



Clientless SSL VPN

Clientless SSL VPN lets users establish a secure, remote-access VPN tunnel to the adaptive 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 adaptive 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 [Customizing the Clientless SSL VPN User Experience](#).

Security Precautions

Clientless SSL VPN connections on the adaptive 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 adaptive 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 adaptive 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 adaptive security appliance does not permit communication with sites that present expired certificates. Nor does the adaptive 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.

By default, the adaptive security appliance permits all portal traffic to all web resources (e.g., HTTPS, CIFS, RDP, and plug-ins). The adaptive security appliance clientless service rewrites each URL to one that is meaningful only to the adaptive security appliance; the user cannot use the rewritten URL displayed on the page accessed to confirm that they are on the site they requested (see example Figures 68-1 and 68-2).

Figure 68-1 Example URL Typed by User

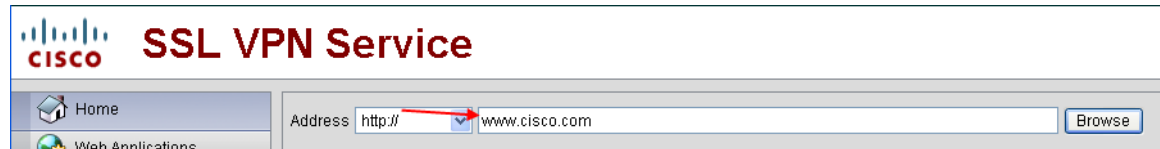
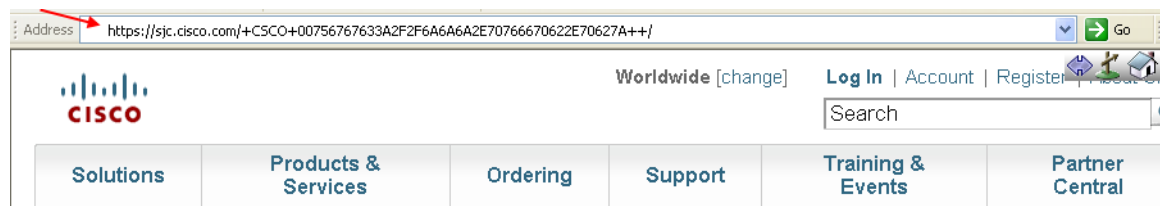


Figure 68-2 Same URL Rewritten by Security Appliance and displayed on the Browser Window



Caution

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. The procedure that follows steps you through the recommendations in this statement.

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. To assign a web ACL to a DAP, edit the DAP record, and select the web ACL on the **Network ACL Filters** tab.
- Step 3** Disable URL entry on the *portal page*, the page that opens upon the establishment of 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

Release 8.3(1) supports browser-based (clientless) VPN access from the following platforms:

- Windows 7 x86 (32-bit) and x64 (64-bit) via Internet Explorer 8.x and Firefox 3.x.
- Windows Vista x64 via Internet Explorer 7.x–8.x, or Firefox 3.x.
- Windows Vista x86 SP2, or Vista SP1 with [KB952876](#) or later, via Internet Explorer 7.x, or Firefox 3.x.
- Windows XP x64 via Internet Explorer 7.x–8.x and Firefox 3.x.
- Windows XP x86 SP2 or later via Internet Explorer 6.x–8.x, or Firefox 3.x.
- Mac OS 10.6.x or 10.5 32- and 64-bit via Safari 3.x–4.x and Firefox 3.x with Sun JRE 1.5 or later. Certificate authentication, including the DoD Common Access Card and SmartCard, works with the Safari keychain only.
- Linux via Firefox 3.x

ActiveX pages require that you enable ActiveX Relay 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.

The ASA supports clientless access to Lotus iNotes 8.5.

The ASA does not support clientless access to Web Folders from Windows 7, Vista, Internet Explorer 8, Mac OS, and Linux. Windows XP SP2 requires a [Microsoft hotfix](#) to support Web Folders.

The ASA does not support DSA certificates; it does support RSA certificates.

See the following sections for the platforms supported by these clientless applications:

- [Port Forwarding Requirements and Restrictions, page 68-23](#)
- [Smart Tunnel Requirements and Limitations, page 68-35](#)
- [Plug-in Requirements and Restrictions, page 68-77](#)

Clientless SSL VPN Access

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

- Enable or disable adaptive 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 adaptive security appliance memory that clientless SSL VPN can use.

To configure clientless SSL VPN services for individual users, the best practice is to choose the **Configuration > VPN > General > Group Policy > Add/Edit > WebVPN** pane. Then choose the **Configuration > Properties > Device Administration > User Accounts > VPN Policy** pane 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 adaptive 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 adaptive 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—Click 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

[Customizing the Clientless SSL VPN User Experience](#)

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 adaptive 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 ACE (access control entry), the adaptive 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 adaptive 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 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.

For information about access rules and ACLs (including IPv6), see the [“Information About Access Rules” section on page 31-1](#).

For information about configuring access rules and ACLs (including IPv6), see [“Configuring Access Rules” section on page 31-7](#).

For information about EtherType access rules and ACLs, see the [“Configuring Access Rules” section on page 31-7](#).

Fields

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

Add/Edit ACE

An Access Control Entry (or “access rule”) 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.

For information about access rules (including IPv6), see the [“Information About Access Rules” section on page 31-1](#).

For information about configuring access rules (including IPv6), see the [“Configuring Access Rules” section on page 31-7](#).

Fields

- Action—Permits or denies access to the specific networks, subnets, hosts, and web servers specified in the Filter group field.
- 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 field.
 - 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 field.

- 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 field.
- 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 adaptive 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 adaptive 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 adaptive 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 adaptive 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, click **Enable Secure Desktop**.

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



Note If you click **Browse Flash** 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**.

If you click this button, the Uninstall Cisco Secure Desktop dialog window asks if you want to delete the Cisco Secure Desktop image that was named in the “Secure Desktop Image field” and all Cisco Secure Desktop data files (including the entire Cisco Secure Desktop configuration) from the flash device. Click **Yes** if you want to remove these files from both the running configuration and the flash device, or click **No** to remove them from the running configuration, but retain them on the flash device.

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—Click 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 adaptive 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 choose the path of the `securedesktop_asa_<n>_<n>*.pkg` file to be transferred, click **Browse Local Files**. 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 box removes the contents of the Local File Path and Flash File System Path fields.
- To close the Upload Image dialog box, 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 Secure Desktop Image 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 adaptive 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 adaptive security appliance handle non-standard applications and web resources so they display correctly over a clientless SSL VPN connection. An ACPF 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.

Cisco TAC may help with ACPF to address specific rendering issues if the smart tunneling feature is not working or cannot be used.

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

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

Fields

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

Add/Edit APCF Profile

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

Fields

- **Flash file**—Click to locate an APCF file stored on the adaptive 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 pane 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 **Refresh**.

- **Upload** —Click to upload an APCF file from a local computer to the adaptive security appliance flash file system. The Upload APCF package pane displays.
- **URL**—Click 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, choose it, and click **Open**. ASDM inserts the file path into the Local File Path field.
- **Flash File System Path**—Displays the path on the adaptive security appliance to upload the APCF file.
- **Browse Flash**—Click to identify the location on the adaptive 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 adaptive 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 **Close**.
- **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 adaptive security appliance uses cookies to interact with applications such as Microsoft Word on the endpoint. The cookie expiration time set by the adaptive security appliance can cause Word to malfunction when accessing documents on a SharePoint server if the time on the adaptive security appliance is incorrect. To prevent this malfunction, set the ASA clock properly. We recommend configuring the adaptive security appliance to dynamically synchronize with NTP services. For instructions, see the [“Clock Accuracy for SharePoint Access”](#) section on page 68-12.

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 adaptive security appliance passes the login credentials that the user of clientless SSL VPN entered to log in to the adaptive security appliance (username and password) to those particular internal servers. You configure the adaptive security appliance to respond to a specific authentication method for a

particular range of servers. The authentication methods you can configure the adaptive 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 adaptive 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 adaptive security appliance. When auto signon is enabled, the adaptive security appliance passes on the login credentials that the user entered to log into the adaptive 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—From the subnet mask menu, choose 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 adaptive 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 (for example, HTTP Basic) and one of those servers attempts to authenticate with a different method (for example, NTLM), the adaptive 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—Click 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 adaptive 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**—Choose one of the following options from the drop-down menu to specify the objects the server uses in association with the user. The adaptive 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.

Choose a Java Code Signer from the drop down list.

To configure a Java Code Signer, choose **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**—Click to enable caching. The default value is disable.

- Parameters—Lets you define the terms for caching.
 - Enable caching of compressed content—Click to cache compressed content. When you disable this parameter, the adaptive security appliance stores objects before it compresses them.
 - Maximum Object Size—Enter the maximum size in KB of a document that the adaptive security appliance can cache. The adaptive 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 adaptive security appliance can cache. The adaptive 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 adaptive 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 adaptive 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 adaptive security appliance. The adaptive security appliance therefore lets you create rewrite rules that let users browse certain sites and applications without going through the adaptive 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

Table 68-1

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, choose **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 pane 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 0s and 1s) 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 adaptive 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 choose one of the options from 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 click **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 adaptive 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 box lets you maintain exceptions to the “Global Encoding Type” attribute setting in the Add CIFS Encoding window. That pane 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 adaptive 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 choose 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 click **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 adaptive 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 adaptive 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 ACEs (access control entries) 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 adaptive 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 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, choose 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, choose 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, choose 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 choose it and click **Edit**.

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

The relative position of an ACE in an ACL determines the sequence with which the adaptive 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, choose it and click the up or down icon above the table.
- To move an ACE, choose 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 dialog box opens, providing you with an opportunity to change the values. Click **OK**.

