



Basic Clientless SSL VPN Configuration

- [Clientless SSL VPN Security Precautions, page 15-1](#)
- [Verifying Clientless SSL VPN Server Certificates, page 15-2](#)
- [Configuring Browser Access to Plug-ins, page 15-3](#)
- [Configuring Port Forwarding, page 15-8](#)
- [Configuring File Access, page 15-16](#)
- [Ensuring Clock Accuracy for SharePoint Access, page 15-18](#)
- [Virtual Desktop Infrastructure \(VDI\), page 15-19](#)
- [Using SSL to Access Internal Servers, page 15-21](#)
- [Configuring Browser Access to Client-Server Plug-ins, page 15-25](#)

Revised: March 12, 2014

Clientless SSL VPN Security Precautions

By default, the ASA allows all portal traffic to all Web resources (for example HTTPS, CIFS, RDP, and plug-ins). Clientless SSL VPN rewrites each URL to one that is meaningful only to the ASA. The user cannot use this URL to confirm that they are connected to the website they requested. To avoid placing users at risk from phishing websites, 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. We recommend switching off URL Entry on these policies to prevent user confusion over what is accessible.

Figure 15-1 Example URL Entered by User

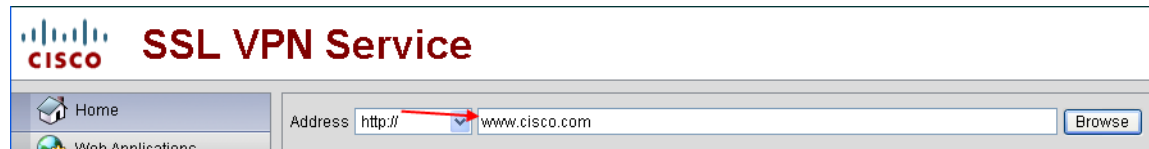
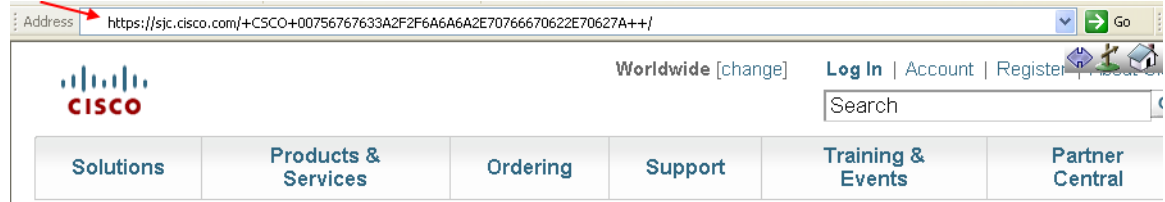


Figure 15-2 Same URL Rewritten by Security Appliance and Displayed in Browser Window



Switching Off URL Entry on the Portal Page

The portal page opens when the user establishes a browser-based connection.

Prerequisites

Configure a group policy for all users who require Clientless SSL VPN access, and enable Clientless SSL VPN only for that group policy.

DETAILED STEPS

	Command	Purpose
Step 1	<code>webvpn</code>	Switches to group policy clientless ssl vpn configuration mode.
Step 2	<code>url-entry</code>	Controls the ability of the user to enter any HTTP/HTTPS URL.
Step 3	(Optional) <code>url-entry disable</code>	Switches off URL Entry.

Verifying Clientless SSL VPN Server Certificates

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 introduced support for SSL server certificate verification against a list of trusted certificate authority (CA) certificates for Clientless SSL VPN.

When connecting to a remote server with a Web browser using the HTTPS protocol, the server provides a digital certificate signed by a certificate authority (CA) to identify itself. Web browsers include 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).

The ASA provides trusted pool certificate management facilities in the form of a 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. It is inactive until activated by the administrator by issuing the `crypto ca import default` command.



Note

ASA trustpools are similar but not identical to Cisco IOS trustpools.

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 15-4](#)
- [Installing Plug-ins Redistributed by Cisco, page 15-5](#)
- [Providing Access to a Citrix XenApp Server, page 15-6](#)

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 list 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 list next to the Address field of the portal page.

