CHAPTER 12

Advanced Clientless SSL VPN Configuration

June 18, 2014

Microsoft Kerberos Constrained Delegation Solution

Many organizations want to authenticate their Clientless VPN users and extend their authentication credentials seamlessly to web-based resources using authentication methods beyond what the ASA SSO feature can offer today. With the growing demand to authenticate remote access users with smart cards and One-time Passwords (OTPs), the SSO feature falls short in meeting that demand, because it forwards only conventional user credentials, such as static username and password, to clientless web-based resources when authentication is required.

For example, neither certificate- nor OTP-based authentication methods encompass a conventional username and password necessary for the ASA to seamlessly perform SSO access to web-based resources. When authenticating with a certificate, a username and password are not required for the ASA to extend to web-based resources, making it an unsupported authentication method for SSO. On the other hand, OTP does include a static username; however, the password is dynamic and will subsequently change throughout the VPN session. In general, Web-based resources are configured to accept static usernames and passwords, thus also making OTP an unsupported authentication method for SSO.

Microsoft's Kerberos Constrained Delegation (KCD), a new feature introduced in software release 8.4 of the ASA, provides access to Kerberos-protected Web applications in the private network. With this benefit, you can seamlessly extend certificate- and OTP-based authentication methods to Web applications. Thus, with SSO and KCD working together although independently, many organizations can now authenticate their clientless VPN users and extend their authentication credentials seamlessly to Web applications using all authentication methods supported by the ASA.

Requirements

In order for the **kcd-server** command 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, using its unique format, 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.

Understanding 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 Microsoft Web services protected by Kerberos. Examples of such Web services or applications include Outlook Web Access (OWA), Sharepoint, and Internet Information Server (IIS).

Note Web services from providers other than Microsoft are not currently supported.

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.

Protocol 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.

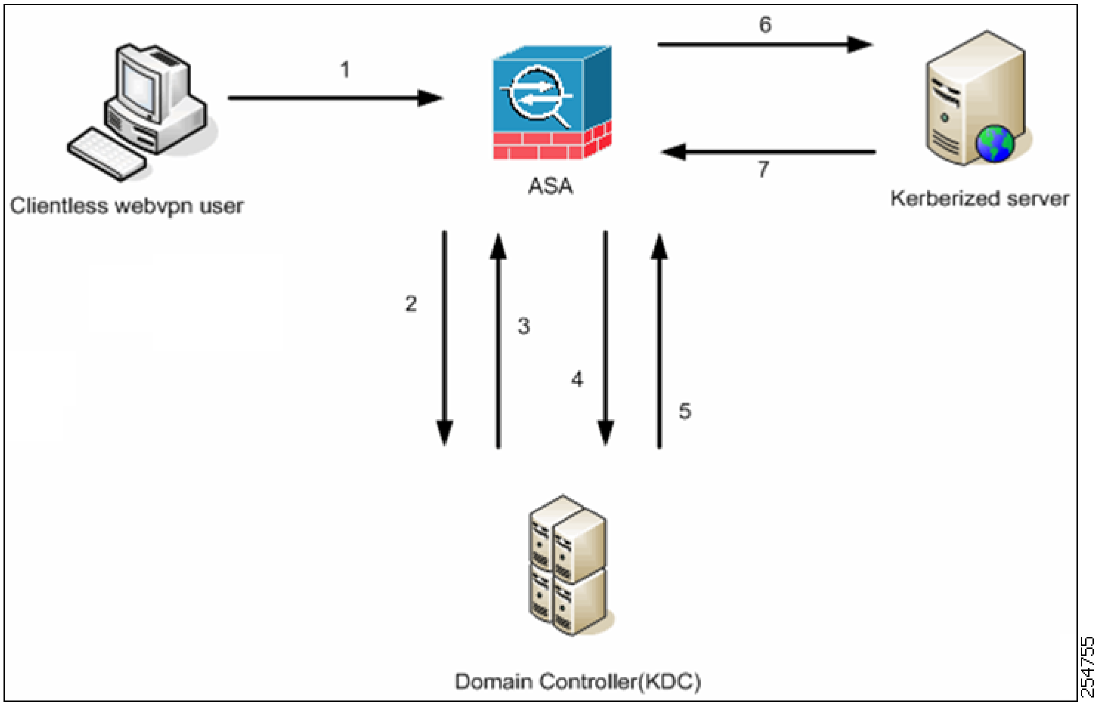
For more information on constrained delegation, see RFC 1510 via the IETF website (http://www.ietf.org).

