Configure Sterling Secure Proxy Single Sign-on to Work with CA SiteMinder

Refer to the following table before you configure Sterling Secure Proxy and Sterling External Authentication Server:

Section	Description
Software Requirements on page 2	
Configure Token Validation and Authorization Handling on page 2	Use this procedure if you want to validate the token and check the authorization of the user associated with the token.
Custom Token Manager on page 4	This section describes how the Custom Token Manager works with CA SiteMinder to validate tokens.
User Authentication Exit on page 5	This section describes how the CA SiteMinder user authentication exit works and how to disable the user authorization check.
Modify the Token Validation Interval in Sterling Secure Proxy on page 6	This section describes how to change how often the token is validated in Sterling Secure Proxy. Use this procedure if you need to change the default validation interval of 60 seconds.
Configure Token Validation by URI in Sterling Secure Proxy on page 6	Use this procedure if you need to validate tokens by URI.

Software Requirements

This single sign-on solution requires the following software:

- Sterling Secure Proxy version 3.3.01 (with patch 3) or later
- Sterling External Authentication Server version 2.3.01 (with patch 4) or later
- CA Siteminder

Configure Token Validation and Authorization Handling

This procedure is required to display user authentication errors with a customized message based on the returned error code, or to redirect the browser to an external page based on the returned error code.

To configure token validation and authorization handling, edit the extendedTokenAuthHandling.properties file. This file is located in <*install_dir*>/Signon/resources, where *install_dir* is the directory where Sterling Secure Proxy is installed.

The extendedTokenAuthHandling.properties file is deployed as sampleOf_extendedTokenAuthHandling.properties. To enable this option, rename the file to extendedTokenAuthHandling.properties.

The extendedTokenAuthHandling.properties file contains the following properties:

Property	Value
AUTHORIZATION_CODE_PREFIX	The prefix of the response code. AUTZ (uppercase) is the only valid value.
default.messageKey	The default message key. This key and the message displayed to the user is specified in a separate message file.
default.responseType	The default response type. AUTHORIZATION (uppercase) is the only valid value.
default.htmlPage	The default html page that Sterling Secure Proxy displays when authorization fails.
ResponseCode.responseType	The response type for this error. AUTHORIZATION (uppercase) is the only valid value.
ResponseCode.messageKey	The message key for this error message. This key and the message displayed to the user is specified in a separate message file.
ResponseCode.redirectTo	Web site that Sterling Secure Proxy redirects the user to when this error occurs.
ResponseCode.htmlPage	The html page that Sterling Secure Proxy displays when this error occurs.

Note: *ResponseCode* is the response code returned from the user authentication exit. Currently, this value is AUTZ300D.

If the htmlPage property is specified, the redirectTo property is ignored. If htmlPage is not specified and redirectTo is specified, messageKey is ignored. Refer to the following table when you configure the extendedTokenAuthHandling.properties file:

messageKey Specified?	htmlPage Specified?	redirectTo Specified?	Action taken by Sterling Secure Proxy
Yes	Yes	Yes	Displays the htmlPage with message
Yes	Yes	No	Displays the htmlPage with message
Yes	No	Yes	Redirects to the redirectTo URL
No	Yes	Yes	Displays the htmlPage with the default message
No	No	Yes	Redirects to the redirectTo URL
Yes	No	No	Displays the default page with message
No	No	No	Displays the default page with default message

A sample extendedTokenAuthHandling.properties file is shown below:

```
AUTHORIZATION_CODE_PREFIX = AUTZ

default.messageKey      =   TOKEN_VALIDATION_FAILED
default.responseType    =   AUTHORIZATION
default.htmlPage        =   error.html

AUTZ300D.responseType   =   AUTHORIZATION
AUTZ300D.messageKey     =   RESOURCE_NOT_ALLOWED
AUTZ300D.redirectTo     =   http://unauthorized.yoursite.com
AUTZ300D.htmlPage       =   error.html
```

The messages that Sterling Secure Proxy displays on the page are configured in the Signon/resources/messageBundle.properties file. This file contains the messageKey and the associated message to display. A sample messageBundle.properties file is shown below:

```
TOKEN_VALIDATION_FAILED =You are not authorized to view this page.

RESOURCE_NOT_ALLOWED =You are not allowed to view this page.
```

Custom Token Manager

This section describes how the Custom Token Manager works with Sterling Secure Proxy and Sterling External Authentication Server.

The following information is passed to the Custom Token Manager in Sterling External Authentication Server from Sterling Secure Proxy when validating a token.

Information Passed	Description	Example
Token	The SSO token cookie	
Action	The HTTP method.	GET, POST
URL	The URL of the resource the user is trying to access	http://host:port/myFG/foo.html
DestinationServiceName	The destination service name (configured in the Netmap Outbound Node for the Adapter	myFG
Client IP address	IP address of the client accessing resource	10.20.30.50

The Custom Token Manager validates the token by calling the CA SiteMinder decodeSSOToken API. This API decrypts the token and returns attributes specified when the token was generated. One of the token attributes returned is the session ID. The Custom Token Manager calls the CA SiteMinder login API to validate that the session ID is still active, and if it is active, to update its last access timestamp. The login API requires a protected resource. For this resource, the Custom Token Manager uses the destination service name if specified in the Netmap Outbound Node; otherwise it uses the value of the agent.resource property configured on the Custom Token Manager properties.

