

Advanced Clientless SSL VPN Configuration

- Microsoft Kerberos Constrained Delegation Solution, on page 1
- Configure the Use of External Proxy Servers, on page 6
- Use HTTPS for Clientless SSL VPN Sessions, on page 8
- Configure Application Profile Customization Framework, on page 9
- Configure Session Settings, on page 14
- Encoding, on page 15
- Configure Content Caching, on page 17
- Content Rewrite, on page 18
- Use Email over Clientless SSL VPN, on page 20
- Configure Bookmarks, on page 20

Microsoft Kerberos Constrained Delegation Solution

Microsoft's Kerberos Constrained Delegation (KCD) provides access to Kerberos-protected Web applications in the private network.

In order for Kerberos Constrained Delegation to function, the ASA must establish a trust relationship between the source domain (the domain where the ASA resides) and the target or resource domain (the domain where the Web services reside). The ASA crosses the certification path from the source to the destination domain and acquires the necessary tickets on behalf of the remote access user to access the services.

This crossing of the certificate path is called cross-realm authentication. During each phase of cross-realm authentication, the ASA relies on the credentials at a particular domain and the trust relationship with the subsequent domain.

How KCD Works

Kerberos relies on a trusted third party to validate the digital identity of entities in a network. These entities (such as users, host machines, and services running on hosts) are called principals and must be present in the same domain. Instead of secret keys, Kerberos uses tickets to authenticate a client to a server. The ticket is derived from the secret key and consists of the client's identity, an encrypted session key, and flags. Each ticket is issued by the key distribution center and has a set lifetime.

The Kerberos security system is a network authentication protocol used to authenticate entities (users, computers, or applications) and protect network transmissions by scrambling the data so that only the device that the information was intended for can decrypt it. You can configure KCD to provide Clientless SSL VPN

users with SSO access to any Web services protected by Kerberos. Examples of such Web services or applications include Outlook Web Access (OWA), Sharepoint, and Internet Information Server (IIS).

Two extensions to the Kerberos protocol were implemented: *protocol transition* and *constrained delegation*. These extensions allow the Clientless SSL VPN remote access users to access Kerberos-authenticated applications in the private network.

P*rotocol transition* provides you with increased flexibility and security by supporting different authentication mechanisms at the user authentication level and by switching to the Kerberos protocol for security features (such as mutual authentication and constrained delegation) in subsequent application layers. *Constrained delegation* provides a way for domain administrators to specify and enforce application trust boundaries by limiting where application services can act on a user's behalf. This flexibility improves application security designs by reducing the chance of compromise by an untrusted service.

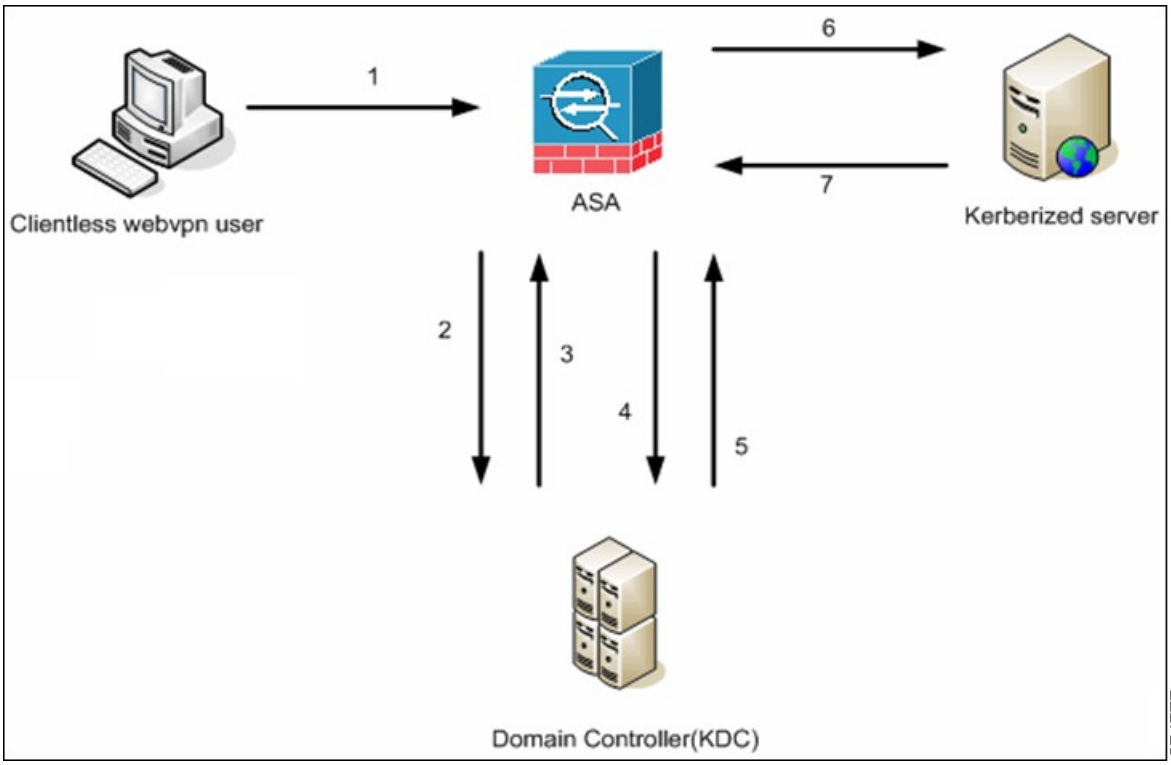
For more information on constrained delegation, see RFC 1510 via the IETF website (http://www.ietf.org).