Authentication Flow with KCD

Figure 12-1 depicts the packet and process flow a user will experience 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 12-1 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, 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.ASA requests a service ticket from the KDC 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 ASA using a non-Kerberos authentication protocol is transparently authenticated to the key distribution center using Kerberos.

4. 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. 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 acknowledgement if there is an authentication failure. If the Kerberos authentication fails, the expected behavior is to fall back to basic authentication.

Adding a Windows Service Account in Active Directory

The KCD implementation on the ASA requires a service account, or in other words, an Active Directory user account with privileges necessary to add computers, such as adding the ASA to the domain. For our example, the Active Directory username JohnDoe depicts a service account with the required privileges. For more information on how to implement user privileges in Active Directory, contact Microsoft Support or visit http://microsoft.com.

Configuring DNS for KCD

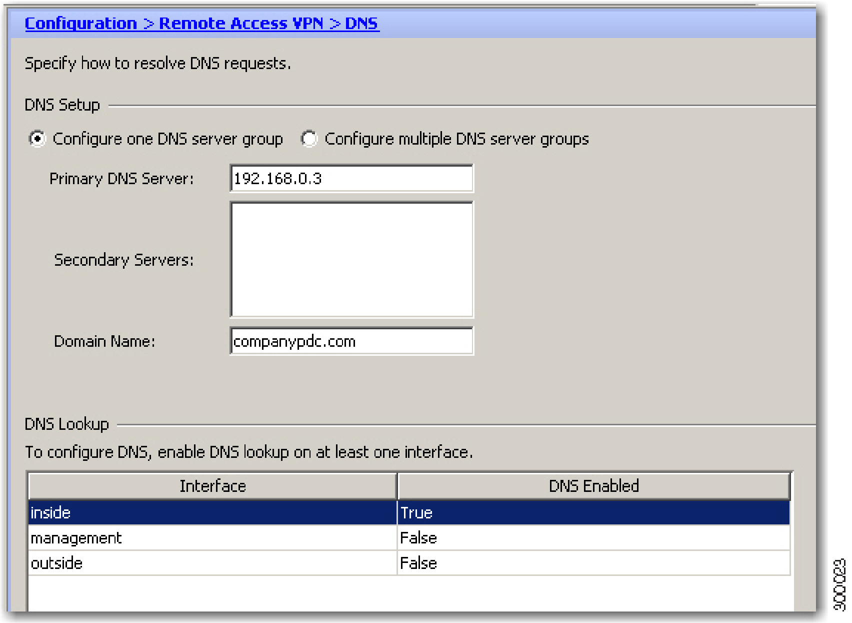
This section outlines configuration procedures necessary to configure DNS on the ASA. When using KCD as the authentication delegation method on the ASA, DNS is required to enable hostname resolution and communication between the ASA, Domain Controller (DC), and services trusted for delegation.

Step 1 From ASDM, navigate to **Configuration > Remote Access VPN > DNS** and configure the DNS setup as shown in Figure 12-2:

- DNS Server Group—Enter the DNS server IP address(es), such as 192.168.0.3.
- Domain Name—Enter the domain name in which the DC is a member.

Step 2 Enable DNS Lookup on the appropriate interface. Clientless VPN deployments require DNS Lookups via the internal corporate network, typically the *inside* interface.

Figure 12-2 ASA DNS Configuration Example



Configuration > Remote Access VPN > DNS

Specify how to resolve DNS requests.

