CHAPTER 28

VPN Policy Object Reference

There are several policy objects that you use exclusively with VPN-related policies. This reference explains the configuration of these policy objects.

This chapter contains the following topics:

ASA Group Policies Dialog Box

Use the Add or Edit ASA Group Policies dialog box to create, copy, and edit an ASA user group policies object.

ASA group policies are configured on ASA security appliances in Easy VPN topologies, IPSec VPNs, and SSL VPNs. When you configure an Easy VPN, IPSec VPN or SSL VPN connection, you must create group policies to which remote clients will belong. A user group policy is a set of user-oriented attribute/value pairs for SSL VPN connections that are stored either internally (locally) on the device or externally on a AAA server. The tunnel group uses a user group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users rather than having to specify each attribute individually for each user.

Note You must select the technology (Easy VPN/IPSec VPN, SSL VPN, or Easy VPN/IPSec VPN and SSL VPN) for which you are creating the object. If you are editing an existing ASA group policies object, the technology is already selected, and you cannot change it. Depending on the selected technology, the appropriate settings are available for configuration.

Navigation Path

Select **ASA Group Policies** in the Policy Object Manager Window, page 6-3. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Tip You can also access this dialog box from the **Remote Access VPN > Group Policies** policy.

Related Topics

- Configuring Connection Profiles (ASA), page 26-18
- Creating Group Policies (ASA), page 26-31

Field Reference

Table 28-1 Add or Edit ASA Group Policies Dialog Box, including Technology Settings

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>Name</td><td>The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.</td></tr>
<tr><td>Description</td><td>An optional description of the object.</td></tr>
<tr><td colspan="2"><b>Settings Pane</b>
The body of the dialog box is a pane with a table of contents on the left and settings related to the item selected in the table of contents on the right.
You must first configure technology settings, then you can select items from the table of contents on the left and configure the options you require. Your selections on the Technology page control which options are available on these pages and in the table of contents.
The top folders in the table of contents represent the VPN technologies or other settings that you can configure, and are explained next.</td></tr>
</table>

Table 28-1 Add or Edit ASA Group Policies Dialog Box, including Technology Settings

Element	Description
Technology settings	These settings control what you can define in the group policy: • **Group Policy Type**—Whether you are storing the group policy on the ASA device itself (**Internal**) or on a AAA server (**External**). You cannot change this option when editing an object. If you select **External**, the only attributes you can configure are the name of the AAA server group object that identifies the AAA server and its password. • **Technology**—The types of VPN for which this object defines group policies. You cannot change this option when editing an object. You can configure settings for Easy VPN/IPSec VPN, SSL VPN, or both. The default is both. • **External Server Group**—If you are storing the group policy attributes on an external AAA server, specify the AAA server group that will be used for authentication. Click **Select** to select the object from a list or to create a new object. After you select an external server group, the **Password** and **Confirm** fields become active. Enter the alphanumeric password to use for authenticating with the server in both fields. The password can be a maximum of 128 characters; spaces are not allowed.
DNS/WINS	The DNS and WINS servers and the domain name that should be pushed to clients associated with the group. See ASA Group Policies DNS/WINS Settings, page 28-18.
Split Tunneling	Settings to allow a remote client to conditionally direct encrypted packets through a secure tunnel to the central site and simultaneously allow clear text tunnels to the Internet through a network interface. See ASA Group Policies Split Tunneling Settings, page 28-19.
Easy VPN/IPSec VPN	Settings for Easy VPN and remote access IPSec VPNs: • Client Configuration—The Cisco client parameters for the group. See ASA Group Policies Client Configuration Settings, page 28-4. • Client Firewall Attributes—The firewall settings for VPN clients for the group. See ASA Group Policies Client Firewall Attributes, page 28-5. • Hardware Client Attributes—The VPN 3002 Hardware Client settings for the group. See ASA Group Policies Hardware Client Attributes, page 28-7. • IPSec—The tunneling protocols, filters, connection settings, and servers for the group. See ASA Group Policies IPSec Settings, page 28-9.

Table 28-1 Add or Edit ASA Group Policies Dialog Box, including Technology Settings

Element	Description
SSL VPN	Settings for SSL VPN: • Clientless—Settings for the clientless mode of access to the corporate network in an SSL VPN. See ASA Group Policies SSL VPN Clientless Settings, page 28-11. • Full Client—Settings for the full client mode of access to the corporate network in an SSL VPN. See ASA Group Policies SSL VPN Full Client Settings, page 28-13. • Settings—The general settings that are required for clientless/port forwarding in an SSL VPN. See ASA Group Policies SSL VPN Settings, page 28-15.
Connection Settings	The connection settings for the group, such as the session and idle timeouts, including the banner text. See ASA Group Policies Connection Settings, page 28-20.

ASA Group Policies Client Configuration Settings

Use the Client Configuration settings page to configure the Cisco client parameters for the ASA group policy for Easy VPN or remote access VPN.

Navigation Path

Select **Easy VPN/IPSec VPN > Client Configuration** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-2 ASA Group Policies Client Configuration Settings

Element	Description
Store Password on Client System	Whether to allow users to store a password on their local systems. Enable this feature only if you are certain that the local systems will be in secure sites.
Enable IPsec over UDP UDP Port	Whether to allow a Cisco VPN client or hardware client to connect using UDP to a security appliance that is running NAT. If you select this option, specify the UDP port number within the range of 4001-49151. In IPsec negotiations, the security appliance listens on the configured port and forwards UDP traffic for that port even if other filter rules drop UDP traffic. **Note** The Cisco VPN client must also be configured to use IPsec over UDP, which is configured by default on certain devices.

Table 28-2 ASA Group Policies Client Configuration Settings (Continued)

Element	Description
IPsec Backup Servers Servers List	Specify the backup server configuration: • **Keep Client Configuration**—The security appliance sends no backup server information to the client. The client uses its own backup server list, if configured. This is the default. • **Clear Client Configuration**—The client uses no backup servers. The security appliance pushes a null server list. • **Use Specified Backup Servers**—Use the backup servers you specify in the servers list. Enter the IP addresses of the servers, or the name of a network/host object. Click **Select** to select the object from a list or to create a new object. You can configure backup servers either on the client or on the primary security appliance. If you configure backup servers on the security appliance, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.

ASA Group Policies Client Firewall Attributes

Use the Client Firewall Attributes settings to configure the firewall settings for VPN clients for the ASA group policy for Easy VPN or IPSec VPN. Only VPN clients running Microsoft Windows can use these firewall settings.

Navigation Path

Select **Easy VPN/IPSec VPN > Client Firewall Attributes** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-3 ASA Group Policies Client Firewall Attributes

Element	Description
Firewall Mode	The firewall requirements for client systems for the group: • **No Firewall**—Do not use a firewall. You cannot configure any other options on the page. • **Firewall Required**—All users in this group must use the designated firewall. The security appliance drops any session that attempts to connect without the designated firewall installed and running. In this case, the security appliance notifies the VPN client that its firewall configuration does not match. **Note** Make sure the group does not include any clients other than Windows VPN Clients. Any other clients in the group (including VPN 3002 Hardware Clients) are unable to connect if you require a client firewall. • **Firewall Optional**—Users can use a firewall but it is not required. This option allows all 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 firewalls and others do not. For example, you might have clients with systems that do not run Microsoft windows, or your clients have not all had the opportunity to install firewall software.
Firewall Type	The type of firewall that you are making required or optional. The list shows all of the supported firewall software, which includes software from Cisco, Network ICE, Sygate, and Zone Labs. • If you select Custom Firewall, you must fill in the fields in the Custom Firewall group. You also need to configure the policy source; select options only if they are supported by the vendor. • Some firewall types require you to specify the source of the policy implemented by the firewall.

Table 28-3 ASA Group Policies Client Firewall Attributes (Continued)

Element	Description
Policy Source	Some types of firewall allow you to configure where the client firewall should obtain its policies: • Get Policy From Remote Firewall—The policy is configured in the client firewall application. This is how most client firewalls work. • Use Specified Policy—The policy you specify should be pushed to the client firewall application, which should use your policy. You must enter the name of an extended access control list policy object, or click **Select** to select one from a list or to create a new one, in both in the **Inbound Traffic Policy** and **Outbound Traffic Policy** fields.
Custom Firewall	The attributes that define the required or optional firewall if you select custom firewall as the firewall type: • Vendor ID—The number that identifies the vendor of the custom firewall. Values are 1-255. • Product ID—The number that identifies the product or model of the custom firewall. Values are 1-32 or 255. Multiple ranges are allowed, for example, 4-12, 24-32. Use 255 for all supported products. • Description—An optional description of the custom firewall, for example, the name of the vendor and product.

ASA Group Policies Hardware Client Attributes

Use the Hardware Client Attributes settings to configure the VPN 3002 Hardware Client settings for the ASA group policy in an Easy VPN or IPSec VPN.

Navigation Path

Select **Easy VPN/IPSec VPN > Hardware Client Attributes** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-4 ASA Group Policies Hardware Client Attributes

Element	Description
Require Interactive Client Authentication	Whether to enable secure unit authentication, which provides additional security by requiring VPN hardware clients to authenticate with a username and password each time that the client initiates a tunnel. The hardware client does not have a saved username and password. **Note** Secure unit authentication requires that you have an authentication server group configured for the tunnel group the hardware clients use. If you require secure unit authentication on the primary security appliance, be sure to configure it on any backup servers as well.
Require Individual User Authentication	Whether to require that individual users behind a hardware client authenticate to gain access to the network across the tunnel. Individual users authenticate according to the order of authentication servers that you configure. If you do not select this option, the security appliance allows inheritance of a value for user authentication from another group policy.
Enable Cisco IP Phone Bypass	Whether to allow IP phones behind hardware clients to connect without undergoing a user authentication processes. Secure unit authentication remains in effect for other users.
Enable LEAP Bypass	Whether to enable Lightweight Extensible Authentication Protocol (LEAP) packets from wireless devices behind a VPN hardware client to travel across a VPN tunnel prior to user authentication. This action lets workstations using Cisco wireless access point devices establish LEAP authentication and then authenticate again per user authentication. **Note** LEAP is an 802.1X wireless authentication method that implements mutual authentication between a wireless client on one side of a connection and a RADIUS server on the other side. The credentials used for authentication, including a password, are always encrypted before they are transmitted over the wireless medium.
Allow Network Extension Mode	Whether to enable network extension mode for hardware clients. Network extension mode lets hardware clients present a single, routable network to the remote private network over the VPN tunnel. IPsec encapsulates all traffic from the private network behind the hardware client to networks behind the security appliance. PAT does not apply. Devices behind the security appliance have direct access to devices on the private network behind the hardware client over the tunnel, and only over the tunnel, and vice versa. The hardware client must initiate the tunnel, but after the tunnel is up, either side can initiate data exchange.
Idle Timeout Mode	How to handle periods of inactivity from individual clients: • Specified Timeout—If there is no communication activity by a user behind a hardware client for the number of minutes you specify, the security appliance terminates the client's access. Values are 1-35791394 minutes. • Unlimited Timeout—User sessions are not terminated due to inactivity.

ASA Group Policies IPSec Settings

Use the IPsec settings to specify tunneling protocols, filters, connection settings, and servers for the ASA group policy for Easy VPN or IPSec VPN. This creates security associations that govern authentication, encryption, encapsulation, and key management.

Navigation Path

Select **Easy VPN/IPSec VPN > IPsec** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-5 ASA Group Policies IPSec Settings

Element	Description
Enable Re-Authentication on IKE Re-Key	Whether the security appliance should prompt the user to enter a username and password during initial Phase 1 IKE negotiation and also prompt for user authentication whenever an IKE rekey occurs, providing additional security. Reauthentication fails if no user is at the other end of the connection.
Enable IPsec Compression	Whether to enable data compression, which speeds up transmission rates for remote dial-in users connecting with modems. ⚠ **Caution** Data compression increases the memory requirement and CPU usage for each user session and consequently decreases the overall throughput of the security appliance. For this reason, it is recommended that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users and enable compression only for them.
Enable Perfect Forward Secrecy (PFS)	Whether to enable the use of Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. In IPsec negotiations, PFS ensures that each new cryptographic key is unrelated to any previous key.
Tunnel Group Lock	Tunnel group lock restricts users by checking if the group configured in the VPN client is the same as the tunnel group to which the user is assigned. If it is not, the security appliance prevents the user from connecting. If you do not specify a tunnel name, the security appliance authenticates users without regard to the assigned group. Group locking is disabled by default.

Table 28-5 ASA Group Policies IPSec Settings (Continued)

Element	Description
Client Access Rules table	The access rules for clients. These rules control which types of clients are denied access, if any. You can have up to 25 rules, and combined they are limited to 255 characters. **Tip** If you define any rule, an implicit deny all rule is added. Thus, if a client matches no permit rule, the client is denied access. If you create rules, ensure that you have permit rules for all allowed clients. You can use * as a wildcard to match partial strings. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type or version is the rule that applies. If a lower priority rule contradicts, the security appliance ignores it. • To add a rule, click the **Add Row** button to open the Add or Edit Client Access Rules Dialog Box, page 28-10. • To edit a rule, select it and click the **Edit Row** button. • To delete a rule, select it and click the **Delete** button.

Add or Edit Client Access Rules Dialog Box

Use the Client Access Rules dialog box to create or edit the priority, action, VPN client type and VPN client version for a client access rule.

Navigation Path

From ASA Group Policies IPSec Settings, page 28-9, click the **Add Row** button beneath the Client Access Rules table, or select a rule and click the **Edit Row** button.

Field Reference

Table 28-6 Add or Edit Client Access Rules Dialog Box

Element	Description
Priority	The relative priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type or version is the rule that applies. If a lower priority rule contradicts, the security appliance ignores it. Values are 1-65535.
Action	Whether this rule permits or denies traffic access to the client.

Table 28-6 Add or Edit Client Access Rules Dialog Box (Continued)

Element	Description
VPN Client Type VPN Client Version	The type or version of VPN client to which this rule applies. Spaces are allowed. You can use * as a wildcard to match zero or more characters. You can use n/a for clients that do not send their type or version. The strings you enter in these fields must match the strings displayed using the **show vpn-sessiondb remote** command on the ASA device. Following are some examples, where priority, permit/deny, type, and version are shown in order: • **3 Deny * version 3.*** is a priority 3 rule that denies all client types with software version 3.x. • **5 Permit VPN3002 *** is a priority 5 rule that allows VPN3002 clients of all software versions. • **255 Permit * *** is a priority 255 rule that allows all types and versions of clients. This is useful if you are only trying to deny specific types of clients without wanting to create permit rules for all the other types.

ASA Group Policies SSL VPN Clientless Settings

Use the Clientless settings to configure the clientless mode of access to the corporate network in an SSL VPN for the ASA group policy object.

When a user connects to the SSL VPN in clientless mode, the user logs into the SSL VPN portal page. From the portal page, the user can access all available HTTP sites, access web e-mail, and browse Common Internet File System (CIFS) file servers, depending on how you configure the portal.

Navigation Path

Select **SSL VPN > Clientless** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-7 ASA Group Policies SSL VPN Clientless Settings

Element	Description
Portal Page Websites	The name of the SSL VPN bookmarks policy object that includes the web site URLs to display on the portal page. These web sites help users access desired resources. Enter the name of the object or click **Select** to select it from a list or to create a new object.
Allow Users to Enter Websites	Whether to allow the remote user to enter web site URLs directly into the browser. If you do not select this option, the user can access only those URLs included on the portal.
Enable File Server Browsing	Whether to allow the remote user to browse for file shares on the CIFS file servers.