- To copy an ACE, choose it and click the double-page icon above the table. Choose 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 dialog box 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
•	—	•	—	—

Configuring 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 adaptive 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 adaptive 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.

- The port forwarding applet displays the local port and the remote port as the same when the local IP address 127.0.0.1 is being used and cannot be updated by the clientless SSL VPN connection from the ASA. As a result, the ASA creates new IP addresses 127.0.0.2, 127.0.0.3, and so on for local proxy IDs. Because you can modify the hosts file and use different loopbacks, the remote port is used as the local port in the applet. To connect, you can use Telnet with the host name, without specifying the port. The correct local IP addresses are available in the local hosts file.

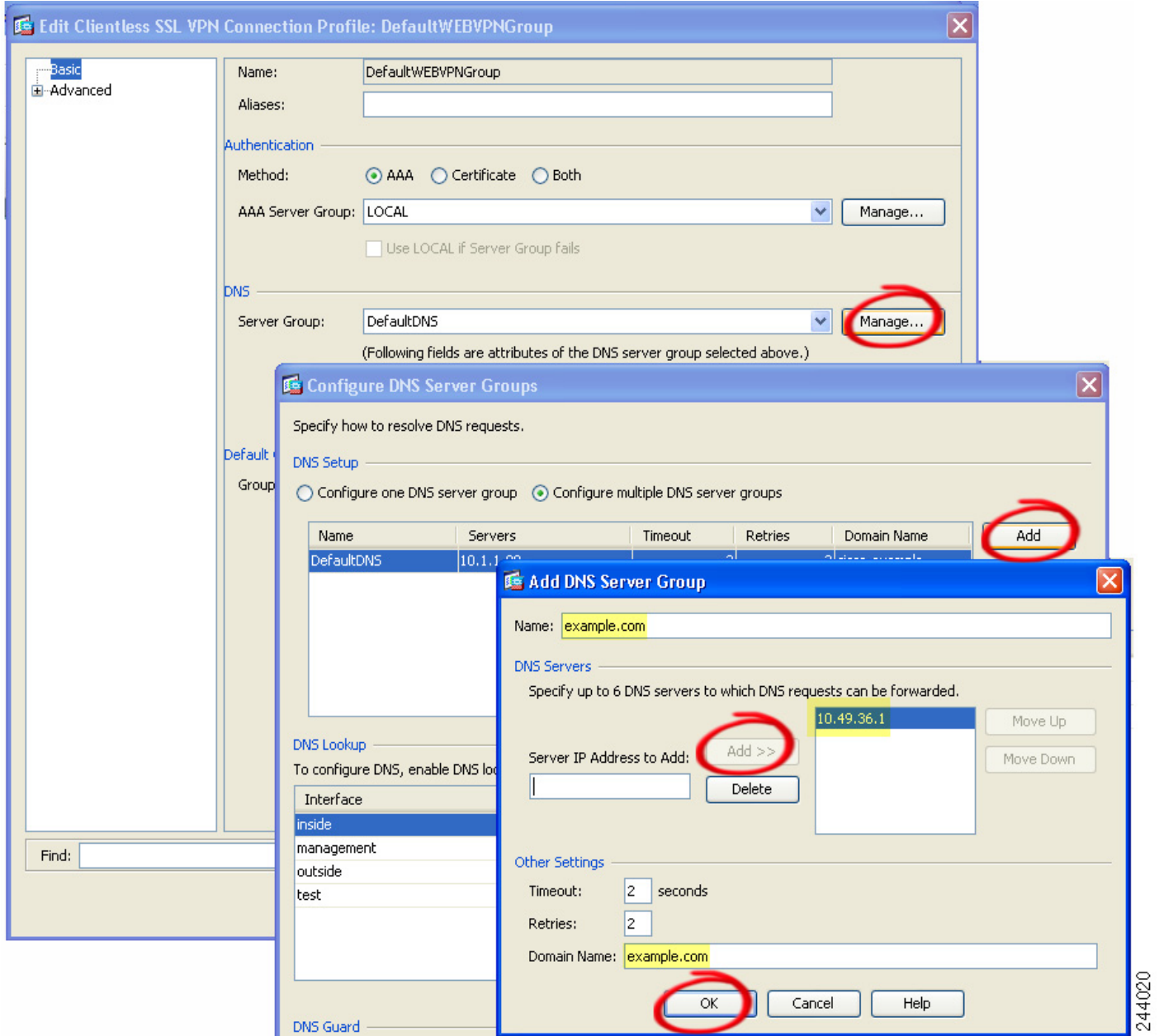
Configuring DNS for Port Forwarding

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 adaptive 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 68-3](#))

Figure 68-3 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**.

244020

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 [Add/Edit Port Forwarding List, page 68-26](#). 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 adaptive 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 choose 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 adaptive 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 adaptive 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 adaptive 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 pane lets you set rules for when the adaptive 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 adaptive 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) Click 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
•	—	•	—	—

SSO Servers

The SSO Server pane 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.

The following sections describe the procedures for setting up SSO with both SiteMinder and SAML Browser Post Profile.

- [Auto Signon](#)—configures SSO with basic HTTP or NTLM authentication.
- [Configuring Session Settings](#) —configures SSO with the HTTP Form protocol.

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 adaptive 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 adaptive 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 adaptive 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 adaptive 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 adaptive 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 adaptive 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. To configure the SAML Server for Browser Post Profile, perform the following steps:

-
- Step 1** Configure the SAML server parameters to represent the asserting party (the adaptive 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 adaptive 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 steps:

-
- 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 adaptive 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 adaptive security appliance are SiteMinder and SAML Browser Post Profile.
- **URL**—Enter the SSO server URL to which the adaptive 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 adaptive 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 adaptive 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
•	—	•	—	—

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 operating system. 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. You can also specify which group policy homepage can use smart tunnel (with the use-smart-tunnel CLI command or on the Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Edit Internal Group Policy of the GUI). Following the configuration of a list, you can assign it to one or more group policies or local user policies. The internal company resources are accessed through the VPN gateway, but smart tunnel allows direct Internet access without going through the VPN gateway.

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**.
- To specify logoff procedures for a VPN session, choose one of the following options:
 - If you enable the **Click on smart-tunnel logoff icon in the system tray** radio button, a notification icon appears in the system tray when smart tunnel is started. You can use the icon to log off a VPN session. If you select this option, the VPN session persists even when all browser windows have been closed. This option enables you to gain clientless SSL VPN access from a browser, start an application (such as terminal service client), and then close the browser.
 - If the **Logoff smart-tunnel when its parent process, such as a browser, terminates** radio button is enabled, you are logged off after all browser windows have been closed.

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 (Portal > Bookmarks). You can create a bookmark independent of whether you created a smart tunnel application list (as long as your bookmark page does not use a non-browser application such as JAVA).

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 adaptive 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:

- 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 adaptive 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 adaptive security appliance by default passes all browser traffic through the VPN session if the browser process is the same. The adaptive 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.
- If it takes too long for smart tunnel to load, perform the following:
 - Clear the SSL state (with Internet Explorer, go to **Tools > Internet Options > Content**).
 - Disable the **Check for server certificate revocation** check box (with Internet Explorer, go to **Tools > Internet Options > Advanced > Security**).

- Delete cookies (with Internet Explorer, go to **Tools > Internet Options > General**).

Windows Requirements and Limitations

In addition to the requirements in [Understanding Clientless SSL VPN System Requirements, page 68-3](#), the following requirements and limitations apply to smart tunnel access on Windows:

- ActiveX or Sun JRE 5, Update 1.4 or later (JRE 6 or later recommended) on Windows must be enabled on the browser.
- 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

In addition to the requirements in [Understanding Clientless SSL VPN System Requirements, page 68-3](#), the following requirements and limitations apply to smart tunnel access on Mac OS:

- Smart tunnel supports Mac OS running on an Intel processor only.
- Java Web Start must be enabled on the browser.
- 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.
- 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 68-2 shows example Application ID strings and the associated paths required to support Lotus.

Table 68-2 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	nnotes.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.

Simplifying Configuration of Which Applications to Tunnel

A smart tunnel application list is essentially a filter of what applications are granted access to the tunnel. The default is to allow access for all processes started by the browser. With Smart Tunnel enabled bookmark, the clientless session grants access only to processes initiated by the web browser. For non-browser applications, an administrator can choose to tunnel all applications and thus remove the need to know which applications an end user may invoke. Table 68-3 shows in which situations processes are granted access.

Table 68-3 Access for Smart Tunnel Applications and Enabled Bookmarks

	Smart Tunnel Enabled Bookmark	Smart Tunnel Application Access
Application list specified	Any processes that match a process name in the application list are granted access.	Only processes that match a process name in the application list are granted access.
Smart tunnel is disabled	All processes (and their child processes) are granted access.	No process is granted access.
Smart Tunnel all Applications check box is checked	All processes (and their child processes) are granted access. Note This includes processes initiated by non-Smart Tunnel web pages if the web page is served by the same browser process.	All processes owned by the user who started the browser are granted access but not child processes of those original processes.



Note This configuration is applicable to Windows platforms only.

Follow these steps to configure tunnel policy.

- Step 1** Choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**.
- Step 2** In the User Account window, highlight the username that you want to edit.
- Step 3** Click **Edit**. The Edit User Account window appears.
- Step 4** In the left sidebar of the Edit User Account window, click **VPN Policy > Clientless SSL VPN**.
- Step 5** Perform one of the following:
 - Check the **smart_tunnel_all_applications** check box. All applications will be tunneled without making a list or knowing which executables an end user may invoke for external applications.
 - Or choose from the following tunnel policy options:
 - Uncheck the **Inherit** check box at the Smart Tunnel Policy parameter.
 - Choose from the network list and specify one of the tunnel options: use smart tunnel for the specified network, do not use smart tunnel for the specified network, or use tunnel for all network traffic.

