Sterling Secure Proxy®

Enable Single Sign-On for a Trading Partner

Version 3.2

Sterling Commerce
An IBM Company

Sterling Secure Proxy Enable Single Sign-On for a Trading Partner
Version 3.2

Third Edition

Sterling Commerce, Inc.

4600 Lakehurst Court Dublin, OH 43016-2000 * 614/793-7000

Contents

Configure an HTTP Connection Between SFG and SSP To Enable Single Sign-On for a Trading Partner

Sterling Secure Proxy (SSP) can be used as a proxy with Sterling File Gateway (SFG) and supports a single sign-on connection. Single sign-on (SSO) provides a method of access control that allows a user to log in once to SSP, using the HTTP protocol, and then gain access to SFG without being prompted to log in again. SSO bypasses the normal user authentication process in SFG and instead trusts that SSP has authenticated the user.

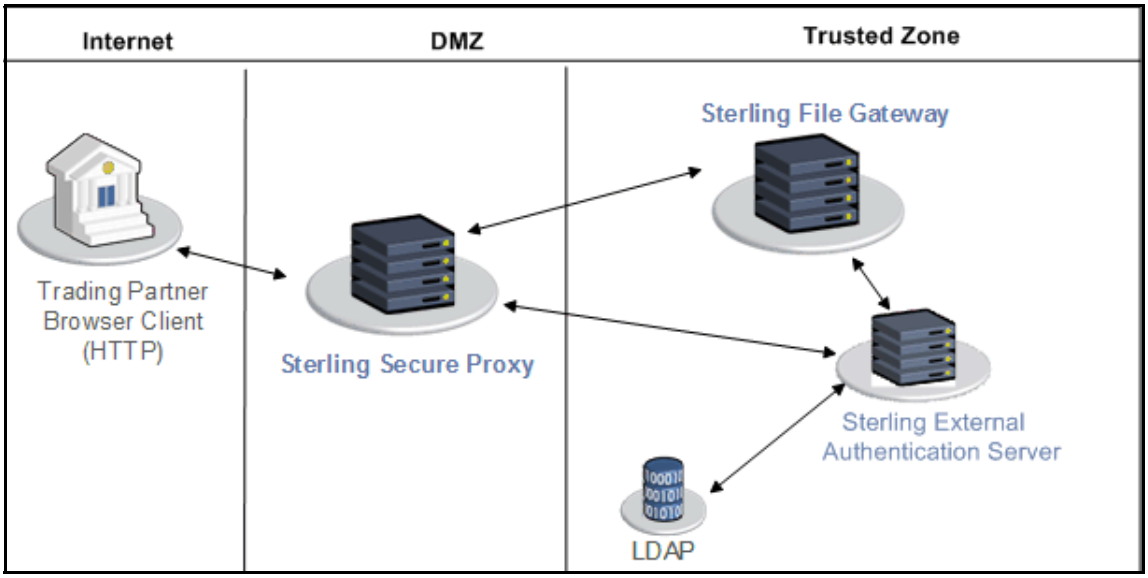
To support single sign-on, configure an SSP login page and configure EA to generate SSO tokens. Configuring SSO allows a trading partner to log on and use the same login session to connect to SSP and SFG. By default, Sterling External Authentication Server (EA) uses Open SAML to create and manage SSO tokens. However, you can customize your environment to use a third-party application, such as RSA Access Manager or SiteMinder, to generate tokens.

This chapter describes how to configure the HTTP protocol in SSP between the trading partner and SSP and between SSP and SFG to enable authentication through EA. It also describes how to configure Sterling External Authentication (EA) to issue tokens to authenticate the connection between SSP and SFG, without the need to log in again for this connection.

Flow of Data for Sign-On Configuration Between SFG and SSP

After you set up the basic single sign-on configuration, trading partners can communicate in a secure environment that provides authentication. The trading partner first connects to Sterling Secure Proxy which then connects to SFG on behalf of the trading partner.

