Configuring VPN Access

The following sections describe the Cisco AnyConnect Secure Mobility client VPN profile and features, and how to configure them:

- Configuring IP Addresses for AnyConnect Clients, page 3-2
- Creating and Editing an AnyConnect Profile, page 3-9
- Deploying the AnyConnect Profile, page 3-12
- Configuring VPN Load Balancing, page 3-12
- Configuring Start Before Logon, page 3-13
- Trusted Network Detection, page 3-21
- Always-on VPN, page 3-24
- Connect Failure Policy for Always-on VPN, page 3-29
- Captive Portal Hotspot Detection and Remediation, page 3-32
- Configuring Split Tunneling, page 3-38
- Configuring DNS and WINS Servers for AnyConnect, page 3-38
- Split DNS, page 3-38
- Configuring Certificate Enrollment using SCEP, page 3-41
- Configuring Certificate Expiration Notice, page 3-47
- Configuring Certificate Matching, page 3-51
- Prompting Users to Select Authentication Certificate, page 3-55
- Configuring a Server List, page 3-56
- Configuring a Backup Server List, page 3-61
- Configuring Connect On Start-up, page 3-61
- Configuring Auto Reconnect, page 3-61
- Proxy Connections, page 3-62
- Optimal Gateway Selection, page 3-64
- Writing and Deploying Scripts, page 3-66
- Authentication Timeout Control, page 3-70
- Proxy Support, page 3-71
- Using a Windows RDP Session to Launch a VPN Session, page 3-73
IP addresses make internetwork connections possible. They are like telephone numbers: both the sender and receiver must have an assigned number to connect. But with VPNs, there are actually two sets of addresses: the first set connects client and server on the public network. Once that connection is made, the second set connects client and server through the VPN tunnel.

In ASA address management, you configure the IP addresses that the client uses to connect to the private network. IP addresses assigned to other resources on your private network are part of your network administration responsibilities, not part of VPN management. In this section, the IP addresses we refer to are available in your private network addressing scheme for client VPN.

This section includes the following topics:

- IP Address Assignment Policies, page 3-2
- Internal IP Address Pools, page 3-3
- Assigning an IP Address to an AnyConnect Connection, page 3-4

### IP Address Assignment Policies

- **Use authentication server** — Retrieve addresses from an external authentication, authorization, and accounting server on a per-user basis. If you are using an authentication server that has IP addresses configured, we recommend using this method. You can configure AAA servers in the Configuration > AAA Setup pane. This method is available for IPv4 and IPv6 assignment policies.

- **Use DHCP** — Obtain IP addresses from a DHCP server. To use DHCP, configure the server in the Configuration > Remote Access VPN > DHCP Server pane. This method is available for IPv4 assignment policies.

- **Use an internal address pool** — Internally configured address pools are the easiest method of address pool assignment. If you use this method, configure the IP address pools in Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools pane. This method is available for IPv4 and IPv6 assignment policies.

  - Allow the reuse of an IP address so many minutes after it is released—Delays the reuse of an IP address after its return to the address pool. Adding a delay helps to prevent problems firewalls can experience when an IP address is reassigned quickly. By default, this is unchecked, meaning the ASA does not impose a delay. If you want one, check the box and enter the number of minutes in the range 1 - 480 to delay IP address reassignment. This configurable element is available for IPv4 assignment policies.

### Configuring IPv4 and IPv6 Address Assignments using ASDM

**Step 1**
Select **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**

**Step 2**
In the IPv4 Policy area, check the address assignment method to enabled it or uncheck the address assignment method to disable it. These methods are enabled by default:
• Use Authentication server. Enables the use of an Authentication Authorization and Accounting (AAA) server you have configured to provide IP addresses.
• Use DHCP. Enables the use of a Dynamic Host Configuration Protocol (DHCP) server you have configured to provide IP addresses.
• Use internal address pools: Enables the use of a local address pool configured on the ASA.

If you enable **Use internal address pools**, you can also enable the reuse of an IPv4 address after it has been released. You can specify a range of minutes from 0 to 480 after which the IP v4 address can be reused.

**Step 3**
In the IPv6 Policy area, check the address assignment method to enable it or uncheck the address assignment method to disable it. These methods are enabled by default:
• Use Authentication server. Enables the use of an Authentication Authorization and Accounting (AAA) server you have configured to provide IP addresses.
• Use internal address pools: Enables the use of a local address pool configured on the ASA.

**Step 4**
Click **Apply**.

**Step 5**
Click **OK**.

---

**Internal IP Address Pools**

To configure IPv4 or IPv6 address pools to use for VPN remote access tunnels, open ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add/Edit IP Pool**.

To delete an address pool, open ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools**. Select the address pool you want to delete and click **Delete**.

The ASA uses address pools based on the connection profile or group policy for the connection. The order in which you specify the pools is important. If you configure more than one address pool for a connection profile or group policy, the ASA uses them in the order in which you added them to the ASA.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

**Note**
The ASA’s outside interface addresses, for both IPv4 and IPv6, cannot overlap with the private side address space as defined by address pools.

**Configuring Local IPv4 Address Pools Using ASDM**

The IP Pool area shows each configured address pool by name with their IP address range, for example: 10.10.147.100 to 10.10.147.177. If no pools exist, the area is empty. The ASA uses these pools in the order listed: if all addresses in the first pool have been assigned, it uses the next pool, and so on.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

**Step 1**
Select **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**.
Step 2 To add an IPv4 address, click **Add > IPv4 Address pool**. To edit an existing address pool, select the address pool in the address pool table and click **Edit**.

Step 3 In the Add/Edit IP Pool dialog box, enter this information:
- **Pool Name**—Enter the name of the address pool. It can be up to 64 characters
- **Starting Address**—Enter the first IP address available in each configured pool. Use dotted decimal notation, for example: 10.10.147.100.
- **Ending Address**—Enter the last IP address available in each configured pool. User dotted decimal notation, for example: 10.10.147.177.
- **Subnet Mask**—Identifies the subnet on which this IP address pool resides.

Step 4 Click **OK**.

Step 5 Click **Apply**.

### Configuring Local IPv6 Address Pools Using ASDM

The IP Pool area shows each configured address pool by name with a starting IP address range, the address prefix, and the number of addresses configurable in the pool. If no pools exist, the area is empty. The ASA uses these pools in the order listed: if all addresses in the first pool have been assigned, it uses the next pool, and so on.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

Step 1 Select **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**.

Step 2 To add an IPv6 address, click **Add > IPv6 Address pool**. To edit an existing address pool, select the address pool in the address pool table and click **Edit**.

Step 3 In the Add/Edit IP Pool dialog box enter this information:
- **Name**—Displays the name of each configured address pool.
- **Starting IP Address**—Enter the first IP address available in the configured pool. For example: 2001:DB8::1.
- **Prefix Length**—Enter the IP address prefix length in bits. For example 32 represents /32 in CIDR notation. The prefix length defines the subnet on which the pool of IP addresses resides.
- **Number of Addresses**—Identifies the number of IPv6 addresses, starting at the Starting IP Address, there are in the pool.

Step 4 Click **OK**.

Step 5 Click **Apply**.

### Assigning an IP Address to an AnyConnect Connection

Use one of these methods to assign an IP address to a VPN connection:
• Assigning IP Addresses using Internal Address Pools, page 3-5—An internal pool is associated with a group policy and configured on the ASA. These addresses can be IPv4 or IPv6.
• Assigning IP Addresses Using DHCP, page 3-5—Associating a DHCP server with a group policy that is configured on the ASA. These addresses can only be IPv4.
• Assigning IP Addresses to a Local User, page 3-6—Assigning an IP address to a user configured on the ASA. These addresses can be IPv4 or IPv6.

Assigning IP Addresses using Internal Address Pools

The Add or Edit Group Policy dialog box lets you specify address pools, tunneling protocols, filters, connection settings, and servers for the internal Network (Client) Access group policy being added or modified. For each of the fields on this dialog box, checking the Inherit check box lets the corresponding setting take its value from the default group policy. Inherit is the default value for all the attributes in this dialog box.

You can configure both IPv4 and IPv6 address pools for the same group policy. If both versions of IP addresses are configured in the same group policy, clients configured for IPv4 will get an IPv4 address, clients configured for IPv6 will get an IPv6 address, and clients configured for both IPv4 and IPv6 addresses will get both an IPv4 and an IPv6 address.

---

**Step 1**  
Connect to the ASA using ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

**Step 2**  
Create a new group policy or the group policy you want to configure with an internal address pool and click **Edit**.

The General attributes pane is selected by default in the group policy dialog.

**Step 3**  
Use the Address Pools field to specify an IPv4 address pool for this group policy. Click Select to add or edit an IPv4 address pool. See Configuring Local IPv4 Address Pools Using ASDM, page 3-3 for more information.

**Step 4**  
Use the IPv6 Address Pools field to specify an IPv6 address pools to use for this group policy. Click Select to add or edit a IPv6 address pool. See Configuring Local IPv6 Address Pools Using ASDM, page 3-4.

**Step 5**  
Click **OK**.

**Step 6**  
Click **Apply**.

---

Assigning IP Addresses Using DHCP

To assign IPv4 addresses using a DHCP server, configure the IP address Assignment policy to use DHCP follow the instructions below. You cannot assign IPv6 addresses to AnyConnect clients using a DHCP server.

---

**Step 1**  
Connect to the ASA using ASDM.

**Step 2**  
Select **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**.

**Step 3**  
Click **Use DHCP**.

**Step 4**  
Click **Apply**.
Assigning IP Addresses to a Local User

ASA administrators can create accounts for individual users on the ASA. These accounts can be configured to use a group policy or they can have many of the same VPN attributes found in group policies configured specifically in the local user policy. These individual users can also have some AnyConnect attributes defined for their account.

This section describes how to configure all the attributes of a local user.

Prerequisites

This procedure describes how to edit an existing user. To add a user select Configuration > Remote Access VPN > AAA/Local Users > Local Users and click Add. For more information see “Adding a User Account to the Local Database” in Chapter 42, Configuring AAA Servers and the Local Database in the Cisco ASA 5500 Configuration Guide Using ASDM.

Guidelines

By default, the Inherit check box is checked for each setting on the Edit User Account screen, which means that the user account inherits the value of that setting from the default group policy, DfltGrpPolicy.

To override each setting, uncheck the Inherit check box, and enter a new value. The detailed steps that follow describe each of the settings on the Edit User Account screen.

Detailed Steps

Step 1 Start ASDM and select Configuration > Remote Access VPN > AAA/Local Users > Local Users.

Step 2 Select the user you want to configure and click Edit. The Edit User Account screen opens.

Step 3 In the left pane, click VPN Policy.

Step 4 Specify a group policy for the user. The user policy will inherit the attributes of this group policy. If there are other fields on this screen that are set to Inherit the configuration from the Default Group Policy, the attributes specified in this group policy will take precedence over those in the Default Group Policy.

Step 5 Specify which tunneling protocols are available for the user, or whether the value is inherited from the group policy. Check the desired Tunneling Protocols check boxes to choose the VPN tunneling protocols that are available for use. Only the selected protocols are available for use. The choices are as follows:

- Clientless SSL VPN (VPN via SSL/TLS) uses a web browser to establish a secure remote-access tunnel to a VPN Concentrator; requires neither a software nor hardware client. Clientless SSL VPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file shares (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.

- The SSL VPN Client lets users connect after downloading the Cisco AnyConnect Client application. Users use a clientless SSL VPN connection to download this application the first time. Client updates then occur automatically as needed whenever the user connects.
• IPsec IKEv1—IP Security Protocol. Regarded as the most secure protocol, IPsec provides the most complete architecture for VPN tunnels. Both Site-to-Site (peer-to-peer) connections and Cisco VPN client-to-LAN connections can use IPsec IKEv1.

• IPsec IKEv2—IPsec IKEv2-Supported by the AnyConnect Secure Mobility Client. AnyConnect connections using IPsec with IKEv2 can make use of the same feature set available to SSL VPN Connections.

• L2TP over IPsec allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the ASA and private corporate networks.

Note
If no protocol is selected, an error message appears.

Step 6
Specify which filter (IPv4 or IPv6) to use, or whether to inherit the value from the group policy. Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol. To configure filters and rules, choose Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options > Filter.

Click Manage to display the ACL Manager pane, on which you can add, edit, and delete ACLs and ACEs.

Step 7
Specify whether to inherit the Connection Profile (tunnel group) lock or to use the selected tunnel group lock, if any. Selecting a specific lock restricts users to remote access through this group only. Tunnel Group Lock restricts users by checking if the group configured in the VPN client is the same as the users assigned group. If it is not, the ASA prevents the user from connecting. If the Inherit check box is not checked, the default value is None.

Step 8
Specify whether to inherit the Store Password on Client System setting from the group. Uncheck the Inherit check box to activate the Yes and No radio buttons. Click Yes to store the logon password on the client system (potentially a less-secure option). Click No (the default) to require the user to enter the password with each connection. For maximum security, we recommend that you not allow password storage.

Step 9
Specify an Access Hours policy to apply to this user, create a new access hours policy for the user, or leave the Inherit box checked. The default value is Inherit, or, if the Inherit check box is not checked, the default value is Unrestricted.

Click Manage to open the Add Time Range dialog box, in which you can specify a new set of access hours.

Step 10
Specify the number of simultaneous logons by the user. The Simultaneous logons parameter specifies the maximum number of simultaneous logons allowed for this user. The default value is 3. The minimum value is 0, which disables logon and prevents user access.

Note
While there is no maximum limit, allowing several simultaneous connections could compromise security and affect performance.

Step 11
Specify the maximum connection time for the user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, check the Unlimited check box (the default).
Configuring IP Addresses for AnyConnect Clients

Chapter 3      Configuring VPN Access

Step 12 Specify the Idle Timeout for the user in minutes. If there is no communication activity on the connection by this user in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 10080 minutes. This value does not apply to users of clientless SSL VPN connections.

Step 13 Configure the Session Alert Interval. If you uncheck the Inherit check box, the Default checkbox is checked automatically. This sets the session alert interval to 30 minutes. If you want to specify a new value, uncheck the Default check box and specify a session alert interval from 1 to 30 minutes in the minutes box.

Step 14 Configure the Idle Alert Interval. If you uncheck the Inherit check box, the Default checkbox is checked automatically. This sets the idle alert interval to 30 minutes. If you want to specify a new value, uncheck the Default check box and specify a session alert interval from 1 to 30 minutes in the minutes box.

Step 15 To set a dedicated IPv4 address for this user, enter an IPv4 address and subnet mask in the Dedicated IPv4 Address (Optional) area.

Step 16 To set a dedicated IPv6 address for this user, enter an IPv6 address with an IPv6 prefix in the Dedicated IPv6 Address (Optional) field. The IPv6 prefix indicates the subnet on which the IPv6 address resides.

Step 17 To configure clientless SSL settings, in the left pane, click Clientless SSL VPN. To override each setting, uncheck the Inherit check box, and enter a new value.

Step 18 Click Apply.

The changes are saved to the running configuration.

Configuring IPv4 or IPv6 Traffic to Bypass the VPN

The Client Bypass Protocol feature allows you to configure how the AnyConnect client manages IPv4 traffic when the ASA is expecting only IPv6 traffic or how AnyConnect manages IPv6 traffic when the ASA is only expecting IPv4 traffic.

When the AnyConnect client makes a VPN connection to the ASA, the ASA could assign the client an IPv4, IPv6, or both an IPv4 and IPv6 address.

If Client Bypass Protocol is enabled for one IP protocol and an address pool is not configured for that protocol (in other words, no IP address for that protocol was pushed to client from the ASA) any IP traffic using that protocol will not be sent through the VPN tunnel, it will be sent from the AnyConnect client in the clear.

On the other hand, if Client Bypass Protocol is disabled, and an address pool is not configured for that protocol, the client will drop all traffic for that IP protocol once the VPN tunnel is established.

For example, assume that the ASA assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped and if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

You configure the Client Bypass Protocol on the ASA for group policies.

Step 1 Connect to the ASA using ASDM.
Step 3 Select a group policy and click Edit.
Step 4 Select Advanced > AnyConnect.
Step 5  Next to Client Bypass Protocol, uncheck Inherit if this is a group policy other than the default group policy.

Step 6  Choose one of these options:
- Click Disable to drop IP traffic for which the ASA did not assign an address.
- Click Enable to send that IP traffic in the clear.

Step 7  Click OK.

Step 8  Click Apply.

---

Creating and Editing an AnyConnect Profile

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.

Note
If you manually deploy the VPN profile, you must also upload the profile to the ASA. When the client system connects, AnyConnect verifies that the profile on the client matches the profile on the ASA.

If you have disabled profile updates, and the profile on the ASA is different from the client, then the manually deployed profile won’t work.

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

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

Step 2  Select Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. The AnyConnect Client Profile pane opens.

Step 3  Click Add. The Add AnyConnect Client Profile window opens (Figure 3-1).
Step 4 Specify a name for the profile. Unless you specify a different value for Profile Location, ASDM creates an XML file on the ASA flash memory with the same name.

Note When specifying a name, avoid the inclusion of the .xml extension. If you name the profile example.xml, ASDM adds an .xml extension automatically and changes the name to example.xml.xml. Even if you change the name back to example.xml in the Profile Location field on the ASA, the name returns to example.xml.xml when you connect with AnyConnect by remote access. If the profile name is not recognized by AnyConnect (because of the duplicate .xml extension), IKEv2 connections may fail.

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 as shown in Figure 3-2. Enable AnyConnect features in the panes of the profile editor. When you finish, click OK.
Figure 3-2  Editing a Profile

This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.4 later. You can select a profile to edit, change group policy or delete. You can select the Add button to add a new profile, pressing the Update or Export button in the upload and download of client profile between local and database.

The profile usage mode is introduced with the Secure Mobility Solution. The field contains different profile usage in AnyConnect versions 2.3 and later.

