



SSL VPN User Interface Reference

The pages that you access by selecting the **SSL VPN** folder from the **Policy selector** in **Device View** help you configure SSL VPNs. The following topics describe the pages that help you to create SSL VPNs for Cisco 870, 1800, 2800, 3700, 3800, 7200, and 7301 Series routers running IOS software version 12.4(6)T and later, and Adaptive Security Appliance (ASA) 5500 devices software version 7.1 and 7.2, and to configure the policies that will be assigned to them.

For more information, see [Chapter 11, “Managing Remote Access VPNs”](#).

**Note**

You must have read-write permissions to modify an SSL VPN policy. For more information, see [Modify Policies Permissions, page 2-13](#).

These topics describe the main pages available from the SSL VPN folder:

- [SSL VPN Server Wizard \(IOS\), page I-2](#)
- [User Groups Selector Page, page I-7](#)
- [Create User Group Wizard, page I-8](#)
- [SSL VPN Policy Page \(IOS\), page I-15](#)
- [SSL VPN Wizard for ASA Device, page I-23](#)
- [SSL VPN Access Policy Page, page I-29](#)
- [SSL VPN Connection Profiles Policy Page, page I-31](#)
- [ASA User Groups Policy Page, page I-46](#)
- [Cisco Secure Desktop Page \(ASA\), page I-48](#)
- [SSL VPN Global Settings Page, page I-49](#)

SSL VPN Server Wizard (IOS)

Use the SSL VPN wizard to configure a basic SSL VPN connection on your server device. The wizard creates the policies required for a basic SSL VPN to function. After configuring the wizard, you can create new policies or modify the connection from the SSL VPN folder.

**Note**

SSL VPN server configuration is supported on Cisco 870, 1800, 2800, 3700, 3800, 7200, and 7301 Series routers running IOS software version 12.4(6)T and later.

These topics describe the steps for configuring an SSL VPN connection on an IOS device, using the SSL VPN wizard:

- [Gateway and Context Page \(IOS\), page I-2](#)
- [Portal Page Customization Page, page I-5](#)

Navigation Path

1. Select **View > Device View** or click the **Device View** button on the toolbar.
2. From the Device Selector, select the IOS router on which you want to configure an SSL VPN connection.
3. Select **SSL VPN > SSL VPN Wizard** from the Policy selector.

Related Topics

- [Using the Wizard to Create an IOS SSL VPN Connection, page 12-7](#)

Gateway and Context Page (IOS)

A gateway and context must be configured on a device before a remote user can access resources on a private network behind the SSL VPN. Use this step of the SSL VPN wizard to specify a gateway and context configuration, including information that will allow users to access a portal page.

For more information about how to configure a gateway and context, see [Configuring an SSL VPN Gateway and Context, page 12-8](#).

Navigation Path

In Device view, open the [SSL VPN Server Wizard \(IOS\)](#), page I-2, then click **SSL VPN Server Wizard**.

Related Topics

- [SSL VPN Server Wizard \(IOS\)](#), page I-2
- [Configuring an SSL VPN Gateway and Context](#), page 12-8
- [Configuring User Groups on an IOS Device](#), page 12-18
- [Understanding SSL VPN Gateway Objects](#), page 9-208
- [Creating SSL VPN Gateway Objects](#), page 9-209
- [Understanding Port List Objects](#), page 9-168
- [Understanding AAA Server Group Objects](#), page 9-15

Field Reference

Table I-1 *SSL VPN Wizard—Gateway and Context Page*

Element	Description
Gateway	<p>The gateway to be used as a proxy for connections to the protected resources in your SSL VPN.</p> <p>Options are:</p> <ul style="list-style-type: none"> • Use Existing Gateway—When selected, enables you to use an existing gateway for your SSL VPN. • Create Using IP Address—When selected, enables you to configure a new gateway using a reachable (public static) IP address on the router. • Create Using Interface—When selected, enables you to configure a new gateway using the public static IP address of the router interface.
Gateway Name	<p>Specify the name of the gateway.</p> <p>If you selected to use an existing gateway, you can click Select to open a dialog box from which you can select a gateway from a list of SSL VPN gateway objects, or create a new gateway object.</p> <p>Note After selecting the gateway, the port number and digital certificate required to establish a secure connection are displayed in the relevant fields.</p>

Table I-1 **SSL VPN Wizard—Gateway and Context Page (Continued)**

IP Address	<p>Available only if you selected to create a new gateway using the router's IP address.</p> <p>Specify the IP address that will be used to configure the gateway.</p>
Interface	<p>Available only if you selected to create a new gateway using the router's interface.</p> <p>Specify the interface that will be used to configure the gateway. You can click Select to open a dialog box from which you can select an interface from a list of interface or interface role objects.</p>
Port	<p>Available only if you selected to create a new gateway using the router's IP address or interface.</p> <p>Specify the number of the port that will carry the HTTPS traffic (between 1024 and 65535). The default is 443, unless HTTP port redirection is enabled, in which case the default HTTP port number is 80.</p> <p>You can click Select to open the Port List Selector from which you can select a port list object. A port list object is a named definition of one or more port ranges that you use when defining service objects.</p>
Trustpoint	<p>Available only if you selected to create a new gateway using the router's IP address or interface.</p> <p>The digital certificate required to establish a secure connection. If you need to configure a specific CA certificate, a self-signed certificate is generated when an SSL VPN gateway is activated. All gateways on the router can use the same certificate.</p>
Context Name	<p>The name of the context that identifies the resources needed to support the SSL VPN tunnel between the remote clients and the corporate or private intranet.</p> <p>Tip To simplify the management of multiple context configurations, it is recommended to use the domain or virtual hostname for the context name.</p>
Portal Page URL	<p>The URL that will be displayed on the Portal page to access the SSL VPN gateway.</p>

Table I-1 **SSL VPN Wizard—Gateway and Context Page (Continued)**

User Groups	<p>The names of the user groups that will be used in your SSL VPN connection, and whether Full Tunnel access mode is enabled or disabled for them (see Configuring User Groups on an IOS Device, page 12-18).</p> <p>You can click Edit to open the User Groups Selector, in which you can select the required user groups, and from which you can create and edit user groups. See User Groups Selector Page, page I-7.</p>
Authentication Server Group	<p>The name of the authentication server group (LOCAL if the users are defined on the local device).</p> <p>You can click Select to open a dialog box from which you can select an AAA server group from a list of AAA server group objects.</p>
Authentication Domain	<p>Specifies a list or method for SSL VPN remote user authentication.</p> <p>Note If you do not specify a list or method, the SSL VPN gateway uses global AAA parameters for remote-user authentication.</p>
Accounting Server Group	<p>The name of the accounting server group.</p> <p>You can click Select to open a dialog box from which you can select an AAA server group from a list of AAA server group objects.</p>

Portal Page Customization Page

Use this step of the SSL VPN wizard to define the appearance of the portal page. The portal page allows the remote user access to all websites available on the SSL VPN networks.

Navigation Path

1. In Device view, open the [SSL VPN Server Wizard \(IOS\), page I-2](#), and click **SSL VPN Server Wizard**.
2. In the [Gateway and Context Page \(IOS\), page I-2](#), click **Next**.

Related Topics

- [Customizing the SSL VPN Portal Page, page 12-10](#)
- [SSL VPN Server Wizard \(IOS\), page I-2](#)
- [Configuring an SSL VPN Policy \(IOS\), page 12-11](#)

Field Reference

Table I-2 SSL VPN Wizard—Portal Page Customization Page

Element	Description
Title	The title that is displayed in the title bar of the portal page. The default title is “SSL VPN Service”.
Logo	The logo to be displayed on the title bar of the SSL VPN login and portal page. Options are: <ul style="list-style-type: none"> • None—No logo is displayed. • Default—To use the default logo. • Custom—When selected, enables you to specify your own logo. Specify the source image file for the logo in the Logo File field, or click Select to select an image file. The source image file for the logo can be a gif, jpg, or png file, with a filename of up to 255 characters, and up to 100 kilobytes in size.
Login Message	The message that will be displayed to the user upon login.
Primary Title Color	The color of the title bars on the login and portal pages of the SSL VPN. Click Select to open a dialog box in which you can choose the required color for the title bars.
Secondary Title Color	The color of the secondary title bars on the login and portal pages of the SSL VPN. Click Select to open a dialog box in which you can choose the required color for the secondary title bars.
Primary Text Color	The color of the text on the title bars of the login and portal pages. Options are white or black (the default). Note The color of the text must be aligned with the color of the text on the title bar.
Secondary Text Color	The color of the text on the secondary title bars of the login and portal pages. Options are white or black (the default). Note The color of the text must be aligned with the color of the text on the secondary title bar.

Table I-2 **SSL VPN Wizard—Portal Page Customization Page (Continued)**

Preview	A preview of how the portal page will appear.
---------	---

User Groups Selector Page

**Note**

The User Groups Selector is available if the selected device is a Cisco IOS router or ASA device.

In the User Groups Selector page you can select the user group(s) that will be used in your SSL VPN connection. From this page, you can open the User Group wizard in which you can create a new user group. See [Create User Group Wizard, page I-8](#).

Navigation Path

In Device view, select the required device in the Device selector.

- If you selected an IOS router:
 - Open the [SSL VPN Server Wizard \(IOS\), page I-2](#), and click **SSL VPN Server Wizard**.
 - On the [Gateway and Context Page \(IOS\), page I-2](#), click **Edit** alongside the User Groups table.
- If you selected an ASA device:
 - Open the [SSL VPN Wizard for ASA Device, page I-23](#), click **SSL VPN Server Wizard**, then click **Next** on the [Access Page \(ASA\), page I-23](#) Access Page (ASA).
 - On the [Connection Profile Page \(ASA\), page I-25](#), click **Edit** alongside the User Groups table.

Related Topics

- [SSL VPN Server Wizard \(IOS\), page I-2](#)
- [Understanding User Groups in SSL VPN, page 12-17](#)
- [Configuring User Groups on an IOS Device, page 12-18](#)
- [Configuring User Groups on an ASA Device, page 12-19](#)

- [Creating User Group Objects, page 9-199](#)

Field Reference

Table I-3 **User Groups Selector Page**

Element	Description
Available User Groups	<p>Lists the predefined user groups available for selection.</p> <p>Select the required user group(s) and click >>.</p> <p>If the required user group is not included in the list, click Create to open the Create User Group Wizard in which you can create a user group. See Create User Group Wizard, page I-8.</p> <p>In Security Manager, user groups are objects. To modify the properties of a user group, select it and click Edit. The Edit User Groups dialog box opens, enabling you to edit the user group object.</p>
Selected User Groups	<p>Displays the selected user groups.</p> <p>To remove user group(s) from this list, select them and click <<.</p> <p>To modify the properties of a user group, select it and click Edit. The Edit User Groups dialog box opens, enabling you to edit the user group object.</p> <p>Note To specify a user group as the default user group, select it and click Set As Default. This option is only available for an IOS router.</p>
>> button	Click to move selected user group(s) from the Available User Groups list to the Selected User Groups list.
<< button	Click to remove selected user group(s) from the Selected User Groups list to the Available User Groups list.
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.</p>

Create User Group Wizard

Use the Create User Group wizard to create a new user group that will be configured on an IOS router or ASA device in your SSL VPN connection.

