



Configuring Clientless SSL VPN

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

- [Information About Clientless SSL VPN, page 91-2](#)
- [Licensing Requirements, page 91-2](#)
- [Prerequisites for Clientless SSL VPN, page 91-5](#)
- [Guidelines and Limitations, page 91-5](#)
- [Configuring Clientless SSL VPN Access, page 91-6](#)
- [Configuring the Setup for Cisco Secure Desktop, page 91-13](#)
- [Configuring Application Profile Customization Framework, page 91-15](#)
- [Using Auto Signon, page 91-25](#)
- [Configuring Session Settings, page 91-28](#)
- [Java Code Signer, page 91-28](#)
- [Encoding, page 91-29](#)
- [Content Cache, page 91-30](#)
- [Content Rewrite, page 91-31](#)
- [Configuring Browser Access to Plug-ins, page 91-33](#)
- [Understanding How KCD Works, page 91-38](#)
- [Configuring Application Access, page 91-45](#)
- [Configuring Port Forwarding, page 91-55](#)
- [Application Access User Notes, page 91-64](#)
- [Configuring File Access, page 91-68](#)
- [Ensuring Clock Accuracy for SharePoint Access, page 91-69](#)
- [Customizing the Clientless SSL VPN User Experience, page 91-69](#)
- [Using Clientless SSL VPN with PDAs, page 91-74](#)
- [Using E-Mail over Clientless SSL VPN, page 91-74](#)
- [Configuring Portal Access Rules, page 91-75](#)
- [Clientless SSL VPN End User Setup, page 91-77](#)
- [Configuring Browser Access to Client-Server Plug-ins, page 91-124](#)
- [Customizing the AnyConnect Client, page 91-137](#)

- [Configuring Bookmarks, page 91-146](#)
- [Sending an Administrator's Alert to Clientless SSL VPN Users, page 91-155](#)

Information About Clientless SSL VPN

**Note**

When the ASA is configured for clientless SSL VPN, you cannot enable security contexts (also called firewall multimode) or Active/Active stateful failover. Therefore, these features become unavailable.

Clientless SSL VPN lets users establish a secure, remote-access VPN tunnel to an ASA using a web browser. Users do not need a software or hardware client.

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

- Internal websites
- Web-enabled applications
- NT/Active Directory file shares
- E-mail proxies, including POP3S, IMAP4S, and SMTPS
- Microsoft Outlook Web Access Exchange Server 2000, 2003, and 2007
- Microsoft Web App to Exchange Server 2010 in 8.4(2) and later.
- Application Access (that is, smart tunnel or port forwarding access to other TCP-based applications)

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

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

Licensing Requirements

The following table shows the licensing requirements for this feature:

**Note**

This feature is not available on No Payload Encryption models.

Model	License Requirement ^{1,2}
ASA 5505	AnyConnect Premium license: <ul style="list-style-type: none"> • Base License or Security Plus license: 2 sessions. • <i>Optional permanent or time-based licenses: 10 or 25 sessions.</i> • <i>Shared licenses are not supported.</i>³
ASA 5510	AnyConnect Premium license: <ul style="list-style-type: none"> • Base and Security Plus License: 2 sessions. • <i>Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.</i> • <i>Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</i>
ASA 5520	AnyConnect Premium license: <ul style="list-style-type: none"> • Base License: 2 sessions. • <i>Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.</i> • <i>Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</i>
ASA 5540	AnyConnect Premium license: <ul style="list-style-type: none"> • Base License: 2 sessions. • <i>Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.</i> • <i>Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</i>
ASA 5550	AnyConnect Premium license: <ul style="list-style-type: none"> • Base License: 2 sessions. • <i>Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.</i> • <i>Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</i>
ASA 5580	AnyConnect Premium license: <ul style="list-style-type: none"> • Base License: 2 sessions. • <i>Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.</i> • <i>Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</i>
ASA 5512-X	AnyConnect Premium license: <ul style="list-style-type: none"> • Base License: 2 sessions. • <i>Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.</i> • <i>Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</i>

Model	License Requirement ^{1,2}
ASA 5515-X	AnyConnect Premium license: <ul style="list-style-type: none"> Base License: 2 sessions. Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions. Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.
ASA 5525-X	AnyConnect Premium license: <ul style="list-style-type: none"> Base License: 2 sessions. Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions. Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.
ASA 5545-X	AnyConnect Premium license: <ul style="list-style-type: none"> Base License: 2 sessions. Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions. Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.
ASA 5555-X	AnyConnect Premium license: <ul style="list-style-type: none"> Base License: 2 sessions. Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions. Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.
ASA 5585-X with SSP-10	AnyConnect Premium license: <ul style="list-style-type: none"> Base License: 2 sessions. Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions. Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.
ASA 5585-X with SSP-20, -40, and -60	AnyConnect Premium license: <ul style="list-style-type: none"> Base License: 2 sessions. Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions. Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.
ASASM	AnyConnect Premium license: <ul style="list-style-type: none"> Base License: 2 sessions. Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions. Optional Shared licenses³: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.

1. If you start a clientless SSL VPN session and then start an AnyConnect client session from the portal, 1 session is used in total. However, if you start the AnyConnect client first (from a standalone client, for example) and then log into the clientless SSL VPN portal, then 2 sessions are used.
2. The maximum combined VPN sessions of *all* types cannot exceed the maximum sessions shown in this table.
3. A shared license lets the ASA act as a shared license server for multiple client ASAs. The shared license pool is large, but the maximum number of sessions used by each individual ASA cannot exceed the maximum number listed for permanent licenses.

Prerequisites for Clientless SSL VPN

See the [Supported VPN Platforms, Cisco ASA 5500 Series](#) for the platforms and browsers supported by ASA Release 9.0.

Guidelines and Limitations

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

Observing Clientless SSL VPN Security Precautions

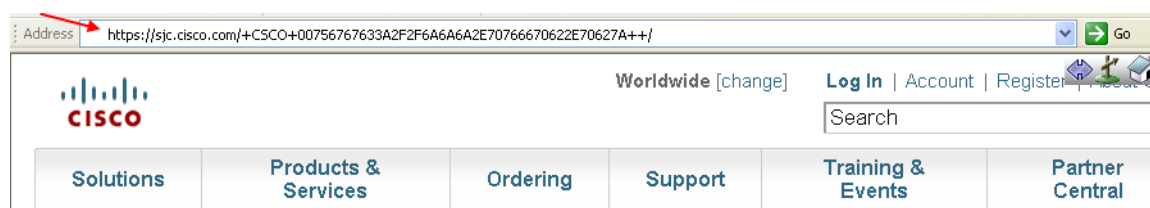
By default, the ASA permits all portal traffic to all web resources (e.g., HTTPS, CIFS, RDP, and plug-ins). The ASA clientless service rewrites each URL to one that is meaningful only to itself; the user cannot use the rewritten URL displayed on the page accessed to confirm that they are on the site they requested. To avoid placing users at risk, assign a web ACL to the policies configured for clientless

access – group-policies, dynamic access policies, or both – to control traffic flows from the portal. For example, without such an ACL, users could receive an authentication request from an outside fraudulent banking or commerce site. Also, we recommend disabling URL Entry on these policies to prevent user confusion over what is accessible.

Figure 91-1 Example URL Typed by User



Figure 91-2 Same URL Rewritten by Security Appliance and displayed on the Browser Window



Detailed Steps

We recommend that you do the following to minimize risks posed by clientless SSL VPN access:

- Step 1** Configure a group policy for all users who need clientless SSL VPN access, and enable clientless SSL VPN only for that group policy.
- Step 2** With the group policy open, choose **General > More Options > Web ACL** and click **Manage**.
- Step 3** Create a web ACL to do one of the following: permit access only to specific targets within the private network, permit access only to the private network, deny Internet access, or permit access only to reputable sites.
- Step 4** Assign the web ACL to any policies (group policies, dynamic access policies, or both) that you have configured for clientless access. To assign a web ACL to a DAP, edit the DAP record, and select the web ACL on the **Network ACL Filters** tab.
- Step 5** Disable URL entry on the *portal page*, the page that opens upon the establishment of a browser-based connection. To do so, click **Disable** next to URL Entry on both the group policy Portal frame and the DAP **Functions** tab. To disable URL entry on a DAP, use ASDM to edit the DAP record, click the **Functions** tab, and check **Disable** next to URL Entry.
- Step 6** Instruct users to enter external URLs in the native browser address field above the portal page or open a separate browser window to visit external sites.

Configuring Clientless SSL VPN Access

When configuring Clientless SSL VPN access, you can do the following:

- Enable or disable ASA interfaces for clientless SSL VPN sessions.
- Choose a port for clientless SSL VPN connections.
- Set a maximum number of simultaneous clientless SSL VPN sessions.

Detailed Steps

-
- Step 1** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies** pane to configure or create a group policy for clientless access.
- Step 2** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.
- Enable or disable **Allow Access** for each ASA interface.

The Interface columns lists the configured interfaces. The WebVPN Enabled field displays the current status for clientless SSL VPN on the interface. (A green check next to Yes indicates that clientless SSL VPN is enabled. A red circle next to No indicates that clientless SSL VPN is disabled.)
 - Click the **Port Setting** button, and enter the port number that you want to use for clientless SSL VPN sessions. The default port is 443, for HTTPS traffic; the range is 1 through 65535. If you change the port number, all current clientless SSL VPN connections terminate, and current users must reconnect. You also lose connectivity to ASDM, and a prompt displays, inviting you to reconnect.
- Step 3** Navigate to **Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions**, and enter the maximum number of clientless SSL VPN sessions you want to allow in the Maximum Other VPN Sessions field. Be aware that the different ASA models support clientless SSL VPN sessions as follows: ASA 5510 supports a maximum of 250; ASA 5520 maximum is 750; ASA 5540 maximum is 2500; ASA 5550 maximum is 5000.
-

Clientless SSL VPN Server Certificate Verification

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

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

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



Note

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

Enabling HTTP Server Verification

To enable HTTPS Server Verification for Clientless SSL VPN users:

- Step 1** In the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**.

Figure 91-3 Enabling HTTPS Server Verification in the ASDM

Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool

Configure Trusted Certificate Pool (Trustpool) to enable clientless SSL VPN users to identify remote HTTPS sites as secure. Remote servers' SSL certificates will be checked against a list of trusted CA certificates.

HTTPS Server Verification

☒ Enable SSL server certificate check

When server certificate verification fails, ☐ allow user to proceed to https site
☒ disconnect user from https site

Trusted Certificate Pool

Issued To	Issued By	Expiry Date	Usage

Import Bundle
Export Pool
Clear Pool
Certificate Details

Apply Reset

244271

- Step 2** Select the **Enable SSL Certificate check** check box.
- Step 3** You must decide which action you want to be taken if server certificate verification fails. Click **disconnect user from https site** to disconnect if the server could not be verified. Alternatively, click **allow user to proceed to https site** to allow the user to continue the connection, even if the check failed.
- Step 4** Click **Apply** to save your changes.

Importing a Certificate Bundle

You can import individual certificates or bundles of certificates from a variety of locations in one of the following formats:

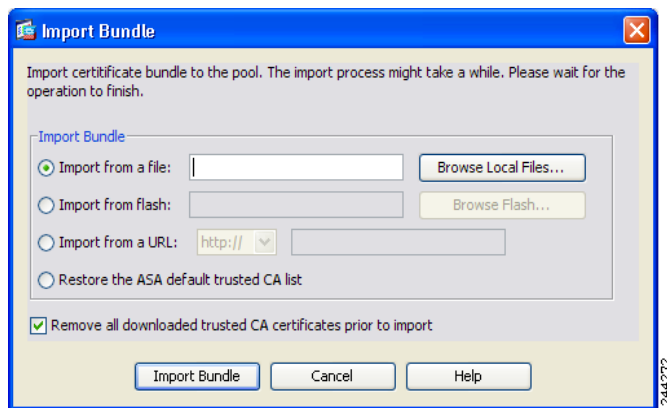
- x509 certificates in DER format wrapped in a pkcs7 structure

- a file of concatenated x509 certificates in PEM format (complete with PEM header)

To import a certificate or bundle:

Step 1 In the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**.

Step 2 Click **Import Bundle**.



Step 3 Select the location of the bundle:

- If the bundle is stored on your machine, click **Import from a file**, then click **Browse Local Files** and navigate to the bundle.
- If the bundle is stored on the ASA flash file system, click **Import from flash**, then click **Browse Flash** and navigate to the file.
- If the bundle is hosted on a server, click **Import from a URL**, select the protocol from the list, and enter the URL in the box.

Step 4 Click **Import Bundle**. Alternatively, click **Cancel** to abandon your changes.



Note You can select the **Remove all downloaded trusted CA certificates prior to import** check box to clear the trustpool before importing a new bundle.

Exporting the Trustpool

When you have correctly configured the Trustpool you should export the pool. This will enable you to restore the Trustpool to this point, for example if you wish to remove a certificate that was added to the trustpool after the export. You can export the pool to the ASA flash file system or your local file system.

In the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**, then click **Export Pool**.

To export to the local file system:

Step 1 Click **Export to a file**.

Step 2 Click **Browse Local Files**.

Step 3 Navigate to the folder where you want to save the trustpool.

- Step 4** Enter a unique memorable name for the trustpool in the **File name** box.
- Step 5** Click **Select**.
- Step 6** Click **Export Pool** to save the file. Alternatively, click **Cancel** to stop saving.

Removing Certificates

To remove all certificates, in the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**, then click **Clear Pool**.



Note

Before clearing the trustpool you should export the current trustpool to enable you to restore your current settings.

Restoring the Default Trusted Certificate Authority List

To restore the default trusted Certificate Authority (CA) list, in the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**, then click **Restore default trusted CA list** and click **Import Bundle**.

Updating the Trustpool

The trustpool should be updated if either of the following conditions exists:

- Any certificate in the trustpool is due to expire or has been re-issued.
- The published CA certificate bundle contains additional certificates that are required by a specific application.

A full update will replace all the certificates in the trustpool.

A practical update enables you to add new certificates or replace existing certificates.

Removing a Certificate Bundle

Clearing the trustpool removal will remove all certificates that are not part of the default bundle.

You cannot remove the default bundle. To clear the trustpool, in the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**, then click **Clear Pool**.



Note

	Command	Purpose
Step 1	webvpn	Switches to group policy webvpn configuration mode.
Step 2	url-entry disable	Disables URL entry.

Configuring ACLs

ACLs constrain user access to specific networks, subnets, hosts, and web servers. The Web ACLs table displays the filters configured on the ASA application to the clientless SSL VPN traffic. The table shows the name of each access control list (ACL), and below and indented to the right of the ACL name, the ACEs (access control entries) assigned to the ACL.

Each ACL permits or denies access to specific networks, subnets, hosts, and web servers. Each ACE specifies one rule that serves the function of the ACL.

Guidelines

If you do not define any filters, all connections are permitted.

Restrictions

- The ASA supports only an inbound ACL on an interface.
- At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an ACE (access control entry), the ASA denies it. ACEs are referred to as rules in this topic.

Detailed Steps

Web ACLs are configured on the page **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.

-
- Step 1** Click **Add ACL** to add an ACL or ACE. To insert a new ACE before or after an existing ACE, click **Insert** or **Insert After**.
- Step 2** Click **Edit** to highlight the ACE you want to change.
- Step 3** Highlight the ACL or ACE you want to remove and click **Delete**. When you delete an ACL, you must delete all of its ACEs. No warning is provided, and or undelete.
- Step 4** Use the **Move Up** and **Move Down** buttons to change the order of ACLs or ACEs. The ASA checks ACLs to be applied to clientless SSL VPN sessions and their ACEs in the sequence determined by their position in the ACLs list until it finds a match.
- Step 5** Click **+** to expand or **-** to collapse the list of ACEs under each ACL. The priority of the ACEs under each ACL is displayed. The order in the list determines priority.
- Step 6** (Optional) Click **Find** to search for a web ACL. Start typing in the field, and the tool searches the beginning characters of every field for a match. You can use wild cards to expand your search. For example, typing *sal* in the Find field matches a web ACL named sales but not a customization object named wholesalers. If you type **sal* in the Find field, the search finds the first instance of either sales or wholesalers in the table.
- Step 7** Use the up and down arrows to skip up or down to the next string match. Check the **Match Case** checkbox to make your search case sensitive.
- Step 8** (Optional) Highlight a web ACL and click **Assign** to assign the selected web ACL to one or more VPN group policies, dynamic access policies, or user policies.
- Step 9** When you create an ACE, by default it is enabled. Clear the check box to disable an ACE.

The IP address or URL of the application or service to which the ACE applies is displayed. The TCP service to which the ACE applies is also displayed. The Action field displays whether the ACE permits or denies clientless SSL VPN access. The time range associated with the ACE and the logging behavior (either disabled or with a specified level and time interval) is also displayed.

Adding or Editing ACEs

An Access Control Entry (or “access rule”) permits or denies access to specific URLs and services. You can configure multiple ACEs for an ACL. ACLs apply ACEs in priority order, acting on the first match.

Detailed Steps

-
- Step 1** Permit or deny access to specific networks, subnets, hosts, and web servers specified in the Filter group field.
- Step 2** Specify a URL or an IP address to which you want to apply the filter (permit or deny user access):
- URL—Applies the filter to the specified URL.
 - Protocols (unlabeled)—Specifies the protocol part of the URL address.
 - ://x—Specifies the URL of the Web page to which to apply the filter.
 - TCP—Applies the filter to the specified IP address, subnet, and port.
 - IP Address—Specifies the IP address to which to apply the filter.
 - Netmask—Lists the standard subnet mask to apply to the address in the IP Address field.
 - Service—Identifies the service (such as https, kerberos, or any) to be matched. Displays a list of services from which you can select the service to display in the Service field.
 - Boolean operator (unlabeled)—Lists the boolean conditions (equal, not equal, greater than, less than, or range) to use in matching the service specified in the service field.
- Step 3** The Rule Flow Diagram graphically depicts the traffic flow using the filter. This area may be hidden.
- Step 4** Specify the logging rules. The default is Default Syslog.
- Logging—Choose enable if you want to enable a specific logging level.
 - Syslog Level—Grayed out until you select Enable for the Logging attribute. Lets you select the type of syslog messages you want the ASA to display.
 - Log Interval—Lets you select the number of seconds between log messages.
 - Time Range—Lets you select the name of a predefined time-range parameter set.
 - ...—Click to browse the configured time ranges or to add a new one.

Configuration Examples for ACLs for Clientless SSL VPN

Examples

Here are examples of ACLs for clientless SSL VPN:

Action	Filter	Effect
Deny	url http://*.yahoo.com/	Denies access to all of Yahoo!
Deny	url cifs://fileserver/share/directory	Denies access to all files in the specified location.
Deny	url https://www.example.com/ directory/file.html	Denies access to the specified file.
Permit	url https://www.example.com/directory	Permits access to the specified location
Deny	url http://*:8080/	Denies HTTPS access to anywhere via port 8080.

Action	Filter	Effect
Deny	url http://10.10.10.10	Denies HTTP access to 10.10.10.10.
Permit	url any	Permits access to any URL. Usually used after an ACL that denies url access.

Configuring the Setup for Cisco Secure Desktop

The Cisco Secure Desktop Setup window displays the version and state of the Cisco Secure Desktop image if it is installed on the ASA, indicates whether it is enabled, and shows the size of the cache used to hold the Cisco Secure Desktop and SSL VPN Client on the ASA.

You can use the buttons in this window as follows:

To transfer a copy of a Cisco Secure Desktop image from your local computer to the flash device of the ASA, click **Upload**.

To prepare to install or upgrade Cisco Secure Desktop, use your Internet browser to download a `securedesktop_asa_<n>_<n>*.pkg` file from <http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop> to any location on your PC. Then use this button to transfer a copy from your local computer to the flash device. Click **Browse Flash** to install it into the running configuration. Finally, click **Enable Secure Desktop**.

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



Note

If you click **Browse Flash** to upgrade or downgrade the Cisco Secure Desktop image, select the package to install, and click **OK**, the Uninstall Cisco Secure Desktop dialog window asks you if you want to delete the Cisco Secure Desktop distribution currently in the running configuration from the flash device. Click **Yes** if you want to save space on the flash device, or click **No** to reserve the option to revert to this version of Cisco Secure Desktop.

- To remove the Cisco Secure Desktop image and configuration file (`sdesktop/data.xml`) from the running configuration, click **Uninstall**.

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

Detailed Steps

The Cisco Secure Desktop image loaded into the running configuration is displayed in the Location field. By default, the filename is in the format `securedesktop_asa_<n>_<n>*.pkg`.

-
- Step 1** Click **Browse Flash** to insert or modify the value in this field.
- Step 2** Click **Enable Secure Desktop** and click **Apply** to do the following:
- Make sure the file is a valid Cisco Secure Desktop image.
 - Create an “sdesktop” folder on disk0 if one is not already present.

- c. Insert a data.xml (Cisco Secure Desktop configuration) file into the sdesktop folder if one is not already present.
- d. Load the data.xml file into the running configuration.



Note If you transfer or replace the data.xml file, disable and then enable Cisco Secure Desktop to load the file.

- e. Enable Cisco Secure Desktop.

Uploading Images

The Upload Image dialog box lets you transfer a copy of a Cisco Secure Desktop image from your local computer to the flash device on the ASA. Use this window to install or upgrade Cisco Secure Desktop.

Prerequisites

- Before using this window, use your Internet browser to download a securedesktop_asa_<n>_<n>*.pkg file from <http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop> to any location on your local computer.

Detailed Steps

You can use the buttons in this window as follows:

- To choose the path of the securedesktop_asa_<n>_<n>*.pkg file to be transferred, click **Browse Local Files**. The Selected File Path dialog box displays the contents of the folder you last accessed on your local computer. Navigate to the securedesktop_asa_<n>_<n>*.pkg file, select it, and click **Open**.
- To select the target directory for the file, click **Browse Flash**. The Browse Flash dialog box displays the contents of the flash card.
- To upload the securedesktop_asa_<n>_<n>*.pkg file from your local computer to the flash device, click **Upload File**. A Status window appears and remains open for the duration of the file transfer. Following the transfer, an Information window displays the message, “File is uploaded to flash successfully.” Click **OK**. The Upload Image dialog box removes the contents of the Local File Path and Flash File System Path fields.
- To close the Upload Image dialog box, click **Close**. Click this button after you upload the Cisco Secure Desktop image to the flash device or if you decide not to upload it. If you uploaded it, the filename appears in the Secure Desktop Image field of the Cisco Secure Desktop Setup window. If you did not upload it, a Close Message dialog box prompts, “Are you sure you want to close the dialog without uploading the file?” Click **OK** if you do not want to upload the file. The Close Message and Upload Image dialog boxes close, revealing the Cisco Secure Desktop Setup pane. Otherwise, click **Cancel** in the Close Message dialog box. The dialog box closes, revealing the Upload Image dialog box again, with the values in the fields intact. Click **Upload File**.

- Step 1** Specify the path to the securedesktop_asa_<n>_<n>*.pkg file on your local computer. Click **Browse Local** to automatically insert the path in this field, or enter the path. For example:

D:\Documents and Settings\Windows_user_name.AMER\My Documents\My Downloads\securedesktop_asa_3_1_1_16.pkg

ASDM inserts the file path into the Local File Path field.

- Step 2** Specify the destination path on the flash device of the ASA and the name of the destination file. Click **Browse Flash** to automatically insert the path into this field, or enter the path. For example:

disk0:/securedesktop_asa_3_1_1_16.pkg

The file name of the Cisco Secure Desktop image that you selected on your local computer is displayed in the Browse Flash dialog box. We recommend that you use this name to prevent confusion. Confirm that this field displays the same name of the local file you selected and click **OK**. The Browse Flash dialog box closes. ASDM inserts the destination file path into the Flash File System Path field.

Configuring Application Profile Customization Framework

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

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

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

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

Restrictions

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

Managing APCF Profiles

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

- Step 1** Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Application Helper, where you can perform the following functions.
- Click **Add/Edit** to create a new APCF profile or change an existing one.
 - Select **Flash file** to locate an APCF file stored on the ASA flash memory.
Then click **Upload** to get an APCF file from a local computer to the ASA flash file system, or Browse to upload select an APCF file that is already in flash memory.
 - Select **URL** to retrieve the APCF file from an HTTP, HTTPS, FTP, or TFTP server.
 - Click **Delete** to remove an existing APCF profile. No confirmation or undo exists.
 - Click **Move Up** or **Move Down** to rearrange APCF profiles within the list. The order determines which the APCF profile is used.

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

Uploading APCF Packages

Detailed Steps

- Step 1** The path to the APCF file on your computer is shown. Click **Browse Local** to automatically insert the path in this field, or enter the path.
- Step 2** Click to locate and choose the APCF file on your computer that you want to transfer. The Select File Path dialog box displays the contents of the folder you last accessed on your local computer. Navigate to the APCF file, choose it, and click **Open**. ASDM inserts the file path into the Local File Path field.
- Step 3** The path on the ASA to upload the APCF file is shown in the Flash File System Path. Click **Browse Flash** to identify the location on the ASA to which you want to upload the APCF file. The Browse Flash dialog box displays the contents of flash memory.
- Step 4** The file name of the APCF file you selected on your local computer is displayed. We recommend that you use this name to prevent confusion. Confirm that this file displays the correct filename, and click **OK**. The Browse Flash dialog box closes. ASDM inserts the destination file path in the Flash File System Path field.
- Step 5** Click **Upload File** when you have identified the location of the APCF file on your computer, and the location where you want to download it to the ASA.
- Step 6** A Status window appears and remains open for the duration of the file transfer. Following the transfer, an Information window displays the message, “File is uploaded to flash successfully.” Click **OK**. The Upload Image dialog window removes the contents of the Local File Path and Flash File System Path fields, indicating you can upload another file. To do so, repeat these instructions. Otherwise, click **Close**.
- Step 7** Close the Upload Image dialog window. Click **Close** after you upload the APCF file to flash memory or if you decide not to upload it. If you do upload it, the filename appears in the APCF File Location field of the APCF window. If you do not upload it, a Close Message dialog box prompts, “Are you sure you want to close the dialog without uploading the file?” Click **OK** if you do not want to upload the file. The Close Message and Upload Image dialog boxes close, revealing the APCF Add/Edit pane. Otherwise, click **Cancel** in the Close Message dialog box. The dialog box closes, revealing the Upload Image dialog box again, with the values in the fields intact. Click **Upload File**.

Managing APCF Packets

- Step 1** Use the following commands to add, edit, and delete APCF packets and put them in priority order:
- **APCF File Location**—Displays information about the location of the APCF package. This can be on the ASA flash memory, or on an HTTP, HTTPS, FTP, or TFTP server.
 - **Add/Edit**—Click to add or edit a new or existing APCF profile.
 - **Delete**—Click to remove an existing APCF profile. There is no confirmation or undo.
 - **Move Up**—Click to rearrange APCF profiles within a list. The list determines the order in which the ASA attempts to use APCF profiles.
- Step 2** Click **Flash file** to locate an APCF file stored on the ASA flash memory.

- Step 3** Enter the path to an APCF file stored on flash memory. If you already added a path, it displays to an APCF file stored on flash memory after you browse to locate it.
- Step 4** Click Browse Flash to browse flash memory to locate the APCF file. A Browse Flash Dialog pane displays. Use the Folders and Files columns to locate the APCF file. Highlight the APCF file and click **OK**. The path to the file then displays in the Path field.



Note If you do not see the name of an APCF file that you recently downloaded, click **Refresh**.

- **Upload**—Click to upload an APCF file from a local computer to the ASA flash file system. The Upload APCF package pane displays.
- **URL**—Click to use an APCF file stored on an HTTP, HTTPS or TFTP server.
- **ftp, http, https, and tftp (unlabeled)**—Identify the server type.
- **URL (unlabeled)**—Enter the path to the FTP, HTTP, HTTPS, or TFTP server.

APCF Syntax

APCF profiles use XML format, and sed script syntax, with the XML tags in [Table 91-1](#).

Guidelines

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

Table 91-1 **APCF XML Tags**

Tag	Use
<APCF>...</APCF>	The mandatory root element that opens any APCF XML file.
<version>1.0</version>	The mandatory tag that specifies the APCF implementation version. Currently the only version is 1.0.
<application>...</application>	The mandatory tag that wraps the body of the XML description.
<id> text </id>	The mandatory tag that describes this particular APCF functionality.
<apcf-entities>...</apcf-entities>	The mandatory tag that wraps a single or multiple APCF entities.
<js-object>...</js-object> <html-object>...</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	One of these tags specifies type of content or the stage at which the APCF processing should take place.