Host Scan configuration can be performed by going to Secure Desktop Manager Host Scan. If Host Scan is enabled under Secure Desktop Manager, you will need to request ADP.

Profile Name: remote_sales_team

Preferences (Part 1):
- User Start Before Login
- Show Pre-Connect Message
- Certificate Store Override
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List
- Auto-Connect On Start
- Parameter On Connect
- Local Use Access
- Auto-Reconnect
- Auto-Reconnect Behavior
- Documents On Disconnect
- Auto-Update
- IKE Secure SD Integration
- Windows Login Enforcement
- Windows Login
- Windows Wint Establishment
- Remote Access
- Window Server Connection
- PPTP Protocol Support

Profile Location: Profile Location
Deploying the AnyConnect Profile

**Note** You must include the ASA in the host list in the profile so the client GUI displays all the user controllable settings on the initial VPN connection. If you do not add the ASA address or FQDN as a host entry in the profile, then filters do not apply for the session. For example, if you create a certificate match and the certificate properly matches the criteria, but you do not add the ASA as a host entry in that profile, the certificate match is ignored. For more information about adding host entries to the profile, see Configuring a Server List, page 3-56.

**Step 1** Associate a client profile with a group policy. Select **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

**Step 2** Add a new group policy or select a group policy from the group policies table and click **Edit**.

**Step 3** Select **Advanced > AnyConnect Client**.

**Step 4** Uncheck **Inherit** and select an AnyConnect profile to download using the Select AnyConnect Client Profile dialog box.

**Step 5** When you have finished with the configuration, click **OK** and then **Apply**.

Configuring VPN Load Balancing

Configuring load balancing for AnyConnect clients is documented fully in “Configuring Load Balancing,” in Chapter 67, Configuring IKE, Load Balancing, and NAC in *Cisco ASA 5500 Series Configuration Guide using ASDM, 6.4 and 6.6*.

In addition to the guidelines defined there, be aware of these guidelines:

- Clients with IPv6 addresses can make AnyConnect connections through the ASA cluster’s public-facing IPv6 address or through a Global Site Selector (GSS) server. Similarly, clients with IPv6 addresses can make AnyConnect VPN connections through the ASA cluster’s public-facing IPv4 address or through a GSS server. Either type of connection can be load-balanced within the ASA cluster.

**Note** Connections may fail if the DNS Time-To-Live (TTL) for entries in the GSS DNS Server are less than the time it takes AnyConnect to fully connect. We recommend setting a DNS TTL of at least 300 seconds (five minutes).

For clients with IPv6 addresses to successfully connect to the ASA’s public-facing IPv4 address, a device that can perform network address translation from IPv6 to IPv4 needs to be in the network.

- When performing certificate verification for load balancing with AnyConnect, and the connection is redirected by an IP address, the client does all name checking through this IP address. The customer needs to make sure that this IP address is listed in the certificates common name or the **subject alt name**. If the IP address is not present in these fields, then the certificate will be deemed untrusted.
• Following the guidelines defined in RFC 2818, if a **subject alt name** is included in the certificate, we only use the **subject alt name** for name checks and we ignore the common name. Make sure that the IP address of the server presenting the certificate is defined in the **subject alt name** of the certificate.

For a standalone ASA, the IP address is the IP of that ASA. In a clustering situation, it depends on the certificate configuration. If the cluster uses one certificate, then it would be the IP of the cluster, and the certificate would contain Subject Alternative Name extensions that have each ASA’s IP and FQDN. If the cluster uses multiple certificates, then it should once again be the IP address of the ASA.

## Configuring Start Before Logon

Start Before Logon (SBL) allows a user to establish their VPN connection to the enterprise infrastructure before logging on to Windows.

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

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

Reasons you might consider enabling SBL for your users include:

• The user’s computer is joined to an Active Directory infrastructure.

• The user cannot have cached credentials on the computer (the group policy disallows cached credentials).

• The user must run logon scripts that execute from a network resource or need access to a network resource.

• A user has network-mapped drives that require authentication with the Microsoft Active Directory infrastructure.

• Networking components (such as MS NAP/CS NAC) exist that might require connection to the infrastructure.

To enable the SBL feature, you must make changes to the AnyConnect profile and enable the ASA to download an AnyConnect module for SBL.

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

SBL creates a network that is equivalent to being on the local corporate LAN. For example, with SBL enabled, since the user has access to the local infrastructure, the logon scripts that would normally run when a user is in the office would also be available to the remote user. This includes domain logon scripts, group policy objects and other Active Directory functionality that normally occurs when a user logs on to their system.
In another example, a system might be configured to not allow cached credentials to be used to log on to the computer. In this scenario, users must be able to communicate with a domain controller on the corporate network for their credentials to be validated before gaining access to the computer.

SBL requires a network connection to be present at the time it is invoked. In some cases, this might not be possible, because a wireless connection might depend on credentials of the user to connect to the wireless infrastructure. Since SBL mode precedes the credential phase of a logon, a connection would not be available in this scenario. In this case, the wireless connection needs to be configured to cache the credentials across logon, or another wireless authentication needs to be configured, for SBL to work. If the Network Access Manager is installed, you must deploy machine connection to ensure that an appropriate connection is available. For more information, see Chapter 4, “Configuring Network Access Manager”.

AnyConnect is not compatible with fast user switching.

This section covers the following topics:

- Installing Start Before Logon Components (Windows Only), page 3-14
- Configuring Start Before Logon (PLAP) on Windows Systems, page 3-16

### Installing Start Before Logon Components (Windows Only)

The Start Before Logon components must be installed after the core client has been installed. Additionally, the Start Before Logon components require that the core client software is installed. If you are pre-deploying AnyConnect and the Start Before Logon components using the MSI files (for example, you are at a big company that has its own software deployment—Altiris, Active Directory, or SMS), then you must get the order right. The order of the installation is handled automatically when the administrator loads AnyConnect if it is web deployed or web updated.

> **Note**
> AnyConnect cannot be started by third-party Start Before Logon applications.

### Start Before Logon Differences Between Windows Versions

The procedures for enabling SBL differ slightly on Windows 7 and Vista systems. Pre-Vista systems use a component called VPNGINA (which stands for virtual private network graphical identification and authentication) to implement SBL. Windows 7 and Vista systems use a component called PLAP to implement SBL.

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

> **Note**
> In this section, VPNGINA refers to the Start Before Logon feature for pre-Vista platforms, and PLAP refers to the Start Before Logon feature for Windows 7 and Vista systems.
A GINA is activated when a user presses the Ctrl+Alt+Del key combination. With PLAP, the Ctrl+Alt+Del key combination opens a window where the user can choose either to log in to the system or to activate any Network Connections (PLAP components) using the Network Connect button in the lower-right corner of the window.

The sections that immediately follow describe the settings and procedures for both VPNGINA and PLAP SBL. For a complete description of enabling and using the SBL feature (PLAP) on a Windows 7 or Vista platform, see the “Configuring Start Before Logon (PLAP) on Windows Systems” section on page 3-16.

**Enabling SBL in the AnyConnect Profile**

To enable SBL in the AnyConnect profile, follow these steps:

| Step 1 | Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9). |
| Step 2 | Go to the Preferences pane and check **Use Start Before Logon**. |
| Step 3 | (Optional) To give the remote user control over using SBL, check **User Controllable**. |

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

**Enabling SBL on the Security Appliance**

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

| Step 1 | Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. |
| Step 2 | Select a group policy and click **Edit**. |
| Step 3 | Select **Advanced > AnyConnect Client** in the left navigation pane. AnyConnect Client settings display. |
| Step 4 | Uncheck **Inherit** for the Optional Client Module for Download setting. |
| Step 5 | Select the **AnyConnect SBL** module in the drop-down list. |

**Troubleshooting SBL**

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

| Step 1 | Ensure that the AnyConnect profile is loaded on the ASA, ready to be deployed. |
| Step 2 | Delete prior profiles (search for them on the hard drive to find the location, *.xml). |
| Step 3 | Using Windows Add/Remove Programs, uninstall the SBL Components. Reboot the computer and retest. |
| Step 4 | Clear the user’s AnyConnect log in the Event Viewer and retest. |
| Step 5 | Browse back to the security appliance to install AnyConnect again. |
Configuring Start Before Logon (PLAP) on Windows Systems

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

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

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

Installing PLAP

The vpnplap.dll and vpnplap64.dll components are part of the existing GINA installation package, so you can load a single, add-on SBL package on the security appliance, which then installs the appropriate component for the target platform. PLAP is an optional feature. The installer software detects the underlying operating system and places the appropriate DLL in the system directory. For systems before Windows 7 and Vista, the installer installs the vpngina.dll component on 32-bit versions of the operating system. On Windows 7 or Vista, or the Windows 2008 server, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component.

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

Once installed, PLAP is not active until you modify the user profile <profile.xml> file to activate SBL. See the “Enabling SBL in the AnyConnect Profile” section on page 3-15. After activation, the user invokes the Network Connect component by clicking Switch User, then the Network Connect icon in the lower, right part of the screen.

Note
If the user mistakenly minimizes the user interface, the user can restore it by pressing the Alt+Tab key combination.
Logging on to a Windows 7 or Windows Vista PC using PLAP

Users can log on to Windows 7 or Windows Vista with PLAP enabled by following these steps, which are Microsoft requirements. The examples screens are for Windows Vista:

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

*Figure 3-3   Example Logon Window Showing the Network Connect Button*

The Vista logon window appears with a Switch User button. (Figure 3-4).
Step 2  The user clicks **Switch User** (circled in red in this figure). The Vista Network Connect window displays. The network logon icon is circled in red.

*Note*  If the user is already connected through an AnyConnect connection and clicks **Switch User**, that VPN connection remains. If the user clicks **Network Connect**, the original VPN connection terminates. If the user clicks **Cancel**, the VPN connection terminates.
Step 3  The user clicks the **Network Connect** button in the lower-right corner of the window to launch AnyConnect. The AnyConnect logon window opens.

Step 4  The user uses this GUI to log in as usual.

---

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

Step 5  When the user connects, the user sees a screen similar to the Vista Network Connect window, except that it has the Microsoft Disconnect button in the lower-right corner (Figure 3-5). This button is the only indication that the connection was successful.
The user clicks the icon associated with their logon. In this example, the user clicks **VistaAdmin** to complete logging onto the computer.

⚠️ **Caution**

Once the connection is established, you have a few minutes to log on. The user logon session times out after approximately a two minute idle timeout and a disconnect is issued to the AnyConnect PLAP component, causing the VPN tunnel to disconnect.
Disconnected from AnyConnect Using PLAP

After successfully establishing a VPN session, the PLAP component returns to the original window, this time with a Disconnect button displayed in the lower-right corner of the window (circled in Figure 3-6). When the user clicks **Disconnect**, the VPN tunnel disconnects.

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

- When a user logs on to a PC using PLAP but then presses **Cancel**.
- When the PC is shut down before the user logs on to the system.
- When Windows times out the user logon session and returns to the “Press CTRL + ALT + DEL to log on” screen.

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

Trusted Network Detection

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

**Note**

For the equivalent feature for the Web Security module, see Secure Trusted Network Detection, page 6-27.

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

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

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

You configure TND in the AnyConnect VPN Client profile. No changes are required to the ASA configuration.

Trusted Network Detection Requirements

Trusted Network Detection (TND) is supported on computers running the Microsoft Windows and Mac OS X operating systems supported by this release of AnyConnect.

Trusted Network Detection with or without Always-On configured is supported on IPv6 and IPv4 VPN connections to the ASA over IPv4 and IPv6 networks.
Configuring Trusted Network Detection

To configure TND in the client profile, follow these steps:

**Step 1** Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2** Go to the Preferences (Part 2) pane.

**Step 3** Check Automatic VPN Policy.

*Note* Automatic VPN Policy does not prevent users from manually controlling a VPN connection.

**Step 4** Select a Trusted Network Policy—the action the client takes when the user is inside the corporate network (the trusted network). The options are:

- Disconnect—The client terminates the VPN connection in the trusted network.
- Connect—The client starts a VPN connection in the trusted network.
- Do Nothing—The client takes no action in the trusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection (TND).
- Pause—AnyConnect suspends the VPN session (instead of disconnecting) if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user’s convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.

**Step 5** Select an Untrusted Network Policy—the action the client takes when the user is outside the corporate network. The options are:

- Connect—The client starts a VPN connection upon the detection of an untrusted network.
- Do Nothing—The client starts a VPN connection upon the detection of an untrusted network. This option disables always-on VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.

**Step 6** Specify Trusted DNS Domains—Specify the DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. You can assign multiple DNS suffixes if you add them to the split-dns list and specify a default domain on the ASA. See Table 3-1 for more examples of DNS suffix matching.

You must have a DNS entry for the headend server that is resolvable by DNS. If your connections are by IP address, you need a DNS server that can resolve mus.cisco.com. If mus.cisco.com is not resolvable via DNS, captive portal detection will not work as expected.

The AnyConnect client builds the DNS suffix list in the following order:

- the domain passed by the head end
- the split-DNS suffix list passed by the head end
- the public interface’s DNS suffixes, if configured. If not, the primary and connection-specific suffixes, along with the parent suffixes of the primary DNS suffix (if the corresponding box is checked in the Advanced TCP/IP Settings)

**Step 7** Specify Trusted DNS Servers—All DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 203.0.113.1,2001:DB8::1. Wildcards (*) are not supported for DNS server addresses.
You can configure either TrustedDNSDomains, TrustedDNSServers, or both. If you configure TrustedDNSServers, be sure to enter all your DNS servers, so your site(s) will all be part of the Trusted Network.

An active interface will be considered as an In-Trusted-Network if it matches ALL the rules in the VPN profile.

### Table 3-1  DNS Suffix Matching Examples

<table>
<thead>
<tr>
<th>To Match this DNS Suffix:</th>
<th>Use this Value for TrustedDNSDomains:</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com (only)</td>
<td>*example.com</td>
</tr>
<tr>
<td>example.com</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>*example.com</td>
</tr>
<tr>
<td>anyconnect.cisco.com</td>
<td>OR example.com, anyconnect.example.com</td>
</tr>
<tr>
<td>asa.example.com</td>
<td>*example.com</td>
</tr>
<tr>
<td>AND</td>
<td>OR asa.example.com, anyconnect.example.com</td>
</tr>
<tr>
<td>example.cisco.com</td>
<td></td>
</tr>
</tbody>
</table>

Wildcards (*) are supported for DNS suffixes.

## TND and Users with Multiple Profiles Connecting to Multiple Security Appliances

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

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

The following workarounds will help you prevent this problem:

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

You can configure AnyConnect to establish a VPN session automatically after the user logs in to a computer. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer expires. The group policy assigned to the session specifies these timer values. If AnyConnect loses the connection with the ASA, the ASA and the client retain the resources assigned to the session until one of these timers expire. AnyConnect continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.

**Note**

If always-on is enabled, but the user does not log on, AnyConnect does not establish the VPN connection. AnyConnect starts the VPN connection only post-login.

*(Post logon)* always-on VPN enforces corporate policies to protect the computer from security threats by preventing access to Internet resources when the computer is not in a trusted network.

**Caution**

Always-on VPN does not support connecting through a proxy.

When AnyConnect detects always-on VPN in the profile, it protects the endpoint by deleting all other AnyConnect profiles and ignores any public proxies configured to connect to the ASA.

To enhance the protection against threats, we recommend the following additional protective measures if you configure always-on VPN:

- Pre-deploy a profile configured with always-on VPN to the endpoints to limit connectivity to the pre-defined ASAs. Predeployment prevents contact with a rogue server.
- Restrict administrator rights so that users cannot terminate processes. A PC user with admin rights can bypass an always-on VPN policy by stopping the agent. If you want to ensure fully-secure always-on VPN, you must deny local admin rights to users.
- Restrict access to the following folders or the Cisco sub-folders on Windows computers:
  - For Windows XP users: C:\Document and Settings\All Users
  - For Windows Vista and Windows 7 users: C:\ProgramData

Users with limited or standard privileges may sometimes have write access to their program data folders. They could use this access to delete the AnyConnect profile file and thereby circumvent the always-on feature.

- Predeploy a group policy object (GPO) for Windows users to prevent users with limited rights from terminating the GUI. Predeploy equivalent measures for Mac OS users.

**Always-on VPN Requirements**

Support for always-on VPN requires one of the following licensing configurations:

- An AnyConnect Premium license on the ASA.
- An AnyConnect Essentials license on the ASA and a Cisco Secure Mobility for AnyConnect license on the WSA.

Always-on VPN requires a valid server certificate configured on the ASA; otherwise, it fails and logs an event indicating the certificate is invalid.
Ensure your server certificates can pass strict mode if you configure always-on VPN.

Always-on VPN supports computers running the Microsoft Windows and Mac OS X operating systems supported by this release.

To prevent the download of an always-on VPN profile that locks a VPN connection to a rogue server, the AnyConnect client requires a valid, trusted server certificate to connect to a secure gateway.

**Tip**

We strongly recommend purchasing a digital certificate from a certificate authority (CA) and enrolling it on the secure gateways.

If you generate a self-signed certificate, users connecting receive a certificate warning. They can respond by configuring the browser to trust that certificate to avoid subsequent warnings.

**Note**

We do not recommend using a self-signed certificate because of the possibility a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateways.

ASDM provides an Enroll ASA SSL VPN with Entrust button on the Configuration > Remote Access VPN > Certificate Management > Identity Certificates panel to facilitate enrollment of a public certificate to resolve this issue on an ASA. The Add button on this panel lets you import a public certificate from a file or generate a self-signed certificate:

**Figure 3-7** Add Identity Certificate dialog

![Add Identity Certificate dialog](image)

**Note**

These instructions are intended only as a guideline for configuring certificates. For details, click the ASDM Help button, or see the ASDM or CLI guide for the secure gateway you are configuring.

