

General VPN Setup

- System Options, on page 1
- Configure Maximum VPN Sessions, on page 3
- Configure DTLS, on page 3
- Configure DNS Server Groups, on page 4
- Configure the Pool of Cryptographic Cores, on page 5
- Client Addressing for SSL VPN Connections, on page 5
- Group Policies, on page 6
- Connection Profiles, on page 41
- IKEv1 Connection Profiles, on page 58
- **IKEv2 Connection Profiles**, on page 63
- Mapping Certificates to IPsec or SSL VPN Connection Profiles, on page 65
- Site-to-Site Connection Profiles, on page 69
- AnyConnect VPN module of Cisco Secure Client Image, on page 75
- AnyConnect Client External Browser SAML Package, on page 76
- Configure AnyConnect Client VPN Connections, on page 78
- AnyConnect Client HostScan, on page 85
- Install or Upgrade HostScan/Secure Firewall Posture, on page 85
- Configure Posture Settings, on page 86
- Uninstall HostScan/Secure Firewall Posture, on page 87
- Assign AnyConnect Client Feature Modules to Group Policies, on page 87
- HostScan/Secure Firewall Posture Related Documentation, on page 89
- Secure Client Solution, on page 89
- AnyConnect Client Customization and Localization, on page 91
- AnyConnect Client Custom Attributes, on page 93
- IPsec VPN Client Software , on page 96
- Zone Labs Integrity Server, on page 96
- ISE Policy Enforcement, on page 97

System Options

The **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options** pane (also reached using **Configuration > Site-to-Site VPN > Advanced > System Options)** lets you configure features specific to IPsec and VPN sessions on the ASA.

- Limit the maximum number of active IPsec VPN sessions—Enables or disables limiting the maximum number of active IPsec VPN sessions. The range depends on the hardware platform and the software license.
  - Maximum IPsec Sessions—Specifies the maximum number of active IPsec VPN sessions allowed. This field is active only when you choose the preceding check box to limit the maximum number of active IPsec VPN sessions.
- L2TP Tunnel Keep-alive Timeout—Specifies the frequency, in seconds, of keepalive messages. The range is 10 through 300 seconds. The default is 60 seconds. This is an advanced system option for Network (Client) Access only.
- Reclassify existing flows when VPN tunnels establish
- Preserve stateful VPN flows when the tunnel drops—Enables or disables preserving IPsec tunneled flows in Network-Extension Mode (NEM). With the persistent IPsec tunneled flows feature enabled, as long as the tunnel is recreated within the timeout dialog box, data continues flowing successfully because the security appliance still has access to the state information. This option is disabled by default.



Note Tunneled TCP flows are not dropped, so they rely on the TCP timeout for cleanup. However, if the timeout is disabled for a particular tunneled flow, that flow remains in the system until being cleared manually or by other means (for example, by a TCP RST from the peer).

- IPsec Security Association Lifetime—Configures the duration of a Security Association (SA). This parameter specifies how to measure the lifetime of the IPsec SA keys, which is how long the IPsec SA lasts until it expires and must be renegotiated with new keys.
  - **Time**—Specifies the SA lifetime in terms of hours (hh), minutes (mm) and seconds (ss).
  - **Traffic Volume**—Defines the SA lifetime in terms of kilobytes of traffic. Enter the number of kilobytes of payload data after which the IPsec SA expires, or check unlimited. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.
- Enable PMTU (Path Maximum Transmission Unit) Aging—Allows an administrator to enable PMTU aging.
  - Interval to Reset PMTU of an SA (Security Association)—Enter the number of seconds at which the PMTU value is reset to its original value.
- Enable inbound IPsec sessions to bypass interface access-lists. Group policy and per-user authorization ACLs still apply to the traffic—By default, the ASA allows VPN traffic to terminate on an ASA interface; you do not need to allow IKE or ESP (or other types of VPN packets) in an access rule. When this option is checked, you also do not need an access rule for local IP addresses of decrypted VPN packets. Because the VPN tunnel was terminated successfully using VPN security mechanisms, this feature simplifies configuration and maximizes the ASA performance without any security risks. (Group policy and per-user authorization ACLs still apply to the traffic.)

  You can require an access rule to apply to the local IP addresses by unchecking this option. The access rule applies to the local IP address, and not to the original client IP address used before the VPN packet was decrypted.

- Permit communication between VPN peers connected to the same interface—Enables or disables this feature.

  You can also redirect incoming client VPN traffic back out through the same interface unencrypted as well as encrypted. If you send VPN traffic back out through the same interface unencrypted, you should enable NAT for the interface so that publicly routable addresses replace your private IP addresses (unless you already use public IP addresses in your local IP address pool).

- Compression Settings—Specifies the features for which you want to enable compression: WebVPN, and SSL VPN Client. Compression is enabled by default.

Configure Maximum VPN Sessions

To specify the maximum allowed number of VPN sessions or AnyConnect Client VPN sessions, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Advanced** > **Maximum VPN Sessions**.

Step 2 In the **Maximum** AnyConnect Client **Sessions** field, enter the maximum number of sessions allowed.

Valid values range from 1 to the maximum number of sessions that are allowed by your license.

Step 3 In the **Maximum Other VPN Sessions** field, enter the maximum number of VPN sessions allowed, which includes Cisco VPN client (IPsec IKEv1) and LAN-to-LAN VPN sessions.

Valid values range from 1 to the maximum number of sessions that are allowed by your license.

Step 4 Click **Apply**.

Configure DTLS

Datagram Transport Layer Security (DTLS) allows the AnyConnect Client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Before you begin

See, SSL Settingsto configure DTLS on this headend, and which version of DTLS is used.

In order for DTLS to fall back to a TLS connection, Dead Peer Detection (DPD) must be enabled. If you do not enable DPD, and the DTLS connection experiences a problem, the connection terminates instead of falling back to TLS. For more information on DPD, see Internal Group Policy, AnyConnect Client, Dead Peer Detection, on page 32.

Procedure

Step 1 Specify DTLS options for AnyConnect Client VPN connections:

a) Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles , Access Interfaces** section.

b) In the **Interface** table, in the row for the interface you are configuring for AnyConnect Client connections, check the protocols you want to enable on the interface.

- When you check or enable **SSL Access / Allow Access**, **Enable DTLS** is checked or enabled by default.
- To disable DTLS, uncheck **Enable DTLS**. SSL VPN connections will connect with an SSL VPN tunnel only.

c) Choose **Port Settings** to configure **SSL Ports**.

- **HTTPS Port**—The port to enable for HTTPS (browser-based) SSL connections. The range is 1-65535. The default is port 443.
- **DTLS Port**—The UDP port to enable for DTLS connections. The range is 1-65535. The default is port 443.

Step 2 Specify DTLS options for specific group policies.

a) Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, then **Add/Edit > Advanced >** AnyConnect Client.

b) Choose Inherit (default), Enable or Disable for **Datagram Transport Layer Security (DTLS)**.

c) Choose Inherit (default), Enable or Disable for **DTLS Compression**, which configures compression for DTLS.

Configure DNS Server Groups

The **Configuration > Remote Access VPN > DNS** dialog box displays the configured DNS servers in a table, including the server group name, servers, timeout in seconds, number of retries allowed, and domain name. You can add, edit, or delete DNS server groups in this dialog box.

- Add or Edit—Opens the Add or Edit DNS Server Group dialog box. Help for which exists elsewhere
- Delete—Removes the selected row from the table. There is no confirmation or undo.
- DNS Server Group—Selects the server to use as the DNS server group for this connection. The default is DefaultDNS.
- Manage—Opens the Configure DNS Server Groups dialog box.

Configure the Pool of Cryptographic Cores

You can change the allocation of cryptographic cores on Symmetric Multi-Processing (SMP) platforms to increase the throughput of AnyConnect Client TLS/DTLS traffic. These changes can accelerate the SSL VPN datapath and provide customer-visible performance gains in AnyConnect Client, smart tunnels, and port forwarding. These steps describe configuring the pool of cryptographic cores in either single or multiple context mode.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Advanced** > **Crypto Engine**.

Step 2 From the Accelerator Bias drop-down list, specify how to allocate crypto accelerator processors:

Note
This field only shows up if the feature is available on the device.

- **balanced**—Equally distributes cryptography hardware resources (Admin/SSL and IPsec cores).
- **ipsec**—Allocates cryptography hardware resources to favor IPsec (includes SRTP encrypted voice traffic).
- **ssl**—Allocates cryptography hardware resources to favor Admin/SSL. Use this bias when you support SSL-based AnyConnect Client remote access VPN sessions.

Step 3 Click **Apply**.

Client Addressing for SSL VPN Connections

Use this dialog box to specify the global client address assignment policy and to configure interface-specific address pools. You can also add, edit, or delete interface-specific address pools using this dialog box. The table at the bottom of the dialog box lists the configured interface-specific address pools.

- Global Client Address Assignment Policy—Configures a policy that affects all IPsec and SSL VPN Client connections (including AnyConnect Client connections). The ASA uses the selected sources in order, until it finds an address:
  - Use authentication server—Specifies that the ASA should attempt to use the authentication server as the source for a client address.
  - Use DHCP—Specifies that the ASA should attempt to use DHCP as the source for a client address.
  - Use address pool—Specifies that the ASA should attempt to use address pools as the source for a client address.
- Interface-Specific IPv4 Address Pools—Lists the configured interface-specific address pools.
- Interface-Specific IPv6 Address Pools—Lists the configured interface-specific address pools.

- Add—Opens the Assign Address Pools to Interface dialog box, on which you can choose an interface and choose an address pool to assign.
- Edit—Opens the Assign Address Pools to Interface dialog box with the interface and address pool fields filled in.
- Delete—Deletes the selected interface-specific address pool. There is no confirmation or undo.

Assign Address Pools to Interface

Use this dialog box to choose an interface and assign one or more address pools to that interface.

- Interface—Select the interface to which you want to assign an address pool. The default is DMZ.
- Address Pools—Specify an address pool to assign to the specified interface.
- Select—Opens the Select Address Pools dialog box, in which you can choose one or more address pools to assign to this interface. Your selection appears in the Address Pools field of the Assign Address Pools to Interface dialog box.

Select Address Pools

The Select Address Pools dialog box shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you add, edit, or delete entries from that list.

- Add—Opens the Add IP Pool dialog box, on which you can configure a new IP address pool.
- Edit—Opens the Edit IP Pool dialog box, on which you can modify a selected IP address pool.
- Delete—Removes the selected address pool. There is no confirmation or undo.
- Assign—Displays the address pool names that remained assigned to the interface. Double-click each unassigned pool you want to add to the interface. The Assign field updates the list of pool assignments.

Add or Edit an IP Address Pool

Configures or modifies an IP address pool.

- Name—Specifies the name assigned to the IP address pool.
- Starting IP Address—Specifies the first IP address in the pool.
- Ending IP Address—Specifies the last IP address in the pool.
- Subnet Mask—Selects the subnet mask to apply to the addresses in the pool.

Group Policies

A group policy is a collection of user-oriented attribute/value pairs stored either internally on the ASA or externally on a RADIUS or LDAP server. A group policy assigns attributes to a client when the establish a VPN connection. By default, VPN users have no group policy association. The group policy information is used by VPN connection profiles (tunnel groups) and user accounts.

The ASA supplies a default group policy named DfltGrpPolicy. The default group parameters are those that are most likely to be common across all groups and users, which can help streamline the configuration task. New groups can "inherit" parameters from this default group, and users can "inherit" parameters from their group or the default group. You can override these parameters as you configure groups and users.

You can configure internal and external group policies. An internal group policy is stored locally, and an external group policy is stored externally on a RADIUS or LDAP server.

In the Group Policy dialog boxes, you configure the following kinds of parameters:

- General attributes: Name, banner, address pools, protocols, filtering, and connection settings.
- Servers: DNS and WINS servers, DHCP scope, and default domain name.
- Advanced attributes: Split tunneling, IE browser proxy, and AnyConnect Client, and IPsec client.

Before configuring these parameters, you should configure:

- Access hours (General | More Options | Access Hours).
- Filters (General| More Options | Filters).
- IPsec Security Associations (Configuration | Policy Management | Traffic Management | Security Associations).
- Network lists for filtering and split tunneling (Configuration | Policy Management | Traffic Management | Network Lists).
- User authentication servers and the internal authentication server (Configuration | System | Servers | Authentication).

You can configure these types of group policies:

- External Group Policies, on page 8—An external group policy points the ASA to the RADIUS or LDAP server to retrieve much of the policy information that would otherwise be configured in an internal group policy. External group policies are configured the same way for Network (Client) Access VPN connections and Site-to-Site VPN connections.
- Internal Group Policies, on page 10—These connections are initiated by a VPN client installed on the endpoint. The Secure Client and Cisco VPN IPsec client are examples of VPN clients. After the VPN client is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.
- AnyConnect Client Internal Group Policies, on page 15
- Site-to-Site Internal Group Policies, on page 38

Group Policy Pane Fields

The Configuration > Remote Access VPN > Network (Client) Access > Group Policies pane in ASDM lists the currently configured group policies. The Add, Edit, and Delete buttons to help you manage VPN group policies, as described below.

- Add—Offers a drop-down list on which you can choose whether to add an internal or an external group policy. If you simply click Add, then by default, you create an internal group policy. Clicking Add opens the Add Internal Group Policy dialog box or the Add External Group Policy dialog box, which let you

add a new group policy to the list. This dialog box includes three menu sections. Click each menu item to display its parameters. As you move from item to item, ASDM retains your settings. When you have finished setting parameters on all menu sections, click **Apply** or **Cancel**.

- Edit—Displays the Edit Group Policy dialog box, which lets you modify an existing group policy.
- Delete—Lets you remove a AAA group policy from the list. There is no confirmation or undo.
- Assign—Lets you assign a group policy to one ore more connection profiles.
- Name—Lists the name of the currently configured group policies.
- Type—Lists the type of each currently configured group policy.
- Tunneling Protocol—Lists the tunneling protocol that each currently configured group policy uses.
- Connection Profiles/Users Assigned to—Lists the connection profiles and users configured directly on the ASA that are associated with this group policy.

External Group Policies

External group policies retrieve attribute values authorization and authentication from an external server. The group policy identifies the RADIUS or LDAP server group that the ASA can query for attributes, and specifies the password to use when retrieving those attributes.

External group names on the ASA refer to user names on the RADIUS server. In other words, if you configure external group X on the ASA, the RADIUS server sees the query as an authentication request for user X. So external groups are really just user accounts on the RADIUS server that have special meaning to the ASA. If your external group attributes exist in the same RADIUS server as the users that you plan to authenticate, there must be no name duplication between them.

Before you configure the ASA to use an external server, you must configure that server with the correct ASA authorization attributes and, from a subset of these attributes, assign specific permissions to individual users. Follow the instructions in “External Server for Authorization and Authentication” to configure your external server.

These RADIUS configurations include RADIUS with LOCAL authentication, RADIUS with Active Directory/Kerberos Windows DC, RADIUS with NT/4.0 Domain, and RADIUS with LDAP.

External Group Policy Fields

- Name—Identifies the group policy to be added or changed. For Edit External Group Policy, this field is display-only.
- Server Group—Lists the available server groups to which to apply this policy.
- New—Opens a dialog box that lets you choose whether to create a new RADIUS server group or a new LDAP server group. Either of these options opens the Add AAA Server Group dialog box.
- Password—Specifies the password for this server group policy.

For information about creating and configuring AAA servers, see the *Cisco ASA Series General Operations ASDM Configuration Guide*, the *AAA Servers and Local Database* chapter.

Password Management with AAA Servers

The ASA supports password management for the RADIUS and LDAP protocols. It supports the "password-expire-in-days" option only for LDAP. The other parameters are valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The ASA ignores this command if RADIUS or LDAP authentication has not been configured.



Note Some RADIUS servers that support MS-CHAP currently do not support MS-CHAPv2. This feature requires MS-CHAPv2, so check with your vendor.

The ASA generally supports password management for the following connection types when authenticating with LDAP or with any RADIUS configuration that supports MS-CHAPv2:

- AnyConnect VPN client
- IPsec VPN client
- IPsec IKEv2 clients

Password management is *not* supported for Kerberos/Active Directory (Windows password) or NT 4.0 Domain. Some RADIUS servers, for example, Cisco ACS, can proxy the authentication request to another authentication server. However, from the perspective of the ASA, it is communicating only to a RADIUS server.



Note For LDAP, the method to change a password is proprietary for the different LDAP servers on the market. Currently, the ASA implements the proprietary password management logic only for Microsoft Active Directory and Sun LDAP servers.

Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.

Password Support with AnyConnect Client

The ASA supports the following password management features for AnyConnect Client:

- Password expiration notice, when the user tries to connect.
- Password expiration reminders, before the password has expired.
- Password expiration override. The ASA ignores password expiration notices from the AAA server, and authorizes the user's connection.

When password management is configured, the ASA notifies remote users when they try to log in that their current password has expired, or is about to expire. The ASA then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using the old password, and change the password later.

The AnyConnect Client cannot initiate password change, it can only respond to a change request from the AAA server through the ASA. The AAA server must be a RADIUS server proxying to AD, or an LDAP server.

The ASA does not support password management under the following conditions:

- when using LOCAL (internal) authentication
- when using LDAP authorization
- when using RADIUS authentication only, and when the users reside on the RADIUS server database

Setting password expiration override tells the ASA to ignore account-disabled indications from a AAA server. This can be a security risk. For example, you may not want to change the Administrators' password.

Enabling password management causes the ASA to send MS-CHAPv2 authentication requests to the AAA server.

Internal Group Policies

Internal Group Policy, General Attributes

On the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** pane, the Add or Edit Group Policy dialog box lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified. For each of the fields in 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 of the attributes in this dialog box.

You configure the general attributes of an internal group policy in ASDM by selecting **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General.** The following attributes apply to SSL VPN and IPsec sessions. Thus, some attributes are present for one type of session, but not the other.

- **Name**—Specifies the name of this group policy, up to 64 characters; spaces are allowed. For the Edit function, this field is read-only.
- **Banner**—Specifies the banner text to present to users at login. The length can be up to 4000 characters. There is no default value.

  The IPsec VPN client supports full HTML for the banner. However, the clientless portal and the AnyConnect Client support partial HTML. To ensure the banner displays properly to remote users, follow these guidelines:

  - For IPsec client users, use the /n tag.
  - For AnyConnect Client users, use the <BR> tag.

- **SCEP forwarding URL**—Address of the CA, required when SCEP Proxy is configured in the client profile.
- **Address Pools**—Specifies the name of one or more IPv4 address pools to use for this group policy. If the Inherit check box is checked, the group policy uses the IPv4 address pool specified in the Default Group Policy. See for information on adding or editing an IPv4 address pool.



Note You can specify both an IPv4 and an IPv6 address pool for an internal group policy.

Select—Uncheck the Inherit checkbox to activate this button. Click **Select** to open the Address Pools dialog box, which shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you choose, add, edit, delete, and assign entries from that list.

- **IPv6 Address Pools**—Specifies the name of one or more IPv6 address pools to use for this group policy.

  Select—Uncheck the Inherit checkbox to activate this button. Click **Select** to open the Select Address Pools dialog box, as previously described. See for information on adding or editing an IPv6 address pool.

- **More Options**—Click the down arrows at the right of the field to display additional configurable options for this group policy.
- **Tunneling Protocols**—Specifies the tunneling protocols that this group can use. Users can use only the selected protocols. The choices are as follows:
  - **Clientless SSL VPN**—Specifies the use of VPN via SSL/TLS, which uses a web browser to establish a secure remote-access tunnel to an ASA; 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 share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
  - **SSL VPN Client**—Specifies the use of the Cisco AnyConnect VPN client or the legacy SSL VPN client. If you are using the AnyConnect Client, you must choose this protocol for Mobile User Security (MUS) to be supported.
  - **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**—Supported by the Secure Client. AnyConnect Client connections using IPsec with IKEv2 provide advanced features such as software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy.
  - **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 security appliance and private corporate networks. L2TP uses PPP over UDP (port 1701) to tunnel the data. The security appliance must be configured for IPsec transport mode.
- **Filter**—Specifies which access control list to use for an IPv4 or an IPv6 connection, 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. Note that the VPN filter applies to initial connections only. It does not apply to secondary connections, such as a SIP media connection, that are opened due to the action of application inspection. To configure filters and rules, click **Manage**.
- **NAC Policy**—Selects the name of a Network Admission Control policy to apply to this group policy. You can assign an optional NAC policy to each group policy. The default value is --None--.
- **Manage**—Opens the Configure NAC Policy dialog box. After configuring one or more NAC policies, the NAC policy names appear as options in the drop-down list next to the NAC Policy attribute.
- **Access Hours**—Selects the name of an existing access hours policy, if any, applied to this user or create a new access hours policy. The default value is Inherit, or, if the Inherit check box is not checked, the default value is --Unrestricted--. Click **Manage** to open the Browse Time Range dialog box, in which you can add, edit, or delete a time range.

- **Simultaneous Logins**—Specifies the maximum number of simultaneous logins allowed for this user. The default value is 3. The minimum value is 0, which disables login and prevents user access.

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

- **Restrict Access to VLAN**—(Optional) Also called "VLAN mapping," this parameter specifies the egress VLAN interface for sessions to which this group policy applies. The ASA forwards all traffic from this group to the selected VLAN. Use this attribute to assign a VLAN to the group policy to simplify access control. Assigning a value to this attribute is an alternative to using ACLs to filter traffic on a session. In addition to the default value (Unrestricted), the drop-down list shows only the VLANs that are configured in this ASA.

Note This feature works for HTTP connections, but not for FTP and CIFS.

- **Connection Profile (Tunnel Group) Lock**—This parameter permits remote VPN access only with the selected connection profile (tunnel group), and prevents access with a different connection profile. The default inherited value is None.
- **Maximum Connect Time**—If the **Inherit** check box is not checked, this parameter sets the maximum user connection time in minutes.

  At the end of this time, the system terminates the connection. The minimum is 1minute, and the maximum is 35791394 minutes. To allow unlimited connection time, check **Unlimited** (default).
- **Idle Timeout**—If the **Inherit** check box is not checked, this parameter sets the idle timeout in minutes.

  If there is no communication activity on the connection in this period, the system terminates the connection. The minimum time is 1 minute, the maximum time is 10080 minutes, and the default is 30 minutes. To allow unlimited connection time, check **Unlimited**.
- **Security Group Tag (SGT)**—Enter the numerical value of the SGT tag that will be assigned to VPN users connecting with this group policy.
- **On smart card removal**—With the default option, Disconnect, the client tears down the connection if the smart card used for authentication is removed. Click **Keep the connection** if you do not want to require users to keep their smart cards in the computer for the duration of the connection.

  Smart card removal configuration only works on Microsoft Windows using RSA smart cards.
- **Disable Delete tunnel with no delay in Simultaneous Session preempt**—When a given user reaches the allowed **Simultaneous Logins** limit, the user's next login attempt requires the system to first delete the oldest session. This deletion can take a few seconds, which can prevent the user from establishing a new session immediately. Select this option to instruct the system to establish the new session without waiting for the deletion of the oldest session to complete.
- **Maximum Connection Time Alert Interval**—The interval of time before max connection time is reached that a message will be displayed to the user.

If you uncheck the **Inherit** check box, the **Default** check box is checked automatically. This sets the session alert interval to 30 minutes. If you want to specify a new value, uncheck **Default** and specify a session alert interval from 1 to 30 minutes.

- **Periodic Certificate Authentication Interval**—The interval of time in hours, before certificate authentication is redone periodically.

  If the **Inherit** check box is not checked, you can set the interval for performing periodic certificate verification. The range is between 1 and 168 hours, and the default is disabled. To allow unlimited verification, check Unlimited.

