Configuring Clientless SSL VPN

This chapter describes how to configure clientless SSL VPN and includes the following sections:

- Information About Clientless SSL VPN, page 1-1
- Licensing Requirements, page 1-2
- Prerequisites for Clientless SSL VPN, page 1-4
- Guidelines and Limitations, page 1-4
- Configuring Application Profile Customization Framework, page 1-11
- Using Single Sign-on with Clientless SSL VPN, page 1-16
- Encoding, page 1-33
- Configuring Connection Profile Attributes for Clientless SSL VPN, page 1-35
- Understanding How KCD Works, page 1-45
- Configuring Application Access, page 1-51
- Configuring Port Forwarding, page 1-63
- Application Access User Notes, page 1-70
- Configuring File Access, page 1-73
- Ensuring Clock Accuracy for SharePoint Access, page 1-77
- Using Clientless SSL VPN with PDAs, page 1-77
- Using E-Mail over Clientless SSL VPN, page 1-77
- Configuring Portal Access Rules, page 1-79
- Clientless SSL VPN End User Setup, page 1-83
- Configuring Browser Access to Client-Server Plug-ins, page 1-99
- Changing a Group Policy or User Attributes to Use the Customization Object, page 1-118
- Capturing Data, page 1-119

Information About Clientless SSL VPN

Note

When the ASA is configured for clientless SSL VPN, you cannot enable security contexts (also called firewall multimode) or Active/Active stateful failover. Therefore, these features become unavailable.
Clientless SSL VPN lets users establish a secure, remote-access VPN tunnel to an ASA using a web browser. Users do not need a software or hardware client.

Clientless SSL VPN provides secure and easy access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach HTTP Internet sites. They include:

- Internal websites
- Web-enabled applications
- NT/Active Directory file shares
- E-mail proxies, including POP3S, IMAP4S, and SMTPS
- Microsoft Web App to Exchange Server 2010 in 8.4(2) and later.
- Application Access (that is, smart tunnel or port forwarding access to other TCP-based applications)

Clientless SSL VPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide the secure connection between remote users and specific, supported internal resources that you configure at an internal server. The ASA recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to resources by users of clientless SSL VPN sessions on a group basis. Users have no direct access to resources on the internal network.

### Licensing Requirements

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
</table>
| ASA 5505 | AnyConnect Premium license:  
- Base License or Security Plus license: 2 sessions.  
- Optional permanent or time-based licenses: 10 or 25 sessions.  
- Shared licenses are not supported.  
| ASA 5510 | AnyConnect Premium license:  
- Base and Security Plus License: 2 sessions.  
- Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.  
- Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.  
| ASA 5520 | AnyConnect Premium license:  
- Base License: 2 sessions.  
- Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.  
- Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.  

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5540</td>
<td>AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>• Base License: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td>ASA 5550</td>
<td>AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>• Base License: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td>ASA 5580</td>
<td>AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>• Base License: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>• Base License: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td>ASA 5515-X</td>
<td>AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>• Base License: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td>ASA 5525-X</td>
<td>AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>• Base License: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td>AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>• Base License: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.</td>
</tr>
<tr>
<td></td>
<td>• Optional Shared licenses: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
</tbody>
</table>
Prerequisites for Clientless SSL VPN

See the Supported VPN Platforms, Cisco ASA 5500 Series for the platforms and browsers supported by ASA Release 9.0.

Guidelines and Limitations

- ActiveX pages require that you enable ActiveX Relay or enter `activex-relay` on the associated group policy. If you do so or assign a smart tunnel list to the policy, and the browser proxy exception list on the endpoint specifies a proxy, the user must add a “shutdown.webvpn.relay.” entry to that list.
• The ASA does not support clientless access to Windows Shares (CIFS) Web Folders from Windows 7, Vista, Internet Explorer 8-9, Mac OS X, and Linux.
• Certificate authentication, including the DoD Common Access Card and SmartCard, works with the Safari keychain only.
• The ASA does not support DSA or RSA certificates for clientless SSL VPN connections.
• Some domain-based security products have requirements above those requests that originate from the ASA.
• Inspecting configuration control and other inspection features under the Modular Policy Framework are not supported.
• The `vpn-filter` command under group policy is for client-based access and is thus not supported. `Filter` under webvpn mode in group policy is for clientless-based access.
• Neither NAT or PAT is applicable to the client.
• The ASA does not support the use of the QoS rate limiting commands, such as `police` or `priority-queue`.
• The ASA does not support the use of connection limits, checking either via the static or the Modular Policy Framework `set connection` command.
• Some components of Clientless SSL VPN require the Java Runtime Environment (JRE). With Mac OS X v10.7 and later Java is not installed by default. For details of how to install Java on Mac OS X see [http://java.com/en/download/faq/java_mac.xml](http://java.com/en/download/faq/java_mac.xml).
• If you have several group policies configured for the clientless portal, they are displayed in a drop-down on the logon page. If the top of the list of group policies is one that requires a certificate, then as soon as the user gets to the logon page, they must have a matching certificate. If not all your group policies use certificates, then configure the list to display a non-certificate policy first. Name your group policies to sort alphabetically, or prefix them with numbers so an AAA policy shows up first. For example, 1-AAA, 2-Certificate. Or, create a "dummy" group policy named Select-a-Group, and make sure that shows up first.

**Observing Clientless SSL VPN Security Precautions**

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

**Figure 1-1 Example URL Typed by User**

![SSL VPN Service](http://www.cisco.com)
Disabling URL Entry on the Portal Page

The portal page is the page that opens when the user establishes a browser-based connection. Follow these steps to disable the URL entry on the portal page.

Prerequisites

- Configure a group policy for all users who need clientless SSL VPN access, and enable clientless SSL VPN only for that group policy.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>webvpn</td>
</tr>
<tr>
<td></td>
<td>Switches to group policy webvpn configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>url-entry</td>
</tr>
<tr>
<td></td>
<td>Controls the ability of the user to enter any HTTP/HTTPS URL.</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) url-entry disable</td>
</tr>
<tr>
<td></td>
<td>Disables URL entry.</td>
</tr>
</tbody>
</table>

Clientless SSL VPN Server Certificate Verification

When connecting to a remote SSL-enabled server through clientless SSL VPN, it is important to know that you can trust the remote server, and that it is in fact the server you are trying to connect to. ASA 9.0 introduces support for SSL server certificate verification against a list of trusted certificate authority (CA) certificates for clientless SSL VPN.

When you connect to a remote server via a web browser using the HTTPS protocol, the server will provide a digital certificate signed by a CA to identify itself. Web browsers ship with a collection of CA certificates which are used to verify the validity of the server certificate. This is a form of public key infrastructure (PKI).

Just as browsers provide certificate management facilities, so does the ASA in the form of trusted certificate pool management facility: trustpools. This can be thought of as a special case of trustpoint representing multiple known CA certificates. The ASA includes a default bundle of certificates, similar to that provided with web browsers, but it is inactive until activated by the administrator by issuing the `crypto ca import default` command.
Note

If you are already familiar with trustpools from Cisco IOS then you should be aware that the ASA version is similar, but not identical.

Using SSL to Access Internal Servers

Clientless SSL VPN uses SSL and its successor, TLS1 to provide a secure connection between remote users and specific, supported internal resources at an internal server. This section includes the following topics:

- Using HTTPS for Clientless SSL VPN Sessions, page 1-7
- Configuring Clientless SSL VPN and ASDM Ports, page 1-8
- Configuring Support for Proxy Servers, page 1-8
- Configuring SSL/TLS Encryption Protocols, page 1-11

Using HTTPS for Clientless SSL VPN Sessions

To permit clientless SSL VPN sessions on an interface, perform the following steps:

Prerequisites

In a web browser, users enter the ASA address in the format https:// address where address is the IP address or DNS hostname of the ASA interface.

Restrictions

- You must enable clientless SSL VPN sessions on the ASA interface that users connect to.
- You must use HTTPS to access the ASA or load balancing cluster.
Chapter 1  Configuring Clientless SSL VPN

Using SSL to Access Internal Servers

Beginning with Version 8.0(2), the ASA supports both clientless SSL VPN sessions and ASDM administrative sessions simultaneously on Port 443 of the outside interface. You do, however, have the option to configure these applications on different interfaces.

### Configuring Clientless SSL VPN and ASDM Ports

**Command Purpose**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable (with the name of interface you want to use for clientless SSL VPN sessions)</td>
<td>Enables clientless SSL VPN sessions on the interface called outside.</td>
</tr>
</tbody>
</table>

**Example:**

hostname(config)# webvpn
hostname(config-webvpn)# enable outside

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>port port_number</td>
<td>Changes the SSL listening port for clientless SSL VPN. Enables clientless SSL VPN on port 444 of the outside interface. With this configuration, remote users initiating clientless SSL VPN sessions enter https://&lt;outside_ip&gt;:444 in the browser.</td>
</tr>
</tbody>
</table>

**Example:**

hostname(config)# http server enable
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# port 444
hostname(config-webvpn)# enable outside

### Configuring Support for Proxy Servers

**Command Purpose**

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>port argument of http server enable</td>
<td>(Privileged exec mode) Changes the listening port for ASDM. Specifies that HTTPS ASDM sessions use port 444 on the outside interface. Clientless SSL VPN is also enabled on the outside interface and uses the default port (443). With this configuration, remote users initiate ASDM sessions by entering https://&lt;outside_ip&gt;:444</td>
</tr>
</tbody>
</table>

**Example:**

hostname(config)# http server enable 444
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# enable outside

The ASA can terminate HTTPS connections and forward HTTP and HTTPS requests to proxy servers. These servers act as intermediaries between users and the public or private network. Requiring network access via a proxy server that the organization controls provides another opportunity for filtering, to assure secure network access and administrative control.

---

Cisco ASA Series CLI Configuration Guide

1-8
When configuring support for HTTP and HTTPS proxy services, you can assign preset credentials to send with each request for basic authentication. You can also specify URLs to exclude from HTTP and HTTPS requests.

**Restrictions**

You can specify a proxy autoconfiguration (PAC) file to download from an HTTP proxy server, however, you may not use proxy authentication when specifying the PAC file.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configures the ASA to use an external proxy server to handle HTTP and HTTPS requests.</td>
</tr>
<tr>
<td></td>
<td>Note Proxy NTLM authentication is not supported in <strong>http-proxy</strong>. Only proxy without authentication and basic authentication are supported.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Excludes URLs from those that can be sent to the proxy server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Provides the hostname or IP address for the external proxy server.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Proxy autoconfiguration file downloaded to the ASA that uses a JavaScript function to identify a proxy for each URL.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Accompanies each proxy request with a password to provide basic, proxy authentication.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Sent to the proxy server with each HTTP or HTTPS request.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Provides the port number used by the proxy server. The default HTTP port is 80. The default HTTPS port is 443. The ASA uses each of these ports if you do not specify an alternative value. The range is 1-65535.</td>
</tr>
</tbody>
</table>
Using SSL to Access Internal Servers

Chapter 1 Configuring Clientless SSL VPN

The ASA clientless SSL VPN configuration supports only one `http-proxy` and one `https-proxy` command each. For example, if one instance of the `http-proxy` command is already present in the running configuration and you enter another, the CLI overwrites the previous instance.

Note Proxy NTLM authentication is not supported in `http-proxy`. Only proxy without authentication and basic authentication are supported.
Chapter 1      Configuring Clientless SSL VPN

Configuring Application Profile Customization Framework

Configuring SSL/TLS Encryption Protocols

Prerequisites

Port Forwarding requires Oracle Java Runtime Environment (JRE). Port forwarding does not work when a user of clientless SSL VPN connects with some SSL versions. Refer to the compatibility matrix for supported JRE versions.

Authenticating with Digital Certificates

SSL uses digital certificates for authentication. The ASA creates a self-signed SSL server certificate when it boots; or you can install in the ASA an SSL certificate that has been issued in a PKI context. For HTTPS, this certificate must then be installed on the client.

Restrictions

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

For more information on authentication and authorization using digital certificates, see the “Using Certificates and User Login Credentials” section on page 1-9.

Configuring Application Profile Customization Framework

Clientless SSL VPN includes an Application Profile Customization Framework 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.

Multiple APCF profiles can run in parallel on an ASA. Within an APCF profile script, multiple APCF rules can apply. In this case, the ASA processes the oldest rule first (based on configuration history), then the next oldest rule, and so forth.

You can configure multiple APCF profiles 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, and so forth.

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.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>webvpn</strong></td>
</tr>
<tr>
<td></td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>apcf</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>hostname(config)# webvpn</td>
</tr>
<tr>
<td></td>
<td>hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml</td>
</tr>
<tr>
<td></td>
<td>hostname(config)# webvpn</td>
</tr>
<tr>
<td></td>
<td>hostname(config-webvpn)# apcf</td>
</tr>
<tr>
<td></td>
<td><a href="https://myserver:1440/apcf/apcf2.xml">https://myserver:1440/apcf/apcf2.xml</a></td>
</tr>
<tr>
<td></td>
<td>Identifies and locates an APCF profile that you want to load on the ASA.</td>
</tr>
<tr>
<td></td>
<td>Shows how to enable an APCF profile named apcf1.xml, located on flash memory.</td>
</tr>
<tr>
<td></td>
<td>Shows how to enable an APCF profile named apcf2.xml, located on an https server called myserver, port 1440 with the path being /apcf.</td>
</tr>
</tbody>
</table>

### APCF Syntax

APCF profiles use XML format, and sed script syntax, with the XML tags in Table 1-1.

#### 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>
<thead>
<tr>
<th>Tag</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;APCF&gt;…&lt;/APCF&gt;</td>
<td>The mandatory root element that opens any APCF XML file.</td>
</tr>
<tr>
<td>&lt;version&gt;1.0&lt;/version&gt;</td>
<td>The mandatory tag that specifies the APCF implementation version. Currently the only version is 1.0.</td>
</tr>
<tr>
<td>&lt;application&gt;…&lt;/application&gt;</td>
<td>The mandatory tag that wraps the body of the XML description.</td>
</tr>
<tr>
<td>&lt;id&gt; text &lt;/id&gt;</td>
<td>The mandatory tag that describes this particular APCF functionality.</td>
</tr>
<tr>
<td>&lt;apcf-entities&gt;…&lt;/apcf-entities&gt;</td>
<td>The mandatory tag that wraps a single or multiple APCF entities.</td>
</tr>
<tr>
<td>&lt;js-object&gt;…&lt;/js-object&gt;</td>
<td>One of these tags specifies type of content or the stage at which the APCF processing should take place.</td>
</tr>
<tr>
<td>&lt;html-object&gt;…&lt;/html-object&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;process-request-header&gt;…&lt;/process-request-header&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;process-response-header&gt;…&lt;/process-response-header&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;preprocess-response-body&gt;…&lt;/preprocess-response-body&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;postprocess-response-body&gt;…&lt;/postprocess-response-body&gt;</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-1 APCF XML Tags (continued)

<table>
<thead>
<tr>
<th>Tag</th>
<th>Use</th>
</tr>
</thead>
</table>
| `<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>`. |
| `<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. |
### Configuring Application Profile Customization Framework

#### 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>
```

### Table 1-1 APCF XML Tags (continued)

<table>
<thead>
<tr>
<th>Tag</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;delete-header&gt;</code></td>
<td>Child element of the action tag used to delete the specified HTTP header specified by the child element <code>&lt;header&gt;</code> tag shown below.</td>
</tr>
<tr>
<td><code>&lt;header&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td><code>&lt;rewrite-header&gt;</code></td>
<td><code>&lt;header&gt;Connection&lt;/header&gt;</code></td>
</tr>
<tr>
<td><code>&lt;value&gt;close&lt;/value&gt;</code></td>
<td><code>&lt;header&gt;Connection&lt;/header&gt;</code></td>
</tr>
<tr>
<td><code>&lt;do&gt;</code></td>
<td><code>&lt;header&gt;Connection&lt;/header&gt;</code></td>
</tr>
</tbody>
</table>

**Child element of the action tag used to delete the specified HTTP header specified by the child element `<header>` tag shown below.**

**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:**

