



Configuring the SSL VPN Client

The SSL VPN Client (SVC) is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers. The SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the security appliance.

To establish an SVC session, the remote user enters the IP address of a WebVPN interface of the security appliance in the browser, and the browser connects to that interface and displays the WebVPN login window. If the user satisfies the login and authentication, and the security appliance identifies the user as *requiring* the SVC, the security appliance downloads the SVC to the remote computer. If the security appliance identifies the user as having the *option* to use the SVC, the security appliance downloads the SVC to the remote computer while presenting a link on the window to skip the SVC installation.

After downloading, the SVC installs and configures itself, and then the SVC either remains or uninstalls itself (depending on the configuration) from the remote computer when the connection terminates.

This section covers the following topics:

- [Installing SVC, page 3-2](#)
- [Configuring SVC, page 3-5](#)
- [Viewing SVC Sessions, page 3-14](#)
- [Logging Off SVC Sessions, page 3-16](#)

Installing SVC

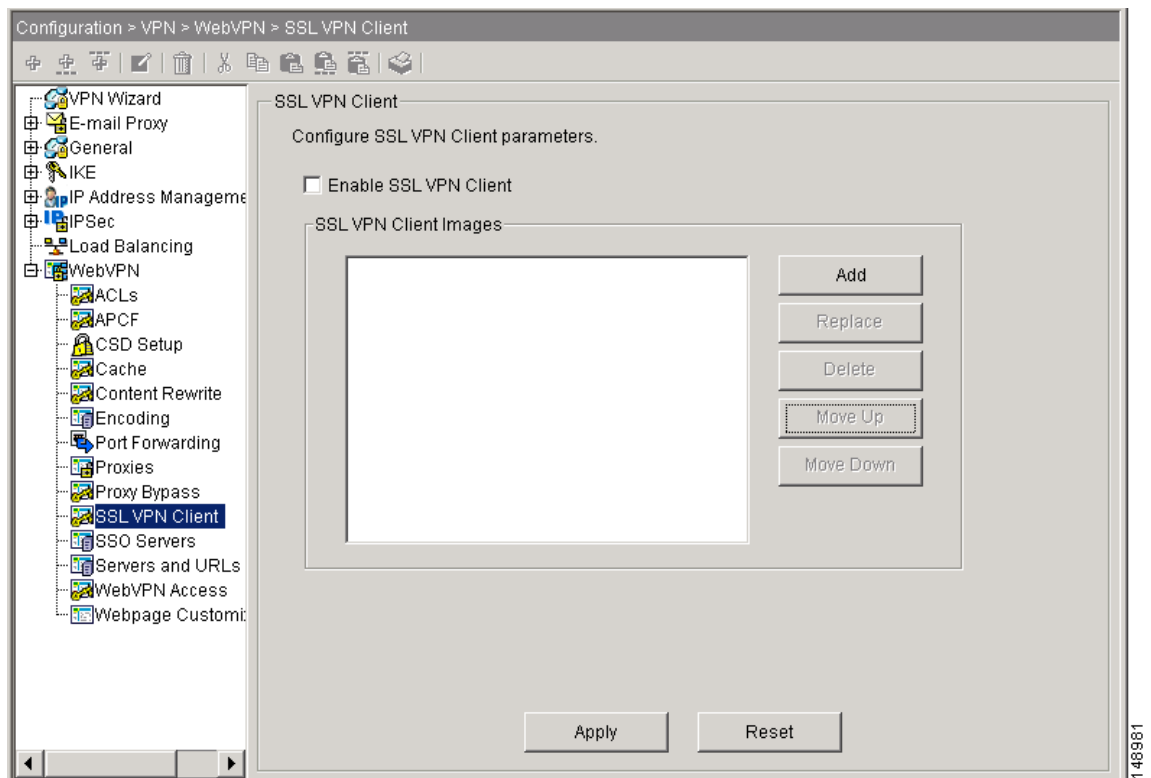
Installing SVC consists of uploading the SVC images to the flash memory, identifying to the security appliance the files on the flash memory to be used as SVC images, and setting the order in which it downloads the images to the remote computer.

Perform the following steps to install SVC:

- Step 1** Upload the SVC images to the security appliance. On the ASDM toolbar, Select **Configuration > VPN > WebVPN > SSL VPN Client**. The SSL VPN Client panel appears. (Figure 3-1).

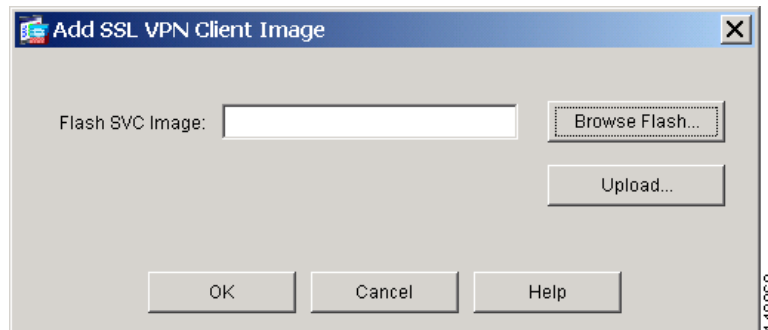
This window lists any SVC files that have been identified as SVC images. The order in which they appear in the table reflects the order that they download to the remote computer.