DNS Setup

● Configure one DNS server group ○ Configure multiple DNS server groups

Primary DNS Server: 192.168.0.3

Secondary Servers:

Domain Name: companypdc.com

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
management	False
outside	False

Configuring the ASA to Join the Active Directory Domain

This section outlines configuration procedures necessary to enable the ASA to act as part of the Active Directory domain. KCD requires the ASA to be a member of the Active Directory domain. This configuration enables the functionality necessary for constrained delegation transactions between the ASA and the KCD server.

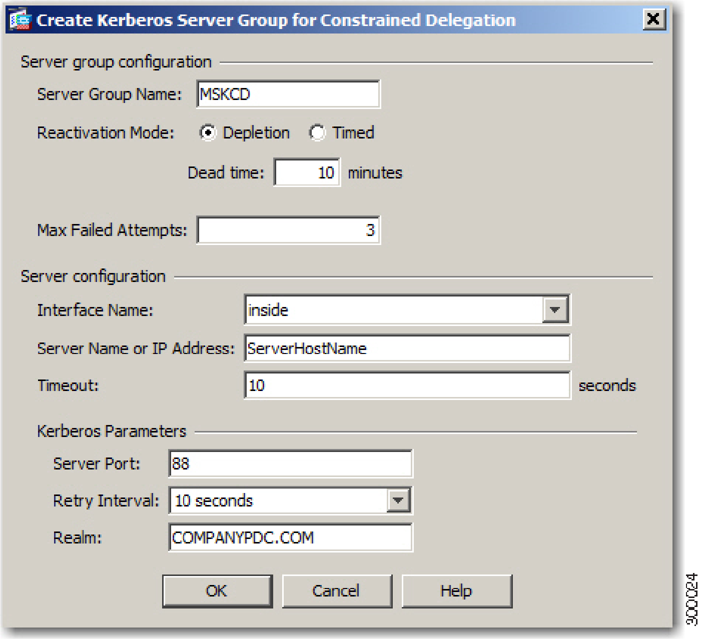
Step 1 From ASDM, navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Microsoft KCD Server**, as shown in Figure 12-4.

Step 2 Click **New** to add a Kerberos server group for constrained delegation and configure the following (see Figure 12-4):

- Server Group Configuration
  - Server Group Name—Define the name of the constrained delegation configuration on the ASA, such as MSKCD, which is the default value. You can configure multiple server groups for redundancy; however, you can assign only one server group to the KCD server configuration used to request service tickets on behalf of VPN users.
  - Reactivation Mode—Click the radio button for the required mode (**Depletion** or **Timed**). In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive. In Timed mode, failed servers are reactivated after 30 seconds of downtime. Depletion is the default configuration.
  - Dead Time—If you choose the Depletion reactivation mode, you must add a dead time interval. Ten minutes is the default configuration. The interval represents the duration of time, in minutes, that elapses between the deactivating of the last server in a group and the subsequent re-enabling of all servers.

  - Max Failed Attempts—Set the number of failed connection attempts allowed before declaring an unresponsive server to be inactive. Three attempts is the default.
- Server Configuration
  - Interface Name—Choose the interface on which the server resides. In general, authentication server deployments reside on the internal corporate network, typically via the *inside* interface.
  - Server Name—Define the hostname of the domain controller, such as ServerHostName.
  - Timeout—Specify the maximum time, in seconds, to wait for a response from the server. Ten seconds is the default.
- Kerberos Parameter
  - Server Port—88 is the default and the standard port used for KCD.
  - Retry Interval—Choose the desired retry interval. Ten seconds is the default configuration.
  - Realm—Enter the domain name of the DC in all uppercase. The KCD configuration on the ASA requires the realm value to be in uppercase. A realm is an authentication domain. A service can accept authentication credentials only from entities in the same realm. The realm must match the domain name that the ASA joins.

