



Configuring Single Sign-on for WebVPN

This chapter presents example procedures for configuring SSO for WebVPN users. It includes the following sections:

- [Using Single Sign-on with WebVPN, page 7-1](#)
- [Configuring SSO Authentication Using SiteMinder, page 7-2](#)
- [Configuring SSO with the HTTP Form Protocol, page 7-9](#)

Using Single Sign-on with WebVPN

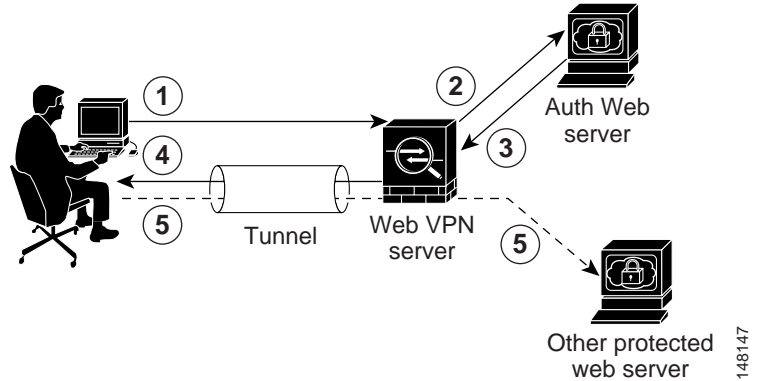
Single sign-on lets WebVPN users enter a username and password only once to access multiple protected services and web servers. In general, the SSO mechanism either starts as part of the AAA process or just after successful user authentication to a AAA server. The WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server.

While WebVPN supports three SSO authentication methods, two can be configured with ASDM: SSO with the Computer Associates eTrust SiteMinder server (formerly Netegrity SiteMinder), and SSO using the HTTP Form protocol. The third method, SSO with HTTP Basic and NTLMv1 (NT LAN Manager) authentication, is currently only configurable using the security appliance command line interface.

Figure 7-1 illustrates the following major SSO authentication steps that are used by all three methods:

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

Figure 7-1 SSO Authentication Using HTTP Forms



Configuring SSO Authentication Using SiteMinder

This section describes configuring the security appliance to support SSO with SiteMinder. You would typically choose to implement SSO with SiteMinder if your website security infrastructure already incorporates SiteMinder. With this method, SSO authentication is separate from AAA and happens once the AAA process completes. If you want to configure SSO for a WebVPN user or group, you must first configure a AAA server, such as a RADIUS or LDAP server. You can then setup SSO support for WebVPN.

This section includes the following topics:

- [Configuring the Security Appliance for SiteMinder, page 7-2](#)
- [Assigning the SSO Server to Group Policies and Users, page 7-4](#)
- [Adding the Cisco Authentication Scheme to SiteMinder, page 7-8](#)

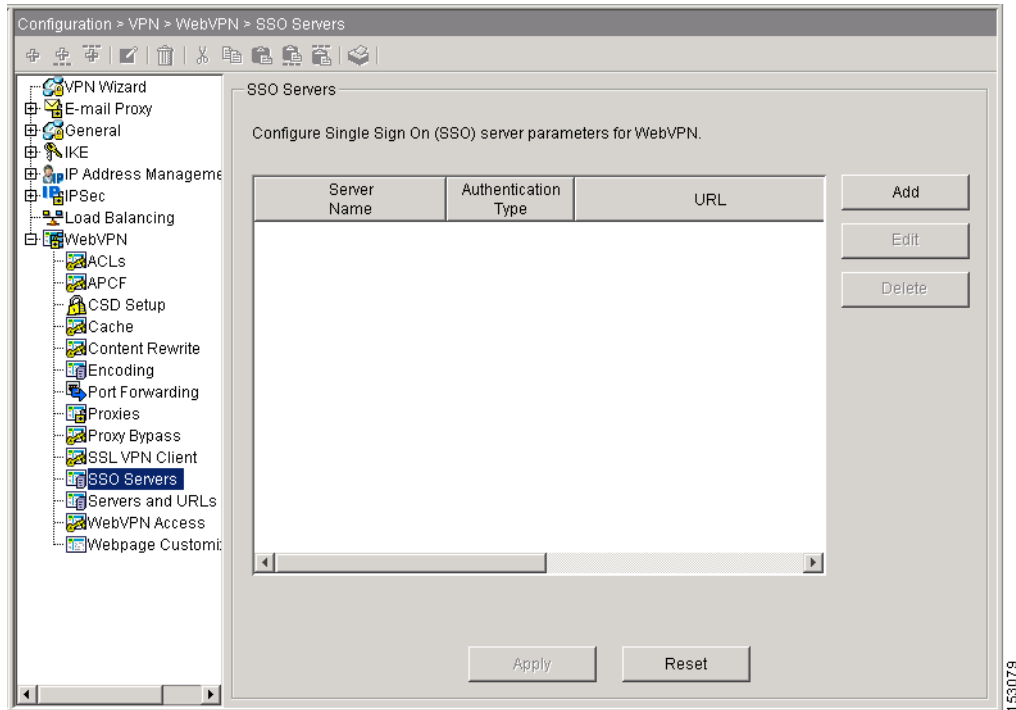
Configuring the Security Appliance for SiteMinder