Table 91-1 *APCF XML Tags (continued)*

Tag	Use
<code><conditions>... </conditions></code>	<p>A child element of the pre/post-process tags that specifies criteria for processing such as:</p> <ul style="list-style-type: none"> <code>http-version</code> (such as 1.1, 1.0, 0.9) <code>http-method</code> (get, put, post, webdav) <code>http-scheme</code> ("http/", "https/", other) <code>server-regexp</code> regular expression containing ("a".. "z" "A".. "Z" "0".. "9" "._*[]?") <code>server-fnmatch</code> (regular expression containing ("a".. "z" "A".. "Z" "0".. "9" "._*[]?+()\{\},"), <code>user-agent-regexp</code> <code>user-agent-fnmatch</code> <code>request-uri-regexp</code> <code>request-uri-fnmatch</code> <p>If more than one of condition tags is present, the ASA performs a logical AND for all tags.</p>
<code><action> ... </action></code>	<p>Wraps one or more actions to perform on the content under specified conditions; you can use the following tags to define these actions (shown below): <code><do></code>, <code><sed-script></code>, <code><rewrite-header></code>, <code><add-header></code>, <code><delete-header></code>.</p>
<code><do>...</do></code>	<p>Child element of the action tag used to define one of the following actions:</p> <ul style="list-style-type: none"> <code><no-rewrite/></code>—Do not mangle the content received from the remote server. <code><no-toolbar/></code>—Do not insert the toolbar. <code><no-gzip/></code>—Do not compress the content. <code><force-cache/></code>—Preserve the original caching instructions. <code><force-no-cache/></code>—Make object non-cacheable. <code><downgrade-http-version-on-backend></code>—Use HTTP/1.0 when sending the request to remote server.
<code><sed-script> TEXT </sed-script></code>	<p>Child element of the action tag used to change the content of text-based objects. The Text must be a valid Sed script. The <code><sed-script></code> applies to the <code><conditions></code> tag defined before it.</p>
<code><rewrite-header></rewrite-header></code>	<p>Child element of the action tag. Changes the value of the HTTP header specified in the child element <code><header></code> tag shown below.</p>
<code><add-header></add-header></code>	<p>Child element of the action tag used to add a new HTTP header specified in the child element <code><header></code> tag shown below.</p>

Table 91-1 **APCF XML Tags (continued)**

Tag	Use
<code><delete-header></delete-header></code>	Child element of the action tag used to delete the specified HTTP header specified by the child element <code><header></code> tag shown below.
<code><header></header></code>	Specifies the name HTTP header to be rewritten, added, or deleted. For example, the following tag changes the value of the HTTP header named Connection: <pre> <rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header> </pre>

Configuration Examples for APCF**Example:**

```

<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
    <process-request-header>
      <conditions>
        <server-fnmatch>*.example.com</server-fnmatch>
      </conditions>
      <action>
        <do><no-gzip/></do>
      </action>
    </process-request-header>
  </apcf-entities>
</application>
</APCF>

```

Example:

```

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

```

Managing Passwords

Optionally, you can configure the ASA to warn end users when their passwords are about to expire.

The ASA supports password management for the RADIUS and LDAP protocols. It supports the “password-expire-in-days” option for LDAP only.

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

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

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

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

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

Prerequisites

- Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.

If you are using an LDAP directory server for authentication, password management is supported with the Sun Java System Directory Server (formerly named the Sun ONE Directory Server) and the Microsoft Active Directory.

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

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

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

Detailed Steps

-
- Step 1** Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Add or Edit > Advanced > General > Password Management.

- Step 2** Click the Enable password management option.
-

Adding the Cisco Authentication Scheme to SiteMinder

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

Prerequisites

Configuring the SiteMinder Policy Server requires experience with SiteMinder.

Detailed Steps

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

-
- Step 1** With the SiteMinder Administration utility, create a custom authentication scheme, being sure to use the following specific arguments:
- In the Library field, enter **smjavaapi**.
 - In the Secret field, enter the same secret configured on the ASA.
You configure the secret on the ASA using the **policy-server-secret** command at the command line interface.
 - In the Parameter field, enter **CiscoAuthApi**.
- Step 2** Using your Cisco.com login, download the file **cisco_vpn_auth.jar** from <http://www.cisco.com/cisco/software/navigator.html> and copy it to the default library directory for the SiteMinder server. This .jar file is also available on the Cisco ASA CD.

Configuring the SAML POST SSO Server

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

Detailed Steps

-
- Step 1** Configure the SAML server parameters to represent the asserting party (the ASA):
- Recipient consumer URL (same as the assertion consumer URL configured on the ASA)
 - Issuer ID, a string, usually the hostname of appliance
 - Profile type -Browser Post Profile
- Step 2** Configure certificates.
- Step 3** Specify that asserting party assertions must be signed.
- Step 4** Select how the SAML server identifies the user:
- Subject Name Type is DN
 - Subject Name format is uid=<user>

Configuring SSO with the HTTP Form Protocol

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

Prerequisites

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

Restrictions

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

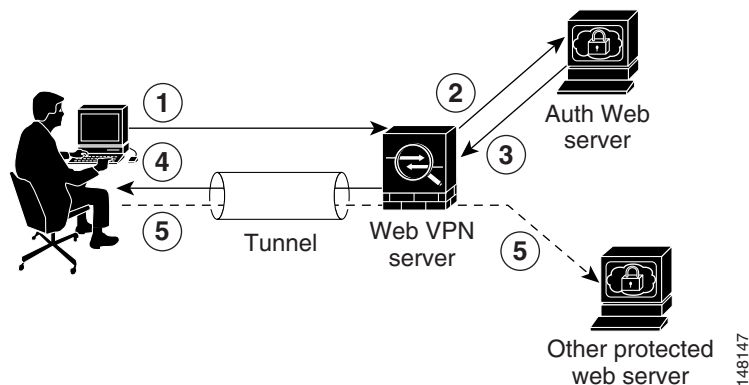
- The authentication cookie must be set for successful request and not set for unauthorized logons. In this case, ASA cannot distinguish successful from failed authentication.

Detailed Steps

The ASA again serves as a proxy for users of clientless SSL VPN to an authenticating web server but, in this case, it uses HTTP Form protocol and the POST method for requests. You must configure the ASA to send and receive form data. [Figure 91-4](#) illustrates the following SSO authentication steps:

-
- Step 1** A user of clientless SSL VPN first enters a username and password to log into the clientless SSL VPN server on the ASA.
 - Step 2** The clientless SSL VPN server acts as a proxy for the user and forwards the form data (username and password) to an authenticating web server using a POST authentication request.
 - Step 3** If the authenticating web server approves the user data, it returns an authentication cookie to the clientless SSL VPN server where it is stored on behalf of the user.
 - Step 4** The clientless SSL VPN server establishes a tunnel to the user.
 - Step 5** The user can now access other websites within the protected SSO environment without reentering a username and password.

Figure 91-4 SSO Authentication Using HTTP Forms



While you would expect to configure form parameters that let the ASA include POST data such as the username and password, you initially might not be aware of additional hidden parameters that the web server requires. Some authentication applications expect hidden data which is neither visible to nor entered by the user. You can, however, discover hidden parameters the authenticating web server expects by making a direct authentication request to the web server from your browser without the ASA in the middle acting as a proxy. Analyzing the web server response using an HTTP header analyzer reveals hidden parameters in a format similar to the following:

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

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

Gathering HTTP Form Data

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

Prerequisites

These steps require a browser and an HTTP header analyzer.

Detailed Steps

- Step 1** Start your browser and HTTP header analyzer, and connect directly to the web server login page without going through the ASA.
- Step 2** After the web server login page has loaded in your browser, examine the login sequence to determine if a cookie is being set during the exchange. If the web server has loaded a cookie with the login page, configure this login page URL as the *start-URL*.
- Step 3** Enter the username and password to log in to the web server, and press **Enter**. This action generates the authentication POST request that you examine using the HTTP header analyzer.

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

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05
-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5Fzmjnk3DRNwNjk2KcqVCFbIr
NT9%2bJ0H0KPshFtg6rB1UV2PxxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmye
mco%2FHTTP/1.1
```

```
Host: www.example.com
```

```
(BODY)
```

```
SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%
2Fwww.example.com%2Femco%2Fmyemco%2Fsmauthreason=0
```

- Step 4** Examine the POST request and copy the protocol, host, and the complete URL to configure the action-uri parameter.
- Step 5** Examine the POST request body and copy the following:
 - a. Username parameter. In the preceding example, this parameter is *USERID*, not the value *anyuser*.
 - b. Password parameter. In the preceding example, this parameter is *USER_PASSWORD*.

- c. Hidden parameter. This parameter is everything in the POST body except the username and password parameters. In the preceding example, the hidden parameter is:
 SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0

Figure 91-5 highlights the action URI, hidden, username and password parameters within sample output from an HTTP analyzer. This is only an example; output varies widely across different websites.

Figure 91-5 Action-uri, hidden, username and password parameters

The screenshot shows an HTTP analyzer window with a list of requests at the top. The selected request is a POST to /auth/login. The 'Headers' tab is active, showing various headers. The 'Post Data' tab is also visible, showing the request body. The body contains a URL-encoded string: passurl=&page=1&user=userid&passwd=user_password&x=32&y=5. The Host header is webauth.example.com. The request is annotated with numbered circles 1, 2, and 3.

1 POST /auth/login HTTP/1.1

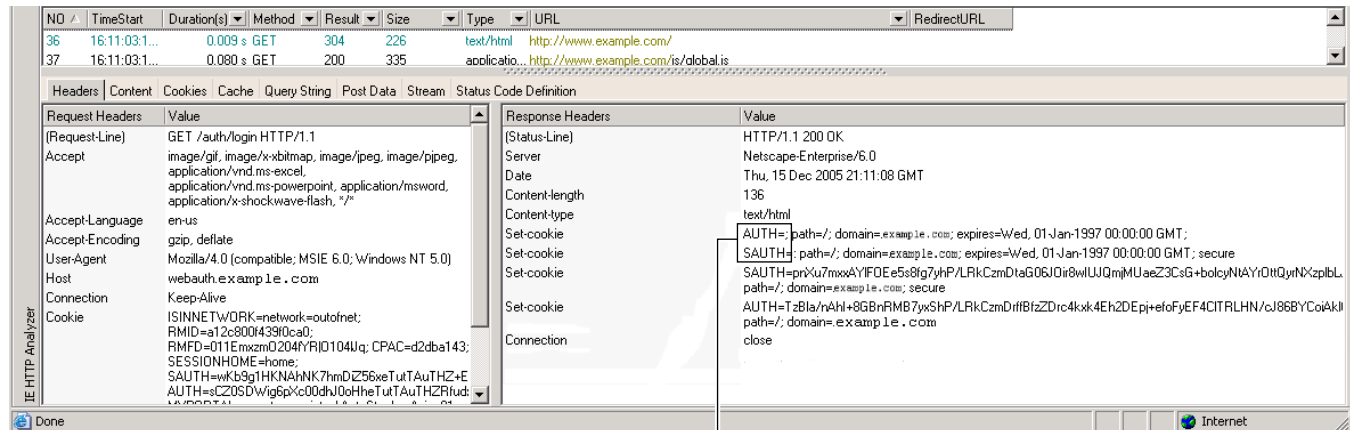
8 Host: webauth.example.com

2 14 passurl=&page=1&user=userid&passwd=user_password&x=32&y=5

3

Step 6 If you successfully log in to the web server, examine the server response with the HTTP header analyzer to locate the name of the session cookie set by the server in your browser. This is the **auth-cookie-name** parameter.

In the following server response header, the name of the session cookie is SMSESSION. You just need the name, not the value. Figure 91-6 shows an example of authorization cookies in HTTP analyzer output. This is only an example; output varies widely across different websites.

Figure 91-6 Authorization cookies in sample HTTP analyzer output

1 AUTH=; path=/; domain=example.com; expires=Wed, 01-Jan-1997 00:00:00 GMT;
SAUTH=; path=/; domain=example.com; expires=Wed, 01-Jan-1997 00:00:00 GMT; secure

249532

1 Authorization cookies

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

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

Using Auto Signon

The Auto Signon window or tab lets you configure or edit auto signon for users of clientless SSL VPN. Auto signon is a simplified single signon method that you can use if you do not already have an SSO method deployed on your internal network. With auto signon configured for particular internal servers, the ASA passes the login credentials that the user of clientless SSL VPN entered to log in to the ASA (username and password) to those particular internal servers. You configure the ASA to respond to a specific authentication method for a particular range of servers. The authentication methods you can configure the ASA to respond to consists of authentication using Basic (HTTP), NTLM, FTP and CIFS, or all of these methods.

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

Auto signon is a straight-forward method for configuring SSO for particular internal servers. This section describes the procedure for setting up SSO with auto signon. If you already have SSO deployed using Computer Associates SiteMinder SSO server, or if you have Security Assertion Markup Language (SAML) Browser Post Profile SSO, and if you want to configure the ASA to support this solution, see the “SSO Servers” section on page 91-61.

The following fields are displayed:

- **IP Address**—In conjunction with the following Mask, displays the IP address range of the servers to be authenticated to as configured with the Add/Edit Auto Signon dialog box. You can specify a server using either the server URI or the server IP address and mask.
- **Mask**—In conjunction with the preceding IP Address, displays the IP address range of the servers configured to support auto signon with the Add/Edit Auto Signon dialog box.
- **URI**—Displays a URI mask that identifies the servers configured with the Add/Edit Auto Signon dialog box.
- **Authentication Type**—Displays the type of authentication—Basic (HTTP), NTLM, FTP and CIFS, or all of these methods—as configured with the Add/Edit Auto Signon dialog box.

Restrictions

- Do not enable auto signon for servers that do not require authentication or that use credentials different from the ASA. When auto signon is enabled, the ASA passes on the login credentials that the user entered to log into the ASA regardless of what credentials are in user storage.
- If you configure one method for a range of servers (for example, HTTP Basic) and one of those servers attempts to authenticate with a different method (for example, NTLM), the ASA does not pass the user login credentials to that server.

Detailed Steps

-
- Step 1** Click to add or edit an auto signon instruction. An auto signon instruction defines a range of internal servers using the auto signon feature and the particular authentication method.
- Step 2** Click to delete an auto signon instruction selected in the Auto Signon table.
- Step 3** Click **IP Block** to specify a range of internal servers using an IP address and mask.
- **IP Address**—Enter the IP address of the first server in the range for which you are configuring auto sign-on.
 - **Mask**—From the subnet mask menu, choose the subnet mask that defines the server address range of the servers supporting auto signon.
- Step 4** Click **URI** to specify a server supporting auto signon by URI, then enter the URI in the field next to this button.
- Step 5** Determine the authentication method assigned to the servers. For the specified range of servers, the ASA can be configured to respond to Basic HTTP authentication requests, NTLM authentication requests, FTP and CIFS authentication requests, or requests using any of these methods.
- **Basic**—Click this button if the servers support basic (HTTP) authentication.
 - **NTLM**—Click this button if the servers support NTLMv1 authentication.



Note

NTLM is not the most secure choice and other better alternatives exist. NTLM does not support recent cryptographic methods such as AES or SHA-256. Cisco recommends that applications not use NTLM.

- FTP/CIFS—Click this button if the servers support FTP and CIFS authentication
 - Basic, NTLM, and FTP/CIFS—Click this button if the servers support all of the above.
-

Accessing Virtual Desktop Infrastructure (VDI)

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

Supported Mobile Devices

- iPad—Citrix Receiver version 4.x or later
- iPhone/iTouch—Citrix Receiver version 4.x or later
- Android 2.x/3.x/4.0/4.1 phone—Citrix Receiver version 2.x or later
- Android 4.0 phone—Citrix Receiver version 2.x or later

Limitations

Citrix Receiver clients access only one XenApp/XenDesktop server at a time.


Detailed Steps

- Step 1** Browse to Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies.
- Step 2** Edit the DfltGrpPolicy and expand the More options menu from the left-side menu.
- Step 3** Choose **VDI Access**. Click **Add** or **Edit** to provide VDI server details.
- Server (Host Name or IP Address)—Address of the XenApp or XenDesktop server. This value can be a clientless macro.
 - Port Number (Optional)—Port number for connecting to the Citrix server. This value can be a clientless macro.
 - Active Directory Domain Name—Domain for logging into the virtualization infrastructure server. This value can be a clientless macro.
 - Use SSL Connection—Check the checkbox if you want the server to connect using SSL.
 - 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.
-

Configuring Session Settings

The clientless SSL VPN Add/Edit Internal Group Policy > More Options > Session Settings window lets you specify personalized user information between clientless SSL VPN sessions. By default, each group policy inherits the settings from the default group policy. Use this window to specify personalized clientless SSL VPN user information for the default group policy and any group policies for which you want to differentiate these values.

Detailed Steps

-
- Step 1** Click none or choose the file server protocol (smb or ftp) from the User Storage Location drop-down menu. Cisco recommends using CIFS for user storage. You can set up CIFS without using a username/password or a port number. If you choose CIFS, enter the following syntax: **cifs//cifs-share/user/data**. If you choose smb or ftp, use the following syntax to enter the file system destination into the adjacent text field:
- username:password@host:port-number/path*
- For example
- mike:mysecret@ftpsrvr3:2323/public**
-  **Note** Although the configuration shows the username, password, and preshared key, the ASA uses an internal algorithm to store the data in an encrypted form to safeguard it.
-
- Step 2** Type the string, if required, for the security appliance to pass to provide user access to the storage location.
- Step 3** Choose one of the following options from the Storage Objects drop-down menu to specify the objects the server uses in association with the user. The ASA store these objects to support clientless SSL VPN connections.
- cookies,credentials
 - cookies
 - credentials
- Step 4** Enter the limit in KB transaction size over which to time out the session. This attribute applies only to a single transaction. Only a transaction larger than this value resets the session expiration clock.
-

Java Code Signer

Code signing appends a digital signature to the executable code itself. This digital signature provides enough information to authenticate the signer as well as to ensure that the code has not been subsequently modified since signed.

Code-signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.

Choose the configured certificate that you want to employ in Java object signing from the drop down list.

To configure a Java Code Signer, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer**.

Java objects which have been transformed by clientless SSL VPN can subsequently be signed using a PKCS12 digital certificate associated with a trustpoint. In the Java Trustpoint pane, you can configure the clientless SSL VPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location.

To import a trustpoint, choose **Configuration > Properties > Certificate > Trustpoint > Import**.

Encoding

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

Character encoding, also called “character coding” and “a character set,” is the pairing of raw data (such as 0s and 1s) with characters to represent the data. The language determines the character encoding method to use. Some languages use a single method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the remote user can change it. The browser can also detect the encoding specified on the page, and render the document accordingly.

The encoding attribute lets you specify the value of the character-encoding method used on the portal page to ensure that the browser renders it properly, regardless of the region in which the user is using the browser, and regardless of any changes made to the browser.

By default, the ASA applies the “Global Encoding Type” to pages from Common Internet File System servers. The mapping of CIFS servers to their appropriate character encoding, globally with the “Global Encoding Type” attribute, and individually with the file-encoding exceptions displayed in the table, provides for the accurate handling and display of CIFS pages when the proper rendering of filenames or directory paths, as well as pages, is an issue.

Detailed Steps

Step 1 Global Encoding Type determines the character encoding that all clientless SSL VPN portal pages inherit except for those from the CIFS servers listed in the table. You can type the string or choose one of the options from the drop-down list, which contains the most common values, as follows:

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis



Note

- unicode
- windows-1252
- none



Note If you click **none** or specify a value that the browser on the clientless SSL VPN session does not support, it uses its own default encoding.

You can type a string consisting of up to 40 characters, and equal to one of the valid character sets identified in <http://www.iana.org/assignments/character-sets>. You can use either the name or the alias of a character set listed on that page. The string is case-insensitive. The command interpreter converts upper-case to lower-case when you save the ASA configuration.

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

Step 3 Choose the character encoding that the CIFS server should provide for clientless SSL VPN portal pages. You can type the string, or choose one from the drop-down list, which contains only the most common values, as follows:

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis



Note If you are using Japanese Shift_jis Character encoding, click **Do not specify** in the Font Family area of the associated Select Page Font pane to remove the font family.

- unicode
- windows-1252
- none

If you click **none** or specify a value that the browser on the clientless SSL VPN session does not support, it uses its own default encoding.

You can type a string consisting of up to 40 characters, and equal to one of the valid character sets identified in <http://www.iana.org/assignments/character-sets>. You can use either the name or the alias of a character set listed on that page. The string is case-insensitive. The command interpreter converts upper-case to lower-case when you save the ASA configuration.

Content Cache

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

Detailed Steps

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

Step 2 If **Enable Cache** is unchecked, check it.

Step 3 Define the terms for caching.

- **Maximum Object Size**—Enter the maximum size in KB of a document that the ASA can cache. The ASA measures the original content length of the object, not rewritten or compressed content. The range is 0 to 10,000 KB; the default is 1000 KB
- **Minimum Object Size**—Enter the minimum size in KB of a document that the ASA can cache. The ASA measures the original content length of the object, not rewritten or compressed content. The range is 0 to 10,000 KB; the default is 0 KB.



Note The Maximum Object Size must be greater than the Minimum Object Size.

- **Expiration Time**—Enter an integer between 0 and 900 to set the number of minutes to cache objects without revalidating them. The default is one minute.
- **LM Factor**—Enter an integer between 1 and 100; the default is 20.

The LM factor sets the policy for caching objects which have only the last-modified timestamp. This revalidates objects that have no server-set change values. The ASA estimates the length of time since the object has changed, also called the expiration time. The estimated expiration time equals the time elapsed since the last change multiplied by the LM factor. Setting the LM factor to 0 forces immediate revalidation, while setting it to 100 results in the longest allowable time until revalidation.

The expiration time sets the amount of time to for the ASA to cache objects that have neither a last-modified time stamp nor an explicit server-set expiry time.

- **Cache static content**—Check to cache all content that is not subject to rewrite, for example, PDF files and images.
- **Restore Cache Default**—Click to restore default values for all cache parameters.

Content Rewrite

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

Clientless SSL VPN processes application traffic through a content transformation/rewriting engine that includes advanced elements such as JavaScript, VBScript, Java, and multi-byte characters to proxy HTTP traffic which may have different semantics and access control rules depending on whether the user is using an application within or independently of an SSL VPN device.

By default, the security appliance rewrites, or transforms, all clientless traffic. You might not want some applications and web resources (for example, public websites) to go through the ASA. The ASA therefore lets you create rewrite rules that let users browse certain sites and applications without going through the ASA. This is similar to split-tunneling in a VPN connection.

You can create multiple rewrite rules. The rule number is important because the security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

[“Configuration Example for Content Rewrite Rules”](#) shows example content rewrite rules.



Note These improvements were made to Content Rewriter in ASA 9.0:

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

Detailed Steps

The Content Rewrite table has the following columns:

- Rule Number—Displays an integer that indicates the position of the rule in the list.
- Rule Name—Provides the name of the application for which the rule applies.
- Rewrite Enabled—Displays content rewrite as enabled or disabled.
- Resource Mask—Displays the resource mask.

The following steps explain how to add a rewrite entry or edit a selected rewrite entry.

-
- Step 1** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Rewrite**.
- Step 2** Click Add or Edit to create or update an content rewriting rule.
- Step 3** Enable content rewrite must be checked to enable this rule.
- Step 4** Enter a number for this rule. This number specifies the priority of the rule, relative to the others in the list. Rules without a number are at the end of the list. The range is 1 to 65534.
- Step 5** (Optional) Provide an alphanumeric string that describes the rule, maximum 128 characters.
- Step 6** Enter a string to match the application or resource to apply the rule to. The string can be up to 300 characters. You can use one of the following wildcards, but you must specify at least one alphanumeric character.
- * — Matches everything. ASDM does not accept a mask that consists of a * or *.*.
 - ? —Matches any single character.
 - [!seq] — Matches any character not in sequence.
 - [seq] — Matches any character in sequence.

Configuration Example for Content Rewrite Rules

Table 91-2 **Content Rewrite Rules**

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

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 91-34](#)
- [Installing Plug-ins Redistributed By Cisco, page 91-34](#)
- [Providing Access to a Citrix XenApp Server, page 91-36](#)

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

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

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

[Table 91-3](#) 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.

* Not a recommended plug-in.

Table 91-3 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 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://

When the user in a clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection. The plug-ins support single sign-on (SSO). Refer to the [“Configuring SSO with the HTTP Form Protocol” section on page 91-22](#) for implementation details.

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

Prerequisites

- Clientless SSL VPN must be enabled on the ASA to provide remote access to the plug-ins.
- To configure SSO support for a plug-in, you install the plug-in, add a bookmark entry to display a link to the server, and specify SSO support when adding the bookmark.
- The minimum access rights required for remote use belong to the guest privilege mode.

- Plug-ins require ActiveX or Oracle Java Runtime Environment (JRE), see the [compatibility matrix](#) for version requirements.

Restrictions



Note

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

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

Preparing the Security Appliance for a Plug-in

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

Prerequisites

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

Restrictions

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

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

- [Installing Plug-ins Redistributed By Cisco, page 91-34](#)
- [Providing Access to a Citrix XenApp Server, page 91-36](#)

Installing Plug-ins Redistributed By Cisco

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

Prerequisites

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

Plug-ins Redistributed by Cisco

Table 91-4

Protocol	Description	Source of Redistributed Plug-in *
RDP	<p>HOBLink JWT is a Native Java RDP client which supports RDP 7.0 for remote access to Windows Terminal services.</p> <p>Note Since properoRDP and HOBSOft both use RDP as the plugin protocol, customers will not be able to use HOBSOft for one set of users and properoRDP for the rest via GroupPolicy etc.</p> <p>Use this plug-in if you want to use a single plug-in for Windows, Mac OS X and Linux operating systems. See This Document for a list of all supported operating systems.</p>	<p>Customers can download this plugin from these locations:</p> <p>HOBSOft Cisco.com Proper Java RDP</p>
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 5.2 of the RDP and RDP2 protocols are supported. Version 5.2 and later are not supported.</p>	<p>The original source of the redistributed plug-in is http://properjavardp.sourceforge.net/</p>
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>	<p>The original source of the redistributed plug-in is http://properjavardp.sourceforge.net/</p>
SSH	<p>The Secure Shell-Telnet plug-in lets the remote user establish a Secure Shell (v1 or v2) or Telnet connection to a remote computer.</p> <p>Note Because keyboard-interactive authentication is not supported by JavaSSH, it cannot be supported with SSH plugin. (Keyboard interactive is a generic authentication method used to implement different authentication mechanisms.)</p>	<p>The web site containing the source of the redistributed plug-in is http://javassh.org/</p>
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>	<p>The web site containing the source of the redistributed plug-in is http://www.tightvnc.com/</p>

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

These plug-ins are available on the [Cisco Adaptive Security Appliance Software Download](#) site.

Detailed Steps

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

Step 1 Create a temporary directory named `plugins` on the computer you use to establish ASDM sessions with the ASA, and download the plug-ins you want from the Cisco website to the `plugins` directory.

Step 2 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins**.

This pane displays the currently loaded plug-ins that are available to clientless SSL sessions. The hash and date of these plug-ins are also provided.

Step 3 Click **Import**.

The Import Client-Server Plug-in dialog box opens.

Step 4 Use the following descriptions to enter the Import Client-Server Plug-in dialog box field values.

- Plug-in Name—Select one of the following values:
 - **ica** to provide plug-in access to Citrix MetaFrame or Web Interface services
 - **rdp** to provide plug-in access to Remote Desktop Protocol services
 - **ssh,telnet** to provide plug-in access to *both* Secure Shell and Telnet services
 - **vnc** to provide plug-in access to Virtual Network Computing services



Note Any undocumented options in this menu are experimental and are not supported.

- Select the location of the plugin file—Select one of the following options and insert a path into its text field.
 - Local computer—Enter the location and name of the plug-in into the associated Path field, or click **Browse Local Files** and navigate to the plug-in, choose it, then click **Select**.
 - Flash file system—Enter the location and name of the plug-in into the associated Path field, or click **Browse Flash** and navigate to the plug-in, choose it, then click **OK**.
 - Remote Server—Choose **ftp**, **tftp**, or **HTTP** from the drop-down menu next to the associated Path attribute, depending on which service is running on the remote server. Enter the host name or address of the server and the path to the plug-in into the adjacent text field.

Step 5 Click **Import Now**.

Step 6 Click **Apply**.

The plug-in is now available for future clientless SSL VPN sessions.

Providing Access to a Citrix XenApp Server

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

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

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

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

- [Preparing the Citrix XenApp Server for Clientless SSL VPN Access](#)

- [Creating and Installing the Citrix Plug-in](#)

Preparing the Citrix XenApp Server for Clientless SSL VPN Access

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



Note

If you are not already providing support for a plug-in, you must follow the instructions in the [“Preparing the Security Appliance for a Plug-in”](#) section on page 91-34 before using this section.

Creating and Installing the Citrix Plug-in

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

Detailed Steps

-
- Step 1** Download the ICA plug-in file from the Cisco Software Download web site. This file contains files that Cisco customized for use with the Citrix plug-in.
- Step 2** Download the [Citrix Java client](#) from the Citrix site. On Citrix download site, select Citrix Receiver, Receivers by Platform, and click Find. Expand Receiver for Other Platforms, and download Receiver for Java. JICAComponents.tar.gz a gzip'd tar file, which you can open with 7-Zip or other unix-compatible tools.
- Step 3** Extract the following files from the Citrix Java client, then add them to the ica-plugin.zip file:
- JICA-configN.jar
 - JICAEngN.jar
- You can use WinZip to perform this step.
- Step 4** Ensure the EULA included with the Citrix Java client grants you the rights and permissions to deploy the client on your web servers.
- Step 5** Install the plug-in by using ASDM, or entering the following CLI command in privileged EXEC mode:
- ```
import webvpn plug-in protocol ica URL
```
- URL is the host name or IP address and path to the ica-plugin.zip file.



### Note

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

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

- Step 6** Establish an SSL VPN clientless session and click the bookmark or enter the URL for the Citrix server. Use the [Client for Java Administrator's Guide](#) as needed.
-

# Microsoft Kerberos Constrained Delegation Solution

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

For example, neither certificate- or OTP-based authentication methods encompass a conventional username and password necessary for the ASA to seamlessly perform SSO access to web-based resources. When authenticating with a certificate, a username and password is not required for the ASA to extend to web-based resources, making it an unsupported authentication method for SSO. On the other hand, OTP does include a static username; however, the password is dynamic and will subsequently change throughout the VPN session. In general, Web-based resources are configured to accept static usernames and passwords, thus also making OTP an unsupported authentication method for SSO.

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

## Requirements

In order for the **kcd-server** command to function, the ASA must establish a trust relationship between the *source* domain (the domain where the ASA resides) and the *target* or *resource* domain (the domain where the web services reside). The ASA, using its unique format, crosses the certification path from the source to the destination domain and acquires the necessary tickets on behalf of the remote access user to access the services.

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

## Understanding How KCD Works

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

The Kerberos security system is a network authentication protocol used to authenticate entities (users, computers, or applications) and protect network transmissions by scrambling the data so that only the device that the information was intended for can decrypt it. You can configure KCD to provide Clientless SSL VPN (also known as WebVPN) users with SSO access to any web services protected by Kerberos. Examples of such web services or applications include Outlook Web Access (OWA), Sharepoint, and Internet Information Server (IIS).

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

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

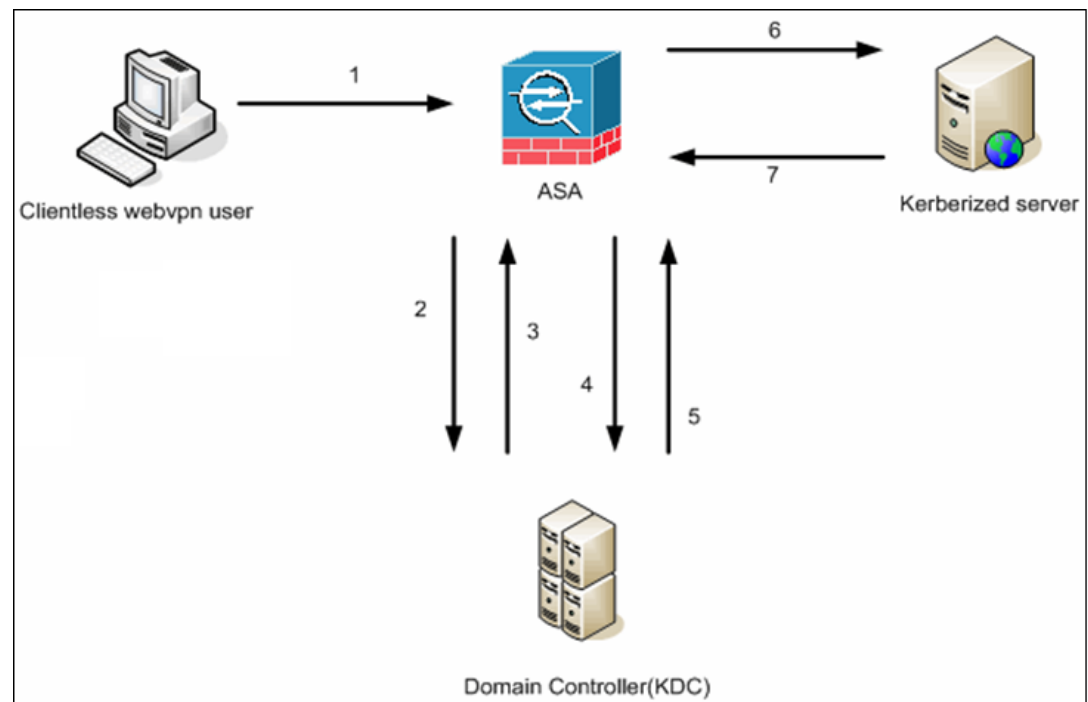
For more information on constrained delegation, see RFC 1510 via the IETF website (<http://www.ietf.org>).

## Authentication Flow with KCD

Figure 91-7 depicts the packet and process flow a user will experience directly and indirectly when accessing resources trusted for delegation via the clientless portal. This process assumes that the following tasks have been completed:

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

**Figure 91-7 KCD Process**



**Note**

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

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

**Note**

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

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

**Note**

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

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

## Adding Windows Service Account in Active Directory

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



## Configuring DNS for KCD

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

- Step 1** From ASDM, navigate to **Configuration > Remote Access VPN > DNS** and configure the DNS setup as shown in [Figure 91-8](#):
- DNS Server Group—Enter the DNS server IP address(es), such as 192.168.0.3.
  - Domain Name—Enter the domain name in which the DC is a member.
- Step 2** Enable DNS Lookup on the appropriate interface. Clientless VPN deployments require DNS Lookups via the internal corporate network, typically the *inside* interface.

**Figure 91-8 ASA DNS Configuration Example**

Configuration > Remote Access VPN > DNS

Specify how to resolve DNS requests.

DNS Setup

☒ Configure one DNS server group ☐ Configure multiple DNS server groups

Primary DNS Server: 192.168.0.3

Secondary Servers:

Domain Name: companydc.com

DNS Lookup

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

| Interface  | DNS Enabled |
|------------|-------------|
| inside     | True        |
| management | False       |
| outside    | False       |

## Configuring the ASA to Join the Active Directory Domain

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

- Step 1** From ASDM, navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Microsoft KCD Server**, as shown in [Figure 91-9](#).
- Step 2** Click **New** to add a Kerberos Server Group for Constrained Delegation and configure the following (see [Figure 91-9](#)):
- Server Group Configuration

- **Server Group Name**—Define the name of the constrained delegation configuration on the ASA, such as MSKCD, which is the default value. You can configure multiple server groups for redundancy; however, you can only assign one server group to the KCD server configuration used to request service tickets on behalf of VPN users.
- **Reactivation Mode**—Click the radio button for the mode you want to use (**Depletion** or **Timed**). In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive. In Timed mode, failed servers are reactivated after 30 seconds of down time. Depletion is the default configuration.
- **Dead Time**—If you choose the Depletion reactivation mode, you must add a dead time interval. Ten minutes is the default configuration. The interval represents the duration of time, in minutes, that elapses between the disabling of the last server in a group and the subsequent re-enabling of all servers.
- **Max Failed Attempts**—Set the number of failed connection attempts allowed before declaring an unresponsive server to be inactive. Three attempts is the default.
- **Server Configuration**
  - **Interface Name**—Choose the interface on which the server resides. In general, authentication server deployments reside on the internal corporate network, typically via the *inside* interface.
  - **Server Name**—Define the hostname of the domain controller, such as ServerHostName.
  - **Timeout**—Specify the maximum time, in seconds, to wait for a response from the server. Ten seconds is the default.
- **Kerberos Parameter**
  - **Server Port**—88 is the default and the standard port used for KCD.
  - **Retry Interval**—Choose the desired retry interval. Ten seconds is the default configuration.
  - **Realm**—Enter the domain name of the DC in all uppercase. The KCD configuration on the ASA requires the realm value to be in uppercase. A realm is an authentication domain. A service can accept authentication credentials only from entities in the same realm. The realm must match the domain name which the ASA joins.

**Figure 91-9 KCD Server Group Configuration**

- Step 3** Click **OK** to apply your configuration and then configure the Microsoft KCD Server to request service tickets on behalf of the remote access user (see [Figure 91-9](#)). The Microsoft KCD Server configuration window appears upon clicking **OK**.

## Configuring Kerberos Server Groups

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

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

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



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

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

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

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

**Note**

Under the Server Table section, the previously configured DC hostname, ServerHostName, was automatically applied to the KCD Server configuration (see [Figure 91-10](#)).

**Figure 91-10 KCD Server Configuration**

[Configuration](#) > [Remote Access VPN](#) > [Clientless SSL VPN Access](#) > [Advanced](#) > [Microsoft KCD Server](#) ☐

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

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

Kerberos Server Group for Constrained Delegation:

Server access credential

Username:  Password:

Server group configuration

Reactivation Mode: ☒ Depletion ☐ Timed

Dead time:  minutes

Max Failed Attempts:

Server table

| Server Name or IP Address | Interface | Timeout |
|---------------------------|-----------|---------|
| ServerHostName            | inside    | 10      |

**Step 3** Click **Apply**.

**Note**

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

To confirm if the ASA has successfully joined the domain, execute the following command from the ASA prompt as shown in [Figure 91-11](#):