```xml
<rewrite-header>
  <header>Connection</header>
  <value>close</value>
</rewrite-header>
```
Managing Passwords

Optionally, you can configure the ASA to warn end users when their passwords are about to expire. The ASA supports password management for the RADIUS and LDAP protocols. It supports the “password-expire-in-days” option for LDAP only.

You can configure password management for IPsec remote access and SSL VPN tunnel-groups. When you configure password management, the ASA notifies the remote user at login that the user’s current password is about to expire or has expired. The ASA then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password.

This command is valid for AAA servers that support such notification.

The ASA, releases 7.1 and later, generally supports password management for the following connection types when authenticating with LDAP or with any RADIUS configuration that supports MS-CHAPv2:

- AnyConnect VPN Client
- IPsec VPN Client
- Clientless SSL VPN

The RADIUS server (for example, Cisco ACS) could proxy the authentication request to another authentication server. However, from the ASA perspective, it is talking only to a RADIUS server.

Prerequisites

- Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.
- If you are using an LDAP directory server for authentication, password management is supported with the Sun Java System Directory Server (formerly named the Sun ONE Directory Server) and the Microsoft Active Directory.

Sun—The DN configured on the ASA to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.

Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.

Restrictions

- Some RADIUS servers that support MSCHAP currently do not support MSCHAPv2. This command requires MSCHAPv2 so check with your vendor.
- Password management is not supported for any of these connection types for Kerberos/Active Directory (Windows password) or NT 4.0 Domain.
- For LDAP, the method to change a password is proprietary for the different LDAP servers on the market. Currently, the ASA implements the proprietary password management logic only for Microsoft Active Directory and Sun LDAP servers.
- The ASA ignores this command if RADIUS or LDAP authentication has not been configured.
### Using Single Sign-on with Clientless SSL VPN

Single sign-on support lets users of clientless SSL VPN enter a username and password only once to access multiple protected services and web servers. In general, the SSO mechanism either starts as part of the AAA process or just after successful user authentication to a AAA server. 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. If the server approves the authentication request, it returns an SSO authentication cookie to the clientless SSL VPN server. The ASA keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server.

This section describes the four SSO authentication methods supported by clientless SSL VPN: HTTP Basic and NTLMv1 (NT LAN Manager) authentication, the Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder), and Version 1.1 of Security Assertion Markup Language (SAML), the POST-type SSO server authentication.

This section includes:
- Configuring SSO with HTTP Basic or NTLM Authentication, page 1-17
- Configuring SSO Authentication Using SiteMinder, page 1-18
- Configuring SSO Authentication Using SAML Browser Post Profile, page 1-20
- Configuring SSO with the HTTP Form Protocol, page 1-23
### Configuring SSO with HTTP Basic or NTLM Authentication

This section describes single sign-on with HTTP Basic or NTLM authentication. You can configure the ASA to implement SSO using either or both of these methods. The `auto-signon` command configures the ASA to automatically pass clientless SSL VPN user login credentials (username and password) on to internal servers. You can enter multiple `auto-signon` commands. The ASA processes them according to the input order (early commands take precedence). You specify the servers to receive the login credentials using either IP address and IP mask, or URI mask.

Use the `auto-signon` command in any of three modes: `webvpn` configuration, `webvpn` group-policy mode, or `webvpn` username mode. Username supersedes group, and group supersedes global. The mode you choose depends upon scope of authentication you want:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>webvpn configuration</code></td>
<td>All clientless SSL VPN users globally.</td>
</tr>
<tr>
<td><code>webvpn group-policy</code></td>
<td>A subset of clientless SSL VPN users defined by a group policy.</td>
</tr>
<tr>
<td><code>webvpn username configuration</code></td>
<td>An individual user of clientless SSL VPN.</td>
</tr>
</tbody>
</table>

#### Detailed Steps

The following example commands present various possible combinations of modes and arguments.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configures auto-signon for all users of clientless SSL VPN to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255 using NTLM authentication.</td>
</tr>
<tr>
<td>Example: hostname(config)# <code>webvpn</code> hostname(config-webvpn)# <code>auto-signon allow ip 10.1.1.1 255.255.255.0 auth-type ntlm</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures auto-signon for all users of clientless SSL VPN, using basic HTTP authentication, to servers defined by the URI mask <code>https://*.example.com/*</code>.</td>
</tr>
<tr>
<td>Example: hostname(config)# <code>webvpn</code> hostname(config-webvpn)# <code>auto-signon allow uri https://*.example.com/* auth-type basic</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures auto-signon for clientless SSL VPN sessions associated with the ExamplePolicy group policy, using either basic or NTLM authentication, to servers defined by the URI mask.</td>
</tr>
<tr>
<td>Example: hostname(config)# <code>group-policy ExamplePolicy attributes</code> hostname(config-group-policy)# <code>webvpn</code> hostname(config-group-webvpn)# <code>auto-signon allow uri https://*.example.com/* auth-type all</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures auto-signon for a user named Anyuser to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255 using HTTP Basic authentication.</td>
</tr>
<tr>
<td>Example: hostname(config)# <code>username Anyuser attributes</code> hostname(config-username)# <code>webvpn</code> hostname(config-username-webvpn)# <code>auto-signon allow ip 10.1.1.1 255.255.255.0 auth-type basic</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures auto-signon with a specific port and realm for authentication.</td>
</tr>
<tr>
<td>Example: (config-webvpn)# `smart-tunnel auto-signon &lt;host-list&gt; [use-domain] [realm &lt;realm string&gt;] [port &lt;port num&gt;] [host &lt;host mask&gt;</td>
<td>ip &lt;address&gt; [subnet mask]]`</td>
</tr>
</tbody>
</table>
Configuring SSO Authentication Using SiteMinder

This section describes configuring the ASA to support SSO with SiteMinder. You would typically choose to implement SSO with SiteMinder if your website security infrastructure already incorporates SiteMinder. With this method, SSO authentication is separate from AAA and happens once the AAA process completes.

Prerequisites

- Specifying the SSO server.
- Specifying the URL of the SSO server to which the ASA makes SSO authentication requests.
- Specifying a secret key to secure the communication between the ASA and the SSO server. This key is similar to a password: you create it, save it, and enter it on both the ASA and the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.

Optionally, you can do the following configuration tasks in addition to the required tasks:
- Configuring the authentication request timeout.
- Configuring the number of authentication request retries.

Restrictions

If you want to configure SSO for a user or group for clientless SSL VPN access, you must first configure a AAA server, such as a RADIUS or LDAP server. You can then set up SSO support for clientless SSL VPN.

Detailed Steps

This section presents specific steps for configuring the ASA to support SSO authentication with CA SiteMinder. To configure SSO with SiteMinder, perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>webvpn</td>
</tr>
<tr>
<td>Step 2</td>
<td>sso-server with the type option</td>
</tr>
<tr>
<td>Example:</td>
<td>hostname(config)# webvpn</td>
</tr>
<tr>
<td></td>
<td>hostname(config-webvpn)# sso-server Example type siteminder</td>
</tr>
<tr>
<td></td>
<td>hostname(config-webvpn-sso-siteminder)#</td>
</tr>
<tr>
<td>Step 3</td>
<td>config-webvpn-sso-siteminder</td>
</tr>
<tr>
<td>Step 4</td>
<td>web-agent-url</td>
</tr>
<tr>
<td>Example:</td>
<td>hostname(config-webvpn-sso-siteminder)#</td>
</tr>
<tr>
<td></td>
<td>hostname(config-webvpn-sso-siteminder)#</td>
</tr>
</tbody>
</table>
### Command

#### Step 5  
**policy-server-secret**

**Example:**
```
hostname(config-webvpn-sso-siteminder)# policy-server-secret AtaL8rD8!
```

Specifies a secret key to secure the authentication communication between the ASA and SiteMinder.

#### Step 6  
**request-timeout**

**Example:**
```
hostname(config-webvpn-sso-siteminder)# request-timeout 8
```

Specifies the number of seconds before a failed SSO authentication attempt times out. The default number of seconds is 5, and the possible range is 1 to 30.

#### Step 7  
**max-retry-attempts**

**Example:**
```
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4
```

Specifies the number of times the ASA retries a failed SSO authentication attempt before the authentication times out. The default is 3 retry attempts, and the possible range is 1 to 5 attempts.

#### Step 8  
**username-webvpn**

**group-policy-webvpn**

If specifying authentication for a user.  
If specifying authentication for a group.

#### Step 9  
**sso-server value**

**Example:**
```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value
```

Specifies the SSO authentication for either a group or a user.

Assigns the SSO server named Example to the user named Anyuser.

#### Step 10  
**test sso-server**

**Example:**
```
hostname# test sso-server Example username Anyuser
INFO: Attempting authentication request to sso-server Example for user Anyuser
INFO: STATUS: Success
```

Tests the SSO server configuration.

Tests the SSO server named Example using the username Anyuser.

### Adding the Cisco Authentication Scheme to SiteMinder

In addition to configuring the ASA for SSO with SiteMinder, you must also configure your CA SiteMinder Policy Server with the Cisco authentication scheme, a Java plug-in you download from the Cisco web site.

**Prerequisites**

Configuring the SiteMinder Policy Server requires experience with SiteMinder.
Detailed Steps
This section presents general tasks, not a complete procedure. To configure the Cisco authentication scheme on your SiteMinder Policy Server, perform the following steps:

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

- In the Library field, enter `smjavaapi`.
- In the Secret field, enter the same secret configured on the ASA.

You configure the secret on the ASA using the `policy-server-secret` command at the command line interface.

- 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.

Configuring SSO Authentication Using SAML Browser Post Profile

This section describes configuring the ASA to support Security Assertion Markup Language (SAML), Version 1.1 POST profile Single Sign-On (SSO) for authorized users.

After a session is initiated, the ASA authenticates the user against a configured AAA method. Next, the ASA (the asserting party) generates an assertion to the relying party, the consumer URL service provided by the SAML server. If the SAML exchange succeeds, the user is allowed access to the protected resource. Figure 1-3 shows the communication flow:

![SAML Communication Flow](image)

Prerequisites
To configure SSO with an SAML Browser Post Profile, you must perform the following tasks:

- Specify the SSO server with the `sso-server` command.
- Specify the URL of the SSO server for authentication requests (the `assertion-consumer-url` command)
- Specify the ASA hostname as the component issuing the authentication request (the `issuer` command)
- Specify the trustpoint certificates use for signing SAML Post Profile assertions (the `trustpoint` command)
Optionally, in addition to these required tasks, you can do the following configuration tasks:

- Configure the authentication request timeout (the `request-timeout` command)
- Configure the number of authentication request retries (the `max-retry-attempts` command)

**Restrictions**

- SAML SSO is supported only for clientless SSL VPN sessions.
- The ASA currently supports only the Browser Post Profile type of SAML SSO Server.
- The SAML Browser Artifact method of exchanging assertions is not supported.

**Detailed Steps**

This section presents specific steps for configuring the ASA to support SSO authentication with SAML Post Profile. To configure SSO with SAML-V1.1-POST, perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>webvpn</code></td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>sso-server</code> with the <code>type</code> option</td>
<td>Creates an SSO server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Creates an SSO server named Sample of type SAML-V1.1-POST.</td>
</tr>
<tr>
<td>hostname(config)# <code>webvpn</code></td>
<td></td>
</tr>
<tr>
<td>hostname(config-webvpn)# <code>sso-server</code> <code>sample</code> <code>type</code> SAML-V1.1-post</td>
<td></td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>sso saml</code></td>
<td>Switches to webvpn-sso-saml configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>assertion-consumer-url</code></td>
<td>Specifies the authentication URL of the SSO server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Sends authentication requests to the URL <a href="http://www.Example.com/webvpn.">http://www.Example.com/webvpn.</a></td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)#</td>
<td></td>
</tr>
<tr>
<td>assertion-consumer-url <code>http://www.example.com/webvpn</code></td>
<td></td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>a unique string</code></td>
<td>Identifies the ASA itself when it generates assertions. Typically, this issuer name is the hostname for the ASA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)# <code>issuer</code> <code>myasa</code></td>
<td></td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>trust-point</code></td>
<td>Specifies the identification certificate for signing the assertion.</td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)# <code>trust-point</code> <code>mytrustpoint</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>request-timeout</code></td>
<td>Configures the number of seconds before a failed SSO authentication attempt times out.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Sets the number of seconds before a request times out to 8. The default number of seconds is 5, and the possible range is 1 to 30 seconds.</td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)# <code>request-timeout</code> <code>8</code></td>
<td></td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)#</td>
<td></td>
</tr>
</tbody>
</table>
Using Single Sign-on with Clientless SSL VPN

Chapter 1 Configuring Clientless SSL VPN

Configuring the SAML POST SSO Server

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

**Detailed Steps**

**Step 1** Configure the SAML server parameters to represent the asserting party (the ASA):
- Recipient consumer URL (same as the assertion consumer URL configured on the ASA)
- Issuer ID, a string, usually the hostname of appliance
- Profile type - Browser Post Profile

**Step 2** Configure certificates.

**Step 3** Specify that asserting party assertions must be signed.

**Step 4** Select how the SAML server identifies the user:
- Subject Name Type is DN

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8</td>
<td>Configures the number of times the ASA retries a failed SSO authentication attempt before the authentication times out.</td>
</tr>
<tr>
<td>max-retry-attempts</td>
<td>Sets the number of retries to 4. The default is 3 retry attempts, and the possible range is 1 to 5 attempts.</td>
</tr>
<tr>
<td>Example:</td>
<td>Configures the number of times the ASA retries a failed SSO authentication attempt before the authentication times out.</td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)# max-retry-attempts 4</td>
<td></td>
</tr>
<tr>
<td>hostname(config-webvpn-sso-saml)#</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>webvpn</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>If assigning an SSO server to a group policy. If assigning an SSO server to a user policy.</td>
</tr>
<tr>
<td>group-policy-webvpn</td>
<td></td>
</tr>
<tr>
<td>username-webvpn</td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td>Specifies SSO authentication for either a group or a user.</td>
</tr>
<tr>
<td>sso-server</td>
<td>Assigns the SSO server named Example to the user named Anyuser.</td>
</tr>
<tr>
<td>value</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>hostname(config)# username Anyuser attributes</td>
<td></td>
</tr>
<tr>
<td>hostname(config-username)# webvpn</td>
<td></td>
</tr>
<tr>
<td>hostname(config-username-webvpn)# sso-server value sample</td>
<td></td>
</tr>
<tr>
<td>hostname(config-username-webvpn)#</td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td>(Privileged exec mode) Tests the SSO server configuration.</td>
</tr>
<tr>
<td>test sso-server</td>
<td>Tests the SSO server Example using the username Anyuser.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>hostname# test sso-server Example username Anyuser</td>
<td></td>
</tr>
<tr>
<td>INFO: Attempting authentication request to sso-server sample for user Anyuser</td>
<td></td>
</tr>
<tr>
<td>INFO: STATUS: Success</td>
<td></td>
</tr>
</tbody>
</table>

---
• Subject Name format is uid=<user>

---

## Configuring SSO with the HTTP Form Protocol

This section describes using the HTTP Form protocol for SSO. HTTP Form protocol is an approach to SSO authentication that can also qualify as a AAA method. It provides a secure method for exchanging authentication information between users of clientless SSL VPN and authenticating web servers. You can use it in conjunction with other AAA servers such as RADIUS or LDAP servers.

### Prerequisites

To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

### Restrictions

As a common protocol, it is applicable only when the following conditions are met for the web server application used for authentication:

- The authentication cookie must be set for successful request and not set for unauthorized logons. In this case, ASA cannot distinguish successful from failed authentication.

### Detailed Steps

The ASA again serves as a proxy for users of clientless SSL VPN to an authenticating web server but, in this case, it uses HTTP Form protocol and the POST method for requests. You must configure the ASA to send and receive form data. Figure 1-4 illustrates the following SSO authentication steps:

| Step 1 | A user of clientless SSL VPN first enters a username and password to log into the clientless SSL VPN server on the ASA. |
| Step 2 | The clientless SSL VPN server acts as a proxy for the user and forwards the form data (username and password) to an authenticating web server using a POST authentication request. |
| Step 3 | If the authenticating web server approves the user data, it returns an authentication cookie to the clientless SSL VPN server where it is stored on behalf of the user. |
| Step 4 | The clientless SSL VPN server establishes a tunnel to the user. |
| Step 5 | The user can now access other websites within the protected SSO environment without reentering a username and password. |
While you would expect to configure form parameters that let the ASA include POST data such as the username and password, you initially might not be aware of additional hidden parameters that the web server requires. Some authentication applications expect hidden data which is neither visible to nor entered by the user. You can, however, discover hidden parameters the authenticating web server expects by making a direct authentication request to the web server from your browser without the ASA in the middle acting as a proxy. Analyzing the web server response using an HTTP header analyzer reveals hidden parameters in a format similar to the following:

\[ \text{<param name>=<URL encoded value>&<param name>=<URL encoded>} \]

Some hidden parameters are mandatory and some are optional. If the web server requires data for a hidden parameter, it rejects any authentication POST request that omits that data. Because a header analyzer does not tell you if a hidden parameter is mandatory or not, we recommend that you include all hidden parameters until you determine which are mandatory.

To configure SSO with the HTTP Form protocol, you must perform the following:

- Configure the uniform resource identifier on the authenticating web server to receive and process the form data (**action-uri**).
- Configure the username parameter (**user-parameter**).
- Configure the user password parameter (**password-parameter**).

You might also need to do the following tasks depending upon the requirements of authenticating web server:

- Configure a starting URL if the authenticating web server requires a pre-login cookie exchange (**start-url**).
- Configure any hidden authentication parameters required by the authenticating web server (**hidden-parameter**).
- Configure the name of an authentication cookie set by the authenticating web server (**auth-cookie-name**).
### Chapter 1      Configuring Clientless SSL VPN

Using Single Sign-on with Clientless SSL VPN

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> aaa-server-host</td>
<td>Switches to the aaa-server-host configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> start-url</td>
<td>If the authenticating web server requires it, specifies the URL from which to retrieve a pre-login cookie from the authenticating web server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies the authenticating web server URL</td>
</tr>
<tr>
<td></td>
<td><a href="http://example.com/east/Area.do?Page-Grp1">http://example.com/east/Area.do?Page-Grp1</a> in the testgrp1 server group with an IP address of 10.0.0.2.</td>
</tr>
<tr>
<td><strong>Step 3</strong> action-uri</td>
<td>Specifies a URI for an authentication program on the authenticating web server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>A URI can be entered on multiple, sequential lines.</td>
</tr>
<tr>
<td></td>
<td>The maximum number of characters per line is 255.</td>
</tr>
<tr>
<td></td>
<td>The maximum number of characters for a complete URI is 2048.</td>
</tr>
<tr>
<td></td>
<td>You must include the hostname and protocol in the action URI. In this example, these appear at the start of the URI in <a href="http://www.example.com">http://www.example.com</a>.</td>
</tr>
<tr>
<td><strong>Step 4</strong> user-parameter</td>
<td>Configures a username parameter for the HTTP POST request.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configures the username parameter userid.</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.example.com/auth/index.html/appdir/authc/forms/MCologin.fcc?TYPE=33554433&amp;REALM_ID=06-000a1311-a828-1185-ab41-8333b16a0008&amp;GUID=6SMAUTHREASON=0&amp;METHO">http://www.example.com/auth/index.html/appdir/authc/forms/MCologin.fcc?TYPE=33554433&amp;REALM_ID=06-000a1311-a828-1185-ab41-8333b16a0008&amp;GUID=6SMAUTHREASON=0&amp;METHO</a></td>
</tr>
<tr>
<td></td>
<td>D=GET&amp;SMAGENTNAME=$SM$5FZmjnk3DRNWNjk2KcqcVFb1RN79%2bJOHKnPshFlgtg6zBlUV2P%kHqLw%3d%3d&amp;TARGET=https%3A%2F%2Fauth.example.com</td>
</tr>
<tr>
<td><strong>Step 5</strong> password-parameter</td>
<td>Configures a user password parameter for the HTTP POST request.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configures a user password parameter named user_password.</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.example.com/auth/index.html/appdir/authc/forms/MCologin.fcc?TYPE=33554433&amp;REALM_ID=06-000a1311-a828-1185-ab41-8333b16a0008&amp;GUID=6SMAUTHREASON=0&amp;METHO">http://www.example.com/auth/index.html/appdir/authc/forms/MCologin.fcc?TYPE=33554433&amp;REALM_ID=06-000a1311-a828-1185-ab41-8333b16a0008&amp;GUID=6SMAUTHREASON=0&amp;METHO</a></td>
</tr>
<tr>
<td></td>
<td>D=GET&amp;SMAGENTNAME=$SM$5FZmjnk3DRNWNjk2KcqcVFb1RN79%2bJOHKnPshFlgtg6zBlUV2P%kHqLw%3d%3d&amp;TARGET=https%3A%2F%2Fauth.example.com</td>
</tr>
</tbody>
</table>

---

**Command Purpose**

**Step 1** aaa-server-host

Switches to the aaa-server-host configuration mode.

**Step 2** start-url

If the authenticating web server requires it, specifies the URL from which to retrieve a pre-login cookie from the authenticating web server.

**Example:**

```plaintext
hostname(config)# aaa-server testgrp1 protocol http-form
hostname(config)# aaa-server testgrp1 host 10.0.0.2
hostname(config-aaa-server-host)# start-url http://example.com/east/Area.do?Page-Grp1
```

**Step 3** action-uri

Specifies a URI for an authentication program on the authenticating web server.

**Example:**

```plaintext
http://www.example.com/auth/index.html/appdir/authc/forms/MCologin.fcc?TYPE=33554433&REALM_ID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=6SMAUTHREASON=0&METHO   
```

**Step 4** user-parameter

Configures a username parameter for the HTTP POST request.

**Example:**

```plaintext
hostname(config-aaa-server-host)# user-parameter userid
```

**Step 5** password-parameter

Configures a user password parameter for the HTTP POST request.

**Example:**

```plaintext
hostname(config-aaa-server-host)# password-parameter user_password
```
### Command and Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><strong>hidden-parameter</strong></td>
<td>Specifies hidden parameters for exchange with the authenticating web server.</td>
</tr>
</tbody>
</table>
|      | **Example:**                                 | Shows an example hidden parameter excerpted from a POST request. This hidden parameter includes four form entries and their values, separated by &. The four entries and their values are:  
• SMENC with a value of ISO-8859-1.  
• SMLOCALE with a value of US-EN.  
• target with a value of https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do.  
• %3FEMCOPageCode%3DENG.  
• smauthreason with a value of 0. |
|      | **To specify this hidden parameter, enter the following commands:** |                                                                          |
|      | `hostname(config)# aaa-server testgrp1 host example.com` |                                                                          |
|      | `hostname(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe` |                                                                          |
|      | `hostname(config-aaa-server-host)# hidden-parameter target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0` |                                                                          |
| 7    | **auth-cookie-name**                         | Specifies the name for the authentication cookie.                       |
|      | **Example:**                                 | Specifies the authentication cookie name of SsoAuthCookie.              |
|      | `hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie` |                                                                          |
| 8    | **tunnel-group general-attributes**          | Switches to tunnel-group general-attributes configuration mode.         |
| 9    | **authentication-server-group**              | Configures a tunnel-group to use the SSO server configured in the previous steps. |
|      | **Example:**                                 | Configures the tunnel-group named /testgroup/ to use the SSO server(s) named /testgrp1/” | `hostname(config)# tunnel-group testgroup general-attributes`  
`hostname(config-tunnel-general)#authentication-server-group testgrp1` |
| 10   | **aaa-server-host**                          | Switches to aaa-server-host configuration mode.                         |
Gathering HTTP Form Data

This section presents the steps for discovering and gathering necessary HTTP Form data. If you do not know what parameters the authenticating web server requires, you can gather parameter data by analyzing an authentication exchange using the following steps:

Prerequisites
These steps require a browser and an HTTP header analyzer.
Using Single Sign-on with Clientless SSL VPN

Detailed Steps

**Step 1** Start your browser and HTTP header analyzer, and connect directly to the web server login page without going through the ASA.

**Step 2** After the web server login page has loaded in your browser, examine the login sequence to determine if a cookie is being set during the exchange. If the web server has loaded a cookie with the login page, configure this login page URL as the start-URL.

**Step 3** Enter the username and password to log in to the web server, and press **Enter**. This action generates the authentication POST request that you examine using the HTTP header analyzer.

An example POST request—with host HTTP header and body—follows:

```
POST /emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$FZmjnk3DRNwNjK2KqqVCfb1rNT9%2bH0KPsIftg6rBIUV2PxfkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2FHTTP/1.1
Host: www.example.com
``` 

**Step 4** Examine the POST request and copy the protocol, host, and the complete URL to configure the action-uri parameter.

**Step 5** Examine the POST request body and copy the following:

a. Username parameter. In the preceding example, this parameter is **USERID**, not the value **anyuser**.

b. Password parameter. In the preceding example, this parameter is **USER_PASSWORD**.

c. Hidden parameter. This parameter is everything in the POST body except the username and password parameters. In the preceding example, the hidden parameter is:

```
``` 

Figure 1-5 highlights the action URI, hidden, username and password parameters within sample output from an HTTP analyzer. This is only an example; output varies widely across different websites.
Step 6  If you successfully log in to the web server, examine the server response with the HTTP header analyzer to locate the name of the session cookie set by the server in your browser. This is the **auth-cookie-name** parameter.

In the following server response header, the name of the session cookie is SMSESSION. You just need the name, not the value.
Set-Cookie: SMSESSION=yN4yP5hHVNDgs4FT8dn7+Rwev4lsE49X1Kc+ltwle0gnjnhbtkUnR8XWP3hvDH6PZ
bH10hT4/LDRTA8ngDB/bteX15x9y8WFWawg3CtVa30dOxHFr8jy5D5gevK3Z4ujgu1r06f4a0dSS
O5epWwncsB7IFXc+f+M1gw0o88uH1241+G5l1g79WVcpuxF11AO66d/gtD400W5YKKE12Kmode+yQ
zzwfr22c17E51Mr8GdC57K7qVc5rQ6G8jQ6QK2+R5ch741bZCMa5DUSVqVqVqSCW8OMHNgwp25
3X5W5aVh/b6/7TM093QV+vl3Nw0gd1Y7fBqehch7FrVroU1F8oFzoZMrMyZI5H5Vh70b95pwp0
d0pZliAza43jup05f6CKuLeudYIwqNq6ZanZettP6c1gPjY0n0a7QdN7q9knSPJsekrH9h1RbH
pLl/3B1Q94vBD2YuTuiI36T1P14hW50lCAYRj72/bfYj+1y2u78emZM+UeFyX4hCp492y83R5L2W
remP95V5I41XZBFPnuU/3V5j5fniBuLr/cdfk005+pa3V6/nHoKErSgyxj/2m8a8VD9m41LxxaUIUbcm
koh9T1ms1vKzX0JO+0F0oU6O/xEdl1A4Ngk4cpi2sXbIarALp6B13+tb84M1HGHG9CPCeZxg0
i/kon9yMauHyRz+om6w6tchAmChv1C3dpodXnt8DpabqiW6VDTrv135Pyf3Uv7WdaubwSl5xbU3jY
2JXQnUtWb977NCyzU2oToN+daEREW6ueyJbBMkXyzUBL4515U5N50B4CVv5KDkXAp3N0NfG6
RM6dpfMELYoNylz70h23fVQ/7Y71w/k7o1/8/vBa13iv38edSczu/An1N4c2u6WqZooG8/dapWriH
hNco4LlJogCet3.w3mHkFxc2YwZU4XZsja5yBnFbe5PTFVfma5dc/EmNor9W0R0HNT
QaHP5rg5dTNqunkDEMDtHbfeP3F90cPejVzihM6gI6SPE/C5UAJ ie;Domain=.example.com;Path=

Figure 1-6 shows an example of authorization cookies in HTTP analyzer output. This is only one example; output varies widely across different websites.

Figure 1-6
Authorization cookies in sample HTTP analyzer output

Step 7
In some cases, the server may set the same cookie regardless of whether the authentication was successful or not, and such a cookie is unacceptable for SSO purposes. To confirm that the cookies are different, repeat Step 1 through Step 6 using invalid login credentials and then compare the “failure” cookie with the “success” cookie.

You now have the necessary parameter data to configure the ASA for SSO with HTTP Form protocol.
Configuring SSO for Plug-ins

Plug-ins support single sign-on (SSO). They use the same credentials (username and password) entered to authenticate the clientless SSL VPN session. Because the plug-ins do not support macro substitution, you do not have the option to perform SSO on different fields, such as the internal domain password or the attribute on a RADIUS or LDAP server.

To configure SSO support for a plug-in, you install the plug-in and add a bookmark entry to display a link to the server, specifying SSO support using the `cisco_sso=1` parameter. The following examples show plug-in bookmarks enabled for SSO:

- `ssh://ssh-server/?cisco_sso=1`
- `rdp://rdp-server/?Parameter1=value&Parameter2=value&cisco_sso=1`

Configuring SSO with Macro Substitution

This section describes using macro substitution for SSO. Configuring SSO with macro substitution allows you to inject certain variables into bookmarks to substitute for dynamic values.

Note

Smart tunnel bookmarks support auto-signon but not variable substitution. For example, a SharePoint bookmark configured for smart tunnel uses the same username and password credentials to log into the application as the credentials used to log into clientless SSL VPN. You can use variable substitutions and auto signon simultaneously or separately.

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 administrator determines the pre-load page and URL, which specifies where you want the post login request 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 following variables (or macros) allow for substitutions in bookmarks and forms-based HTTP POST operations:

- `CSCO_WEBVPN_USERNAME` — user login ID
- `CSCO_WEBVPN_PASSWORD` — user login password
- `CSCO_WEBVPN_INTERNAL_PASSWORD` — user internal (or domain) password. This cached credential is not authenticated against a AAA server. When you enter this value, the security appliance uses it as the password for auto signon, instead of the password/primary password value.

Note

You cannot use any of these three variables in GET-based http(s) bookmarks. Only POST-based http(s) and cifs bookmarks can use these variables.

- `CSCO_WEBVPN_CONNECTION_PROFILE` — user login group drop-down (connection profile alias)
- `CSCO_WEBVPN_MACRO1` — set with the RADIUS-LDAP Vendor Specific Attribute (VSA). If you are mapping from LDAP with an ldap-attribute-map command, use the WebVPN-Macro-Substitution-Value1 Cisco attribute for this macro. See the Active Directory ldap-attribute-mapping examples at http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118.
The CSCO_WEBVPN_MACRO1 macro substitution with RADIUS is performed by VSA#223 (see Table 1-2).

<table>
<thead>
<tr>
<th>Table 1-2</th>
<th>VSA#223</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebVPN-Macro-Value1</td>
<td>Y 223</td>
</tr>
<tr>
<td>WebVPN-Macro-Value2</td>
<td>Y 224</td>
</tr>
</tbody>
</table>

A value such as www.cisco.com/email dynamically populates a bookmark on the Clientless SSL VPN portal, such as https://CSCO_WEBVPN_MACRO1 or https://CSCO_WEBVPN_MACRO2 for the particular DAP or group policy.

- CSCO_WEBVPN_MACRO2 —set with RADIUS-LDAP Vendor Specific Attribute (VSA). If you are mapping from LDAP with an ldap-attribute-map command, use the WebVPN-Macro-Substitution-Value2 Cisco attribute for this macro. See the Active Directory ldap-attribute-mapping examples at http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118.

The CSCO_WEBVPN_MACRO2 macro substitution with RADIUS is performed by VSA#224 (see Table 1-2).

Each time clientless SSL VPN recognizes one of these six strings in an end-user request (in the form of a bookmark or Post Form), it replaces the string with the user-specified value and then passes the request to a remote server.

If the lookup of the username and password fails on the ASA, an empty string is substituted, and the behavior converts back as if no auto sign-in is available.

Note

Accessing Virtual Desktop Infrastructure (VDI)

In a VDI model, administrators publish enterprise applications or desktops pre-loaded with enterprise applications, and end users remotely access these applications. These virtualized resources appear just as any other resources, such as email, so that users do not need to go through a Citrix Access Gateway to access them. Users log onto the ASA using Citrix Receiver mobile client, and the ASA connects to a pre-defined Citrix XenApp or XenDesktop Server. The administrator must configure the Citrix server’s address and logon credentials under Group Policy so that when users connect to their Citrix Virtualized resource, they enter the ASA’s SSL VPN IP address and credentials instead of pointing to the Citrix Server’s address and credentials. When the ASA has verified the credentials, the receiver client starts to retrieve entitled applications through the ASA.

Supported Mobile Devices

- iPad—Citrix Receiver version 4.x or later
- iPhone/iTouch—Citrix Receiver version 4.x or later
- Android 2.x/3.x/4.0/4.1 phone—Citrix Receiver version 2.x or later
- Android 4.0 phone—Citrix Receiver version 2.x or later
Limitations
Citrix Receiver clients access only one XenApp/XenDesktop server at a time.

Detailed Steps
If both username and group policy are configured, username settings take precedence over group policy. Enter the following:

```
configure terminal
group-policy DfltGrpPolicy attributes
  webvpn
    vdi type <citrix> url <url> domain <domain> username <username> password <password>
configure terminal
username <username> attributes
  webvpn
    vdi type <citrix> url <url> domain <domain> username <username> password <password>
```

The syntax options are defined as follows:
- **type**—Type of VDI. For a Citrix Receiver type, this value must be `citrix`.
- **url**—Full URL of the XenApp or XenDesktop server including http or https, hostname, and port number, as well as the path to the XML service.
- **username**—Username for logging into the virtualization infrastructure server. This value can be a clientless macro.
- **password**—Password for logging into the virtualization infrastructure server. This value can be a clientless macro.
- **domain**—Domain for logging into the virtualization infrastructure server. This value can be a clientless macro.

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.
Encoding

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  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

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](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.

### Creating and Applying Clientless SSL VPN Policies for Accessing Resources

Creating and applying policies for clientless SSL VPN that govern access to resources at an internal server includes the following task:

- **Assigning Users to Group Policies**

Chapter 1, “Configuring Connection Profiles, Group Policies, and Users” includes step-by-step instructions for all of these tasks.

### Assigning Users to Group Policies

Assigning users to group policies simplifies the configuration by letting you apply policies to many users. You can use an internal authentication server on the ASA or an external RADIUS or LDAP server to assign users to group policies. See Chapter 1, “Configuring Connection Profiles, Group Policies, and Users” for a thorough explanation of ways to simplify configuration with group policies.

### Configuring Connection Profile Attributes for Clientless SSL VPN

Table 1-3 provides a list of connection profile attributes that are specific to clientless SSL VPN. In addition to these attributes, you configure general connection profile attributes common to all VPN connections. For step-by-step information on configuring connection profiles, see Chapter 1, “Configuring Connection Profiles, Group Policies, and Users.”

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Sets the authentication method.</td>
</tr>
<tr>
<td>customization</td>
<td>Identifies the name of a previously defined customization to apply.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits from tunnel-group WebVPN attribute configuration mode.</td>
</tr>
<tr>
<td>nbns-server</td>
<td>Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.</td>
</tr>
</tbody>
</table>

In earlier releases, “connection profiles” were known as “tunnel groups.” You configure a connection profile with tunnel-group commands. This chapter often uses these terms interchangeably.
Configuring Group Policy and User Attributes for Clientless SSL VPN

Table 1-3 Connection Profile Attributes for Clientless SSL VPN

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-alias</td>
<td>Specifies the alternate names by which the server can refer to a connection profile.</td>
</tr>
<tr>
<td>group-url</td>
<td>Identifies one or more group URLs. If you establish URLs with this attribute, this group is selected automatically for users when they access using these URLs.</td>
</tr>
<tr>
<td>dns-group</td>
<td>Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values.</td>
</tr>
<tr>
<td>help</td>
<td>Provides help for tunnel group configuration commands.</td>
</tr>
<tr>
<td>hic-fail-group-policy</td>
<td>Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to “Use Failure Group-Policy” or “Use Success Group-Policy, if criteria match.”</td>
</tr>
<tr>
<td>no</td>
<td>Removes an attribute value pair.</td>
</tr>
<tr>
<td>override-svc-download</td>
<td>Overrides downloading the group-policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.</td>
</tr>
<tr>
<td>pre-fill-username</td>
<td>Configures username to certificate binding on this tunnel-group.</td>
</tr>
<tr>
<td>proxy-auth</td>
<td>Identifies this tunnel-group as a specific proxy authentication tunnel group.</td>
</tr>
<tr>
<td>radius-reject-message</td>
<td>Enables the display of the RADIUS reject message on the login screen when authentication is rejected.</td>
</tr>
<tr>
<td>secondary-pre-fill-username</td>
<td>Configures the secondary username to certificate binding on this tunnel-group.</td>
</tr>
<tr>
<td>without-csd</td>
<td>Disables CSD for a tunnel group.</td>
</tr>
</tbody>
</table>

Table 1-4 Group Policy and User Attributes for Clientless SSL VPN

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>activex-relay</td>
<td>Lets a user who has established a clientless SSL VPN session use the browser to launch Microsoft Office applications. The applications use the session to download and upload ActiveX. The ActiveX relay remains in force until the clientless SSL VPN session closes.</td>
</tr>
<tr>
<td>auto-signon</td>
<td>Sets values for auto signon, which requires only that the user enter username and password credentials only once for a clientless SSL VPN connection.</td>
</tr>
<tr>
<td>customization</td>
<td>Assigns a customization object to a group-policy or user.</td>
</tr>
</tbody>
</table>
Configuring Clientless SSL VPN

Configuring Browser Access to Plug-ins

Table 1-4   Group Policy and User Attributes for Clientless SSL VPN

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny-message</td>
<td>Specifies the message delivered to a remote user who logs into clientless SSL VPN successfully, but has no VPN privileges.</td>
</tr>
<tr>
<td>file-browsing</td>
<td>Enables CIFS file browsing for file servers and shares. Browsing requires NBNS (Master Browser or WINS).</td>
</tr>
<tr>
<td>file-entry</td>
<td>Allows users to enter file server names to access.</td>
</tr>
<tr>
<td>filter</td>
<td>Sets the name of the webtype access list.</td>
</tr>
<tr>
<td>hidden-shares</td>
<td>Controls the visibility of hidden shares for CIFS files.</td>
</tr>
<tr>
<td>homepage</td>
<td>Sets the URL of the web page that displays upon login.</td>
</tr>
<tr>
<td>html-content-filter</td>
<td>Configures the content and objects to filter from the HTML for this group policy.</td>
</tr>
<tr>
<td>http-comp</td>
<td>Configures compression.</td>
</tr>
</tbody>
</table>
| http-proxy         | Configures the ASA to use an external proxy server to handle HTTP requests.  
|                    | Note  Proxy NTLM authentication is not supported in http-proxy. Only proxy without authentication and basic authentication are supported. |
| keep-alive-ignore  | Sets the maximum object size to ignore for updating the session timer.  |
| port-forward       | Applies a list of clientless SSL VPN TCP ports to forward. The user interface displays the applications on this list. |
| post-max-size      | Sets the maximum object size to post.                                   |
| smart-tunnel       | Configures a list of programs and several smart tunnel parameters to use smart tunnel.                          |
| sso-server         | Sets the name of the SSO server.                                         |
| storage-objects    | Configures storage objects for the data stored between sessions.        |
| svc                | Configures SSL VPN Client attributes.                                    |
| unix-auth-gid      | Sets the UNIX group ID.                                                 |
| unix-auth-uid      | Sets the UNIX user ID.                                                  |
| upload-max-size    | Sets the maximum object size to upload.                                 |
| url-entry          | Controls the ability of the user to enter any HTTP/HTTP URL.            |
| url-list           | Applies a list of servers and URLs that clientless SSL VPN portal page displays for end user access.              |
| user-storage       | Configures a location for storing user data between sessions.           |

Configuring Browser Access to Plug-ins

The following sections describe the integration of browser plug-ins for clientless SSL VPN browser access:

- Preparing the Security Appliance for a Plug-in, page 1-39
- Installing Plug-ins Redistributed By Cisco, page 1-40
- Providing Access to a Citrix XenApp Server, page 1-42
A browser plug-in is a separate program that a web browser invokes to perform a dedicated function, such as connect a client to a server within the browser window. The ASA lets you import plug-ins for download to remote browsers in clientless SSL VPN sessions. Of course, Cisco tests the plug-ins it redistributes, and in some cases, tests the connectivity of plug-ins we cannot redistribute. However, we do not recommend importing plug-ins that support streaming media at this time.

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

- (Cisco-distributed plug-ins only) Unpacks the jar file specified in the URL.
- Writes the file to the ASA file system.
- Populates the drop-down menu next to the URL attributes in ASDM.
- Enables the plug-in for all future clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down menu next to the Address field of the portal page.

Table 1-5 shows the changes to the main menu and address field of the portal page when you add the plug-ins described in the following sections.

<table>
<thead>
<tr>
<th>Plug-in</th>
<th>Main Menu Option Added to Portal Page</th>
<th>Address Field Option Added to Portal Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ica</td>
<td>Citrix MetaFrame Services</td>
<td>ica://</td>
</tr>
<tr>
<td>rdp</td>
<td>Terminal Servers</td>
<td>rdp://</td>
</tr>
<tr>
<td>rdp2*</td>
<td>Terminal Servers Vista</td>
<td>rdp2://</td>
</tr>
<tr>
<td>ssh,telnet</td>
<td>Secure Shell</td>
<td>ssh://</td>
</tr>
<tr>
<td></td>
<td>Telnet services (supporting v1 and v2)</td>
<td>telnet://</td>
</tr>
<tr>
<td>vnc</td>
<td>Virtual Network Computing services</td>
<td>vnc://</td>
</tr>
</tbody>
</table>

* Not a recommended plug-in.

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

The plug-ins support single sign-on (SSO). Refer to the “Configuring SSO with the HTTP Form Protocol” section on page 1-23 for implementation details.

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

Prerequisites

- Clientless SSL VPN must be enabled on the ASA to provide remote access to the plug-ins.
- To configure SSO support for a plug-in, you install the plug-in, add a bookmark entry to display a link to the server, and specify SSO support when adding the bookmark.
- The minimum access rights required for remote use belong to the guest privilege mode.
- Plug-ins require ActiveX or Oracle Java Runtime Environment (JRE), see the compatibility matrix for version requirements.
Restrictions

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

- The plug-ins support single sign-on (SSO). They use the same credentials entered to open the clientless SSL VPN session. Because the plug-ins do not support macro substitution, you do not have the options to perform SSO on different fields such as the internal domain password or on an attribute on a RADIUS or LDAP server.
- A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.
- If you use stateless failover instead of stateful failover, clientless features such as bookmarks, customization, and dynamic access-policies are not synchronized between the failover ASA pairs. In the event of a failover, these features do not work.

Preparing the Security Appliance for a Plug-in

Before installing a plug-in, prepare the ASA as follows:

Prerequisites
Make sure clientless SSL VPN (“webvpn”) is enabled on an ASA interface.

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

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 show running-config</td>
<td>Shows whether webvpn is enabled on the ASA.</td>
</tr>
<tr>
<td>Step 2 Install an SSL certificate onto the ASA interface</td>
<td>Provides a fully-qualified domain name (FQDN) for remote user connection.</td>
</tr>
</tbody>
</table>

Go to the section that identifies the type of plug-in you want to provide for clientless SSL VPN access.
- Installing Plug-ins Redistributed By Cisco, page 1-40
- Providing Access to a Citrix XenApp Server, page 1-42
Installing Plug-ins Redistributed By Cisco

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

**Prerequisites**

Make sure clientless SSL VPN ("webvpn") is enabled on an interface on the ASA. To do so, enter the `show running-config` command.

**Plug-ins Redistributed by Cisco**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
<th>Source of Redistributed Plug-in</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Table 1-6</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td><strong>Description</strong></td>
<td><strong>Source of Redistributed Plug-in</strong></td>
</tr>
<tr>
<td>RDP</td>
<td>HOBLink JWT is a Native Java RDP client which supports RDP 7.0 for remote access to Windows Terminal services.</td>
<td>Customers can download this plugin from these locations:</td>
</tr>
<tr>
<td></td>
<td><em>Note</em> Since properoRDP and HOBSoft both use RDP as the plugin protocol, customers will not be able to use HOBSoft for one set of users and properoRDP for the rest via GroupPolicy etc.</td>
<td>HOBSoft</td>
</tr>
<tr>
<td></td>
<td>Use this plug-in if you want to use a single plug-in for Windows, Mac OS X and Linux operating systems. See This Document for a list of all supported operating systems.</td>
<td>Cisco.com</td>
</tr>
<tr>
<td></td>
<td>The original source of the redistributed plug-in is <a href="http://properjavardp.sourceforge.net/">http://properjavardp.sourceforge.net/</a></td>
<td>Proper Java RDP</td>
</tr>
<tr>
<td>RDP</td>
<td>Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2.</td>
<td>The original source of the redistributed plug-in is <a href="http://properjavardp.sourceforge.net/">http://properjavardp.sourceforge.net/</a></td>
</tr>
<tr>
<td></td>
<td>Supports Remote Desktop ActiveX Control.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>We recommend using this plug-in that supports both RDP and RDP2. Only versions up to 5.2 of the RDP and RDP2 protocols are supported. Version 5.2 and later are not supported.</td>
<td></td>
</tr>
<tr>
<td>RDP2</td>
<td>Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2.</td>
<td>The original source of the redistributed plug-in is <a href="http://properjavardp.sourceforge.net/">http://properjavardp.sourceforge.net/</a></td>
</tr>
<tr>
<td></td>
<td>Supports Remote Desktop ActiveX Control.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Note</em> This legacy plug-in supports only RDP2. We do not recommend using this plug-in, instead, use the RDP plug-in above.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 1  Configuring Clientless SSL VPN

Configuring Browser Access to Plug-ins

Table 1-6

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
<th>Source of Redistributed Plug-in *</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>The Secure Shell-Telnet plug-in lets the remote user establish a Secure Shell (v1 or v2) or Telnet connection to a remote computer.</td>
<td>The web site containing the source of the redistributed plug-in is <a href="http://javassh.org/">http://javassh.org/</a></td>
</tr>
<tr>
<td>Note</td>
<td>Because keyboard-interactive authentication is not supported by JavaSSH, it cannot be supported with SSH plugin. (Keyboard interactive is a generic authentication method used to implement different authentication mechanisms.)</td>
<td></td>
</tr>
<tr>
<td>VNC</td>
<td>The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing (also known as VNC server or service) turned on. This version changes the default color of the text and contains updated French and Japanese help files.</td>
<td>The web site containing the source of the redistributed plug-in is <a href="http://www.tightvnc.com/">http://www.tightvnc.com/</a></td>
</tr>
</tbody>
</table>

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

These plug-ins are available on the Cisco Adaptive Security Appliance Software Download site.

Detailed Steps

Follow these steps to provide clientless SSL VPN browser access to a plug-in redistributed by Cisco.

Step 1

Note

The ASA does not retain the import webvpn plug-in protocol command in the configuration. Instead, it loads the contents of the cisco-config/97/plugin directory automatically. A secondary ASA obtains the plug-ins from the primary ASA.
Configuring Browser Access to Plug-ins

As an example of how to provide clientless SSL VPN browser access to third-party plug-ins, this section describes how to add clientless SSL VPN support for the Citrix XenApp Server Client.

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

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

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

- Preparing the Citrix XenApp Server for Clientless SSL VPN Access
- Creating and Installing the Citrix Plug-in

Providing Access to a Citrix XenApp Server

As an example of how to provide clientless SSL VPN browser access to third-party plug-ins, this section describes how to add clientless SSL VPN support for the Citrix XenApp Server Client.

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

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

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

- Preparing the Citrix XenApp Server for Clientless SSL VPN Access
- Creating and Installing the Citrix Plug-in

Preparing the Citrix XenApp Server for Clientless SSL VPN Access

You must configure the Citrix Web Interface software to operate in a mode that does not use the (Citrix) "secure gateway." Otherwise, the Citrix client cannot connect to the Citrix XenApp Server.

Note If you are not already providing support for a plug-in, you must follow the instructions in the "Preparing the Security Appliance for a Plug-in" section on page 1-39 before using this section.

Creating and Installing the Citrix Plug-in

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

**Step 1**
Download the ICA plug-in file from the Cisco Software Download web site. This file contains files that Cisco customized for use with the Citrix plug-in.

**Step 2**
Download the **Citrix Java client** from the Citrix site.
On Citrix download site, select Citrix Receiver, Receivers by Platform, and click Find. Expand Receiver for Other Platforms, and download Receiver for Java. JICAComponents.tar.gz a gzip'd tar file, which you can open with 7-Zip or other unix-compatible tools.

**Step 3**
Extract the following files from the Citrix Java client, then add them to the ica-plugin.zip file:
- JICA-configN.jar
- JICAEngN.jar
You can use WinZip to perform this step.

**Step 4**
Ensure the EULA included with the Citrix Java client grants you the rights and permissions to deploy the client on your web servers.

**Step 5**
Install the plug-in by using ASDM, or entering the following CLI command in privileged EXEC mode:

```
import webvpn plug-in protocol ica URL
```
*URL* is the host name or IP address and path to the ica-plugin.zip file.

**Note**
We recommend that you add a bookmark to make it easy for users to connect. Adding a bookmark is required if you want to provide SSO support for Citrix sessions. We also recommend that you use URL parameters in the bookmark the provide convenient viewing, for example:

```
ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```

**Step 6**
Establish an SSL VPN clientless session and click the bookmark or enter the URL for the Citrix server. Use the **Client for Java Administrator's Guide** as needed.
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 (OTP), the SSO feature falls short in meeting that demand, because it only forwards conventional user credentials, such as static username and password, to clientless web-based resources when authentication is required.

For example, neither certificate- or 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 is 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 (also known as WebVPN) 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 or WebVPN remote access users to access Kerberos authenticated applications in the private network.

The 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 1-7 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
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.

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.

Before Configuring KCD

To configure the ASA for cross-realm authentication, you must use the following commands:
### Understanding How KCD Works

#### Step 1
**ntp hostname**

**Example:**
```
hostname(config)# config t
#Create an alias for the Domain Controller
hostname(config)# name 10.1.1.10 DC
#Configure the Name server
```

Joins the Active Directory domain.

Shows a 10.1.1.10 domain controller (which is reachable inside the interface) with a domain name of private.net and a service account on the domain controller using dcuser as the username and dcuser123! as the password.

#### Step 2
**dns domain-lookup**
**dns server-group**

**Example:**
```
hostname(config)# ntp server DC
#Enable a DNS lookup by configuring the DNS server and Domain name
hostname(config)# dns domain-lookup inside
hostname(config)# dns server-group DefaultDNS
hostname(config-dns-server-group)# name-server DC
hostname(config-dns-server-group)# domain-name private.net
#Configure the AAA server group with Server and Realm
hostname(config)# aaa-server KerberosGroup protocol Kerberos
hostname(config-asa-server-group)# aaa-server KerberosGroup (inside) host DC
hostname(config-asa-server-group)# Kerberos-realm PRIVATE.NET
#Configure the Domain Join
hostname(config)# webvpn
hostname(config-webvpn)# kcd-server KerberosGroup
username dcuser password dcuser123!
 hostname(config)#
```

Performs a lookup.

Shows a domain name of private.net and a service account on the domain controller using dcuser as the username and dcuser123! as the password.

### Configuring KCD

To have the ASA join a Windows Active Directory domain and return a success or failure status, follow these commands:

#### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>webvpn</strong></td>
</tr>
<tr>
<td></td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>kcd-server</strong></td>
</tr>
</tbody>
</table>
Chapter 1 Configuring Clientless SSL VPN

Understanding How KCD Works

To display the domain controller information and the domain join status, follow these commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>kcd-server aaa-server-group</td>
</tr>
<tr>
<td></td>
<td>Specifies the domain controller name and realm. The AAA server group must be a Kerberos type.</td>
</tr>
<tr>
<td></td>
<td>Shows sample output.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>ASA(config)# aaa-server KG protocol kerberos</td>
</tr>
<tr>
<td></td>
<td>ASA(config)# aaa-server KG (inside) host DC</td>
</tr>
<tr>
<td></td>
<td>ASA(config-aaa-server-host_# kerberos-realm test.edu</td>
</tr>
<tr>
<td></td>
<td>ASA(webvpn-config)# kcd-server KG username user1 password abc123</td>
</tr>
<tr>
<td></td>
<td>ASA(webvpn-config)# no kcd-server</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional)</td>
</tr>
<tr>
<td></td>
<td>no kcd-server</td>
</tr>
<tr>
<td></td>
<td>Removes the specified behavior for the ASA.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional)</td>
</tr>
<tr>
<td></td>
<td>kcd-server name reset</td>
</tr>
<tr>
<td></td>
<td>Resets the named kcd-server to the internal state.</td>
</tr>
<tr>
<td>Step 6</td>
<td>kcd-server &lt;aaa-kerberos-grp&gt; username &lt;user&gt; password &lt;pass&gt;</td>
</tr>
<tr>
<td></td>
<td>Checks for the presence of a kcd-server and starts the domain join process.</td>
</tr>
<tr>
<td></td>
<td>The Active Directory username and password are used only in exec-mode and are not saved in the configuration.</td>
</tr>
<tr>
<td></td>
<td>Note Administrative privileges are required for initial join. A user with service-level privileges on the domain controller will not get access.</td>
</tr>
<tr>
<td></td>
<td>user—Does not correspond to a specific administrative user but simply a user with service-level privileges to add a device on the Windows domain controller.</td>
</tr>
<tr>
<td></td>
<td>pass—The password does not correspond to a specific password but simply a user with service-level password privileges to add a device on the Windows domain controller.</td>
</tr>
<tr>
<td>Step 7</td>
<td>no kcd-server</td>
</tr>
<tr>
<td></td>
<td>Removes the specified behavior for the ASA.</td>
</tr>
</tbody>
</table>

Showing KCD Status Information

To display the domain controller information and the domain join status, follow these commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>webvpn</td>
</tr>
<tr>
<td></td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>show webvpn kcd</td>
</tr>
<tr>
<td></td>
<td>Displays the domain controller information and the domain join status.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>ASA# show webvpn kcd</td>
</tr>
<tr>
<td></td>
<td>KCD-Server Name: DC</td>
</tr>
<tr>
<td></td>
<td>User : user1</td>
</tr>
<tr>
<td></td>
<td>Password : ****</td>
</tr>
<tr>
<td></td>
<td>KCD State : Joined</td>
</tr>
<tr>
<td></td>
<td>Shows sample output returned from this command.</td>
</tr>
</tbody>
</table>

Showing Cached Kerberos Tickets

To display all Kerberos tickets cached on the ASA, enter the following commands:
### Understanding How KCD Works

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>webvpn</code> Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>show aaa kerberos</code> Displays all Kerberos tickets cached on the ASA.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`show aaa kerberos [username user</td>
</tr>
<tr>
<td></td>
<td>• user—Used to view the Kerberos tickets of a specific user</td>
</tr>
<tr>
<td></td>
<td>• hostname—Used to view the Kerberos tickets issued for a specific host</td>
</tr>
</tbody>
</table>

#### Example:

ASA# `show aaa kerberos`

<table>
<thead>
<tr>
<th>Default Principal</th>
<th>Valid Starting</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:asa@example.COM">asa@example.COM</a></td>
<td>06/29/10 18:33:00</td>
<td>06/30/10 18:33:00</td>
</tr>
<tr>
<td>krbtgt/example.COM@example.COM</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 17:33:00</td>
<td>06/30/10 17:33:00</td>
</tr>
<tr>
<td>asa$/example.COM@example.COM</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 17:33:00</td>
<td>06/30/10 17:33:00</td>
</tr>
<tr>
<td>http/owa.example.com@example.COM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ASA# `show aaa kerberos username kcduser`

<table>
<thead>
<tr>
<th>Default Principal</th>
<th>Valid Starting</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 17:33:00</td>
<td>06/30/10 17:33:00</td>
</tr>
<tr>
<td>asa$/example.COM@example.COM</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 17:33:00</td>
<td>06/30/10 17:33:00</td>
</tr>
<tr>
<td>http/owa.example.com@example.COM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ASA# `show aaa kerberos host owa.example.com`

<table>
<thead>
<tr>
<th>Default Principal</th>
<th>Valid Starting</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 06/30/10</td>
<td>17:33:00</td>
</tr>
<tr>
<td>http/owa.example.com@example.COM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ASA# `show aaa kerberos username kcduser`

<table>
<thead>
<tr>
<th>Default Principal</th>
<th>Valid Starting</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 17:33:00</td>
<td>06/30/10 17:33:00</td>
</tr>
<tr>
<td>asa$/example.COM@example.COM</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 17:33:00</td>
<td>06/30/10 17:33:00</td>
</tr>
<tr>
<td>http/owa.example.com@example.COM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ASA# `show aaa kerberos host owa.example.com`

<table>
<thead>
<tr>
<th>Default Principal</th>
<th>Valid Starting</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 17:33:00</td>
<td>06/30/10 17:33:00</td>
</tr>
<tr>
<td>asa$/example.COM@example.COM</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:kcduser@example.COM">kcduser@example.COM</a></td>
<td>06/29/10 17:33:00</td>
<td>06/30/10 17:33:00</td>
</tr>
<tr>
<td>http/owa.example.com@example.COM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Shows sample output returned from this command.
Clearing Cached Kerberos Tickets

To clear all Kerberos ticket information on the ASA, follow these commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>clear aaa kerberos tickets</td>
<td>Clears all Kerberos ticket information on the ASA.</td>
</tr>
<tr>
<td>clear aaa kerberos tickets [username user</td>
<td></td>
</tr>
<tr>
<td>] host ip [hostname]</td>
<td></td>
</tr>
<tr>
<td>• user—Used to clear the Kerberos tickets of a specific user</td>
<td></td>
</tr>
<tr>
<td>• hostname—Used to clear the Kerberos tickets of a specific host</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

Restriction

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

**Detailed Steps**

**Configuring Application Access**

The following sections describe how to enable smart tunnel access and port forwarding on clientless SSL VPN sessions, specify the applications to be provided with such access, and provide notes on using it:

- Configuring Smart Tunnel Log Off
- Configuring Smart Tunnel Access

**Configuring Smart Tunnel Log Off**

To configure smart tunnel access, you create a smart tunnel list containing one or more applications eligible for smart tunnel access, and the endpoint operating system associated with the list. Because each group policy or local user policy supports one smart tunnel list, you must group the nonbrowser-based applications to be supported into a smart tunnel list. After creating a list, you assign it to one or more group policies or local user policies.

The following sections describe smart tunnels and how to configure them:

- About Smart Tunnels
- Why Smart Tunnels?
- Adding Applications to Be Eligible for Smart Tunnel Access
- Adding Applications to Be Eligible for Smart Tunnel Access
- About Smart Tunnel Lists
About Smart Tunnels

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

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

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

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

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

Why Smart Tunnels?

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

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

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

Prerequisites

See the Supported VPN Platforms, Cisco ASA 5500 Series for the platforms and browsers supported by ASA Release 9.0 smart tunnels.

The following requirements and limitations apply to smart tunnel access on Windows:

- ActiveX or Oracle Java Runtime Environment (JRE) 4 update 15 or later (JRE 6 or later recommended) on Windows must be enabled on the browser.

  ActiveX pages require that you enter the **activex-relay** command on the associated group policy. If you do so or assign a smart tunnel list to the policy, and the browser proxy exception list on the endpoint specifies a proxy, the user must add a “shutdown.webvpn.relay.” entry to this list.
Chapter 1      Configuring Clientless SSL VPN

Configuring Application Access

• Only Winsock 2, TCP-based applications are eligible for smart tunnel access.
• For Mac OS X only, Java Web Start must be enabled on the browser.

Restrictions

• Smart tunnel supports only proxies placed between computers running Microsoft Windows and the security appliance. Smart Tunnel uses the Internet Explorer configuration, which sets system-wide parameters in Windows. That configuration may include proxy information:
  – If a Windows computer requires a proxy to access the ASA, then there must be a static proxy entry in the client's browser, and the host to connect to must be in the client's list of proxy exceptions.
  – If a Windows computer does not require a proxy to access the ASA, but does require a proxy to access a host application, then the ASA must be in the client's list of proxy exceptions.

Proxy systems can be defined the client’s configuration of static proxy entry or automatic configuration, or by a PAC file. Only static proxy configurations are currently supported by Smart Tunnels.
• Kerberos constrained delegation (KCD) is not supported for smart tunnels.
• For Windows, if you want to add smart tunnel access to an application started from the command prompt, you must specify “cmd.exe” in the Process Name of one entry in the smart tunnel list, and specify the path to the application itself in another entry, because “cmd.exe” is the parent of the application.
• With HTTP-based remote access, some subnets may block user access to the VPN gateway. To fix this, place a proxy in front of the ASA to route traffic between the web and the end user. That proxy must support the CONNECT method. For proxies that require authentication, Smart Tunnel supports only the basic digest authentication type.
• When smart tunnel starts, the ASA by default passes all browser traffic through the VPN session if the browser process is the same. The ASA only also does this if a tunnel-all policy (the default) applies. If the user starts another instance of the browser process, it passes all traffic through the VPN session. If the browser process is the same and the security appliance does not provide access to a URL, the user cannot open it. As a workaround, assign a tunnel policy that is not tunnel-all.
• A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.
• The Mac version of smart tunnel does not support POST bookmarks, form-based auto sign-on, or POST macro substitution.
• For Mac OS X users, only those applications started from the portal page can establish smart tunnel connections. This requirement includes smart tunnel support for Firefox. Using Firefox to start another instance of Firefox during the first use of a smart tunnel requires the user profile named csco_st. If this user profile is not present, the session prompts the user to create one.
• In Mac OS X, applications using TCP that are dynamically linked to the SSL library can work over a smart tunnel.
• Smart tunnel does not support the following on Mac OS X:
  – Proxy services.
  – Auto sign-on.
  – Applications that use two-level name spaces.
  – Console-based applications, such as Telnet, SSH, and cURL.
  – Applications using dlopen or dlsym to locate libsocket calls.
– Statically linked applications to locate libsocket calls.

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

---

**Adding Applications to Be Eligible for Smart Tunnel Access**

The clientless SSL VPN configuration of each ASA supports *smart tunnel lists*, each of which identifies one or more applications eligible for smart tunnel access. Because each group policy or username supports only one smart tunnel list, you must group each set of applications to be supported into a smart tunnel list.

**About Smart Tunnel Lists**

For each group policy and username, you can configure clientless SSL VPN to do one of the following:

- Start smart tunnel access automatically upon user login.
- Enable smart tunnel access upon user login, but require the user to start it manually, using the **Application Access > Start Smart Tunnels** button on the clientless SSL VPN Portal Page.

**Restrictions**

The smart tunnel logon options are mutually exclusive for each group policy and username. Use only one.

**Detailed Steps**

The following smart tunnel commands are available to each group policy and username. The configuration of each group policy and username supports only one of these commands at a time, so when you enter one, the ASA replaces the one present in the configuration of the group policy or username in question with the new one, or in the case of the last command, simply removes the smart-tunnel command already present in the group policy or username.
## Configuring and Applying Smart Tunnel Policy

The smart tunnel policy requires a per group policy/username configuration. Each group policy/username references a globally configured list of networks. When the smart tunnel is turned on, you can allow traffic outside of the tunnel with the use of 2 CLIs: one configures the network (a set of hosts), and the other uses the specified smart-tunnel network to enforce a policy on a user. The following commands create a list of hosts to use for configuring smart tunnel policies:

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>smart-tunnel auto-start list</td>
<td>Starts smart tunnel access automatically upon user login.</td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
<tr>
<td>smart-tunnel enable list</td>
<td>Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the Application Access &gt; Start Smart Tunnels button on the clientless SSL VPN portal page.</td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
<tr>
<td>smart-tunnel disable</td>
<td>Prevents smart tunnel access.</td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
<tr>
<td>no smart-tunnel [auto-start list</td>
<td>enable list</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Refer to Automating Smart Tunnel Access for the option you want to use.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>[no] smart-tunnel network &lt;network name&gt; ip &lt;ip&gt; &lt;netmask&gt;</td>
<td>Creates a list of hosts to use for configuring smart tunnel policies. &lt;network name&gt; is the name to apply to the tunnel policy. &lt;ip&gt; is the IP address of the network. &lt;netmask&gt; is the netmask of the network.</td>
</tr>
</tbody>
</table>
Step 3

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] smart-tunnel network &lt;network name&gt; host &lt;host mask&gt;</td>
<td>Establishes the hostname mask, such as *.cisco.com.</td>
</tr>
</tbody>
</table>

Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] smart-tunnel tunnel-policy ((excludespecified</td>
<td>tunnelspecified) &lt;network name&gt;</td>
</tr>
</tbody>
</table>

**Configuring and Applying a Smart Tunnel Tunnel Policy**

Like the split tunnel configuration in SSL VPN client, the smart tunnel tunnel policy is a per group-policy/username configuration. Each group policy/username references a globally configured list of networks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] smart-tunnel tunnel-policy ((excludespecified</td>
<td>tunnelspecified) &lt;network name&gt;</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ciscoasa(config-webvpn)# [no] smart-tunnel network &lt;network name&gt; ip &lt;ip&gt; &lt;netmask&gt;</code></td>
<td>Applies a tunnel policy to a group-policy/user policy. One command specifies host and the other specifies network IPs; use only one.</td>
</tr>
<tr>
<td><code>ciscoasa(config-webvpn)# [no] smart-tunnel network &lt;network name&gt; host &lt;host mask&gt;</code></td>
<td>Smart tunnel tunnel policy configuration is a good option when a vendor wants to provide a partner with clientless access to an internal inventory server page upon login without going through the clientless portal first. Creates a tunnel policy that contains only one host (assuming the inventory pages are hosted at <a href="http://www.example.com">www.example.com</a> (10.5.2.2), and you want to configure both IP address and name for the hosts. Applies the tunnel-specified tunnel policy to the partner’s group policy.</td>
</tr>
<tr>
<td>Example: <code>ciscoasa(config-webvpn)# smart-tunnel network inventory ip 10.5.2.2</code></td>
<td>Specifies the group policy home page and enables smart tunnel on it. Without writing a script or uploading anything, an administrator can specify which homepage to connect with via smart tunnel.</td>
</tr>
<tr>
<td><code>ciscoasa(config-webvpn)# smart-tunnel tunnel-policy tunnelspecified inventory</code></td>
<td>By default, configuration of a smart tunnel application is not necessary because all processes initiated by the browser with smart tunnel enabled have access to the tunnel. However, because no portal is visible, you may want to enable the logout notification icon.</td>
</tr>
<tr>
<td><code>(Optional)</code></td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config-group-webvpn)# homepage value http://www.example.com</code></td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config-group-webvpn)# homepage use-smart-tunnel</code></td>
<td></td>
</tr>
<tr>
<td><code>(Optional)</code></td>
<td></td>
</tr>
<tr>
<td><code>ciscoasa(config-webvpn)# smart-tunnel notification-icon</code></td>
<td></td>
</tr>
</tbody>
</table>

### Creating a Smart Tunnel Auto Sign-On Server List
### Command Purpose

**webvpn**

Switches to webvpn configuration mode.