Table 28-7 ASA Group Policies SSL VPN Clientless Settings (Continued)

Element	Description
Enable File Server Entry	Whether to allow the remote user to locate file shares on the CIFS file servers by entering the names of the file shares.
Enable Hidden Shares	Whether to make hidden CIFS shares visible, and thus accessible, to users.
HTTP Proxy	The type of access you want to allow to the external HTTP proxy server to which the security appliance forwards HTTP connections. You can enable access, disable access, or select Auto Start, which starts the proxy automatically upon user login.
Filter ACL	The name of the web type access control list policy object to use to restrict user access to the SSL VPN. Enter the name of the object or click **Select** to select it from a list or to create a new object.
Enable ActiveX Relay	Whether to enable ActiveX relay, which allows users to start ActiveX programs from the portal page. This allows users to start Microsoft Office applications from the web browser and upload and download Office documents.
UNIX Authentication Group ID	The UNIX authentication group ID.
UNIX Authentication User ID	The UNIX authentication user ID.
Smart Tunnel	The name of the smart tunnel list policy object assigned to this group. Click **Select** to select it from a list or to create a new object. A smart tunnel is a connection between a Winsock 2, TCP-based application and a private site. The connection uses a clientless (browser-based) SSL VPN session with the security appliance as the pathway, and the security appliance as a proxy server. Thus, smart tunnels do not require users to have administrator privileges. For more information, see Configuring SSL VPN Smart Tunnels for ASA Devices, page 26-71.
Auto Start Smart Tunnel	Whether to start smart tunnel access automatically upon user login. If you do not select this option, the user must start the tunnel manually through the Application Access tools on the portal page. Auto sign-on supports only applications that use HTTP and HTTPS using the Microsoft WININET library on a Microsoft Windows operating system. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.
Port Forwarding List	The name of the port forwarding list policy object assigned to this group. Port forwarding lists contain the set of applications that users of clientless SSL VPN sessions can access over forwarded TCP ports. Enter the name of the object or click **Select** to select it from a list or to create a new object.

Table 28-7 ASA Group Policies SSL VPN Clientless Settings (Continued)

Element	Description
Auto Start Port Forwarding	Whether to start port forwarding automatically upon user login.
Port Forwarding Applet Name	The application name or short description to display on the Port Forwarding Java applet screen on the portal, up to 64 characters. This is the name of the applet users will download to act as a TCP proxy on the client machine for the services configured on the SSL VPN gateway.

ASA Group Policies SSL VPN Full Client Settings

Use the Full Client settings to configure the full client mode of access to the corporate network in an SSL VPN for the ASA group policy object.

Full client mode enables access to the corporate network completely over an SSL VPN tunnel. In full client access mode, the tunnel connection is determined by the group policy configuration. The full client software, SSL VPN Client (SVC) or AnyConnect, is downloaded to the remote client, so that a tunnel connection is established when the remote user logs in to the SSL VPN gateway.

Tip To enable full client access, you must configure the **Remote Access VPN > SSL VPN > Other Settings** policy on the device to identify AnyConnect image packages to install on the device. The images must be on the device so that users can download them. For more information, see Understanding SSL VPN Client Settings, page 26-56 and Add and Edit File Object Dialog Boxes, page 28-24.

Navigation Path

Select **SSL VPN > Full Client** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-8 ASA Group Policies SSL VPN Full Client Settings

Element	Description
Enable Full Client	Whether to enable full client mode.
Mode	The mode in which to operate the SSL VPN: • **Use Other Access Modes if AnyConnect Client Download Fails**—If the full client fails to download to the remote user, allow the user to make clientless or thin client access to the VPN. • **Full Client Only**—Prohibit clientless or thin client access. The user must have the full client installed and functional to connect to the VPN.
Keep AnyConnect Client on Client System	Whether to leave the AnyConnect client installed on the client system after the client disconnects. If you do not leave the client installed, it must be download each time the user connects to the gateway.

Table 28-8 ASA Group Policies SSL VPN Full Client Settings (Continued)

Element	Description
Enable Compression	Whether to enable data compression, which speeds up transmission rates for remote dial-in users connecting with modems. **Caution** Data compression increases the memory requirement and CPU usage for each user session and consequently decreases the overall throughput of the security appliance. For this reason, it is recommended that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users and enable compression only for them.
Enable Keepalive Messages	Whether to exchange keepalive messages between peers to demonstrate that they are available to send and receive data in the tunnel. Keepalive messages transmit at set intervals, and any disruption in that interval results in the creation of a new tunnel using a backup device. If you select this option, enter the time interval (in seconds) that the remote client waits between sending IKE keepalive packets in the **Interval** field.
Client Dead Peer Detection Timeout (sec)	The time interval, in seconds, that the Dead Peer Detection (DPD) timer is reset each time a packet is received over the SSL VPN tunnel from the remote user. DPD is used to send keepalive messages between peer devices only when no incoming traffic is received and outbound traffic needs to be sent.
Gateway Dead Peer Detection Timeout (sec)	The time interval, in seconds, that the Dead Peer Detection (DPD) timer is reset each time a packet is received over the SSL VPN tunnel from the gateway.
Key Renegotiation Method	The method by which the tunnel key is refreshed for the remote user group client: • **Disabled**—Disables the tunnel key refresh. • **Use Existing Tunnel**—Renegotiates the SSL tunnel connection. • **Create New Tunnel—**Initiates a new tunnel connection. Enter the time interval (in minutes) between the tunnel refresh cycles in the **Interval** field.
Enable Datagram Transport Layer Security	Whether to enable Datagram Transport Layer Security (DTLS) connections for the group. Enabling 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 some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Table 28-8 ASA Group Policies SSL VPN Full Client Settings (Continued)

Element	Description
AnyConnect Module	The module that the AnyConnect client needs to enable optional features. • **vpngina**—Select this module to enable the Start Before Logon (SBL) feature, which is a graphical identification and authentication (GINA) module for the AnyConnect client VPN connection. • If other options are listed, see the release notes for the Cisco AnyConnect VPN Client for an explanation of the feature.
AnyConnect MTU	The maximum transmission unit (MTU) size for SSL VPN connections established by the Cisco AnyConnect VPN Client.
AnyConnect Profile Name	The name of the AnyConnect profile to use for the group. You must configure this name and relate it to a profile in the **Remote Access VPN > SSL VPN > Other Settings** policy.
Prompt User to Choose Client Time User Has to Choose Default Location	Whether to ask the user to download the client. Enter the number of seconds the user has to make a selection in the **Time User Has to Choose** field. The default is 120 seconds. If you do not select this option, the user is immediately taken to the default location. The user is also taken to the default location after the time to choose expires. • **Web Portal**—The portal page is loaded in the web browser. • **AnyConnect Client**—The AnyConnect client is downloaded.

ASA Group Policies SSL VPN Settings

Use the SSL VPN Settings to configure attributes that are required for clientless and port forwarding (thin client) access modes to work, including auto signon rules for user access to servers. Auto Signon configures the security appliance to automatically pass SSL VPN user login credentials (username and password) on to internal servers. You can configure multiple auto signon rules.

Navigation Path

Select **SSL VPN > Settings** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-9 ASA Group Policies SSL VPN Settings

Element	Description
Home Page	The URL of the SSL VPN home page. The page is displayed when users log into the VPN. If you do not enter a URL, no home page is displayed.
Authentication Failure Message	The message to deliver to a remote user who successfully logs into the VPN but has no VPN privileges, and so can do nothing. The default message is: "Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information."

Table 28-9 ASA Group Policies SSL VPN Settings (Continued)

Element	Description
Minimum Keepalive Object Size (kilobytes)	The minimum size (in kilobytes) of an IKE keepalive packet that can be stored in the cache on the security appliance.
Single Sign On Server	The name of the single sign on (SSO) server policy object that identifies the server to use for this group, if any. An SSO server allows users to enter their username and password once and be able to access other server in the network without logging into each of them. If configure an SSO server, also configure the auto signon rules table. Enter the name of the object or click **Select** to select it from a list or to create a new object. For more information, see Add or Edit Single Sign On Server Dialog Boxes, page 28-44.
Enable HTTP Compression	Whether to allow an HTTP compressed object to be cached on the security appliance.
Auto Signon Rules table	If you configure a single sign on server, the auto signon rules table contains the rules that determine which internal servers are provided the user's credentials. Thus, you can provide single sign on for some servers in your network but not others. Each rule is an allow rule, and indicates the IP address, subnet, or Universal Resource Identifier (URI) that identifies the server, and the type of authentication that will be sent to the server when the user tries to access it (either basic HTML, NTLM, FTP, or all of these). The rules are processed in order, top to bottom, and the first match is applied. Therefore, be sure to order the rules correctly using the up and down arrow buttons. If the user accesses a server that is not identified in one of these rules, the user must log into the server to gain access. • To add a rule, click the **Add Row** button to open the Add or Edit Auto Signon Rules Dialog Box, page 28-17. • To edit a rule, select it and click the **Edit Row** button. • To delete a rule, select it and click the **Delete Row** button.
Portal Page Customization	The name of the SSL VPN customization policy object that defines the appearance of the portal web page. The portal page allows the remote user access to all the resources available on the SSL VPN network. If you do not specify an object, the default page appearance is used. Enter the name of the object or click **Select** to select it from a list or to create a new object. For more information, see Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63.

Table 28-9 ASA Group Policies SSL VPN Settings (Continued)

Element	Description
User Storage Location	The location where personalized user information is stored between clientless SSL VPN sessions. If you do not specify a location, information is not stored between sessions. Stored information is encrypted. Enter a file system designation in the following format: **protocol://username:password@host:port/path** Where **protocol** is the protocol of the server, **username** and **password** are a valid user account on the server, and **host** is the name of the server. Also indicate the **port** number (if you do not use the default for the protocol) and directory **path** of the location on the server to use. For example: **cifs://newuser:12345678@anyfiler02a/new_share**
Storage Key	The storage key used to protect data stored between sessions. Spaces are not supported.
Post Max Size	The maximum size allowed for a posted object. The range is 0 through 2147483647 (which is the default). Specify 0 to prevent posting.
Upload Max Size	The maximum size allowed for a uploaded object. The range is 0 through 2147483647 (which is the default). Specify 0 to prevent uploading.
Download Max Size	The maximum size allowed for a downloaded object. The range is 0 through 2147483647 (which is the default). Specify 0 to prevent downloads.

Add or Edit Auto Signon Rules Dialog Box

Use the Add or Edit Auto Signon Rules dialog box to configure the Auto Signon rules that the security appliance uses to pass SSL VPN user login credentials on to an internal server.

Navigation Path

Open the ASA Group Policies SSL VPN Settings, page 28-15, then click **Create**, or select an item in the table and click **Edit**.

Field Reference

Table 28-10 Add or Edit Auto Signon Rules Dialog Box

Element	Description
Allow IP	Select this option to configure an IP address or subnet for the rule. Any server within this subnet is supplied the specified login credentials. • To enter the IP address of a single server, enter the full IP address and use 255.255.255.255 as the subnet mask. • To specify a subnet, enter the network address and subnet mask, for example, IP address 10.100.10.0 mask 255.255.255.0. If you want the appliance to send credentials to any internal server the user tries to access, create rules for all of your internal networks. You might be able to do this with a single rule.
Allow URI	Select this option to configure a Universal Resource Identifier (URI) for the rule. This identifies the internal server based on URI rather than IP address. For example, **https://*.example.com/*** creates a rule for all web pages on any server in the example.com domain. Use the asterisk as a wildcard to apply to zero or more characters.
Authentication Type	The type of credentials that the security appliance will pass on to the servers covered by this rule: Basic HTML, NTLM (NT LAN Manager) authentication, FTP, or all of these methods. The default option is **All**. Use the default unless you want to limit logins to a certain type.

ASA Group Policies DNS/WINS Settings

Use the DNS/WINS settings to define the DNS and WINS servers and the domain name that should be pushed to clients associated with the ASA group policy. These settings apply to Easy VPN, remote access IPSec VPN, and SSL VPN configurations.

Navigation Path

Select **DNS/WINS** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-11 ASA Group Policies DNS/WINS Settings

Element	Description
Primary DNS Server	The IP address of the primary DNS server for the group. Enter the IP address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.
Secondary DNS Server	The IP address of the secondary DNS server for the group. Enter the IP address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.
Primary WINS Server	The IP address of the primary WINS server for the group. Enter the IP address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.

Table 28-11 ASA Group Policies DNS/WINS Settings (Continued)

Element	Description
Secondary WINS Server	The IP address of the primary WINS server for the group. Enter the IP address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.
DHCP Network Scope	The scope of the DHCP network for the group. Enter the IP network address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.
Default Domain	The default domain name for the group. The default, blank, is none.

ASA Group Policies Split Tunneling Settings

Use the Split Tunneling settings to configure a secure tunnel to the central site and simultaneous clear text tunnels to the Internet. These settings apply to Easy VPN, remote access IPSec VPN, and SSL VPN configurations.

Split tunneling lets a remote client conditionally direct packets over an IPsec or SSL VPN tunnel in encrypted form or to a network interface in clear text form. With split tunneling enabled, packets not bound for destinations on the other side of the tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. The split tunneling policy is applied to specific networks.

Tip For optimum security, we recommend that you not enable split tunneling.

Navigation Path

Select **Split Tunneling** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-12 ASA Group Policies Split Tunneling Settings

Element	Description
DNS Names	A list of domain names to be resolved through the split tunnel. All other names are resolved using the public DNS server. If you do not enter a list, the list is inherited from the default group policy. Separate multiple entries with spaces or commas. The entire string can be a maximum of 255 characters.
Tunnel Option	The policy you want to enable for split tunneling: • Disabled—(Default) No traffic goes in the clear or to any other destination than the security appliance. Remote users reach networks through the corporate network and do not have access to local networks. • Tunnel Specified Traffic—Tunnel all traffic from or to the networks permitted in the network ACL. Traffic to all other addresses travels in the clear and is routed by the remote user's Internet service provider. • Exclude Specified Traffic—Traffic goes in the clear from and to the networks permitted in the network ACL. This 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. This option applies only to the Cisco VPN Client.
Networks	The name of a standard access control list policy object that identifies the networks that require traffic to travel across the tunnel and those that do not require tunneling. How permit and deny are interpreted depends on your selection for **Tunnel Option**. Enter the name of the object, or click **Select** to select it from a list or to create a new object. If you do not specify an ACL, the network list is inherited from the default group policy.

ASA Group Policies Connection Settings

Use the Connection Settings to configure the connection characteristics for the ASA group policy, including access control and session timeouts. These settings are used for Easy VPN, remote access VPN, or SSL VPN sessions.

Navigation Path

Select **Connection Settings** from the table of contents in the ASA Group Policies Dialog Box, page 28-1.

Field Reference

Table 28-13 ASA Group Policies Connection Settings

Element	Description
Filter ACL	The name of the extended access control list (ACL) policy object to use to restrict user access to the VPN. Enter the name of the object or click **Select** to select it from a list or to create a new object.
Banner Text	The banner, or welcome text, to display on remote clients when they connect to the VPN. You can enter up to 500 characters.
Access hours	The name of a time range policy object that specifies the times that users are allowed to access the VPN. If you do not specify a time range, users can access the VPN at all times. Specify a time range if you want to limit access to the network to certain hours, such as the typical work days and work hours for your organization. Enter the name of the object or click **Select** to select it from a list or to create a new object. For more information, see Configuring Time Range Objects, page 6-53.
Max Simultaneous Logins	The number of simultaneous logins a single user is allowed. Values are 0-2147483647. The default is 3. Specify 0 to disable logins and prevent user access.
Max Connection Time	The maximum amount of time a user is allowed to be connected to the VPN. Select one of the following: • Specified Connection time—Use the maximum time value that you enter. Values are 1-35791394 minutes. After the time is exceeded, the security appliance closes the connection. • Unlimited Connection time—The security appliance does not close connections based on connection time.
Idle Timeout	The amount of time a user is allowed to be connected to the VPN while the connection is idle, that is, there is no communication activity. Select one of the following: • Specified Timeout—Use the time out value you enter. Values are 1-4473924 minutes. When the idle time is exceeded, the security appliance closes the connection. The default is 30 minutes. • Unlimited Timeout—The security appliance does not close idle connections.

Add or Edit Secure Desktop Configuration Dialog Box

Use the Add or Edit Cisco Secure Desktop Configuration dialog box to create, copy, and edit Cisco Secure Desktop Configuration objects for IOS routers. You can configure the settings required for Windows clients who are connecting from different location types, enable or restrict web browsing and file access for Windows CE clients, and configure the cache cleaner for Macintosh and Linux clients.

Cisco Secure Desktop (CSD) secures network endpoints by providing a reliable means of eliminating all traces of sensitive data by providing a single, secure location for session activity and removal on the client system.

This policy object uses the Secure Desktop Manager application to configure the settings. For an example of configuring settings, see *Cisco Secure Desktop on IOS Configuration Example Using SDM* at http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa7b.shtml. The first part of the configuration example explains setting up SDM, which you can ignore. Instead, look for the sections that describe setting up Windows locations midway through the example. The screen shots will help you identify when you are looking at CSD configuration.