Add or Edit Smart Tunnel List

The Add Smart Tunnel List dialog box lets you add to the security appliance configuration a list of applications that can access smart tunnel. 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. 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. This user-specified name is saved and then returned onto the GUI. The string is unique for the operating system. 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 operating system, 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 operating systems require 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 operating system 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 68-4 Example Smart Tunnel Entries

Smart Tunnel Support	Application ID (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

Table 68-4 Example Smart Tunnel Entries

Smart Tunnel Support	Application ID (Any unique string is OK.)	Process Name	OS
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 fails 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
•	—	•	—	—

Logging Off Smart Tunnel

This section describes how to ensure that the smart tunnel is properly logged off. Smart tunnel can be logged off when all browser windows have been closed, or you can right click the notification icon and confirm log out.

**Note**

We strongly recommend the use of the logout button on the portal. This method pertains to clientless SSL VPNs and logs off regardless of whether smart tunnel is used or not. The notification icon should be used only when using standalone applications without the browser.

Without Using Notification Icon

If you choose to not use the notification icon, the VPN session closes when the user quits the browser, and the end user is logged off after all browsers are closed. For example, if you started a smart tunnel from Internet Explorer, the smart tunnel is turned off when no iexplore.exe is running. Smart tunnel can determine that the VPN session has ended even if the user closed all browsers without logging out.

**Note**

In some cases, a lingering browser process is unintentional and is strictly a result of an error. Also, when a Secure Desktop is used, the browser process can run in another desktop even if the user closed all browsers within the secure desktop. Therefore, smart tunnel declares all browser instances gone when no more visible windows exist in the current desktop.

**Note**

Portal logout still takes effect and is not impacted.

See the *Cisco Security Appliance Command Reference Guide*

(http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html) for the CLI command that configures log out properties and controls whether the user is presented with a logout icon for logging out.

Using the Notification Icon

If you want the user to keep accessing the VPN, even after all browsers are closed, choose the notification icon for log off. The VPN session will not close, even when the user has quit the browser; therefore, if a user is accessing some non-browser application (such as vnc), the connectivity remains even after all browsers are closed, but logout can still occur using the notification icon. Smart Tunnel may not detect a log off event that happens outside of the browser (such as logging off with the console CLI).

The clientless portal may take awhile to detect a log off and actually exit the portal, even though the user is logged off immediately. The icon remains until the next operation that is tunneled by Smart Tunnel (such as when an application tries to create a new connection).

**Note**

This icon is an alternative way to log out of SSL VPN. It is not an indicator of VPN session status.

To enable the icon in the notification area, follow these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**.
- Step 2** Enable the **Click on smart-tunnel logoff icon in the system tray** radio button.
- Step 3** In the Smart Tunnel Networks portion of the window, check **Add** and enter both the IP address and hostname of the network which should include the icon.

**Note**

If you right click the icon, a single menu item appears which prompts the user to log out of the SSL VPN.

Customizing the Clientless SSL VPN User Experience

You can customize the clientless SSL VPN user experience, including the logon, portal, and logout pages. There are two methods you can use. You can customize pre-defined page components in the Add/Edit Customization Object window. This window adds, or makes changes to, an XML file stored on the adaptive security appliance (a customization object) that is used to customize the pages. Alternatively, you can export the XML file to a local computer or server, make changes to the XML tags, and re-import the file to the adaptive security appliance. Either method creates a customization object that you apply to a connection profile or group policy.

Rather than customizing the pre-defined components of the logon page, you can create your own page and import it to the adaptive security appliance for full customization. To do this see [Replacing the Logon Page with your own Fully Customized Page, page 68-46](#).

The following sections describe how to create a customization object:

- [Customizing the Logon Page, page 68-44](#)
- [Customizing the Portal Page, page 68-49](#)
- [Customizing the Logout Page, page 68-50](#)

Customizing the Logon Page

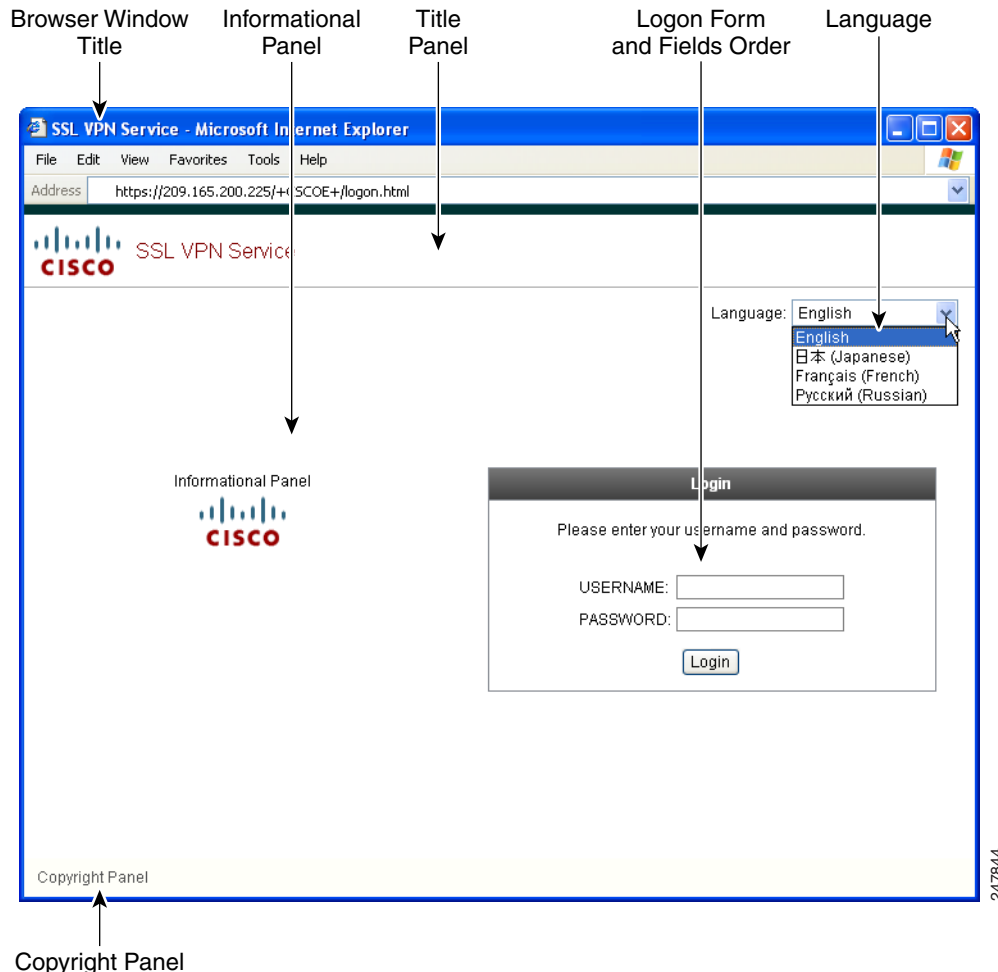
You can customize pre-defined components of the logon page, including titles, language options, and messages to users. Alternatively, you can completely replace the page with your own custom page (full customization). The following sections detail both procedures:

- [Customizing the Logon Page with the Customization Editor, page 68-45](#)
- [Replacing the Logon Page with your own Fully Customized Page, page 68-46](#)

Customizing the Logon Page with the Customization Editor

Figure 68-4 shows the logon page and the pre-defined components you can customize:

Figure 68-4 Components of Clientless Logon Page



To customize all the components of the logon page, follow this procedure. You can preview your changes for each component by clicking the Preview button:

- Step 1** Specify pre-defined customization. Go to Logon Page and select **Customize pre-defined logon page components**. Specify a title for the browser window.
- Step 2** Display and customize the title panel. Go to Logon Page > Title Panel and check **Display title panel**. Enter text to display as the title and specify a logo. Specify any font styles.
- Step 3** Specify language options to display. Go to Logon Page > Language and check **Enable Language Selector**. Add or delete any languages to display to remote users. Languages in the list require translation tables that you configure in Configuration > Remote Access VPN > Language Localization.
- Step 4** Customize the logon form. Go to Logon Page > Logon Form. Customize the text of the form and the font style in the panel. The secondary password field appears to users only if a secondary authentication server is configured in the connection profile.

- Step 5** Arrange the position of the logon form fields. Go to Logon Page > Form Fields Order. Use the up and down arrow buttons to change the order that the fields are displayed.
- Step 6** Add messages to users. Go to Logon Page > Informational Panel and check **Display informational panel**. Add text to display in the panel, change the position of the panel relative to the logon form, and specify a logo to display in this panel.
- Step 7** Display a copyright statement. Go to Logon Page > Copyright Panel and check **Display copyright panel**. Add text to display for copyright purposes.
- Step 8** Click OK, then apply the changes to the customization object you edited.

