



## CHAPTER 38

# Clientless SSL VPN

---

Clientless SSL VPN 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. Clientless SSL VPN 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. Clientless SSL VPN 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 network resources on a user or group basis. Users have no direct access to these resources.

Clientless SSL VPN works on the platform in single, routed mode.

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

## Security Precautions

Clientless SSL VPN connections on the security appliance differ from remote access IPSec connections, particularly with respect to how they interact with SSL-enabled servers, and precautions to follow to reduce security risks.

In a clientless SSL VPN connection, the security appliance acts as a proxy between the end user web browser and target web servers. When a user connects to an SSL-enabled web server, the security appliance establishes a secure connection and validates the server SSL certificate. The browser never receives the presented certificate, so it cannot examine and validate the certificate.



---

**Note** Browser-based VPN access does not save form-based authentication values to permanent local storage.

---

The current implementation of clientless SSL VPN on the security appliance does not permit communication with sites that present expired certificates. Nor does the security appliance perform trusted CA certificate validation to those SSL-enabled sites. Therefore, users do not benefit from certificate validation of pages delivered from an SSL-enabled web server before they use a web-enabled service.

**Caution**

By default, the security appliance permits all portal traffic to all web resources (e.g., HTTPS, CIFS, RDP, and plug-ins). The security appliance clientless service rewrites each URL to one that is meaningful only to itself; the user cannot use the rewritten URL displayed on the page accessed to confirm that they are on the site they requested. To avoid placing users at risk, please assign a web ACL to the policies configured for clientless access – group-policies, dynamic access policies, or both – to control traffic flows from the portal. For example, without such an ACL, users could receive an authentication request from an outside fraudulent banking or commerce site. Also, we recommend disabling URL Entry on these policies to prevent user confusion over what is accessible. We recommend that you do the following to minimize risks posed by clientless SSL VPN access:

- 
- Step 1** Configure a group policy for all users who need clientless SSL VPN access, and enable clientless SSL VPN only for that group policy.
  - Step 2** With the group policy open, choose General > More Options > Web ACL and click **Manage**. Create a web ACL to do one of the following: permit access only to specific targets within the private network, permit access only to the private network, deny Internet access, or permit access only to reputable sites. Assign the web ACL to any policies (group policies, dynamic access policies, or both) that you have configured for clientless access. On a DAP, you select the web ACL on the Network ACL Filters tab.
  - Step 3** Disable URL entry on the *portal page*, the page that opens when they establish a browser-based connection. To do so, click Disable next to URL Entry on both the group policy Portal frame and the DAP Functions tab.
  - Step 4** Instruct users to enter external URLs in the native browser address field above the portal page or open a separate browser window to visit external sites.
- 

## Understanding Clientless SSL VPN System Requirements

Clientless SSL VPN supports access from the following OSs and browsers.

| OSs  | Browser and Java Versions                                    | Feature Notes <sup>1</sup>  |
|--|--|---|
| Windows Vista SP2<br>Vista SP1 with <a href="#">KB952876</a> or later. | Microsoft Internet Explorer 7<br>Firefox 2.0 or later.       | Windows Vista does not support Windows Shares (CIFS) Web Folders.<br>Additional requirements and limitations apply to <a href="#">smart tunnel</a> and <a href="#">port forwarding</a> .  |
| Windows XP SP2 or later.   | Microsoft Internet Explorer 7 and 6<br>Firefox 2.0 or later. | Windows XP SP2 or later requires <a href="#">Microsoft KB892211 hotfix</a> to support Web Folders.<br>Additional requirements and limitations apply to <a href="#">smart tunnel</a> and <a href="#">port forwarding</a> .   |
| Windows 2000 SP4.  | Microsoft Internet Explorer 7 and 6<br>Firefox 2.0 or later. | Windows Vista does not support Windows Shares (CIFS) Web Folders.<br>Windows 2000 SP4 requires <a href="#">Microsoft KB892211 hotfix</a> to support Web Folders.<br>Additional requirements and limitations apply to <a href="#">smart tunnel</a> and <a href="#">port forwarding</a> . |

| OSs                           | Browser and Java Versions                     | Feature Notes <sup>1</sup>  |
|-------------------------------|---|---|
| Apple: Mac OS X 10.4 and 10.5 | Safari 2.0 or later, or Firefox 2.0 or later. | Certificate authentication, including the DoD Common Access Card and SmartCard, works with the Safari keychain only.<br><br>Web folders do not support Mac OS.<br><br>Additional requirements and limitations apply to <a href="#">smart tunnel</a> and <a href="#">port forwarding</a> . |
| Linux                         | Firefox 2.0 or later.                         | Web folders and smart tunnel do not support Linux.<br><br>Additional requirements apply to <a href="#">port forwarding</a> .  |

1. For Microsoft Outlook Exchange communication using the MAPI protocol, remote users must use AnyConnect.

ActiveX pages require that you use the ActiveX Relay default setting (Enable) on the associated group policy. If you do so or assign a smart tunnel list to the policy, and the browser proxy exception list on the endpoint specifies a proxy, the user must add a “shutdown.webvpn.relay.” entry to that list.

Clientless SSL VPN access does not support Windows Shares (CIFS) Web Folders on Windows 7, Vista, Internet Explorer 8, Mac OS, and Linux. Windows XP SP2 requires a [Microsoft hotfix](#) to support Web Folders.

See the following sections for the platforms supported by the clientless applications they name:

- [Port Forwarding Requirements and Restrictions, page 38-21](#)
- [Smart Tunnel Requirements and Limitations, page 38-39](#)
- [Plug-in Requirements and Restrictions, page 38-72](#)

## Configuring 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 ACLs to be used for clientless SSL VPN sessions, and the ACL entries 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 ACLs to be applied to clientless SSL VPN sessions and their ACEs in the sequence determined by 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.
- Enabled—Shows whether the ACE is enabled. When you create an ACE, by default it is enabled. Clear the check box to disable an ACE.
- 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 clientless SSL VPN 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 ACLs for clientless SSL VPN:

| 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.                        |
| 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 |
| •             | —           | •                | —        | —      |

# Configuring the Setup for Cisco Secure Desktop

The Cisco Secure Desktop Setup window displays the version and state of the Cisco Secure Desktop image if it is installed on the security appliance, indicates whether it is enabled, and shows the size of the cache used to hold the Cisco Secure Desktop and SSL VPN Client on the security appliance.

You can use the buttons in this window as follows:

- To transfer a copy of a Cisco Secure Desktop image from your local computer to the flash device of the security appliance click **Upload**.

To prepare to install or upgrade Cisco Secure Desktop, 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 your local computer to the flash device. Click **Browse Flash** to install it into the running configuration. Finally, check **Enable Secure Desktop**.

- To install or replace the Cisco Secure Desktop image on the flash device of the security appliance, click **Browse Flash**.



## Note

If you click the **Browse Flash** button to upgrade or downgrade the Cisco Secure Desktop image, select the package to install, and click **OK**, the Uninstall Cisco Secure Desktop dialog window asks you if you want to delete the Cisco Secure Desktop 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 Cisco Secure Desktop.

- To remove the Cisco Secure Desktop image and configuration file (`sdesktop/data.xml`) from the running configuration, click **Uninstall**.

## Fields

The Cisco Secure Desktop Setup pane displays the following fields:

- Location—Displays the Cisco Secure Desktop image loaded into the running configuration. By default, the filename is in the format `securedesktop_asa_<n>_<n>*.pkg`. Click **Browse Flash** to insert or modify the value in this field.
- Enable Secure Desktop—Check and click **Apply** to do the following:
  - Make sure the file is a valid Cisco Secure Desktop image.
  - Create an “sdesktop” folder on disk0 if one is not already present.
  - Insert a `data.xml` (Cisco Secure Desktop configuration) file into the sdesktop folder if one is not already present.
  - Load the `data.xml` file into the running configuration.



## Note

If you transfer or replace the `data.xml` file, disable and then enable Cisco Secure Desktop to load the file.

- Enable Cisco Secure Desktop.

## 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

The Upload Image dialog box lets you transfer a copy of a Cisco Secure Desktop image from your local computer to the flash device on the security appliance. Use this window to install or upgrade Cisco Secure Desktop.



### 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.

You can use the buttons in this window as follows:

- To select the path of the `securedesktop_asa_<n>_<n>*.pkg` file to be transferred, click **Upload**. 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**.
- To select the target directory for the file, click **Browse Flash**. The Browse Flash dialog box displays the contents of the flash card.
- To upload the `securedesktop_asa_<n>_<n>*.pkg` file from your local computer to the flash device, click **Upload File**. 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.
- To close the Upload Image dialog window, click **Close**. Click this button after you upload the Cisco Secure Desktop image to the flash device or if you decide not to upload it. If you uploaded it, the filename appears in the Location field of the Cisco Secure Desktop 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 Cisco Secure Desktop 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**.

### Fields

The Upload Image dialog box displays the following fields:

- 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
```

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:/securedesktop_asa_3_1_1_16.pkg`
- File Name—Located in the Browse Flash dialog box that opens if you click **Browse Flash**, this field displays the name of the Cisco Secure Desktop image 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.

### Modes

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

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

## Configuring Application Helper

Clientless SSL VPN 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 clientless SSL VPN 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.

Typically, Cisco TAC helps you write and apply an Apcf.

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—Click to rearrange Apcf profiles within a list. The list determines the order in which the security appliance attempts to use Apcf profiles.

### Add/Edit Apcf Profile

This panel lets you add or edit and Apcf 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 APCF file stored on the security appliance flash memory.
- Path—Displays the path to an APCF 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 APCF file. A Browse Flash Dialog panel displays. Use the Folders and Files columns to locate the APCF file. Highlight the APCF 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 APCF file that you recently downloaded, click the Refresh button.

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

- Local File Path—Shows the path to the APCF file on your computer. Click **Browse Local** to automatically insert the path in this field, or enter the path.
- Browse Local Files—Click to locate and choose the APCF 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 APCF 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 APCF file.
- Browse Flash—Click to identify the location on the security appliance to which you want to upload the APCF 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 |
| •             | —           | •                | —        | —      |

## Clock Accuracy for SharePoint Access

The clientless SSL VPN server on the security appliance uses cookies to interact with applications such as Microsoft Word on the endpoint. The cookie expiration time set by the security appliance can cause Word to malfunction when accessing documents on a SharePoint server if the time on the security appliance is incorrect. To prevent this malfunction, set the ASA clock properly. We recommend configuring the security appliance to dynamically synchronize with NTP services. For instructions, see [System Time](#).

## Auto Signon

The Auto Signon window or tab lets you configure or edit auto signon for users of clientless SSL VPN. 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 user of clientless SSL VPN entered to log in 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 consists of authentication using Basic (HTTP), NTLM, FTP and CIFS, or all of these 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, or if you have Security Assertion Markup Language (SAML) Browser Post Profile SSO, and if you want to configure the security appliance to support this solution, see [SSO Servers](#).

**Note**

Do not enable auto signon for servers that do not require authentication or that use credentials different from the security appliance. When auto signon is enabled, the security appliance passes on the login credentials that the user entered to log into the security appliance regardless of what credentials are in user storage.

**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, FTP and CIFS, or all of these methods—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 sign-on.
  - **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 Basic HTTP authentication requests, NTLM authentication requests, FTP and CIFS authentication requests, or requests using any of these methods.
  - **Basic**—Click this button if the servers support basic (HTTP) authentication.
  - **NTLM**—Click this button if the servers support NTLMv1 authentication.
  - **FTP/CIFS**—Click this button if the servers support FTP and CIFS authentication
  - **Basic, NTLM, and FTP/CIFS**—Click this button if the servers support all of the above.

**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 user 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 |
| •             | —           | •                | —        | —      |

## Configuring Session Settings

The Clientless SSL VPN Add/Edit Internal Group Policy > More Options > Session Settings window lets you specify personalized user information between clientless SSL VPN sessions. By default, each group policy inherits the settings from the default group policy. Use this window to specify personalized clientless SSL VPN user information for the default group policy and any group policies for which you want to differentiate these values.

**Fields**

- **User Storage Location**—Choose none or choose the file server protocol (smb or ftp) from the drop-down menu. If you choose smb or ftp, use the following syntax to enter the file system destination into the adjacent text field:

*username:password@host:port-number/path*

For example

**mike:mysecret@ftpserver3:2323/public**

**Note**

Although the configuration shows the username, password, and preshared key, the security appliance uses an internal algorithm to store the data in an encrypted form to safeguard it.

- **Storage Key**—Type the string, if required, for the security appliance to pass to provide user access to the storage location.

- **Storage Objects**—Select one of the following options from the drop-down menu to specify the objects the server uses in association with the user. The security appliance store these objects to support clientless SSL VPN connections.
  - cookies,credentials
  - cookies
  - credentials
- **Transaction Size**—Enter the limit in KB over which to time out the session. This attribute applies only to a single transaction. Only a transaction larger than this value resets the session expiration clock.

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

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

## Java Code Signer

Code signing appends a digital signature to the executable code itself. This digital signature provides enough information to authenticate the signer as well as to ensure that the code has not been subsequently modified since signed.

Code-signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.

To select a Java Code Signer, use the drop down list.

To configure a Java Code Signer, go to Configuration > Remote Access VPN > Certificate Management > Java Code Signer.

## Content Cache

Caching enhances the performance of clientless SSL VPN. It stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. The use of the cache reduces traffic, with the result that many applications run more efficiently.

### Fields

- **Enable cache**—Check to enable caching. The default value is disable.
- **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.

- **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.
- **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.

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.

- **Cache static content**—Click to cache all content that is not subject to rewrite, for example, PDF files and images.
- **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 pane lists all applications for which content rewrite is enabled or disabled.

Clientless SSL VPN 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.

By default, the security appliance rewrites, or transforms, all clientless traffic. 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.

“[Example Content Rewrite Rules](#)” shows example content rewrite rules.

**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—Click to enable content rewrite for this rewrite rule.
- Rule Number—(Optional) Enter a number for this rule. This number specifies the priority of the rule, relative to the others 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 a string to match the application or resource to apply the rule to. The string can be up to 300 characters. You can use one of the following wildcards, but you must specify at least one alphanumeric character.
  - \* — Matches everything. ASDM does not accept a mask that consists of a \* or \*.\*
  - ? —Matches any single character.
  - [!seq] — Matches any character not in sequence.
  - [seq] — Matches any character in sequence.

**Example Content Rewrite Rules**

| Function   | Enable content rewrite | Rule Number | Rule Name              | Resource Mask |
|--|------------------------|-------------|------------------------|---------------|
| Force all HTTP URLs to be delivered outside of ASA (split-tunneling) | Check                  | 1           | split-tunnel-all-http  | http://*      |
| Force all HTTPS URLs to be delivered outside of ASA                  | Check                  | 2           | split-tunnel-all-https | https://*     |

**Modes**

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

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

# Java Code Signer

Java objects which have been transformed by clientless SSL VPN can subsequently be signed using a PKCS12 digital certificate associated with a trustpoint. In the Java Trustpoint pane, you can configure the clientless SSL VPN 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**

- Code Signer Certificate —Choose the configured certificate 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 view or specify the character encoding for clientless SSL VPN portal pages.

*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 a single method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the remote user can change it. 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 used on the portal page to ensure that the browser renders it properly, regardless of the region in which the user is using the browser, and regardless of any changes made to the browser.

By default, the security appliance applies the “Global Encoding Type” to pages from Common Internet File System servers. The mapping of CIFS servers to their appropriate character encoding, globally with the “Global 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, is an issue.

### Fields

- **Global Encoding Type**—This attribute determines the character encoding that all clientless SSL VPN portal pages inherit except for those from the CIFS servers listed in the table. You can type the string or select one of the options in the drop-down list, which contains 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 clientless SSL VPN session 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 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 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

The Add CIFS Server Encoding dialog window lets you maintain exceptions to the “Global Encoding Type” attribute setting in the Add CIFS 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 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 clientless SSL VPN 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 clientless SSL VPN session 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 |
| •             | —           | •                | —        | —      |

## Web ACLs

The Web ACLs table displays the filters configured on the security appliance applicable to clientless SSL VPN traffic. The table shows the name of each access control list (ACL), and below and indented to the right of the ACL name, the access control entries (ACEs) assigned to the ACL.

Each ACL permits or denies access permits or denies access to specific networks, subnets, hosts, and web servers. Each ACE specifies one rule that serves the function of the ACL.

You can configure ACLs to apply to clientless SSL VPN traffic. The following rules apply:

- If you do not configure any filters, all connections are permitted.
- The security appliance supports only an inbound ACL on an interface.
- At the end of each ACL, an implicit, unwritten rule denies all traffic that is not explicitly permitted.

You can use the following wildcard characters to define more than one wildcard in the Webtype access list entry:

- Enter an asterisk “\*” to match no characters or any number of characters.
- Enter a question mark “?” to match any one character exactly.
- Enter square brackets “[ ]” to create a range operator that matches any one character in a range.

The following examples show how to use wildcards in Webtype access lists.

- The following example matches URLs such as `http://www.cisco.com/` and `http://wwz.caco.com/`:  