These pages describe the configuration steps of the Create User Group wizard:

- [Name and Access Method Page, page I-9](#)
- [Full Tunnel Access Mode Page, page I-10](#)
- [Clientless and Thin Client Access Modes Page, page I-13](#)

Navigation Path

1. In Device view, select the required IOS or ASA device.
2. Select **SSL VPN > SSL VPN Wizard**, then click **SSL VPN Server Wizard**.
3. Open the User Groups Selector page as follows:
 - If you selected an IOS router, click **Edit** alongside the User Groups table in the Gateway and Context page.
 - If you selected an ASA device, click **Next** in the Access page, then click **Edit** alongside the User Groups table in the Connection Profiles page.
4. In the [User Groups Selector Page, page I-7](#), click **Create**. The Create User Group wizard opens, displaying the Name and Access Method page opens.

Related Topics

- [Understanding User Groups in SSL VPN, page 12-17](#)
- [Configuring User Groups on an IOS Device, page 12-18](#)
- [Configuring User Groups on an ASA Device, page 12-19](#)
- [Creating a New User Group, page 12-21](#)

Name and Access Method Page

Use this step of the Create User Group wizard to define a name for your user group, and optionally, select the remote access method(s) that will be used to access the SSL-enabled gateway (IOS router) or ASA security appliance.

Navigation Path

In the [User Groups Selector Page, page I-7](#), click **Create**.

Related Topics

- [Create User Group Wizard, page I-8](#)
- [SSL VPN Access Modes, page 12-3](#)

- [Full Tunnel Access Mode Page, page I-10](#)
- [Clientless and Thin Client Access Modes Page, page I-13](#)

Field Reference

Table I-4 Create User Group Wizard—Name and Access Method Page

Element	Description
Name	The name of the user group. You can enter up to 128 characters, including uppercase and lowercase characters and most alphanumeric or symbol characters.
Access Method	Select the required remote access mode option(s), as follows: <ul style="list-style-type: none"> • Full Tunnel—To access to the corporate network completely over an SSL VPN tunnel. This is the recommended option. • Clientless—To access the internal or corporate network using a web browser on the client machine. • Thin Client—To download a Java applet that acts as a TCP proxy on the client machine.

Full Tunnel Access Mode Page

This page is only available if you selected the **Full Tunnel** option in step 1 of the wizard ([Name and Access Method Page, page I-9](#)).

In the Full Tunnel page of the Create User Group wizard, you can configure the Full Tunnel Client mode that enables access to the corporate network completely over an SSL VPN tunnel.



Note

The SSL VPN Client (SVC) software must be installed on the device in order for Full tunnel mode to work properly.

The SVC is managed using a FlexConfig policy. For more information, see [Predefined FlexConfig Policy Objects, page 20-8](#).

Navigation Path

In Device view, open the [Create User Group Wizard, page I-8](#), select the **Full Tunnel** access method option, then click **Next**.

Related Topics

- [Create User Group Wizard, page I-8](#)
- [SSL VPN Access Modes, page 12-3](#)
- [Configuring the Full Tunnel Access Mode, page 12-23](#)

Field Reference

Table I-5 *Create User Group Wizard—Full Tunnel Page*

Element	Description
Use Other Access Modes if SSL VPN Client Download Fails	<p>When selected, enables the remote client to use clientless or thin client access modes if the SVC download fails.</p> <p>Note For the full tunnel access mode to work properly, the SSL VPN Client (SVC) software must be installed on the device.</p>
Full Tunnel	<p>When selected, enables the Full Tunnel access mode to be configured.</p> <p>Note For the full tunnel access mode to work properly, the SSL VPN Client (SVC) software must be installed on the device.</p>
Client IP Address Pools	<p>Available only if the selected device is an IOS router.</p> <p>The IP address ranges of the address pool that full tunnel clients will draw from, when they log on.</p> <p>You can click Select to open the Networks/Hosts Selector from which you can make your selection(s).</p>
Primary DNS Server	<p>The IP address of the primary DNS server to be used for the Full Tunnel SSL VPN connection.</p> <p>You can click Select to open the Networks/Hosts Selector from which you can make your selection.</p>
Secondary DNS Server	<p>The IP address of a secondary DNS server to be used for the Full Tunnel SSL VPN connection.</p> <p>You can click Select to open the Networks/Hosts Selector from which you can make your selection.</p>

Table I-5 Create User Group Wizard—Full Tunnel Page (Continued)

Default DNS Domain	The domain name of the DNS server to be used for the Full Tunnel SSL VPN connection.
Primary WINS Server	The IP address of the primary WINS server to be used for the Full Tunnel SSL VPN connection. You can click Select to open the Networks/Hosts Selector from which you can make your selection.
Secondary WINS Server	The IP address of a secondary WINS server to be used for the Full Tunnel SSL VPN connection. You can click Select to open the Networks/Hosts Selector from which you can make your selection.
Split Tunnel Option	Specifies the traffic that will be secured or transmitted unencrypted across the public network: <ul style="list-style-type: none"> • Disabled—Split tunneling is disabled and no traffic will be secured. • Exclude Specified Networks—Split tunneling is enabled. You can specify the networks to which traffic is transmitted in the clear (unencrypted). • Tunnel Specified Networks—Split tunneling is enabled. All traffic from or to the specified networks will be secured.
Destinations	Available if the selected device is an IOS router and split tunneling is enabled. The specified networks to which traffic is transmitted secured or unencrypted, depending on the selected Split Tunneling option. Multiple entries are separated by commas. Accepted formats are: <ul style="list-style-type: none"> • <i>a.b.c.d</i> where <i>a,b,c,d</i> = 0-255 (host). • <i>a.b.c.d/e</i> where <i>a,b,c,d</i> = 0-255 and <i>e</i> = 1-32 (subnet). • <i>a.b.c.d-e.f.g.h</i> where <i>a,b,c,d,e,f,g,h</i> = 0-255 (range). • Freeform text that is the name of the network/host object. You can click Select to open the Networks/Hosts Selector from which you can make your selection(s) from a list of available network and host objects.

Table I-5 **Create User Group Wizard—Full Tunnel Page (Continued)**

Networks	<p>Available if the selected device is an ASA security appliance and split tunneling is enabled.</p> <p>The networks to be used for split tunneling.</p> <p>Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of a list of addresses on the private network.</p> <p>You can click Select to open the Access Control Lists selector, from which you can select the required access control list.</p>
Exclude Local LANs	<p>Available if the selected device is an IOS router and split tunneling is enabled.</p> <p>When selected, disallows a non split-tunneling connection to access the local subnetwork at the same time as the client.</p>
Split DNS Names	<p>A list of domain names that must be tunneled or resolved to the private network. All other names will be resolved via the public DNS server.</p>

Clientless and Thin Client Access Modes Page

In the Clientless and Thin Client page of the Create User group wizard, you can configure the Clientless and/or Thin Client modes to be used for accessing the corporate network in your SSL VPN.

For more information about how to configure the Clientless and Thin Client access modes, see [Configuring the Clientless and Thin Client Access Modes, page 12-25](#).



Note

This page is only available if you selected the **Clientless** and/or **Thin Client** options in step 1 of the wizard ([Name and Access Method Page, page I-9](#)).

Navigation Path

In Device view, open the [Create User Group Wizard, page I-8](#), select the **Clientless** and/or **Thin Client** access method options, then click **Next**, or click **Next** in the Full Tunnel page.

Related Topics

- [Create User Group Wizard, page I-8](#)
- [Configuring the Clientless and Thin Client Access Modes, page 12-25](#)
- [SSL VPN Access Modes, page 12-3](#)
- [Understanding URL List Objects, page 9-196](#)
- [Understanding Port Forwarding List Objects, page 9-165](#)

Field Reference**Table I-6 Create User Group Wizard—Clientless and Thin Client Page**

Element	Description
Clientless	
Portal Page Websites	<p>A list of websites that will be displayed on the portal page as a bookmark to enable users to access the resources available on the SSL VPN websites.</p> <p>You can click Select to open the URL List Selector from which you can select the required URL List from a list of URL List objects.</p>
Allow Users to Enter Websites	When selected, enables remote users to input the website URLs directly.
Thin Client	
Port Forwarding List	<p>The Port Forwarding List, that defines the mapping of the port number on the client machine to the application's IP address and port behind the SSL VPN gateway.</p> <p>You can click Select to open the Port Forwarding List Selector from which you can select the required Port Forwarding List from a list of Port Forwarding List objects.</p>
Port Forwarding Applet Name	<p>Available only if the selected device is an ASA security appliance.</p> <p>The Java applet that will be used as a TCP proxy on the client machine. The Java applet starts a new SSL connection for every client connection.</p> <p>The Java applet initiates an HTTP request from the remote user client to the ASA device. The name and port number of the internal email server is included in the HTTP request. A TCP connection is created to that internal email server and port.</p>

Table I-6 Create User Group Wizard—Clientless and Thin Client Page (Continued)

Download Port Forwarding Applet on Client Login	When selected, enables a port-forwarding Java applet to be automatically downloaded when the remote client logs in.
---	---

SSL VPN Policy Page (IOS)

Use this page to view the SSL VPN connection policies currently defined on your IOS router. From this page, you can create, edit, or delete SSL VPN policies.

For more information, see [Configuring an SSL VPN Policy \(IOS\)](#), page 12-11.

Navigation Path

1. Select **View > Device View** or click the **Device View** button on the toolbar.
2. From the Device Selector, select the IOS router on which you want to view or configure an SSL VPN policy.
3. Select **SSL VPN > SSL VPN Policy** from the Policy selector.

Related Topics

- [Working with SSL VPN Policies](#), page 12-5
- [Configuring SSL VPN on an IOS Device](#), page 12-6
- [SSL VPN Context Editor Dialog Box \(IOS\)](#), page I-16

Field Reference

Table I-7 SSL VPN (IOS) Policy Page

Element	Description
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables , page 3-24.
Name	The name of the context that defines the virtual configuration of the SSL VPN. Note To simplify the management of multiple context configurations, the context name should be the same as the domain or virtual hostname.