Authentication Flow with KCD

The following figure depicts the packet and process flow a user experiences directly and indirectly when accessing resources trusted for delegation via the clientless portal. This process assumes that the following tasks have been completed:

- Configured KCD on ASA.
- Joined the Windows Active Directory and ensured services are trusted for delegation.
- Delegated ASA as a member of the Windows Active Directory domain.

Figure 1: KCD Process



Note A clientless user session is authenticated by the ASA using the authentication mechanism configured for the user. (In the case of smartcard credentials, ASA performs LDAP authorization with the userPrincipalName from the digital certificate against the Windows Active Directory).

1. After successful authentication, the user logs in to the ASA clientless portal page. The user accesses a Web service by entering a URL in the portal page or by clicking on the bookmark. If the Web service requires authentication, the server challenges ASA for credentials and sends a list of authentication methods supported by the server.

Note KCD for Clientless SSL VPN is supported for all authentication methods (RADIUS, RSA/SDI, LDAP, digital certificates, and so on). Refer to the AAA Support table at http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492.

2. Based on the HTTP headers in the challenge, the ASA determines whether the server requires Kerberos authentication. (This is part of the SPNEGO mechanism.) If connecting to a backend server requires Kerberos authentication, the ASA requests a service ticket for itself on behalf of the user from the key distribution center.
3. The key distribution center returns the requested tickets to the ASA. Even though these tickets are passed to the ASA, they contain the user's authorization data. The ASA requests a service ticket from the KCD for the specific service that the user wants to access.

Note Steps 1 to 3 comprise protocol transition. After these steps, any user who authenticates to the ASA using a non-Kerberos authentication protocol is transparently authenticated to the key distribution center using Kerberos.

4. The ASA requests a service ticket from the key distribution center for the specific service that the user wants to access.
5. The key distribution center returns a service ticket for the specific service to the ASA.
6. The ASA uses the service ticket to request access to the Web service.
7. The Web server authenticates the Kerberos service ticket and grants access to the service. The appropriate error message is displayed and requires acknowledgment if there is an authentication failure. If the Kerberos authentication fails, the expected behavior is to fall back to basic authentication.

Create a Kerberos Server Group for Constrained Delegation

To use Kerberos Constrained Delegation, you must first configure a Kerberos AAA server group. The server group must contain the Active Directory (AD) domain controller.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Microsoft KCD Server**.

Step 2 Click **New** next to the Kerberos Server Group for Constrained Delegation drop-down list.

If you already configured the Kerberos AAA server group you need, you can simply select the server group now and skip this procedure.

Step 3 Enter a name for the group in the **Server Group Name** field or keep the default name.

Step 4 Click **Depletion** or **Timed** in the **Reactivation Mode** field.

In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive. In depletion mode, when a server is deactivated, it remains inactive until all other servers in the group are inactive. When and if this occurs, all servers in the group are reactivated. This approach minimizes the occurrence of connection delays due to failed servers.

In Timed mode, failed servers are reactivated after 30 seconds of down time.

Step 5 If you chose the Depletion reactivation mode, enter a time interval in the **Dead Time** field.

The dead time is the duration of time, in minutes, that elapses between the disabling of the last server in a group and the subsequent re-enabling of all servers.

Step 6 Specify the maximum number of failed AAA transactions with a AAA server in the group before trying the next server.

This option sets the number of failed AAA transactions before declaring a nonresponsive server to be inactive.

Step 7 Choose the **Interface Name** through which the AD domain controller can be reached.

Step 8 Enter either the name or IP address for the domain controller that you are adding to the group.

Step 9 Specify the timeout value for connection attempts to the server.

Specify the timeout interval (1-300 seconds) for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts (based on the retry interval) until the timeout is reached. If the number of consecutive failed transactions reaches the maximum-failed-attempts limit specified in the AAA server group, the AAA server is deactivated and the ASA starts sending requests to another AAA server if it is configured.

Step 10 Specify the server port. The server port is either port number 88, or the TCP port number used by the ASA to communicate with the Kerberos server.

Step 11 Select the retry interval, which is the time the system waits before retrying a connection request. You can select from 1-10 seconds. The default is 10 seconds.

Step 12 Configure the Kerberos realm.

Kerberos realm names use numbers and upper case letters only, and can be up to 64 characters. The name should match the output of the Microsoft Windows **set USERDNSDOMAIN** command when it is run on the Active Directory server for the Kerberos realm. In the following example, EXAMPLE.COM is the Kerberos realm name:

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

Although the ASA accepts lower case letters in the name, it does not translate lower case letters to upper case letters. Be sure to use upper case letters only.

Step 13 Click **OK**.

Configure Kerberos Constrained Delegation (KCD)

The following procedure explains how to implement Kerberos Constrained Delegation (KCD).

Before you begin

- Enable DNS lookup on the interface through which the domain controller is reached. When using KCD as the authentication delegation method, DNS is required to enable hostname resolution and communication between the ASA, Domain Controller (DC), and the services trusted for delegation. Clientless VPN deployments require DNS Lookups through the internal corporate network, typically the inside interface.

  For example, go to **Configuration** > **Device Management** > **DNS** > **DNS Client**, then in the **DNS Lookup** table, click the **DNS Enabled** cell in the inside interface row and select **True**.