Navigation Path

Select **Tools > Policy Object Manager**, then select **Cisco Secure Desktop (Router)** from the Object Type Selector. Right-click inside the work area and select **New Object**, or right-click a row and select **Edit Object**.

Related Topics

- Creating Cisco Secure Desktop Configuration Objects, page 26-61
- Policy Object Manager Window, page 6-3

Field Reference

Table 28-14 Add or Edit Secure Desktop Configuration Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object (up to 1024 characters).
Windows Location Settings	
Windows Locations	The names of the locations that you want to configure for Windows clients connecting from specific locations, such as Work, Home, or Insecure. When you create a location, an item for the location is added to the table of contents, where you can select the settings folders related to the location and configure its properties. The settings include a definition of how to determine if a client is connecting from that particular location. For each location you want to configure, enter its name in the **Location to Add** field and click **Add** to move it to the **Locations** list. You can reorder the locations using the Move Up/Move Down buttons. CSD checks locations in the order listed in this dialog box, and grants privileges to client PCs based on the first location definition they match. You can create a default location, such as Insecure, as the final location and configure the strictest security for it. For more information, see Creating Cisco Secure Desktop Configuration Objects, page 26-61.
Close all open browser windows after installation	Whether to close all the open browser windows after installing the Secure Desktop application.

Table 28-14 Add or Edit Secure Desktop Configuration Dialog Box (Continued)

Element	Description
VPN Feature Policy	Select the check boxes to enable these features if installation or location matching fails: • Web Browsing • File Access • Port Forwarding • Full Tunneling
Windows CE	
VPN Feature Policy	The Windows CE options enable you to configure a VPN feature policy to enable or restrict web browsing and remote server file access for remote clients running Microsoft Windows CE. You cannot configure locations for these clients.
Mac and Linux Cache Cleaner	
Launch Cleanup Upon Global Timeout	Whether to set a global timeout after which CSD launches the cache cleaner. Select a timeout (the default is 30 minutes), and select whether to allow the user to reset the timeout value.
Launch Cleanup Upon Exiting of Browser	Whether to start the cache cleaner when the user closes all web browser windows.
Enable Canceling of Cleaning	Whether to allow the remote user to cancel the cleaning of the cache.
Secure Delete	The number of passes for CSD to perform a secure cleanup. The default is 1 pass. CSD encrypts and writes the cache to the remote client's disk. Upon termination of the Secure Desktop, CSD converts all bits occupied by the cache to all 0's, then to all 1's, and then to randomized 0's and 1's.
Enable Web Browsing if Mac or Linux Installation Fails	Whether to allow web browsing (but not other remote access features) if the cache cleaner installation fails.
VPN Feature Policy	Whether to allow web browsing, remote server file access, and port forwarding for Macintosh and Linux clients. Port forwarding permits the use of the Secure Desktop to connect a client application installed on the local PC to the TCP/IP port of a peer application on a remote server.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.

Credentials Dialog Box

Use the Credentials dialog box to create, copy and edit Credential objects.

Credential objects are used in Easy VPN configuration during IKE Extended Authentication (Xauth) when authenticating user access to the network and network services. When negotiating tunnel parameters for establishing IPsec tunnels in an Easy VPN configuration, Xauth identifies the user who requests the IPsec connection. If the VPN server is configured for Xauth, the client waits for a "username/password" challenge after the IKE SA has been established. When the end user responds to the challenge, the response is forwarded to the IPsec peers for an additional level of authentication. You can save the Xauth credentials (username and password) on the device itself so you do not need to enter them manually each time the Easy VPN tunnel is established.

Navigation Path

Select **Tools > Policy Object Manager**, then select **Credentials** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Easy VPN and IKE Extended Authentication (Xauth)
- Client Connection Characteristics Page, page 24-15
- Policy Object Manager Window, page 6-3

Field Reference

Table 28-15 Credentials Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object (up to 1024 characters).
Username	The name that will be used to identify the user during Xauth authentication.
Password Confirm	The password for the user, entered in both fields. The password must be alphanumeric and a maximum of 128 characters. Spaces are not allowed.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add and Edit File Object Dialog Boxes

Use the Add and Edit File Object dialog boxes to create, copy, and edit file objects. File objects represent files that are used in device configurations, typically for remote access VPN policies and policy objects. Such files include Anyconnect client profile and image files, image (graphic) files, plug-in jar files, and Cisco Secure Desktop package files.

Tip Before you can add a file to a file object, you must copy the file to the Security Manager server. You cannot select files from a network server or your workstation. Do not copy the file directly to the file repository.

When you create a file object, Security Manager makes a copy of the file in its storage system. These files are backed up whenever you create a backup of the Security Manager database, and they are restored if you restore the database. When you deploy configurations that specify a file object, the associated file is download to the device in the appropriate directory.

After you create a file object, you typically should not edit it. If you need to replace the file, edit the file object to select the new file, or create a new file object. If the file is editable, you can edit the file object to identify the file's location in the file repository, and use the desired editor to open and edit the file outside of Security Manager. The file repository is the **CSCOpx\MDC\FileRepository** folder in the installation directory (typically, C:\Program Files). The files are organized in subfolders named for the file type.

When you delete a file object, the associated file is not deleted from the file repository.

Navigation Path

Select **Tools > Policy Object Manager**, then select **File Objects** from the Object Type Selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Understanding and Managing SSL VPN Support Files, page 26-5
- Configuring SSL VPN Client Settings, page 26-57
- Defining Browser Plug-ins, page 26-55
- Configuring Cisco Secure Desktop Policies on ASA Devices, page 26-26
- SSL VPN Customization Dialog Box—Informational Panel, page 28-56
- SSL VPN Customization Dialog Box—Title Panel, page 28-52

Field Reference

Table 28-16 Add and Edit File Object Dialog Boxes

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6. If you do not enter a name, the name of the file is used for the object name.
Description	An optional description of the object.
File Type	The type of file. If you create the object while configuring a policy, the correct file type is pre-selected. Options are: • Image—For graphic files. • Cisco Secure Desktop Package • Plug-In—For browser plug-in files. • AnyConnect Profile • AnyConnect Image

Table 28-16 Add and Edit File Object Dialog Boxes (Continued)

Element	Description
File	The name and full path of the file. The file must be on the Security Manager server. Click **Browse** to select the file. For file objects that you are editing, the path indicates the location in the Security Manager file repository. **Tip** Security Manager comes with a number of files that you can use with SSL VPN configurations. If you are creating a file object for Anyconnect images or profiles, Cisco Secure Desktop clients, or plug-ins, you can find some files in the **C:\Program Files\CSCOpx\objects\sslvpn** folder.
File Name on Device	The file name you want to use when the file is downloaded to the device when you deploy policies. The default is to use the same file name as the original file. If the object was created by discovering policies from the device, this field uses the original name of the file as it existed on the device. This might not be the same name as it exists on the Security Manager server if the original name duplicated existing file names on the server.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.

Add or Edit IKE Proposal Dialog Box

Use the IKE Proposal dialog box to create, copy, and edit an IKE proposal object.

Internet Key Exchange (IKE) proposal objects contain the parameters required for IKE proposals when defining remote access and site-to-site VPN policies. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes security associations (SAs) for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. For more information about IKE proposals, see the following topics:

- Understanding IKE, page 22-1
- Deciding Which Encryption Algorithm to Use, page 22-2
- Deciding Which Hash Algorithm to Use, page 22-2
- Deciding Which Diffie-Hellman Group to Use, page 22-3
- Deciding Which Authentication Method to Use, page 22-3

Navigation Path

Select **Tools > Policy Object Manager**, then select **IKE Proposals** from the Object Type Selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Tip You can also access this dialog box by selecting a device, selecting **Remote Access VPN > IPSec VPN > IKE Proposal**, and clicking the **Add** or **Edit** button.

Related Topics

- Creating Policy Objects, page 6-6
- Policy Object Manager Window, page 6-3
- Add or Edit IPSec Transform Set Dialog Box, page 28-28

Field Reference

Table 28-17 IKE Proposal Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 128 characters is allowed.
Description	A description of the policy object. A maximum of 1024 characters is allowed.
Priority	The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. Valid values range from 1 to 10000. The lower the number, the higher the priority. If you leave this field blank, Security Manager assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.
Encryption Algorithm	The encryption algorithm used to establish the Phase 1 SA for protecting Phase 2 negotiations: • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Hash Algorithm	The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are: • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.

Table 28-17 IKE Proposal Dialog Box (Continued)

Element	Description
Modulus Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: • 1—Diffie-Hellman Group 1 (768-bit modulus). • 2—Diffie-Hellman Group 2 (1024-bit modulus). • 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). • 7—Diffie-Hellman Group 7 (163-bit elliptical curve field size). • 14—Diffie-Hellman Group 14 (2048-bit modulus, considered good protection for 128-bit keys). • 15—Diffie-Hellman Group 15 (3072-bit modulus, considered good protection for 192-bit keys). • 16—Diffie-Hellman Group 16 (4096-bit modulus, considered good protection for 256-bit keys).
Lifetime	The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 60 to 86400 seconds.
Authentication Method	The method of authentication to use between the two peers: • Preshared Key—Preshared keys allow for a secret key to be shared between two peers and used by IKE during the authentication phase. If one of the participating peers is not configured with the same preshared key, the IKE SA cannot be established. • Certificate—An authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. This method provides non-repudiation of communication between two peers, meaning that it can be proved that the communication actually took place. When you use this authentication method, the peers are configured to obtain digital certificates from a Certification Authority (CA).
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.

Add or Edit IPSec Transform Set Dialog Box

Use the Add or Edit IPSec Transform Set dialog box to create, copy and edit IPSec transform set objects.

You can create IPSec transform set objects for use in IPSec proposals when defining IPSec-protected traffic in site-to-site and remote access VPNs. When you create an IPSec transform set object, you select the mode in which IPSec should operate, as well as define the required encryption and authentication types. Additionally, you can select whether to include compression in the transform set. During IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Two different security protocols are included within the IPSec standard:

- Encapsulating Security Protocol (ESP)—Provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.
- Authentication Header (AH)—Provides authentication and anti-replay services. AH does not provide encryption and has largely been superseded by ESP. AH is IP protocol type 51.

Note We recommend using both encryption and authentication on IPSec tunnels.

Navigation Path

Select **Tools > Policy Object Manager**, then select **IPSec Transform Sets** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- About Transform Sets, page 22-7
- IPsec Proposal Editor Dialog Box (for PIX and ASA Devices), page 27-75
- IPsec Proposal Editor Dialog Box (for IOS Routers and Catalyst 6500/7600 Devices), page 27-77
- Configuring an IPsec Proposal on a Remote Access VPN Server, page 26-39
- Configuring IPsec Proposals, page 22-9
- Configuring an IPsec Proposal for Easy VPN, page 24-5
- Policy Object Manager Window, page 6-3
- Add or Edit IKE Proposal Dialog Box, page 28-26
- Creating Policy Objects, page 6-6

Field Reference

Table 28-18 IPSec Transform Set Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 128 characters is allowed.
Description	A description of the policy object. A maximum of 1024 characters is allowed.

Table 28-18 IPSec Transform Set Dialog Box (Continued)

Element	Description
Mode	The mode in which the IPSec tunnel operates: • Tunnel—Tunnel mode encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet. • Transport—Transport mode encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.
ESP Encryption	The Encapsulating Security Protocol (ESP) encryption algorithm that the transform set should use: • (Blank)—Do not use ESP encryption. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. A 3DES license is required to use this option. • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • ESP-Null—A null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this is typically used for testing purposes only.

Table 28-18 IPSec Transform Set Dialog Box (Continued)

Element	Description
ESP Hash Algorithm AH Hash Algorithm	The ESP or AH hash algorithm to use in the transform set for authentication. The default is to use SHA for ESP authentication and to not use AH authentication. • None—Does not perform ESP or AH authentication. • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5, but requires more processing time. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA, but is less secure. **Note** We recommend using both encryption and authentication on IPSec tunnels.
Compression (IOS devices only.)	Whether to compress the data in the IPSec tunnel using the Lempel-Ziv-Stac (LZS) algorithm.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.

Add and Edit LDAP Attribute Map Dialog Boxes

Use the Add and Edit LDAP (Lightweight Directory Access Protocol) Attribute Map dialog boxes to populate the attribute map with name mappings that translate Cisco LDAP attribute names to custom, user-defined attribute names.

If you are introducing a security appliance to an existing LDAP directory, your existing custom LDAP attribute names and values are probably different from the Cisco attribute names and values. Rather than renaming your existing attributes, you can create LDAP attribute maps that map your custom attribute names and values to Cisco attribute names and values. By using simple string substitution, the security appliance then presents you with only your own custom names and values. You can then bind these attribute maps to LDAP servers or remove them as needed. You can also delete entire attribute maps or remove individual name and value entries.

For more information regarding LDAP support on ASA, PIX, and FWSM devices, see Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-21.

Navigation Path

Select **Tools > Policy Object Manager**, then select **LDAP Attribute Map** from the Object Type selector. Right-click inside the table and select **New Object**, or right-click a row and select **Edit Object**.

Related Topics

- Creating AAA Server Objects, page 6-25
- AAA Server Dialog Box—LDAP Settings, page 6-32

Field Reference

Table 28-19 Add and Edit LDAP Attribute Map Dialog Boxes

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object.
Attribute Map table	The table shows the mapped values. Each entry shows the customer map name, Cisco map name, and the attribute mapping of customer name to Cisco name. • To add a mapping, click the **Add Row** button to open the Add and Edit LDAP Attribute Map Value Dialog Boxes, page 28-32. • To edit a mapping, select it and click the **Edit Row** button. • To delete a mapping, select it and click the **Delete Row** button.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add and Edit LDAP Attribute Map Value Dialog Boxes

Use the Add and Edit LDAP Attribute Map Value dialog boxes to populate the attribute map with value mappings that apply user-defined attribute values to the custom attribute name and to the matching Cisco attribute name and value.

Navigation Path

From the Add and Edit LDAP Attribute Map Dialog Boxes, page 28-31, click the **Add Row** button to add a new mapping, or select a row and click the **Edit Row** button.

Field Reference

Table 28-20 Add and Edit LDAP Attribute Map Value Dialog Boxes

Element	Description
Customer Map Name	The name of your attribute map that relates to the Cisco map.
Cisco Map Name	The Cisco attribute map name you want to map to the customer map name.
Customer to Cisco Map Value table	The mappings of customer names to Cisco names. • To add a mapping, click the **Add Row** button to open the Add and Edit Map Value Dialog Boxes, page 28-33. • To edit a mapping, select it and click the **Edit Row** button. • To delete a mapping, select it and click the **Delete Row** button.

Add and Edit Map Value Dialog Boxes

Use the Add and Edit Map Value dialog boxes to map a customer LDAP attribute value to a Cisco map value. Enter the value from your LDAP map that you want to equate with a Cisco value.

Navigation Path

From the Add and Edit LDAP Attribute Map Value Dialog Boxes, page 28-32, click the **Add Row** button to add a new mapping, or select a row and click the **Edit Row** button.

PKI Enrollment Dialog Box

Use the PKI Enrollment dialog box to view, create, copy, or edit Public-Key Infrastructure (PKI) enrollment objects. A PKI enrollment object represents an external certification authority (CA) server that responds to certificate requests from devices in the network.

You can create PKI enrollment objects to define the properties of a CA server used when devices exchange certificates as part of an IPsec network. When you create a PKI enrollment object, you define a name for the server and the URL for enrollment. You must specify whether the devices you wish to enroll with this server should retrieve the CA server's own certificate using the Simple Certificate Enrollment Process (SCEP) or use a certificate that you have entered manually into the device configuration. You must also select the method of support used by the CA server for revocation checking.

Note You do not have to define enrollment parameters in order to create or import a trustpoint in Security Manager.

In addition, you can optionally define the following:

- Whether the CA server is acting as a Registration Authority (RA) server.
- Enrollment parameters, including retry settings and RSA key pair settings.
- Additional attributes to include in the certificate request.
- The list of trusted CA servers located above this server in the PKI hierarchy.

Navigation Path

Select **Tools > Policy Object Manager**, then select **PKI Enrollments** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Tip You can also open this dialog box from the **Remote Access VPN > Public Key Infrastructure** policy.