[Table 15-1](#) 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 15-1 *Effects of Plug-ins on the Clientless SSL VPN Portal Page*

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

* 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 list 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, page 19-12](#) for implementation details.

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

Ensure that Clientless SSL VPN 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

	Command	Purpose
Step 1	<code>show running-config</code>	Shows whether Clientless SSL VPN is enabled on the ASA.
Step 2	Install an SSL certificate onto the ASA interface	Provides a fully-qualified domain name (FQDN) for remote user connection.

Go to the section that identifies the type of plug-in to provide for Clientless SSL VPN access.

- [Installing Plug-ins Redistributed by Cisco](#), page 15-5
- [Providing Access to a Citrix XenApp Server](#), page 15-6

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

Ensure Clientless SSL VPN is enabled on an interface on the ASA. To do so, enter the **show running-config** command.

Table 15-2 Plug-ins Redistributed by Cisco

Protocol	Description	Source of Redistributed Plug-in *
RDP	<p>Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2.</p> <p>Supports Remote Desktop ActiveX Control.</p> <p>We recommend using this plug-in that supports both RDP and RDP2. Only versions up to 5.1 of the RDP and RDP2 protocols are supported. Version 5.2 and later are not supported.</p>	http://properjavardp.sourceforge.net/
RDP2	<p>Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2.</p> <p>Supports Remote Desktop ActiveX Control.</p> <p>Note This legacy plug-in supports only RDP2. We do not recommend using this plug-in; instead, use the RDP plug-in above.</p>	http://properjavardp.sourceforge.net/
SSH	<p>The Secure Shell-Telnet plug-in lets the remote user establish a Secure Shell (v1 or v2) or Telnet connection to a remote computer.</p> <p>Note Because keyboard-interactive authentication is not supported by JavaSSH, it cannot be supported with SSH plugin (used to implement different authentication mechanisms).</p>	http://javassh.org/
VNC	<p>The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing (also known as VNC server or service) turned on. This version changes the default color of the text and contains updated French and Japanese help files.</p>	http://www.tightvnc.com/

* 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

**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.

	Command	Purpose
Step 1	<pre>import webvpn plug-in protocol [rdp rdp2 [ssh telnet] vnc] URL Example: hostname# import webvpn plug-in protocol ssh,telnet tftp://local_tftp_server/plugins/ssh-plugin.jar Accessing tftp://local_tftp_server/plugins/ssh-plugin.jar...!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Writing file disk0:/cisco_config/97/plugin/ssh... !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!! 238510 bytes copied in 3.650 secs (79503 bytes/sec)</pre>	<p>Installs the plug-in onto the flash device of the ASA. <i>protocol</i> is one of the following values: ssh, telnet provides plug-in access to <i>both</i> Secure Shell and Telnet services.</p> <p>Note Do not enter this command once for SSH and once for Telnet. When typing the <code>ssh,telnet</code> string, do not insert a space.</p> <p><i>URL</i> is the remote path to the plug-in .jar file. Enter the hostname or address of the TFTP or FTP server and the path to the plug-in.</p>
Step 2	<p>(Optional)</p> <pre>revert webvpn plug-in protocol protocol Example: hostname# revert webvpn plug-in protocol rdp</pre>	<p>Switches off and removes Clientless SSL VPN support for a plug-in, as well as removing it from the flash drive of the ASA.</p>

Step 1 .

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, page 15-4](#) before using this section.

Creating and Installing the Citrix Plug-in

DETAILED STEPS

-
- Step 1** Download the [ica-plugin.zip](#) file from the Cisco Software Download website. This file contains files that Cisco customized for use with the Citrix plug-in.
- Step 2** Download the [Citrix Java client](#) from the Citrix site. In the download area of the Citrix website, select **Citrix Receiver**, and **Receiver for Other Platforms**, and click **Find**. Click the **Receiver for Java** hyperlink and download the archive..
- Step 3** Extract the following files from the archive, and then add them to the ica-plugin.zip file:
- JICA-configN.jar
 - JICAEngN.jar
- 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 hostname or IP address and path to the ica-plugin.zip file.
-  **Note** Adding a bookmark is required to provide SSO support for Citrix sessions. We 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.
-