Figure 12-3 KCD Server Group Configuration



Create Kerberos Server Group for Constrained Delegation

Server group configuration

Server Group Name: MSKCD

Reactivation Mode: ● Depletion ○ Timed

Dead time: 10 minutes

Max Failed Attempts: 3

Server configuration

Interface Name: inside

Server Name or IP Address: ServerHostName

Timeout: 10 seconds

Kerberos Parameters

Server Port: 88

Retry Interval: 10 seconds

Realm: COMPANYPDC.COM

Step 3 Click **OK** to apply your configuration and then configure the Microsoft KCD server to request service tickets on behalf of the remote access user (see Figure 12-4). The Microsoft KCD Server configuration window appears upon clicking **OK**.

Configuring 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.

Restrictions

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

DETAILED STEPS

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.

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 Sign-on using basic HTTP and/or NTLMv1 authentication.
- HTTP Form protocol, or Computer Associates eTrust SiteMinder (formerly Netegrity SiteMinder).
- SAML, Version 1.1 Browser Post Profile.

Restrictions

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.

- Configuring SiteMinder and SAML Browser Post Profile, page 12-8—Configures SSO with basic HTTP or NTLM authentication.
- Configuring Session Settings—Configures SSO with the HTTP Form protocol.

The SSO mechanism starts either as part of the AAA process (HTTP Form) 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 ASA 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 ASA 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 (for example RADIUS, LDAP). 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 ASA, for SiteMinder SSO, you must also 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.

DETAILED STEPS

Use the SAML server documentation provided by the server software vendor to configure the SAML server in Relying Party mode. The following fields are displayed:

- 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 ASA currently supports the SiteMinder type and the SAML Browser Post Profile type.
- URL—*Display only.* Displays the SSO server URL to which the ASA 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 ASA 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.
- Assign—Highlight an SSO server and click this button to assign the selected server to one or more VPN group policies or user policies.

Step 1 Configure the SAML server parameters to represent the asserting party (the ASA):

- Recipient consumer (Web Agent) URL (same as the assertion consumer URL configured on the ASA)
- Issuer ID, a string, usually the hostname of the 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 ASA for SSO with SiteMinder, you must also configure your CA SiteMinder policy server with the Cisco authentication scheme, provided as a Java plug-in. This section presents general steps, 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.

Prerequisites

Configuring the SiteMinder policy server requires experience with SiteMinder.

DETAILED STEPS

Step 1 With the SiteMinder Administration utility, create a custom authentication scheme being sure to use the following specific values:

- 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/cisco/software/navigator.html and copy it to the default library directory for the SiteMinder server. This .jar file is also available on the Cisco ASA CD.

Adding or Editing 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, page 12-18. To set use basic HTML or NTLM authentication, use the **auto sign-on** command at the command-line interface.

DETAILED STEPS

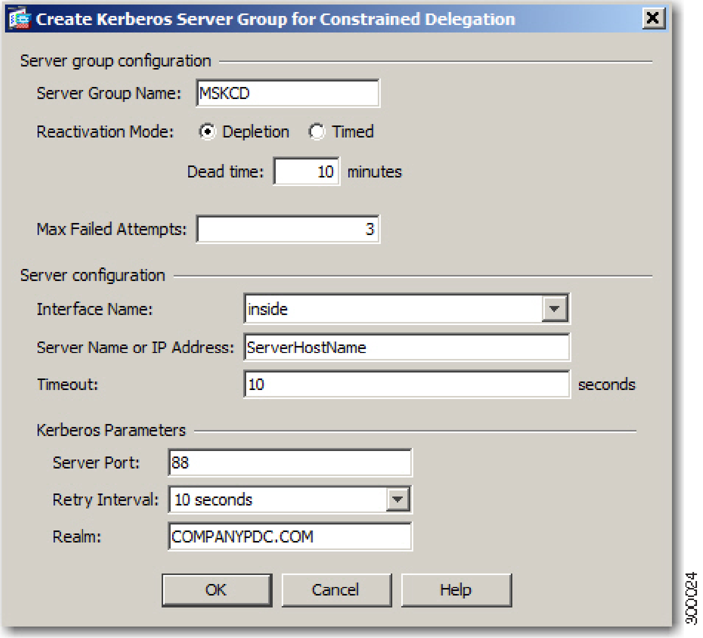
Step 1 If adding a server, enter the name of the new SSO server. If editing a server, this field is display only; it displays the name of the selected SSO server.