Following is an illustration of the flow of data:



Following are the steps that occur during a single sign-on session between a trading partner, SSP, and SFG when EA is used to generate and manage tokens:

1. The trading partner requests a connection to Sterling File Gateway.
2. Sterling Secure Proxy receives the request and the SSL handshake between SSP and the trading partner begins. If SSL authentication is configured, the proxy submits its certificate to the trading partner. If client authentication is configured, the trading partner then submits its certificate to SSP for authentication. You can optionally configure SSP to enforce client authentication and send the certificate to EA for validation.
3. SSP presents a login page to the trading partner, who provides his user ID and password.
4. SSP sends the user ID and password to Sterling External Authentication (EA) and then validates it against information stored in LDAP.
5. If the credentials are valid, EA creates an OpenSAML v2 token and SSP returns a cookie associated with the token to the trading partner.
6. The trading partner sends an HTTP request to SFG and includes the cookie.
7. SSP checks for the cookie and validates the token using EA.
8. SSP then connects to SFG and performs an SSL handshake. It then sends the HTTP request with the cookie from the trading partner to SFG.
9. SFG then validates the token against EA and begins normal operation.

Prerequisites

Before you configure a single sign-on configuration, install and configure the following components:

- ✦ Sterling External Authentication Server version 2.2 or later

- Sterling File Gateway (SFG) build 4318 or later
- An LDAP server
- A user store in the LDAP server with user definitions for each trading partner connection
- A user store on SFG with the same user definitions as defined in the LDAP database
- An External Authentication Server definition in SSP
- Sterling Secure Proxy version 3.2 or later

Configuration Considerations

Before you complete the single sign-on configuration, be aware of the following considerations:

- Only the HTTP protocol supports single sign-on connections.
- Each single sign-on user you create in SFG must be assigned to the user group called File Gateway Partner Users.
- Customize the SSP login page—When you configure the basic scenario, you use the default SSP login page. The default page provides basic information, including user name and password. To customize this page, to include additional information and your logo, complete the procedure, *Customize the Login Page* on page 24.
- If you are using a load balancer to run multiple SSP engines, avoid login credential errors by configuring the load balancer to use sticky sessions based on the IP source address.

Organization of Single Sign-On Scenarios

This document provides instructions on how to configure single sign-on between SSP and HTTP-enabled trading partners and between SSP and SFG.

Configure the Basic Scenario to Enable a Connection to the myFileGateway Application

Configure the basic scenario to allow you to quickly become operational using single sign-on to connect to myFileGateway, the trading partner interface in SFG. After you complete this scenario, test the connection to ensure that you have correctly configured it. After you determine that it works, add SSL/TLS support. You then have a basic configuration and can begin operation.

Configure Advanced Features

After you configure the basic SSO setup, determine if your environment requires an advanced feature. Following are the advanced features:

- Customize the OpenSAML v2 tokens—You use the default token generation definition when you configure the basic single sign-on definition. To customize the token definition, you can modify the named identity provider, the token signing key, or how long a token can be used before it expires. Refer to *Customize Token Definitions Created by EA* on page 24.

- Use a third-party application to configure tokens. The basic scenario uses EA to configure and manage tokens. To use a third-party application to configure tokens, you complete additional setup procedures. Refer to *Allow a Third- Party Provider to Create Tokens* on page 22.

Configure Optional Features

SSP provides the following optional features and you can configure them as required for your environment. Refer to the HTTP Reverse Proxy Configuration chapter in the *Sterling Secure Proxy Configuration Guide* for instructions on how to configure the following features:

- Modify the HTTP connection requirement between SSP and inbound nodes by defining a specific IP address, a wildcard peer pattern, or an IP/subnet pattern.
- Secure the outbound HTTP connection between SSP and SFG using SSL or TLS.
- Authenticate an inbound certificate using EA.
- Define alternate nodes for failover support.

Sterling External Authentication provides the ability to configure multifactor authentication. In addition to configuring client authentication in SSP, EA can also authenticate the IP address, certificate, password, and/or group access. Refer to *Sterling External Authentication Server Implementation Guide*.

Worksheets

Before you complete each procedure, gather the information you need to configure it, on the worksheet provided. For each worksheet:

- Provide a value for each SSP feature listed. Fields listed in the worksheet are required.
- Accept default values for fields not listed.
- Note the Configuration Manager field where you will specify the value.