## Viewing the Plug-ins Installed on the Security Appliance

### DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                                                                        | Purpose                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Step 1 | <pre>show import webvpn plug</pre> <p><b>Example:</b></p> <pre>hostname# show import webvpn plug ssh rdp vnc ica</pre>                                                                                                                                                                                         | Lists the Java-based client applications available to users of Clientless SSL VPN. |
| Step 2 | <pre>show import webvpn plug detail</pre> <p><b>Example:</b></p> <pre>hostname show import webvpn plug post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tues, 29 Apr 2008 19:57:03 GMT rdp fHeyReIOUwDCgAL9HdTs PnjdBoc= Tues, 15 Sep 2009 23:23:56 GMT rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT</pre> | Includes hash and date of the plug-in.                                             |

## Configuring Port Forwarding

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

- [Information About Port Forwarding, page 15-8](#)
- [Configuring DNS for Port Forwarding](#)
- [Making Applications 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
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP (FTP over SSH)
- SSH

- Telnet
- Windows Terminal Service
- XDDTS

Other TCP-based applications may also work, but we have not tested them. Protocols 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.
- Unlike port forwarding and smart tunnel access, a plug-in does not require the client application to be installed on the remote computer.

When configuring port forwarding on the 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

- The remote host must be running a 32-bit version of one of the following:
  - Microsoft Windows Vista, Windows XP SP2 or SP3; or Windows 2000 SP4.
  - Apple Mac OS X 10.4 or 10.5 with Safari 2.0.4(419.3).
  - Fedora Core 4
- The remote host must also be running Oracle Java Runtime Environment (JRE) 5 or later.
- Browser-based users of Safari on Mac OS X 10.5.3 must identify a client certificate for use with the URL of the 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 switch off Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer's vulnerability to attack.
- Ensure Oracle Java Runtime Environment (JRE) 1.5.x or later is installed on the remote computers to support port forwarding (application access) and digital certificates. If JRE 1.4.x is running and the user authenticates with a digital certificate, the application fails to start because JRE cannot access the Web browser certificate store.

## 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 protocols that use UDP.
- 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.
- Port forwarding does not support connections to personal digital assistants.
- Because port forwarding requires downloading the Java applet and configuring the local client, and because doing so requires administrator permissions on the local system, it is unlikely that users will be able to use applications when they connect from public remote systems.

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 hostname, 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:

|        | Command                                                                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>dns server-group</code>                                                                                                                                                                                                                                                                                                                      | Enters the dns server-group mode.<br><br>Configures a DNS server group named example.com.                                                                                                                                                                                                                                                                                                         |
| Step 2 | <code>domain-name</code><br><br><b>Example:</b><br>hostname(config)# <code>dns server-group example.com</code><br>hostname(config-dns-server-group)# <code>domain-name example.com</code>                                                                                                                                                          | Specifies the domain name. The default domain-name setting is DefaultDNS.                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <code>name-server</code><br><br><b>Example:</b><br>hostname(config-dns-server-group)# <code>name-server 192.168.10.10</code>                                                                                                                                                                                                                       | Resolves the domain name to an IP address.                                                                                                                                                                                                                                                                                                                                                        |
| Step 4 | <code>webvpn</code>                                                                                                                                                                                                                                                                                                                                | Switches to Clientless SSL VPN configuration mode.                                                                                                                                                                                                                                                                                                                                                |
| Step 5 | <code>tunnel-group webvpn</code>                                                                                                                                                                                                                                                                                                                   | Switches to tunnel-group Clientless SSL VPN configuration mode.                                                                                                                                                                                                                                                                                                                                   |
| Step 6 | (Required only if you are using a domain name other than the default one [DefaultDNS].)<br><br><code>dns-group</code><br><br><b>Example:</b><br>asa2(config-dns-server-group)# <code>exit</code><br>asa2(config)# <code>tunnel-group DefaultWEBVPNGroup webvpn-attributes</code><br>asa2(config-tunnel-webvpn)# <code>dns-group example.com</code> | Specifies the domain name that the tunnel groups will use. By default, the security appliance assigns the default Clientless SSL VPN group 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. |

## Making Applications 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 to provide access. Because each group policy or username supports only one port forwarding list, you must group each set of ca supported into a list. To display the port forwarding list entries already present in the ASA configuration, enter the following commands:

**DETAILED STEPS**

|               | <b>Command</b>                            | <b>Purpose</b>                                                                      |
|---------------|-------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Step 1</b> | <code>show run webvpn port-forward</code> | Displays the port forwarding list entries already present in the ASA configuration. |
| <b>Step 2</b> | <code>webvpn</code>                       | Switches to Clientless SSL VPN configuration mode.                                  |

|        | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <p><b>port-forward</b> {&lt;list name&gt; &lt;local port&gt; &lt;remote server&gt; &lt;remote port&gt; &lt;description&gt;}</p> <p><b>Example:</b><br/> <pre>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 DDTSSserver 22 DDTs over SSH hostname(config-webvpn)# port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet</pre></p> | <p>Adds a port forwarding entry to a list.</p> <ul style="list-style-type: none"> <li>• <i>list_name</i>—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.</li> <li>• <i>local_port</i>—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.</li> <li>• <i>remote_server</i>—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.</li> </ul> <p><b>Note</b> 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 <b>domain-name group</b> and <b>dns-group</b> commands described in that section is DefaultDNS.</p> <ul style="list-style-type: none"> <li>• <i>remote_port</i>—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.</li> <li>• <i>description</i>—Application name or short description that displays on the end user Port Forwarding Java applet screen. Maximum 64 characters.</li> </ul> <p>Shows how to create a port forwarding list called SalesGroupPorts that provides access to these applications.</p> |
| Step 4 | <p>(Optional)</p> <pre>no port-forward &lt;list name&gt; &lt;local port&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>Removes an entry from the list, specifying both the list and the local port.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

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.

### Prerequisites

Before initiating the **port-forward enable <list name>** command, the user is required to start port forwarding manually, using **Application Access > Start Applications** on the Clientless SSL VPN portal page.

### 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.

|        | Command                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>port-forward auto-start &lt;list name&gt;</code>                                           | Starts port forwarding automatically upon user login.                                                                                                                                                                                                                                                                               |
|        | <code>port-forward enable &lt;list name&gt;</code>                                               | Enables port forwarding upon user login.                                                                                                                                                                                                                                                                                            |
|        | <code>port-forward disable</code>                                                                | Prevents port forwarding.                                                                                                                                                                                                                                                                                                           |
|        | <code>no port-forward [auto-start &lt;list name&gt;   enable &lt;list name&gt;   disable]</code> | Removes a <b>port-forward</b> command from the group policy or username configuration, which then inherits the <b>[no] port-forward</b> command from the default group policy. The keywords following the <b>no port-forward</b> command are optional; however, they restrict the removal to the named <b>port-forward</b> command. |

Step 7

## Automating Port Forwarding

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

## DETAILED STEPS

|        | Command                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>webvpn</code>                                                                                                                                                                                              | Switches to Clientless SSL VPN configuration mode.                                                                                                                                                                                                                                                                                                  |
| Step 2 | <code>group-policy webvpn</code><br><code>username webvpn</code>                                                                                                                                                 | Switches to group-policy Clientless SSL VPN configuration mode.<br><br>Switches to username Clientless SSL VPN configuration mode.                                                                                                                                                                                                                  |
| Step 3 | <code>port-forward auto-start &lt;list name&gt;</code><br><br><b>Example:</b><br><code>hostname(config-group-policy)# webvpn</code><br><code>hostname(config-group-webvpn)# port-forward auto-start apps1</code> | Starts port forwarding automatically upon user login.<br><br><i>list_name</i> names the port forwarding list already present in the ASA Clientless SSL VPN configuration. You cannot assign more than one port forwarding list to a group policy or username.<br><br>Assigns the port forwarding list named <code>apps1</code> to the group policy. |
| Step 4 | <code>show run webvpn port-forward</code>                                                                                                                                                                        | Displays the port forwarding list entries present in the ASA configuration.                                                                                                                                                                                                                                                                         |
| Step 5 | (Optional)<br><code>no port-forward</code>                                                                                                                                                                       | Removes the <b>port-forward</b> command from the group policy or username and reverts to the default.                                                                                                                                                                                                                                               |

## Enabling and Switching off Port Forwarding

By default, port forwarding is switched off.