Figure 3-1 SSL VPN Client Window



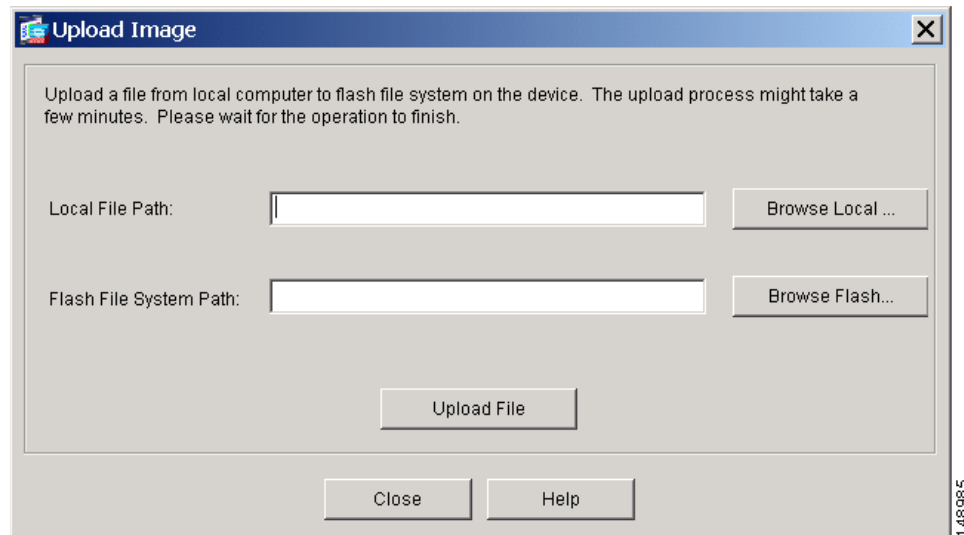
To add an SVC image, Click **Add**. The Add SSL VPN Client Image dialog box appears (Figure 3-2).

Figure 3-2 Add SSL VPN Client Image Dialog



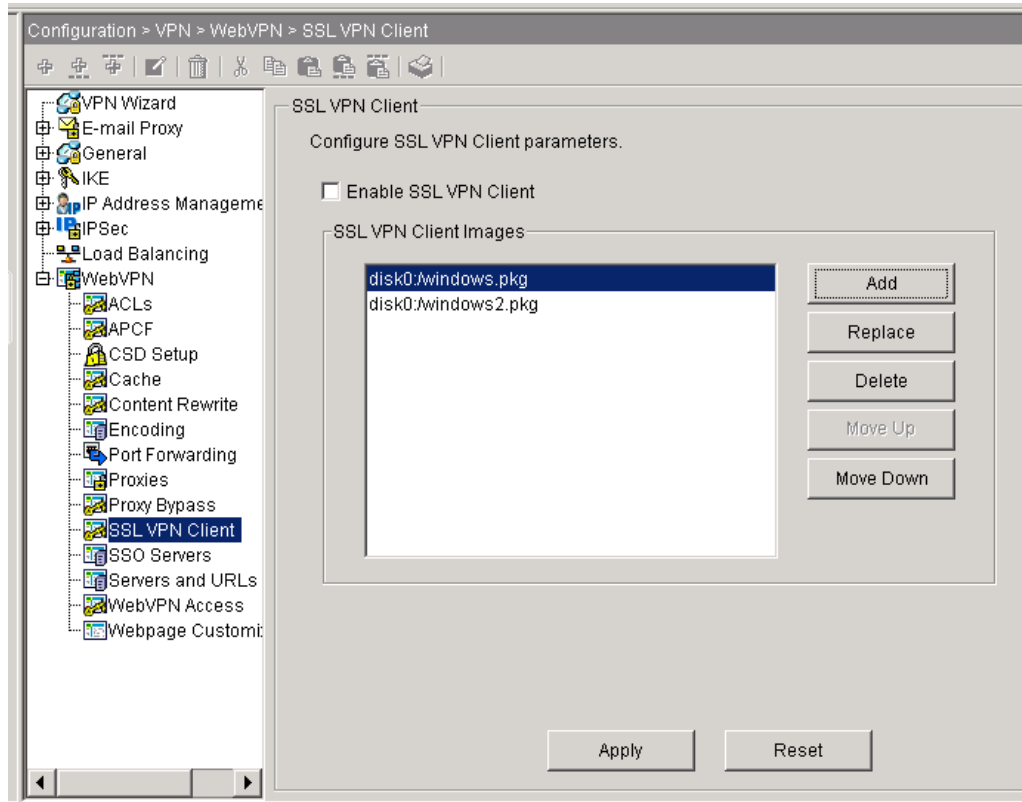
If you already have an image located in the flash memory of the security appliance, you can enter the name of the image in the Flash SVC Image field, and click **OK**. Otherwise, click **Upload** to browse the computer that is running ASDM. The Upload Image dialog box appears (Figure 3-3).

Figure 3-3 Upload Image Dialog



Enter the paths for the Local File Path and the Flash File System Path, or browse for the paths, and click **Upload File**. The SSL VPN Client window now shows the SVC images you identified (Figure 3-4).