- Configure DNS to use the Active Directory (AD) domain controller as the DNS server, with the domain realm as the DNS domain.

  For example, go to **Configuration** > **Device Management** > **DNS** > **DNS Client**, then add 10.1.1.10 off the inside interface as the **Primary DNS Server**, and EXAMPLE.COM as the Domain Name. (If you have multiple server groups, select the DefaultDNS server group and add the domain controller.)

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Microsoft KCD Server**.

Step 2 Either select an existing Kerberos AAA server group, or click **New** to create a new group.

If you create a new group, see Create a Kerberos Server Group for Constrained Delegation, on page 3.

Step 3 In Server Access Credentials, configure the options needed to join the AD domain.

When configured for KCD, the ASA initiates an AD domain join with the configured server in order to acquire Kerberos keys. These keys are required for the ASA to request service tickets on behalf of clientless SSL VPN users.

- **Username**, **Password**—A username defined on the domain controller that the system can use to join the domain, and the password for the user account. The user account must have administrative privileges or service level privileges for adding devices to the domain.

Step 4 (Optional.) Adjust the Server Group Configuration settings if necessary. For an explanation of the options, see Create a Kerberos Server Group for Constrained Delegation, on page 3.

Step 5 (Optional.) Add, edit, delete, or test servers in the Kerberos server group table. For an explanation of the parameters for a Kerberos server, see Create a Kerberos Server Group for Constrained Delegation, on page 3.

Monitoring Kerberos Constrained Delegation

You can use the following commands to monitor KCD. Use **Tools** > **Command Line Interface** or an SSH session to enter these commands.

- **show webvpn kcd**

  Shows the KCD configuration and join status.

```
ciscoasa# show webvpn kcd

KCD state:      Domain Join Complete
Kerberos Realm: EXAMPLE.COM
ADI version:    6.8.0_1252
Machine name:   ciscoasa
ADI instance:   root      1181  1178  0 15:35 ?        00:00:01 /asa/bin/start-adi
Keytab file:    -rw------- 1 root root 79 Jun 16 16:06 /etc/krb5.keytab
```

- **show aaa kerberos** [**username** *user_id*]

  Shows the Kerberos tickets cached on the system. You can view all tickets, or just those tickets for a given user.

```
ASA# show aaa kerberos

Default Principal      Valid Starting        Expires             Service Principal
asa@example.COM        06/29/10 18:33:00     06/30/10 18:33:00
krbtgt/example.COM@example.COM
kcduser@example.COM    06/29/10 17:33:00     06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM    06/29/10 17:33:00     06/30/10 17:33:00
http/owa.example.com@example.COM
```

- **clear aaa kerberos tickets** [**username** *user_id*]

  Clears the Kerberos tickets cached on the system. You can clear all tickets, or just those tickets for a given user.

Configure the Use of External Proxy Servers

Use the Proxies pane to configure the ASA 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.

Procedure

Step 1 Click Use an HTTP Proxy Server.

Step 2 Identify the HTTP proxy server by its IP address or hostname.

Step 3 Enter the hostname or IP address of the external HTTP proxy server.

Step 4 Enter the port that listens for HTTP requests. The default port is 80.

Step 5 (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.

Step 6 (Optional) Enter this keyword to accompany each HTTP proxy request with a username to provide basic, proxy authentication.

Step 7 Enter a password to send to the proxy server with each HTTP request.

Step 8 As an alternative to specifying the IP address of the HTTP proxy server, you can choose Specify PAC File URL 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 ASA ignores it.

Step 9 Choose whether to use an HTTPS proxy server.

Step 10 Click to identify the HTTPS proxy server by its IP address or hostname.

Step 11 Enter the hostname or IP address of the external HTTPS proxy server.

Step 12 Enter the port that listens for HTTPS requests. The default port is 443.

Step 13 (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.

Step 14 (Optional) Enter a keyword to accompany each HTTPS proxy request with a username to provide basic, proxy authentication.

Step 15 Enter a password to send to the proxy server with each HTTPS request.

Use HTTPS for Clientless SSL VPN Sessions

In addition to configuring HTTPS, enable HTTP Strict-Transport-Security (HSTS), a web security policy mechanism which helps to protect websites against protocol downgrade attacks and cookie hijacking. HSTS redirects the UA/Browser to HTTPS websites to connect to the web servers securely until the specified timeout expires by sending the following directive:

```
Strict-Transport-Security: max-age="31536000; includesubdomains; preload
```

Where:

http-headers—configures different HTTP headers sent from the ASA to browsers. Set the submode or reset all the http-headers settings:

- hsts-client—starts handling HSTS header from HTTP servers to act as HSTS clients
  - enable—allows you to enable or disable HSTS policy. When enabled, the HSTS policy is enforced for known HSTS hosts and HSTS headers.
- hsts-server—Configures the HSTS header to be sent from the ASA to browsers. The header lets ASA tell browsers to only allow access using HTTPS instead of HTTP.
  - include-sub-domains—allows domain owners to submit what domains should be included in the HSTS preload list for web browsers.



Note To set an additional redirect from your HTTPS site, you must still have the HSTS header in the redirect (rather than the page it redirects to).