## DETAILED STEPS

|        | Command                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>port-forward [enable &lt;list name&gt;   disable]</code><br><br><b>Example:</b><br><code>hostname(config-group-policy)# webvpn</code><br><code>hostname(config-group-webvpn)# port-forward enable apps1</code> | Enables port forwarding. You do not have to start port forwarding manually if you entered <b>port-forward auto-start list_name</b> from the previous table.<br><br><i>list_name</i> is the name of the port forwarding list already present in the ASA Clientless SSL VPN configuration. You cannot assign more than one port forwarding list to a group policy or username.<br><br>Assigns the port forwarding list named <code>apps1</code> to the group policy. |
| Step 2 | <code>show running-config port-forward</code>                                                                                                                                                                        | Displays the port forwarding list entries.                                                                                                                                                                                                                                                                                                                                                                                                                         |

|        | Command                                         | Purpose                                                                                               |
|--------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Step 3 | (Optional)<br><code>no port-forward</code>      | Removes the <b>port-forward</b> command from the group policy or username and reverts to the default. |
| Step 4 | (Optional)<br><code>port-forward disable</code> | Switches off port forwarding.                                                                         |

## 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.



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 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 the **nbns-server** command. If you use a hostname, the ASA requires a DNS server to resolve it to an IP address.

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>webvpn</code>                                                                                                                                                                                                                                                                                                   | Switches to Clientless SSL VPN configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <code>tunnel-group webvpn</code>                                                                                                                                                                                                                                                                                      | Switches to tunnel-group Clientless SSL VPN configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 3 | <p><code>nbns-server {IPaddress   hostname} [master] [timeout timeout] [retry retries]</code></p> <p><b>Example:</b></p> <pre>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</pre> | <p>Browses a network or domain for each NetBIOS Name Server (NBNS).</p> <ul style="list-style-type: none"> <li><b>master</b> 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.</li> <li><b>timeout</b> 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.</li> <li><b>retries</b> 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.</li> </ul> |
| Step 4 | <code>hostname# show tunnel-group webvpn-attributes</code>                                                                                                                                                                                                                                                            | Displays the NBNS servers already present in the connection profile configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|        | Command                                                                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <p>(Optional)</p> <pre>character-encoding <i>charset</i></pre> <p><b>Example:</b></p> <pre>hostname(config)# webvpn hostname(config-webvpn)# character-encoding shift_jis hostname(config-webvpn)# customization DfltCustomization hostname(config-webvpn-custom)# page style background-color:white</pre> | <p>Specifies the character set to encode in Clientless SSL VPN portal pages delivered to remote users. By default, the encoding type set on the remote browser determines the character set for Clientless SSL VPN portal pages, so you need to set the character encoding only if it is necessary to ensure proper encoding on the browser.</p> <p><i>charset</i> is a string consisting of up to 40 characters, and is equal to one of the valid character sets identified in <a href="http://www.iana.org/assignments/character-sets">http://www.iana.org/assignments/character-sets</a>. You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850.</p> <p><b>Note</b> The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the <b>page style</b> command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the <b>no page style</b> command in webvpn customization command mode to remove the font family.</p> <p>Sets the character-encoding attribute to support Japanese Shift_JIS characters, removes the font family, and retains the default background color.</p> |
| Step 6 | <p>(Optional)</p> <pre>file-encoding {<i>server-name</i>   <i>server-ip-address</i>} <i>charset</i></pre> <p><b>Example:</b></p> <pre>hostname(config-webvpn)# file-encoding 10.86.5.174 cp860</pre>                                                                                                       | <p>Specifies the encoding for Clientless SSL VPN portal pages from specific CIFS servers. Thus, you can use different file-encoding values for CIFS servers that require different character encodings.</p> <p>Sets the file-encoding attribute of the CIFS server 10.86.5.174 to support IBM860 (alias “CP860”) characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

For a complete description of these commands, see the 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 the section on setting the date and time in the general operations configuration guide.

# Virtual Desktop Infrastructure (VDI)

The ASA supports connections to Citrix and VMWare VDI servers.

- For Citrix, the ASA allows access through clientless portal to user's running Citrix Receiver.
- VMWare is configured as a (smart tunnel) application.

