



CHAPTER 28

WebVPN

WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach HTTPS Internet sites. WebVPN uses Secure Socket Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to WebVPN resources on a user or group basis. Users have no direct access to resources on the internal network.

WebVPN works on the platform in single, routed mode.

For information on configuring WebVPN for end users, see [WebVPN End User Set-up](#).

WebVPN Security Precautions

WebVPN connections on the security appliance are very different from remote access IPSec connections, particularly with respect to how they interact with SSL-enabled servers, and precautions to reduce security risks.

In a WebVPN connection, the security appliance acts as a proxy between the end user web browser and target web servers. When a WebVPN user connects to an SSL-enabled web server, the security appliance establishes a secure connection and validates the server SSL certificate.

The current implementation of WebVPN does not permit communication with sites that present expired certificates. Nor does the security appliance perform trusted CA certificate validation. Therefore, WebVPN users cannot analyze the certificate an SSL-enabled web server presents before communicating with it.

To minimize the risks involved with SSL certificates:

- Configure a group policy for all users who need WebVPN access and enable the WebVPN feature only for that group policy.
- Limit Internet access for WebVPN users. One way to do this is to clear the **Enable URL entry** check box on the Configuration > VPN > General > Group Policy > WebVPN panel. Then configure links to specific targets within the private network (Configuration > VPN > WebVPN > Servers and URLs).

- Educate users. If an SSL-enabled site is not inside the private network, users should not visit this site over a WebVPN connection. They should open a separate browser window to visit such sites, and use that browser to view the presented certificate.

ACLs

You can configure ACLs (Access Control Lists) to apply to user sessions. These are filters that permit or deny user access to specific networks, subnets, hosts, and web servers.

- If you do not define any filters, all connections are permitted.
- The security appliance supports only an inbound ACL on an interface.
- At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry (ACE), the security appliance denies it. ACEs are referred to as rules in this topic.

This pane lets you add and edit WebVPN ACLs and the ACL entries that each ACL contains. It also displays summary information about ACLs and ACEs, and lets you enable or disable them, and change their priority order.

Fields

- Add ACL—Click to add an ACL or ACE. To insert a new ACE before or after an existing ACE, click Insert or Insert After.
- Edit—Click to edit the highlighted ACE. When you delete an ACL, you also delete all of its ACEs. No warning or undelete.
- Delete—Click to delete the highlighted ACL or ACE. When you delete an ACL, you also delete all of its ACEs. No warning or undelete.
- Move UP/Move Down—Highlight an ACL or ACE and click these buttons to change the order of ACLs and ACEs. The security appliance checks WebVPN ACLs and their ACEs in priority order according to their position in the ACLs list box until it finds a match.
- +/-—Click to expand (+) or collapse (-) to view or hide the list of ACEs under each ACL.
- No—Displays the priority of the ACEs under each ACL. The order in the list determines priority.
- Address—Displays the IP address or URL of the application or service to which the ACE applies.
- Service—Displays the TCP service to which the ACE applies.
- Action—Displays whether the ACE permits or denies WebVPN access.
- Time—Displays the time range associated with the ACE.
- Logging (Interval)—Displays the configured logging behavior, either disabled or with a specified level and time interval.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add ACL

This pane lets you create a new ACL.

Fields

- **ACL Name**—Enter a name for the ACL. Maximum 55 characters.

Add/Edit ACE

An Access Control Entry permits or denies access to specific URLs and services. You can configure multiple ACEs for an ACL. ACLs apply ACEs in priority order, acting on the first match.

Fields

- **Action**—Permits or denies access to the specific networks, subnets, hosts, and web servers specified in the Filter group box.
- **Filter**—Specifies a URL or an IP address to which you want to apply the filter (permit or deny user access).
 - **URL**—Applies the filter to the specified URL.
 - **Protocols (unlabeled)**—Specifies the protocol part of the URL address.
 - **://x**—Specifies the URL of the Web page to which to apply the filter.
 - **TCP**—Applies the filter to the specified IP address, subnet, and port.
 - **IP Address**—Specifies the IP address to which to apply the filter.
 - **Netmask**—Lists the standard subnet mask to apply to the address in the IP Address box.
 - **Service**—Identifies the service (such as https, kerberos, or any) to be matched. Displays a list of services from which you can select the service to display in the Service box.
 - **Boolean operator (unlabeled)**—Lists the boolean conditions (equal, not equal, greater than, less than, or range) to use in matching the service specified in the service box.
- **Rule Flow Diagram**—Graphically depicts the traffic flow using this filter. This area might be hidden.
- **Options**—Specifies the logging rules. The default is Default Syslog.
 - **Logging**—Choose enable if you want to enable a specific logging level.
 - **Syslog Level**—Grayed out until you select Enable for the Logging attribute. Lets you select the type of syslog messages you want the security appliance to display.
 - **Log Interval**—Lets you select the number of seconds between log messages.
 - **Time Range**—Lets you select the name of a predefined time-range parameter set.
 - **...**—Click to browse the configured time ranges or to add a new one.

Examples

Here are examples of WebVPN ACLs:

Action	Filter	Effect
Deny	url http://*.yahoo.com/	Denies access to all of Yahoo!
Deny	url cifs://fileserver/share/directory	Denies access to all files in the specified location.

Action	Filter	Effect
Deny	url https://www.company.com/ directory/file.html	Denies access to the specified file.
Permit	url https://www.company.com/directory	Permits access to the specified location
Deny	url http://*:8080/	Denies HTTPS access to anywhere via port 8080.
Deny	url http://10.10.10.10	Denies HTTP access to 10.10.10.10.
Permit	url any	Permits access to any URL. Usually used after an ACL that denies url access.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

APCF

WebVPN includes an Application Profile Customization Framework option that lets the security appliance handle non-standard applications and web resources so they display correctly over a WebVPN connection. An APCF profile contains a script that specifies when (pre, post), where (header, body, request, response), and what data to transform for a particular application. The script is in XML and uses sed (stream editor) syntax to transform strings/text.

You can configure multiple APCF profiles on a security appliance to run in parallel. Within an APCF profile script, multiple APCF rules can apply. In this case, the security appliance processes the oldest rule first, based on configuration history, the next oldest rule next, and so forth.

You can store APCF profiles on the security appliance flash memory, or on an HTTP, HTTPS, FTP, or TFTP server. Use this panel to add, edit, and delete APCF packages, and to put them in priority order.

Fields

- **APCF File Location**—Displays information about the location of the APCF package. This can be on the security appliance flash memory, or on an HTTP, HTTPS, FTP, or TFTP server.
- **Add/Edit**—Click to add or edit a new or existing APCF profile.
- **Delete**—Click to remove an existing APCF profile. There is no confirmation or undo.
- **Move Up/Move Down**—Click to rearrange APCF profiles within a list. This determines the order in which the security appliance attempts to use APCF profiles.

Add/Edit APCF Profile

This panel lets you add or edit an APCR package, which includes identifying its location, which can be either on the security appliance flash memory, or on an HTTP, HTTPS, or TFTP server.