To configure SSO with a new SiteMinder server, perform the following steps:

-
- Step 1** In the main Cisco ASDM window, choose **Configuration > VPN > WebVPN > SSO Servers**.

The SSO Servers area appears in the window on the right as shown in [Figure 7-2](#).

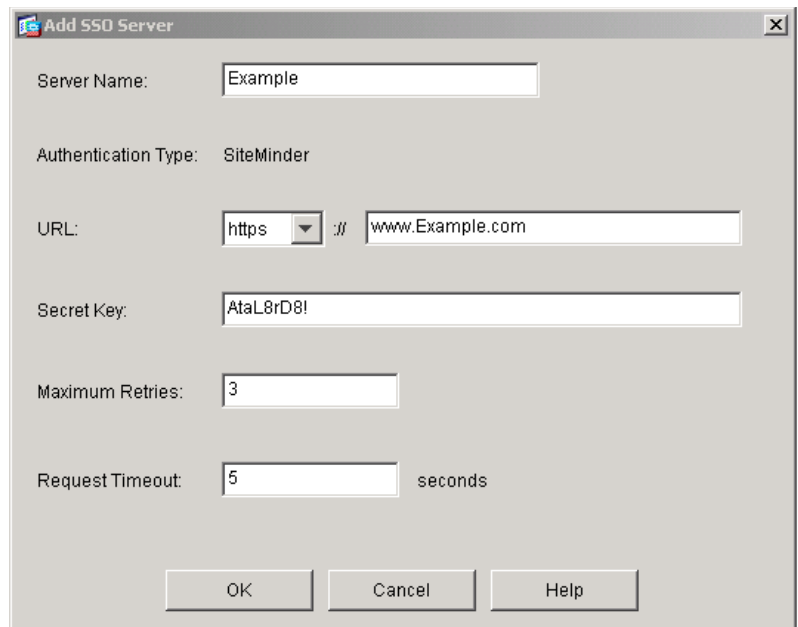
Figure 7-2 ASDM Window with SSO Servers Area Displayed



Step 2 Click **Add** in the SSO Servers area.

The Add SSO Server dialog box appears as shown in Figure 7-3.

Figure 7-3 Add SSO Server Dialog Box



Step 3 In the Server Name field, enter the name of the SiteMinder SSO server.

The minimum number of characters is 4, and the maximum is 31.

In this example, the server name is *Example*.

Step 4 Enter the SSO server URL by performing the following steps:

- a. Choose either **HTTP** or **HTTPS** from the menu.

In this example, we choose HTTPS to secure the authentication messages between the security appliance and the SiteMinder server.

- b. Enter the rest of the complete server URL.

In this example, the rest of the URL is *www.Example.com*.

This is the SSO server URL to which the security appliance makes SSO authentication requests.

Step 5 Enter the secret key in the Secret Key field.

This is the 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.

The secret key is similar to a password: you create it, save it, and enter it on both the security appliance and the SiteMinder Policy Server. See [Adding the Cisco Authentication Scheme to SiteMinder, page 7-8](#).

In this example, the secret key is *AtaL8rD8!*.

Step 6 In the Maximum Retries field, enter the number of times the security appliance retries a failed SSO authentication attempt. This step is optional.

The range is 1 to 5 retries, and the default number of retries is 3.

In this example, the maximum retries is 3.

Step 7 In the Request Timeout field, enter the number of seconds before a failed SSO authentication attempt times out. This step is optional.

The range is from 1 to 30 seconds inclusive, and the default is 5 seconds.

In this example, timeout occurs after 5 seconds.

Step 8 Click **OK** to enter this new SSO server in the SSO Server table in the ASDM window.

Step 9 Click **Apply** to add the new SSO server to the running security appliance configuration.