Configure Internal Group Policy, Server Attributes

Configure DNS servers, WINS servers and DHCP Scope in the Group Policy > Servers window. DNS and WINS servers are applied to full-tunnel clients (IPsec, AnyConnect Client, SVC, and L2TP/IPsec) only and are used for name resolution. DHCP scope is used when DHCP-address assignment is in place.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add/Edit** > **Servers**.

Step 2 Unless you are editing the DefaultGroupPolicy, uncheck the DNS Servers **Inherit** checkbox and add the IPv4 or IPv6 addresses of the DNS servers you want this group to use. You can specify two IPv4 addresses and two IPv6 addresses.

If you specify more than one DNS server, the remote access client attempts to use the DNS servers in the order you specify in this field.

Changes you make here override the DNS setting configured on the ASDM in the **Configuration > Remote Access VPN > DNS** window for clients using this group policy.

Step 3 Uncheck the WINS Servers **Inherit** checkbox and enter the IP addresses of the primary and secondary WINS servers. The first IP address you specify is that of the primary WINS server. The second (optional) IP address you specify is that of the secondary WINS server. .

Step 4 Expand the **More Options** area by clicking the double down arrow in the More Options bar.

Step 5 Uncheck DHCP Scope **Inherit** and define the DHCP scope.

If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same subnet identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group.

If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

To specify a scope, enter a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.

We recommend using the IP address of an interface whenever possible for routing purposes. For example, if the pool is 10.100.10.2-10.100.10.254, and the interface address is 10.100.10.1/24, use 10.100.10.1 as the

DHCP scope. Do not use the network number. You can use DHCP for IPv4 addressing only. If the address you choose is not an interface address, you might need to create a static route for the scope address.

Step 6 If there is no default domain specified in the **Configuration** > **Remote Access VPN** > **DNS** window, you must specify the default domain in the **Default Domain** field. Use the domain name and top level domain for example, example.com.

Step 7 Click **OK**.

Step 8 Click **Apply**.

Internal Group Policy, Browser Proxy

Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > Browser Proxy

This dialog box configures attributes that will be pushed down to the client to reconfigure Microsoft Internet Explorer settings:

- Proxy Server Policy—Configures the Microsoft Internet Explorer browser proxy actions ("methods") for a client PC.
  - Do not modify client proxy settings—Leaves the HTTP browser proxy server setting in Internet Explorer unchanged for this client PC.
  - Do not use proxy—Disables the HTTP proxy setting in Internet Explorer for the client PC.
  - Select proxy server settings from the following—Enables the following check boxes for your selections: Auto detect proxy, Use proxy server settings given below, and Use proxy auto configuration (PAC) given below.
  - Auto detect proxy—Enables the use of automatic proxy server detection in Internet Explorer for the client PC.
  - Use proxy server settings specified below—Sets the HTTP proxy server setting in Internet Explorer to use the value configured in the Proxy Server Name or IP Address field.
  - Use proxy auto configuration (PAC) given below—Specifies the use of the file specified in the Proxy Auto Configuration (PAC) field as the source for auto configuration attributes.
- Proxy Server Settings—Configures the proxy server parameters for Microsoft clients using Microsoft Internet Explorer.
  - Server Address and Port—Specifies the IP address or name and the port of an Microsoft Internet Explorer server that is applied for this client PC.
  - Bypass Proxy Server for Local Addresses—Configures Microsoft Internet Explorer browser proxy local-bypass settings for a client PC. Click **Yes** to enable local bypass or **No** to disable local bypass.
  - Exception List—Lists the server names and IP addresses that you want to exclude from proxy server access. Enter the list of addresses that you do not want to have accessed through a proxy server. This list corresponds to the Exceptions list in the Proxy Settings dialog box in Internet Explorer.
- Proxy Auto Configuration Settings—The PAC URL specifies the URL of the auto-configuration file. This file tells the browser where to look for proxy information. To use the proxy auto-configuration (PAC) feature, the remote user must use the Cisco AnyConnect VPN client.

Many network environments define HTTP proxies that connect a web browser to a particular network resource. The HTTP traffic can reach the network resource only if the proxy is specified in the browser and the client routes the HTTP traffic to the proxy. SSLVPN tunnels complicate the definition of HTTP proxies because the proxy required when tunneled to an enterprise network can differ from that required when connected to the Internet via a broadband connection or when on a third-party network.

In addition, companies with large networks might need to configure more than one proxy server and let users choose between them, based on transient conditions. By using .pac files, an administrator can author a single script file that determines which of numerous proxies to use for all client computers throughout the enterprise.

The following are some examples of how you might use a PAC file:

- Choosing a proxy at random from a list for load balancing.
- Rotating proxies by time of day or day of the week to accommodate a server maintenance schedule.
- Specifying a backup proxy server to use in case the primary proxy fails.
- Specifying the nearest proxy for roaming users, based on the local subnet.

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. Use the PAC URL field to specify the URL from which to retrieve the .pac file. Then the browser uses the .pac file to determine the proxy settings.

- Proxy Lockdown
  - Allow Proxy Lockdown for Client System - Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect Client VPN session. In addition, from Windows 10 version 1703 (or later), enabling this feature also hides the system proxy tab in Settings app for the duration of an AnyConnect Client VPN session. Disabling the feature leaves the display of the Connections tab in Microsoft Internet Explorer and Proxy tab in Settings app unchanged; the default setting for them can be to show or hide, depending on the user registry settings.



Note Hiding the system proxy tab in the Settings app for the duration of an AnyConnect Client VPN session needs AnyConnect version 4.7.03052 or later.

AnyConnect Client Internal Group Policies

Internal Group Policy, Advanced, AnyConnect Client

- Keep Installer on Client System—Enable to allow permanent client installation on the remote computer. Enabling disables the automatic uninstalling feature of the client. The client remains installed on the remote computer for subsequent connections, reducing the connection time for the remote user.
- Compression—Compression increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred.

- Datagram TLS—Datagram Transport Layer Security avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.
- Ignore Don't Defrag (DF) Bit—This feature allows the force fragmentation of packets that have the DF bit set, allowing them to pass through the tunnel. An example use case is for servers in your network that do not respond correctly to TCP MSS negotiations.
- Client Bypass Protocol—The Client Protocol Bypass feature allows you to configure how the AnyConnect Client manages IPv4 traffic when ASA is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

  When the AnyConnect Client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the AnyConnect Client connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or "in the clear."

  For example, assume that the ASA assigns only an IPv4 address to an AnyConnect Client 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; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

  If establishing an IPsec tunnel (as opposed to an SSL connection), the ASA is not notified whether or not IPv6 is enabled on the client, so ASA always pushes down the client bypass protocol setting.

- FQDN of This Device—This information is used by the client after network roaming in order to resolve the ASA IP address used for re-establishing the VPN session. This setting is critical to support roaming between networks of different IP protocols (such as IPv4 to IPv6).



Note You cannot use the ASA FQDN present in the AnyConnect Client profile to derive the ASA IP address after roaming. The addresses may not match the correct device (the one the tunnel was established to) in the load balancing scenario.

  If the device FQDN is not pushed to the client, the client tries to reconnect to whatever IP address the tunnel had previously established. In order to support roaming between networks of different IP protocols (from IPv4 to IPv6), AnyConnect Client must perform name resolution of the device FQDN after roaming, so that it can determine which ASA address to use for re-establishing the tunnel. The client uses the ASA FQDN present in its profile during the initial connection. During subsequent session reconnects, it always uses the device FQDN pushed by ASA (and configured by the administrator in the group policy), when available. If the FQDN is not configured, the ASA derives the device FQDN (and sends it to the client) from whatever is set under Device Setup > Device Name/Password and Domain Name.

  If the device FQDN is not pushed by the ASA, the client cannot re-establish the VPN session after roaming between networks of different IP protocols.

- MTU—Adjusts the MTU size for SSL connections. Enter a value in bytes, from 256 to 1410 bytes. By default, the MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.
- Keepalive Messages—Enter a number, from 15 to 600 seconds, in the Interval field to enable and adjust the interval of keepalive messages to ensure that a connection through a proxy, firewall, or NAT device

remains open, even if the device limits the time that the connection can be idle. Adjusting the interval also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

- **Optional Client Modules to Download**—To minimize download time, the AnyConnect Client requests downloads (from the ASA) only of modules that it needs for each feature that it supports. You must specify the names of modules that enable other features. The AnyConnect Client includes the following modules (some earlier versions have fewer modules):
  - AnyConnect Client DART—The Diagnostic AnyConnect Client Reporting Tool (DART) captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
  - AnyConnect Client Network Access Manager—Formerly called the Cisco Secure Services Client, this module provides 802.1X (Layer 2) and device authentication for access to both wired and wireless networks.
  - AnyConnect Client SBL—Start Before Logon (SBL) forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect Client before the Windows login dialog box appears.
  - Secure Firewall Posture Module—Formerly called the Cisco Secure Desktop HostScan feature, the posture module is integrated into AnyConnect Client and provides AnyConnect Client the ability to gather credentials for posture assessment prior to creating a remote access connection to the ASA.
  - ISE Posture—Uses the OPSWAT v3 library to perform posture checks to assess an endpoint's compliance. You can then restrict network access until the endpoint is in compliance or can elevate local user privileges.
  - AMP Enabler—Used as medium for deploying Advanced Malware Protection (AMP) for endpoints. It pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base.
  - Network Visibility Module—Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics. The NVM collects the endpoint telemetry and logs both the flow data and the file reputation in the syslog and also exports the flow records to a collector (a third-party vendor), which performs the file analysis and provides a UI interface.
  - Umbrella Roaming Security Module—Provides DNS-layer security when no VPN is active. It provides a subscription to either Cisco Umbrella Roaming service or OpenDNS Umbrella services, which add Intelligent Proxy and IP-Layer Enforcement features. The Umbrella Security Roaming profile associates each deployment with the corresponding service and automatically enables the corresponding protection level (whether content filtering, multiple policies, robust reporting, active directory integration, or basic DNS-layer security).

- Always-On VPN—Determine if the always-on VPN flag setting in the AnyConnect Client service profile is disabled or if the AnyConnect Client service profile setting should be used. The always-on VPN feature lets AnyConnnect automatically establish a VPN session after the user logs onto a computer. The VPN session remains up until the user logs off the computer. If the physical connection is lost, the session remains up, and AnyConnect Client continually attempts to reestablish the physical connection with the adaptive security appliance to resume the VPN session.

  Always-on VPN permits the enforcement of corporate policies to protect the device from security threats. You can use it to help ensure AnyConnect Client establishes a VPN session whenever the endpoint is

not in a trusted network. If enabled, a policy is configured to determine how network connectivity is managed in the absence of a connection.

Note Always-On VPN requires an AnyConnect Client release that supports Secure Client features.

- Client Profiles to Download—A profile is a group of configuration parameters that the AnyConnect Client uses to configure VPN, Network Access Manager, Web Security, ISE Posture, AMP Enabler, Network Visibility Module, and Umbrella Roaming Security module settings. Click **Add** to launch the Select AnyConnect Client Profiles window where you can specify previously-created profiles for this group policy.

Configure Split-Tunneling for AnyConnect Client Traffic

Split tunneling directs some of the AnyConnect Client network traffic through the VPN tunnel (encrypted) and other network traffic outside the VPN tunnel (unencrypted or “in the clear”).

Split tunneling is configured by creating a split tunneling policy, configuring an access control list for that policy, and adding the split tunnel policy to a group policy. When the group policy is sent to the client, that client uses the ACLs in the split tunneling policy to decide where to direct network traffic.

Note Split tunneling is a traffic management feature, not a security feature. For optimum security, we recommend that you do not enable split tunneling.

For Windows clients, firewall rules from the ASA are evaluated first, then the ones on the client. For Mac OS X, the firewall and filter rules on the client are not used. For Linux systems, starting with AnyConnect version 3.1.05149, you can configure AnyConnect Client to evaluate the client's firewall and filter rules, by adding a custom attribute named circumvent-host-filtering to a group profile, and setting it to true.

When you create access lists:

- You can specify both IPv4 and IPv6 addresses in an access control list.
- If you use a standard ACL, only one address or network is used.
- If you use extended ACLs, the source network is the split-tunneling network. The destination network is ignored.
- Access lists configured with any or with a split include or exclude of 0.0.0.0/0.0.0.0 or ::/0 will not be sent to the client. To send all traffic over the tunnel, choose **Tunnel All Networks** for the split-tunnel **Policy**.
- Address 0.0.0.0/255.255.255.255 or ::/128 is sent to the client only when the split-tunnel policy is **Exclude Network List Below**. This configuration tells the client not to tunnel traffic destined for any local subnets.
- AnyConnect Client passes traffic to all sites specified in the split tunneling policy, and to all sites that fall within the same subnet as the IP address assigned by the ASA. For example, if the IP address assigned by the ASA is 10.1.1.1 with a mask of 255.0.0.0, the endpoint device passes all traffic destined to 10.0.0.0/8, regardless of the split tunneling policy. Therefore, use a netmask for the assigned IP address that properly references the expected local subnet.

Before you begin

- You must create an access list with the appropriate ACEs.
- If you created a split tunnel policy for IPv4 networks and another for IPv6 networks, then the network list you specify is used for both protocols. So, the network list should contain access control entries (ACEs) for both IPv4 and IPv6 traffic. If you have not created these ACLs, see the general operations configuration guide.

In the following procedure, in all cases where there is an Inherit checkbox next to a field, leaving the Inherit check box checked means that the group policy you are configuring uses the same values for that field as the default group policy. Unchecking Inherit lets you specify new values specific to your group policy.

Procedure

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

Step 2 Click **Add** to add a new group policy or choose an existing group policy and click **Edit**.

Step 3 Select **Advanced** > **Split Tunneling**.

Step 4 In the **DNS Names** field, enter the domain names that are to be resolved by AnyConnect Client via the tunnel. These names correspond to hosts in the private network. If split-include tunneling is configured, the network list must include the specified DNS servers. You can enter a full qualified domain name, IPv4 or IPv6 address in the field.

A dynamic split tunneling domain name requires at least one domain name label besides the top level domain. Because dynamic split tunneling is meant to target flows matching specific domain names, specifying just a top level domain (such as *org*) is unacceptable. You are required to enter the top level domain and at least one domain name label (such as *domain.org)*.

Step 5 To disable split tunneling, click **Yes** to enable **Send All DNS Lookups Through Tunnel**. This option ensures that DNS traffic is not leaked to the physical adapter; it disallows traffic in the clear. If DNS resolution fails, the address remains unresolved, and the AnyConnect Client does not try to resolve the address outside the VPN.

To enable split tunneling, choose **No** (the default). This setting tells the client to send DNS queries over the tunnel according to the split tunnel policy.

Step 6 To configure split-tunneling, uncheck the **Inherit** check box and choose a split-tunneling policy. If you do not uncheck **Inherit**, your group policy uses the split tunneling settings defined in the default group policy, **DfltGrpPolicy**. The default split tunneling policy setting in the default group policy is to Tunnel All Networks.

To define the split tunneling policy, chose from the drop-downs **Policy** and **IPv6 Policy**. The Policy field defines the split tunneling policy for IPv4 network traffic. The IPv6 Policy field selects the split tunneling policy for IPv6 network traffic. Other than that difference, these fields have the same purpose.

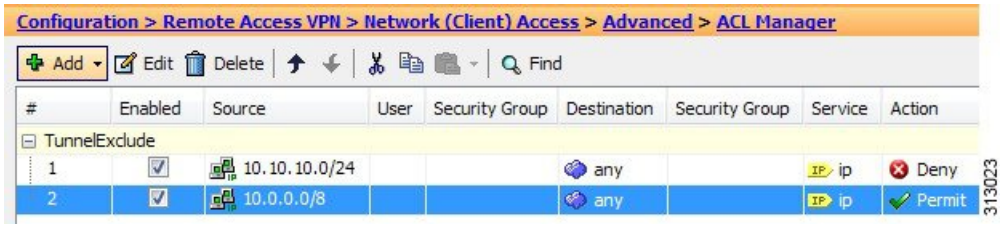
Unchecking **Inherit** allows you to choose one of these policy options:

- **Exclude Network List Below**—Defines a list of networks to which traffic is sent in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.

- **Tunnel Network List Below**—Tunnels all traffic from or to the networks specified in the Network List. Traffic to addresses in the include network list are tunneled. Data to all other addresses travels in the clear and is routed by the remote user's Internet service provider.

  For versions of ASA 9.1.4 and higher, when you specify an include list, you can also specify an exclude list that is a subset of the include range. Those excluded subnets are not tunneled, and the rest of the include list networks are. Networks in the exclusion list that are not a subset of the include list are ignored by the client. For Linux, you must add a custom attribute to the group policy to support excluded subnets.

  For example:



Note
If the split-include network is an exact match of a local subnet (such as 192.168.1.0/24), the corresponding traffic is tunneled. If the split-include network is a superset of a local subnet (such as 192.168.0.0/16), the corresponding traffic, except the local subnet traffic, is tunneled. To also tunnel the local subnet traffic, you must add a matching split-include network (specifying both 192.168.1.0/24 and 192.168.0.0/16 as split-include networks).

If the split-include network is invalid, such as 0.0.0.0/0.0.0.0, then split tunneling is disabled (everything is tunneled).

- **Tunnel All Networks**—This policy specifies that all traffic is tunneled. This, in effect, disables split tunneling. Remote users reach Internet networks through the corporate network and do not have access to local networks. This is the default option.

Step 7 In the **Network List** field, choose the access control list for the split-tunneling policy. If Inherit is checked, the group policy uses the network list specified in the default group policy.

Select the **Manage** command button to open the ACL Manager dialog box, in which you can configure access control lists to use as network lists. For more information about how to create or edit a network list, see the general operations configuration guide.

Extended ACL lists can contain both IPv4 and IPv6 addresses.

Step 8 The **Intercept DHCP Configuration Message from Microsoft Clients** reveals additional parameters specific to DHCP Intercept. DHCP Intercept lets Microsoft XP clients use split-tunneling with the ASA.

- Intercept—Specifies whether to allow the DHCP Intercept to occur. If you do not choose Inherit, the default setting is No.
- Subnet Mask—Selects the subnet mask to use.

Step 9 Click **OK**.

Configure Dynamic Split Tunneling

With dynamic split tunneling, you can dynamically provision split exclude tunneling after tunnel establishment based on the host DNS domain name. Dynamic split tunneling is configured by creating a custom attribute and adding it to a group policy.

Before you begin

To use this feature, you must have AnyConnect release 4.5 (or later). Refer to About Dynamic Split Tunneling for further explanation.

Procedure

Step 1 Browse to **Configuration > Remote Access VPN > Network (Client) Access > Advanced >** AnyConnect Client **Custom Attributes** screen.

Step 2 Click **Add** and enter `dynamic-split-exclude-domains` as an attribute type and enter a description.

Step 3 After you click to apply this new attribute, click on the **AnyConnect Client custom attribute names** link at the top of the UI screen.

Step 4 Add the corresponding custom attribute names for each cloud/web service that needs access by the client from outside the VPN tunnel. For example, add Google_domains to represent a list of DNS domain names pertaining to Google web services. Define these domains in the Value portion of the AnyConnect Client Custom Attribute Names screen, using the comma-separated-values (CSV) format, which separates domains by a comma character. AnyConnect Client only takes into account the first 20,000 characters, excluding separator characters (roughly 300 typically-sized domain names). Domain names beyond that limit are ignored.

A custom attribute cannot exceed 421 characters. If a larger value is entered, ASDM breaks it into multiple values capped at 421 characters. All values for a certain attribute type and name are concatenated by ASA when the configuration is pushed to the client.

Step 5 Attach the dynamic split-exclude tunneling attributes to a certain group policy by browsing to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 6 You can either create a new group policy or click **Edit** to manage an existing group policy.

What to do next

If split include tunneling is configured, a dynamic split exclusion is enforced only if at least one of the DNS response IP addresses is part of the split-include network. If there is no overlap between any of the DNS response IP addresses and any of the split-include networks, enforcing dynamic split exclusion is not necessary since traffic matching all DNS response IP addresses is already excluded from tunneling.

Configure Dynamic Split Exclude Tunneling

Follow these configuration steps to enable dynamic split exclude tunneling using ASDM. When both dynamic split exclude and include domains are defined, enhanced dynamic split exclude tunneling with domain name matching is enabled. For eample, an administrator could configure all traffic to example.com to be excluded except www.example.com. *Example.com* is the dynamic split exclude domain and *www.example.com* is the dynamic split include domain.

Note You must have AnyConnect release 4.5 (or later) to use dynamic split exclude tunneling. Additionally, AnyConnect release 4.6 (and later) added a refinement for enhanced dynamic split include and split exclude when domains for both are configured. Dynamic split exclude applies to all of tunnel-all, split-exclude and split-include configurations.

Before you begin

Refer to the *Dynamic Split Tunneling* section for AnyConnect Client requirements.

Procedure

Step 1 Browse to **Configuration > Remote Access VPN > Network (Client) Access > Advanced >** AnyConnect Client **Custom Attributes** screen.

Step 2 Click **Add** and enter `dynamic-split-exclude-domains` as an attribute type and enter a description.

Step 3 After you click to apply this new attribute, click on the **AnyConnect Client custom attribute names** link at the top of the UI screen.

Step 4 Add the corresponding custom attribute names for each cloud/web service that needs access by the client from outside the VPN tunnel. For example, add Google_domains to represent a list of DNS domain names pertaining to Google web services. Define these domains in the Value portion of the AnyConnect Client Custom Attribute Names screen, using the comma-separated-values (CSV) format, which separates domains by a comma character. AnyConnect Client only takes into account the first 5000 characters, excluding separator characters (roughly 300 typically-sized domain names). Domain names beyond that limit are ignored.

A custom attribute cannot exceed 421 characters. If a larger value is entered, ASDM breaks it into multiple values capped at 421 characters. All values for a certain attribute type and name are concatenated by ASA when the configuration is pushed to the client.

Step 5 Attach the dynamic split-exclude tunneling attributes to a certain group policy by browsing to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 6 You can either create a new group policy or click **Edit** to manage an existing group policy.

Step 7 In the left-hand menu, click **Advanced >** AnyConnect Client **> Custom Attributes** and choose your attribute type from the drop down.

Configure Dynamic Split Include Tunneling

Follow these configuration steps to enable dynamic split include tunneling using ASDM. When both dynamic split exclude and include domains are defined, enhanced dynamic split include tunneling with domain name matching is enabled. For eample, an administrator could configure all traffic to domain.com to be included except www.domain.com. *Domain.com* is the dynamic split include domain and *www.domain.com* is the dynamic split exclude domain.

Note You must have AnyConnect release 4.6 (or later) to use dynamic split include tunneling. Additionally, AnyConnect release 4.6 (and later) added a refinement for enhanced dymanic split include and split exclude when domains for both are configured. Dynamic split include applies only to split-include configuration.

Before you begin

Refer to the *Dynamic Split Tunneling* section for AnyConnect Client requirements.

Procedure

Step 1 Browse to **Configuration > Remote Access VPN > Network (Client) Access > Advanced >** AnyConnect Client **Custom Attributes** screen.

Step 2 Click **Add** and enter `dynamic-split-include-domains` as an attribute type and enter a description.

Step 3 After you click to apply this new attribute, click on the **AnyConnect Client custom attribute names** link at the top of the UI screen.

Step 4 Add the corresponding custom attribute names for each cloud/web service that needs access by the client from outside the VPN tunnel. For example, add Google_domains to represent a list of DNS domain names pertaining to Google web services. Define these domains in the Value portion of the AnyConnect Client Custom Attribute Names screen, using the comma-separated-values (CSV) format, which separates domains by a comma character. AnyConnect Client only takes into account the first 5000 characters, excluding separator characters (roughly 300 typically-sized domain names). Domain names beyond that limit are ignored.

A custom attribute cannot exceed 421 characters. If a larger value is entered, ASDM breaks it into multiple values capped at 421 characters. All values for a certain attribute type and name are concatenated by ASA when the configuration is pushed to the client.