**smart-tunnel auto-signon** list [use-domain] [realm realm-string] [port port-num] [ip ip-address [netmask] | host hostname-mask]

Use for each server you want to add to the server list

- **list** — names the list of remote servers. Use quotation marks around the name if it includes a space. The string can be up to 64 characters. The ASA creates the list if it is not already present in the configuration. Otherwise, it adds the entry to the list. Assign a name that will help you to distinguish.

- **use-domain** (optional) — Adds the Windows domain to the username if authentication requires it. If you enter this keyword, be sure to specify the domain name when assigning the smart tunnel list to one or more group policies, or usernames.

- **realm** — Configures a realm for the authentication. Realm is associated with the protected area of the website and is passed back to the browser either in the authentication prompt or in the HTTP headers during authentication. Once auto-sign is configured and a realm string is specified, users can configure the realm string on a web application (such as Outlook Web Access) and access web applications without signing on.

- **port** — Specifies which port performs auto sign-on. For Firefox, if no port number is specified, auto sign is performed on HTTP and HTTPS, accessed by the default port numbers 80 and 443 respectively.

- **ip** — Specifies the server by its IP address and netmask.

- **ip-address[netmask]** — Identifies the sub-network of hosts to auto-authenticate to.

- **host** — Specifies the server by its host name or wildcard mask. Using this option protects the configuration from dynamic changes to IP addresses.

- **hostname-mask** — Specifies which host name or wildcard mask to auto-authenticate to.

**show running-config webvpn smart-tunnel**

Displays the smart tunnel auto sign-on list entries.

(Optional)

[no] smart-tunnel auto-signon list [use-domain] [realm realm-string] [port port-num] [ip ip-address [netmask] | host hostname-mask]

Removes an entry from the list of servers, specifying both the list and IP address or hostname as it appears in the ASA configuration.
Following the configuration of the smart tunnel auto sign-on server list, you must assign it to a group policy or a local user policy for it to become active, as described in the next section.

The next step is to add servers to the server list.

### Adding Servers to a Smart Tunnel Auto Sign-on Server List

The following steps describe how to add servers to the list of servers for which to provide auto sign-on in smart tunnel connections, and assign that list to a group policies or a local user.

#### Prerequisites

You must use the `smart-tunnel auto-signon list` command to create a list of servers first. You can assign only one list to a group policy or username.

#### Restrictions

- The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using Internet Explorer and Firefox.
- Firefox requires the administrator to specify hosts using an exact host name or IP address (instead of a host mask with wild cards, a subnet using IP addresses, or a netmask). For example, within Firefox, you cannot enter *.cisco.com and expect auto sign-on to host email.cisco.com.

#### Detailed Steps

To enable smart tunnel auto sign-on in clientless (browser-based) SSL VPN sessions, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>config-webvpn</code></td>
<td>Switches to config-webvpn configuration mode.</td>
</tr>
<tr>
<td><code>smart-tunnel auto-signon HR use-domain ip 192.32.22.56 255.255.255.0</code></td>
<td>Adds all hosts in the subnet and adds the Windows domain to the username if authentication requires it. (Optional)</td>
</tr>
<tr>
<td><code>no smart-tunnel auto-signon HR use-domain ip 192.32.22.56 255.255.255.0</code></td>
<td>Removes that entry from the list and the list named HR if the entry removed is the only entry in the list.</td>
</tr>
<tr>
<td><code>no smart-tunnel auto-signon HR</code></td>
<td>Removes the entire list from the ASA configuration.</td>
</tr>
<tr>
<td><code>smart-tunnel auto-signon intranet host *.example.com</code></td>
<td>Adds all hosts in the domain to the smart tunnel auto sign-on list named intranet.</td>
</tr>
<tr>
<td><code>no smart-tunnel auto-signon intranet host *.example.com</code></td>
<td>Removes that entry from the list.</td>
</tr>
</tbody>
</table>

Following the configuration of the smart tunnel auto sign-on server list, you must assign it to a group policy or a local user policy for it to become active, as described in the next section.
## Automating Smart Tunnel Access

To start smart tunnel access automatically upon user login, enter the following commands:

### Requirements

For Mac OS X, you must click the link for the application in the portal’s Application Access panel, with or without auto-start configured.
## Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>group-policy webvpn OR username webvpn</td>
<td>Switches to group-policy webvpn configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Switches to username webvpn configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>smart-tunnel auto-start list</td>
<td>Starts smart tunnel access automatically upon user login. <em>list</em> is the name of the smart tunnel list already present.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assigns the smart tunnel list named <em>apps1</em> to the group policy.</td>
</tr>
<tr>
<td>4</td>
<td>show running-config webvpn smart-tunnel</td>
<td>Views the smart tunnel list entries in the SSL VPN configuration.</td>
</tr>
<tr>
<td>5</td>
<td>(Optional) no smart-tunnel</td>
<td>Removes the smart-tunnel command from the group policy or username and reverts to the default.</td>
</tr>
</tbody>
</table>

## Enabling and Disabling Smart Tunnel Access

By default, smart tunnels are disabled.

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>group-policy webvpn OR username webvpn</td>
<td>Switches to group-policy webvpn configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Switches to username webvpn configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>smart-tunnel [enable list</td>
<td>disable]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assigns the smart tunnel list named <em>apps1</em> to the group policy.</td>
</tr>
<tr>
<td>4</td>
<td>show running-config webvpn smart-tunnel</td>
<td>Shows the smart tunnel list entries in the SSL VPN configuration.</td>
</tr>
</tbody>
</table>
Configuring Application Access

Configuring Smart Tunnel Log Off

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

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

When Its Parent Process Terminates

This practice requires the closing of all browsers to signify log off. The smart tunnel lifetime is now tied to the starting process lifetime. For example, if you started a smart tunnel from Internet Explorer, the smart tunnel is turned off when no iexplore.exe is running. Smart tunnel can determine that the VPN session has ended even if the user closed all browsers without logging out.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no smart-tunnel</td>
<td>Removes the smart-tunnel command from the group policy or local user policy and reverts to the default group-policy.</td>
</tr>
<tr>
<td>6</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td></td>
<td>smart-tunnel disable</td>
<td>Disables smart tunnel access.</td>
</tr>
</tbody>
</table>
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>[no] smart-tunnel notification-icon</td>
</tr>
</tbody>
</table>
| | Allows administrators to turn on the notification icon on a global basis. This command configures log out properties and controls whether the user is presented with a logout icon for logging out, as opposed to having logout triggered by closing browser windows. This command also controls logging off when a parent process terminates, which is automatically turned on or off when the notification icon is turned on or off.  
notification-icon is the keyword that specifies when to use the icon for logout. |
| | Note The *no* version of this CLI is the default, in which case, closing all browser windows logs off the SSL VPN session. |
| | Note Portal logout still takes effect and is not impacted. |
| **Step 2** | *.*.webvpn.* |
| | When using a proxy and adding to the proxy list exception, it ensures that smart tunnel is properly closed when you log off, regardless of icon usage or not. |

**With A Notification Icon**

You may also choose to disable logging off when a parent process terminates so that a session survives if you close a browser. For this practice, you use a notification icon in the system tray to log out. The icon remains until the user clicks the icon to logout. If the session has expired before the user has logged out, the icon remains until the next connection is tried. You may have to wait for the session status to update in the system tray.

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

**Configuring Port Forwarding**

The following sections describe port forwarding and how to configure it:

- Information About Port Forwarding, page 1-64
- Configuring DNS for Port Forwarding
- Adding Applications to Be Eligible for Port Forwarding
- Assigning a Port Forwarding List
- Automating Port Forwarding
Information About Port Forwarding

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

- Lotus Notes
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP (FTP over SSH)
- SSH
- TELNET
- Windows Terminal Service

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

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

Consider the following alternatives to port forwarding:

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

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

Prerequisites

- Refer to the Supported VPN Platforms, Cisco ASA 5500 Series compatibility guide for port forwarding pre-requisites.
- Browser-based users of Safari on Mac OS X 10.5.3 must identify a client certificate for use with the URL of the ASA, once with the trailing slash and once without it, because of the way Safari interprets URLs. For example,
  - https://example.com/
  - https://example.com
  For details, go to the Safari, Mac OS X 10.5.3: Changes in client certificate authentication.
- Users of Microsoft Windows Vista or later who use port forwarding or smart tunnels must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the Tools > Internet Options > Security tab. Vista (or later) users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer’s vulnerability to attack.
Restrictions

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

- Port forwarding does not support Microsoft Outlook Exchange (MAPI) proxy. However, you can configure smart tunnel support for Microsoft Office Outlook in conjunction with Microsoft Outlook Exchange Server.

- A stateful failover does not retain sessions established using Application Access (either port forwarding or smart tunnel access). Users must reconnect following a failover.

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

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

Configuring DNS for Port Forwarding

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 dns server-group</td>
<td>Enters the dns server-group mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>hostname(config)# dns server-group example.com</td>
<td>Configures a DNS server group named example.com.</td>
</tr>
<tr>
<td>hostname(config-dns-server-group)# domain-name example.com</td>
<td></td>
</tr>
<tr>
<td>hostname(config-dns-server-group)# name-server 192.168.10.10</td>
<td></td>
</tr>
<tr>
<td>Step 2 domain-name</td>
<td>Specifies the domain name. The default setting of domain-name is DefaultDNS.</td>
</tr>
<tr>
<td>Step 3 name-server</td>
<td>Resolves the domain name to an IP address.</td>
</tr>
<tr>
<td>Step 4 webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
</tbody>
</table>
Configuring Port Forwarding

Adding Applications to Be Eligible for Port Forwarding

The clientless SSL VPN configuration of each ASA supports port forwarding lists, each of which specifies local and remote ports used by the applications for which you want to provide access. Because each group policy or username supports only one port forwarding list, you must group each set of applications to be supported into a list. To display the port forwarding list entries already present in the ASA configuration, enter the following commands:

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show run webvpn port-forward</td>
</tr>
<tr>
<td>Step 2</td>
<td>webvpn</td>
</tr>
</tbody>
</table>

---

### Command Purpose

**Step 5**

- **tunnel-group webvpn**
  - Switches to tunnel-group webvpn configuration mode.

**Step 6**

- *(Required only if you are using a domain name other than the default one [DefaultDNS])*
  - **dns-group**
  - **Example:**
    
    asa2(config-dns-server-group)# exit
    asa2(config)# tunnel-group DefaultWEBVPNGroup
    webvpn-attributes
    asa2(config-tunnel-webvpn)# dns-group example.com

  - Specifies the domain name the tunnel groups will use. By default, the security appliance assigns the Default WEBVPNGroup as the default tunnel group for clientless connections. Follow this instruction if the ASA uses that tunnel group to assign settings to the clientless connections. Otherwise, follow this step for each tunnel configured for clientless connections.

---

---

---
### Step 3

**Command**

```
port-forward {list_name local_port remote_server remote_port description}
```

**Purpose**

Adds a port forwarding entry to a list.

- **list_name**—Name for a set of applications (technically, a set of forwarded TCP ports) for users of clientless SSL VPN sessions to access. The ASA creates a list using the name you enter if it does not recognize it. Otherwise, it adds the port forwarding entry to the list. Maximum 64 characters.

- **local_port**—Port that listens for TCP traffic for an application running on the user’s computer. You can use a local port number only once for each port forwarding list. Enter a port number in the range 1-65535 or port name. To avoid conflicts with existing services, use a port number greater than 1024.

- **remote_server**—DNS name or IP address of the remote server for an application. The IP address can be in IPv4 or IPv6 format. We recommend a DNS name so that you do not have to configure the client applications for a specific IP address.

- **remote_port**—Port to connect to for this application on the remote server. This is the actual port the application uses. Enter a port number in the range 1-65535 or port name.

- **description**—Application name or short description that displays on the end user Port Forwarding Java applet screen. Maximum 64 characters.

**Example:**

```
hostname(config)# webvpn
hostname(config-webvpn)# port-forward
SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
hostname(config-webvpn)# port-forward
SalesGroupPorts 20025 SMTPSserver 25 Send Mail
hostname(config-webvpn)# port-forward
SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
hostname(config-webvpn)# port-forward
SalesGroupPorts 20023 Telnetserver 23 Telnet
```

### Step 4

**(Optional)**

**Command**

```
no port-forward list_name local_port
```

**Purpose**

Removes an entry from the list, specifying both the list and the local port.

**Note**

The DNS name must match the one assigned to the tunnel group to establish the tunnel and resolve to an IP address, per the instructions in the previous section. The default setting for both the **domain-name group** and **dns-group** commands described in that section is DefaultDNS.

- **remote_port**—Port to connect to for this application on the remote server. This is the actual port the application uses. Enter a port number in the range 1-65535 or port name.

- **description**—Application name or short description that displays on the end user Port Forwarding Java applet screen. Maximum 64 characters.

**Example:**

```
hostname(config)# webvpn
hostname(config-webvpn)# port-forward
SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
hostname(config-webvpn)# port-forward
SalesGroupPorts 20025 SMTPSserver 25 Send Mail
hostname(config-webvpn)# port-forward
SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
hostname(config-webvpn)# port-forward
SalesGroupPorts 20023 Telnetserver 23 Telnet
```
Following the configuration of a port forwarding list, assign the list to group policies or usernames, as described in the next section.

Assigning a Port Forwarding List

You can add or edit a named list of TCP applications to associate with users or group policies for access over clientless SSL VPN connections. For each group policy and username, you can configure clientless SSL VPN to do one of the following:

- Start port forwarding access automatically upon user login.

**Note**

These options are mutually exclusive for each group policy and username. Use only one.

**Detailed Steps**

These commands are available to each group policy and username. The configuration of each group policy and username supports only one of these commands at a time, so when you enter one, the ASA replaces the one present in the configuration of the group policy or username in question with the new one, or in the case of the last command, simply removes the **port-forward** command from the group policy or username configuration.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>port-forward auto-start list_name</code></td>
<td>Starts port forwarding automatically upon user login.</td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
<tr>
<td><code>port-forward enable list_name</code></td>
<td>Enables port forwarding upon user login.</td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
<tr>
<td><code>port-forward disable</code></td>
<td>Prevents port forwarding.</td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
<tr>
<td>`no port-forward [auto-start list_name</td>
<td>enable list_name</td>
</tr>
</tbody>
</table>

For details, go to the section that addresses the option you want to use.

**Automating Port Forwarding**

To start port forwarding automatically upon user login, enter the following commands:
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>webvpn</td>
</tr>
<tr>
<td></td>
<td>Switches to webvpn configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2  | group-policy webvpn  
|         | username webvpn |
|         | Switches to group-policy webvpn configuration mode.  
|         | Switches to username webvpn configuration mode. |
| Step 3  | port-forward auto-start list_name |
|         | Starts port forwarding automatically upon user login.  
|         | list_name names the port forwarding list already present in the ASA webvpn configuration. You cannot assign more than one port forwarding list to a group policy or username.  
|         | Assigns the port forwarding list named apps1 to the group policy. |
| Step 4  | show run webvpn port-forward |
|         | Displays the port forwarding list entries present in the ASA configuration. |
| Step 5  | (Optional)  
|         | no port-forward |
|         | Removes the port-forward command from the group policy or username and reverts to the default. |

Enabling and Disabling Port Forwarding

By default, port forwarding is disabled.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>port-forward [enable list_name / disable]</td>
</tr>
</tbody>
</table>
|         | Enables port forwarding. You do not have to start port forwarding manually if you entered port-forward auto-start list_name from the previous table.  
|         | list_name is the name of the port forwarding list already present in the ASA webvpn configuration. You cannot assign more than one port forwarding list to a group policy or username.  
|         | Assigns the port forwarding list named apps1 to the group policy. |
| Step 2  | show running-config port-forward |
|         | Views the port forwarding list entries. |
Application Access User Notes

The following sections provide information about using application access:

- Closing Application Access to Prevent hosts File Errors
- Closing Application Access to Prevent hosts File Errors
- Recovering from hosts File Errors When Using Application Access

Closing Application Access to Prevent hosts File Errors

To prevent hosts file errors that can interfere with Application Access, close the Application Access window properly when you finish using Application Access. To do so, click the close icon.

Recovering from hosts File Errors When Using Application Access

The following errors can occur if you do not close the Application Access window properly:

- The next time you try to start Application Access, it might be disabled; you receive a Backup HOSTS File Found error message.
- The applications themselves might be disabled or might malfunction, even when you are running them locally.

These errors can result from terminating the Application Access window in any improper way. For example:

- Your browser crashes while you are using Application Access.
- A power outage or system shutdown occurs while you are using Application Access.
- You minimize the Application Access window while you are working, then shut down your computer with the window active (but minimized).

This section includes the following topics:

- Understanding the hosts File
- Stopping Application Access Improperly
- Reconfiguring a Host’s File Automatically Using Clientless SSL VPN
- Reconfiguring hosts File Manually
Understanding the hosts File

The hosts file on your local system maps IP addresses to host names. When you start Application Access, clientless SSL VPN modifies the hosts file, adding clientless SSL VPN-specific entries. Stopping Application Access by properly closing the Application Access window returns the file to its original state.

<table>
<thead>
<tr>
<th>Before invoking Application Access...</th>
<th>hosts file is in original state.</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Application Access starts....</td>
<td>• Clientless SSL VPN copies the hosts file to hosts.webvpn, thus creating a backup.</td>
</tr>
<tr>
<td></td>
<td>• Clientless SSL VPN then edits the hosts file, inserting clientless SSL VPN-specific information.</td>
</tr>
<tr>
<td>When Application Access stops...</td>
<td>• Clientless SSL VPN copies the backup file to the hosts file, thus restoring the hosts file to its original state.</td>
</tr>
<tr>
<td></td>
<td>• Clientless SSL VPN deletes hosts.webvpn.</td>
</tr>
<tr>
<td>After finishing Application Access...</td>
<td>hosts file is in original state.</td>
</tr>
</tbody>
</table>

**Note**

Microsoft anti-spyware software blocks changes that the port forwarding Java applet makes to the hosts file. See [www.microsoft.com](http://www.microsoft.com) for information on how to allow hosts file changes when using anti-spyware software.

Stopping Application Access Improperly

When Application Access terminates abnormally, the hosts file remains in a clientless SSL VPN-customized state. Clientless SSL VPN checks the state the next time you start Application Access by searching for a hosts.webvpn file. If it finds one, a Backup HOSTS File Found error message (Figure 1-8) appears, and Application Access is temporarily disabled.

Once you shut down Application Access improperly, you leave your remote access client/server applications in limbo. If you try to start these applications without using clientless SSL VPN, they might malfunction. You might find that hosts that you normally connect to are unavailable. This situation could commonly occur if you run applications remotely from home, fail to quit the Application Access window before shutting down the computer, then try to run the applications later from the office.

Reconfiguring a Host’s File Automatically Using Clientless SSL VPN

If you are able to connect to your remote access server, follow these steps to reconfigure the host’s file and re-enable both Application Access and the applications.

**Detailed Steps**

**Step 1**
Start clientless SSL VPN and log in. The home page opens.

**Step 2**
Click the Applications Access then Start Applications, a Backup HOSTS File Found message appears. (See Figure 1-8.)
Step 3  Choose one of the following options:

- **Restore from backup**—Clientless SSL VPN forces a proper shutdown. It copies the hosts.webvpn backup file to the hosts file, restoring it to its original state, then deletes hosts.webvpn. You then have to restart Application Access.

- **Do nothing**—Application Access does not start. The remote access home page reappears.

- **Delete backup**—Clientless SSL VPN deletes the hosts.webvpn file, leaving the hosts file in its clientless SSL VPN-customized state. The original hosts file settings are lost. Application Access then starts, using the clientless SSL VPN-customized hosts file as the new original. Choose this option only if you are unconcerned about losing hosts file settings. If you or a program you use might have edited the hosts file after Application Access has shut down improperly, choose one of the other options, or edit the hosts file manually. (See “Reconfiguring hosts File Manually.”)

---

### Reconfiguring hosts File Manually

If you are not able to connect to your remote access server from your current location, or if you have customized the hosts file and do not want to lose your edits, follow these steps to reconfigure the hosts file and reenable both Application Access and the applications.

**Detailed Steps**

1. **Locate and edit your hosts file.** The most common location is `c:\windows\system32\drivers\etc\hosts`.

