

Cisco ASA Adaptive Security Appliance Single Sign-On: Solution Brief

October 2012

Contents

Introduction	3
Single Sign-On Benefits	3
Supported Applications	3
Supported Software Releases	3
SSO Methods.....	3
Macro Substitution	5
Auto Sign-On Configuration Examples.....	6
Web Application with HTTP Authentication: Microsoft SharePoint.....	6
File Shares: CIFS and FTP	7
Java Plug-ins	8
Form-Based Auto Sign-On: Citrix XenApp and XenDesktop.....	8
Form-Based Auto Sign-On: Outlook Web Access.....	9
Form-Based Auto Sign-On: Predefined Templates.....	10
Form-Based Auto Sign-On: Capture Tool	12
Auto Sign-On for Smart Tunnels	14
Auto Sign-On for External Portal Page	17
Deployment Considerations	18
Auto Sign-On Customization.....	18
Troubleshooting Common Problems.....	19
Conclusion	21

Introduction

Cisco® ASA 5500 Series Adaptive Security Appliances SSL VPN Edition offers flexible client and clientless Secure Sockets Layer (SSL) VPN capabilities, enabling secure connections across public networks to mobile users, contractors, and business partners. One of the key advantages of the clientless SSL VPN is the ability to offer a consolidated web portal that provides convenient remote access to corporate resources such as web servers, file shares, Remote Desktop Protocol (RDP) servers, and office productivity applications such as email and collaboration applications. As the workforce continues to seek higher productivity tools with mobile solutions, it is critical for employers to provide secure and seamless remote access solutions that are flexible and scalable.

This solution brief gives security engineers and administrators an overview, configuration examples, and best practices for using Single Sign-On (SSO) functionality on the ASA. Basic working knowledge of ASA and clientless SSL VPN is assumed. After reading this document, you should have a good understanding of the components involved in the solution and will be well equipped to review other detailed collateral.

Single Sign-On Benefits

Single Sign-On (SSO) technology greatly enhances the user experience by offering a single login clientless portal to IT approved applications and data. More importantly, the end-user can also apply his/her existing secure credentials (i.e.- Microsoft Active Directory) and get authenticated once to gain access to those applications that the IT administrator had approved. In summary, SSO removes the complexity of offering clientless access to disparate applications across the network and replaces this with the single point of access to these business systems. It also helps organizations enforce unified authentication for secure access to multiple applications and services, thus improving overall security.

Supported Applications

The clientless SSL VPN solution provides SSO to many applications, including:

- **Email:** Outlook Web App (OWA) 2003, 2007 and 2010, Domino Web Access 8.5
- **Collaboration:** SharePoint 2003, 2007, and 2010
- **Virtual Resources:** Citrix XenDesktop and XenApp Version 4, 5, and 6
- **Java Plug-ins:** RDP, Virtual Network Computing (VNC), Secure Shell (SSH) Protocol, and Telnet
- **File Shares:** Common Internet File System (CIFS) and FTP
- **Web Applications:** Any web server utilizing either basic HTTP, NT LAN Manager (NTLM), Forms-based POST parameters, or Kerberos tickets for authentication

For more information about clientless applications supported on the Cisco ASA 5500 Series, visit:

<http://www.cisco.com/en/US/partner/docs/security/asa/compatibility/asa-vpn-compatibility.html#wp146723>.

Supported Software Releases

Cisco ASA Software Release 8.4 or later is recommended for the most comprehensive Single Sign-On support. For previous releases, please consult the ASA administration guide for the release.

SSO Methods

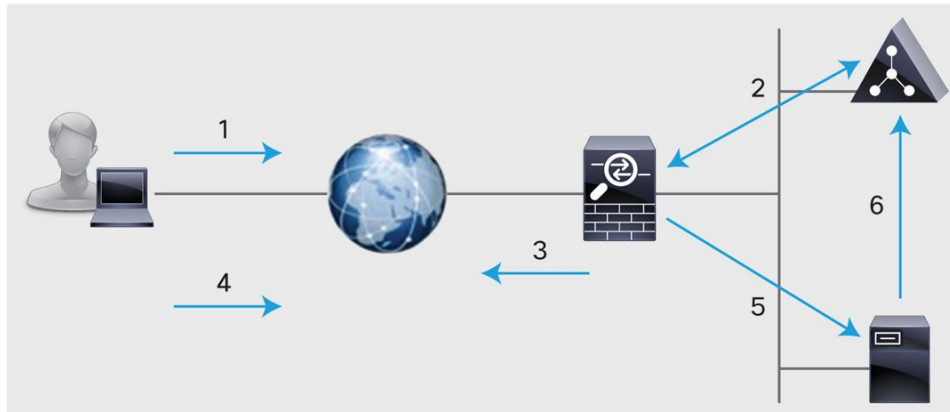
Clientless SSL VPN on the Cisco ASA 5500 Series VPN gateway offers three different methods of Single Sign-On that support various deployments as needed by the security administrators.

Auto Sign-On

Auto Sign-On functionality submits the same clientless SSL VPN login credentials to the back-end applications such as web servers, CIFS/FTP file shares, and web applications that use smart tunnels and Java plug-ins. The servers must accept either basic HTTP, NT LAN Manager Version 1 (NTLMv1), FTP, or CIFS authentication.

Figure 1 shows the Auto Sign-On process flow.

Figure 1. Auto Sign-On Process Flow



1. User logs in to ASA clientless SSL VPN
2. ASA validates user credentials with authentication server
3. ASA publishes the clientless portal with approved bookmarks
4. User launches the bookmark to web application
5. ASA submits user login credentials to the web server
6. Web server validates user credentials with authentication server

Furthermore, SSO to web applications that require login credentials to be specified as part of the Form parameters in an HTTP POST request (for example, Citrix and OWA) is also supported. This method is also called Form-Based Auto Sign-On or Auto Sign-On with HTTP Form Protocol.

Note: Auto Sign-On relies on submitting user name and static passwords to the back-end servers. Hence, Auto Sign-On doesn't provide SSO when clientless VPN users are authenticated with Certificates or dynamic passwords such as one-time password (OTP). Fortunately, the ASA supports double authentication so that static passwords can be combined with Certificates or OTP to provide SSO.

Kerberos Constrained Delegation

Step 1 Kerberos Constrained Delegation (KCD), introduced in Cisco ASA Software Release 8.4, provides SSO to Kerberos-protected web applications. The ASA authenticates the clientless user with either static passwords, one-time passwords (OTP), or certificates. The ASA then requests the key distribution center (KDC) for the service ticket on behalf of the user for a specific web application. Finally, ASA submits the service tickets to the web server for authentication and the user is granted access to the web application. For further configuration details about KCD, please review the latest ASA administrator guide at:

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_clientless_ssl.html#wp1666120.