```
show webvpn kcd
```

**Figure 91-11 ASA Domain Membership Confirmation**

```
HalfThrotle-1/pri/act# sho webvpn kcd
Kerberos Realm: WEST.LOCAL
Domain Join : Complete
=====
```

1500031

## Configuring Bookmarks to Access the Kerberos Authenticated Services

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

### Restriction

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

### Detailed Steps

- 
- |               |                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Navigate to <b>Configuration &gt; Remote Access VPN &gt; Clientless VPN Access &gt; Portal &gt; Bookmarks</b> on the ASDM GUI. |
| <b>Step 2</b> | In Bookmark List, enter the URL to reference for the service location.                                                         |
- 

## Configuring Application Access

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

- [Configuring Smart Tunnel Access](#)
- [Configuring Smart Tunnel Log Off](#)

## Configuring Smart Tunnel Access

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

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

- [About Smart Tunnels](#)
- [Why Smart Tunnels?](#)
- [Configuring a Smart Tunnel \(Lotus example\)](#)

- [Simplifying Configuration of Which Applications to Tunnel](#)
- [About Smart Tunnel Lists](#)
- [Creating a Smart Tunnel Auto Sign-On Server List](#)
- [Adding Servers to a Smart Tunnel Auto Sign-on Server List](#)
- [Enabling and Disabling Smart Tunnel Access](#)

## About Smart Tunnels

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

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

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

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

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

## Why Smart Tunnels?

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

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

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

### Prerequisites

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

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

- ActiveX or Oracle Java Runtime Environment (JRE) 4 update 15 or later (JRE 6 or later recommended) on Windows must be enabled on the browser.
- Only Winsock 2, TCP-based applications are eligible for smart tunnel access.

- For Mac OS X only, Java Web Start must be enabled on the browser.

### Restrictions

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

Proxy systems can be defined the client's configuration of static proxy entry or automatic configuration, or by a PAC file. Only static proxy configurations are currently supported by Smart Tunnels.

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

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

## Configuring a Smart Tunnel (Lotus example)

To configure a Smart Tunnel, perform the following steps:



### Note

These example instructions provide the minimum instructions required to add smart tunnel support for an application. See the field descriptions in the sections that follow for more information.

### Detailed Steps

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**.
- Step 2** Double-click the smart tunnel list to which you want to add an application; or click **Add** to create a list of applications, enter a name for this list in the List Name field, and click **Add**.  
For example, click **Add** in the Smart Tunnels pane, enter Lotus in the List Name field, and click **Add**.
- Step 3** Click **Add** in the Add or Edit Smart Tunnel List dialog box.
- Step 4** Enter a string in the Application ID field to serve as a unique index to the entry within the smart tunnel list.
- Step 5** Enter the filename and extension of the application into the Process Name dialog box.

[Table 91-5](#) shows example Application ID strings and the associated paths required to support Lotus.

**Table 91-5 Smart Tunnel Example: Lotus 6.0 Thick Client with Domino Server 6.5.5**

| Application ID Example | Minimum Required Process Name |
|------------------------|-------------------------------|
| lotusnotes             | notes.exe                     |
| lotusnlnotes           | nlnotes.exe                   |
| lotusntaskldr          | ntaskldr.exe                  |
| lotusnfileret          | nfileret.exe                  |

- Step 6** Select **Windows** next to OS.
- Step 7** Click **OK**.
- Step 8** Repeat Steps 3–7 for each application to add to the list.
- Step 9** Click **OK** in the Add or Edit Smart Tunnel List dialog box.
- Step 10** Assign the list to the group policies and local user policies to which you want to provide smart tunnel access to the associated applications, as follows:
- To assign the list to a group policy, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit > Portal** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.



- To assign the list to a local user policy, choose **Configuration > Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.

## Simplifying Configuration of Which Applications to Tunnel

A smart tunnel application list is essentially a filter of what applications are granted access to the tunnel. The default is to allow access for all processes started by the browser. With Smart Tunnel enabled bookmark, the clientless session grants access only to processes initiated by the web browser. For non-browser applications, an administrator can choose to tunnel all applications and thus remove the need to know which applications an end user may invoke. Table 91-6 shows in which situations processes are granted access.

**Table 91-6** Access for Smart Tunnel Applications and Enabled Bookmarks

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

### Restrictions

This configuration is applicable to Windows platforms only.

### Detailed Steps

Follow these steps to configure tunnel policy.

- Step 1** Choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**.
- Step 2** In the User Account window, highlight the username that you want to edit.
- Step 3** Click **Edit**. The Edit User Account window appears.
- Step 4** In the left sidebar of the Edit User Account window, click **VPN Policy > Clientless SSL VPN**.
- Step 5** Perform one of the following:
  - Check the **smart\_tunnel\_all\_applications** check box. All applications will be tunneled without making a list or knowing which executables an end user may invoke for external applications.
  - Or choose from the following tunnel policy options:
    - Uncheck the **Inherit** check box at the Smart Tunnel Policy parameter.

- Choose from the network list and specify one of the tunnel options: use smart tunnel for the specified network, do not use smart tunnel for the specified network, or use tunnel for all network traffic.

## Adding Applications to Be Eligible for Smart Tunnel Access

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

The Add or Edit Smart Tunnel entry dialog box lets you specify the attributes of an application in a smart tunnel list.

- 
- Step 1** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**, and choose a Smart Tunnel application list to edit, or add a new one.
- Step 2** For a new list, enter a unique name for the list of applications or programs. Do not use spaces.
- Following the configuration of the smart tunnel list, the list name appears next to the Smart Tunnel List attribute in the Clientless SSL VPN group policies and local user policies. Assign a name that will help you to distinguish its contents or purpose from other lists that you are likely to configure.
- Step 3** Click Add and add as many applications as you need to this smart tunnel list. The parameters are described below:
- **Application ID** - Enter a string to name the entry in the smart tunnel list. This user-specified name is saved and then returned onto the GUI. The string is unique for the operating system. It typically names the application to be granted smart tunnel access. To support multiple versions of an application for which you choose to specify different paths or hash values, you can use this attribute to differentiate entries, specifying the operating system, and name and version of the application supported by each list entry. The string can be up to 64 characters.
  - **Process Name** - Enter the filename or path to the application. The string can be up to 128 characters.
- Windows requires an exact match of this value to the right side of the application path on the remote host to qualify the application for smart tunnel access. If you specify only the filename for Windows, SSL VPN does not enforce a location restriction on the remote host to qualify the application for smart tunnel access.
- If you specify a path and the user installed the application in another location, that application does not qualify. The application can reside on any path as long as the right side of the string matches the value you enter.
- To authorize an application for smart tunnel access if it is present on one of several paths on the remote host, either specify only the name and extension of the application in this field; or create a unique smart tunnel entry for each path.

**Note**

A sudden problem with smart tunnel access may be an indication that a *Process Name* value is not up-to-date with an application upgrade. For example, the default path to an application sometimes changes following the acquisition of the company that produces the application and the next application upgrade.

For Windows, if you want to add smart tunnel access to an application started from the command prompt, you must specify “cmd.exe” in the Process Name of one entry in the smart tunnel list, and specify the path to the application itself in another entry, because “cmd.exe” is the parent of the application.

- OS - Click **Windows** or **Mac** to specify the host operating system of the application.
- Hash (Optional and only applicable to Windows) - To obtain this value, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at <http://support.microsoft.com/kb/841290/>. After installing FCIV, place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:/fciv.exe), then enter **fciv.exe -sha1 application** at the command line (for example, **fciv.exe -sha1 c:\msimn.exe**) to display the SHA-1 hash.

The SHA-1 hash is always 40 hexadecimal characters.

Before authorizing an application for smart tunnel access, clientless SSL VPN calculates the hash of the application matching the *Application ID*. It qualifies the application for smart tunnel access if the result matches the value of *Hash*.

Entering a hash provides a reasonable assurance that SSL VPN does not qualify an illegitimate file that matches the string you specified in the *Application ID*. Because the checksum varies with each version or patch of an application, the *Hash* you enter can only match one version or patch on the remote host. To specify a hash for more than one version of an application, create a unique smart tunnel entry for each *Hash* value.



**Note**

You must update the smart tunnel list in the future if you enter *Hash* values and you want to support future versions or patches of an application with smart tunnel access. A sudden problem with smart tunnel access may be an indication that the application list containing *Hash* values is not up-to-date with an application upgrade. You can avoid this problem by not entering a hash.

- Step 4** Click **OK** to save the application, and create how ever many applications you need for this smart tunnel list.
- Step 5** When you are done creating your smart tunnel list, you must assign it to a group policy or a local user policy for it to become active, as follows:
- To assign the list to a group policy, choose **Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add or Edit > Portal** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.
  - To assign the list to a local user policy, choose **Config > Remote Access VPN> AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.

**Table 91-7 Example Smart Tunnel Entries**

| Smart Tunnel Support       | Application ID<br>(Any unique string<br>is OK.) | Process Name | OS      |
|----------------------------|-------------------------------------------------|--------------|---------|
| Mozilla Firefox.           | firefox                                         | firefox.exe  | Windows |
| Microsoft Outlook Express. | outlook-express                                 | msimn.exe    | Windows |

**Table 91-7**      **Example Smart Tunnel Entries**

| Smart Tunnel Support                                                                                                                                                   | Application ID<br>(Any unique string<br>is OK.) | Process Name                             | OS      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|------------------------------------------|---------|
| More restrictive alternative—Microsoft Outlook Express only if the executable file is in a predefined path.                                                            | outlook-express                                 | \Program Files\Outlook Express\msimn.exe | Windows |
| Open a new Terminal window on a Mac. (Any subsequent application launched from within the same Terminal window fails because of the one-time-password implementation.) | terminal                                        | Terminal                                 | Mac     |
| Start smart tunnel for a new window                                                                                                                                    | new-terminal                                    | Terminal open -a MacTelnet               | Mac     |
| Start application from a Mac Terminal window.                                                                                                                          | curl                                            | Terminal curl www.example.com            | Mac     |

## About Smart Tunnel Lists

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

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

### Restrictions

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

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

The Smart Tunnel Auto Sign-on Server List dialog box lets you add or edit lists of servers which will automate the submission of login credentials during smart tunnel setup. Auto Sign-on over a smart tunnel is available for Internet Explorer and Firefox.

- 
- Step 1**      Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**, and make sure Smart Tunnel Auto Sign-on Server List is expanded to display.
- Step 2**      Click **Add**, and enter a unique name for a list of remote servers that will help you to distinguish its contents or purpose from other lists that you are likely to configure. The string can be up to 64 characters. Do not use spaces.
- 

After you create a smart tunnel auto sign-on list, that list name appears next to the Auto Sign-on Server List attribute under Smart Tunnel in the clientless SSL VPN group policy and local user policy configurations.

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

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

- Step 1** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**, select one of the lists, and click **Edit**.
- Step 2** Click the **Add** button on the Add Smart Tunnel Auto Sign-on Server List dialog to add one more more server smart tunnel servers.
- Step 3** Enter the hostname or IP address of the server to auto-authenticate to:
- If you select Hostname, enter a hostname or wildcard mask to auto-authenticate to. You can use the following wildcard characters:
    - \* to match any number of characters or zero characters
    - ? to match any single character
    - [] to match any single character in the range expressed inside the brackets
    - For example, enter \*.example.com. Using this option protects the configuration from dynamic changes to IP addresses.
  - If you select IP Address, enter an IP address.



**Note** Firefox does not support a host mask with wild cards, a subnet using IP addresses, or a netmask; you must use an exact host name or IP address. For example, within Firefox, if you enter \*.cisco.com, auto sign-on to host email.cisco.com will fail.

- Step 4** Windows Domain (Optional) - Click to add the Windows domain to the username, if authentication requires it. If you do so, be sure to specify the domain name when assigning the smart tunnel list to one or more group policies or local user policies.

- Step 5** HTTP-based Auto Sign-On (Optional)

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

Use the address format used in the source code of the web pages on the intranet. If you are configuring smart tunnel auto sign-on for browser access and some web pages use host names and others use IP addresses, or you do not know, specify both in different smart tunnel auto sign-on entries. Otherwise, if a link on a web page uses a different format than the one you specify, it fails when the user clicks it.



**Note** If administrators do not know the corresponding realm, they should perform logon once and get the string from the prompt dialog.

- Port Number - Specify a port number for the corresponding hosts. For Firefox, if no port number is specified, auto sign-on is performed on HTTP and HTTPS, accessed by default port numbers 80 and 443 respectively.

- Step 6** Click **OK**.

- Step 7** Following the configuration of the smart tunnel auto sign-on server list, you must assign it to a group policy or a local user policy for it to become active, as follows:

- To assign the list to a group policy:
    1. Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**, and open a group policy,
    2. Select the Portal tab, find the Smart Tunnel area, and choose the auto sign-on server list from the drop-down list next to the Auto Sign-on Server List attribute.
  - To assign the list to a local user policy:
    1. choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**, and edit the local user you want to assign an auto sign-on server list to.
    2. Navigate to VPN Policy > Clientless SSL VPN, and find the Auto Sign-on Server setting under the Smart Tunnel area
    3. Uncheck Inherit, and choose a server list from the drop-down list next to the Auto Sign-on Server List attribute.
- 

## Enabling and Disabling Smart Tunnel Access

By default, smart tunnels are disabled.

If you enable smart tunnel access, the user will have to start it manually, using the **Application Access > Start Smart Tunnels** button on the clientless SSL VPN portal page.

## Configuring Smart Tunnel Log Off

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



### Note

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

---

## When Its Parent Process Terminates

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



### Note

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

---

## With A Notification Icon

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



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

### Detailed Steps

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

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



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

## Configuring Port Forwarding

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

- [Information About Port Forwarding, page 91-55](#)
- [Configuring DNS for Port Forwarding](#)
- [Adding Applications to Be Eligible for Port Forwarding](#)
- [Adding/Editing Port Forwarding Entry](#)
- [Assigning a Port Forwarding List](#)
- [Enabling and Disabling Port Forwarding](#)

## Information About Port Forwarding

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

- Lotus Notes
- Microsoft Outlook Express
- Perforce

- Sametime
- Secure FTP (FTP over SSH)
- SSH
- TELNET
- Windows Terminal Service

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

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

Consider the following alternatives to port forwarding:

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

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

#### Prerequisites

- Refer to the [Supported VPN Platforms, Cisco ASA 5500 Series](#) compatibility guide for port forwarding pre-requisites.
- Browser-based users of Safari on Mac OS X 10.5.3 must identify a client certificate for use with the URL of the ASA, once with the trailing slash and once without it, because of the way Safari interprets URLs. For example,
  - <https://example.com/>
  - <https://example.com>

For details, go to the [Safari, Mac OS X 10.5.3: Changes in client certificate authentication](#).

- Users of Microsoft Windows Vista or later who use port forwarding or smart tunnels must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the **Tools > Internet Options > Security** tab. Vista (or later) users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer's vulnerability to attack.

#### Restrictions

- Port forwarding supports only TCP applications that use static TCP ports. Applications that use dynamic ports or multiple TCP ports are not supported. For example, SecureFTP, which uses port 22, works over clientless SSL VPN port forwarding, but standard FTP, which uses ports 20 and 21, does not.
- Port forwarding does not support Microsoft Outlook Exchange (MAPI) proxy. However, you can configure smart tunnel support for Microsoft Office Outlook in conjunction with Microsoft Outlook Exchange Server.
- A stateful failover does not retain sessions established using Application Access (either port forwarding or smart tunnel access). Users must reconnect following a failover.

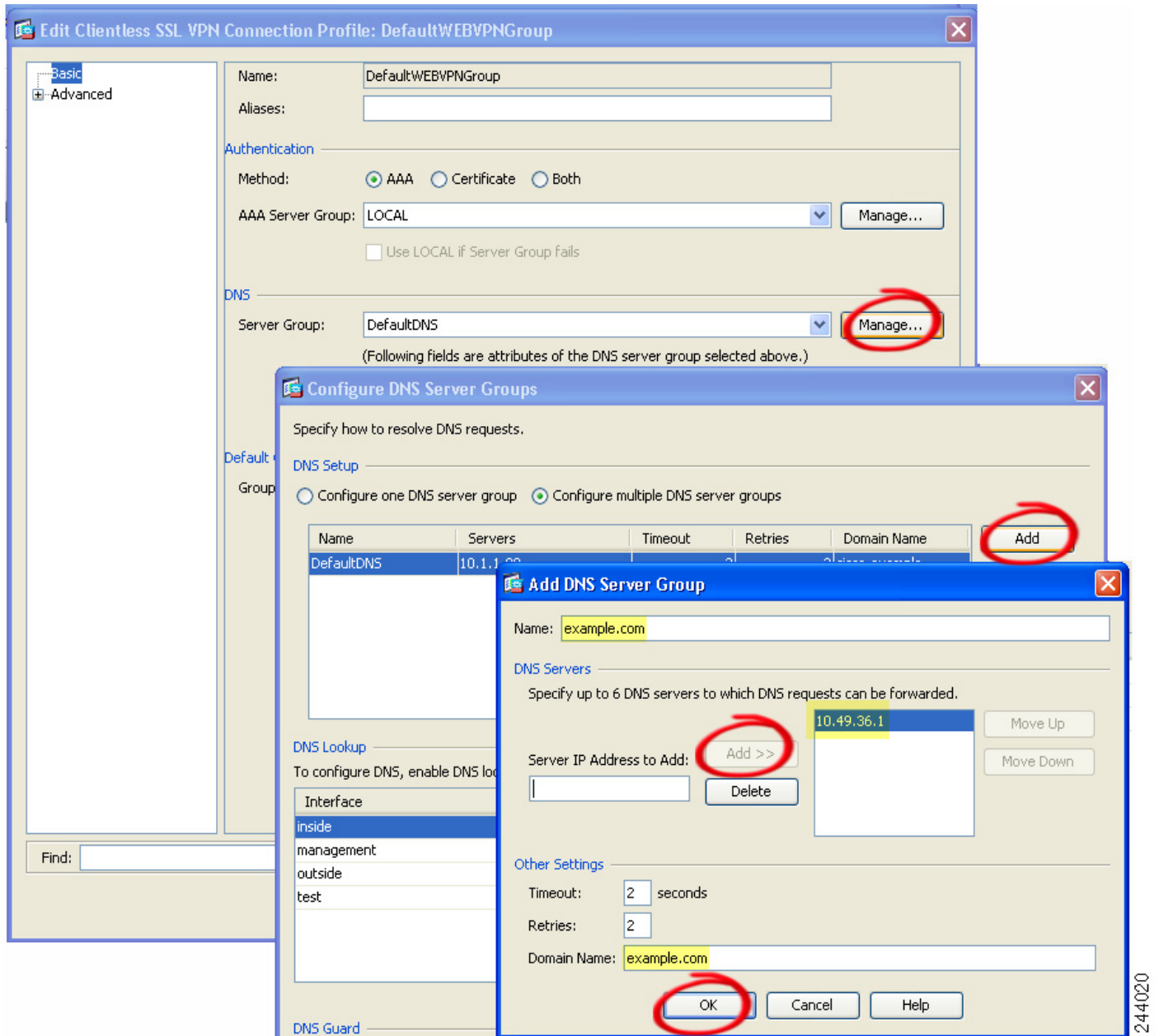


- The Java applet displays in its own window on the end user HTML interface. It shows the contents of the list of forwarded ports available to the user, as well as which ports are active, and amount of traffic in bytes sent and received.
- The port forwarding applet displays the local port and the remote port as the same when the local IP address 127.0.0.1 is being used and cannot be updated by the clientless SSL VPN connection from the ASA. As a result, the ASA creates new IP addresses 127.0.0.2, 127.0.0.3, and so on for local proxy IDs. Because you can modify the hosts file and use different loopbacks, the remote port is used as the local port in the applet. To connect, you can use Telnet with the host name, without specifying the port. The correct local IP addresses are available in the local hosts file.

## Configuring DNS for Port Forwarding

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

- 
- Step 1** Click **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.  
The DefaultWEBVPNGroup entry is the default connection profile used for clientless connections.
- Step 2** Highlight the DefaultWEBVPNGroup entry, then click **Edit** if your configuration uses it for clientless connections. Otherwise, highlight a connection profile used in your configuration for clientless connections, then click **Edit**.  
The Basic window opens.
- Step 3** Scan to the DNS area and select the DNS server from the drop-down list. Note the domain name, disregard the remaining steps, and go to the next section if ASDM displays the DNS server you want to use. You need to enter the same domain name when you specify the remote server while configuring an entry in the port forwarding list. Continue with the remaining steps if the DNS server is not present in the configuration.
- Step 4** Click **Manage** in the DNS area.  
The Configure DNS Server Groups window opens.
- Step 5** Click **Configure Multiple DNS Server Groups**.  
A window displays a table of DNS server entries.
- Step 6** Click **Add**.  
The Add DNS Server Group window opens.
- Step 7** Enter a new server group name in the Name field, and enter the IP address and domain name (see [Figure 91-12](#)).

**Figure 91-12** Example DNS Server Values for Port Forwarding

Note the domain name you entered. You need it when you specify the remote server later while configuring a port forwarding entry.

- Step 8** Click **OK** until the Connection Profiles window becomes active again.