```
access-list test webtype permit url http://ww?.c*co*/
```

- The following example matches URLs such as `http://www.cisco.com` and `ftp://wwz.carrier.com`:  

```
access-list test webtype permit url *://ww?.c*co*/
```

- The following example matches URLs such as `http://www.cisco.com:80` and `https://www.cisco.com:81`:

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

The range operator “[ ]” in the preceding example specifies that either character **0** or **1** can occur.

- The following example matches URLs such as `http://www.google.com` and `http://www.boogie.com`:  

```
access-list test webtype permit url http://www.[a-zloo?*/
```

The range operator “[ ]” in the preceding example specifies that any character in the range from **a** to **z** can occur.

- The following example matches URLs such as `http://www.cisco.com/anything/crazy/url/ddtscgiz`:  

```
access-list test webtype permit url htt*://*/cgi?*
```

- The following example permit a range of IP addresses from 10.2.2.20 through 10.2.2.31:  

```
10.2.2.[20-31]
```

The range operator “[ ]” in the preceding example specifies that any address in the range from 20 to 31 can occur.



### Note

To match any http URL, you must enter `http://*/*` instead of the former method of entering `http://*`.

You can add ACLs and ACEs as follows:

- To add an ACL, click the down arrow next to the plus sign above the table and click **Add ACL**.



**Note** An ACL must be present before you can add an ACE.

- To add an ACE to an ACL that is already present in the table, select it, then click the down arrow next to the plus sign above the table and click **Add ACE**.
- To insert an ACE before an ACE that is already present in the table, select it, then click the down arrow next to the plus sign above the table and click **Insert**.
- To insert an ACE after an ACE that is already present in the table, select it, then click the down arrow next to the plus sign above the table and click **Insert After**.

To change the values assigned to an ACE, double-click it, or select it and click **Edit**.

To remove an ACL or an ACE, select the entry in the table and click **Delete**.

The relative position of an ACE in an ACL determines the sequence with which the security appliance applies it to traffic on the interface. You can reorganize and reuse the ACEs present in the table as follows.

- To move an ACE above or below another ACE, select it and click the up or down icon above the table.
- To move an ACE, select the ACE, click the scissors icon above the table. Select the target ACL or ACE, click the arrow next to the clipboard icon, and click **Paste** to paste above the selection or **Paste After** to paste after the selection. The Edit ACE window opens, providing you with an opportunity to change the values. Click **OK**.
- To copy an ACE, select it and click the double-page icon above the table. Select the target ACL or ACE, click the arrow next to the clipboard icon, and click **Paste** to paste above the selection or **Paste After** to paste after the selection. The Edit ACE window opens, providing you with an opportunity to change the values. Click **OK**.

### 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

Both the Port Forwarding pane and Configure Port Forwarding Lists dialog box let you view the port forwarding lists. Both the Port Forwarding pane and the Add or Edit Port Forwarding Entry dialog box let you specify the name of a port forwarding list, and add, view, edit, and delete port forwarding entries to the list.

To add, change, or remove a port forwarding list, do one of the following:

- To add a port forwarding list and add entries to it, click **Add**. The Add Port Forwarding List dialog box opens. After you name the list, click **Add** again. ASDM opens the Add Port Forwarding Entry dialog box, which lets you assign the attributes of an entry to the list. After doing so and clicking **OK**, ASDM displays those attributes in the list. Repeat as needed to complete the list, then click **OK** in the Add Port Forwarding List dialog box.
- To change a port forwarding list, double-click the list or choose the list in the table and click **Edit**. Then click **Add** to insert a new entry into the list, or click an entry in the list and click **Edit** or **Delete**.
- To remove a list, select the list in the table and click **Delete**.

## Why Port Forwarding?

Port forwarding is the legacy technology for supporting TCP-based applications over a clientless SSL VPN connection. You may choose to use port forwarding because you have built earlier configurations that support this technology.

Please consider the following alternatives to port forwarding:

- Smart tunnel access offers the following advantages to users:
  - Smart tunnel offers better performance than plug-ins.
  - Unlike port forwarding, smart tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
  - Unlike port forwarding, smart tunnel does not require users to have administrator privileges.
- Unlike port forwarding and smart tunnel access, a plug-in does not require the client application to be installed on the remote computer.

When configuring port forwarding on the security appliance, you specify the port the application uses. When configuring smart tunnel access, you specify the name of the executable file or its path.

## Port Forwarding Requirements and Restrictions

The following restrictions apply to port forwarding:

- The remote host must be running a 32-bit version of one of the following:
  - Microsoft Windows Vista, Windows XP SP2 or SP3; or Windows 2000 SP4.
  - Apple Mac OS X 10.4 or 10.5 with Safari 2.0.4(419.3).
  - Fedora Core 4
- The remote host must also be running Sun JRE 1.5 or later.
- Browser-based users of Safari on Mac OS X 10.5.3 must identify a client certificate for use with the URL of the security appliance, once with the trailing slash and once without it, because of the way Safari interprets URLs. For example,
  - <https://example.com/>
  - <https://example.com>

For details, go to the [Safari, Mac OS X 10.5.3: Changes in client certificate authentication](#).

- Users of Microsoft Windows Vista who use port forwarding or smart tunnels must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the **Tools > Internet Options > Security** tab. Vista users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer's vulnerability to attack.
- Port forwarding supports only 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 clientless SSL VPN port forwarding, but standard FTP, which uses ports 20 and 21, does not.
- Port forwarding does not support protocols that use UDP.
- The security appliance does not support the Microsoft Outlook Exchange (MAPI) proxy. For Microsoft Outlook Exchange communication using the MAPI protocol, remote users must use AnyConnect.
- A stateful failover does not retain sessions established using Application Access (either port forwarding or smart tunnel access). Users must reconnect following a failover.
- Port forwarding does not support connections to personal digital assistants.
- 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 or later 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 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.

- 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.
- You must configure DNS for port forwarding, as described in the next section.

## Configuring DNS for Port Forwarding

Port Forwarding forwards the domain name of the remote server or its IP address to the ASA for resolution and connection. In other words, the port forwarding applet accepts a request from the application and forwards it to the ASA. The ASA makes the appropriate DNS queries and establishes the connection on behalf of the port forwarding applet. The port forwarding applet only makes DNS queries to the ASA. It updates the host file so that when a port forwarding application attempts a DNS query, the query redirects to a loopback address.

Configure the security appliance to accept the DNS requests from the port forwarding applet as follows:

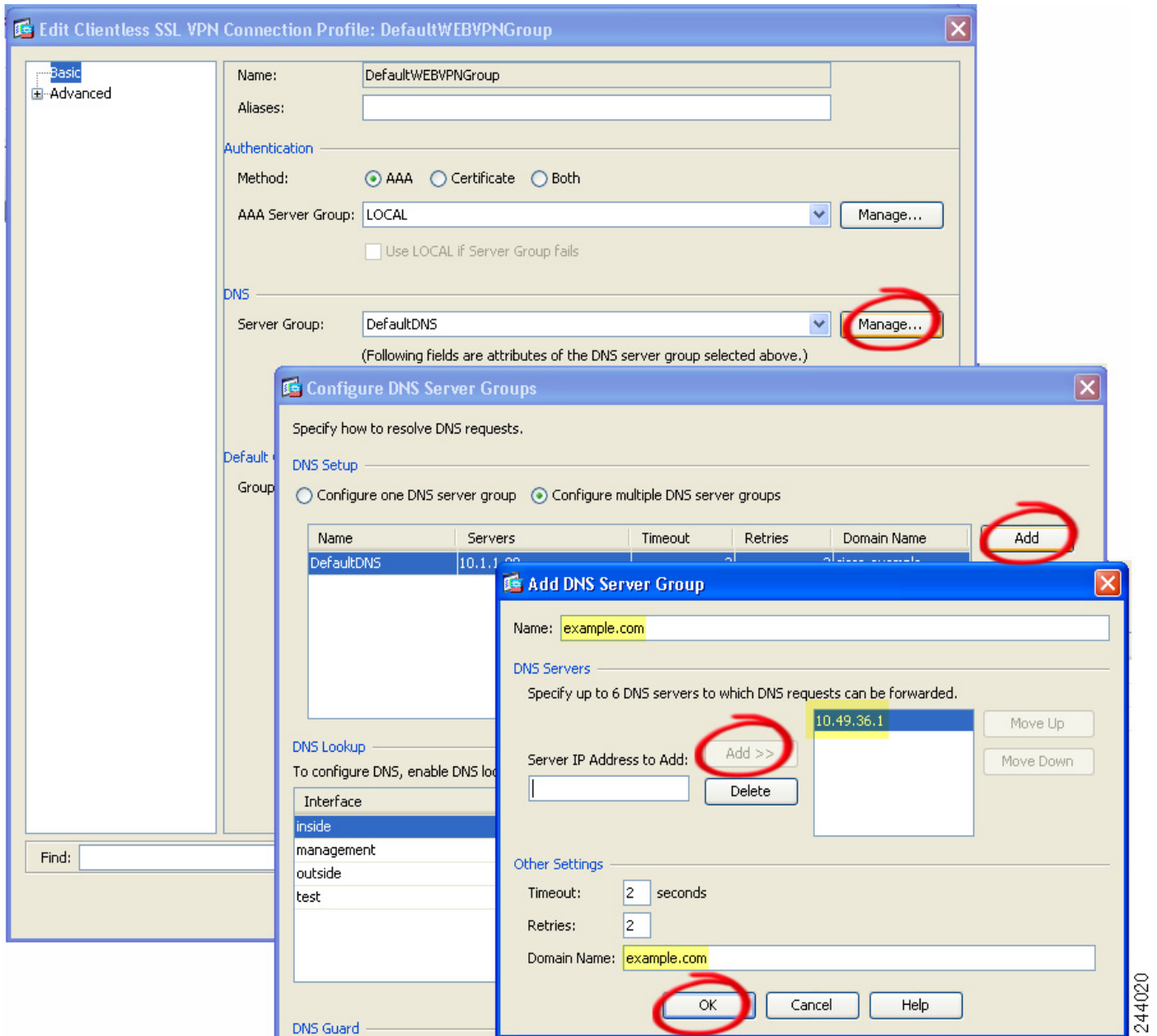
---

**Step 1** Click **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

The DefaultWEBVPNGroup entry is the default connection profile used for clientless connections.

- Step 2** Highlight the DefaultWEBVPNGroup entry, then click **Edit** if your configuration uses it for clientless connections. Otherwise, highlight a connection profile used in your configuration for clientless connections, then click **Edit**.
- The Basic window opens.
- Step 3** Scan to the DNS area and select the DNS server from the drop-down list. Note the domain name, disregard the remaining steps, and go to the next section if ASDM displays the DNS server you want to use. You need to enter the same domain name when you specify the remote server while configuring an entry in the port forwarding list. Continue with the remaining steps if the DNS server is not present in the configuration.
- Step 4** Click **Manage** in the DNS area.
- The Configure DNS Server Groups window opens.
- Step 5** Click **Configure Multiple DNS Server Groups**.
- A window displays a table of DNS server entries.
- Step 6** Click **Add**.
- The Add DNS Server Group window opens.
- Step 7** Enter a new server group name in the Name field, and enter the IP address and domain name (see [Figure 38-1](#))

Figure 38-1 Example DNS Server Values for Port Forwarding



Note the domain name you entered. You need it when you specify the remote server later while configuring a port forwarding entry.

- Step 8** Click **OK** until the Connection Profiles window becomes active again.
- Step 9** Repeat Steps 2–8 for each remaining connection profile used in your configuration for clientless connections.
- Step 10** Click **Apply**.

**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 List

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

**Fields**

- List Name—Alpha-numeric name for the list. Maximum 64 characters.
- Local TCP Port—Local port that listens for traffic for the application.
- Remote Server—IP address or DNS name of the remote server.
- Remote TCP Port—Remote port that listens for traffic for the application.
- Description—Text that describes the TCP application.

**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 dialog boxes let you specify TCP applications to associate with users or group policies for access over clientless SSL VPN connections. Assign values to the attributes in these windows as follows:

- Local TCP Port—Type a TCP 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—Enter either the domain name or IP address of the remote server. We recommend using a domain name so that you do not have to configure the client applications for the specific IP address.

**Caution**

The DNS name assigned to the Remote Server parameter must match the Domain Name and Server Group parameters to establish the tunnel and resolve to an IP address, per the instructions in [Configuring DNS for Port Forwarding, page 38-22](#). The default setting for both the Domain and Server Group parameters is DefaultDNS.

- 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 |
| •             | —           | •                | —        | —      |

## Configuring the Use of External Proxy Servers

Use the Proxies pane to configure the security appliance to use external proxy servers to handle HTTP requests and HTTPS requests. These servers act as an intermediary between users and the Internet. Requiring all Internet access via servers you control provides another opportunity for filtering to assure secure Internet access and administrative control.

**Note**

HTTP and HTTPS proxy services do not support connections to personal digital assistants.

**Fields**

Use an HTTP proxy server—Click to use an external HTTP proxy server.

- Specify IP address of proxy server—Click to identify the HTTP proxy server by its IP address or hostname.
- IP Address—Enter the hostname or IP address of the external HTTP proxy server
- Port—Enter the port that listens for HTTP requests. The default port is 80.
- Exception Address List— (Optional) Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the HTTP proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards:
  - \* to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string.
  - ? to match any single character, including slashes and periods.
  - [x-y] to match any single character in the range of x and y, where x represents one character and y represents another character in the ANSI character set.
  - [!x-y] to match any single character that is not in the range.

- **UserName**—(Optional) Enter this keyword to accompany each HTTP proxy request with a username to provide basic, proxy authentication.
- **Password**—Enter a password to send to the proxy server with each HTTP request.
- **Specify PAC file URL**—As an alternative to specifying the IP address of the HTTP proxy server, you can click this option to specify a Proxy autoconfiguration file to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL. Enter **http://** and type the URL of the proxy autoconfiguration file into the adjacent field. If you omit the **http://** portion, the security appliance ignores it.

Use an HTTPS proxy server—Click to use an external HTTPS proxy server.

- **Specify IP address of proxy server**—Click to identify the HTTPS proxy server by its IP address or hostname.
- **IP Address**—Enter the hostname or IP address of the external HTTPS proxy server
- **Port**—Enter the port that listens for HTTPS requests. The default port is 443.
- **Exception Address List**— (Optional) Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the HTTPS proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards:
  - \* to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string.
  - ? to match any single character, including slashes and periods.
  - [x-y] to match any single character in the range of x and y, where x represents one character and y represents another character in the ANSI character set.
  - [!x-y] to match any single character that is not in the range.
- **UserName**—(Optional) Enter this keyword to accompany each HTTPS proxy request with a username to provide basic, proxy authentication.
- **Password**—Enter a password to send to the proxy server with each HTTPS request.

### Modes

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

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

## Configuring 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.example.com/hrbenefits`, `hrbenefits` is the path. Similarly, for the URL `www.example.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—(radio button) Click to use a port for proxy bypass. The valid port numbers are 20000-21000.
  - Port (field)—Enter a high-numbered port for the security appliance to reserve for proxy bypass.
  - Path Mask—(radio button) Click to use a URL for proxy bypass.
  - Path Mask—(Field) Enter a URL for proxy bypass. It can contain a regular expression.
- URL—Define target URLs for proxy bypass.
  - URL—(drop-down list) Select either http or https as the protocol.
  - URL (text field)—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 |
| •             | —           | •                | —        | —      |

## DTLS Settings

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

If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect with an SSL VPN tunnel only.

### Fields

- Interface—Displays a list of interfaces on the security appliance.
- DTLS Enabled—Check to enable DTLS connections with the AnyConnect client on the interfaces.
- UDP Port (default 443)—(Optional) Specify a separate UDP port for DTLS connections.

### 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 Settings

The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. The client gives remote users the benefits of an SSL VPN client without the need for network administrators to install and configure clients on remote computers.

Without a previously-installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

The AnyConnect client can be downloaded from the security appliance, or it can be installed manually on the remote PC by the system administrator. For more information about installing the client manually, see the *Cisco AnyConnect VPN Client Administrator Guide*.

The security appliance downloads the client based on the group policy or local user policy attributes. You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

#### Fields

- SSL VPN Client Images table—Displays the package files specified as SSL VPN client images, and allows you to establish the order that the security appliance downloads the images to the remote PC.
  - Add—Displays the Add SSL VPN Client Image window, where you can specify a file in flash memory as a client image file, or where you can browse flash memory for a file to specify as a client image. You can also upload a file from a local computer to the flash memory.
  - Replace—Displays the Replace SSL VPN Client Image window, where you can specify a file in flash memory as an client image to replace an image highlighted in the SSL VPN Client Images table. You can also upload a file from a local computer to the flash memory.
  - Delete—Deletes an image from the table. This does not delete the package file from flash.
  - Move Up and Move Down—changes the order in which the security appliance downloads the client images to the remote PC. It downloads the image at the top of the table first. Therefore, you should move the image used by the most commonly-encountered operating system to the top.
- SSL VPN Client Profiles table—Displays the XML files specified as SSL VPN client profiles. These profiles display host information in the AnyConnect VPN Client user interface.
  - Add—Displays the Add SSL VPN Client Profiles window, where you can specify a file in flash memory as a profile, or where you can browse flash memory for a file to specify as a profile. You can also upload a file from a local computer to the flash memory.
  - Edit—Displays the Edit SSL VPN Client Profiles window, where you can specify a file in flash memory as a profile to replace a profile highlighted in the SSL VPN Client Profiles table. You can also upload a file from a local computer to the flash memory.
  - Delete—Deletes a profile from the table. This does not delete the XML file from flash.
- Cache File System—The security appliance expands SSL VPN client and CSD images in cache memory. Adjust the size of cache memory to ensure the images have enough space to expand.

**Modes**

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

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

## Add/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 add as an SSL VPN client image, or to replace an image already listed in the table. You can also browse the flash memory for a file to identify, or you can upload a file from a local computer.

**Fields**

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

**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

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 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 image.
- Browse Local Files—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 a client image.
- Flash File System Path—Identifies the filename of the file in the flash memory of the security appliance that you want to identify as an SSL VPN client image.
- Browse Flash—Displays the Browse Flash Dialog 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 a client image.
- Upload File—Initiates the file upload.

**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 SSL VPN Client Profiles

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 profile. These profiles display host information in the AnyConnect VPN Client user interface. You can also browse the local computer or the flash memory of the security appliance for a file to identify.

**Fields**

- Profile Name—Associates a name with the XML file that appears in the table. Provide any name that makes it easy for you to remember the hosts identified in the XML profile file.
- Profile Package—Identifies the filename of the file in flash memory on the local computer that you want to identify as an SSL VPN client profile.
- 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 a profile.
- Upload File—Initiates the file upload.

**Modes**

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

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

## Upload Package

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 profile. 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 profile.
- **Browse Local Files**—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 a client profile.
- **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 client profile.
- **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 a client profile.
- **Upload File**—Initiates the file upload.

### Modes

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

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

## Bypass Interface Access List

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

- **Enable inbound IPSec sessions to bypass interface access-lists.** Group policy and per-user authorization access lists still apply to the traffic—By default, the security appliance allows VPN traffic to terminate on a security appliance interface; you do not need to allow IKE or ESP (or other types of VPN packets) in an access rule. When this option is checked, you also do not need an access rule for local IP addresses of decrypted VPN packets. Because the VPN tunnel was terminated successfully using VPN security mechanisms, this feature simplifies configuration and maximizes the security appliance performance without any security risks. (Group policy and per-user authorization access lists still apply to the traffic.)

## SSO Servers

The SSO Server window lets you configure or delete single sign-on (SSO) for users of clientless SSL VPN connecting to a Computer Associates SiteMinder SSO server or to a Security Assertion Markup Language (SAML), Version 1.1, Browser Post Profile SSO server. SSO support, available only for clientless SSL VPN, lets users access different secure services on different servers without entering a username and password more than once.

You can choose from four methods when configuring SSO: Auto Signon using basic HTTP and/or NTLMv1 authentication, HTTP Form protocol, or Computer Associates eTrust SiteMinder (formerly Netegrity SiteMinder), or SAML, Version 1.1 Browser Post Profile.

**Note**

---

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

---

This section describes the procedures for setting up SSO with both SiteMinder and SAML Browser Post Profile.

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

The SSO mechanism either starts as part of the AAA process (HTTP Forms) or just after successful user authentication to either a AAA server (SiteMinder) or a SAML Browser Post Profile server. In these cases, the clientless SSL VPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the clientless SSL VPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS.

If the authenticating server approves the authentication request, it returns an SSO authentication cookie to the clientless SSL VPN 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.

## Configuring SiteMinder and SAML Browser Post Profile

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

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

For SAML Browser Post Profile you must configure a Web Agent (Protected Resource URL) for authentication. For the specifics of setting up a SAML Browser Post Profile SSO server, see [SAML POST SSO Server Configuration](#).

### 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 and the SAML Browser Post Profile 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 |
| •             | —           | •                | —        | —      |

## SAML POST SSO Server Configuration

Use the SAML server documentation provided by the server software vendor to configure the SAML server in Relying Party mode. The following steps list the values required to configure the SAML Server for Browser Post Profile:

- 
- Step 1** Configure the SAML server parameters to represent the asserting party (the security appliance):
- Recipient consumer (Web Agent) URL (same as the assertion consumer URL configured on the ASA)
  - Issuer ID, a string, usually the hostname of appliance
  - Profile type -Browser Post Profile
- Step 2** Configure certificates.
- Step 3** Specify that asserting party assertions must be signed.
- Step 4** Select how the SAML server identifies the user:
- Subject Name Type is DN
  - Subject Name format is uid=<user>

## 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. This .jar file is also available on the Cisco security appliance CD.

## Add/Edit SSO Servers

This SSO method uses CA SiteMinder and SAML Browser Post Profile. You can also set up SSO using the HTTP Form protocol, or Basic HTML and NTLM authentication. To use the HTTP Form protocol, see [Configuring Session Settings](#). 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 types currently supported by the security appliance are SiteMinder and SAML Browser Post Profile.
- **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 the security appliance, the SSO server, 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 |
| •             | —           | •                | —        | —      |

## Clientless SSL VPN Access

The Clientless SSL VPN Access panel lets you accomplish the following tasks:

- Enable or disable security appliance interfaces for clientless SSL VPN sessions.
- Choose a port for clientless SSL VPN connections.
- Set a global timeout value for clientless SSL VPN sessions.
- Set a maximum number of simultaneous clientless SSL VPN sessions.