  - max-age—(which is configurable after clicking Enable HSTS checkbox) specifies the time in seconds that the web server must be regarded as an HSTS host and must be accessed securely using HTTPS only. Default is 3153600 seconds (one year). Range is 0-2147483647 seconds.
  - preload—tells the browser to load the list of domains that are already registered with UA/Browser; that now must be treated as HSTS hosts. The preloaded lists implementation is UA/browser dependent and each UA/browser can specify further restrictions on what the other directives can be. For example, Chrome's preload list specifies that the HSTS max-age be at least 18 weeks (10,886,400 seconds).
- x-content-type-options—enables sending "X-Content-Type-Options: nosniff" response header
- x-xss-protection—enables sending "X-XSS-Protection: 1[; mode=block]" response header

Procedure

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Proxies**.

Step 2 Click **Enable HSTS Server** to submit what domains should be included in the HSTS preload list for browsers. **Enable HSTS Subdomains** and **Enable HSTS Preload** take effect and are enabled by default when you enable HSTS Server.

Step 3 Specify **HSTS Max Age**, the amount of time in seconds that HSTS remains in effect.

The value ranges from <0-2147483647> seconds. Default is 31536000 seconds (one year). Once this limit is reached, HSTS is no longer in effect.

The amount of time in seconds that HSTS remains in effect. The value ranges from <0-2147483647> seconds. Default is 31536000 seconds (1year). Once this limit is reached, HSTS is no longer in effect.

Configure Application Profile Customization Framework

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

You can configure and run multiple APCF profiles in parallel on an ASA. Within an APCF profile script, multiple APCF rules can apply. The ASA processes the oldest rule first, based on configuration history, the next oldest rule next.

You can store APCF profiles on the ASA flash memory, or on an HTTP, HTTPS, or TFTP server.

We recommend that you configure an APCF profile only with the assistance of Cisco personnel.

Manage APCF Profiles

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

Procedure

Step 1 Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Application Helper, where you can perform the following functions.

- Click **Add/Edit** to create a new APCF profile or change an existing one.
  - Select **Flash file** to locate an APCF file stored on the ASA flash memory.

    Then click **Upload** to get an APCF file from a local computer to the ASA flash file system, or Browse to upload choose an APCF file that is already in flash memory.
  - Select URL to retrieve the APCF file from an HTTP, HTTPS, FTP, or TFTP server.
- Click **Delete** to remove an existing APCF profile. No confirmation or undo exists.
- Click **Move Up** or **Move Down** to rearrange APCF profiles within the list. The order determines which the APCF profile is used.

Step 2 Click **Refresh** if you do not see the changes you made in the list.

Upload APCF Packages

Procedure

Step 1 The path to the APCF file on your computer is shown. Click **Browse Local** to automatically insert the path in this field, or enter the path.

Step 2 Click to locate and choose the APCF file to transfer on your computer. 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.

Step 3 The path on the ASA to upload the APCF file is shown in the Flash File System Path. Click **Browse Flash** to identify the location on the ASA to upload the APCF file to. The Browse Flash dialog box displays the contents of flash memory.

Step 4 The file name of the APCF file you selected on your local computer is displayed. 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.

Step 5 Click **Upload File** when you have identified the location of the APCF file on your computer, and the location to download it to the ASA.

Step 6 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**.

Step 7 Close the Upload Image dialog window. Click **Close** 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**

Manage APCF Packets

Procedure

Step 1 Use the following commands to add, edit, and delete APCF packets and put them in priority order:

- **APCF File Location**—Displays information about the location of the APCF package. This can be in the ASA flash memory, or on an HTTP, HTTPS, FTP, or TFTP server.
- **Add/Edit**—Click to add or edit a new or existing APCF profile.

- **Delete**—Click to remove an existing APCF profile. There is no confirmation or undo.
- **Move Up**—Click to rearrange APCF profiles within a list. The list determines the order in which the ASA attempts to use APCF profiles.

Step 2 Click **Flash File** to locate an APCF file stored in the ASA flash memory.

Step 3 Enter the path to an APCF file stored in flash memory. If you already added a path, it redirects to an APCF file stored in flash memory after you browse to locate it.

Step 4 Click **Browse Flash** 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 ASA 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.

APCF Syntax

APCF profiles use XML format, and sed script syntax, with the XML tags in the following table.

Guidelines for APCF

Misuse of an APCF profile can result in reduced performance and undesired rendering of content. In most cases, Cisco Engineering supplies APCF profiles to solve specific application rendering issues.

Table 1: APCF XML Tags

Tag	Use
<APCF>...</APCF>	The mandatory root element that opens any AP
<version>1.0</version>	The mandatory tag that specifies the APCF im version. Currently the only version is 1.0.
<application>...</application>	The mandatory tag that wraps the body of the description.
<id> text </id>	The mandatory tag that describes this particula functionality.
<apcf-entities>...</apcf-entities>	The mandatory tag that wraps a single or mult entities.