2. **Check to see if any lines contain the string:** 
   
   ```
   # added by WebVpnPortForward
   ```
   
   If any lines contain this string, your hosts file is clientless SSL VPN-customized. If your hosts file is clientless SSL VPN-customized, it looks similar to the following example:

   ```
   server1  # added by WebVpnPortForward
   server1.example.com invalid.cisco.com  # added by WebVpnPortForward
   server2  # added by WebVpnPortForward
   server2.example.com invalid.cisco.com  # added by WebVpnPortForward
   server3  # added by WebVpnPortForward
   server3.example.com invalid.cisco.com  # added by WebVpnPortForward
   # Copyright (c) 1993-1999 Microsoft Corp.
   ```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each entry should be kept on an individual line. The IP address should be placed in the first column followed by the corresponding host name. The IP address and the host name should be separated by at least one space.
#
# Additionally, comments (such as these) may be inserted on individual lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#      38.25.63.10     x.example.com              # x client host
127.0.0.1       localhost

Step 3 Delete the lines that contain the string: # added by WebVpnPortForward

Step 4 Save and close the file.

Step 5 Start clientless SSL VPN and log in.

The home page appears.

Step 6 Click the Application Access link.

The Application Access window appears. Application Access is now enabled.

---

**Configuring File Access**

Clientless SSL VPN serves remote users with HTTPS portal pages that interface with proxy CIFS and/or FTP clients running on the ASA. Using either CIFS or FTP, clientless SSL VPN provides users with network access to the files on the network, to the extent that the users meet user authentication requirements and the file properties do not restrict access. The CIFS and FTP clients are transparent; the portal pages delivered by clientless SSL VPN provide the appearance of direct access to the file systems.

When a user requests a list of files, clientless SSL VPN queries the server designated as the master browser for the IP address of the server containing the list. The ASA gets the list and delivers it to the remote user on a portal page.

Clientless SSL VPN lets the user invoke the following CIFS and FTP functions, depending on user authentication requirements and file properties:

- Navigate and list domains and workgroups, servers within a domain or workgroup, shares within a server, and files within a share or directory
- Create directories
- Download, upload, rename, move, and delete files

The ASA uses a master browser, WINS server, or DNS server, typically on the same network as the ASA or reachable from that network, to query the network for a list of servers when the remote user clicks **Browse Networks** in the menu of the portal page or on the toolbar displayed during the clientless SSL VPN session.

The master browser or DNS server provides the CIFS/FTP client on the ASA with a list of the resources on the network, which clientless SSL VPN serves to the remote user.
Chapter 1      Configuring Clientless SSL VPN

Configuring File Access

Note
Before configuring file access, you must configure the shares on the servers for user access.

CIFS File Access Requirement and Limitation

To access `\server\share\subfolder\personal folder`, the user must have a minimum of read permission for all parent folders, including the share itself.

Use Download or Upload to copy and paste files to and from CIFS directories and the local desktop. The Copy and Paste buttons are intended for remote to remote actions only, not local to remote, or remote to local.

The CIFS browse server feature does not support double-byte character share names (share names exceeding 13 characters in length). This only affects the list of folders displayed, and does not affect user access to the folder. As a workaround, you can pre-configure the bookmark(s) for the CIFS folder(s) that use double-byte share names, or the user can enter the URL or bookmark of the folder in the format `cifs://server/<long-folder-name>`. For example:

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

Adding Support for File Access

Configure file access as follows:

Note
The first procedure describes how to specify the master browser and WINS servers. As an alternative, you can use ASDM to configure URL lists and entries that provide access to file shares.

Adding a share in ASDM does not require a master browser or a WINS server. However, it does not provide support for the Browse Networks link. You can use a hostname or an IP address to refer to ServerA when entering this command. If you use a hostname, the ASA requires a DNS server to resolve it to an IP address.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>Step 2 tunnel-group webvpn</td>
<td>Switches to tunnel-group webvpn configuration mode.</td>
</tr>
</tbody>
</table>
### Step 3

**nbns-server \{IPaddress | hostname\} \{master\} \{timeout timeout \{retry retries\}**

Browses a network or domain for each NetBIOS Name Server (NBNS).

- **master** is the computer designated as the master browser. The master browser maintains the list of computers and shared resources. Any NBNS server you identify with this command without entering the master portion of the command must be a Windows Internet Naming Server (WINS). Specify the master browser first, then specify the WINS servers. You can specify up to three servers, including the master browser, for a connection profile.

- **retries** is the number of times to retry queries to the NBNS server. The ASA recycles through the list of servers this number of times before sending an error message. The default value is 2; the range is 1 through 10.

- **timeout** is the number of seconds the ASA waits before sending the query again, to the same server if it is the only one, or another server if there are more than one. The default timeout is 2 seconds; the range is 1 to 30 seconds.

**Example:**

```
hostname(config-tunnel-webvpn)## nbns-server
192.168.1.20 master
hostname(config-tunnel-webvpn)## nbns-server
192.168.1.41
hostname(config-tunnel-webvpn)## nbns-server
192.168.1.47
```

### Step 4

**show tunnel-group webvpn-attributes**

Displays the NBNS servers already present in the connection profile configuration.
For a complete description of these commands, see the Cisco Security Appliance Command Reference.
Ensuring Clock Accuracy for SharePoint Access

The clientless SSL VPN server on the ASA uses cookies to interact with applications such as Microsoft Word on the endpoint. The cookie expiration time set by the ASA can cause Word to malfunction when accessing documents on a SharePoint server if the time on the ASA is incorrect. To prevent this malfunction, set the ASA clock properly. We recommend configuring the ASA to dynamically synchronize the time with an NTP server. For instructions, see “Setting the Date and Time.”

Using Clientless SSL VPN with PDAs

You can access clientless SSL VPN from your Pocket PC or other certified personal digital assistant device. Neither the ASA administrator nor the clientless SSL VPN user need do anything special to use clientless SSL VPN with a certified PDA.

Cisco has certified the following PDA platform:

- HP iPaq H4150
- Pocket PC 2003
- Windows CE 4.20.0, build 14053
- Pocket Internet Explorer (PIE)
- ROM version 1.10.03ENG
- ROM Date: 7/16/2004

Some differences in the PDA version of clientless SSL VPN exist:

- A banner web page replaces the popup clientless SSL VPN window.
- An icon bar replaces the standard clientless SSL VPN floating toolbar. This bar displays the Go, Home and Logout buttons.
- The Show Toolbar icon is not included on the main clientless SSL VPN portal page.
- Upon clientless SSL VPN logout, a warning message provides instructions for closing the PIE browser properly. If you do not follow these instructions and you close the browser window in the common way, PIE does not disconnect from clientless SSL VPN or any secure website that uses HTTPS.

Restrictions

- Clientless SSL VPN supports OWA 2000 and OWA 2003 Basic Authentication. If Basic Authentication is not configured on an OWA server and a clientless SSL VPN user attempts to access that server, access is denied.
- Unsupported clientless SSL VPN features:
  - Application Access and other Java-dependent features.
  - HTTP proxy.
  - The Citrix Metaframe feature (if the PDA does not have the corresponding Citrix ICA client software).

Using E-Mail over Clientless SSL VPN

Clientless SSL VPN supports several ways to access e-mail. This section includes the following methods:
• Configuring E-mail Proxies
• Configuring Web E-mail: MS Outlook Web App

Configuring E-mail Proxies

Clientless SSL VPN supports IMAP4S, POP3S, and SMTPS e-mail proxies. The following attributes apply globally to e-mail proxy users.

Restrictions
E-mail clients such as MS Outlook, MS Outlook Express, and Eudora lack the ability to access the certificate store.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 accounting-server-group</td>
<td>Specifies the previously configured accounting servers to use with e-mail proxy.</td>
</tr>
<tr>
<td>Step 2 authentication</td>
<td>Specifies the authentication method(s) for e-mail proxy users. The default values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• IMAP4S: Mailhost (required)</td>
</tr>
<tr>
<td></td>
<td>• POP3S Mailhost (required)</td>
</tr>
<tr>
<td></td>
<td>• SMTPS: AAA</td>
</tr>
<tr>
<td>Step 3 authentication-server-group</td>
<td>Specifies the previously configured authentication servers to use with e-mail proxy. The default is LOCAL.</td>
</tr>
<tr>
<td>Step 4 authorization-server-group</td>
<td>Specifies the previously configured authorization servers to use with clientless SSL VPN.</td>
</tr>
<tr>
<td>Step 5 authorization-required</td>
<td>Requires users to authorize successfully to connect. The default is Disabled.</td>
</tr>
<tr>
<td>Step 6 authorization-dn-attributes</td>
<td>Identifies the DN of the peer certificate to use as a username for authorization. The defaults are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Primary attribute: CN</td>
</tr>
<tr>
<td></td>
<td>• Secondary attribute: OU</td>
</tr>
<tr>
<td>Step 7 default-group-policy</td>
<td>Specifies the name of the group policy to use. The default is DfltGrpPolicy.</td>
</tr>
<tr>
<td>Step 8 enable</td>
<td>Enables e-mail proxy on the specified interface. The default is disabled.</td>
</tr>
<tr>
<td>Step 9 name-separator</td>
<td>Defines the separator between the e-mail and VPN usernames and passwords. The default is colon (:).</td>
</tr>
<tr>
<td>Step 10 outstanding</td>
<td>Configures the maximum number of outstanding non-authenticated sessions. The default is 20.</td>
</tr>
</tbody>
</table>
Chapter 1      Configuring Clientless SSL VPN

Configuring Portal Access Rules

This enhancement allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in the HTTP header. If the ASA denies a clientless SSL VPN session, it returns an error code to the endpoint immediately.

The ASA evaluates this access policy before the endpoint authenticates to the ASA. As a result, in the case of a denial, fewer ASA processing resources are consumed by additional connection attempts from the endpoint.

Prerequisites
Log on to the ASA and enter global configuration mode. In global configuration mode, the ASA displays this prompt:

```
hostname(config) #
```
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 webvpn</td>
<td>Enter webvpn configuration mode.</td>
</tr>
<tr>
<td>Example: hostname(config)# webvpn</td>
<td></td>
</tr>
<tr>
<td>Step 2 portal-access-rule priority [{permit</td>
<td>deny [code code]}] {any</td>
</tr>
<tr>
<td>Example: hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match <em>Thunderbird</em></td>
<td></td>
</tr>
<tr>
<td>hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match &quot;<em>my_agent</em>&quot;</td>
<td></td>
</tr>
</tbody>
</table>

Optimizing Clientless SSL VPN Performance

The ASA provides several ways to optimize clientless SSL VPN performance and functionality. Performance improvements include caching and compressing web objects. Functionality tuning includes setting limits on content transformation and proxy-bypass. APCF provides an additional method of tuning content transformation. The following sections explain these features:

- Configuring Caching
- Configuring Content Transformation

Configuring Caching

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

By default, caching is enabled. You can customize the way caching works for your environment by using the caching commands in cache mode.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>webvpn Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>disable Disables caching.</td>
</tr>
<tr>
<td>Step 3</td>
<td>expiry-time Configures an expiration time for caching objects.</td>
</tr>
<tr>
<td>Step 4</td>
<td>lmfactor Configures terms for revalidating cached objects.</td>
</tr>
<tr>
<td>Step 5</td>
<td>max-object-size Sets a maximum size for objects to cache.</td>
</tr>
<tr>
<td>Step 6</td>
<td>min-object-size Sets a minimum size for objects to cache.</td>
</tr>
<tr>
<td>Step 7</td>
<td>cache-static-content Caches all cacheable web objects, content not subject to rewriting. Examples include images and PDF files.</td>
</tr>
</tbody>
</table>

Configuring Content Transformation

By default, the ASA processes all clientless SSL VPN traffic through a content transformation/rewriting engine that includes advanced elements such as JavaScript and Java to proxy HTTP traffic that may have different semantics and access control rules depending on whether the user is accessing an application within or independently of an SSL VPN device.

Some web resources require highly individualized treatment. The following sections describe functionality that provides such treatment:

- Configuring a Certificate for Signing Rewritten Java Content
- Disabling Content Rewrite
- Using Proxy Bypass

Subject to the requirements of your organization and the web content involved, you might use one of these features.

Configuring a Certificate for Signing Rewritten Java Content

Java objects which have been transformed by clientless SSL VPN can subsequently be signed using a PKCS12 digital certificate associated with a trustpoint.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>crypto ca import</td>
</tr>
<tr>
<td></td>
<td>Imports a certificate.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ava-trustpoint</td>
</tr>
<tr>
<td></td>
<td>Employs a certificate.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>hostname(config)# crypto ca import mytrustpoint</td>
</tr>
<tr>
<td></td>
<td>pkcs12 mypassphrase</td>
</tr>
<tr>
<td></td>
<td>Enter the base 64 encoded PKCS12.</td>
</tr>
<tr>
<td></td>
<td>End with the word “quit” on a line by itself.</td>
</tr>
<tr>
<td></td>
<td>[ PKCS12 data omitted ]</td>
</tr>
<tr>
<td></td>
<td>quit</td>
</tr>
<tr>
<td></td>
<td>INFO: Import PKCS12 operation completed</td>
</tr>
<tr>
<td></td>
<td>successfully.</td>
</tr>
<tr>
<td></td>
<td>hostname(config)# webvpn</td>
</tr>
<tr>
<td></td>
<td>hostname(config)# java-trustpoint mytrustpoint</td>
</tr>
</tbody>
</table>

Disabling Content Rewrite

You might 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 an IPsec VPN connection.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>webvpn</td>
</tr>
<tr>
<td></td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>rewrite</td>
</tr>
<tr>
<td></td>
<td>Specifies applications and resources to access</td>
</tr>
<tr>
<td></td>
<td>outside a clientless SSLN VPN tunnel. You can use</td>
</tr>
<tr>
<td></td>
<td>this command multiple times.</td>
</tr>
<tr>
<td>Step 3</td>
<td>disable</td>
</tr>
<tr>
<td></td>
<td>Used in combination with the rewrite command.</td>
</tr>
<tr>
<td></td>
<td>The order number of rules is important because</td>
</tr>
<tr>
<td></td>
<td>the security appliance searches rewrite rules by order</td>
</tr>
<tr>
<td></td>
<td>number, starting with the lowest, and applies the</td>
</tr>
<tr>
<td></td>
<td>first rule that matches.</td>
</tr>
</tbody>
</table>

Using Proxy Bypass

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

You can use this command multiple times. The order in which you configure entries is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.
If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the ASA. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is everything in a URL after the .com or .org or other types of domain name. For example, in the URL www.example.com/hrbenefits, hrbenefits is the path. Similarly, for the URL www.example.com/hrinsurance, hrinsurance is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the * wildcard as follows: /hr*.

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>proxy-bypass</td>
<td>Configures proxy bypass.</td>
</tr>
</tbody>
</table>

### Clientless SSL VPN End User Setup

This section is for the system administrator who sets up clientless SSL VPN for end users. It describes how to customize the end-user interface.

This section summarizes configuration requirements and tasks for a remote system. It specifies information to communicate to users to get them started using clientless SSL VPN. It includes the following topics:

- Defining the End User Interface
- Customizing Clientless SSL VPN Pages, page 1-86
- Customizing Help, page 1-103
- Requiring Usernames and Passwords
- Communicating Security Tips
- Configuring Remote Systems to Use Clientless SSL VPN Features
- Translating the Language of User Messages

### Defining the End User Interface

The clientless SSL VPN end user interface consists of a series of HTML panels. A user logs on to clientless SSL VPN by entering the IP address of an ASA interface in the format https://address. The first panel that displays is the login screen (Figure 1-9).
Viewing the Clientless SSL VPN Home Page

After the user logs in, the portal page opens.

The home page displays all of the clientless SSL VPN features you have configured, and its appearance reflects the logo, text, and colors you have selected. This sample home page includes all available clientless SSL VPN features with the exception of identifying specific file shares. It lets users browse the network, enter URLs, access specific websites, and use Application Access (port forwarding and smart tunnels) to access TCP applications.

Viewing the Clientless SSL VPN Application Access Panel

To start port forwarding or smart tunnels, a user clicks the Go button in the Application Access box. The Application Access window opens (Figure 1-10).
Figure 1-10  Clientless SSL VPN Application Access Window

This window displays the TCP applications configured for this clientless SSL VPN connection. To use an application with this panel open, the user starts the application in the normal way.

A stateful failover does not retain sessions established using Application Access. Users must reconnect following a failover.

Viewing the Floating Toolbar

The floating toolbar shown in Figure 1-11 represents the current clientless SSL VPN session.

Figure 1-11  Clientless SSL VPN Floating Toolbar
Be aware of the following characteristics of the floating toolbar:

- The toolbar lets you enter URLs, browse file locations, and choose preconfigured web connections without interfering with the main browser window.
- If you configure your browser to block popups, the floating toolbar cannot display.
- If you close the toolbar, the ASA prompts you to confirm that you want to end the clientless SSL VPN session.

See Table 1-10 on page 1-106 for detailed information about using clientless SSL VPN.

**Customizing Clientless SSL VPN Pages**

You can change the appearance of the portal pages displayed to clientless SSL VPN users. This includes the Login page displayed to users when they connect to the security appliance, the Home page displayed to users after the security appliance authenticates them, the Application Access window displayed when users launch an application, and the Logout page displayed when users log out of clientless SSL VPN sessions.

After you customize the portal pages, you can save your customization and apply it to a specific connection profile, group policy, or user. The changes do not take effect until you reload the ASA, or you disable and then enable clientless SSL.

You can create and save many customization objects, enabling the security appliance to change the appearance of portal pages for individual users or groups of users.

This section includes the following topics:

- Information About Customization, page 1-86
- Exporting a Customization Template, page 1-87
- Editing the Customization Template, page 1-87
- Importing a Customization Object, page 1-93
- Applying Customizations to Connection Profiles, Group Policies and Users, page 1-93
- Login Screen Advanced Customization, page 1-95

**Information About Customization**

The ASA uses customization objects to define the appearance of user screens. A customization object is compiled from an XML file which contains XML tags for all the customizable screen items displayed to remote users. The ASA software contains a customization template that you can export to a remote PC. You can edit this template and import the template back into the ASA as a new customization object.

When you export a customization object, an XML file containing XML tags is created at the URL you specify. The XML file created by the customization object named Template contains empty XML tags, and provides the basis for creating new customization objects. This object cannot be changed or deleted from cache memory but can be exported, edited, and imported back into the ASA as a new customization object.
Customization Objects, Connection Profiles, and Group Policies

Initially, when a user first connects, the default customization object (named DfltCustomization) identified in the connection profile (tunnel group) determines how the logon screen appears. If the connection profile list is enabled, and the user selects a different group which has its own customization, the screen changes to reflect the customization object for that new group.

After the remote user is authenticated, the screen appearance is determined by whether a customization object that has been assigned to the group policy.

Exporting a Customization Template

When you export a customization object, an XML file is created at the URL you specify. The customization template (named Template) contains empty XML tags and provides the basis for creating new customization objects. This object cannot be changed or deleted from cache memory but can be exported, edited, and imported back into the ASA as a new customization object.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>export webvpn customization</td>
<td>Exports a customization object and allows you to make changes to the XML tags.</td>
</tr>
<tr>
<td>hostname$ export webvpn customization</td>
<td>Exports the default customization object (DfltCustomization) and creates the XML file named dflt_custom.</td>
</tr>
</tbody>
</table>

Example:

```
Example:  
<custom>  
  <localization>  
    <languages>en,ja,zh,ru,ua</languages>  
    <default-language>en</default-language>  
  </localization>  
  <auth-page>  
    <window>  
      <title-text l10n="yes"><![CDATA[SSL VPN Service]]></title-text>  
    </window>  
    <full-customization>  
      <mode>disable</mode>  
      <url></url>  
    </full-customization>  
  <language-selector>  
```

Editing the Customization Template

This section shows the contents of the customization template and has convenient figures to help you quickly choose the correct XML tag and make changes that affect the screens.