- Configure the amount of security appliance memory that clientless SSL VPN can use.

To configure clientless SSL VPN 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 clientless SSL VPN connections on configured security appliance interfaces.
  - Interface—Displays names of all configured interfaces.
  - WebVPN Enabled—Displays current status for clientless SSL VPN on the interface.
    - A green check next to Yes indicates that clientless SSL VPN is enabled.
    - A red circle next to No indicates that clientless SSL VPN is disabled.
  - Enable/Disable—Click to enable or disable clientless SSL VPN on the highlighted interface.
- Port Number—Enter the port number that you want to use for clientless SSL VPN sessions. The default port is 443, for HTTPS traffic; the range is 1 through 65535. If you change the port number, All current clientless SSL VPN 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 clientless SSL VPN 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 clientless SSL VPN sessions you want to allow. Be aware that the different ASA models support clientless SSL VPN sessions as follows: ASA 5510 supports a maximum of 250; ASA 5520 maximum is 750; ASA 5540 maximum is 2500; ASA 5550 maximum is 5000.
- **WebVPN Memory Size**—Enter the percent of total memory or the amount of memory in kilobytes that you want to allocate to clientless SSL VPN 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, ASA 5550—4G. When you change the memory size, the new setting takes effect only after the system reboots.
- **WebVPN Memory (unlabeled)**—Choose to allocate memory for clientless SSL VPN 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 clientless SSL VPN 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

[Clientless SSL VPN End User Set-up](#)

## Configuring Smart Tunnel Access

The Smart Tunnels table displays the smart tunnel lists, each of which identifies one or more applications eligible for smart tunnel access, and its associated OS. Because each group policy or local user policy supports one smart tunnel list, you must group the nonbrowser-based applications to be supported into a smart tunnel list. Following the configuration of a list, you can assign it to one or more group polices or local user policies.

The Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels window lets you do the following:

- To add a smart tunnel list and add applications to the list, click **Add**. The Add Smart Tunnel List dialog box opens. After you name the list, click **Add** again. ASDM opens the Add Smart Tunnel Entry dialog box, which lets you assign the attributes of a smart tunnel to the list. After doing so and clicking OK, ASDM displays those attributes in the list. Repeat as needed to complete the list, then click **OK** in the Add Smart Tunnel List dialog box.

- To change a smart tunnel list, double-click the list or choose the list in the table and click **Edit**. Then click **Add** to insert a new set of smart tunnel attributes into the list, or choose an entry in the list and click **Edit** or **Delete**.
- To remove a list, choose the list in the table and click **Delete**.

Following the configuration and assignment of a smart tunnel list, you can make a smart tunnel easy to use by adding a bookmark for the service and clicking the Enable Smart Tunnel Option in the Add or Edit Bookmark dialog box.

## About Smart Tunnels

A smart tunnel is a connection between a TCP-based application and a private site, using a clientless (browser-based) SSL VPN session with the security appliance as the pathway, and the security appliance as a proxy server. You can identify applications to which you want to grant smart tunnel access, and specify the local path to each application. For applications running on Microsoft Windows, you can also require a match of the SHA-1 hash of the checksum as a condition for granting smart tunnel access.

Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access.

Configuring smart tunnels requires one of the following procedures, depending on whether the application is a client or is a web-enabled application:

- Create one or more smart tunnel lists of the client applications, then assign the list to the group policies or local user policies for whom you want to provide smart tunnel access.
- Create one or more bookmark list entries that specify the URLs of the web-enabled applications eligible for smart tunnel access, then assign the list to the DAPs, group policies, or local user policies for whom you want to provide smart tunnel access.

You can also list web-enabled applications for which to automate the submission of login credentials in smart tunnel connections over clientless SSL VPN sessions.

## Why Smart Tunnels?

Smart tunnel access lets a client TCP-based application use a browser-based VPN connection to connect to a service. It offers the following advantages to users, compared to plug-ins and the legacy technology, port forwarding:

- Smart tunnel offers better performance than plug-ins.
- Unlike port forwarding, smart tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
- Unlike port forwarding, smart tunnel does not require users to have administrator privileges.

The advantage of a plug-in is that it does not require the client application to be installed on the remote computer.

## Smart Tunnel Requirements and Limitations

The following sections categorize the smart tunnel requirements and limitations.

## General Requirements and Limitations

Smart tunnel has the following general requirements and limitations:

- The remote host originating the smart tunnel must be running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000; or Mac OS 10.4 or 10.5.
- Smart tunnel auto sign-on supports only Microsoft Internet Explorer on Windows.
- The browser must be enabled with Java, Microsoft ActiveX, or both.
- Smart tunnel supports only proxies placed between computers running Microsoft Windows and the security appliance. Smart tunnel uses the Internet Explorer configuration (that is, the one intended for system-wide use in Windows). If the remote computer requires a proxy server to reach the security appliance, the URL of the terminating end of the connection must be in the list of URLs excluded from proxy services. If the proxy configuration specifies that traffic destined for the ASA goes through a proxy, all smart tunnel traffic goes through the proxy.

In an HTTP-based remote access scenario, sometimes a subnet does not provide user access to the VPN gateway. In this case, a proxy placed in front of the ASA to route traffic between the web and the end user's location provides web access. However, only VPN users can configure proxies placed in front of the ASA. When doing so, they must make sure these proxies support the CONNECT method. For proxies that require authentication, smart tunnel supports only the basic digest authentication type.

- When smart tunnel starts, the security appliance by default passes all browser traffic through the VPN session if the browser process is the same. The security appliance also does this if a tunnel-all policy applies. If the user starts another instance of the browser process, it passes all traffic through the VPN session. If the browser process is the same and the security appliance does not provide access to a URL, the user cannot open it. As a workaround, assign a tunnel policy that is not tunnel-all.
- A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

## Windows Requirements and Limitations

The following requirements and limitations apply to Windows only:

- Only Winsock 2, TCP-based applications are eligible for smart tunnel access.
- The security appliance does not support the Microsoft Outlook Exchange (MAPI) proxy. Neither port forwarding nor the smart tunnel supports MAPI. For Microsoft Outlook Exchange communication using the MAPI protocol, remote users must use AnyConnect.
- Users of Microsoft Windows Vista who use smart tunnel or port forwarding must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the **Tools > Internet Options > Security** tab. Vista users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases vulnerability to attack.

## Mac OS Requirements and Limitations

The following requirements and limitations apply to Mac OS only:

- Safari 3.1.1 or later, or Firefox 3.0 or later.
- Sun JRE 1.5 or later.

- Only applications started from the portal page can establish smart tunnel connections. This requirement includes smart tunnel support for Firefox. Using Firefox to start another instance of Firefox during the first use of a smart tunnel requires the user profile named `cisco_st`. If this user profile is not present, the session prompts the user to create one.
- Applications using TCP that are dynamically linked to the SSL library can work over a smart tunnel.
- The PowerPC MAC operating system is not support with smart tunnel.
- Smart tunnel does not support the following on Mac OS:
  - Proxy services.
  - Auto sign-on.
  - Applications that use two-level name spaces.
  - Console-based applications, such as Telnet, SSH, and cURL.
  - Applications using `dlopen` or `dlsym` to locate `libsocket` calls.
  - Statically linked applications to locate `libsocket` calls.

## Configuring a Smart Tunnel (Lotus example)

To configure a Smart Tunnel, perform the following steps:



### Note

These example instructions provide the minimum instructions required to add smart tunnel support for an application. See the field descriptions in the sections that follow for more information.

- 
- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**.
- Step 2** Double-click the smart tunnel list to which you want to add an application; or click **Add** to create a list of applications, enter a name for this list in the List Name field, and click **Add**.
- For example, click **Add** in the Smart Tunnels pane, enter Lotus in the List Name field, and click **Add**.
- Step 3** Click **Add** in the Add or Edit Smart Tunnel List dialog box.
- Step 4** Enter a string in the Application ID field to serve as a unique index to the entry within the smart tunnel list.
- Step 5** Enter the filename and extension of the application into the Process Name dialog box.

[Table 38-1](#) shows example Application ID strings and the associated paths required to support Lotus.

**Table 38-1 Smart Tunnel Example: Lotus 6.0 Thick Client with Domino Server 6.5.5**

| Application ID Example | Minimum Required Process Name |
|------------------------|-------------------------------|
| lotusnotes             | notes.exe                     |
| lotusnnotes            | nlnotes.exe                   |
| lotusntaskldr          | ntaskldr.exe                  |
| lotusnfileret          | nfileret.exe                  |

- Step 6** Select **Windows** next to OS.

- Step 7** Click **OK**.
- Step 8** Repeat Steps 3–7 for each application to add to the list.
- Step 9** Click **OK** in the Add or Edit Smart Tunnel List dialog box.
- Step 10** Assign the list to the group policies and local user policies to which you want to provide smart tunnel access to the associated applications, as follows:
  - To assign the list to a group policy, choose **Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add or Edit > Portal** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.
  - To assign the list to a local user policy, choose **Configuration > Remote Access VPN> AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.

## Add or Edit Smart Tunnel List

The Add Smart Tunnel List dialog box lets you add a list of smart tunnel entries to the security appliance configuration. The Edit Smart Tunnel List dialog box lets you modify the contents of the list.

### Field

- List Name—Enter a unique name for the list of applications or programs. There is no restriction on the number of characters in the name. Do not use spaces.

Following the configuration of the smart tunnel list, the list name appears next to the Smart Tunnel List attribute in the clientless SSL VPN group policies and local user policies. Assign a name that will help you to distinguish its contents or purpose from other lists that you are likely to configure.

### Modes

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

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

## Add or Edit Smart Tunnel Entry

The Add or Edit Smart Tunnel Entry dialog box lets you specify the attributes of an application in a smart tunnel list.

- Application ID—Enter a string to name the entry in the smart tunnel list. The string is unique for the OS. It typically names the application to be granted smart tunnel access. To support multiple versions of an application for which you choose to specify different paths or hash values, you can use this attribute to differentiate entries, specifying the OS, and name and version of the application supported by each list entry. The string can be up to 64 characters.
- Process Name—Enter the filename or path to the application. The string can be up to 128 characters.

Windows requires an exact match of this value to the right side of the application path on the remote host to qualify the application for smart tunnel access. If you specify only the filename for Windows, SSL VPN does not enforce a location restriction on the remote host to qualify the application for smart tunnel access.

If you specify a path and the user installed the application in another location, that application does not qualify. The application can reside on any path as long as the right side of the string matches the value you enter.

To authorize an application for smart tunnel access if it is present on one of several paths on the remote host, either specify only the name and extension of the application in this field; or create a unique smart tunnel entry for each path.



---

**Note** A sudden problem with smart tunnel access may be an indication that a *Process Name* value is not up-to-date with an application upgrade. For example, the default path to an application sometimes changes following the acquisition of the company that produces the application and the next application upgrade.

---

For Windows, if you want to add smart tunnel access to an application started from the command prompt, you must specify “cmd.exe” in the Process Name of one entry in the smart tunnel list, and specify the path to the application itself in another entry, because “cmd.exe” is the parent of the application.

Mac OS requires the full path to the process, and is case-sensitive. To avoid specifying a path for each username, insert a tilde (~) before the partial path (e.g., ~/bin/vnc).

- OS—Click **Windows** or **Mac** to specify the host OS of the application.
- Hash—(Optional and applicable only for Windows) To obtain this value, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at <http://support.microsoft.com/kb/841290/>. After installing FCIV, place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:/fciv.exe), then enter **fciv.exe -sha1 application** at the command line (for example, **fciv.exe -sha1 c:\msimn.exe**) to display the SHA-1 hash.

The SHA-1 hash is always 40 hexadecimal characters.

Before authorizing an application for smart tunnel access, clientless SSL VPN calculates the hash of the application matching the *Application ID*. It qualifies the application for smart tunnel access if the result matches the value of *Hash*.

Entering a hash provides a reasonable assurance that SSL VPN does not qualify an illegitimate file that matches the string you specified in the *Application ID*. Because the checksum varies with each version or patch of an application, the *Hash* you enter can only match one version or patch on the remote host. To specify a hash for more than one version of an application, create a unique smart tunnel entry for each *Hash* value.



---

**Note** You must update the smart tunnel list in the future if you enter *Hash* values and you want to support future versions or patches of an application with smart tunnel access. A sudden problem with smart tunnel access may be an indication that the application list containing *Hash* values is not up-to-date with an application upgrade. You can avoid this problem by not entering a hash.

---

Following the configuration of the smart tunnel list, you must assign it to a group policy or a local user policy for it to become active, as follows:

- To assign the list to a group policy, choose **Config > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit > Portal** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.
- To assign the list to a local user policy, choose **Config > Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.

**Table 38-2 Example Smart Tunnel Entries**

| Smart Tunnel Support   | Application ID<br>(Any unique string is OK.) | Process Name                             | OS      |
|--|--|--|---------|
| Mozilla Firefox.   | firefox                                      | firefox.exe                              | Windows |
| Microsoft Outlook Express.   | outlook-express                              | msimn.exe                                | Windows |
| More restrictive alternative—Microsoft Outlook Express only if the executable file is in a predefined path.  | outlook-express                              | \Program Files\Outlook Express\msimn.exe | Windows |
| Open a new Terminal window on a Mac. (Any subsequent application launched from within the same Terminal window fails because of the one-time-password implementation.) | terminal                                     | Terminal                                 | Mac     |
| Start smart tunnel for a new window  | new-terminal                                 | Terminal open -a MacTelnet               | Mac     |
| Start application from a Mac Terminal window.  | curl   | Terminal curl www.example.com            | Mac     |

### Modes

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

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

## Add or Edit Smart Tunnel Auto Sign-on Server List

The Add Smart Tunnel Auto Sign-on Server List dialog box lets you add one or more lists of servers for which to automate the submission of login credentials during smart tunnel setup. The Edit Smart Tunnel Auto-signon Server List dialog box lets you modify the contents of these lists.

### Field

- List Name—Enter a unique name for the list of remote servers. The string can be up to 64 characters. Do not use spaces.

Following the configuration of the smart tunnel auto sign-on list, the list name appears next to the Auto Sign-on Server List attribute under Smart Tunnel in the Clientless SSL VPN group policy and local user policy configurations. Assign a name that will help you to distinguish its contents or purpose from other lists that you are likely to configure.

### Modes

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

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

## Add or Edit Smart Tunnel Auto Sign-on Server Entry

The Add or Edit Smart Tunnel Entry dialog box lets you identify a server to be added to a smart tunnel auto sign-on list. You can identify it by its hostname, or IP address and subnet mask.



### Caution

Use the address format used in the source code of the web pages on the intranet. If you are configuring smart tunnel auto sign-on for browser access and some web pages use host names and others use IP addresses, or you do not know, specify both in different smart tunnel auto sign-on entries. Otherwise, if a link on a web page uses a different format than the one you specify, it will fail when the user clicks it.

- Host name—Enter a hostname or wildcard mask to auto-authenticate to. You can use the following wildcard characters:
  - \* to match any number of characters or zero characters
  - ? to match any single character
  - [] to match any single character in the range expressed inside the brackets

For example, enter \*.example.com. Using this option protects the configuration from dynamic changes to IP addresses.

- IP Address—Enter an IP address to auto-authenticate to.
- Subnet Mask—Sub-network of hosts associated with the IP address.
- Use Windows domain name with user name (Optional) —Click to add the Windows domain to the username if authentication requires it. If you do so, be sure to specify the domain name when assigning the smart tunnel list to one or more group policies or local user policies.

Following the configuration of the smart tunnel auto sign-on server list, you must assign it to a group policy or a local user policy for it to become active, as follows:

- To assign the list to a group policy, choose **Config > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit > Portal**, find the Smart Tunnel area, and choose the list name from the drop-down list next to the Auto Sign-on Server List attribute.
- To assign the list to a local user policy, choose **Config > Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN**, find the Smart Tunnel area, and choose the list name from the drop-down list next to the Auto Sign-on Server List attribute.

**Modes**

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

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

## Configuring Customization Objects

You can customize all end-user visible content on the clientless SSL VPN portal. To do so, you create an XML customization object, using an XML template, the Customization Editor in ASDM, or by exporting and editing an already existing customization object, which you then reimport to the security appliance.

Version 8.0 software extends the functionality for configuring customization, and the new process is incompatible with previous versions. During the upgrade to 8.0 software, the security appliance preserves a current configuration by using old settings to generate new customization objects. This process occurs only once, and is more than a simple transformation from the old format to the new one because the old values are only a partial subset of the new ones.



**Note**

Version 7.2 portal customizations and URL lists work in the Beta 8.0 configuration only if clientless SSL VPN (WebVPN) is enabled on the appropriate interface in the Version 7.2(x) configuration file *before* you upgrade to Version 8.0.

From the current pane, you can add a new customization object, based on a template, or you can modify an already-imported customization object.

**Fields**

**Add**—Click to invoke the Add Customization pane, which lets you make a copy of the default customization object and save it with a unique name. Then you can use the ASDM SSL VPN Customization Editor to modify it to suit your requirements.

**Edit**—Click to edit an existing, highlighted customization object. Doing so invokes the SSL VPN Customization Editor.

**Delete**—Click to delete a customization object.

**Import**—Click to import a customization object, which is an XML file. For information about creating such an XML file, click this link: [Creating XML-Based Portal Customization Objects and URL Lists](#).

**Export**—Click to export an exiting, highlighted customization object. Doing so lets you edit the object, and then reimport it to this security appliance or to another one.

**Customization Objects**—Lists the existing customization objects on the security appliance.

**OnScreen Keyboard**—Specify when to display the OnScreen Keyboard to end users. This keyboard provides additional security by eliminating the need to enter keystrokes on a physical keyboard for passwords when users log on or otherwise authenticate.

**Modes**

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

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

## Add Customization Object

To add a customization object, create a copy of and provide a unique name for the DfltCustomization object. Then you can modify or edit it to meet your requirements.

### Field

Customization Object Name—Enter a name for the new customization object. Maximum 64 characters, no spaces.

### Modes

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

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

## Import/Export Customization Object

You can import or export already-existing customization objects. Import an object that you want to apply to end users. Export a customization object already resident on the security appliance for editing purposes, after which you can reimport it.

### Fields

- Customization Object Name—Identify the customization object by name. Maximum 64 characters, no spaces.
- Select a file—Choose the method by which you want to import or export the customization file.
  - Local computer—Choose this method to import a file that resides on the local PC.
  - Path—Provide the path to the file.
  - Browse Local Files—Browse to the path for the file.
  - Flash file system—Choose this method to export a file that resides on the security appliance.
  - Path—Provide the path to the file.
  - Browse Flash—Browse to the path for the file.
  - Remote server—Select this option to import a customization file that resides on a remote server accessible from the security appliance.
  - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
- Import/Export Now—Click to import or export the file.

**Modes**

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

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

## Creating XML-Based Portal Customization Objects and URL Lists

This section includes the following topics:

- [Understanding the XML Customization File Structure](#)
- [Customization Example](#)
- [Using the Customization Template](#)

### Understanding the XML Customization File Structure

Table 38-3 presents the file structure for an XML customization object.



**Note**

An empty tag `<param></param>` in an XML customization file is the equivalent of a CLI command with a trivial value:

```
(hostname)# param value ""
```

Absence of a parameter/tag results in a default/inherited value, while presence results in setting the parameter/tag value even it is an empty string.

**Table 38-3 XML-Based Customization File Structure**

| Tag                | Type        | Values                 | Preset value    | Description   |
|--------------------|-------------|------------------------|-----------------|---|
| <b>custom</b>      | <b>node</b> |                        |                 | <b>Root tag</b>   |
| <b>auth-page</b>   | <b>node</b> |                        |                 | <b>Tag-container of authentication page configuration</b> |
| <b>window</b>      | <b>node</b> |                        |                 | <b>Browser window</b>                                     |
| title-text         | string      | Arbitrary string       | empty string    |   |
| <b>title-panel</b> | <b>node</b> |                        |                 | <b>The page top panel with a logo and a text</b>          |
| mode               | text        | enable  <b>disable</b> | disable         |   |
| text               | text        | Arbitrary string       | empty string    |   |
| logo-url           | text        | Arbitrary URL          | empty image URL |   |

**Table 38-3 XML-Based Customization File Structure**

|                               |                        |                        |                   |  |
|-------------------------------|------------------------|------------------------|-------------------|--|
| <b>copyright-panel</b>        | <b>node</b>            |                        |                   | <b>The page bottom panel with a copyright information</b>                          |
| mode                          | text                   | enable  <b>disable</b> | disable           |  |
| text                          | text                   | Arbitrary URL          | empty string      |  |
| <b>info-panel</b>             | <b>node</b>            |                        |                   | <b>The panel with a custom text and image</b>                                      |
| mode                          | string                 | enable  <b>disable</b> | disable           |  |
| image-position                | string                 | <b>above</b>  below    | above             | The image position, relative to text   |
| image-url                     | string                 | Arbitrary URL          | empty image       |  |
| text                          | string                 | Arbitrary string       | empty string      |  |
| <b>logon-form</b>             | <b>node</b>            |                        |                   | <b>The form with username, password, group prompt</b>                              |
| title-text                    | string                 | Arbitrary string       | Logon             |  |
| message-text                  | string                 | Arbitrary string       | empty string      |  |
| username-prompt-text          | string                 | Arbitrary string       | Username          |  |
| password-prompt-text          | string                 | Arbitrary string       | Password          |  |
| internal-password-prompt-text | string                 | Arbitrary string       | Internal Password |  |
| group-prompt-text             | string                 | Arbitrary string       | Group             |  |
| submit-button-text            | string                 | Arbitrary string       | Logon             |  |
| <b>logout-form</b>            | <b>node</b>            |                        |                   | <b>The form with a logout message and the buttons to login or close the window</b> |
| title-text                    | string                 | Arbitrary string       | Logout            |  |
| message-text                  | string                 | Arbitrary string       | Empty string      |  |
| login-button-text             | string                 | Arbitrary string       | Login             |  |
| close-button-text             | string                 | Arbitrary string       | Close window      |  |
| <b>language-selector</b>      | <b>node</b>            |                        |                   | <b>The drop-down box to select a language</b>                                      |
| mode                          | string                 | enable disable         | disable           |  |
| title                         | text                   |                        | Language          | The prompt text to select language   |
| <b>language</b>               | <b>node (multiple)</b> |                        |                   |  |
| code                          | string                 |                        |                   |  |

Table 38-3 XML-Based Customization File Structure

|                  |                 |  |                 |   |
|------------------|-----------------|--|-----------------|---|
| text             | string          |  |                 |   |
| portal           | node            |  |                 | Tag-container of the portal page configuration  |
| window           | node            |  |                 | see authentication page description   |
| title-text       | string          | Arbitrary string   | Empty string    |   |
| title-panel      | node            |  |                 | see authentication page description   |
| mode             | string          | enable/disable   | Disable         |   |
| text             | string          | Arbitrary string   | Empty string    |   |
| logo-url         | string          | Arbitrary URL  | Empty image URL |   |
| navigation-panel | node            |  |                 | The panel on the left with application tabs   |
| mode             | string          | enable/disable   | enable          |   |
| application      | node (multiple) |  | N/A             | The node changes defaults for the configured (by id) application  |
| id               | string          | For stock application<br>web-access<br>file-access<br>app-access<br>net-access<br>help<br><br>For ins:<br>Unique plug-in | N/A             |   |
| tab-title        | string          |  | N/A             |   |
| order            | number          |  | N/A             | Value used to sort elements. The default element order values have step 1000, 2000, 3000, etc. For example, to insert an element between the first and second element, use a value 1001 – 1999. |

**Table 38-3 XML-Based Customization File Structure**

|                    |                        |                  |         |  |
|--------------------|------------------------|------------------|---------|--|
| url-list-title     | string                 |                  | N/A     | If the application has bookmarks, the title for the pane with grouped bookmarks  |
| mode               | string                 | enable disable   | N/A     |  |
| <b>toolbar</b>     | <b>node</b>            |                  |         |  |
| mode               | string                 | enable disable   | Enable  |  |
| prompt-box-title   | string                 | Arbitrary string | Address | Title for URL prompt box   |
| browse-button-text | string                 | Arbitrary string | Browse  | Browse button text   |
| logout-prompt-text | string                 | Arbitrary string | Logout  |  |
| <b>column</b>      | <b>node (multiple)</b> |                  |         | <b>One column will be shown by default</b>   |
| width              | string                 |                  | N/A     |  |
| order              | number                 |                  | N/A     | Value used to sort elements.   |
| <b>url-lists</b>   | <b>node</b>            |                  |         | <b>URL lists are considered to be default elements on the portal home page, if they are not explicitly disabled</b>  |
| mode               | string                 | group   nogroup  | group   | Modes:<br>group – elements grouped by application type i.e. Web Bookmarks, File Bookmarks)<br>no-group – url-lists are shown in separate panes<br>disable – do not show URL lists by default |
| <b>pane</b>        | <b>node (multiple)</b> |                  |         | <b>Allows to configure extra panes</b>   |
| mode               | string                 | enable disable   |         | Used to temporarily disable the pane without removing its configuration  |
| title              | string                 |                  |         |  |

**Table 38-3 XML-Based Customization File Structure**

|          |        |  |  |  |
|----------|--------|--|--|--|
| type     | string |  |  | Supported types:<br>RSS<br>IMAGE<br>TEXT<br>HTML |
| url      | string |  |  | URL for<br>RSS,IMAGE or<br>HTML type paned       |
| url-mode | string |  |  | Modes: mangle,<br>no-mangle                      |
| text     | string |  |  | Text for TEXT type<br>panes                      |
| column   | number |  |  |  |

### Customization Example

The following example illustrates the following customization options:

- Hides tab for the File access application
- Changes title and order of Web Access application
- Defines two columns on the home page
- Adds an RSS pane
- Adds three panes (text, image, and html) at the top of second pane