Step 5 Attach the dynamic split-include tunneling attributes to a certain group policy by browsing to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 6 You can either create a new group policy or click **Edit** to manage an existing group policy.

Step 7 In the left-hand menu, click **Advanced >** AnyConnect Client **> Custom Attributes** and choose your attribute type from the drop down.

Configure the Management VPN Tunnel

A management VPN tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. You can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint OS login scripts which require corporate network connectivity will also benefit from this feature.

The management VPN tunnel is meant to be transparent to the end user; therefore, network traffic initiated by user applications is not impacted, by default, but instead directed outside the management VPN tunnel.

If a user complains of slow logins, it may be an indication that the management tunnel was not configured appropriately. Refer to the Cisco Secure Client Administration Guide for additional requirements, incompatibilities, limitations, and troubleshooting of management VPN tunnel.

Before you begin

Requires AnyConnect release 4.7 (or later)

Procedure

Step 1 You must configure the authentication method of the tunnel group as "certificate only" by navigating to **Configuration** > **Remote Access > Network (Client) Access >** AnyConnect Client **Connection Profiles > Add/Edit** and choosing it from the Method drop-down menu under Authentication.

Step 2 Then from that same window, choose **Advanced > Group Alias/Group URL** and add the group URL to be specified in the management VPN profile.

Step 3 The group policy for this tunnel group must have split include tunneling configured for all IP protocols with address pool configured in the the tunnel group: choose Tunnel Network List Below from **Remote Access VPN** > **Network (Client) Access > Group Policies > Edit > Advanced > Split Tunneling** .

Step 4 (Optional) Management VPN tunnel requires split include tunneling configuration, by default, to avoid impacting user initiated network communication (since it is meant to be transparent). You can override this behavior by configuring the custom attribute in the group policy used by the management tunnel connection: AnyConnect Client Custom Attributes, on page 93.
If an address pool is not configured in the tunnel group for both IP protocols, you must enable *Client Bypass Protocol* in the group policy, so that traffic matching the IP protocol without address pool is not disrupted by the management VPN tunnel.

Step 5 Create the profile and choose management VPN tunnel for profile usage: Configure AnyConnect Client Profiles, on page 78.

Configure Linux to Support Excluded Subnets

When **Tunnel Network List Below** is configured for split tunneling, Linux requires extra configuration to support exclude subnets. You must create a custom attribute named circumvent-host-filtering, set it to true, and associate with the group policy that is configured for split tunneling.

Procedure

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

Step 2 Click **Add**, create a custom attribute named **circumvent-host-filtering**, and set the value to **true**.

Step 3 Edit the group policy you plan to use for client firewall, and navigate to **Advanced** > AnyConnect Client > **Custom Attributes**.

Step 4 Add the custom attribute that you created, **circumvent-host-filtering**, to the group policy you will use for split tunneling.

Internal Group Policy, AnyConnect Client Attributes

Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced >AnyConnect Client, contains configurable attributes for the AnyConnect Client in this group policy.

- Keep Installer on Client System—Enable permanent client installation on the remote computer. Enabling disables the automatic uninstalling feature of the client. The client remains installed on the remote computer for subsequent connections, reducing the connection time for the remote user.



Note Keep Installer on Client System is not supported after version 2.5 of the AnyConnect Client.

- Datagram Transport Layer Security (DTLS)—Avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.
- DTLS Compression— Configures compression for DTLS.
- SSL Compression—Configures compression for SSL/TLS.
- Ignore Don't Defrag (DF) Bit—This feature allows the force fragmentation of packets that have the DF bit set, allowing them to pass through the tunnel. An example use case is for servers in your network that do not respond correctly to TCP MSS negotiations.
- Client Bypass Protocol—Client Protocol Bypass configures how the AnyConnect Client manages IPv4 traffic when ASA is expecting only IPv6 traffic, or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

  When the AnyConnect Client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. The Client Bypass Protocol determines whether to drop traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or "in the clear."

  For example, assume that the ASA assigns only an IPv4 address to an AnyConnect Client 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; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

- FQDN of This Device—This information is used by the client after network roaming in order to resolve the ASA IP address used for re-establishing the VPN session. This setting is critical to support roaming between networks of different IP protocols (such as IPv4 to IPv6).



Note You cannot use the ASA FQDN present in the AnyConnect Client profile to derive the ASA IP address after roaming. The addresses may not match the correct device (the one the tunnel was established to) in the load balancing scenario.

If the device FQDN is not pushed to the client, the client tries to reconnect to whatever IP address the tunnel had previously established. In order to support roaming between networks of different IP protocols (from IPv4 to IPv6), AnyConnect Client must perform name resolution of the device FQDN after roaming, so that it can determine which ASA address to use for re-establishing the tunnel. The client uses the ASA FQDN present in its profile during the initial connection. During subsequent session reconnects, it always uses the device FQDN pushed by ASA (and configured by the administrator in the group policy), when available. If the FQDN is not configured, the ASA derives the device FQDN (and sends it to the client) from whatever is set under Device Setup > Device Name/Password and Domain Name.

If the device FQDN is not pushed by the ASA, the client cannot re-establish the VPN session after roaming between networks of different IP protocols.

- MTU—Adjusts the MTU size for SSL connections. Enter a value in bytes, from 256 to 1410 bytes. By default, the MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.
- Keepalive Messages—Enter a number, from 15 to 600 seconds, in the Interval field to enable and adjust the interval of keepalive messages to ensure that an connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle. Adjusting the interval also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.
- Optional Client Modules to Download—To minimize download time, the AnyConnect Client requests downloads (from the ASA) only of modules that it needs for each feature that it supports. You must specify the names of modules that enable other features. The AnyConnect Client, version 4.0, includes the following modules (previous versions have fewer modules):
  - AnyConnect Client DART—The Diagnostic AnyConnect Client Reporting Tool (DART) captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
  - AnyConnect Client Network Access Manager—Formerly called the Cisco Secure Services Client, this module provides 802.1X (Layer 2) and device authentication for access to both wired and wireless network.
  - AnyConnect Client SBL—Start Before Logon (SBL) forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect Client before the Windows login dialog box appears.
  - AnyConnect Client Web Security Module—Formerly called ScanSafe Hostscan, this module is integrated into AnyConnect Client. It deconstructs the elements of a web page so that it can analyze each element simultaneously. It can then allow acceptable content and block malicious or unacceptable content based on a security policy that is defined.
  - AnyConnect Client Telemetry Module—Sends information about the origin of malicious content to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA), which uses this data to provide better URL filtering rules.



Note Telemetry is not supported by AnyConnect 4.0.

  - ASA Posture Module—Formerly called the Cisco Secure Desktop HostScan feature, the posture module is integrated into AnyConnect Client and provides AnyConnect Client the ability to gather credentials for posture assessment prior to creating a remote access connection to the ASA.
  - ISE Posture—Uses the OPSWAT v3 library to perform posture checks to assess an endpoint's compliance. You can then restrict network access until the endpoint is in compliance or can elevate local user privileges.
  - AMP Enabler—Used as medium for deploying Advanced Malware Protection (AMP) for endpoints. It pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base.

- Network Visibility Module—Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics. The NVM collects the endpoint telemetry and logs both the flow data and the file reputation in the syslog and also exports the flow records to a collector (a third-party vendor), which performs the file analysis and provides a UI interface.
- Umbrella Roaming Security Module—Provides DNS-layer security when no VPN is active. It provides a subscription to either Cisco Umbrella Roaming service or OpenDNS Umbrella services, which add Intelligent Proxy and IP-Layer Enforcement features. The Umbrella Security Roaming profile associates each deployment with the corresponding service and automatically enables the corresponding protection level (whether content filtering, multiple policies, robust reporting, active directory integration, or basic DNS-layer security).

- Always-On VPN—Determine if the always-on VPN flag setting in the AnyConnect Client service profile is disabled or if the AnyConnect Client service profile setting should be used. The always-on VPN feature lets AnyConnnect automatically establish a VPN session after the user logs onto a computer. The VPN session remains up until the user logs off the computer. If the physical connection is lost, the session remains up, and AnyConnect Client continually attempts to reestablish the physical connection with the adaptive security appliance to resume the VPN session.

  Always-on VPN permits the enforcement of corporate policies to protect the device from security threats. You can use it to help ensure AnyConnect Client establishes a VPN session whenever the endpoint is not in a trusted network. If enabled, a policy is configured to determine how network connectivity is managed in the absence of a connection.



Note Always-On VPN requires an AnyConnect Client release that supports AnyConnect Secure Mobility features.

- Client Profiles to Download—A profile is a group of configuration parameters that the AnyConnect Client uses to configure VPN, Network Access Manager, Web Security, ISE Posture, AMP Enabler, Network Visibility Module, and Umbrella Roaming Security module settings. Click **Add** to launch the Select AnyConnect Client Profiles window, where you can specify previously created profiles for this group policy.

Internal Group Policy, AnyConnect Client Login Settings

In the Internal Group policy's **Advanced** > AnyConnect Client > **Login Setting** pane, you can enable the ASA to prompt remote users to download the AnyConnect Client, or direct the connection to a Clientless SSL VPN portal page.

- Post Login Setting—Choose to prompt the user and set the timeout to perform the default post login selection.
- Default Post Login Selection—Choose an action to perform after login.

Using Client Firewall to Enable Local Device Support for VPN

In the Internal Group policy's **Advanced** > **AnyConnect Client** > **Client Firewall** pane, you can configure rules to send down to the client system's firewall that affects how public and private networks are handled by the client.

When remote users connect to the ASA, all traffic is tunneled through the VPN connection, so users cannot access resources on their local network. This includes printers, cameras, and Windows Mobile devices (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 as a result of unrestricted access to the local network. You can configure the ASA to deploy endpoint OS firewall rules that 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.



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.

When client firewall rules are configured on the ASA, and the VPN connection is being established on the endpoint,

- The ASA sends the firewall rules information to the client.
- The client would then apply firewall rules as needed.

The following sections describe procedures on how to do this:

- Deploying a Client Firewall for Local Printer Support, on page 29
- Configure Tethered Devices Support for VPN, on page 31

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 Client 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 Client 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.

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:

- The *deny ip any any* private rules is not allowed.
- 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'.
- HostScan (now named Secure Firewall Posture) 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:

Source Port	Destination Port	Traffic Direction Affected
Specific port number	Specific port number	Inbound and outbound
A range or 'All' (value of 0)	A range or 'All' (value of 0)	Inbound and outbound
Specific port number	A range or 'All' (value of 0)	Inbound only
A range or 'All' (value of 0)	Specific port number	Outbound only

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 choose that ACL for Public Network Rule in the Client Firewall pane of a group policy, that list contains the following ACEs:

.

Table 1: ACL Rules in AnyConnect Client_Local_Print

Description	Permission	Interface	Protocol	Source Port	Destination Address	Destination Port
Deny all	Deny	Public	Any	Default	Any	Default
LPD	Allow	Public	TCP	Default	Any	515
IPP	Allow	Public	TCP	Default	Any	631
Printer	Allow	Public	TCP	Default	Any	9100
mDNS	Allow	Public	UDP	Default	224.0.0.251	5353
LLMNR	Allow	Public	UDP	Default	224.0.0.252	5355
NetBios	Allow	Public	TCP	Default	Any	137
NetBios	Allow	Public	UDP	Default	Any	137
Note The default port range is 1 to 65535.						

Note To enable local printing, you must enable the Local LAN Access feature in the client profile with a defined ACL rule allow Any Any.

Configure Local Print Support for VPN

To enable end users to print to their local printer, create a standard ACL in the group policy. The ASA sends that ACL to the VPN client, and the VPN client modify the client's firewall configuration.

Procedure

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**.

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

Step 4 Create an ACL containing the ACEs described above. Add this ACL as a Private 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 (Part 2)** in the profile editor and checking **Apply last local VPN resource rules**.

Configure Tethered Devices Support for VPN

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.



Note For Windows Mobile devices that need to sync with the computer running AnyConnect Client, specify the IPv4 destination address as 169.254.0.0, or the IPv6 destination address fe80::/64 in the ACL.

Procedure

Step 1 In ASDM, go to **Group Policy > Advanced > Split Tunneling**.

Step 2 Uncheck **Inherit** next to the Network List field and click Manage.

Step 3 Click the **Extended ACL** tab.

Step 4 Click **Add > 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**.

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**.

Internal Group Policy, AnyConnect Client Key Regeneration

Rekey Negotiation occurs when the ASA and the client perform a rekey and they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

In the Internal Group policy's **Advanced > AnyConnect Client > Key Regeneration** pane, you configure parameters for rekey:

- Renegotiation Interval—Uncheck the **Unlimited** check box to specify the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).
- Renegotiation Method—Uncheck the Inherit check box to specify a renegotiation method different from the default group policy. Select the **None** radio button to disable rekey, choose either the **SSL** or **New Tunnel** radio button to establish a new tunnel during rekey.

Note Configuring the Renegotiation Method as **SSL** or **New Tunnel** specifies that the client establishes a new tunnel during rekey instead of the SSL renegotiation taking place during the rekey. See the command reference for a history of the **anyconnect ssl rekey** command.

Internal Group Policy, AnyConnect Client, Dead Peer Detection

Dead Peer Detection (DPD) ensures that the ASA (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed. To enable dead peer detection (DPD) and set the frequency with which either the AnyConnect Client or the ASA gateway performs DPD.

Note When the connection is interrupted on the client-side, ASA does not drop the AnyConnect Client sesssion because of DPD or keepalive unconditionally. DPD is only triggered by ASA when some data flow is there from ASA to client. Once DPD is triggered, it makes three retries for each child session (SSL/DTLS) before tearing them down.

If data flow is not there, DPD is not triggered, ASA has a hardcoded 5-minute TCP inactivity timeout that automatically closes SSL/DTLS tunnel connections when no data or keepalive packets flow for exactly 5 minutes, regardless of the configured VPN idle timeout setting. After the child sessions are teared down, **vpn-idle-timeout** command is only responsible for controlling the maximum time for a parent session. For further details on DPD, keepalives, and timeout attributes, see Answer AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer.

Before you begin

- This feature applies to connectivity between the ASA gateway and the AnyConnect Client SSL VPN Client only. It does not work with IPsec since DPD is based on the standards implementation that does not allow padding.
- If you enable DTLS, enable Dead Peer Detection (DPD) also. DPD enables a failed DTLS connection to fallback to TLS. Otherwise, the connection terminates.
- When DPD is enabled on the ASA, you can use the Optimal MTU (OMTU) function to find the largest endpoint MTU at which the client can successfully pass DTLS packets. Implement OMTU by sending a padded DPD packet to the maximum MTU. If a correct echo of the payload is received from the head end, the MTU size is accepted. Otherwise, the MTU is reduced, and the probe is sent again until the minimum MTU allowed for the protocol is reached.

Procedure

Step 1 Go to the desired group policy.

- Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, **Add** or **Edit** the desired group policy, then open the **Advanced** > AnyConnect Client > **Dead Peer Detection** pane.

- Or, to reach a specific users policy, go to **Configuration > Device Management > Users/AAA > User Accounts**, Add or Edit the desired user account, then open the **VPN Policy >** AnyConnect Client **> Dead Peer Detection** pane.

Step 2 Set Gateway Side Detection.

Uncheck the **Disable** check box to specify that DPD is performed by the security appliance (gateway). Enter the interval, from 30 (default) to 3600 seconds, that the security appliance performs DPD. A value of 300 is recommended.

Step 3 Set Client Side Detection.

Uncheck the **Disable** check box to specify that DPD is performed by the client. Then enter the interval, from 30 (default) to 3600 seconds, that the client performs DPD. A value of 30 seconds is recommended.

Internal Group Policy, AnyConnect Client Customization of Clientless Portal

In the Internal Group policy's **Advanced > AnyConnect Client > Customization** pane, you can customize the Clientless Portal log on page for a group policy.

- Portal Customization—Selects the customization to apply to the AnyConnect Client/SSL VPN portal page. You can choose a preconfigured portal customization object, or accept the customization provided in the default group policy. The default is DfltCustomization.
  - Manage—Opens the Configure GUI Customization objects dialog box, in which you can specify that you want to add, edit, delete, import, or export a customization object.
- Homepage URL (optional)—Specifies a homepage URL to display in the Clientless Portal for users associated with the group policy. The string must begin with either http:// or https://. Clientless users are immediately brought to this page after successful authentication. AnyConnect Client launches the default web browser to this URL upon successful establishment of the VPN connection.

Note AnyConnect Client does not currently support this field on the Linux platform, Android mobile devices, and Apple iOS mobile devices. If set, it is ignored by these AnyConnect Clients.

- Use Smart Tunnel for Homepage—Create a smart tunnel to connect to the portal instead of using port forwarding.
- Access Deny Message—To create a message to display to users for whom access is denied, enter it in this field.

Configure AnyConnect Client Custom Attributes in an Internal Group Policy

The Internal Group policy's **Advanced > AnyConnect Client > Custom Attributes pane** lists the custom attributes that are currently assigned to this policy. In this dialog box you can associate previously defined custom attributes to this policy, or define custom attributes and then associate them with this policy.

Custom attributes are sent to and used by the AnyConnect Client to configure features such as Deferred Upgrade. A custom attribute has a type and a named value. The type of the attribute is defined first, then one

or more named values of this type can be defined. For details about the specific custom attributes to configure for a feature, see the *Cisco Secure Client Administrator Guide* for the AnyConnect Client release you are using.

Custom attributes can also be predefined in **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Client Custom Attributes** and **AnyConnect Client Custom Attribute Names**. Predefined custom attributes are used by both Dynamic Access Policies and Group Policies.

Use this procedure to Add or Edit a custom attribute. You can also Delete a configured custom attribute, but custom attributes cannot be edited or deleted if they are also associated with another group policy.

Procedure

Step 1 Go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add/Edit** > **Advanced** > AnyConnect Client > **Custom Attributes**

Step 2 Click **Add** to open the **Create Custom Attribute** pane.

Step 3 Select a predefined **Attribute type** from the drop-down list or configure the attribute type by doing the following:

a) Click **Manage**, in the **Configure Custom Attribute Types** pane, click **Add**.

b) In the **Create Custom Attribute Type** pane, enter the new attribute **Type** and **Description**, both fields are required. For the AnyConnect Client custom attributes options, refer to AnyConnect Client Custom Attributes, on page 93.

c) Click **OK** to close this pane, then Click **OK** again to choose the newly defined custom attribute type.

Step 4 Choose **Select Value**.

Step 5 Select a predefined named value from the **Select value** drop-down list or configure a new named value by doing the following:

a) Click **Manage**, in the Configure Custom Attributes pane, click **Add**.

b) In the **Create Custom Attribute Name** pane, choose the attribute **Type** you previously selected or configured and enter the new attribute **Name** and **Value**, both fields are required.

To add a value, click **Add**, enter the value, and click **OK**. The value cannot exceed 420 characters. If your value exceeds this length, add multiple values for the additional value content. The configured values are concatenated before being sent to the AnyConnect Client.

c) Click **OK** to close this pane, then Click **OK** again to choose the newly defined named value of this attribute.

Step 6 Click **OK** in the **Create Custom Attribute** pane.

IPsec (IKEv1) Client Internal Group Policies

Internal Group Policy, General Attributes for IPsec (IKEv1) Client

The **Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec (IKEv1) Client** Add or Edit Group Policy > IPsec dialog box lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified:

- Re-Authentication on IKE Re-key—Enables or disables reauthentication when IKE re-key occurs, unless the Inherit check box is checked. The user has 30 seconds to enter credentials, and up to three attempts before the SA expires at approximately two minutes and the tunnel terminates.
- Allow entry of authentication credentials until SA expires—Allows users the time to reenter authentication credentials until the maximum lifetime of the configured SA.
- IP Compression—Enables or disables IP Compression, unless the Inherit check box is checked.
- Perfect Forward Secrecy—Enables or disables perfect forward secrecy (PFS), unless the Inherit check box is selected. PFS ensures that the key for a given IPsec SA was not derived from any other secret (like some other keys). In other words, if someone were to break a key, PFS ensures that the attacker would not be able to derive any other key. If PFS were not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPsec protected data, and then use knowledge of the IKE SA secret to compromise the IPsec SAs set up by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPsec. The attacker would have to break each IPsec SA individually.
- Store Password on Client System—Enables or disables storing the password on the client system.



Note Storing the password on a client system can constitute a potential security risk.

- IPsec over UDP—Enables or disables using IPsec over UDP.
- IPsec over UDP Port—Specifies the UDP port to use for IPsec over UDP.
- Tunnel Group Lock—Locks the chosen tunnel group, unless the Inherit check box or the value None is selected.
- IPsec Backup Servers—Activates the Server Configuration and Server IP Addresses fields, so you can specify the UDP backup servers to use if these values are not inherited.
  - Server Configuration—Lists the server configuration options to use as an IPsec backup server. The available options are: Keep Client Configuration (the default), Use the Backup Servers Below, and Clear Client Configuration.
  - Server Addresses (space delimited)—Specifies the IP addresses of the IPsec backup servers. This field is available only when the value of the Server Configuration selection is Use the Backup Servers Below.

About Access Rules for IPsec (IKEv1) Client in an Internal Group Policy

The Client Access Rules table in this dialog box lets you view up to 25 client access rules. Configure the following fields when adding a client access rule:

- Priority—Select a priority for this rule.
- Action—Permit or deny access based on this rule.
- VPN Client Type—Specify the type of VPN client to which this rule applies, software or hardware, and for software clients, all Windows clients or a subset in free-form text.

- VPN Client Version—Specify the version or versions of the VPN client to which this rule applies. This column contains a comma-separated list of software or firmware images appropriate for this client. The entry is free-form text and ***** matches any version.

Client Access Rules Definitions

- If you do not define any rules, the ASA permits all connection types. But users might still inherit any rules that exist in the default group policy.
- When a client matches none of the rules, the ASA denies the connection. If you define a deny rule, you must also define at least one permit rule; otherwise, the ASA denies all connections.
- The * character is a wildcard, which you can enter multiple times in each rule.
- There is a limit of 255 characters for an entire set of rules.
- You can enter **n/a** for clients that do not send client type and/or version.

Internal Group Policy, Client Firewall for IPsec (IKEv1) Client

The Add or Edit Group Policy Client Firewall dialog box lets you configure firewall settings for VPN clients for the group policy being added or modified. Only VPN clients running on Microsoft Windows can use these firewall features. They are currently not available to hardware clients or other (non-Windows) software clients.

Remote users connecting to the ASA with the VPN client can choose the appropriate firewall option.

In the first scenario, a remote user has a personal firewall installed on the PC. The VPN client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN client drops the connection to the ASA. (This firewall enforcement mechanism is called Are You There (AYT), because the VPN client monitors the firewall by sending it periodic “are you there?” messages; if no reply comes, the VPN client knows the firewall is down and terminates its connection to the ASA.) The network administrator might configure these PC firewalls originally, but with this approach, each user can customize his or her own configuration.

In the second scenario, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN client PCs. A common example would be to block Internet traffic to remote PCs in a group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called push policy or Central Protection Policy (CPP). On the ASA, you create a set of traffic management rules to enforce on the VPN client, associate those rules with a filter, and designate that filter as the firewall policy. The ASA pushes this policy down to the VPN client. The VPN client then in turn passes the policy to the local firewall, which enforces it.

Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec (IKEv1) Client > Client Firewall

Fields

- **Inherit**—Determines whether the group policy obtains its client firewall setting from the default group policy. This option is the default setting. When set, it overrides the remaining attributes in this dialog boxing dims their names.
- **Client Firewall Attributes**—Specifies the client firewall attributes, including what type of firewall (if any) is implemented and the firewall policy for that firewall.

- **Firewall Setting**—Lists whether a firewall exists, and if so, whether it is required or optional. If you choose No Firewall (the default), none of the remaining fields in this dialog box are active. If you want users in this group to be firewall-protected, choose either the Firewall Required or Firewall Optional setting.