You can use a text editor or an XML editor to edit the XML file. The following example shows the XML tags of the customization template. Some redundant tags have been removed for easier viewing:

Example:

```
Example:  
<custom>  
  <localization>  
    <languages>en,ja,zh,ru,ua</languages>  
    <default-language>en</default-language>  
  </localization>  
  <auth-page>  
    <window>  
      <title-text l10n="yes"><![CDATA[SSL VPN Service]]></title-text>  
    </window>  
    <full-customization>  
      <mode>disable</mode>  
      <url></url>  
    </full-customization>  
  <language-selector>  
```
<mode>disable</mode>
<title l10n="yes">Language:</title>
<language>
<code>en</code>
<text>English</text>
</language>
<language>
<code>zh</code>
<text>简体中文</text>
</language>
<language>
<code>ja</code>
<text>日本語</text>
</language>
<language>
<code>ru</code>
<text>Русский</text>
</language>
<language>
<code>ua</code>
<text>Українська</text>
</language>
</language-selector>
<logon-form>
<title-text l10n="yes">Login</title-text>
<title-background-color>#666666</title-background-color>
<title-font-color>#ffffff</title-font-color>
<message-text l10n="yes">Please enter your username and password.</message-text>
<username-prompt-text l10n="yes">USERNAME:</username-prompt-text>
<password-prompt-text l10n="yes">PASSWORD:</password-prompt-text>
<internal-password-prompt-text l10n="yes">Internal Password:</internal-password-prompt-text>
<internal-password-first>no</internal-password-first>
<group-prompt-text l10n="yes">GROUP:</group-prompt-text>
<submit-button-text l10n="yes">Login</submit-button-text>
<title-font-color>#ffffff</title-font-color>
<title-background-color>#666666</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
<border-color>#858A91</border-color>
</logon-form>
<logout-form>
<title-text l10n="yes">Logout</title-text>
<message-text l10n="yes">Goodbye.<br>For your own security, please:<br>
Clear the browser's cache<br>Delete any downloaded files<br>Close the browser's window]</message-text>
<login-button-text l10n="yes">Logon</login-button-text>
<hide-login-button>no</hide-login-button>
<title-background-color>#666666</title-background-color>
<title-font-color>#ffffff</title-font-color>
<title-font-color>#ffffff</title-font-color>
<title-background-color>#666666</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
<border-color>#858A91</border-color>
</logout-form>
<title-panel>
Chapter 1 Configuring Clientless SSL VPN

Customizing Clientless SSL VPN Pages

<mode>enable</mode>
<text l10n="yes"> <![CDATA[SSL VPN Service]]> </text>
<logo-url l10n="yes"> /+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style>
<background-color> <![CDATA[#ffffff]]> </background-color>
<font-size> <![CDATA[larger]]> </font-size>
<font-color> <![CDATA[#800000]]> </font-color>
<font-weight> <![CDATA[bold]]> </font-weight>
</title-panel>

<info-panel>
<mode>disable</mode>
<image-url l10n="yes"> /+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes"></text>
</info-panel>

<copyright-panel>
<mode>disable</mode>
<text l10n="yes"></text>
</copyright-panel>
</auth-page>
</portal>
<title-panel>
<mode>enable</mode>
<text l10n="yes"> <![CDATA[SSL VPN Service]]> </text>
<logo-url l10n="yes"> /+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style>
<background-color> <![CDATA[#ffffff]]> </background-color>
<font-size> <![CDATA[larger]]> </font-size>
<font-color> <![CDATA[#800000]]> </font-color>
<font-weight> <![CDATA[bold]]> </font-weight>
</title-panel>

<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
<application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
<application>
<mode>enable</mode>
<id>web-access</id>
<tab-title l10n="yes"> <![CDATA[Web Applications]]> </tab-title>
<url-list-title l10n="yes"> <![CDATA[Web Bookmarks]]> </url-list-title>
<order>2</order>
</application>
<application>
<mode>enable</mode>
<id>file-access</id>
<tab-title l10n="yes"> <![CDATA[Browse Networks]]> </tab-title>
<url-list-title l10n="yes"> <![CDATA[File Folder Bookmarks]]> </url-list-title>
<order>3</order>
</application>
<application>
<mode>enable</mode>
<id>app-access</id>
<tab-title l10n="yes"> <![CDATA[Application Access]]> </tab-title>
<order>4</order>
</application>
<application>
<mode>enable</mode>
<id>net-access</id>

Figure 1-12 shows the Logon page and its customizing XML tags. All these tags are nested within the higher-level tag <auth-page>.

**Figure 1-12 Logon Page and Associated XML Tags**

Figure 1-13 shows the Language Selector drop-down list that is available on the Logon page, and the XML tags for customizing this feature. All these tags are nested within the higher-level <auth-page> tag.

**Figure 1-13 Language Selector on Logon Screen and Associated XML Tags**

Figure 1-14 shows the Information Panel that is available on the Logon page, and the XML tags for customizing this feature. This information can appear to the left or right of the login box. These tags are nested within the higher-level <auth-page> tag.
Figure 1-14  Information Panel on Logon Screen and Associated XML Tags

Clientless SSLVPN Service provided by the Cisco ASA5500 Series Adaptive Security Appliance.

Figure 1-15 shows the Portal page and the XML tags for customizing this feature. These tags are nested within the higher-level <auth-page> tag.

Figure 1-15  Portal Page and Associated XML Tags
Importing a Customization Object

After you edit and save the XML file, import it into flash memory of the ASA using the following commands:

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>imports an XML file into cache memory of the ASA. When you import the customization object, the ASA checks the XML code for validity. If the code is valid, the ASA stores the object in a hidden location in cache memory.</td>
</tr>
</tbody>
</table>

**Example:**

```plaintext
hostname# import webvpn customization
import tftp://209.165.201.22/customization/General.xml
Accessing tftp://209.165.201.22/customization/General.xml...!!!

Writing file disk0:/csco_config/97/custom1...

329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Imports the customization object *General.xml* from the URL 209.165.201.22/customization and names it *custom1*.

**Applying Customizations to Connection Profiles, Group Policies and Users**

After you create a customization, you can apply the customization to a connection profile (tunnel group), a group, or a user, with the customization command. The options displayed with this command are different depending on the mode you are in.

**Note**

After you customize the portal pages, the changes do not take effect until you reload the ASA, or you disable and then enable clientless SSL.

For more information about configuring connection profiles, group policies, and users, see Chapter 1, “Configuring Connection Profiles, Group Policies, and Users.”
### Customizing Clientless SSL VPN Pages

#### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
webvpn | Switches to webvpn configuration mode. |
| **Step 2** | 
- tunnel-group name
  OR
  group-policy name
  OR
  username name | Switches to tunnel-group webvpn configuration mode for name. |
  Switches to group-policy webvpn configuration for name. |
  Switches to username webvpn configuration for name. |
| **Step 3** | 
customization name | Applies a customization to a connection profile. name is the name of a customization to apply to the connection profile. |
  Enters tunnel-group webvpn configuration mode and enables the customization cisco for the connection profile cisco_telecommutes. |
  Applies a customization to a group or use. The following options are included: |
    - **none** disables the customization for the group or user, prevents the value from being inherited, and displays the default clientless SSL VPN pages. |
    - **value** name is the name of a customization |
  Enters group policy webvpn configuration mode, queries the security appliance for a list of customizations, and enables the customization cisco for the group policy cisco_sales. |
  Enters username webvpn configuration mode and enables the customization cisco for the user cisco_employee. |

**Example:**

hostname(config)# tunnel-group cisco_telecommuters
webvpn-attributes
hostname(config-group-webvpn)# customization cisco

OR

customization {none | value name}

**Example:**

hostname(config)# group-policy cisco_sales
attributes
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# customization value cisco

**Example:**

hostname(config)# username cisco_employee attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value cisco
Login Screen Advanced Customization

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

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

This section describes the modifications you need to make to your HTML code and the tasks required to configure the ASA to use your code.

Figure 1-16 shows the standard Cisco login screen that displays to clientless SSL VPN users. The Login form is displayed by a function called by the HTML code.

![Figure 1-16 Standard Cisco Login Page](image)

Figure 1-17 shows the Language Selector drop-down list. This feature is an option for clientless SSL VPN users and is also called by a function in the HTML code of the login screen.
Figure 1-17  Language Selector Drop-down List

Figure 1-18 shows a simple example of a custom login screen enabled by the Full Customization feature.

Figure 1-18  Example of Full Customization of Login Screens

The following HTML code is used as an example and is the code that displays:

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

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap ITC" size="6" color="#FF00FF">
```
The indented code injects the Login form and the Language Selector on the screen. The function `csco_ShowLoginForm('lform')` injects the logon form. `csco_ShowLanguageSelector('selector')` injects the Language Selector.

### Modifying Your HTML File

Follow these steps to modify your HTML file:

#### Detailed Steps

**Step 1** Name your file `logon.inc`. When you import the file, the ASA recognizes this filename as the logon screen.

**Step 2** Modify the paths of images used by the file to include `/+CSCOU+/`.

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

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

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

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">
<table>
```

Editing the Customization Object

The ASA has a default customization object, named Template, which contains all currently employed XML tags along with comments about how to use them. You can export the default template to a file, edit the file for your organization, and import the edited template as a new customization object. You cannot change or delete Template; you must choose a new name for your customization object.

⚠️ Warning  Editing a customization template with a Microsoft Windows editor, such as Notepad, will add a Byte order mark to the beginning of the file. ASDM cannot import a file with this character. If you plan to edit a customization template in Windows, use an editor that does not add that character, for example, Notepad++ or VIM.

Export the Default Customization Template

Use the export command to download the customization template from the ASA, as follows:

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

This example exports the customization template to default.xml.

Import the Edited Customization Template

Import your edited customization template using a new name. The following example imports an XML object called custom.xml, and names it General on the ASA.