Field Definitions

Field definitions are provided for all single sign-on functions. Refer to *Single Sign-On Field Definitions in SSP* on page 26 and *Single Sign-On Tokens Field Definitions in EA* on page 28. For additional field definitions, refer to the *Sterling Secure Proxy Configuration Guide.*

Basic Single Sign-On Scenario

Complete the following tasks to define an HTTP configuration between a trading partner and SSP and between SSP and Sterling File Gateway to support a single sign-on connection:

- Configure SSP to support basic single sign-on.
- Use the default single sign-on configuration in EA to manages OpenSAML v2 tokens.
- Prepare Sterling File Gateway to support the single sign-on option.
- Validate the connections between the trading partner, SSP, and SFG.

Configure SSP for Basic Single Sign-On

Complete the following procedures to configure SSP for basic single sign-on:

- Create an SSO configuration.
- Create an SSP policy to support a single sign-on connection to SFG.
- Define a netmap to identify inbound and outbound connections.
- Define an HTTP adapter.

Create an SSO Configuration

The SSO configuration defines the location of the files used to present the SSP login page and resources used to display the page. The basic configuration uses the default settings. Advanced configurations provide information about customizing the configuration.

Before you create an SSO configuration, gather the following information:

Configuration Manager Field	Feature	Value
Name	SSO configuration file.	_____

To define an SSO configuration:

1. Click Advanced from the menu bar.
2. Click **Actions>New SSO Configuration**.
3. Type a configuration name in the **Name** field.
4. Click **Save**.

Create an HTTP Policy to Support a Single-Sign On Connection

The HTTP policy defines how you impose controls to authenticate a trading partner trying to access a Sterling File Gateway server over the public Internet.

Before you create an HTTP policy to enable single sign-on, gather the following information:

Configuration Manager Field	Feature	Value
Policy Name	Name of policy.	_____
User Authentication Type	User authentication.	Application Authentication
External Authentication Profile	Name of the profile you defined in Sterling External Authentication Server.	_____
Internal User ID	Trading partner ID required to connect to the Sterling File Gateway server.	SSO token from External Authentication

To define a policy to support a single sign-on connection to SFG:

1. Click **Configuration** from the menu bar.
2. Click **Actions>New Policy>HTTP Policy**.
3. Type a **Policy Name**.
4. Click the **Advanced** tab.
5. Do one of the following:
   - If the trading partner connects using a browser, in the **User Authentication Type** field, select Application Authentication.

     The values, Through External Authentication and SSO token from External Authentication, are selected by default.
   - If the trading partner connects using a non-browser client, do the following:
     a. In the **User Authentication Type** field, select Basic Authentication.
     b. Enable **Through External Authentication**.
     c. From the **Internal User ID** field, enable SSO token from External Authentication.

   Note: Configure application authentication if the trading partner connects through a browser. For non-browser client connections, configure basic authentication.
6. Type the definition you defined in EA in the **External Authentication Profile** field.
7. Click **Save**.

Create an HTTP Netmap to Support a Single Sign-On Connection to myFileGateway

You create a netmap and define inbound connection information for your external trading partners. You also define outbound connection information for the Sterling File Gateway server that SSP connects to and identify an HTTP server adapter with the URL of /myfilegateway. The netmap is associated with a policy and an adapter.

Before you create a netmap, gather the following information:

Configuration Manager Field	Feature	Value
Netmap Name	Netmap name.	_____
Inbound Trading Partner Information		
Inbound Node Name	Name to assign to inbound node definition (trading partner).	_____

Configuration Manager Field	Feature	Value
Peer Address Pattern	Host name or IP address pattern.	* * allows all trading partners configured on the SFG server to connect to the SSP server. Use this value for testing purposes. To create a more specific node definition, see *Define Inbound HTTP Node Connection Definitions* in the *Sterling Secure Proxy Configuration Guide*.
Policy	Name of policy you created in the procedure, *Create an HTTP Policy to Support a Single-Sign On Connection* on page 9.	Select this value from a pull-down list.
Outbound SFG Server Connection		
Node Name	Outbound server node name.	_____
Primary Destination Address	Host name or IP address to connect to the SFG server.	_____
Primary Destination Port	Port number to connect to the SFG server.	_____