Fields

- **Flash file**—Check to locate an APCR file stored on the security appliance flash memory.
- **Path**—Displays the path to an APCR file stored on flash memory after you browse to locate it. You can also manually enter the path in this field.
- **Browse Flash**—Click to browse flash memory to locate the APCR file. A Browse Flash Dialog panel displays. Use the Folders and Files columns to locate the APCR file. Highlight the APCR file and click **OK**. The path to the file then displays in the Path field.



Note If you do not see the name of an APCR file that you recently downloaded, click the Refresh button.

- **Upload** —Click to upload an APCR file from a local computer to the security appliance flash file system. The Upload APCR package pane displays.
- **URL**—Check to use an APCR file stored on an HTTP, HTTPS or TFTP server.
- **http/https/tftp (unlabeled)**—Identify the server type.
- **URL (unlabeled)**—Enter the path to the HTTP, HTTPS, or TFTP server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Upload APCR package

Fields

- **Local File Path**—Shows the path to the APCR file on your computer. Click **Browse Local** to automatically insert the path in this field, or enter the path.
- **Browse Local**—Click to locate and choose the APCR file on your computer that you want to transfer. The Select File Path dialog box displays the contents of the folder you last accessed on your local computer. Navigate to the APCR file, select it, and click **Open**. ASDM inserts the file path into the Local File Path field.
- **Flash File System Path**—Displays the path on the security appliance to upload the APCR file.
- **Browse Flash**—Click to identify the location on the security appliance to which you want to upload the APCR file. The Browse Flash dialog box displays the contents of flash memory.

- **File Name**—Located in the Browse Flash dialog box that opens when you click Browse Flash, this field displays the name of the APCF file you selected on your local computer. We recommend that you use this name to prevent confusion. Confirm that this file displays the correct filename, and click **OK**. The Browse Flash dialog box closes. ASDM inserts the destination file path in the Flash File System Path field.
- **Upload File**—Click when you have identified the location of the APCF file on your computer, and the location where you want to download it to the security appliance.
- A Status window appears and remains open for the duration of the file transfer. Following the transfer, an Information window displays the message, “File is uploaded to flash successfully.” Click **OK**. The Upload Image dialog window removes the contents of the Local File Path and Flash File System Path fields, indicating you can upload another file. To do so, repeat these instructions. Otherwise, click the **Close** button.
- **Close**—Closes the Upload Image dialog window. Click this button after you upload the APCF file to flash memory or if you decide not to upload it. If you do upload it, the filename appears in the APCF File Location field of the APCF window. If you do not upload it, a Close Message dialog box prompts, “Are you sure you want to close the dialog without uploading the file?” Click **OK** if you do not want to upload the file. The Close Message and Upload Image dialog boxes close, revealing the APCF Add/Edit pane. Otherwise, click **Cancel** in the Close Message dialog box. The dialog box closes, revealing the Upload Image dialog box again, with the values in the fields intact. Click **Upload File**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Auto Signon

The Auto Signon window or tab lets you configure or edit auto signon for WebVPN users. Auto signon is a simplified single signon method that you can use if you do not already have an SSO method deployed on your internal network. With auto signon configured for particular internal servers, the security appliance passes the login credentials that the WebVPN user used to login to the security appliance (username and password) to those particular internal servers. You configure the security appliance to respond to a specific authentication method for a particular range of servers. The authentication methods you can configure the security appliance to respond to are NTLM authentication, HTTP Basic authentication, or both methods.

Auto signon is a straight-forward method for configuring SSO for particular internal servers. This section describes the procedure for setting up SSO with auto signon. If you already have SSO deployed using Computer Associates’ SiteMinder SSO server and want to configure the security appliance to support this solution, see [SSO Servers](#). If you use SSO with HTTP Forms protocol and want to configure the security appliance to support this method, see [AAA Setup](#).

Fields

- IP Address—*Display only*. In conjunction with the following Mask, displays the IP address range of the servers to be authenticated to as configured with the Add/Edit Auto Signon dialog box. You can specify a server using either the server URI or the server IP address and mask.
- Mask—*Display only*. In conjunction with the preceding IP Address, displays the IP address range of the servers configured to support auto signon with the Add/Edit Auto Signon dialog box.
- URI—*Display only*. Displays a URI mask that identifies the servers configured with the Add/Edit Auto Signon dialog box.
- Authentication Type—*Display only*. Displays the type of authentication—basic HTTP, NTLM, or basic and NTLM—as configured with the Add/Edit Auto Signon dialog box.
- Add/Edit—Click to add or edit an auto signon instruction. An auto signon instruction defines a range of internal servers using the auto signon feature and the particular authentication method.
- Delete—Click to delete an auto signon instruction selected in the Auto Signon table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Auto Signon Entry

The Add/Edit Auto Signon Entry dialog box lets you add or edit a new auto signon instruction. An auto signon instruction defines a range of internal servers using the auto signon feature and the particular authentication method.

Fields

- IP Block—Click this button to specify a range of internal servers using an IP address and mask.
 - IP Address—Enter the IP address of the first server in the range for which you are configuring auto-signon.
 - Mask—In the subnet mask menu, click the subnet mask that defines the server address range of the servers supporting auto signon.
- URI—Click this button to specify a server supporting auto signon by URI, then enter the URI in the field next to this button.
- Authentication Type—The authentication method assigned to the servers. For the specified range of servers, the security appliance can be configured to respond to HTTP Basic authentication requests, NTLM authentication requests, or requests using either method.
 - Basic—Click this button to assign basic HTTP authentication.
 - NTLM—Click this button use NTLMv1 authentication.
 - Basic and NTLM—Click this button use either HTTP Basic or NTLMv1 authentication.

**Note**

If you configure one method for a range of servers (e.g., HTTP Basic) and one of those servers attempts to authenticate with a different method (e.g., NTLM), the security appliance does not pass the users login credentials to that server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

CSD Setup

This window lets you view the version and state of the CSD distribution package, and install, upgrade, enable, and disable CSD.

Fields

CSD Setup

- **Secure Desktop Image**—Displays the CSD distribution package loaded into the running configuration. This field should display the filename in the format `securedesktop_asa_<n>_<n>*.pkg`. Use the **Browse Flash** button to insert or modify the value in this field. You can also use this field to view the version of CSD. (The Configuration CSD Secure Desktop Manager also displays the CSD version.)
- **Enable Secure Desktop**—Check and click **Apply** to do the following:
 - a. Make sure the file is a valid CSD distribution package.
 - b. Create an “sdesktop” folder on disk0 if one is not already present.
 - c. Insert a data.xml (CSD configuration) file into the sdesktop folder if one is not already present.
 - d. Load the data.xml file into the running configuration.

**Note**

If you transfer or replace the data.xml file, disable and then enable CSD to load the file.

- e. Enable CSD.
- **Browse Flash**—Click to view the contents of the flash device and choose or type the filename of the CSD distribution package to install into the running configuration. You can use this button to install, upgrade or downgrade CSD. Click **Apply** to save the CSD setup.

**Note**

If you click the **Browse Flash** button to upgrade or downgrade the CSD distribution package, select the package to install, and click **OK**, the Uninstall CSD dialog window asks you if you want to delete the CSD distribution currently in the running configuration from the flash device. Click **Yes** if you want to save space on the flash device, or click **No** to reserve the option to revert to this version of CSD.