Table I-7 **SSL VPN (IOS) Policy Page (Continued)**

Gateway	The gateway defined for the SSL VPN connection.
Domain	The domain or virtual hostname of the SSL VPN connection.
Status	The current status of the SSL VPN connection—In Service or Out of Service.
Policies	The user groups associated with the SSL VPN connection.
Create button	Click to open the SSL VPN Context Editor to create an SSL VPN policy. See SSL VPN Context Editor Dialog Box (IOS) , page I-16.
Edit button	Select a row of an SSL VPN policy in the table, then click to open the SSL VPN Context Editor to edit its properties. See SSL VPN Context Editor Dialog Box (IOS) , page I-16.
Delete button	Select the rows of one or more SSL VPN policies, then click to remove from the list.

SSL VPN Context Editor Dialog Box (IOS)

Use this dialog box to create or modify an SSL VPN policy (context). For more information, see [Configuring an SSL VPN Policy \(IOS\)](#), page 12-11.

These tabs are available on the SSL VPN Context Editor dialog box:

- [General Tab](#), page I-17
- [Portal Page Tab](#), page I-19
- [Secure Desktop Tab](#), page I-20
- [Advanced Tab](#), page I-22

Navigation Path

Open the [SSL VPN Policy Page \(IOS\)](#), page I-15, then click **Create**, or select a policy in the table and click **Edit**. For more information, see [Table I-7 on page I-15](#). The SSL VPN Context Editor opens with the General tab displayed.

General Tab

Use the General tab of the SSL VPN Context Editor dialog box to define or edit the general settings required for an SSL VPN policy. General settings include specifying the gateway, domain, AAA servers for accounting and authentication, and user groups.

Navigation Path

The General tab appears when you open the [SSL VPN Context Editor Dialog Box \(IOS\)](#), page I-16. You can also open it by clicking the **General** tab from any other tab in the SSL VPN Context Editor dialog box.

Related Topics

- [Configuring General Settings for an IOS SSL VPN Policy](#), page 12-11
- [SSL VPN Context Editor Dialog Box \(IOS\)](#), page I-16
- [Understanding SSL VPN Gateway Objects](#), page 9-208
- [Understanding AAA Server Group Objects](#), page 9-15
- [Creating User Group Objects](#), page 9-199

Field Reference

Table I-8 *SSL VPN Context Editor > General Tab (IOS)*

Element	Description
Name	The name of the context that defines the virtual configuration of the SSL VPN. Note To simplify the management of multiple context configurations, the context name is the same as the domain or virtual hostname.
Gateway	The gateway to be used in the SSL VPN policy. You can click Select to open a dialog box from which you can select the gateway from a list of SSL VPN gateway objects. A gateway object provides the interface and port configuration for an SSL VPN connection.
Domain	The domain or virtual hostname of the SSL VPN connection.
Portal Page URL	The URL that will appear on the Portal page enabling a user to access the SSL VPN gateway.

Table I-8 SSL VPN Context Editor > General Tab (IOS) (Continued)

Enable SSL VPN	When selected, activates the SSL VPN connection, putting it “In Service”. When deselected, puts the SSL VPN connection “Out of Service”.
Authentication Server Group	The authentication server group (LOCAL if the users are defined on the local device). You can click Select to open a dialog box from which you can select an AAA server group from a list of AAA server group objects.
Authentication Domain	A list or method for SSL VPN remote user authentication. Note If a list or method is not specified, the SSL VPN gateway uses global AAA parameters for remote-user authentication.
Accounting Server Group	The accounting server group. You can click Select to open a dialog box from which you can select an AAA server group from a list of AAA server group objects.
User Groups	A table listing the user group(s) that will be used in your SSL VPN policy. User groups define the resources available to users when connecting to an SSL VPN gateway. Using the buttons below the table, you can add user groups, edit their properties, and delete them from the table.
Create button	Click to add a user group(s) to the User Groups table. The User Groups Selector Page, page I-7 opens, from which you can select the required user group(s). If the required user group is not included in the Selector, click Create to open the Add User Group dialog box in which you can create a new user group object.
Edit button	Select a user group in the User Groups table, then click Edit to modify its properties. The Edit User Group dialog box opens, enabling you to edit the user group object.
Delete button	Select the rows of one or more user groups, then click to remove from the table.

Table I-8 **SSL VPN Context Editor > General Tab (IOS) (Continued)**

OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.</p>
-----------	---

Portal Page Tab

Use the Portal Page tab of the SSL VPN Context Editor dialog box to define or edit the customization of the login page and portal page for the SSL VPN policy.

Navigation Path

Open the [SSL VPN Context Editor Dialog Box \(IOS\)](#), page I-16, then click the **Portal Page** tab.

Related Topics

- [Configuring the Portal Page for an IOS SSL VPN Policy](#), page 12-13
- [SSL VPN Context Editor Dialog Box \(IOS\)](#), page I-16

Field Reference

Table I-9 **SSL VPN Context Editor > Portal Page Tab (IOS)**

Element	Description
Title	<p>The title displayed in the title bar of the portal page.</p> <p>The default title is “SSL VPN Service”.</p>
Logo	<p>The logo displayed on the title bar of the SSL VPN login and portal page.</p> <p>Options are:</p> <ul style="list-style-type: none"> • None—No logo is displayed. • Default—To use the default logo. • Custom—When selected, enables you to specify your own logo. Specify the source image file for the logo in the Logo File field, or click Select to select an image file. <p>The source image file for the logo can be a gif, jpg, or png file, with a filename of up to 255 characters, and up to 100 kilobytes in size.</p>

Table I-9 **SSL VPN Context Editor > Portal Page Tab (IOS) (Continued)**

Login Message	The message that will be displayed to the user upon login.
Primary Title Color	The color of the title bars on the login and portal pages of the SSL VPN. Click Select to open a dialog box in which you can choose the required color for the title bars.
Secondary Title Color	The color of the secondary title bars on the login and portal pages of the SSL VPN. Click Select to open a dialog box in which you can choose the required color for the secondary title bars.
Primary Text Color	The color of the text on the title bars of the login and portal pages. Options are white or black (the default). Note The color of the text must be aligned with the color of the text on the title bar.
Secondary Text Color	The color of the text on the secondary title bars of the login and portal pages. Options are white or black (the default). Note The color of the text must be aligned with the color of the text on the secondary title bar.
Preview	A preview of how the portal page will appear.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Secure Desktop Tab

Use the Secure Desktop tab to configure the Cisco Secure Desktop (CSD) software on your selected IOS router.

Cisco Secure Desktop (CSD) provides a single, secure location for session activity and removal on the client system, ensuring that sensitive data is shared only for the duration of an SSL VPN session. For more information, see [Configuring the Secure Desktop Software for an IOS SSL VPN Policy, page 12-15](#).

**Note**

The Secure Desktop Client software must be installed and activated on a device in order for an SSL VPN policy to work properly.

The CSD is managed using a FlexConfig policy. For more information, see [Predefined FlexConfig Policy Objects, page 20-8](#).

Navigation Path

Open the [SSL VPN Context Editor Dialog Box \(IOS\), page I-16](#), then click the **Secure Desktop** tab.

Related Topics

- [Configuring the Cisco Secure Desktop Software, page 12-44](#)
- [SSL VPN Context Editor Dialog Box \(IOS\), page I-16](#)
- [Understanding Secure Desktop Configuration Objects, page 9-171](#)

Field Reference

Table I-10 **SSL VPN Context Editor > Secure Desktop Tab (IOS)**

Element	Description
Enable	When selected, enables the CSD on the device.
Configuration	Specify the filename of the CSD distribution package to install into the running configuration (the securedesktop_asa_<n>_<n>*.pkg file to be uploaded from your local computer to the flash device). You can click Select to open the Secure Desktops Selector from which you can select a CSD distribution package file from a list of CSD distribution package objects.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Advanced Tab

Use the Advanced tab of the SSL VPN Context Editor dialog box to define or edit the maximum number of SSL VPN users, and other advanced settings required for an SSL VPN policy.

Navigation Path

Open the [SSL VPN Context Editor Dialog Box \(IOS\)](#), page I-16, then click the **Advanced** tab.

Related Topics

- [Configuring Advanced Settings for an IOS SSL VPN Policy](#), page 12-16
- [SSL VPN Context Editor Dialog Box \(IOS\)](#), page I-16

Field Reference

Table I-11 **SSL VPN Context Editor > Advanced Tab (IOS)**

Element	Description
Maximum Number of Users	The maximum number of SSL VPN user sessions that can be configured. You can specify a value in the range 1-1000.
VRF Name	If Virtual Routing Forwarding (VRF) is configured on the device, the name of the VRF instance that is associated with the SSL VPN context. Note Only one VRF instance can be associated with each SSL VPN context. For information about VRF, see Understanding VRF-Aware IPsec , page 10-51.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

SSL VPN Wizard for ASA Device

Use the SSL VPN wizard to configure a basic SSL VPN connection profile on your server device. The wizard creates the policies required for a basic SSL VPN to function. After configuring the wizard, you can create new policies or modify the connection profile from the SSL VPN folder.

**Note**

SSL VPN server configuration is supported on ASA 5500 devices running software version 7.1 and 7.2.

**Note**

For security appliances running ASA 8.0 or 8.1, SSL VPN policies are not available for configuration from the Security Manager interface.

These topics describe the steps for configuring an SSL VPN connection profile on an ASA device:

- [Access Page \(ASA\), page I-23](#)
- [Connection Profile Page \(ASA\), page I-25](#)

Navigation Path

1. Select **View > Device View** or click the **Device View** button on the toolbar.
2. From the Device Selector, select the ASA device on which you want to configure an SSL VPN connection profile.
3. Select **SSL VPN > SSL VPN Wizard** from the Policy selector.

Related Topics

- [Using the Wizard to Create an ASA SSL VPN Connection Profile, page 12-27](#)

Access Page (ASA)

Use the Access page of the SSL VPN Configuration Wizard to configure the security appliance interfaces for SSL VPN sessions, select a port for SSL VPN connection profiles, and specify the URLs that will be displayed on the Portal page to access the connection profiles.

Navigation Path

In Device view, open the [SSL VPN Wizard for ASA Device, page I-23](#), then click **SSL VPN Wizard**.