Replacing the Logon Page with your own Fully Customized Page

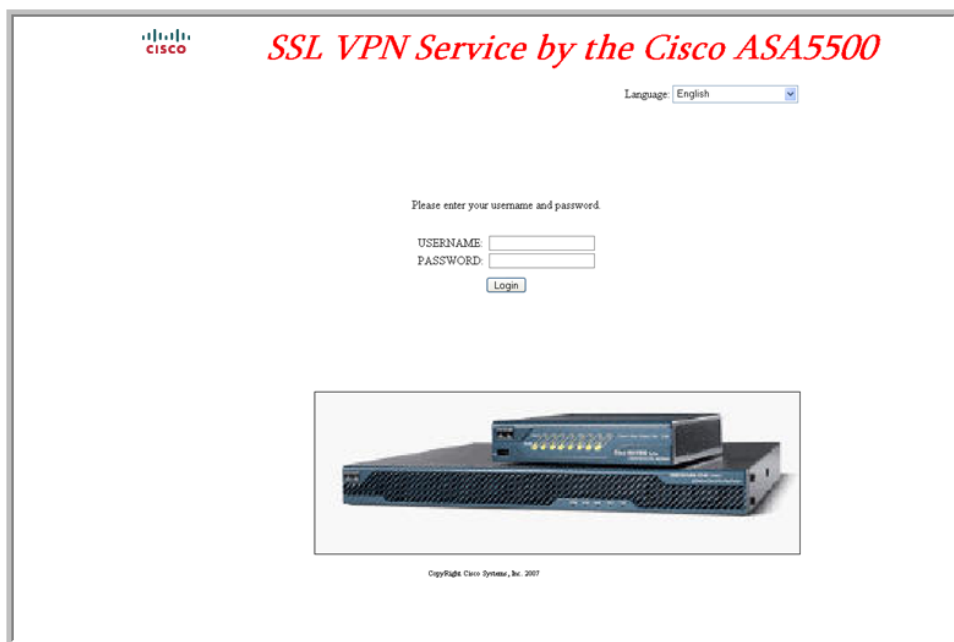
If you prefer to use your own, custom login screen, rather than changing specific components of the logon page we provide, you can perform this advanced customization using the Full Customization feature.

With Full Customization, you provide the HTML for your own login screen, and you insert Cisco HTML code that calls functions on the adaptive security appliance that create the Login form and the Language Selector drop-down list.

This document describes the modifications you need to make to your HTML code and the tasks required to configure the adaptive security appliance to use your code.

Figure 68-5 shows a simple example of a custom login screen enabled by the Full Customization feature.

Figure 68-5 Example of Full Customization of Logon Page



The following sections describe the tasks to customize the login screen:

- [Create the Custom Login Screen File](#)
- [Import the File and Images](#)

- [Configure the Security Appliance to use the Custom Login Screen](#)

Create the Custom Login Screen File

The following HTML code is used as an example and is the code that displays the screen shown in [Figure 68-5](#):

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7">&nbsp;</font><i><b><font
color="#FF0000" size="7" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font></b></i></p>

<body onload="cscs_ShowLoginForm('lform');cscs_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">

</td></tr>

</table>
```

The indented code injects the Login form and the Language Selector on the screen. The function **cscs_ShowLoginForm('lform')** injects the logon form. **cscs_ShowLanguageSelector('selector')** injects the Language Selector.

Follow these steps to modify your HTML file:

-
- Step 1** Name your file **logon.inc**. When you import the file, the adaptive security appliance recognizes this filename as the logon screen.
 - Step 2** Modify the paths of images used by the file to include **/+CSCOU+/**.

Files that are displayed to remote users before authentication must reside in a specific area of the adaptive security appliance cache memory represented by the path **/+CSCOU+/**. Therefore, the source for each image in the file must include this path. For example:

```
src="/+CSCOU+/asa5520.gif"
```

- Step 3** Insert the special HTML code below. This code contains the Cisco functions, described earlier, that inject the login form and language selector onto the screen.

```
<body onload="cisco_ShowLoginForm('lform');cisco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">

</td></tr>

</table>
```

Import the File and Images

Follow these steps to import your HTML file and any images to the adaptive security appliance:

- Step 1** Import the file and images as Web Content.
- Go to **Clientless SSL VPN Access > Portal > Web Contents**.
- Click **Import** (1). The **Import Web Content** window displays. Enter the **Source** information (2). In the **Destination** area, select **No** for *Require Authentication to access its content* (3). This ensures the files are stored in the area of flash memory accessible to users before authentication.
- Step 2** Import any images used by the file as Web Content using the same window.

Configure the Security Appliance to use the Custom Login Screen

Follow these steps to enable the adaptive security appliance to use the new login screen in a customization object:

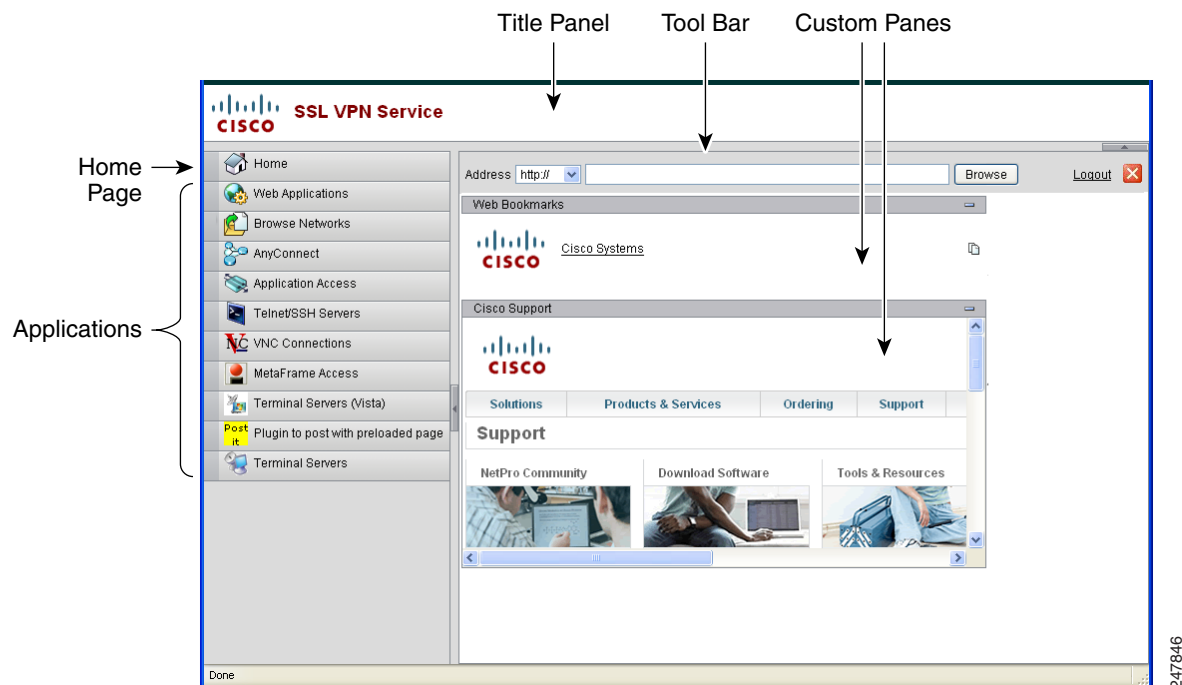
- Step 1** Select a customization object. Go to **Clientless SSL VPN Access > Portal > Customization**. Select a customization object in the table and click **Edit**. The **Edit Customization Object** window displays.
- Step 2** In the navigation pane, select **Logon Page**.
- Step 3** Choose **Replace pre-defined logon page with a custom page**.
- Step 4** Click **Manage** to import your logon page file. The **Import Web Content** window displays.

- Step 5** In the Destination area, select **No** to ensure your logon page is visible to users before they authenticate.
- Step 6** Back in the Edit Customization Object window, click **General** and enable the customization object for the connection profile and/or group policies you desire.

Customizing the Portal Page

Figure 68-6 shows the portal page and the pre-defined components you can customize:

Figure 68-6 Customizable Components of the Portal Page



In addition to customizing the components of the page, you can divide the portal page into custom panes that display text, an image, an RSS feed, or HTML. In Figure 68-6, the portal page is divided into one column with two rows.

To customize the portal page, follow this procedure. You can preview your changes for each component by clicking the **Preview** button:

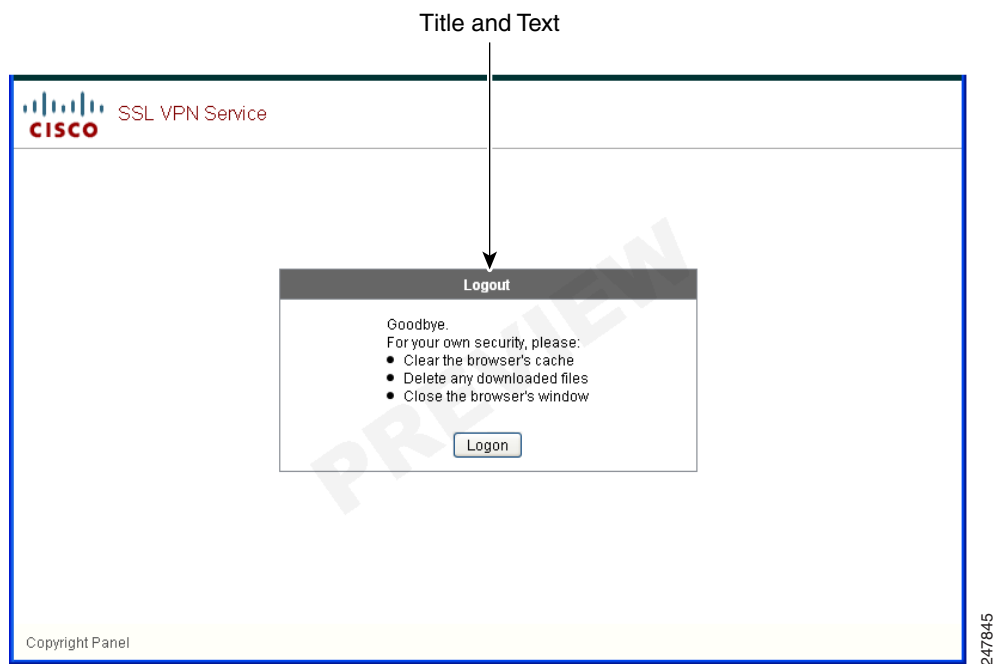
- Step 1** Go to Portal Page and specify a title for the browser window.
- Step 2** Display and customize the title panel. Go to Portal Page > Title Panel and check **Display title panel**. Enter text to display as the title and specify a logo. Specify any font styles.
- Step 3** Enable and customize the toolbar. Go to Portal Page > Toolbar and check **Display toolbar**. Customize the Prompt Box, Browse button, and Logout prompt as desired.