- **Upload**—Lets you transfer a copy of a CSD distribution package from your local computer to the flash device. To prepare to install or upgrade CSD, use your Internet browser to download a `securedesktop_asa_<n>_<n>*.pkg` file from <http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop> to any location on your PC. Then use this button to transfer a copy from you local computer to the flash device. Finally, click **Browse Flash** to install it into the running configuration.
- **Uninstall**—Lets you remove the CSD image and configuration file (`sdesktop/data.xml`) from the running configuration. If you click this button, the Uninstall CSD dialog window asks if you want to delete the CSD image that was named in the “Secure Desktop Image field” and all CSD data files (including the entire CSD configuration) from the flash device. Click **Yes** if you want to remove these files from both the running configuration and the flash device, or click **No** to remove them from the running configuration, but retain them on the flash device.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Upload Image

This dialog window lets you transfer a copy of a CSD distribution package from your local computer to the flash device on the security appliance. Use this window to install or upgrade CSD.



Note

Before using this window, use your Internet browser to download a `securedesktop_asa_<n>_<n>*.pkg` file from <http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop> to any location on your local computer.

Fields

Use the fields and options in this window as follows:

- **Local File Path**—Specifies the path to the `securedesktop_asa_<n>_<n>*.pkg` file on your local computer. Click **Browse Local** to automatically insert the path in this field, or enter the path. For example:

```
D:\Documents and Settings\Windows_user_name.AMER\My Documents\My Downloads\securedesktop_asa_3_1_1_16.pkg
```
- **Browse Local**—Click to select the path of the `securedesktop_asa_<n>_<n>*.pkg` file to be transferred. The Selected File Path dialog box displays the contents of the folder you last accessed on your local computer. Navigate to the `securedesktop_asa_<n>_<n>*.pkg` file, select it, and click **Open**.
 ASDM inserts the file path into the Local File Path field.
- **Flash File System Path**—Specifies the destination path on the flash device of the security appliance and the name of the destination file. Click **Browse Flash** to automatically insert the path into this field, or enter the path. For example,

disk0:/secredesktop_asa_3_1_1_16.pkg

- **Browse Flash**—Click to select the target directory for the file. The Browse Flash dialog box displays the contents of the flash card.
- **File Name**—Located in the Browse Flash dialog box that opens if you click **Browse Flash**, this field displays the name of the CSD distribution package you selected on your local computer. We recommend that you use this name to prevent confusion. Confirm that this field displays the same name of the local file you selected and click **OK**. The Browse Flash dialog box closes. ASDM inserts the destination file path into the Flash File System Path field.
- **Upload File**—Uploads the securedesktop_asa_<n>_<n>*.pkg file from your local computer to the flash device. A Status window appears and remains open for the duration of the file transfer. Following the transfer, an Information window displays the message, “File is uploaded to flash successfully.” Click **OK**. The Upload Image dialog window removes the contents of the Local File Path and Flash File System Path fields, indicating you can upload another file. To do so, repeat these instructions. Otherwise, click the **Close** button.
- **Close**—Closes the Upload Image dialog window. Click this button after you upload the CSD distribution package to the flash device or if you decide not to upload it. If you uploaded it, the filename appears in the Secure Desktop Image field of the CSD Setup window. If you did not upload it, a Close Message dialog box prompts, “Are you sure you want to close the dialog without uploading the file?” Click **OK** if you do not want to upload the file. The Close Message and Upload Image dialog boxes close, revealing the CSD Setup pane. Otherwise, click **Cancel** in the Close Message dialog box. The dialog box closes, revealing the Upload Image dialog box again, with the values in the fields intact. Click **Upload File**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Cache

Caching enhances WebVPN performance. It stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, with the result that many applications run much more efficiently.

Fields

- **Enable cache**—Check to enable caching.
- **Parameters**—Lets you define the terms for caching.
 - **Enable caching of compressed content**—Check to cache compressed content. When you disable this parameter, the security appliance stores objects before it compresses them.
 - **Maximum Object Size**—Enter the maximum size in KB of a document that the security appliance can cache. The security appliance measures the original content length of the object, not rewritten or compressed content. The range is 0 to 10,000 KB; the default is 1000 KB

- Minimum Object Size—Enter the minimum size in KB of a document that the security appliance can cache. The security appliance measures the original content length of the object, not rewritten or compressed content. The range is 0 to 10,000 KB; the default is 0 KB.



Note The Maximum Object Size must be greater than the Minimum Object Size.

- LM Factor—Enter an integer between 1 and 100; the default is 20.

The LM factor sets the policy for caching objects which have only the last-modified timestamp. This revalidates objects that have no server-set change values. The security appliance estimates the length of time since the object has changed, also called the expiration time. The estimated expiration time equals the time elapsed since the last change multiplied by the LM factor. Setting the LM factor to 0 forces immediate revalidation, while setting it to 100 results in the longest allowable time until revalidation.

- Expiration Time—Enter an integer between 0 and 900 to set the number of minutes to cache objects without revalidating them. The default is one minute.

The expiration time sets the amount of time to for the security appliance to cache objects that have neither a last-modified time stamp nor an explicit server-set expiry time.

- Restore Cache Default—Click to restore default values for all cache parameters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Content Rewrite

The Content Rewrite panel lists all applications for which content rewrite is enabled or disabled.

WebVPN processes application traffic through a content transformation/rewriting engine that includes advanced elements such as JavaScript, VBScript, Java, and multi-byte characters to proxy HTTP traffic which may have different semantics and access control rules depending on whether the user is using an application within or independently of an SSL VPN device.

You might not want some applications and web resources, for example, public websites, to go through the security appliance. The security appliance therefore lets you create rewrite rules that let users browse certain sites and applications without going through the security appliance. This is similar to split-tunneling in an IPsec VPN connection.

You can create multiple rewrite rules. The rule number is important because the security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

Fields

- Content Rewrite
 - Rule Number—Displays an integer that indicates the position of the rule in the list.

- Rule Name—Provides the name of the application for which the rule applies.
- Rewrite Enabled—Displays content rewrite as enabled or disabled.
- Resource Mask—Displays the resource mask.
- Add/Edit—Click to add a rewrite entry or edit a selected rewrite entry.
- Delete—Click to delete a selected rewrite entry.

.Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Content Rewrite Rule

- Enable content rewrite—Check to enable content rewrite for this rewrite rule.
- Rule Number—(Optional) Enter 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 1 to 65534.
- Rule Name—(Optional) Provide an alphanumeric string that describes the rule, maximum 128 characters.
- Resource Mask—Enter the resource mask. This is a word, length up to 300 characters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Java Trustpoint

Java objects which have been transformed by WebVPN can subsequently be signed using a PKCS12 digital certificate associated with a trustpoint. In the Java Trustpoint pane, you can configure the WebVPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location. To import a trustpoint, see Configuration > Properties > Certificate > Trustpoint > Import.

Fields

- Java Trustpoint—Choose the configured trustpoint that you want to employ in Java object signing.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Encoding

This window lets you specify the character encoding for WebVPN portal pages to remote clients.

Character encoding, also called “character coding” and “a character set,” is the pairing of raw data (such as 0’s and 1’s) with characters to represent the data. The language determines the character encoding method to use. Some languages use the same method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the remote user can change this. The browser can also detect the encoding specified on the page, and render the document accordingly.