Related Topics

- Understanding Public Key Infrastructure Policies, page 22-26
- Prerequisites for Successful PKI Enrollment, page 22-28
- Configuring Public Key Infrastructure Policies, page 26-33
- Configuring Public Key Infrastructure Policies, page 22-31 (site-to-site VPN)
- Policy Object Manager Window, page 6-3

Field Reference

Table 28-21 PKI Enrollment Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object.
CA Information tab	Use this tab to enter settings related to the Certificate Authority server, its certificate, and its level of revocation checking support. For information on the specific settings, see PKI Enrollment Dialog Box—CA Information Tab, page 28-35.
Enrollment Parameters tab	Use this tab to enter settings related to PKI enrollment. For information on the specific settings, see PKI Enrollment Dialog Box—Enrollment Parameters Tab, page 28-39. **Note** You do not have to define enrollment parameters in order to create or import a trustpoint in Security Manager.
Certificate Subject Name tab	Use this tab to enter optional information to be included in the certificate, including subject attributes. For information on the specific settings, see PKI Enrollment Dialog Box—Certificate Subject Name Tab, page 28-40.
Trusted CA Hierarchy tab	Use this tab to define trusted CA servers that are arranged in a hierarchical framework. For information on the specific settings, see PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab, page 28-42.

Table 28-21 PKI Enrollment Dialog Box (Continued)

Element	Description
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

PKI Enrollment Dialog Box—CA Information Tab

Use the CA Information tab of the PKI Enrollment Dialog Box, page 28-33 to:

- Define the name and location of the external certificate authority (CA) server.
- Manually paste the certificate, if known.
- Define the server's level of support for revocation checking.

Navigation Path

Go to the PKI Enrollment Dialog Box, page 28-33 and click the **CA Information** tab.

Related Topics

- PKI Enrollment Dialog Box—Enrollment Parameters Tab, page 28-39
- PKI Enrollment Dialog Box—Certificate Subject Name Tab, page 28-40
- PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab, page 28-42

Field Reference

Table 28-22 PKI Enrollment Dialog Box—CA Information Tab

Element	Description
CA Server Nickname	The name used to identify the CA server in the certificate request. If you leave this field blank, the domain name is used. You must leave this field blank for Verisign CAs. Also, keep the following in mind: • You cannot configure two CA servers with the same name but different URLs on the same device. • The CA name cannot match the name of a trusted CA configured as part of the same PKI enrollment object (as defined on the PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab, page 28-42). • When the device is configured as part of a VPN, do not configure a device-level override that uses the same CA name as that of the CA server used by any of the peers. (This is not a problem when the device and its peers use a tiered PKI hierarchy.)

Table 28-22 PKI Enrollment Dialog Box—CA Information Tab (Continued)

Element	Description
Enrollment Type	The type of enrollment you want to perform. Security Manager completes the enrollment only if you configure URL enrollment. If you select another type, you must complete the enrollment using your own methods. • Self-Signed Certificate (ASA only)—To configure the **enrollment self** command. • Terminal (ASA only)—To configure the **enrollment terminal** command. • URL—To configure the URL for the CA server so that you can complete automatic enrollment. • None—Do not configure any enrollment command.
Enrollment URL	The URL of the CA server to which devices should attempt to enroll. The URL can be in the following formats: • SCEP—Uses an HTTP URL in the form of **http://CA_name:port**, where CA_name is the host DNS name or IP address of the CA server. The port number is mandatory. • TFTP—Uses the format **tftp://certserver/file_specification**. Use this option when you do not have direct access to the CA server. The TFTP server transfers certificate requests and certificates. • Other supported formats include: bootflash, cns, flash, ftp, null, nvram, rcp, scp, system. **Note** If the CA cgi-bin script location at the CA is not the default (/cgi-bin/pkiclient.exe), you must also include the nonstandard script location in the URL, in the form of **http://CA_name:port/script_location**, where script_location is the full path to the CA scripts.

Table 28-22 PKI Enrollment Dialog Box—CA Information Tab (Continued)

Element	Description
CA Certificate Source Fingerprint Certificate (URL enrollment only.)	How to obtain the certificate: • **Retrieve CA Certificate Using SCEP** (the default)—Have the router retrieve the certificate from the CA server using the Simple Certificate Enrollment Process (SCEP). Enter the fingerprint for the CA server in hexadecimal format. If the value you enter does not match the fingerprint on the certificate, the certificate is rejected. Using the fingerprint to verify the authenticity of the CA's certificate helps prevent an unauthorized party from substituting a fake certificate in place of the real one. **Tip** You can obtain the CA's fingerprint by contacting the server directly, or by entering the following address in a web browser: **http://URLHostName/certsrv/mscep/mscep.dll**. Using the fingerprint is supported only on Cisco IOS software releases 12.3(12) or higher, 12.3(14)T or higher, 12.4 or higher, 12.2(33)XNA or higher. • **Enter CA Certificate from CA Server Manually**—Copy and Paste up to three certificates from another device into the **Certificate** field (using your browser's Paste function or the Ctrl-V keyboard shortcut). Each certificate must begin with the word "certificate" and end with the word "quit". Use this option when you want the PKI enrollment object to represent predefined certificates.

Table 28-22 PKI Enrollment Dialog Box—CA Information Tab (Continued)

Element	Description
Revocation Check Support	The type of certificate revocation checking to be performed: • Checking Not Performed—This is the default. The device does not perform any revocation checking, even if a CRL is on the device. • CRL Check Required—The device must check a CRL. If no CRL exists on the device and the device cannot obtain one, certificates are rejected and a tunnel cannot be established. This is the default. • OCSP Check Required—The device must check revocation status from an OCSP server. If this check fails, certificates are rejected. • CRL Check Attempted—The device tries to download the latest CRL from the specified LDAP server. If the download fails, however, certificates are accepted. • OCSP Check Attempted—The device tries to check revocation status from an OCSP server. If this fails, however, certificates are accepted. • CRL or OCSP Check Required—The device first checks for a CRL. If a CRL does not exist or cannot be obtained, the device tries to check revocation status from an OCSP server. If both options fail, certificates are rejected. • OCSP or CRL Check Required—The device first tries to check revocation status from an OCSP server. If this fails, the device checks for a CRL. If both options fail, certificates are rejected. • CRL and OCSP Checks Attempted—The device first checks for a CRL. If a CRL does not exist or cannot be obtained, the device tries to check revocation status from an OCSP server. If both options fail, however, certificates are accepted. • OCSP and CRL Checks Attempted—The device first tries to check revocation status from an OCSP server. If this fails, the device tries to download the latest CRL. If both options fail, however, certificates are accepted.
OCSP Server URL	The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with **http://**
CRL Server URL	The URL of the LDAP server from which the CRL can be downloaded if you require CRL checks. This URL must start with **ldap://** **Note** You must include a port number in the URL when using this AAA server on ASA devices, otherwise LDAP will fail.
Enable Registration Authority Mode (PIX 6.3)	For PIX 6.3 devices, whether the CA server operates in RA (Registration Authority) mode. A Registration Authority is a server that acts as a proxy for the actual CA so that CA operations can continue when the CA server is offline. **Note** Cisco IOS routers configure RA mode automatically, if required.

PKI Enrollment Dialog Box—Enrollment Parameters Tab

Use the Enrollment Parameters tab of the PKI Enrollment Dialog Box, page 28-33 to define the retry settings to use when the device contacts the CA server as well as the settings for generating the RSA key pair to associate with the certificate.

If the PKI enrollment object represents a Microsoft CA, you can define the challenge password required to validate the router's identity.

Note You do not have to define enrollment parameters in order to create or import a trustpoint in Security Manager.

Navigation Path

Go to the PKI Enrollment Dialog Box, page 28-33 and click the **Enrollment Parameters** tab.

Related Topics

- PKI Enrollment Dialog Box—CA Information Tab, page 28-35
- PKI Enrollment Dialog Box—Certificate Subject Name Tab, page 28-40
- PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab, page 28-42

Field Reference

Table 28-23 PKI Enrollment Dialog Box—Enrollment Parameters Tab

Element	Description
Challenge Password	The password used by the CA server to validate the identity of the device. This password is mandatory for PIX 6.3 devices, but optional for PIX/ASA 7.0+ devices and Cisco IOS routers. You can obtain the password by contacting the CA server directly or by entering the following address in a web browser: **http://URLHostName/certsrv/mscep/mscep.dll**. The password is good for 60 minutes from the time you obtain it from the CA server. Therefore, it is important that you deploy the password as soon as possible after you create it. **Note** Each password is valid for a single enrollment by a single device. Therefore, we do not recommend that you assign a PKI enrollment object where this field is defined to a VPN, unless you first configure a device-level override for each device in the VPN. For more information, see Understanding Policy Object Overrides for Individual Devices, page 6-13.
Retry Period	The interval between certificate request attempts, in minutes. Values can be 1 to 60 minutes. The default is 1 minute.
Retry Count	The number of retries that should be made if no certificate is issued upon the first request. Values can be 1 to 100. The default is 10.

Table 28-23 PKI Enrollment Dialog Box—Enrollment Parameters Tab (Continued)

Element	Description
Certificate Auto-Enrollment (IOS devices only.)	The percentage of the current certificate's lifetime after which the router requests a new certificate. For example, if you enter 70, the router requests a new certificate after 70% of the lifetime of the current certificate has been reached. Values range from 10% to 100%. If you do not specify a value, the router requests a new certificate after the old certificate expires.
Include Device's Serial Number	Whether to include the serial number of the device in the certificate. **Tip** The CA uses the serial number to either authenticate certificates or to later associate a certificate with a particular device. If you are in doubt, include the serial number, as it is useful for debugging purposes.
RSA Key Pair Name (PIX 7.0+, ASA, IOS devices only.)	If the key pair you want to associate with the certificate already exists, this field specifies the name of that key pair. If the key pair does not exist, this field specifies the name to assign to the key pair that will be generated during enrollment. **Note** If you do not specify an RSA key pair, the fully qualified domain name (FQDN) key pair is used instead. On PIX and ASA devices, the key pair must exist on the device before deployment.
RSA Key Size (IOS devices only.)	If the key pair does not exist, defines the desired key size (modulus), in bits. If you want a modulus between 512 and 1024, enter an integer that is a multiple of 64. If you want a value higher than 1024, enter 1536 or 2048. The recommended size is 1024. **Note** The larger the modulus size, the more secure the key. However, keys with larger modulus sizes take longer to generate (a minute or more when larger than 512 bits) and longer to process when exchanged.
RSA Encryption Key Size (IOS devices only.)	The size of the second key, which is used to request separate encryption, signature keys, and certificates.
Source Interface (IOS devices only.)	The source address for all outgoing connections sent to a CA or LDAP server during authentication, enrollment, and when obtaining a revocation list. This parameter may be necessary when the CA server or LDAP server cannot respond to the address from which the connection originated (for example, due to a firewall). If you do not define a value in this field, the address of the outgoing interface is used. Enter the name of an interface or interface role, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it.

PKI Enrollment Dialog Box—Certificate Subject Name Tab

Use the Certificate Subject Name tab of the PKI Enrollment Dialog Box, page 28-33 to optionally define additional information about the device in certificate requests sent to the CA server. This information is placed in the certificate and can be viewed by any party who receives the certificate from the router.

Enter all information using the standard LDAP X.500 format.

Navigation Path

Go to the PKI Enrollment Dialog Box, page 28-33 and click the **Certificate Subject Name** tab.

Related Topics

- PKI Enrollment Dialog Box—CA Information Tab, page 28-35
- PKI Enrollment Dialog Box—Enrollment Parameters Tab, page 28-39
- PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab, page 28-42

Field Reference

Table 28-24 PKI Enrollment Dialog Box—Certificate Subject Name Tab

Element	Description
Include Device's FQDN	Whether to include the device's fully qualified domain name (FQDN) in the certificate request. The name is taken from the Hostname policy (ensure that you specify both the hostname and domain name in the policy to get a valid full-qualified domain name). If you do not configure the Hostname policy, the name is derived from the display name for the device in Security Manager, *display_name***.null**, which is unlikely to give you the desired results.
Include Device's IP Address	The interface whose IP address is included in the certificate request. Enter the name of the interface or interface role, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it.
Common Name (CN)	The X.500 common name to include in the certificate.
Organization Unit (OU)	The name of the organization unit (for example, a department name) to include in the certificate. **Note** When you configure PKI server objects for Cisco EzVPN Remote components, this field must contain the name of the client group to which the component connects. Otherwise, the component will not be able to connect. Although this information is not required for the EzVPN Server, including it does not create configuration problems. For more information about EzVPN, see Understanding Easy VPN, page 24-1.
Organization (O)	The organization or company name to include in the certificate.
Locality (L)	The locality to include in the certificate.
State (ST)	The state or province to include in the certificate.
Country (C)	The country to include in the certificate.
Email (E)	The email address to include in the certificate.

PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab

Use the Trusted CA Hierarchy tab of the PKI Enrollment Dialog Box, page 28-33 to define the trusted CA servers within a hierarchical PKI framework. Within this framework, all enrolled peers can validate each other's certificates if they share a trusted root CA certificate or a common subordinate CA.

Select the CA servers (as defined as PKI enrollment objects) to include in the hierarchy in the Available Servers list and click >> to move them to the selected list. You can do the reverse to remove servers.

If the PKI enrollment object you need is not yet defined, click the **Create (+)** button beneath the available servers list to create the object. You can also select an object and click the **Edit** button to change its definition, if needed.

Navigation Path

Go to the PKI Enrollment Dialog Box, page 28-33 and click the **Trusted CA Hierarchy** tab.

Related Topics

- PKI Enrollment Dialog Box—CA Information Tab, page 28-35
- PKI Enrollment Dialog Box—Enrollment Parameters Tab, page 28-39
- PKI Enrollment Dialog Box—Certificate Subject Name Tab, page 28-40

Add or Edit Port Forwarding List Dialog Boxes

Use the Port Forwarding List dialog box to create, copy and edit port forwarding list policy objects. You can create port forwarding list objects to use when you are configuring the thin client access mode for SSL VPN.

Port forwarding allows users to access applications (such as Telnet, e-mail, VNC, SSH, and Terminal services) inside the enterprise through an SSL VPN session. When port forwarding is enabled, the hosts file on the SSL VPN client is modified to map the application to the port number configured in the forwarding list. A port forwarding list object defines the mappings of port numbers on the remote client to the application's IP address and port behind the SSL VPN gateway.

Navigation Path

Select **Tools > Policy Object Manager**, then select **Port Forwarding List** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- SSL VPN Access Modes, page 26-4
- ASA Group Policies SSL VPN Clientless Settings, page 28-11
- User Group Dialog Box—Thin Client Settings, page 28-79
- Clientless and Thin Client Access Modes Page, page 27-8
- Policy Object Manager Window, page 6-3

Field Reference

Table 28-25 Port Forwarding List Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object.
Port Forwarding List table	The port forwarding entries that are defined in the object. The entries show the mapping of the local port to the remote server and port. • To add a mapping, click the **Add Row** button to open the Add or Edit A Port Forwarding Entry Dialog Box, page 28-43. • To edit a mapping, select it and click the **Edit Row** button. • To delete a mapping, select it and click the **Delete Row** button.
Include Port Forwarding Lists	The names of other port forwarding list objects to include in the object. Enter the name of the object or click **Select** to select it from a list or to create a new object. Separate multiple entries with commas. When you add other port forwarding lists, the entries from those lists are treated as if they were directly entered into this object, and the names of the included objects are not reflected in the device configuration commands during deployment.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add or Edit A Port Forwarding Entry Dialog Box

Use the Add or Edit A Port Forwarding Entry dialog boxes to create a new port forwarding list entry or edit an existing one.

Navigation Path

Go to the Add or Edit Port Forwarding List Dialog Boxes, page 28-42 and click the **Add Row** button or select an entry and click the **Edit Row** button beneath the Port Forwarding List table.

Field Reference

Table 28-26 Add or Edit A Port Forwarding Entry Dialog Box

Element	Description
Local TCP Port	The port number to which the local application is mapped (between 1 and 65535).
Remote Server IP Address Name	The IP address or fully qualified domain name of the remote server. Select the type of entry and enter the IP address or name. For the IP address, you can enter the name of a network/host object that specifies the remote server's IP address, or click **Select** to select it from a list or to create a new object.
Remote TCP Port	The port number of the application for which port forwarding is configured (between 1 and 65535).
Description	A description of the port forwarding entry. This information is mandatory on Cisco IOS devices.