Figure 3-4 SSL VPN Client Window with SVC Images

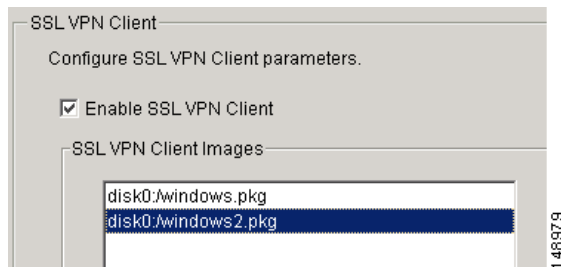


Step 2 Click on an image name, and use the **Move Down** button to change the position of the image within the list.

This establishes the order in which the security appliance downloads them to the remote computer. It downloads the SVC image at the top of the list of images first. Therefore, you should move the image used by the most commonly-encountered operating system to the top of the list.

Step 3 Check the **Enable SSL VPN Client** check box to enable the security appliance to download the SVC image(s) (Figure 3-5).

Figure 3-5 Enable SSL VPN Client Check Box

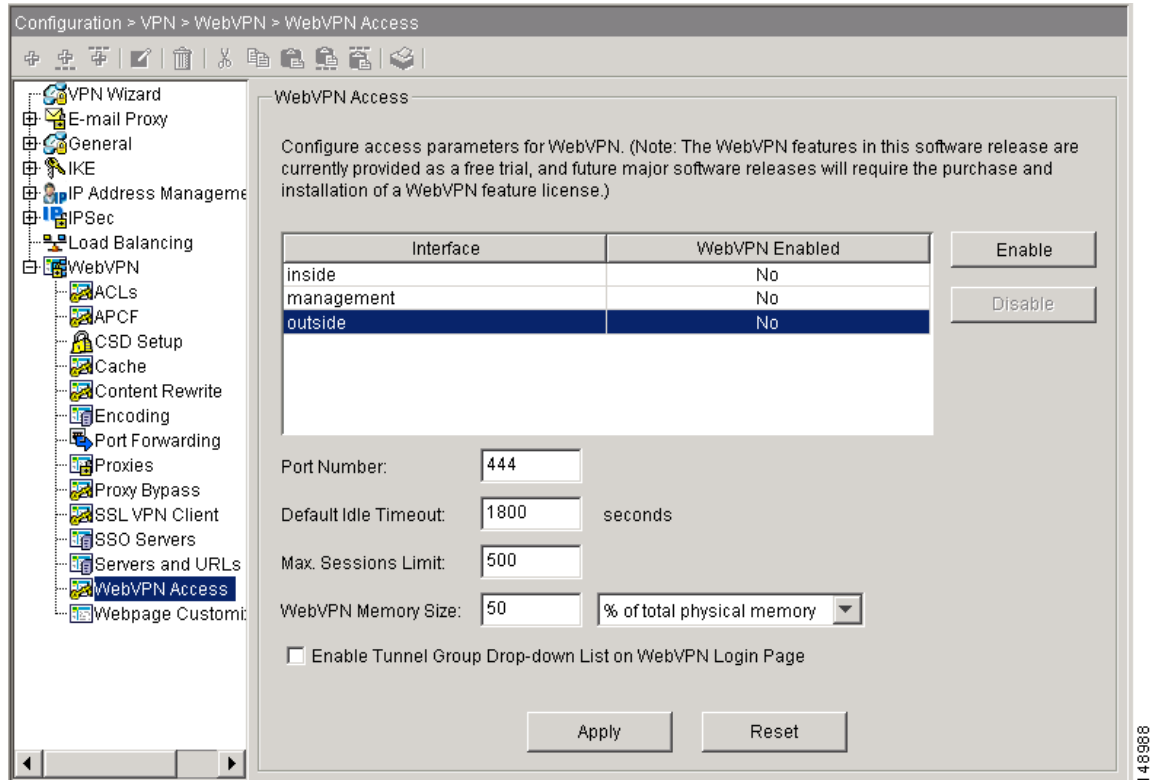


Configuring SVC

To configure SVC, perform the following steps:

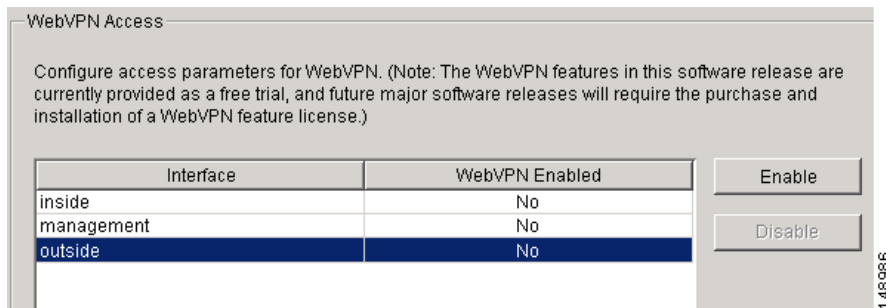
- Step 1** Enable WebVPN on an interface. From the navigation pane, choose **WebVPN Access**. The WebVPN Access window appears (Figure 3-6).

Figure 3-6 WebVPN Access Window



Highlight an interface and click **Enable** (Figure 3-7).

Figure 3-7 Enabling the Interface



Step 2 Configure a method of address assignment. You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a tunnel group.