  If you choose **Firewall Required**, all users in this group must use the designated firewall. The ASA drops any session that attempts to connect without the designated, supported firewall installed and running. In this case, the ASA notifies the VPN client that its firewall configuration does not match.



Note If you require a firewall for a group, make sure the group does not include any clients other than Windows VPN clients. Any other clients in the group (including ASA 5505 in client mode) are unable to connect.

  If you have remote users in this group who do not yet have firewall capacity, choose **Firewall Optional**. The Firewall Optional setting allows all the users in the group to connect. Those who have a firewall can use it; users that connect without a firewall receive a warning message. This setting is useful if you are creating a group in which some users have firewall support and others do not—for example, you may have a group that is in gradual transition, in which some members have set up firewall capacity and others have not yet done so.

- **Firewall Type**—Lists firewalls from several vendors, including Cisco. If you choose Custom Firewall, the fields under Custom Firewall become active. The firewall you designate must correlate with the firewall policies available. The specific firewall you configure determines which firewall policy options are supported.
- **Custom Firewall**—Specifies the vendor ID, Product ID and description for the custom firewall.
  - **Vendor ID**—Specifies the vendor of the custom firewall for this group policy.
  - **Product ID**—Specifies the product or model name of the custom firewall being configured for this group policy.
  - **Description**—(Optional) Describes the custom firewall.
- **Firewall Policy**—Specifies the type and source for the custom firewall policy.
  - **Policy defined by remote firewall (AYT)**—Specifies that the firewall policy is defined by the remote firewall (Are You There). Policy defined by remote firewall (AYT) means that remote users in this group have firewalls located on their PCs. The local firewall enforces the firewall policy on the VPN client. The ASA allows VPN clients in this group to connect only if they have the designated firewall installed and running. If the designated firewall is not running, the connection fails. Once the connection is established, the VPN client polls the firewall every 30 seconds to make sure that it is still running. If the firewall stops running, the VPN client ends the session.
  - **Policy pushed (CPP)**—Specifies that the policy is pushed from the peer. If you choose this option, the Inbound Traffic Policy and Outbound Traffic Policy lists and the Manage button become active. The ASA enforces on the VPN clients in this group the traffic management rules defined by the filter you choose from the Policy Pushed (CPP) drop-down list. The choices available on the menu are filters defined in thisASA, including the default filters. Keep in mind that the ASA pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the ASA. For example, “in” and “out” refer to traffic coming into the VPN client or going outbound from the VPN client. If the VPN client also has a local firewall, the policy pushed from

the ASA works with the policy of the local firewall. Any packet that is blocked by the rules of either firewall is dropped.

- **Inbound Traffic Policy**—Lists the available push policies for inbound traffic.
- **Outbound Traffic Policy**—Lists the available push policies for outbound traffic.
- **Manage**—Displays the ACL Manager dialog box, in which you can configure Access Control Lists (ACLs).

Site-to-Site Internal Group Policies

The Group Policy for Site-to-Site VPN connections specifies tunneling protocols, filters, and connection settings. For each of the fields in 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 of the attributes in this dialog box.

Fields

The following attributes appear in the Add Internal Group Policy > General dialog box. They apply to SSL VPN and IPsec sessions. Thus, several are present for one type of session, but not the other.

- Name—Specifies the name of this group policy. For the Edit function, this field is read-only.
- Tunneling Protocols—Specifies the tunneling protocols that this group allows. Users can use only the selected protocols. The choices are as follows:
  - Clientless SSL VPN—Specifies the use of VPN via SSL/TLS, which uses a web browser to establish a secure remote-access tunnel to a ASA; 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 share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
  - SSL VPN Client—Specifies the use of the Cisco AnyConnect VPN client or the legacy SSL VPN client. If you are using the AnyConnect Client, you must choose this protocol for MUS to be supported.
  - 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—Supported by the Secure Client. AnyConnect Client connections using IPsec with IKEv2 provide advanced features such as software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy.
  - 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 security appliance and private corporate networks. L2TP uses PPP over UDP (port 1701) to tunnel the data. The security appliance must be configured for IPsec transport mode.
- **Filter**—(Network (Client) Access only) Specifies which access control list 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. Note that the VPN filter applies to initial connections only. It does not apply to secondary

connections, such as a SIP media connection, that are opened due to the action of application inspection. To configure filters and rules, see the Group Policy dialog box. Click **Manage** to open the ACL Manager, where you can view and configure ACLs.

- **Idle Timeout**—If the **Inherit** check box is not checked, this parameter sets the idle timeout in minutes.

  If there is no communication activity on the connection in this period, the system terminates the connection. The minimum time is 1 minute, the maximum time is 10080 minutes, and the default is 30 minutes. To allow unlimited connection time, check **Unlimited**.

- **Maximum Connect Time**—If the **Inherit** check box is not checked, this parameter sets the maximum user connection time in minutes.

  At the end of this time, the system terminates the connection. The minimum is 1minute, and the maximum is 35791394 minutes. To allow unlimited connection time, check **Unlimited** (default).

- **Periodic Certificate Authentication Interval**—The interval of time in hours, before certificate authentication is redone periodically.

  If the **Inherit** check box is not checked, you can set the interval for performing periodic certificate verification. The range is between 1 and 168 hours, and the default is disabled. To allow unlimited verification, check Unlimited.

Configure VPN Policy Attributes for a Local User

This procedure describes how to edit an existing user. To add a user choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users** and click **Add**. For more information see the general operations configuration guide.

Before you begin

By default the user account inherits the value of each setting from the default group policy, DfltGrpPolicy. To override each setting, uncheck the **Inherit** check box, and enter a new value.

Procedure

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

Step 2 Select the user you want configure and click **Edit**.

Step 3 In the left-hand 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 set 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 one of the following tunneling protocols:

- The SSL VPN Client lets users connect after downloading the 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—Supported by the AnyConnect Client. AnyConnect Client connections using IPsec with IKEv2 provide advanced features such as software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy.
- 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. Note that the VPN filter applies to initial connections only. It does not apply to secondary connections, such as a SIP media connection, that are opened due to the action of application inspection.

a) To configure filters and rules, choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add/Edit** > **General** > **More Options** > **Filter.**
b) 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 login 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 Configure **Connection Settings**.

a) 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.

b) Specify the number of simultaneous logins by the user. The Simultaneous Logins parameter specifies the maximum number of simultaneous logins allowed for this user. The default value is 3. The minimum value is 0, which disables login and prevents user access.

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

c) Specify the **Maximum Connect Time** for the VPN connection in minutes. At the end of this time, the system terminates the connection.

If the **Inherit** check box is not checked, this parameter specifies the maximum user connection time in minutes. The minimum is 1minute, and the maximum is 35791394 minutes (over 4000 years). To allow unlimited connection time, check **Unlimited** (default).

d) Specify the **Idle Timeout** for the VPN connection in minutes. If there is no communication activity on the connection in this period, the system terminates the connection.

If the **Inherit** check box is not checked, this parameter specifies the idle timeout in minutes.The minimum time is 1 minute, the maximum time is 10080 minutes, and the default is 30 minutes. To allow unlimited connection time, check **Unlimited**.

Step 10 Configure **Timeout Alerts**.

a) Specify the **Maximum Connection Time Alert Interval**.

If you uncheck the **Inherit** check box, the **Default** check box is checked automatically. This sets the max connection alert interval to 30 minutes. If you want to specify a new value, uncheck **Default** and specify a session alert interval from 1 to 30 minutes.

b) Specify the **Idle Alert Interval**.

If you uncheck the **Inherit** check box, the **Default** check box is checked automatically. This sets the idle alert interval to 30 minutes. If you want to specify a new value, uncheck **Default** and specify a session alert interval from 1 to 30 minutes.

Step 11 To set a dedicated IPv4 address for this user, enter an IPv4 address and subnet mask in the **Dedicated IPv4 Address (Optional)** area.

Step 12 To set a dedicated IPv6 address for this user, enter an IPv6 address with an IPv6 prefix in the **Dedicated IPv6 Address (Optional)** area. The IPv6 prefix indicates the subnet on which the IPv6 address resides.

Step 13 Configure specific AnyConnect Client settings, by clicking on these options in the left-hand pane. To override each setting, uncheck the **Inherit** check box, and enter a new value.

Step 14 Click **OK** to apply the changes to the running configuration.

Connection Profiles

Connection Profiles, also known as tunnel-groups, configure connection attributes for VPN connections. These attributes apply to the AnyConnect VPN client, Clientless SSL VPN connections, and to IKEv1and IKEv2 third-party VPN clients.

AnyConnect Client Connection Profile, Main Pane

On the main pane of the AnyConnect Client Connection Profile you can enable client access on the interfaces, and add, edit, and delete connection profiles. You can also specify whether you want to allow a user to choose a particular connection at login.

- Access Interfaces—Lets you choose from a table the interfaces on which to enable access. The fields in this table include the interface name and check boxes specifying whether to allow access.

- In the Interface table, in the row for the interface you are configuring for AnyConnect Client connections, check the protocols you want to enable on the interface. You can allow SSL Access, IPsec access, or both.

  When checking SSL, DTLS (Datagram Transport Layer Security) is enabled by default. DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

  When checking IPsec (IKEv2) access, client services are enabled by default. Client services include enhanced AnyConnect Client features including software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy. If you disable client services, the AnyConnect Client still establishes basic IPsec connections with IKEv2.

- Device Certificate—Lets you specify a certificate for authentication for either an RSA key or an ECDSA key. See Specify a Device Certificate, on page 43.
- Port Setting—Configure port numbers for HTTPS and DTLS (RA client only) connections. See Connection Profiles, Port Settings, on page 43.
- Bypass interface access lists for inbound VPN sessions—Enable inbound VPN sessions to bypass interface ACLs is checked by default. The security appliance allows all VPN traffic to pass through the interface ACLs. For example, even if the outside interface ACL does not permit the decrypted traffic to pass through, the security appliance trusts the remote private network and permits the decrypted packets to pass through. You can change this default behavior. If you want the interface ACL to inspect the VPN protected traffic, uncheck this box.

- Login Page Setting
  - Allow the user to choose a connection profile, identified by its alias, on the login page. If you do not check this check box, the default connection profile is DefaultWebVPNGroup.
  - Shutdown portal login page.—Shows the web page when the login is disabled.

- Connection Profiles—Configure protocol-specific attributes for connections (tunnel groups).
  - Add/Edit—Click to Add or Edit a Connection Profile (tunnel group).
  - Name—The name of the Connection Profile.
  - Aliases—Other names by which the Connection Profile is known.
  - SSL VPN Client Protocol—Specifies whether SSL VPN client have access.
  - Group Policy—Shows the default group policy for this Connection Profile.
  - Allow user to choose connection, identified by alias in the table above, at login page—Check to enable the display of Connection Profile (tunnel group) aliases on the Login page.

- Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.—This option specifies the relative preference of the group URL and certificate values during the connection profile selection process. If the ASA fails to match the preferred value, it chooses the connection profile that matches the other value. Check this option only if you want to rely on the preference used by many older ASA software releases to match the group URL specified by the VPN endpoint to the connection profile that specifies the same group URL. This option is unchecked by default. If it is unchecked, the ASA prefers to match

the certificate field value specified in the connection profile to the field value of the certificate used by the endpoint to assign the connection profile.

Specify a Device Certificate

The **Specify Device Certificate** pane allows you to specify a certificate that identifies the ASA to the client when it attempts to create a connection. This screen is for AnyConnect Client Connection Profiles and Clientless Connection Profiles. Certain AnyConnect Client features, such as Alway-on IPsec/IKEv2, require that a valid and trusted device certificate be available on the ASA.

As of ASA Release 9.4.1, ECDSA certificates can be used for SSL connections (from both AnyConnect Clients and Clientless SSL). Prior to this release, ECDSA certificates were only supported and configured for AnyConnect Client IPsec connections.

Procedure

Step 1 (For VPN connections only) In the **Certificate with RSA Key** area, perform one of these tasks:

- Keep the **Use the same device certificate for SSL and IPsec IKEv2** box checked if you want to choose one certificate to authenticate clients using either protocol. You can choose the certificate from those available in the list box or click **Manage** to create an identity certificate to use.
- Uncheck the **Use the same device certificate for SSL and IPsec IKEv2** check box to specify separate certificates for SSL connections or IPsec connections.

Step 2 Choose a certificate from the **Device Certificate** list box.

If you do not see the certificate you want, click the **Manage** button to manage the identity certificates on the ASA.

Step 3 (For VPN connections only) In the Certificate with ECDSA key field, choose the ECDSA certificate from the list box or click **Manage** to create an ECDSA identity certificate.

Step 4 Click **OK**.

Connection Profiles, Port Settings

Configure port numbers for SSL and DTLS connection (remote access only) connections in the connection profile panes in ASDM:

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Connection Profiles

Fields

- HTTPS Port—The port to enable for HTTPS (browser-based) SSL connections. The range is 1-65535. The default is port 443.
- DTLS Port—The UDP port to enable for DTLS connections. The range is 1-65535. The default is port 443.

AnyConnect Client Connection Profile, Basic Attributes

To set the basic attributes for an AnyConnect VPN module of Cisco Secure Client connection, choose Add or Edit in the AnyConnect Client Connection Profiles section. The Add (or Edit) AnyConnect Client Connection Profile > Basic dialog box opens.

- Name—For Add, specify the name of the connection profile you are adding. For Edit, this field is not editable.
- Aliases—(Optional) Enter one or more alternative names for the connection. You can add spaces or punctuation to separate the names.
- Authentication—Choose one of the following methods to use to authenticate the connection and specify a AAA server group to use in authentication.
  - Method— The authentication protocol has been extended to define a protocol exchange for multiple-certificate authentication and utilize this for both session types. You can validate multiple certificates per session with AnyConnect Client SSL and IKEv2 client protocols. Choose the type of authentication to use: AAA, AAA and certificate, Certificate only, SAML, Multiple certificates and AAA, Multiple certificates, SAML and certificate, or Multiple certificates and SAML. Depending on your selection, you may need to provide a certificate in order to connect.
  - AAA Server Group—Choose a AAA server group from the drop-down list. The default setting is LOCAL, which specifies that the ASA handles the authentication. Before making a selection, you can click **Manage** to open a dialog box over this dialog box to view or make changes to the ASA configuration of AAA server groups.
    - Choosing something other than LOCAL makes available the Use LOCAL if Server Group Fails check box.
    - Use LOCAL if Server Group fails—Check to enable the use of the LOCAL database if the group specified by the Authentication Server Group attribute fails.
- SAML Identity Provider—Choose the SAML IdP server for single sign-on (SSO) authentication.
  - SAML Server—Select the SAML server from the drop-down for AnyConnect Client single sign-on authentication, or click **Manage** to add an SSO server and configure the following parameters:
    - **IDP Entity ID**—The entity ID of the SAML Idp.
    - **Sign In URL**—URL for signing into the IdP. The url value must contain 4 to 500 characters.
    - **Sign Out URL**—(Optional) URL for redirecting to when signing out of the IdP. The url value must contain 4 to 500 characters.
    - **Base URL**—(Optional) URL is provided to third-party IdPs to redirect end-users back to the ASA.

      When base-url is configured, we use it as the base URL of the AssertionConsumerService and SingleLogoutService attribute in **show saml metadata**.

      When base-url is not configured, the URL is determined by the ASA's hostname and domain-name. For example, we use `https://ssl-vpn.cisco.com` when hostname is `ssl-vpn` and domain-name is `cisco.com`.

      An error occurs if neither base-url nor the hostname/domain-name are configured when entering **show saml metadata**.

- **Identity Provider Certificate**—Specifies the trustpoint that contains the IdP certificate for the ASA to verify SAML assertions. Choose a previously configured trustpoint.
- **Service Provider Certificate**—(Optional) Specifies the trustpoint that contains the ASA (SP)'s certificate for the IdP to verify ASA's signature or encrypted SAML assertion. Choose a previously configured trustpoint.
- **Request Signature**—Use the drop-down to choose which signing method you prefer for the SAML IdP server. You can choose rsa-sha1, rsa-sha256, rsa-sha384, or rsa-sha512.
- **Request Timeout**—(Optional) Timeout of the SAML request in seconds. The range is from 1 to 7200.

  If specified, this overrides NotOnOrAfter if the sum of NotBefore and timeout-in-seconds is earlier than NotOnOrAfter.

  If not specified, NotBefore and NotOnOrAfter in the assertion is used to determine the validity.
- **Enable IDP only accessible on internal network**—Check this check box to enable IDP only if it is accessible on the internal network.
- **Request IDP reauthentication at login**—Check this check box to enable IDP reauthentication at login.
- **Clock-skew**—Clock skew which will tolerate the NotBefore and NotOnOrAfter SAML assertions. By default, the clock-skew must be disabled. The default value is 1 second and the range is from 1 to 180 seconds.

- SAML IDP TrustPoint—Choose the SAML IdP TrustPoint for single sign-on (SSO) authentication.
  - IDP TrustPoint—Select the SAML IdP trustpoint that contains the IdP certificate for the ASA to verify SAML assertions.

- SAML Login Experience—Choose the SAML IdP TrustPoint for single sign-on (SSO) authentication.
  - VPN Client Embedded Browser—The VPN client uses its embedded browser for web authentication, so the authentication applies to the VPN connection only.
  - Default OS Browser—The VPN client uses the system’s default browser for web authentication. This option enables single sign-on (SSO) and support for web authentication methods, such as biometric authentication, that cannot be performed in the embedded browser.

    When you choose the default OS browser for SSO authentication, you must configure an external browser package for AnyConnect Client to use the default browser. See AnyConnect Client External Browser SAML Package, on page 76.

- SAML UserName Match—Select to match the certificate username to the SAML username.
- Client Address Assignment—Choose the DHCP servers, client address pools, and client IPv6 address pools to use.
- Client Address Assignment—Choose the DHCP servers, client address pools, and client IPv6 address pools to use.
  - DHCP Servers—Enter the name or IP address of a DHCP server to use.

- Client Address Pools—Enter pool name of an available, configured pool of IPv4 addresses to use for client address assignment. Before making a selection, you can click **Select** to open a dialog box over this dialog box to view or make changes to the address pools. See for more information on adding or editing an IPv4 address pool.
- Client IPv6 Address Pools—Enter the pool name of an available, configured pool of IPv6 addresses to use for client address assignment. Before making a selection, you can click **Select** to open a dialog box over this dialog box to view or make changes to the address pools. See for more information on adding or editing an IPv6 address pool.

•
• Default Group Policy—Select the group policy to use.
  - Group Policy—Select the VPN group policy that you want to assign as the default group policy for this connection. A VPN group policy is a collection of user-oriented attribute-value pairs that can be stored internally on the device or externally on a RADIUS server. The default value is DfltGrpPolicy. You can click **Manage** to open a dialog box over this one to make changes to the group policy configuration.
  - Enable SSL VPN client protocol—Check to enable SSL for this VPN connection.
  - Enable IPsec (IKEv2) client protocol—Check to enable IPsec using IKEv2 for this connection.
  - DNS Servers—Enter the IP address(s) of DNS servers for this policy.
  - WINS Servers—Enter the IP address(s) of WINS servers for this policy.
  - Domain Name—Enter a default domain name.
• Find—Enter a GUI label or a CLI command to use as a search string, then click **Next** or **Previous** to begin the search.

Connection Profile, Advanced Attributes

The Advanced menu items and their dialog boxes configure the following characteristics for this connection:

- General attributes
- Client Addressing attributes
- Authentication attributes
- Authorization attributes
- Accounting attributes
- Name server attributes



Note SSL VPN and secondary authentication attributes apply only to SSL VPN connection profiles.

AnyConnect Client Connection Profile, General Attributes

- Enable Simple Certificate Enrollment (SCEP) for this Connection Profile
- Strip the realm from username before passing it on to the AAA server
- Strip the group from username before passing it on to the AAA server
- Group Delimiter
- Enable Password Management—Lets you configure parameters relevant to notifying users about password expiration.
  - Notify user __ days prior to password expiration—Specifies that ASDM must notify the user at login a specific number of days before the password expires. The default is to notify the user 14 days prior to password expiration and every day thereafter until the user changes the password. The range is 1 through 180 days.
  - Notify user on the day password expires—Notifies the user only on the day that the password expires.

    In either case, and, if the password expires without being changed, the ASA offers the user the opportunity to change the password. If the current password has not expired, the user can still log in using that password.

    This does not change the number of days before the password expires, but rather, it enables the notification. If you choose this option, you must also specify the number of days.
- Translate Assigned IP Address to Public IP Address—In rare situations, you might want to use a VPN peer's real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer's real public IP address if, for example, your inside servers and network security is based on the peer's real IP address. You can enable this feature on one interface per tunnel group.
  - Enable the address translation on interface—Enables the address translation and allows you to choose which interface the address appears on. *Outside* is the interface to which the AnyConnect Client connects, and *inside* is the interface specific to the new tunnel group.



Note Because of routing issues and other limitations, we do not recommend using this feature unless you know you need it.

- Find—Enter a GUI label or a CLI command to use as a search string, then click **Next** or **Previous** to begin the search.

Connection Profile, Client Addressing

The Client Addressing pane on a connection profile assigns IP address pools on specific interfaces for use with this connection profile. The Client Addressing pane is common for all client connection profiles, and is available from the following ASDM paths:

- **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**

- **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles**
- **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv2) Connection Profiles**

The address pools you configure here can also be configured on the Basic pane of the Connection Profile.

The AnyConnect Client Connection Profile can assign IPv6 as well as IPv4 address pools.

To configure client addressing, open a remote access client connection profile (AnyConnect Client, IKEv1 or IKEv2), and select **Advanced** > **Client Addressing**.

- To view or change the configuration of address pools, click **Add** or **Edit** in the dialog box. The Assign Address Pools to Interface dialog box opens. This dialog box lets you assign IP address pools to the interfaces configured on the ASA. Click **Select**. Use this dialog box to view the configuration of address pools. You can change their address pool configuration as follows:
  - To add an address pool to the ASA, click **Add**. The Add IP Pool dialog box opens.
  - To change the configuration of an address pool on the ASA, click **Edit**. The Edit IP Pool dialog box opens if the addresses in the pool are not in use.

    You cannot modify an address pool if it is already in use. If you click **Edit** and the address pool is in use, ASDM displays an error message and lists the connection names and usernames that are using the addresses in the pool.
  - To remove address pool on the ASA, choose that entry in the table and click **Delete**.

    You cannot remove an address pool if it is already in use. If you click **Delete** and the address pool is in use, ASDM displays an error message and lists the connection names that are using the addresses in the pool.
- To assign address pools to an interface, click **Add**. The Assign Address Pools to Interface dialog box opens. Select the interface to be assigned an address pool. Click **Select** next to the Address Pools field. The Select Address Pools dialog box opens. Double-click each unassigned pool you want to assign to the interface or choose each unassigned pool and click **Assign**. The adjacent field displays the list of pool assignments. Click **OK** to populate the Address Pools field with the names of these address pools, then **OK** again to complete the configuration of the assignment.
- To change the address pools assigned to an interface, double-click the interface, or choose the interface and click **Edit**. The Assign Address Pools to Interface dialog box opens. To remove address pools, double-click each pool name and press the **Delete** button on the keyboard. Click **Select** next to the Address Pools field if you want to assign additional fields to the interface. The Select Address Pools dialog box opens. Note that the Assign field displays the address pool names that remained assigned to the interface. Double-click each unassigned pool you want to add to the interface. The Assign field updates the list of pool assignments. Click **OK** to revise the Address Pools field with the names of these address pools, then **OK** again to complete the configuration of the assignment.
- To remove an entry, choose the entry and click **Delete**.

Related Topics

Connection Profile, Client Addressing, Add or Edit, on page 49
Connection Profile, Address Pools, on page 49
Connection Profile, Advanced, Add or Edit IP Pool, on page 49

Connection Profile, Client Addressing, Add or Edit

To assign address pools to Connection Profile, select **Advanced > Client Addressing**, then select **Add** or **Edit**.