External SSO Servers

The Cisco ASA VPN gateway also supports external SSO servers that require SAML assertions (that is, Computer Associates eTrust Site Minder). After the user is authenticated with the ASA, the ASA (the asserting party) generates a SAML assertion to the relying party (the SSO server). If the SAML exchange succeeds, the user is allowed access to the protected resource. For further implementation details, please review the latest ASA administrator guide at:

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_clientless_ssl.html#wp2310501.

Macro Substitution

Macro substitution functionality on the Cisco ASA 5500 Series simplifies Auto Sign-On configuration because it allows certain variables to be defined in the authentication request. Each time clientless SSL VPN recognizes one of the variable strings in an end-user request (in a bookmark or a POST Form), it replaces the variable string with the user-session specific value before passing the request to a remote server.

For example, let's say a bookmark is defined as below:

cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@192.168.1.2

When the user johndoe logs into the ASA with the password **j0hnPa\$\$w0rd**, and then clicks the above bookmark, the ASA dynamically navigates the user to:

cifs://johndoe:j0hnPa\$\$w0rd@192.168.1.2

When the user **maryjoe** logs in and clicks on the same bookmark, her request will be:

cifs://maryjoe:m@ryPa\$\$w0rd@192.168.1.2

Thus, a single bookmark can provide SSO experience to multiple users without the need to enter any username or password. The ASA 5500 Series currently supports the variables listed in Table 1 for macro substitution.

Table 1. Variables Available for Macro Substitution

CSCO_WEBVPN_USERNAME	User login ID
CSCO_WEBVPN_PASSWORD	User password
CSCO_WEBVPN_PRIMARY_USERNAME	Primary user login ID. This is applicable when double authentication is configured.
CSCO_WEBVPN_SECONDARY_USERNAME	Secondary user login ID. This is applicable when double authentication is configured.
CSCO_WEBVPN_PRIMARY_PASSWORD	Primary user login password. This is applicable when double authentication is configured.
CSCO_WEBVPN_SECONDARY_PASSWORD	Secondary user login password. This is applicable when double authentication is configured.
CSCO_WEBVPN_INTERNAL_PASSWORD	Internal or domain password. When this value is entered, the security appliance uses it as the password for Auto Sign-On, instead of the password or primary password value.
CSCO_WEBVPN_CONNECTION_PROFILE	User login group drop-down (connection profile alias).
CSCO_WEBVPN_MACRO1	Set with RADIUS Vendor Specific Attribute (VSA) 223. Also, when the LDAP Attribute Map is configured, the value of the Cisco attribute WebVPN-Macro-Substitution-Value1 is copied to this variable.
CSCO_WEBVPN_MACRO2	Set with RADIUS Vendor Specific Attribute (VSA) 224. Also, when the LDAP Attribute Map is configured, the value of the Cisco attribute WebVPN-Macro-Substitution-Value2 is copied to this variable.

Auto Sign-On Configuration Examples

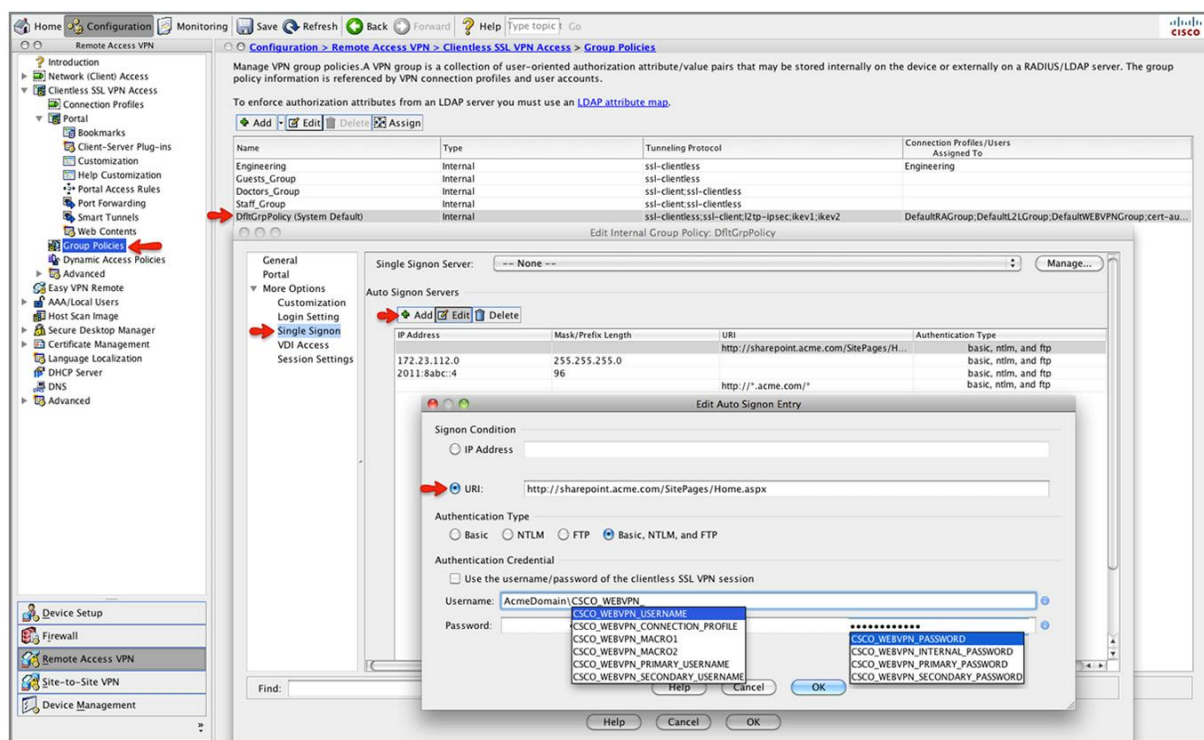
Web Application with HTTP Authentication: Microsoft SharePoint

The Cisco ASA submits login credentials to web applications such as SharePoint that support HTTP authentication (basic HTTP or NTLM). The administrator has to configure Auto Sign-On servers under the VPN Group Policy.

The server list can include the IP address, IP mask, or URI mask of the internal server (Figure 2). The ASA processes the list according to the first matched rule. The administrator has options to select the authentication type and also configure the specific variables that should be used for authentication purposes.

Note: Cisco ASA Software Release 9.0 is required for SharePoint 2010 support.