The encoding attribute lets you specify the value of the character-encoding method into the WebVPN portal page to ensure that the browser renders it properly, regardless of the region in which the user is using the browser, or any changes made to the browser.

By default, the security appliance applies the “Global WebVPN Encoding Type” to pages from Common Internet File System servers. The mapping of CIFS servers to their appropriate character encoding, globally with the “Global WebVPN Encoding Type” attribute, and individually with the file-encoding exceptions displayed in the table, provides for the accurate handling and display of CIFS pages when the proper rendering of filenames or directory paths, as well as pages, are an issue.

Fields

- Global WebVPN Encoding Type —This attribute determines the character encoding that all WebVPN portal pages inherit except for those from the CIFS servers listed in the table. You can type the string, or select one from the drop-down list, which contains only the most common values, as follows:
 - big5
 - gb2312
 - ibm-850
 - iso-8859-1
 - shift_jis



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.

- unicode
- windows-1252
- none

If you choose **none** or specify a value that the browser on the WebVPN client does not support, it uses its own default encoding.

You can type a string consisting 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.

- CIFS Server—Name or IP address of each CIFS server for which the encoding requirement differs from the “Global WebVPN Encoding Type” attribute setting.

A difference in the encoding of the CIFS server filename and directory indicates that you might need to add an entry for the server to ensure the encoding is correct.

- Encoding Type—Displays the character encoding override for the associated CIFS server.
- Add—Click once for each CIFS server for which you want to override the “Global WebVPN Encoding Type” setting.
- Edit—Select a CIFS server in the table and click this button to change its character encoding.
- Delete—Select a CIFS server in the table and click this button to delete the associated entry from the table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Encoding

This dialog window lets you maintain exceptions to the “Global WebVPN Encoding Type” attribute setting in the Configuration > VPN > WebVPN > Encoding window. That window contains the Add and Edit buttons that open this dialog box.

Fields

- CIFS Server—Enter the name or IP address of a CIFS server for which the encoding requirement differs from the “Global WebVPN Encoding Type” attribute setting. The security appliance retains the case you specify, although it ignores the case when matching the name to a server.
- Encoding Type —Choose the character encoding that the CIFS server should provide for WebVPN portal pages. You can type the string, or select one from the drop-down list, which contains only the most common values, as follows:
 - big5
 - gb2312
 - ibm-850
 - iso-8859-1

- shift_jis



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.

- unicode
- windows-1252
- none

If you choose **none** or specify a value that the browser on the WebVPN client does not support, it uses its own default encoding.

You can type a string consisting 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.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Port Forwarding

Port forwarding lets users access TCP-based applications over a WebVPN connection. Such applications include the following:

Lotus Notes	Secure FTP (FTP over SSH)
Outlook Express	SSH
Outlook	Telnet
Perforce	Windows Terminal Service
Sametime	XDDTS

Other TCP-based applications may also work, but we have not tested them. Protocols that use UDP do not work.



Note

Port forwarding supports only those TCP applications that use static TCP ports. Applications that use dynamic ports or multiple TCP ports are not supported. For example, SecureFTP, which uses port 22, works over WebVPN port forwarding, but standard FTP, which uses ports 20 and 21, does not.

Port forwarding does not support connections to personal digital assistants.

Port Forwarding and JRE

Because port forwarding requires downloading the Java applet and configuring the local client, and because doing so requires administrator permissions on the local system, it is unlikely that users will be able to use applications when they connect from public remote systems.



Caution

Make sure Sun Microsystems Java™ Runtime Environment (JRE) 1.5.x is installed on the remote computers to support port forwarding (application access) and digital certificates. If JRE 1.4.x is running and the user authenticates with a digital certificate, the application fails to start because JRE cannot access the web browser's certificate store.

The Java applet displays in its own window on the end user HTML interface. It shows the contents of the list of forwarded ports available to the user, as well as which ports are active, and amount of traffic in bytes sent and received.

Port Forwarding and User Authentication Via Digital Certificates Incompatibility

Neither port forwarding nor the ASDM JAVA applet work with user authentication using digital certificates. JAVA does not have the ability to access the web browser keystore. Therefore JAVA cannot use certificates that the browser uses to authenticate users, and the application cannot start.

Fields

- Configure port forwarding lists for application access over WebVPN group—To configure application access, create one or more named lists of applications, and then assign a list, by name, to a user (Configuration > Properties > Device Administration > User Accounts > Add/Edit User Account / WebVPN tab) or a group policy (Configuration > VPN > General > Add/Edit Group Policy > WebVPN tab). You can associate a user or group policy with one list only.
 - List Name—Displays the names of application lists configured for WebVPN.
 - Local TCP Port—Displays the local port that listens for traffic for the application.
 - Remote Server—Displays the IP address or DNS name of the remote server.
 - Remote TCP Port—Displays the remote port that listens for traffic for the application.
 - Description—Displays text that describes the TCP application.
- Add/Edit—Click to add or modify a port forwarding list.
- Delete—Click to remove an existing port forwarding list. There is no confirmation or undo.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

For More Information

[WebVPN End User Set-up](#)

Add/Edit Port Forwarding List

The Add/Edit Port Forwarding List panels let you add or edit a named list of TCP applications to associate with users or group policies for access over WebVPN connections.

Fields

- List Name—Enter an alpha-numeric name for the list. Maximum 64 characters.
 - Local TCP Port—Displays the local port that listens for traffic for the application.
 - Remote Server—Displays the IP address or DNS name of the remote server.
 - Remote TCP Port—Displays the remote port that listens for traffic for the application.
 - Description—Displays text that describes the TCP application.
- Add/Edit—Click to add or modify a port forwarding list.
- Delete—Click to remove an existing port forwarding list. There is no confirmation or undo.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Port Forwarding Entry

The Add/Edit Port Forwarding Entry panels let you configure specific applications for a named port forwarding list.

Fields

- Local TCP Port—Type a port number for the application to use. You can use a local port number only once for a listname. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.
- Remote Server—Type either the DNS name or IP address of the remote server. We recommend using hostnames so that you do not have to configure the client applications for specific IP addresses.
- Remote TCP Port—Type the well-know port number for the application.
- Description—Type a description of the application. Maximum 64 characters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Proxies

The security appliance can terminate HTTPS connections and forward HTTP/HTTPS requests to HTTP and HTTPS proxy servers. These servers act as an intermediary between users and the Internet. Requiring all Internet access via a server you control provides another opportunity for filtering to assure secure Internet access and administrative control.

Be aware that HTTP/HTTPS proxy does not support connections to personal digital assistants.

Fields

- HTTP—Lets you define an HTTP proxy server.
 - IP Address—Enter the IP address of the HTTP proxy server.
 - Port—Enter the port that listens for HTTP requests. The default port is 80.
- HTTPS—Lets you define an HTTPS proxy server.
 - IP Address—Enter the IP address of the HTTPS proxy server.
 - Port—Enter the port that listens for HTTPS requests. The default port is 443.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Proxy Bypass

You can configure the security appliance to use proxy bypass when applications and web resources work better with the special content rewriting this feature provides. Proxy bypass is an alternative method of content rewriting that makes minimal changes to the original content. It is often useful with custom web applications.