```
<custom name="Default">
  <auth-page>

    <window>
      <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
      <mode>enable</mode>
      <text l10n="yes">XYZ WebVPN</text>
      <logo-url>http://www.xyz.com/images/XYZ.gif</logo-url>
    </title-panel>

    <copyright>
      <mode>enable</mode>
      <text l10n="yes">(c)Copyright, XYZ Inc., 2006</text>
    </copyright>

    <info-panel>
      <mode>enable</mode>
      <image-url>/+CSCOE+/custom/XYZ.jpg</image-url>
      <text l10n="yes">
        <![CDATA[
          <div>
            <b>Welcome to WebVPN !.</b>
          </div>
        ]]>
      </text>
    </info-panel>
  </auth-page>
</custom>
```

```

    ]]>
  </text>
</info-panel>

<logon-form>
  <form>
    <title-text l10n="yes">title WebVPN Logon</title>
    <message-text l10n="yes">message WebVPN Logon</title>
    <username-prompt-text l10n="yes">Username</username-prompt-text>
    <password-prompt-text l10n="yes">Password</password-prompt-text>
    <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
    <group-prompt-text l10n="yes">Group</group-prompt-text>
    <submit-button-text l10n="yes">Logon</submit-button-text>
  </form>
</logon-form>

<logout-form>
  <form>
    <title-text l10n="yes">title WebVPN Logon</title>
    <message-text l10n="yes">message WebVPN Logon</title>
    <login-button-text l10n="yes">Login</login-button-text>
    <close-button-text l10n="yes">Logon</close-button-text>
  </form>
</logout-form>

<language-selector>
  <language>
    <code l10n="yes">code1</code>
    <text l10n="yes">text1</text>
  </language>
  <language>
    <code l10n="yes">code2</code>
    <text l10n="yes">text2</text>
  </language>
</language-selector>

</auth-page>

<portal>

  <window>
    <title-text l10n="yes">title WebVPN Logon</title>
  </window>

  <title-panel>
    <mode>enable</mode>
    <text l10n="yes">XYZ WebVPN</text>
    <logo-url>http://www.xyz.com/logo.gif</logo-url>
  </title-panel>

  <navigation-panel>
    <mode>enable</mode>
  </navigation-panel>

  <application>
    <id>file-access</id>
    <mode>disable</mode>
  </application>
  <application>
    <id>web-access</id>
    <tab-title>XYZ Intranet</tab-title>
    <order>3001</order>
  </application>

```

```

    <column>
      <order>2</order>
      <width>40%</width>
    </column>
  </column>
  <column>
    <column>
      <order>1</order>
      <width>60%</width>
    </column>
  </column>

  <url-lists>
    <mode>no-group</mode>
  </url-lists>

  <pane>
    <id>rss_pane</id>
    <type>RSS</type>
    <url>rss.xyz.com?id=78</url>
  </pane>

  <pane>
    <id>text_pane</id>
    <type>TEXT</type>
    <url>rss.xyz.com?id=78</url>
    <column>1</column>
    <row>0</row>
    <text>Welcome to XYZ WebVPN Service</text>
  </pane>

  <pane>
    <type>IMAGE</type>
    <url>http://www.xyz.com/logo.gif</url>
    <column>1</column>
    <row>2</row>
  </pane>

  <pane>
    <type>HTML</type>
    <title>XYZ news</title>
    <url>http://www.xyz.com/news.html</url>
    <column>1</column>
    <row>3</row>
  </pane>

</portal>

</custom>

```

## Using the Customization Template

A customization template, named *Template*, contains all currently employed tags with corresponding comments that describe how to use them. Use the export command to download the customization template from the security appliance, as follows:

```
hostname# export webvpn customization Template tftp://webserver/default.xml
hostname#
```

You cannot change or delete the file *Template*. When you export it as in this example, you are saving it to a new name, *default.xml*. After you make your changes to this file, using it to create a customization object that meets the needs of your organization, you import it to the security appliance, either as *default.xml* or another name of your choosing. For example,

```
hostname# import webvpn customization General tftp://webserver/custom.xml
```

```
hostname#
```

where you import an XML object called *custom.xml* and name it *General* on the security appliance.

## The Customization Template

The customization template, named *Template*, follows.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--
```

```
Copyright (c) 2007,2008 by Cisco Systems, Inc.
All rights reserved.
```

Note: all white spaces in tag values are significant and preserved.

```
Tag: custom
```

```
Description: Root customization tag
```

```
Tag: custom/languages
```

```
Description: Contains list of languages, recognized by ASA
```

```
Value: string containing comma-separated language codes. Each language code is
a set dash-separated alphanumeric characters, started with
alpha-character (for example: en, en-us, irokese8-language-us)
```

```
Default value: en-us
```

```
Tag: custom/default-language
```

```
Description: Language code that is selected when the client and the server
were not able to negotiate the language automatically.
```

```
For example the set of languages configured in the browser
is "en,ja", and the list of languages, specified by
'custom/languages' tag is "cn,fr", the default-language will be
used.
```

```
Value: string, containing one of the language coded, specified in
'custom/languages' tag above.
```

```
Default value: en-us
```

```
*****
```

```
Tag: custom/auth-page
```

```
Description: Contains authentication page settings
```

```
*****
```

```
Tag: custom/auth-page/window
```

```
Description: Contains settings of the authentication page browser window
```

```
Tag: custom/auth-page/window/title-text
```

```
Description: The title of the browser window of the authentication page
```

```
Value: arbitrary string
```

```
Default value: Browser's default value
```

```
*****
```

```
Tag: custom/auth-page/title-panel
```

```
Description: Contains settings for the title panel
```

```
Tag: custom/auth-page/title-panel/mode
```

```
Description: The title panel mode
```

```
Value: enable|disable
```

```
Default value: disable
```

```

Tag: custom/auth-page/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-page/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder, lighter etc.
Default value: empty string

Tag: custom/auth-page/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string

Tag: custom/auth-page/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/auth-page/title-panel/style
Description: CSS style of the title panel
Value: CSS style string
Default value: empty string

*****

Tag: custom/auth-page/copyright-panel
Description: Contains the copyright panel settings

Tag: custom/auth-page/copyright-panel/mode
Description: The copyright panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/copyright-panel/text
Description: The copyright panel text
Value: arbitrary string
Default value: empty string

*****

Tag: custom/auth-page/info-panel
Description: Contains information panel settings

```

Tag: custom/auth-page/info-panel/mode  
Description: The information panel mode  
Value: enable|disable  
Default value: disable

Tag: custom/auth-page/info-panel/image-position  
Description: Position of the image, above or below the informational panel text  
Values: above|below  
Default value: above

Tag: custom/auth-page/info-panel/image-url  
Description: URL of the information panel image (imported via "import webvpn webcontent")  
Value: URL string  
Default value: empty image URL

Tag: custom/auth-page/info-panel/text  
Description: Text of the information panel  
Text: arbitrary string  
Default value: empty string

\*\*\*\*\*

Tag: custom/auth-page/logon-form  
Description: Contains logon form settings

Tag: custom/auth-page/logon-form/title-text  
Description: The logon form title text  
Value: arbitrary string  
Default value: "Logon"

Tag: custom/auth-page/logon-form/message-text  
Description: The message inside of the logon form  
Value: arbitrary string  
Default value: empty string

Tag: custom/auth-page/logon-form/username-prompt-text  
Description: The username prompt text  
Value: arbitrary string  
Default value: "Username"

Tag: custom/auth-page/logon-form/password-prompt-text  
Description: The password prompt text  
Value: arbitrary string  
Default value: "Password"

Tag: custom/auth-page/logon-form/internal-password-prompt-text  
Description: The internal password prompt text  
Value: arbitrary string  
Default value: "Internal Password"

Tag: custom/auth-page/logon-form/group-prompt-text  
Description: The group selector prompt text  
Value: arbitrary string  
Default value: "Group"

Tag: custom/auth-page/logon-form/submit-button-text  
Description: The submit button text  
Value: arbitrary string  
Default value: "Logon"

Tag: custom/auth-page/logon-form/internal-password-first  
Description: Sets internal password first in the order  
Value: yes|no

Default value: no

Tag: custom/auth-page/logon-form/title-font-color  
 Description: The font color of the logon form title  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

Tag: custom/auth-page/logon-form/title-background-color  
 Description: The background color of the logon form title  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

Tag: custom/auth-page/logon-form/font-color  
 Description: The font color of the logon form  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

Tag: custom/auth-page/logon-form/background-color  
 Description: The background color of the logon form  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

\*\*\*\*\*

Tag: custom/auth-page/logout-form  
 Description: Contains the logout form settings

Tag: custom/auth-page/logout-form/title-text  
 Description: The logout form title text  
 Value: arbitrary string  
 Default value: "Logout"

Tag: custom/auth-page/logout-form/message-text  
 Description: The logout form message text  
 Value: arbitrary string  
 Default value: Goodbye.  
                   For your own security, please:  
                   Clear the browser's cache  
                   Delete any downloaded files  
                   Close the browser's window

Tag: custom/auth-page/logout-form/login-button-text  
 Description: The text of the button sending the user to the logon page  
 Value: arbitrary string  
 Default value: "Logon"

\*\*\*\*\*

Tag: custom/auth-page/language-selector  
 Description: Contains the language selector settings

Tag: custom/auth-page/language-selector/mode  
 Description: The language selector mode  
 Value: enable|disable  
 Default value: disable

Tag: custom/auth-page/language-selector/title  
 Description: The language selector title  
 Value: arbitrary string  
 Default value: empty string

Tag: custom/auth-page/language-selector/language (multiple)  
Description: Contains the language settings

Tag: custom/auth-page/language-selector/language/code  
Description: The code of the language  
Value (required): The language code string

Tag: custom/auth-page/language-selector/language/text  
Description: The text of the language in the language selector drop-down box  
Value (required): arbitrary string

\*\*\*\*\*

Tag: custom/portal  
Description: Contains portal page settings

\*\*\*\*\*

Tag: custom/portal/window  
Description: Contains the portal page browser window settings

Tag: custom/portal/window/title-text  
Description: The title of the browser window of the portal page  
Value: arbitrary string  
Default value: Browser's default value

\*\*\*\*\*

Tag: custom/portal/title-panel  
Description: Contains settings for the title panel

Tag: custom/portal/title-panel/mode  
Description: The title panel mode  
Value: enable|disable  
Default value: disable

Tag: custom/portal/title-panel/text  
Description: The title panel text.  
Value: arbitrary string  
Default value: empty string

Tag: custom/portal/title-panel/logo-url  
Description: The URL of the logo image (imported via "import webvpn webcontent")  
Value: URL string  
Default value: empty image URL

Tag: custom/portal/title-panel/background-color  
Description: The background color of the title panel  
Value: HTML color format, for example #FFFFFF  
Default value: #FFFFFF

Tag: custom/auth-pa/title-panel/font-color  
Description: The background color of the title panel  
Value: HTML color format, for example #FFFFFF  
Default value: #000000

Tag: custom/portal/title-panel/font-weight  
Description: The font weight  
Value: CSS font size value, for example bold, bolder, lighter etc.  
Default value: empty string

Tag: custom/portal/title-panel/font-size  
Description: The font size  
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.

Default value: empty string

Tag: custom/portal/title-panel/gradient  
 Description: Specifies using the background color gradient  
 Value: yes|no  
 Default value:no

Tag: custom/portal/title-panel/style  
 Description: CSS style for title text  
 Value: CSS style string  
 Default value: empty string

\*\*\*\*\*

Tag: custom/portal/application (multiple)  
 Description: Contains the application setting

Tag: custom/portal/application/mode  
 Description: The application mode  
 Value: enable|disable  
 Default value: enable

Tag: custom/portal/application/id  
 Description: The application ID. Standard application ID's are: home, web-access, file-access, app-access, network-access, help  
 Value: The application ID string  
 Default value: empty string

Tag: custom/portal/application/tab-title  
 Description: The application tab text in the navigation panel  
 Value: arbitrary string  
 Default value: empty string

Tag: custom/portal/application/order  
 Description: The order of the application's tab in the navigation panel. Applications with lesser order go first.  
 Value: arbitrary number  
 Default value: 1000

Tag: custom/portal/application/url-list-title  
 Description: The title of the application's URL list pane (in group mode)  
 Value: arbitrary string  
 Default value: Tab title value concatenated with "Bookmarks"

\*\*\*\*\*

Tag: custom/portal/navigation-panel  
 Description: Contains the navigation panel settings

Tag: custom/portal/navigation-panel/mode  
 Description: The navigation panel mode  
 Value: enable|disable  
 Default value: enable

\*\*\*\*\*

Tag: custom/portal/toolbar  
 Description: Contains the toolbar settings

Tag: custom/portal/toolbar/mode  
 Description: The toolbar mode  
 Value: enable|disable  
 Default value: enable

Tag: custom/portal/toolbar/prompt-box-title  
 Description: The universal prompt box title  
 Value: arbitrary string  
 Default value: "Address"

Tag: custom/portal/toolbar/browse-button-text  
 Description: The browse button text  
 Value: arbitrary string  
 Default value: "Browse"

Tag: custom/portal/toolbar/logout-prompt-text  
 Description: The logout prompt text  
 Value: arbitrary string  
 Default value: "Logout"

\*\*\*\*\*

Tag: custom/portal/column (multiple)  
 Description: Contains settings of the home page column(s)

Tag: custom/portal/column/order  
 Description: The order the column from left to right. Columns with lesser order values go first  
 Value: arbitrary number  
 Default value: 0

Tag: custom/portal/column/width  
 Description: The home page column width  
 Value: percent  
 Default value: default value set by browser  
 Note: The actual width may be increased by browser to accommodate content

\*\*\*\*\*

Tag: custom/portal/url-lists  
 Description: Contains settings for URL lists on the home page

Tag: custom/portal/url-lists/mode  
 Description: Specifies how to display URL lists on the home page:  
     group URL lists by application (group) or  
     show individual URL lists (nogroup).  
 URL lists fill out cells of the configured columns, which are not taken  
 by custom panes.  
 Use the attribute value "nodisplay" to not show URL lists on the home page.