VDI servers can also be accessed through bookmarks on the Clientless Portal, like other server applications.

## Limitations

- Authentication using certificates or Smart Cards is not supported for auto sign-on, since these forms of authentication do not allow the ASA in the middle.
- The XML service must be installed and configured on the XenApp and XenDesktop servers.
- Client certificate verifications, double Auth, internal passwords and CSD (all of CSD, not just Vault) are not supported when standalone mobile clients are used.

## Citrix Mobile Support

A mobile user running the Citrix Receiver can connect to the Citrix server by:

- Connecting to the ASA with AnyConnect, and then connecting to the Citrix server.
- Connecting to the Citrix server through the ASA, without using the AnyConnect client. Logon credentials can include:
  - A connection profile alias (also referred to as a tunnel-group alias) in the Citrix logon screen. A VDI server can have several group policies, each with different authorization and connection settings.
  - An RSA SecureID token value, when the RSA server is configured. RSA support includes next token for an invalid entry, and also for entering a new PIN for an initial or expired PIN.

## 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

### Certificate Limitations

- Certificate/Smart Card authentication is not supported as means of auto sign-on.
- Client certificate verifications and CSD are not supported
- Md5 signature in the certificates are not working because of security issue, which is a known problem on iOS: <http://support.citrix.com/article/CTX132798>

- SHA2 signature is not supported except for Windows, as described on the Citrix website: <http://www.citrix.com/>
- A key size >1024 is not supported

#### Other Limitations

- HTTP redirect is not supported; the Citrix Receiver application does not work with redirects.
- XML service must be installed and configured on the XenApp and XenDesktop servers.

## About Citrix Mobile Receiver User Logon

The logon for mobile users connecting to the Citrix server depends on whether the ASA has configured the Citrix server as a VDI server or a VDI proxy server.

When the Citrix server is configured as a VDI server:

1. Using the AnyConnect Secure Mobility Client, connect to ASA with VPN credentials.
2. Using Citrix Mobile Receiver, connect to Citrix server with Citrix server credentials (if single-signon is configured, the Citrix credentials are not required).

When the ASA is configured as a VDI proxy server:

1. Using Citrix Mobile Receiver, connect to the ASA entering credentials for both the VPN and Citrix server. After the first connection, if properly configured, subsequent connections only require VPN credentials.

## Configuring the ASA to Proxy a Citrix Server

You can configure the ASA to act as a proxy for the Citrix servers, so that connections to the ASA appear to the user like connections to the Citrix servers. The AnyConnect client is not required when you enable VDI proxy in ASDM. The following high-level steps show how the end user connects to Citrix.

1. A mobile user opens Citrix Receiver and connects to ASA's URL.
2. The user provides credentials for the XenApp server and the VPN credentials on the Citrix logon screen.
3. For each subsequent connection to the Citrix server, the user only needs to enter the VPN credentials.

Using the ASA as a proxy for XenApp and XenDesktop removes the requirement for a Citrix Access Gateway. XenApp server info is logged on the ASA, and displays in ASDM.

Configure the Citrix server's address and logon credentials, and assign that VDI server to a Group Policy or username. If both username and group-policy are configured, username settings override group-policy settings.

#### Additional Information

<http://www.youtube.com/watch?v=JMM2RzppaG8> - This video describes the advantages of using that ASA as a Citrix proxy.

## Assigning a VDI Server to a Group Policy

VDI servers are configured and assigned to Group Policies by:

- Adding the VDI server on the VDI Access pane, and assigning a group policy to the server.

- Adding a VDI server to the group policy.

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.

## Using SSL to Access Internal Servers

|        | Command           | Purpose                                                         |
|--------|-------------------|-----------------------------------------------------------------|
| Step 1 | webvpn            | Switches to group policy Clientless SSL VPN configuration mode. |
| Step 2 | url-entry disable | Switches off URL Entry.                                         |

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 15-22](#)
- [Configuring Clientless SSL VPN and ASDM Ports, page 15-22](#)
- [Configuring Support for Proxy Servers, page 15-23](#)
- [Configuring SSL/TLS Encryption Protocols, page 15-25](#)