Figure 2. Single Sign-On to SharePoint



In the example, ASA will submit login credentials to all the web and file servers in the 172.23.112.0/24 subnet or any web server with the URL that includes acme.com.

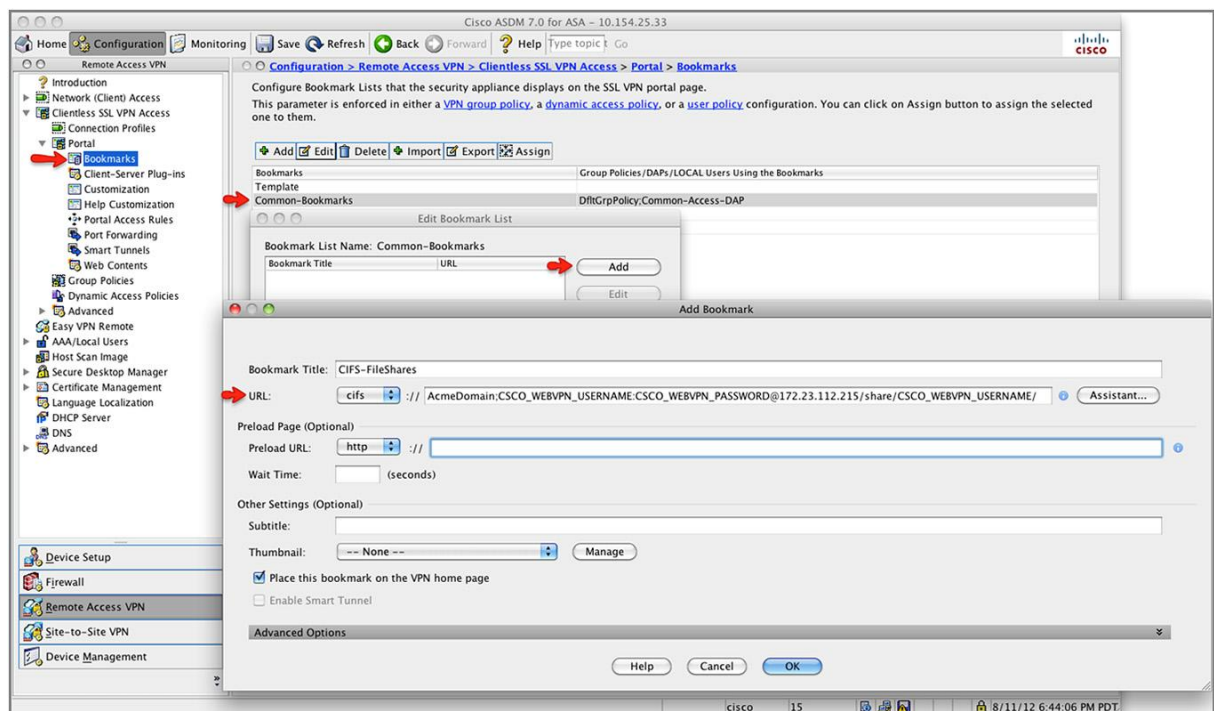
Note: Starting with Cisco ASA Software Release 9.0 and later, you can also enter an IPv6 subnet (example: 2011:8abc::4/96) as the Auto Sign-On server list.

File Shares: CIFS and FTP

There are two methods to achieve SSO for file shares.

- Configure the Auto Sign-On server list under the VPN Group Policy. Make sure the IP subnet includes the specific CIFS server, as shown in the example in Figure 2.
- Configure the bookmark using macro substitution. This method is preferred when the bookmark is associated with a Dynamic Access Policy (DAP) (Figure 3).

Figure 3. CIFS Auto Sign-On Inside Bookmark



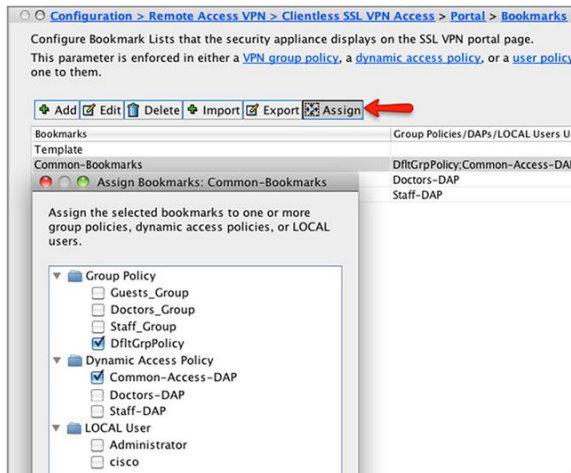
Sample URL:

cifs://AcmeDomain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@172.23.112.215/share/CSCO_WEBVPN_USERNAME.

Note: You will have to customize the path, username, and password variables based on your deployment.

The bookmark is then associated with the Group Policy, User Policy, or Dynamic Access Policy (Figure 4).

Figure 4. Assign Bookmark to Group Policy



Java Plug-ins

To enable SSO for Java plug-ins, the bookmark has to be edited to include the parameter `cscsso=1`.

When the `cscsso` parameter is present in the URL, ASA will submit the VPN username and password for authentication.

Example URLs:

- `rdp://rdp1-server/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768&cscsso=1`
- `ssh://ssh-server/?cscsso=1`
- `telnet://telnet-server/?cscsso=1`
- `vnc://ts-server/?cscsso=1`

Note: If the internal password is entered for the session, it will override any of the password fields (password, primary password, and secondary password).

Note: Java plug-ins do not support macro substitution.

Form-Based Auto Sign-On: Citrix XenApp and XenDesktop

Cisco ASA Software Release 9.0 has introduced preconfigured templates and tools to simplify the SSO process. We will discuss these options in a later section.

For prior releases, to achieve Auto Sign-On to applications that require POST parameters as part of HTTP request, the bookmark has to be edited as shown in Figure 5.

Figure 5. Citrix XenApp SSO Bookmark

Bookmark Title: Citrix XenApp SSO Bookmark

URL: <http://citrix.acme.net/Citrix/XenApp/auth/login.aspx>

Preload Page (Optional)

Preload URL: <http://>

Wait Time: (seconds)

Other Settings (Optional)

Subtitle: Citrix XenApp bookmark

Thumbnail: -- None -- Manage

☒ Place this bookmark on the VPN home page

☐ Enable Smart Tunnel

Advanced Options

URL Method: ☐ Get ☒ Post

Post Parameters

Name	Value
username	CSCO_WEBVPN_USERNAME
password	CSCO_WEBVPN_PASSWORD
domain	AcmeDomain

Help Cancel OK

Note: For XenDesktop, the URL will be: <http://citrix.acme.net/DesktopWeb/auth/login.aspx>.