- Interface—Select the interface to which you want to assign an address pool. The default is DMZ.
- Address Pools—Specify an address pool to assign to the specified interface.
- Select—Opens the Select Address Pools dialog box, in which you can choose one or more address pools to assign to this interface. Your selection appears in the Address Pools field of the Assign Address Pools to Interface dialog box.

Connection Profile, Address Pools

The Select Address Pools dialog box in Connection Profile > Advanced shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment. You can add, edit, or delete connection profiles from that list.

- Add—Opens the Add IP Pool dialog box, on which you can configure a new IP address pool.
- Edit—Opens the Edit IP Pool dialog box, on which you can modify a selected IP address pool.
- Delete—Removes the selected address pool. There is no confirmation or undo.
- Assign—Displays the address pool names that remained assigned to the interface. Double-click each unassigned pool you want to add to the interface. The Assign field updates the list of pool assignments.

Connection Profile, Advanced, Add or Edit IP Pool

The Add or Edit IP Pool dialog box in Connection Profile > Advanced lets you specify or modify a range of IP addresses for client address assignment.

- Name—Specifies the name assigned to the IP address pool.
- Starting IP Address—Specifies the first IP address in the pool.
- Ending IP Address—Specifies the last IP address in the pool.
- Subnet Mask—Selects the subnet mask to apply to the addresses in the pool.

AnyConnect Client Connection Profile, Authentication Attributes

On the Connection Profile > Advanced >Authentication tab, you can configure the following fields:

- Interface-specific Authentication Server Groups—Manages the assignment of authentication server groups to specific interfaces.
  - Add or Edit—Opens the Assign Authentication Server Group to Interface dialog box, in which you can specify the interface and server group, and specify whether to allow fallback to the LOCAL database if the selected server group fails. The Manage button in this dialog box opens the Configure AAA Server Groups dialog box. Your selections appear in the Interface/Server Group table.
  - Delete—Removes the selected server group from the table. There is no confirmation or undo.

- Username Mapping from Certificate—Lets you specify the methods and fields in a digital certificate from which to extract the username.

Note This feature is not supported in multiple context mode.

- Pre-fill Username from Certificate—Extracts the username from the specified certificate field and uses it for username/password authentication and authorization, according to the options that follow in this panel.
- Hide username from end user—Specifies to not display the extracted username to the end user.
- Use script to choose username—Specify the name of a script to use to choose a username from a digital certificate. The default is --None--.
- Add or Edit—Opens the Add or Edit Script Content dialog box, in which you can define a script to use in mapping the username from the certificate.
- Delete—Deletes the selected script. There is no confirmation or undo.
- Use the entire DN as the username—Specifies that you want to use the entire Distinguished Name field of the certificate as the username.
- Specify the certificate fields to be used as the username—Specifies one or more fields to combine into the username.

  Possible values for primary and secondary attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.

Attribute	Definition
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.

- Primary Field—Selects the first field to use from the certificate for the username. If this value is found, the secondary field is ignored.
- Secondary Field—Selects the field to use if the primary field is not found.

- Certificate Mapping for Multi-Certificate Authentication—Manages the assignment of certificate to be used for primary authentication.
  - First Certificate—Click this option if you want the machine issued certificate to be used for primary authentication.
  - Second Certificate—Click this option if you want the user certificate issued from client to be used for primary authentication.

- Find—Enter a GUI label or a CLI command to use as a search string, then click **Next** or **Previous** to begin the search.

Connection Profile, Secondary Authentication Attributes

Secondary Authentication under Connection Profile > Advanced lets you configure secondary authentication, which is also know as double authentication. When secondary authentication is enabled, the end user must present two sets of valid authentication credentials in order to log on. You can use secondary authentication in conjunction with pre-filling the username from a certificate. The fields in this dialog box are similar to those you configure for primary authentication, but these fields relate only to secondary authentication.

When double authentication is enabled, these attributes choose one or more fields in a certificate to use as the username. Configuring the secondary username from certificate attribute forces the security appliance to use the specified certificate field as the second username for the second username/password authentication.



Note If you also specify the secondary authentication server group, along with the secondary username from certificate, only the primary username is used for authentication.

- Secondary Authorization Server Group—Specifies an authorization server group from which to extract secondary credentials.
  - Server Group—Select an authorization server group to use as the secondary server AAA group. The default is none. The secondary server group cannot be an SDI server group.
  - Manage—Opens the Configure AAA Server Groups dialog box.

- Use LOCAL if Server Group fails—Specifies to fall back to the LOCAL database if the specified server group fails.
- Use primary username—Specifies that the login dialog must request only one username.
- Attributes Server—Select whether this is the primary or secondary attributes server.



Note If you also specify an authorization server for this connection profile, the authorization server settings take precedence—the ASA ignores this secondary authentication server.

- Session Username Server—Select whether this is the primary or secondary session username server.

- Interface-Specific Authorization Server Groups—Manages the assignment of authorization server groups to specific interfaces.
  - Add or Edit—Opens the Assign Authentication Server Group to Interface dialog box, in which you can specify the interface and server group, and specify whether to allow fallback to the LOCAL database if the selected server group fails. The Manage button in this dialog box opens the Configure AAA Server Groups dialog box. Your selections appear in the Interface/Server Group table.
  - Delete—Removes the selected server group from the table. There is no confirmation or undo.
- Username Mapping from Certificate—Specify the fields in a digital certificate from which to extract the username.
- Pre-fill Username from Certificate—Check to extract the names to be used for secondary authentication from the primary and secondary fields specified in this panel. You must configure the authentication method for both AAA and certificates before checking this attribute. To do so, return to the Basic panel in the same window and check **Both** next to Method.
- Hide username from end user—Check to hide the username to be used for secondary authentication from the VPN user.
- Fallback when a certificate is unavailable —This attribute is configurable only if "Hide username from end user" is checked. Uses HostScan (now called Secure Firewall Posture) data to pre-fill the username for secondary authentication if a certificate is unavailable.
- Password—Choose one of the following methods to retrieve the password to be used for secondary authentication:
  - Prompt—Prompt the user for the password.
  - Use Primary—Reuse the primary authentication password for all secondary authentications.
  - Use—Enter a common secondary password for all secondary authentications.
- Specify the certificate fields to be used as the username—Specifies one or more fields to match as the username. To use this username in the pre-fill username from certificate feature for the secondary username/password authentication or authorization, you must also configure the pre-fill-username and secondary-pre-fill-username.
  - Primary Field—Selects the first field to use from the certificate for the username. If this value is found, the secondary field is ignored.

- Secondary Field—Selects the field to use if the primary field is not found.

The options for primary and secondary field attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.

- Use the entire DN as the username—Uses the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.
- Use script to select username—Names the script from which to extract a username from a digital certificate. The default is --None--.
  - Add or Edit—Opens the Add or Edit Script Content dialog box, in which you can define a script to use in mapping the username from the certificate.
  - Delete—Deletes the selected script. There is no confirmation or undo.
- Certificate Mapping for Multi-Certificate Authentication—Manages the assignment of certificate to be used for secondary authentication.

- First Certificate—Click this option if you want the machine issued certificate to be used for secondary authentication.
- Second Certificate—Click this option if you want the user certificate issued from client to be used for secondary authentication.

AnyConnect Client Connection Profile, Authorization Attributes

The Authorization dialog box in an AnyConnect Client Connection profile lets you view, add, edit, or delete interface-specific authorization server groups. Each row of the table in this dialog box shows the status of one interface-specific server group: the interface name, its associated server group, and whether fallback to the local database is enabled if the selected server group fails.

The fields in this pane are identical for AnyConnect Client, IKEv1, IKEv2 and Clientless SSL connection profiles.

- Authorization Server Group—Specifies an authorization server group from which to draw authorization parameters.
  - Server Group—Selects an authorization server group to use. The default is none.
  - Manage—Opens the Configure AAA Server Groups dialog box.
  - Users must exist in the authorization database to connect—Select this check box to require that users meet this criterion.
- Interface-specific Authorization Server Groups—Manages the assignment of authorization server groups to specific interfaces.
  - Add or Edit—Opens the Assign Authentication Server Group to Interface dialog box, in which you can specify the interface and server group, and specify whether to allow fallback to the LOCAL database if the selected server group fails. The Manage button in this dialog box opens the Configure AAA Server Groups dialog box. Your selections appear in the Interface/Server Group table.
  - Delete—Removes the selected server group from the table. There is no confirmation or undo.
- Username Mapping from Certificate—Specify the fields in a digital certificate from which to extract the username.
  - Use script to select username—Specifies the name of a script to use to choose a username from a digital certificate. The default is --None--. For more information about creating scripts to select create a username from certificate fields, see
  - Add or Edit—Opens the Add or Edit Script Content dialog box, in which you can define a script to use in mapping the username from the certificate.
  - Delete—Deletes the selected script. There is no confirmation or undo.
  - Use the entire DN as the username—Specifies that you want to use the entire Distinguished Name field of the certificate as the username.
  - Specify the certificate fields to be used as the username—Specifies one or more fields to combine into the username.

- Primary Field—Selects the first field to use in the certificate for the username. If this value is found, the secondary field is ignored.
- Secondary Field—Selects the field to use if the primary field is not found.

- Find—Enter a GUI label or a CLI command to use as a search string, then click Next or Previous to begin the search.

AnyConnect Client Connection Profile, Authorization, Add Script Content to Select Username

If you select **use a script to select username** in the Authorization pane of the AnyConnect Client, and you click the Add or Edit button, you will see the following fields.

Scripts can use certificate fields for authorization that are not listed in the other mapping options.



Note Both AnyConnect Client and clientless WebVPN display "Unknown" in the username field when pre-fill-username from certificate using a script cannot find the username in the client certificate.

- Script Name—Specify the name of the script. The script name must be the same in both authorization and authentication.You define the script here, and CLI uses the same script to perform this function.
- Select script parameters—Specify the attributes and content of the script.
- Value for Username—Select an attribute from the drop-down list of standard DN attributes to use as the username (Subject DN).
- No Filtering—Specify that you want to use the entire specified DN name.
- Filter by substring— Specify the Starting Index (the position in the string of the first character to match) and Ending Index (number of characters to search). If you choose this option, the starting index cannot be blank. If you leave the ending index blank, it defaults to -1, indicating that the entire string is searched for a match.

  For example, suppose you selected the DN attribute Common Name (CN), which contains a value of host/user. The following table shows some possible ways you might filter this value using the substring option to achieve various return values. The Return Value is what is actually pre-filled as the username.

Table 2: Filtering by Substring

Starting Index	Ending Index	Return Value
1	5	host/
6	10	user
6	-1	user

Using a negative index, as in the third row of this table, specifies to count from the end of the string backwards to the end of the substring, in this case, the "r" of "user."

When using filtering by substrings, you should know the length of the substring that you are seeking. From the following examples, use either the regular expression matching or the custom script in Lua format:

- Example 1: Regular Expression Matching—Enter a regular expression to apply to the search in the Regular Expression field. Standard regular expression operators apply. For example, suppose you want to use a regular expression to filter everything up to the @ symbol of the "Email Address (EA)" DN value. The regular expression ^[^@]* would be one way to do this. In this example, if the DN value contained a value of user1234@example.com, the return value after the regular expression would be user1234.
- Example 2: Use custom script in LUA format—Specify a custom script written in the LUA programming language to parse the search fields. Selecting this option makes available a field in which you can enter your custom LUA script; for example, the script:

```
return cert.subject.cn..'/'..cert.subject.l
```

combines two DN fields, username (cn) and locality (l), to use as a single username and inserts the slash (/) character between the two fields.

The table below lists the attribute names and descriptions that you can use in a LUA script.

Note LUA is case-sensitive.

Table 3: Attribute Names and Descriptions

Attribute Name	Description
cert.subject.c	Country
cert.subject.cn	Common Name
cert.subject.dnq	DN qualifier
cert.subject.ea	E-mail Address
cert.subject.genq	Generational qualified
cert.subject.gn	Given Name
cert.subject.i	Initials
cert.subject.l	Locality
cert.subject.n	Name
cert.subject.o	Organization
cert.subject.ou	Organization Unit
cert.subject.ser	Subject Serial Number
cert.subject.sn	Surname
cert.subject.sp	State/Province
cert.subject.t	Title

cert.subject.uid	User ID
cert.issuer.c	Country
cert.issuer.cn	Common Name
cert.issuer.dnq	DN qualifier
cert.issuer.ea	E-mail Address
cert.issuer.genq	Generational qualified
cert.issuer.gn	Given Name
cert.issuer.i	Initials
cert.issuer.l	Locality
cert.issuer.n	Name
cert.issuer.o	Organization
cert.issuer.ou	Organization Unit
cert.issuer.ser	Issuer Serial Number
cert.issuer.sn	Surname
cert.issuer.sp	State/Province
cert.issuer.t	Title
cert.issuer.uid	User ID
cert.serialnumber	Certificate Serial Number
cert.subjectaltname.upn	User Principal Name

If an error occurs while activating a tunnel group script, causing the script not to activate, the administrator's console displays an error message.

Connection Profiles, Accounting

The Accounting pane in Connection Profile > Advanced sets accounting options globally across the ASA.

- Accounting Server Group—Choose the previously-defined server group to use for accounting.
- Manage—Opens the Configure AAA Server Groups dialog box, where you can create an AAA server group.

Connection Profile, Group Alias and Group URL

The GroupAlias/Group URL dialog box in Connection Profile > Advanced configures attributes that affect what the remote user sees upon login.

The name of the tab in the connection profile is Group URL/Group Alias for AnyConnect Client.

- **Login and Logout (Portal) Page Customization** (Clientless SSL VPN only)—Configures the look and feel of the user login page by specifying which preconfigured customization attributes to apply. The default is DfltCustomization. Click **Manage** to create a new customization object.
- **Enable the display of Radius Reject-Message on the login screen**—Select this check box to display the RADIUS-reject message on the login dialog box when authentication is rejected.
- **Enable the display of SecurId message on the login screen**—Select this check box to display SecurID messages on the login dialog box.
- **Connection Aliases**—The connection aliases and their status. A connection alias appears on the user login page if the connection is configured to allow users to choose a particular connection (tunnel group) at login. Click the buttons to **Add** or **Delete** aliases. To edit an alias, double-click the alias in the table and edit the entry. To change the enabled status, select or deselect the checkbox in the table.
- **Group URLs**—The group URLs and their status. A group URL appears on the user login page if the connection is configured to allow users to choose a particular group at login. Click the buttons to **Add** or **Delete** URLs. To **Edit** a URL, double-click the URL in the table and edit the entry. To change the enabled status, select or deselect the checkbox in the table.

IKEv1 Connection Profiles

IKEv1 connection profiles define authentication policies for native and third-party VPN clients, including L2TP-IPsec. IKEv1 connection profiles are configured on the **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles** pane.

- **Access Interfaces**—Selects the interfaces to enable for IPsec access. The default is no access.
- **Connection Profiles**—Shows in tabular format the configured parameters for existing IPsec connections. The Connections table contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters. The table contains the following columns:
  - **Name**—Specifies the name or IP address of the IPsec IKEv1 connection.
  - **IPsec Enabled**—Indicates whether the IPsec protocol is enabled. You enable this protocol on the Add or Edit IPsec Remote Access Connection, Basic dialog box.
  - **L2TP/IPsec Enabled**—Indicates whether the L2TP/IPsec protocol is enabled. You enable this protocol on the Add or Edit IPsec Remote Access Connection, Basic dialog box.
  - **Authentication Server Group**—Name of the group of servers that can provide authentication.
  - **Group Policy**—Indicates the name of the group policy for this IPsec connection.

Note Delete removes the selected server group from the table. There is no confirmation or undo.

IPsec Remote Access Connection Profile, Basic Tab

The Add or Edit IPsec Remote Access Connection Profile Basic dialog box on **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Basic** lets you configure common attributes for IPsec IKEv1 VPN connections, including L2TP-IPsec.

- **Name**—Name of this connection profile.
- **IKE Peer Authentication**—Configures IKE peers.
  - **Pre-shared key**—Specifies the value of the pre-shared key for the connection. The maximum length of a pre-shared key is 128 characters.
  - **Identity Certificate**—Selects the name of an identity certificate, if any identity certificates are configured and enrolled. **Manage** opens the **Manage Identity Certificates** dialog box, on which you can add, edit, delete, export, and show details for a selected certificate.
- **User Authentication**—Specifies information about the servers used for user authentication. You can configure more authentication information in the Advanced section.
  - **Server Group**—Selects the server group to use for user authentication. The default is LOCAL. If you select something other than LOCAL, the Fallback check box becomes available. To add a server group, click the **Manage** button.
  - **Fallback**—Specifies whether to use LOCAL for user authentication if the specified server group fails.
- **Client Address Assignment**—Specifies attributes relevant to assigning client attributes.
  - **DHCP Servers**—Specifies the IP address of a DHCP server to use. You can add up to 10 servers, separated by spaces.
  - **Client Address Pools**—Specifies up to 6 predefined address pools. To define an address pool, click the **Select** button.
- **Default Group Policy**—Specifies attributes relevant to the default group policy.
  - **Group Policy**—Selects the default group policy to use for this connection. The default is DfltGrpPolicy. To define a new group policy to associate with this group policy, click **Manage**.
  - **Enable IPsec protocol** and **Enable L2TP over IPsec protocol**—Selects the protocol or protocols to use for this connection.

Add/Edit Remote Access Connections, Advanced, General

Use this dialog box to specify whether to strip the realm and group from the username before passing them to the AAA server, and to specify password management parameters.

- **Strip the realm from username before passing it on to the AAA server**—Enables or disables stripping the realm (administrative domain) from the username before passing the username on to the AAA server. Check the Strip Realm check box to remove the realm qualifier of the username during authentication. You can append the realm name to the username for AAA: authorization, authentication and accounting. The only valid delimiter for a realm is the @ character. The format is username@realm, for example, JaneDoe@example.com. If you check this Strip Realm check box, authentication is based on the username alone. Otherwise, authentication is based on the full username@realm string. You must check this box if your server is unable to parse delimiters.



Note You can append both the realm and the group to a username, in which case the ASA uses parameters configured for the group and for the realm for AAA functions. The format for this option is username[@realm]]<#or!>group], for example, JaneDoe@example.com#VPNGroup. If you choose this option, you must use either the # or ! character for the group delimiter because the ASA cannot interpret the @ as a group delimiter if it is also present as the realm delimiter.

The ASA does not include support for the user@grouppolicy. Only the L2TP/IPsec client supports the tunnel switching via user@tunnelgroup.

- **Strip the group from the username before passing it on to the AAA server**—Enables or disables stripping the group name from the username before passing the username on to the AAA server. Check Strip Group to remove the group name from the username during authentication. This option is meaningful only when you have also checked the Enable Group Lookup box. When you append a group name to a username using a delimiter, and enable Group Lookup, the ASA interprets all characters to the left of the delimiter as the username, and those to the right as the group name. Valid group delimiters are the @, #, and ! characters, with the @ character as the default for Group Lookup. You append the group to the username in the format username<delimiter>group, the possibilities being, for example, JaneDoe@VPNGroup, JaneDoe#VPNGroup, and JaneDoe!VPNGroup.
- **Password Management**—Lets you configure parameters relevant to overriding an account-disabled indication from a AAA server and to notifying users about password expiration.
  - **Enable notification upon password expiration to allow user to change password**—Checking this check box makes the following two parameters available. You can choose either to notify the user at login a specific number of days before the password expires or to notify the user only on the day that the password expires. The default is to notify the user 14 days prior to password expiration and every day thereafter until the user changes the password. The range is 1 through 180 days.



Note This does not change the number of days before the password expires, but rather, it enables the notification. If you choose this option, you must also specify the number of days.

In either case, and, if the password expires without being changed, the ASA offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password.

This parameter is valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The ASA ignores this command if RADIUS or LDAP authentication has not been configured.

This feature requires the use of MS-CHAPv2.

IKEv1 Client Addressing

Client Addressing configuration is common for client Connection Profiles. See Connection Profile, Client Addressing, on page 47 for more information.

IKEv1 Connection Profile, Authentication

This dialog box is available for IPsec on Remote Access and Site-to-Site tunnel groups. The settings in this dialog box apply to this connection profile (tunnel group) globally across the ASA. To set authentication server group settings per interface, click **Advanced**. This dialog box lets you configure the following attributes:

- **Authentication Server Group**—Lists the available authentication server groups, including the LOCAL group (the default). You can also choose None. Selecting something other than None or Local makes available the Use LOCAL if Server Group Fails check box.
- **Use LOCAL if Server Group fails**—Enables or disables fallback to the LOCAL database if the group specified by the Authentication Server Group attribute fails.

  You can configure authentication on the basis of username alone by unchecking the Enable Group Lookup box. Checking both the Enable Group Lookup box and Strip Group lets you maintain a database of users with group names appended on your AAA server, and at the same time authenticate users on the basis of their username alone.

IKEv1 Connection Profile, Authorization

Configuring Authorization is common for client Connection Profiles. See AnyConnect Client Connection Profile, Authentication Attributes, on page 49 for more information.

IKEv1 Connection Profile, Accounting

Configuring Accounting is common for client Connection Profiles. See Connection Profiles, Accounting, on page 57 for more information.

IKEv1 Connection Profile, IPsec

Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Advanced > IPsec

- **Send certificate chain**—Enables or disables sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
- **IKE Peer ID Validation**—Selects whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate.

- **IKE Keep Alive**—Enables and configures ISAKMP keep alive monitoring.
  - **Disable Keep Alives**—Enables or disables ISAKMP keep alives.
  - **Monitor Keep Alives**—Enables or disables ISAKMP keep alive monitoring. Selecting this option makes available the Confidence Interval and Retry Interval fields.
  - **Confidence Interval**—Specifies the ISAKMP keep alive confidence interval. This is the number of seconds the ASA should allow a peer to idle before beginning keepalive monitoring. The minimum is 10 seconds; the maximum is 300 seconds. The default for a remote access group is 300 seconds.
  - **Retry Interval**—Specifies number of seconds to wait between ISAKMP keep alive retries. The default is 2 seconds.
  - **Head end will never initiate keepalive monitoring**—Specifies that the central-site ASA never initiates keepalive monitoring.

IKEv1 Connection Profile, IPsec, IKE Authentication

Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Advanced > IPsec > IKE Authentication

- **Default Mode**—Lets you choose the default authentication mode, none, xauth, or hybrid, as above.
- **Interface-Specific Mode**—Specifies the authentication mode on a per-interface basis.
  - **Add/Edit/Delete**—Add/Edit/Delete move an interface/authentication mode pair selection from the Interface/Authentication Modes table.
  - **Interface**—Select a named interface. The default interfaces are inside and outside, but if you have configured a different interface name, that name also appears in the list.
  - **Authentication Mode**—Lets you choose the authentication mode, none, xauth, or hybrid, as above.

IKEv1 Connection Profile, IPsec, Client Software Update

Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Advanced > IPsec > Client Software Update

Client VPN Software Update Table—Lists the client type, VPN Client revisions, and image URL for each client VPN software package installed. For each client type, you can specify the acceptable client software revisions and the URL or IP address from which to download software upgrades, if necessary. The client update mechanism (described in detail under the Client Update dialog box) uses this information to determine whether the software each VPN client is running is at an appropriate revision level and, if appropriate, to provide a notification message and an update mechanism to clients that are running outdated software.

- **Client Type**—Identifies the VPN client type.
- **VPN Client Revisions**—Specifies the acceptable revision level of the VPN client.
- **Location URL**—Specifies the URL or IP address from which the correct VPN client software image can be downloaded. For dialog boxes-based VPN clients, the URL must be of the form http:// or https://. For ASA 5505 in client mode, the URL must be of the form tftp://.