Add or Edit Single Sign On Server Dialog Boxes

Use the Add or Edit Single Sign On Server dialog box to create, copy, and edit single sign on (SSO) server objects for use with SSL VPNs (as configured in ASA group policy objects). For information on how to configure SSO servers in an ASA group policy, see ASA Group Policies SSL VPN Settings, page 28-15.

Single sign-on lets users access different secure services on different servers without entering a username and password more than once. In the authentication, the security appliance acts as a proxy for the SSL VPN user to the SSO server. You can configure this object to identify either a Computer Associates SiteMinder SSO server or a Security Assertion Markup Language (SAML) Browser Post Profile version 1.1 server.

The SSO mechanism starts as part of the AAA process or just after successful user authentication to an AAA server. The SSL VPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the SSL VPN server sends an SSO authentication request, including username and password, to the authenticating server. If the server approves the authentication request, it returns an SSO authentication cookie to the SSL VPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure web sites within the domain protected by the SSO server.

If you want to configure SSO for an SSL VPN group, you must also configure a AAA server, such as a RADIUS or LDAP server.

Note The SAML Browser Artifact profile method of exchanging assertions is not supported.

Navigation Path

Select **Single Sign On Servers** in the Policy Object Manager Window, page 6-3. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

You can also create the object when configuring an ASA user group object for SSL VPN (see ASA Group Policies SSL VPN Settings, page 28-15).

Field Reference

Table 28-27 Add or Edit Single Sign-On Server Dialog Box

Element	Description
Name	The object name, which must be 4 to 31 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object.
Authentication Type	The type of SSO server to use with clientless SSL VPN connections. The other attributes on the page change based on your selection. • **SiteMinder**—Computer Associates SiteMinder SSO server. • **SAML POST**—Security Assertion Markup Language (SAML) Browser Post Profile server.
URL (SiteMinder only.)	The URL of the SiteMinder SSO server to which the security appliance makes authentication requests. Select whether to use HTTP or HTTPS and enter the URL. **Tip** For HTTPS communication, make sure that the SSL encryption settings match on both the security appliance and the SiteMinder server. On the security appliance, you can verify this with the **ssl encryption** command.
Secret Key Confirm (SiteMinder only.)	The key used to encrypt authentication communications with the SiteMinder server, if any. The key can contain any alphanumeric characters. There is no minimum or maximum number of characters. Enter the same key in both fields. **Tip** If you enter a secret key, you must configure the same key in the SiteMinder server using the Cisco Java plug-in authentication scheme.
Assertion URL (SAML POST only.)	The URL for the SAML-type SSO assertion consumer service. Select whether to use HTTP or HTTPS and enter the URL, which must be fewer than 255 characters.
Assertion Issuer (SAML POST only.)	The name of the security device that is sending assertions to a SAML-type SSO server. This is usually the name of the security appliance, for example, asa.example.com. The name must be fewer than 65 characters.
Trustpoint (SAML POST only.)	The name of the PKI enrollment policy object that identifies the certificate authority (CA) server that acts as the trustpoint that contains the certificate to use to sign the SAML-type browser assertion. Enter the name or click **Select** to select it from a list or to create a new object.
Max Retries	The number of times the security appliance retries a failed SSO authentication attempt before the authentication times out. The range is 1 to 5 retries, and the default is 3 retries.
Request Timeout	The number of seconds before a failed SSO authentication attempt times out. The range is 1 to 30 seconds, and the default is 5 seconds.

Table 28-27 Add or Edit Single Sign-On Server Dialog Box (Continued)

Element	Description
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add or Edit Bookmarks Dialog Boxes

Use the Add and Edit Bookmarks dialog boxes to configure browser-based clientless SSL VPN bookmarks (URL lists) for an SSL VPN Bookmark object. From this dialog box, you can change the order of the bookmark entries within the table, create, copy, edit, and delete SSL VPN Bookmark objects.

An SSL VPN Bookmark object defines the URLs that are displayed on the portal page after a successful login.

Navigation Path

Select **Tools > Policy Object Manager**, then select **SSL VPN Bookmarks** from the Object Type Selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Configuring SSL VPN Bookmark Lists for ASA and IOS Devices, page 26-68
- Using the Post URL Method and Macro Substitutions in SSL VPN Bookmarks, page 26-70
- Localizing SSL VPN Web Pages for ASA Devices, page 26-66

Field Reference

Table 28-28 Add and Edit Bookmarks Dialog Boxes

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object.
Bookmarks Heading (IOS) (IOS devices only)	The heading that is displayed above the URLs listed on the portal page of an SSL†VPN hosted on an IOS device.

Table 28-28 Add and Edit Bookmarks Dialog Boxes (Continued)

Element	Description
Bookmarks	The list of bookmark entries for the object. • To change the order of an entry, select it and click the Move Up or Move Down arrow buttons. The order of entries in the table defines the order in which the bookmarks are presented to the user. • To add an entry, click the Add button and fill in the Add Bookmark Entry dialog box (see Add and Edit Bookmark Entry Dialog Boxes, page 28-47). • To edit an entry, select it and click the Edit button. • To delete an entry, select it and click the Delete button.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add and Edit Bookmark Entry Dialog Boxes

Use the Add and Edit Bookmark Entry dialog boxes to create or edit a bookmark to be included in an SSL VPN Bookmark object.

You can use non-English, non-ASCII languages for the text to display for bookmarks if you are configuring the object for use on an ASA device. For more information about how you can configure the SSL VPN portal in local languages, see Localizing SSL VPN Web Pages for ASA Devices, page 26-66.

Navigation Path

In the Policy Object Manager, from the Add or Edit Bookmarks Dialog Boxes, right-click inside the Bookmarks table, then select **Add Row** or right-click a row, then select **Edit Row**.

Related Topics

- Configuring SSL VPN Bookmark Lists for ASA and IOS Devices, page 26-68
- Using the Post URL Method and Macro Substitutions in SSL VPN Bookmarks, page 26-70

Field Reference

Table 28-29 Add and Edit Bookmark Entry Dialog Boxes

Element	Description
Bookmark Option	Select whether you want to define a new SSL VPN Bookmark entry or use the entries from an existing object: • **Enter Bookmark**—You want to define a bookmark entry. • **Include Existing Bookmarks**—You want to include bookmark entries defined in an existing SSL VPN Bookmark object. Enter the name of the object or click **Select** to select it from a list or to create a new object.
Title	The text label that the user sees for the bookmark.
URL	The Universal Resource Locator address for the bookmark. Select the protocol for the bookmark and enter the rest of the URL in the edit box.
Advanced Group The settings in the Advanced group are applicable only to SSL VPN portals hosted on ASA devices running software version 8.x. Do not configure these settings for SSL VPN Bookmark objects that you will use on other devices.	
Subtitle	An additional user-visible title that describes the bookmark entry.
Thumbnail	The File object that represents an icon you want to associate with the bookmark on the Portal. Enter the name of the File object or click **Select** to select it from a list or to create a new object.
Authentication Access	Whether to display the thumbnail only on the Portal page. If you deselect this option, the thumbnail is also displayed on the Logon page.
Enable Favorite URL Option	Whether to display the bookmark entry on the portal home page. Deselect the check box if you want the bookmark entry to appear on the application page only.
Enable Smart Tunnel Option	Whether to open the bookmark in a new window that uses the smart tunnel functionality to pass data to and from the security appliance.
URL Method	Select the required URL method from the list: • **Get**—Select this option if you want simple data retrieval. • **Post**—Select this option when processing the data might involve changes to it, for example, storing or updating data, ordering a product, or sending e-mail. If you select this option, you must configure the Post parameters in the Post Parameters table.
Post Parameters	The list of the names and values of the Post parameters for the bookmark entry. • To add a parameter, click the Add button and fill in the Add Post Parameter dialog box (see Add and Edit Post Parameter Dialog Boxes, page 28-49). • To edit a parameter, select it and click the Edit button. • To delete a parameter, select it and click the Delete button.

Add and Edit Post Parameter Dialog Boxes

Use the Add and Edit Post Parameter dialog boxes to create a new Post parameter entry or edit an existing one in the table. For a detailed discussion of Post parameters, see Using the Post URL Method and Macro Substitutions in SSL VPN Bookmarks, page 26-70.

Navigation Path

In the Policy Object Manager, from the Add and Edit Bookmark Entry Dialog Boxes, right-click inside the Post Parameters table, then select **Add Row** or right-click a row, then select **Edit Row**.

Related Topics

- Configuring SSL VPN Bookmark Lists for ASA and IOS Devices, page 26-68
- Using the Post URL Method and Macro Substitutions in SSL VPN Bookmarks, page 26-70

Field Reference

Table 28-30 Add and Edit Post Parameter Dialog Boxes

Element	Description
Name	The name of the post parameter exactly as defined in the corresponding HTML form. For example, **param_name** in <input name="*param_name*" value="*param_value*">.
Value	The value of the post parameter exactly as defined in the corresponding HTML form. For example, **param_value** in <input name="*param_name*" value="*param_value*">.

Add and Edit SSL VPN Customization Dialog Boxes

Use the Add and Edit SSL VPN Customization dialog boxes to create, copy, and edit SSL VPN Customization objects. An SSL VPN Customization policy object describes how to customize web pages for a browser-based clientless SSL VPN hosted on an ASA 8.x device. For more information, see Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63.

You can use non-English, non-ASCII languages for the text to display on these pages. For more information about how you can configure the SSL VPN portal in local languages, see Localizing SSL VPN Web Pages for ASA Devices, page 26-66.

Navigation Path

Select **Tools > Policy Object Manager**, then select **SSL VPN Customization** from the Object Type Selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63
- Localizing SSL VPN Web Pages for ASA Devices, page 26-66
- Creating Your Own SSL VPN Logon Page for ASA Devices, page 26-67

Field Reference

Table 28-31 Add and Edit SSL VPN Customization Dialog Boxes

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object.
Settings Pane The body of the dialog box is a pane with a table of contents on the left and settings related to the item selected in the table of contents on the right. Before configuring settings, click the Preview button to see the default settings to help you determine what, if anything, you want to change. The top folders in the table of contents represent the SSL VPN web pages that you can customize, and are explained next.	
Logon Page	The Logon web page is the one users see first when connecting to the SSL VPN portal. It is used for logging into the VPN. Select the following items in the Logon Page folder in the table of contents to view and change the settings: • **Logon Page**—The Browser Window Title field defines the title of the web page, which is displayed in the browser's title bar. • **Title Panel**—The title displayed in the web page itself. For more information about the settings, see SSL VPN Customization Dialog Box—Title Panel, page 28-52. • **Language**—The languages you will support for the Logon, Portal, and Logout pages. For more information about the settings, see SSL VPN Customization Dialog Box—Language, page 28-53. • **Logon Form**—The labels and colors used in the form that accepts user logon information. For more information about the settings, see SSL VPN Customization Dialog Box—Logon Form, page 28-55. • **Informational Panel**—An extra informational panel for conveying information to users. For more information about the settings, see SSL VPN Customization Dialog Box—Informational Panel, page 28-56. • **Copyright Panel**—The copyright information on the logon page. For more information about the settings, see SSL VPN Customization Dialog Box—Copyright Panel, page 28-56. • **Full Customization**—If you do not want to use the security appliance's built-in logon page, even customized, you can instead enable full customization and supply your own web page. For more information about creating a custom Logon page and the settings, see Creating Your Own SSL VPN Logon Page for ASA Devices, page 26-67 and SSL VPN Customization Dialog Box—Full Customization, page 28-57.

Table 28-31 Add and Edit SSL VPN Customization Dialog Boxes (Continued)

Element	Description
Portal Page	The Portal web page is the one users see after logging into the SSL VPN; it is the home page. Select the following items in the Portal Page folder in the table of contents to view and change the settings: • **Portal Page**—The **Browser Window Title** field defines the title of the web page, which is displayed in the browser's title bar. • **Title Panel**—The title displayed in the web page itself. For more information about the settings, see SSL VPN Customization Dialog Box—Title Panel, page 28-52. • **Toolbar**—The toolbar displayed above the main part of the Portal page. For more information about the settings, see SSL VPN Customization Dialog Box—Toolbar, page 28-58. • **Applications**—The application buttons that will appear on the page. For more information about the settings, see SSL VPN Customization Dialog Box—Applications, page 28-58. • **Custom Panes**—The layout of the main part of the Portal page. The default is a single column with no internal panes. For more information about the settings, see SSL VPN Customization Dialog Box—Custom Panes, page 28-59. • **Home Page**—How and whether to display URL lists on the home page. For more information about the settings, see SSL VPN Customization Dialog Box—Home Page, page 28-61.
Logout Page	The Logout web page is the one users see after logging out of the SSL VPN. For more information about the settings, see SSL VPN Customization Dialog Box—Logout Page, page 28-62.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The Overrides field indicates the number of devices that have overrides for this object.

SSL VPN Customization Dialog Box—Title Panel

Use the Title Panel page of the SSL VPN Customization dialog box to determine whether the Logon page or Portal page will have a title displayed in the web page itself. If you enable the title panel, you can specify the title, font, font size and weight, styles, and colors used. You can also select a File object that identifies a logo graphic.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Logon Page > Title Panel** in the table of contents to configure the title of the Logon page, or **Portal Page > Title Panel** to configure the title of the Portal page.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63
- Localizing SSL VPN Web Pages for ASA Devices, page 26-66

Field Reference

Table 28-32 SSL VPN Customization Dialog Box—Title Panel

Element	Description
Display Title Panel	Whether to display a title panel within the web page. The default is to not display a title. If you select this option, you can configure the title using the other fields on this page.
Gradient	Whether to have the background color change in a gradual progression.
Title Text	The text to display in the title panel.
Font Weight Font Size Font Color	The characteristics of the font used for the title text. You can select a weight, font size, and color. Click **Select** to choose a font color.
Background Color	The color of the background of the title panel. Click **Select** to choose a color.
Style (CSS)	Cascading Style Sheet (CSS) parameters that define the style characteristics of the title panel. You can include a maximum of 256 characters. **Tip** For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.
Logo Image	The File policy object that identifies the logo image you want to include in the title panel, if any. Enter the name of the File object or click **Select** to select it from a list or to create a new object. **Tip** The image file can be a GIF, JPG, or PNG file, and it can be up to 100 kilobytes in size. For more information about File objects, see Add and Edit File Object Dialog Boxes, page 28-24.

SSL VPN Customization Dialog Box—Language

Use the Language page of the SSL VPN Customization dialog box identify the languages you will support on the browser-based clientless SSL VPN portal. If you want to configure translation tables for other languages on the ASA device and use them, you can configure the supported languages and allow users to choose their language. Before you configure these settings, read Localizing SSL VPN Web Pages for ASA Devices, page 26-66.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Logon Page > Language** in the table of contents.

Related Topics

- Localizing SSL VPN Web Pages for ASA Devices, page 26-66
- Add and Edit SSL VPN Customization Dialog Boxes, page 28-49
- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-33 SSL VPN Customization Dialog Box—Language

Element	Description
Automatic Browser Language Selection	This table lists the languages you will support on the web pages for automatic browser language selection. Automatic browser language select allows the ASA device to negotiate with the user's web browser to determine the language in which to present the web pages. You must configure a translation table on the ASA device for any language you list here. For more detailed information about automatic browser language selection, see Localizing SSL VPN Web Pages for ASA Devices, page 26-66. Languages are listed by their abbreviation in the table. The languages are evaluated top to bottom until a match is found. The language that is indicated as the default language (indicated as True in the table) is used if the device is unable to negotiate a different language with the browser. If you do not specify a default, English is the default. • To add a language, click the Add Row button below the table. • To edit a language, select it and click the Edit Row button. • To delete a language, select it and click the Delete Row button.
Enable Language Selector	Whether to display the Language Selector on the Logon page. The Language Selector allows users to select their preferred language. The Language Selector is complementary to the automatic browser language selection capability.

Table 28-33 SSL VPN Customization Dialog Box—Language (Continued)

Element	Description
Language Selector Prompt	The text label for the Language Selector prompt.
Language Table	The list of languages included in the Language Selector drop-down list. You must configure a translation table on the ASA device for any language you list here. For more detailed information, see Localizing SSL VPN Web Pages for ASA Devices, page 26-66. The table lists the languages by abbreviation and title, or the common name of the language. The title is the text displayed in the drop-down list. You can change the language title but not the abbreviation. • To add a language, click the Add Row button below the table. • To edit a language, select it and click the Edit Row button. • To delete a language, select it and click the Delete Row button.