## Using HTTPS for Clientless SSL VPN Sessions

### 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.

|        | Command                                                                                                                                                                                                                 | Purpose                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Step 1 | <code>webvpn</code>                                                                                                                                                                                                     | Switches to Clientless SSL VPN configuration mode.                   |
| Step 2 | <p><code>enable &lt;name of interface to use for Clientless SSL VPN sessions&gt;</code></p> <p><b>Example:</b><br/> <code>hostname(config)# webvpn</code><br/> <code>hostname(config-webvpn)# enable outside</code></p> | Enables Clientless SSL VPN sessions on the interface called outside. |

## Configuring Clientless SSL VPN and ASDM Ports

From 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 can configure these applications on different interfaces.

|        | Command             | Purpose                                            |
|--------|---------------------|----------------------------------------------------|
| Step 1 | <code>webvpn</code> | Switches to Clientless SSL VPN configuration mode. |

|        | Command                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 2 | <pre>port port_number</pre> <p><b>Example:</b></p> <pre>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</pre> | <p>Changes the SSL listening port for Clientless SSL VPN.</p> <p>Enables Clientless SSL VPN on port 444 of the outside interface. With this configuration, remote users initiating Clientless SSL VPN sessions enter <code>https://&lt;outside_ip&gt;:444</code> in the browser.</p>                                                                             |
| Step 3 | <pre>http server enable</pre> <p><b>Example:</b></p> <pre>hostname(config)# http server enable hostname(config)# http 192.168.3.0 255.255.255.0 outside hostname(config)# webvpn hostname(config-webvpn)# enable outside</pre>                                 | <p>(Privileged mode) Changes the listening port for ASDM.</p> <p>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 <code>https://&lt;outside_ip&gt;:444</code></p> |

## Configuring Support for Proxy Servers

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.

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.

|        | Command                                                                                   | Purpose                                                                                                                                                                                                                                                    |
|--------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>webvpn</code>                                                                       | Switches to Clientless SSL VPN configuration mode.                                                                                                                                                                                                         |
| Step 2 | <code>http-proxy</code> and <code>https-proxy</code>                                      | <p>Configures the ASA to use an external proxy server to handle HTTP and HTTPS requests.</p> <p><b>Note</b> Proxy NTLM authentication is not supported in <b>http-proxy</b>. Only proxy without authentication and basic authentication are supported.</p> |
| Step 3 | <code>http-proxy host [port] [exclude url] [username username {password password}]</code> | Configure HTTP proxy.                                                                                                                                                                                                                                      |

|         | Command                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <code>https-proxy host [port] [exclude url] [username username {password password}]</code>                                                                                                        | Configure HTTPS proxy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5  | <code>http-proxy pac url</code>                                                                                                                                                                   | Set the PAC file URL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 6  | (Optional)<br><code>exclude</code>                                                                                                                                                                | Excludes URLs from those that can be sent to the proxy server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 7  | <code>host</code>                                                                                                                                                                                 | Provides the hostname or IP address for the external proxy server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 8  | <code>pac</code>                                                                                                                                                                                  | Proxy autoconfiguration file downloaded to the ASA that uses a JavaScript function to identify a proxy for each URL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 9  | (Optional, and only available if you specify a username)<br><code>password</code>                                                                                                                 | Accompanies each proxy request with a password to provide basic, proxy authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 10 | <code>password</code>                                                                                                                                                                             | Password to send to the proxy server with each HTTP or HTTPS request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 11 | (Optional)<br><code>port</code>                                                                                                                                                                   | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 12 | <code>url</code>                                                                                                                                                                                  | If you entered <b>exclude</b> , enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards: <ul style="list-style-type: none"> <li>– * to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string.</li> <li>– ? to match any single character, including slashes and periods.</li> <li>– [x-y] to match any single character in the range of x and y, where x represents one character and y represents another character in the ANSI character set.</li> <li>– [!x-y] to match any single character that is not in the range.</li> </ul> |
| Step 13 | If you entered <b>http-proxy pac</b> , follow it with <b>http://</b> and type the URL of the proxy autoconfiguration file. (If you omit the <b>http://</b> portion, the CLI ignores the command.) | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 14 | (Optional)<br><code>username</code>                                                                                                                                                               | Accompanies each HTTP proxy request with a username for basic, proxy authentication. Only the <b>http-proxy host</b> command supports this keyword.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 15 | <code>username</code>                                                                                                                                                                             | Username to send to the proxy server with each HTTP or HTTPS request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|         | Command                                                                                                                                                                    | Purpose                                                                                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 16 | <b>Example:</b><br><pre>hostname(config-webvpn)# http-proxy 209.165.201.1 user jsmith password mysecretdonttell  hostname(config-webvpn)</pre>                             | Shows how to configure use of an HTTP proxy server with an IP address of 209.165.201.1 using the default port, sending a username and password with each HTTP request.                       |
| Step 17 | <b>Example:</b><br><pre>hostname(config-webvpn)# http-proxy 209.165.201.1 exclude www.example.com username jsmith password mysecretdonttell  hostname(config-webvpn)</pre> | Shows the same command, except when the ASA receives the specific URL <code>www.example.com</code> in an HTTP request, it resolves the request instead of passing it on to the proxy server. |
| Step 18 | <b>Example:</b><br><pre>hostname(config-webvpn)# http-proxy pac http://www.example.com/pac  hostname(config-webvpn)</pre>                                                  | Shows how to specify a URL to serve a proxy autoconfiguration file to the browser.                                                                                                           |