IKEv1 Connection Profile, PPP

To configure the authentication protocols permitted for a PPP connection using this IKEv1 Connection Profile, open **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Advanced > PPP**.

This dialog box applies *only* to IPsec IKEv1 remote access connection profiles.

- **CHAP**—Enables the use of the CHAP protocol for a PPP connection.
- **MS-CHAP-V1**—Enables the use of the MS-CHAP-V1 protocol for a PPP connection.
- **MS-CHAP-V2**—Enables the use of the MS-CHAP-V2 protocol for a PPP connection.
- **PAP**—Enables the use of the PAP protocol for a PPP connection.
- **EAP-PROXY**—Enables the use of the EAP-PROXY protocol for a PPP connection. EAP refers to the Extensible Authentication protocol.

IKEv2 Connection Profiles

IKEv2 connection profiles define EAP, Certificate-based, and pre-shared key-based authentication for AnyConnect VPN module of Cisco Secure Clients. The configuration panel in ASDM is **Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) Connection Profiles**.

- Access Interfaces—Selects the interfaces to enable for IPsec access. The default is that no access is selected.
- Bypass interface access lists for inbound VPN sessions—Check this check box to bypass interface access lists for inbound VPN sessions. Access lists for group policy and user policy always apply to all traffic.
- Connection Profiles—Shows in tabular format the configured parameters for existing IPsec connections. The Connection Profiles table contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters. The table contains the following columns:
  - Name—Specifies the name or IP address of the IPsec connection.
  - IKEv2 Enabled—Specifies that the IKEv2 protocol is enabled if checked.
  - Authentication Server Group—Specifies the name of the server group used for authentication.
  - Group Policy—Indicates the name of the group policy for this IPsec connection.



Note Delete removes the selected server group from the table. There is no confirmation or undo.

IPsec IKEv2 Connection Profile, Basic Tab

The Add or Edit IPsec Remote Access Connection Profile Basic dialog box configures common attributes for IPsec IKEv2 connections.

- **Name**—Identifies the name of the connection.
- **IKE Peer Authentication**—Configures IKE peers.
  - **Pre-shared key**—Specifies the value of the pre-shared key for the connection. The maximum length of a pre-shared key is 128 characters.
  - **Enable Certificate Authentication**—Allows you to use certificates for authentication if checked.
  - **Enable peer authentication using EAP**—Allows you to use EAP for authentication if checked. You must use certificates for local authentication if you check this check box.
  - **Send an EAP identity request to the client**—Enables you to send an EAP request for authentication to the remote access VPN client.
- Post Quantum Key—Check this check box to specify the post quantum pre-shared key (PPK). PPK is a 256-bit 64 character hexadecimal string and protects the session from quantum computer attacks.
  - Post Quantum Key Identity—Specify the ID of the PPK.
- **Mobike RRC**—Enable/disable mobike RRC.
  - **Enable Return Routability Check for mobike**—Enable/disable Return Routability checking for dynamic IP address changes in IKE/IPSEC security associations on which mobike is enabled.
- **User Authentication**—Specifies information about the servers used for user authentication. You can configure more authentication information in the Advanced section.
  - **Server Group**—Selects the server group to use for user authentication. the default is LOCAL. If you choose something other than LOCAL, the Fallback check box becomes available.
  - **Manage**—Opens the Configure AAA Server Groups dialog box.
  - **Fallback**—Specifies whether to use LOCAL for user authentication if the specified server group fails.
- **Client Address Assignment**—Specifies attributes relevant to assigning client attributes.
  - **DHCP Servers**—Specifies the IP address of a DHCP server to use. You can add up to 10 servers, separated by spaces.
  - **Client Address Pools**—Specifies up to 6 predefined address pools. Click Select to open the Address Pools dialog box.
- **Default Group Policy**—Specifies attributes relevant to the default group policy.
  - **Group Policy**—Selects the default group policy to use for this connection. The default is DfltGrpPolicy.
  - **Manage**—Opens the Configure Group Policies dialog box, from which you can add, edit, or delete group policies.

- **Client Protocols**—Selects the protocol or protocols to use for this connection. By default, both IPsec and L2TP over IPsec are selected.
- **Enable IKEv2 Protocol**—Enables the IKEv2 protocol for use in remote access connection profiles. This is an attribute of the group policy that you just selected.

IPsec Remote Access Connection Profile, Advanced, IPsec Tab

The IPsec table on IPsec (IKEv2) Connection Profiles has the following fields.

- Send certificate chain—Check to enable or disable sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
- IKE Peer ID Validation—Choose from the drop-down list whether IKE peer ID validation is not checked, required, or checked if it is supported by a certificate.

Mapping Certificates to IPsec or SSL VPN Connection Profiles

When the ASA receives an IPsec connection request with client certificate authentication, it assigns a connection profile to the connection according to policies you configure. That policy can be to use rules you configure, use the certificate OU field, use the IKE identity (i.e. hostname, IP address, key ID), the peer IP address, or a default connection profile. For SSL connections, the ASA only uses the rules you configure.

For IPsec or SSL connections using rules, the ASA evaluates the attributes of the certificate against the rules until it finds a match. When it finds a match, it assigns the connection profile associated with the matched rule to the connection. If it fails to find a match, it assigns the default connection profile (DefaultRAGroup for IPsec and DefaultWEBVPNGroup for SSL VPN) to the connection and lets the user choose the connection profile from a drop-down list displayed on the portal page (if it is enabled). The outcome of the connection attempt once in this connection profile depends on whether or not the certificate is valid and the authentication settings of the connection profile.

A certificate group matching policy defines the method to use for identifying the permission groups of certificate users.

Configure the matching policy on the Policy pane. If you choose to use rules for matching, go to Rules pane to specify the rules.

Certificate to Connection Profile Maps, Policy

For IPsec connections, a certificate group matching policy defines the method to use for identifying the permission groups of certificate users. The settings for thse policies are configured on **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Policy**

- **Use the configured rules to match a certificate to a group**—Lets you use the rules you have defined under Rules.
- **Use the certificate OU field to determine the group**—Lets you use the organizational unit field to determine the group to which to match the certificate. This is selected by default.

- **Use the IKE identity to determine the group**—Lets you use the identity you previously defined under **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters**. The IKE identity can be hostname, IP address, key ID, or automatic.
- **Use the peer IP address to determine the group**—Lets you use the peer's IP address. This is selected by default.
- **Default to Connection Profile**—Lets you choose a default group for certificate users that is used when none of the preceding methods resulted in a match. This is selected by default. Click the default group in the Default to group list. The group must already exist in the configuration. If the group does not appear in the list, you must define it by using **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Certificate to Connection Profile Maps Rules

For IPsec connections, a certificate group matching policy defines the method to use for identifying the permission groups of certificate users. Profile maps are created on **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules**.

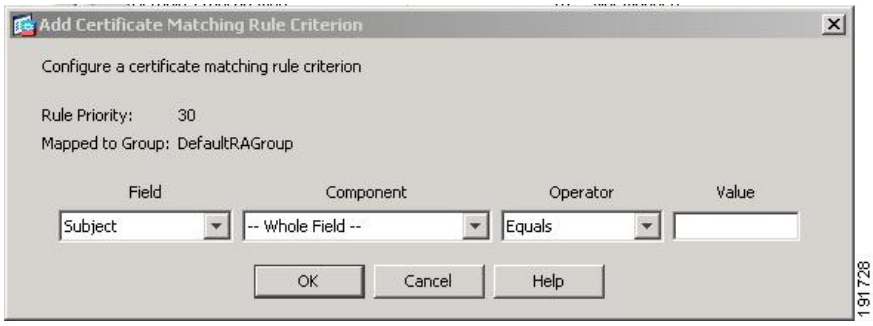
This pane has a list of certificate to connection profile maps, and mapping criteria.

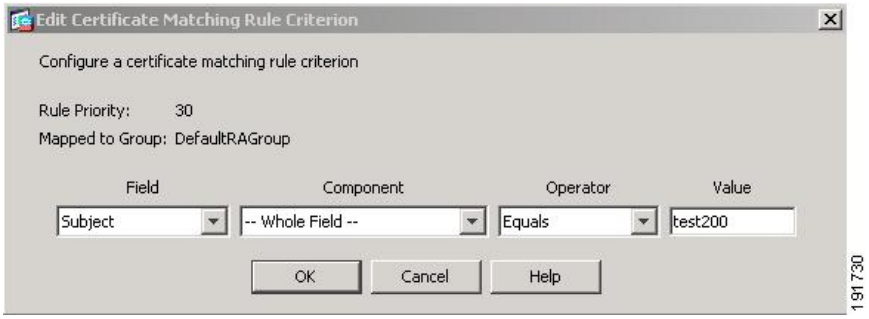
Certificate to Connection Profile Maps, add Certificate Matching Rule Criterion

Create map profiles to map connection profiles to mapping rules.

- Map—Choose one of the following:
  - Existing—Select the name of the map to include the rule.
  - New—Enter a new map name for a rule.
- Priority—Type a decimal to specify the sequence with which the ASA evaluates the map when it receives a connection request. For the first rule defined, the default priority is 10. The ASA evaluates each connection against the map with the lowest priority number first.
- Mapped to Connection Profile—Select the connection profile, formerly called a “tunnel group,” to map to this rule.

If you do not assign a rule criterion to the map, as described in the next section, the ASA ignores the map entry.





Add/Edit Certificate Matching Rule Criterion

Use this dialog box to configure a certificate matching rule criterion which you can map to a connection profile.

- Rule Priority—(Display only). Sequence with which the ASA evaluates the map when it receives a connection request. The ASA evaluates each connection against the map with the lowest priority number first.
- Mapped to Group—(Display only). Connection profile to which the rule is assigned.
- Field—Select the part of the certificate to be evaluated from the drop-down list.
  - Subject—The person or system that uses the certificate. For a CA root certificate, the Subject and Issuer are the same.
  - Alternative Subject—The subject alternative names extension allows additional identities to be bound to the subject of the certificate.
  - Issuer—The CA or other entity (jurisdiction) that issued the certificate.
  - Extended Key Usage—An extension of the client certificate that provides further criteria that you can choose to match.
- Component—(Applies only if Subject of Issuer is selected.) Select the distinguished name component used in the rule:

DN Field	Definition
Whole Field	The entire DN.
Country (C)	The two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
Common Name (CN)	The name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.
DN Qualifier (DNQ)	A specific DN attribute.
E-mail Address (EA)	The e-mail address of the person, system or entity that owns the certificate.
Generational Qualifier (GENQ)	A generational qualifier such as Jr., Sr., or III.
Given Name (GN)	The first name of the certificate owner.

DN Field	Definition
Initials (I)	The first letters of each part of the certificate owner's name.
Locality (L)	The city or town where the organization is located.
Name (N)	The name of the certificate owner.
Organization (O)	The name of the company, institution, agency, association, or other entity.
Organizational Unit (OU)	The subgroup within the organization.
Serial Number (SER)	The serial number of the certificate.
Surname (SN)	The family name or last name of the certificate owner.
State/Province (S/P)	The state or province where the organization is located.
Title (T)	The title of the certificate owner, such as Dr.
User ID (UID)	The identification number of the certificate owner.
Unstructured Name (UNAME)	The unstructuredName attribute type specifies the name or names of a subject as an unstructured ASCII string.
IP Address (IP)	IP address field.

- Operator—Select the operator used in the rule:
  - Equals—The distinguished name field must exactly match the value.
  - Contains—The distinguished name field must include the value within it.
  - Does Not Equal—The distinguished name field must not match the value
  - Does Not Contain—The distinguished name field must not include the value within it.
- Value—Enter up to 255 characters to specify the object of the operator. For Extended Key Usage, choose one of the pre-defined values in the drop-down list, or you can enter OIDs for other extensions. The pre-defined values include the following:

Selection	Key Usage Purpose	OID String
clientauth	**Client Authentication**	**1.3.6.1.5.5.7.3.2**
codesigning	Code Signing	1.3.6.1.5.5.7.3.3
emailprotection	Secure Email Protection	1.3.6.1.5.5.7.3.4
ocspsigning	OCSP Signing	1.3.6.1.5.5.7.3.9
serverauth	Server Authentication	1.3.6.1.5.5.7.3.1
timestamping	Time Stamping	1.3.6.1.5.5.7.3.8

Site-to-Site Connection Profiles

The Connection Profiles dialog box shows the attributes of the currently configured Site-to-Site connection profiles (tunnel groups), it also lets you choose the delimiter to use when parsing connection profile names, and lets you add, modify, or delete connection profiles.

The ASA supports IPsec LAN-to-LAN VPN connections for IPv4 or IPv6 using IKEv1 or IKEv2 and supports both inside and outside networks using the inner and outer IP headers.

Fields on the Site to Site Connection Profile Pane

- Access Interfaces—Displays a table of device interfaces where you can enable access by a remote peer device on the interface:
  - Interface—The device interface to enable or disable access.
  - Allow IKEv1 Access—Check to enable IPsec IKEv1 access by a peer device.
  - Allow IKEv2 Access—Check to enable IPsec IKEv2 access by a peer device.
- Connection Profiles—Displays a table of connection profiles where you can add, edit, or delete profiles:
  - Add—Opens the Add IPsec Site-to-Site connection profile dialog box.
  - Edit—Opens the Edit IPsec Site-to-Site connection profile dialog box.
  - Delete—Removes the selected connection profile. There is no confirmation or undo.
  - Name—The name of the connection profile.
  - Interface—The interface the connection profile is enabled on.
  - Local Network—Specifies the IP address of the local network.
  - Remote Network—Specifies the IP address of the remote network.
  - IKEv1 Enabled—Shows IKEv1 enabled for the connection profile.
  - IKEv2 Enabled—Shows IKEv2 enabled for the connection profile.
  - Group Policy—Shows the default group policy of the connection profile.

Add or Edit Site-to-Site Connection Profile

The Add or Edit IPsec Site-to-Site Connection dialog box lets you create or modify an IPsec Site-to-Site connection. These dialog boxes let you specify the peer IP address (IPv4 or IPv6), specify a connection name, choose an interface, specify IKEv1 and IKEv2 peer and user authentication parameters, specify protected networks, and specify encryption algorithms.



Note When you create a Site-to-Site VPN connection profile, open the connection profile and then cancel it without making any configuration changes, if you see the Apply button highlighted, discard the changes.

The ASA supports LAN-to-LAN VPN connections to Cisco or third-party peers when the two peers have IPv4 inside and outside networks (IPv4 addresses on the inside and outside interfaces).

For LAN-to-LAN connections using mixed IPv4 and IPv6 addressing, or all IPv6 addressing, the security appliance supports VPN tunnels if both peers are ASAs, and if both inside networks have matching addressing schemes (both IPv4 or both IPv6).

Specifically, the following topologies are supported when both peers are ASAs:

- The ASAs have IPv4 inside networks and the outside network is IPv6 (IPv4 addresses on the inside interfaces and IPv6 addresses on the outside interfaces).
- The ASAs have IPv6 inside networks and the outside network is IPv4 (IPv6 addresses on the inside interface and IPv4 addresses on the outside interfaces).
- The ASAs have IPv6 inside networks and the outside network is IPv6 (IPv6 addresses on the inside and outside interfaces).

Fields on the Basic Panel

- Peer IP Address—Lets you specify an IP address (IPv4 or IPv6) and whether that address is static.
- Connection Name—Specifies the name assigned to this connection profile. For the Edit function, this field is display-only. You can specify that the connection name is the same as the IP address specified in the Peer IP Address field.
- Interface—Selects the interface to use for this connection.
- Protected Networks—Selects or specifies the local and remote network protected for this connection.
  - IP Address Type—Specifies the address is an IPv4 or IPv6 address.
  - Local Network—Specifies the IP address of the local network.
  - ...—Opens the Browse Local Network dialog box, in which you can choose a local network.
  - Remote Network—Specifies the IP address of the remote network.
- IPsec Enabling—Specifies the group policy for this connection profile and the key exchange protocol specified in that policy:
  - Group Policy Name—Specifies the group policy associated with this connection profile.
  - Manage—Opens the Browse Remote Network dialog box, in which you can choose a remote network.
  - Enable IKEv1—Enables the key exchange protocol IKEv1 in the specified group policy.
  - Enable IKEv2—Enables the key exchange protocol IKEv2 in the specified group policy.
- IKEv1 Settings tab—Specifies authentication and encryption settings for IKEv1:
  - Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Device Certificate—Specifies the name of the identity certificate, if available, to use for authentication.

- Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
- IKE Policy—Specifies one or more encryption algorithms to use for the IKE proposal.
- Manage—Opens the Configure IKEv1 Proposals dialog box.
- IPsec Proposal—Specifies one or more encryption algorithms to use for the IPsec IKEv1 proposal.

- IKEv2 Settings tab—Specifies authentication and encryption settings for IKEv2:
  - Local Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Local Device Certificate—Specifies the name of the identity certificate, if available, to use for authentication.
  - Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
  - Remote Peer Pre-shared Key—Specify the value of the remote peer pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Remote Peer Certificate Authentication—Check Allowed to allow certificate authentication for IKEv2 connections for this connection profile.
  - Manage—Opens the Manage CA Certificates dialog where you can view certificates and add new ones.
  - Enable RSA Signature Hash—Check this check box to enable RSA signature hash. RSA is a type of encryption.
  - IKE Policy—Specifies one or more encryption algorithms to use for the IKE proposal.
  - Manage—Opens the Configure IKEv1 Proposals dialog box.
  - IPsec Proposal—Specifies one or more encryption algorithms to use for the IPsec IKEv1 proposal.
  - Select—Opens the Select IPsec Proposals (Transform Sets) dialog box, where you can assign a proposal to the connection profile for IKEv2 connections.

This connection profile also has the following parameters:

- Advanced > Crypto Map Entry. For more information, see Site-to-Site Connection Profile, Crypto Map Entry, on page 73.

Site-to-Site Tunnel Groups

The ASDM pane **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups** specifies attributes for the IPsec site-to-site connection profiles (tunnel groups). In addition, you can choose IKE peer and user authentication parameters, configure IKE keepalive monitoring, and choose a default group policy.

- Name—Specifies the name assigned to this tunnel group. For the Edit function, this field is display-only.

- IKE Authentication—Specifies the pre-shared key and Identity certificate parameters to use when authenticating an IKE peer.
  - Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Identity Certificate—Specifies the name of the ID certificate to use for authentication, if available.
  - Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
  - IKE Peer ID Validation—Specifies whether to check IKE peer ID validation. The default is Required.
- IPsec Enabling—Specifies the group policy for this connection profile and the key exchange protocol specified in that policy:
  - Group Policy Name—Specifies the group policy associated with this connection profile.
  - Manage—Opens the Browse Remote Network dialog box, in which you can choose a remote network.
  - Enable IKEv1—Enables the key exchange protocol IKEv1 in the specified group policy.
  - Enable IKEv2—Enables the key exchange protocol IKEv2 in the specified group policy.
- IKEv1 Settings tab—Specifies authentication and encryption settings for IKEv1:
  - Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Device Certificate—Specifies the name of the identity certificate, if available, to use for authentication.



Note Some profiles may be unable to determine whether an endpoint is remote access or LAN-to-LAN. If it cannot determine the tunnel group, it defaults to

```
tunnel-group-map default-group <tunnel-group-name>
```

(default is *DefaultRAGroup*).

  - Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
  - IKE Policy—Specifies one or more encryption algorithms to use for the IKE proposal.
  - Manage—Opens the Configure IKEv1 Proposals dialog box.
  - IPsec Proposal—Specifies one or more encryption algorithms to use for the IPsec IKEv1 proposal.
- IKEv2 Settings tab—Specifies authentication and encryption settings for IKEv2:
  - Local Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.

- Local Device Certificate—Specifies the name of the identity certificate, if available, to use for authentication.
- Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
- Remote Peer Pre-shared Key—Specify the value of the remote peer pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
- Remote Peer Certificate Authentication—Check Allowed to allow certificate authentication for IKEv2 connections for this connection profile.
- Manage—Opens the Manage CA Certificates dialog where you can view certificates and add new ones.
- IKE Policy—Specifies one or more encryption algorithms to use for the IKE proposal.
- Manage—Opens the Configure IKEv1 Proposals dialog box.
- IPsec Proposal—Specifies one or more encryption algorithms to use for the IPsec IKEv1 proposal.
- Select—Opens the Select IPsec Proposals (Transform Sets) dialog box, where you can assign a proposal to the connection profile for IKEv2 connections.

- IKE Keepalive —Enables and configures IKE keepalive monitoring. You can choose only one of the following attributes.
  - Disable Keep Alives—Enables or disables IKE keep alives.
  - Monitor Keep Alives—Enables or disables IKE keep alive monitoring. Selecting this option makes available the Confidence Interval and Retry Interval fields.
  - Confidence Interval—Specifies the IKE keep alive confidence interval. This is the number of seconds the ASA should allow a peer to idle before beginning keepalive monitoring. The minimum is 10 seconds; the maximum is 300 seconds. The default for a remote access group is 10 seconds.
  - Retry Interval—Specifies number of seconds to wait between IKE keep alive retries. The default is 2 seconds.
  - Head end will never initiate keepalive monitoring—Specifies that the central-site ASA never initiates keepalive monitoring.

Site-to-Site Connection Profile, Crypto Map Entry

In this dialog box, specify crypto parameters for the current Site-to-Site Connection Profile.

- **Priority**—A unique priority (1 through 65,543, with 1 the highest priority). When IKE negotiation begins, the peer that initiates the negotiation sends all of its policies to the remote peer, and the remote peer searches for a match with its own policies, in priority order.
- **Perfect Forward Secrecy**—Ensures that the key for a given IPsec SA was not derived from any other secret (like some other keys). If someone were to break a key, PFS ensures that the attacker would not be able to derive any other key. If you enable PFS, the Diffie-Hellman Group list becomes active.

    - **Diffie-Hellman Group**—An identifier which the two IPsec peers use to derive a shared secret without transmitting it to each other. The choices are Group 1 (768-bits), Group 2 (1024-bits), and Group 5 (1536-bits).

- **Enable NAT-T**— Enables NAT Traversal (NAT-T) for this policy, which lets IPsec peers establish both remote access and LAN-to-LAN connections through a NAT device.
- **Enable Reverse Route Injection**—Provides the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint.
- **Security Association Lifetime**—Configures the duration of a Security Association (SA). This parameter specifies how to measure the lifetime of the IPsec SA keys, which is how long the IPsec SA lasts until it expires and must be renegotiated with new keys.
    - **Time**—Specifies the SA lifetime in terms of hours (hh), minutes (mm) and seconds (ss).
    - **Traffic Volume**—Defines the SA lifetime in terms of kilobytes of traffic. Enter the number of kilobytes of payload data after which the IPsec SA expires. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.
- Static Crypto Map Entry Parameters—Configure these additional parameters when the Peer IP Address is specified as Static:
    - Connection Type—Specify the allowed negotiation as bidirectional, answer-only, or originate-only.
    - Send ID Cert. Chain—Enables transmission of the entire certificate chain.
    - IKE Negotiation Mode—Sets the mode for exchanging key information for setting up the SAs, Main or Aggressive. It also sets the mode that the initiator of the negotiation uses; the responder auto-negotiates. Aggressive Mode is faster, using fewer packets and fewer exchanges, but it does not protect the identity of the communicating parties. Main Mode is slower, using more packets and more exchanges, but it protects the identities of the communicating parties. This mode is more secure and it is the default selection. If you choose Aggressive, the Diffie-Hellman Group list becomes active.
    - Diffie-Hellman Group—An identifier which the two IPsec peers use to derive a shared secret without transmitting it to each other. The choices are Group 1 (768-bits), Group 2 (1024-bits), and Group 5 (1536-bits).

Managing CA Certificates

Managing CA Certificates applies to Remote Access and Site-to-Site VPN:

- On Site-to_site: Click Manage under IKE Peer Authentication to open the Manage CA Certificates dialog box.
- On Remote Access VPN, click **Certificate Management** > **CA Certificates**.

