range of IP addresses that it considers as assigned to remote devices. Typically, the adaptive security appliance assigns these IP addresses to devices that connect using VPN functionality. When the Web Security appliance receives a transaction from one of the configured IP addresses, it considers the user as a remote user. With this configuration, the Web Security appliance does not communicate with any adaptive security appliance.
- **Integrate with a Cisco ASA**. The Web Security appliance administrator configures the Web Security application to communicate with one or more adaptive security appliances. The adaptive security appliance maintains an IP address-to-user mapping and communicates that information to the Web Security appliance. When the Web Proxy receives a transaction, it obtains the IP address and checks the IP address-to-user mapping to determine the user name. When you integrate with an adaptive security appliance, you can enable single sign-on for remote users. With this configuration, the Web Security appliances communicates with the adaptive security appliance.
  - Add—Opens the Add Access Control Configuration dialog box where you can add one or more Web Security appliances that the adaptive security appliance can communicate with.

- Edit—Opens the Edit Access Control Configuration dialog box for the selected connection.
- Delete—Removes the selected connection from the table. There is no confirmation or undo.

Step 2 If you choose to enable Mobile User Security Service, it starts the connection with the client through the VPN. When the Web Security appliance is configured to integrate with an adaptive security appliance, it tries to establish an HTTPS connection with all configured adaptive security appliances when it first starts up. When the connection is established, the Web Security appliance authenticates with the adaptive security appliance using the configured ASA access password. After successful authentication, the adaptive security appliance sends the IP address-to-user mapping to the Web Security appliance. If no WSA is present, the status is disabled.

Step 3 If you choose to enable the service, specify which port number for the service to use. The port must be between 1 and 65535 and must match the corresponding value provisioned into the WSA with the management system. The default is 11999.

Step 4 Change the WSA access password, if desired. You can change the Web Security appliance access password that is required for authentication between the adaptive security appliance and the Web Security appliance. This password must match the corresponding password configured on the Web Security appliance.

Step 5 In the WSA Access Password field, specify the shared secret password required for authentication between the ASA and WSA.

Step 6 Re-enter the specified password.

Step 7 Show WSA Sessions allows you to view session information of WSAs connected to the ASA.The host IP address of the WSA that is connected (or has been connected) and the duration of the connection is returned in a dialog box.

Configuring a Proxy Server For Endpoint to WSA Traffic

You must set up a web proxy to redirect web traffic from the endpoint to the WSA. To do this, either set up a transparent proxy using a WCCP router or follow these instructions to set up an explicit proxy:

Step 1 Launch ASDM on your ASA and select **Remote Access VPN > Network (Client) Access > Group Policies.**

Step 2 Select the group policy configured for web vpn and click **Edit**.

Step 3 In the left pane of the Edit Internal Group Policy window, expand the Advanced node and select Browser Proxy.

Step 4 Uncheck **Inherit** in the Proxy Server Policy area.

Step 5 Select **Select proxy server settings from the following** and check **Use proxy server settings given below**.

Step 6 Expand the Proxy Server Settings area and uncheck the Server Address and Port **Inherit** checkbox. Specify the WSA's IP address and port number.

Step 7 Uncheck the Bypass server for local addresses **Inherit** checkbox and select **Yes**.

Step 8 If you want, enter a list of addresses that will not be accessed through a proxy server by unchecking the Exceptions List **Inherit** check box and entering the IP addresses. You can make exceptions for these IP addresses in the Exception list area.

Step 9 Click **OK**.

Step 10 Click **Apply**.