Form-Based Auto Sign-On: Outlook Web Access

To achieve Auto Sign-On to Outlook Web Access (OWA) 2007, use the bookmark shown in Figure 6.

Figure 6. Auto Sign-On to OWA 2007

Bookmark Title: OWA 2007

URL: <http://owa.acme.net/owa/auth/owaauth.dll>

Preload Page (Optional)

Preload URL: <http://>

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

Thumbnail: -- None -- Manage

☒ Place this bookmark on the VPN home page

☐ Enable Smart Tunnel

Advanced Options

URL Method: ☐ Get ☒ Post

Post Parameters

Name	Value
destination	http://owa.acme.net/owa
username	AcmeDomain\CSCO_WEBVPN_USERNAME
password	CSCO_WEBVPN_PASSWORD
forcedownlevel	0
trusted	0
flags	0

To achieve Auto Sign-On to Outlook Web Access (OWA) 2010, use the bookmark shown in Figure 7.

Figure 7. Auto Sign-On to OWA 2010

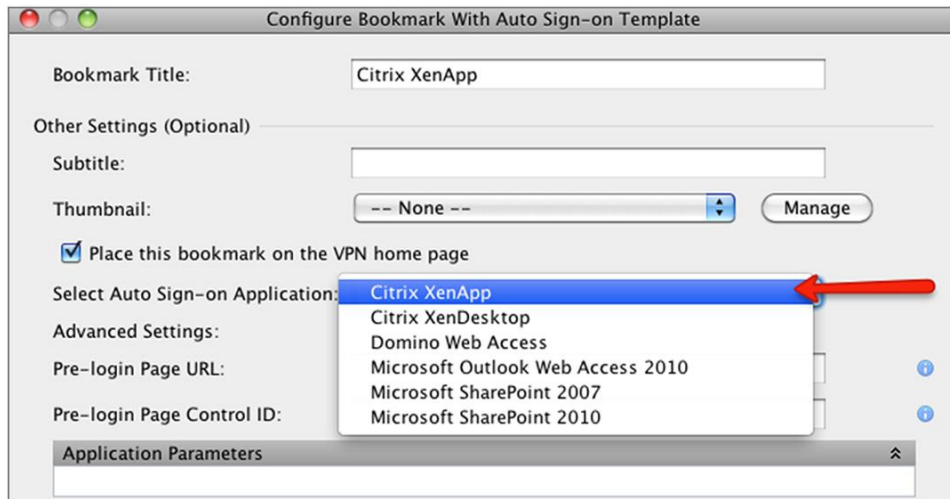
Form-Based Auto Sign-On: Predefined Templates

Cisco ASA Release 9.0 introduced predefined templates that simplify Auto Sign-On configuration. When creating the bookmark, there are three options. Please select **Predefined Application Templates** (Figure 8).

Figure 8. Predefined Templates for Auto Sign-On

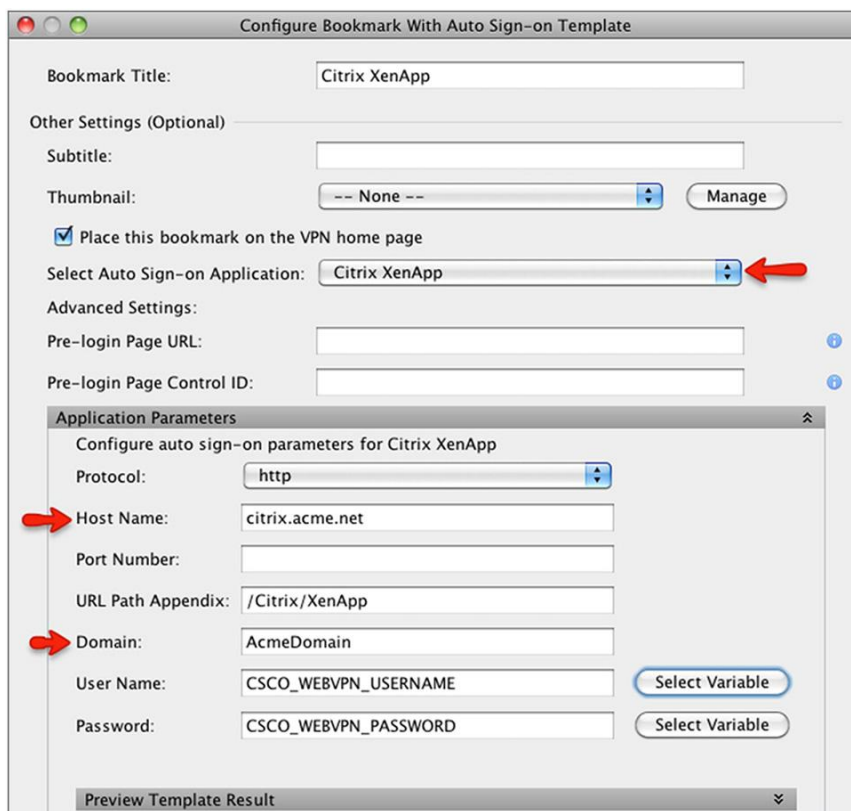
You can then select the specific application for which you want to enable Auto Sign-On. In the example shown in Figure 9, we select Citrix XenApp.

Figure 9. Select Application for Auto Sign-On



After selecting the application, you will have to enter few parameters specific to your deployment, as shown in the example in Figure 10.

Figure 10. Configuration for Citrix XenApp Using Predefined Templates



When you save the bookmark and reopen it, the template will automatically generate the final bookmark, as in Figure 11.

Figure 11. Citrix XenApp Bookmark Auto-Generated by the Template

Name	Value
user	CSCO_WEBVPN_USERNAME
domain	AcmeDomain
password	CSCO_WEBVPN_PASSWORD

Form-Based Auto Sign-On: Capture Tool

For applications that are not supported by the predefined templates, Cisco ASA Release 9.0 also introduced a capture tool that can be used to determine the POST parameters. We will illustrate the capture tool with the OWA 2010 application. First, we'll create a bookmark with basic parameters. The user is then instructed to access the bookmark through the clientless VPN. The capture tool automatically identifies the parameters required to achieve Auto Sign-On.

First, when creating a new bookmark, select the third option shown in Figure 12: HTML form auto-submit.