Related Topics

- [SSL VPN Wizard for ASA Device, page I-23](#)
- [Defining the ASA SSL VPN Access Parameters, page 12-28](#)
- [Understanding Interface Role Objects, page 9-132](#)
- [Understanding Port List Objects, page 9-168](#)

Field Reference

Table I-12 **SSL VPN Wizard—Access Page (ASA)**

Element	Description
Interfaces	<p>Specify the interfaces on which you want to enable the SSL VPN connection profiles.</p> <p>You can click Select to open a dialog box from which you can select an interface from a list of interface or interface role objects.</p>
Port	<p>Specify the port number you want to use for the SSL VPN sessions.</p> <p>The default port is 443, for HTTPS traffic. The port number can be 443, or within the range of 1024-65535. If you change the port number, all current SSL VPN connections terminate, and current users must reconnect.</p> <p>Note If HTTP port redirection is enabled, the default HTTP port number is 80.</p> <p>You can click Select to open the Port List Selector dialog box from which you can make your selection, or create a new port list.</p>
Portal Page URLs	The URLs that will be displayed on the Portal page to access the SSL VPN connection profile.
Allow Users to Select Connection Profile in Portal Page	<p>When selected, enables you to select a tunnel group at login from a list of tunnel group connection profiles configured on the device. This is the default setting.</p> <p>When deselected, the user cannot select a tunnel group at login.</p>

Table I-12 **SSL VPN Wizard—Access Page (ASA) (Continued)**

Enable SSL VPN Access	When selected, enables the SSL VPN functionality on the ASA device. This is the default setting. When deselected, disables the SSL VPN functionality on the ASA device.
-----------------------	--

Connection Profile Page (ASA)

Use the Connection Profile page of the SSL VPN wizard to configure the tunnel group policies on your security appliance. You can specify a name for the tunnel connection profile policy that you are adding, select the user group policy, specify address pools for this policy, and specify authentication server group settings.

Navigation Path

1. In Device view, open the [SSL VPN Wizard for ASA Device, page I-23](#), click **SSL VPN Wizard**.
2. In the [Access Page \(ASA\), page I-23](#), click **Next**.

Related Topics

- [SSL VPN Wizard for ASA Device, page I-23](#)
- [Defining the ASA SSL VPN Connection Profile Parameters, page 12-29](#)
- [Configuring User Groups on an ASA Device, page 12-19](#)
- [Understanding ASA User Group Objects, page 9-42](#)
- [Understanding SSL VPN Customization Objects, page 9-203](#)
- [Understanding Network/Host Objects, page 9-144](#)
- [Understanding AAA Server Group Objects, page 9-15](#)

Field Reference

Table I-13 **SSL VPN Wizard—Connection Profile Page (ASA)**

Element	Description
Connection Profile Name	The name of the tunnel group that contains the policies for this SSL VPN connection profile.

Table I-13 **SSL VPN Wizard—Connection Profile Page (ASA) (Continued)**

Default User Group	<p>The default user group associated with the device.</p> <p>You can click Select to open the ASA User Groups Selector from which you can select a user group from a list of ASA user group objects.</p> <p>If the required default user group is not included in the list, click Create to open the Create User Group Wizard in which you can create a user group. See Create User Group Wizard, page I-8.</p> <p>ASA user groups are objects. If you want to modify the properties of a user group in the list, select it and click Edit. The Edit User Groups dialog box opens, enabling you to edit the user group object.</p>
Full Tunnel	<p>Indicates whether full tunnel access mode was configured for the user group or not.</p>
User Groups	<p>The names of the user groups that will be used in your SSL VPN connection profile, and whether Full Tunnel access mode is enabled or disabled for them.</p> <p>Note All SSL VPN connection profiles on an ASA device share one user group. Each time you create a connection profile using the wizard, the User Groups list may be populated with data from the previous connection profile defined on the device.</p> <p>Click Edit to open the User Groups Selector, in which you can select the required ASA user groups from a list of ASA user group objects. See User Groups Selector Page, page I-7.</p> <p>If a required user group is not included in the User Groups Selector, click Create to open the Create User Group Wizard in which you can create a user group. See Create User Group Wizard, page I-8.</p> <p>To modify the properties of a user group in the User Groups Selector, select it and click Edit. The Edit User Groups dialog box opens, enabling you to edit the user group object.</p>

Table I-13 **SSL VPN Wizard—Connection Profile Page (ASA) (Continued)**

Portal Page Customization	<p>Specify the customization profile that defines the appearance of the portal page that allows the remote user access to all the resources available on the SSL VPN networks.</p> <p>Customization profiles are predefined objects. You can click Select to open the SSL VPN Customization Selector dialog box that lists all available customization objects, from which you can make your selection.</p> <p>Note You can set up different login windows for different groups by using a combination of customization profiles and tunnel groups. For example, assuming that you had created a customization profile called salesgui, you can create an SSL VPN tunnel group called sales that uses that customization profile.</p>
Group URL	<p>The URL that is associated with the tunnel group connection profile. This URL provides users with direct access to the portal page of the tunnel group connection profile.</p> <p>A group URL is made up of the host name or IP address of the ASA device and port number, and the alias used to identify the SSL VPN connection profile.</p> <p>Select a protocol (http or https) from the list, and specify the group URL including the name of the connection profile, in the field provided.</p> <p>Note If you do not specify a group URL, you can access the portal page by entering the portal page URL, and then selecting the tunnel group connection profile alias from a list of configured tunnel group connection profile aliases configured on the device. See Access Page (ASA), page I-23.</p>
Global IP Address Pool	<p>The address pools from which IP addresses will be assigned. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools.</p> <p>Address pools are predefined network objects. If you want to use a different address pool, or select additional address pools, click Select to open the Network/Hosts selector from which you can make your selection(s).</p>

Table I-13 SSL VPN Wizard—Connection Profile Page (ASA) (Continued)

Authentication Method	<p>Select the authentication method to use for the SSL VPN connection profile:</p> <ul style="list-style-type: none"> • AAA—Select if you want users to provide a username and password that the security appliance checks against a previously configured AAA server. • Certificate—Select if you want users to be provided with a certificate during SSL negotiation. If you configure authentication using digital certificates, you can specify whether to send the entire certificate chain (which sends the peer the identity certificate and all issuing certificates) or just the issuing certificates (including the root certificate and any subordinate CA certificates). • Both—Select if you require both AAA and certificate authentication, in which case users must provide both a certificate and a username and password.
Authentication Server Group	<p>The name of the authentication server group (LOCAL if the tunnel group is configured on the local device).</p> <p>You can click Select to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.</p>
User LOCAL if Server Group Fails	<p>Available if you selected LOCAL for the authentication server group.</p> <p>When selected, enables fallback to the local database for authentication if the selected authentication server group fails.</p>
Authorization Server Group	<p>The name of the authorization server group (LOCAL if the tunnel group is configured on the local device).</p> <p>You can click Select to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.</p>
Accounting Server Group	<p>The name of the accounting server group.</p> <p>You can click Select to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.</p>

SSL VPN Access Policy Page

Use the SSL VPN Access Policy page to configure access parameters for your SSL VPN. For information about configuring an Access policy, see [Configuring an Access Policy, page 12-32](#).

Navigation Path

1. Select **View > Device View** or click the **Device View** button on the toolbar.
2. From the Device Selector, select the ASA device on which you want to configure an SSL VPN Access policy.
3. Select **SSL VPN > Access** from the Policy selector.

Related Topics

- [Configuring an Access Policy, page 12-32](#)
- [Understanding Interface Role Objects, page 9-132](#)
- [Understanding Port List Objects, page 9-168](#)

Field Reference

Table I-14 **SSL VPN Access Policy Page**

Element	Description
Interfaces to Enable SSL VPN Service	Specify the interfaces on which you want to enable SSL VPN. You can click Select to open a dialog box from which you can select interfaces from a list of available interface or interface role objects.
Port Number	The port number that you want to use for SSL VPN sessions. The default port is 443, for HTTPS traffic; the range is 1024 through 65535. If you change the port number, All current SSL VPN connections terminate, and current users must reconnect. Note If HTTP port redirection is enabled, the default HTTP port number is 80. Enter the name of a port list, or click Select to open the Port List Selector from which you can make your selection, or create a port list object. A port list object is a named definition of one or more port ranges that you use when defining service objects.

Table I-14 **SSL VPN Access Policy Page (Continued)**

Default Idle Timeout	<p>Amount of time, in seconds, that an SSL VPN session can be idle before the security appliance terminates it.</p> <p>This value applies only if the Idle Timeout value in the group policy for the user is set to zero (0), which means there is no timeout value; otherwise the group policy Idle Timeout value takes precedence over the timeout you configure here. The minimum value you can enter is 1 minute. The default is 30 minutes (1800 seconds). Maximum is 24 hours (86400 seconds).</p> <p>We recommend that you set this attribute to a short time period. This is because a browser set to disable cookies (or one that prompts for cookies and then denies them) can result in a user not connecting but nevertheless appearing in the sessions database. If the Simultaneous Logins attribute for the group policy is set to one, the user cannot log back in because the database indicates that the maximum number of connections already exists. Setting a low idle timeout removes such phantom sessions quickly, and lets a user log in again.</p>
Max Session Limit	<p>The maximum number of SSL VPN sessions you want to allow.</p> <p>Be aware that the different ASA models support SSL VPN sessions as follows: ASA 5510 supports a maximum of 150; ASA 5520 maximum is 750; ASA 5540 maximum is 2500.</p>
Allow Users to Select Connection Profile in Portal Page	<p>When selected, includes a list of configured tunnel groups on the SSL VPN end-user interface, from which users can select a tunnel when they log on. This is the default setting.</p> <p>When deselected, the user cannot select a tunnel group on login.</p>
Enable SSL VPN Access	<p>When selected, enables the SSL VPN functionality on the ASA device. This is the default setting.</p> <p>When deselected, disables the SSL VPN functionality on the ASA device.</p>
Save button	<p>Available only if you are authorized to modify this policy.</p> <p>Saves your changes to the server but keeps them private.</p> <p>Note To publish your changes, click the Submit button on the toolbar.</p>

SSL VPN Connection Profiles Policy Page

Use the Connection Profiles Policy page to view the SSL VPN connection profile policies currently defined on the security appliance. From this page, you can create, edit, or delete connection profile policies.

Navigation Path

1. Select **View > Device View** or click the **Device View** button on the toolbar.
2. From the Device Selector, select the ASA device on which you want to configure an SSL VPN Connection Profiles policy.
3. Select **SSL VPN > Connection Profiles** from the Policy selector.