Use the Advanced button to specify the domain name and IP address of the outside interface if you are generating a self-signed interface.
Following the enrollment of a certificate, assign it to the outside interface. To do so, choose Configuration > Remote Access VPN > Advanced > SSL Settings, edit the “outside” entry in the Certificates area, and select the certificate from the Primary Enrolled Certificate drop-down list.

**Figure 3-8 Assigning a Certificate to the Outside Interface (ASDM 6.3 Example)**

Add the certificate to all the secure gateways and associate it with the IP address of the outside interfaces.

**Adding Load-Balancing Backup Cluster Members to the Server List**

Always-on VPN affects the load balancing of AnyConnect VPN sessions. With always-on VPN disabled, when the client connects to a master device within a load balancing cluster, the client complies with a redirection from the master device to any of the backup cluster members. With always-on enabled, the client does not comply with a redirection from the master device unless the address of the backup cluster member is specified in the server list of the client profile. Therefore, be sure to add any backup cluster members to the server list.

To specify the addresses of backup cluster members in the client profile, use ASDM to add a load-balancing backup server list by following these steps:

**Step 1** Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2** Go to the Server List pane.
Step 3 Choose a server that is a master device of a load-balancing cluster and click Edit.

Step 4 Enter an FQDN or IP address of any load-balancing cluster member.

Configuring Always-on VPN

To configure AnyConnect to establish a VPN session automatically only when it detects that the computer is in an untrusted network,

Step 1 Configure TND (see Configuring Trusted Network Detection, page 3-22).

Step 2 Check Always On.

Configuring a Policy to Exempt Users from Always-on VPN

By default, always-on VPN is disabled. You can configure exemptions to override an always-on policy. For example, you might want to let certain individuals establish VPN sessions with other companies or exempt the always-on VPN policy for noncorporate assets.

You can set the always-on VPN parameter in group policies and dynamic access policies to override the always-on policy. Doing so lets you specify exceptions according to the matching criteria used to assign the policy. If an AnyConnect policy enables always-on VPN and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.

The following procedure configures a dynamic access policy that uses AAA or endpoint criteria to match sessions to noncorporate assets, as follows:

Step 1 Choose Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add or Edit.
Step 2 Configure criteria to exempt users from always-on VPN. For example, use the Selection Criteria area to specify AAA attributes to match user logon IDs.

Step 3 Click the AnyConnect tab on the bottom half of the Add or Edit Dynamic Access Policy window.

Step 4 Click Disable next to “Always-On for AnyConnect VPN” client.

If a Cisco AnyConnect Secure Mobility client policy enables always-on VPN and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.

Disconnect Button for Always-on VPN

AnyConnect supports a Disconnect button for always-on VPN sessions. If you enable it, AnyConnect displays a Disconnect button upon the establishment of a VPN session. Users of always-on VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as the following:

- Performance issues with the current VPN session.
- Reconnection issues following the interruption of a VPN session.

The Disconnect button locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session.
**Connect Failure Policy for Always-on VPN**

The connect failure policy determines whether the computer can access the internet if always-on VPN is enabled and AnyConnect cannot establish a VPN session (for example, when a secure gateway is unreachable). The fail-close policy disables network connectivity—except for VPN access. The fail-open policy permits network connectivity. Regardless of the connect failure policy, AnyConnect continues to try to establish the VPN connection. The following table explains the fail open and fail close policies:

---

**Caution**

Disabling the Disconnect button can at times hinder or prevent VPN access.

If the user clicks Disconnect during an always-on VPN session, AnyConnect locks all interfaces to prevent data from leaking out and protects the computer from internet access except for that required to establish a new VPN session. AnyConnect locks all interfaces, regardless of the connect failure policy.

---

**Caution**

The Disconnect locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. For the reasons noted above, disabling the Disconnect button can at times hinder or prevent VPN access.

---

**Disconnect Button Requirements**

The requirements for the disconnect option for always-on VPN match those in the “Always-on VPN Requirements” section on page 3-24.

---

**Enabling and Disabling the Disconnect Button**

By default, the profile editor enables the Disconnect button when you enable always-on VPN. You can view and change the Disconnect button setting, as follows:

**Step 1**

Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2**

Go to the Preferences (Part 2) pane.

**Step 3**

Check or uncheck Allow VPN Disconnect.

---
Chapter 3  Configuring VPN Access

Connect Failure Policy for Always-on VPN

Connect Failure Policy Requirements

Support for the connect failure policy feature requires one of the following licenses:

- AnyConnect Premium (SSL VPN Edition)
- Cisco AnyConnect Secure Mobility

You can use a Cisco AnyConnect Secure Mobility license to provide support for the connect failure policy in combination with either an AnyConnect Essentials or an AnyConnect Premium license.

The connect failure policy supports only computers running Microsoft Windows 7, Vista, or XP and Mac OS X 10.6 and 10.7.
Configuring a Connect Failure Policy

By default, the connect failure policy prevents Internet access if always-on VPN is configured and the VPN is unreachable. To configure a connect failure policy,

**Step 1** Configure TND (see Configuring Trusted Network Detection, page 3-22).

**Step 2** Check Always On.

**Step 3** Set the Connect Failure Policy parameter to one of the following settings:

- **Closed**—(Default) Restricts network access when the secure gateway is unreachable. AnyConnect does this by enabling packet filters that block all traffic from the endpoint that is not bound for a secure gateway to which the computer is allowed to connect.

  The fail-closed policy prevents captive portal remediation (described in the next sections) unless you specifically enable it as part of the policy. The restricted state permits the application of the local resource rules imposed by the most recent VPN session if Apply Last VPN Local Resources is enabled in the client profile. For example, these rules could determine access to active sync and local printing. The network is unblocked and open during an AnyConnect software upgrade when Always-On is enabled. The purpose of the Closed setting is to help protect corporate assets from network threats when resources in the private network that protect the endpoint are not available.

- **Open**—This setting permits network access by browsers and other applications when the client cannot connect to the ASA. An open connect failure policy does not apply if you enable the Disconnect button and the user clicks Disconnect.
Captive Portal Hotspot Detection and Remediation

Many facilities that offer Wi-Fi and wired access, such as airports, coffee shops, and hotels, require the user to pay before obtaining access, agree to abide by an acceptable use policy, or both. These facilities use a technique called captive portal to prevent applications from connecting until the user opens a browser and accepts the conditions for access.

The following sections describe the captive portal detection and remediation features.

Captive Portal Remediation Requirements

Support for both captive portal detection and remediation requires one of the following licenses:

- AnyConnect Premium (SSL VPN Edition)
- Cisco AnyConnect Secure Mobility

You can use a Cisco AnyConnect Secure Mobility license to provide support for captive portal detection and remediation in combination with either an AnyConnect Essentials or an AnyConnect Premium license.

Captive portal detection and remediation is supported on the Microsoft Windows and Mac OS X operating systems supported by this release of AnyConnect.

Captive Portal Hotspot Detection

AnyConnect displays the “Unable to contact VPN server” message on the GUI if it cannot connect, regardless of the cause. VPN server specifies the secure gateway. If always-on is enabled, and a captive portal is not present, the client continues to attempt to connect to the VPN and updates the status message accordingly.

If always-on VPN is enabled, the connect failure policy is closed, captive portal remediation is disabled, and AnyConnect detects the presence of a captive portal, the AnyConnect GUI displays the following message once per connection and once per reconnect:

The service provider in your current location is restricting access to the Internet. The AnyConnect protection settings must be lowered for you to log on with the service provider. Your current enterprise security policy does not allow this.

If AnyConnect detects the presence of a captive portal and the AnyConnect configuration differs from that described above, the AnyConnect GUI displays the following message once per connection and once per reconnect:

The service provider in your current location is restricting access to the Internet. You need to log on with the service provider before you can establish a VPN session. You can try this by visiting any website with your browser.

Captive portal detection is enabled by default, and is non-configurable.

AnyConnect does not modify any browser configuration settings during Captive Portal detection.
Captive Portal Hotspot Remediation

_Captive portal remediation_ is the process of satisfying the requirements of a captive portal hotspot to obtain network access.

AnyConnect does not remediate the captive portal, it relies on the end user to perform the remediation. The end user performs the captive portal remediation by meeting the requirements of the provider of the hotspot. These requirements could be paying a fee to access the network, signing an acceptable use policy, both, or some other requirement defined by the provider.

Captive portal remediation needs to be explicitly allowed in an AnyConnect VPN Client profile if AnyConnect Always-on is enabled and the Connect failure policy is set to **Closed**. If Always-on is enabled and the Connect Failure policy is set to **Open**, you don’t need to explicitly allow captive portal remediation in an AnyConnect VPN Client profile because the user is not restricted from getting access to the network.

Configuring Support for Captive Portal Hotspot Remediation

You need to enable captive portal remediation in an AnyConnect VPN client policy if the Always-on feature is enabled and the connect failure policy is set to closed. If the connect failure policy is set to open, your users are not restricted from network access, and so, are capable of remediating a captive portal without any other configuration of the AnyConnect VPN client policy.

By default, support for captive portal remediation is disabled. Use this procedure to enable captive portal remediation:

---

**Step 1** Configure a connect failure policy (see Configuring a Connect Failure Policy, page 3-31).

**Step 2** If you set the connect failure policy to closed, configure the following parameters:

- **Allow Captive Portal Remediation**—Check to let the Cisco AnyConnect Secure Mobility client lift the network access restrictions imposed by the closed connect failure policy. By default, this parameter is unchecked to provide the greatest security; however, you must enable it if you want the client to connect to the VPN if a captive portal is preventing it from doing so.

- **Remediation Timeout**—Enter the number of minutes that AnyConnect lifts the network access restrictions. The user needs enough time to satisfy the captive portal requirements.

If always-on VPN is enabled, and the user clicks **Connect**, or a reconnect is in progress, a message window indicates the presence of a captive portal. The user can then open a web browser window to remediate the captive portal.

---

If Users Cannot Access a Captive Portal Page

If users cannot access a captive portal remediation page, ask them to try the following steps until they can remediate:

---

**Step 1** Disable and re-enable the network interface. This action triggers a captive portal detection retry.

**Step 2** Terminate any applications that use HTTP, such as instant messaging programs, e-mail clients, IP phone clients, and all but one browser to perform the remediation. The captive portal may be actively inhibiting DoS attacks by ignoring repetitive attempts to connect, causing them to time out on the client end. The attempt by many applications to make HTTP connections exacerbates this problem.
False Captive Portal Detection

AnyConnect can falsely assume it is in a captive portal in the following situations.

- If AnyConnect attempts to contact an ASA with a certificate containing an incorrect server name (CN), then the AnyConnect client will think it is in a “captive portal” environment.
  
  To prevent this, make sure the ASA certificate is properly configured. The CN value in the certificate must match the name of the ASA server in the VPN client profile.

- If there is another device on the network before the ASA, and that device responds to the client's attempt to contact an ASA by blocking HTTPS access to the ASA, then the AnyConnect client will think it is in a “captive portal” environment. This situation can occur when a user is on an internal network, and connects through a firewall to connect to the ASA.

  If you need to restrict access to the ASA from inside the corporation, configure your firewall such that HTTP and HTTPS traffic to the ASA's address does not return an HTTP status. HTTP/HTTPS access to the ASA should either be allowed or completely blocked (also known as black-holed) to ensure that HTTP/HTTPS requests sent to the ASA will not return an unexpected response.

Client Firewall with Local Printer and Tethered Device Support

When users connect to the ASA, all traffic is tunneled through the connection and users cannot access resources on their local network. This includes printers, cameras, and tethered devices that synchronize with the local computer. Enabling Local LAN Access in the client profile resolves this problem, however it can introduce a security or policy concern for some enterprises because it allows unrestricted access to the local network. You can use the ASA to deploy endpoint OS firewall capabilities to restrict access to particular types of local resources, such as printers and tethered devices.

To do so, enable client firewall rules for specific ports for printing. The client distinguishes between inbound and outbound rules. For printing capabilities, the client opens ports required for outbound connections, but blocks all incoming traffic.

The Client Firewall feature is supported on the Windows, Mac OS X, and Linux operating systems supported by this release.

Note

Be aware that users logged in as administrators have the ability to modify the firewall rules deployed to the client by the ASA. Users with limited privileges cannot modify the rules. For either user, the client reapplies the firewall rules when the connection terminates.

If you configure the client firewall, and the user authenticates to an Active Directory (AD) server, the client still applies the firewall policies from the ASA. However, the rules defined in the AD group policy take precedence over the rules of the client firewall.

The following sections describe procedures on how to do this:

- Deploying a Client Firewall for Local Printer Support, page 3-35
- Tethered Devices Support, page 3-37
Usage Notes about Firewall Behavior

The following notes clarify how the AnyConnect client uses the firewall:

- The source IP is not used for firewall rules. The client ignores the source IP information in the firewall rules sent from the ASA. The client determines the source IP depending on whether the rules are public or private. Public rules are applied to all interfaces on the client. Private rules are applied to the Virtual Adapter.

- The ASA supports many protocols for ACL rules. However, the AnyConnect firewall feature supports only TCP, UDP, ICMP, and IP. If the client receives a rule with a different protocol, it treats it as an invalid firewall rule, and then disables split tunneling and uses full tunneling for security reasons.

- Starting in ASA 9.0, the Public Network Rule and Private Network Rule support unified access control lists. These access control lists can be used to define IPv4 and IPv6 traffic in the same rule.

Be aware of the following differences in behavior for each operating system:

- For Windows computers, deny rules take precedence over allow rules in Windows Firewall. If the ASA pushes down an allow rule to the AnyConnect client, but the user has created a custom deny rule, the AnyConnect rule is not enforced.

- On Windows Vista, when a firewall rule is created, Vista takes the port number range as a comma-separated string. The port range can be a maximum of 300 ports. For example, from 1-300 or 5000-5300. If you specify a range greater than 300 ports, the firewall rule is applied only to the first 300 ports.

- Windows users whose firewall service must be started by the AnyConnect client (not started automatically by the system) may experience a noticeable increase in the time it takes to establish a VPN connection.

- On Mac computers, the AnyConnect client applies rules sequentially in the same order the ASA applies them. Global rules should always be last.

- For third-party firewalls, traffic is passed only if both the AnyConnect client firewall and the third-party firewall allow that traffic type. If the third-party firewall blocks a specific traffic type that the AnyConnect client allows, the client blocks the traffic.

- For Linux systems, starting with AnyConnect version 3.1.05149, you can configure AnyConnect to evaluate the client's firewall and filter rules. To configure AnyConnect to allow local firewall and filter rules, add a custom attribute named circumvent-host-filtering to a group profile, and set it to true.

Deploying a Client Firewall for Local Printer Support

The ASA supports the AnyConnect client firewall feature with ASA version 8.3(1) or later, and ASDM version 6.3(1) or later. This section describes how to configure the client firewall to allow access to local printers, and how to configure the client profile to use the firewall when the VPN connection fails.

Limitations and Restrictions of the Client Firewall

The following limitations and restrictions apply to using the client firewall to restrict local LAN access:

- Due to limitations of the OS, the client firewall policy on computers running Windows XP is enforced for inbound traffic only. Outbound rules and bidirectional rules are ignored. This would include firewall rules such as 'permit ip any any'.

- Host Scan and some third-party firewalls can interfere with the firewall.
The following table clarifies what direction of traffic is affected by the source and destination port settings:

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Destination Port</th>
<th>Traffic Direction Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific port number</td>
<td>Specific port number</td>
<td>Inbound and outbound</td>
</tr>
<tr>
<td>A range or 'All' (value of 0)</td>
<td>A range or 'All' (value of 0)</td>
<td>Inbound and outbound</td>
</tr>
<tr>
<td>Specific port number</td>
<td>A range or 'All' (value of 0)</td>
<td>Inbound only</td>
</tr>
<tr>
<td>A range or 'All' (value of 0)</td>
<td>Specific port number</td>
<td>Outbound only</td>
</tr>
</tbody>
</table>

**Example ACL Rules for Local Printing**

The ACL AnyConnect_Client_Local_Print is provided with ASDM to make it easy to configure the client firewall. When you select that ACL for Public Network Rule in the Client Firewall pane of a group policy, that list contains the following ACEs:

**Table 3-2  ACL Rules in AnyConnect_Client_Local_Print**

<table>
<thead>
<tr>
<th>Description</th>
<th>Permission</th>
<th>Interface</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny all</td>
<td>Deny</td>
<td>Public</td>
<td>Any</td>
<td>Default¹</td>
<td>Any</td>
<td>Default</td>
</tr>
<tr>
<td>LPD</td>
<td>Allow</td>
<td>Public</td>
<td>TCP</td>
<td>Default</td>
<td>Any</td>
<td>515</td>
</tr>
<tr>
<td>IPP</td>
<td>Allow</td>
<td>Public</td>
<td>TCP</td>
<td>Default</td>
<td>Any</td>
<td>631</td>
</tr>
<tr>
<td>Printer</td>
<td>Allow</td>
<td>Public</td>
<td>TCP</td>
<td>Default</td>
<td>Any</td>
<td>9100</td>
</tr>
<tr>
<td>mDNS</td>
<td>Allow</td>
<td>Public</td>
<td>UDP</td>
<td>Default</td>
<td>224.0.0.251</td>
<td>5353</td>
</tr>
<tr>
<td>LLMNR</td>
<td>Allow</td>
<td>Public</td>
<td>UDP</td>
<td>Default</td>
<td>224.0.0.252</td>
<td>5355</td>
</tr>
<tr>
<td>NetBios</td>
<td>Allow</td>
<td>Public</td>
<td>TCP</td>
<td>Default</td>
<td>Any</td>
<td>137</td>
</tr>
<tr>
<td>NetBios</td>
<td>Allow</td>
<td>Public</td>
<td>UDP</td>
<td>Default</td>
<td>Any</td>
<td>137</td>
</tr>
</tbody>
</table>

¹. The port range is 1 to 65535.