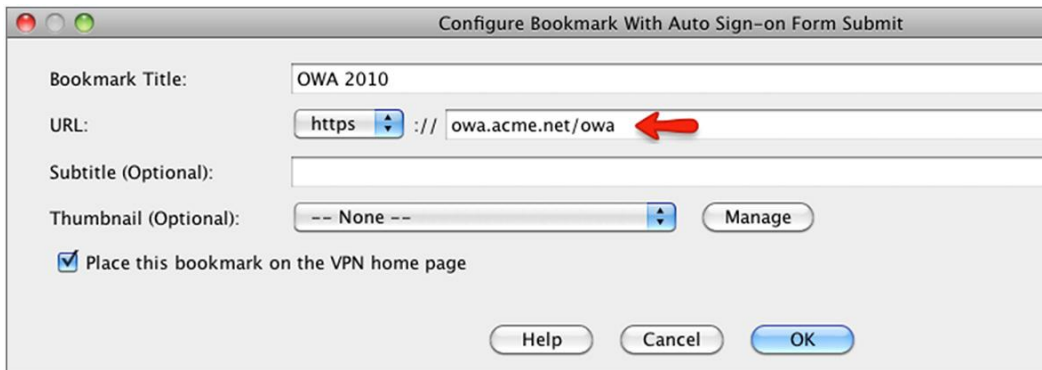
Figure 12. Bookmark with Capture Tool

Select an option to use for bookmark creation:

- ☐ URL with GET or POST method
This is the traditional bookmark using the GET method, or the POST method with parameters.
- ☐ Predefined application templates (Microsoft OWA, SharePoint, Citrix XenApp/XenDesktop, Lotus Domino)
This option simplifies bookmark creation with users selecting a predefined ASDM template that contains the pre-filled necessary values for certain well-known Microsoft OWA 2010 and Citrix XenApp.
- ☒ HTML form auto-submit
This option lets you create bookmark for any complex auto sign-on application. It will require 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 policy or user.
2- Edit the bookmark in ASDM again. Use the capture function to capture the SSL VPN parameters and edit them in the bookmark.

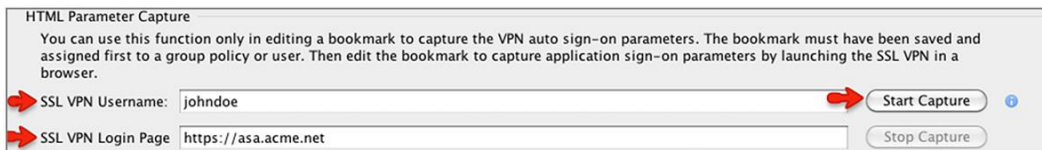
Enter the basic parameters such as the server URL (Figure 13).

Figure 13. OWA Server URL



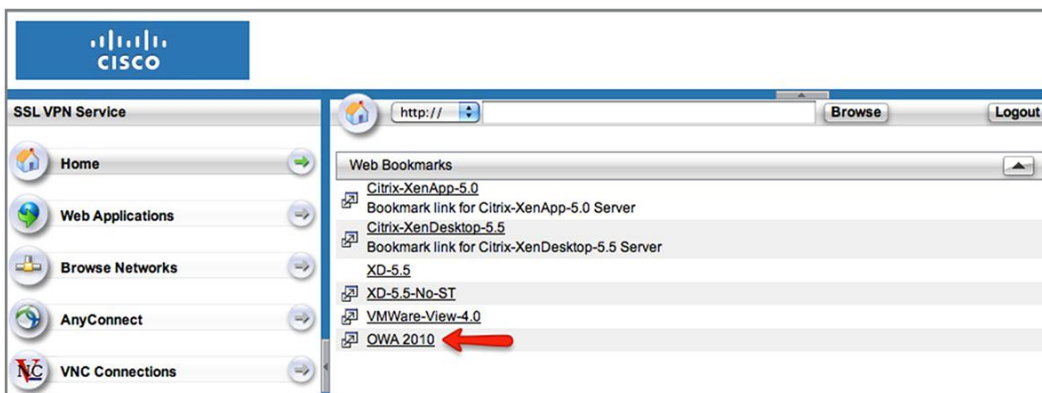
Save the bookmark, then assign it to the appropriate Group Policy, DAP Record, or User Policy (as shown earlier in Figure 4) and finally reopen the bookmark. Enter the SSL VPN username and the login page URL. Then click “Start Capture”.

Figure 14. Start Capture



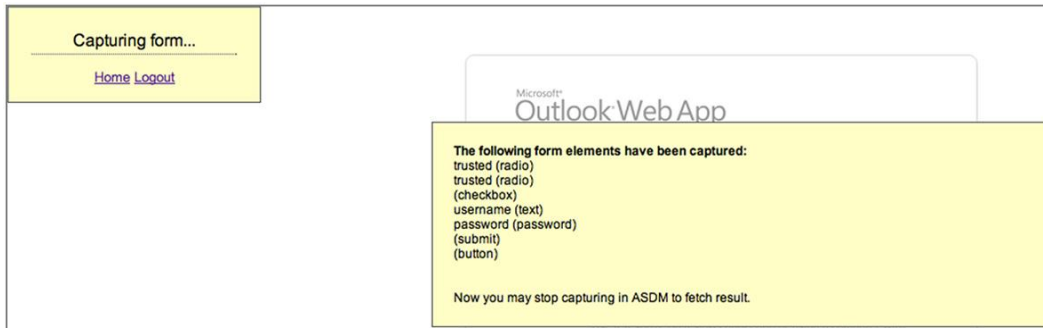
The user is then instructed to log in to the clientless SSL VPN portal and navigate to the bookmark (Figure 15).

Figure 15. User Access to Clientless Bookmark



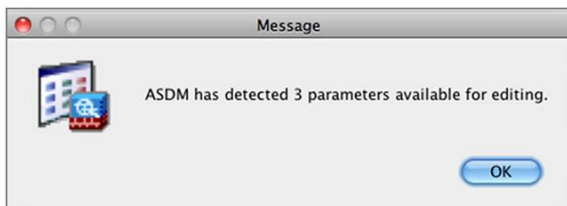
The portal will display the message shown in Figure 16.

Figure 16. Capture Notification



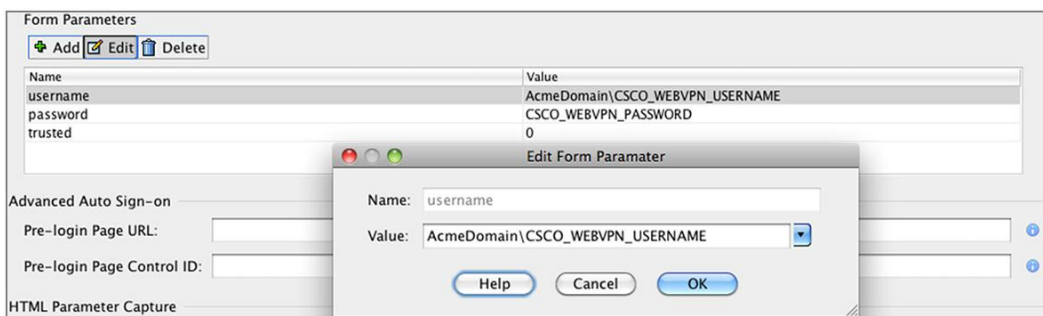
You should now edit the bookmark in Cisco Adaptive Security Device Manager (ASDM) and click “Stop Capture”. You will see the notification shown in Figure 17.