You can configure multiple proxy bypass entries. The order in which you configure them is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

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. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is the text in a URL that follows the domain name. For example, in the URL `www.mycompany.com/hrbenefits`, *hrbenefits* is the path. Similarly, for the URL `www.mycompany.com/hrinsurance`, *hrinsurance* 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 * wildcard as follows: `/hr*`.

Fields

- Interface—Displays the VLAN configured for proxy bypass.
- Port—Displays the port configured for proxy bypass.
- Path Mask—Displays the URI path to match for proxy bypass.
- URL—Displays the target URLs.
- Rewrite—Displays the rewrite options. These are a combination of XML, link, or none.
- Add/Edit—Click to add a proxy bypass entry or edit a selected entry.
- Delete—Click to delete a proxy bypass entry.

.Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Proxy Bypass Rule

This panel lets you set rules for when the security appliance performs little or no content rewriting.

Fields

- Interface Name—Select the VLAN for proxy bypass.
- Bypass Condition—Specify either a port or a URI for proxy bypass.
 - Port—Select to use a port for proxy bypass. Valid port numbers are 20000-21000.
 - Port (unlabeled)—Enter a high-numbered port for the security appliance to reserve for proxy bypass.
 - Path Mask—Select to use a URL for proxy bypass.
 - Path Mask—Enter a URL for proxy bypass. It can contain a regular expression.
- URL—Define target URLs for proxy bypass.
 - Protocol—Select either http or https as the protocol.
 - URL (unlabeled)—Enter a URL to which you want to apply proxy bypass.
- Content to Rewrite—Specifies the content to rewrite. The choices are none or a combination of XML, links, and cookies.
 - XML—Check to rewrite XML content.
 - Hostname—Check to rewrite links.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

SSL VPN Client

This window lets you enable the security appliance to download SVC image files to remote computers. The SVC Image Files pane displays files existing in flash memory identified as SVC images. The order of the files in this pane indicates the order in which they are downloaded to the remote computer.

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 screen. 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 user screen 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.

The security appliance might have several unique SVC images residing in cache memory for different remote computer operating systems. When the user attempts to connect, the security appliance can consecutively download portions of these images to the remote computer until the image and operating system match, at which point it downloads the entire SVC. You can order the SVC images to minimize connection setup time, with the first image downloaded representing the most commonly-encountered remote computer operating system.

Fields

- **Enable**—Enables the security appliance to download SVC image files to remote computers.
- **Add**—Displays the Add SSL VPN Client Image window, where you can specify a file in flash memory as an SVC image file, or where you can browse flash memory for a file to specify as an SVC image. You can also upload a file from a local computer to the flash memory.
- **Replace**—Displays the Replace SSL VPN Client Image window, where you can specify a file in flash memory as an SVC image to replace an SVC image highlighted in the SVC Image Files table. You can also upload a file from a local computer to the flash memory.
- **Delete**—Deletes an SVC image that you highlight in the SVC Image Files pane.
- **Move Up and Move Down**—changes the order in which the security appliance downloads the SVC images to the remote computer. It downloads the SVC image at the top of the SVC Image Files pane first. Therefore, you should move the SVC image used by the most commonly-encountered operating system to the top of the pane.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

For More Information

[WebVPN End User Set-up](#)

Add SSL VPN Client Image

In this window, you can specify a filename for a file on the security appliance flash memory that you want to identify as an SSL VPN Client (SVC) image. You can also browse the flash memory for a file to identify, or you can upload a file from a local computer to the flash memory.

Fields

- Flash SVC Image—Specify the filename of the file in flash memory that you want to identify as an SSL VPN Client (SVC) image.
- Browse Flash—Displays the Browse Flash Dialog window where you can view all the files on flash memory.
- Upload—Displays the Upload Image window where you can upload a file from a local PC that you want to identify as an SVC image.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add SSL VPN Client Browse Flash Dialog

In this window, you can browse the flash memory of the security appliance for a file that you want to identify as an SSL VPN Client (SVC) image. You can also browse the flash memory for a file to identify, or you can upload a file from a local computer to the flash memory.

Fields

- Flash SVC Image—Identifies the filename of the file in flash memory that you want to identify as an SSL VPN Client (SVC) image.

- Browse Flash—Displays the Browse Flash Dialog window where you can view all the files on flash memory.
- Upload—Displays the Upload Image window where you can upload a file from a local PC that you want to identify as an SVC image.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add SSL VPN Client Upload Flash Dialog

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

Fields

- Local File Path—Identifies the filename of the file in on the local computer that you want to identify as an SSL VPN Client (SVC) image.
- Browse Local—Displays the Select File Path window where you can view all the files on local computer and where you can select a file to identify as an SVC image.
- Flash File System Path—Identifies the filename of the file in the flash memory of the security appliance that you want to identify as an SSL VPN Client (SVC) image.
- Browse Flash—Displays the Browse Flash Dialog window where you can view all the files on flash memory of the security appliance and where you can select a file to identify as an SVC image.

Replace SSL VPN Client Image

In this window, you can specify a filename for a file on the security appliance flash memory that you want to identify as an SSL VPN Client (SVC) image to replace a file previously identified as an SVC image. You can also browse the flash memory for a file to identify, or you can upload a file from a local computer to the flash memory.

Fields

- Flash SVC Image—Specify the filename of the file in flash memory that you want to identify as an SSL VPN Client (SVC) image.
- Browse Flash—Displays the Browse Flash Dialog window where you can view all the files on flash memory.
- Upload—Displays the Upload Image window where you can upload a file from a local PC that you want to identify as an SVC image.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Replace SSL VPN Client Upload Flash Dialog

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

Fields

- **Local File Path**—Identifies the filename of the file in on the local computer that you want to identify as an SSL VPN Client (SVC) image.
- **Browse Local**—Displays the Select File Path window where you can view all the files on local computer and where you can select a file to identify as an SVC image.
- **Flash File System Path**—Identifies the filename of the file in the flash memory of the security appliance that you want to identify as an SSL VPN Client (SVC) image.
- **Browse Flash**—Displays the Browse Flash Dialog window where you can view all the files on flash memory of the security appliance and where you can select a file to identify as an SVC image.

SSO Servers

The SSO Server window lets you configure or delete single sign-on (SSO) for WebVPN users using Computer Associates' SiteMinder SSO server. SSO support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once.

You can choose from three methods when configuring SSO: Auto Signon using basic HTTP and/or NTLMv1 authentication, HTTP Form protocol, or Computer Associates eTrust SiteMinder (formerly Netegrity SiteMinder). This section describes the procedure for setting up SSO with SiteMinder.

- To configure SSO with basic HTTP or NTLM authentication, see [Auto Signon](#).
- To configure SSO with the HTTP Form protocol, see [AAA Setup](#).

The SSO mechanism either starts as part of the AAA process (HTTP Forms) or just after successful user authentication to a AAA server (SiteMinder). In both cases, the WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. This cookie is kept on the security appliance on behalf of the user and used to authenticate the user to secure websites within the domain protected by the SSO server.