Tag	Use
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	One of these tags specifies type of content or the s which the APCF processing should take place.
<conditions>… </conditions>	A child element of the pre/post-process tags that s criteria for processing such as: • http-version (such as 1.1, 1.0, 0.9) • http-method (get, put, post, webdav) • http-scheme (“http/”, “https/”, other) • server-regexp regular expression containing ("A".."Z" | "0".."9" | ".-_*[]?") • server-fnmatch (regular expression containin | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"), • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • If more than one of condition tags is present, performs a logical AND for all tags.
<action> … </action>	Wraps one or more actions to perform on the cont specified conditions; you can use the following tag these actions (shown below): • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

Tag	Use
<do>…</do>	Child element of the action tag used to define following actions: • <no-rewrite/>—Do not mangle the conte from the remote server. • <no-toolbar/>—Do not insert the toolbar. • <no-gzip/>—Do not compress the conten • <force-cache/>—Preserve the original ca instructions. • <force-no-cache/>—Make object non-ca • < downgrade-http-version-on-backend>— when sending the request to remote serve
<sed-script> TEXT </sed-script>	Child element of the action tag used to change text-based objects. The Text must be a valid S <sed-script> applies to the <conditions> tag d it.
<rewrite-header></rewrite-header>	Child element of the action tag. Changes the v HTTP header specified in the child element <h shown below.
<add-header></add-header>	Child element of the action tag used to add a n header specified in the child element <header> below.
<delete-header></delete-header>	Child element of the action tag used to delete t HTTP header specified by the child element < shown below.

<header></header>	Specifies the name HTTP header to be rewritt deleted. For example, the following tag change the HTTP header named Connection:
	
	`<rewrite-header>`
	`<header>Connection</header>`
	`<value>close</value>`
	`</rewrite-header>`

Configuration Examples for APCF

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
```

```
          <server-fnmatch>*.example.com</server-fnmatch>
        </conditions>
          <action>
            <do><no-gzip/></do>
          </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>

<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
          <rewrite-header>
               <header>Content-Type</header>
               <value>text/html</value>
          </rewrite-header>
         </action>
      </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

Configure 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.

Procedure

Step 1 Click **none** or choose the file server protocol (smb or ftp) from the User Storage Location drop-down menu. Cisco recommends using CIFS for user storage. You can set up CIFS without using a username/password or a port number. If you choose CIFS, enter the following syntax:

cifs//cifs-share/user/data

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 ASA uses an internal algorithm to store the data in an encrypted form to safeguard it.

Step 2 Type the string, if required, for the security appliance to provide user access to the storage location.

Step 3 Choose one of the following options from the Storage Objects drop-down menu to specify the objects that the server uses in association with the user. The ASA stores these objects to support Clientless SSL VPN connections.

- cookies,credentials
- cookies
- credentials

Step 4 Enter the limit in KB transaction size 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.

Encoding

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 ASA 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.

View or Specify Character Encoding

With encoding, you can view or specify the character encoding for Clientless SSL VPN portal pages.

Procedure

Step 1 Global Encoding Type 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
- unicode
- windows-1252
- none

Note
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 ASA configuration.

Step 2 Enter the name or IP address of a CIFS server for which the encoding requirement differs from the "Global Encoding Type" attribute setting. The ASA retains the case you specify, although it ignores the case when matching the name to a server.

Step 3 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 ASA configuration.

Configure Content Caching

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.

Note Enabling the content cache may cause some systems to become less reliable. If you experience random crashes after enabling the content cache, disable it.

Procedure

Step 1 Select Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Cache.

Step 2 If Enable Cache is unchecked, check it.

Step 3 Define the terms for caching.

- Maximum Object Size—Enter the maximum size in KB of a document that the ASA can cache. The ASA 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 ASA can cache. The ASA 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 ASA 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 for the ASA to cache objects that have neither a last-modified time stamp nor an explicit server-set expiry time.
- Cache static content—Check 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.

Content Rewrite

The Content Rewrite pane lists all applications for which content rewrite is enabled or switched off.

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 may not want some applications and Web resources (for example, public websites) to go through the ASA. The ASA therefore lets you create rewrite rules that let users browse certain sites and applications without going through the ASA. This is similar to split-tunneling in a VPN connection.

These improvements were made to Content Rewriter in ASA 9.0:

- Content rewrite added support for HTML5.
- The Clientless SSL VPN rewriter engines were significantly improved to provide better quality and efficacy. As a result, you can expect a better end-user experience for Clientless SSL VPN users.



Note In ASA 9.9.2, the Content Rewriter is a new Service Worker based client-side rewriter that uses third party libraries to parse HTML and JavaScript. grammar-based parser also transfers a process of content rewriting on the client-side, which makes an ASA performance better.

The grammar-based parser does not have file size limitations and complexity, unlike the old rewriter.

The client-side rewriter can rewrite only JavaScript, CSS, and HTML files.

Follow these guidelines to ensure content rewrite works properly:

- Ensure that you have a valid SSL certificate on ASA and the client system.
- Ensure that you are using a web browser that support Service Worker and Cache features.
  - The enhanced Content Rewriter supports only Chrome and Firefox web browsers.
  - If you are using Firefox, ensure that you are not in private browsing mode.
- If you have an Application Profile Customization Framework (APCF) with the *postprocess-response-body* entity applied to a specific file, the file is rewritten on the server because ASA does not support APCF on the client.

Content Rewrite Limitations

Clientless WebVPN rewriter is not able to detect URL assignments made using JavaScript bracket notation, as they are dynamically set at runtime.

Create Rewrite Rules

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.

The Content Rewrite table has the following columns:

- 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 switched off.
- Resource Mask—Displays the resource mask.

Procedure

Step 1 Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Rewrite.

Step 2 Click Add or Edit to create or update a content rewriting rule.

Step 3 Check **Enable content rewrite** to enable this rule.

Step 4 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.

Step 5 (Optional) Provide an alphanumeric string that describes the rule, maximum 128 characters.

Step 6 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.