To create a netmap and define inbound and outbound nodes:

1. Click **Configuration** from the menu bar.
2. Click **Actions>New Netmap>HTTP Netmap**.
3. Type a **Netmap Name**.
4. To define an inbound node definition, click the **Inbound Nodes** tab and click **New**.
5. Specify the following values:
   - Inbound Node Name
   - Peer Address Pattern
   - Policy
6. Click **OK**.
7. To define an outbound node definition, click the **Outbound Nodes** tab and click **New**.
8. Specify the following values:
   - Outbound Node Name
   - Primary Destination Address
   - Primary Destination Port
9. Click **OK**.
10. Click **Save**.

Define the HTTP Reverse Proxy Adapter Used for the Single Sign-On Connection

An HTTP adapter definition specifies system-level communications information necessary for HTTP connections to and from SSP. You can create multiple adapter definitions. Before you begin this procedure, make sure that you have an engine definition to associate with the adapter. Refer to the *Sterling Secure Proxy Installation Guide* for instructions.

Note: Make sure the engine is running when you configure the adapter. If it is running, configuration information is transmitted to the engine when you save it.

Before you create an HTTP adapter, gather the following information:

Configuration Manager Field	Feature	Value
Adapter Name	Adapter name.	_____
Listen Port	Listen port to use for inbound connections.	_____
Netmap	Netmap to associate with the adapter.	_____
Routing Type	How traffic is routed through SSP.	standardRouting
Standard Routing Node	SFG server where inbound connections are routed. Define an outbound node in the netmap definition.	_____
Engine	SSP engine that will be used as the proxy.	_____
SSO Configuration	Name of the SSO configuration you created in *Create an SSO Configuration* on page 9.	_____
External Authentication Server	Name of the EA server. Refer to the *Sterling Secure Proxy Configuration Guide* for instructions to configure an EA server.	_____
Properties Key	Define the key called default.app.url to identify the SFG application to connect to.	/myfilegateway

To define an HTTP adapter that supports single sign-on to the myFileGateway application in SFG:

1. Click **Configuration** from the menu bar.
2. Click **Actions>New Adapter>HTTP Reverse Proxy**.
3. Specify values in the following fields:
   - Adapter Name
   - Listen Port
   - Netmap
   - Standard Routing Node
   - Engine

4. Click the **Advanced** tab.
5. Specify values in the following fields:
   - SSO Configuration
   - External Authentication Server
6. Click the **Properties** tab.
7. Use the arrow to move to page 2 in the properties list.
8. Select the default.app.url property and set its value to /myfilegateway.

> **Note:** After editing a property value, be sure to click **OK** before moving to another page in the property list. Otherwise, the value you defined is lost.

9. Click **Save**.

Configure Sterling EA to Support Single Sign-On

To allow an SSO connection between a trading partner and SSP to route traffic to SFG, you configure Open SAML v2.0 tokens in Sterling External Authentication Server. You can authenticate an inbound connection against information stored in an LDAP database by configuring EA to define how the connection is authenticated. The EA definition determines which options are enabled. Refer to *Sterling External Authentication Server Implementation Guide* for instructions on configuring an EA definition.

The EA server generates and manages tokens. A default configuration called SEAS-SAML is enabled when you install EA. If you use the default configuration, EA is enabled as the identity provider name, token signing keys are automatically generated and the token is set to expire after fifteen minutes. Use the default configuration when you configure the basic single sign-on environment.

To customize the EA configuration for the single sign-on environment, refer to *Customize Token Definitions Created by EA* on page 24. You can customize the provider name of the token, token signing key, or length of time until a token expires.

Prepare SFG to Support Single Sign-On with SSP

Before you enable single sign-on between a trading partner and Sterling File Gateway (SFG), when using Sterling Secure Proxy, you must modify the SFG installation. The files required to enable SSO are stored on the External Authentication Server installation.