- Step 4** Customize the Applications list. Go to Portal Page > Applications and check **Show navigation panel**. The applications populated in the table are those applications you enabled in the adaptive security appliance configuration, including client-server plugins and port forwarding applications.

- Step 5** Create custom panes in the portal page space. Go to Portal Page > Custom Panes and divide the window into rows and columns for text, images, RSS feeds, or HTML pages, as desired.
- Step 6** Specify a home page URL. Go to Portal Page > Home Page and check **Enable custom intranet web page**. Choose a bookmark mode that defines how bookmarks are organized.

Customizing the Logout Page

Figure 68-7 shows the logout page you can customize:

Figure 68-7 Components of the Logout Page



To customize the logout page, follow this procedure. You can preview your changes for each component by clicking the **Preview** button:

- Step 1** Go to Logout Page. Customize the title or text as you desire.
- Step 2** For the convenience of the user, you can display the Login button on the Logout page. To do this, check **Show logon button**. Customize the button text, if desired.
- Step 3** Customize the title font or background, as desired.
- Step 4** Click OK, then apply the changes to the customization object you edited.

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 adaptive 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 adaptive security appliance.
 - Path—Provide the path to the file.
 - Browse Flash—Browse to the path for the file.
 - Remote server—Choose this option to import a customization file that resides on a remote server accessible from the adaptive 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 68-5 presents the file structure for an XML customization object.



Note

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 68-5 XML-Based Customization File Structure

Tag	Type	Values	Preset value	Description
custom	node	—	—	Root tag
auth-page	node	—	—	Tag-container of authentication page configuration
window	node	—	—	Browser window
title-text	string	Arbitrary string	empty string	—
title-panel	node	—	—	The page top pane with a logo and a text
mode	text	enable/disable	disable	—
text	text	Arbitrary string	empty string	—
logo-url	text	Arbitrary URL	empty image URL	—
copyright-panel	node	—	—	The page bottom pane with a copyright information
mode	text	enable/disable	disable	—
text	text	Arbitrary URL	empty string	—
info-panel	node	—	—	The pane with a custom text and image
mode	string	enable/disable	disable	—

Table 68-5 XML-Based Customization File Structure (continued)

image-position	string	abovelow	above	The image position, relative to text
image-url	string	Arbitrary URL	empty image	—
text	string	Arbitrary string	empty string	—
logon-form	node	—	—	The form with username, password, group prompt
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	—
logout-form	node	—	—	The form with a logout message and the buttons to login or close the window
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	—
language-selector	node	—	—	The drop-down list to select a language
mode	string	enable disable	disable	—
title	text	—	Language	The prompt text to select language
language	node (multiple)	—	—	—
code	string	—	—	—
text	string	—	—	—
portal	node	—	—	Tag-container of the portal page configuration
window	node	—	—	see authentication page description
title-text	string	Arbitrary string	Empty string	—

Table 68-5 XML-Based Customization File Structure (continued)

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 pane 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 web-access file-access app-access net-access help For ins: 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.
url-list-title	string	—	N/A	If the application has bookmarks, the title for the panel with grouped bookmarks
mode	string	enable/disable	N/A	v
toolbar	node	—	—	—
mode	string	enable/disable	Enable	—
prompt-box-title	string	Arbitrary string	Address	Title for URL prompt list
browse-button-text	string	Arbitrary string	Browse	Browse button text

Table 68-5 XML-Based Customization File Structure (continued)

logout-prompt-text	string	Arbitrary string	Logout	—
column	node (multiple)	—	—	One column will be shown by default
width	string	—	N/A	—
order	number	—	N/A	Value used to sort elements.
url-lists	node	—	—	URL lists are considered to be default elements on the portal home page, if they are not explicitly disabled
mode	string	group nogroup	group	Modes: group – elements grouped by application type i.e. Web Bookmarks, File Bookmarks) no-group – url-lists are shown in separate panes disable – do not show URL lists by default
panel	node (multiple)	—	—	Allows to configure extra panes
mode	string	enable disable	—	Used to temporarily disable the panel without removing its configuration
title	string	—	—	—
type	string	—	—	Supported types: RSS IMAGE TEXT HTML
url	string	—	—	URL for RSS,IMAGE or HTML type paned
url-mode	string	—	—	Modes: mangle, no-mangle
text	string	—	—	Text for TEXT type 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">EXAMPLE WebVPN</text>
      <logo-url>http://www.example.com/images/EXAMPLE.gif</logo-url>
    </title-panel>

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

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