SSO authentication with SiteMinder is separate from AAA and occurs after the AAA process completes. To set up SSO for a user or group, you must first configure a AAA server (RADIUS, LDAP and so forth). After a user authenticates to the AAA server, the WebVPN server uses HTTPS to send an authentication request to the SiteMinder SSO server.

Besides configuring the security appliance, you must also configure your CA SiteMinder Policy Server with the Cisco authentication scheme. See [Adding the Cisco Authentication Scheme to SiteMinder](#).

Fields

- **Server Name**—*Display only*. Displays the names of configured SSO Servers. The minimum number of characters is 4, and the maximum is 31.
- **Authentication Type**—*Display only*. Displays the type of SSO server. The security appliance currently supports the SiteMinder type.
- **URL**—*Display only*. Displays the SSO server URL to which the security appliance makes SSO authentication requests.
- **Secret Key**—*Display only*. Displays the secret key used to encrypt authentication communications with the SSO server. The key can be comprised of any regular or shifted alphanumeric character. There is no minimum or maximum number of characters.
- **Maximum Retries**—*Display only*. Displays the number of times the security appliance retries a failed SSO authentication attempt. The range is 1 to 5 retries, and the default number of retries is 3.
- **Request Timeout (seconds)**—*Display only*. Displays the number of seconds before a failed SSO authentication attempt times out. The range is 1 to 30 seconds, and the default number of seconds is 5.
- **Add/Edit**—Opens the Add/Edit SSO Server dialog box.
- **Delete**—Deletes the selected SSO server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Adding the Cisco Authentication Scheme to SiteMinder

Besides configuring the security appliance for SSO with SiteMinder, you must also configure your CA SiteMinder Policy Server with the Cisco authentication scheme, provided as a Java plug-in.



Note

- Configuring the SiteMinder Policy Server requires experience with SiteMinder.
- This section presents general tasks, not a complete procedure.
- Refer to the CA SiteMinder documentation for the complete procedure for adding a custom authentication scheme.

To configure the Cisco authentication scheme on your SiteMinder Policy Server, perform the following tasks:

-
- Step 1** With the Siteminder Administration utility, create a custom authentication scheme being sure to use the following specific arguments:
- In the Library field, enter **smjavaapi**.
 - In the Secret field, enter the same secret configured in the Secret Key field of the Add SSO Server dialog to follow.
 - In the Parameter field, enter **CiscoAuthAPI**.
- Step 2** Using your Cisco.com login, download the file **cisco_vpn_auth.jar** from <http://www.cisco.com/cgi-bin/tablebuild.pl/asa> and copy it to the default library directory for the SiteMinder server.

Add/Edit SSO Server



Note

This SSO method uses CA SiteMinder. You can also set up SSO using the HTTP Form protocol, or Basic HTML and NTLM authentication. To use the HTTP Form protocol, see [AAA Setup](#). To set use basic HTML or NTLM authentication, use the **auto-signon** command at the command line interface.

Fields

- **Server Name**—If adding a server, enter the name of the new SSO server. If editing a server, this field is display only; it displays the name of the selected SSO server.
- **Authentication Type**—*Display only*. Displays the type of SSO server. The type currently supported by the security appliance is SiteMinder.
- **URL**—Enter the SSO server URL to which the security appliance makes SSO authentication requests.
- **Secret Key**—Enter a secret key used to encrypt authentication requests to the SSO server. Key characters can be any regular or shifted alphanumeric characters. There is no minimum or maximum number of characters. The secret key is similar to a password: you create it, save it, and configure it. It is configured on both the security appliance and the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.
- **Maximum Retries**—Enter the number of times the security appliance retries a failed SSO authentication attempt before the authentication times-out. The range is from 1 to 5 retries inclusive, and the default is 3 retries.
- **Request Timeout**—Enter the number of seconds before a failed SSO authentication attempt times out. The range is from 1 to 30 seconds inclusive, and the default is 5 seconds.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Servers and URLs

The Servers and URLs lets you view, add, and populate lists servers and URLs for access over WebVPN.



Note

File access requires that you configure a NetBIOS server (Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN > NetBIOS Servers).

Fields

Configure lists of servers and URLs for access over WebVPN—To configure file and URL access, create one or more named lists of file servers and URLs, and then assign the listname to individual users (Configuration > Properties > Device Administration > User Accounts > Add/Edit User Account / WebVPN tab > Other) or a group policy (Configuration > VPN > General > Add/Edit Group Policy > WebVPN tab > Other). You can associate a user or group policy with only one list.

- List Name—Names of server and URL lists configured for WebVPN.
- URL Display Name—Names end users see for the individual servers and URLs in the list.
- URL—URLs or paths to servers in the list.
- Add—Click to add a list of servers and URLs.
- Edit—Select a list in the Servers and URLs box and click this button to modify it.
- Delete—Select a list in the Servers and URLs box and click this button to remove it. ASDM removes the list without confirming the request.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

WebVPN Access

The WebVPN Access panel lets you accomplish the following tasks:

- Enable or disable security appliance interfaces for WebVPN sessions
- Choose a port for WebVPN connections

- Set a global timeout value for WebVPN sessions
- Set a maximum number of simultaneous WebVPN sessions
- Configure the amount of security appliance memory that WebVPN can use.

To configure WebVPN services for individual users, the best practice is to use the **Configuration > VPN > General > Group Policy > Add/Edit > WebVPN** panel. Then use the **Configuration > Properties > Device Administration > User Accounts > VPN Policy** panel to assign the group policy to a user.

Fields

- Configure access parameters for WebVPN—Lets you enable or disable WebVPN connections on configured security appliance interfaces.
 - Interface—Displays names of all configured interfaces.
 - WebVPN Enabled—Displays current status for WebVPN on the interface.
 - A green check next to Yes indicates that WebVPN is enabled.
 - A red circle next to No indicates that WebVPN is disabled.
 - Enable/Disable—Click to enable or disable WebVPN on the highlighted interface.
- Port Number—Enter the port number that you want to use for WebVPN sessions. The default port is 443, for HTTPS traffic; the range is 1 through 65535. If you change the port number, All current WebVPN connections terminate, and current users must reconnect. You also lose connectivity to ASDM, and a prompt displays, inviting you to reconnect.
- Default Idle Timeout—Enter the amount of time, in seconds, that a WebVPN session can be idle before the security appliance terminates it. 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).

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.

- Max. Sessions Limit—Enter the maximum number of WebVPN sessions you want to allow. Be aware that the different ASA models support WebVPN sessions as follows: ASA 5510 supports a maximum of 150; ASA 5520 maximum is 750; ASA 5540 maximum is 2500.
- WebVPN Memory Size—Enter the percent of total memory or the amount of memory in kilobytes that you want to allocate to WebVPN processes. The default is 50% of memory. Be aware that the different ASA models have different total amounts of memory as follows: ASA 5510—256 MB; ASA5520 —512 MB; ASA 5540—1GB. When you change the memory size, the new setting takes effect only after the system reboots.
- WebVPN Memory (unlabeled)—Choose to allocate memory for WebVPN either as a percentage of total memory or as an amount of memory in kilobytes.
- Enable Tunnel Group Drop-down List on WebVPN Login— Check to include a drop-down list of configured tunnel groups on the WebVPN end-user interface. Users select a tunnel group from this list when they log on. This field is checked by default. If you uncheck it, the user cannot select a tunnel group at logon.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

For More Information

[WebVPN End User Set-up](#)

Webpage Customization

Webpage Customization lets you customize the appearance of the WebVPN page that appears to WebVPN users when they connect to the security appliance. You can also customize pages that display to WebVPN users after the security appliance authenticates them, including the WebVPN Home page and the Application Access page.