Add and Edit Language Dialog Boxes

Use the Add and Edit Language dialog boxes to add or edit an entry for a language you will support for automatic browser language selection or in the Language Selector drop-down list.

Navigation Path

From the SSL VPN Customization Dialog Box—Language page, click the **Add Row** button for either the Automatic Browser Language Selection table or the Language Selector table, or select a row and click the **Edit Row** button.

Related Topics

- Localizing SSL VPN Web Pages for ASA Devices, page 26-66
- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-34 Add and Edit Language Dialog Boxes

Element	Description
Language	The list of languages that you can support on the browser-based clientless SSL VPN web pages, listed by their abbreviation.
Default (Automatic Browser Language Selection only)	Whether the language should be defined as the default language for the portal. The default language is used if the ASA device cannot negotiate a language with the client's browser.
Title (Language Selector only)	The name of the language that should appear in the Language Selector on the Logon page.

SSL VPN Customization Dialog Box—Logon Form

Use the Logon Form settings of the SSL VPN Customization dialog box to customize the title of the login box, login prompts of the SSL VPN page (including username, password, and group prompts), login buttons, and style elements of the login box that appears to browser-based clientless SSL VPN users when they initially connect to the security appliance.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Logon Page > Logon Form** in the table of contents.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-35 SSL VPN Customization Dialog Box—Logon Page

Element	Description
Title	The text displayed as the title of the login box.
Message	The message that appears in the login box above the username and password fields. You can enter a maximum of 256 characters.
Username Prompt	The text of the prompt for the username entry field.
Password Prompt	The text of the prompt for the password entry field.
Secondary Username Prompt Secondary Password Prompt	The prompts for a second username and password if you require two login credentials. You can enable secondary authentication only if the Connection Profile policy is configured to require it. The secondary username and password prompt are displayed only if you configure them. If you leave the username prompt blank, the primary username is used and the secondary password must be associated with the primary username.
Internal Password Prompt	The text of the prompt for the internal password entry field.
Show Internal Password First	Whether the prompt for the internal password should be placed above the password prompt. The internal password is required when using a clientless SSL VPN to access an internal protected website.
Group Selector Prompt	The text of the prompt for the Group Selector drop-down list.
Button Text	The name of the button the user clicks to log onto the SSL VPN.
Border Color	The color of the border of the login box. Click **Select** to choose a color.
Title Font Color	The color of the font for the login box title. Click **Select** to choose a color.
Title Background Color	The background color for the Title area of the login box. Click **Select** to choose a color.
Font Color	The color of the font of the login form. Click **Select** to choose a color.
Background Color	The background color for the login form. Click **Select** to choose a color.

SSL VPN Customization Dialog Box—Informational Panel

Use the Informational Panel page of the SSL VPN Customization dialog box to customize the appearance of the Informational panel in the Logon page. The Informational panel is an area where you can provide extra information to the user, and is optional.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Logon Page > Informational Panel** in the table of contents.

Related Topics

- Add and Edit SSL VPN Customization Dialog Boxes, page 28-49
- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-36 SSL VPN Customization Dialog Box—Informational Panel

Element	Description
Display Informational Panel	Whether to display the Informational panel. The default is to not display the panel. If you select this option, you can configure the panel using the other fields on this page.
Panel Position	The location of the Informational panel, either to the left of the Logon box or to the right of it.
Text	The text that appears in the Informational panel. You can enter a maximum of 256 characters.
Logo Image	The File policy object that identifies the logo image you want to include in the Informational panel, if any. Enter the name of the File object or click **Select** to select it from a list or to create a new object. **Tip** The image file can be a GIF, JPG, or PNG file, and it can be up to 100 kilobytes in size. For more information about File objects, see Add and Edit File Object Dialog Boxes, page 28-24.
Image Position	The position of the logo image in the panel, either above the text or below it.

SSL VPN Customization Dialog Box—Copyright Panel

Use the Copyright Panel page of the SSL VPN Customization dialog box to customize the appearance of the Copyright panel in the Logon page. The Copyright panel provides your copyright information, appears at the bottom of the page, and is optional.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Logon Page > Copyright Panel** in the table of contents.

Related Topics

- Add and Edit SSL VPN Customization Dialog Boxes, page 28-49
- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-37 SSL VPN Customization Dialog Box—Copyright Panel

Element	Description
Display Copyright Panel	Whether to display the Copyright panel. The default is to not display the panel. If you select this option, you can configure the panel using the other fields on this page.
Text	The text that appears in the copyright panel. You can enter a maximum of 256 characters.

SSL VPN Customization Dialog Box—Full Customization

Use the Full Customization page of the SSL VPN Customization dialog box to identify your own custom Logon page. The custom page replaces the Logon page settings available on the dialog box. For information on creating a custom Logon page, see Creating Your Own SSL VPN Logon Page for ASA Devices, page 26-67.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Logon Page > Full Customization** in the table of contents.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-38 SSL VPN Customization Dialog Box—Full Customization

Element	Description
Enable Full Customization	Whether you want to use your own custom Logon page. If you enable full customization, all of the other Logon page configuration settings are ignored.
Custom Page	The custom Logon page. You must copy the file to the Security Manager server before specifying it here. Click **Browse** to select the file. For information on selecting files, see Selecting or Specifying a File or Directory on the Server File System, page 1-35.

SSL VPN Customization Dialog Box—Toolbar

Use the Toolbar page of the SSL VPN Customization dialog box to customize the appearance of the toolbar in the Portal page. The toolbar appears above the main body of the Portal page and includes a field to allow users to enter URLs to browse. The toolbar is optional.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Portal Page > Toolbar** in the table of contents.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-39 SSL VPN Customization Dialog Box—Toolbar

Element	Description
Display Toolbar	Whether to display the toolbar. The default is to not display the toolbar. If you select this option, you can configure the toolbar using the other fields on this page.
Prompt Box Title	The text of the prompt for the field where users select the protocol of the target web page and enter the URL.
Browse Button Text	The name of the button the user clicks to go to the target URL.
Logout Prompt	The text of the prompt for logging out of the SSL VPN.

SSL VPN Customization Dialog Box—Applications

Use the Applications page of the SSL VPN Customization dialog box to customize the application links that appear in the Portal page. This page lists all the application links that you can display in the navigational panel on the left side of the SSL VPN portal page.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Portal Page > Applications** in the table of contents.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-40 SSL VPN Customization Dialog Box—Applications

Element	Description
No. Move Up and Move Down buttons (below the table)	The sequential number of the application in the table. To change the order of an application, select it and click the Move Up or Move down buttons to the desired position. The applications appear on the Portal page in the order represented here.
Applications	The graphic associated with an application.
Title	The name of the application. Standard applications include Home, Web Applications, Browse Networks, Application Access, and AnyConnect Client. Also listed are the browser plug-ins that you create when you configure the SSL VPN global settings are also available for selection from this page. Double-click a title to make it editable so that you can change the name.
Enable	Whether the application is included on the Portal page.

SSL VPN Customization Dialog Box—Custom Panes

Use the Custom Panes page of the SSL VPN Customization dialog box to customize the appearance of the main body of the Portal page. By creating custom panes and specifying a column layout, you can create a grid of information that can help you present portal information effectively to your end users.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Portal Page > Custom Panes** in the table of contents.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-41 SSL VPN Customization Dialog Box—Custom Panes

Element	Description
Columns table	The list of columns that the main body of the Portal page should be divided into. You define the column based on a percentage of the width of the page. The percentages should add up to 100. If they do not add up to 100, the device will adjust the column widths. Create the columns as you want them to appear, left to right, on the Portal page. • To add a column, click the Add Row button below the table. • To edit a column, select it and click the Edit Row button. • To delete a column, select it and click the Delete Row button.
Custom Panes table	The custom panes that should appear in the main body of the Portal page. The table shows whether a pane is enabled to appear, the type of pane, its characteristics, and the column and row in which it will appear on the page. The panes can display plain text or include a URL for HTML, image, or RSS links. For more detailed information about the settings, see Add or Edit Custom Pane Dialog Boxes, page 28-60. • To add a custom pane, click the Add Row button below the table. • To edit a custom pane, select it and click the Edit Row button. • To delete a custom pane, select it and click the Delete Row button.

Add and Edit Column Dialog Boxes

Use the Add or Edit Column dialog box to create or edit columns in the main body of the Portal page for browser-based clientless SSL VPNs. Enter the desired width of the column as a percentage of the total area in the Percentage field.

Navigation Path

From the SSL VPN Customization Dialog Box—Custom Panes page, click the **Add Row** button in the Column table, or select a column and click the **Edit Row** button.

Add or Edit Custom Pane Dialog Boxes

Use the Add or Edit Custom Pane dialog box to create or edit a pane to display in the main body or the Portal page of a browser-based clientless SSL VPN.

Navigation Path

From the SSL VPN Customization Dialog Box—Custom Panes page, click the **Add Row** button in the Custom Pane table, or select a pane and click the **Edit Row** button.

Field Reference

Table 28-42 Add and Edit Custom Pane Dialog Boxes

Element	Description
Enable	Whether to display the custom pane on the Portal page.
Type	The type of content to show in the pane, one of: • Text—Plain text. You can include HTML mark up. • HTML—HTML content provided by a URL. • Image—An Image provided by a URL. • RSS—An RSS feed provided by a URL.
Show Title Title	Whether to display a title in the pane. If you select this option, enter the title in the Title field.
Show Border	Whether to display a border around the pane.
Column Row	The column and row numbers in which the pane should appear. Select or enter the number for each to specify the desired grid location.
Height	The height of the pane in pixels.
URL (HTML, Image, and RSS content only.)	The URL that hosts the content you want to display in the pane.
Text (Text content only.)	The text you want to display in the pane. You can include HTML markup in the text.

SSL VPN Customization Dialog Box—Home Page

Use the Home Page page in the SSL VPN Customization dialog box to customize the appearance of the URL and file lists on the Portal page and the content of the main body of the Portal page. URL lists are considered to be default elements on the portal home page unless they are explicitly disabled.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Portal Page > Home Page** in the table of contents.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-43 SSL VPN Customization Dialog Box—Home Page

Element	Description
Enable Custom Intranet Web Page	Whether to display a custom Intranet web page, which also enables URL bookmarks to be displayed on the Portal page. If you select this option, you can configure the panel using the other fields on this page.
URL List Mode	How you want to display URL lists on the home page. If you display URL lists, they are displayed in the column cells that are not occupied by custom panes (as configured on Portal Page > Custom Panes). The options are: • **Group By Application**—Bookmarks are grouped by application type. For example, Web Bookmarks, File Bookmarks. • **No Group**—URL lists are shown as separate panes. • **Do Not Display**—URL lists are not shown.
Custom Intranet Web Page URL	The URL of the custom web page that you want to be loaded as the home page. This page is displayed in the main body of the Portal page. If you specify a custom page, the settings on the Custom Panes page are ignored, and bookmark lists appear on the application pages that are accessed through the navigation panel on the left of the Portal page.

SSL VPN Customization Dialog Box—Logout Page

Use the Logout Page page of the SSL VPN Customization dialog box to customize the appearance of the Logout page for browser-based clientless SSL VPNs. The Logout page appears after the user logs out of the VPN.

Navigation Path

From the Add and Edit SSL VPN Customization Dialog Boxes, select **Logout Page** in the table of contents.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63

Field Reference

Table 28-44 SSL VPN Customization Dialog Box—Logout Page

Element	Description
Title	The text to display in the title panel.
Text	The message to display on the Logout page. Click Preview to see the default logout message. You can enter a maximum of 256 characters.
Show Login Button Login Button Text	Whether to display the Login button on the page. Displaying the button makes it easier for the user to log back into the portal. If you enable the button, you can specify the name of the button in the Login Button Text field.

Table 28-44 SSL VPN Customization Dialog Box—Logout Page (Continued)

Element	Description
Border Color	The color of the border around the logout box. Click **Select** to choose a color.
Title Font Color Title Background Color	The color of the font and background for the title area of the page. Click **Select** to choose a color.
Font Color Background Color	The font and background color of the message that appears in the logout box. Click **Select** to choose a color.

Add or Edit SSL VPN Gateway Dialog Box

Use the Add or Edit SSL VPN Gateway dialog box to create, copy and edit SSL VPN gateway objects. You use these objects when you are configuring an SSL VPN connection on an IOS device. For more information, see Gateway and Context Page (IOS), page 27-10.

An SSL VPN gateway acts as a proxy for connections to protected resources that are accessed through an SSL-encrypted connection between the gateway and a web-enabled browser on a remote device. You can configure only one gateway per SSL VPN.

Navigation Path

Select **Tools > Policy Object Manager**, then select **SSL VPN Gateway** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Gateway and Context Page (IOS), page 27-10
- General Tab, page 27-107
- Policy Object Manager Window, page 6-3

Field Reference

Table 28-45 Add and Edit SSL VPN Gateway Dialog Boxes

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object (up to 1024 characters).

Table 28-45 Add and Edit SSL VPN Gateway Dialog Boxes (Continued)

Element	Description
IP Address	The IP address for the gateway, which is the address to which remote users connect: - **Use Static IP Address**—Specify the address that you want to use. You must also configure this address on an interface on the router. - **Obtained from Interface**—Specify the interface role that resolves to a single interface on the device. The IP address configured for the interface is used. This option allows you to identify the external interface you want to use for connections without having to explicitly enter the IP address. If you have to change the address on the interface, you do not have to also reconfigure this object.
Port	The number of the port that will carry the HTTPS traffic. You can also enter the name of a port list object that specifies the single port number, or click **Select** to select the object from a list. The default is the HTTPS object, which specifies port 443. If you do not use port 443, you can enter another port number between 1025 and 65535.
Trustpoint	The digital certificate required to establish the secure connection. A self-signed certificate is generated when an SSL VPN gateway is activated.
Enable Gateway	Whether to activate the SSL VPN gateway.
Specify SSL Encryption Algorithms	Whether to restrict the encryption algorithms used for the connection, or to specify a different order of use. The default is to make all algorithms available in this order of preference: 3DES and SHA1, AES and SHA1, RC4 and MD5. Select the priority order for the algorithms. Select None to eliminate one or two algorithms.
Redirect HTTP Traffic HTTP Port	Whether to have the gateway redirect HTTP traffic over secure HTTP (HTTPS). Traffic that comes to this port is redirected to the port you specify in the Port field. Enter the port number for HTTP traffic in the **HTTP Port** field. You can enter a number or the name of a port list object, or click **Select** to select an object from a list or to create a new object. The HTTP port is normally 80. However, you can enter any other number that is used in your network between 1025-65535.
Hostname	The hostname for the gateway. - Do Not Specify—No hostname is assigned; the IP address to the gateway is used. - Use the host and domain names of the device—These are defined in the **Platform > Device Admin > Hostname** policy. - Use the Object—The hostname is the value defined in a text policy object. Enter the name of the object or click **Select** to select it from a list or to create a new object.

Table 28-45 Add and Edit SSL VPN Gateway Dialog Boxes (Continued)

Element	Description
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add and Edit Smart Tunnel List Dialog Boxes

Use the Add and Edit Smart Tunnel Lists dialog boxes to create, copy, and edit SSL VPN smart tunnel objects.

An SSL VPN smart tunnel list object lists the applications that are eligible for smart tunnel access to a private site. You can configure the clientless settings of an ASA group policy with a smart tunnel list to allow users to access the specified applications through the SSL VPN portal. For an explanation of the types of applications that support smart tunnel access, see Configuring SSL VPN Smart Tunnels for ASA Devices, page 26-71.

You can include other SSL VPN smart tunnel list objects in an object. Thus, you can create a smaller set of objects that identify your basic list of applications, then create other objects that create the required combination of applications. For example, you might want all three of your ASA group policies to allow smart tunnel access to applications A and B, but the remaining applications are unique for each group. By creating a single object that specifies A and B, you can include that object in each of the SSL VPN smart tunnel list objects for the group policies, and these objects need only specify their unique applications in the applications table.