```

</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">EXAMPLE WebVPN</text>
    <logo-url>http://www.example.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>EXAMPLE Intranet</tab-title>
    <order>3001</order>
  </application>

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

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

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

  <pane>
    <id>text_pane</id>
    <type>TEXT</type>
    <url>rss.example.com?id=78</url>
  </pane>

```

```

    <column>1</column>
    <row>0</row>
    <text>Welcome to EXAMPLE WebVPN Service</text>
</pane>

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

<pane>
  <type>HTML</type>
  <title>EXAMPLE news</title>
  <url>http://www.example.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 adaptive 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 adaptive 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 adaptive security appliance.

The Customization Template

The customization template, named *Template*, follows:

```

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

```

```

Copyright (c) 2008,2009 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 tite 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+/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>
- <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 adaptive security appliance displays help content on the application panes during clientless sessions. Each clientless application pane 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 68-6](#) shows the clientless application panels and predetermined filenames for the help content.

Table 68-6 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 ¹	ssh,telnet-hlp.inc
Plug-in	VNC Connections	vnc-hlp.inc

1. This plug-in is capable of doing both `sshv1` and `sshv2`.

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 adaptive 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 by performing the following steps:

-
- Step 1** Use your browser to establish a clientless session with the adaptive 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 68-7](#), to the address of the adaptive security appliance, substituting *language* as described below, then press **Enter**.

Table 68-7 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/ <i>language</i> /app-access-hlp.inc
Standard	Browse Networks	/+CSCOE+/help/ <i>language</i> /file-access-hlp.inc
Standard	AnyConnect Client	/+CSCOE+/help/ <i>language</i> /net-access-hlp.inc
Standard	Web Access	/+CSCOE+/help/ <i>language</i> /web-access-hlp.inc
Plug-in	Terminal Servers	/+CSCOE+/help/ <i>language</i> /rdp-hlp.inc
Plug-in	Telnet/SSH Servers	/+CSCOE+/help/ <i>language</i> /ssh,telnet-hlp.inc
Plug-in	VNC Connections	/+CSCOE+/help/ <i>language</i> /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 (for example, do not use <html>, <title>, <body>, <head>, <h1>, <h2>, etc. You can use character tags, such as the tag, and the <p>, , , and 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 68-7](#), 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 (for example, do not use <html>, <title>, <body>, <head>, <h1>, <h2>, etc. You can use character tags, such as the tag, and the <p>, , , and tags to structure content.

Save the file as HTML only. Use the filename in the Filename column of [Table 68-6](#).

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 box 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, choose the filename 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—Indicate 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—Indicate if the source or destination file is located in flash memory on the adaptive 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—Indicate if the source or destination file is on a remote server:

- **Path**—Choose 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 adaptive 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 adaptive 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 adaptive 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 adaptive 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 68-8 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 68-8 *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://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://



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

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

RDP Plug-in ActiveX Debug Quick Reference

To set up and use an RDP plug-in, you must add a new environment variable. For the process of adding a new environment variable, use the following steps:

-
- Step 1** Right click on My Computer to access the System Properties and choose the **Advanced** tab.
 - Step 2** On the Advanced tab, choose the environment variables button.
 - Step 3** In the new user variable dialog box, enter the RF_DEBUG variable.
 - Step 4** Verify the new Environment Variable in the user variables section.
 - Step 5** If you used the client computer with versions of WebVPN before version 8.3, you must remove the old Cisco Portforwarder Control. Go to the C:/WINDOWS/Downloaded Program Files directory, right click on the portforwarder control, and choose **Remove**.
 - Step 6** Clear all of the Internet Explorer browser cache.
 - Step 7** Launch your WebVPN session and establish an RDP session with the RDP ActiveX Plug-in.
- You can now observe events in the Windows Application Event viewer.
-

Plug-in Requirements and Restrictions

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

The plug-ins do not work if the security appliance configures the clientless session to use a proxy server.



Note The remote desktop protocol plug-in does not support load balancing with a session broker. Because of the way the protocol handles the redirect from the session broker, the connection fails. If a session broker is not used, the plug-in works.

The plug-ins support single sign-on (SSO). They use the *same* credentials entered to open the clientless SSL VPN session. Because the plug-ins do not support macro substitution, you do not have the options to perform SSO on different fields such as the internal domain password or on an attribute on a Radius or LDAP server.

To configure SSO support for a plug-in, you install the plug-in, add a bookmark entry to display a link to the server, and specify SSO support when adding the bookmark.

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.

Plug-ins require ActiveX or Sun JRE 5, Update 1.4 or later (JRE 6 or later recommended) to be enabled on the browser. An ActiveX version of the RDP plug-in is unavailable for 64-bit browsers.

Preparing the Security Appliance for a Plug-in

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

- Step 1** Make sure clientless SSL VPN (“webvpn”) is enabled on a adaptive security appliance interface.
- Step 2** Install an SSL certificate onto the adaptive 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 adaptive 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](#)

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 68-9 *Plug-ins Redistributed by Cisco*

Cisco Download Link	Protocol	Description	Source of Redistributed Plug-in *
rdp2-plugin.090211.jar	RDP	Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2. Supports Remote Desktop ActiveX Control. We recommend using this plug-in that supports both RDP and RDP2. Only versions up to 5.2 of the RDP and RDP2 protocols are supported. Version 5.2 and later are not supported.	Cisco redistributes this plug-in without any changes to it per GNU General Public License.
rdp2-plugin.090211.jar	RDP2	Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2. Supports Remote Desktop ActiveX Control. Note This legacy plug-in supports only RDP2.	Cisco redistributes this plug-in without any changes to it per the GNU General Public License.
rdp-plugin.080506.jar	RDP	Accesses Microsoft Terminal Services hosted by Windows 2003 R1. Supports Remote Desktop ActiveX Control. Note This legacy plug-in supports only RDP.	Cisco redistributes this plug-in without any changes to it per the GNU General Public License.

Table 68-9 Plug-ins Redistributed by Cisco

Cisco Download Link	Protocol	Description	Source of Redistributed Plug-in *
ssh-plugin.080430.jar	SSH	<p>The Secure Shell-Telnet plug-in lets the remote user establish a Secure Shell (v1 or v2) or Telnet connection to a remote computer.</p> <p>Note Because keyboard-interactive authentication is not supported by JavaSSH, it cannot be supported with SSH plugin. (Keyboard interactive is a generic authentication method used to implement different authentication mechanisms.)</p>	Cisco redistributes this plug-in without any changes to it per the GNU General Public License.
vnc-plugin.080130.jar	VNC	<p>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 (also known as VNC server or service) turned on. This version changes the default color of the text and contains updated French and Japanese help files.</p>	Cisco redistributes this plug-in without any changes to it per the GNU General Public License.

* Consult the plug-in documentation for information on deployment configuration and restrictions.

To retrieve a plug-in redistributed by Cisco and import it into the adaptive 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 adaptive 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. The hash and date of these plug-ins are also provided.
- 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 or Web Interface 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 adaptive 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

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 or Citrix Web Interface (for XenDesktop).



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 adaptive security appliance, clientless SSL VPN users can use a connection to the adaptive security appliance to access Citrix MetaFrame or Web Interface 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 adaptive security appliance performs the connectivity functions of the Citrix secure gateway when the Citrix client connects to the Citrix MetaFrame Server or Web Interface. 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 68-77 before using the next section, if you are not already providing support for a plug-in.

Follow Steps 1 – 4 at <http://support.citrix.com/article/CTX117597> if you are configuring access to Web Interface (for XenDesktop), or you later upgrade to it, to avoid Cookies Required errors.

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.jar
- You 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 adaptive 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 adaptive security appliance and click the bookmark.
- Use the [Client for Java Administrator's Guide](#) as needed.
-

## POST Plug-ins for Homepage SSO and Application-only Portals

The POST plug-in was developed to solve some key single sign-on (SSO) and homepage requirements for certain key applications like Citrix Web Interface. This clientless SSL VPN plug-in has the following key capabilities:

- The option to display the homepage for a Web application (such as Citrix) in the right frame, as part of the default clientless portal, or as the only frame in the page (completely hiding anything that is part of the Cisco portal).
- The option for SSO on the homepage or with an application using WebVPN variables (also known as macros) (and therefore HTTP-POST parameters).
- The option to preload a page before issuing a POST request. This option becomes necessary when a logon page for an application sets some cookies.

POST plug-in has the following capabilities and restrictions:

- It is strictly an HTML/JavaScript code and not a JAVA plug-in. It contains no client components.
- No support on Firefox. It is supported only on Internet Explorer and Mac Safari.
- Does not support URLs with queries such as <http://example.company.com/names?Login>. The ? character is not supported.
- A POST plug-in adds approximately a 10-second delay to make sure an intermediate page is fully loaded with all objects for an application. This delay is beneficial for an application such as Citrix where an intermediate page performs client detection functions.

### Configuring POST Plug-ins

Obtain the plug-in (such as `post-plugin.080414.jar`) from Plugins (Latest) at `post-plugin.zip` or from <http://www.cisco.com/cisco/software/navigator.html>. Use the following procedures to configure the POST plug-in.

- 
- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins**.
  - Step 2** Click **Import**.  
The Import Client-Server Plug-in dialog box opens.
  - Step 3** Choose **post** from the Plug-in Name (Protocol) drop-down menu.
  - Step 4** 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, and 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 5** Click **Import Now**.

- Step 6** Click **Apply**.  
 The POST plug-in is now available for clientless SSL VPN sessions.

## Configuring and Applying the POST URL

POST plug-ins are configured with the customization object. For example, to make a Citrix portal the homepage after a Clientless SSL VPN login, follow these steps:

- Step 1** Add the POST URL of the Citrix server to the customization object in the Custom Intranet Web Page URL field (see [Figure 68-8](#)).

Adding POST URL, it becomes the following:

```
http
post://my-citrix-service.abcd.com/Citrix/AccessPlatform/auth/login.aspx?LoginType=Explicit
&user=CSCO_WEBVPN_USERNAME&password=CSCO_WEBVPN_PASSWORD&cisco_preload=http://my-citrix-ser
vice.abcd.com&cisco_ispopup=yes.
```

**Figure 68-8** SSL VPN Customization Editor Window



- Step 2** Apply the customization object to the group or user.  
 For additional information on configuring SSO and the required parameters, refer to the SSL VPN deployment guide at the following URL:  
[http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl\\_vpn\\_deployment\\_guide/deploy.html#wp1002989](http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html#wp1002989).

## Language Localization

The adaptive 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 adaptive security appliance to translate these user messages and includes the following sections:

- [Understanding Language Translation, page 68-84](#)

- [Creating a Translation Table, page 68-85](#)
- [Add/Edit Localization Entry, page 68-86](#)
- [Import/Export Language Localization, page 68-95](#)

## Understanding Language Translation

Each functional area and its messages that are visible to remote users are organized into translation domains. [Table 68-10](#) shows the translation domains and the functional areas translated.

**Table 68-10 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.                                                   |
| <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 adaptive 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 adaptive security appliance. Because you can customize the logon and logout pages, portal page, and URL bookmarks for clientless sessions, the adaptive 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**

To create a translation table, perform the following steps:

- 
- Step 1** Choose **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** Choose 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 68-9](#).
  - 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 in 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.                                      |
| <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.                                                   |
| <b>plugin-telnet,ssh</b> | Messages for the Telnet and SSH plug-in.                                                            |
| <b>plugin-vnc</b>        | Messages for the VNC plug-in.                                                                       |

Language—Specify a language. Use an abbreviation that is compatible with the language options of your browser. The adaptive 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 |
| •             | —           | •                | —        | —      |

# Customizing the AnyConnect Client

You can customize the AnyConnect VPN client to display your own corporate image to remote users, including clients running on Windows, Linux, and Mac OS X computers.



---

**Note** Customization is not supported for the AnyConnect client running on a Windows Mobile device.

---

You can use one of three methods to customize the client:

- Rebrand the client by importing individual client GUI components, such as the corporate logo and icons, to the adaptive security appliance which deploys them to remote computers with the installer.
- Import your own program (Windows and Linux only) that provides its own GUI or CLI and uses the AnyConnect API.
- Import a transform (Windows only) that you create for more extensive rebranding. The adaptive security appliance deploys it with installer.
- Create Scripts that deploy with the client and run when the client establishes or terminates a VPN connection.

The following sections explain how to customize the AnyConnect client:

- [Customizing AnyConnect by Importing Resource Files, page 68-87](#)
- [Customizing AnyConnect with you own GUI and Scripts, page 68-88](#)
- [Customizing AnyConnect GUI Text and Messages, page 68-92](#)
- [Customizing the Installer Program using Installer Transforms, page 68-93](#)
- [Localizing the Install Program using Installer Transforms, page 68-94](#)

## Customizing AnyConnect by Importing Resource Files

You can customize the AnyConnect client by importing your own custom files to the security appliance, which deploys the new files with the client. For detailed information about about the original GUI icons and information about their sizes, see the *AnyConnect VPN Client Administrators Guide*. You can use this information to create your custom files.

To import and deploy your custom files with the client, follow this procedure:

---

**Step 1** Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources**.

Click **Import**. The Import AnyConnect Customization Object window displays.

**Step 2** Enter the Name of the file to import. See the *AnyConnect VPN Client Administrators Guide* for the filenames of all the GUI components that you can replace.

**Note**

The filenames of your custom components must match the filenames used by the AnyConnect client GUI. The filenames of the GUI components are different for each OS and are case sensitive for Mac and Linux. For example, if you want to replace the corporate logo for Windows clients, you must import your corporate logo as *company\_logo.bmp*. If you import it as a different filename, the AnyConnect installer does not change the component. However, if you deploy your own executable to customize the GUI, the executable can call resource files using any filename.

**Step 3** Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table.

**Note**

If you import an image as a resource file (such as *company\_logo.bmp*), the image you import customizes the AnyConnect client until you reimport another image using the same filename. For example, if you replace *company\_logo.bmp* with a custom image, and then delete the image, the client continues to display your image until you import a new image (or the original Cisco logo image) using the same filename.

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

## Customizing AnyConnect with you own GUI and Scripts

For Windows, Linux, or Mac (PPP or Intel-based) computers, you can deploy your own client that uses the AnyConnect client API. You replace the AnyConnect GUI or the AnyConnect CLI by replacing the client binary files.

You can also download and run scripts that run when the client establishes a connection (an *OnConnect* script), or when the client terminates a session (an *OnDisconnect* script). Some examples that show how you might want to use this feature include:

- Refreshing the group policy upon VPN connection.
- Mapping a network drive upon VPN connection, and un-mapping it after disconnection.

- Logging on to a service upon VPN connection, and logging off after disconnection.

For complete information about customizing the AnyConnect GUI and creating and deploying scripts, see the *AnyConnect VPN Client Administrators Guide*.

The following sections describe how to import binary executables and scripts to the adaptive security appliance:

[Importing your own GUI as a Binary Executable, page 68-89](#)

[Importing Scripts, page 68-90](#)

## Importing your own GUI as a Binary Executable

For Windows, Linux, or Mac (PPP or Intel-based) computers, you can deploy your own client that uses the AnyConnect client API. You replace the AnyConnect GUI or the AnyConnect CLI by replacing the client binary files. [Table 68-11](#) lists the filenames of the client executable files for the different operating systems.

**Table 68-11** Filenames of Client Executables

| Client OS | Client GUI File            | Client CLI File |
|-----------|----------------------------|-----------------|
| Windows   | vpnui.exe                  | vpncli.exe      |
| Linux     | vpnui                      | vpn             |
| Mac       | Not supported <sup>1</sup> | vpn             |

1. Not supported by adaptive security appliance deployment. However, you can deploy an executable for the Mac that replaces the client GUI using other means, such as Altiris Agent.

Your executable can call any resource files, such as logo images, that you import to the adaptive security appliance (See [Table 68-11](#)). Unlike replacing the pre-defined GUI components, when you deploy your own executable, can use any filenames for your resource files.

We recommend that you sign your custom Windows client binaries (either GUI or CLI version) that you import to the adaptive security appliance. A signed binary has a wider range of functionality available to it. If the binaries are not signed the following functionality is affected:

- **Web-Launch**—The clientless portal is available and the user can authenticate. However, the behavior surrounding tunnel establishment does not work as expected. Having an unsigned GUI on the client results in the client not starting as part of the clientless connection attempt. And once it detects this condition, it aborts the connection attempt.
- **SBL**—The Start Before Logon feature requires that the client GUI used to prompt for user credentials be signed. If it is not, the GUI does not start. Because SBL is not supported for the CLI program, this affects only the GUI binary file.
- **Auto Upgrade**—During the upgrade to a newer version of the client, the old GUI exits, and after the new GUI installs, the new GUI starts. The new GUI does not start unless it is signed. As with Web-launch, the VPN connection terminates if the GUI is not signed. However, the upgraded client remains installed.



### Note

The adaptive 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 Guide* and the *Release Notes for Cisco AnyConnect VPN Client*.

## Importing Scripts

AnyConnect lets you download and run scripts when the following events occur:

- Upon the establishment of a new AnyConnect client VPN session with the security appliance. We refer to a script triggered by this event as an *OnConnect* script because it requires this filename prefix.
- Upon the tear-down of an AnyConnect client VPN session with the security appliance. We refer to a script triggered by this event as an *OnDisconnect* script because it requires this filename prefix.

Thus, the establishment of a new AnyConnect VPN session initiated by Trusted Network Detection triggers the *OnConnect* script (assuming the requirements are satisfied to run the script). The reconnection of a persistent AnyConnect VPN session after a network disruption does not trigger the *OnConnect* script.

These instructions assume you know how to write scripts and run them from the command line of the targeted endpoint to test them.



### Note

The AnyConnect software download site provides some example scripts; if you examine them, please remember that they are only examples; they may not satisfy the local computer requirements for running them, and are unlikely to be usable without customizing them for your network and user needs. Cisco does not support example scripts or customer-written scripts.

For complete information about deploying scripts, and their limitations and restrictions, see the *AnyConnect VPN Client Administrators Guide*.

## Writing, Testing, and Deploying Scripts

Deploy AnyConnect scripts as follows:

- Step 1** Write and test the script using the OS type on which it will run when AnyConnect launches it.



### Note

Scripts written on Microsoft Windows computers have different line endings than scripts written on Mac OS and Linux. Therefore, you should write and test the script on the targeted OS. If a script cannot run properly from the command line on the native OS, AnyConnect cannot run it properly either.

- Step 2** To import a script, go to **Network (Client) Access > AnyConnect Customization/Localization > Script**. The Customization Scripts pane displays.



### Note

Microsoft Windows Mobile does not support this option. You must deploy scripts using the manual method for this OS.

- Step 3** Enter a name for the script. Be sure to specify the correct extension with the name. For example, *myscript.bat*.

- Step 4** Choose a script action: *Script runs when client connects* or *Script runs when client disconnects*.

AnyConnect adds the prefix *scripts\_* and the prefix *OnConnect* or *OnDisconnect* to your filename to identify the file as a script on the adaptive security appliance. When the client connects, the adaptive security appliance downloads the script to the proper target directory on the remote computer, removing the *scripts\_* prefix and leaving the remaining *OnConnect* or *OnDisconnect* prefix. For example, if you

import the script *myscript.bat*, the script appears on the adaptive security appliance as *scripts\_OnConnect\_myscript.bat*. On the remote computer, the script appears as *OnConnect\_myscript.bat*.

To ensure the scripts run reliably, configure all adaptive security appliances to deploy the same scripts. If you want to modify or replace a script, use the same name as the previous version and assign the replacement script to all of the adaptive security appliances that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- Step 5** Select a file as the source of the script. The name does not need to be the same as the name you provided for the script. ASDM imports the file from any source file, creating the new name you specify for Name in Step 3.

Table 68-12 shows the locations of scripts on the remote computer:

**Table 68-12 Required Script Locations**

| OS                            | Directory                                                                                               |
|-------------------------------|---------------------------------------------------------------------------------------------------------|
| Microsoft Windows 7 and Vista | %ALLUSERPROFILE%\Cisco\Cisco AnyConnect VPN Client\Scripts                                              |
| Microsoft Windows XP          | %ALLUSERPROFILE%\Application Data\Cisco\Cisco AnyConnect VPN Client\Scripts                             |
| Linux                         | /opt/cisco/vpn/scripts<br><b>Note</b> Assign execute permissions to the file for User, Group and Other. |
| Mac OS X                      | /opt/cisco/vpn/scripts                                                                                  |
| Windows Mobile                | %PROGRAMFILES%\Cisco AnyConnect VPN Client\Scripts                                                      |

### 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 |
| •             | —           | •                | —        | —      |

## Customizing AnyConnect GUI Text and Messages

Change text and messages displayed on the AnyConnect client GUI displayed to remote users in this pane. This pane also shares functionality with the Language Localization pane. For more extensive language translation, go to Configuration > Remote Access VPN > Language Localization.

To change messages that appear on the AnyConnect GUI, perform the following steps:

- 
- Step 1** Click **Template** to expand the template area. Click **Export** to export the English language template to your local PC or a remote device.
- Step 2** Edit the template and make changes to any messages. The text contained between the quotes of the msgid field represents the default text. *Do not* change this text. To display a different message, insert your custom text between the quotes of msgstr. The example below shows a message containing connection termination information:
- ```
msgid ""
"The VPN connection has been disconnected due to the system suspending. The
"reconnect capability is disabled. A new connection requires re-
"authentication and must be started manually. Close all sensitive networked
"applications."
msgstr ""
```
- Step 3** Click **Import** to import the file you edited as a new translation template.
- Step 4** 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 5** Click **Apply to make your changes to the** adaptive security appliance.
-

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.

Template—Expands the Template area:

- **View**—Displays the contents of the English language template.
- **Export**—Launches the Export Language Localization dialog where you can export the English language template to a URL where you can make changes.

Modes

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

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

Customizing the Installer Program using Installer Transforms

You can perform more extensive customizing of the AnyConnect client GUI (Windows only) by creating your own transform that deploys with the client installer program. You import the transform to the adaptive security appliance, which deploys it with the installer program.

To create an MSI transform, you can download and install the free database editor from Microsoft, named Orca. With this tool, you can modify existing installations and even add new files. The Orca tool is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK. The following URL leads to the bundle containing the Orca program:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp

After you install the SDK, the Orca MSI is located here:

C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi.

Install the Orca software, then access the Orca program from your Start > All Programs menu.

To import your transform, follow these steps:

- Step 1** Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms**. Click **Import**. The Import AnyConnect Customization Objects windows displays.
- Step 2** Enter the Name of the file to import. Unlike the names of other customizing objects, the name is not significant to the adaptive security appliance and is for your own convenience.
- Step 3** Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table.



Note Windows is the only valid choice for applying a transform.

Sample Transform

While offering a tutorial on creating transforms is beyond the scope of this document, we provide the text below as representative of some entries in a transform. These entries replace *company_logo.bmp* with a local copy and install the custom profile *MyProfile.xml*.