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 is supported.

## Configuring SSL/TLS Encryption Protocols

Port forwarding requires the 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

Email 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 section on using certificates and user login credentials in the general operations configuration guide.

## 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 `cisco-config/97/plugin` directory on the ASA file system.
- Populates the drop-down list 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 list next to the Address field of the portal page.

[Table 15-3](#) 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 15-3** Effects of Plug-ins on the Clientless SSL VPN Portal Page

| Plug-in    | Main Menu Option Added to Portal Page | Address Field Option Added to Portal Page |
|------------|---------------------------------------|-------------------------------------------|
| ica        | Citrix Client                         | citrix://                                 |
| rdp        | Terminal Servers                      | rdp://                                    |
| rdp2       | Terminal Servers Vista                | rdp2://                                   |
| ssh,telnet | SSH                                   | ssh://                                    |
|            | Telnet                                | telnet://                                 |
| vnc        | VNC Client                            | vnc://                                    |



### Note

A secondary 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 list 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.

- 
- 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 Clientless SSL VPN 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 Clientless SSL VPN 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

- Step 1** Ensure that Clientless SSL VPN 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

### DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                                                                                                             | Purpose                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Step 1 | <pre>import webvpn webcontent &lt;file&gt; &lt;url&gt;</pre> <p><b>Example:</b></p> <pre>hostname# import webvpn webcontent /+CSCOU+/login.inc tftp://209.165.200.225/login.inc !!!!* Web resource `+CSCOU+/login.inc' was successfully initialized hostname#</pre>                                                                                 | Imports the file and images as Web Content.                  |
| Step 2 | <pre>export webvpn customization &lt;file&gt; &lt;URL&gt;</pre> <p><b>Example:</b></p> <pre>hostname2# export webvpn customization template tftp://209.165.200.225/sales_vpn_login !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! %INFO: Customization object 'Template' was exported to tftp://10.21.50.120/sales _vpn_login</pre> | Exports a customization template.                            |
| Step 3 | <p>Change the full customization mode tag in the file to enable.</p> <p><b>Example:</b></p> <pre>&lt;full-customization&gt;   &lt;mode&gt;enable&lt;/mode&gt;   &lt;url&gt;+CSCOU+/login.inc&lt;/url&gt; &lt;/full-customization&gt;</pre>                                                                                                          | Supplies the URL of the login file stored in the ASA memory. |

|        | Command                                                                                                                                                                                                                                                                                                             | Purpose |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Step 4 | Import the file as a new customization object<br><br><b>Example:</b><br><pre>hostname# import webvpn customization sales_vpn_login tftp://10.21.50.120/sales_vpn_login\$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! %INFO: customization object 'sales_vpn_login' was successfully imported</pre> | —       |
| Step 5 | Apply the customization object to a Connection Profile (tunnel group)<br><br><b>Example:</b><br><pre>hostname (config) # tunnel-group Sales webvpn-attributes hostname (config-tunnel-webvpn) #customization sales_vpn_login</pre>                                                                                  | —       |