- Step 9** Repeat Steps 2–8 for each remaining connection profile used in your configuration for clientless connections.
- Step 10** Click **Apply**.

## Adding Applications to Be Eligible for Port Forwarding

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

Following the configuration of a port forwarding list, assign the list to group policies or usernames, as described in the next section.

## Adding/Editing Port Forwarding Entry

The Add/Edit Port Forwarding Entry dialog boxes let you specify TCP applications to associate with users or group policies for access over clientless SSL VPN connections. Assign values to the attributes in these windows as follows:

### Prerequisites

The DNS name assigned to the Remote Server parameter must match the Domain Name and Server Group parameters to establish the tunnel and resolve to an IP address, per the instructions in the [“Assigning a Port Forwarding List” section on page 91-59](#). The default setting for both the Domain and Server Group parameters is DefaultDNS.

### Detailed Steps

- 
- |               |                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Click <b>Add</b> .                                                                                                                                                                                    |
| <b>Step 2</b> | Type a TCP port number for the application to use. You can use a local port number only once for a listname. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535. |
| <b>Step 3</b> | Enter either the domain name or IP address of the remote server. We recommend using a domain name so that you do not have to configure the client applications for the specific IP address.           |
| <b>Step 4</b> | Type the well-known port number for the application.                                                                                                                                                  |
| <b>Step 5</b> | Type a description of the application. The maximum is 64 characters.                                                                                                                                  |
| <b>Step 6</b> | (Optional) Highlight a port forwarding list and click <b>Assign</b> to assign the selected list to one or more group policies, dynamic access policies, or user policies.                             |
- 

## 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.
- Enable port forwarding access upon user login, but require the user to start it manually, using the **Application Access > Start Applications** button on the clientless SSL VPN Portal Page.

**Note**

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

**Detailed Steps**

The Add or Edit Port Forwarding List dialog box lets you add or edit the following:

- 
- Step 1** Provide an alphanumeric name for the list. The maximum is 64 characters.
- Step 2** Enter which local port listens for traffic for the application. You can use a local port number only once for a listname. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

**Note**

Enter the IP address or DNS name of the remote server. We recommend using a domain name so that you do not have to configure the client applications for the specific IP address.

- Step 3** Enter the remote port that listens for traffic for the application.
- Step 4** Describe the TCP application. The maximum is 64 characters.
- For details, go to the section that addresses the option you want to use.
- 

## Enabling and Disabling Port Forwarding

By default, port forwarding is disabled.

If you enable port forwarding, the user will have to start it manually, using the **Application Access > Start Applications** button on the clientless SSL VPN portal page.

## Configuring the Use of External Proxy Servers

Use the Proxies pane to configure the ASA to use external proxy servers to handle HTTP requests and HTTPS requests. These servers act as an intermediary between users and the Internet. Requiring all Internet access via servers you control provides another opportunity for filtering to assure secure Internet access and administrative control.

**Restrictions**

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

**Detailed Steps**

- 
- Step 1** Click Use an HTTP proxy server.
- Step 2** Identify the HTTP proxy server by its IP address or hostname.
- Step 3** Enter the hostname or IP address of the external HTTP proxy server.
- Step 4** Enter the port that listens for HTTP requests. The default port is 80.
- Step 5** (Optional) Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the HTTP proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards:

- \* to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string.
  - ? to match any single character, including slashes and periods.
  - [x-y] to match any single character in the range of *x* and *y*, where *x* represents one character and *y* represents another character in the ANSI character set.
  - [!x-y] to match any single character that is not in the range.
- Step 6** (Optional) Enter this keyword to accompany each HTTP proxy request with a username to provide basic, proxy authentication.
- Step 7** Enter a password to send to the proxy server with each HTTP request.
- Step 8** As an alternative to specifying the IP address of the HTTP proxy server, you can choose Specify PAC file URL to specify a Proxy autoconfiguration file to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL. Enter **http://** and type the URL of the proxy autoconfiguration file into the adjacent field. If you omit the **http://** portion, the ASA ignores it.
- Step 9** Choose if you want to use an HTTPS proxy server.
- Step 10** Click to identify the HTTPS proxy server by its IP address or hostname.
- Step 11** Enter the hostname or IP address of the external HTTPS proxy server.
- Step 12** Enter the port that listens for HTTPS requests. The default port is 443.
- Step 13** (Optional) Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the HTTPS proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards:
- \* to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string.
  - ? to match any single character, including slashes and periods.
  - [x-y] to match any single character in the range of *x* and *y*, where *x* represents one character and *y* represents another character in the ANSI character set.
  - [!x-y] to match any single character that is not in the range.
- Step 14** (Optional) Enter this keyword to accompany each HTTPS proxy request with a username to provide basic, proxy authentication.
- Step 15** Enter a password to send to the proxy server with each HTTPS request.
- 

## SSO Servers

The SSO Server pane lets you configure or delete single sign-on (SSO) for users of clientless SSL VPN connecting to a Computer Associates SiteMinder SSO server or to a Security Assertion Markup Language (SAML), Version 1.1, Browser Post Profile SSO server. SSO support, available only for clientless SSL VPN, lets users access different secure services on different servers without entering a username and password more than once.

You can choose from four methods when configuring SSO: Auto Signon using basic HTTP and/or NTLMv1 authentication, HTTP Form protocol, or Computer Associates eTrust SiteMinder (formerly Netegrity SiteMinder), or SAML, Version 1.1 Browser Post Profile.

**Restrictions**

The SAML Browser Artifact profile method of exchanging assertions is not supported.

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

- [Configuring SiteMinder and SAML Browser Post Profile, page 91-62](#)—configures SSO with basic HTTP or NTLM authentication.
- [Configuring Session Settings](#) —configures SSO with the HTTP Form protocol.

The SSO mechanism either starts as part of the AAA process (HTTP Forms) or just after successful user authentication to either a AAA server (SiteMinder) or a SAML Browser Post Profile server. In these cases, the clientless SSL VPN server running on the ASA acts as a proxy for the user to the authenticating server. When a user logs in, the clientless SSL VPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS.

If the authenticating server approves the authentication request, it returns an SSO authentication cookie to the clientless SSL VPN server. This cookie is kept on the ASA on behalf of the user and used to authenticate the user to secure websites within the domain protected by the SSO server.

## Configuring SiteMinder and SAML Browser Post Profile

SSO authentication with SiteMinder or with SAML Browser Post Profile is separate from AAA and occurs after the AAA process completes. To set up SiteMinder SSO for a user or group, you must first configure a AAA server (RADIUS, LDAP and so forth). After the AAA server authenticates the user, the clientless SSL VPN server uses HTTPS to send an authentication request to the SiteMinder SSO server.

In addition to configuring the ASA, for SiteMinder SSO, you also must configure your CA SiteMinder Policy Server with the Cisco authentication scheme. See [Adding the Cisco Authentication Scheme to SiteMinder](#).

For SAML Browser Post Profile you must configure a Web Agent (Protected Resource URL) for authentication.

**Detailed Steps**

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

- **Server Name**—*Display only*. Displays the names of configured SSO Servers. The minimum number of characters is 4, and the maximum is 31.
- **Authentication Type**—*Display only*. Displays the type of SSO server. The ASA currently supports the SiteMinder type and the SAML Browser Post Profile type.
- **URL**—*Display only*. Displays the SSO server URL to which the ASA makes SSO authentication requests.
- **Secret Key**—*Display only*. Displays the secret key used to encrypt authentication communications with the SSO server. The key can be comprised of any regular or shifted alphanumeric character. There is no minimum or maximum number of characters.
- **Maximum Retries**—*Display only*. Displays the number of times the ASA retries a failed SSO authentication attempt. The range is 1 to 5 retries, and the default number of retries is 3.
- **Request Timeout (seconds)**—*Display only*. Displays the number of seconds before a failed SSO authentication attempt times out. The range is 1 to 30 seconds, and the default number of seconds is 5.

- Add/Edit—Opens the Add/Edit SSO Server dialog box.
- Delete—Deletes the selected SSO server.
- Assign—Highlight an SSO server and click this button to assign the selected server to one or more VPN group policies or user policies.

- 
- Step 1** Configure the SAML server parameters to represent the asserting party (the ASA):
- Recipient consumer (Web Agent) URL (same as the assertion consumer URL configured on the ASA)
  - Issuer ID, a string, usually the hostname of appliance
  - Profile type -Browser Post Profile
- Step 2** Configure certificates.
- Step 3** Specify that asserting party assertions must be signed.
- Step 4** Select how the SAML server identifies the user:
- Subject Name Type is DN
  - Subject Name format is uid=<user>
- 

## Adding the Cisco Authentication Scheme to SiteMinder

Besides configuring the ASA for SSO with SiteMinder, you must also configure your CA SiteMinder Policy Server with the Cisco authentication scheme, provided as a Java plug-in. This section presents general tasks, not a complete procedure. Refer to the CA SiteMinder documentation for the complete procedure for adding a custom authentication scheme. To configure the Cisco authentication scheme on your SiteMinder Policy Server, perform the following steps:

### Prerequisites

Configuring the SiteMinder Policy Server requires experience with SiteMinder.

### Detailed Steps

- 
- Step 1** With the Siteminder Administration utility, create a custom authentication scheme being sure to use the following specific arguments:
- In the Library field, enter **smjavaapi**.
  - In the Secret field, enter the same secret configured in the Secret Key field of the Add SSO Server dialog to follow.
  - In the Parameter field, enter **CiscoAuthApi**.
- Step 2** Using your Cisco.com login, download the file **cisco\_vpn\_auth.jar** from <http://www.cisco.com/cisco/software/navigator.html> and copy it to the default library directory for the SiteMinder server. This .jar file is also available on the Cisco ASA CD.
-

## Adding or Editing SSO Servers

This SSO method uses CA SiteMinder and SAML Browser Post Profile. You can also set up SSO using the HTTP Form protocol, or Basic HTML and NTLM authentication. To use the HTTP Form protocol, see [Configuring Session Settings](#). To set use basic HTML or NTLM authentication, use the **auto-signon** command at the command line interface.



**Note** NTLM is not the most secure choice and other better alternatives exist. NTLM does not support recent cryptographic methods such as AES or SHA-256. Cisco recommends that applications not use NTLM.

### Detailed Steps

- Step 1** If adding a server, enter the name of the new SSO server. If editing a server, this field is display only; it displays the name of the selected SSO server.
- Step 2** *Display only.* Displays the type of SSO server. The types currently supported by the ASA are SiteMinder and SAML Browser Post Profile.
- Step 3** Enter a secret key used to encrypt authentication requests to the SSO server. Key characters can be any regular or shifted alphanumeric characters. There is no minimum or maximum number of characters. The secret key is similar to a password: you create it, save it, and configure it. It is configured on the ASA, the SSO server, and the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.
- Step 4** Enter the number of times the ASA retries a failed SSO authentication attempt before the authentication times-out. The range is from 1 to 5 retries inclusive, and the default is 3 retries.
- Step 5** Enter the number of seconds before a failed SSO authentication attempt times out. The range is from 1 to 30 seconds inclusive, and the default is 5 seconds.

## Application Access User Notes

The following sections provide information about using application access:

- [Closing Application Access to Prevent hosts File Errors](#)
- [Closing Application Access to Prevent hosts File Errors](#)
- [Recovering from hosts File Errors When Using Application Access](#)

## Closing Application Access to Prevent hosts File Errors

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

## Recovering from hosts File Errors When Using Application Access

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



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

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

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

This section includes the following topics:

- [Understanding the hosts File](#)
- [Stopping Application Access Improperly](#)
- [Reconfiguring a Host's File Automatically Using Clientless SSL VPN](#)
- [Reconfiguring hosts File Manually](#)

## Understanding the hosts File

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

|                                       |                                                                                                                                                                                                                                                                |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Before invoking Application Access... | hosts file is in original state.                                                                                                                                                                                                                               |
| When Application Access starts....    | <ul style="list-style-type: none"> <li>• Clientless SSL VPN copies the hosts file to <code>hosts.webvpn</code>, thus creating a backup.</li> <li>• Clientless SSL VPN then edits the hosts file, inserting clientless SSL VPN-specific information.</li> </ul> |
| When Application Access stops...      | <ul style="list-style-type: none"> <li>• Clientless SSL VPN copies the backup file to the <code>hosts</code> file, thus restoring the hosts file to its original state.</li> <li>• Clientless SSL VPN deletes <code>hosts.webvpn</code>.</li> </ul>            |
| After finishing Application Access... | hosts file is in original state.                                                                                                                                                                                                                               |



### Note

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

## Stopping Application Access Improperly

When Application Access terminates abnormally, the `hosts` file remains in a clientless SSL VPN-customized state. Clientless SSL VPN checks the state the next time you start Application Access by searching for a `hosts.webvpn` file. If it finds one, a `Backup HOSTS File Found` error message (Figure 91-13) appears, and Application Access is temporarily disabled.

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

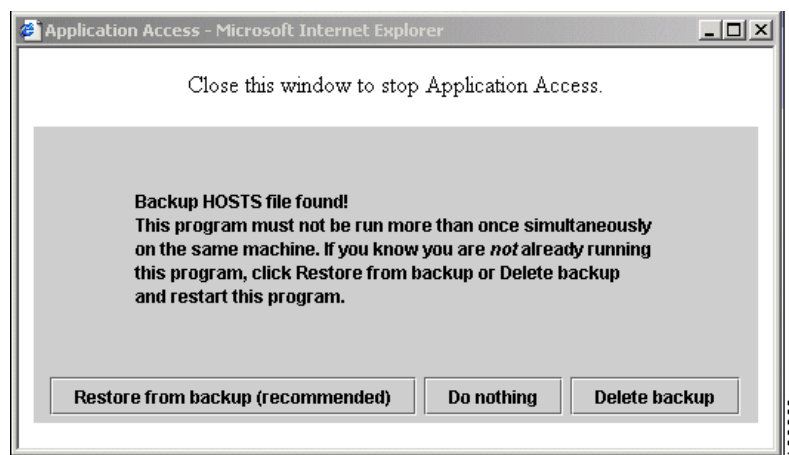
## Reconfiguring a Host's File Automatically Using Clientless SSL VPN

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

### Detailed Steps

- 
- Step 1** Start clientless SSL VPN and log in. The home page opens.
- Step 2** Click the **Applications Access** then **Start Applications**, a `Backup HOSTS File Found` message appears. (See Figure 91-13.)

**Figure 91-13** Backup HOSTS File Found Message



- Step 3** Choose one of the following options:
- **Restore from backup**—Clientless SSL VPN forces a proper shutdown. It copies the `hosts.webvpn` backup file to the `hosts` file, restoring it to its original state, then deletes `hosts.webvpn`. You then have to restart Application Access.
  - **Do nothing**—Application Access does not start. The remote access home page reappears.
  - **Delete backup**—Clientless SSL VPN deletes the `hosts.webvpn` file, leaving the `hosts` file in its clientless SSL VPN-customized state. The original `hosts` file settings are lost. Application Access then starts, using the clientless SSL VPN-customized `hosts` file as the new original. Choose this

option only if you are unconcerned about losing hosts file settings. If you or a program you use might have edited the hosts file after Application Access has shut down improperly, choose one of the other options, or edit the hosts file manually. (See [“Reconfiguring hosts File Manually.”](#))

## Reconfiguring hosts File Manually

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

### Detailed Steps

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

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

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward

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

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

**Step 4** Save and close the file.

**Step 5** Start clientless SSL VPN and log in.

The home page appears.

**Step 6** Click the **Application Access** link.

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

## Configuring File Access

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

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

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

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

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

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

**Note**

---

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

---

## CIFS File Access Requirement and Limitation

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

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

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

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

## Adding Support for File Access

Configure file access as follows:

**Note**

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

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

For a complete description of these commands, see the *Cisco Security Appliance Command Reference*.

## Ensuring Clock Accuracy for SharePoint Access

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

## Customizing the Clientless SSL VPN User Experience

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

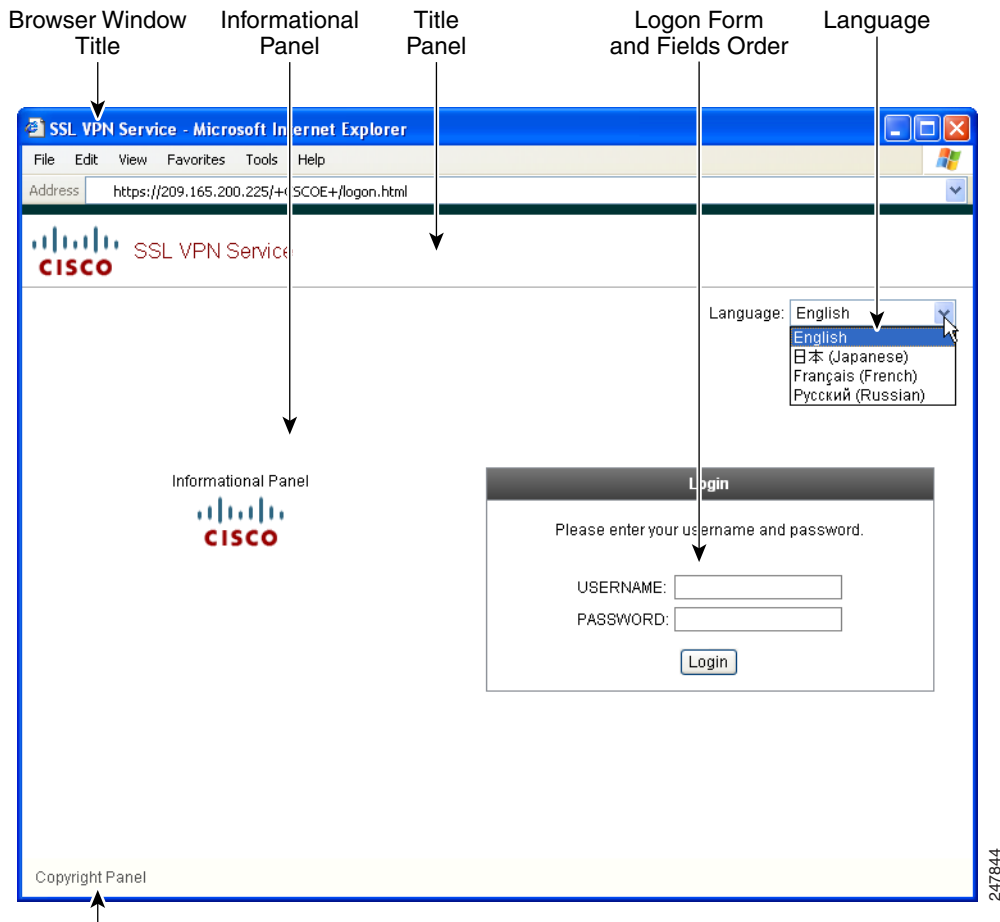
Rather than customizing the pre-defined components of the logon page, you can create your own page and import it to the ASA for full customization. To do this see the [“Replacing the Logon Page with your own Fully Customized Page”](#) section on page 91-71.

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

- [Customizing the Logon Page with the Customization Editor, page 91-69](#)
- [Replacing the Logon Page with your own Fully Customized Page, page 91-71](#)

## Customizing the Logon Page with the Customization Editor

[Figure 91-14](#) shows the logon page and the pre-defined components you can customize:

**Figure 91-14 Components of Clientless Logon Page**

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

- Step 1** Specify pre-defined customization. Go to Logon Page and select **Customize pre-defined logon page components**. Specify a title for the browser window.
- Step 2** Display and customize the title panel. Go to Logon Page > Title Panel and check **Display title panel**. Enter text to display as the title and specify a logo. Specify any font styles.
- Step 3** Specify language options to display. Go to Logon Page > Language and check **Enable Language Selector**. Add or delete any languages to display to remote users. Languages in the list require translation tables that you configure in Configuration > Remote Access VPN > Language Localization.
- Step 4** Customize the logon form. Go to Logon Page > Logon Form. Customize the text of the form and the font style in the panel. The secondary password field appears to users only if a secondary authentication server is configured in the connection profile.
- Step 5** Arrange the position of the logon form fields. Go to Logon Page > Form Fields Order. Use the up and down arrow buttons to change the order that the fields are displayed.
- Step 6** Add messages to users. Go to Logon Page > Informational Panel and check **Display informational panel**. Add text to display in the panel, change the position of the panel relative to the logon form, and specify a logo to display in this panel.

- Step 7** Display a copyright statement. Go to Logon Page > Copyright Panel and check **Display copyright panel**. Add text to display for copyright purposes.
- Step 8** Click **OK**, then apply the changes to the customization object you edited.
- 

## Replacing the Logon Page with your own Fully Customized Page

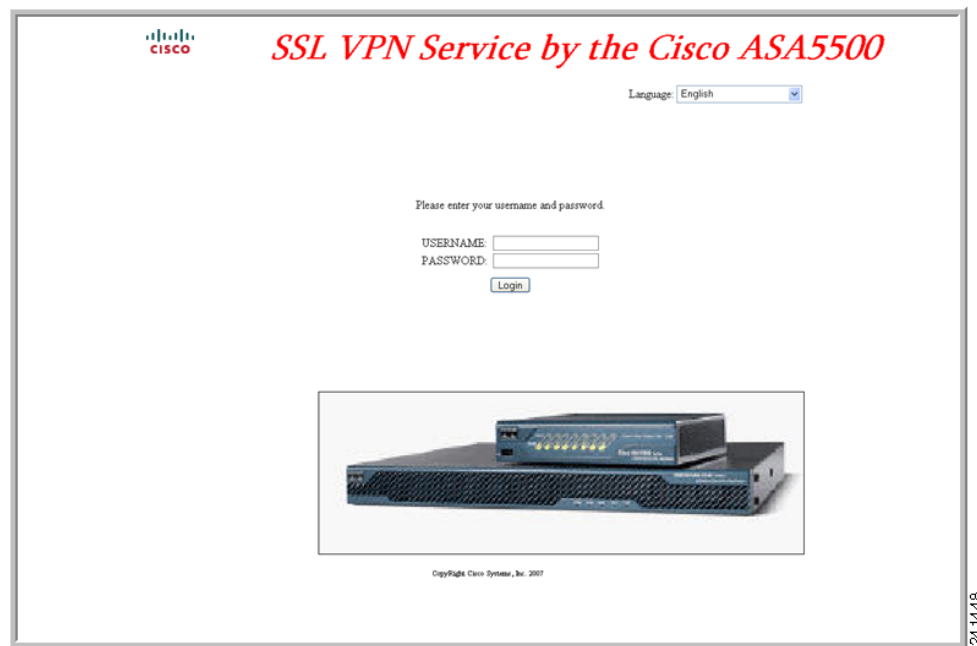
If you prefer to use your own, custom login screen, rather than changing specific components of the logon page we provide, you can perform this advanced customization using the Full Customization feature.

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

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

Figure 91-15 shows a simple example of a custom login screen enabled by the Full Customization feature.

**Figure 91-15** Example of Full Customization of Logon Page



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

- [Creating the Custom Login Screen File](#)
- [Importing the File and Images](#)
- [Configuring the Security Appliance to use the Custom Login Screen](#)

## Creating the Custom Login Screen File

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

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

<p align="center">
<font face="Snap
ITC" size="6" color="#FF00FF">
 <i> SSL VPN Service by the Cisco
ASA5500</i></p>

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

<table>

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

</td></tr>

</table>
```

The indented code injects the Login form and the Language Selector on the screen. The function **cscs\_ShowLoginForm('lform')** injects the logon form. **cscs\_ShowLanguageSelector('selector')** injects the Language Selector.