To create an IP address pool, choose **Configuration > VPN > IP Address Management > IP Pools**. Click **Add**. The Add IP Pool dialog appears (Figure 3-8).

Figure 3-8 Add IP Pool Dialog

The screenshot shows a dialog box titled "Add IP Pool". It contains the following fields and values:

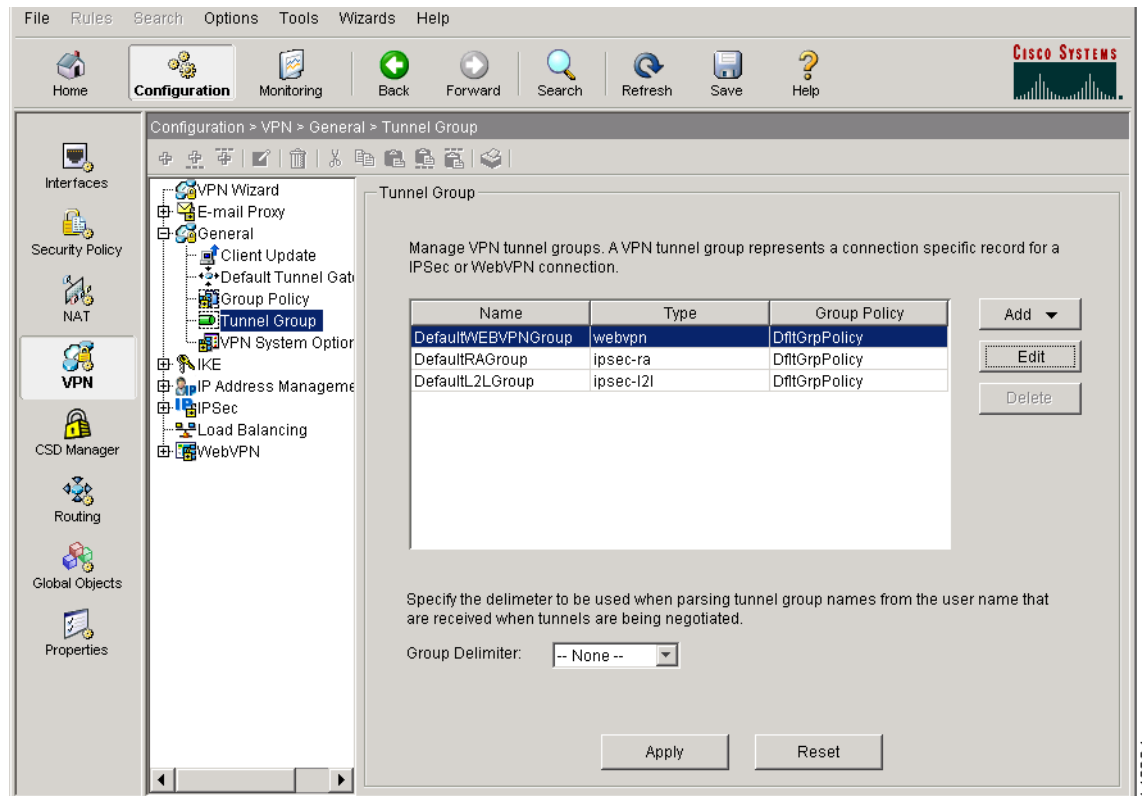
- Name: vpn_users
- Starting IP Address: 209.165.200.230
- Ending IP Address: 209.165.200.250
- Subnet Mask: 255.255.255.0

At the bottom of the dialog are three buttons: OK, Cancel, and Help. A vertical number "148978" is visible on the right side of the dialog box.

Enter the name of the new IP address pool. Enter the starting and ending IP addresses, and enter the subnet mask and click **OK**.

- Step 3** Assign the IP address pool to a tunnel group. To do this, choose **Configuration > VPN > General > Tunnel Group**. The Tunnel Group panel appears (Figure 3-9):

Figure 3-9 Tunnel Group Window



- Step 4** Highlight a tunnel group in the table, and click **Edit**.
The Edit Tunnel Group dialog appears.
- Step 5** Click the **Client Address Assignment** tab.
The **Client Address Assignment** tab appears (Figure 3-10), containing the Address Pools group box:

Figure 3-10 Edit Tunnel Group, General Tab, Client Address Assignment Tab

Edit Tunnel Group

Name: Type:

General | WebVPN

Configure general access attributes from the following sub-tabs.

Basic | AAA | **Client Address Assignment** | Advanced

To specify whether to use DHCP or address pools for address assignment, go to Configuration > VPN > IP Address Management > Assignment.

DHCP Servers

IP Address:

Address Pools

To configure interface-specific address pools, go to the Advanced tab.