**Note**

To enable local printing, you must enable the **Local LAN Access** feature in the client profile. If you do this with the CLI, you must add an ACL rule `allow Any Any`.

**Configuring Local Print Support**

**Step 1**
Enable the AnyConnect client firewall in a group policy. Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

**Step 2**
Select a group policy and click **Edit**. The Edit Internal Group Policy window displays.

**Step 3**
Select **Advanced > AnyConnect Client > Client Firewall**. Click **Manage** for the Private Network Rule.

**Step 4**
Create an ACL and specify an ACE using the rules in **Table 3-2**. Add this ACL as a Public Network Rule.

**Step 5**
If you enabled the Automatic VPN Policy always-on and specified a closed policy, in the event of a VPN failure, users have no access to local resources. You can apply the firewall rules in this scenario by going to **Preferences (Cont) in the profile editor and checking Apply last local VPN resource rules**.
Tethered Devices Support

To support tethered devices and protect the corporate network, create a standard ACL in the group policy, specifying destination addresses in the range that the tethered devices use. Then specify the ACL for split tunneling as a network list to exclude from tunneled VPN traffic. You must also configure the client profile to use the last VPN local resource rules in case of VPN failure.

Follow these steps:

Step 1 In ASDM, go to Group Policy > Advanced > Split Tunneling.
Step 2 Uncheck Inherit next to the Network List field and click Manage. The ACL Manager displays.
Step 3 Click the Extended ACL tab.
Step 4 Click Add and then Add ACL. Specify a name for the new ACL.
Step 5 Choose the new ACL in the table and click Add and then Add ACE. The Edit ACE window displays.
Step 6 For Action, choose the Permit radio button.
Step 7 In the destination criteria area, specify the IPv4 destination address as 169.254.0.0 or the IPv6 destination address fe80::/64.
Step 8 For Service, choose IP.
Step 9 Click OK.
Step 10 Click OK to save the ACL.
Step 11 In the Split Tunneling pane for the internal group policy, uncheck Inherit for the Policy or IPv6 Policy, depending on the IP address you specified in step 7, and choose Exclude Network List Below. For Network List, choose the ACL you created.
Step 12 Click OK.
Step 13 Click Apply.

New Installation Directory Structure for Mac OS X

In previous releases of AnyConnect, AnyConnect components were installed in the opt/cisco/vpn path. In release 3.0.4 or later, AnyConnect components are installed in the /opt/cisco/anyconnect path.

ScanCenter Hosted Configuration Support for Web Security Client Profile

The ScanCenter Hosted Configuration for the Web Security Hosted Client Profile gives administrators the ability to provide new Web Security client profiles to Web Security clients. Devices with Web Security can download a new client profile from the cloud (hosted configuration files reside on the ScanCenter server). The only prerequisite for this feature is for the device to have Web Security installed with a valid client profile.
Administrators use the Web Security Profile Editor to create the client profile files and then upload the clear text XML file to a ScanCenter server. This XML file must contain a valid license key from ScanSafe. The Hosted Configuration feature uses the license key when retrieving a new client profile file from the Hosted Configuration (ScanCenter) server. Once the new client profile file is on the server, devices with Web Security automatically poll the server and download the new client profile file, provided that the license in the existing Web Security client profile is the same as a license associated with a client profile on the Hosted server. Once a new client profile has been downloaded, Web Security will not download the same file again until the administrator makes a new client profile file available.

**Note**

Web Security client devices must be pre-installed with a valid client profile file containing a ScanSafe license key before it can use the Hosted Configuration feature.

### Configuring DNS and WINS Servers for AnyConnect

DNS Servers and WINS servers are configured in a Network (Client) Access group policy. See Configuring Server Attributes for an Internal Group Policy in the General VPN Setup chapter of the Cisco ASA Series VPN ASDM Configuration Guide.

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy.**

### Configuring Split Tunneling


After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy.**

### Split DNS

When split DNS is configured in the Network (Client) Access group policy, AnyConnect tunnels specific DNS queries to the private DNS server (also configured in the group policy). All other DNS queries go to the DNS resolver on the client operating system, in the clear, for DNS resolution. If split DNS is not configured, AnyConnect tunnels all DNS queries.

### Requirements for Split DNS

Split DNS supports standard and update queries (including A, AAAA, NS, TXT, MX, SOA, ANY, SRV, PTR, and CNAME). PTR queries matching any of the tunneled networks are allowed through the tunnel. AnyConnect split DNS is supported on Windows and Mac OS X platforms.

For Mac OS X, AnyConnect can use true split-DNS for a certain IP protocol only if one of the following conditions is met:
- split-DNS is configured for one IP protocol (such as IPv4), and Client Bypass Protocol is configured for the other IP protocol (such as IPv6) in the group policy (with no address pool configured for the latter IP protocol).
- split-DNS is configured for both IP protocols

## Configuring Split DNS

To configure split DNS in the group policy do the following:

1. Configure at least one DNS server:
   

   Ensure the private DNS servers specified do not overlap with the DNS servers configured for the client platform. If they do, name resolution does not function properly and queries may be dropped.

   Refer to Configuring Split Tunneling for an Internal Group Policy in the General VPN Setup chapter of the Cisco ASA Series VPN ASDM Configuration Guide, for the remainder of the configuration steps.

2. Configure split-include tunneling:
   
   On the Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling pane, choose the Tunnel Network List Below policy, and specify a Network List of addresses to be tunneled.

   Split-DNS does not support the Exclude Network List Below split-tunneling policy. You must use the Tunnel Network List Below split-tunneling policy to configure split-DNS.

3. Configure split DNS:
   
   On the Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling pane, uncheck Send All DNS lookups through tunnel, and specifying the names of the domains whose queries will be tunneled in DNS Names.

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy.

## Verify Split DNS Using AnyConnect Logs

To verify if split-DNS is enabled, search the AnyConnect logs for an entry containing “Received VPN Session Configuration Settings.” That entry indicates Split DNS:enabled when enabled. There are separate log entries for IPv4 and IPv6 split DNS.

## Checking Which Domains Use Split DNS

You can use any tool or application that relies on the operating system’s DNS resolver for domain name resolution. For example, you can use a ping or web browser to test the split DNS solution. Other tools such as nslookup or dig circumvent the OS DNS resolver.

To use the client to check which domains are used for split DNS, follow these steps:

### Step 1

Run `ipconfig/all` and record the domains listed next to DNS Suffix Search List.
Establish a VPN connection and again check the domains listed next to DNS Suffix Search List. Those extra domains added after establishing the tunnel are the domains used for split DNS.

**Note** This process assumes that the domains pushed from the ASA do not overlap with the ones already configured on the client host.

### Network Roaming

AnyConnect 3.1 supports roaming between IPv4 and IPv6 networks. The AnyConnect client uses the fully qualified domain name (FQDN) of the ASA to maintain the connection to that secure gateway as AnyConnect moves between the two types of networks.

In order to accommodate roaming between NAT46 and NAT64 enabled networks (which typically also involves DNS46 and DNS64 configurations), the client performs name resolution of the ASA FQDN whenever network roaming is detected during the VPN session to determine the ASA IP address to use for re-establishing the VPN session.

In ASA environments using load-balancing, it is not feasible to determine why the profile FQDN cannot be resolved during roaming without setting the FQDN of the ASA. That is because you cannot guarantee that the IP address of the ASA the clients first reach belongs to the ASA of the device they are connected to.

**Note** The mentioned ASA FQDN is not the profile FQDN used to originally establish the VPN tunnel, it is the ASA device FQDN pushed to client during the tunnel establishment.

### Prerequisite

Configuring Network Roaming between IPv4 and IPv6 networks is configured in the group policy on the ASA.

See “Configuring Network (Client) Access Internal Group Policies” in Chapter 73, General VPN Setup in the *ASA Series ASDM Configuration Guide* for instructions on how to add or edit an internal group policy.

### Configuring Network Roaming Between IPv4 and IPv6 Networks

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

**Step 2** Select the group policy you are going to configure and click **Edit**.

**Step 3** Click **Advanced > AnyConnect** in the Edit Internal Group Policy page.

**Step 4** In the FQDN row, uncheck FQDN and add the FQDN of the ASA in the FQDN text box.

If the above is not set, the ASA pushes the FQDN defined in the Hostname and Domain Name fields on the ASA in this location: **Configuration > Device Setup > Device Name/Password**. The domain name must be filled in to make it an FQDN.
Configuring Certificate Enrollment using SCEP

About Certificate Enrollment using SCEP

The AnyConnect Secure Mobility Client can use the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate as part of client authentication. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology.

Certificate enrollment using SCEP is supported by AnyConnect IPsec and SSL VPN connections to the ASA in the following ways:

- **SCEP Proxy:** The ASA acts as a proxy for SCEP requests and responses between the client and the CA.
  - The CA must be accessible to the ASA, not the AnyConnect client, since the client does not access the CA directly.
  - Enrollment is always initiated automatically by the client. No user involvement is necessary.
  - SCEP Proxy is supported in AnyConnect 3.0 and higher.

- **Legacy SCEP:** The AnyConnect client communicates with the CA directly to enroll and obtain a certificate.
  - The CA must be accessible to the AnyConnect client, not the ASA, through an established VPN tunnel or directly on the same network the client is on.
  - Enrollment is initiated automatically by the client and may be initiated manually by the user if configured.
  - Legacy SCEP is supported in AnyConnect 2.4 and higher.

**SCEP Proxy Enrollment**

The following steps describe the process in which a certificate is obtained and a certificate-based connection is made when AnyConnect and the ASA are configured for SCEP Proxy.

1. The user connects to the ASA headend using a connection profile configured for both certificate and AAA authentication. The ASA requests a certificate and AAA credentials for authentication from the client.

2. The user enters their AAA credentials but a valid certificate is not available. This situation triggers the client to send an automatic SCEP enrollment request after the tunnel has been established using the entered AAA credentials.

3. The ASA forwards the enrollment request to the CA and returns the CA’s response to the client.

4. If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to an ASA tunnel group.
If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact their administrator.

**SCEP Proxy Notes**
- The client automatically renews the certificate before it expires, without user intervention, if the Certificate Expiration Threshold field is set in the VPN profile.
- SCEP Proxy enrollment requires the use of SSL for both SSL and IPsec tunnel certificate authentication.

**Legacy SCEP Enrollment**

The following steps describe the process in which a certificate is obtained and a certificate-based connection is made when AnyConnect is configured for Legacy SCEP.

1. The user initiates a connection to the ASA headend using a tunnel group configured for certificate authentication. The ASA requests a certificate for authentication from the client.
2. A valid certificate is not available on the client, the connection cannot be established. This certificate failure indicates that SCEP enrollment needs to occur.
3. The user must then initiate a connection to the ASA headend using a tunnel group configured for AAA authentication only whose address matches the Automatic SCEP Host configured in the client profile. The ASA requests the AAA credentials from the client.
4. The client presents a dialog box for the user to enter their AAA credentials.
   - If the client is configured for manual enrollment and the client knows it needs to initiate SCEP enrollment (see Step 2), a **Get Certificate** button will display on the credentials dialog box. If the client has direct access to the CA on their network, the user will be able to manually obtain a certificate by clicking this button at this time.
   - **Note** If access to the CA relies on the VPN tunnel being established, manual enrollment cannot be done at this time since there is currently no VPN tunnel established (AAA credentials have not been entered).
5. The user enters their AAA credentials and establishes a VPN connection.
6. The client knows it needs to initiate SCEP enrollment (see Step 2), it initiates an enrollment request to the CA through the established VPN tunnel, and a response is received from the CA.
7. If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to an ASA tunnel group.
   - If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact their administrator.
8. If the client is configured for manual enrollment and the Certificate Expiration Threshold value is met, a **Get Certificate** button will display on a presented tunnel group selection dialog box. The user will be able to manually renew their certificate by clicking this button.

**Legacy SCEP Notes**
- If you use manual Legacy SCEP enrollment, we recommend you enable CA Password in the client profile. The CA Password is the challenge password or token that is sent to the certificate authority to identify the user.
• If the certificate expires and the client no longer has a valid certificate, the client repeats the Legacy SCEP enrollment process.

**SCEP Guidelines and Limitations**

• ASA Load balancing is supported with SCEP enrollment.
• Clientless (browser-based) VPN access to the ASA does not support SCEP proxy, but WebLaunch (clientless-initiated AnyConnect) does.
• The ASA does not indicate why an enrollment failed, although it does log the requests received from the client. Connection problems must be debugged on the CA or the client.
• All SCEP-compliant CAs, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA are supported.
• The CA must be in auto-grant mode; polling for certificates is not supported.
• Some CA’s can be configured to email users an enrollment password, this provides an additional layer of security. The password can also be configured in the AnyConnect client profile, which becomes part of SCEP request that the CA verifies before granting the certificate.

**Windows Certificate Warning**

When Windows clients first attempt to retrieve a certificate from a certificate authority they may see a warning. When prompted, users must click **Yes**. This allows them to import the root certificate. It does not affect their ability to connect with the client certificate.

**Identifying Enrollment Connections to Apply Policies**

On the ASA, the aaa.cisco.sceprequired attribute can be used to catch the enrollment connections and apply the appropriate policies in the selected DAP record.

**Certificate-Only Authentication and Certificate Mapping on the ASA**

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

**Configuring SCEP Proxy Certificate Enrollment**

**Configuring a VPN Client Profile for SCEP Proxy Enrollment**

**Step 1** Launch the Profile Editor from ASDM, or use the stand-alone VPN Profile Editor (see the Creating and Editing an AnyConnect Profile, page 3-9).

**Step 2** In the ASDM, Click **Add** (or **Edit**) to create (or edit) an AnyConnect Profile. On the stand-alone editor, open an existing profile or continue to create a new one.
Chapter 3 Configuring VPN Access

Configuring Certificate Enrollment using SCEP

Step 3 Click **Certificate Enrollment** in the AnyConnect Client Profile tree on the left.

Step 4 In the **Certificate Enrollment** pane, check **Certificate Enrollment**.

Step 5 Configure the **Certificate Contents** to be requested in the enrollment certificate. For definitions of the certificate fields, see AnyConnect Profile Editor, Certificate Enrollment, page 3-84.

**Note**
- If you use `%machineid%`, then Hostscan/Posture must be loaded for the desktop client.
- For mobile clients, at least one certificate field must be specified.

---

Configuring the ASA to support SCEP Proxy Enrollment

For SCEP Proxy, a single ASA connection profile supports certificate enrollment and the certificate authorized VPN connection.

**Prerequisite**
Configure a client profile for SCEP Proxy, for example, ac_vpn_scep_proxy. See Configuring a VPN Client Profile for SCEP Proxy Enrollment, page 3-43.

Step 1 Create a group policy, for example, cert_group. Set the following fields:
- On General, enter the URL to the CA in **SCEP Forwarding URL**.
- On the Advanced > AnyConnect Client pane, uncheck **Inherit for Client Profiles to Download** and specify the client profile configured for SCEP Proxy. For example, specify the ac_vpn_scep_proxy client profile.

Step 2 Create a connection profile for certificate enrollment and certificate authorized connection, for example, cert_tunnel.
- Authentication: Both (AAA and Certificate)
- Default Group Policy: cert_group
- On Advanced > General, check **Enable SCEP Enrollment for this Connection Profile**.
- On Advanced > GroupAlias/Group URL, create a Group URL containing the group (cert_group) for this connection profile.

---

Configuring Legacy SCEP Certificate Enrollment

Configuring a VPN Client Profile for Legacy SCEP Enrollment

Step 1 Launch the Profile Editor from ASDM, or use the stand-alone VPN Profile Editor (see the Creating and Editing an AnyConnect Profile, page 3-9).

Step 2 In the ASDM, Click Add (or Edit) to create (or edit) an AnyConnect Profile. On the stand-alone editor, open an existing profile or continue to create a new one.

Step 3 Click **Certificate Enrollment** in the AnyConnect Client Profile tree on the left.

Step 4 In the **Certificate Enrollment** pane, check **Certificate Enrollment**.

Step 5 Specify an **Automatic SCEP Host** to direct the client to retrieve the certificate.
Enter the FQDN or IP address, and the alias of the connection profile (tunnel group) that is configured for SCEP certificate retrieval. For example, if asa.cisco.com is the host name of the ASA and scep_eng is the alias of the connection profile, enter asa.cisco.com/scep-eng.

When the user initiates the connection, the address chosen or specified must match this value exactly for Legacy SCEP enrollment to succeed. For example, if this field is set to an FQDN, but the user specifies an IP address, SCEP enrollment will fail.

**Step 6**

Configure the Certificate Authority attributes:

- **Note**
  Your CA server administrator can provide the CA URL and thumbprint. Retrieve the thumbprint directly from the server, not from a “fingerprint” or “thumbprint” attribute field in an issued certificate.

  a. Specify a CA URL to identify the SCEP CA server. Enter an FQDN or IP Address. For example: http://ca01.cisco.com/certsrv/mscep/mscep.dll.

  b. (Optional) Check Prompt For Challenge PW to prompt the user for their username and one-time password.

  c. (Optional) Enter a Thumbprint for the CA certificate. Use SHA1 or MD5 hashes. For example: 8475B661D2E341D4B223A464E6AA8B8CA123AB.

**Step 7**

Configure the Certificate Contents to be requested in the enrollment certificate. For definitions of the certificate fields, see AnyConnect Profile Editor, Certificate Enrollment, page 3-84.

- **Note**
  If you use %machineid%, then Hostscan/Posture must be loaded on the client.

**Step 8**

(Optional) Check Display Get Certificate Button to permit users to manually request provisioning or renewal of authentication certificates. The button is visible to users if the certificate authentication fails.