Follow these steps to modify your HTML file:

- 
- Step 1** Name your file **logon.inc**. When you import the file, the ASA recognizes this filename as the logon screen.
  - Step 2** Modify the paths of images used by the file to include **/+CSCOU+/.** Files that are displayed to remote users before authentication must reside in a specific area of the ASA cache memory represented by the path **/+CSCOU+/.** Therefore, the source for each image in the file must include this path. For example:

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



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

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

<table>

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

</td></tr>

</table>
```

## Importing the File and Images

Follow these steps to import your HTML file and any images to the ASA:

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

## Configuring the Security Appliance to use the Custom Login Screen

Follow these steps to enable the ASA to use the new login screen in a customization object:

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

- Step 4** Click Manage to import your logon page file. The Import Web Content window displays.
- Step 5** In the Destination area, select **No** to ensure your logon page is visible to users before they authenticate.
- Step 6** Back in the Edit Customization Object window, click General and enable the customization object for the connection profile and/or group policies you desire.
- 

## Using Clientless SSL VPN with PDAs

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

Cisco has certified the following PDA platform:

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

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

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

### Restrictions

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

## Using E-Mail over Clientless SSL VPN

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

- [Configuring E-mail Proxies](#)

- [Configuring Web E-mail: MS Outlook Web App](#)

## Configuring E-mail Proxies

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

### Restrictions

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

1 With the Eudora e-mail client, SMTPS works only on port 465, even though the default port for SMTPS connections is 988.

## Configuring Web E-mail: MS Outlook Web App

The ASA supports Microsoft Outlook Web App to Exchange Server 2010 and Microsoft Outlook Web Access to Exchange Server 2007, 2003, and 2000. OWA requires that users perform the following steps:

### Detailed Steps

- 
- |               |                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Enter the URL of the e-mail service into the address field or click an associated bookmark in the clientless SSL VPN session. |
| <b>Step 2</b> | When prompted, enter the e-mail server username in the format <i>domain\username</i> .                                        |
| <b>Step 3</b> | Enter the e-mail password.                                                                                                    |
- 

## Configuring Portal Access Rules

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

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

### Prerequisites

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

```
hostname(config)#
```

### Detailed Steps

- 
- |               |                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Start ASDM and select <b>Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Portal Access Rule</b> . |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|

The Portal Access Rule window opens.

**Step 2** Click **Add** to create a portal access rule or select an existing rule and click **Edit**.

The Add (or Edit) Portal Access Rule dialog box opens.

**Step 3** Enter a rule number from 1-65535 in the Rule Priority field.

Rules are processed in order of priority from 1-65535.

**Step 4** In the User Agent field, enter the name of the user agent you want to find in the HTTP header.

- Surround the string with wildcards (\*) to generalize the string; for example, \*Thunderbird\*. We recommend using wildcards in your search string. Without wildcards, the rule may not match any strings or it may match many fewer strings than you expect.
- If your string contains a space, ASDM automatically adds quotes to the beginning and end of the string when it saves the rule. For example, if you enter `my agent`, ASDM will save the string as `"my agent"`. ASA will then search for matches of `my agent`.

Do not add quotes to a string with spaces yourself unless you want ASA to match the quotes you added to the string. For example, if you enter `"my agent"` ASDM will save the string as `"\"my agent\""` and try to find a match for `"my agent"` and it will not find `my agent`.

- If you want to use wildcards with a string that contains a space, start and end the entire string with wildcards, for example, `*my agent*` and ASDM will automatically surround that string with quotes when it saves the rule.

**Step 5** In the Action field, select either **Deny** or **Permit**.

The ASA will deny or permit a clientless SSL VPN connection based on this setting.

**Step 6** Enter an HTTP message code in the Returned HTTP Code field.

The HTTP message number 403 is pre-populated in the field and is the default value for portal access rules. The allowed range of message codes is 200-599.

**Step 7** Click **OK**.

**Step 8** Click **Apply**.

## Using Proxy Bypass

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

You can configure multiple proxy bypass entries. The order in which you configure them is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the ASA. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

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

### Detailed Steps

You can set rules for when the ASA performs little or no content rewriting:

- 
- Step 1** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Proxy Bypass**.
- Step 2** Select the Interface name for proxy bypass.
- Step 3** Specify either a port or a URI for proxy bypass:
- Port—(radio button) Click to use a port for proxy bypass. The valid port numbers are 20000-21000.
  - Port (field)—Enter a high-numbered port for the ASA to reserve for proxy bypass.
  - Path Mask—(radio button) Click to use a URL for proxy bypass.
  - Path Mask—(Field) Enter a URL for proxy bypass. It can contain a regular expression.
- Step 4** Define target URLs for proxy bypass:
- URL—(drop-down list) Click either http or https as the protocol.
  - URL (text field)—Enter a URL to which you want to apply proxy bypass.
- Step 5** Specify the content to rewrite. The choices are none or a combination of XML, links, and cookies.
- XML—Check to rewrite XML content.
  - Hostname—Check to rewrite links.
- 

## Clientless SSL VPN End User Setup

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

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

- [Defining the End User Interface](#)
- [Customizing Clientless SSL VPN Pages, page 91-80](#)
- [Customizing Help, page 91-127](#)
- [Requiring Usernames and Passwords](#)
- [Communicating Security Tips](#)
- [Configuring Remote Systems to Use Clientless SSL VPN Features](#)

## Defining the End User Interface

The clientless SSL VPN end user interface consists of a series of HTML panels. A user logs on to clientless SSL VPN by entering the IP address of an ASA interface in the format `https://address`. The first panel that displays is the login screen ([Figure 91-16](#)).

**Figure 91-16** Clientless SSL VPN Login Screen

SSL VPN Service

Login

Please enter your username and password.

USERNAME:

PASSWORD:

Login

191936

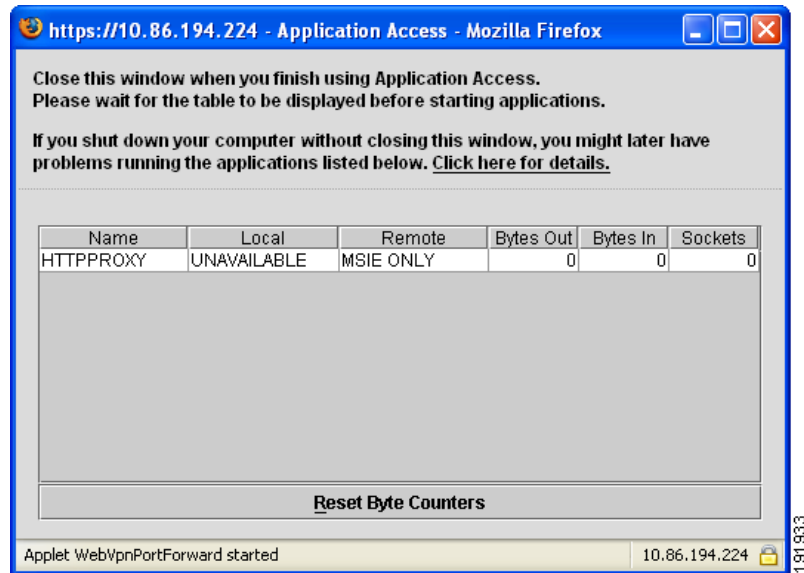
## Viewing the Clientless SSL VPN Home Page

After the user logs in, the portal page opens.

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

## Viewing the Clientless SSL VPN Application Access Panel

To start port forwarding or smart tunnels, a user clicks the **Go** button in the Application Access box. The Application Access window opens ([Figure 91-17](#)).

**Figure 91-17** Clientless SSL VPN Application Access Window

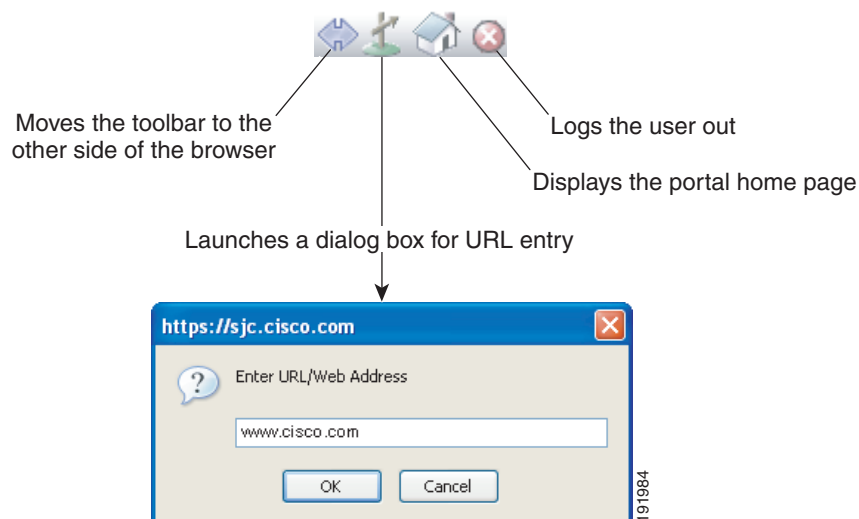
This window displays the TCP applications configured for this clientless SSL VPN connection. To use an application with this panel open, the user starts the application in the normal way.

**Note**

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

## Viewing the Floating Toolbar

The floating toolbar shown in [Figure 91-18](#) represents the current clientless SSL VPN session.

**Figure 91-18** Clientless SSL VPN Floating Toolbar

Be aware of the following characteristics of the floating toolbar:

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

See [Table 91-15 on page 91-129](#) for detailed information about using clientless SSL VPN.

## Customizing Clientless SSL VPN Pages

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

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

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

This section includes the following topics:

- [Information About Customization, page 91-80](#)
- [Exporting a Customization Template, page 77-84](#)
- [Editing the Customization Template, page 91-81](#)
- [Login Screen Advanced Customization, page 91-87](#)
- [Login Screen Advanced Customization, page 91-87](#)

## Information About Customization

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

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

### Customization Objects, Connection Profiles, and Group Policies

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



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

## Exporting a Customization Template

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

## Editing the Customization Template

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

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

**Example:**

```
<custom>
 <localization>
 <languages>en,ja,zh,ru,ua</languages>
 <default-language>en</default-language>
 </localization>
 <auth-page>
 <window>
 <title-text l10n="yes"><![CDATA[SSL VPN Service]]></title-text>
 </window>
 <full-customization>
 <mode>disable</mode>
 <url></url>
 </full-customization>
 <language-selector>
 <mode>disable</mode>
 <title l10n="yes">Language:</title>
 <language>
 <code>en</code>
 <text>English</text>
 </language>
 <language>
 <code>zh</code>
 <text>ä¸­æ– (Chinese)</text>
 </language>
 <language>
 <code>ja</code>
 <text>æ—æ—æ— (Japanese)</text>
 </language>
 <language>
 <code>ru</code>
 <text>Ð½ÑÑÐ°Ð¹ (Russian)</text>
 </language>
 <language>
 <code>ua</code>
 <text>Ð£Ð°ÐºÑÑÐ°Ð½ÑÑÐ°Ð½ÑÑÐ° (Ukrainian)</text>
 </language>
 </language-selector>
 <logon-form>
```

```

<title-text l10n="yes"><![CDATA[Login]]></title-text>
<title-background-color><![CDATA[#666666]]></title-background-color>
<title-font-color><![CDATA[#ffffff]]></title-font-color>
<message-text l10n="yes"><![CDATA[Please enter your username and
password.]]></message-text>
 <username-prompt-text l10n="yes"><![CDATA[USERNAME:]]></username-prompt-text>
 <password-prompt-text l10n="yes"><![CDATA[PASSWORD:]]></password-prompt-text>
 <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
 <internal-password-first>no</internal-password-first>
 <group-prompt-text l10n="yes"><![CDATA[GROUP:]]></group-prompt-text>
 <submit-button-text l10n="yes"><![CDATA[Login]]></submit-button-text>
<title-font-color><![CDATA[#ffffff]]></title-font-color>
<title-background-color><![CDATA[#666666]]></title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
<border-color>#858A91</border-color>
</logon-form>
<logout-form>
 <title-text l10n="yes"><![CDATA[Logout]]></title-text>
 <message-text l10n="yes"><![CDATA[Goodbye.

For your own security, please:

Clear the browser's cache

Delete any downloaded files

Close the browser's window]]></message-text>
 <login-button-text l10n="yes">Logon</login-button-text>
 <hide-login-button>no</hide-login-button>
 <title-background-color><![CDATA[#666666]]></title-background-color>
 <title-font-color><![CDATA[#ffffff]]></title-font-color>
 <title-font-color><![CDATA[#ffffff]]></title-font-color>
 <title-background-color><![CDATA[#666666]]></title-background-color>
 <font-color>#000000</font-color>
 <background-color>#ffffff</background-color>
 <border-color>#858A91</border-color>
</logout-form>
<title-panel>
 <mode>enable</mode>
 <text l10n="yes"><![CDATA[SSL VPN Service]]></text>
 <logo-url l10n="yes">+/CSCOU+/cscou_logo.gif</logo-url>
 <gradient>yes</gradient>
 <style></style>
 <background-color><![CDATA[#ffffff]]></background-color>
 <font-size><![CDATA[larger]]></font-size>
 <font-color><![CDATA[#800000]]></font-color>
 <font-weight><![CDATA[bold]]></font-weight>
</title-panel>
<info-panel>
 <mode>disable</mode>
 <image-url l10n="yes">+/CSCOU+/clear.gif</image-url>
 <image-position>above</image-position>
 <text l10n="yes"></text>
</info-panel>
<copyright-panel>
 <mode>disable</mode>
 <text l10n="yes"></text>
</copyright-panel>
</auth-page>
<portal>
 <title-panel>
 <mode>enable</mode>

```

```

<text l10n="yes"><![CDATA[SSL VPN Service]]></text>
<logo-url l10n="yes">/+CSCOU+/cisco_logo.gif</logo-url>
<gradient>yes</gradient>
<style></style>
<background-color><![CDATA[#ffffff]]></background-color>
<font-size><![CDATA[larger]]></font-size>
<font-color><![CDATA[#800000]]></font-color>
<font-weight><![CDATA[bold]]></font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
<application>
 <mode>enable</mode>
 <id>home</id>
 <tab-title l10n="yes">Home</tab-title>
 <order>1</order>
</application>
<application>
 <mode>enable</mode>
 <id>web-access</id>
 <tab-title l10n="yes"><![CDATA[Web Applications]]></tab-title>
 <url-list-title l10n="yes"><![CDATA[Web Bookmarks]]></url-list-title>
 <order>2</order>
</application>
<application>
 <mode>enable</mode>
 <id>file-access</id>
 <tab-title l10n="yes"><![CDATA[Browse Networks]]></tab-title>
 <url-list-title l10n="yes"><![CDATA[File Folder Bookmarks]]></url-list-title>
 <order>3</order>
</application>
<application>
 <mode>enable</mode>
 <id>app-access</id>
 <tab-title l10n="yes"><![CDATA[Application Access]]></tab-title>
 <order>4</order>
</application>
<application>
 <mode>enable</mode>
 <id>net-access</id>
 <tab-title l10n="yes">AnyConnect</tab-title>
 <order>4</order>
</application>
<application>
 <mode>enable</mode>
 <id>help</id>
 <tab-title l10n="yes">Help</tab-title>
 <order>1000000</order>
</application>
<toolbar>
 <mode>enable</mode>
 <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
 <prompt-box-title l10n="yes">Address</prompt-box-title>
 <browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
<column>
 <width>100%</width>
 <order>1</order>
</column>
<pane>
 <type>TEXT</type>
 <mode>disable</mode>
 <title></title>
 <text></text>

```

```

 <notitle></notitle>
 </column></column>
 </row></row>
 </height></height>
</pane>
<pane>
 <type>IMAGE</type>
 <mode>disable</mode>
 <title></title>
 <url l10n="yes"></url>
 <notitle></notitle>
 <column></column>
 <row></row>
 <height></height>
</pane>
<pane>
 <type>HTML</type>
 <mode>disable</mode>
 <title></title>
 <url l10n="yes"></url>
 <notitle></notitle>
 <column></column>
 <row></row>
 <height></height>
</pane>
<pane>
 <type>RSS</type>
 <mode>disable</mode>
 <title></title>
 <url l10n="yes"></url>
 <notitle></notitle>
 <column></column>
 <row></row>
 <height></height>
</pane>
<url-lists>
 <mode>group</mode>
</url-lists>
<home-page>
 <mode>standard</mode>
 <url></url>
</home-page>
</portal>
</custom>

```

Figure 91-19 shows the Logon page and its customizing XML tags. All these tags are nested within the higher-level tag `<auth-page>`.

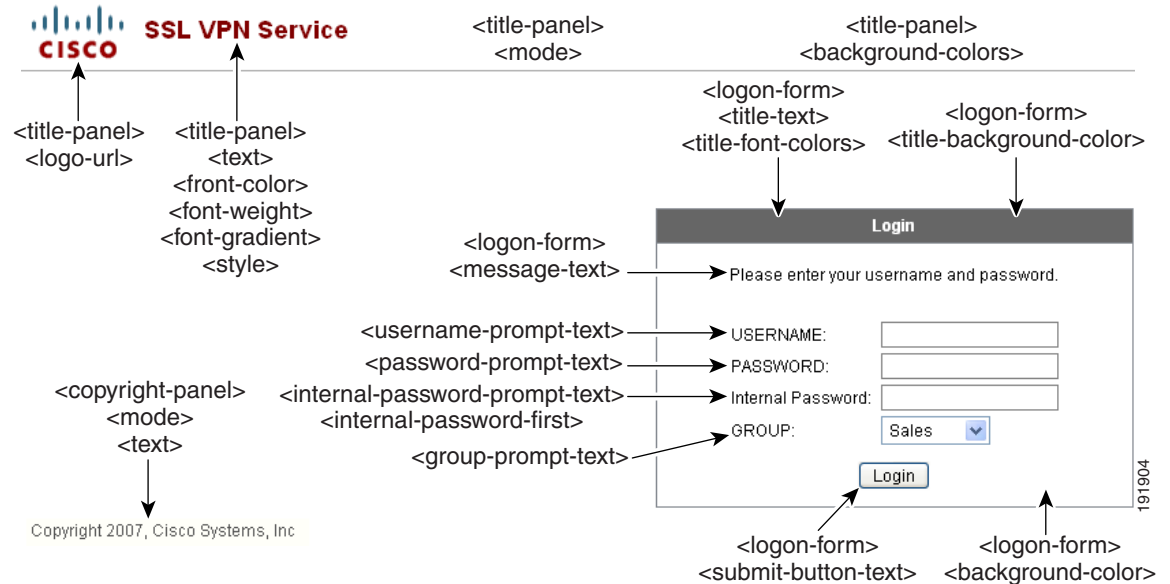
**Figure 91-19 Logon Page and Associated XML Tags**

Figure 91-20 shows the Language Selector drop-down list that is available on the Logon page, and the XML tags for customizing this feature. All these tags are nested within the higher-level `<auth-page>` tag.

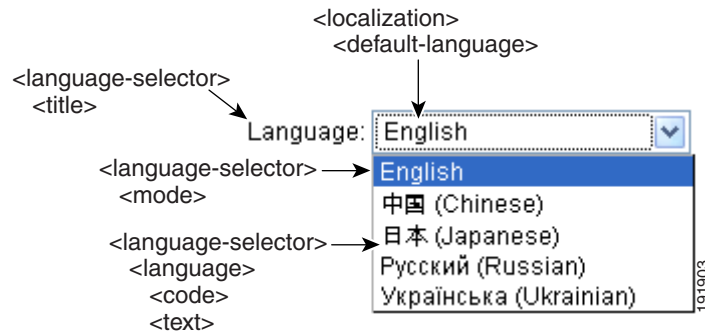
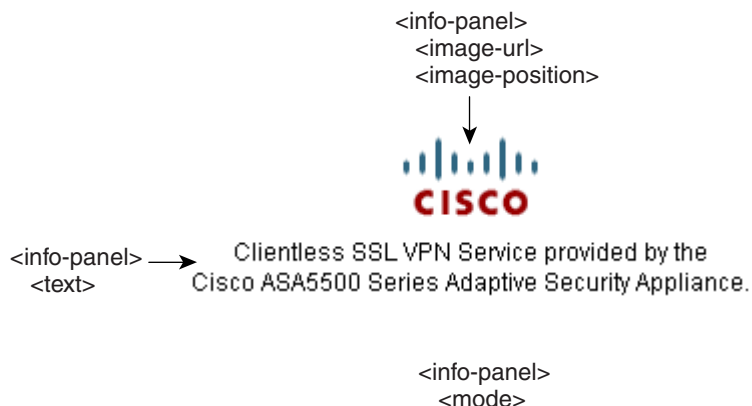
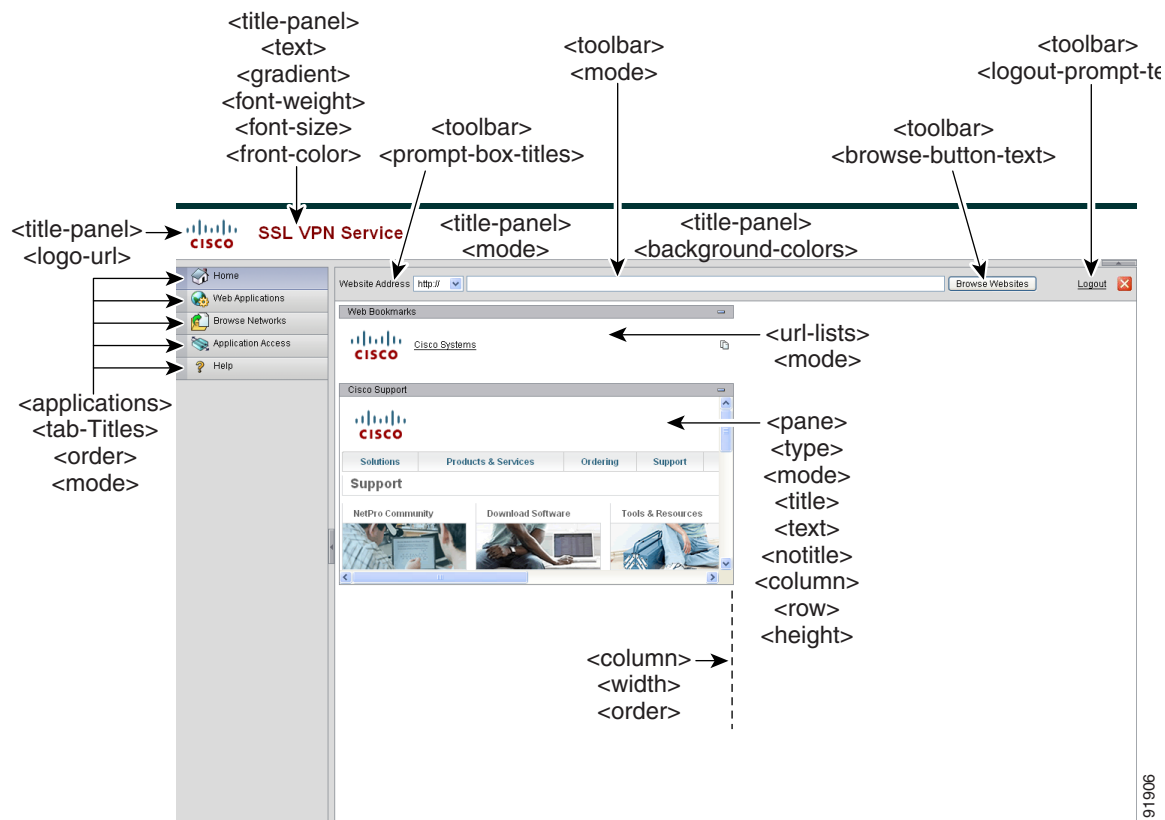
**Figure 91-20 Language Selector on Logon Screen and Associated XML Tags**

Figure 91-21 shows the Information Panel that is available on the Logon page, and the XML tags for customizing this feature. This information can appear to the left or right of the login box. These tags are nested within the higher-level `<auth-page>` tag.

**Figure 91-21 Information Panel on Logon Screen and Associated XML Tags**

191905

Figure 91-22 shows the Portal page and the XML tags for customizing this feature. These tags are nested within the higher-level `<auth-page>` tag.

**Figure 91-22 Portal Page and Associated XML Tags**

191906

## Login Screen Advanced Customization

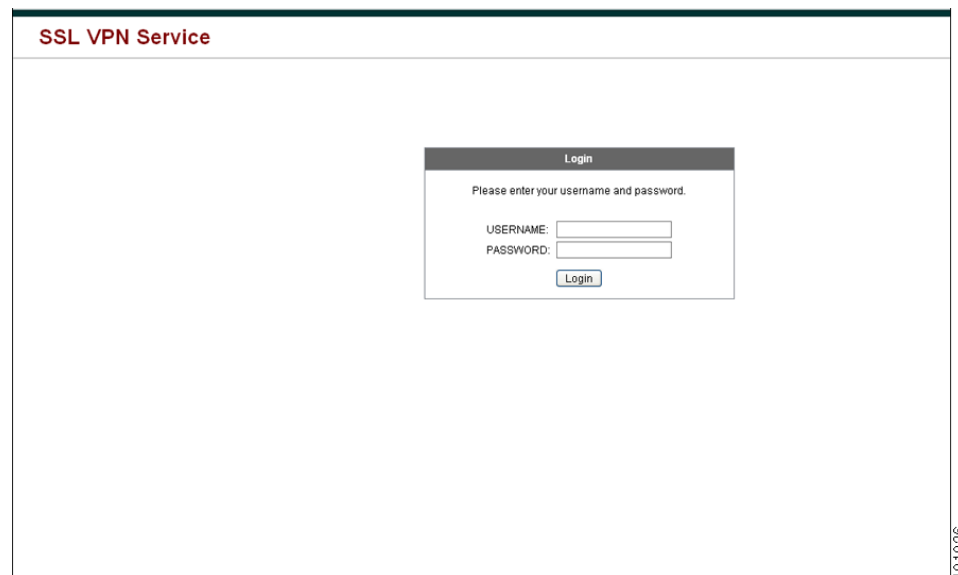
If you prefer to use your own, custom login screen, rather than changing specific screen elements of the login screen we provide, you can perform this advanced customization using the *Full Customization* feature.

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

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

[Figure 91-23](#) shows the standard Cisco login screen that displays to clientless SSL VPN users. The Login form is displayed by a function called by the HTML code.

**Figure 91-23** Standard Cisco Login Page



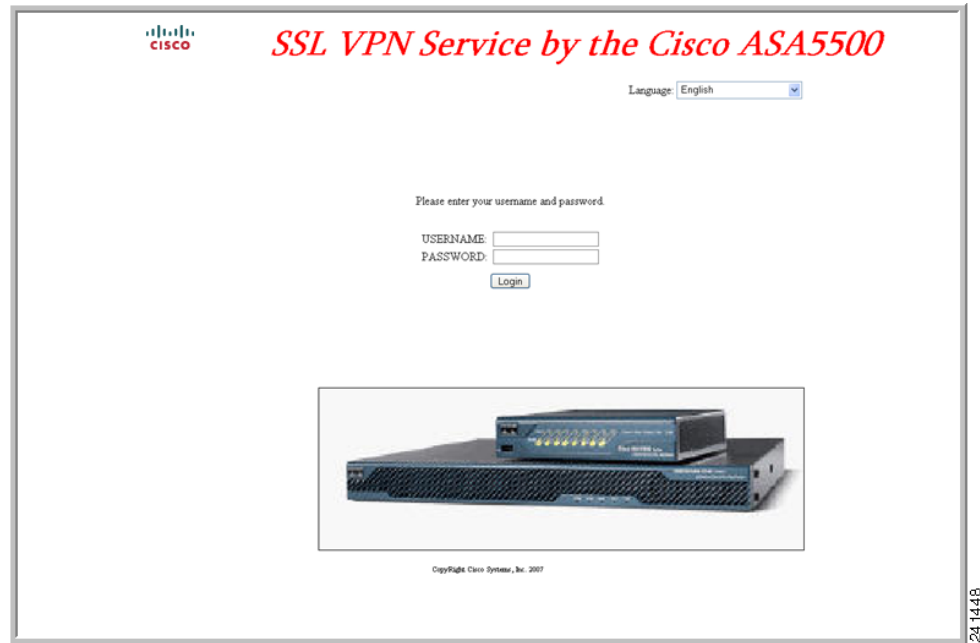
[Figure 91-24](#) shows the Language Selector drop-down list. This feature is an option for clientless SSL VPN users and is also called by a function in the HTML code of the login screen.

**Figure 91-24** Language Selector Drop-down List



Figure 91-25 shows a simple example of a custom login screen enabled by the Full Customization feature.

**Figure 91-25 Example of Full Customization of Login Screens**



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

**Example:**

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

<p align="center">
<font face="Snap
ITC" size="6" color="#FF00FF">
 <i> SSL VPN Service by the Cisco
ASA5500</i></p>

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

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
```



```

 <p> </p>
 <p> </p>
 <p>Loading...</p>
 </div>
</td>
</tr>
<tr>
 <td width="251"></td>
 <td width="1"></td>
 <td align=right valign=right width="800">

 </td></tr>

</table>

```

The indented code injects the Login form and the Language Selector on the screen. The function **cscs\_ShowLoginForm('lform')** injects the logon form. **cscs\_ShowLanguageSelector('selector')** injects the Language Selector.

## Modifying Your HTML File

Follow these steps to modify your HTML file:

### Detailed Steps

- Step 1** Name your file **logon.inc**. When you import the file, the ASA recognizes this filename as the logon screen.
- Step 2** Modify the paths of images used by the file to include **/+CSCOU+/**.
- Files that are displayed to remote users before authentication must reside in a specific area of the ASA cache memory represented by the path **/+CSCOU+/**. Therefore, the source for each image in the file must include this path. For example:

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

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

```

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

<table>

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

```

```

<td align=right valign=right width="800">

</td></tr>

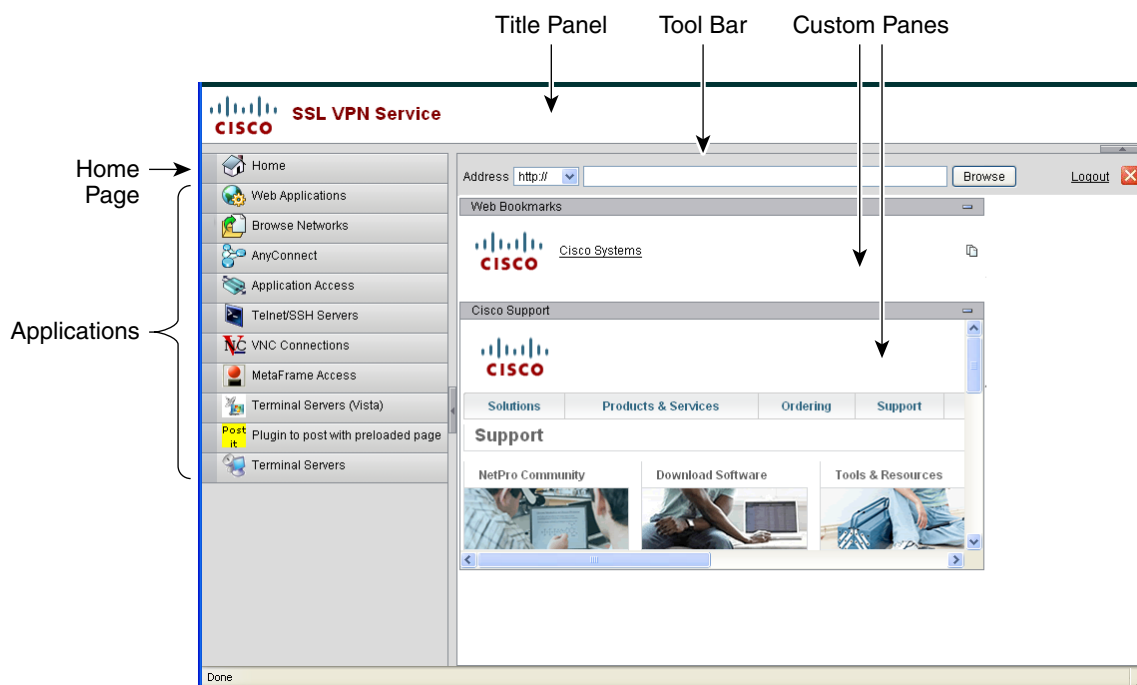
</table>

```

## Customizing the Portal Page

Figure 91-26 shows the portal page and the pre-defined components you can customize:

**Figure 91-26 Customizable Components of the Portal Page**



In addition to customizing the components of the page, you can divide the portal page into custom panes that display text, an image, an RSS feed, or HTML. In Figure 91-26, the portal page is divided into one column with two rows.

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

- Step 1** Go to Portal Page and specify a title for the browser window.
- Step 2** Display and customize the title panel. Go to Portal Page > Title Panel and check **Display title panel**. Enter text to display as the title and specify a logo. Specify any font styles.
- Step 3** Enable and customize the toolbar. Go to Portal Page > Toolbar and check **Display toolbar**. Customize the Prompt Box, Browse button, and Logout prompt as desired.
- Step 4** Customize the Applications list. Go to Portal Page > Applications and check **Show navigation panel**. The applications populated in the table are those applications you enabled in the ASA configuration, including client-server plugins and port forwarding applications.
- Step 5** Create custom panes in the portal page space. Go to Portal Page > Custom Panes and divide the window into rows and columns for text, images, RSS feeds, or HTML pages, as desired.