Value: group|nogroup|nodisplay  
 Default value: group

\*\*\*\*\*

Tag: custom/portal/pane (multiple)  
 Description: Contains settings of the custom pane on the home page

Tag: custom/portal/pane/mode  
 Description: The mode of the pane  
 Value: enable|disable  
 Default value: disable

Tag: custom/portal/pane/title  
 Description: The title of the pane  
 Value: arbitrary string  
 Default value: empty string

```

Tag: custom/portal/pane/notitle
Description: Hides pane's title bar
Value: yes|no
Default value: no

Tag: custom/portal/pane/type
Description: The type of the pane. Supported types:
    TEXT - inline arbitrary text, may contain HTML tags;
    HTML - HTML content specified by URL shown in the individual iframe;
    IMAGE - image specified by URL
    RSS - RSS feed specified by URL
Value: TEXT|HTML|IMAGE|RSS
Default value: TEXT

Tag: custom/portal/pane/url
Description: The URL for panes with type HTML,IMAGE or RSS
Value: URL string
Default value: empty string

Tag: custom/portal/pane/text
Description: The text value for panes with type TEXT
Value: arbitrary string
Default value:empty string

Tag: custom/portal/pane/column
Description: The column where the pane located.
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/row
Description: The row where the pane is located
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/height
Description: The height of the pane
Value: number of pixels
Default value: default value set by browser

*****

Tag: custom/portal/browse-network-title
Description: The title of the browse network link
Value: arbitrary string
Default value: Browse Entire Network

Tag: custom/portal/access-network-title
Description: The title of the link to start a network access session
Value: arbitrary string
Default value: Start AnyConnect

-->
= <custom>
= <localization>
<languages>en, ja, zh, ru, ua</languages>
<default-language>en</default-language>
</localization>
= <auth-page>
= <window>
= <title-text l10n="yes">
- <![CDATA[
WebVPN Service

```

```

]]>
</title-text>
</window>
= <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
= <language>
<code>en</code>
<text>English</text>
</language>
= <language>
<code>zh</code>
<text>?? (Chinese)</text>
</language>
= <language>
<code>ja</code>
<text>?? (Japanese)</text>
</language>
= <language>
<code>ru</code>
<text>?????? (Russian)</text>
</language>
= <language>
<code>ua</code>
<text>???????? (Ukrainian)</text>
</language>
</language-selector>
= <logon-form>
= <title-text l10n="yes">
- <![CDATA[
Login
]]>
</title-text>
= <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
= <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
= <message-text l10n="yes">
- <![CDATA[
Please enter your username and password.
]]>
</message-text>
= <username-prompt-text l10n="yes">
- <![CDATA[
USERNAME:
]]>
</username-prompt-text>
= <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:
]]>
</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
= <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:
]]>

```

```

</group-prompt-text>
= <submit-button-text l10n="yes">
- <![CDATA[
Login
]]>
</submit-button-text>
= <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
= <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
= <logout-form>
= <title-text l10n="yes">
- <![CDATA[
Logout
]]>
</title-text>
= <message-text l10n="yes">
- <![CDATA[
Goodbye.
]]>
</message-text>
</logout-form>
= <title-panel>
<mode>enable</mode>
= <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
= <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
= <font-size>
- <![CDATA[
larger
]]>
</font-size>
= <font-color>
- <![CDATA[
#800000
]]>
</font-color>
= <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
= <info-panel>
<mode>disable</mode>

```

```

<image-url l10n="yes"/>+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
= <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
</auth-page>
= <portal>
= <title-panel>
<mode>enable</mode>
= <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes"/>+CSCOU+/cisco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
= <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
= <font-size>
- <![CDATA[
larger
]]>
</font-size>
= <font-color>
- <![CDATA[
#800000
]]>
</font-color>
= <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
= <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
= <application>
<mode>enable</mode>
<id>web-access</id>
= <tab-title l10n="yes">
- <![CDATA[
Web Applications
]]>
</tab-title>
= <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks
]]>
</url-list-title>
<order>2</order>
</application>

```

```

- <application>
  <mode>enable</mode>
  <id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks
]]>
</url-list-title>
<order>3</order>
</application>
- <application>
  <mode>enable</mode>
  <id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access
]]>
</tab-title>
<order>4</order>
</application>
- <application>
  <mode>enable</mode>
  <id>net-access</id>
  <tab-title l10n="yes">AnyConnect</tab-title>
  <order>4</order>
</application>
- <application>
  <mode>enable</mode>
  <id>help</id>
  <tab-title l10n="yes">Help</tab-title>
  <order>1000000</order>
</application>
- <toolbar>
  <mode>enable</mode>
  <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
  <prompt-box-title l10n="yes">Address</prompt-box-title>
  <browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
- <column>
  <width>100%</width>
  <order>1</order>
</column>
- <pane>
  <type>TEXT</type>
  <mode>disable</mode>
  <title />
  <text />
  <notitle />
  <column />
  <row />
  <height />
</pane>
- <pane>
  <type>IMAGE</type>
  <mode>disable</mode>
  <title />
  <url l10n="yes" />
  <notitle />
  <column />

```

```

<row />
<height />
</pane>
= <pane>
<type>HTML</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
= <pane>
<type>RSS</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
= <url-lists>
<mode>group</mode>
</url-lists>
</portal>
</custom>

```

## Help Customization

The security appliance displays help content on the application panels during clientless sessions. Each clientless application panel displays its own help file content using a predetermined filename. For example, the help content displayed on the Application Access panel is from the file named `app-access-hlp.inc`. [Table 38-4](#) shows the clientless application panels and predetermined filenames for the help content.

**Table 38-4** Clientless Applications

| Application Type | Panel              | Filename            |
|------------------|--------------------|---------------------|
| Standard         | Application Access | app-access-hlp.inc  |
| Standard         | Browse Networks    | file-access-hlp.inc |
| Standard         | AnyConnect Client  | net-access-hlp.inc  |
| Standard         | Web Access         | web-access-hlp.inc  |
| Plug-in          | MetaFrame Access   | ica-hlp.inc         |
| Plug-in          | Terminal Servers   | rdp-hlp.inc         |
| Plug-in          | Telnet/SSH Servers | ssh,telnet-hlp.inc  |
| Plug-in          | VNC Connections    | vnc-hlp.inc         |

You can customize the help files provided by Cisco or create help files in other languages. Then use the Import button to copy them to the flash memory of the security appliance for display during subsequent clientless sessions. You can also export previously imported help content files, customize them, and reimport them to flash memory.

The following sections describe how to customize or create help content visible on clientless sessions:

- [Customizing a Help File Provided by Cisco](#)
- [Creating Help Files for Languages Not Provided by Cisco](#)

**Fields**

**Import**—Click to launch the Import Application Help Content dialog, where you can import new help content to flash memory for display during clientless sessions.

**Export**—Click to retrieve previously imported help content selected from the table.

**Delete**—Click to delete previously imported help content selected from the table.

**Language**—Displays the abbreviation of the language rendered by the browser. This field is *not* used for file translation; it indicates the language used in the file. To identify the name of a language associated with an abbreviation in the table, display the list of languages rendered by your browser. For example, a dialog window displays the languages and associated language codes when you use one of the following procedures:

- Open Internet Explorer and choose **Tools > Internet Options > Languages > Add**.
- Open Mozilla Firefox and choose **Tools > Options > Advanced > General**, click **Choose** next to Languages, and click **Select a language to add**.

**Filename**—Displays the filename the help content file was imported as.

**Modes**

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

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

**Customizing a Help File Provided by Cisco**

To customize a help file provided by Cisco, you need to get a copy of the file from the flash memory card first. Get the copy and customize it as follows:

- 
- Step 1** Use your browser to establish a clientless session with the security appliance.
  - Step 2** Display the help file by appending the string in “URL of Help File in Flash Memory of the Security Appliance” in [Table 38-5](#), to the address of the security appliance, substituting *language* as described below, then press Enter.

**Table 38-5 Help Files Provided by Cisco for Clientless Applications**

| Application Type | Panel              | URL of Help File in Flash Memory of the Security Appliance |
|------------------|--------------------|--|
| Standard         | Application Access | /+CSCOE+/help/language/app-access-hlp.inc                  |
| Standard         | Browse Networks    | /+CSCOE+/help/language/file-access-hlp.inc                 |
| Standard         | AnyConnect Client  | /+CSCOE+/help/language/net-access-hlp.inc                  |
| Standard         | Web Access         | /+CSCOE+/help/language/web-access-hlp.inc                  |
| Plug-in          | Terminal Servers   | /+CSCOE+/help/language/rdp-hlp.inc                         |
| Plug-in          | Telnet/SSH Servers | /+CSCOE+/help/language/ssh,telnet-hlp.inc                  |
| Plug-in          | VNC Connections    | /+CSCOE+/help/language/vnc-hlp.inc                         |

*language* is the abbreviation for the language rendered by the browser. It is *not* used for file translation; it indicates the language used in the file. For help files provided by Cisco in English, enter the abbreviation **en**.

The following example address displays the English version of the Terminal Servers help:

**https://address\_of\_security\_appliance/+CSCOE+/help/en/rdp-hlp.inc**

**Step 3** Choose File > Save (Page) As.



**Caution** Do not change the contents of the File name box.

**Step 4** Change the Save as type option to “Web Page, HTML only” and click Save.

**Step 5** Use your preferred HTML editor to customize the file.



**Note** You can use most HTML tags, but do *not* use tags that define the document and its structure (e.g., do not use <html>, <title>, <body>, <head>, <h1>, <h2>, etc. You can use character tags, such as the <b> tag, and the <p>, <ol>, <ul>, and <li> tags to structure content.

**Step 6** Save the file as HTML only, using the original filename and extension.

**Step 7** Make sure the filename matches the one in [Table 38-5](#), and that it does not have an extra filename extension.

Return to ASDM and choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import** to import the modified help file into flash memory.

### Creating Help Files for Languages Not Provided by Cisco

Use standard HTML to create help files in other languages. We recommend creating a separate folder for each language you want to support.



**Note** You can use most HTML tags, but do *not* use tags that define the document and its structure (e.g., do not use <html>, <title>, <body>, <head>, <h1>, <h2>, etc. You can use character tags, such as the <b> tag, and the <p>, <ol>, <ul>, and <li> tags to structure content.

Save the file as HTML only. Use the filename in the Filename column of [Table 38-4](#).

Return to ASDM and choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import** to import the new help file into flash memory.

## Import/Export Application Help Content

Use the Import Application Help Content dialog box to import help files to flash memory for display on the portal pages during clientless sessions. Use the Export Application Help Content dialog box to retrieve previously imported help files for subsequent editing.

### Fields

**Language**—For the Import Application Help Content dialog box only, this field specifies the language rendered by the browser. (This Language field is inactive in the Export Application Help Content dialog box.) This field is not used for file translation; it indicates the language used in the file. Click the dots next to the Language field, double-click the row containing the language used in the help file in the Browse Language Code dialog box, confirm the abbreviation in the Language Code field matches the abbreviation in the row, and click **OK**. If the language for which you want to provide help content is not present in the Browse Language Code dialog box, enter the abbreviation for the language you want into the Language Code field and click **OK**, or enter it into the Language text box to the left of the dots. To identify the abbreviation for the language of a help file to be imported if it is not present in the Browse Language Code dialog box, display the list of languages and abbreviations rendered by your browser. For example, a dialog window displays the languages and associated language codes when you use one of the following procedures:

- Open Internet Explorer and choose **Tools > Internet Options > Languages > Add**.
- Open Mozilla Firefox and choose **Tools > Options > Advanced > General**, click **Choose** next to Languages, and click **Select a language to add**.

**File Name**—If you are importing, specify the file name from the drop-down list for the new help content file. If you are exporting, this field is unavailable.

**Select a File**—Configure the parameters for the source file (if importing) or destination file (if exporting):

**Local computer**—Select if the source or destination file is on a local computer:

- Path—Identify the path of the source or destination file.
- Browse Local Files—Click to browse the local computer for the source or destination file.

**Flash file system**—Select if the source or destination file is located in flash memory on the security appliance:

- Path—Identify the path of the source or destination file in flash memory.
- Browse Flash—Click to browse the flash memory for the source or destination file.

**Remote server**—Select if the source or destination file is on a remote server:

- Path—Select the file transfer (copy) method, either ftp, tftp, or http (for importing only), and specify the path.

### Modes

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

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

## Configuring Browser Access to Client-Server Plug-ins

The Client-Server Plug-in table displays the plug-ins the security appliance makes available to browsers in clientless SSL VPN sessions.

To add, change, or remove a plug-in, do one of the following:

- To add a plug-in, click **Import**. The Import Plug-ins dialog box opens.
- To remove a plug-in, choose it and click **Delete**.

## About Installing Browser Plug-ins

A browser plug-in is a separate program that a web browser invokes to perform a dedicated function, such as connect a client to a server within the browser window. The security appliance lets you import plug-ins for download to remote browsers in clientless SSL VPN sessions. Of course, Cisco tests the plug-ins it redistributes, and in some cases, tests the connectivity of plug-ins we cannot redistribute. However, we do not recommend importing plug-ins that support streaming media at this time.



**Note** Per the GNU General Public License (GPL), Cisco redistributes plug-ins without having made any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.

The security appliance does the following when you install a plug-in onto the flash device:

- (Cisco-distributed plug-ins only) Unpacks the jar file specified in the *URL*.
- Writes the file to the `cisco-config/97/plugin` directory on the security appliance file system.
- Populates the drop-down menu next to the URL attributes in ASDM.
- Enables the plug-in for all future clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down menu next to the Address field of the portal page.

Table 38-6 shows the changes to the main menu and address field of the portal page when you add the plug-ins described in the following sections.

**Table 38-6** Effects of Plug-ins on the Clientless SSL VPN Portal Page

| Plug-in | Main Menu Option Added to Portal Page | Address Field Option Added to Portal Page |
|---------|---------------------------------------|---|
| ica     | Citrix Client                         | citrix://                                 |
| rdp     | Terminal Servers                      | rdp://                                    |
| rdp2    | Terminal Servers Vista                | rdp2://                                   |

**Table 38-6** Effects of Plug-ins on the Clientless SSL VPN Portal Page

| Plug-in    | Main Menu Option Added to Portal Page | Address Field Option Added to Portal Page |
|------------|---------------------------------------|---|
| ssh,telnet | SSH                                   | ssh://                                    |
|            | Telnet                                | telnet://                                 |
| vnc        | VNC Client                            | vnc://                                    |

**Note**

A secondary security appliance obtains the plug-ins from the primary security appliance.

When the user in a clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.

**Note**

Some Java plug-ins may report a status of connected or online even when a session to the destination service is not set up. The open-source plug-in reports the status, not the security appliance.

Before installing the first plug-in, you must follow the instructions in the next section.

## Plug-in Requirements and Restrictions

Clientless SSL VPN must be enabled on the security appliance to provide remote access to the plug-ins.

The minimum access rights required for remote use belong to the guest privilege mode.

A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.

## Preparing the Security Appliance for a Plug-in

Before installing a plug-in, prepare the security appliance by performing the following steps:

- Step 1** Make sure clientless SSL VPN (“webvpn”) is enabled on a security appliance interface.
- Step 2** Install an SSL certificate onto the security appliance interface to which remote users use a fully-qualified domain name (FQDN) to connect.

**Note**

Do not specify an IP address as the common name (CN) for the SSL certificate. The remote user attempts to use the FQDN to communicate with the security appliance. The remote PC must be able to use DNS or an entry in the System32\drivers\etc\hosts file to resolve the FQDN.