**Step 9**

(Optional) Enable SCEP for a specific host in the server list. Doing this overrides the SCEP settings in the Certificate Enrollment pane described above.

  a. Click Server List in the AnyConnect Client Profile tree on the left to go to the Server List pane.

  b. Add or Edit a server list entry.

  c. Specify the Automatic SCEP Host and Certificate Authority attributes as described in Steps 5 and 6 above.

---

### Configuring the ASA to support Legacy SCEP Enrollment

For Legacy SCEP on the ASA, a connection profile and group policy must be created for certificate enrollment, and a second connection profile and group policy must be created for the certificate authorized VPN connection.

**Prerequisite**

Configure a client profile for Legacy SCEP, for example, ac_vpn__legacy_scep. See Configuring a VPN Client Profile for Legacy SCEP Enrollment, page 3-44.

**Step 1**

Create a group policy for enrollment, for example, cert_enroll_group. Set the following fields:
• On the Advanced > AnyConnect Client pane, uncheck **Inherit for Client Profiles to Download** and specify the client profile configured for Legacy SCEP. For example, specify the `ac_vpn_legacy_scep` client profile.

**Step 2** Create a second group policy for authorization, for example, `cert_auth_group`.

**Step 3** Create a connection profile for enrollment, for example, `cert_enroll_tunnel`. Set the following fields:
  • On the Basic pane, set the Authentication Method to AAA.
  • On the Basic pane, set the Default Group Policy to `cert_enroll_group`.
  • On Advanced > GroupAlias/Group URL, create a Group URL containing the enrollment group (`cert_enroll_group`) for this connection profile.
  • Do not enable the connection profile on the ASA. It is not necessary to expose the group to users in order for them to have access to it.

**Step 4** Create a connection profile for authorization, for example, `cert_auth_tunnel`. Set the following fields.
  • On the Basic pane, set the Authentication Method to Certificate.
  • On the Basic pane, set the Default Group Policy to `cert_auth_group`.
  • Do not enable this connection profile on the ASA. It is not necessary to expose the group to users in order for them to access it.

**Step 5** (Optional) On the General pane of each group policy, set **Connection Profile (Tunnel Group) Lock** to the corresponding SCEP connection profile, which restricts traffic to the SCEP-configured connection profile.

---

**Using a Windows 2008 Server Certificate Authority for SCEP**

If your Certificate Authority software is running on a Windows 2008 server, you may need to make one of the following configuration changes to the server to support SCEP with AnyConnect.

**Disabling the SCEP Password on the Certificate Authority**

The following steps describe how to disable the SCEP challenge password, so clients will not need to provide an out-of-band password before SCEP enrollment.

**Step 1** On the Certificate Authority server, launch the Registry Editor. You can do this by selecting Start > Run, typing `regedit`, and clicking **OK**.

**Step 2** Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword`. If the EnforcePassword key doesn't exist, create it as a new Key.

**Step 3** Edit EnforcePassword, and set it to '0'. If it doesn't exist, create it as a REG-DWORD.

**Step 4** Exit regedit, and reboot the certificate authority server.

**Setting the SCEP Template on the Certificate Authority**

The following steps describe how to create a certificate template, and assign it as the default SCEP template.

**Step 1** Launch the Server Manager. You can do this by selecting Start > Admin Tools > Server Manager.
Step 2 Expand Roles > Certificate Services (or AD Certificate Services).
Step 3 Navigate to CA Name > Certificate Templates.
Step 4 Right click Certificate Templates > Manage.
Step 5 From the Cert Templates Console, right click User template and choose Duplicate
Step 6 Choose **Windows Server 2008 version** for new template, and click **OK**.
Step 7 Change the template display name to something descriptive, such as NDES-IPSec-SSL.
Step 8 Adjust the Validity Period for your site. Most sites choose three or more years to avoid expired certificates.
Step 9 On the Cryptography tab, set the minimum key size for your deployment. We recommend that you specify a key size of at least **2048**.
Step 10 On the Subject Name tab, select **Supply in Request**.
Step 11 On the Extensions tab, set the Application Policies to include at least:
   - Client Authentication
   - IP security end system
   - IP security IKE intermediate
   - IP security tunnel termination
   - IP security user

These values are valid for SSL or IPSec.
Step 12 Click **Apply**, then **OK** to save new template.
Step 13 From Server manager > Certificate Services-CA Name, right click Certificate Templates, select New > Certificate Template to Issue, select the new template you created (in this example, NDES-IPSec-SSL), and click **OK**.
Step 14 Edit the registry. You can do this by selecting Start > Run, regedit, and clicking **OK**.
Step 15 Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP.
Step 16 Set the value of the following 3 keys to **NDES-IPSec-SSL**.
   - EncryptionTemplate
   - GeneralPurposeTemplate
   - SignatureTemplate
Step 17 17. Click **Save**, and reboot the certificate authority server.

---

**Configuring Certificate Expiration Notice**

Configure AnyConnect to warn users that their authentication certificate is about to expire. The **Certificate Expiration Threshold** setting specifies the number of days before the certificate’s expiration date that AnyConnect warns users that their certificate is expiring. AnyConnect warns the user upon each connect until the certificate has actually expired or a new certificate has been acquired.

**Note**
The Certificate Expiration Threshold feature cannot be used with RADIUS.
Step 1 Launch the Profile Editor from ASDM, or use the stand-alone VPN Profile Editor (see the Creating and Editing an AnyConnect Profile, page 3-9).

Step 2 In the ASDM, Click Add (or Edit) to create (or edit) an AnyConnect Profile. On the stand-alone editor, open an existing profile or continue to create a new one.

Step 3 Click Certificate Enrollment in the AnyConnect Client Profile tree on the left.

Step 4 In the Certificate Enrollment pane, check Certificate Enrollment.

Step 5 Specify a Certificate Expiration Threshold.
   This is the number of days before the certificate expiration date, that AnyConnect warns users that their certificate is going to expire.
   The default is 0 (no warning displayed). The range is 0-180 days.

Step 6 Click OK.

---

### Configuring a Certificate Store

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

For Windows, you can control which certificate store the client uses for locating certificates. You may want to configure the client to restrict certificate searches to only the user store or only the machine store. For Mac and Linux, you can create a certificate store for PEM-format certificate files.

These certificate store search configurations are stored in the AnyConnect client profile.

---

**Note**

You can also configure more certificate store restrictions in the AnyConnect local policy. The AnyConnect local policy is an XML file you deploy using enterprise software deployment systems and is separate from the AnyConnect client profile. The settings in the file restrict the use of the Firefox NSS (Linux and Mac), PEM file, Mac native (keychain) and Windows Internet Explorer native certificate stores. For more information, see Chapter 8, “Enabling FIPS and Additional Security.”

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

- Controlling the Certificate Store on Windows, page 3-48
- Creating a PEM Certificate Store for Mac and Linux, page 3-50

---

### Controlling the Certificate Store on Windows

Windows provides separate certificate stores for the local machine and for the current user. The client profile specifies which certificate store the AnyConnect client searches for certificates.
Users with administrative privileges on the computer have access to both certificate stores. Users without administrative privileges only have access to the user certificate store. Windows XP users usually have administrative privileges, and Windows 7 users usually do not.

In the Preferences (Part 1) pane of Profile Editor, use the Certificate Store list box to configure in which certificate store AnyConnect searches for certificates. Use the Certificate Store Override checkbox to allow AnyConnect to search the machine certificate store for users with non-administrative privileges.

Figure 3-10  Certificate Store list box and Certificate Store Override check box

Table 3-4 shows examples of Certificate Store and Certificate Store Override configurations.

Certificate Store has three possible settings:
- All—(default) Search all certificate stores.
- Machine—Search the machine certificate store (the certificate identified with the computer).
- User—Search the user certificate store.

Certificate Store Override has two possible settings:
- checked—Allows AnyConnect to search a computer’s machine certificate store even when the user does not have administrative privileges.
- cleared—(default) Does not allow AnyConnect to search the machine certificate store of a user without administrative privileges.

Table 3-4 shows examples of Certificate Store and Certificate Store Override configurations.
AnyConnect supports certificate authentication using a Privacy Enhanced Mail (PEM) formatted file store. Instead of relying on browsers to verify and sign certificates, the client reads PEM-formatted certificate files from the file system on the remote computer and verifies and signs them.

Restrictions for PEM File Filenames

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

- All certificate files must end with the extension `.pem`.

<table>
<thead>
<tr>
<th>Certificate Store Setting</th>
<th>Certificate Store Override Setting</th>
<th>AnyConnect Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>cleared</td>
<td>AnyConnect searches all certificate stores. AnyConnect is not allowed to access the machine store when the user has non-administrative privileges. This is the default setting. This setting is appropriate for the majority of cases. Do not change this setting unless you have a specific reason or scenario requirement to do so. <strong>Note</strong> Access-control for the machine store can vary depending on the Windows version and security settings. Because of this, the user may be unable to use certificates in the machine store even though they have administrative privileges. In this case, select Certificate Store Override to allow machine store access.</td>
</tr>
<tr>
<td>All</td>
<td>checked</td>
<td>AnyConnect searches all certificate stores. AnyConnect is allowed to access the machine store when the user has non-administrative privileges.</td>
</tr>
<tr>
<td>Machine</td>
<td>checked</td>
<td>AnyConnect searches the machine certificate store. AnyConnect is allowed to search the machine store of non-administrative accounts.</td>
</tr>
<tr>
<td>Machine</td>
<td>cleared</td>
<td>AnyConnect searches the machine certificate store. AnyConnect is not allowed to search the machine store when the user has non-administrative privileges. <strong>Note</strong> This configuration might be used when only a limited group of users are allowed to authenticate using a certificate.</td>
</tr>
<tr>
<td>User</td>
<td>not applicable</td>
<td>AnyConnect searches in the user certificate store only. The certificate store override is not applicable because non-administrative accounts have access to this certificate store.</td>
</tr>
</tbody>
</table>
• All private key files must end with the extension .key.
• A client certificate and its corresponding private key must have the same filename. For example: client.pem and client.key

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

Storing User Certificates

To create the PEM file certificate store, create the paths and folders listed in Table 5. Place the appropriate certificates in these folders:

Table 3-4  PEM File Certificate Store Folders and Types of Certificates Stored

<table>
<thead>
<tr>
<th>PEM File Certificate Store Folders</th>
<th>Type of Certificates Stored</th>
</tr>
</thead>
<tbody>
<tr>
<td>~/.cisco/certificates/ca</td>
<td>Trusted CA and root certificates</td>
</tr>
<tr>
<td>~/.cisco/certificates/client</td>
<td>Client certificates</td>
</tr>
<tr>
<td>~/.cisco/certificates/client/private</td>
<td>Private keys</td>
</tr>
</tbody>
</table>

Note: The requirements for machine certificates are the same as for PEM file certificates, with the exception of the root directory. For machine certificates, substitute /opt/.cisco for ~/.cisco. Otherwise, the paths, folders, and types of certificates listed in Table 5 apply.

Configuring Certificate Matching

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

• Key Usage
• Extended Key Usage
• Distinguished Name

The profile can contain none or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate.

Note: We do not recommend using a self-signed certificate because of the possibility a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.

Note: The AnyConnect client does not support certificate verification using certificate revocation lists (CRL).
Note

Many sites position the Certificate Authority they use to validate server certificates inside the corporate network. That means that a client cannot verify CRL when it is trying to connect to a headend, since the CRL is not accessible on the public network.

The client operating system can be configured to verify CRL in Windows and Mac OS X, but we ignore that setting.

Certificate Key Usage Matching

Certificate Matching Key Usage offers a set of constraints on the broad types of operations that can be performed with a given certificate. The supported set is listed in the Key Usage list on the VPN client profile, and includes:

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

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

The example in the “Certificate Matching Example” section on page 3-54 shows how you might configure these attributes.

Extended Certificate Key Usage Matching

This matching allows an administrator to limit the certificates that can be used by the client, based on the Extended Key Usage fields in the VPN client profile. Table 3-6 lists the well known set of constraints with their corresponding object identifiers (OIDs).

<table>
<thead>
<tr>
<th>Constraint</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerAuth</td>
<td>1.3.6.1.5.5.7.3.1</td>
</tr>
<tr>
<td>ClientAuth</td>
<td>1.3.6.1.5.5.7.3.2</td>
</tr>
<tr>
<td>CodeSign</td>
<td>1.3.6.1.5.5.7.3.3</td>
</tr>
<tr>
<td>EmailProtect</td>
<td>1.3.6.1.5.5.7.3.4</td>
</tr>
<tr>
<td>IPSecEndSystem</td>
<td>1.3.6.1.5.5.7.3.5</td>
</tr>
<tr>
<td>IPSecTunnel</td>
<td>1.3.6.1.5.5.7.3.6</td>
</tr>
</tbody>
</table>
Custom Extended Match Key

All other OIDs (such as 1.3.6.1.5.5.7.3.11, used in some examples in this document) are considered “custom.” As an administrator, you can add your own OIDs if the OID you want is not in the well known set.

Certificate Distinguished Name Mapping

The client profile Certificate Matching pane’s Distinguished Name table contains certificate identifiers that limit the certificates that can be used by the client to those matching the specified criteria and criteria match conditions. When you click the Add button, you can add one of the criteria to the list, and set a value or wildcard to match the contents of that criteria. Table 3-7 lists the supported criteria:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>SubjectCommonName</td>
</tr>
<tr>
<td>SN</td>
<td>SubjectSurName</td>
</tr>
<tr>
<td>GN</td>
<td>SubjectGivenName</td>
</tr>
<tr>
<td>N</td>
<td>SubjectUnstructName</td>
</tr>
<tr>
<td>I</td>
<td>SubjectInitials</td>
</tr>
<tr>
<td>GENQ</td>
<td>SubjectGenQualifier</td>
</tr>
<tr>
<td>DNQ</td>
<td>SubjectDnQualifier</td>
</tr>
<tr>
<td>C</td>
<td>SubjectCountry</td>
</tr>
<tr>
<td>L</td>
<td>SubjectCity</td>
</tr>
<tr>
<td>SP</td>
<td>SubjectState</td>
</tr>
<tr>
<td>ST</td>
<td>SubjectState</td>
</tr>
<tr>
<td>O</td>
<td>SubjectCompany</td>
</tr>
<tr>
<td>OU</td>
<td>SubjectDept</td>
</tr>
<tr>
<td>T</td>
<td>SubjectTitle</td>
</tr>
<tr>
<td>EA</td>
<td>SubjectEmailAddr</td>
</tr>
<tr>
<td>DC</td>
<td>DomainComponent</td>
</tr>
<tr>
<td>ISSUER-CN</td>
<td>IssuerCommonName</td>
</tr>
</tbody>
</table>
AnyConnect Secure Mobility Client Administrators Guide

Chapter 3      Configuring VPN Access

### Configuring Certificate Matching

The profile can contain zero or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. *Distinguished Name* matching offers additional match criteria, including the ability for the administrator to specify that a certificate must or must not have the specified string, as well as whether wild carding for the string should be allowed.

#### Certificate Matching Example

**Note**

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

To configure certificate matching in the client profile, follow these steps:

**Step 1** Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2** Go to the **Certificate Matching** pane.

**Step 3** Check the Key Usage and Extended Key Usage settings to choose acceptable client certificates. A certificate must match at least one of the specified key to be selected. For descriptions of these usage settings, see the “AnyConnect Profile Editor, Certificate Matching” section on page 3-82.

**Step 4** Specify any Custom Extended Match Keys. These should be well-known MIB OID values, such as 1.3.6.1.5.5.7.3.11. You can specify zero or more custom extended match keys. A certificate must match all the specified key(s) to be selected. The key should be in OID form. For example: 1.3.6.1.5.5.7.3.11
Step 5  Next to the Distinguished Names table, click Add to launch the Distinguished Name Entry window:

- **Name**—A distinguished name.
- **Pattern**—The string to use in the match. The pattern to be matched should include only the portion of the string you want to match. There is no need to include pattern match or regular expression syntax. If entered, this syntax will be considered part of the string to search for.
  
  For example, if a sample string was abc.cisco.com and the intent is to match on cisco.com, the pattern entered should be cisco.com.
- **Operator**—The operator to be used in performing the match.
  - Equal—Equivalent to ==
  - Not Equal—Equivalent to !=
- **Wildcard**—Include wildcard pattern matching. The pattern can be anywhere in the string.
- **Match Case**—Enables case-sensitive match with pattern.

---

### Prompting Users to Select Authentication Certificate

You can configure the AnyConnect to present a list of valid certificates to users and let them choose the certificate with which they want to authenticate the session. This configuration is available only for Windows 7, XP, and Vista. By default, user certificate selection is disabled.

**Note**

We do not recommend using a self-signed certificate because of the possibility a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.

To enable certificate selection, follow these steps in the AnyConnect profile:

**Step 1**  Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2**  Go to the Preferences (Part 2) pane and uncheck **Disable Certificate Selection**. The client now prompts the user to select the authentication certificate.

---

### Users Configuring Automatic Certificate Selection in AnyConnect Preferences

Enabling user certificate selection exposes the Automatic certificate selection checkbox in the AnyConnect Preferences dialog box. Users will be able to turn Automatic certificate selection on and off by checking or unchecking Automatic certificate selection.

**Figure 3-19** shows the Automatic Certificate Selection check box the user sees in the Preferences window:
Configuring a Server List

One of the main uses of the profile is to let the user list the connection servers. This server list consists of host name and host address pairs. The host name can be an alias used to refer to the host, an FQDN, or an IP address. The server list displays a list of server hostnames on the AnyConnect GUI in the Connect to drop-down list (Figure 3-20). The user can select a server from this list.

Initially, the host at the top of the list is the default server, and appears first in the GUI drop-down list. If the user selects an alternate server from the list, the client records the choice in the user preferences file on the remote computer, and the selected server becomes the new default server.

To configure a server list, follow this procedure:

**Step 1** Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2** Click Server List. The Server List pane opens.

**Step 3** Click Add. The Server List Entry window opens (Figure 3-21).
Figure 3-13 Adding a Server List

Step 4 Enter a **Host Display Name**, which is an alias that refers to the secure gateway.