- Step 6** Specify a home page URL. Go to Portal Page > Home Page and check **Enable custom intranet web page**. Choose a bookmark mode that defines how bookmarks are organized.
- Configure a timeout alert message and a tooltip. Go to Portal Page > Timeout Alerts. See [Configuring Custom Portal Timeout Alerts](#) for full instructions.
- 

## Configuring Custom Portal Timeout Alerts

So that users of the clientless SSL VPN feature can manage their time in the VPN session, the clientless SSL VPN portal page displays a countdown timer showing the total time left before the clientless VPN session expires. Sessions can timeout due to inactivity or because they have reached the end of a maximum allowed connection time that you have configured.

You can create custom messages to alert users that their session is about to end because of an idle timeout or a session timeout. Your custom message replaces the default idle timeout message. The default message is, "Your session will expire in %s ." The %s place holder in your message is replaced by a ticking countdown timer.

- 
- Step 1** Start ASDM and select **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization**.
- Step 2** Click **Add** to add a new customization object or select an existing customization object and click **Edit** to add a custom idle timeout message to an existing customization object.
- Step 3** In the Add / Edit Customization Object pane, expand the Portal Page node on the navigation tree and click **Timeout Alerts**.
- Step 4** Check **Enable alert visual tooltip (red background for timer countdown)**. This displays the countdown timer as a tool tip on a red background. When users click the Time left area, the time area expands to display your custom timeout alert message. If you leave this box unchecked, users see the custom timeout alerts in a pop-up window.
- Step 5** Enter a message in the Idle Timeout Message box and in the Session Timeout Message box. An example of a message could be, Warning: Your session will end in %s. Please complete your work and prepare to close your applications.
- Step 6** Click **OK**.
- Step 7** Click **Apply**.
- 

## Specifying a Custom Timeout Alert in a Customization Object File

If you desire, you can edit an existing customization object file outside of the ASA and import it to the ASA. For more information about Importing and Exporting Customization objects see [Importing/Exporting Customization Object, page 91-94](#). See also, [Creating XML-Based Portal Customization Objects and URL Lists, page 91-94](#).

The timeout messages are configured in the <timeout-alerts> XML element of your XML customization object file. The <timeout-alerts> element is a child of the <portal> element. The <portal> element is a child of the <custom> element.

The <timeout-alerts> element is placed after the <home-page> element and before any <application> elements in the order of the <portal> child elements.

You need to specify these child-elements of `<timeout-alerts>`:

- `<alert-tooltip>` – If set to “yes”, users see the countdown timer on a red background as a tool tip. Clicking the count down timer expands the tooltip to display your custom message. If set to “no” or if is undefined, users receive your custom messages in pop-up windows.
- `<session-timeout-message>` – Enter your custom session timeout message in this element. If set and not empty, users receive your custom message instead of the default message. The `%s` place holder in the message will be replaced with a ticking countdown timer.
- `<idle-timeout-message>` – Enter your custom idle timeout message in this element. If set and not empty, users receive your custom message instead of the default message. The `%s` place holder will be replaced with a ticking countdown timer.

### Configuration Example for Timeout-alert Element and Child Elements

This example shows only the `<timeout-alerts>` elements of the `<portal>` element.



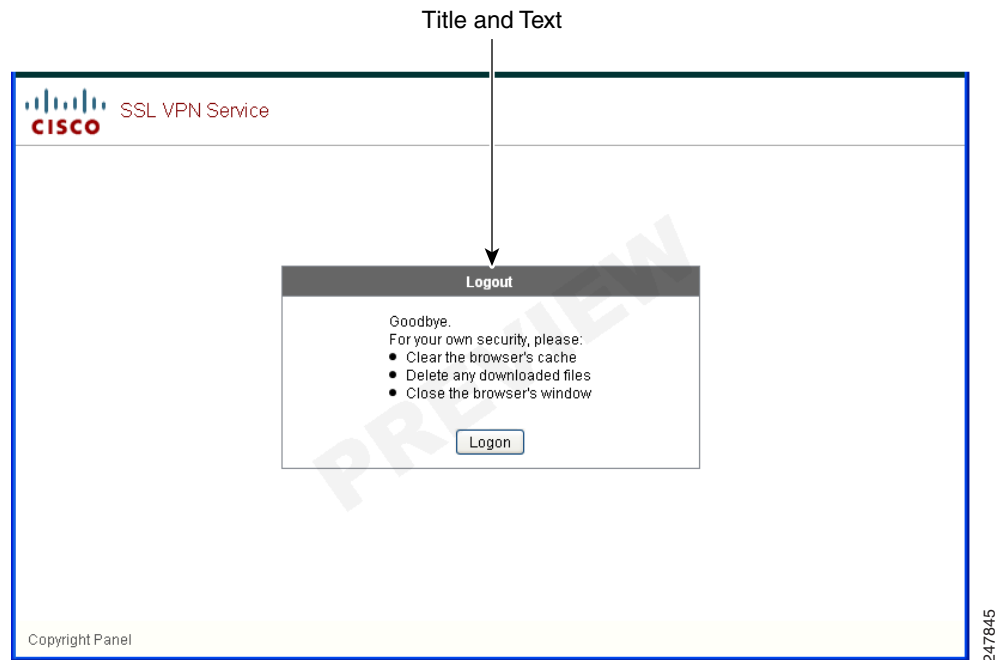
#### Note

Do not cut and paste this example into an existing customization object.

```
<portal>
 <window></window>
 <title-panel></title-panel>
 <toolbar></toolbar>
 <url-lists></url-lists>
 <navigation-panel></navigation-panel>
 <home-page>
 <timeout-alerts>
 <alert-tooltip>yes</alert-tooltip>
 <idle-timeout-message>You session expires in %s due to idleness.</idle-timeout-message>
 <session-timeout-message>Your session expires in %s.</session-timeout-message>
 </timeout-alerts>
 <application></application>
 <column></column>
 <pane></pane>
 <external-portal></external-portal>
</portal>
```

## Customizing the Logout Page

Figure 91-27 shows the logout page you can customize:

**Figure 91-27** Components of the Logout Page

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

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

## Customizing the External Portal Page

### Adding Customization Object

To add a customization object, create a copy of and provide a unique name for the DfltCustomization object. Then you can modify or edit it to meet your requirements.

#### Detailed Steps

- 
- Step 1** Click **Add** and enter a name for the new customization object. Maximum 64 characters, no spaces.

- Step 2** (Optional) Click **Find** to search for a customization object. Start typing in the field, and the tool searches the beginning characters of every field for a match. You can use wild cards to expand your search. For example, typing *sal* in the Find field matches a customization object named sales but not a customization object named wholesalers. If you type *\*sal* in the Find field, the search finds the first instance of either sales or wholesalers in the table.
- Use the up and down arrows to skip up or down to the next string match. Check the **Match Case** checkbox to make your search case sensitive.
- Step 3** Specify when the onscreen keyboard shows on portal pages. The choices are as follows:
- Do not show OnScreen Keyboard
  - Show only for the login page
  - Show for all portal pages requiring authentication
- Step 4** (Optional) Highlight a customization object and click **Assign** to assign the selected object to one or more group policies, connection profiles, or LOCAL users.
- 

## Importing/Exporting Customization Object

You can import or export already-existing customization objects. Import an object that you want to apply to end users. Export a customization object already resident on the ASA for editing purposes, after which you can reimport it.

### Detailed Steps

---

- Step 1** Identify the customization object by name. Maximum 64 characters, no spaces.
- Step 2** Choose the method by which you want to import or export the customization file:
- Local computer—Choose this method to import a file that resides on the local PC.
  - Path—Provide the path to the file.
  - Browse Local Files—Browse to the path for the file.
  - Flash file system—Choose this method to export a file that resides on the ASA.
  - Path—Provide the path to the file.
  - Browse Flash—Browse to the path for the file.
  - Remote server—Choose this option to import a customization file that resides on a remote server accessible from the ASA.
  - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
- Step 3** Click to import or export the file.
- 

## Creating XML-Based Portal Customization Objects and URL Lists

This section includes the following topics:

- [Understanding the XML Customization File Structure, page 91-101](#)

- [Configuration Example for Customization, page 91-104](#)
- [Understanding the XML Customization File Structure, page 91-101](#)
- [Help Customization, page 91-119](#)
- [Import/Export Application Help Content, page 91-122](#)

## Understanding the XML Customization File Structure

Table 91-9 presents the file structure for an XML customization object.



### Note

Absence of a parameter/tag results in a default/inherited value, while presence results in setting the parameter/tag value even it is an empty string.

**Table 91-8 XML-Based Customization File Structure**

Tag	Type	Values	Preset value	Description
<b>custom</b>	<b>node</b>	—	—	<b>Root tag</b>
<b>auth-page</b>	<b>node</b>	—	—	<b>Tag-container of authentication page configuration</b>
<b>window</b>	<b>node</b>	—	—	<b>Browser window</b>
title-text	string	Arbitrary string	empty string	—
<b>title-panel</b>	<b>node</b>	—	—	<b>The page top pane with a logo and a text</b>
mode	text	enable disable	disable	—
text	text	Arbitrary string	empty string	—
logo-url	text	Arbitrary URL	empty image URL	—
<b>copyright-panel</b>	<b>node</b>	—	—	<b>The page bottom pane with a copyright information</b>
mode	text	enable disable	disable	—
text	text	Arbitrary URL	empty string	—
<b>info-panel</b>	<b>node</b>	—	—	<b>The pane with a custom text and image</b>
mode	string	enable disable	disable	—
image-position	string	above below	above	The image position, relative to text
image-url	string	Arbitrary URL	empty image	—
text	string	Arbitrary string	empty string	—
<b>logon-form</b>	<b>node</b>	—	—	<b>The form with username, password, group prompt</b>
title-text	string	Arbitrary string	Logon	—

**Table 91-8 XML-Based Customization File Structure (continued)**

message-text	string	Arbitrary string	empty string	—
username-prompt-text	string	Arbitrary string	Username	—
password-prompt-text	string	Arbitrary string	Password	—
internal-password-prompt-text	string	Arbitrary string	Internal Password	—
group-prompt-text	string	Arbitrary string	Group	—
submit-button-text	string	Arbitrary string	Logon	—
<b>logout-form</b>	<b>node</b>	—	—	<b>The form with a logout message and the buttons to login or close the window</b>
title-text	string	Arbitrary string	Logout	—
message-text	string	Arbitrary string	Empty string	—
login-button-text	string	Arbitrary string	Login	—
close-button-text	string	Arbitrary string	Close window	—
<b>language-selector</b>	<b>node</b>	—	—	<b>The drop-down list to select a language</b>
mode	string	enable disable	disable	—
title	text	—	Language	The prompt text to select language
<b>language</b>	<b>node (multiple)</b>	—	—	—
code	string	—	—	—
text	string	—	—	—
<b>portal</b>	<b>node</b>	—	—	<b>Tag-container of the portal page configuration</b>
<b>window</b>	<b>node</b>	—	—	<b>see authentication page description</b>
title-text	string	Arbitrary string	Empty string	—
<b>title-panel</b>	<b>node</b>	—	—	<b>see authentication page description</b>
mode	string	enable disable	Disable	—
text	string	Arbitrary string	Empty string	—
logo-url	string	Arbitrary URL	Empty image URL	—
<b>navigation-panel</b>	<b>node</b>	—	—	<b>The pane on the left with application tabs</b>
mode	string	enable disable	enable	—



**Table 91-8 XML-Based Customization File Structure (continued)**

application	node (multiple)	—	N/A	The node changes defaults for the configured (by id) application
id	string	For stock application web-access file-access app-access net-access help  For ins: Unique plug-in	N/A	—
tab-title	string	—	N/A	—
order	number	—	N/A	Value used to sort elements. The default element order values have step 1000, 2000, 3000, etc. For example, to insert an element between the first and second element, use a value 1001 – 1999.
url-list-title	string	—	N/A	If the application has bookmarks, the title for the panel with grouped bookmarks
mode	string	enable disable	N/A	v
<b>toolbar</b>	<b>node</b>	—	—	—
mode	string	enable disable	Enable	—
prompt-box-title	string	Arbitrary string	Address	Title for URL prompt list
browse-button-text	string	Arbitrary string	Browse	Browse button text
logout-prompt-text	string	Arbitrary string	Logout	—
<b>column</b>	<b>node (multiple)</b>	—	—	<b>One column will be shown by default</b>
width	string	—	N/A	—
order	number	—	N/A	Value used to sort elements.

**Table 91-8 XML-Based Customization File Structure (continued)**

url-lists	node	—	—	URL lists are considered to be default elements on the portal home page, if they are not explicitly disabled
mode	string	group   nogroup	group	Modes: group – elements grouped by application type i.e. Web Bookmarks, File Bookmarks) no-group – url-lists are shown in separate panes disable – do not show URL lists by default
panel	node (multiple)	—	—	Allows to configure extra panes
mode	string	enable disable	—	Used to temporarily disable the panel without removing its configuration
title	string	—	—	—
type	string	—	—	Supported types: RSS IMAGE TEXT HTML
url	string	—	—	URL for RSS,IMAGE or HTML type paned
url-mode	string	—	—	Modes: mangle, no-mangle
text	string	—	—	Text for TEXT type panes
column	number	—	—	—

## Configuration Example for Customization

The following example illustrates the following customization options:

- Hides tab for the File access application
- Changes title and order of Web Access application

- Defines two columns on the home page
- Adds an RSS pane
- Adds three panes (text, image, and html) at the top of second pane

```

<custom name="Default">
 <auth-page>

 <window>
 <title-text l10n="yes">title WebVPN Logon</title>
 </window>

 <title-panel>
 <mode>enable</mode>
 <text l10n="yes">EXAMPLE WebVPN</text>
 <logo-url>http://www.example.com/images/EXAMPLE.gif</logo-url>
 </title-panel>

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

 <info-panel>
 <mode>enable</mode>
 <image-url>/+CSCOE+/custom/EXAMPLE.jpg</image-url>
 <text l10n="yes">
 <![CDATA[
 <div>
 Welcome to WebVPN !.
 </div>
]]>
 </text>
 </info-panel>
 <logon-form>
 <form>
 <title-text l10n="yes">title WebVPN Logon</title>
 <message-text l10n="yes">message WebVPN Logon</title>
 <username-prompt-text l10n="yes">Username</username-prompt-text>
 <password-prompt-text l10n="yes">Password</password-prompt-text>
 <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
 <group-prompt-text l10n="yes">Group</group-prompt-text>
 <submit-button-text l10n="yes">Logon</submit-button-text>
 </form>
 </logon-form>
 <logout-form>
 <form>
 <title-text l10n="yes">title WebVPN Logon</title>
 <message-text l10n="yes">message WebVPN Logon</title>
 <login-button-text l10n="yes">Login</login-button-text>
 <close-button-text l10n="yes">Logon</close-button-text>
 </form>
 </logout-form>

 <language-selector>
 <language>
 <code l10n="yes">code1</code>
 <text l10n="yes">text1</text>
 </language>
 <language>
 <code l10n="yes">code2</code>
 <text l10n="yes">text2</text>
 </language>
 </language-selector>
 </auth-page>
</custom>

```

```

 </language>
 </language-selector>

</auth-page>
<portal>

 <window>
 <title-text l10n="yes">title WebVPN Logon</title>
 </window>

 <title-panel>
 <mode>enable</mode>
 <text l10n="yes">EXAMPLE WebVPN</text>
 <logo-url>http://www.example.com/logo.gif</logo-url>
 </title-panel>

 <navigation-panel>
 <mode>enable</mode>
 </navigation-panel>

 <application>
 <id>file-access</id>
 <mode>disable</mode>
 </application>
 <application>
 <id>web-access</id>
 <tab-title>EXAMPLE Intranet</tab-title>
 <order>3001</order>
 </application>

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

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

 <pane>
 <id>rss_pane</id>
 <type>RSS</type>
 <url>rss.example.com?id=78</url>
 </pane>
 <pane>
 <type>IMAGE</type>
 <url>http://www.example.com/logo.gif</url>
 <column>1</column>
 <row>2</row>
 </pane>

 <pane>
 <type>HTML</type>
 <title>EXAMPLE news</title>
 <url>http://www.example.com/news.html</url>
 <column>1</column>
 <row>3</row>
 </pane>

</portal>

```

&lt;/custom&gt;

## Understanding the XML Customization File Structure

Table 91-9 presents the file structure for an XML customization object.


**Note**

Absence of a parameter/tag results in a default/inherited value, while presence results in setting the parameter/tag value even it is an empty string.

**Table 91-9 XML-Based Customization File Structure**

Tag	Type	Values	Preset value	Description
<b>custom</b>	<b>node</b>	—	—	<b>Root tag</b>
<b>auth-page</b>	<b>node</b>	—	—	<b>Tag-container of authentication page configuration</b>
<b>window</b>	<b>node</b>	—	—	<b>Browser window</b>
title-text	string	Arbitrary string	empty string	—
<b>title-panel</b>	<b>node</b>	—	—	<b>The page top pane with a logo and a text</b>
mode	text	enable disable	disable	—
text	text	Arbitrary string	empty string	—
logo-url	text	Arbitrary URL	empty image URL	—
<b>copyright-panel</b>	<b>node</b>	—	—	<b>The page bottom pane with a copyright information</b>
mode	text	enable disable	disable	—
text	text	Arbitrary URL	empty string	—
<b>info-panel</b>	<b>node</b>	—	—	<b>The pane with a custom text and image</b>
mode	string	enable disable	disable	—
image-position	string	above below	above	The image position, relative to text
image-url	string	Arbitrary URL	empty image	—
text	string	Arbitrary string	empty string	—
<b>logon-form</b>	<b>node</b>	—	—	<b>The form with username, password, group prompt</b>
title-text	string	Arbitrary string	Logon	—
message-text	string	Arbitrary string	empty string	—

**Table 91-9 XML-Based Customization File Structure (continued)**

username-prompt-text	string	Arbitrary string	Username	—
password-prompt-text	string	Arbitrary string	Password	—
internal-password-prompt-text	string	Arbitrary string	Internal Password	—
group-prompt-text	string	Arbitrary string	Group	—
submit-button-text	string	Arbitrary string	Logon	
<b>logout-form</b>	<b>node</b>	—	—	<b>The form with a logout message and the buttons to login or close the window</b>
title-text	string	Arbitrary string	Logout	—
message-text	string	Arbitrary string	Empty string	—
login-button-text	string	Arbitrary string	Login	
close-button-text	string	Arbitrary string	Close window	—
<b>language-selector</b>	<b>node</b>	—	—	<b>The drop-down list to select a language</b>
mode	string	enable disable	disable	—
title	text	—	Language	The prompt text to select language
<b>language</b>	<b>node (multiple)</b>	—	—	—
code	string	—	—	—
text	string	—	—	—
<b>portal</b>	<b>node</b>	—	—	<b>Tag-container of the portal page configuration</b>
<b>window</b>	<b>node</b>	—	—	<b>see authentication page description</b>
title-text	string	Arbitrary string	Empty string	—
<b>title-panel</b>	<b>node</b>	—	—	<b>see authentication page description</b>
mode	string	enable disable	Disable	—
text	string	Arbitrary string	Empty string	—
logo-url	string	Arbitrary URL	Empty image URL	—
<b>navigation-panel</b>	<b>node</b>	—	—	<b>The pane on the left with application tabs</b>
mode	string	enable disable	enable	—

**Table 91-9 XML-Based Customization File Structure (continued)**

application	node (multiple)	—	N/A	The node changes defaults for the configured (by id) application
id	string	For stock application web-access file-access app-access net-access help  For ins: Unique plug-in	N/A	—
tab-title	string	—	N/A	—
order	number	—	N/A	Value used to sort elements. The default element order values have step 1000, 2000, 3000, etc. For example, to insert an element between the first and second element, use a value 1001 – 1999.
url-list-title	string	—	N/A	If the application has bookmarks, the title for the panel with grouped bookmarks
mode	string	enable disable	N/A	v
<b>toolbar</b>	<b>node</b>	—	—	—
mode	string	enable disable	Enable	—
prompt-box-title	string	Arbitrary string	Address	Title for URL prompt list
browse-button-text	string	Arbitrary string	Browse	Browse button text
logout-prompt-text	string	Arbitrary string	Logout	—
<b>column</b>	<b>node (multiple)</b>	—	—	<b>One column will be shown by default</b>
width	string	—	N/A	—
order	number	—	N/A	Value used to sort elements.

**Table 91-9 XML-Based Customization File Structure (continued)**

url-lists	node	—	—	URL lists are considered to be default elements on the portal home page, if they are not explicitly disabled
mode	string	group   nogroup	group	Modes: group – elements grouped by application type i.e. Web Bookmarks, File Bookmarks) no-group – url-lists are shown in separate panes disable – do not show URL lists by default
panel	node (multiple)	—	—	Allows to configure extra panes
mode	string	enable disable	—	Used to temporarily disable the panel without removing its configuration
title	string	—	—	—
type	string	—	—	Supported types: RSS IMAGE TEXT HTML
url	string	—	—	URL for RSS,IMAGE or HTML type paned
url-mode	string	—	—	Modes: mangle, no-mangle
text	string	—	—	Text for TEXT type panes
column	number	—	—	—

## Configuration Example for Customization

The following example illustrates the following customization options:

- Hides tab for the File access application
- Changes title and order of Web Access application



- Defines two columns on the home page
- Adds an RSS pane
- Adds three panes (text, image, and html) at the top of second pane

```

<custom name="Default">
 <auth-page>

 <window>
 <title-text l10n="yes">title WebVPN Logon</title>
 </window>

 <title-panel>
 <mode>enable</mode>
 <text l10n="yes">EXAMPLE WebVPN</text>
 <logo-url>http://www.example.com/images/EXAMPLE.gif</logo-url>
 </title-panel>

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

 <info-panel>
 <mode>enable</mode>
 <image-url>/+CSCOE+/custom/EXAMPLE.jpg</image-url>
 <text l10n="yes">
 <![CDATA[
 <div>
 Welcome to WebVPN !.
 </div>
]]>
 </text>
 </info-panel>
 <logon-form>
 <form>
 <title-text l10n="yes">title WebVPN Logon</title>
 <message-text l10n="yes">message WebVPN Logon</title>
 <username-prompt-text l10n="yes">Username</username-prompt-text>
 <password-prompt-text l10n="yes">Password</password-prompt-text>
 <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
 <group-prompt-text l10n="yes">Group</group-prompt-text>
 <submit-button-text l10n="yes">Logon</submit-button-text>
 </form>
 </logon-form>
 <logout-form>
 <form>
 <title-text l10n="yes">title WebVPN Logon</title>
 <message-text l10n="yes">message WebVPN Logon</title>
 <login-button-text l10n="yes">Login</login-button-text>
 <close-button-text l10n="yes">Logon</close-button-text>
 </form>
 </logout-form>

 <language-selector>
 <language>
 <code l10n="yes">code1</code>
 <text l10n="yes">text1</text>
 </language>
 <language>
 <code l10n="yes">code2</code>
 <text l10n="yes">text2</text>
 </language>
 </language-selector>
 </auth-page>
</custom>

```

```

 </language>
 </language-selector>

</auth-page>
<portal>

 <window>
 <title-text l10n="yes">title WebVPN Logon</title>
 </window>

 <title-panel>
 <mode>enable</mode>
 <text l10n="yes">EXAMPLE WebVPN</text>
 <logo-url>http://www.example.com/logo.gif</logo-url>
 </title-panel>

 <navigation-panel>
 <mode>enable</mode>
 </navigation-panel>

 <application>
 <id>file-access</id>
 <mode>disable</mode>
 </application>
 <application>
 <id>web-access</id>
 <tab-title>EXAMPLE Intranet</tab-title>
 <order>3001</order>
 </application>

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

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

 <pane>
 <id>rss_pane</id>
 <type>RSS</type>
 <url>rss.example.com?id=78</url>
 </pane>
 <pane>
 <type>IMAGE</type>
 <url>http://www.example.com/logo.gif</url>
 <column>1</column>
 <row>2</row>
 </pane>

 <pane>
 <type>HTML</type>
 <title>EXAMPLE news</title>
 <url>http://www.example.com/news.html</url>
 <column>1</column>
 <row>3</row>
 </pane>

</portal>

```

```
</custom>
```

## Editing the Customization Object

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



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

### Export the Default Customization Template

Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization, select **Template**, and click the **Export** button.

### Import the Edited Customization Template

Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization, click the **Import** button, and choose a name for your new customization object.

## The Customization Template

The customization template, named *Template*, follows:

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

Copyright (c) 2008,2009 by Cisco Systems, Inc.  
All rights reserved.

Note: all white spaces in tag values are significant and preserved.

Tag: custom

Description: Root customization tag

Tag: custom/languages

Description: Contains list of languages, recognized by ASA

Value: string containing comma-separated language codes. Each language code is a set dash-separated alphanumeric characters, started with alpha-character (for example: en, en-us, irokese8-language-us)

Default value: en-us

Tag: custom/default-language

Description: Language code that is selected when the client and the server were not able to negotiate the language automatically.

For example the set of languages configured in the browser is "en,ja", and the list of languages, specified by 'custom/languages' tag is "cn,fr", the default-language will be used.

Value: string, containing one of the language coded, specified in 'custom/languages' tag above.

Default value: en-us

\*\*\*\*\*

Tag: custom/auth-page

Description: Contains authentication page settings

\*\*\*\*\*

Tag: custom/auth-page/window

Description: Contains settings of the authentication page browser window

Tag: custom/auth-page/window/title-text

Description: The title of the browser window of the authentication page

Value: arbitrary string

Default value: Browser's default value

\*\*\*\*\*

Tag: custom/auth-page/title-panel

Description: Contains settings for the title panel

Tag: custom/auth-page/title-panel/mode

Description: The title panel mode

Value: enable|disable

Default value: disable

Tag: custom/auth-page/title-panel/text

Description: The title panel text.

Value: arbitrary string

Default value: empty string

Tag: custom/auth-page/title-panel/logo-url

Description: The URL of the logo image (imported via "import webvpn webcontent")

Value: URL string

Default value: empty image URL

Tag: custom/auth-page/title-panel/background-color

Description: The background color of the title panel

Value: HTML color format, for example #FFFFFF

Default value: #FFFFFF

Tag: custom/auth-page/title-panel/font-color

Description: The background color of the title panel

Value: HTML color format, for example #FFFFFF

Default value: #000000

Tag: custom/auth-page/title-panel/font-weight

Description: The font weight

Value: CSS font size value, for example bold, bolder, lighter etc.

Default value: empty string

Tag: custom/auth-page/title-panel/font-size

Description: The font size

Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.