Assigning the SSO Server to Group Policies and Users

After you configure the SSO server, you must specify SSO authentication for either a group policy or a user. This section includes:

- [Assigning the SSO Server to a Group Policy, page 7-4](#)
- [Assigning the SSO Server to a User, page 7-6](#)

Assigning the SSO Server to a Group Policy



Note

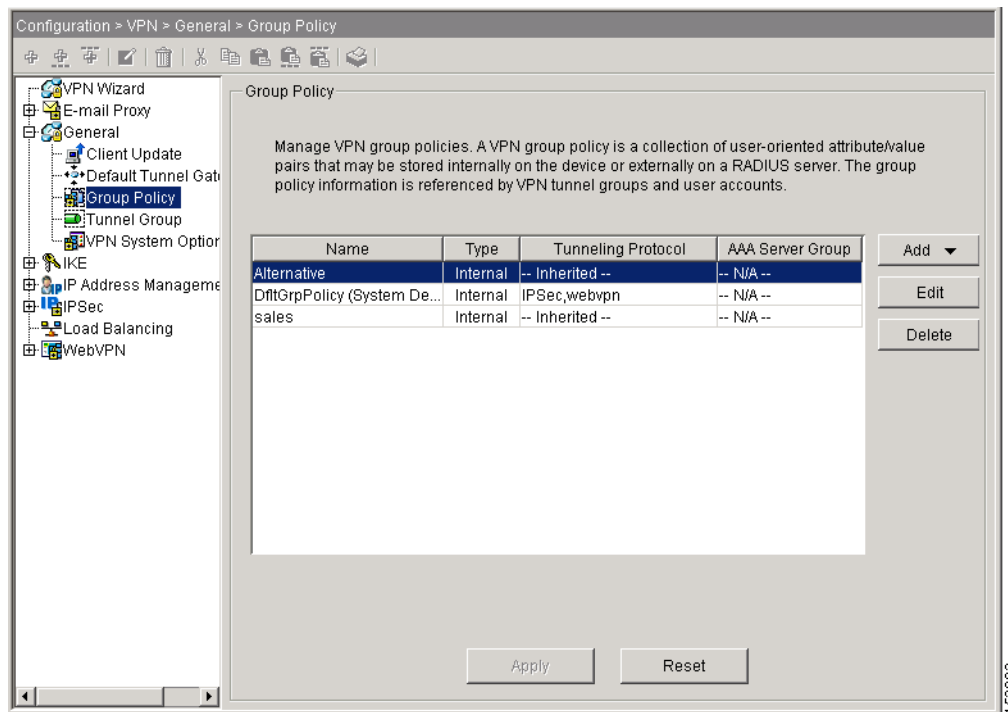
Comprehensive procedures for configuring group policies are provided elsewhere in this guide. The following steps are only those that apply to configuring a SiteMinder SSO server.

To assign the SSO server to a group policy, perform the following steps:

Step 1 In the main Cisco ASDM window, choose **Configuration > VPN > General > Group Policy**.

The Group Policy area appears in the window as shown in [Figure 7-4](#).

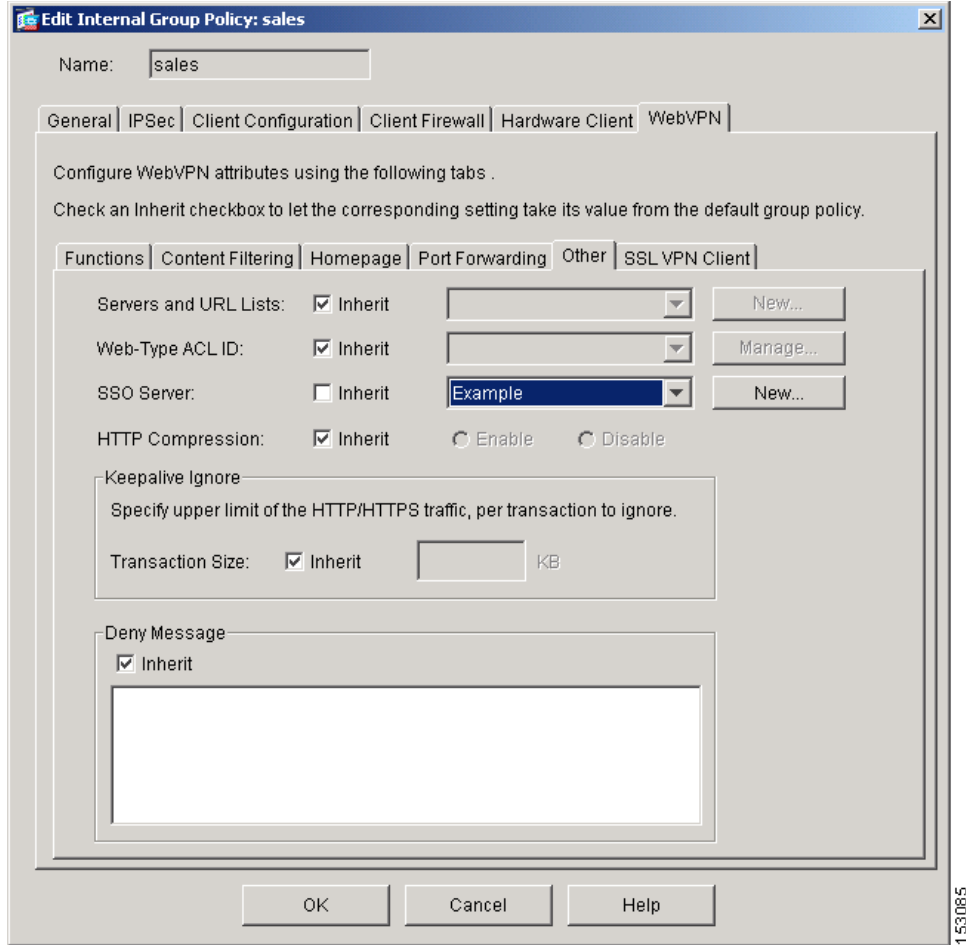
Figure 7-4 ASDM Window with Group Policy Area Displayed