Related Topics

- [Configuring an SSL VPN Connection Profile Policy, page 12-35](#)
- [Understanding SSL VPN Connection Profile Policies, page 12-33](#)
- [Understanding User Groups in SSL VPN, page 12-17](#)

Field Reference

Table I-15 **SSL VPN Connection Profiles (ASA) Policy Page**

Element	Description
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .
Connection Profile Name	The name of the configured SSL VPN Connection Profile policy.
Alias	If defined, an alternate name by which the user can select the SSL VPN connection profile at login.
URL	The URL the user enters in the browser to access the security appliance.
Default User Group	The default user group assigned to the SSL VPN connection profile, if one is defined. Note The default user group for the connection profile is used if you do not assign a specific user group. See Configuring User Groups on an ASA Device, page 12-19 .

Table I-15 **SSL VPN Connection Profiles (ASA) Policy Page (Continued)**

Thin Client	An indication (Enabled or Disabled) of whether Thin Client access mode is configured for the user group associated with the connection profile. See SSL VPN Access Modes, page 12-3 .
Full Tunnel	An indication (Enabled or Disabled) of whether Full Tunnel access mode is configured for the user group associated with the connection profile. See SSL VPN Access Modes, page 12-3 .
Create button	Opens the Add/Edit SSL VPN Connection Profile Dialog Box, page I-32 to create an SSL VPN Connection Profile policy.
Edit button	Opens the Add/Edit SSL VPN Connection Profile Dialog Box, page I-32 in which you can edit the properties of a selected SSL VPN Connection Profile policy.
Delete button	Deletes the selected SSL VPN Connection Profile policies from the table.
Save button	Available only if you are authorized to modify this policy. Saves your changes to the server but keeps them private. Note To publish your changes, click the Submit button on the toolbar.

Add/Edit SSL VPN Connection Profile Dialog Box

Use this dialog box to create or modify an SSL VPN Connection Profile policy.



Note

This dialog box is available only when the selected device is an ASA device.

For more information, see [Configuring an SSL VPN Connection Profile Policy, page 12-35](#).

These tabs are available in the Add/Edit SSL VPN Connection Profile dialog box:

- [Basic Tab \(ASA\), page I-33](#)
- [AAA Tab \(ASA\), page I-37](#)
- [Settings Tab \(ASA\), page I-42](#)

Navigation Path

Open the [SSL VPN Connection Profiles Policy Page, page I-31](#), then click **Create**, or select a connection profile in the table and click **Edit** (see [Table I-15 on page I-31](#)). The Add/Edit SSL VPN Connection Profile dialog box opens with the Basic tab displayed.

Basic Tab (ASA)

Use the Basic tab of the Add/Edit SSL VPN Connection Profile dialog box to configure the basic parameters for an SSL VPN Connection Profile policy.

For more information, see [Defining Basic Parameters, page 12-35](#).

Navigation Path

The Basic tab appears when you open the [Add/Edit SSL VPN Connection Profile Dialog Box, page I-32](#). You can also open it by clicking the **Basic** tab from any other tab in the Add/Edit SSL VPN Connection Profile dialog box.

Related Topics

- [Defining Basic Parameters, page 12-35](#)
- [Add/Edit SSL VPN Connection Profile Dialog Box, page I-32](#)
- [Understanding ASA User Group Objects, page 9-42](#)
- [Understanding Network/Host Objects, page 9-144](#)

Field Reference

Table I-16 *Add/Edit SSL VPN Connection Profile > Basic Tab (ASA)*

Element	Description
Connection Profile Name	The name of the tunnel group that contains the policies for this SSL VPN connection profile.
Default User Group	If required, the default user group associated with the device. You can click Select to open the ASA User Groups Selector from which you can select a user group from a list of ASA user group objects.

Table I-16 Add/Edit SSL VPN Connection Profile > Basic Tab (ASA) (Continued)

Alternate User Group	If required, an alternate user group to be applied to the tunnel group. You can click Select to open the ASA User Groups Selector from which you can select a user group from a list of ASA user group objects.
DNS Group	The DNS group to use for the SSL VPN tunnel group. The DNS group resolves the hostname to the appropriate DNS server for the tunnel group.
Global IP Address Pool	The address pools from which IP addresses will be assigned. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools. Address pools are predefined network objects. You can click Select to open the Network/Hosts selector from which you can make your selection(s).
Group Aliases	
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .
Alias	The alternate name by which the tunnel group is referred to. A group alias creates one or more alternate names by which a user can refer to a tunnel group. This feature is useful when the same group is known by several common names (such as “Devtest” and “QA”). If you want the actual name of the tunnel group to appear on this list, you must specify it as an alias. The group alias that you specify here appears on the login page. Each tunnel group can have multiple aliases or no alias. For more information, see Understanding SSL VPN Connection Profile Policies, page 12-33 .
Status	Specifies whether a group alias is enabled or not. If enabled, the group alias appears in a list during login.
Create button	Opens the Add/Edit Group Alias Dialog Box, page I-35 for creating a group alias.
Edit button	Opens the Add/Edit Group Alias Dialog Box, page I-35 for editing the settings of a selected group alias in the table.
Delete button	Deleted one or more group aliases that are selected in the table.
Group URLs	
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .

Table I-16 Add/Edit SSL VPN Connection Profile > Basic Tab (ASA) (Continued)

URL	<p>The URL associated with the tunnel group connection profile.</p> <p>You can configure multiple URLs (or no URLs) for a tunnel group. Each URL can be enabled or disabled individually. You must use a separate specification for each URL, specifying the entire URL using either the HTTP or HTTPS protocol.</p> <p>For more information, see Understanding SSL VPN Connection Profile Policies, page 12-33.</p>
Status	Specifies whether a group URL is enabled or not. If enabled, it eliminates the need to select a group during login.
Create button	Click to open the Add Group URL dialog box for creating a group URL. See Add/Edit Group URL Dialog Box, page I-36 .
Edit button	Select a group URL in the table, then click to open the Edit Group URL dialog box to edit its settings. See Add/Edit Group URL Dialog Box, page I-36 .
Delete button	Select the rows of one or more group URLs, then click to remove from the list.
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.</p>

Add/Edit Group Alias Dialog Box

Use the Add/Edit Group Alias dialog box to create or edit a group alias for an SSL VPN connection profile. Specifying the group alias creates one or more alternate names by which the user can refer to a tunnel group.

Navigation Path

Open the [Basic Tab \(ASA\), page I-33](#), then click **Create** below the Group Aliases table, or select a row in the table and click **Edit**.

Related Topics

- [SSL VPN Connection Profiles Policy Page, page I-31](#)
- [Add/Edit SSL VPN Connection Profile Dialog Box, page I-32](#)

- [Basic Tab \(ASA\), page I-33](#)

Field Reference

Table I-17 Add/Edit SSL VPN Connection Profile > Add/Edit Group Alias Dialog Box

Element	Description
Enabled	Indicates whether the group alias is enabled or not.
Group Alias	An alternative name for the SSL VPN connection profile. The group alias that you specify here appears in a list on the user's login page. Each group can have multiple aliases or no alias, each specified in separate commands.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Add/Edit Group URL Dialog Box

Use this dialog box to specify incoming URLs or IP addresses for the tunnel group. If a group URL is enabled in a tunnel group, the security appliance selects the associated tunnel group and presents the user with only the username and password fields in the login window.



Note

You can configure multiple URLs or addresses (or none) for a group. Each URL or address can be enabled or disabled individually.

You cannot associate the same URL or address with multiple groups. The security appliance verifies the uniqueness of the URL or address before accepting the URL or address for a tunnel group.

Navigation Path

Open the [Basic Tab \(ASA\), page I-33](#), then click **Create** below the Group URLs table, or select a row in the table and click **Edit**.

Related Topics

- [SSL VPN Connection Profiles Policy Page, page I-31](#)

- [Add/Edit SSL VPN Connection Profile Dialog Box](#), page I-32
- [Basic Tab \(ASA\)](#), page I-33

Field Reference

Table I-18 *Add/Edit SSL VPN Connection Profile > Add/Edit Group URL Dialog Box*

Element	Description
Enabled	Indicates whether the group URL is enabled or not.
Group URL	Select a protocol (http or https) from the list, and specify the incoming URL for the group in the field provided.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

AAA Tab (ASA)

Use the AAA tab of the Add/Edit SSL VPN Connection Profile dialog box to configure the AAA authentication parameters for an SSL VPN Connection Profile policy.

Navigation Path

Open the [Add/Edit SSL VPN Connection Profile Dialog Box](#), page I-32, then click the **AAA** tab.

Related Topics

- [Defining AAA Parameters](#), page 12-37
- [SSL VPN Connection Profiles Policy Page](#), page I-31
- [Understanding AAA Server Group Objects](#), page 9-15

Field Reference

Table I-19 Add/Edit SSL VPN Connection Profile > AAA Tab (ASA)

Element	Description
Authentication	<p>Select the authentication method to use for the SSL VPN connection profile from these options:</p> <ul style="list-style-type: none"> • AAA—Select if you want users to provide a username and password that the security appliance checks against a previously configured AAA server. • Certificate—Select if you want users to be provided with a certificate during SSL negotiation. <p>If you configure authentication using digital certificates, you can specify whether to send the entire certificate chain (which sends the peer the identity certificate and all issuing certificates) or just the issuing certificates (including the root certificate and any subordinate CA certificates).</p> <ul style="list-style-type: none"> • Both—Select if you require both AAA and certificate authentication, in which case users must provide both a certificate and a username and password.
Authentication Server Group	<p>The name of the authentication server group (LOCAL if the tunnel group is configured on the local device).</p> <p>You can click Select to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.</p> <p>Note If you want to set the authentication server group per interface, see Add/Edit SSL VPN Interface Specific Authentication Server Groups, page I-41.</p>
User LOCAL if Server Group Fails	<p>Available if you selected LOCAL for the authentication server group.</p> <p>When selected, enables fallback to the local database for authentication if the selected authentication server group fails.</p>
Authorization Server Group	<p>When selected, enables you to specify the name of the authorization server group (LOCAL if the tunnel group is configured on the local device).</p> <p>You can click Select to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.</p>
LOCAL Authorization	<p>When selected, enables authorization on the local device.</p>

Table I-19 Add/Edit SSL VPN Connection Profile > AAA Tab (ASA) (Continued)