Configuration Example for Content Rewrite Rules

Table 2: Content Rewrite Rules

Function	Enable Content Rewrite	Rule Number	Rule Name	Resource Mask
Switch off rewriter for HTTP URLs at youtube.com	Unchecked	1	no-rewrite-youtube	*.youtube.com/*
Enable rewriter for all HTTP URLs that do not match above rules	Check	65,535	rewrite-all	*

Use Email over Clientless SSL VPN

Configure Web email: MS Outlook Web App

The ASA supports Microsoft Outlook Web App to Exchange Server 2010 and Microsoft Outlook Web Access to Exchange Server 2013.

Procedure

Step 1 Enter the URL of the email service into the address field or click an associated bookmark in the Clientless SSL VPN session.

Step 2 When prompted, enter the email server username in the format domain\username.

Step 3 Enter the email password.

Configure Bookmarks

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

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

You can now use bookmarks with macro substitutions for auto sign-on on some Web pages. The former POST plug-in approach was created so that administrators could specify a POST bookmark with sign-on macros and receive a kick-off page to load prior to posting the POST request. This POST plug-in approach eliminated those requests that required the presence of cookies or other header items. Now an an administrator determines the pre-load page and URL, which specifies where the post login request is sent. A pre-load page enables an endpoint browser to fetch certain information that is sent along to the webserver or Web application rather than just using a POST request with credentials.

The existing bookmark lists are displayed. You can add, edit, delete, import, or export the bookmark list. You can configure lists of servers and URLs for access and order the items in the designated URL list.

Before you begin

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. Switch off URL Entry on these policies to prevent user confusion over what is accessible.

Procedure

Step 1 Specify the name of the list to be added or choose the name of the list to be modified or deleted.

The bookmark title and actual associated URL are displayed.

Step 2 (Optional) Click **Add** to configure a new server or URL. You can add one of the following:

- Add a Bookmark for a URL with a GET or Post Method
- Add a URL for a Predefined Application Template
- Add a Bookmark for an Auto Sign-on Application

Step 3 (Optional) Click **Edit** to make changes to the server, URL, or display name.

Step 4 (Optional) Click **Delete** to remove the selected item from the URL list. No confirmation or undo exists.

Step 5 (Optional) Choose the location from which 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 ASA.
- Remote server—Click to import a file that resides on a remote server accessible from the ASA.
- 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.

Step 6 (Optional) Highlight a bookmark and click **Assign** to assign the selected bookmark to one or more group policies, dynamic access policies, or LOCAL users.

Step 7 (Optional) Change the position of the selected item in the URL list using the **Move Up** or **Move Down** options.

Step 8 Click OK.

What to do next

Read about Clientless SSL VPN Security Precautions.

Add a Bookmark for a URL with a GET or Post Method

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

Before you begin

To access a shared folder on your network, use the format \\server\share\subfolder\<personal folder>. The user must have list permission for all points above <personal folder>.

Procedure

Step 1 Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Bookmarks**, and click the **Add** button.

Step 2 Select **URL with GET or POST Method** to use for bookmark creation.

Step 3 Enter a name for this bookmark, which will be displayed on the portal.

Step 4 Use the URL drop-down menu to choose the URL type: http, https, cifs, or ftp. The URL drop-down shows standard URL types, plus types for all the plug-ins you installed.

Step 5 Enter the DNS name or IP address for this bookmark (URL). 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*

Example:

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

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

To provide single sign-on support for a plug-in, use the parameter-value pair **csco_sso=1**:

host/**?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

Step 6 (Optional) Enter a preload URL. When you enter a preload URL, you can also enter the wait time, which is the time you allow for loading of the page until you are forwarded to the actual POST URL.

Step 7 As a subtitle, provide additional user-visible text that describes the bookmark entry.

Step 8 Use the Thumbnail drop-down menu to choose an icon to associate with the bookmark on the end-user portal.

Step 9 Click **Manage** to import or export images to use as thumbnails.

Step 10 Click to open the bookmark in a new window that uses the smart tunnel feature to pass data through the ASA 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.

Step 11 Check **Allow the Users to Bookmark the Link** 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 Clientless SSL VPN portal.

Step 12 (Optional) Choose **Advanced Options** to configure further bookmark characteristics.

- URL Method—Choose **Get** for simple data retrieval. Choose **Post** when processing the data may involve changes to it, for example, storing or updating data, ordering a product, or sending email.
- Post Parameters—Configure the particulars of the Post URL method.

Add a URL for a Predefined Application Template

This option simplifies bookmark creation with users selecting a predefined ASDM template that contains the pre-filled necessary values for certain well-defined applications.

Before you begin

Predefined application templates are currently available for the following applications only:

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

Procedure

Step 1 Enter a name for the bookmark to display for the user.

Step 2 As a subtitle, provide additional user-visible text that describes the bookmark entry.

Step 3 Use the Thumbnail drop-down menu to choose an icon to associate with the bookmark on the end-user portal.

Step 4 Click **Manage** to import or export images to use as thumbnails.

Step 5 (Optional) Select the Place This Bookmark on the VPN Home Page check box.

Step 6 In the Select Auto Sign-on Application list, click the required application. The available applications are:

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

Step 7 Enter the URL of the page which is loaded before the login page. This page will require user interaction to proceed to the login screen. The URL will allow * to substitute an arbitrary number of symbols, for example http*://www.example.com/test.

Step 8 Enter the Pre-login Page Control ID. This is the ID of the control / tag that will get a click event on the pre-login page URL to proceed to the login page.