- Step 2** In the Group Policy table, click the group policy to which you want to assign the SiteMinder SSO server.
- Step 3** Click **Edit**.

The Edit Internal Group Policy dialog box appears as shown in [Figure 7-5](#).

Figure 7-5 The Edit Internal Group Policy Dialog Box



- Step 4** Click the **General** tab and then click the **Other** tab on the General tab.
- Step 5** Next to SSO Server, do the following:
- Clear the SSO Server **Inherit** check box.
 - Choose the new SSO server from the menu.
- In this example, the SSO server is named Example.
- Step 6** Click **OK** to return to the ASDM window.
- Step 7** Click **Apply** to enter the assignment into the running security appliance configuration.

Assigning the SSO Server to a User



Note

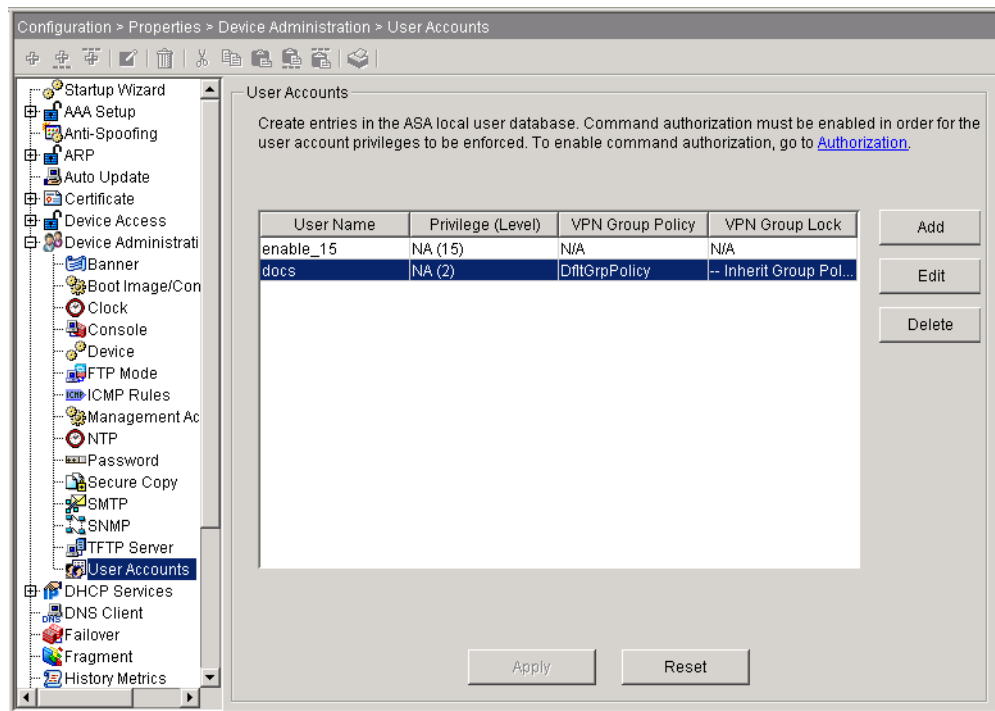
Comprehensive procedures for configuring users are provided elsewhere in this guide. The following steps are only those that apply to configuring a SiteMinder SSO server.

You can also assign the SSO server to a user by performing the following steps:

Step 1 In the main Cisco ASDM window, choose **Configuration > Properties > Device Administration > Users**.

The User Accounts area appears in the window as shown in [Figure 7-6](#).