Navigation Path

Select **Tools > Policy Object Manager**, then select **SSL VPN Smart Tunnel Lists** from the Object Type selector. Right-click inside the work area and select **New Object**, or right-click a row and select **Edit Object**.

Related Topics

- ASA Group Policies SSL VPN Clientless Settings, page 28-11
- Configuring SSL VPN Smart Tunnels for ASA Devices, page 26-71
- Policy Object Manager Window, page 6-3

Field Reference

Table 28-46 Add and Edit Smart Tunnel Lists Dialog Boxes

Element	Description
Name	The object name, which can be up to 64 characters. Spaces are not allowed. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object.
Smart Tunnel Entries table	The applications to which users will be allowed smart tunnel access through the SSL VPN, including the name of the application and its location on client workstations. • To add an application, click the **Add Row** button to open the Add and Edit A Smart Tunnel Entry Dialog Boxes, page 28-66. • To edit an application, select it and click the **Edit Row** button. • To delete an application, select it and click the **Delete Row** button.
Include Smart Tunnel Lists	The other SSL VPN smart tunnel list objects that you want to include in this object, if any. Enter the names of the objects or click **Select** to select them from a list or to create new objects. Separate multiple entries with commas.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add and Edit A Smart Tunnel Entry Dialog Boxes

Use the Add and Edit A Smart Tunnel Entry dialog boxes to create a new smart tunnel entry or edit an existing entry in the table in the SSL VPN Smart Tunnel Lists dialog box.

Navigation Path

From Add and Edit Smart Tunnel List Dialog Boxes, page 28-65, click the **Add Row** button beneath the Smart Tunnel Entries table, or select an entry and click the **Edit Row** button.

Related Topics

- Configuring SSL VPN Smart Tunnels for ASA Devices, page 26-71
- Policy Object Manager Window, page 6-3

Field Reference

Table 28-47 Add and Edit Smart Tunnel Entry Dialog Boxes

Element	Description
App Name	The name of the application to which you are allowing smart tunnel access. The name can be up to 64 characters. Consider including the version number of the application if you are allowing more than one version smart tunnel access.
App Path	The filename and optionally, the path, of the application. This entry can be up to 128 characters. Use one of the following: • Filename—For example, **outlook.exe**. By only specifying the file name, it does not matter where users install the application on their workstations. However, the file name must match exactly. • Full path and filename—For example, **C:\Program Files\Microsoft Office\OFFICE11\OUTLOOK.EXE**. This allows the application smart tunnel access only if it is installed in the specified directory, which you can use to enforce organizational standards. **Tips** • If you specify the full path, and the smart tunnel application stops working after it had been working for a while, it is likely that a product upgrade changed the installation path. Add a new entry that accounts for the new path. • If you are granting smart tunnel access to an application that is started from the command line, create one entry for **cmd.exe** (the Windows command line), and another entry for the application.

Table 28-47 Add and Edit Smart Tunnel Entry Dialog Boxes (Continued)

Element	Description
Hash Value	(Optional) The hash value for the application. By specifying a hash value, you can ensure that the user does not rename another application to use a supported filename and thus start an unsupported and undesired application over the smart tunnel. To obtain the hash value, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at http://support.microsoft.com/kb/841290/. Place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:\temp) and then enter **fciv.exe -sha1** application at the command line (for example, **fciv.exe -sha1 c:\msimn.exe**) to display the SHA-1 hash. Copy and paste the value into this field. The SHA-1 hash is always 40 hexadecimal characters. Before authorizing an application for smart tunnel access, clientless SSL VPN calculates the hash of the application matching the App Name. It qualifies the application for smart tunnel access if the result matches the value of hash. Because the checksum varies with each version or patch of an application, the hash you enter can match only one version or patch on the remote host. To specify a hash for more than one version of an application, create a unique smart tunnel entry for each hash value. **Tip** Hash values require maintenance. You must update the smart tunnel list if you want to support future versions or patches of an application for which you supply a hash value. A sudden problem with smart tunnel access might be an indication that the application list containing hash values is not up-to-date with an application upgrade. You can avoid this problem by not entering a hash.

Add or Edit User Group Dialog Box

Use the Add or Edit User Group dialog box to create or edit a user group object. User group objects are used in Easy VPN topologies, remote access VPNs, and SSL VPNs for IOS devices.

When you configure a remote access VPN, SSL VPN, or Easy VPN server, you can create user groups to which remote clients belong. The remote clients must be configured with the same group name as the user group on the VPN server in order to connect to the server; otherwise, no connection is established. When the remote client connects to the VPN server successfully, the group policies for that particular user group are pushed to all remote clients belonging to the user group.

For more information about user groups, see:

- Understanding User Group Policies (IOS), page 26-42
- Configuring User Group Policies, page 26-43
- Configuring a User Group Policy for Easy VPN, page 24-10
- Configuring an SSL VPN Policy (IOS), page 26-60

Note You must select the technology (Easy VPN/Remote Access VPN, or SSL VPN) for which you are creating the user group object. If you are editing an existing user group object, the technology is already selected and you cannot change it. Depending on the selected technology, the appropriate settings are available for configuration.

Navigation Path

Select **Tools > Policy Object Manager**, then select **User Groups** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Tip You can also access this dialog box from the **Remote Access VPN > IPSec VPN > User Groups** or the **Remote Access VPN > SSL VPN** policies.

Related Topics

- Policy Object Manager Window, page 6-3

Field Reference

Table 28-48 User Group Dialog Box

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>Name</td><td>The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.</td></tr>
<tr><td>Description</td><td>An optional description of the object.</td></tr>
<tr><td colspan="2"><b>Settings Pane</b>
The body of the dialog box is a pane with a table of contents on the left and settings related to the item selected in the table of contents on the right.
You must first configure technology settings, then you can select items from the table of contents on the left and configure the options you require. Your selections on the Technology page control which options are available on these pages and in the table of contents.
The top folders in the table of contents represent the VPN technologies or other settings that you can configure, and are explained next.</td></tr>
<tr><td>Technology settings</td><td>These settings control what you can define in the group policy:
• <b>Group Name</b>—The name for the user group (up to 128 characters). Configure the same user group name within the remote client or device to ensure that the appropriate group attributes are downloaded.
• <b>Technology</b>—The types of VPN for which this object defines group policies. You cannot change this option when editing an object, or if you are creating the user group object while editing a VPN policy. You can configure settings for Easy VPN/Remote Access IPSec VPN or SSL VPN, but not both.</td></tr>
</table>

Table 28-48 User Group Dialog Box (Continued)

Element	Description
Easy VPN/Remote Access IPSec VPN pages	When you select Easy VPN/Remote Access IPSec VPN as the technology, you can configure settings on the following pages: • User Group Dialog Box—General Settings, page 28-70 • User Group Dialog Box—DNS/WINS Settings, page 28-72 • User Group Dialog Box—Split Tunneling, page 28-72 • User Group Dialog Box—IOS Client Settings, page 28-73 • User Group Dialog Box—IOS Xauth Options, page 28-75 • User Group Dialog Box—IOS Client VPN Software Update, page 28-76 • User Group Dialog Box—Advanced PIX Options, page 28-77
SSL VPN pages	When you select SSL VPN as the technology, you can configure settings on the following pages: • User Group Dialog Box—Clientless Settings, page 28-78 • User Group Dialog Box—Thin Client Settings, page 28-79 • User Group Dialog Box—SSL VPN Full Tunnel Settings, page 28-79 • User Group Dialog Box—DNS/WINS Settings, page 28-72 • User Group Dialog Box—SSL VPN Split Tunneling, page 28-81 • User Group Dialog Box—Browser Proxy Settings, page 28-83 • User Group Dialog Box—SSL VPN Connection Settings, page 28-84
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.

User Group Dialog Box—General Settings

The general settings you configure for your user group include the authentication method, IP address pool information, and connection attributes for PIX 6.3 Firewalls.

Note These settings apply in Easy VPN and remote access IPSec VPN configurations.

Navigation Path

Select **General** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Related Topics

- Configuring Preshared Key Policies, page 22-23

Field Reference

Table 28-49 User Group Dialog Box—General Settings

Element	Description
Preshared Key	The preshared key that will be used to authenticate the clients associated to the user group. **Note** You do not have to enter a preshared key if you are using digital certificates for group authentication. In regular IPsec VPNs, preshared keys allow for one or more peers to use individual shared secrets to authenticate encrypted tunnels. A preshared key must be configured on each participating peer. If one of the participating peers is not configured with the same preshared key, the IKE SA cannot be established. In Easy VPN authentication, the same Easy VPN server key is used for the spoke configuration to ensure that the server/client keys match. In remote access IPSec VPN authentication, the same key is used to negotiate a VPN connection between the remote access VPN server and the remote clients.
IP Address Pool Subnet/Ranges	The IP address ranges for a local pool that will be used to allocate an internal IP address to a client. Remote clients are assigned IP addresses from this pool. Separate multiple entries with commas. The default is 172.16.0.1-172.16.4.254.
Backup Servers IP Address	The IP address of the servers to be used as backups for the Easy VPN or remote access IPSec VPN server. The router tries to connect to these servers if the primary connection to the Easy VPN or remote access VPN server fails. Separate multiple entries with commas.
PIX Only Attributes	These attributes apply only to PIX 6.3 devices. • **Idle Time**—The timeout period for VPN connections, in seconds. If no communication occurs on the connection during this period, the device terminates the connection. The minimum is 60 seconds, and the maximum time is 35791394 minutes. The default is 30 minutes. • **Max Time**—The maximum amount of time for VPN connections, in seconds. At the end of the time, the device terminates the connection. The minimum is 60 seconds, and the maximum is 35791394 minutes. There is no default.

User Group Dialog Box—DNS/WINS Settings

Configure the DNS/WINS settings for your user group to define the DNS and WINS servers and the domain name that should be pushed to clients associated with the user group.

Note The DNS/WINS settings you configure for a user group apply in Easy VPN, remote access VPN, and SSL VPN configurations.

Navigation Path

Select **DNS/WINS** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Field Reference

Table 28-50 User Group Dialog Box—DNS/WINS Settings

Element	Description
Primary DNS Server	The IP address of the primary DNS server for the group. Enter the IP address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.
Secondary DNS Server	The IP address of the secondary DNS server for the group. Enter the IP address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.
Domain Name	The domain name of the DNS server you want to configure on the user group.
Primary WINS Server	The IP address of the primary WINS server for the group. Enter the IP address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.
Secondary WINS Server	The IP address of the primary WINS server for the group. Enter the IP address or the name of a network/host object, or click **Select** to select an object from a list or to create a new object.

User Group Dialog Box—Split Tunneling

Split tunneling lets a remote client conditionally direct packets over an IPsec or SSL VPN tunnel in encrypted form or to a network interface in clear text form. With split tunneling enabled, packets not bound for destinations on the other side of the tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

The split tunneling policy is applied to a specific network. When you configure split tunneling, you can transmit both secured and unsecured traffic on the same interface. You must specify which traffic will be secured and what the destination of that traffic is, so that you have a secure tunnel to the central site, while the clear (unsecured) traffic is transmitted across the public network.

Tip For optimum security, we recommend that you not enable split tunneling.

Note Split tunneling can be applied in Easy VPN, remote access VPN, and SSL VPN configurations. For information about configuring split tunneling for SSL VPN, see User Group Dialog Box—SSL VPN Split Tunneling, page 28-81.

Navigation Path

Select **Split Tunneling** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68 when configuring Easy VPN/Remote Access IPSec VPN.

Field Reference

Table 28-51 User Group Dialog Box—Split Tunneling

Element	Description
Split Tunneling	The networks for which you want to tunnel traffic. Traffic to all other addresses travels in the clear and is routed by the remote user's Internet service provider. You can identify the networks using one of these options: • **Protected Networks**—Specify the networks by network addresses. Enter the addresses or network/host objects, or click **Select** to select the objects from a list or to create new objects. For information on specifying addresses, see Specifying IP Addresses During Policy Definition, page 6-68. • **ACL**—Specify the networks using an extended access control list policy object. Enter the name of the object or click **Select** to select the object from a list or to create a new object.
Split DNS	A list of domain names that must be tunneled or resolved to the private network. All other names will be resolved through the public DNS server. You can enter multiple domain names separated by commas.

User Group Dialog Box—IOS Client Settings

Configure IOS client settings to define Cisco IOS specific options for your user group, including firewall settings for VPN clients.

Note These settings apply in Easy VPN and remote access IPSec VPN configurations.

Navigation Path

Select **Client Settings (IOS)** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Field Reference

Table 28-52 User Group Dialog Box—Client Settings (IOS)

Element	Description
Enable Firewall Are-You-There (Not available on 7600 series or ASR routers.)	This feature may be used if a VPN client is running the Black Ice or Zone Alarm personal firewall. When selected, it ensures that the personal firewall is running at connection time and throughout the connection. The Firewall-Are-U-There attribute is sent by the Black Ice and Zone Alarm personal firewalls if the server prompts them to do so. If the personal firewall stops running, the connection is terminated. If this feature is enabled and there is no personal firewall running on the server, the connection is never established.
Mode	A Central Policy Push (CPP) firewall policy on a server allows or denies a tunnel on the basis of whether the remote device has a required firewall for a local AAA server. The Mode option specifies whether the Central Policy Push (CPP) policy is optional or mandatory, as follows: • **Optional**—If the CPP policy is defined as optional, and is included in the Easy VPN server configuration, the tunnel setup is continued even if the client does not confirm the defined policy. • **Required**—If the CPP policy is defined as mandatory and is included in the Easy VPN server configuration, the tunnel setup is allowed only if the client confirms this policy. Otherwise, the tunnel is terminated.
Firewall Type	The type of firewall that you are making required or optional. The list shows all of the supported firewall software, which includes software from Cisco and Zone Labs.
Policy Type	Specifies the CPP firewall policy type: • **Check Presence**—Instructs the server to check for the presence of the specified firewall type. • **Central Policy Push**—The actual policy, such as the input and output access lists, that must be applied by the specified client firewall type. Specify the following: – The access control list to be used. Enter the name of the extended ACL object or click **Select** to select it from a list or to create a new object. – The direction of the access control list—Inbound or Outbound.
Include Local LAN	Whether to allow a non split-tunneling connection to access the local LAN at the same time as the client.
Perfect Forward Secrecy	Whether to enable Perfect Forward Secrecy (PFS). If PFS is enabled, the server is configured to notify the client of the central-site policy about whether PFS is required for any IPsec SA. The Diffie-Hellman (D-H) group that is proposed for PFS is the same that was negotiated in Phase 1 of the IKE negotiation.

User Group Dialog Box—IOS Xauth Options

IOS Xauth options configure IKE Extended Authentication (Xauth) user authentication and connection parameters for the user group, including the banner text.

Note These settings apply in Easy VPN and remote access VPN configurations.

Navigation Path

Select **Xauth Options (IOS)** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Field Reference

Table 28-53 User Group Dialog Box—IOS Xauth Options

Element	Description
Banner	The banner text that is displayed to Easy VPN remote clients during Xauth and web-based activation the first time the Easy VPN tunnel is brought up. A maximum of 1024 characters is allowed.
Maximum Logins Per User	The maximum number of connections a user can establish simultaneously. The maximum is 10.
Maximum Connections	The maximum number of client connections to the Easy VPN Server from this group. The maximum is 5000 per group.
Enable Group-Lock	Whether to enable group lock, which requires that the user enter the extended Xauth username in one of the following formats: • username/groupname • username\groupname • username@groupname • username%groupname The group that is specified after the delimiter is then compared to the group identifier that is sent during IKE aggressive mode. The groups must match or the connection is rejected. **Note** Do not select this option if you are using RSA signature authentication mechanisms such as certificates.
Enable Save Password	Whether to allow users to save their Xauth password locally on the client. On subsequent authentications, users can activate the password by using the check box on the software client or by adding the username and password to the Cisco IOS hardware client profile. After users activate the password, their username and password are sent to the server automatically during Xauth. This option is useful only if users have static passwords, that is, they are not one-time passwords such as those that are generated by a token.

User Group Dialog Box—IOS Client VPN Software Update

Client VPN Software Update (IOS) settings configure, for an IOS VPN client, the platform type, VPN Client revisions, and image URL for each client VPN software package installed, for your user group.

The Client Update feature is supported on IOS routers version 12.4(2)T and later, and Catalyst 6500/7600 devices version 12.2(33)SRA and later.