Prepare SFG to Support Single Sign-On on UNIX or Linux

To prepare SFG to support SSO on UNIX or Linux:

1. From the EA server, copy the files and subdirectories from the *EA_install_dir*/lib/sterling/sfg-sso-plugin directory to a location that is accessible to the SFG server, where *EA_install_dir* is the location of the EA installation.

   Note: If you use FTP to copy the files to the SFG server, be sure to transfer the .jar files in binary mode (TYPE I).

2. On the SFG server, move to the *SFG_install_dir*/properties directory, where *SFG_install_dir* is the location of the SFG installation.
3. Type the following command to copy the SSO properties file to the SFG server, where *base_dir* is the location where you copied the files in step 1:

```
cp base_dir/sfg-sso-plugin/properties/authentication_policy.properties_seas-auth_ext.in .
```

4. Stop SFG if it is running.
5. From the *SFG_install_dir*/bin directory, type the following commands:

```
./install3rdParty.sh seas-sso 1.0 -j base_dir/sfg-sso-plugin/seas-sso.jar
./install3rdParty.sh seas-sso 1.0 -p base_dir/sfg-sso-plugin/properties/seas-sso.properties
./install3rdParty.sh seas-auth 1.0 -p base_dir/sfg-sso-plugin/properties/seas-auth.properties
```

6. From the *SFG_install_dir*/jar/seas-sso/1.0 directory, create a subdirectory named private.
7. Move to the /private directory.
8. Type the following command to copy the jar files to the /private directory on the SFG server:

```
 cp base_dir/sfg-sso-plugin/private/*.jar .
```

Change the Properties File to Support Single Sign-On on UNIX or Linux

Before Sterling File Gateway is configured to support single sign-on from an SSP environment, you must modify properties. Do not make changes directly to the properties files. Instead, make changes to a file called customer_overrides.properties. This prevents custom settings from being overwritten when you apply patches. The customer_overrides.properties file is not changed during upgrades or patches. Refer to the Sterling Integrator customer_overrides.properties topic for more information. This documentation is located on the Sterling Commerce Customer Center Documentation web site.

To modify the properties file to enable single-sign on:

1. In the *install_dir*/properties directory, locate or create the customer_overrides.properties file.

2. Open the file in a text editor and add the properties that you want to override.
   a. Add the following values to configure signon:
      - security.SSO_FORWARD_URL.MYFILEGATEWAY.LOGOUT= /Signon/logout
      - security.SSO_FORWARD_URL.MYFILEGATEWAY.TIMEOUT= /Signon/timeout
      - security.SSO_FORWARD_URL.MYFILEGATEWAY. VALIDATION_FAILED=/Signon/validationerror
   b. Add the following connection parameters to configure EA:
      - seas-sso.EA_HOST=*IP address or host name of EA server*
      - seas-sso.EA_PORT=*listen port of EA server*
      - seas-sso.EA_PS_NAME=*perimeter server used to connect to EA*
      - seas-sso.EA_SECURE_CONNECTION=enables a secure EA

        true sets connections to EA as secure and *false* sets the connection as clear. If this parameter is true, you must also define the EA_SYSTEM_CERT and EA_TRUSTED_CERT[1].
      - seas-sso.EA_SYSTEM_CERT=name of the system certificate in the system certificate store, if the connection is secure
      - seas-sso.EA_TRUSTED_CERT[1]=name of the trusted certificate used by EA for secure connections
3. Save and close the file.
4. Stop and restart Sterling Secure to use the new values.

Prepare SFG to Support Single Sign-On on Windows

To prepare SFG to support SSO on Windows:

1. From the EA server, copy the files and subdirectories from the *EA_install_dir*\lib\sterling\sfg-sso-plugin directory to a location that is accessible to by the SFG server.

   Note: If you use FTP to copy the files to the SFG server, be sure to transfer the .jar files in binary mode (TYPE I).