User Must Exist in the Authorization Database to Connect	<p>When selected, defines that the username of the remote client must exist in the database before a successful connection can be established. If the username does not exist in the authorization database, then the connection is denied.</p> <p>Select this check box if you want the security appliance to allow only users in the authorization database to connect. By default this feature is disabled. You must have a configured authorization server to use this feature.</p>
Accounting Server Group	<p>The name of the accounting server group.</p> <p>You can click Select to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.</p>
Use Entire DN as the Username	<p>When selected, enables you to use the entire Distinguished Name (DN) as the identifier for the username.</p> <p>A distinguished name (DN) is a unique identification, made up of individual fields, that can be used as the identifier when matching users to a tunnel group. DN rules are used for enhanced certificate authentication on ASA devices.</p>
Specify Individual DN fields as the Username	<p>When selected (the default), enables you to use individual DN fields as the username when matching users to the tunnel group.</p> <p>A DN certificate is made up of different field identifiers that can be used to match users to tunnel groups.</p>
Primary DN Field	<p>Available if you selected to use individual DN fields as the username.</p> <p>Select the primary DN field identifier to be used for identification from the list. The default is UID (User ID).</p>
Secondary DN Field	<p>Available if you selected to use individual DN fields as the username.</p> <p>Select the secondary DN field identifier to be used for identification. Select None if no secondary field identifier is required.</p>

Table I-19 Add/Edit SSL VPN Connection Profile > AAA Tab (ASA) (Continued)

<p>Override Account-Disabled Indication from AAA Server</p>	<p>When selected, enables you to override the “account-disabled” indicator from an AAA server. This configuration is valid for servers, such as RADIUS with NT LDAP, and Kerberos, that return an “account-disabled” indication.</p> <p>Note If you are using an LDAP directory server for authentication, password management is supported with the Sun Microsystems JAVA System Directory Server (formerly named the Sun ONE Directory Server) and the Microsoft Active Directory.</p> <p>Sun—The DN configured on the security appliance to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.</p> <p>Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.</p>
<p>Enable Notification Upon Password Expiration to Allow User to Change Password</p>	<p>When selected, enables the security appliance to notify the remote user at login that the current password is about to expire or has expired, then offers the user the opportunity to change the password.</p> <p>Note If you do not also check the Enable Notification Prior to Expiration check box, the security appliance does not notify the user of the pending expiration, but the user can change the password after it expires.</p>
<p>Enable Notification Prior to Expiration</p>	<p>Available only if you selected the Enable Notification Upon Password Expiration to Allow User to Change Password check box.</p> <p>When selected, enables you to specify the number of days before expiration to warn the user about the pending expiration.</p> <p>If the current password has not yet expired, the user can still log in using that password. This parameter is valid for AAA servers that support such notification—RADIUS, RADIUS with an NT server, and LDAP servers. The security appliance ignores this command if RADIUS or LDAP authentication has not been configured.</p> <p>Note The selection of this check box just enables the notification. You must specify the number of days for it to take effect.</p>

Table I-19 Add/Edit SSL VPN Connection Profile > AAA Tab (ASA) (Continued)

Notify Prior to Expiration	Available only if you selected the Enable Notification Prior to Expiration check box. Specifies the number of days before the current password expires to notify the user of the pending expiration. The range is 1 through 180 days.
Interface-Specific Authentication Server Groups	
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .
Interface	The interface associated with the authentication server group.
Server Group	The server group associated with the selected interface role.
Fallback	Indicates whether fallback to the LOCAL database, if the selected server group fails, is enabled or not.
Create button	Opens a dialog box that lets you add an interface-specific authentication group to the list. See Add/Edit SSL VPN Interface Specific Authentication Server Groups, page I-41 .
Edit button	Opens a dialog box in which you can edit a selected interface-specific authentication group from the table. See Add/Edit SSL VPN Interface Specific Authentication Server Groups, page I-41 .
Delete button	Deletes one or more selected interface-specific authentication groups from the table.
Save button	Saves your changes to the server but keeps them private. Note To publish your changes, click the Submit button on the toolbar.

Add/Edit SSL VPN Interface Specific Authentication Server Groups

Use the Add/Edit SSL VPN Interface Specific Authentication Server Groups dialog box to configure interface-specific authentication for your SSL VPN connection profile policy. This setting overrides the global authentication server group settings configured on the [Basic Tab \(ASA\), page I-33](#).

Navigation Path

Open the [AAA Tab \(ASA\), page I-37](#), then click **Create** below the Interface Specific Authentication Server Groups table, or select a row in the table and click **Edit**.

Related Topics

- [SSL VPN Connection Profiles Policy Page, page I-31](#)
- [Add/Edit SSL VPN Connection Profile Dialog Box, page I-32](#)
- [AAA Tab \(ASA\), page I-37](#)
- [Understanding Interface Role Objects, page 9-132](#)
- [Understanding AAA Server Group Objects, page 9-15](#)

Field Reference

Table I-20 *Add/Edit SSL VPN Connection Profile > Add/Edit SSL VPN Interface Specific Authentication Server Groups*

Element	Description
Interface	The interface to be associated with the authentication server group. You can click Select to open a dialog box that lists all available interfaces and interface roles, from which you can make your selection, or create interface role objects.
Server Group	The server group to be associated with the selected interface. You can click Select to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.
Use LOCAL if server group fails	When selected, enables fallback to the LOCAL database if the selected server group fails.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Settings Tab (ASA)

Use the Settings tab of the Add/Edit SSL VPN Connection Profile dialog box to configure the WINS servers for the connection profile policy, select a customized look and feel for the SSL VPN end-user logon web page, DHCP servers to be used for client address assignment, and establish an association between an interface and client IP address pools.

Navigation Path

Open the [Add/Edit SSL VPN Connection Profile Dialog Box](#), page I-32, then click the **Settings** tab. You can also open the Settings tab by clicking it from any other tab on the Add/Edit SSL VPN Connection Profile dialog box.

Related Topics

- [Defining Servers and Address Pools](#), page 12-40
- [SSL VPN Connection Profiles Policy Page](#), page I-31
- [Add/Edit SSL VPN Connection Profile Dialog Box](#), page I-32
- [Understanding WINS Server List Objects](#), page 9-211
- [Understanding Network/Host Objects](#), page 9-144
- [Understanding SSL VPN Customization Objects](#), page 9-203

Field Reference

Table I-21 *Add/Edit SSL VPN Connection Profile > Settings Tab (ASA)*

Element	Description
WINS Servers List	<p>The name of the WINS (Windows Internet Naming Server) servers list to use for CIFS name resolution.</p> <p>SSL VPN uses the CIFS protocol to access or share files on remote systems. When you attempt a file-sharing connection to a Windows computer by using its computer name, the file server you specify corresponds to a specific WINS server name that identifies a resource on the network.</p> <p>A WINS servers list defines a list of WINS servers, which are used to translate Windows file server names to IP addresses. The security appliance queries the WINS servers to map WINS names to IP addresses. You must configure at least one, and up to three WINS servers for redundancy. The security appliance uses the first server on the list for WINS/CIFS name resolution. If the query fails, it uses the next server.</p> <p>WINS server lists are predefined objects. If you want to use a different WINS servers list, click Select to open the WINS Server List Selector dialog box that lists all available WINS Servers list objects, and in which you can create WINS Servers list objects.</p>

Table I-21 Add/Edit SSL VPN Connection Profile > Settings Tab (ASA) (Continued)

Portal Page Customization	<p>Defines the appearance of the portal page that allows the remote user access to all the resources available on the SSL VPN networks.</p> <p>Specify the SSL VPN customization profile in the field provided.</p> <p>Customization profiles are predefined objects. You can click Select to open the SSL VPN Customization Selector dialog box, from which you can make your selection or create new customization objects.</p> <p>Note You can set up different login windows for different groups by using a combination of customization profiles and tunnel groups. For example, assuming that you had created a customization profile called salesgui, you can create an SSL VPN tunnel group called sales that uses that customization profile.</p>
DHCP Servers	<p>The DHCP servers to be used for client address assignments. The server uses the DHCP servers in the order listed. You can add up to 10 servers.</p> <p>DHCP servers are predefined network objects. You can click Select to open the Network/Hosts selector that lists all available network hosts, and in which you can create network host objects.</p>
Client IP Address Pool	
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .
Interface	The interface associated with the address pool.
Address Pool	The address pool associated with the selected interface role.
Create button	Open a dialog box that lets you add an interface-specific client address pool to the list. See Add/Edit SSL VPN Interface Specific Client Address Pools, page I-45 .
Edit button	Opens a dialog box that lets you edit a selected item in the Client IP Address Pool table, See Add/Edit SSL VPN Interface Specific Client Address Pools, page I-45 .
Delete button	Deletes one or more interface-specific client address pools selected in the table.
Save button	<p>Saves your changes to the server but keeps them private.</p> <p>Note To publish your changes, click the Submit button on the toolbar.</p>

Add/Edit SSL VPN Interface Specific Client Address Pools

Use the Add/Edit SSL VPN Interface Specific Client Address Pools dialog box to configure interface-specific client address pools for your SSL VPN connection profile policy. This setting overrides the global IP address pools configured on the [Basic Tab \(ASA\)](#), page I-33.

Navigation Path

Open the [Settings Tab \(ASA\)](#), page I-42, then click **Create** below the Client IP Address Pool table, or select a row in the table and click **Edit**.

Related Topics

- [SSL VPN Connection Profiles Policy Page](#), page I-31
- [Add/Edit SSL VPN Connection Profile Dialog Box](#), page I-32
- [Settings Tab \(ASA\)](#), page I-42
- [Creating Interface Role Objects](#), page 9-133
- [Creating Network/Host Objects](#), page 9-148

Field Reference

Table I-22 *Add/Edit SSL VPN Connection Profile > Add/Edit SSL VPN Interface Specific Client Address Pools*

Element	Description
Interface	The interface to assign a client address to. You can click Select to open a dialog box that lists all available interfaces and interface roles, from which you can make your selection or create interface role objects.
Address Pool	The address pool to be used to assign a client address to the selected interface. Address pools are predefined network objects. You can click Select to open a dialog box that lists all available network hosts, and in which you can create or edit network host objects.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

ASA User Groups Policy Page

In the User Groups Policy page, you can view the ASA User Group policies defined for your ASA SSL VPN connection profile. From this page, you can specify new ASA user groups and edit existing ones.

Navigation Path

1. Select **View > Device View** or click the **Device View** button on the toolbar.
2. From the Device Selector, select the ASA device on which you want to configure the user groups.
3. Select **SSL VPN > User Groups** from the Policy selector.

Related Topics

- [Configuring ASA User Groups Policy in Your SSL VPN, page 12-42](#)
- [Understanding ASA User Group Objects, page 9-42](#)

Field Reference

Table I-23 **ASA User Groups Policy Page**

Element	Description
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .
User Group	The name of the ASA user group assigned to the SSL VPN connection profile.
Type	Indicates whether the user groups are assigned to your remote access VPN server, SSL VPN connection profile, or both.
Thin Client	An indication (True or False) of whether Thin Client access mode is configured for your user group.
Full Tunnel	An indication (True or False) of whether Full Tunnel access mode is configured for your user group.
Create button	ASA user groups are predefined objects. Click to open a dialog box from which you can select a user group from a list of predefined ASA user group objects, or create new ones. See Add User Group Selector Dialog Box (ASA), page I-47 .