Figure 17. ASDM Notification



You will then have to edit the values for the form parameters detected by the ASDM (Figure 18). You have the option to enter any of the macro variables that we discussed earlier.

Figure 18. Edit the Bookmark Parameters



After this step, whenever the user clicks the same bookmark in the clientless portal, they will be automatically signed on to the OWA.

Auto Sign-On for Smart Tunnels

Auto Sign-On is supported when the Smart Tunnel option is enabled for web bookmarks. Auto Sign-On is not supported when using the native client-server applications.

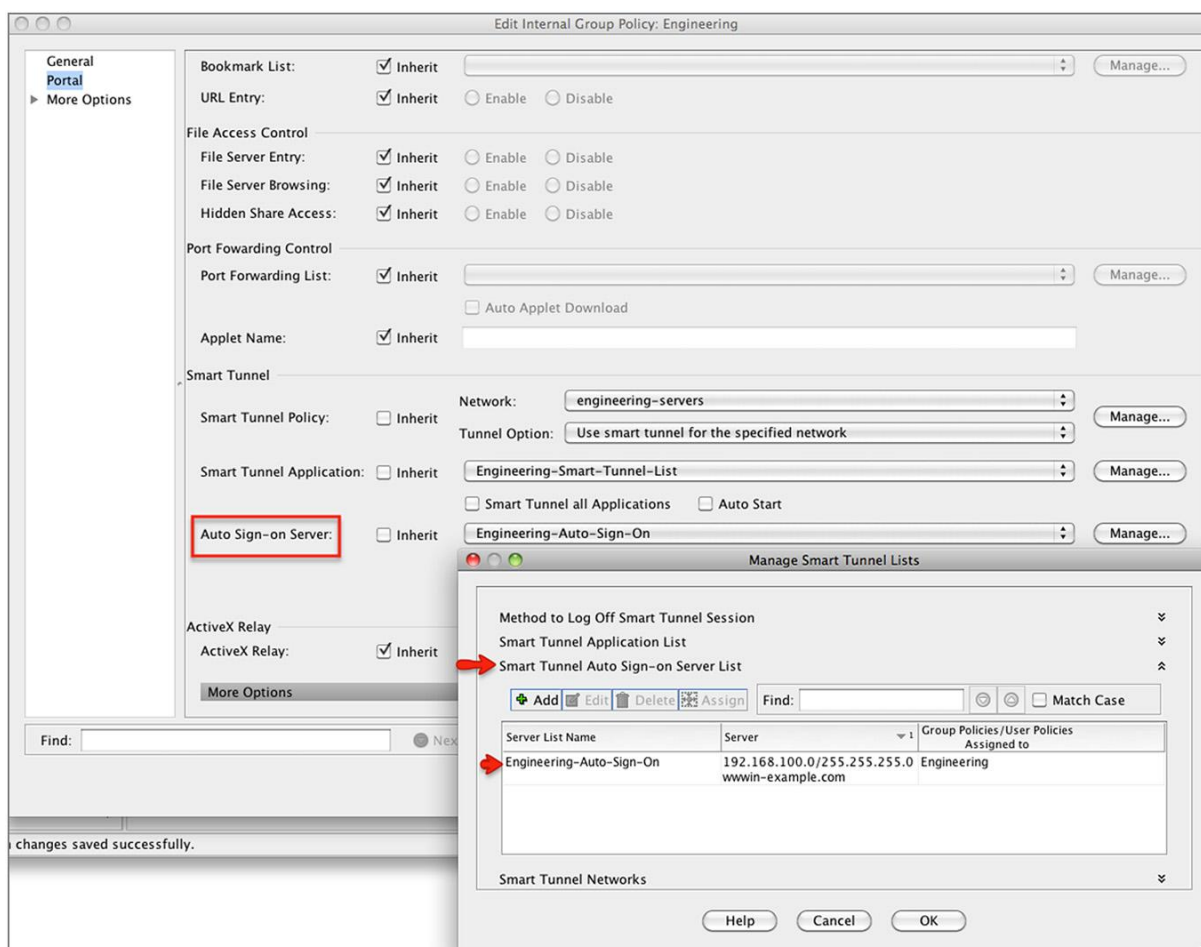
Auto Sign-On Servers for Basic/NTLM/FTP Authentication

Administrators can specify the server lists to which the smart tunnel will perform Auto Sign-On (Figure 19). ASA submits the clientless SSL VPN username and passwords to the internal servers.

Note: Auto Sign-On configured for smart tunnel doesn't support macro substitution.

Note: When configuring the network for the Auto Sign-On server list for smart tunnels, you must enter both the IP address and hostname of the network.

Figure 19. Auto Sign-On Server List for Smart Tunnel



Note: Starting with Cisco ASA Release 9.0, you can also enter an IPv6 subnet (example: 2011:8abc::4/96) as the Auto Sign-On server list.

Form-Based Auto Sign-On and Macro Substitution

Web bookmarks that require Forms-based POST parameters can be configured to use smart tunnels. In addition, Cisco ASA Release 8.3 introduced the support of macro substitution as part of the POST parameters (Figure 20).