Step 2 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 ASA, the SSO server, and the SiteMinder policy server using the Cisco Java plug-in authentication scheme.

Step 3 Enter the number of times thatthe ASA 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.

Step 4 Enter the number of seconds before a failed SSO authentication attempt times out. The range is from1 to 30 seconds inclusive, and the default is 5 seconds.

Figure 12-4 KCD Server Group Configuration



Create Kerberos Server Group for Constrained Delegation

Server group configuration

Server Group Name: MSKCD

Reactivation Mode: ● Depletion ○ Timed

Dead time: 10 minutes

Max Failed Attempts: 3

Server configuration

Interface Name: inside

Server Name or IP Address: ServerHostName

Timeout: 10 seconds

Kerberos Parameters

Server Port: 88

Retry Interval: 10 seconds

Realm: COMPANYPDC.COM

Step 5 Click **OK** to apply your configuration and then configure the Microsoft KCD Server to request service tickets on behalf of the remote access user (see Figure 12-4). The Microsoft KCD Server configuration window appears upon clicking **OK**.

Configuring Kerberos Server Groups

The Kerberos Server Group for Constrained Delegation, MSKCD, is automatically applied to the KCD Server Configuration. You can also configure Kerberos Server groups and manage them under **Configuration > Remote Access VPN > AAA/Local User > AAA Server Groups**.

Step 1 Under the Server Access Credential section, configure the following:

- Username—Define a Service Account (Active Directory username) such as JohnDoe, which has been granted privileges necessary to add computer accounts to the Active Directory domain. The username does not correspond to a specific administrative user but simply to a user with service-level privileges. This service account is used by the ASA to add a computer account for itself to the Active Directory domain at every reboot. You must configure the computer account separately to request Kerberos tickets on behalf of the remote users.

Note Administrative privileges are required for initial join. A user with service-level privileges on the domain controller will not get access.

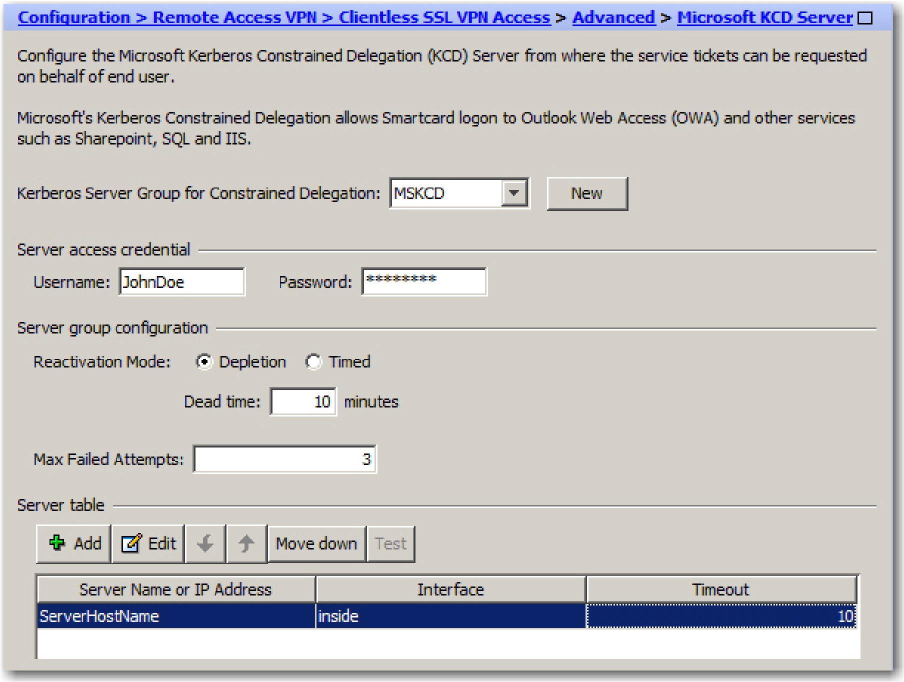
- Password—Define the password associated with the username (such as Cisco123). The password does not correspond to a specific password but simply to a service-level password privilege to add a device on the Window domain controller.