- If you enter an FQDN or an IP address here, then the entry in the Host Name field becomes a label for the server in the connection drop-down list in the AnyConnect Client tray fly-out.
- If you only specify an FQDN here, and no IP address in the FQDN or IP field, then the FQDN in the Hostname field will be resolved by a DNS server.
- If you enter 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.

Step 5 Enter a **FQDN or IP** Address of the headend, if required.

Step 6 Specify a **User Group** (optional). The client uses the User Group in conjunction with the Host Address to form a group-based URL.

**Note** If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile.
Step 7  (For AnyConnect release 3.0.1047 or later.) To setup server list settings for mobile devices, check the Additional mobile-only settings checkbox and click Edit. See Configuring Server List Entries for Mobile Devices for more information.

Step 8  Under the Backup Server List, you can configure a list of backup servers the client can access if the user-selected server fails. If the server fails, the client attempts to connect to the server at the top of the list first, and moves down the list, if necessary. Enter an IP address or an FQDN for each backup secure gateway.

Step 9  Under the Load Balancing Server List (optional). If the host secure gateway is part of a load balancing cluster of security appliances, and the always-on feature is enabled, add the backup devices in the cluster. If you do not add those servers here, the always-on feature blocks access to backup devices in the load balancing cluster.

Step 10  Specify the Primary Protocol (optional) for the client when connecting to this ASA, either SSL or IPsec using IKEv2. The default is SSL.

Step 11  To disable the default authentication method (the proprietary AnyConnect EAP method), check Standard Authentication Only, and choose a method from the drop-down list.

Note  Changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.

Step 12  If you choose IKE as the Primary Protocol, enter the IKE Identity, which is a group or domain that serves as the client identity. The client sends the string as the ID_GROUP type IDi payload. By default, the string is *$AnyConnectClient$*.

Step 13  In CA URL, specify the URL of the SCEP CA server (optional). Enter an FQDN or IP Address. For example, http://ca01.cisco.com.

a. Check Prompt For Challenge Password (optional) to enable the user to make certificate requests manually. When the user clicks Get Certificate, the client prompts the user for a username and one-time password.

b. Enter the certificate thumbprint of the CA. Use SHA1 or MD5 hashes. Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.

Step 14  Click OK. The new server list entry you configured appears in the server list table (Figure 3-22).
Configuring Connections for Mobile Devices

**Prerequisites**

- Perform steps 1-6 of Configuring a Server List, page 3-56.
- You must be using Profile Editor version 3.0.1047 or later.
- Supported on Apple mobile devices, running Apple iOS version 4.1 or later.

**Guidelines**

AnyConnect VPN client profiles delivered to mobile devices from the ASA cannot be re-configured or deleted from the mobile device. When users create their own client profiles on their devices for new VPN connections, they will be able to configure, edit, and delete those profiles.

**Detailed Steps**

- **Step 1** In the Server List Entry dialog box, check Additional mobile-only settings and click Edit.
- **Step 2** In the Apple iOS / Android Settings area, you can configure these attributes for devices running Apple iOS or Android operating systems:
  a. Choose the Certificate Authentication type:
     - **Automatic**—AnyConnect automatically chooses the client certificate with which to authenticate. In this case, AnyConnect views all the installed certificates, disregards those certificates that are out of date, applies the certificate matching criteria defined in VPN client profile, and then authenticates using the certificate that matches the criteria. This happens every time the user attempts to establish a VPN connection.
     - **Manual**—AnyConnect searches for the certificate with which to authenticate just as it does with automatic authentication. In the manual certificate authentication type, however, once AnyConnect finds a certificate that matches the certificate matching criteria defined in the VPN client profile, it assigns that certificate to the connection and it will not search for new certificates when users attempt to establish new VPN connections.
– **Disabled**—Client Certificate will never be used for authentication.

**b.** If you check the *Make this Server List Entry active when profile is imported* check box, you are defining this server list entry as the default connection once the VPN profile has been downloaded to the device. Only one server list entry can have this designation. The default value is unchecked.

**Step 3** In the Apple iOS Only Settings area, you can configure these attributes for devices running Apple iOS operating systems only:

**a.** Configure the *Reconnect when roaming between 3G/Wifi networks* checkbox. The box is checked by default so AnyConnect will attempt to maintain the VPN connection when switching between 3G and Wifi networks. If you uncheck the box, AnyConnect will not attempt to maintain the VPN connection which switching between 3G and Wifi networks.

**b.** Configure the *Connect on Demand* checkbox.

This area allows you to configure the Connect on Demand functionality provided by Apple iOS. You can create lists of rules that will be checked whenever other applications initiate network connections that are resolved using the Domain Name System (DNS).

*Connect on Demand* can only be checked if the Certificate Authentication field is set to *Manual* or *Automatic*. If the Certificate Authentication field is set to *Disabled*, this checkbox is grayed out. The Connect on Demand rules, defined by the *Match Domain or Host* and the *On Demand Action* fields, can still be configured and saved when the checkbox is grayed out.

**c.** In the *Match Domain or Host* field, enter the host names (host.example.com), domain names (.example.com), or partial domains (.internal.example.com) for which you want to create a Connect on Demand rule. Do not enter IP addresses (10.125.84.1) in this field.

**d.** In the *On Demand Action* field, specify one of these actions when a user attempts to connect to the domain or host defined in the previous step:

– **Always connect**—iOS will always attempt to initiate a VPN connection when rules in this list are matched.

– **Connect if needed**—iOS will attempt to initiate a VPN connection when rules in this list are matched only if the system could not resolve the address using DNS.

– **Never connect**—iOS will never attempt to initiate a VPN connection when rules in this list are matched. Any rules in this list will take precedence over Always connect or Connect if needed rules.

When Connect On Demand is enabled, the application automatically adds the server address to this list. This prevents a VPN connection from being automatically established if you try accessing the server’s clientless portal with a web browser. This rule can be removed if you do not want this behavior.

**e.** Once you have created a rule using the *Match Domain or Host* field and the *On Demand Action* field, click *Add*.

The rule is displayed in the rules list below.

**Step 4** Click *OK*.

**Step 5** Return to step 8 of *Configuring a Server List*, page 3-56.
Configuring a Backup Server List

You can configure a list of backup servers the client uses in case the user-selected server fails. These servers are specified in the Backup Servers pane of the AnyConnect profile. In some cases, the list might specify host specific overrides. Follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Go to the Backup Servers pane and enter host addresses of the backup servers.</td>
</tr>
</tbody>
</table>

Configuring Connect On Start-up

Connect on Start-up automatically establishes a VPN connection with the secure gateway specified by the VPN client profile. Upon connecting, the client replaces the local profile with the one provided by the secure gateway, if the two do not match, and applies the settings of that profile.

By default, Connect on Start-up is disabled. When the user launches the AnyConnect client, the GUI displays the settings configured by default as user-controllable. The user must select the name of the secure gateway in the Connect to drop-down list in the GUI and click Connect. Upon connecting, the client applies the settings of the client profile provided by the security appliance.

AnyConnect has evolved from having the ability to establish a VPN connection automatically upon the startup of AnyConnect to having that VPN connection be “always-on” by the Post logon Always-on feature. The disabled by default configuration of Connect on Start-up element reflects that evolution. If your enterprise’s deployment uses the Connect on Start-up feature, consider using the Trusted Network Detection feature instead.

Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network. For information on configuring Trusted Network Detection, see the “Configuring Trusted Network Detection” section on page 3-22.

By default, Connect on Start-up is disabled. To enable it, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose Preferences in the navigation pane.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check Connect On Start-up.</td>
</tr>
</tbody>
</table>

Configuring Auto Reconnect

Unlike the IPsec VPN client, AnyConnect can recover from VPN session disruptions and can reestablish a session, regardless of the media used for the initial connection. For example, it can reestablish a session on wired, wireless, or 3G.
You can configure the Auto Reconnect feature to attempt to reestablish a VPN connection if you lose connectivity (the default behavior). You can also define the reconnect behavior during and after system suspend or system resume. A system suspend is a low-power standby, Windows “hibernation,” or Mac OS or Linux “sleep.” A system resume is a recovery following a system suspend.

**Step 1**
Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2**
Choose Preferences (Part 1) in the navigation pane.

**Step 3**
Check Auto Reconnect.

**Note**
If you uncheck Auto Reconnect, the client does not attempt to reconnect, regardless of the cause of the disconnection. Cisco highly recommends using the default setting (enabled) for this feature. Disabling this setting can cause interruptions in VPN connectivity over unstable connections.

**Step 4**
Choose the Auto Reconnect Behavior (not supported for Linux):

- Disconnect On Suspend—AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resume.
- Reconnect After Resume—The client retains resources assigned to the VPN session during a system suspend and attempts to reconnect after the system resume.

### Proxy Connections

AnyConnect supports VPN sessions through transparent or non-transparent proxy servers. Local, Private and Public proxies are supported, with some restrictions.

### Limitations

IPv6 proxies are not supported. This will be added in a future release of AnyConnect for Windows Vista and later.

### Local Proxy Connections

A local proxy runs on the same PC as AnyConnect, and is sometimes used as a transparent proxy. Some examples of a transparent proxy service include:

- Acceleration software provided by some wireless data cards
- Network component on some antivirus software, such as Kaspersky

### Limitations

- Either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license is required
- Local proxies are only supported on Microsoft Windows:
Chapter 3      Configuring VPN Access

Proxy Connections

Guidelines

Local proxies are defined in the AnyConnect VPN client profile. By default, AnyConnect is configured to support local proxy services to establish a VPN session.

Disabling Local Proxy Connections

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Profile Editor from ASDM or the stand-alone VPN Profile Editor.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Preferences (Part 2) in the navigation pane.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Uncheck <strong>Allow Local Proxy Connections</strong> near the top of the panel.</td>
</tr>
</tbody>
</table>

Private Proxy Connections

Private proxy servers are used on a corporate network to prevent corporate users from accessing certain Web sites based on corporate usage policies, for example, pornography, gambling, or gaming sites.

Group Policies on the ASA enforce private proxy settings on the Client system when a VPN connection is established. When the Client disconnects, those settings are reverted back to their original values. This allows an administrator to enforce corporate usage policies when VPN users connect to the corporate network.

Limitations

Linux is not supported.

Configuring a Private Proxy Connection

Private proxies are configured in the group policy.

- In the ASA CLI, the command in the group-policy submode is ‘msie-proxy’.
- In ASDM, edit a group policy, and configure the proxy server under Advanced > Browser Proxy.

Verifying the Proxy Settings

- For Windows: Find the Proxy settings in the Registry under:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- For Mac OSX: Open a Terminal window, and type:
  scutil --proxy

---

– Windows 7 (32-bit and 64-bit)
– Windows Vista (32-bit and 64-bit)-SP2 or Vista Service Pack 1 with KB952876
– Windows 8
Public Proxy Connections

Public Proxies are usually used to anonymize web traffic.

Public Proxy servers may also require a username and password, and are referred to as Authenticating Proxy Servers. There are two types of authentication that AnyConnect supports: Basic and NTLM. When the proxy server is configured to require authentication, AnyConnect dialogs manage the authentication process. After successfully authenticating to the Proxy Server, the AnyConnect menus prompt for the ASA username and password.

Limitations

- Only TLS is supported, not DTLS.
- Public Proxies are not supported for Mac and Linux.

Configuring a Public Proxy

When Windows Internet Options are configured to use a public proxy on a client, AnyConnect uses that connection.

Step 1  Open Internet Options from Internet Explorer or the Control Panel.

Step 2  Select the Connections Tab, and click the LAN Settings button.

Step 3  Configure the LAN to use a proxy server, and enter the IP address of the Proxy server.

Optimal Gateway Selection

Using the Optimal Gateway Selection (OGS) feature, you can minimize latency for Internet traffic without user intervention. With OGS, AnyConnect identifies and selects which secure gateway is best for connection or reconnection. OGS begins upon first connection or upon a reconnection at least four hours after the previous disconnection.

For best performance, users who travel to distant locations connect to a secure gateway nearest their location. Your home and office will get similar results from the same gateway, so no switch of secure gateways will typically occur in this instance. Connection to another secure gateway occurs rarely and only occurs if the performance improvement is at least 20%.

OGS is not a security feature, and it performs no load balancing between secure gateway clusters or within clusters. You can optionally give the end user the ability to enable or disable the feature.

The minimum round trip time (RTT) solution selects the secure gateway with the fastest RTT between the client and all other gateways. The client always reconnects to the last secure gateway if the time elapsed has been less than four hours. Factors such as load and temporary fluctuations of the network connection may affect the selection process, as well as the latency for Internet traffic.

OGS maintains a cache of its RTT results to minimize the number of measurements it must perform in the future. Upon starting AnyConnect with OGS enabled, OGS determines where the user is located by obtaining network information (such as DNS suffix and DNS server IP). The RTT results, along with this location, are stored in the OGS cache. During the next 14 days, the location is determined with this same
method whenever AC restarts, and the cache deciphers whether it already has RTT results. A headend is
selected based on the cache without needing to re-RRT the headends. At the end of 14 days, the results
for this location are removed from the cache, and restarting AC results in a new set of RTTs.

It contacts only the primary servers to determine the optimal one. Once determined, the connection
algorithm is as follows:

1. Attempt to connect to the optimal server.
2. If that fails, try the optimal server’s backup server list.
3. If that fails, try each remaining server in the OGS selection list, ordered by its selection results.

Refer to the “AnyConnect Profile Editor, Backup Servers” section on page 3-82 for additional
information on backup servers.

Optimal Gateway Selection Requirements

AnyConnect supports Optimal Gateway Select on VPN endpoints running the Windows and Mac OS X
operating systems qualified for this release.

This feature is available for IPv4 clients only.

Configuring Optimal Gateway Selection

You control the activation and deactivation of OGS and specify whether end users may control the
feature themselves in the AnyConnect profile. Follow these steps to configure OGS using the Profile
Editor:

Step 1  Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section
on page 3-9).

Step 2  Check the Enable Optimal Gateway Selection check box to activate OGS.

Step 3  Check the User Controllable check box to make OGS configurable for the remote user accessing the
client GUI.

Note  When OGS is enabled, we recommend that you also make the feature user controllable. A user
may need the ability to choose a different gateway from the profile if the AnyConnect client is
unable to establish a connection to the OGS-selected gateway.

Step 4  At the Suspension Time Threshold parameter, enter the minimum time (in hours) the VPN must have
been suspended before invoking a new gateway-selection calculation. The default is 4 hours.

Note  You can configure this threshold value using the Profile Editor. By optimizing this value in
combination with the next configurable parameter (Performance Improvement Threshold), you
can find the correct balance between selecting the optimal gateway and reducing the number of
times to force the re-entering of credentials.

Step 5  At the Performance Improvement Threshold parameter, enter the percentage of performance
improvement that is required before triggering the client to re-connect to another secure gateway
following a system resume. The default is 20%.
Note
If too many transitions are occurring and users have to re-enter credentials quite frequently, you should increase either or both of these thresholds. Adjust these values for your particular network to find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials.

If OGS is enabled when the client GUI starts, **Automatic Selection** displays in the *VPN: Ready to connect* panel next to the Connect button. You cannot change this selection. OGS automatically chooses the optimal secure gateway and displays the selected gateway on the status bar. You may need to click **Select** to start the connection process.

If you made the feature user controllable, the user can manually override the selected secure gateway with the following steps:

**Step 1**
If currently connected, click **Disconnect**.

**Step 2**
Click **Advanced**.

**Step 3**
Open the Preferences tab and uncheck **Enable Optimal Gateway Selection**.

**Step 4**
Choose the desired secure gateway.

Note
If AAA is being used, end users may have to re-enter their credentials when transitioning to a different secure gateway. The use of certificates eliminates this.

**OGS and Sleep Mode**

AnyConnect must have an established connection at the time the endpoint is put into sleep or hibernation mode. You must enable the AutoReconnect (ReconnectAfterResume) settings on ASDM’s profile editor (Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile). If you make it user controllable here, you can configure it on the AnyConnect Secure Mobility Client Preferences tab before the device is put to sleep. When both of these are set, the device comes out of sleep, and AC automatically runs OGS, using the selected headend for its reconnection attempt.

**OGS and Proxy Detection**

If automatic proxy detection is configured, you cannot perform OGS. It also does not operate with proxy auto-configuration (PAC) files configured.

**Writing and Deploying Scripts**

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

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

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

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

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

AnyConnect supports script launching during WebLaunch and standalone launches.

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

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

This section covers the following topics:

- **Scripting Requirements and Limitations**, page 3-67
- **Writing, Testing, and Deploying Scripts**, page 3-68
- **Configuring the AnyConnect Profile for Scripting**, page 3-69
- **Troubleshooting Scripts**, page 3-70

### Scripting Requirements and Limitations

Be aware of the following requirements and limitations for scripts:

#### Number of Scripts Supported

AnyConnect runs only one OnConnect and one OnDisconnect script; however, these scripts may launch other scripts.

#### File Formats

AnyConnect identifies the OnConnect and OnDisconnect script by the filename. It looks for a file whose name begins with OnConnect or OnDisconnect regardless of file extension. The first script encountered with the matching prefix is executed. It recognizes an interpreted script (such as VBS, Perl, or Bash) or an executable.

#### Script Language

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

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

Enabling the Script

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

Client GUI Termination

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

Running Scripts on 64-bit Windows

The AnyConnect client is a 32-bit application. When running on a 64-bit Windows version, such as Windows 7 x64 and Windows Vista SP2 x64, when it executes a batch script, it uses the 32-bit version of cmd.exe.

Because the 32-bit cmd.exe lacks some commands that the 64-bit cmd.exe supports, some scripts could stop executing when attempting to run an unsupported command, or run partially and stop. For example, the msg command, supported by the 64-bit cmd.exe, may not be understood by the 32-bit version of Windows 7 (found in %WINDIR%\SysWOW64).