Figure 20. Form-Based Single-Sign-On with Smart Tunnel and Macro Substitution

Add Bookmark

Bookmark Title: Exchange 2003 with Smart Tunnel

URL: **https**:// mail.example.com/exchweb/bin/auth/owaauth.dll

Preload Page (Optional)

Preload URL: **http**://

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

Thumbnail: -- None -- **Manage**

☒ Place this bookmark on the VPN home page

Enable Smart Tunnel ⓘ

Advanced Options

URL Method: ☐ Get ☒ **Post**

Post Parameters

Add **Edit** **Delete**

Name	Value
destination	https://mail.example.com/exchange
username	EXAMPLE\CSCO_WEBVPN_USERNAME
password	CSCO_WEBVPN_PASSWORD
SubmitCode	Log On

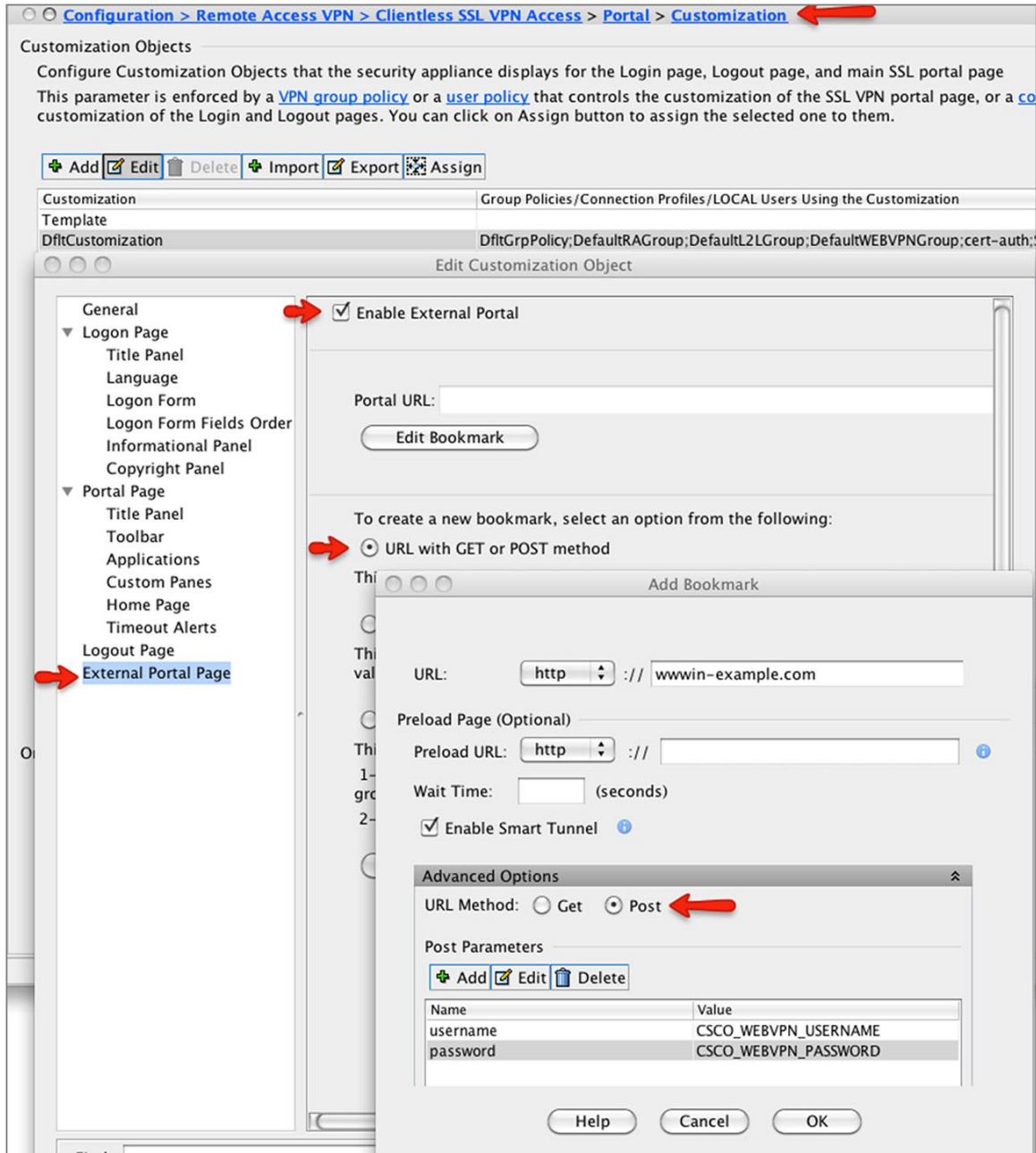
Post Script ⓘ

Help **Cancel** **OK**

Auto Sign-On for External Portal Page

The External Portal Page feature in the Cisco ASA 5500 Series allows the administrator to bypass the main clientless portal and redirect the user to a custom URL. ASA Release 8.3 introduced the feature to enable Form-based Auto Sign-On along with Smart Tunnel option for the external portal page (Figure 21).

Figure 21. Auto Sign-On for External Portal Page



Note: The VPN Group Policy also has an attribute **Home-page URL** under the Customization panel. This option should be used only when you need a unified homepage for both the Cisco AnyConnect® Client and clientless SSL VPN. If the homepage is used exclusively for clientless SSL VPN, the External Portal Page (as shown in Figure 21) is preferred. The External Portal Page also supports Form-based Single Sign-On.

To achieve Auto Sign-On for this homepage URL (Figure 22), you have to ensure that the specific URL is included in the Auto Sign-On server list (Figure 23).

Figure 22. Enable Homepage URL in the Group Policy

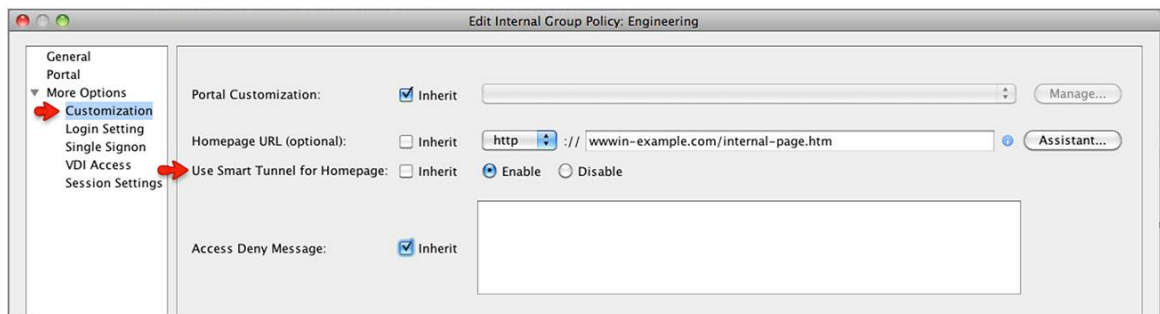
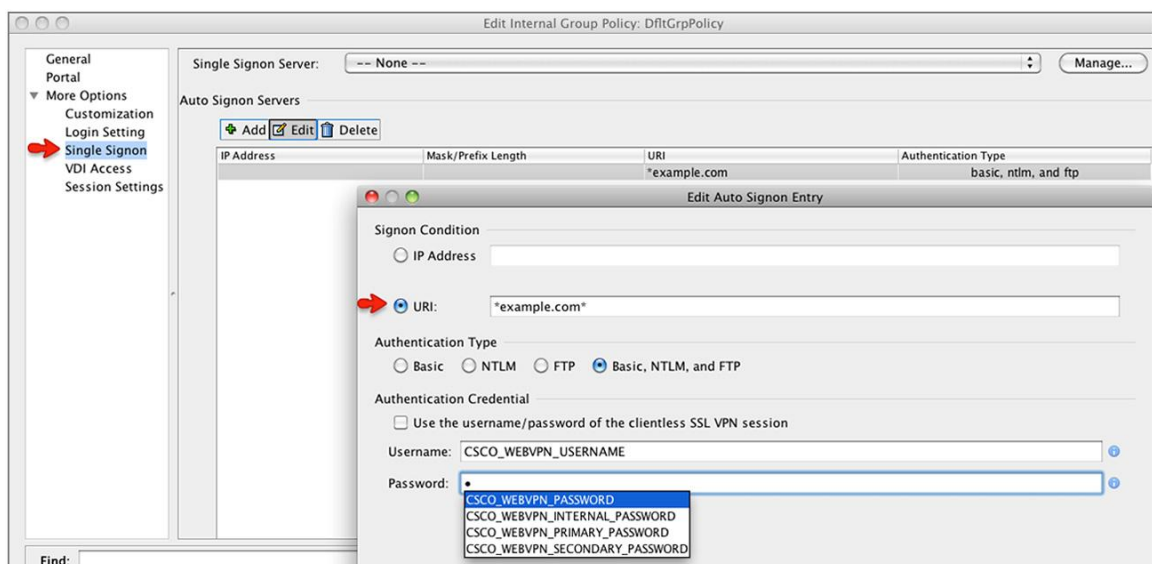