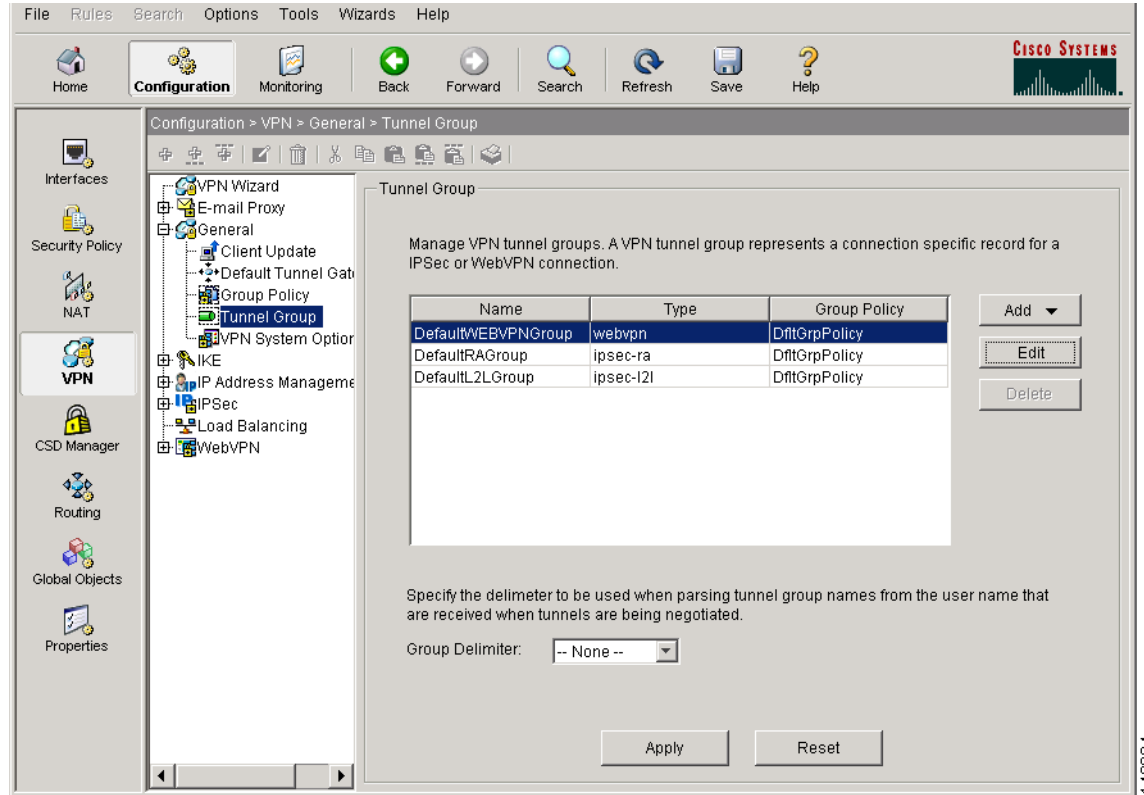
Available Pools	Assigned pools
vpn_users	

148973

In the Address Pools group box, choose an address pool to assign to the tunnel group and click **Add**.

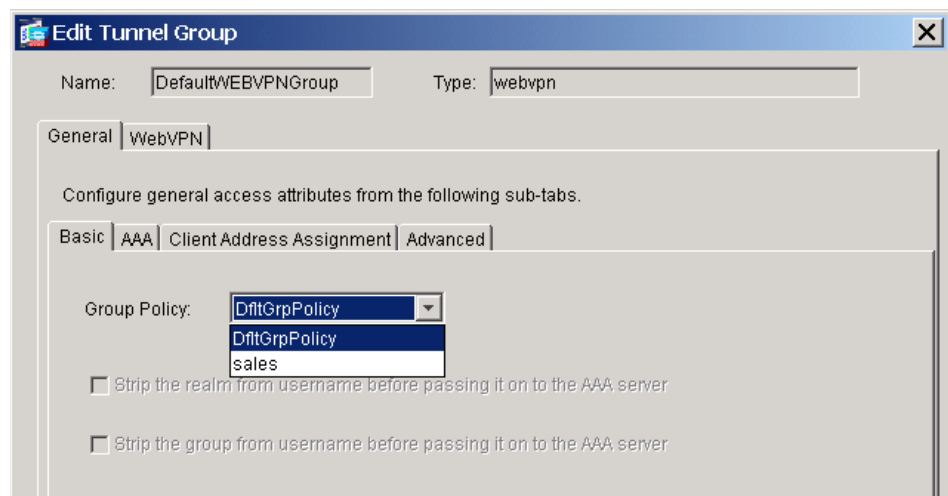
Step 6 Assign a default group policy to the tunnel group. Select **Configuration > VPN > General > Tunnel Group**. The Tunnel Group window appears (Figure 3-11).

Figure 3-11 Tunnel Group Window



Choose a WebVPN tunnel group from the table, and click **Edit**. The Edit Tunnel Group dialog, **General** tab appears (Figure 3-12).