Therefore, when you create a script, use commands supported by the 32-bit cmd.exe.

Writing, Testing, and Deploying Scripts

Deploy AnyConnect scripts as follows:

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

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

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

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

  If you use ASDM version 6.3 or later, the ASA adds the prefix scripts_ and the prefix OnConnect or OnDisconnect to your filename to identify the file as a script. When the client connects, the security appliance downloads the script to the proper target directory on the remote computer, removing the scripts_ prefix and leaving the remaining OnConnect or OnDisconnect prefix. For example, if you import the script myscript.bat, the script appears on the security appliance as scripts_OnConnect_myscript.bat. On the remote computer, the script appears as OnConnect_myscript.bat.
If you use an ASDM version earlier than 6.3, you must import the scripts with the following prefixes:
- scripts_OnConnect
- scripts_OnDisconnect

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

- Use an enterprise software deployment system to deploy scripts manually to the VPN endpoints on which you want to run the scripts.

If you use this method, use the script filename prefixes below:
- OnConnect
- OnDisconnect

Install the scripts in the directory shown in Table 3-8.

### Table 3-7 Required Script Locations

<table>
<thead>
<tr>
<th>OS</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7 and Vista</td>
<td>%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script</td>
</tr>
<tr>
<td>Microsoft Windows XP</td>
<td>%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Script</td>
</tr>
<tr>
<td>Linux (On Linux, assign execute permissions to the file for User, Group and Other.)</td>
<td>/opt/cisco/anyconnect</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>/opt/cisco/anyconnect/script</td>
</tr>
</tbody>
</table>

### Configuring the AnyConnect Profile for Scripting

To enable scripting in the client profile, follow these steps:

**Step 1** Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2** Choose **Preferences (Part 2)** in the navigation pane.

**Step 3** Check **Enable Scripting**. The client launches scripts on connecting or disconnecting the VPN connection.

**Step 4** Check **User Controllable** to let users enable or disable the running of On Connect and OnDisconnect scripts.

**Step 5** Check **Terminate Script On Next Event** to enable the client to terminate a running script process if a transition to another scriptable event occurs. For example, the client terminates a running On Connect script if the VPN session ends and terminates a running OnDisconnect script if AnyConnect starts a new
Authentication Timeout Control

By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out. Use the instructions in the following sections to change the value of this timer.

Authentication Timeout Control Requirements

AnyConnect supports this feature on all OSs supported by AnyConnect.

Support for this feature requires either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.
Configuring Authentication Timeout

To change the number of seconds AnyConnect waits for an authentication from the secure gateway before terminating the connection attempt, follow these steps:

**Step 1** Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2** Choose Preferences (Part 2) in the navigation pane.

**Step 3** Enter a number of seconds in the range 10–120 into the **Authentication Timeout Values** text box.

Proxy Support

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

Configuring the Client to Ignore Browser Proxy Settings

You can specify a policy in the AnyConnect profile to bypass the Microsoft Internet Explorer proxy configuration settings on the user’s PC. It is useful when the proxy configuration prevents the user from establishing a tunnel from outside the corporate network.

**Note** Connecting through a proxy is not supported with the always-on feature enabled. Therefore, if you enable always-on, configuring the client to ignore proxy settings is unnecessary.

Follow these steps to enable AnyConnect to ignore Internet Explorer proxy settings:

**Step 1** Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2** Go to the **Preferences (Part 2)** pane.

**Step 3** In the Proxy Settings drop-down list, choose **IgnoreProxy**. Ignore Proxy causes the client to ignore all proxy settings. No action is taken against proxies that reach the ASA.

**Note** AnyConnect does not support **Override** as a proxy setting.

Private Proxy

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

An AnyConnect Essentials license is the minimum ASA license activation requirement for this feature. AnyConnect supports this feature on computers running:

- Internet Explorer on Windows
- Safari on Mac OS

Configuring a Group Policy to Download a Private Proxy

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

Note: In a Mac environment, the proxy information that is pushed down from the ASA (upon a VPN connection) is not viewed in the browser until you open up a terminal and issue a “scutil --proxy”.

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

Internet Explorer Connections Tab Lockdown

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

- The ASA configuration specifies Connections tab lockdown.
- The ASA configuration specifies a private-side proxy.
- A Windows group policy previously locked down the Connections tab (overriding the no lockdown ASA group policy setting).

You can configure the ASA to allow or not allow proxy lockdown, in the group policy. To do this using ASDM, follow this procedure:

**Step 1** Go to Configuration > Remote Access VPN > Network (Client) Access > Group Policies.
**Step 2** Choose a group policy and click Edit. The Edit Internal Group Policy window displays.
**Step 3** In the navigation pane, go to Advanced > Browser Proxy. The Proxy Server Policy pane displays.
**Step 4** Click Proxy Lockdown to display more proxy settings.
**Step 5** Uncheck Inherit and select Yes to enable proxy lockdown and hide the Internet Explorer Connections tab for the duration of the AnyConnect session or select No to disable proxy lockdown and expose the Internet Explorer Connections tab for the duration of the AnyConnect session.
**Step 6** Click OK to save the Proxy Server Policy changes.
Step 7  Click Apply to save the Group Policy changes.

Proxy Auto-Configuration File Generation for Clientless Support

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

Using a Windows RDP Session to Launch a VPN Session

With the Windows Remote Desktop Protocol (RDP), you can allow users to log on to a computer running the Cisco AnyConnect Secure Mobility client and create a VPN connection to a secure gateway from the RDP session. A split tunneling VPN configuration is required for this to function correctly.

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

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

You can use the following settings for Windows Logon Enforcement:

- **Single Local Logon**—Allows only one local user to be logged on during the entire VPN connection. With this setting, a local user can establish a VPN connection while one or more remote users are logged on to the client PC, but if the VPN connection is configured for all-or-nothing tunneling, then the remote logon is disconnected because of the resulting modifications of the client PC routing table for the VPN connection. If the VPN connection is configured for split-tunneling, the remote logon might or might not be disconnected, depending on the routing configuration for the VPN connection. The SingleLocalLogin setting has no effect on remote user logons from the enterprise network over the VPN connection.

- **SingleLogon**—Allows only one user to be logged on during the entire VPN connection. If more than one user is logged on and has an established VPN connection, either locally or remotely, the connection is not allowed. If a second user logs on, either locally or remotely, the VPN connection is terminated.

Note  When you select the SingleLogon setting, no additional logons are allowed during the VPN connection, so a remote logon over the VPN connection is not possible.

The Windows VPN Establishment settings in the client profile specify the behavior of the client when a user who is remotely logged on to a computer running AnyConnect establishes a VPN connection. The possible values are:

- **Local Users Only**—Prevents a remotely logged-on user from establishing a VPN connection. AnyConnect client versions 2.3 and earlier operated in this manner.
AnyConnect over L2TP or PPTP

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

To send traffic destined for the secure gateway over a PPP connection, AnyConnect uses the point-to-point adapter generated by the external tunnel. When establishing a VPN tunnel over a PPP connection, the client must exclude traffic destined for the ASA from the tunneled traffic intended for destinations beyond the ASA. To specify whether and how to determine the exclusion route, use the PPP Exclusion setting in the AnyConnect profile. The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI.

The following sections describe how to set up PPP exclusion:

- Configuring AnyConnect over L2TP or PPTP
- Instructing Users to Override PPP Exclusion
Configuring AnyConnect over L2TP or PPTP

By default, PPP Exclusion is disabled. To enable PPP exclusion in the profile, follow these steps:

**Step 1** Launch the Profile Editor from ASDM (see the “Creating and Editing an AnyConnect Profile” section on page 3-9).

**Step 2** Go to the Preferences (Part 2) pane.

**Step 3** Choose a PPP Exclusion Method. Checking User Controllable for this field lets users view and change these settings:

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

**Step 4** In the PPP Exclusion Server IP field, enter the IP address of the security gateway used for PPP exclusion. Checking User Controllable for this field lets users view and change this IP address.

Instructing Users to Override PPP Exclusion

If automatic detection does not work, and you configured PPP Exclusion as user controllable, the user can override the settings by editing the AnyConnect preferences file on the local computer. The following procedure describes how to do this:

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

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

- **Windows**: %LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml. For example,
  - Windows Vista—C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml
  - Windows XP—C:\Documents and Secure Mobility VPN Client\preferences.xml
- **Mac OS X**: /Users/username/.anyconnect
- **Linux**: /home/username/.anyconnect