2. On the SFG server, move to the *SFG_install_dir*\properties directory.
3. Type the following command to copy the SSO security.properties file to the SFG server, where *base_dir* is the location where you copied the files in step 1:

   ```
   copy base_dir\sfg-sso-plugin\properties\security.properties_seas-sso_ext.in .
   ```

4. Stop SFG if it is running.

5. From the *SFG_install_dir*\bin directory, type the following commands:

```
./install3rdParty.sh seas-sso 1.0 -j base_dir/sfg-sso-plugin/seas-sso.jar
./install3rdParty.sh seas-sso 1.0 -p base_dir/sfg-sso-plugin/properties/seas-sso.properties
./install3rdParty.sh seas-auth 1.0 -p base_dir/sfg-sso-plugin/properties/seas-auth.properties
```

6. From the *SFG_install_dir*\jar\seas-sso\1.0 directory, create a subdirectory named private.
7. Go to the \private directory.
8. Type the following command to copy the jar files to the SFG server:

```
copy base_dir\sfg-sso-plugin\private\*.jar .
```

Change the Properties File to Support Single Sign-On on Windows

Before Sterling File Gateway is configured to support single sign-on from an SSP environment, you must modify properties. Do not make changes directly to the properties files. Instead, make changes to a file called customer_overrides.properties. This prevents custom settings from being overwritten when you apply patches. The customer_overrides.properties file is not changed during upgrades or patches. Refer to the Sterling Integrator customer_overrides.properties topic for more information.

To modify the properties file to enable single-sign on:

1. In the *install_dir*\properties directory, locate or create the customer_overrides.properties file.
2. Open the file in a text editor and add the properties that you want to override.
   a. Add the following values to configure signon:
      - security.SSO_FORWARD_URL.MYFILEGATEWAY.LOGOUT= \Signon\logout
      - security.SSO_FORWARD_URL.MYFILEGATEWAY.TIMEOUT= \Signon\timeout
      - security.SSO_FORWARD_URL.MYFILEGATEWAY. VALIDATION_FAILED=\Signon\validationerror

   b. Add the following connection parameters to the override file to configure EA:
      - seas-sso.EA_HOST=*IP address or host name of EA server*
      - seas-sso.EA_PORT=*listen port of EA server*
      - seas-sso.EA_PS_NAME=*perimeter server used to connect to EA*
      - seas-sso.EA_SECURE_CONNECTION=enables a secure EA

        true sets connections to EA as secure and *false* sets the connection as clear.

        If this parameter is true, you must also define the EA_SYSTEM_CERT and EA_TRUSTED_CERT[1].
      - seas-sso.EA_SYSTEM_CERT=name of the system certificate in the system certificate store, if the connection is secure
      - seas-sso.EA_TRUSTED_CERT[1]=name of the trusted certificate used by EA for secure connections
3. Save and close the file.
4. Stop and restart Sterling Secure Proxy to use the new values.

Verify That SFG is Configured for Single Sign-On

Before you configure additional functions, make sure that SFG is ready for use in a single sign-on environment. To verify the configuration, start SFG.

View the authentication.log and security.log to make sure the SFG files were updated. If the update was successful, log files display the success messages.

- Authentication.log file displays the following messages:

```
ALL 000000000000 GLOBAL_SCOPE SSOAuthenticationPolicy GIS is configured to support
single sign-on
ALL 000000000000 GLOBAL_SCOPE SSOAuthenticationPolicy SSO Property :
SSO_AUTHENTICATION_CLASS.1 = Class name :
com.sterlingcommerce.seas.gis.sso.plugin.SeasSsoProvider
ALL 000000000000 GLOBAL_SCOPE SecurityManager SSO Authentication - A new SSO
Authentication Policy has been installed.
ALL 000000000000 GLOBAL_SCOPE SecurityManager SSO Authentication:Enabled
ALL 000000000000 GLOBAL_SCOPE SecurityManager SSO Authentication on Page:Enabled
ALL 000000000000 GLOBAL_SCOPE SecurityManager Number of SSO Authentication
Plug-In:1
ALL 000000000000 GLOBAL_SCOPE SecurityManager SSO configuration
policy....SSOAuthenticationPolicy isComplete=true isEnabled=true
httpUserIdHeader=SM_USER
ALL 000000000000 GLOBAL_SCOPE SecurityManager initialization complete.
```

- Security.log displays the following message:

```
ALL 000000000000 GLOBAL_SCOPE SEAS-SSO: Plug-in initialized
```

Verify the SSP Connections

To verify that the engine can receive and initiate communications sessions after configuring the basic single sign-on environment, establish a connection between an HTTP client and the HTTP Reverse Proxy adapter to ensure that the SSP login page is displayed.