Default value: empty string

Tag: custom/auth-page/title-panel/gradient

Description: Specifies using the background color gradient

Value: yes|no

Default value: no

Tag: custom/auth-page/title-panel/style

Description: CSS style of the title panel  
 Value: CSS style string  
 Default value: empty string

\*\*\*\*\*

Tag: custom/auth-page/copyright-panel  
 Description: Contains the copyright panel settings

Tag: custom/auth-page/copyright-panel/mode  
 Description: The copyright panel mode  
 Value: enable|disable  
 Default value: disable

Tag: custom/auth-page/copyright-panel/text  
 Description: The copyright panel text  
 Value: arbitrary string  
 Default value: empty string

\*\*\*\*\*

Tag: custom/auth-page/info-panel  
 Description: Contains information panel settings

Tag: custom/auth-page/info-panel/mode  
 Description: The information panel mode  
 Value: enable|disable  
 Default value: disable

Tag: custom/auth-page/info-panel/image-position  
 Description: Position of the image, above or below the informational panel text  
 Values: above|below  
 Default value: above

Tag: custom/auth-page/info-panel/image-url  
 Description: URL of the information panel image (imported via "import webvpn webcontent")  
 Value: URL string  
 Default value: empty image URL

Tag: custom/auth-page/info-panel/text  
 Description: Text of the information panel  
 Text: arbitrary string  
 Default value: empty string

\*\*\*\*\*

Tag: custom/auth-page/logon-form  
 Description: Contains logon form settings

Tag: custom/auth-page/logon-form/title-text  
 Description: The logon form title text  
 Value: arbitrary string  
 Default value: "Logon"

Tag: custom/auth-page/logon-form/message-text  
 Description: The message inside of the logon form  
 Value: arbitrary string  
 Default value: empty string

Tag: custom/auth-page/logon-form/username-prompt-text  
 Description: The username prompt text  
 Value: arbitrary string  
 Default value: "Username"

Tag: custom/auth-page/logon-form/password-prompt-text

Description: The password prompt text  
 Value: arbitrary string  
 Default value: "Password"

Tag: custom/auth-page/logon-form/internal-password-prompt-text  
 Description: The internal password prompt text  
 Value: arbitrary string  
 Default value: "Internal Password"

Tag: custom/auth-page/logon-form/group-prompt-text  
 Description: The group selector prompt text  
 Value: arbitrary string  
 Default value: "Group"

Tag: custom/auth-page/logon-form/submit-button-text  
 Description: The submit button text  
 Value: arbitrary string  
 Default value: "Logon"

Tag: custom/auth-page/logon-form/internal-password-first  
 Description: Sets internal password first in the order  
 Value: yes|no  
 Default value: no

Tag: custom/auth-page/logon-form/title-font-color  
 Description: The font color of the logon form title  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

Tag: custom/auth-page/logon-form/title-background-color  
 Description: The background color of the logon form title  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

Tag: custom/auth-page/logon-form/font-color  
 Description: The font color of the logon form  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

Tag: custom/auth-page/logon-form/background-color  
 Description: The background color of the logon form  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

\*\*\*\*\*

Tag: custom/auth-page/logout-form  
 Description: Contains the logout form settings

Tag: custom/auth-page/logout-form/title-text  
 Description: The logout form title text  
 Value: arbitrary string  
 Default value: "Logout"

Tag: custom/auth-page/logout-form/message-text  
 Description: The logout form message text  
 Value: arbitrary string  
 Default value: Goodbye.  
                   For your own security, please:  
                   Clear the browser's cache

Delete any downloaded files  
Close the browser's window

Tag: custom/auth-page/logout-form/login-button-text  
Description: The text of the button sending the user to the logon page  
Value: arbitrary string  
Default value: "Logon"

\*\*\*\*\*

Tag: custom/auth-page/language-selector  
Description: Contains the language selector settings

Tag: custom/auth-page/language-selector/mode  
Description: The language selector mode  
Value: enable|disable  
Default value: disable

Tag: custom/auth-page/language-selector/title  
Description: The language selector title  
Value: arbitrary string  
Default value: empty string

Tag: custom/auth-page/language-selector/language (multiple)  
Description: Contains the language settings

Tag: custom/auth-page/language-selector/language/code  
Description: The code of the language  
Value (required): The language code string

Tag: custom/auth-page/language-selector/language/text  
Description: The text of the language in the language selector drop-down box  
Value (required): arbitrary string

\*\*\*\*\*

Tag: custom/portal  
Description: Contains portal page settings

\*\*\*\*\*

Tag: custom/portal/window  
Description: Contains the portal page browser window settings

Tag: custom/portal/window/title-text  
Description: The title of the browser window of the portal page  
Value: arbitrary string  
Default value: Browser's default value

\*\*\*\*\*

Tag: custom/portal/title-panel  
Description: Contains settings for the title panel

Tag: custom/portal/title-panel/mode  
Description: The title panel mode  
Value: enable|disable  
Default value: disable

Tag: custom/portal/title-panel/text  
Description: The title panel text.  
Value: arbitrary string  
Default value: empty string

Tag: custom/portal/title-panel/logo-url  
 Description: The URL of the logo image (imported via "import webvpn webcontent")  
 Value: URL string  
 Default value: empty image URL

Tag: custom/portal/title-panel/background-color  
 Description: The background color of the title panel  
 Value: HTML color format, for example #FFFFFF  
 Default value: #FFFFFF

Tag: custom/auth-pa/title-panel/font-color  
 Description: The background color of the title panel  
 Value: HTML color format, for example #FFFFFF  
 Default value: #000000

Tag: custom/portal/title-panel/font-weight  
 Description: The font weight  
 Value: CSS font size value, for example bold, bolder, lighter etc.  
 Default value: empty string

Tag: custom/portal/title-panel/font-size  
 Description: The font size  
 Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.  
 Default value: empty string

Tag: custom/portal/title-panel/gradient  
 Description: Specifies using the background color gradient  
 Value: yes|no  
 Default value: no

Tag: custom/portal/title-panel/style  
 Description: CSS style for title text  
 Value: CSS style string  
 Default value: empty string

\*\*\*\*\*

Tag: custom/portal/application (multiple)  
 Description: Contains the application setting

Tag: custom/portal/application/mode  
 Description: The application mode  
 Value: enable|disable  
 Default value: enable

Tag: custom/portal/application/id  
 Description: The application ID. Standard application ID's are: home, web-access, file-access, app-access, network-access, help  
 Value: The application ID string  
 Default value: empty string

Tag: custom/portal/application/tab-title  
 Description: The application tab text in the navigation panel  
 Value: arbitrary string  
 Default value: empty string

Tag: custom/portal/application/order  
 Description: The order of the application's tab in the navigation panel. Applications with lesser order go first.  
 Value: arbitrary number  
 Default value: 1000

Tag: custom/portal/application/url-list-title  
 Description: The title of the application's URL list pane (in group mode)  
 Value: arbitrary string



Default value: Tab title value concatenated with "Bookmarks"

\*\*\*\*\*

Tag: custom/portal/navigation-panel

Description: Contains the navigation panel settings

Tag: custom/portal/navigation-panel/mode

Description: The navigation panel mode

Value: enable|disable

Default value: enable

\*\*\*\*\*

Tag: custom/portal/toolbar

Description: Contains the toolbar settings

Tag: custom/portal/toolbar/mode

Description: The toolbar mode

Value: enable|disable

Default value: enable

Tag: custom/portal/toolbar/prompt-box-title

Description: The universal prompt box title

Value: arbitrary string

Default value: "Address"

Tag: custom/portal/toolbar/browse-button-text

Description: The browse button text

Value: arbitrary string

Default value: "Browse"

Tag: custom/portal/toolbar/logout-prompt-text

Description: The logout prompt text

Value: arbitrary string

Default value: "Logout"

\*\*\*\*\*

Tag: custom/portal/column (multiple)

Description: Contains settings of the home page column(s)

Tag: custom/portal/column/order

Description: The order the column from left to right. Columns with lesser order values go first

Value: arbitrary number

Default value: 0

Tag: custom/portal/column/width

Description: The home page column width

Value: percent

Default value: default value set by browser

Note: The actual width may be increased by browser to accommodate content

\*\*\*\*\*

Tag: custom/portal/url-lists

Description: Contains settings for URL lists on the home page

Tag: custom/portal/url-lists/mode

Description: Specifies how to display URL lists on the home page:

group URL lists by application (group) or

show individual URL lists (nogroup).

URL lists fill out cells of the configured columns, which are not taken by custom panes.  
Use the attribute value "nodisplay" to not show URL lists on the home page.

Value: group|nogroup|nodisplay

Default value: group

\*\*\*\*\*

Tag: custom/portal/pane (multiple)

Description: Contains settings of the custom pane on the home page

Tag: custom/portal/pane/mode

Description: The mode of the pane

Value: enable|disable

Default value: disable

Tag: custom/portal/pane/title

Description: The title of the pane

Value: arbitrary string

Default value: empty string

Tag: custom/portal/pane/notitle

Description: Hides pane's title bar

Value: yes|no

Default value: no

Tag: custom/portal/pane/type

Description: The type of the pane. Supported types:

TEXT - inline arbitrary text, may contain HTML tags;

HTML - HTML content specified by URL shown in the individual iframe;

IMAGE - image specified by URL

RSS - RSS feed specified by URL

Value: TEXT|HTML|IMAGE|RSS

Default value: TEXT

Tag: custom/portal/pane/url

Description: The URL for panes with type HTML, IMAGE or RSS

Value: URL string

Default value: empty string

Tag: custom/portal/pane/text

Description: The text value for panes with type TEXT

Value: arbitrary string

Default value: empty string

Tag: custom/portal/pane/column

Description: The column where the pane located.

Value: arbitrary number

Default value: 1

Tag: custom/portal/pane/row

Description: The row where the pane is located

Value: arbitrary number

Default value: 1

Tag: custom/portal/pane/height

Description: The height of the pane

Value: number of pixels

Default value: default value set by browser

\*\*\*\*\*

Tag: custom/portal/browse-network-title

Description: The title of the browse network link  
 Value: arbitrary string  
 Default value: Browse Entire Network

Tag: custom/portal/access-network-title  
 Description: The title of the link to start a network access session  
 Value: arbitrary string  
 Default value: Start AnyConnect

```
-->
- <custom>
- <localization>
<languages>en,ja,zh,ru,ua</languages>
<default-language>en</default-language>
</localization>
- <auth-page>
- <window>
- <title-text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</title-text>
</window>
- <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
- <language>
<code>en</code>
<text>English</text>
</language>
- <language>
<code>zh</code>
<text>?? (Chinese)</text>
</language>
- <language>
<code>ja</code>
<text>?? (Japanese)</text>
</language>
- <language>
<code>ru</code>
<text>?????? (Russian)</text>
</language>
- <language>
<code>ua</code>
<text>???????? (Ukrainian)</text>
</language>
</language-selector>
- <logon-form>
- <title-text l10n="yes">
- <![CDATA[
Login
]]>
</title-text>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
```

```

- <message-text l10n="yes">
- <![CDATA[
Please enter your username and password.
]]>
</message-text>
- <username-prompt-text l10n="yes">
- <![CDATA[
USERNAME:
]]>
</username-prompt-text>
- <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:
]]>
</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
- <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:
]]>
</group-prompt-text>
- <submit-button-text l10n="yes">
- <![CDATA[
Login
]]>
</submit-button-text>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
- <logout-form>
- <title-text l10n="yes">
- <![CDATA[
Logout
]]>
</title-text>
- <message-text l10n="yes">
- <![CDATA[
Goodbye.
]]>
</message-text>
</logout-form>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/cisco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[

```

```

#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
- <info-panel>
<mode>disable</mode>
<image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
- <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
</auth-page>
- <portal>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/cisco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>

```

```

- <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
- <application>
<mode>enable</mode>
<id>web-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Web Applications
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks
]]>
</url-list-title>
<order>2</order>
</application>
- <application>
<mode>enable</mode>
<id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks
]]>
</url-list-title>
<order>3</order>
</application>
- <application>
<mode>enable</mode>
<id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access
]]>
</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>net-access</id>
<tab-title l10n="yes">AnyConnect</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>help</id>
<tab-title l10n="yes">Help</tab-title>
<order>1000000</order>
</application>
- <toolbar>
<mode>enable</mode>
<logout-prompt-text l10n="yes">Logout</logout-prompt-text>
<prompt-box-title l10n="yes">Address</prompt-box-title>
<browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>

```

```

- <column>
 <width>100%</width>
 <order>1</order>
</column>
- <pane>
 <type>TEXT</type>
 <mode>disable</mode>
 <title />
 <text />
 <notitle />
</column>
</row>
<height />
</pane>
- <pane>
 <type>IMAGE</type>
 <mode>disable</mode>
 <title />
 <url l10n="yes" />
 <notitle />
</column>
</row>
<height />
</pane>
- <pane>
 <type>HTML</type>
 <mode>disable</mode>
 <title />
 <url l10n="yes" />
 <notitle />
</column>
</row>
<height />
</pane>
- <pane>
 <type>RSS</type>
 <mode>disable</mode>
 <title />
 <url l10n="yes" />
 <notitle />
</column>
</row>
<height />
</pane>
- <url-lists>
 <mode>group</mode>
</url-lists>
</portal>
</custom>

```

## Help Customization

The ASA displays help content on the application panes during clientless sessions. Each clientless application pane displays its own help file content using a predetermined filename. For example, the help content displayed on the Application Access panel is from the file named app-access-hlp.inc. [Table 91-10](#) shows the clientless application panels and predetermined filenames for the help content.

**Table 91-10** Clientless Applications

Application Type	Panel	Filename
Standard	Application Access	app-access-hlp.inc
Standard	Browse Networks	file-access-hlp.inc
Standard	AnyConnect Client	net-access-hlp.inc
Standard	Web Access	web-access-hlp.inc
Plug-in	MetaFrame Access	ica-hlp.inc
Plug-in	Terminal Servers	rdp-hlp.inc
Plug-in	Telnet/SSH Servers <sup>1</sup>	ssh,telnet-hlp.inc
Plug-in	VNC Connections	vnc-hlp.inc

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

You can customize the help files provided by Cisco or create help files in other languages. Then use the Import button to copy them to the flash memory of the ASA for display during subsequent clientless sessions. You can also export previously imported help content files, customize them, and reimport them to flash memory.

The following sections describe how to customize or create help content visible on clientless sessions:

- [Customizing a Help File Provided By Cisco](#)
- [Creating Help Files for Languages Not Provided by Cisco](#)

## Detailed Steps

- 
- Step 1** Click **Import** to launch the Import Application Help Content dialog, where you can import new help content to flash memory for display during clientless sessions.
- Step 2** (Optional) Click **Export** to retrieve previously imported help content selected from the table.
- Step 3** (Optional) Click **Delete** to delete previously imported help content selected from the table.
- Step 4** The abbreviation of the language rendered by the browser is displayed. This field is *not* used for file translation; it indicates the language used in the file. To identify the name of a language associated with an abbreviation in the table, display the list of languages rendered by your browser. For example, a dialog window displays the languages and associated language codes when you use one of the following procedures:
- Open Internet Explorer and choose **Tools > Internet Options > Languages > Add**.
  - Open Mozilla Firefox and choose **Tools > Options > Advanced > General**, click **Choose** next to Languages, and click **Select a language to add**.

The filename that the help content file was imported as is provided.

---

## Customizing a Help File Provided by Cisco

To customize a help file provided by Cisco, you need to get a copy of the file from the flash memory card first. Get the copy and customize it by performing the following steps:



- Step 1** Use your browser to establish a clientless session with the ASA.
- Step 2** Display the help file by appending the string in “URL of Help File in Flash Memory of the Security Appliance” in [Table 91-11](#), to the address of the ASA, substituting *language* as described below, then press **Enter**.

**Table 91-11 Help Files Provided by Cisco for Clientless Applications**

Application Type	Panel	URL of Help File in Flash Memory of the Security Appliance
Standard	Application Access	/+CSCOE+/help/ <i>language</i> /app-access-hlp.inc
Standard	Browse Networks	/+CSCOE+/help/ <i>language</i> /file-access-hlp.inc
Standard	AnyConnect Client	/+CSCOE+/help/ <i>language</i> /net-access-hlp.inc
Standard	Web Access	/+CSCOE+/help/ <i>language</i> /web-access-hlp.inc
Plug-in	Terminal Servers	/+CSCOE+/help/ <i>language</i> /rdp-hlp.inc
Plug-in	Telnet/SSH Servers	/+CSCOE+/help/ <i>language</i> /ssh,telnet-hlp.inc
Plug-in	VNC Connections	/+CSCOE+/help/ <i>language</i> /vnc-hlp.inc

*language* is the abbreviation for the language rendered by the browser. It is *not* used for file translation; it indicates the language used in the file. For help files provided by Cisco in English, enter the abbreviation **en**.

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

**https://address\_of\_security\_appliance/+CSCOE+/help/en/rdp-hlp.inc**

- Step 3** Choose **File > Save (Page) As**.



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

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

- Step 5** Use your preferred HTML editor to customize the file.



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

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

- Step 7** Make sure the filename matches the one in [Table 91-12](#), and that it does not have an extra filename extension.

Return to ASDM and choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import** to import the modified help file into flash memory.

## Creating Help Files for Languages Not Provided by Cisco

Use standard HTML to create help files in other languages. We recommend creating a separate folder for each language you want to support.

**Note**

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

Save the file as HTML only. Use the filename in the Filename column.

Return to ASDM and choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import** to import the new help file into flash memory.

## Import/Export Application Help Content

Use the Import Application Help Content dialog box to import help files to flash memory for display on the portal pages during clientless sessions. Use the Export Application Help Content dialog box to retrieve previously imported help files for subsequent editing.

### Detailed Steps

- 
- Step 1** The Language field specifies the language rendered by the browser but is not used for file translation. (This field is inactive in the Export Application Help Content dialog box.) Click the dots next to the Language field and double-click the row containing the language shown in the Browse Language Code dialog box. Confirm the abbreviation in the Language Code field matches the abbreviation in the row and click **OK**.
- Step 2** If the language for which you want to provide help content is not present in the Browse Language Code dialog box, perform the following
1. Display the list of languages and abbreviations rendered by your browser.
  2. Enter the abbreviation for the language in the Language Code field and click **OK**.
- OR
- You can also enter it into the Language text box to the left of the dots.
- A dialog box displays the languages and associated language codes when you use one of the following procedures:
- Open Internet Explorer and choose **Tools > Internet Options > Languages > Add**.
  - Open Mozilla Firefox and choose **Tools > Options > Advanced > General**, click **Choose** next to Languages, and click **Select a language to add**.
- Step 3** If you are importing, choose the new help content file from the File Name drop-down list. If you are exporting, this field is unavailable.
- Step 4** Configure the parameters for the source file (if importing) or destination file (if exporting):
- Local computer—Indicate if the source or destination file is on a local computer:
    - Path—Identify the path of the source or destination file.
    - Browse Local Files—Click to browse the local computer for the source or destination file.
  - Flash file system—Indicate if the source or destination file is located in flash memory on the ASA:
    - Path—Identify the path of the source or destination file in flash memory.
    - Browse Flash—Click to browse the flash memory for the source or destination file.

- Remote server—Indicate if the source or destination file is on a remote server:
  - Path—Choose the file transfer (copy) method, either ftp, tftp, or http (for importing only), and specify the path.

## Customizing a Help File Provided by Cisco

To customize a help file provided by Cisco, you need to get a copy of the file from the flash memory card first. Get the copy and customize it by performing the following steps:

- Step 1** Use your browser to establish a clientless session with the ASA.
- Step 2** Display the help file by appending the string in “URL of Help File in Flash Memory of the Security Appliance” in Table 91-12, to the address of the ASA, substituting *language* as described below, then press **Enter**.

**Table 91-12 Help Files Provided by Cisco for Clientless Applications**

Application Type	Panel	URL of Help File in Flash Memory of the Security Appliance
Standard	Application Access	/+CSCOE+/help/ <i>language</i> /app-access-hlp.inc
Standard	Browse Networks	/+CSCOE+/help/ <i>language</i> /file-access-hlp.inc
Standard	AnyConnect Client	/+CSCOE+/help/ <i>language</i> /net-access-hlp.inc
Standard	Web Access	/+CSCOE+/help/ <i>language</i> /web-access-hlp.inc
Plug-in	Terminal Servers	/+CSCOE+/help/ <i>language</i> /rdp-hlp.inc
Plug-in	Telnet/SSH Servers	/+CSCOE+/help/ <i>language</i> /ssh,telnet-hlp.inc
Plug-in	VNC Connections	/+CSCOE+/help/ <i>language</i> /vnc-hlp.inc

*language* is the abbreviation for the language rendered by the browser. It is *not* used for file translation; it indicates the language used in the file. For help files provided by Cisco in English, enter the abbreviation **en**.

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

**`https://address_of_security_appliance/+CSCOE+/help/en/rdp-hlp.inc`**

- Step 3** Choose **File > Save (Page) As**.



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

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

- Step 5** Use your preferred HTML editor to customize the file.



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

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

- Step 7** Make sure the filename matches the one in [Table 91-12](#), and that it does not have an extra filename extension.

---

Return to ASDM and choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import** to import the modified help file into flash memory.

## Creating Help Files for Languages Not Provided by Cisco

Use standard HTML to create help files in other languages. We recommend creating a separate folder for each language you want to support.



### Note

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

Save the file as HTML only. Use the filename in the Filename column of [Table 91-14](#).

Return to ASDM and choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import** to import the new help file into flash memory.

## 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 menu next to the URL attributes in ASDM.

- Enables the plug-in for all future clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down menu next to the Address field of the portal page.

Table 91-13 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 91-13** *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 menu and enter the URL in the Address field to establish a connection.



**Note**

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

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

### Prerequisites

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



**Note**

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

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

### Requirements

- Per the GNU General Public License (GPL), Cisco redistributes plug-ins without having made any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.

- Clientless SSL VPN must be enabled on the ASA to provide remote access to the plug-ins.
- A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.
- Plug-ins require that ActiveX or Oracle Java Runtime Environment (JRE) 1.4.2 (or later) is enabled on the browser. There is no ActiveX version of the RDP plug-in for 64-bit browsers.

## RDP Plug-in ActiveX Debug Quick Reference

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

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

## Preparing the Security Appliance for a Plug-in

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

- 
- Step 1** Make sure clientless SSL VPN (“webvpn”) is enabled on an ASA interface.
  - Step 2** Install an SSL certificate onto the ASA interface to which remote users use a fully-qualified domain name (FQDN) to connect.



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

---

# Customizing Help

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

Each application panel displays its own help file content using a predetermined filename. The prospective location of each is in the `/+CSCOE+/help/language/` URL within flash memory of the ASA. [Table 91-14](#) shows the details about each of the help files you can maintain for VPN sessions.

**Table 91-14 VPN Application Help Files**

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

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

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

The following sections describe how to customize the help contents:

- [Customizing a Help File Provided By Cisco, page 91-127](#)
- [Creating Help Files for Languages Not Provided by Cisco, page 91-128](#)
- [Requiring Usernames and Passwords, page 91-128](#)

## Customizing a Help File Provided By Cisco

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

### Detailed Steps

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

- Step 2** Display the help file by appending the string in “URL of Help File in Flash Memory of the Security Appliance” in [Table 91-14](#), to the address of the ASA, then press Enter.



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

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

**`https://address_of_security_appliance/CSCOE/help/en/rdp-hlp.inc`**

- Step 3** Choose **File > Save (Page) As**.



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

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

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



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

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

- Step 7** Make sure the filename matches the one in [Table 91-14](#), and that it does not have an extra filename extension.

See “[Requiring Usernames and Passwords](#)” to import the modified file.

## Creating Help Files for Languages Not Provided by Cisco

Use HTML to create help files in other languages.

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

Save the file as HTML only. Use the filename following the last slash in “URL of Help File in Flash Memory of the Security Appliance” in [Table 91-14](#).

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

### Restrictions

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

## Requiring Usernames and Passwords

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



Table 91-15 lists the type of usernames and passwords that clientless SSL VPN users might need to know.

**Table 91-15** *Username and Passwords to Give to Users of Clientless SSL VPN Sessions*

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

## Communicating Security Tips

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

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

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

## Configuring Remote Systems to Use Clientless SSL VPN Features

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

- [Starting Clientless SSL VPN](#), page 91-130
- [Using the Clientless SSL VPN Floating Toolbar](#), page 91-130
- [Browsing the Web](#), page 91-131
- [Browsing the Network \(File Management\)](#), page 91-131
- [Using Port Forwarding](#), page 91-133
- [Using E-mail Via Port Forwarding](#), page 91-134

- [Using E-mail Via Web Access, page 91-135](#)
- [Using E-mail Via E-mail Proxy, page 91-135](#)
- [Using Smart Tunnel, page 91-135](#)

You may configure user accounts differently and different clientless SSL VPN features can be available to each user.

## Starting Clientless SSL VPN

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

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



### Note

See the [Cisco ASA 5500 Series VPN Compatibility Reference](#) for the list of web browsers supported by clientless SSL VPN.

### Prerequisites

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

### Restrictions

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

## Using the Clientless SSL VPN Floating Toolbar

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

The floating toolbar represents the current clientless SSL VPN session. If you click the **Close** button, the ASA prompts you to confirm that you want to close the clientless SSL VPN session.



### Tip

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

### Restrictions

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

## Browsing the Web

Using clientless SSL VPN does not ensure that communication with every site is secure. See [Communicating Security Tips](#).

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

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

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

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

### Prerequisites

- You need the username and password for protected websites.

### Restrictions

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

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

## Browsing the Network (File Management)

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



### Note

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

### Prerequisites

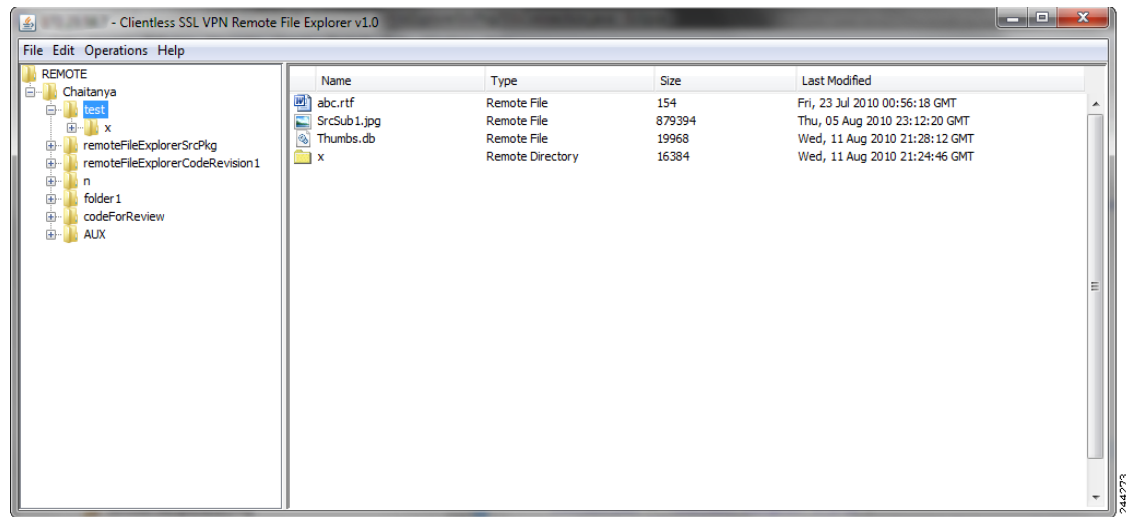
- You must configure file permissions for shared remote access.
- You must have the server names and passwords for protected file servers.
- You must have the domain, workgroup, and server names where folders and files reside.

### Restrictions

Only shared folders and files are accessible via clientless SSL VPN.

## Using the Remote File Explorer

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

**Figure 91-28** Clientless SSL VPN Remote File Explorer

The browser enables the user to:

- Browse the remote file system
- Rename files
- Move or copy files within the remote file system and between the remote and local file systems.
- Perform bulk uploads and downloads of files

**Note**

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

**Renaming a File or Folder**

To rename a file or folder:

- 
- Step 1** Click the file or folder to be renamed.
  - Step 2** Select **Edit > Rename**.
  - Step 3** When prompted, enter the new name in the dialog.
  - Step 4** Click **OK** to rename the file or folder. Alternative, click **Cancel** to leave the name unchanged.
- 

**Moving or Copying Files or Folders on the Remote Server**

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

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

**Step 5** Select **Edit > Paste**.

---

### Copying Files from the Local System Drive to the Remote Folder

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

### Uploading and Downloading Files

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

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

This functionality has the following restrictions:

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

## Using Port Forwarding



#### Note

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

#### Prerequisites

- On Mac OS X, only the Safari browser supports this feature.
- You must have client applications installed.
- You must have Cookies enabled on the browser.
- You must have administrator access on the PC if you use DNS names to specify servers, because modifying the hosts file requires it.
- You must have Oracle Java Runtime Environment (JRE) version 1.4.x and 1.5.x installed.

If JRE is not installed, a pop-up window displays, directing users to a site where it is available. On rare occasions, the port forwarding applet fails with Java exception errors. If this happens, do the following:

- a. Clear the browser cache and close the browser.

- b. Verify that no Java icons are in the computer task bar.
  - c. Close all instances of Java.
  - d. Establish a clientless SSL VPN session and launch the port forwarding Java applet.
- You must have JavaScript enabled on the browser. By default, it is enabled.
- If necessary, you must configure client applications.

**Note**

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

**Restrictions**

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

**Detailed Steps**

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

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

**Note**

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

## Using E-mail Via Port Forwarding

To use e-mail, start Application Access from the clientless SSL VPN home page. The mail client is then available for use.

**Note**

If you are using an IMAP client and you lose your mail server connection or are unable to make a new connection, close the IMAP application and restart clientless SSL VPN.

**Prerequisites**

You must fulfill requirements for application access and other mail clients.

**Restrictions**

We have tested Microsoft Outlook Express versions 5.5 and 6.0.

Clientless SSL VPN should support other SMTPS, POP3S, or IMAP4S e-mail programs via port forwarding, such as Lotus Notes and Eudora, but we have not verified them.

## Using E-mail Via Web Access

The following e-mail applications are supported:

- Microsoft Outlook Web App to Exchange Server 2010.  
OWA requires Internet Explorer 7 or later, or Firefox 3.01 or later.
- Microsoft Outlook Web Access to Exchange Server 2007, 2003, and 2000.  
For best results, use OWA on Internet Explorer 8.x or later, or Firefox 8.x.
- Lotus iNotes

**Prerequisites**

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

**Restrictions**

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

## Using E-mail Via E-mail Proxy

The following legacy e-mail applications are supported:

- Microsoft Outlook 2000 and 2002
- Microsoft Outlook Express 5.5 and 6.0

See the instructions and examples for your mail application in [Using E-Mail over Clientless SSL VPN](#).

**Prerequisites**

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

**Restrictions**

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

## Using Smart Tunnel

Administration privileges are not required to use Smart Tunnel.