Figure 7-6 ASDM Window with User Accounts Area Displayed

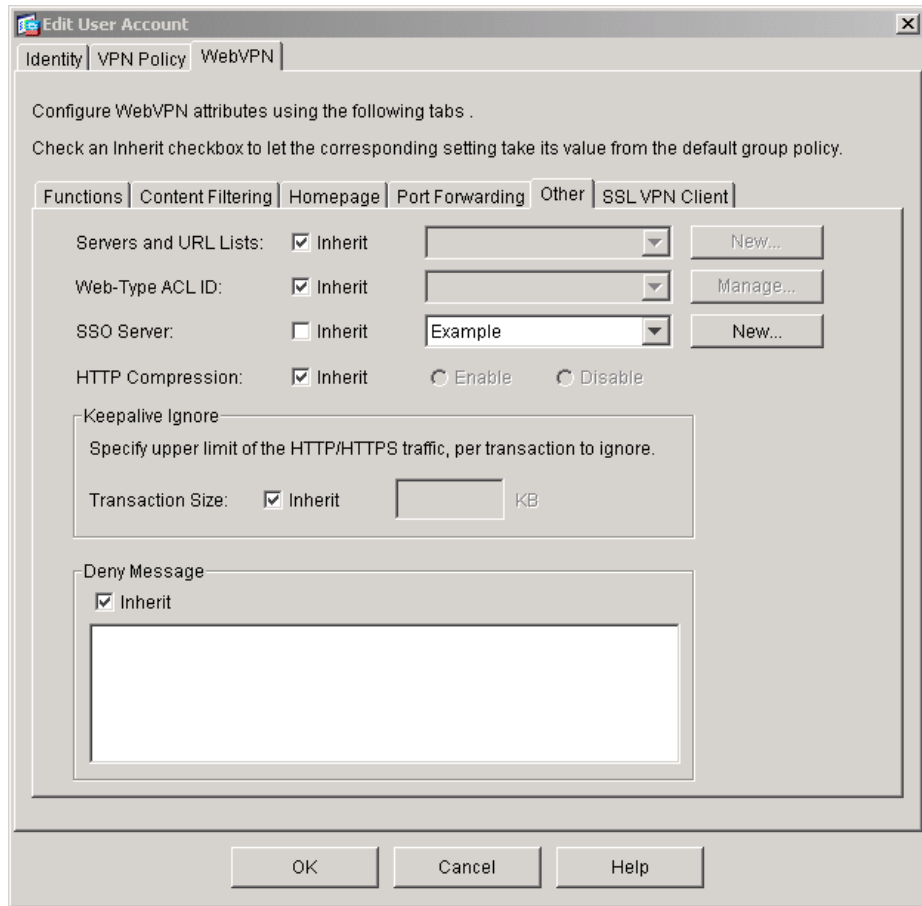


Step 2 From the User Accounts table, click the User Name you want to assign the SiteMinder SSO server to.

Step 3 Click **Add**.

The Edit User Account dialog box appears as shown in [Figure 7-7](#).

Figure 7-7 The Edit User Account Dialog Box



- Step 4** Click the **WebVPN** tab and then click the **Other** tab on the WebVPN tab.
- Step 5** Next to SSO Server, do the following:
 - Clear the SSO Server **Inherit** check box.
 - Choose the new SSO server from the menu.

In this example, the SSO server is named Example, as shown in [Figure 7-7](#).
- Step 6** Click **OK** to return to the ASDM window.
- Step 7** Click **Apply** to enter the assignment into the running security appliance configuration.

Adding the Cisco Authentication Scheme to SiteMinder

Besides configuring the security appliance for SSO with SiteMinder, you must also configure your Computer Associates SiteMinder Policy Server with the Cisco authentication scheme, provided as a Java plug-in.



Note

- Configuring the SiteMinder Policy Server requires experience with SiteMinder.
- 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 these following tasks:

-
- 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 security appliance.
- You configure this on the security appliance with either the **policy-server-secret** command at the command line interface or in the Secret Key field of the Add SSO Server dialog box in ASDM.
- In the Parameter field, enter **CiscoAuthAPI**.
- Step 2** Copy the file **cisco_vpn_auth.jar** from the CD to the default library directory for the SiteMinder server.

Configuring SSO with the HTTP Form Protocol

This section describes using the HTTP Form protocol for SSO. The HTTP Form protocol is a common approach to SSO authentication that can also qualify as a AAA method. It provides a secure method for exchanging authentication information between WebVPN users and authenticating web servers. As a common protocol, it is highly compatible with web servers and web-based SSO products, and you can use it in conjunction with other AAA servers such as RADIUS or LDAP servers.

As with SiteMinder, the security appliance serves as a proxy for WebVPN users to an authenticating web server but, in this case, it uses HTTP Form protocol and the POST method for requests. You must configure the security appliance to send and receive form data.



Note

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

While you would expect to configure form parameters that let the security appliance 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 that the authenticating web server expects by making a direct authentication request to the web server from your browser without the security appliance in the middle acting as a proxy. Analyzing the web server response using a 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.