Use this dialog box to view, add, edit, and delete entries on the list of CA certificates available for IKE peer authentication. The Manage CA Certificates dialog box lists information about currently configured certificates, including information about whom the certificate was issued to, who issued the certificate, when the certificate expires, and usage data.

- Add or Edit—Opens the Install Certificate dialog box or the Edit Certificate dialog box, which let you specify information about and install a certificate.
- Show Details—Displays detailed information about a certificate that you choose in the table.
- Delete—Removes the selected certificate from the table. There is no confirmation or undo.

Site-to-Site Connection Profile, Install Certificate

Use this dialog box to install a new CA certificate. You can get the certificate in one of the following ways:

- Install from a file by browsing to the certificate file.
- Paste the previously acquired certificate text in PEM format into the box in this dialog box.
- Use SCEP—Specifies the use of the Simple Certificate Enrollment Protocol (SCEP) Add-on for Certificate Services runs on the Windows Server 2003 family. It provides support for the SCEP protocol, which allows Cisco routers and other intermediate network devices to obtain certificates.
  - SCEP URL: http://—Specifies the URL from which to download SCEP information.
  - Retry Period—Specifies the number of minutes that must elapse between SCEP queries.
  - Retry Count—Specifies the maximum number of retries allowed.
- More Options—Opens the Configure Options for CA Certificate dialog box.

Use this dialog box to specify details about retrieving CA Certificates for this IPsec remote access connection. The dialog boxes in this dialog box are: Revocation Check, CRL Retrieval Policy, CRL Retrieval Method, OCSP Rules, and Advanced.

Use the Revocation Check dialog box to specify information about CA Certificate revocation checking.

- The radio buttons specify whether to check certificates for revocation. Choose **Do not check certificates for revocation** or Check Certificates for revocation.
- Revocation Methods area—Lets you specify the method–CRL or OCSP–to use for revocation checking, and the order in which to use these methods. You can choose either or both methods.

AnyConnect VPN module of Cisco Secure Client Image

The **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software** pane lists the AnyConnect Client images that are configured in ASDM.

AnyConnect Client Images table—Displays the package files configured in ASDM, and allows you to establish the order that the ASA downloads the images to the remote PC.

- Add—Displays the Add AnyConnect Client Image dialog box, where you can specify a file in flash memory as a client image file, or you can browse flash memory for a file to specify as a client image. You can also upload a file from a local computer to the flash memory.
- Replace—Displays the Replace AnyConnect Client Image dialog box, where you can specify a file in flash memory as an client image to replace an image highlighted in the SSL VPN Client Images table. You can also upload a file from a local computer to the flash memory.

- Delete—Deletes an image from the table. This does not delete the package file from flash.
- Move Up and Move Down—The up and down arrows change the order in which the ASA downloads the client images to the remote PC. It downloads the image at the top of the table first. Therefore, you should move the image used by the most commonly-encountered operating system to the top.

AnyConnect VPN module of Cisco Secure Client Image, Add/Replace

In this pane, you can specify a filename for a file on the ASA flash memory that you want to add as an AnyConnect Client image, or to replace an image already listed in the table. You can also browse the flash memory for a file to identify, or you can upload a file from a local computer.

- Flash SVC Image—Specify the file in flash memory that you want to identify as an SSL VPN client image.
- Browse Flash—Displays the Browse Flash dialog box where you can view all the files on flash memory.
- Upload—Displays the Upload Image dialog box where you can upload a file from a local PC that you want to identify as an client image.
- Regular expression to match user-agent—Specifies a string that the ASA uses to match against the User-Agent string passed by the browser. For mobile users, you can decrease the connection time of the mobile device by using the feature. When the browser connects to the ASA, it includes the User-Agent string in the HTTP header. When the ASA receives the string, if the string matches an expression configured for an image, it immediately downloads that image without testing the other client images.

AnyConnect VPN module of Cisco Secure Client Image, Upload Image

In this pane, you can specify the path of a file on the local computer or in flash memory of the security appliance that you want to identify as an AnyConnect Client image. You can also browse the local computer or the flash memory of the security appliance for a file to identify.

- Local File Path—Identifies the filename of the file in on the local computer that you want to identify as an SSL VPN client image.
- Browse Local Files—Displays the Select File Path dialog box where you can view all the files on local computer and can choose a file to identify as a client image.
- Flash File System Path—Identifies the filename of the file in the flash memory of the security appliance that you want to identify as an SSL VPN client image.
- Browse Flash—Displays the Browse Flash Dialog dialog box where you can view all the files on flash memory of the security appliance and where you can choose a file to identify as a client image.
- Upload File—Initiates the file upload.

AnyConnect Client External Browser SAML Package

The **Configuration > Remote Access VPN > Network (Client) Access >AnyConnect External Browser** pane lists the AnyConnect Client external browser packages available for AnyConnect Client SAML single sign-on (SSO) authentication.

AnyConnect Client External Browser Package Images—Displays the external browser package files configured in ASDM.

- **Add**—Displays the Add AnyConnect Client External Browser Image dialog box, where you can specify a file in flash memory as an external package image file, or you can browse flash memory for a file to specify as the external browser package file.
- **Replace**—Displays the Replace AnyConnect Client External Browser Package dialog box, where you can specify a file in flash memory as an external browser package to replace an existing package file.
- **Delete**—Deletes an external browser package file from the table. This does not delete the package file from flash.
- **Move Up and Move Down**—The up and down arrows change the order in which the ASA downloads the external browser package to the remote PC.

AnyConnect Client External Browser SAML Package Images, Add/Replace

In this pane, you can specify a filename for a file on the ASA flash memory that you want to add as an AnyConnect Client external browser package image, or to replace an image already listed in the table. You can also browse the flash memory for a file to identify, or you can upload a file from a local computer.

- **AnyConnect Client External Browser Package** —Specify the file in flash memory that you want to identify as an external browser package image.
- **Browse Flash**—Displays the Browse Flash dialog box where you can view all the files on flash memory.
- **Upload**—Displays the Upload Image dialog box where you can upload a file from a local PC that you want to identify as an external browser package image.

AnyConnect Client External Browser SAML Package Images, Upload Image

In this pane, you can specify the path of a file on the local computer or in flash memory of the security appliance that you want to identify as an AnyConnect Client image. You can also browse the local computer or the flash memory of the security appliance for a file to identify.

- **Local File Path**—Identifies the filename of the file in on the local computer that you want to identify as an external browser package image.
- **Browse Local Files**—Displays the Select File Path dialog box where you can view all the files on local computer and can choose a file to identify as an external browser package image..
- **Flash File System Path**—Identifies the filename of the file in the flash memory of the security appliance that you want to identify as an external browser package image.
- **Browse Flash**—Displays the Browse Flash Dialog dialog box where you can view all the files on flash memory of the security appliance and where you can choose a file to identify as an external browser package image..
- **Upload File**—Initiates the file upload.

Configure AnyConnect Client VPN Connections

Guidelines and Limitations for AnyConnect Client Connections

Recommendation for Session Tokens

When the ASA authenticates a VPN connection request from AnyConnect Client, a session token is returned to the client for enhanced security. Starting with AnyConnect 4.9 (MR1), the ASA and AnyConnect Client support a mechanism that provides enhanced security for the session token. You can configure a DAP rule to reject connection attempts from AnyConnect Client versions that do not support token security. See Use DAP to Check Session Token Security.

Configure AnyConnect Client Profiles

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

For more information about creating and deploying AnyConnect Client profiles and controlling client features, see the AnyConnect VPN Client Administrator Guide.

Client profiles are configured in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**:

Add/Import—Displays the Add AnyConnect Client Profiles dialog box, where you can specify a file in flash memory as a profile, or where you can browse flash memory for a file to specify as a profile. You can also upload a file from a local computer to the flash memory.

- Profile Name—Specify an AnyConnect Client profile for this group policy.
- Profile Usage—Displays the usage assigned to the profile when originally created: VPN, Network Access Manager, Web Security, ISE Posture, AMP Enabler, Network Visibility Module, Umbrella Roaming Security, or management VPN tunnel. If ASDM does not recognize the usage specified in the XML file, the drop-down list becomes selectable and you can choose a usage type manually.
- Profile Location—Specify a path to the profile file in the ASA flash memory. If the file does not exist, the ASA creates one based on the profile template.
- Group Policy—Specify a group policy for this profile. The profile downloads to users belonging to the group policy along with the AnyConnect Client.

Edit—Displays the Edit SSL VPN Client Profile window, where you can change the settings contained in the profile for AnyConnect Client features.

Export

- Device Profile Path—Displays the path and filename of the profile file.
- Local Path—Specify the path and filename to export the profile file.

- Browse Local—Click to launch a window to browse the local device file system.

Delete—Deletes a profile from the table. This does not delete the XML file from flash.

AnyConnect Client Profiles Table—Displays the XML files specified as AnyConnect Client profiles:

Exempt AnyConnect Client Traffic from Network Address Translation

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

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

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

Table 4: Network Addressing for Configuring Identity NAT for VPN Clients

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

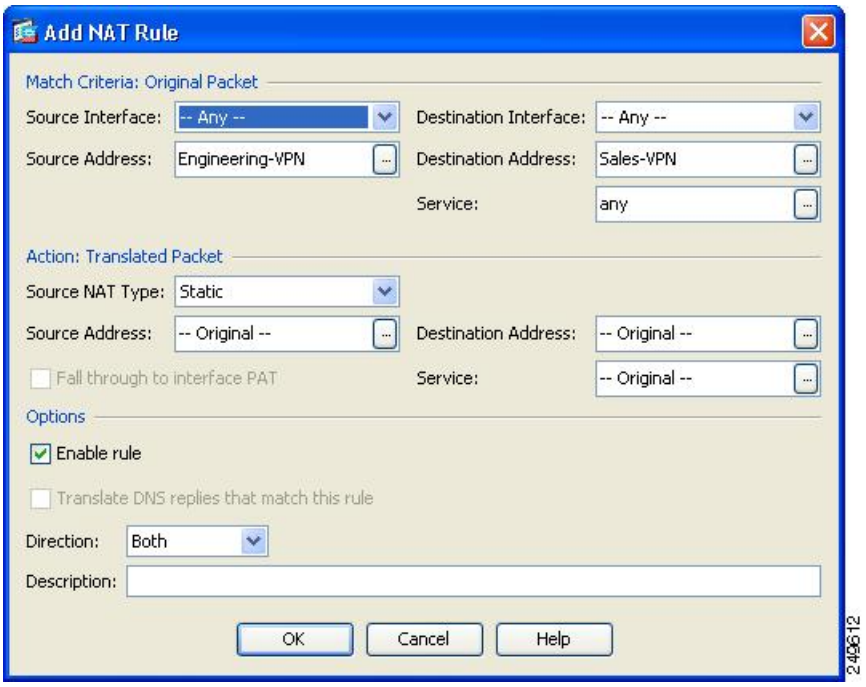
Procedure

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

Step 2 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach the hosts in the Sales VPN address pool. In the NAT Rules pane, navigate to **Add > Add NAT Rule** Before "Network Object" NAT rules so that the ASA evaluates this rule before other rules in the Unified NAT table.

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

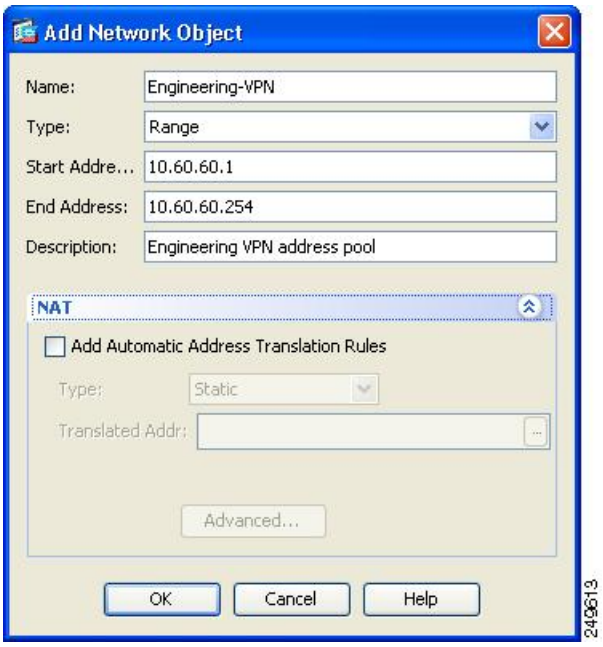
Figure 1: Add NAT rule dialog box



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

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

Figure 2: Create Network Object for a VPN address pool



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

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

c) In the Options area, configure these fields:

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

d) Click **OK**.

e) Click **Apply**.

CLI example:

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

f) Click Send.

Step 3 When ASA is performing NAT, in order for two hosts in the same VPN pool to connect to each other, or for those hosts to reach the Internet through the VPN tunnel, you must enable the Enable traffic between two or more hosts connected to the same interface option. To do this, in ASDM, choose **Configuration > Device**

Setup > Interface Settings > Interfaces. At the bottom of the Interface panel, check Enable traffic between two or more hosts connected to the same interface and click Apply.

CLI example:

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

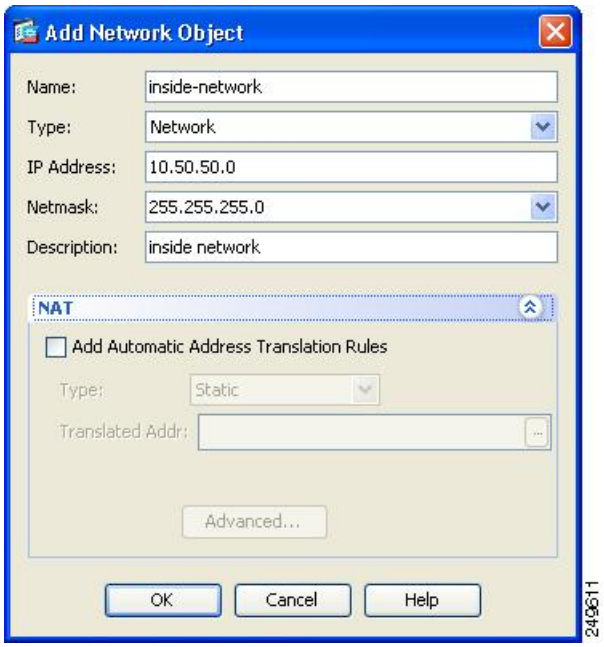
Step 4 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach other hosts in the Engineering VPN address pool. Create this rule just as you created the rule in in the previously, except that you specify the Engineering VPN address pool as both the Source address and the Destination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

Step 5 Create a NAT rule so that the Engineering VPN remote access clients can reach the "inside" network. In the NAT Rules pane, choose Add > Add NAT Rule Before "Network Object" NAT rules so that this rule will be processed before other rules.

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

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

Figure 3: Add inside-network object



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

- Source NAT Type: Static

- Source Address: Original
- Destination Address: Original
- Service: Original

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

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

d) Click **OK**.

e) Click **Apply**.

CLI example

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

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

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

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

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

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

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

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

d) In the Options area, configure these fields:

- Check Enable rule.

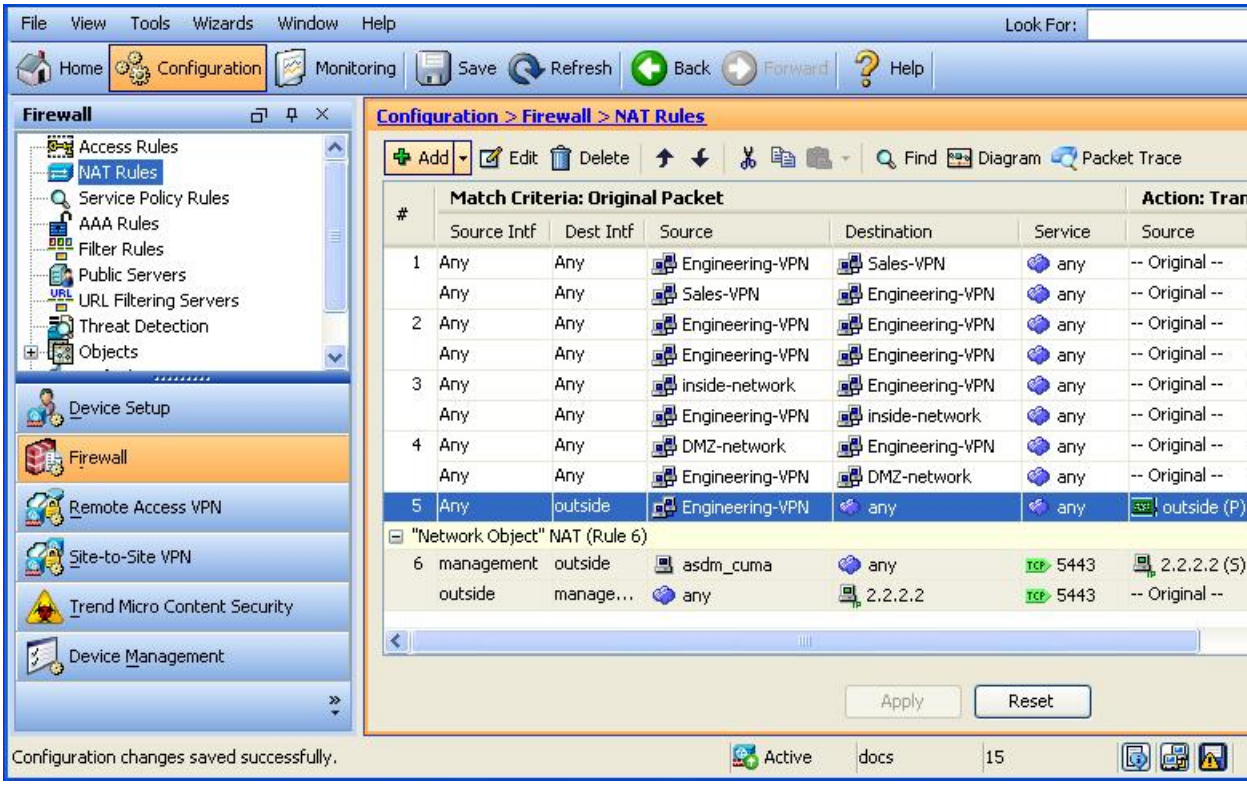
- Uncheck or leave empty the Translate DNS replies that match this rule.
- Direction: Both
- Description: Add a Description for this rule.

e) Click **OK**.
f) Click **Apply**.

CLI example:

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

Figure 4: Unified NAT table



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

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

AnyConnect Client HostScan

AnyConnect Client HostScan, now called Secure Firewall Posture, provides the Secure Client the ability to identify the operating system, antimalware, and firewall software installed on the host. The Secure Firewall Posture/HostScan application gathers this information. Posture assessment requires Secure Firewall Posture/HostScan to be installed on the host.

The ASDM UI is dynamic in that if HostScan is loaded, it will reflect HostScan. When Secure Firewall Posture is loaded, it will reflect Secure Firewall Posture. The different naming depends on the version you are running.

Prerequisites for HostScan/Secure Firewall Posture

The AnyConnect Client with the Secure Firewall Posture/HostScan module requires these minimum ASA components:

- ASA 8.4
- ASDM 6.4

You must install Secure Firewall Posture/HostScan to use the SCEP authentication feature.

Refer to Supported VPN Platforms, Cisco ASA Series for what operating systems are supported for Secure Firewall Posture/HostScan installation.

Licensing for AnyConnect Client HostScan/Secure Firewall Posture

These are the licensing requirements for Secure Firewall Posture/HostScan:

- AnyConnect Client Advantage (Apex) for basic HostScan/Secure Firewall Posture.
- Advanced Endpoint Assessment license is required for remediation.

HostScan Packaging

You can load the HostScan package on to the ASA as a standalone package: **hostscan-version.pkg**. This file contains the HostScan software as well as the HostScan library and support charts.

Install or Upgrade HostScan/Secure Firewall Posture

Use this procedure to install or upgrade the HostScan/Secure Firewall Posture package and enable it using ASDM. The ASDM UI is dynamic in that if HostScan is loaded, it will reflect HostScan. When Secure Firewall Posture is loaded, it will reflect Secure Firewall Posture. The different naming depends on the version you are running.

Before you begin

Note If you are attempting to upgrade to HostScan version 4.6.x or later from a 4.3.x version or earlier, you will receive an error message due to the fact that all existing AV/AS/FW DAP policies and LUA script(s) that you have previously established are incompatible with HostScan 4.6.x or greater.

There is a one time migration procedure that must be done to adapt your configuration. This procedure involves leaving this dialog box to migrate your configuration to be comptaible with HostScan 4.4.x before saving this configuration. Abort this procedure and refer to the AnyConnect Client HostScan 4.3.x to 4.6.x Migration Guide for detailed instructions. Briefly, migration involves navigating to the ASDM DAP policy page to review and manually deleting the incompatible AV/AS/FW attributes, and then reviewing and rewriting LUA scripts.

Procedure

Step 1 Download the secure-firewall-posture-*version*-k9.pkg file to your computer if you are using version 5. For version 4.x, the file is hostscan_*version*-k9.pkg.

Step 2 Open ASDM and choose **Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Image**. If you are using the HostScan 4.x version, the path will be **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image**.

Step 3 Click **Upload** to prepare to transfer a copy of the HostScan/Secure Firewall Posture package from your computer to a drive on the ASA.

Step 4 In the Upload Image dialog box, click **Browse Local Files** to search for the HostScan/Secure Firewall Posture package on your local computer.

Step 5 Choose the hostscan_*version*-k9.pkg or secure-firewall-posture-*version*-k9.pkg file you downloaded above and click **Select**. The path to the file you selected is in the Local File Path field, and the Flash File System Path field reflects the destination path of the HostScan/Secure Firewall Posture package. If your ASA has more than one flash drive, you can edit the Flash File System Path to indicate another flash drive.

Step 6 Click **Upload File.** ASDM transfers a copy of the file to the flash card. An Information dialog box displays that the file has been successfully uploaded to flash.

Step 7 Click **OK**.

Step 8 In the Use Uploaded Image dialog, click **OK** to use the HostScan/Secure Firewall Posture package file you just uploaded as the current image.

Step 9 Check **Enable HostScan** or **Enable Posture Image**if it is not already checked.

Step 10 Click **Apply**.

Step 11 From the File menu, choose **Save Running Configuration To Flash**.

Configure Posture Settings

For each device, you can configure the posture settings.

Before you begin

Ensure that you have the HostScan/Secure Firewall Posture package.

Procedure

Step 1 Choose **Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Settings**.

Step 2 In the left pane, select a device from the device list.

For each device, you can view the **Basic Posture** attributes and the **Posture Extensions**.

Step 3 By default, the Endpoint Detection and Response (EDR) security software communicates with its respective server to retrieve information. You can configure the following settings for EDR updates:

- Check the **For EDR update, Skip Internet Check after VPN is active** check box if you want the EDR to skip the internet connection check when the VPN tunnel is active.
- Check the **For EDR update, Skip Internet Check before VPN is active** check box to enable HostScan/Secure Firewall Posture assessment without verifying if the security software is up-to-date. If you uncheck the check box, the posture assessment may fail due to lack of connectivity, resulting in denied network access depending on the policy. We recommend that you verify the internet connectivity before posture assessment.

Uninstall HostScan/Secure Firewall Posture

Uninstalling HostScan/Secure Firewall Posture package removes it from view on the ASDM interface and prevents the ASA from deploying it even when it is enabled. Uninstalling HostScan/Secure Firewall Posture does not delete the package from the flash drive.

Procedure

Step 1 In ASDM, navigate to **Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Image** to uninstall Secure Firewall Posture. If you are using AnyConnect version 4.x and uninstalling HostScan, navigate to **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image**.

Step 2 Click **Uninstall**, and then **Yes** to confirm.

Step 3 Click **Uninstall**.