After the token is validated, the Custom Token Manager calls the CA SiteMinder authorize API to authorize the specified action and resource. The resource is the path part of the URL. For example, if the URL is "http://host:port/myFG/foo.html", the resource is "/myFG/foo.html".

The client IP address is used to call the CA SiteMinder login API and authorize API. CA SiteMinder policies can specify IP address restrictions. By passing the client IP address, CA SiteMinder IP address restrictions can be enforced. The client IP address will also be written to the CA SiteMinder audit log.

When authorization fails, the following error will be logged in seas.log and the audit log:

```
AUTH074E Authentication failed for <userid>. Exception encountered during
custom exit: AUTH071E Authentication failed for <userid> (Reason: not
authorized to access resource <resource>).
```

User Authentication Exit

This section describes how the user authentication exit process works and how to disable the user authorization check if required.

The CA SiteMinder user authentication exit is invoked when authenticating a user through the HTTP internal logon portal, HTTP basic authentication, and through the FTP, SFTP, and Sterling Connect:Direct protocol adapters. It is not invoked when using the HTTP external logon portal.

The following information is passed to the user authentication exit in Sterling External Authentication Server from Sterling Secure Proxy when authenticating a user.

Information Passed	Description	Example
Userid	User ID	Partner1
Password	The user password	Password
DestinationServiceName	The destination service name (configured in the Netmap Outbound Node for the Adapter)	myFG
Client IP address	IP address of the clint	10.30.30.50

The user authentication exit calls the CA SiteMinder login API to authenticate the user and password. The login API requires a protected resource. For this resource, the user authentication exit uses the destination service name if it is specified in the Netmap Outbound Node; otherwise it uses the value of the agent.resource property configured on the user authentication exit properties.

By default, the user authentication exit will also authorize the user against the resource used on the login API. If the authorization fails, the user is logged out and an AUTZ300D response code is returned to Sterling Secure Proxy.

Use the following procedure to disable the user authorization check:

1. Launch the Sterling External Authentication Server user interface and log in.
2. On the Authentication Definitions window, select the profile to modify.
3. Ensure the Authenticate using custom exits check box is selected and press the ... button.
4. Click the ... button next to Java Class Properties.
5. Type authorize.enable in the Key field.
6. Type false in the Value field.
7. Click OK.
8. Click OK on the Update authentication definition page.

Modify the Token Validation Interval in Sterling Secure Proxy

This procedure is optional.

The Token Validation Interval defines how long Sterling Secure Proxy caches the token for validation. The default value is 60 seconds. If a request is made while the token is cached, the token of that request will not be validated again. If you set this value to 0, Sterling Secure Proxy will not cache the token and will validate every request. To change this setting, complete the following procedure:

1. Launch the Sterling Secure Proxy Configuration Manager and log in.
2. Click Advanced from the menu bar.
3. From the navigation menu, click SSO Configurations.
4. Click the SSO configuration to modify.
5. Click on the Properties tab.
6. Click the Add button to add a new property.
7. Type sso.token.validation.interval in the Key field.
8. Type the new Token Validation Interval (in seconds) in the Value field.
9. Click the Save button to save the configuration.

Configure Token Validation by URI in Sterling Secure Proxy

This procedure is optional

When Token Validation by URI is enabled, Sterling Secure Proxy caches the validation status of all URIPaths for each HTTP connection. If the token with the URIPath has been validated and, therefore, authorized, Sterling Secure Proxy does not call Sterling External Authentication Server to validate the token with the associated URL again.

Sterling Secure Proxy will validate an HTTP request with an SSO token if any of the following conditions are met:

- Sterling Secure Proxy has no previous record about this token.
- The previous status for this URIPath was not authorized.
- The last token validation time is longer than the Token Validation Interval.
- The last token in this HTTP connection is different from the current token.

Sterling Secure Proxy creates a unique cache of the validation status for every HTTP connection. Resources from the same URIPath can get validated more than once depending on how and when the browser makes the connection. For example, the browser can request http://host:port/myfilegateway/isomorphic/system/modules/ISC_History.js on one connection and /myfilegateway/isomorphic/system/modules/ISC_Core.js on another connection. Both of these requests will trigger a call to Sterling External Authentication Server to validate the token.

However, if both requests were made on the same connection, Sterling Secure Proxy will only call Sterling External Authentication Server for the first request unless the validation of the token fails.

The Token Validation by URI option is disabled by default. To enable Token Validation by URI, complete the following procedure:

Note: Token Validation by URI can impact performance. If you do not require authorization, consider leaving this feature disabled or increasing the Token Validation Interval.

1. Launch the Sterling Secure Proxy Configuration Manager and log in.
2. Click Configuration from the menu bar.
3. From the navigation menu, click Adapters.
4. Select the HTTP Adapter configuration to modify.
5. Click on the Properties tab.
6. Click the Add button to add a new property.
7. Type enable.token.validation.by.uri in the Key field.
8. Type true in the Value field.
9. Click the Save button to save the configuration.