```
hostname# import webvpn customization General tftp://webserver/custom.xml
hostname#
```
Configuring Browser Access to Client-Server Plug-ins

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

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

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

The following sections describe the integration of browser plug-ins for Clientless SSL VPN browser access:

- About Installing Browser Plug-ins
- Preparing the Security Appliance for a Plug-in
- Installing Plug-ins Redistributed By Cisco

About Installing Browser Plug-ins

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

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

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

Table 1-8 shows the changes to the main menu and address field of the portal page when you add the plug-ins described in the following sections.

<table>
<thead>
<tr>
<th>Plug-in</th>
<th>Main Menu Option Added to Portal Page</th>
<th>Address Field Option Added to Portal Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ica</td>
<td>Citrix Client</td>
<td>citrix://</td>
</tr>
<tr>
<td>rdp</td>
<td>Terminal Servers</td>
<td>rdp://</td>
</tr>
<tr>
<td>rdp2</td>
<td>Terminal Servers Vista</td>
<td>rdp2://</td>
</tr>
<tr>
<td>ssh, telnet</td>
<td>SSH</td>
<td>ssh://</td>
</tr>
<tr>
<td></td>
<td>Telnet</td>
<td>telnet://</td>
</tr>
<tr>
<td>vnc</td>
<td>VNC Client</td>
<td>vnc://</td>
</tr>
</tbody>
</table>

Note: A secondary ASA obtains the plug-ins from the primary ASA.
When the user in a clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.

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

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

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

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

- The plug-ins support single sign-on (SSO). They use the same credentials entered to open the clientless SSL VPN session. Because the plug-ins do not support macro substitution, you do not have the options to perform SSO on different fields such as the internal domain password or on an attribute on a RADIUS or LDAP server.
- To configure SSO support for a plug-in, you install the plug-in, add a bookmark entry to display a link to the server, and specify SSO support when adding the bookmark.
- The minimum access rights required for remote use belong to the guest privilege mode.

Requirements
- Per the GNU General Public License (GPL), Cisco redistributes plug-ins without having made any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.
- Clientless SSL VPN must be enabled on the ASA to provide remote access to the plug-ins.
- A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.
- Plug-ins require that ActiveX or Oracle Java Runtime Environment (JRE) 1.4.2 (or later) is enabled on the browser. There is no ActiveX version of the RDP plug-in for 64-bit browsers.

RDP Plug-in ActiveX Debug Quick Reference

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

Step 1 Right-click My Computer to access the System Properties, and choose the Advanced tab.
Step 2 On the Advanced tab, choose the environment variables button.
Step 3 In the new user variable dialog box, enter the RF_DEBUG variable.
Step 4 Verify the new Environment Variable in the user variables section.
Step 5  If you used the client computer with versions of WebVPN before version 8.3, you must remove the old Cisco Portforwarder Control. Go to the C:/WINDOWS/Downloaded Program Files directory, right-click portforwarder control, and choose Remove.

Step 6  Clear all of the Internet Explorer browser cache.

Step 7  Launch your WebVPN session and establish an RDP session with the RDP ActiveX Plug-in.

You can now observe events in the Windows Application Event viewer.

Preparing the Security Appliance for a Plug-in

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

Step 1  Make sure clientless SSL VPN (“webvpn”) is enabled on an ASA interface.

Step 2  Install an SSL certificate onto the ASA interface to which remote users use a fully-qualified domain name (FQDN) to connect.

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

Configuring the ASA to Use the New HTML File

Follow these steps to configure the ASA to use the new HTML file you just customized in the previous steps.
## Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Step 1</strong> import webvpn webcontent</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> import webvpn webcontent</td>
</tr>
<tr>
<td>hostname# import webvpn webcontent</td>
<td>hostname# import webvpn webcontent</td>
</tr>
<tr>
<td>!!!!* Web resource <code>/+CSCOU+/login.inc</code> was successfully initialized</td>
<td>!!!!* Web resource <code>/+CSCOU+/login.inc</code> was successfully initialized</td>
</tr>
<tr>
<td>hostname#</td>
<td>hostname#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Step 2</strong> export webvpn customization</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> export webvpn customization template</td>
</tr>
<tr>
<td>hostname2# export webvpn customization template tftp://209.165.200.225/sales_vpn_login</td>
<td>hostname2# export webvpn customization template tftp://209.165.200.225/sales_vpn_login</td>
</tr>
<tr>
<td>!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!</td>
<td>!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!</td>
</tr>
<tr>
<td>%INFO: Customization object 'Template' was exported to tftp://10.21.50.120/sales_vpn_login</td>
<td>%INFO: Customization object 'Template' was exported to tftp://10.21.50.120/sales_vpn_login</td>
</tr>
<tr>
<td>hostname#</td>
<td>hostname#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Step 3</strong> Change the full customization mode tag in the file to enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> &lt;full-customization&gt;</td>
</tr>
<tr>
<td>&lt;full-customization&gt;</td>
<td>&lt;full-customization&gt;</td>
</tr>
<tr>
<td>&lt;mode&gt;enable&lt;/mode&gt;</td>
<td>&lt;mode&gt;enable&lt;/mode&gt;</td>
</tr>
<tr>
<td>&lt;url&gt;/+CSCOU+/login.inc&lt;/url&gt;</td>
<td>&lt;url&gt;/+CSCOU+/login.inc&lt;/url&gt;</td>
</tr>
<tr>
<td>&lt;/full-customization&gt;</td>
<td>&lt;/full-customization&gt;</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Step 4</strong> Import the file as a new customization object</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> import webvpn customization</td>
</tr>
<tr>
<td>hostname# import webvpn customization sales_vpn_login tftp://10.21.50.120/sales_vpn_login</td>
<td>hostname# import webvpn customization sales_vpn_login tftp://10.21.50.120/sales_vpn_login</td>
</tr>
<tr>
<td>!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!</td>
<td>!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!</td>
</tr>
<tr>
<td>%INFO: customization object 'sales_vpn_login' was successfully imported</td>
<td>%INFO: customization object 'sales_vpn_login' was successfully imported</td>
</tr>
<tr>
<td>hostname#</td>
<td>hostname#</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Step 5</strong> Apply the customization object to a Connection Profile (tunnel group)</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>hostname(config)# tunnel-group Sales webvpn-attributes</td>
<td>hostname(config)# tunnel-group Sales webvpn-attributes</td>
</tr>
<tr>
<td>hostname(config-tunnel-webvpn)#customization sales_vpn_login</td>
<td>hostname(config-tunnel-webvpn)#customization sales_vpn_login</td>
</tr>
</tbody>
</table>
Customizing Help

The ASA displays help content on the application panels during VPN sessions. You can customize the help files provided by Cisco or create help files in other languages. You then import them to flash memory for display during subsequent sessions. You can also retrieve previously imported help content files, modify them, and reimport them to flash memory.

Each application panel displays its own help file content using a predetermined filename. The prospective location of each is in the `/+CSCOE+/help/language` URL within flash memory of the ASA. Table 1-9 shows the details about each of the help files you can maintain for VPN sessions.

Table 1-9  
**VPN Application Help Files**

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Panel</th>
<th>URL of Help File in Flash Memory of the Security Appliance</th>
<th>Help File Provided By Cisco in English?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Application Access</td>
<td><code>/+CSCOE+/help/language/app-access-hlp.inc</code></td>
<td>Yes</td>
</tr>
<tr>
<td>Standard</td>
<td>Browse Networks</td>
<td><code>/+CSCOE+/help/language/file-access-hlp.inc</code></td>
<td>Yes</td>
</tr>
<tr>
<td>Standard</td>
<td>AnyConnect Client</td>
<td><code>/+CSCOE+/help/language/net-access-hlp.inc</code></td>
<td>Yes</td>
</tr>
<tr>
<td>Standard</td>
<td>Web Access</td>
<td><code>/+CSCOE+/help/language/web-access-hlp.inc</code></td>
<td>Yes</td>
</tr>
<tr>
<td>Plug-in</td>
<td>MetaFrame Access</td>
<td><code>/+CSCOE+/help/language/ica-hlp.inc</code></td>
<td>No</td>
</tr>
<tr>
<td>Plug-in</td>
<td>Terminal Servers</td>
<td><code>/+CSCOE+/help/language/rdp-hlp.inc</code></td>
<td>Yes</td>
</tr>
<tr>
<td>Plug-in</td>
<td>Telnet/SSH Servers</td>
<td><code>/+CSCOE+/help/language/ssh,telnet-hlp.inc</code></td>
<td>Yes</td>
</tr>
<tr>
<td>Plug-in</td>
<td>VNC Connections</td>
<td><code>/+CSCOE+/help/language/vnc-hlp.inc</code></td>
<td>Yes</td>
</tr>
</tbody>
</table>

*language* is the abbreviation of the language rendered by the browser. This field is not used for file translation; it indicates the language used in the file. To specify a particular language code, copy the language abbreviation from the list of languages rendered by your browser. For example, a dialog window displays the languages and associated language codes when you use one of the following procedures:

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

The following sections describe how to customize the help contents:

- Customizing a Help File Provided By Cisco, page 1-103
- Creating Help Files for Languages Not Provided by Cisco, page 1-104
- Importing a Help File to Flash Memory, page 1-105
- Exporting a Previously Imported Help File from Flash Memory, page 1-105

Customizing a Help File Provided By Cisco

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

Step 1 Use your browser to establish a clientless SSL VPN session with the ASA.

Step 2 Display the help file by appending the string in “URL of Help File in Flash Memory of the Security Appliance” in Table 1-9, to the address of the ASA, then press Enter.

Note Enter en in place of language to get the help file in English.

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

Step 3 Choose File > Save (Page) As.

Note Do not change the contents of the File name box.

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

Step 5 Use your preferred HTML editor to modify the file.

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

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

Step 7 Make sure the filename matches the one in Table 1-9, and that it does not have an extra filename extension.

See “Importing a Help File to Flash Memory” to import the modified file.

Creating Help Files for Languages Not Provided by Cisco

Use HTML to create help files in other languages.

We recommend creating a separate folder for each language you want to support.

Save the file as HTML only. Use the filename following the last slash in “URL of Help File in Flash Memory of the Security Appliance” in Table 1-9.

See the next section to import the files for display during VPN sessions.

Restrictions

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

To import a help content file to flash memory for display in clientless SSL VPN sessions, follow these steps:

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| import webvpn webcontent destination_url source_url | | • destination_url is the string in the URL of Help File in Flash Memory of the Security Appliance column of Table 1-9VPN Application Help Files.  
• source_url is the URL of the file to import. Valid prefixes are ftp://, http://, and tftp://. |

**Example:**
```
hostname# import webvpn webcontent  
/+CSCOE+/help/en/app-access-hlp.inc  
tftp://209.165.200.225/app-access-hlp.inc
```

Copies the help file `app-access-hlp.inc` to flash memory from the TFTP server at 209.165.200.225. The URL includes the abbreviation `en` for the English language.

## Exporting a Previously Imported Help File from Flash Memory

To retrieve a previously imported help content file for subsequent edits, follow these steps:

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| export webvpn webcontent source_url destination_url | | • source_url is the string in “URL of Help File in Flash Memory of the Security Appliance” in Table 1-9.  
• destination_url is the target URL. Valid prefixes are ftp:// and tftp://. The maximum number of characters is 255. |

**Example:**
```
hostname# export webvpn webcontent  
/+CSCOE+/help/en/file-access-hlp.inc  
tftp://209.165.200.225/file-access-hlp.inc
```

Copies the English language help file `file-access-hlp.inc` displayed on the Browser Networks panel to TFTP Server 209.165.200.225.
Requiring Usernames and Passwords

Depending on your network, during a remote session users might have to log in to any or all of the following: the computer itself, an Internet service provider, clientless SSL VPN, mail or file servers, or corporate applications. Users might have to authenticate in many different contexts, requiring different information, such as a unique username, password, or PIN.

Table 1-10 lists the type of usernames and passwords that clientless SSL VPN users might need to know.

<table>
<thead>
<tr>
<th>Login Username/Password Type</th>
<th>Purpose</th>
<th>Entered When</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Access the computer</td>
<td>Starting the computer</td>
</tr>
<tr>
<td>Internet Service Provider</td>
<td>Access the Internet</td>
<td>Connecting to an Internet service provider</td>
</tr>
<tr>
<td>Clientless SSL VPN</td>
<td>Access remote network</td>
<td>Starting clientless SSL VPN</td>
</tr>
<tr>
<td>File Server</td>
<td>Access remote file server</td>
<td>Using the clientless SSL VPN file browsing feature to access a remote file server</td>
</tr>
<tr>
<td>Corporate Application Login</td>
<td>Access firewall-protected internal server</td>
<td>Using the clientless SSL VPN web browsing feature to access an internal protected website</td>
</tr>
<tr>
<td>Mail Server</td>
<td>Access remote mail server via clientless SSL VPN</td>
<td>Sending or receiving e-mail messages</td>
</tr>
</tbody>
</table>

Communicating Security Tips

Advise users to always click the logout icon on the toolbar to close the clientless SSL VPN session. (Closing the browser window does not close the session.)

Clientless SSL VPN ensures the security of data transmission between the remote PC or workstation and the ASA on the corporate network. Advise users that using clientless SSL VPN does not ensure that communication with every site is secure. If a user then accesses a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate ASA to the destination web server is not private because it is not encrypted.

"Observing Clientless SSL VPN Security Precautions" on page 5 addresses an additional tip to communicate with users, depending on the steps you follow within that section.

Configuring Remote Systems to Use Clientless SSL VPN Features

This section describes how to set up remote systems to use clientless SSL VPN and includes the following topics:

- Starting Clientless SSL VPN, page 1-107
- Using the Clientless SSL VPN Floating Toolbar, page 1-107
You may configure user accounts differently and different clientless SSL VPN features can be available to each user.

Starting Clientless SSL VPN

You can connect to the internet using any supported connection including:

- home DSL, cable, or dial-ups
- public kiosks
- hotel hook-ups
- airport wireless nodes
- internet cafes

See the Cisco ASA 5500 Series VPN Compatibility Reference for the list of web browsers supported by clientless SSL VPN.

Prerequisites

- Cookies must be enabled on the browser in order to access applications via port forwarding.
- You must have a URL for clientless SSL VPN. The URL must be an https address in the following form: https://address, where address is the IP address or DNS hostname of an interface of the ASA (or load balancing cluster) on which SSL VPN is enabled. For example, https://cisco.example.com.
- You must have a clientless SSL VPN username and password.

Restrictions

- Clientless SSL VPN supports local printing, but it does not support printing through the VPN to a printer on the corporate network.

Using the Clientless SSL VPN Floating Toolbar

A floating toolbar is available to simplify the use of clientless SSL VPN. The toolbar lets you enter URLs, browse file locations, and choose preconfigured web connections without interfering with the main browser window.

The floating toolbar represents the current clientless SSL VPN session. If you click the Close button, the ASA prompts you to confirm that you want to close the clientless SSL VPN session.
Configuring Remote Systems to Use Clientless SSL VPN Features

Chapter 1 Configuring Clientless SSL VPN

Tip
To paste text into a text field, use Ctrl-V. (Right-clicking is disabled on the toolbar displayed during the clientless SSL VPN session.)

Restrictions
If you configure your browser to block popups, the floating toolbar cannot display.

Browsing the Web

Using clientless SSL VPN does not ensure that communication with every site is secure. See Communicating Security Tips.

The look and feel of web browsing with clientless SSL VPN might be different from what users are accustomed to. For example:

- The title bar for clientless SSL VPN appears above each web page.
- You access websites by:
  - Entering the URL in the Enter Web Address field on the clientless SSL VPN Home page
  - Clicking on a preconfigured website link on the clientless SSL VPN Home page
  - Clicking a link on a webpage accessed via one of the previous two methods

Also, depending on how you configured a particular account, it might be that:

- Some websites are blocked
- Only the websites that appear as links on the clientless SSL VPN Home page are available

Prerequisites
- You need the username and password for protected websites.

Restrictions
Also, depending on how you configured a particular account, it might be that:

- Some websites are blocked
- Only the websites that appear as links on the clientless SSL VPN Home page are available

Browsing the Network (File Management)

Users might not be familiar with how to locate their files through your organization network.

Note
Do not interrupt the Copy File to Server command or navigate to a different screen while the copying is in progress. Interrupting the operation can cause an incomplete file to be saved on the server.

Prerequisites
- You must configure file permissions for shared remote access.
- You must have the server names and passwords for protected file servers.
- You must have the domain, workgroup, and server names where folders and files reside.
Restrictions
Only shared folders and files are accessible via clientless SSL VPN.

Using the Remote File Explorer

The Remote File Explorer provides the user with a way to browse the corporate network from their web browser. When the user clicks the Remote File System icon on the Cisco SSL VPN portal page, an applet is launched on the user’s system displaying the remote file system in a tree and folder view.

The browser enables the user to:
- Browse the remote file system
- Rename files
- Move or copy files within the remote file system and between the remote and local file systems.
- Perform bulk uploads and downloads of files

Note
This functionality requires the Oracle Java Runtime Environment (JRE) 1.4 or later is installed on the user’s machine and Java enabled in the web browser. Launching remote files requires JRE 1.6 or later.

Renaming a File or Folder

To rename a file or folder:

Step 1  Click the file or folder to be renamed.
Step 2  Select Edit > Rename.
Step 3  When prompted, enter the new name in the dialog.
Step 4  Click OK to rename the file or folder. Alternative, click Cancel to leave the name unchanged.
Moving or Copying Files or Folders on the Remote Server

To move or copy a file or folder on the remote server:

Step 1  Navigate to the source folder containing the file or folder to be moved or copied.
Step 2  Click the file or folder.
Step 3  To copy the file select Edit > Copy. Alternatively, to move the file select Edit > Cut.
Step 4  Navigate to the destination folder.
Step 5  Select Edit > Paste.

Copying Files from the Local System Drive to the Remote Folder

You can copy files between the local file system and the remote file system by dragging and dropping them between the right pane of the Remote File Browser and your local file manager application.

Uploading and Downloading Files

You can download a file by clicking it in the browser, selecting Operations > Download, and providing a location and name to save the file in the Save dialog.

You can upload a file by clicking the destination folder, selecting Operations > Upload, and providing the location and name of the file in the Open dialog.

This functionality has the following restrictions:

- The user cannot view sub-folders for which they are not permitted access.
- Files that the user is not permitted to access cannot be moved or copied, even though they are displayed in the browser.
- The maximum depth of nested folders is 32.
- The tree view does not support drag and drop copying.
- When moving files between multiple instances of the Remote File Explorer, all instances must be exploring the same server (root share).
- The Remote File Explorer can display a maximum of 1500 files and folders in a single folder. If a folder exceeds this limit the folder cannot be displayed.

Using Port Forwarding

Note Users should always close the Application Access window when they finish using applications by clicking the Close icon. Failure to quit the window properly can cause Application Access or the applications themselves to be disabled. See Recovering from hosts File Errors When Using Application Access for details.

Prerequisites

- On Mac OS X, only the Safari browser supports this feature.
- You must have client applications installed.
• You must have Cookies enabled on the browser.
• You must have administrator access on the PC if you use DNS names to specify servers, because modifying the hosts file requires it.
• You must have Oracle Java Runtime Environment (JRE) version 1.4.x and 1.5.x installed.
  If JRE is not installed, a pop-up window displays, directing users to a site where it is available. On rare occasions, the port forwarding applet fails with Java exception errors. If this happens, do the following:
  a. Clear the browser cache and close the browser.
  b. Verify that no Java icons are in the computer task bar.
  c. Close all instances of Java.
  d. Establish a clientless SSL VPN session and launch the port forwarding Java applet.
• You must have JavaScript enabled on the browser. By default, it is enabled.
• If necessary, you must configure client applications.

Note: The Microsoft Outlook client does not require this configuration step. All non-Windows client applications require configuration. To determine if configuration is necessary for a Windows application, check the value of the Remote Server field. If the Remote Server field contains the server hostname, you do not need to configure the client application. If the Remote Server field contains an IP address, you must configure the client application.

Restrictions
Because this feature requires installing Oracle Java Runtime Environment (JRE) and configuring the local clients, and because doing so requires administrator permissions on the local system or full control of C:\windows\System32\drivers\etc, it is unlikely that users will be able to use applications when they connect from public remote systems.

Detailed Steps
To configure the client application, use the server’s locally mapped IP address and port number. To find this information:

1. Start a clientless SSL VPN session and click the Application Access link on the Home page. The Application Access window appears.
2. In the Name column, find the name of the server you want to use, then identify its corresponding client IP address and port number (in the Local column).
3. Use this IP address and port number to configure the client application. Configuration steps vary for each client application.

Note: Clicking a URL (such as one in an e-mail message) in an application running over a clientless SSL VPN session does not open the site over that session. To open a site over the session, paste the URL into the Enter Clientless SSL VPN (URL) Address field.

Using E-mail Via Port Forwarding
To use e-mail, start Application Access from the clientless SSL VPN home page. The mail client is then available for use.
Prerequisites
You must fulfill requirements for application access and other mail clients.

Restrictions
We have tested Microsoft Outlook Express versions 5.5 and 6.0.
Clientless SSL VPN should support other SMTPS, POP3S, or IMAP4S e-mail programs via port forwarding, such as Lotus Notes and Eudora, but we have not verified them.

Using E-mail Via Web Access

The following e-mail applications are supported:
  OWA requires Internet Explorer 7 or later, or Firefox 3.01 or later.
  For best results, use OWA on Internet Explorer 8.x or later, or Firefox 8.x.
- Lotus iNotes

Prerequisites
You must have the web-based e-mail product installed.

Restrictions
Other web-based e-mail applications should also work, but we have not verified them.

Using E-mail Via E-mail Proxy

The following legacy e-mail applications are supported:
- Microsoft Outlook 2000 and 2002
- Microsoft Outlook Express 5.5 and 6.0

See the instructions and examples for your mail application in Using E-Mail over Clientless SSL VPN.

Prerequisites
- You must have the SSL-enabled mail application installed.
- Do not set the ASA SSL version to TLSv1 Only. Outlook and Outlook Express do not support TLS.
- You must have your mail application properly configured.

Restrictions
- Other SSL-enabled clients should also work, but we have not verified them.
Using Smart Tunnel

Administration privileges are not required to use Smart Tunnel.

Note
Java is not automatically downloaded for you as in port forwarder.

Prerequisites
• Smart tunnel requires either ActiveX or JRE (1.4x and 1.5x) on Windows and Java Web Start on Mac OS X.
• You must ensure cookies enabled on the browser.
• You must ensure JavaScript is enabled on the browser.

Restrictions
• Mac OS X does not support a front-side proxy.
• Supports only the operating systems and browsers specified in “Configuring Smart Tunnel Log OffConfiguring Smart Tunnel Access” section on page 1-51.
• Only TCP socket-based applications are supported.

Translating the Language of User Messages

The ASA provides language translation for the entire clientless SSL VPN session. This includes login, logout banners, and portal pages displayed after authentication such as plugins and AnyConnect.

This section describes how to configure the ASA to translate these user messages and includes the following sections:
• Understanding Language Translation, page 1-113
• Creating Translation Tables, page 1-114
• Referencing the Language in a Customization Object, page 1-116
• Changing a Group Policy or User Attributes to Use the Customization Object, page 1-118

Understanding Language Translation

Functional areas and their messages that are visible to remote users are organized into translation domains. Table 1-11 shows the translation domains and the functional areas translated.

<table>
<thead>
<tr>
<th>Translation Domain</th>
<th>Functional Areas Translated</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect</td>
<td>Messages displayed on the user interface of the Cisco AnyConnect VPN Client.</td>
</tr>
<tr>
<td>CSD</td>
<td>Messages for Cisco Secure Desktop.</td>
</tr>
<tr>
<td>customization</td>
<td>Messages on the logon and logout pages, portal page, and all the messages customizable by the user.</td>
</tr>
<tr>
<td>banners</td>
<td>Banners displayed to remote users and messages when VPN access is denied.</td>
</tr>
</tbody>
</table>
Translating the Language of User Messages

Table 1-11 Translation Domains and Functional Areas Affected (continued)

<table>
<thead>
<tr>
<th>Translation Domain</th>
<th>Functional Areas Translated</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortForwarder</td>
<td>Messages displayed to Port Forwarding users.</td>
</tr>
<tr>
<td>url-list</td>
<td>Text that user specifies for URL bookmarks on the portal page.</td>
</tr>
<tr>
<td>webvpn</td>
<td>All the layer 7, AAA and portal messages that are not customizable.</td>
</tr>
<tr>
<td>plugin-ica</td>
<td>Messages for the Citrix plug-in.</td>
</tr>
<tr>
<td>plugin-telnet,ssh</td>
<td>Messages for the Telnet and SSH plug-in.</td>
</tr>
<tr>
<td>plugin-vnc</td>
<td>Messages for the VNC plug-in.</td>
</tr>
</tbody>
</table>

The ASA includes a translation table template for each domain that is part of standard functionality. The templates for plug-ins are included with the plug-ins and define their own translation domains.

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

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

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

After creating translation tables, they are available to customization objects that you create and apply to group policies or user attributes. With the exception of the AnyConnect translation domain, a translation table has no affect, and messages are not translated on user screens until you create a customization object, identify a translation table to use in that object, and specify that customization for the group policy or user. Changes to the translation table for the AnyConnect domain are immediately visible to AnyConnect client users.

Creating Translation Tables

You can create translation tables in both single context mode and multi-context mode:

Note
### Detailed Steps

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>export webvpn translation-table</code></td>
<td>Exports a translation table template to a computer. Shows available translation table templates and tables. Exports the translation table template for the customization domain, which affects messages displayed for users in clientless SSL VPN sessions. The filename of the XML file created is <code>portal</code> (user-specified) and contains empty message fields.</td>
</tr>
</tbody>
</table>

**Example:**
```
hostname$ show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin
Translation Tables:
```

**Example:**
```
hostname$ export webvpn translation-table customization template tftp://209.165.200.225/portal
```
### Translating the Language of User Messages

#### Step 2
Edit the translation table XML file

**Example:**
```xml
# Copyright (C) 2006 by Cisco Systems, Inc.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: ASA"
"Report-Msgid-Bugs-To: vkamyshe@cisco.com"
"POT-Creation-Date: 2007-03-12 18:57 GMT"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>"
"Language-Team: LANGUAGE <LL@li.org>"
"MIME-Version: 1.0"
"Content-Type: text/plain; charset=UTF-8"
"Content-Transfer-Encoding: 8bit"

#: DfltCustomization:24 DfltCustomization:64
msgid "Clientless SSL VPN Service"
msgstr ""
```
Shows a portion of the template that was exported as portal. The end of this output includes a message ID field (msgid) and a message string field (msgstr) for the message SSL VPN, which is displayed on the portal page when a user establishes a clientless SSL VPN session. The complete template contains many pairs of message fields.

#### Step 3
import webvpn translation-table

**Example:**
```sh
hostname# import webvpn translation-table
customization language es-us
tftp://209.165.200.225/portal
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
```
Imports the translation table.
Import the XML file. *es-us* is the abbreviation for Spanish spoken in the United States.

If you import a translation table for the AnyConnect domain, your changes are effective immediately. If you import a translation table for any other domain, you must create a customization object, identify the translation table to use in that object, and specify that customization object for the group policy or user.

#### Referencing the Language in a Customization Object

This section describes how to export the customization template, edit it, and import it as a customization object so that you can refer to it.

---

Cisco ASA Series CLI Configuration Guide
Prerequisites

For the customization object to call these translation tables correctly, the tables must have been previously imported using the same names. These names must be compatible with language options of the browser.

Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>export webvpn customization template</td>
<td>Exports a customization template to a URL where you can edit it.</td>
</tr>
</tbody>
</table>

Example:

```plaintext
hostname# export webvpn customization template tftp://209.165.200.225/sales
```

Exports the template and creates the copy `sales` at the URL specified.

Step 2 | Edit the customization template and reference the previously-imported translation table | Two areas of XML code in the customization template pertain to translation tables. |

Example:

```xml
<localization>
    <languages>en,ja,zh,ru,ua</languages>
    <default-language>en</default-language>
</localization>
```

Specifies the translation table to use.

- The `<languages>` tag in the XML code is followed by the names of the translation tables. In this example, they are en, ja, zh, ru, and ua.
- The `<default-language>` tag specifies the language that the remote user first encounters when connecting to the ASA. In the example code above, the language is English.

Affects the display of the Language Selector and includes the `<language-selector>` tag and the associated `<language>` tags that enable and customize the Language Selector:

- The `<language-selector>` group of tags includes the `<mode>` tag that enables and disables the displaying of the Language Selector and the `<title>` tag that specifies the title of the drop-down box listing the languages.
- The `<language>` group of tags includes the `<code>` and `<text>` tags that map the language name displayed in the Language Selector drop-down box to a specific translation table.

Example:

```xml
<auth-page>
    ...
    
    <language-selector>
        <mode>enable</mode>
        <title l10n="yes">Language:</title>
        <language>
            <code>en</code>
            <text>English</text>
        </language>
        <language>
            <code>es-us</code>
            <text>Spanish</text>
        </language>
    </language-selector>
</auth-page>
```

Step 3 | Save the file after making your changes. | 

---

Cisco ASA Series CLI Configuration Guide
Changing a Group Policy or User Attributes to Use the Customization Object

This section describes how to activate your changes for specific groups or users.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: webvpn</td>
<td>Switches to webvpn configuration mode.</td>
</tr>
<tr>
<td>Step 2: group-policy</td>
<td>Switches to group-policy webvpn configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3: customization</td>
<td>Enables the customization object.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>hostname(config)# group-policy sales attributes</td>
</tr>
<tr>
<td></td>
<td>hostname(config-group-policy)# webvpn</td>
</tr>
<tr>
<td></td>
<td>hostname(config-group-webvpn)# customization value sales</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Enter a name for this bookmark, which will be displayed on the portal.</td>
</tr>
</tbody>
</table>
Capturing Data

The CLI **capture** command lets you log information about websites that do not display properly over a clientless SSL VPN session. This data can help your Cisco customer support engineer troubleshoot problems. The following sections describe how to capture and view clientless SSL VPN session data:

- Creating a Capture File, page 1-119
- Using a Browser to Display Capture Data, page 1-119

Prerequisites

- Enabling clientless SSL VPN capture affects the performance of the security appliance. Be sure to disable the capture after you generate the capture files needed for troubleshooting.

Creating a Capture File

Perform the following steps to capture data about a clientless SSL VPN session to a file.

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>capture capture_name type webvpn user webvpn_username</td>
</tr>
<tr>
<td>Example:</td>
<td>starts the capture utility for clientless SSL VPN.</td>
</tr>
<tr>
<td>hostname$ capture hr type webvpn user user2</td>
<td><em>capture_name</em> is a name you assign to the capture, which is also prepended to the name of the capture files.</td>
</tr>
<tr>
<td>WebVPN capture started.</td>
<td><em>webvpn_user</em> is the username to match for capture.</td>
</tr>
<tr>
<td>capture name hr</td>
<td>Creates a capture named hr, which captures traffic for user2 to a file.</td>
</tr>
<tr>
<td>user name user2</td>
<td></td>
</tr>
<tr>
<td>hostname$ no capture hr</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>(Optional)</td>
</tr>
<tr>
<td>no capture capture_name</td>
<td>Stops the capture utility from capturing packets after a user has logged in and began a clientless SSL VPN session. The capture utility creates a capture_name.zip file, which is encrypted with the password koleso.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Send the .zip file to Cisco Systems or attach it to a Cisco TAC service request.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Unzip the contents of the file using the koleso password.</td>
</tr>
</tbody>
</table>

Using a Browser to Display Capture Data

Perform the following steps to capture data about a clientless SSL VPN session and view it in a browser.
## Capturing Data

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>capture capture_name type webvpn user webvpn_username</td>
</tr>
<tr>
<td></td>
<td>Starts the capture utility for clientless SSL VPN.</td>
</tr>
<tr>
<td></td>
<td>• <code>capture_name</code> is a name you assign to the capture, which is also prepended to the name of the capture files.</td>
</tr>
<tr>
<td></td>
<td>• <code>webvpn_user</code> is the username to match for capture.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>(Optional) no capture capture_name</td>
</tr>
<tr>
<td></td>
<td>Stops the capture utility from capturing packets after a user has logged in and began a clientless SSL VPN session.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Open a browser and enter the following: &lt;br&gt;https://asdm_enabled_interface_of_the_security_appliance:port/admin/capture/capture_name/pcap</td>
</tr>
<tr>
<td></td>
<td>Example: &lt;br&gt;<a href="https://192.0.2.1:60000/admin/capture/hr/pcap">https://192.0.2.1:60000/admin/capture/hr/pcap</a></td>
</tr>
<tr>
<td></td>
<td>Displays the capture named hr in a sniffer format.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Repeat Step 2.</td>
</tr>
</tbody>
</table>