Assign AnyConnect Client Feature Modules to Group Policies

This procedure associates AnyConnect Client feature modules with a group policy. When VPN users connect to the ASA, the ASA downloads and installs these AnyConnect Client feature modules to their endpoint computer.

Before you begin

Log on to the ASA and enter global configuration mode. In global configuration mode, the ASA displays this prompt: hostname(config)#

Procedure

Step 1 Adds an internal group policy for Network Client Access

group-policy *name* **internal**

Example:

```
hostname(config)# group-policy PostureModuleGroup internal
```

Step 2 Edit the new group policy. After entering the command, you receive the prompt for group policy configuration mode, hostname(config-group-policy)#.

group-policy *name* **attributes**

Example:

```
hostname(config)# group-policy PostureModuleGroup attributes
```

Step 3 Enter group policy webvpn configuration mode. After you enter the command, the ASA returns this prompt: hostname(config-group-webvpn)#

webvpn

Step 4 Configure the group policy to download the AnyConnect Client feature modules for all users in the group.

anyconnect modules value *AnyConnect Module Name*

The value of the anyconnect module command can contain one or more of the following values. When specifying more than one module, separate the values with a comma:

value	AnyConnect Module/Feature Name
dart	AnyConnect DART (Diagnostics and Reporting Tool)
vpngina	AnyConnect SBL (Start Before Logon)
posture	Secure Firewall Posture/HostScan
nam	AnyConnect Network Access Manager
none	Used by itself to remove all AnyConnect modules from the group policy.
profileMgmt	AnyConnect Management Tunnel VPN

Example:

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

To remove one of the modules, re-send the command specifying only the module values you want to keep. For example, this command removes the websecurity module:

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

Step 5 Save the running configuration to flash.

After successfully saving the new configuration to flash memory, you receive the message [OK] and the ASA returns you to this prompt hostname(config-group-webvpn)#

write memory

HostScan/Secure Firewall Posture Related Documentation

Once HostScan/Secure Firewall Posture gathers the posture credentials from the endpoint computer, you will need to understand subjects like configuring dynamic access policies and using LUA expressions to make use of the information.

These topics are covered in detail in these documents: Cisco Adaptive Security Device Manager Configuration Guides. See also the Cisco *Secure Client (including AnyConnect) Administrator Guide* for more information about how HostScan/Secure Firewall Posture works with AnyConnect Client.

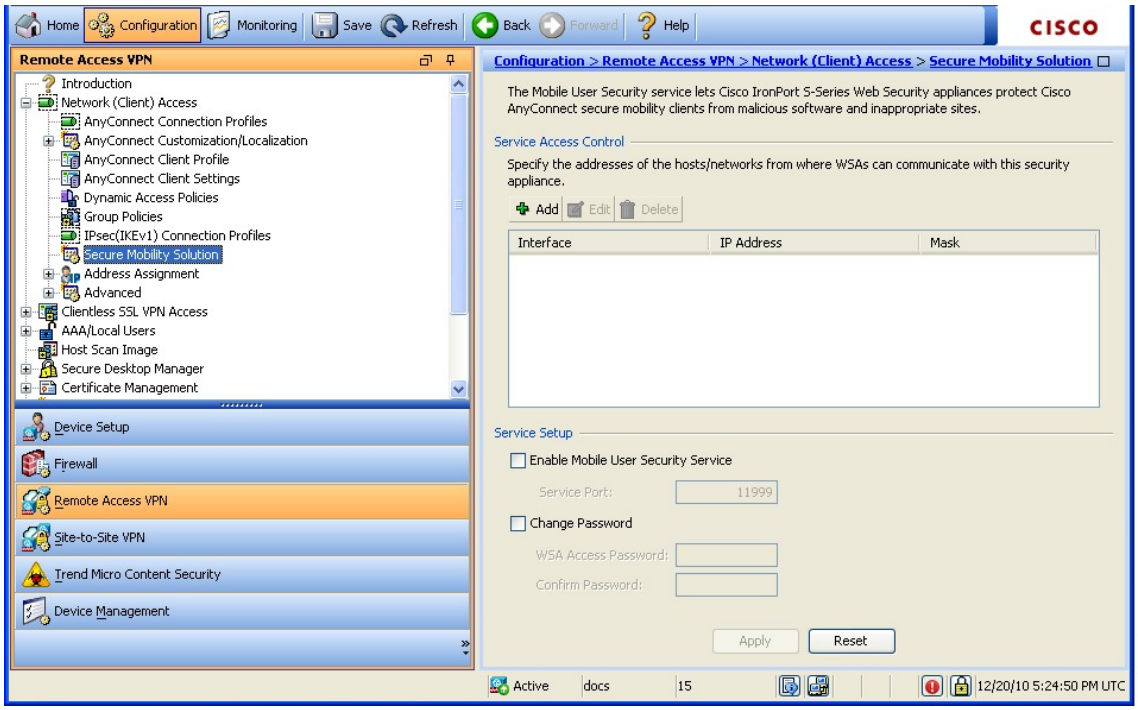
Secure Client Solution

Secure Client protects corporate interests and assets from Internet threats when employees are mobile. Secure Client lets Cisco IronPort S-Series Web Security appliances scan Secure Clients to ensure that clients are protected from malicious software and/or inappropriate sites. The client periodically checks to ensure that Cisco IronPort S-Series Web Security appliance protection is enabled.

Note This feature requires a release of the Cisco IronPort Web Security appliance that provides Secure Client licensing support for the Secure Client. It also requires an AnyConnect Client release that supports the Secure Client feature. AnyConnect 3.1 and higher does not support this feature.

To configure secure mobility solutions, choose **Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution**.

Figure 5: Mobile User Security Window



- Service Access Control—Specifies from which host or network address the WSAs can communicate.
  - Add—Opens the Add MUS Access Control Configuration dialog box for the selected connection.
  - Edit—Opens the Edit MUS Access Control Configuration dialog box for the selected connection.
  - Delete—Removes the selected connection from the table. There is no confirmation or undo.
- Enable Mobile User Security Service—Starts the connection with the client through the VPN. If enabled, you are required to enter a password, used by the WSA when contacting the ASA. If no WSA is present, the status is disabled.
- Service Port—If you choose to enable the service, specify which port number for the service to use. The port must be between 1 and 65535 and must match the corresponding value provisioned into the WSA with the management system. The default is 11999.
- Change Password—Enables you to change the WSA access password.
- WSA Access Password—Specify the shared secret password required for authentication between the ASA and WSA. This password must match the corresponding password provisioned into the WSA with the management system.
- Confirm Password—Re-enter the specified password.
- Show WSA Sessions—Allows you to view session information of WSAs connected to the ASA.The host IP address of the WSA that is connected (or has been connected) and the duration of the connection is returned in a dialog box.

Add or Edit MUS Access Control

The Add or Edit MUS Access Control dialog box under Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution configures Mobile User Security (MUS) access for AnyConnect Clients.

- Interface Name—Use the drop-down list to choose which interface name you are adding or editing.
- IP Address—Enter either an IPv4 or IPv6 address.
- Mask—Use the drop-down list to choose the appropriate mask.

AnyConnect Client Customization and Localization

You can customize the AnyConnect VPN client to display your own corporate image to remote users. The following fields under AnyConnect Client Customization/Localization allow you to import the following types of customized files:

- **Resources**—Modified GUI icons for the AnyConnect Client.
- **Binary**—Executable files to replace the AnyConnect Client installer. This includes GUI files, plus the VPN client profile, scripts and other client files.
- **Script**—Scripts that will run before or after AnyConnect Client makes a VPN connection.
- **GUI Text and Messages**—Titles and messages used by the AnyConnect Client.
- **Customized Installer**—Transforms that modify the client installation.
- **Localized Installer**—Transforms that change the language used by the client.

Each dialog provides the following actions:

- **Import** launches the Import AnyConnect Client Customization Objects dialog, where you can specify a file to import as an object.
- **Export** launches the Export AnyConnect Client Customization Objects dialog, where you can specify a file to export as an object.
- **Delete** removes the selected object.



Note This feature is not supported in multiple-context mode.

AnyConnect Client Customization and Localization, Resources

The filenames of the custom components that you import must match the filenames used by the AnyConnect Client GUI, which are different for each operating system and are case sensitive for Mac and Linux. For example, if you want to replace the corporate logo for Windows clients, you must import your corporate logo as company_logo.png. If you import it as a different filename, the AnyConnect Client installer does not change

the component. However, if you deploy your own executable to customize the GUI, the executable can call resource files using any filename.

If you import an image as a resource file (such as company_logo.bmp), the image you import customizes AnyConnect Client until you reimport another image using the same filename. For example, if you replace company_logo.bmp with a custom image, and then delete the image, the client continues to display your image until you import a new image (or the original Cisco logo image) using the same filename.

AnyConnect Client Customization and Localization, Binary and Script

AnyConnect Client Customization/Localization, Binary

For Windows, Linux, or Mac (PowerPC or Intel-based) computers, you can deploy your own client that uses the AnyConnect Client API. You replace the AnyConnect Client GUI and the AnyConnect Client CLI by replacing the client binary files.

Fields for the **Import** dialog:

- **Name** Enter the name of the AnyConnect Client file that you are replacing.
- **Platform** Select the OS platform that your file runs on.
- **Select a file** The filename does not need to be the same as the name of the imported file.

AnyConnect Client Customization/Localization, Script

For complete information about deploying scripts, and their limitations and restrictions, see the AnyConnect VPN module of Cisco Secure Client Administrators Guide.

Fields for the **Import** dialog:

- **Name**—Enter a name for the script. Be sure to specify the correct extension with the name. For example, myscript.bat.
- **Script Type**—Choose when to run the script.

  AnyConnect Client adds the prefix scripts_ and the prefix OnConnect or OnDisconnect to your filename to identify the file as a script on the ASA. When the client connects, the ASA 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 ASA as scripts_OnConnect_myscript.bat. On the remote computer, the script appears as OnConnect_myscript.bat.

  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 of the ASAs that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- **Platform**—Select the OS platform that your file runs on.
- **Select a file**—The filename does not need to be the same as the name you provided for the script.

ASDM imports the file from any source file, creating the new name you specify for Name.

AnyConnect Client Customization and Localization, GUI Text and Messages

You can edit the default translation table, or create new ones, to change the text and messages displayed on the AnyConnect Client GUI. This pane also shares functionality with the Language Localization pane. For more extensive language translation, go to **Configuration > Remote Access VPN > Language Localization**.

In addition to the usual buttons on the top toolbar, this pane also has an **Add** button, and a Template area with extra buttons.

Add—The Add button opens a copy of the default translation table, which you can edit directly, or save. You can choose the language of the saved file, and edit the language of the text inside the file later.

When you customize messages in the translation table, do not change msgid. Change the text in msgstr.

Specify a language for the template. The template becomes a translation table in cache memory with the name you specify. Use an abbreviation that is compatible with the language options for your browser. For example, if you are creating a table for the Chinese language, and you are using IE, use the abbreviation *zh,* that is recognized by IE.

Template Section

- Click Template to expand the template area, which provides access to the default English translation table.
- Click **View** to view, and optionally save, the default English translation table
- Click **Export** to save a copy of the default English translation table without looking at it.

AnyConnect Client Customization and Localization, Customized Installer Transforms

You can perform more extensive customizing of the AnyConnect Client GUI (Windows only) by creating your own transform that deploys with the client installer program. You import the transform to the ASA, which deploys it with the installer program.

Windows is the only valid choice for applying a transform. For more information about transforms, see the *Cisco Secure Client Administration Guide*.

AnyConnect Client Customization and Localization, Localized Installer Transforms

You can translate messages displayed by the client installer program with a transform. The transform alters the installation, but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.

AnyConnect Client Custom Attributes

Custom attributes are sent to and used by the AnyConnect Client to configure features such as those below. A custom attribute has a type and a named value. Predefined custom attributes are used by both Dynamic Access Policies and Group Policies. For information on configuring these custom attributes, refer to Configure

Secure Client Custom Attributes in an Internal Group Policy. Create and set custom attributes for many different uses:

- **DSCPPreservationAllowed**: To enable DSCP Preservation—Setting this custom attribute controls Differentiated Services Code Point (DSCP) on Windows or Mac operating system platforms for DTLS connection. It allows devices to prioritize latency sensitive traffic and marks prioritized traffic to improve outbound connection quality. For additional information, see the *Enable DSCP Preservation* section in the Cisco Secure Client Administration Guide.

  Values—True/False: By default AnyConnect Client performs DSCP preservation (True). To disable it, set the custom attribute value to false on the headend and reinitiate the connection.

- **DeferredUpdateAllowed or DeferredUpdateAllowed_ComplianceModule**: To enable deferred update on an ASA—If these custom attributes are configured, then when a client update is available, AnyConnect Client opens a dialog asking the user if they would like to update or to defer. For additional information, see Enable AnyConnect Client Deferred Upgrade or *Configure Deferred Update on an ASA* in the Cisco Secure Client Administration Guide .

  Values—True/False: True enables deferred update. If deferred update is disabled (false), the following settings are ignored.

  - **DeferredUpdateMinimumVersion_ComplianceModule or DeferredUpdateMinimumVersion**—Minimum version of AnyConnect Client that must be installed for updates to be deferrable.

    Values—x.x.x, with default of 0.0.0

  - **DeferredUpdateDismissTimeout**—Number of seconds that the deferred upgrade prompt is displayed before being dismissed automatically. Applies only when a deferred update prompt is displayed.

    Values—0 to 300 seconds. Default 150 seconds.

  - **DeferredUpdateDismissResponse**—Action to take when DeferredUpdateDismissTimeout occurs.

    Values—Defer or update. Default is update.

- **dynamic-split-exclude-domains <attribute name> <list of domains> or dynamic-split-include-domains <attribute name> <list of domains>**: To enable dynamic split tunneling—By creating this custom attribute, you can dynamically split exclude tunneling after tunnel establishment based on the host DNS domain name. By adding dynamic-split-exclude-domains, you can enter cloud or web services that need access by the client from outside the VPN tunnel. For additional information, see *About Dynamic Split Tunneling* in the Cisco Secure Client Administration Guide.

  Values—The attribute name is whatever name you choose. For example, anyconnect-custom-data dynamic-split-exclude-domains excludedomains webex.com, ciscospark.com.

- **managementTunnelAllAllowed**: To enable management VPN tunnel—Management VPN tunnel requires split include tunneling configuration, by default, to avoid impacting user-initiated network communication (since it is meant to be transparent).

  Values—true/false. To override this behavior, set both attribute name and value to *true* . AnyConnect Client then proceeds with the management tunnel connection, if the configuration is one of tunnel-all, split-exclude, split-include, or bypass for both IP protocols.

- **UseLocalProfileAsAlternative**: If you want to distribute a profile out-of-band (using SCCM, MDM, SecureX Cloud Management, or the like) without configuring a Cisco Secure Client Profile (previously known as an AnyConnect profile) on the Secure Firewall ASA, you can use the *UseLocalProfileAsAlternative* custom attribute. When you configure this custom attribute, the client uses

the local (on disk) Cisco Secure Client profile for its settings and preferences (rather than the usual defaults). Refer to Predeploying Cisco Secure Client in the administration guide for additional information.

Establishing the session using the local profile only occurs when 1) *UseLocalProfileAsAlternative* is set to enabled, and 2) if an ASA group policy profile is not configured. If you configure this custom attribute and do not undo or remove the Cisco Secure Client profile from the Group Policy configuaration on the ASA, the Cisco Secure Client Profile configured on the Group Policy will be maintained and used for each connection, where the custom attribute setting will be ignored.

Name—disabled/enabled

Values—true/false

- **no-dhcp-server-route**: To set public DHCP server route—This custom attribute allows local DHCP traffic to flow in the clear when Tunnel All Network is configured. AnyConnect Client adds a specific route to the local DHCP server when the AnyConnect Client connects and applies an implicit filter on the LAN adapter of the host machine, blocking all traffic for that route except DHCP traffic. For additional information, see the *Set Public DHCP Server Route* section in the Cisco Secure Client Administration Guide.

  Values—true/false. The no-dhcp-server-route custom attribute must be present and set to true to avoid creating the public DHCP server route upon tunnel establishment.

- **circumvent-host-filtering**: To configure Linux to support excluded subnets—Sets Linux to support exclude subnets when Tunnel Network List Below is configured for split tunneling. For additional information, see Configure Linux to Support Excluded Subnets, on page 24.

  Values—true/false. Set it to true.

- **tunnel-from-any-source**—(Linux only) AnyConnect Client permits packets with any source address in Split-Include or Split-Exclude tunnel mode. It could allow network access inside VM instance or Docker container.

Note Networks used by VM/Docker must be excluded from the tunnel initially.

- **perapp**—The VPN connection is used for a specific set of apps on the mobile device (Android or Apple iOS only). Refer to the Create Per App Custom Attributes section in the *Cisco Secure Client Administration Guide* for additional information.

  Values—Add one or more values by copying the BASE64 format from the policy tool and pasting it here.

To further complete the use of these features, most of the defined custom attributes have to be associated to a certain group policy in the **Configuration > Remote Access VPN > Network (Client) Access > Group Polices** > menu.

IPsec VPN Client Software



Note **The VPN Client is end-of-life and end-of-support.** For information about configuring the VPN client, see the ASDM documentation for ASA version 9.2. **We recommend that you upgrade to the AnyConnect Secure Mobility Client.**

Zone Labs Integrity Server

The **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Zone Labs Integrity Server** panel lets you configure the ASA to support a Zone Labs Integrity Server. This server is part of the Integrity System, a system designed to enforce security policies on remote clients entering the private network. In essence, the ASA acts as a proxy for the client PC to the Firewall Server and relays all necessary Integrity information between the Integrity client and the Integrity server.



Note The current release of the security appliance supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the ASA and then reestablish the client VPN session.

- **Server IP address**—Type the IP address of the Integrity Server. Use dotted decimal notation.
- **Add**—Adds a new server IP address to the list of Integrity Servers. This button is active when an address is entered in the Server IP address field.
- **Delete**—Deletes the selected server from the list of Integrity Servers.
- **Move Up**—Moves the selected server up in the list of Integrity Servers. This button is available only when there is more than one server in the list.
- **Move Down**—Moves the selected server down in the list of Integrity Servers. This button is available only when there is more than one server in the list.
- **Server Port**—Type the ASA port number on which it listens to the active Integrity server. This field is available only if there is at least one server in the list of Integrity Servers. The default port number is 5054, and it can range from 10 to 10000. This field is only available when there is a server in the Integrity Server list.
- **Interface**—Choose the interface ASA interface on which it communicates with the active Integrity Server. This interface name menu is only available when there is a server in the Integrity Server list.
- **Fail Timeout**—Type the number of seconds that the ASA should wait before it declares the active Integrity Server to be unreachable. The default is 10 and the range is from 5 to 20.
- **SSL Certificate Port**—Specify the ASA port to be used for SSL Authorization. The default is port 80.
- **Enable SSL Authentication**—Check to enable authentication of the remote client SSL certificate by the ASA. By default, client SSL authentication is disabled.

- **Close connection on timeout**—Check to close the connection between the ASA and the Integrity Server on a timeout. By default, the connection remains open.
- **Apply**—Click to apply the Integrity Server setting to the ASA running configuration.
- **Reset**—Click to remove Integrity Server configuration changes that have not yet been applied.

ISE Policy Enforcement

The Cisco Identity Services Engine (ISE) is a security policy management and control platform. It automates and simplifies access control and security compliance for wired, wireless, and VPN connectivity. Cisco ISE is primarily used to provide secure access and guest access, support bring your own device (BYOD) initiatives, and enforce usage policies in conjunction with Cisco TrustSec.

The ISE Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is established. When a policy changes for a user or user group in AAA, CoA packets can be sent directly to the ASA from the ISE to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is not required to apply access control lists (ACLs) for each VPN session established with the ASA.

ISE policy enforcement is supported on the following VPN clients:

- IPSec
- AnyConnect Client
- L2TP/IPSec

The system flow is as follows:

1. An end user requests a VPN connection.
2. The ASA authenticates the user to the ISE and receives a user ACL that provides limited access to the network.
3. An accounting start message is sent to the ISE to register the session.
4. Posture assessment occurs directly between the NAC agent and the ISE. This process is transparent to the ASA.
5. The ISE sends a policy update to the ASA via a CoA “policy push.” This identifies a new user ACL that provides increased network access privileges.



Note Additional policy evaluations may occur during the lifetime of the connection, transparent to the ASA, via subsequent CoA updates.

Configure ISE Change of Authorization

Configuring ISE Change of Authorization involves creating a server group containing the ISE RADIUS servers, then using that server group in remote access VPN configuration profiles (tunnels).

Procedure

Step 1 Configure the RADIUS AAA server group for the ISE servers.

The following procedure explains the minimum configuration. You can adjust other settings for the group as desired. Most settings have defaults appropriate for most networks. See the general configuration guide for complete information on configuring RADIUS AAA server groups.

a) Choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **AAA Server Groups**.
b) Click **Add** in the **AAA Server Groups** area.
c) Enter a name for the group in the **AAA Server Group** field.
d) Choose the RADIUS server type from the **Protocol** drop-down list.
e) Select **Enable interim accounting update** and **Update Interval** to enable the periodic generation of RADIUS interim-accounting-update messages.

ISE maintains a directory of active sessions based on the accounting records that it receives from NAS devices like the ASA. However, if ISE does not receive any indication that the session is still active (accounting message or posture transactions) for a period of 5 days, it will remove the session record from its database. To ensure that long-lived VPN connections are not removed, configure the group to send periodic interim-accounting-update messages to ISE for all active sessions.

You can change the interval, in hours, for sending these updates. The default is 24 hours, the range is 1 to 120.

f) Select **Enable dynamic authorization**.

This option enables the RADIUS Dynamic Authorization (ISE Change of Authorization, CoA) services for the AAA server group. When you use the server group in a VPN tunnel, the RADIUS server group will be registered for CoA notification and the ASA will listen to the port for the CoA policy updates from ISE. Do not change the port (1700) unless your ISE server is configured to use a different port. The valid range is 1024 to 65535.

g) If you do not want to use ISE for authentication, select **Use authorization only mode**.

This option indicates that when this server group is used for authorization, the RADIUS Access Request message will be built as an “Authorize Only” request as opposed to the configured password methods defined for the AAA server. If you do configure a common password for the RADIUS server, it will be ignored.

For example, you would use authorize-only mode if you want to use certificates for authentication rather than this server group. You would still use this server group for authorization and accounting in the VPN tunnel.

h) Click **OK** to save the server group.
i) With the server group selected, click **Add** in the **Servers in selected group** list to add the ISE RADIUS servers to the group.

Following are the key attributes. You can adjust the defaults for other settings as needed.

- **Interface Name**—The interface through which you can reach the ISE server.
- **Server Name or IP Address**—The ISE server's hostname or IP address.

- (Optional.) **Server Secret Key**—The key for encrypting the connection. If you do not configure a key, the connection is not encrypted (plain text). The key is a case-sensitive, alphanumeric string of up to 127 characters that is the same value as the key on the RADIUS server.

j) Click **OK** to add the server to the group.

Add any additional ISE servers to the server group.

Step 2 Update the configuration profiles for remote access VPN to use the ISE server group.

The following steps cover the ISE-related configuration options only. There are other options you need to configure to create a functional remote access VPN. Follow the instructions elsewhere in this guide for implementing remote access VPN.

a) Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access**AnyConnect Client **Connection Profiles**.
b) In the **Connection Profiles** table, add or edit a profile.
c) On the **Basic** page, configure the authentication method.

- If you are using the ISE servers for authentication, select **AAA** for **Authentication** > **Method**, then select the ISE AAA server group.
- If you configured the ISE server group for authorization only, select a different authentication method, for example, **Certificate**.

d) On the **Advanced** > **Authorization** page, select the ISE server group for **Authorization Server Group**.
e) On the **Advanced** > **Accounting** page, select the ISE server group.
f) Click **OK** to save your changes.