Fields

- Customization Objects table—Displays the default WebVPN customization object (DfltCustomization), and any customization objects you add.
- Add—Adds a new customization object and displays the Add Customization Object dialog box where you can further customize.
- Edit—For the highlighted object in the Customization Object table, the Edit button displays the Edit Customization Object dialog box, where you can further customize.
- Delete—Deletes the highlighted object in the Customization Object table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Select Font

The Select Font dialog box lets you specify a font family, style, weight, and size.

Fields

- **Font Family**—Lets you customize the font family.
 - **Do not specify**—Specifies the default.

- **Use selection**—Enables a list of font families that you can select from.
- **Font Style**—Lets you customize the font style.
 - **Do not specify**—Specifies the default.
 - **Use selection**—Enables a list of font styles that you can select from.
- **Font Size**—Lets you customize the font size.
 - **Do not specify**—Specifies the default.
 - **Use selection**—Enables a list of font sizes that you can select from.
- **Font Weight**—Lets you customize the font weight.
 - **Do not specify**—Specifies the default.
 - **Use selection**—Enables a list of font weights that you can select from.
- **Preview**—Displays a preview of your selection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Select Foreground Color

The Select Foreground Color dialog box lets you conveniently select custom colors that comprise a style.

Fields

- **Do not specify**—Specifies to use the default.
- **Use selection**—Enables the Swatches, HSB, and RGB tabs where you can select colors.
 - **Swatches tab**—Lets you conveniently select custom colors. Click on a color block to select a color.
 - **HSB tab**—Lets you select custom colors defined by hue, saturation, and brightness (HSB).
Adjust the Spectrum Bar to the basic color of the light spectrum you desire. Then click and drag the mouse over the color plane until you reach the desired shade. Do this for the hue, saturation, and brightness settings. Alternatively, you can adjust the H, S, and B settings manually by clicking the H, S, and B radio buttons and selecting the up or down arrow.
The R, G, and B fields display a translation to RGB values as you drag the mouse.
 - **RGB tab**—Lets you select custom colors defined by red, green, and blue (RGB).
Adjust the red, green, and blue slide bars to the shade that you desire. Alternatively, you can click the up and down arrows on the RGB values to make the values increase or decrease.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Select Background Color

The Select Background Color dialog box lets you conveniently select custom colors that comprise a style.

Fields

- Do not specify—Specifies to use the default.
- Use selection—Enables the Swatches, HSB, and RGB tabs where you can select colors.
 - Swatches tab—Lets you conveniently select custom colors. Click on a color block to select a color.
 - HSB tab—Lets you select custom colors defined by hue, saturation, and brightness (HSB).

Adjust the Spectrum Bar to the basic color of the light spectrum you desire. Then click and drag the mouse over the color plane until you reach the desired shade. Do this for the hue, saturation, and brightness settings. Alternatively, you can adjust the H, S, and B settings manually by clicking the H, S, and B radio buttons and selecting the up or down arrow.

The R, G, and B fields display a translation to RGB values as you drag the mouse.

- RGB tab—Lets you select custom colors defined by red, green, and blue (RGB).
Adjust the red, green, and blue slide bars to the shade that you desire. Alternatively, you can click the up and down arrows on the RGB values to make the values increase or decrease.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Page Title Tab

The Page Title Tab lets you customize the WebVPN page that appears to WebVPN users when they initially connect to the security appliance, including the page style, the title, and the logo.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- **Page Style**—Define the style with CSS parameters (maximum 256 characters).
 - **Configure**—Lets you configure the font, foreground color, and background color, and appears HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- **Title**—Lets you configure the title of the WebVPN page, including the text and style of the text.
 - **Text**—Enter the text that you want to appear in the title.
 - **Style**—Define the style with CSS parameters (maximum 256 characters).
 - **Configure**—Lets you configure the font, foreground color, and background color, and appears HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- **Titlebar Logo**—Lets you specify your own custom logo that appears on the WebVPN page.
 - **None**—No logo appears on the WebVPN page.
 - **Default**—The Cisco logo appears on the WebVPN page.
 - **Custom**—Enter the filename of a custom logo, or click the Browse Flash button to browse for a file.
 - **Browse Flash**—Browse for a custom file.
 - **Upload Logo**—Displays the Upload Logo dialog box where you can browse for logo files located on the computer running ASDM.
- **Sample Preview**—Displays the upload logo using your current title and logo settings.
 - **Preview in Browser**—Displays your current settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Page Title Tab > Upload Logo

The Upload Logo panel lets you locate a logo file on the computer you are using to run ASDM, and to upload that logo to the security appliance.

Fields

- Local File Path—Displays the path to the logo that you define using the **Browse Local** button.
- Browse Local—Click to browse the file structure of the computer you are using to run ASDM and locate the logo.
- Flash File System Path—Displays the path to the logo that you define using the **Browse Flash** button.
- Browse Flash—Click to browse the file structure of Flash memory on the security appliance to decide where you want to locate the logo.
- Upload File—Click to display the Browse Flash dialog box. The name of the logo file you have selected appears in the File Name box. Click OK to set this path to flash memory.

You return to the **Upload Logo** panel. Click the **Upload** button to upload the new logo file to Flash memory. This logo now appears in the **Preview** box.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Login Page Tab > Login Box Tab

The Login Box tab lets you customize the Login box of the WebVPN page that appears to WebVPN users when they initially connect to the security appliance, including the title and the message.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- Login Title—Lets you specify the text to appear in the Login box title and the style of the login title.
 - Text—Enter the text that you want to appear in the Title of the Login Box.
 - Style—Define the style with CSS parameters (maximum 256 characters).

- Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Login Message—Lets you specify the message that appears in the Login box, and the style of that message.
 - Text—Enter the text that you want to appear as the message in the Login box.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Sample Preview—Displays the Login Title and Login Message using your settings.
 - Preview in Browser—Displays the Login Title and Login Message using your current settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Login Page Tab > Login Prompts Tab

The Login Prompts tab lets you customize the login prompts of the WebVPN page that appears to WebVPN users when they initially connect to the security appliance, including the username, password, and group prompts.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- Username Prompt—Lets you customize the username prompt, including the text that appears and the style of that text.
 - Text—Enter the text to display for the username prompt.