Figure 23. Auto Sign-On Server List under the Group Policy



Deployment Considerations

Auto Sign-On Customization

Group Policy and User Policy

The Auto Sign-On server list and web bookmarks can be applied per Group Policy or User Policy. For example, it is possible to have one set of Auto Sign-On server list and bookmarks for Engineering and have entirely different set for Marketing.

Dynamic Access Policy (DAP)

Dynamic Access Policy on the Cisco ASA 5500 Series applies customized security policy based on user identity and device posture status. However, the DAP includes only web bookmarks that have Form-based Auto Sign-On enabled. It is currently not possible to apply a different Auto Sign-On server list based on the DAP record.

Troubleshooting Common Problems

Auto Sign-On Doesn't Work

1. Ensure that the specific back-end server is included in the Auto Sign-On server list associated with the Group Policy or User Policy.
2. Ensure that the correct macro variable is used for the username and password parameters.
 - a. Double Authentication: When double authentication is configured
 - i. The credentials for the first authentication server are saved in the variables CSCO_WEBVPN_PRIMARY_USERNAME and CSCO_WEBVPN_PRIMARY_PASSWORD.
 - ii. The credentials for the second authentication server are saved in the variables CSCO_WEBVPN_SECONDARY_USERNAME and CSCO_WEBVPN_SECONDARY_PASSWORD.

In a typical deployment, the primary authentication server uses RADIUS-based token passwords and the secondary authentication server uses the LDAP-based static password. In this case, you have to use the variables CSCO_WEBVPN_SECONDARY_USERNAME and CSCO_WEBVPN_SECONDARY_PASSWORD to achieve SSO to back-end applications that accept LDAP credentials.

- b. Internal Password: When internal password is configured, the value entered by the user is saved in the CSCO_WEBVPN_INTERNAL_PASSWORD variable.

Form-Based Auto Sign-On Doesn't Work

1. If you are using ASA Release 9.0 or later, use the capture tool in ASDM to determine the required POST parameters (see Figures 24 and 25).
2. For releases prior to ASA 9.0, you will have to use third-party capture tools such as HTTPFox (<https://addons.mozilla.org/en-us/firefox/addon/httpfox/>) HTTPWatch (<http://www.httpwatch.com/download/>), and IE Inspector (<http://www.ieinspector.com/httpanalyzer/download.html>).

Important Note: When using these tools, make sure to capture the traces when connected to the resource directly in clear (that is, without going through the clientless portal).

Figure 24. Sample HTTP Watch Output for OWA

Started	Time Chart	Time	Sent	Received	Method	Result	Type
00:00:00.000		0.565	882	366	POST	302	Redirect to http://10.86.195.133/owa

Headers Sent		Headers Received	
Header	Value	Header	Value
(Request-Line)	POST /owa/auth/owaauth.dll HTTP/1.1	(Status-Line)	HTTP/1.1 302 Moved Temporarily
Accept	image/gif, image/jpeg, image/pjpeg, image/png, application/x-shockwave-flash	Content-Length	0
Accept-Encoding	gzip, deflate	Date	Thu, 30 Apr 2009 14:53:15 GMT
Accept-Language	en-us;pt;q=0.5	Location	http://10.86.195.133/owa
Cache-Control	no-cache	Server	Microsoft-IIS/6.0
Connection	Keep-Alive	Set-Cookie	sessionid=e5760fac-7ac6-4cfa-8841-381d75bf28
Content-Length	125	Set-Cookie	cadata="0uSLP0FJTaa20cz9AD9F6EAQC1IW5Zv
Content-Type	application/x-www-form-urlencoded	X-Powered-By	ASP.NET
Host	10.86.195.133		
Referer	http://10.86.195.133/owa/auth/login.aspx?replaceCurrent=1&url=http%3a%2f%2f10.86.195.133%2fowa		
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB6; Embed		

Figure 25. POST Data and Parameters

Parameter	Value
destination	http://10.86.195.133/owa
flags	0
forcedownlevel	0
password	Foofoo676
trusted	0
username	user1@olympia.com

Additional Help

You can contact Cisco Technical Assistance Center (TAC) for additional help.

- Please provide ASA configuration and full screenshots of the bookmarks.
- For ASA Release 9.0 and later, please provide output of the capture tool as shown in Figure 16.
- Please provide any capture files from the tools such as HTTP Watch and HTTP Fox. Make sure to capture the HTTP requests when connected to the resources directly (that is, without going through the ASA clientless portal).
- Please provide detailed steps to reproduce the problem, including what has been configured.
- Please provide any error messages you've received.
- Please examine logs, which can be found at the local machine's eventviewer (Windows) or /tmp (other platforms)

Conclusion

Clientless SSL VPN on the Cisco ASA 55000 Series offers a convenient portal with all the relevant corporate resources for remote users. The Single Sign-On solution supports various deployments and enables seamless access to corporate resources such as web applications, email, virtual resources, and collaboration applications.

The Single Sign-On solution improves employee productivity and adoption of the remote access solution.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)