Figure 3-12 Edit Tunnel Group Dialog, General Tab, Basic Tab

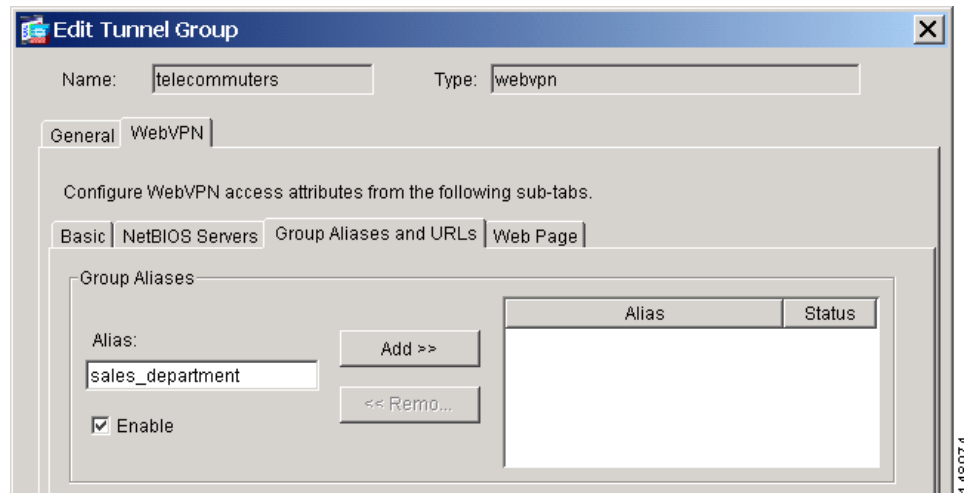


Choose a group policy in the Group Policy list and click **OK**.

Step 7 Create and enable a group alias that appears in the group list on the WebVPN Login page.

Click the **WebVPN** tab, and then click the **Group Aliases and URLs** tab. The Group Aliases and URLs tab appears (Figure 3-13):

Figure 3-13 Edit Tunnel Group Dialog, WebVPN Tab, Group Aliases and URLs Tab



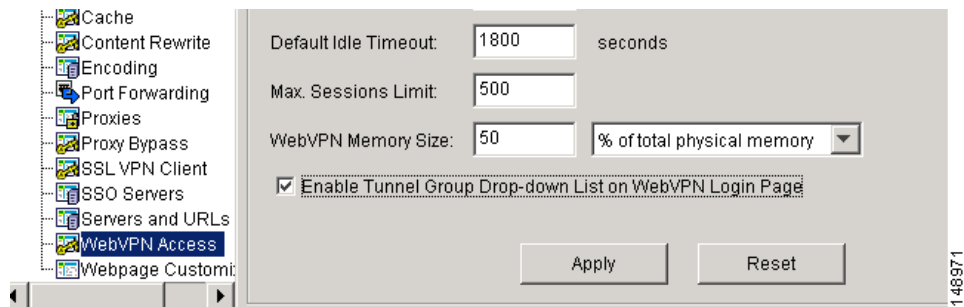
Enter the name of the new alias in the Alias field. Click **Add** to add it as a new alias.

Click the **Enable** check box to enable group aliases and URLs.

Step 8 Enable the display of the tunnel-group list on the WebVPN Login page.

Choose **Configuration > VPN > WebVPN > WebVPN Access**. The WebVPN Access panel appears (Figure 3-14). Click the **Enable Tunnel Group Drop-Down List on WebVPN Login Page** check box, and click **Apply**.

Figure 3-14 WebVPN Access Window, Enable Tunnel Group Drop-Down List on WebVPN Login Page Check Box

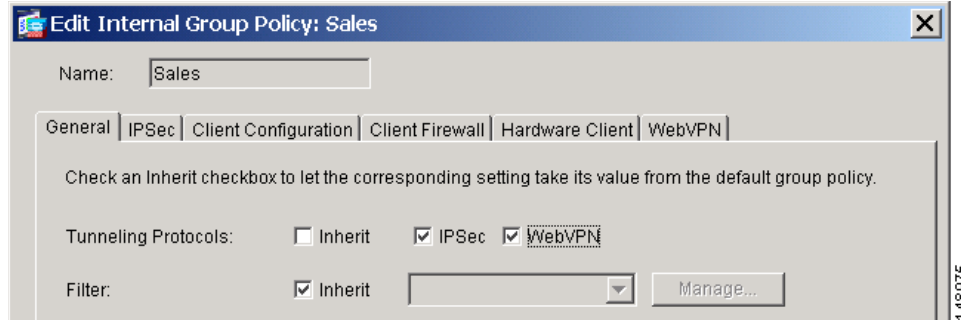


Step 9 Identify WebVPN as a permitted VPN tunneling protocol for the group or user.

Choose **Configuration > VPN > General > Group Policy** from the navigation pane. Highlight the group policy in the Group Policy table, and click **Edit**.

The General Tab of the Edit Internal Group Policy dialog appears (Figure 3-15):

Figure 3-15 Edit Internal Group Policy, GeneralTab



Check the **WebVPN** check box to include WebVPN as a tunneling protocol.

Step 10 Configure SVC features for a user or group. These features are shown in the **SSL VPN Client** tab of both the Edit User Accounts dialog and the Edit Group Policy dialog.