See the section that identifies the type of plug-in you want to provide for clientless SSL VPN access.

- [Installing Plug-ins Redistributed by Cisco](#)
- [Assembling and Installing Third-Party Plug-ins—Example: Citrix Java Presentation Server Client](#)

## Installing Plug-ins Redistributed by Cisco

Cisco redistributes the following open-source, Java-based components to be accessed as plug-ins for web browsers in clientless SSL VPN sessions:

**Table 38-7** Plug-ins Redistributed by Cisco

| Cisco Download Link                    | Protocol | Description  | Source of Redistributed Plug-in  |
|--|----------|--|--|
| <a href="#">rdp2-plugin.090211.jar</a> | RDP2     | Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2.<br>Supports Remote Desktop ActiveX Control.<br><b>Note:</b> You can import the RDP and RDP2 plug-ins to make both of them available to clientless users.                                   | Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The original source of the redistributed plug-in is <a href="http://properjavardp.sourceforge.net/">http://properjavardp.sourceforge.net/</a> |
| <a href="#">rdp-plugin.080506.jar</a>  | RDP      | Accesses Microsoft Terminal Services hosted by Windows 2003 R1.<br>Supports Remote Desktop ActiveX Control.  | Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The source of the redistributed plug-in is <a href="http://properjavardp.sourceforge.net/">http://properjavardp.sourceforge.net/</a>          |
| <a href="#">ssh-plugin.080430.jar</a>  | SSH      | The Secure Shell-Telnet plug-in lets the remote user establish a Secure Shell or Telnet connection to a remote computer.   | Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The web site containing the source of the redistributed plug-in is <a href="http://javassh.org/">http://javassh.org/</a>                      |
| <a href="#">vnc-plugin.080130.jar</a>  | VNC      | The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. This version changes the default color of the text, and contains updated French and Japanese help files. | Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The web site containing the source of the redistributed plug-in is <a href="http://www.tightvnc.com/">http://www.tightvnc.com/</a>            |

To retrieve a plug-in redistributed by Cisco and import it into the security appliance, perform the following steps:

- Step 1** Create a temporary directory named `plugins` on the computer you use to establish ASDM sessions with the security appliance.
- Step 2** Download the plug-ins you want from the Cisco website to the `plugins` directory.
- Step 3** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins**.  
This pane displays the plug-ins that are available to clientless SSL sessions.
- Step 4** Click **Import**.  
The Import Client-Server Plug-in dialog box opens.
- Step 5** Use the following descriptions to enter the field values.

### Fields

The Import Client-Server Plug-in dialog box displays the following fields:

- Plug-in Name—Select one of the following values:
  - **ica** to provide plug-in access to Citrix MetaFrame services. Then specify the path to the ica-plugin.jar file in the Remote Server field, as described below.
  - **rdp** to provide plug-in access to Remote Desktop Protocol services. Then specify the path to the rdp-plugin.jar file in the Remote Server field.
  - **ssh,telnet** to provide plug-in access to *both* Secure Shell and Telnet services. Then specify the path to the ssh-plugin.jar file in the Remote Server field.
  - **vnc** to provide plug-in access to Virtual Network Computing services. Then specify the path to the vnc-plugin.jar file in the Remote Server field.



**Note** Any undocumented options in this menu are experimental and are not supported.

- Select a file—Click one of the following options and insert a path into its text field.
  - Local computer—Click to retrieve the plug-in from the computer with which you have established the ASDM session. Enter the location and name of the plug-in into the associated Path field, or click **Browse Local Files** and navigate to the plug-in, choose it, then click **Select**.
  - Flash file system—Click if the plug-in is present on the file system of the security appliance. Enter the location and name of the plug-in into the associated Path field, or click **Browse Flash** and navigate to the plug-in, choose it, then click **OK**.
  - Remote Server—Click to retrieve the plug-in from a host running an FTP or TFTP server. Choose **ftp**, **tftp**, or **HTTP** from the drop-down menu next to the associated Path attribute, depending on which service is running on the remote server. Enter the host name or address of the server and the path to the plug-in into the adjacent text field.

**Step 6** Click **Import Now**.

Click **Apply**.

The plug-in is now available for future clientless SSL VPN sessions.

### Modes

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

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

## Assembling and Installing Third-Party Plug-ins—Example: Citrix Java Presentation Server Client

The open framework of the security appliance lets you add plug-ins to support third-party Java client/server applications. As an example of how to provide clientless SSL VPN browser access to third-party plug-ins, this section describes how to add clientless SSL VPN support for the Citrix Presentation Server Client.



### Caution

Cisco does not provide direct support for or recommend any particular plug-ins that are not redistributed by Cisco. As a provider of clientless SSL VPN services, you are responsible for reviewing and complying with any license agreements required for the use of plug-ins.

With a Citrix plug-in installed on the security appliance, clientless SSL VPN users can use a connection to the security appliance to access Citrix MetaFrame services.

A stateful failover does not retain sessions established using the Citrix plug-in. Citrix users must reauthenticate after failover.

To provide access to the Citrix plug-in, follow the procedures in the following sections.

### Preparing the Citrix MetaFrame Server for Clientless SSL VPN Access

The security appliance performs the connectivity functions of the Citrix secure gateway when the Citrix client connects to the Citrix MetaFrame Server. Therefore, you must configure the Citrix Web Interface software to operate in a mode that does not use the (Citrix) “secure gateway.” Otherwise, the Citrix client cannot connect to the Citrix MetaFrame Server.

Follow the instructions in the “[Preparing the Security Appliance for a Plug-in](#)” section on page 38-72 before using the next section, if you are not already providing support for a plug-in.

### Creating, Installing, and Testing the Citrix Plug-in

To create and install the Citrix plug-in, perform the following steps:

- 
- Step 1** Download the [ica-plugin.zip](#) file from the [Cisco Software Download website](#).  
This file contains files that Cisco customized for use with the Citrix plug-in.
  - Step 2** Download the [Citrix Java client](#) from the Citrix site.
  - Step 3** Extract the following files from the Citrix Java client:
    - JICA-configN.jar
    - JICAEngN.jarYou can use WinZip to perform this step and the next.
  - Step 4** Add the extracted files to the ica-plugin.zip file.
  - Step 5** Ensure the EULA included with the Citrix Java client grants you the rights and permissions to deploy the client on your web servers.
  - Step 6** Establish an ASDM session with the security appliance, choose **Config > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins > Import**, and import the ica-plugin.zip file.



**Note** Users of clientless SSL VPN sessions cannot enter a URL in the Address box to get SSO support for Citrix sessions. You must insert a bookmark as instructed in the following step if you want to provide SSO support for the Citrix plug-in.

**Step 7** Add a bookmark to the applicable bookmark list to make it easy for users to connect. Choose **ica** and enter the following information into the Address field:

```
citrix-server/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```

See [Add/Edit Bookmark List](#) and [Add Bookmark Entry](#) as needed.

**Step 8** To test the plug-in, establish a clientless session with the security appliance and click the bookmark. Use the [Client for Java Administrator’s Guide](#) as needed.

## Language Localization

The security appliance provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, screens associated with optional plug-ins, and the interface displayed to Cisco AnyConnect VPN Client users.

This section describes how to configure the security appliance to translate these user messages and includes the following sections:

- [Understanding Language Translation, page 38-76](#)
- [Creating a Translation Table, page 38-77](#)
- [Add/Edit Localization Entry, page 38-78](#)
- [Import/Export Language Localization, page 38-81](#)

### Understanding Language Translation

Each functional area and its messages that are visible to remote users are organized into translation domains. shows the translation domains and the functional areas translated.

**Table 38-1 Translation Domains and Functional Areas Affected**

| Translation Domain   | Functional Areas Translated   |
|----------------------|---|
| <b>AnyConnect</b>    | Messages displayed on the user interface of the Cisco AnyConnect VPN Client.                        |
| <b>CSD</b>           | Messages for the Cisco Secure Desktop (CSD).  |
| <b>customization</b> | Messages on the logon and logout pages, portal page, and all the messages customizable by the user. |
| <b>keepout</b>       | Message displayed to remote users when VPN access is denied.  |
| <b>PortForwarder</b> | Messages displayed to Port Forwarding users.  |
| <b>url-list</b>      | Text that user specifies for URL bookmarks on the portal page.                                      |
| <b>webvpn</b>        | All the layer 7, AAA and portal messages that are not customizable.                                 |
| <b>plugin-ica</b>    | Messages for the Citrix plug-in.  |
| <b>plugin-rdp</b>    | Messages for the Remote Desktop Protocol plug-in.   |

Table 38-1 Translation Domains and Functional Areas Affected

| Translation Domain       | Functional Areas Translated              |
|--------------------------|--|
| <b>plugin-telnet,ssh</b> | Messages for the Telnet and SSH plug-in. |
| <b>plugin-vnc</b>        | Messages for the VNC plug-in.            |

The software image package for the security appliance includes a language localization template for each domain that is part of the standard functionality. The templates for plug-ins are included with the plug-ins and define their own translation domains.

You can export the template for a translation domain, which creates an XML file of the template at the URL you provide. The message fields are empty in this file. You can customize the messages and import the template to create a new language localization table that resides in flash memory.

You can also export an existing language localization table. The XML file created displays the messages you edited previously. Reimporting this XML file with the same language name creates a new version of the language localization table, overwriting previous messages.

Some templates are static, but some change based on the configuration of the security appliance. Because you can customize the *logon and logout pages, portal page, and URL bookmarks for clientless sessions*, the **security appliance generates the customization and url-list** translation domain templates dynamically and the template automatically reflects your changes to these functional areas.

After creating language localization tables, they are available to customization objects that you create and apply to group policies or user attributes. A language localization table has no affect and messages are not translated on user screens until you create the customization object, identify a language localization table to use in that object, and specify the customization for the group policy or user.

#### Fields

**Add**—Launches the Add Localization Entry dialog where you can select a localization template to add and you can edit the contents of the template.

**Edit**—Launches the Edit Localization Entry dialog for the selected language in the table, and allows you to edit the previously-imported language localization table.

**Delete**—Deletes a selected language localization table.

**Import**—Launches the Import Language Localization dialog where you can import a language localization template or table.

**Export**—Launches the Export Language Localization dialog where you can export a language localization template or table to a URL where you can make changes to the table or template.

**Language**—The language of existing Language Localization tables.

**Language Localization Template**—The template that the table is based on.

### Creating a Translation Table

The following procedure describes how to create a translation table:

- Step 1** Go to **Remove Access VPN > Clientless SSL VPN Access > Portal > Advanced > Language Localization**. The Language Localization pane displays. Click **Add**. The Add Language Localization window displays.
- Step 2** Select a Language Localization Template from the drop-down box. The entries in the box correspond to functional areas that are translated. For more information about the functionality for each template, see table [Table 38-7](#).
- Step 3** Specify a language for the template. The template becomes a translation table in cache memory with the name you specify. Use an abbreviation that is compatible with the language options for your browser. For example, if you are creating a table for the Chinese language, and you are using IE, use the abbreviation *zh*, that is recognized by IE.
- Step 4** Edit the translation table. For each message represented by the msgid field that you want to translate, enter the translated text between the quotes of the associated msgstr field. The example below shows the message Connected, with the Spanish text in the msgstr field:
- ```
msgid "Connected"
msgstr "Conectado"
```
- Step 5** Click **OK**. The new table appears in the list of translation tables.

### 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 Localization Entry

You can add a new translation table, based on a template, or you can modify an already-imported translation table from this pane.

### Fields

**Language Localization Template**—Select a template to modify and use as a basis for a new translation table. The templates are organized into translation domains and affect certain areas of functionality. The following table shows the translation domains and the functional areas affected:

| Translation Domain   | Functional Areas Translated                                                                         |
|----------------------|-----------------------------------------------------------------------------------------------------|
| <b>AnyConnect</b>    | Messages displayed on the user interface of the Cisco AnyConnect VPN Client.                        |
| <b>CSD</b>           | Messages for the Cisco Secure Desktop (CSD).                                                        |
| <b>customization</b> | Messages on the logon and logout pages, portal page, and all the messages customizable by the user. |
| <b>keepout</b>       | Message displayed to remote users when VPN access is denied.                                        |
| <b>PortForwarder</b> | Messages displayed to Port Forwarding users.                                                        |
| <b>url-list</b>      | Text that user specifies for URL bookmarks on the portal page.                                      |

| Translation Domain | Functional Areas Translated                                         |
|--------------------|---------------------------------------------------------------------|
| webvpn             | All the layer 7, AAA and portal messages that are not customizable. |
| plugin-ica         | Messages for the Citrix plug-in.                                    |
| plugin-rdp         | Messages for the Remote Desktop Protocol plug-in.                   |
| plugin-telnet,ssh  | Messages for the Telnet and SSH plug-in.                            |
| plugin-vnc         | Messages for the VNC plug-in.                                       |

**Language**—Specify a language. Use an abbreviation that is compatible with the language options of your browser. The security appliance creates the new translation table with this name.

**Text Editor**—Use the editor to change the message translations. The message ID field (msgid) contains the default translation. The message string field (msgstr) that follows msgid provides the translation. To create a translation, enter the translated text between the quotes of the msgstr string. For example, to translate the message “Connected” with a Spanish translation, insert the Spanish text between the msgstr quotes:

```
msgid "Connected"
msgstr "Conectado"
```

After making changes, click **Apply** to import the translation table.

### Modes

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

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

# AnyConnect Customization

## Resources

Specify resource files that customize or re-brand the AnyConnect VPN client in this panel.



### Note

The security appliance does not support this feature for the AnyConnect VPN client, versions 2.0 and 2.1. For more information on manually customizing the client, see the AnyConnect VPN Client Administrator’s Guide and the release notes for the AnyConnect VPN Client.

### Fields

**Import**—Launches the Import AnyConnect Customization Objects dialog, where you can specify a file to import as an object.

**Export**—Launches the Export AnyConnect Customization Objects dialog, where you can specify a file to export as an object.

Delete—Removes the selected object.

Platform—The type of remote PC platform supported by the object.

Object Name—The name of the object.

#### Modes

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

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

## Binary

Specify third-party programs that use the AnyConnect VPN client API in this panel. The security appliance downloads these programs to the client for customizing the user interface or the command line interface.



#### Note

The security appliance does not support this feature for the AnyConnect VPN client, versions 2.0 and 2.1. For more information on manually customizing the client, see the AnyConnect VPN Client Administrator's Guide and the release notes for the AnyConnect VPN Client.

#### Fields

Import—Launches the Import AnyConnect Customization Objects dialog, where you can specify a file to import as an object.

Export—Launches the Export AnyConnect Customization Objects dialog, where you can specify a file to export as an object.

Delete—Removes the selected object.

Platform—The type of remote PC platform supported by the object.

Object Name—The name of the object.

#### Modes

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

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

## Installs

Specify files for customizing the AnyConnect client installation in this panel.

**Note**

The security appliance does not support this feature for the AnyConnect VPN client, versions 2.0 and 2.1. For more information on manually customizing the client, see the AnyConnect VPN Client Administrator's Guide and the release notes for the AnyConnect VPN Client.

**Fields**

**Import**—Launches the Import AnyConnect Customization Objects dialog, where you can specify a file to import as an object.

**Export**—Launches the Export AnyConnect Customization Objects dialog, where you can specify a file to export as an object.

**Delete**—Removes the selected object.

**Platform**—The type of remote PC platform supported by the object.

**Object Name**—The name of the object.

**Modes**

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

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

## Import/Export Language Localization

In the Import Translation Table and Export Translation Table windows you can import or export a translation table to the security appliance to provide translation of user messages.

Translation templates are XML files that contain message fields that can be edited with translated messages. You can export a template, edit the message fields, and import the template as a new translation table, or you can export an existing translation table, edit the message fields, and re-import the table to overwrite the previous version.

**Fields**

- **Language**—Enter a name for the language.

When *exporting*, it is automatically filled-in with the name from the entry you selected in the table.

When *importing*, you enter the language name in the manner that you want it to be identified. The imported translation table then appears in the list with the abbreviation you designated. To ensure that your browser recognizes the language, use language abbreviations that are compatible with the language options of the browser. For example, if you are using IE, use **zh** as the abbreviation for the Chinese language.

- **Localization Template Name**—The name of the XML file containing the message fields. The following templates are available:
  - AnyConnect—Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
  - CSD—Messages for the Cisco Secure Desktop (CSD).

- customization—Messages on the logon and logout pages, portal page, and all the messages customizable by the user.
- keepout—Message displayed to remote users when VPN access is denied.
- PortForwarder—Messages displayed to Port Forwarding users.
- url-list—Text that user specifies for URL bookmarks on the portal page.
- webvpn—All the layer 7, AAA and portal messages that are not customizable.
- plugin-ica—Messages for the Citrix plug-in.
- plugin-rdp—Messages for the Remote Desktop Protocol plug-in.
- plugin-telnet,ssh—Messages for the TELNET and SSH plug-in.
- plugin-vnc—Messages for the VNC plug-in.
- **Select a file**—Choose the method by which you want to import or export the file.
  - Remote server—Select this option to import a customization file that resides on a remote server accessible from the security appliance.
  - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
  - Flash file system—Choose this method to export a file that resides on the security appliance.
  - Path—Provide the path to the file.
  - Browse Flash—Browse to the path for the file.
  - Local computer—Choose this method to import a file that resides on the local PC.
  - Path—Provide the path to the file.
  - Browse Local Files—Browse to the path for the file.
- Import/Export Now—Click to import or export the file.

### Modes

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

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

## Configure Bookmarks

The Bookmarks panel lets you add, edit, delete, import, and export bookmark lists.

Use the Bookmarks panel to configure lists of servers and URLs for access over clientless SSL VPN. Following the configuration of a bookmark list, you can assign the list to one or more policies – group policies, dynamic access policies, or both. Each policy can have only one bookmark list. The list names populate a drop-down list on the URL Lists tab of each DAP.

**Caution**

Configuring bookmarks does not prevent the user from visiting fraudulent sites or sites that violate your company's acceptable use policy. In addition to assigning a bookmark list to the group policy, dynamic access policy, or both, apply a web ACL to these policies to control access to traffic flows. Disable URL Entry on these policies to prevent user confusion over what is accessible. See [Security Precautions, page 38-1](#) for instructions.

**Fields**

- Bookmarks—Displays the existing bookmark lists.
- Add—Click to add a new bookmark list.
- Edit—Click to edit the selected bookmark list.
- Delete—Click to delete the selected bookmark list.
- Import—Click to import a bookmark list.
- Export—Click to export a bookmark list.

**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 Bookmark List

The Add/Edit Bookmark List dialog box configure lists of servers and URLs for access over lets you add, edit, or delete a URL list, and also order the items in a designated URL list.

**Fields**

- Bookmark List Name—Specifies the name of the list to be added or selects the name of the list to be modified or deleted.
- Bookmark Title—Specifies the URL name displayed to the user.
- URL—Specifies the actual URL associated with the display name.
- Add—Opens the Add Bookmark Entry dialog box, on which you can configure a new server or URL and display name.
- Edit—Opens the Edit Bookmark Entry dialog box, on which you can configure a new server or URL and display name.
- Delete—Removes the selected item from the URL list. There is no confirmation or undo.
- Move Up/Move Down—Changes the position of the selected item in the URL list.

**Modes**

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

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

## Add Bookmark Entry

The Add Bookmark Entry dialog box lets you create a link or bookmark for a URL list.

### Fields

- **Bookmark Title**—Enter a name for the bookmark to display for the user.
- **URL (drop-down)**—Use the pull-down menu to select the URL type: http, https, cifs, or ftp. The URL types of all imported plug-ins also populate this menu. Select the URL type of a plug-in if you want to display the plug-in as a link on the portal page.
- **URL (text box)**—Enter the DNS name or IP address for the bookmark. For a plug-in, enter the name of the server. Enter a forward slash and a question mark (/?) after the server name to specify optional parameters, then use an ampersand to separate parameter-value pairs, as shown in the following syntax:

*server/?Parameter=Value&Parameter=Value*

For example:

*host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768*

The particular plug-in determines the optional parameter-value pairs that you can enter.

To provide single sign-on support for a plug-in, use the parameter-value pair **cscs\_sso=1**. For example:

*host/?cscs\_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768*



**Note** To access `\\server\share\subfolder\personal` folder, the user must have list permission for all points above `personal` folder.

- **Subtitle**—Provide additional user-visible text that describes the bookmark entry.
- **Thumbnail**—Use the pull-down menu to select an icon to associate with the bookmark on the end-user portal.
- **Manage**—Click to import or export images to use as thumbnails.
- **Enable Smart Tunnel**—Check to open the bookmark in a new window that uses the smart tunnel feature to pass data through the security appliance to or from the destination server. This option lets you provide smart tunnel support for a browser-based application, whereas the Smart Tunnels option, also in the Clientless SSL VPN > Portal menu, lets you add nonbrowser-based applications to a smart tunnel list for assignment to group policies and usernames.
- **Allow the users to bookmark the link**—Check to let clientless SSL VPN users use the Bookmarks or Favorites options on their browsers. Uncheck to prevent access to these options. By unchecking this option, the bookmark does not appear in the Home section of the WebVPN portal.
- **Advanced Options**—(Optional) Open to configure further bookmark characteristics.

- URL Method—Select Get for simple data retrieval. Choose Post when processing the data might involve changes to it, for example, storing or updating data, ordering a product, or sending e-mail.
- Post Parameters—Configure the particulars of the Post URL method.
- Add/Edit—Click to add a post parameter.
- Edit—Click to edit the highlighted post parameter.
- Delete—Click to delete the highlighted post parameter.

### Modes

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

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

## Import/Export Bookmark List

You can import or export already configured bookmark lists. Import lists that are ready to use. Export lists to modify or edit them, and then reimport.

### Fields

- Bookmark List Name—Identify the list by name. Maximum 64 characters, no spaces.
- Select a file—Choose the method by which you want to import or export the list file.
  - Local computer—Select to import a file that resides on the local PC.
  - Flash file system—Select to export a file that resides on the security appliance.
  - Remote server—Select to import a url list file that resides on a remote server accessible from the security appliance.
  - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
  - Browse Local Files/Browse Flash—Browse to the path for the file.
- Import/Export Now—Click to import or export the list file.

### Modes

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

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

## Configure GUI Customization Objects (Web Contents)

This dialogue box lets you import and export web content objects.

### Fields

- File Name—Displays the names of the web content objects.
- File Type—Identifies the file type(s).
- Import/Export—Click to import or export a web content object.
- Delete—Click to delete the object.

## Import/Export Web Content

Web contents can range from a wholly configured home page to icons or images you want to use when you customize the end user portal. You can import or export already configured web contents. Import web contents that are ready for use. Export web contents to modify or edit them, and then reimport.

### Fields

- Source—Choose the location from which you want to import or export the file.
  - Local computer—Select to import or export a file that resides on the local PC.
  - Flash file system—Select to import or export a file that resides on the security appliance.
  - Remote server—Select to import a file that resides on a remote server accessible from the security appliance.
  - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
  - Browse Local Files.../Browse Flash...—Browse to the path for the file.
- Destination
  - Require authentication to access its content? Click Yes or No.
  - WebContent Path: Notice that the prefix to the path changes depending on whether you require authentication. The security appliance uses `/+CSCOE+/` for objects that require authentication, and `/+CSCOU+/` for objects that do not. The security appliance displays `/+CSCOE+/` objects on the portal page only, while `/+CSCOU+/` objects are visible and usable in either the logon or the portal pages.
- Import/Export Now—Click to import or export the file.

### 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 Post Parameter

Use this pane to configure post parameters for bookmark entries and URL lists.

Since these are often personalized resources that contain the user ID and password or other input parameters, you might need to define [Clientless SSL VPN Macro Substitutions](#). Click the link for detailed instructions.

### Fields

- Name, Value—Provide the name and value of the parameters exactly as in the corresponding HTML form, for example: `<input name="param_name" value="param_value">`.

### Modes

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

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

## Clientless SSL VPN Macro Substitutions

Clientless SSL VPN macro substitutions let you configure users for access to personalized resources that contain the user ID and password or other input parameters. Examples of such resources include bookmark entries, URL lists, and file shares.



### Note

For security reasons, password substitutions are disabled for file access URLs (`cifs://`).

Also for security reasons, use caution when introducing password substitutions for web links, especially for non-SSL instances.

We support the following macro substitutions:

| No. | Macro Substitution             | Definition                                                                      |
|-----|--------------------------------|---------------------------------------------------------------------------------|
| 1   | CSCO_WEBVPN_USERNAME           | SSL VPN user login ID                                                           |
| 2   | CSCO_WEBVPN_PASSWORD           | SSL VPN user login password                                                     |
| 3   | CSCO_WEBVPN_INTERNAL_PASSWORD  | SSL VPN user internal resource password                                         |
| 4   | CSCO_WEBVPN_CONNECTION_PROFILE | SSL VPN user login group drop-down, a group alias within the connection profile |
| 5   | CSCO_WEBVPN_MACRO1             | Set via RADIUS/LDAP vendor-specific attribute                                   |
| 6   | CSCO_WEBVPN_MACRO2             | Set via RADIUS/LDAP vendor-specific attribute                                   |

## Using Macros 1 - 4

The security appliance obtains values for the first four substitutions from the SSL VPN Login page, which includes fields for username, password, internal password (optional), and group. It recognizes these strings in user requests, and replaces them with the value specific to the user before it passes the request on to a remote server.

For example, if a URL list contains the link, [http://someserver/homepage/CSCO\\_WEBVPN\\_USERNAME.html](http://someserver/homepage/CSCO_WEBVPN_USERNAME.html), the security appliance translates it to the following unique links:

- For USER1 the link becomes <http://someserver/homepage/USER1.html>
- For USER2 the link is <http://someserver/homepage/USER2.html>

In the following case, [cifs://server/users/CSCO\\_WEBVPN\\_USERNAME](cifs://server/users/CSCO_WEBVPN_USERNAME), lets the security appliance map a file drive to specific users:

- For USER1 the link becomes <cifs://server/users/USER1>
- For USER2 the link is <cifs://server/users/USER2>

## Using Macros 5 and 6

Values for macros 5 and 6 are RADIUS or LDAP vendor-specific attributes (VSAs). These substitutions let you set substitutions configured on either a RADIUS or an LDAP server.

### Example 1: Setting a Homepage

The following example sets a URL for the homepage:

- WebVPN-Macro-Value1 (ID=223), type string, is returned as *wwwin-portal.abc.com*
- WebVPN-Macro-Value2 (ID=224), type string, returned as *401k.com*

To set a home page value, you would configure the macro as

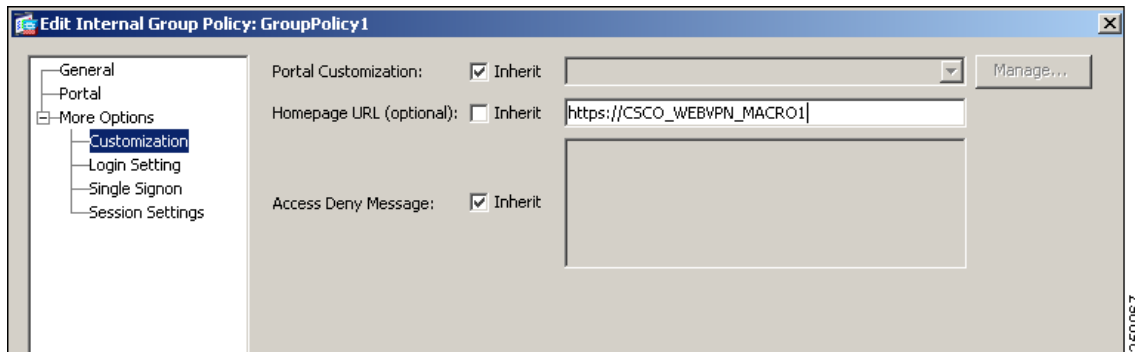
[https://CSCO\\_WEBVPN\\_MACRO1](https://CSCO_WEBVPN_MACRO1), which would translate to <https://wwwin-portal.abc.com>.

The best way to do this is to configure the Homepage URL parameter in ASDM.

Go to the Add/Edit Group Policy pane, from either the Network Client SSL VPN or Clientless SSL VPN Access section of ASDM, as in [Figure 38-2](#). The paths are as follows:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Group Policy > Advanced > SSL VPN Client > Customization > Homepage URL attribute.
- Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add/Edit Group Policy > More Options > Customization > Homepage URL attribute.

Figure 38-2 Using ASDM to Configure a Macro that Sets a Homepage



### Example 2: Setting a Bookmark or URL Entry

You can use an HTTP Post to log in to an OWA resource using an RSA one-time password (OTP) for SSL VPN authentication, and then the static, internal password for OWA e-mail access. The best way to do this is to add or edit a bookmark entry in ASDM, as in Figure 38-3.

There are several paths to the Add Bookmark Entry pane, including the following:

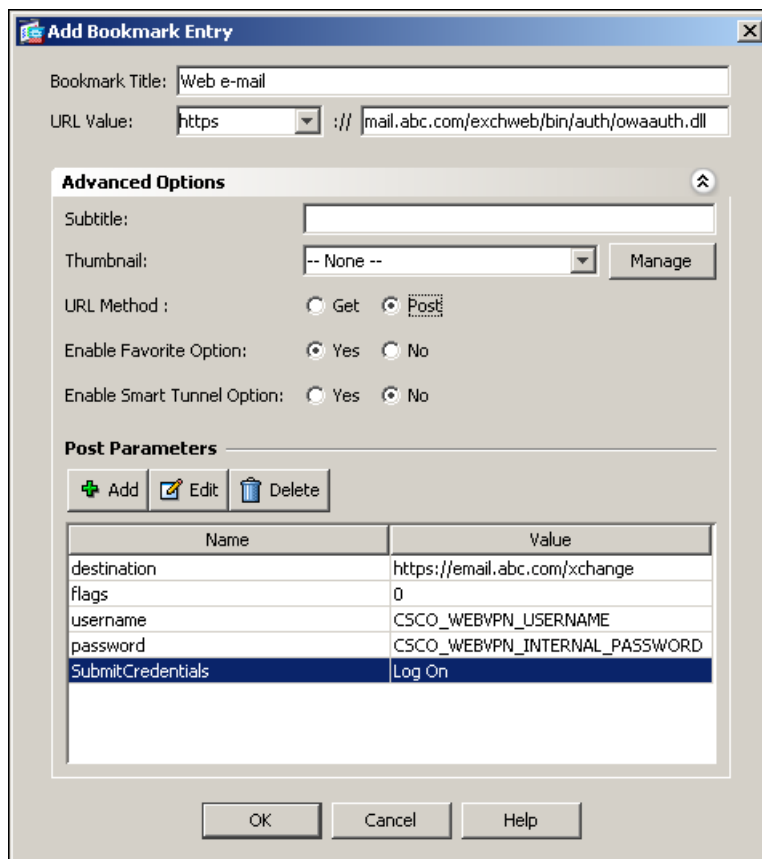
- Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add/Edit Bookmark Lists > Add/Edit Bookmark Entry > Advanced Options area > Add/Edit Post Parameters (available after you click **Post** in the URL Method attribute).

*or*

(Available after you click **Post** in the URL Method attribute):

- Network (Client) Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > URL Lists tab > Manage button > Configured GUI Customization Objects > Add/Edit button > Add/Edit Bookmark List > Add/Edit Bookmark Entry > Advanced Options area > Add/Edit Post Parameters.

Figure 38-3 Configuring a Bookmark Entry



250066