This section describes:

- [Gathering HTTP Form Data, page 7-10](#)
- [Configuring SSO with HTTP Form Protocol, page 7-12](#)

- [Assigning the SSO Server to a Tunnel Group, page 7-15](#)

Gathering HTTP Form Data

This section presents the steps for discovering and gathering the HTTP Form data required to configure SSO if you do not already know what the data is. To gather the data, you must analyze responses from the authenticating web server using an HTTP header analyzer.

To gather parameter data, perform the following steps:

-
- Step 1** Start your browser and HTTP header analyzer, and connect directly to the web server login page without going through the security appliance.
- The web server login page loads into your browser.
- Step 2** Examine the login exchange with your HTTP header analyzer. If the web server has loaded a cookie with the login page, copy this login page URL. It is 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-ac05-83
846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2b
J0H0KPshFtg6rB1UV2PpkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F
HTTP/1.1
Host: www.example.com
(BODY)
SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%2Fw
ww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

- Step 4** Examine the POST request and copy the protocol, host, and the complete URL. This is needed to configure the action-uri parameter later.
- Step 5** Examine the POST request body and copy the following:

- Username parameter

In this example, the parameter is userid (not the value anyuser).

- Password parameter

In this example, the parameter is user_password.

- Hidden parameter

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

```
SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Fe
mco%2Fmyemco%2F&smauthreason=0
```

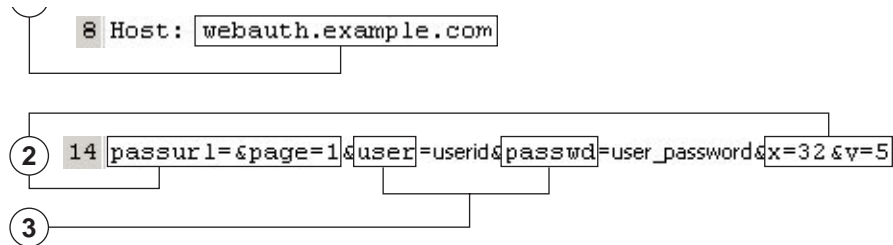
Hidden parameters are typically presented in the following format:

```
<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.

Figure 7-8 highlights the action URI, hidden, username and password parameters found using an HTTP header analyzer. This is only an example; output varies widely across different websites.

Figure 7-8 Action-uri, hidden, username and password parameters



1	Action URI parameter
2	Hidden parameters
3	Username and password parameters

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 Authentication Cookie Name value.

In the following server response header, the name of the session cookie is SMSESSION. You just need the name, not the value.

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev4lhsE49XlKc+1twie0ggnjbhktkUnr8XWP3hvdH6PZPbHIHtWLDKtA8
ngDB/lbYTjIxrbdx8WPWwG3CxVa3adOxHFR8yjd55GevK3ZF4ujgU1lh06fta0dSSOSepWvnsCb7IFxCw+MGiw0o8
8uHa2t4l+SillqfJvcpxfiIAO06D/gtDF400w5YKHEl2KhDEvv+yQzxfEz2c17Ef5iMr8LgGcDK7qvMcvrgUqx68
JQOK2+RSwHQ15bcZmsDU5vQVCvSQWC8OMHNGwps253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V7f1Bqech7+kVrU01
F6oFzr0zM1kMyLr5Hh1VDh7B0k9wp0dUFZiAzaF43jupD5f6CEkuLeudYW1xgNzsr8eqtPK6t1gFJyOn0s7QdnQ7q9
knsPJsekRAH9hrLBhWBLTU/3B1QS94wEGD2YTuiW36TiP14hYwO1CAYRj2/bY3+1YzVu7EmzMQ+UefYxh4cF2gYD8R
ZL2RwmP9JV5l48I3XBFPNUw/3V5jff7nRuLr/CdfK3O08+Pa3V6/nNhokErSgyxjzMd88DVzM41LxxaUDhbcmkohT9I
mzBvKzJX0J+o7FoUDF0xEdIqlAN4GNqk49cpi2sXDbIarALp6B13+tbB4M1HGH+0CPscZXqoi/kon9YmGauHyRs+0m
6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdahug5SxbUzjY2JxQnrUtWb977NCzYu2sOtN+dsEReW
J6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdRka5p3N0Nfq6RM6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8Vb
Ar15ivkE8dSCzuf/AINHtCzuQ6wApzEp9CUoG8/dapWriHjNoi41lJOGcst33wEhxFxcWy2UWxs4EZSjsI5GyBnefS
QTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTnqunkDEdMIHfbcP3F90cZejVzihM6igiS6P/CEJAjE; Domain=.exam
ple.com; Path=/
```

Figure 7-9 shows an example of authorization cookies in HTTP analyzer output. This is only an example; output varies widely across different websites.