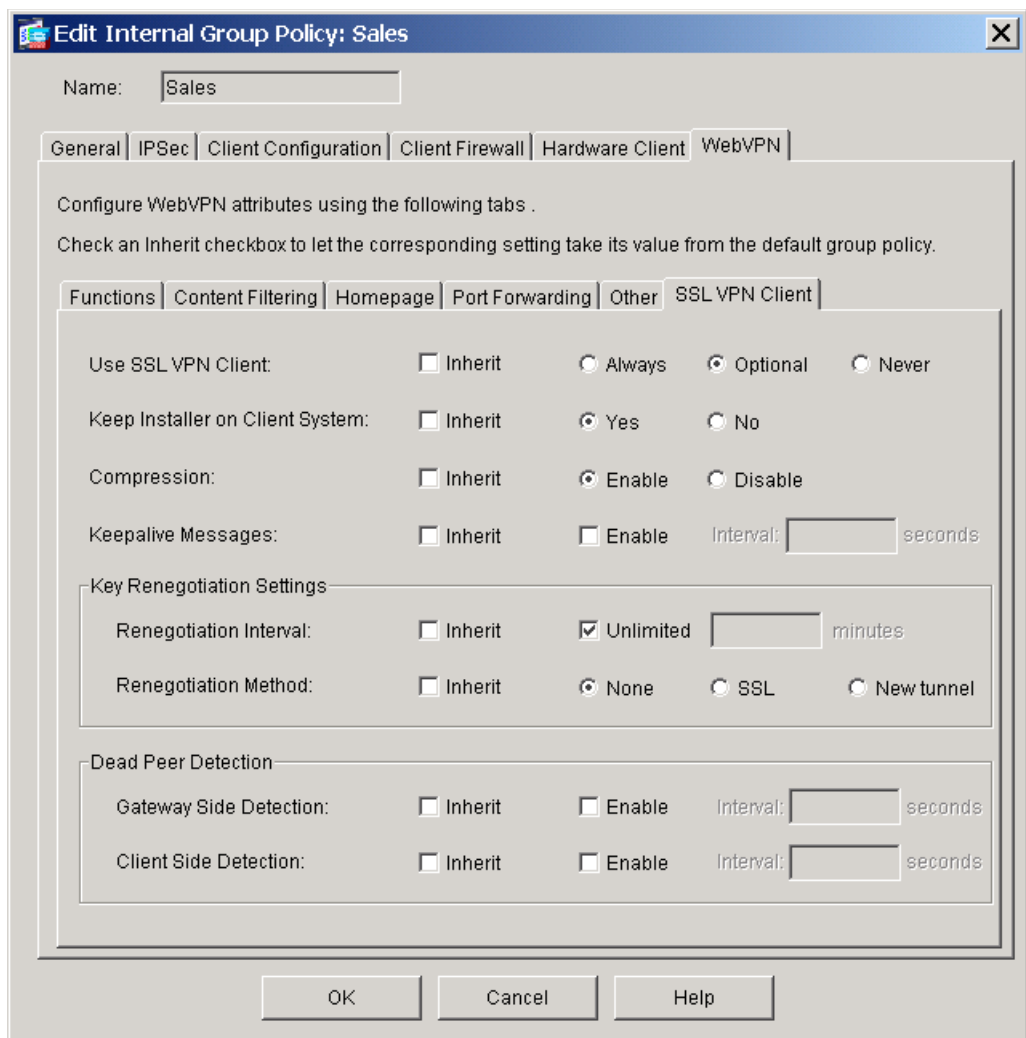
To display the **SSL VPN Client** tab For users:

- Click **Configuration > Properties > Device Administration > User Accounts**. The User Accounts panel appears.
- Choose a user in the table, and click **Edit**. The Edit User Account dialog, **General** tab appears.
- Click the **WebVPN** tab, and then click the **SSL VPN** tab. The **SSL VPN Client** tab appears [Figure 3-16](#).

To display the **SSL VPN Client** tab for groups, do the following:

- Click **Configuration > VPN > WebVPN > Group Policies**. The Group Policy panel appears.
- Choose a group policy in the table, and click **Edit**. The Edit Internal Group Policy dialog, **General** tab appears.
- Click the **WebVPN** tab, and then click the **SSL VPN** tab. The **SSL VPN Client** tab appears. It is identical to the **SSL VPN Client** tab displayed for user accounts in [Figure 3-16](#), but it does not include **Inherit** check boxes for the features.

Figure 3-16 SSL VPN Client Tab



Note

For user accounts, the **SSL VPN Client** tab includes the additional **Inherit** check box for every SVC feature. If you check the **Inherit** check box, the feature is configured according to the setting in the group policy of the user.

Configure the following features on the SSL VPN Client tab:

Use SSL VPN Client—Require the SVC, make it optional, or disable it for the user or group.

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

Compression—SVC compression increases the communications performance between the security appliance and the SVC by reducing the size of the packets being transferred.

Keepalive Messages—Check the **Enable** checkbox to enable and adjust the interval of keepalive messages to ensure that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.

Adjusting the interval also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

The Seconds field specifies the interval of the messages in the range of 15 to 600 seconds.

Rekey Negotiation Settings—When the security appliance and the SVC perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

- **Renegotiation Interval**—Clear the **Unlimited** check box to specify the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).
- **Renegotiation Method**—Check the **None** check box to disable rekey, check the **SSL** check box to specify SSL renegotiation during a rekey, or check the **tunnel** check box to establish a new tunnel during SVC rekey.

Dead Peer Detection—Dead Peer Detection (DPD) ensures that the security appliance (gateway) or the SVC can quickly detect a condition where the peer is not responding, and the connection has failed.

- **Gateway Side Detection**—Check the **Enable** check box to specify that DPD is performed by the security appliance (gateway). Enter the interval, from 30 to 3600 seconds, with which the security appliance performs DPD.
 - **Client Side Detection**—Check the **Enable** check box to specify that DPD is performed by the SVC (client). Enter the interval, from 30 to 3600 seconds, with which the SVC performs DPD.
-

Viewing SVC Sessions

You can view information about active SVC sessions in the Sessions window.