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

```xml
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

**Step 3** Save the file.
Step 4  Exit and restart AnyConnect.

AnyConnect VPN Profile Editor Parameter Descriptions

The following section describes all the settings that appear on the various panes of the profile editor.

AnyConnect Profile Editor, Preferences (Part 1)

Use Start Before Logon (Windows Only)—Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows logon dialog box appears. After authenticating, the logon dialog box appears and the user logs in as usual. SBL also lets you control the use of logon scripts, password caching, mapping network drives to local drives, and more.

Show Pre-connect Message—Displays a message to the user before the user makes the first connection attempt. For example, you could remind the user to insert their smartcard into the reader. For information about setting or changing the pre-connect message, see Changing the Default AnyConnect English Messages, page 12-15.

Certificate Store—Controls which certificate store AnyConnect uses for storing and reading certificates. Windows provides separate certificate stores for the local machine and for the current user. The default setting (All) is appropriate for the majority of cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.

- All—(default) Certificates are stored in both stores.
- Machine—Use the machine store.
- User—Use user certificate store.

Certificate Store Override—Allows you to direct AnyConnect to search for certificates in the Windows machine certificate store. This is useful in cases where certificates are located in the machine store, and users do not have administrator privileges on their machine.

Auto Connect on Start—AnyConnect, when started, automatically establishes a VPN connection with the secure gateway specified by the AnyConnect profile, or to the last gateway to which the client connected.

Minimize On Connect—After establishing a VPN connection, the AnyConnect GUI minimizes.

Local LAN Access—Allows the user complete access to the local LAN connected to the remote computer during the VPN session to the ASA.

Note  Enabling Local LAN Access can potentially create a security weakness from the public network through the user computer into the corporate network. Alternatively, you can configure the security appliance (version 8.3(1) or later) to deploy an SSL client firewall that uses the AnyConnect Client Local Print firewall rule included in the default group policy. In order to enable this firewall rule, you also must enable Automatic VPN Policy, Always On, and Allow VPN Disconnect in this editor, Preferences (Part 2).

Auto Reconnect—AnyConnect attempts to reestablish a VPN connection if you lose connectivity (enabled by default). If you disable Auto Reconnect, it does not attempt to reconnect, regardless of the cause of the disconnection.
Auto Reconnect Behavior:
- **DisconnectOnSuspend (default)**—AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resumes.
- **ReconnectAfterResume**—AnyConnect attempts to reestablish a VPN connection if you lose connectivity.

**Note** Before AnyConnect 2.3, the default behavior in response to a system suspend was to retain the resources assigned to the VPN session and reestablish the VPN connection after the system resume. To retain that behavior, choose **ReconnectAfterResume** for the Auto Reconnect Behavior.

**Auto Update**—When checked, enables the automatic update of the client. If you check User Controllable, then the user can override this setting in the client.

**RSA Secure ID Integration (Windows only)**—Controls how the user interacts with RSA. By default, AnyConnect determines the correct method of RSA interaction (automatic setting).
- **Automatic**—Software or Hardware tokens accepted.
- **Software Token**—Only software tokens accepted.
- **Hardware Token**—Only hardware tokens accepted.

**Windows Logon Enforcement**—Allows a VPN session to be established from a Remote Desktop Protocol (RDP) session. Split tunneling must be configured in the group policy. AnyConnect disconnects the VPN connection when the user who established the VPN connection logs off. If the connection is established by a remote user, and that remote user logs out, the VPN connection terminates.
- **Single Local Logon**—Allows only one local user to be logged on during the entire VPN connection. A local user can establish a VPN connection while one or more remote users are logged on to the client PC.
- **Single Logon**—Allows only one user to be logged on during the entire VPN connection. If more than one user is logged on, either locally or remotely, when the VPN connection is being established, the connection is not allowed. If a second user logs on, either locally or remotely, during the VPN connection, the VPN connection terminates. No additional logons are allowed during the VPN connection, so a remote logon over the VPN connection is not possible.

**Windows VPN Establishment**—Determines the behavior of AnyConnect when a user who is remotely logged on to the client PC establishes a VPN connection. The possible values are:
- **Local Users Only**—Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of AnyConnect.
- **Allow Remote Users**—Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection terminates to allow the remote user to regain access to the client PC. Remote users must wait 90 seconds after VPN establishment if they want to disconnect their remote logon session without causing the VPN connection to be terminated.

**Note** On Vista, the Windows VPN Establishment setting is not currently enforced during Start Before Logon (SBL). AnyConnect does not determine whether the VPN connection is being established by a remote user before logon; therefore, a remote user can establish a VPN connection via SBL even when the Windows VPN Establishment setting is Local Users Only.
• Clear SmartCard PIN—Clears the PIN from the AnyConnect cache when the connection to the ASA is made, just prior to using the certificate. This ensures that a user will always need to enter their PIN to connect; they can’t connect to the VPN with just the certificate.

• IP Protocol Supported—For clients with both an IPv4 and IPv6 address attempting to connect to the ASA using AnyConnect, AnyConnect needs to decide which IP protocol to use to initiate the connection. By default AnyConnect initially attempts to connect using IPv4. If that is not successful, AnyConnect attempts to initiate the connection using IPv6.

This field configures the initial IP protocol and order of fallback.
- IPv4—Only IPv4 connections can be made to the ASA.
- IPv6—Only IPv6 connections can be made to the ASA.
- IPv4, IPv6—First, attempt to make an IPv4 connection to the ASA. If the client cannot connect using IPv4 then try to make an IPv6 connection.
- IPv6, IPv4—First attempt to make an IPv6 connection to the ASA. If the client cannot connect using IPv6 then try to make an IPv4 connection.

**Note**
The IPv4 to IPv6 and IPv6 to IPv4 protocol failover can also happen during the VPN session. If the primary IP protocol is lost, the VPN session will be re-established via the secondary IP protocol, if possible.

For more detailed configuration information about the client features that appear on this pane, see these sections:
- Configuring Start Before Logon (PLAP) on Windows Systems, page 3-16
- Configuring Certificate Expiration Notice, page 3-47
- Configuring Auto Reconnect, page 3-61
- Using a Windows RDP Session to Launch a VPN Session, page 3-73

### AnyConnect Profile Editor, Preferences (Part 2)

**Disable Certificate Selection**—Disables automatic certificate selection by the client and prompts the user to select the authentication certificate.

**Allow Local Proxy Connections**—By default, AnyConnect lets Windows users establish a VPN session through a transparent or non-transparent proxy service on the local PC. Some examples of elements that provide a transparent proxy service include:
- Acceleration software provided by some wireless data cards
- Network component on some antivirus software

Uncheck this parameter if you want to disable support for local proxy connections.

**Proxy Settings**—Specifies a policy in the AnyConnect profile to bypass the Microsoft Internet Explorer or Mac Safari proxy settings on the remote computer. This is useful when the proxy configuration prevents the user from establishing a tunnel from outside the corporate network. Use in conjunction with the proxy settings on the ASA.
- Native—Causes the client to use both the client configured proxy settings and the Internet Explorer configured proxy settings. The native OS proxy settings are used (such as those configured into MSIE in Windows), and proxy settings configured in the global user preferences are pre-pended to these native settings.
- IgnoreProxy—Ignores all Microsoft Internet Explorer or Mac Safari proxy settings on the user computer. No action is taken against proxies that reach the ASA.
- Override (not supported)

**Enable Optimal Gateway Selection**—AnyConnect identifies and selects which secure gateway is best for connection or reconnection based on the round trip time (RTT), minimizing latency for Internet traffic without user intervention. **Automatic Selection** displays in the Connect To drop-down list on the Connection tab of the client GUI.

- Suspension Time Threshold (hours)—The elapsed time from disconnecting to the current secure gateway to reconnecting to another secure gateway. If users experience too many transitions between gateways, increase this time.
- Performance Improvement Threshold (%)—The performance improvement that triggers the client to connect to another secure gateway. The default is 20%.

---

**Note**

If AAA is used, users may have to re-enter their credentials when transitioning to a different secure gateway. Using certificates eliminates this problem.

**Automatic VPN Policy (Windows and Mac only)**—Automatically manages when a VPN connection should be started or stopped according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually.

---

**Note**

Automatic VPN Policy does not prevent users from manually controlling a VPN connection.

- Trusted Network Policy—AnyConnect automatically disconnects a VPN connection when the user is inside the corporate network (the trusted network).
  - Disconnect—Disconnects the VPN connection upon the detection of the trusted network.
  - Connect—Initiates a VPN connection upon the detection of the trusted network.
  - Do Nothing—Takes no action in the trusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
  - Pause—AnyConnect suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user’s convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.

- Untrusted Network Policy—AnyConnect starts the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.
  - Connect—Initiates the VPN connection upon the detection of an untrusted network.
  - Do Nothing—Initiates the VPN connection upon the detection of an untrusted network. This option disables always-on VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.

- Trusted DNS Domains—DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *.cisco.com. Wildcards (*) are supported for DNS suffixes.
• Trusted DNS Servers—DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 192.168.1.2, 2001:DB8::1.

• Always On—Determines whether AnyConnect automatically connects to the VPN when the user logs in to a computer running one of the supported Windows or Mac OS X operating systems. Use this feature to enforce corporate policies to protect the computer from security threats by preventing access to Internet resources when it is not in a trusted network. You can set the always-on VPN parameter in group policies and dynamic access policies to override this setting. Doing so lets you specify exceptions according to the matching criteria used to assign the policy. If an AnyConnect policy enables always-on VPN and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.

After checking Always On, you are able to check Allow VPN Disconnect.

• Allow VPN Disconnect—Determines whether AnyConnect displays a Disconnect button for always-on VPN sessions. Users of always-on VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as the following:
  – Performance issues with the current VPN session.
  – Reconnection issues following the interruption of a VPN session.

  ! Caution
  The Disconnect locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. For the reasons noted above, disabling the Disconnect button can at times hinder or prevent VPN access.

  For more information about this feature, see the “Disconnect Button for Always-on VPN” section on page 3-28.

  After enabling AllowVPN Disconnect, you will be able to configure Connect Failure Policy, Allow Captive Portal Remediation, and Apply Last VPN Local Resource Rules.

• Connect Failure Policy—Determines whether the computer can access the Internet if AnyConnect cannot establish a VPN session (for example, when an ASA is unreachable). This parameter applies only if always-on VPN is enabled.

  ! Caution
  A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. AnyConnect detects most captive portals; however, if it cannot detect a captive portal, the connect failure closed policy prevents all network connectivity. Be sure to read the “Connect Failure Policy for Always-on VPN, page 3-29” before configuring a connect failure policy.

  – Closed—Restricts network access when the VPN is unreachable. The purpose of this setting is to help protect corporate assets from network threats when resources in the private network responsible for protecting the endpoint are unavailable.
  – Open—Permits network access when the VPN is unreachable.

  Connect Failure Policy - If Connect Failure Policy is Closed, then you can configure the next settings.

  – Allow Captive Portal Remediation—Lets AnyConnect lift the network access restrictions imposed by the closed connect failure policy when the client detects a captive portal (hotspot). Hotels and airports typically use captive portals to require the user to open a browser and satisfy
conditions required to permit Internet access. By default, this parameter is unchecked to provide the greatest security; however, you must enable it if you want the client to connect to the VPN if a captive portal is preventing it from doing so.

- Remediation Timeout—Number of minutes AnyConnect lifts the network access restrictions. This parameter applies if the Allow Captive Portal Remediation parameter is checked and the client detects a captive portal. Specify enough time to meet typical captive portal requirements (for example, 5 minutes).

- Apply Last VPN Local Resource Rules—If the VPN is unreachable, the client applies the last client firewall it received from the ASA, which may include ACLs allowing access to resources on the local LAN.

PPP Exclusion —For a VPN tunnel over a PPP connection, specifies whether and how to determine the exclusion route so the client can exclude traffic destined for the secure gateway from the tunneled traffic intended for destinations beyond the secure gateway. The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI. If you make this feature user controllable, users can read and change the PPP exclusion settings.

- Automatic—Enables PPP exclusion. AnyConnect automatically uses the IP address of the PPP server. Instruct users to change the value only if automatic detection fails to get the IP address.

- Disabled—PPP exclusion is not applied.

- Override—Also enables PPP exclusion. If automatic detection fails to get the IP address of the PPP server, and you configured PPP exclusion as user controllable, instruct users to follow the instructions in the “Instructing Users to Override PPP Exclusion” section on page 3-75.

PPP Exclusion Server IP—The IP address of the security gateway used for PPP exclusion.

Enable Scripting—Launches OnConnect and OnDisconnect scripts if present on the security appliance flash memory.

- Terminate Script On Next Event—Terminates a running script process if a transition to another scriptable event occurs. For example, AnyConnect terminates a running OnConnect script if the VPN session ends, and terminates a running OnDisconnect script if the client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the OnConnect or OnDisconnect script launched, and all their script descendents. On Mac OS and Linux, the client terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts.

- Enable Post SBL On Connect Script—Launches the OnConnect script if present and SBL establishes the VPN session. (Only supported if VPN endpoint is running Microsoft Windows 7, XP, or Vista).

Retain VPN On Logoff—Determines whether to keep the VPN session when the user logs off a Windows OS.

- User Enforcement—Specifies whether to end the VPN session if a different user logs on. This parameter applies only if “Retain VPN On Logoff” is checked and the original user logged off Windows when the VPN session was up.

Authentication Timeout Values—By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out. Enter a number of seconds in the range 10–120.

For more detailed configuration information about the client features that appear on this pane, see these sections:

- Proxy Connections, page 3-62
AnyConnect Profile Editor, Backup Servers

You can configure a list of backup servers the client uses in case the user-selected server fails. If the user-selected server fails, the client attempts to connect to the server at the top of the list first, and moves down the list, if necessary.

**Host Address**—Specifies an IP address or a Fully-Qualified Domain Name (FQDN) to include in the backup server list.

**Add**—Adds the host address to the backup server list.

**Move Up**—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.

**Move Down**—Moves the selected backup server down in the list.

**Delete**—Removes the backup server from the server list.

For more information on configuring backup servers, see the “Configuring a Backup Server List” section on page 3-61.

AnyConnect Profile Editor, Certificate Matching

Enable the definition of various attributes that can be used to refine automatic client certificate selection on this pane.

**Key Usage**—Use the following Certificate Key attributes for choosing acceptable client certificates:

- **Decipher_Only**—Deciphering data, and that no other bit (except Key_Agreement) is set.
- **Encipher_Only**—Enciphering data, and any other bit (except Key_Agreement) is not set.
- **CRL_Sign**—Verifying the CA signature on a CRL.
- **Key_Cert_Sign**—Verifying the CA signature on a certificate.
- **Key_Agreement**—Key agreement.
- **Data_Encipherment**—Encrypting data other than Key_Encipherment.
- **Key_Encipherment**—Encrypting keys.
- **Non_Repudiation**—Verifying digital signatures protecting against falsely denying some action, other than Key_Cert_sign or CRL_Sign.
- **Digital_Signature**—Verifying digital signatures other than Non_Repudiation, Key_Cert_Sign or CRL_Sign.
**Extended Key Usage**—Use these Extended Key Usage settings. The OIDs are included in parentheses ():

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

**Custom Extended Match Key (Max 10)**—Specifies custom extended match keys, if any (maximum 10). A certificate must match all the specified key(s) you enter. Enter the key in the OID format (for example, 1.3.6.1.5.5.7.3.11).

**Distinguished Name (Max 10)**—Specifies distinguished names (DNs) for exact match criteria in choosing acceptable client certificates.

**Name**—The distinguished name (DN) to use for matching:

- CN—Subject Common Name
- C—Subject Country
- DC—Domain Component
- DNQ—Subject Dn Qualifier
- EA—Subject Email Address
- GENQ—Subject Gen Qualifier
- GN—Subject Given Name
- I—Subject Initials
- L—Subject City
- N—Subject Unstruct Name
- O—Subject Company
- OU—Subject Department
- SN—Subject Sur Name
- SP—Subject State
- ST—Subject State
- T—Subject Title
- ISSUER-CN—Issuer Common Name
- ISSUER-DC—Issuer Component
- ISSUER-SN—Issuer Sur Name
- ISSUER-GN—Issuer Given Name
- ISSUER-N—Issuer Unstruct Name
- ISSUER-I—Issuer Initials
- ISSUER-GENQ—Issuer Gen Qualifier
- ISSUER-DNQ—Issuer Dn Qualifier
- ISSUER-C—Issuer Country
- ISSUER-L—Issuer City
- ISSUER-SP—Issuer State
- ISSUER-ST—Issuer State
- ISSUER-O—Issuer Company
- ISSUER-OU—Issuer Department
- ISSUER-T—Issuer Title
- ISSUER-EA—Issuer Email Address

**Pattern**—Specifies the string to match. The pattern to be matched should include only the portion of the string you want to match. There is no need to include pattern match or regular expression syntax. If entered, this syntax will be considered part of the string to search for.

For example, if a sample string was abc.cisco.com and the intent is to match cisco.com, the pattern entered should be cisco.com.

**Wildcard**—Enabled includes wildcard pattern matching. With wildcard enabled, the pattern can be anywhere in the string.

**Operator**—The operator to use when performing matches for this DN.
- Equal—equivalent to ==
- Not Equal—equivalent to !=

**Match Case**—Check to enable case-sensitive pattern matching.

For more detailed configuration information about the certificate matching, see the “Configuring Certificate Matching” section on page 3-51.

### AnyConnect Profile Editor, Certificate Enrollment

**Certificate Enrollment**—Enables AnyConnect to use the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate for client authentication.

**Certificate Expiration Threshold**—The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported by RADIUS password-management). The default is zero (no warning displayed). The range of values is zero to 180 days.

**Automatic SCEP Host**—For Legacy SCEP, specifies the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname asa.cisco.com and the connection profile name scep_eng.

**CA URL**—For Legacy SCEP, identifies the SCEP CA server. Enter an FQDN or IP Address of the CA server. For example, http://ca01.cisco.com.

- **Prompt For Challenge PW**—Enable this setting to allow the user make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.
Chapter 3      Configuring VPN Access

AnyConnect Secure Mobility Client Administrators Guide

AnyConnect VPN Profile Editor Parameter Descriptions

- **Thumbprint**—The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.

**Note**
Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in the issued server certificate.

**Certificate Contents**—Specifies certificate contents to include in the SCEP enrollment request:

- **Name (CN)**—Common Name in the certificate.
- **Department (OU)**—Department name specified in certificate.
- **Company (O)**—Company name specified in certificate.
- **State (ST)**—State identifier named in certificate.
- **State (SP)**—Another state identifier.
- **Country (C)**—Country identifier named in certificate.
- **Email (EA)**—Email address. In the following example, Email (EA) is %USER%@cisco.com. %USER% corresponds to the user’s ASA username logon credential.
- **Domain (DC)**—Domain component. In the following example, Domain (DC) is set to cisco.com.
- **SurName (SN)**—The family name or last name.
- **GivenName (GN)**—Generally, the first name.
- **UnstructName (N)**—Undefined name.
- **Initials (I)**—The initials of the user.
- **Qualifier (GEN)**—The generation qualifier of the user. For example, “Jr.” or “III.”
- **Qualifier (DN)**—A qualifier for the entire DN.
- **City (L)**—The city identifier.
- **Title (T)**—The person’s title. For example, Ms., Mrs., Mr.
- **CA Domain**—Used for the SCEP enrollment and is generally the CA domain.
- **Key size**—The size of the RSA keys generated for the certificate to be enrolled. We recommend using a key size of at least 2048.

**Display Get Certificate Button**—Enables the AnyConnect GUI to display the Get Certificate button under the following conditions:

- The certificate is set to expire within the period defined by the Certificate Expiration Threshold (not supported with RADIUS)
- The certificate has expired
- No certificate is present
- The certificate fails to match.

For more detailed configuration information about Certificate Enrollment, see the “Configuring Certificate Enrollment using SCEP” section on page 3-41.

---

**AnyConnect Profile Editor, Mobile Policy**

Set parameters for AnyConnect running on Windows Mobile in this pane:

Note

- **Device Lock Required**—A Windows Mobile device must be configured with a password or PIN before establishing a VPN connection. This only applies to Windows Mobile devices that use the Microsoft Local Authentication Plug-ins (LAPs).
- **Maximum Timeout Minutes**—The maximum number of minutes that must be configured before the device lock takes effect.
- **Minimum Password Length**—Specifies the minimum number of characters for the device lock password or PIN.
- **Password Complexity**—Specifies the complexity for the required device lock password:
  - alpha—Requires an alphanumeric password.
  - pin—Requires a numeric PIN.
  - strong—Requires a strong alphanumeric password which must contain at least 7 characters, including a minimum of 3 from the set of uppercase, lowercase, numerals, and punctuation characters.

**AnyConnect Profile Editor, Server List**

You can configure a list of servers that appear in the client GUI. Users can select servers in the list to establish a VPN connection.

Server List Table Columns:

- **Hostname**—The alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- **Host Address**—IP address or FQDN of the server.
- **User Group**—Used in conjunction with Host Address to form a group-based URL.
- **Automatic SCEP Host**—The Simple Certificate Enrollment Protocol specified for provisioning and renewing a certificate used for client authentication.
- **CA URL**—The URL this server uses to connect to certificate authority (CA).

**Add/Edit**—Launches the Server List Entry dialog where you can specify the server parameters.

**Delete**—Removes the server from the server list.

**Details**—Displays more details about backup servers or CA URLs for the server.

**AnyConnect Profile Editor, Add/Edit Server List**

Add a server and its backup server or load balancing backup device in this pane.

- **Hostname**—Enter an alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- **Host Address**—Specify an IP address or an FQDN for the server.
Note

- If you specify an IP address or FQDN in the Host Address Field, then the entry in the Host Name field becomes a label for the server in the connection drop-down list in the AnyConnect Client tray fly-out.
- If you only specify an FQDN in the Hostname field, and no IP address in the Host Address field, then the FQDN in the Hostname field will be resolved by a DNS server.
- If you enter 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.

User Group—Specify a user group. The user group is used in conjunction with Host Address to form a group-based URL.

Note
If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile.

Backup Server List—you can configure a list of backup servers the client uses in case the user-selected server fails. If the server fails, the client attempts to connect to the server at the top of the list first, and moves down the list, if necessary.

- Host Address—Specifies an IP address or an FQDN to include in the backup server list. If the client cannot connect to the host, it attempts to connect to the backup server.
- Add—Adds the host address to the backup server list.
- Move Up—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.
- Move Down—Moves the selected backup server down in the list.
- Delete—Removes the backup server from the server list.

Load Balancing Server List—if the host for this server list entry is a load balancing cluster of security appliances, and the always-on feature is enabled, specify the backup devices of the cluster in this list. If you do not, the always-on feature blocks access to backup devices in the load balancing cluster.

- Host Address—Specifies an IP address or an FQDN of a backup device in a load-balancing cluster.
- Add—Adds the address to the load balancing backup server list.
- Delete—Removes the load balancing backup server from the list.

Primary Protocol—Specifies the protocol for connecting to this ASA, either SSL or IPsec with IKEv2. The default is SSL.

Standard Authentication Only—By default, the AnyConnect client uses the proprietary AnyConnect EAP authentication method. Check to configure the client to use a standards-based method. However, doing this limits the dynamic download features of the client and disables some features.

Note
Changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.
IKE Identity—If you choose a standards-based EAP authentication method, you can enter a group or domain as the client identity in this field. The client sends the string as the ID_GROUP type IDi payload. By default, the string is *$AnyConnectClient$*.

CA URL—Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, http://ca01.cisco.com.

- **Prompt For Challenge PW**—Enable the user make certificate requests manually. When the user clicks Get Certificate, the client prompts the user for a username and one-time password.
- **Thumbprint**—The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.

\[Note\]

Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.

For more detailed configuration information about creating a server list, see the “Configuring a Server List” section on page 3-56.

**Configuring AnyConnect Client Connection Timeouts**

Use these procedures to terminate or maintain an idle AnyConnect VPN connection.

You can limit how long the ASA keeps an AnyConnect VPN connection available to the user even with no activity. If a VPN session goes idle, you can terminate the connection or re-negotiate the connection.

**Terminating an AnyConnect Connection**

Terminating an AnyConnect connection requires the user to re-authenticate their endpoint to the secure gateway and create a new VPN connection.

The following configuration parameters terminate the VPN session based on a simple timeout:

- **Default Idle Timeout** - Terminates any user's session when the session is inactive for the specified time. The default value is 30 minutes.

  You can only modify default-idle-timeout using the CLI, in webvpn configuration mode. The default is 1800 second. For instructions to configure default-idle-timeout see Configuring Session Timeouts in Cisco ASA 5500 Series Configuration Guide using the CLI.

- **VPN Idle Timeout** - Terminates any user's session when the session is inactive for the specified time. For SSL-VPN only, if vpn-idle-timeout is not configured, then default-idle-timeout is used.

  For instructions to configure VPN idle timeout with the ASDM, see Adding or Editing a Remote Access Internal Group Policy, General Attributes in Cisco ASA 5500 Series Configuration Guide using ASDM.

  For instructions to configure VPN idle timeout with the CLI, see Step 4 of Configuring VPN-Specific Attributes in Cisco ASA 5500 Series Configuration Guide using the CLI.

**Renegotiating and Maintaining the AnyConnect Connection**

The following configuration parameters terminate or renegotiate the tunnel, but do not terminate the session:
- **Keepalive** - The ASA sends keepalive messages at regular intervals. These messages are ignored by the ASA, but are useful in maintaining connections with devices between the client and the ASA.

  For instructions to configure Keepalive with the ASDM, see Configuring AnyConnect VPN Client Connections in *Cisco ASA 5500 Series Configuration Guide using ASDM*.

  For instructions to configure Keepalive with the CLI, see Step 5 of Group-Policy Attributes for AnyConnect Secure Mobility Client Connections in *Cisco ASA 5500 Series Configuration Guide using the CLI*.

- **Dead Peer Detection** - The ASA and AnyConnect client send "R-U-There" messages. These messages are sent less frequently than IPsec's keepalive messages.

  - If the client does not respond to the ASA's DPD messages, the ASA tries three more times before putting the session into "Waiting to Resume" mode. This mode allows the user to roam networks, or enter sleep mode and later recover the connection. If the user does not reconnect before the default idle timeout occurs, the ASA will terminate the tunnel. The recommended gateway DPD interval is 300 seconds.

  - If the ASA does not respond to the client's DPD messages, the client tries three more times before terminating the tunnel. The recommended client DPD interval is 30 seconds.

You can enable both the ASA (gateway) and the client to send DPD messages, and configure a timeout interval.

For instructions to configure DPD with the ASDM, see Dead Peer Detection in *Cisco ASA 5500 Series Configuration Guide using ASDM*.

For instructions to configure DPD with the CLI, see Step 4 of Configuring Group-Policy Attributes for AnyConnect Secure Mobility Client Connections in *Cisco ASA 5500 Series Configuration Guide using the CLI*.

**Best Practices**

- Set Client DPD to 30 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).

- Set Server DPD to 300 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).

- Set Rekey, for both SSL and IPsec to 1 hour (Group Policy > Advanced > AnyConnect Client > Key Regeneration).