Step 9 Enter the Application Parameters. Depending on the application these may include the following:

- Protocol. HTTP or HTTPs.
- hostname. For example www.cisco.com.
- Port Number. The port used by the application.
- URL Path Appendix. For example /Citrix/XenApp. This is normally auto-populated.

- Domain. The domain to connect to.
- User Name. The SSL VPN variable to use as a user name. Click Select Variable to choose a different variable.
- Password. The SSL VPN variable to use as a password. Click Select Variable to choose a different variable.

Step 10 (Optional) Click **Preview** to view the template output. You can click Edit to modify the template.

Step 11 Click **OK** to make your changes. Alternatively, click Cancel to abandon your changes.

Add a Bookmark for an Auto Sign-On Application

This option lets you create a bookmark for any complex auto sign-on application.

Configuring auto sign-on applications requires two steps:

1. Define the bookmark with some basic initial data and without the POST parameters. Save and assign the bookmark to use in a group or user policy.
2. Edit the bookmark again. Use the capture function to capture the SSL VPN parameters and edit them in the bookmark.

Procedure

Step 1 Enter a name for the bookmark to display for the user.

Step 2 Use the URL drop-down menu to choose 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 to display the plug-in as a link on the portal page.

Step 3 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*

Example:

For example, the particular plug-in determines the optional parameter-value pairs that you can enter.

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

To provide single sign-on support for a plug-in, use the parameter-value pair **csco_sso=1**.

```
host/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```

Step 4 As a subtitle, provide additional user-visible text that describes the bookmark entry.

Step 5 Use the Thumbnail drop-down menu to choose an icon to associate with the bookmark on the end-user portal.

Step 6 Click **Manage** to import or export images to use as thumbnails.

Step 7 (Optional) Select the Place This Bookmark on the VPN Home Page check box.

Step 8 Enter the Login Page URL. Wildcards can be used in the URL you enter. For example, you can enter http*://www.example.com/myurl*.

Step 9 Enter the Landing Page URL. The ASA requires the Landing Page to be configured to detect a successful login to the application.

Step 10 (Optional) Enter a Post Script. Some Web applications, such as Microsoft Outlook Web Access, may execute a JavaScript to change the request parameters before the log-on form is submitted. The Post Script field enables you to enter JavaScript for such applications.

Step 11 Add the required Form Parameters. For each required SSL VPN Variable, click Add, enter a Name, and choose a variable from the list. You can click Edit to change parameters and Delete to remove them.

Step 12 Enter the URL of the page which is loaded before the login page. This page will require user interaction to proceed to the login screen. The URL will allow * to substitute an arbitrary number of symbols, for example http*://www.example.com/test.

Step 13 Enter the Pre-login Page Control ID. This is the ID of the control / tag that will get a click event on the pre-login page URL to proceed to the login page.

Step 14 Click OK to make your changes. Alternatively, click Cancel to abandon your changes.

What to do Next

What to do next

When you edit the bookmark you can use the HTML Parameter Capture function to capture the VPN auto sign-on parameters. The bookmark must have been saved and assigned first to a group policy or user.

Enter the SSL VPN Username then click Start Capture. Then use a Web browser to start the VPN session and navigate to the intranet page. To complete the process, click **Stop Capture**. The parameters will then be available for editing and inserted in the bookmark.

Import and Export a 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.

Procedure

Step 1 Identify the bookmark list by name. Maximum is 64 characters, no spaces.

Step 2 Choose a method 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 ASA.
- Remote server—Click to import a url list file that resides on a remote server accessible from the ASA.
- 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.

Import and Export GUI Customization Objects (Web Contents)

This dialog box lets you import and export Web content objects. The names of the Web content objects and their file types are displayed.

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

Procedure

Step 1 Choose the location from which 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 ASA.
- Remote server—Click to import a file that resides on a remote server accessible from the ASA.
- 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.

Step 2 Determine whether authentication is required to access the content.

The prefix to the path changes depending on whether you require authentication. The ASA uses /+CSCOE+/ for objects that require authentication, and /+CSCOU+/ for objects that do not. The ASA displays /+CSCOE+/ objects on the portal page only, while /+CSCOU+/ objects are visible and usable in either the logon or the portal pages.

Step 3 Click to import or export the file.

Add and Edit POST Parameters

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

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.

Procedure

Step 1 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 3: 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 cache and not authenticated by a AAA server. If a user enters thi used as the password for auto sign-on, instead of the passv
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN user login group drop-down, a group alias within t profile
5	CSCO_WEBVPN_MACRO1	Set via the RADIUS/LDAP vendor-specific attribute. If yo this from LDAP via an ldap-attribute-map, the Cisco attril this variable is WEBVPN-Macro-Substitution-Value1. Variable substitution via RADIUS is performed by VSA#1
6	CSCO_WEBVPN_MACRO2	Set via the RADIUS/LDAP vendor-specific attribute. If yo this from LDAP via an ldap-attribute-map, the Cisco attril this variable is WEBVPN-Macro-Substitution-Value2. Variable substitution via RADIUS is performed by VSA#1
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.
11	CSCO_WEBVPN_DYNAMIC_URL	A single bookmark that can generate multiple bookmark l user's portal.
12	CSCO_WEBVPN_MACROLIST	A statically configured bookmark which can use arbitraril provided by LDAP attribute maps.

When the ASA 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 a link to a free browser capture tool, also called an HTTP analyzer: http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe.

Step 2 Use the following guidelines to choose the appropriate variables:

- Use Variables 1 to 4—The ASA 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 ASA 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 ASA map a file
 drive to specific users:
For USER1, the link becomes cifs://server/users/USER1
For USER 2, the link is cifs://server/users/USER2
```