- Style—Define the style with CSS parameters (maximum 256 characters).
- Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Password Prompt—Lets you customize the password prompt, including the text that appears and the style of that text.
 - Text—Enter the text to display for the password prompt.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Group Prompt—Lets you customize the group prompt, including the text that appears and the style of that text.
 - Text—Enter the text to display for the group prompt.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure button—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Sample Preview—Displays the Login box using your current username, password, and group prompt settings.
- Preview in Browser—Displays the Login box using your current username, password, and group prompt settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Login Page Tab > Login Buttons Tab

The Login Buttons tab lets you customize the Login and Clear buttons of the WebVPN page that appears to WebVPN users when they initially connect to the security appliance.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- **Login Button—Lets you customize the Login button, including the text that appears on the button and the style of the button.**
 - Text—Enter the text to display on the Login button.
 - Style—Define the style of the Login button with CSS parameters (maximum 256 characters).
 - Configure button—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- **Clear—Lets you customize the Clear button, including the text that appears on the button and the style of the button.**
 - Text—Enter the text to display on the Clear button.
 - Style—Define the style of the Login button with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- **Sample Preview—Displays the Login and clear buttons using your current settings.**
 - Preview in Browser—Displays the Login and Clear buttons using your current settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Logout Page Tab

The Logout Page tab lets you customize the Logout page that appears to WebVPN users when they Log out of WebVPN service.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- Logout Title—Lets you specify the text to appear in the Logout box title and the style of the logout title.
 - Text—Enter the text that you want to appear as the message in the Logout page.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Logout Message—Lets you specify the message to appear on the Logout page.
 - Text—Enter the text that you want to appear as the message in the Logout page.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Sample Preview—Displays the Logout page using your settings.
 - Preview in Browser—Displays the page using your current settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Home Page Tab > Border Color Tab

The Border Color tab lets you customize the border of the WebVPN Home page that appears to WebVPN users after they are authenticated by the security appliance.

Fields

- Border Style—Use any Cascading Style Sheet (CSS) parameters to define the style, including font styles, and HTML and RGB colors. To easily change the style, use the **Configure** button.
 You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
 RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
 HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- **Configure**—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- **Sample Preview**—Displays the WebVPN Home page using your border settings.
 - **Preview in Browser**—Displays the WebVPN Home page using your border settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Home Page Tab > Web Applications Tab

The Web Applications tab lets you customize the Web Applications box of the WebVPN Home page that appears to authenticated WebVPN users.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- **Title**—Lets you customize the title of the Web Applications box.
 - **Text**—Enter the text that you want to appear as the title.
 - **Style**—Define the style with CSS parameters (maximum 256 characters).
 - **Configure**—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- **Message**—Lets you customize the message (under the title) of the Web Applications box,

- Text—Enter the text that you want to appear as the message.
- Style—Define the style with CSS parameters (maximum 256 characters).
- Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Dropdown—Lets you customize the drop-down list of the Web Applications box.
 - Text—Enter the text that you want to appear in the drop-down list.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Sample Preview—Displays the WebVPN Home page using your Web Application settings.
 - Preview in Browser—Displays the WebVPN Home page using your Web Application in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Home Page Tab > Application Access Tab

The Applications Access tab lets you customize the Applications Access box of the WebVPN Home page that appears to authenticated WebVPN users.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- Title—Lets you customize the title of the Applications Access box.
 - Text—Enter the text that you want to appear as the title.

- Style—Define the style with CSS parameters (maximum 256 characters).
- Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Message—Lets you customize the message under the title of the Applications Access box
 - Text—Enter the text that you want to appear as the message.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Sample Preview—Displays the WebVPN Home page using your Application Access settings.
 - Preview in Browser—Displays the WebVPN Home page using your Application Access settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Home Page Tab > Browse Network Tab

The Browse Networks tab lets you customize the Browse Networks box of the WebVPN Home page that appears to authenticated WebVPN users.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- Title—Lets you customize the title of the Browse Networks box.
 - Text—Enter the text that you want to appear as the title.
 - Style—Define the style with CSS parameters (maximum 256 characters).

- Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Message—Lets you customize the message under the title of the Browse Networks box
 - Text—Enter the text that you want to appear as the message.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Dropdown—Lets you customize the drop-down list of the Browse Networks box.
 - Text—Enter the text that you want to appear in the drop-down list.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Sample Preview—Displays the WebVPN Home page using your Browse Networks settings.
 - Preview in Browser—Displays the WebVPN Home page using your Browse Networks settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Home Page Tab > Web Bookmarks Tab

The Web Bookmarks tab lets you customize the Web Bookmarks title and the appearance of the bookmarks links on the WebVPN Home page that appears to authenticated WebVPN users.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- **Bookmark Title—Lets you customize the title.**
 - Text—Enter the text that you want to appear as the title.
 - Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- **Bookmark Links Style—Define the style with CSS parameters (maximum 256 characters).**
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools
- **Sample Preview—Displays the WebVPN Home page using your Web Bookmarks settings.**
 - Preview in Browser—Displays the WebVPN Home page using your Web Bookmarks settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Home Page Tab > File Bookmarks Tab

The File Bookmarks tab lets you customize the File Bookmarks title and the appearance of the bookmarks links on the WebVPN Home page that appears to authenticated WebVPN users.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- **Bookmark Title—Lets you customize the title.**
 - **Text**—Enter the text that you want to appear as the title.
 - **Style**—Define the style with CSS parameters (maximum 256 characters).
 - **Configure**—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- **Bookmark Links Style**—Define the style with CSS parameters (maximum 256 characters).
 - **Configure**—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools
- **Sample Preview**—Displays the WebVPN Home page using your File Bookmarks settings.
 - **Preview in Browser**—Displays the WebVPN Home page using your File Bookmarks settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Application Access Window Tab

The Application Access Window tab lets you customize the Application Access window that appears to authenticated WebVPN users that select Application Access on the WebVPN Home page.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- **Window Style**—Define the style with CSS parameters (maximum 256 characters).
 - **Configure**—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.

- Warning Message—Enter the text that you want to appear as the warning message.
- Show application details in the application access window—Lets you disable the display of application details that appear on the Application Access Window.
- Sample Preview—Displays the Application Access Window using your settings.
 - Preview in Browser—Displays the Application Access Window using your settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Prompt Dialog Tab

The Prompt Dialog tab lets you customize the appearance of dialog messages that appear to authenticated WebVPN users.

Fields

This tab contains several Style fields. Use any Cascading Style Sheet (CSS) parameters to define the style. To easily change the font, background color and foreground color, use the Configure button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- Dialog Title Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Dialog Message Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Dialog Border Style—Define the style with CSS parameters (maximum 256 characters).
 - Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.

- Sample Preview—Displays a sample of a dialog message using your settings.
 - Preview in Browser—Displays a sample of a dialog message using your settings in a browser window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Webpage Customization Object > Quick Style Configuration

The Quick Style Configuration dialog box lets you apply a single style to multiple WebVPN window customization settings.

Fields

- Select Fields—**click the fields that you want to share a single style.**
- Specify Style—Lets you specify a custom style to use for the fields you have selected.
 - Use custom style—click disable the default style, and supply the custom style.
 - Style—Define the style of the WebVPN page with Cascading Style Sheet (CSS) parameters (maximum 256 characters), including font styles, and HTML and RGB colors. To easily change the style, use the **Configure** button.

You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

For best results, check published HTML and RGB tables. To find tables online, enter RGB in a search engine. For more information about CSS, visit the World Wide Web Consortium (W3C) website at www.w3.org.

- Configure—Lets you configure the font, foreground color, and background color, and displays HTML color swatches, and HSB (Hue, Saturation, Brightness) and RGB (Red, Green, Blue) selection tools.
- Preview—Displays a sample of the style you selected.
- Use default styles—Enables default styles.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