```
DATA CHANGE - Component Component ComponentId
+ MyProfile.xml {39057042-16A2-4034-87C0-8330104D8180}
```

```
Directory_ Attributes Condition KeyPath
Profile_DIR 0 MyProfile.xml
```

```
DATA CHANGE - FeatureComponents Feature_ Component_
```

```

+ MainFeature MyProfile.xml

DATA CHANGE - File File Component_ FileName FileSize Version Language Attributes Sequence
+ MyProfile.xml MyProfile.xml MyProf~1.xml|MyProfile.xml 601 8192 35
<> company_logo.bmp 37302{39430} 8192{0}

DATA CHANGE - Media DiskId LastSequence DiskPrompt Cabinet VolumeLabel Source
+ 2 35

```

Specify transform files for customizing the AnyConnect client installation in this pane.

Fields

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

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

Delete—Removes the selected file.

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

Object Name—The name of the transform.

Modes

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

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

Localizing the Install Program using Installer Transforms

As with the AnyConnect client GUI, you can translate messages displayed by the client installer program. The adaptive security appliance uses transforms to translate the messages displayed by the installer. The transform alters the installation, but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.

Each language has its own transform. You can edit a transform with a transform editor such as Orca, and make changes to the message strings. Then you import the transform to the adaptive security appliance. When the user downloads the client, the client detects the preferred language of the computer (the locale specified during installation of the operating system) and applies the appropriate transform.

We currently offer transforms for 30 languages. These transforms are available in the following .zip file on the AnyConnect client software download page at cisco.com:

```
anyconnect-win-<VERSION>-web-deploy-k9-lang.zip
```

In this file, <VERSION> is the version of AnyConnect release (e.g. 2.2.103).

The package contains the transforms (.mst files) for the available translations. If you need to provide a language to remote users that is not one of the 30 languages we provide, you can create your own transform and import it to the adaptive security appliance as a new language. With Orca, the database

editor from Microsoft, you can modify existing installations and new files. Orca is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK. The following URL leads to the bundle containing the Orca program:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp.

After you install the SDK, the Orca MSI is located here:

C:\Program Files\Microsoft SDK SP1\Microsoft Platform SDK\Bin\Orca.msi.

The following procedure shows how to import a transform to the adaptive security appliance using ASDM:

-
- Step 1** Import a Transform. Go to: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Localized Installer Transforms**. Click **Import**. The Import MST Language Localization window opens.
- Step 2** Choose a language for this transform. Click the Language drop-list to display languages and their industry-recognized abbreviations. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.
- Step 3** Click **Import Now**. A message displays saying you successfully imported the table. Be sure to click **Apply** to save your changes.

Fields

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

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

Delete—Removes the selected transform.

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

Object Name—The name of the transform.

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 dialog boxes you can import or export a translation table to the adaptive 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. This plug-in is capable of doing both sshv1 and sshv2.
 - 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 adaptive 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 adaptive 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
•	—	•	—	—

Configuring 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 68-1](#) 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		
			Multiple	
Routed	Transparent	Single	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 drop-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 **cscsso=1**. For example:

host/?cscsso=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 drop-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 Option—Click to open the bookmark in a new window that uses the smart tunnel feature to pass data through the adaptive security appliance to or from the destination server. All browser traffic passes securely over the SSL VPN tunnel. 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. If you uncheck 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—Choose **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—Click to import a file that resides on the local PC.

- Flash file system—Click to export a file that resides on the adaptive security appliance.
- Remote server—Click to import a url list file that resides on a remote server accessible from the adaptive 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—Click to import or export a file that resides on the local PC.
 - Flash file system—Click to import or export a file that resides on the adaptive security appliance.
 - Remote server—Click to import a file that resides on a remote server accessible from the adaptive 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 adaptive security appliance uses /+CSCOE+/ for objects that require authentication, and /+CSCOU+/ for objects that do not. The adaptive 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.

About Clientless SSL VPN Variable Substitutions

Clientless SSL VPN variables allow for substitutions in URLs and forms-based HTTP post operations. These variables, also known as macros, 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.

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">`.

You can choose one of the supplied variables from the drop-down list, or you can construct a variable. The variables you can choose from the drop-down list include the following:

Table 68-13 Clientless SSL VPN Variables

No.	Variable 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. This is a cached credential, and not authenticated by a AAA server. If a user enters this value, it is used as the password for auto-signon, instead of the password value.
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN user login group drop-down, a group alias within the connection profile

Table 68-13 Clientless SSL VPN Variables

No.	Variable Substitution	Definition
5	CSCO_WEBVPN_MACRO1	Set via RADIUS/LDAP vendor-specific attribute. If you are mapping this from LDAP via an ldap-attribute-map, the Cisco attribute that uses this variable is WEBVPN-Macro-Substitution-Value1. Variable substitution via RADIUS is performed by VSA#223.
6	CSCO_WEBVPN_MACRO2	Set via RADIUS/LDAP vendor-specific attribute. If you are mapping this from LDAP via an ldap-attribute-map, the Cisco attribute that uses this variable is WEBVPN-Macro-Substitution-Value2. Variable substitution via RADIUS is performed by VSA#224.
7	CSCO_WEBVPN_PRIMARY_USERNAME	Primary user login ID for double authentication.
8	CSCO_WEBVPN_PRIMARY_PASSWORD	Primary user login password for double authentication.
9	CSCO_WEBVPN_SECONDARY_USERNAME	Secondary user login ID for double authentication.
10	CSCO_WEBVPN_SECONDARY_PASSWORD	Secondary user login ID for double authentication.

When the adaptive security appliance recognizes one of these six variable strings in an end-user request—in a bookmark or a post form—it replaces it with the user-specific value before passing the request to a remote server.

**Note**

You can obtain the http-post parameters for any application by performing an HTTP Sniffer trace in the clear (without the security appliance involved). Here is the URL to a free browser capture tool, also called an HTTP Analyzer:
<http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe>.

Using Variables 1 - 4

The adaptive 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, the adaptive 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, lets the adaptive 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 Variables 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.

Using Variables 7 - 10

Each time the adaptive security appliance recognizes one of these four strings in an end-user request (a bookmark or a post form), it replaces it with the user-specific value before passing the request to a remote 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.example.com*
- WebVPN-Macro-Value2 (ID=224), type string, is returned as *401k.com*

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

`https://CSCO_WEBVPN_MACRO1`, which would translate to `https://wwwin-portal.example.com`.

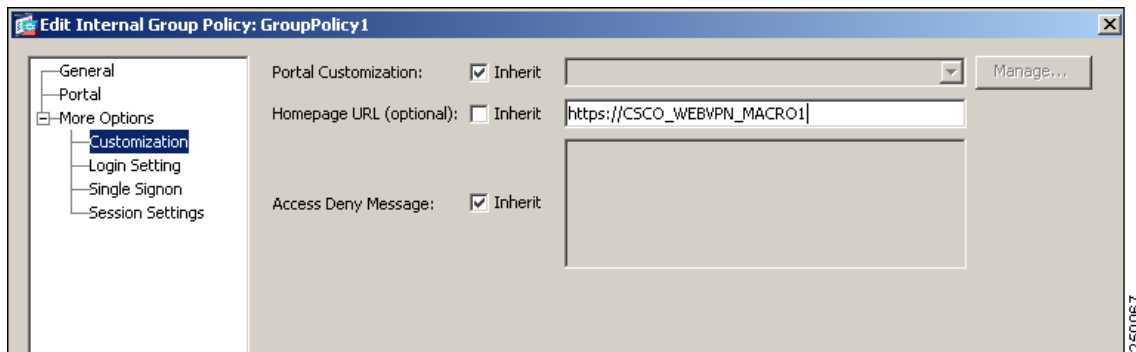
The best way to do this is to configure the Homepage URL parameter in ASDM.

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 68-9 Using ASDM to Configure a Macro that Sets a Homepage](#).

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 68-9 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 ([Figure 68-10](#)).

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

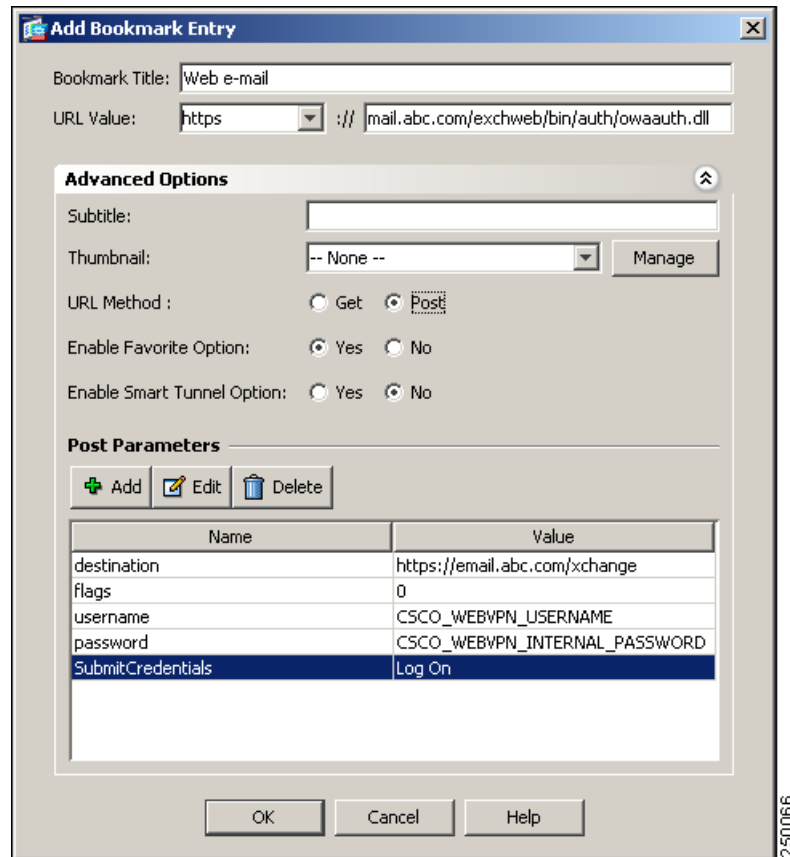
- Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add/Edit Bookmark Lists > Add/Edit Bookmark Entry > Advanced Options area > Add/Edit Post Parameters (available after you click **Post** in the URL Method attribute).

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 68-10 Configuring a Bookmark Entry



250066

Example 3: Configuring File Share (CIFS) URL Substitutions

You can allow a more flexible bookmark configuration by using variable substitution for CIFS URLs.

If you configure the URL `cifs://server/CSCO_WEBVPN_USERNAME`, the adaptive security appliance automatically maps it to the user's file share home directory. This method also allows for password and internal password substitution. The following are example URL substitutions:

```
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
```

```
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

More examples

For more variable substitution examples, see the *Cisco ASA 5500 SSL VPN Deployment Guide* on cisco.com.

Modes

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

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