Figure 7-9 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

```

1	Authorization cookies
---	-----------------------

In some cases, the server may set the same cookie regardless of whether the authentication was successful or not. Such a cookie is unacceptable for SSO purposes.

- Step 7** 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 security appliance for SSO with HTTP Form protocol.

Configuring SSO with HTTP Form Protocol

This section presents an example procedure for configuring SSO with the HTTP Form protocol using the parameters gathered in the previous section. In this procedure, there are steps that are always required and steps that are sometimes required. The steps that are always required are the configuration of the:

- Action URI
- Username parameter
- Password parameter

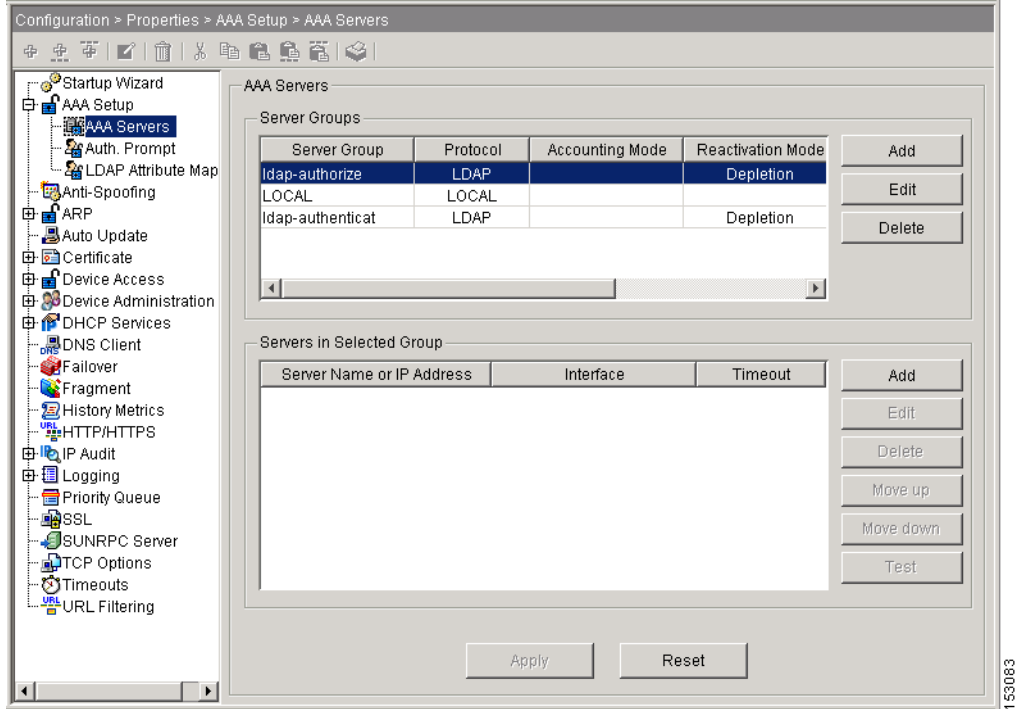
The other steps are only required if the authenticating web server requires them. They are the configuration of:

- A start URL
- Hidden parameters
- An authentication cookie name

Perform the following steps to configure the security appliance to use HTTP Form protocol for SSO:

- Step 1** In the main Cisco ASDM window, choose **Configuration > Properties > AAA Setup > AAA Servers**. The AAA Servers area appears in the window as shown in [Figure 7-10](#).

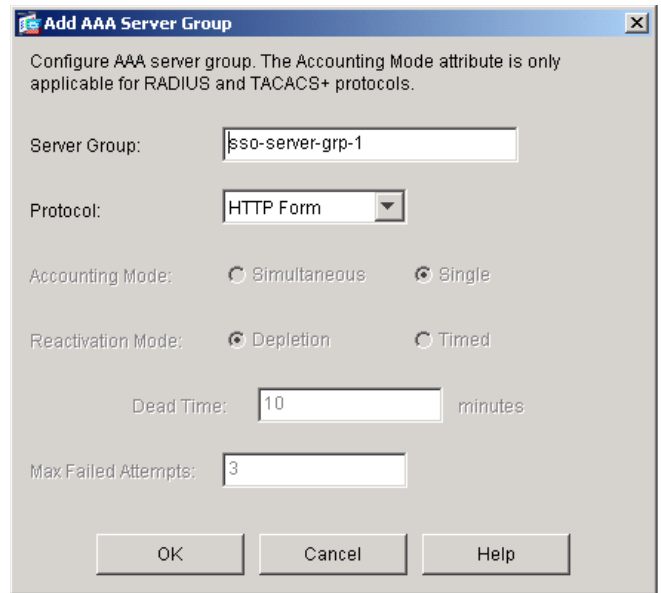
Figure 7-10 ASDM Window with AAA Servers Area Displayed



Step 2 Click **Add** in the Server Groups area.

The Add AAA Server Group dialog box appears as shown in Figure 7-11.

Figure 7-11 The Add AAA Server Group Dialog Box



Step 3 Enter the name of the server group in the Server Group field.

In this example, the name of the server group is sso-server-grp-1.

Step 4 From the Protocol menu, choose **HTTP Form**.

The remaining dialog box elements become unavailable.

- Step 5** Click **OK** to return to the ASDM window.
- Step 6** If it is not already selected, click on the server group you just created to select it.
- Step 7** Click **Add** in the Servers in Selected Group area.

The Add AAA Server dialog box appears. [Figure 7-12](#) shows this dialog box completed with the values described in [Step 8](#) through [Step 16](#).

Figure 7-12 The Add AAA Server Dialog Box

The screenshot shows the 'Add AAA Server' dialog box with the following configuration:

- Server Group: sso-server-grp-1
- Interface Name: inside
- Server Name or IP Address: 10.0.0.3
- Timeout: 10 seconds
- HTTP Form Parameters:
 - Start URL: http://example.com/east/Area.do?Page-Grp1
 - Action URI: http://www.example.com/auth/index.html/appdir... (truncated)
 - Username: userid
 - Password: user_password
 - Hidden Values: SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Ffemco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0
 - Authentication Cookie Name: ExamplAuthCookie

- Step 8** From the Interface Name menu, choose **inside**, **outside**, or **management**.
In this example, we choose **inside**. Interface name selection does not effect functionality.
- Step 9** In the Server Name or IP Address field, enter either the name or address of the authenticating web server.
In this example, we enter the internal IP address.
- Step 10** In the Timeout field, enter the time in seconds before a failed SSO authentication attempt times out.
- Step 11** If the authenticating web server sets a pre-login cookie, configure the start URL from which to retrieve the pre-login cookie from the web server by performing the following steps:
- In the Start URL menu, choose one of the following:
 - http** for unencrypted messaging between the security appliance and the web server
 - or-
 - https** for secure messaging between the security appliance and the web server
 - In the Start URL field, enter the rest of the complete start URL for the authenticating web server.
In this example, the complete start URL is `http://example.com/east/Area.do?Page-Grp1`.

Step 12 In the Action URI field, enter the URI for the authentication program on the web server.

The maximum number of characters for a complete URI is 2048. The action URI in this example follows:

```
http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALM
OID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$S
M$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth
.example.com
```



Note

You must include the hostname and protocol in the action URI. In the preceding example, these appear at the start of the URI in `http://www.example.com`.

Step 13 In the Username field, enter the name of the username parameter for the HTTP POST request.

In this example, the username parameter is named `userid`.

Step 14 In the Password field, enter the name of the password parameter for the HTTP POST request.

In this example, the password parameter is named `user_password`.

Step 15 If the web server expects hidden parameters in the POST request, enter the hidden parameters expected in the Hidden Values field.

In this example, the Hidden Values entry is:

```
SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0
```

This entry, excerpted from a POST request, includes four form entries and their values, each separated by an `&`. The four entries and their values are:

- SMENC with a value of ISO-8859-1
- SMLOCALE with a value of US-EN
- target with a value of `https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG`
- smauthreason with a value of 0

Step 16 Enter the name of the authentication cookie in the Authentication Cookie Name field. This step is optional.

In this example, the authentication cookie name is `ExampAuthCookie`.

Step 17 Click **OK** to return to the ASDM window.

Step 18 Click **Apply** to add the new SSO server and server group to the running configuration.

Assigning the SSO Server to a Tunnel Group

The final task is to assign the new SSO server to a new or existing tunnel group. In this example, we assign the SSO server to a new WebVPN tunnel group named `WebVPNGroup1` by performing the following steps:

Step 1 In the main Cisco ASDM window, choose **Configuration > VPN > General > Tunnel Group**.

Step 2 Click **Add** and choose **WebVPN Access**.

The Add Tunnel Group dialog box appears with the General and Basic tabs displayed.

Step 3 Enter the name of the new tunnel group in the Name field.

In this example, the name is `WebVPNGroup1`.

- Step 4** Click the **AAA** tab and select the new SSO server group from the Authentication Server Group menu. In this example, the name of the server group is sso-server-grp-1.
- Step 5** Click **OK** to return to the **Configuration > VPN > General > Tunnel Group** window, and then click **Apply** to add the tunnel group to the running configuration.