Table I-23 **ASA User Groups Policy Page (Continued)**

Edit button	Select the row of an ASA user group policy in the table, then click to open the Edit ASA User Group dialog box in which you can edit its properties. See ASA User Group Dialog Box, page F-56 .
Delete button	Select the rows of one or more ASA user groups, then click to remove from the list.
Delete button	Select the rows of one or more SSL VPN policies, then click to remove from the list.
Save button	Saves your changes to the server but keeps them private. Note To publish your changes, click the Submit button on the toolbar.

Add User Group Selector Dialog Box (ASA)

The User Group Selector dialog box displays the predefined ASA user group objects that are available for your selection. From this page, you can create new user groups or edit the properties of existing ones.

Navigation Path

Open the [ASA User Groups Policy Page, page I-46](#), then click the **Create** button.

Related Topics

- [ASA User Groups Policy Page, page I-46](#)
- [Understanding ASA User Group Objects, page 9-42](#)
- [Creating ASA User Group Objects, page 9-44](#)

Field Reference

Table I-24 **ASA User Groups Policy > Add User Group Selector**

Element	Description
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .

Table I-24 ASA User Groups Policy > Add User Group Selector (Continued)

Available ASA User Groups	<p>Lists the predefined ASA user groups available for selection.</p> <p>Select the required ASA user group in the list. The selected user group is displayed in the Selected field.</p> <p>ASA user groups are predefined objects. If the required user group is not included in the list, click Create to open the Add ASA User Group dialog box that enables you to create or edit an ASA user group object.</p>
Selected	The selected ASA user group.
Create button	Opens the ASA User Group Dialog Box, page F-56 for creating an ASA user group object.
Edit button	Opens the ASA User Group Dialog Box, page F-56 for editing the selected ASA user group object.
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.</p>

Cisco Secure Desktop Page (ASA)

Use the Cisco Secure Desktop page to configure the Cisco Secure Desktop (CSD) software on your selected ASA device.

Cisco Secure Desktop (CSD) provides a single, secure location for session activity and removal on the client system, ensuring that sensitive data is shared only for the duration of an SSL VPN session.



Note

The Secure Desktop Client software must be installed and activated on a device in order for an SSL VPN policy to work properly.

The CSD is managed using a FlexConfig policy. For more information, see [Predefined FlexConfig Policy Objects, page 20-8](#).

Navigation Path

1. Select **View > Device View** or click the **Device View** button on the toolbar.

2. From the Device Selector, select the ASA device on which you want to configure the SSL VPN global settings.
3. Select **SSL VPN > Cisco Secure Desktop** from the Policy selector.

Related Topics

- [Configuring the Cisco Secure Desktop Software, page 12-44](#)
- [Understanding Secure Desktop Configuration Objects, page 9-171](#)

Field Reference

Table I-25 Cisco Secure Desktop Page (ASA)

Element	Description
Enable	When selected, enables the CSD on the device.
Configuration	Specify the filename of the CSD distribution package to install into the running configuration (the securedesktop_asa_<n>_<n>*.pkg file to be uploaded from your local computer to the flash device). You can click Select to open the Secure Desktops Selector from which you can select a CSD distribution package file from a list of CSD distribution package objects.
Save button	Saves your changes to the server but keeps them private. Note To publish your changes, click the Submit button on the toolbar.

SSL VPN Global Settings Page

Use the SSL VPN Global Settings page to define global settings for caching, content rewriting, character encoding, proxy, and memory size definitions that apply to devices in your VPN topology.

For more information, see [Configuring Global Settings, page 12-45](#).

These tabs are available on the SSL VPN Global Settings page.

- [Performance Tab, page I-50](#)
- [Content Rewrite Tab, page I-52](#)
- [Encoding Tab, page I-55](#)

- [Proxy Tab, page I-58](#)
- [Advanced Tab, page I-62](#)

Navigation Path

1. Select **View > Device View** or click the **Device View** button on the toolbar.
2. From the Device Selector, select the ASA device on which you want to configure the SSL VPN global settings.
3. Select **SSL VPN > Global Settings** from the Policy selector.

Performance Tab

Use the Performance tab of the SSL VPN Global Settings page to specify caching properties that enhance SSL VPN performance. For information on configuring the global performance settings, see [Defining Performance Settings, page 12-46](#).

Navigation Path

The Performance tab appears when you open the [SSL VPN Global Settings Page, page I-49](#). You can also open it by clicking the **Performance** tab from any other tab on the SSL VPN Global Settings page.

Related Topics

- [Defining Performance Settings, page 12-46](#)
- [SSL VPN Global Settings Page, page I-49](#)

Field Reference

Table I-26 **SSL VPN Global Settings > Performance Tab**

Element	Description
Enable	<p>When selected, enables the use of cache settings for the security appliance. This check box is selected by default.</p> <p>When deselected, the cache settings configured on the security appliance do not take effect and all the fields under the Performance tab are grayed out.</p>

Table I-26 **SSL VPN Global Settings > Performance Tab (Continued)**

Maximum Object Size	<p>The maximum size (in kilobytes) of an HTTP object that can be stored in the cache on the security appliance.</p> <p>The maximum size limit for an HTTP object is 10,000 kilobytes. The default is 1000 Kb.</p>
Minimum Object Size	<p>The minimum size of an HTTP object that can be stored in the cache (in kilobytes) on the security appliance.</p> <p>The minimum size range is 0-10,000 Kb. The default is 0 Kb.</p>
Last Modified Factor	<p>Specifies an integer to set a revalidation policy for caching objects that have only the last-modified timestamp, and no other server-set expiration values. The range is 1-100. The default is 20.</p> <p>The Expires response from the origin web server to the security appliance request, which indicates the time that the response expires, also affects caching. This response header indicates the time that the response becomes stale and should not be sent to the client without an up-to-date check (using a conditional GET operation).</p> <p>The security appliance can also calculate an expiration time for each web object before it is written to disk. The algorithm to calculate an object's cache expiration date is as follows:</p> <p>Expiration date = (Today's date - Object's last modified date) * Freshness factor</p> <p>After the expiration date has passed, the object is considered stale and subsequent requests causes a fresh retrieval of the content by the security appliance. Setting the last modified factor to zero is equivalent to forcing an immediate revalidation, while setting it to 100 results in the longest allowable time until revalidation.</p>
Expiration Time	<p>The amount of time (in minutes) that the security appliance caches objects without revalidating them. The range is 0-900 minutes. The default is one minute.</p> <p>Revalidation consists of rejecting the objects from the origin server before serving the requested content to the client browser when the age of the cached object has exceeded its freshness lifetime. The age of a cached object is the time that the object has been stored in the security appliance's cache without the security appliance explicitly contacting the origin server to check if the object is still fresh.</p>

Table I-26 **SSL VPN Global Settings > Performance Tab (Continued)**

Cache Compressed Content	When selected, enables compressed objects (zip, gz, and tar files) for SSL VPN sessions to be cached on the security appliance. When you deselect this check box, the security appliance stores objects before it compresses them.
Cache Static Content	When selected, enables static content to be cached on the security appliance. Each web page comprises static and dynamic objects. The security appliance caches individual static objects, such as image files (*.gif, *.jpeg), java applets (.js), and cascading style sheets (*.css), etc.
Save button	Saves your changes to the server but keeps them private. Note To publish your changes, click the Submit button on the toolbar.

Content Rewrite Tab

Use the Content Rewrite tab of the SSL VPN Global Settings page to enable the security appliance to create rewrite rules that permit users to browse certain sites and applications without going through the security appliance itself.

Navigation Path

Open the [SSL VPN Global Settings Page, page I-49](#), then click the **Content Rewrite** tab.

Related Topics

- [Defining Content Rewrite Rules, page 12-47](#)
- [SSL VPN Global Settings Page, page I-49](#)

Field Reference

Table I-27 **SSL VPN Global Settings > Content Rewrite Tab**

Element	Description
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .

Table I-27 **SSL VPN Global Settings > Content Rewrite Tab (Continued)**

Rule Number	An integer that indicates the position of the rule in the list. The security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.
Rule Name	The name of the application for which the rule applies.
Resource Mask	The application or resource for the rule.
Enable	Indicates whether the content rewrite rule is enabled or not on the security appliance.
Create button	Opens a dialog box that lets you add a content rewrite rule to the list. See Add/Edit Content Rewrite Dialog Box, page I-53 .
Edit button	Opens a dialog box that lets you edit a selected content rewrite rule in the table. See Add/Edit Content Rewrite Dialog Box, page I-53 .
Delete button	Deletes one or more selected content rewrite rules from the table.
Save button	Saves your changes to the server but keeps them private. Note To publish your changes, click the Submit button on the toolbar.

Add/Edit Content Rewrite Dialog Box

Use the Add/Edit Content Rewrite dialog box to configure /rewriting engine that includes advanced elements such as JavaScript, VBScript, Java, and multi-byte characters to proxy HTTP traffic over a SSL VPN connection.

Navigation Path

Open the [Content Rewrite Tab, page I-52](#), then click **Create** below the table, or select a row in the table and click **Edit**.

Related Topics

- [Defining Content Rewrite Rules, page 12-47](#)
- [SSL VPN Global Settings Page, page I-49](#)
- [Content Rewrite Tab, page I-52](#)

Field Reference

Table I-28 **SSL VPN Global Settings > Content Rewrite Tab > Add/Edit Content Rewrite Dialog Box**

Element	Description
Enable	<p>When selected, enables content rewriting on the security appliance for the rewrite rule.</p> <p>Some applications do not require this processing, such as external public websites. For these applications, you might choose to turn off content rewriting.</p>
Rule Number	Specifies a number for this rule. This number specifies the position of the rule in the list. Rules without a number are at the end of the list. The range is from 1 to 65534.
Rule Name	Specifies an alphanumeric string that describes the content rewrite rule. The maximum is 128 bytes.
Resource Mask	<p>Specifies the name of the application or resource to which the rule applies.</p> <p>You can use the following wildcards:</p> <ul style="list-style-type: none"> • *—Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. • ?—Matches any single character. • [!seq]—Matches any character not in sequence. • [seq]—Matches any character in sequence. <p>The maximum is 300 bytes.</p>
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.</p>

Encoding Tab

Use the Encoding tab of the SSL VPN Global Settings page to specify the character set to encode in SSL VPN portal pages to be delivered to remote users. By default, the encoding type set on the remote browser determines the character set for SSL VPN portal pages, so you need to set the character encoding only if it is necessary to ensure proper encoding on the browser.