Choose **Monitoring > VPN > VPN Statistics > Sessions**. The Sessions window appears (Figure 3-17)

Figure 3-17 VPN Statistics Sessions Window

The screenshot shows the Cisco ASDM 5.1 for ASA - 10.86.195.74 interface. The navigation pane on the left shows the path: Monitoring > VPN > VPN Statistics > Sessions. The main window displays the following summary table:

Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
0	0	0	1	0	1	60

Below the summary table, the filter is set to "SSL VPN Client" and "-- All Sessions --". The detailed table shows one active session:

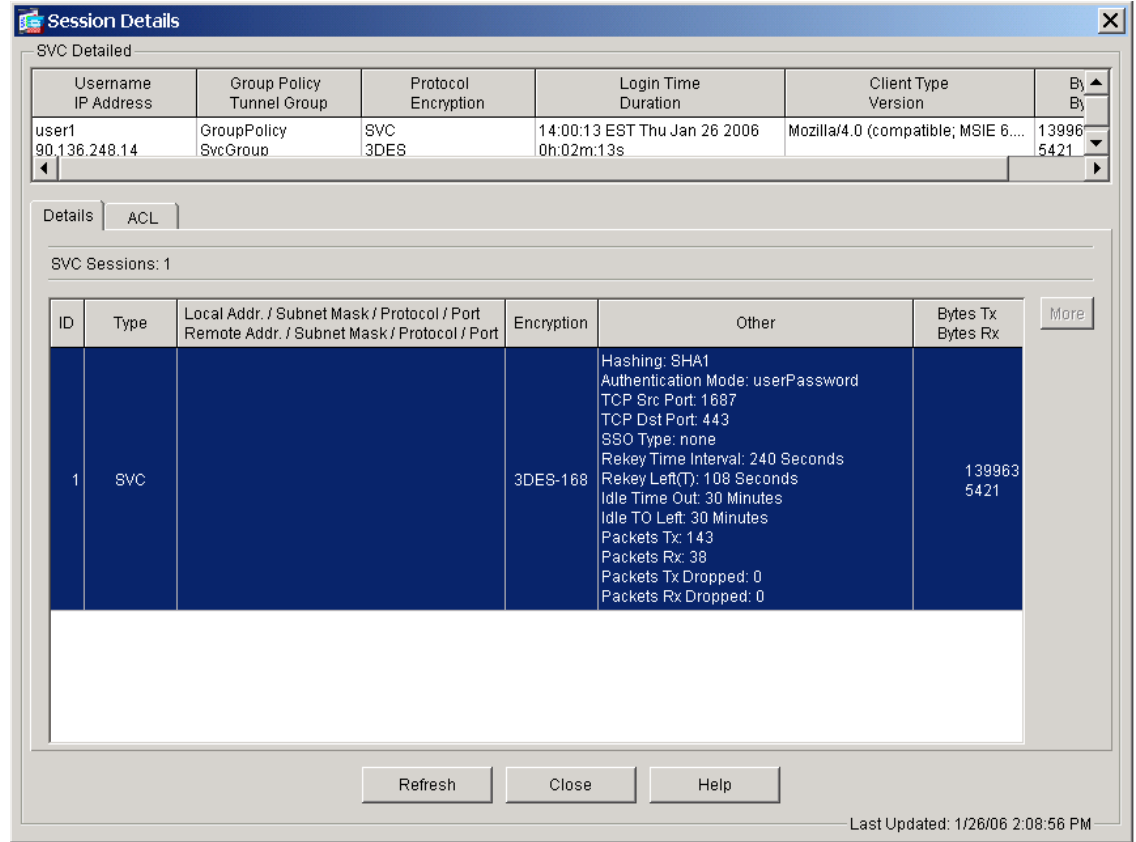
Username	Group Policy	Protocol	Login Time	Details
IP Address	Tunnel Group	Encryption	Duration	Logout
user1	GroupPolicy	SVC	14:00:13 EST Thu J	Logout
90.136.248.14	SvcGroup	3DES	0h:00m:33s	Ping

At the bottom of the window, there is a "Logout Sessions" button and a "Refresh" button. The status bar at the bottom indicates "Data Refreshed Successfully." and "Last Updated: 1/26/06 2:07:16 PM".

You can view details about active SVC sessions in the Session Details window.

Choose a session in the session table, and click **Details**. The Session Details window appears (Figure 3-18):

Figure 3-18 Session Details Window



148982

Logging Off SVC Sessions

To log off all SVC sessions, choose the session that you want to terminate from the list of active sessions in the Session table.

Click **Logout**. The session terminates.

Figure 3-19 Logging Off Sessions

The screenshot shows the 'Sessions' page in the ASDM interface. The left sidebar contains a tree view with 'Sessions' selected. The main area displays a summary table and a list of active sessions.

Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
0	0	0	1	0	1	60

Filter By: SSL VPN Client -- All Sessions -- Filter

Username	Group Policy	Protocol	Login Ti	Details
IP Address	Tunnel Group	Encryption	Duration	
user1	GroupPolicy	SVC	14:00:13 EST Thu J	Logout
90.136.248.14	SvcGroup	3DES	0h:00m:33s	Ping

153012