**Note**

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

### Prerequisites

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

### Restrictions

- Mac OS X does not support a front-side proxy.
- Supports only the operating systems and browsers specified in [“Configuring Smart Tunnel Access” section on page 91-45](#).
- Only TCP socket-based applications are supported.

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

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

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

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

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



### Note

- Step 1** Navigate to **Configuration > Remote Access VPN > Language Localization**. The Language Localization pane displays. Click **Add**. The Add Language Localization window displays.
- Step 2** Choose a Language Localization Template from the drop-down box. The entries in the box correspond to functional areas that are translated.
- Step 3** Specify a language for the template. The template becomes a translation table in cache memory with the name you specify. Use an abbreviation that is compatible with the language options for your browser. For example, if you are creating a table for the Chinese language, and you are using IE, use the abbreviation *zh*, that is recognized by IE.
- Step 4** Edit the translation table. For each message represented by the msgid field that you want to translate, enter the translated text between the quotes of the associated msgstr field. The example below shows the message Connected, with the Spanish text in the msgstr field:

```
msgid "Connected"
msgstr "Conectado"
```



- Step 5** Click **OK**. The new table appears in the list of translation tables.

### Adding/Editing Localization Entry

You can add a new translation table, based on a template, or you can modify an already-imported translation table in this pane.

- Step 1** Select a template to modify and use as a basis for a new translation table. The templates are organized into translation domains and affect certain areas of functionality. The following table shows the translation domains and the functional areas affected:

Translation Domain	Functional Areas Translated
AnyConnect	Messages displayed on the user interface of the Cisco AnyConnect VPN client.
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	Messages on the logon and logout pages, portal page, and all the messages customizable by the user.
keepout	Message displayed to remote users when VPN access is denied.
PortForwarder	Messages displayed to Port Forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA and portal messages that are not customizable.
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.

- Step 2** Specify a language. Use an abbreviation that is compatible with the language options of your browser. The ASA creates the new translation table with this name.

- Step 3** Use the editor to change the message translations. The message ID field (msgid) contains the default translation. The message string field (msgstr) that follows msgid provides the translation. To create a translation, enter the translated text between the quotes of the msgstr string. For example, to translate the message “Connected” with a Spanish translation, insert the Spanish text between the msgstr quotes:

```
msgid "Connected"
msgstr "Conectado"
```

After making changes, click **Apply** to import the translation table.

## Customizing the AnyConnect Client

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

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

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

The following sections explain how to customize the AnyConnect client:

- [Customizing AnyConnect by Importing Resource Files, page 91-138](#)
- [Customizing Your Own AnyConnect GUI Text and Scripts, page 91-139](#)
- [Customizing AnyConnect GUI Text and Messages, page 91-142](#)
- [Customizing the Installer Program Using Installer Transforms, page 91-143](#)
- [Localizing the Install Program using Installer Transforms, page 91-144](#)

#### Restrictions

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

## Customizing AnyConnect by Importing Resource Files

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

#### Detailed Steps

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

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

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

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



#### Note

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

---

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

**Note**

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

- Step 4** Clicking **Import** launches the Import AnyConnect Customization Objects dialog, where you can specify a file to import as an object.
- Step 5** Clicking **Export** launches the Export AnyConnect Customization Objects dialog, where you can specify a file to export as an object.
- Step 6** Clicking **Delete** removes the selected object.
- The type of remote PC platform supported by the object and the object name is displayed.

## Customizing Your Own AnyConnect GUI Text and Scripts

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

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

- Refreshing the group policy upon VPN connection.
- Mapping a network drive upon VPN connection, and un-mapping it after disconnection.
- Logging on to a service upon VPN connection, and logging off after disconnection.

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

The following sections describe how to import binary executables and scripts to the ASA:

- [Importing your own GUI as a Binary Executable, page 91-139](#)
- [Importing Scripts, page 91-140](#)

### Importing your own GUI as a Binary Executable

For Windows, Linux, or Mac (PPP or Intel-based) computers, you can deploy your own client that uses the AnyConnect client API. You replace the AnyConnect GUI or the AnyConnect CLI by replacing the client binary files. [Table 91-16](#) lists the filenames of the client executable files for the different operating systems.

**Table 91-16** *Filenames of Client Executables*

Client OS	Client GUI File	Client CLI File
Windows	vpnui.exe	vpncli.exe

**Table 91-16** *Filename of Client Executables*

Client OS	Client GUI File	Client CLI File
Linux	vpnui	vpn
Mac	Not supported <sup>1</sup>	vpn

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

Your executable can call any resource files, such as logo images, that you import to the ASA (See [Table 91-16](#)). Unlike replacing the pre-defined GUI components, when you deploy your own executable, can use any filenames for your resource files.

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

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

### Restrictions

The ASA does not support this feature for the AnyConnect VPN client, Versions 2.0 and 2.1. For more information on manually customizing the client, see the *AnyConnect VPN Client Administrator Guide* and the *Release Notes for Cisco AnyConnect VPN Client*.

## Importing Scripts

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

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

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

### Prerequisites

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

**Restrictions**

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

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

**Writing, Testing, and Deploying Scripts**

Deploy AnyConnect scripts as follows:

**Restrictions**

- Scripts written on Microsoft Windows computers have different line endings than scripts written on Mac OS X and Linux. Therefore, you should write and test the script on the targeted OS. If a script cannot run properly from the command line on the native OS, AnyConnect cannot run it properly either.
- Microsoft Windows Mobile does not support this option. You must deploy scripts using the manual method for this OS.

- 
- Step 1** Write and test the script using the OS type on which it will run when AnyConnect launches it.
- Step 2** To import a script, go to **Network (Client) Access > AnyConnect Customization/Localization > Script**. The Customization Scripts pane displays.
- Step 3** Enter a name for the script. Be sure to specify the correct extension with the name. For example, *myscript.bat*.
- Step 4** Choose a script action: *Script runs when client connects* or *Script runs when client disconnects*.
- AnyConnect adds the prefix *scripts\_* and the prefix *OnConnect* or *OnDisconnect* to your filename to identify the file as a script on the ASA. When the client connects, the ASA downloads the script to the proper target directory on the remote computer, removing the *scripts\_* prefix and leaving the remaining *OnConnect* or *OnDisconnect* prefix. For example, if you import the script *myscript.bat*, the script appears on the ASA as *scripts\_OnConnect\_myscript.bat*. On the remote computer, the script appears as *OnConnect\_myscript.bat*.
- To ensure the scripts run reliably, configure all ASAs to deploy the same scripts. If you want to modify or replace a script, use the same name as the previous version and assign the replacement script to all of the ASAs that the users might connect to. When the user connects, the new script overwrites the one with the same name.
- Step 5** Select a file as the source of the script. The name does not need to be the same as the name you provided for the script. ASDM imports the file from any source file, creating the new name you specify for Name in Step 3.

Table 91-17 shows the locations of scripts on the remote computer:

**Table 91-17 Required Script Locations**

OS	Directory
Microsoft Windows 7 and Vista	%ALLUSERPROFILE%\Cisco\Cisco AnyConnect VPN Client\Scripts
Microsoft Windows XP	%ALLUSERPROFILE%\Application Data\Cisco\Cisco AnyConnect VPN Client\Scripts

**Table 91-17 Required Script Locations**

OS	Directory
Linux	/opt/cisco/vpn/scripts <b>Note</b> Assign execute permissions to the file for User, Group and Other.
Mac OS X	/opt/cisco/vpn/scripts
Windows Mobile	%PROGRAMFILES%\Cisco AnyConnect VPN Client\Scripts

- Step 6** Click **Import** to launch the Import AnyConnect Customization Objects dialog, where you can specify a file to import as an object.
- Step 7** Click **Export** to launch the Export AnyConnect Customization Objects dialog, where you can specify a file to export as an object.
- Step 8** Click **Delete** to remove a selected object.
- The type of remote PC platform supported by the object and the object name is displayed.

## Customizing AnyConnect GUI Text and Messages

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

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

- Step 1** Click **Template** to expand the template area. Click **Export** to export the English language template to your local PC or a remote device.
- Step 2** Edit the template and make changes to any messages. The text contained between the quotes of the msgid field represents the default text. *Do not* change this text. To display a different message, insert your custom text between the quotes of msgstr. The example below shows a message containing connection termination information:
- ```
msgid ""
"The VPN connection has been disconnected due to the system suspending. The
"reconnect capability is disabled. A new connection requires re-
"authentication and must be started manually. Close all sensitive networked
"applications."
msgstr ""
```
- Step 3** Click **Import** to import the file you edited as a new translation template.
- Step 4** Specify a language for the template. The template becomes a translation table in cache memory with the name you specify. Use an abbreviation that is compatible with the language options for your browser. For example, if you are creating a table for the Chinese language, and you are using IE, use the abbreviation *zh*, that is recognized by IE.
- Step 5** Click **Apply to make your changes to the ASA**.
- Step 6** (Optional) Click **Add** to launch the Add Localization Entry dialog where you can select a localization template to add and you can edit the contents of the template.
- Step 7** (Optional) Click **Edit** to launch the Edit Localization Entry dialog for the selected language in the table, and allows you to edit the previously-imported language localization table.

- Step 8** (Optional) Click **Delete** to delete a selected language localization table.
 - Step 9** (Optional) Click **Import** to launch the Import Language Localization dialog where you can import a language localization template or table.
 - Step 10** (Optional) Click **Export** to launch the Export Language Localization dialog where you can export a language localization template or table to a URL where you can make changes to the table or template.
 - Step 11** (Optional) Specify the language of the localization table.
-

Customizing the Installer Program Using Installer Transforms

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

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


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

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

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

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

To import your transform, follow these steps:

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

Note Windows is the only valid choice for applying a transform.
-
- Step 4** (Optional) Click **Import** to launch the Import AnyConnect Customization Objects dialog, where you can specify a transform file to import.
 - Step 5** (Optional) Click **Export** to launch the Export AnyConnect Customization Objects dialog, where you can specify a transform file to export.
 - Step 6** (Optional) Click **Delete** to remove the selected file.

The type of remote PC platform supported by the transform and the name of the transform is displayed.

Configuration Example for Transform

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

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

Directory_ Attributes Condition KeyPath
Profile_DIR 0 MyProfile.xml

DATA CHANGE - FeatureComponents Feature_ Component_
+ MainFeature MyProfile.xml

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

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

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

Localizing the Install Program using Installer Transforms

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

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

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

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

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

The package contains the transforms (.mst files) for the available translations. If you need to provide a language to remote users that is not one of the 30 languages we provide, you can create your own transform and import it to the ASA as a new language. With Orca, the database editor from Microsoft, you can modify existing installations and new files. Orca is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK. The following link leads to the bundle containing the Orca program:

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

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

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

The following procedure shows how to import a transform to the ASA using ASDM:

-
- Step 1** Import a Transform. Go to: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Localized Installer Transforms**. Click **Import**. The Import MST Language Localization window opens.
- Step 2** Choose a language for this transform. Click the Language drop-list to display languages and their industry-recognized abbreviations. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.
- Step 3** Click **Import Now**. A message displays saying you successfully imported the table.
Be sure to click **Apply** to save your changes.
- Step 4** (Optional) Click **Import** to launch the Import AnyConnect Customization Objects dialog, where you can specify a file to import as a transform.
- Step 5** (Optional) Click **Export** to launch the Export AnyConnect Customization Objects dialog, where you can specify a file to export as a transform.
- Step 6** (Optional) Click **Delete** to remove the selected transform.
The type of remote PC platform supported by the transform and the name are displayed.
-

Importing/Exporting Language Localization

In the Import Translation Table and Export Translation Table dialog boxes, you can import or export a translation table to the ASA to provide translation of user messages.

Translation templates are XML files that contain message fields that can be edited with translated messages. You can export a template, edit the message fields, and import the template as a new translation table, or you can export an existing translation table, edit the message fields, and re-import the table to overwrite the previous version.

Detailed Steps

-
- Step 1** Enter a name for the language.
- When *exporting*, it is automatically filled-in with the name from the entry you selected in the table.
 - When *importing*, you enter the language name in the manner that you want it to be identified. The imported translation table then appears in the list with the abbreviation you designated. To ensure that your browser recognizes the language, use language abbreviations that are compatible with the language options of the browser. For example, if you are using IE, use **zh** as the abbreviation for the Chinese language.
- Step 2** The name of the XML file containing the message fields includes the following:
- AnyConnect—Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
 - CSD—Messages for the Cisco Secure Desktop (CSD).
 - customization—Messages on the logon and logout pages, portal page, and all the messages customizable by the user.
 - keepout—Message displayed to remote users when VPN access is denied.
 - PortForwarder—Messages displayed to Port Forwarding users.
 - url-list—Text that user specifies for URL bookmarks on the portal page.

- webvpn—All the layer 7, AAA and portal messages that are not customizable.
- plugin-ica—Messages for the Citrix plug-in.
- plugin-rdp—Messages for the Remote Desktop Protocol plug-in.
- plugin-telnet,ssh—Messages for the TELNET and SSH plug-in. This plug-in is capable of doing both sshv1 and sshv2.
- plugin-vnc—Messages for the VNC plug-in.

Step 3 Choose the method by which you want to import or export the file:

- Remote server—Select this option to import a customization file that resides on a remote server accessible from the ASA.
- Path—Identify the method to access the file (ftp, http, or https), and provide the file location.
- Flash file system—Choose this method to export a file that resides on the ASA.
- Path—File location.
- Browse Flash—Browse to the path for the file.
- Local computer—Choose this method to import a file that resides on the local PC.
- Path—Provide the path to the file.
- Browse Local Files—Browse to the path for the file.

Step 4 Click **Import/Export Now** to import or export the file.

Configuring Bookmarks

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

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

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

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

Guidelines

Configuring bookmarks does not prevent the user from visiting fraudulent sites or sites that violate your company's acceptable use policy. In addition to assigning a bookmark list to the group policy, dynamic access policy, or both, apply a web ACL to these policies to control access to traffic flows. Disable URL Entry on these policies to prevent user confusion over what is accessible. See the [“Observing Clientless SSL VPN Security Precautions”](#) section on page 91-5 for instructions.

Detailed Steps

-
- Step 1** Specify the name of the list to be added or select the name of the list to be modified or deleted. The bookmark title and actual associated URL are displayed.
- Step 2** (Optional) Click **Add** to configure a new server or URL. See these procedures for additional information:
- [Adding a Bookmark for a URL with a GET or Post Method, page 91-147](#)
 - [Adding a URL for a Predefined Application Template, page 91-148](#)
 - [Adding a Bookmark for an Auto Sign-On Application, page 91-150](#)
- Step 3** (Optional) Click **Edit** to make changes to the server, URL, or display name.
- Step 4** (Optional) Click **Delete** to remove the selected item from the URL list. No confirmation or undo exists.
- Step 5** (Optional) Choose the location from which you want to import or export the file:
- Local computer—Click to import or export a file that resides on the local PC.
 - Flash file system—Click to import or export a file that resides on the ASA.
 - Remote server—Click to import a file that resides on a remote server accessible from the ASA.
 - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
 - Browse Local Files.../Browse Flash...—Browse to the path for the file.
- Step 6** (Optional) Highlight a bookmark and click **Assign** to assign the selected bookmark to one or more group policies, dynamic access policies, or LOCAL users.
- Step 7** (Optional) Change the position of the selected item in the URL list using the **Move Up** or **Move Down** options.
- Step 8** Click OK.
-

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

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

Prerequisites

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

Detailed Steps

-
- Step 1** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**, and click the **Add** button.
- Step 2** Select **URL with GET or POST method** to use for bookmark creation.
- Step 3** Enter a name for this bookmark, which will be displayed on the portal.
- Step 4** Use the URL drop-down menu to select the URL type: http, https, cifs, or ftp. The URL drop-down shows standard URL types, plus types for all the plug-ins you installed.

- Step 5** Enter the DNS name or IP address for this bookmark (URL). For a plug-in, enter the name of the server. Enter a forward slash and a question mark (/?) after the server name to specify optional parameters, then use an ampersand to separate parameter-value pairs, as shown in the following syntax:

```
server/?Parameter=Value&Parameter=Value
```

For example:

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

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

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

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

- Step 6** (Optional) Enter a preload URL. When you enter a preload URL, you can also enter the wait time, which is the time you allow for loading of the page until you are forwarded to the actual POST URL.
- Step 7** As a subtitle, provide additional user-visible text that describes the bookmark entry.
- Step 8** Use the Thumbnail drop-down menu to select an icon to associate with the bookmark on the end-user portal.
- Step 9** Click **Manage** to import or export images to use as thumbnails.
- Step 10** Click to open the bookmark in a new window that uses the smart tunnel feature to pass data through the ASA to or from the destination server. All browser traffic passes securely over the SSL VPN tunnel. This option lets you provide smart tunnel support for a browser-based application, whereas the Smart Tunnels option, also in the Clientless SSL VPN > Portal menu, lets you add nonbrowser-based applications to a smart tunnel list for assignment to group policies and usernames.
- Step 11** Check **Allow the users to bookmark the link** to let clientless SSL VPN users use the Bookmarks or Favorites options on their browsers. Uncheck to prevent access to these options. If you uncheck this option, the bookmark does not appear in the Home section of the WebVPN portal.
- Step 12** (Optional) Choose **Advanced Options** to configure further bookmark characteristics.
- URL Method—Choose **Get** for simple data retrieval. Choose **Post** when processing the data might involve changes to it, for example, storing or updating data, ordering a product, or sending e-mail.
 - Post Parameters—Configure the particulars of the Post URL method.
 - Add/Edit—Click to add a post parameter.
 - Edit—Click to edit the highlighted post parameter.
 - Delete—Click to delete the highlighted post parameter.

Adding a URL for a Predefined Application Template

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

Prerequisites

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

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010

- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010

Detailed Steps

-
- Step 1** Enter a name for the bookmark to display for the user.
- Step 2** As a subtitle, provide additional user-visible text that describes the bookmark entry.
- Step 3** Use the **Thumbnail** drop-down menu to select an icon to associate with the bookmark on the end-user portal.
- Step 4** Click **Manage** to import or export images to use as thumbnails.
- Step 5** (Optional) Select the **Place this bookmark on the VPN home page** check box.
- Step 6** In the **Select Auto Sign-on Application** list, click the required application. The available applications are:
- Citrix XenApp
 - Citrix XenDesktop
 - Domino WebAccess
 - Microsoft Outlook Web Access 2010
 - Microsoft Sharepoint 2007
 - Microsoft SharePoint 2010
- Step 7** Enter the URL of the page which is loaded before the login page. This page will require user interaction to proceed to the login screen. The URL will allow * to substitute an arbitrary number of symbols, for example `http*://www.example.com/test`.
- Step 8** Enter the **Pre-login Page Control ID**. This is the ID of the control / tag that will get a click event on the pre-login page URL to proceed to the login page.
- Step 9** Enter the **Application Parameters**. Depending on the application these may include the following:
- **Protocol**. HTTP or HTTPS.
 - **Host Name**. For example `www.cisco.com`.
 - **Port Number**. The port used by the application.
 - **URL Path Appendix**. For example `/Citrix/XenApp`. This is normally auto-populated.
 - **Domain**. The domain to connect to
 - **User Name**. The SSL VPN Variable to use as a user name. Click **Select Variable** to choose a different variable.
 - **Password**. The SSL VPN Variable to use as a password. Click **Select Variable** to choose a different variable.
- Step 10** (Optional) Click **Preview** to view the template output. You can click **Edit** to modify the template.
- Step 11** Click **OK** to make your changes. Alternatively, click **Cancel** to abandon your changes.
-

Adding a Bookmark for an Auto Sign-On Application

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

Prerequisites

Configuring auto sign-on applications requires two steps:

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

Detailed Steps

-
- Step 1** Enter a name for the bookmark to display for the user.
- Step 2** Use the URL drop-down menu to select the URL type: http, https, cifs, or ftp. The URL types of all imported plug-ins also populate this menu. Select the URL type of a plug-in if you want to display the plug-in as a link on the portal page.
- Step 3** Enter the DNS name or IP address for the bookmark. For a plug-in, enter the name of the server. Enter a forward slash and a question mark (?) after the server name to specify optional parameters, then use an ampersand to separate parameter-value pairs, as shown in the following syntax:
- server/?Parameter=Value&Parameter=Value*
- For example:
- host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768*
- The particular plug-in determines the optional parameter-value pairs that you can enter.
- To provide single sign-on support for a plug-in, use the parameter-value pair **cisco_sso=1**. For example:
- host/?cisco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768*
- Step 4** As a subtitle, provide additional user-visible text that describes the bookmark entry.
- Step 5** Use the **Thumbnail** drop-down menu to select an icon to associate with the bookmark on the end-user portal.
- Step 6** Click **Manage** to import or export images to use as thumbnails.
- Step 7** (Optional) Select the **Place this bookmark on the VPN home page** check box.
- Step 8** Enter the **Login Page URL**. Wildcards can be used in the URL you enter. For example, you can enter `http*://www.example.com/myurl*`.
- Step 9** Enter the **Landing Page URL**. The ASA requires the Landing Page to be configured to detect a successful login to the application.
- Step 10** (Optional) Enter a **Post Script**. Some Web applications, such as Microsoft Outlook Web Access, may execute a JavaScript to change the request parameters before the log-on form is submitted. The **Post Script** field enables you to enter JavaScript for such applications.
- Step 11** Add the required **Form Parameters**. For each required SSL VPN Variable, click **Add**, enter a **Name**, and select a variable from the list. You can click **Edit** to change parameters and **Delete** to remove them.
- Step 12** Enter the URL of the page which is loaded before the login page. This page will require user interaction to proceed to the login screen. The URL will allow * to substitute an arbitrary number of symbols, for example `http*://www.example.com/test`.

- Step 13** Enter the **Pre-login Page Control ID**. This is the ID of the control / tag that will get a click event on the pre-login page URL to proceed to the login page.
- Step 14** Click **OK** to make your changes. Alternatively, click **Cancel** to abandon your changes.

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

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

Importing/Exporting Bookmark List

You can import or export already configured bookmark lists. Import lists that are ready to use. Export lists to modify or edit them, and then reimport.

Detailed Steps

-
- Step 1** Identify the bookmark list by name. Maximum is 64 characters, no spaces.
- Step 2** Choose the method by which you want to import or export the list file:
- Local computer—Click to import a file that resides on the local PC.
 - Flash file system—Click to export a file that resides on the ASA.
 - Remote server—Click to import a url list file that resides on a remote server accessible from the ASA.
 - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
 - Browse Local Files/Browse Flash—Browse to the path for the file.
 - Import/Export Now—Click to import or export the list file.

Importing/Exporting GUI Customization Objects (Web Contents)

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

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

-
- Step 1** Choose the location from which you want to import or export the file:
- Local computer—Click to import or export a file that resides on the local PC.
 - Flash file system—Click to import or export a file that resides on the ASA.
 - Remote server—Click to import a file that resides on a remote server accessible from the ASA.
 - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
 - Browse Local Files.../Browse Flash...—Browse to the path for the file.

- Step 2** Determine whether authentication is required to access the content.
- The prefix to the path changes depending on whether you require authentication. The ASA uses `/+CSCOE+/` for objects that require authentication, and `/+CSCOU+/` for objects that do not. The ASA displays `/+CSCOE+/` objects on the portal page only, while `/+CSCOU+/` objects are visible and usable in either the logon or the portal pages.
- Step 3** Click to import or export the file.
-

Adding/Editing Post Parameter

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

Clientless SSL VPN variables allow for substitutions in URLs and forms-based HTTP post operations. These variables, also known as macros, let you configure users for access to personalized resources that contain the user ID and password or other input parameters. Examples of such resources include bookmark entries, URL lists, and file shares.

Detailed Steps

- Step 1** Provide the name and value of the parameters exactly as in the corresponding HTML form, for example: `<input name="param_name" value="param_value">`.

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

Table 91-18 Clientless SSL VPN Variables

| No. | Variable Substitution | Definition |
|-----|--------------------------------|---|
| 1 | CSCO_WEBVPN_USERNAME | SSL VPN user login ID |
| 2 | CSCO_WEBVPN_PASSWORD | SSL VPN user login password |
| 3 | CSCO_WEBVPN_INTERNAL_PASSWORD | SSL VPN user internal resource password. This is a cached credential, and not authenticated by a AAA server. If a user enters this value, it is used as the password for auto-signon, instead of the password value. |
| 4 | CSCO_WEBVPN_CONNECTION_PROFILE | SSL VPN user login group drop-down, a group alias within the connection profile |
| 5 | CSCO_WEBVPN_MACRO1 | Set via RADIUS/LDAP vendor-specific attribute. If you are mapping this from LDAP via an ldap-attribute-map, the Cisco attribute that uses this variable is WEBVPN-Macro-Substitution-Value1.

Variable substitution via RADIUS is performed by VSA#223. |
| 6 | CSCO_WEBVPN_MACRO2 | Set via RADIUS/LDAP vendor-specific attribute. If you are mapping this from LDAP via an ldap-attribute-map, the Cisco attribute that uses this variable is WEBVPN-Macro-Substitution-Value2.

Variable substitution via RADIUS is performed by VSA#224. |
| 7 | CSCO_WEBVPN_PRIMARY_USERNAME | Primary user login ID for double authentication. |

Table 91-18 Clientless SSL VPN Variables

| No. | Variable Substitution | Definition |
|-----|--------------------------------|--|
| 8 | CSCO_WEBVPN_PRIMARY_PASSWORD | Primary user login password for double authentication. |
| 9 | CSCO_WEBVPN_SECONDARY_USERNAME | Secondary user login ID for double authentication. |
| 10 | CSCO_WEBVPN_SECONDARY_PASSWORD | Secondary user login ID for double authentication. |

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

**Note**

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

Using Variables 1 - 4

The ASA obtains values for the first four substitutions from the SSL VPN Login page, which includes fields for username, password, internal password (optional), and group. It recognizes these strings in user requests and replaces them with the value specific to the user before it passes the request on to a remote server.

For example, if a URL list contains the link, http://someserver/homepage/CSCO_WEBVPN_USERNAME.html, the ASA translates it to the following unique links:

- For USER1 the link becomes <http://someserver/homepage/USER1.html>
- For USER2 the link is <http://someserver/homepage/USER2.html>

In the following case, cifs://server/users/CSCO_WEBVPN_USERNAME, lets the ASA map a file drive to specific users:

- For USER1 the link becomes <cifs://server/users/USER1>
- For USER2 the link is <cifs://server/users/USER2>

Using Variables 5 and 6

Values for macros 5 and 6 are RADIUS or LDAP vendor-specific attributes (VSAs). These substitutions let you set substitutions configured on either a RADIUS or an LDAP server.

Using Variables 7 - 10

Each time the ASA recognizes one of these four strings in an end-user request (a bookmark or a post form), it replaces it with the user-specific value before passing the request to a remote server.

Example 1: Setting a Homepage

The following example sets a URL for the homepage:

- WebVPN-Macro-Value1 (ID=223), type string, is returned as wwwin-portal.example.com
- WebVPN-Macro-Value2 (ID=224), type string, is returned as 401k.com

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

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

The best way to do this is to configure the Homepage URL parameter in ASDM. Without writing a script or uploading anything, an administrator can specify which homepage in the group policy to connect with via smart tunnel.

Go to the Add/Edit Group Policy pane, from either the Network Client SSL VPN or Clientless SSL VPN Access section of ASDM. The paths are as follows:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Group Policy > Advanced > SSL VPN Client > Customization > Homepage URL attribute.
- Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add/Edit Group Policy > More Options > Customization > Homepage URL attribute.

Configuration Example for Setting a Bookmark or URL Entry

You can use an HTTP Post to log in to an OWA resource using an RSA one-time password (OTP) for SSL VPN authentication, and then the static, internal password for OWA e-mail access. The best way to do this is to add or edit a bookmark entry in ASDM.

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

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

or

(Available after you click **Post** in the URL Method attribute):

- Network (Client) Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > URL Lists tab > Manage button > Configured GUI Customization Objects > Add/Edit button > Add/Edit Bookmark List > Add/Edit Bookmark Entry > Advanced Options area > Add/Edit Post Parameters.

Configuration Example for Configuring File Share (CIFS) URL Substitutions

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

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

`cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server`

`cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server`

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

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

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

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

Configuration Example for Customizing External Ports

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

Detailed Steps

-
- | | |
|---------------|---|
| Step 1 | Choose Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization . Highlight the desired customization and choose Edit . |
| Step 2 | Check the Enable External Portal check box. |
| Step 3 | In the URL field, enter the desired external portal so that POST requests are allowed. |
-

Sending an Administrator's Alert to Clientless SSL VPN Users

To send an alert message to clientless SSL VPN users (for example, about connection status), perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | In the main ASDM application window, choose Tools > Administrator's Alert Message to Clientless SSL VPN Users .

The Administrator's Alert Message to Clientless SSL VPN Users dialog box appears. |
| Step 2 | Enter the new or edited alert content that you want to send, and then click Post Alert . |
| Step 3 | To remove current alert content and enter new alert content, click Cancel Alert . |
-