Step 2 Under the Server Group Configuration section, configure the following:

- Reactivation Mode—Click the mode to use (**Depletion** or **Timed**). In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive. In Timed mode, failed servers are reactivated after 30 seconds of down time. Depletion is the default configuration.
- Dead Time—If you choose the Depletion reactivation mode, you must add a dead time interval. The interval represents the duration of time, in minutes, that elapses between the deactivating of the last server in a group and the subsequent re-enabling of all servers. Ten minutes is the default.
- Max Failed Attempts—Set the number of failed connection attempts allowed before declaring a nonresponsive server to be inactive. Three attempts is the default.

Note Under the Server Table section, the previously configured DC hostname, ServerHostName, was automatically applied to the KCD server configuration (see Figure 12-5).

Figure 12-5 KCD Server Configuration



Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Microsoft KCD Server

Configure the Microsoft Kerberos Constrained Delegation (KCD) Server from where the service tickets can be requested on behalf of end user.

Microsoft's Kerberos Constrained Delegation allows Smartcard logon to Outlook Web Access (OWA) and other services such as Sharepoint, SQL and IIS.

Kerberos Server Group for Constrained Delegation: MSKCD New

Server access credential

Username: JohnDoe Password: *********

Server group configuration

Reactivation Mode: ● Depletion ○ Timed

Dead time: 10 minutes

Max Failed Attempts: 3

Server table

Add Edit Move down Test

Server Name or IP Address	Interface	Timeout
ServerHostName	inside	10

300025

Step 3 Click **Apply**.

Note After applying your configuration, the ASA automatically starts the process of joining the Active Directory domain. The ASA's hostname appears in the Computers directory in Active Directory Users and Computers.

To confirm if the ASA has successfully joined the domain, execute the following command from the ASA prompt.:

```
host# show webvpn kcd
Kerberos Realm: WEST.LOCAL
Domain Join: Complete
```

Configuring Bookmarks to Access the Kerberos Authenticated Services

To access Kerberos authenticated services such as Outlook Web Access using the ASA clientless portal, you must configure bookmark lists. Bookmark lists are assigned and displayed to remote access users based on the VPN security policies that they are associated with.

Restrictions

When creating a bookmark to an application that uses Kerberos constrained delegation (KCD), do not check Enable Smart Tunnel.

DETAILED STEPS

Step 1 Navigate to **Configuration > Remote Access VPN > Clientless VPN Access > Portal > Bookmarks** in the ASDM GUI.

Step 2 In Bookmark List, enter the URL to reference for the service location.

Configuring 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.

Restrictions

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

Managing 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.

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 select 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.

Uploading APCF Packages

DETAILED STEPS

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**

Managing APCF Packets

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 Table 12-1.

Guidelines

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 12-1 APCF XML Tags

Tag	Use
<APCF>...</APCF>	The mandatory root element that opens any APCF XML file.
<version>1.0</version>	The mandatory tag that specifies the APCF implementation version. Currently the only version is 1.0.

Table 12-1 APCF XML Tags (continued)

Tag	Use
<application>...</application>	The mandatory tag that wraps the body of the XML description.
<id> text </id>	The mandatory tag that describes this particular APCF functionality.
<apcf-entities>...</apcf-entities>	The mandatory tag that wraps a single or multiple APCF entities.
<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 stage at which the APCF processing should take place.
<conditions>… </conditions>	A child element of the pre/post-process tags that specifies 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" | "A".."Z" | "0".."9" | ".-_*[]?") • server-fnmatch (regular expression containing ("a".."z" | "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, the ASA performs a logical AND for all tags.
<action> … </action>	Wraps one or more actions to perform on the content under specified conditions; you can use the following tags to define these actions (shown below): • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

Table 12-1 APCF XML Tags (continued)