- Use Variables 5 and 6—Values for macros 5 and 6 are RADIUS or LDAP vendor-specific attributes (VSAs). These enable you to set substitutions configured on either a RADIUS or an LDAP server.
- Use Variables 7 to 10—Each time the ASA 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.

```
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.
```

- Use Variable 11—These bookmarks are generated based upon the LDAP attribute map in which CSCO_WEBVPN_DYNAMIC_URL is mapped. Using the *delimiter*parameter, the string received from LDAP is parsed into a list of values. When used in the url field or as a POST parameter in the bookmark, a bookmark for each value from the parsed LDAP string is generated. An example bookmark configuration using CSCO_WEBVPN_DYNAMIC_URL is provided below:

```
<bookmark>
    <title>Test Bookmark</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://CSCO_WEBVPN_DYNAMIC_URL1(".")</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url></login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <<post-param>
        <value>value1</value>
        <name>parameter1</name>
    </post-param>
</bookmark>
```

CSCO_WEBVPN_DYNAMIC_URL is configured in an LDAP attribute map and maps to host1.cisco.com, host2.cisco.com, and host3.cisco.com. According to the delimiter, you get three individual URLs and

three bookmarks generated from this single configuration with http://host1.cisco.com, http://host2.cisco.com, and http://host3.cisco.com.

Additionally, you can use this macro as part of the POST parameters:

```
<bookmark>
    <title>Test Bookmark</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://www.myhost.cisco.com</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url></login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <post-param>
        <value>CSCO_WEBVPN_DYNAMIC_URL(";")</value>
        <name>host</name>
    </bookmark>
```

Using the same mapped LDAP attributes, three bookmarks with target URL http://www.myhost.cisco.com are created, each with a different post parameter and with name *host*and values host1.cisco.com, host2.cisco.com, and host3.cisco.com.

Note
You can use CSCO_WEBVPN_DYNAMIC_URL only in bookmarks. You cannot use it in other places which support macros, such as vdi CLI configuration for Citrix mobile receiver. It cannot be used to define the external portal page.

- Use Variable 12—This macro takes three parameters as input: index, delimiter, and escape. *Index*is an administrator-supplied integer which specifies the number of elements in the list to select. *Delimiter*is an administrator-supplied string which includes the characters used to separate the LDAP-mapped string into a list of values, using one delimiter per use of the macro. *Escape*is the choice to apply the LDAP string before it is substituted into the ASA's request.

  For example, CSCO_WEBVPN_MACROLIST(2, ",", url-encode) specifies to use the second value in the list and to separate the string into a list using a single comma as a separator. The value is URL encoded when it is substituted into the ASA's request to the backend. For escape routine, the following values are used:

  - *None*—No transformation occurs on the string value before sending to the backend server.
  - *url-code*—Each parsed value is URL encoded, except for a list of reserved characters that make up the special characters in a URL.
  - *url-encode-data*—Each parsed value is transformed fully with URL encoding.
  - *base64*—Each parsed value is base 64 encoded.

  An example bookmark configuration using the CSCO_WEBVPN_MACROLIST1 is provided below:

```
<bookmark>
    <title>MyHost</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://www.myhost.cisco.com</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
```

```
    <login-page-url><login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <post-param>
        <value>CSCO_WEBVPN_MACROLIST1(1, ";", url-encode-data)>/value>
        <name>param1</name>
        <value>CSCO_WEBVON_MACROLIST1(2, ";", url-encode-data)</value>
        <name>param2</name>
        <value>CSCO_WEBVPN_MACROLIST1(3, ";", url-encode-data)</value>
        <name>param3</name>
    </post-param>
</bookmark>
```

Using this bookmark, you can browse to www.myhost.cisco.com and automatically have 3 POST parameters sent to the server: param1, param2, and param3. The ASA substitutes the values for CSCO_WEBVPN_MACROLIST1 into the parameters before sending to the backend.

Note
You can use CSCO_WEBVPN_MACROLIST wherever other macros are used.

- The best way to do this is to configure the Homepage URL parameter in ASDM. Without writing a script or uploading anything, an administrator can specify which homepage in the group policy to connect with via smart tunnel. Go to the Add/Edit Group Policy pane, from either the Network Client SSL VPN or Clientless SSL VPN Access section of ASDM. 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

Step 3 Set a bookmark or URL entry. You can use an HTTP Post to log on to an OWA resource using an RSA one-time password (OTP) for SSL VPN authentication, and then the static, internal password for OWA email access. The best way to do this is to add or edit a bookmark entry in ASDM with one of the following paths.

- 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)
- 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

Step 4 Set a more flexible bookmark configuration by configuring File Share (CIFS) URL substitutions. If you configure the URL cifs://server/CSCO_WEBVPN_USERNAME, the ASA 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
```

Customize External Ports

You can use the external portal feature to create your own portal instead of using the pre-configured one. If you set up your own portal, you can bypass the clientless portal and send a POST request to retrieve your portal.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Customization**. Highlight the desired customization and choose **Edit**.

Step 2 Check the Enable External Portal check box.

Step 3 In the URL field, enter the desired external portal so that POST requests are allowed.