For information on configuring the Encoding rules, see [Defining Encoding Rules, page 12-49](#).

Navigation Path

Open the [SSL VPN Global Settings Page, page I-49](#), then click the **Encoding** tab.

Related Topics

- [Defining Encoding Rules, page 12-49](#)
- [SSL VPN Global Settings Page, page I-49](#)

Field Reference

Table I-29 *SSL VPN Global Settings > Encoding Tab*

Element	Description
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Tables, page 3-24 .

Table I-29 **SSL VPN Global Settings > Encoding Tab (Continued)**

Global SSL VPN Encoding Type	<p>Select the attribute that determines the character encoding that all SSL VPN portal pages inherit, except for those portal pages delivered from the CIFS servers listed in the table.</p> <p>By default, the security appliance applies the “Global SSL VPN Encoding Type” to pages from Common Internet File System servers.</p> <p>You can select one of the following values:</p> <ul style="list-style-type: none"> • big5 • gb2312 • ibm-850 • iso-8859-1 • shift_jis <p>Note If you are using Japanese Shift_jis Character encoding, click Do not specify in the Font Family area of the associated Select Page Font pane to remove the font family.</p> <ul style="list-style-type: none"> • unicode • windows-1252 • none <p>If you choose None or specify a value that the browser on the SSL VPN client does not support, it uses its own default encoding.</p> <p>You can enter a string of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets. You can use either the name or the alias of a character set listed on that page. The string is case-insensitive. The command interpreter converts upper-case to lower-case when you save the security appliance configuration.</p>
Common Internet File System Server	The name or IP address of each CIFS server for which the encoding requirement differs from the “Global SSL VPN Encoding Type” attribute setting.
Encoding Type	The character encoding override for the associated CIFS server.
Create button	Opens a dialog box that lets you add a CIFS server for which the encoding requirement differs from the “Global SSL VPN Encoding Type” attribute setting. See Add/Edit File Encoding Dialog Box, page I-57 .

Table I-29 **SSL VPN Global Settings > Encoding Tab (Continued)**

Edit button	Opens a dialog box that lets you edit the settings of a selected CIFS server in the table. See Add/Edit File Encoding Dialog Box, page I-57 .
Delete button	Select the rows of one or more exceptions to the global encoding type attribute setting, then click to remove from the list.
Save button	Saves your changes to the server but keeps them private. Note To publish your changes, click the Submit button on the toolbar.

Add/Edit File Encoding Dialog Box

Use the Add/Edit File Encoding dialog box to configure CIFS servers and associated character encoding, to override the value of the “Global SSL VPN Encoding Type” attribute.

Navigation Path

Open the [Encoding Tab, page I-55](#), then click **Create** below the table, or select a row in the table and click **Edit**.

Related Topics

- [SSL VPN Global Settings Page, page I-49](#)
- [Encoding Tab, page I-55](#)
- [Defining Encoding Rules, page 12-49](#)

Field Reference

Table I-30 **SSL VPN Global Settings > Encoding Tab > Add/Edit File Encoding Dialog Box**

Element	Description
CIFS Server	<p>The name or IP address of a CIFS server for which the encoding requirement differs from the “Global SSL VPN Encoding Type” attribute setting. The security appliance retains the case you specify, although it ignores the case when matching the name to a server.</p> <p>CIFS servers are predefined objects. You can click Select to open the Network/Hosts Selector dialog box that lists all available network hosts, and in which you can create network host objects.</p>
Encoding Type	<p>Select the character encoding that the CIFS server should provide for SSL VPN portal pages. This selection overrides the “Global SSL VPN Encoding Type” attribute setting.</p> <p>If you choose None or specify a value that the browser on the SSL VPN client does not support, it uses its own default encoding.</p>
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.</p>

Proxy Tab

Use the Proxy tab of the SSL VPN Global Settings page to configure the security appliance to terminate HTTPS connections and forward HTTP/HTTPS requests to HTTP and HTTPS proxy servers. On this tab, you can also configure the security appliance to perform minimal content rewriting, and to specify the types of content to rewrite—external links and/or XML.

Navigation Path

Open the [SSL VPN Global Settings Page, page I-49](#), then click the **Proxy** tab.

Related Topics

- [Defining Proxies and Proxy Bypass Rules, page 12-51](#)
- [Defining Content Rewrite Rules, page 12-47](#)

- [SSL VPN Global Settings Page, page I-49](#)
- [Understanding Network/Host Objects, page 9-144](#)
- [Understanding Port List Objects, page 9-168](#)

Field Reference

Table I-31 **SSL VPN Global Settings > Proxy Tab**

Element	Description
HTTP Proxy Server	<p>The IP address of the external HTTP proxy server to which the security appliance forwards HTTP connections.</p> <p>HTTP proxy servers are predefined network objects. You can click Select to open the Networks/Hosts Selector dialog box from which you can make your selection(s), and in which you can create network host objects.</p>
HTTP Proxy Port	<p>The port of the external HTTP proxy server to which the security appliance forwards HTTP connections.</p> <p>You can click Select to open the Port List Selector dialog box from which you can make your selection, or create a port list object. A port list object is a named definition of one or more port ranges that you use when defining service objects.</p>
HTTPS Proxy Server	<p>The IP address of the external HTTPS proxy server to which the security appliance forwards HTTP connections.</p> <p>HTTPS proxy servers are predefined network objects. You can click Select to open the Networks/Hosts Selector dialog box from which you can make your selection(s), and in which you can create network host objects.</p>
HTTPS Proxy Port	<p>The port of the external HTTPS proxy server to which the security appliance forwards HTTPS connections.</p> <p>You can click Select to open the Port List Selector dialog box from which you can make your selection, or create a port list object.</p>
Proxy Bypass	
Interface	The ASA interface configured for proxy bypass.
Port	The port configured for proxy bypass.

Table I-31 **SSL VPN Global Settings > Proxy Tab (Continued)**

Path Mask	The URL path to match for proxy bypass. A path is the text in a URL that follows the domain name. For example, in the URL <code>www.mycompany.com/hrbenefits</code> , <code>hrbenefits</code> is the path. Similarly, for the URL <code>www.mycompany.com/hrinsurance</code> , <code>hrinsurance</code> is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the <code>*</code> wildcard as follows: <code>/hr*</code> .
URL	The target URL for proxy bypass.
Create button	Opens a dialog box that lets you add a proxy bypass rule to the table. See Add/Edit Proxy Bypass Dialog Box, page I-60 .
Edit button	Opens a dialog box that lets you edit the settings of a selected proxy bypass rule in the table. See Add/Edit Proxy Bypass Dialog Box, page I-60 .
Delete button	Deletes one or more proxy bypass rules selected in the table.
Save button	Saves your changes to the server but keeps them private. Note To publish your changes, click the Submit button on the toolbar.

Add/Edit Proxy Bypass Dialog Box

Use the Add/Edit Proxy Bypass dialog box to set proxy bypass rules when the security appliance performs little or no content rewriting.

Navigation Path

Open the [Proxy Tab, page I-58](#), then click **Create** below the table, or select a row in the table and click **Edit**.

Related Topics

- [SSL VPN Global Settings Page, page I-49](#)
- [Proxy Tab, page I-58](#)
- [Defining Proxies and Proxy Bypass Rules, page 12-51](#)
- [Understanding Interface Role Objects, page 9-132](#)
- [Understanding Port List Objects, page 9-168](#)

Field Reference

Table I-32 **SSL VPN Global Settings > Proxy Tab >
Add/Edit Proxy Bypass Dialog Box**

Element	Description
Interface	<p>The interface on the security appliance that is used for proxy bypass.</p> <p>You can click Select to open a dialog box from which you can select an interface from a list of interface or interface role objects.</p>
Bypass Traffic	
On Port	<p>When selected, enables you specify a port number to be used for proxy bypass. Valid port numbers are 20000-21000.</p> <p>You can click Select to open the Port List Selector dialog box from which you can make your selection, or create a port list object. A port list object is a named definition of one or more port ranges that you use when defining service objects.</p> <p>Note If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the security appliance. Use path masks to avoid this restriction.</p>
Matching Specify Pattern	<p>When selected, enables you to specify a URL path to match for proxy bypass.</p> <p>A path is the text in a URL that follows the domain name. For example, in the URL <code>www.mycompany.com/hrbenefits</code>, <i>hrbenefits</i> is the path.</p> <p>You can use the following wildcards:</p> <ul style="list-style-type: none"> • *—Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. • ?—Matches any single character. • [!seq]—Matches any character not in sequence. • [seq]—Matches any character in sequence. <p>The maximum is 128 bytes.</p> <p>Note Path masks can change, so you might need to use multiple path mask statements to exhaust the possibilities.</p>

Table I-32 **SSL VPN Global Settings > Proxy Tab > Add/Edit Proxy Bypass Dialog Box (Continued)**

URL	Select the http or https protocol, then enter a URL to which you want to apply proxy bypass, in the field provided. URLs used for proxy bypass allow a maximum of 128 bytes. The port for HTTP is 80 and for HTTPS it is 443, unless you specify another port.
Rewrite XML	When selected, rewrites XML sites and applications to be bypassed by the security appliance.
Rewrite Hostname	When selected, rewrites external links to be bypassed by the security appliance.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Advanced Tab

Use the Advanced tab of the SSL VPN Global Settings page to configure the amount of security appliance memory that can be used for SSL VPN sessions.

Navigation Path

Open the [SSL VPN Global Settings Page, page I-49](#), then click the **Advanced** tab.

Related Topics

- [Defining Advanced Settings, page 12-53](#)
- [SSL VPN Global Settings Page, page I-49](#)

Field Reference

Table I-33 SSL VPN Global Settings > Advanced Tab

Element	Description
Memory Size	<p>Specify the amount of memory you want to allocate to SSL VPN sessions, as follows:</p> <ul style="list-style-type: none"> • % of Total Physical Memory—As a percentage of total memory. Default is 50%. • Kilobytes—In kilobytes. Different ASA models have different total amounts of memory, as follows: <ul style="list-style-type: none"> – ASA 5510 has 256 MB – ASA 5520 has 512 MB – ASA 5540 has 1GB <p>Note When you change the memory size, the new setting takes effect only after the system reboots.</p>
Save button	<p>Saves your changes to the server but keeps them private.</p> <p>Note To publish your changes, click the Submit button on the toolbar.</p>