Tag	Use
<do>…</do>	Child element of the action tag used to define one of the following actions: • <no-rewrite/>—Do not mangle the content received from the remote server. • <no-toolbar/>—Do not insert the toolbar. • <no-gzip/>—Do not compress the content. • <force-cache/>—Preserve the original caching instructions. • <force-no-cache/>—Make object non-cacheable. • < downgrade-http-version-on-backend>—Use HTTP/1.0 when sending the request to remote server.
<sed-script> TEXT </sed-script>	Child element of the action tag used to change the content of text-based objects. The Text must be a valid Sed script. The <sed-script> applies to the <conditions> tag defined before it.
<rewrite-header></rewrite-header>	Child element of the action tag. Changes the value of the HTTP header specified in the child element <header> tag shown below.
<add-header></add-header>	Child element of the action tag used to add a new HTTP header specified in the child element <header> tag shown below.
<delete-header></delete-header>	Child element of the action tag used to delete the specified HTTP header specified by the child element <header> tag shown below.

<header></header>	Specifies the name HTTP header to be rewritten, added, or deleted. For example, the following tag changes the value of the HTTP header named Connection:
	`<rewrite-header>`
	`<header>Connection</header>`
	`<value>close</value>`
	`</rewrite-header>`

Configuration Examples for APCF

Example:

```
<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>
```

Example:

```
<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>
```

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.

DETAILED STEPS

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 pass 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

With encoding, you can 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 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.

DETAILED STEPS

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

Note

- 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.

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.

DETAILED STEPS

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 to 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.

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.

Configuration Example for Content Rewrite Rules, page 12-22 shows example content rewrite rules.

Note 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.

DETAILED STEPS

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.

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 an content rewriting rule.

Step 3 Enable content rewrite must be checked 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 12-2 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	*

Using Email over Clientless SSL VPN

Clientless SSL VPN supports several ways to access email. This section includes the following methods:

- Configuring Email Proxies
- Configuring Web email: MS Outlook Web App

Configuring Email Proxies

Clientless SSL VPN supports IMAP, POP3, and SMTP email proxies. The following attributes apply globally to email proxy users.

Restrictions

email clients such as MS Outlook, MS Outlook Express, and Eudora lack the ability to access the certificate store.

Configuring 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 2007, 2003, and 2000.

DETAILED STEPS

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.

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.

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.

Guidelines

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. See Clientless SSL VPN Security Precautions, page 11-1 for instructions.

DETAILED STEPS

Step 1 Specify the name of the list to be added or select 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. See these procedures for additional information:

- Adding a Bookmark for a URL with a GET or Post Method, page 12-24
- Adding a URL for a Predefined Application Template, page 12-26
- Adding a Bookmark for an Auto Sign-On Application, page 12-27

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.**

Adding 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.

Prerequisites

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*>.

DETAILED STEPS

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 select 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*

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 **csco_sso=1**. For example:

*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 select 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/Edit—Click to add a post parameter.
- Edit—Click to edit the highlighted post parameter.
- Delete—Click to delete the highlighted post parameter.

Adding 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.

Prerequisites

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

DETAILED STEPS

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 select 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

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.
- P**assword**. 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.

Adding a Bookmark for an Auto Sign-On Application

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

Prerequisites

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.

DETAILED STEPS

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

Step 2 Use the URL 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 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*

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 **csco_sso=1**. For example:

*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 select 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 select 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.

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.

Importing and Exporting 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.

DETAILED STEPS

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.

Importing and Exporting 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. Import Web contents that are ready for use. Export Web contents to modify or edit them, and then reimport.

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.

Adding and Editing 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.

DETAILED STEPS

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 12-3 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.

Table 12-3 Clientless SSL VPN Variables

No.	Variable Substitution	Definition
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 sign-on, instead of the password value.
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN user login group drop-down, a group alias within the connection profile
5	CSCO_WEBVPN_MACRO1	Set via the 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 the 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 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.

Using 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

Using 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.

Using 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.

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. 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.

Configuration Example for Setting 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.

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.

Configuration Example for 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 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

Customizing 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.

DETAILED STEPS

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.