- To add a client, click the **Add Row** button to open the Add/Edit Client Update Dialog Box, page 28-76.
- To edit a client, select it and click the **Edit Row** button.
- To delete a client, select it and click the **Delete Row** button.

Note These settings apply in Easy VPN and remote access VPN configurations.

Navigation Path

Select **Client VPN Software Update (IOS)** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Add/Edit Client Update Dialog Box

Use the Add or Edit Client Update dialog box to configure the platform type, image URL, and VPN Client revisions for a client VPN software package.

Navigation Path

Open the User Group Dialog Box—IOS Client VPN Software Update, page 28-76, then click **Add Row**, or select an item in the table and click **Edit Row**.

Related Topics

- Add or Edit User Group Dialog Box, page 28-68

Field Reference

Table 28-54 Add or Edit Client Update Dialog Box

Element	Description
System Type	The platform on which the IOS VPN client operates. • All Windows (Default)—This option includes any Windows platform for which a VPN client is available. • Macintosh OS X
IOS Image URL	Enter the URL from where the client can be downloaded. The URL must start with http:// or https://.
IOS VPN Client Revisions	Enter the revision level of the VPN client. You can specify more than one client revision separated by commas.

User Group Dialog Box—Advanced PIX Options

The Advanced PIX Options are specifically for PIX 6.3 Firewalls in your user group.

Note These settings apply in Easy VPN and remote access VPN configurations.

Navigation Path

Select **Advanced Options (PIX)** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Field Reference

Table 28-55 User Group Dialog Box—Advanced PIX Options

Element	Description
User Idle Timeout (sec)	The length of time that a VPN tunnel can remain open without user activity, in seconds. Values range from 60-86400 seconds.
User Authentication Server	The AAA server to which remote devices send user authentication requests. Enter the name of the server group or click **Select** to select it from a list or to create a new group. See Understanding AAA Server and Server Group Objects, page 6-20.
Enable Device Pass-Through	Whether to use Media Access Control (MAC) addresses to bypass authentication for devices, such as Cisco IP phones, that do not support AAA authentication. When MAC-based AAA exemption is enabled, the device bypasses the AAA server for traffic that matches both the MAC address of the device and the IP address that was dynamically assigned by a DHCP server. Authorization services are disabled automatically when you bypass authentication. Accounting records continue to be generated (if enabled), but the username is not displayed.
Enable Secure Unit Authentication	Whether to provide increased security when allowing access to the device from a remote client. With Secure Unit Authentication (SUA), you can use one-time passwords, two-factor authentication, and similar authentication schemes to authenticate the remote device during Extended Authentication (Xauth). SUA is specified in the VPN policy on the device and is downloaded to the remote client. This enables SUA and determines the connection behavior of the remote client.
Enable User Authentication	Whether to enable Individual User Authentication (IUA), which supports individually authenticating clients on the inside network of the remote access VPN, based on the IP address of each inside client. IUA supports both static and OTP authentication mechanisms.

User Group Dialog Box—Clientless Settings

Use the Clientless settings to configure the clientless mode of access to the corporate network in an SSL VPN.

In clientless access mode, once a user is authenticated and a session is established, an SSL VPN portal page and toolbar is displayed on the user's web browser. From the portal page, the user can access all available HTTP sites, access web e-mail, and browse Common Internet File System (CIFS) file servers.

Navigation Path

Select **Clientless** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Related Topics

- Clientless and Thin Client Access Modes Page, page 27-8

Field Reference

Table 28-56 User Group Dialog Box—Clientless Settings

Element	Description
Portal Page Websites	The name of the SSL VPN bookmarks policy object that includes the web site URLs to display on the portal page. These web sites help users access desired resources. Enter the name of the object or click **Select** to select it from a list or to create a new object.
Allow Users to Enter Websites	Whether to allow the remote user to enter web site URLs directly into the browser. If you do not select this option, the user can access only those URLs included on the portal.
Enable Common Internet File System (CIFS)	In Clientless mode, files and directories created on Microsoft Windows servers can be accessed by the remote client through the web browser. When you enable the Common Internet File System (CIFS), a list of file server and directory links are displayed on the portal page after login. The CIFS protocol lets you customize permissions on the SSL VPN gateway to allow shared files to be accessed or modified by the remote client, as follows: • **Enable File Browsing**—Whether to allow the remote user to browse for file shares on the CIFS file servers. • **Enable File Entry**—Whether to allow the remote user to locate file shares on the CIFS file servers by entering the names of the file shares.
WINS Server List	The name of the WINS server list policy object that identifies the WINS/NetBIOS servers to use for resolving file server names. You should supply an object if you enable CIFS. Enter the name of the object or click **Select** to select if from a list or to create a new object.
Enable Citrix	Whether to enable remote clients to run Citrix-enabled applications, such as Microsoft Word or Excel, through the SSL VPN as if the application were locally installed, without the need for client software. The Citrix software must be installed on one or more servers on a network that the router can reach.

User Group Dialog Box—Thin Client Settings

Use the Thin Client settings to enable the thin client, or port forwarding, mode of access to the corporate network in an SSL VPN. Port forwarding allows users to access applications (such as Telnet, e-mail, VNC, SSH, and Terminal services) inside the enterprise through an SSL VPN session. A port forwarding list object defines the mappings of port numbers on the remote client to the application's IP address and port behind the SSL VPN gateway.

In thin client access mode, the remote user downloads a Java applet that acts as a TCP proxy on the client machine for the services configured on the SSL VPN gateway. The proxy provides the port forwarding services.

Navigation Path

Select **Thin Client** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Related Topics

- Clientless and Thin Client Access Modes Page, page 27-8

Field Reference

Table 28-57 User Group Dialog Box—Thin Client Settings

Element	Description
Enable Thin Client	Whether to allow thin client access to the SSL VPN.
Port Forward List	The name of the port forwarding list policy object assigned to this group. Port forwarding lists contain the set of applications that users of clientless SSL VPN sessions can access over forwarded TCP ports. Enter the name of the object or click **Select** to select it from a list or to create a new object.
Download Port Forwarding Applet on Client Login	Whether the port forwarding Java applet should be automatically downloaded to the client when a user logs into the SSL VPN. If you do not automatically download the applet, users must download it manually after login.

User Group Dialog Box—SSL VPN Full Tunnel Settings

Use the SSL VPN Full Tunnel settings to enable the full tunnel client access mode in your SSL VPN. When you enable full tunnel access, you should also define DNS/WINS server settings, browser proxy settings, and split tunneling for the user group.

In full tunnel client access mode, the tunnel connection is determined by the group policy configuration. The full tunnel client software, SSL VPN Client (SVC), must be downloaded to the remote client so that a tunnel connection can be established when the remote user logs in to the SSL VPN gateway.

Tip For full tunnel client access to work, you must install the client software on the gateway. The user downloads the client when connecting to the gateway.

Navigation Path

Select **Full Tunnel > Settings** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Related Topics

- Full Tunnel Dialog Box, page 27-7

Field Reference

Table 28-58 User Group Dialog Box—Full Tunnel Settings

Element	Description
Enable Full Tunnel	Whether to enable full tunnel client access to the SSL VPN.
Use Other Access Modes if SSL VPN Client Download Fails	Whether to allow users to connect to the SSL VPN even if a problem prevents the client from downloading, installing, and starting correctly on the user's system.
Full Tunnel Only	If you select **Full Tunnel Only**, a user cannot connect to the SSL VPN if the download fails, which locks the user out of the network. Select **Use Other Access Modes** to allow clientless or thin client access if there is a download problem.
Client IP Address Pool	The IP address ranges of the address pool that full tunnel clients will draw from when they log on. The address pool must be in the same subnet as one of the device's interface IP addresses. Enter the address range separating the first and last IP address with a hyphen, for example, **10.100.10.2-10.100.10.255**. If you enter a single address, the pool has just one address. Do not enter subnet designations. You can also enter the name of a network/host policy object that defines the range, or click **Select** to select the object from a list or to create a new object. Separate multiple ranges with commas.
Filter ACL	The name of an extended access control list (ACL) object that restricts access to the SSL VPN. Enter the name of the object or click **Select** to select it from a list or to create a new object.
Keep SSL VPN Client on Client Computer	Whether to leave the full client installed on the user's workstation after the user disconnects. If you do not allow the client to remain on the user's system, the client must be downloaded each time the user establishes a connection to the SSL VPN gateway.
Home Page URL	The web address of the login home page for the full client.
Client Dead Peer Detection Timeout	The time interval that the Dead Peer Detection (DPD) timer is reset each time a packet is received over the SSL VPN tunnel from the remote user. Enter a value in the range 1-3600 seconds.

Table 28-58 User Group Dialog Box—Full Tunnel Settings (Continued)

Element	Description
Gateway Dead Peer Detection Timeout	The time interval that the Dead Peer Detection (DPD) timer is reset each time a packet is received over the SSL VPN tunnel from the gateway. Enter a value in the range 1-3600 seconds.
Key Renegotiation Method	The method by which the tunnel key is refreshed for the remote user group client: • **Disabled**—Disables the tunnel key refresh. • **Create New Tunnel**—Initiates a new tunnel connection. Enter the time interval (in seconds) between the tunnel refresh cycles in the **Interval** field.

User Group Dialog Box—SSL VPN Split Tunneling

Use the Split Tunneling settings to configure a secure tunnel to the central site and simultaneous clear text tunnels to the Internet for SSL VPNs.

Split tunneling lets a remote client conditionally direct packets over an IPsec or SSL VPN tunnel in encrypted form or to a network interface in clear text form. With split tunneling enabled, packets not bound for destinations on the other side of the tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. The split tunneling policy is applied to specific networks.

Tip For optimum security, we recommend that you not enable split tunneling.

Navigation Path

Select **Full Tunnel > Split Tunneling** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Field Reference

Table 28-59 User Group Dialog Box—Split Tunneling Settings

Element	Description
Tunnel Option	Whether to allow split tunneling and if so, which traffic should be secured or transmitted unencrypted across the public network: • Disabled—(Default) No traffic goes in the clear or to any other destination than the gateway. Remote users reach networks through the corporate network and do not have access to local networks. • Tunnel Specified Traffic—Tunnel all traffic from or to the addresses listed in the **Destinations** field. Traffic to all other addresses travels in the clear and is routed by the remote user's Internet service provider. • Exclude Specified Traffic—Traffic goes in the clear from and to the addresses listed in the **Destinations** field. This 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.
Destinations	The IP addresses for hosts or networks that identify the networks that require traffic to travel across the tunnel and those that do not require tunneling. Whether traffic to these addresses is encrypted and tunneled to the gateway, or sent in the clear, is determined by your selection for **Tunnel Option**. Enter network addresses such as 10.100.10.0/24 or host addresses such as 10.100.10.12. You can also enter the name of a network/host policy object, or click **Select** to select the object from a list or to create a new object. Separate multiple addresses with commas.
Exclude Local LANs	Whether to exclude local LANs from the encrypted tunnel. This option is available only if you selected the **Exclude Specified Traffic** tunnel option. By selecting this option, you do not have to enter local LAN addresses into the destinations field to allow users to communicate with systems (such as printers) that are attached to their LAN. When selected, this attribute disallows a non split-tunneling connection to access the local subnetwork at the same time as the client.
Split DNS Names	A list of domain names to be resolved through the split tunnel to the private network. All other names are resolved using the public DNS server. Enter up to 10 entries in the list of domains, separated by commas. The entire string can be no longer than 255 characters.

User Group Dialog Box—Browser Proxy Settings

Use the Browser Proxy settings to configure proxy bypass for full tunnel access in an SSL VPN.

A security appliance can terminate HTTPS connections and forward HTTP/HTTPS requests to HTTP and HTTPS proxy servers, which act as intermediaries between users and the Internet. Proxy bypass is an alternative method of content rewriting that makes minimal changes to the original content. It is useful with custom web applications.

Tip The browser proxy settings work only for Microsoft Internet Explorer; they do not work for other types of browsers.

Navigation Path

Select **Full Tunnel > Browser Proxy Settings** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Related Topics

- Defining Proxies and Proxy Bypass Rules, page 26-51

Field Reference

Table 28-60 User Group Dialog Box—Browser Proxy Settings

Element	Description
Browser Proxy Option	Whether and how to configure proxy settings on the remote client's browser: • Blank—Do not configure proxy settings. • Do Not Use Proxy Server—Configure the browser to not use a proxy. • Automatically Detect Settings—Configure the browser to automatically detect proxy settings. • Bypass Proxy Server for Local Addresses—Configure the browser to bypass proxy settings configured by the user.
Proxy Server	The address of the proxy server: • IP address—The IP address or the name of a network/host object that specifies the address. Click **Select** to select the object from a list. • Name—The fully qualified domain name, for example, proxy.example.com.
Proxy Server Port	The port number on the server that is used for proxy traffic, for example, 80. Enter a value in the range 1-65535.
Do Not Use Proxy Server for Addresses Beginning With	If you configured a proxy, you can identify specific hosts for which the proxy should be bypassed. If the user opens these hosts in the browser, the proxy is not used in the connection. Enter full IP addresses or fully qualified domain names. For example, 10.100.10.14 or www.cisco.com.

User Group Dialog Box—SSL VPN Connection Settings

Use this SSL VPN Connection Settings page to configure the SSL VPN session connection settings for the user group, including the banner text. An SSL VPN session is disconnected if the client is connected longer than the session timeout or if it is idle longer than the idle timeout.

Navigation Path

Select **Connection Settings** from the table of contents in the Add or Edit User Group Dialog Box, page 28-68.

Field Reference

Table 28-61 User Group Dialog Box—Connection Settings

Element	Description
Idle Timeout	The idle timeout period for the SSL VPN session. The session is disconnected if the client is idle longer than the specified idle timeout. Values range from 0-3600 seconds.
Session Timeout	The timeout period for the SSL VPN session. The session is disconnected when this timeout is reached even if the user is still active. Values range from 1-1209600 seconds.
Banner Text	The banner, for example, a welcome message, that is displayed to remote users when they connect to the SSL VPN. You cannot use double quotes or new lines (carriage returns) in the banner text. However, you can include HTML tags to create the desired layout.

Add or Edit WINS Server List Dialog Box

Use the WINS Server Lists dialog box to create, copy, and edit WINS server list objects. A WINS Server List object defines a list of Windows Internet Naming Server (WINS) servers, which are used to translate Windows file server names to IP addresses.

Navigation Path

Select **Tools > Policy Object Manager**, then select **WINS Server Lists** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Configuring WINS/NetBIOS Name Service (NBNS) Servers To Enable File System Access in SSL VPNs, page 26-73
- Policy Object Manager Window, page 6-3

Field Reference

Table 28-62 WINS Server Lists Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-6.
Description	An optional description of the object.
WINS Server List	The WINS servers that are defined for the object. • To add a server, click the Add button and fill in the Add WINS Server dialog box (see Add or Edit WINS Server Dialog Box, page 28-85). • To edit a server, select it and click the Edit button. • To delete a server, select it and click the Delete button.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-13 and Understanding Policy Object Overrides for Individual Devices, page 6-13. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add or Edit WINS Server Dialog Box

Use the Add/Edit WINS Server dialog box to create a new WINS server entry or edit an existing entry in the table in the WINS Server Lists dialog box.

Navigation Path

From the Add or Edit WINS Server List Dialog Box, click the **Add** button beneath the WINS Server List table, or select a server in the table and click the **Edit** button.

Related Topics

- Configuring WINS/NetBIOS Name Service (NBNS) Servers To Enable File System Access in SSL VPNs, page 26-73

Field Reference

Table 28-63 Add/Edit WINS Server Dialog Box

Element	Description
Server	The IP address of the WINS server used to translate Windows file server names to IP addresses. You can also enter the name of a network/host policy object that identifies the server. Click **Select** to choose a network/hosts object or to create a new object.
Set as Master Browser	Whether to server is a master browser. The master browser maintains the list of computers and shared resources.

Table 28-63 Add/Edit WINS Server Dialog Box (Continued)

Element	Description
Timeout	The period of time the security appliance waits for a response to a WINS query before sending the query again to the same server (if it is the only one), or to the next server (if there is more than one). The default timeout is 2 seconds. The range is between 1 and 30 seconds.
Retries	The number of times to retry sending WINS queries to the configured servers. The security appliance recycles through the list of servers this number of times before sending an error message. The default is 2. The range is between 0 and 10.