Note: Make sure the engine is running when you configure an HTTP adapter. If it is running, configuration files are automatically copied to the engine when you save any update. Configuration files must be available on the engine for communication sessions to be established.

This procedure enables you to verify that the engine can:

- Establish an HTTP session initiated by a trading partner using an HTTP client
- Initiate an outbound session to an SFG server on behalf of the HTTP client connection

To verify the communications sessions:

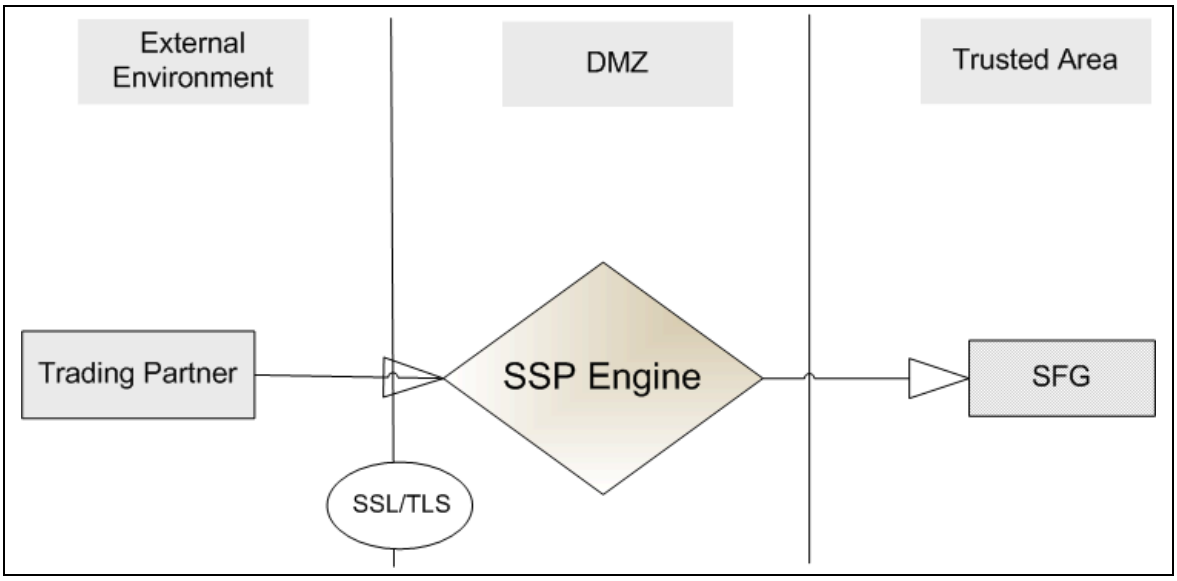
1. Make sure the engine is running.

2. Initiate an HTTP client request to the SSP server for the MyFilegateway URL, http://ssp_host:port/myfilegateway.
3. View the SSP login page used for a single sign-on session.
4. Provide valid logon credentials.
5. View the MyFilegateway home page.

If you can view MyFilegateway home page, you have confirmed that the connections are working. You are ready to add SSL or TLS support to the inbound connection.

Add SSL/TLS Support for an HTTP Connection to Complete the Basic Scenario

This scenario builds on the Basic Single Sign-On Configuration by enabling security for the inbound node you defined in the netmap. Following is a diagram to illustrate the addition of SSL or TLS to the inbound node connection.



Note: Before you configure SSL or TLS support, you must check in your certificates. Refer to Chapter 3, *Manage Certificates for SSL/TLS Transactions with Trading Partners* in the Sterling Secure Proxy Configuration Guide.

Secure the Inbound HTTP Connection Using the SSL or TLS Protocol

The first step in strengthening security is to secure the communications channel. This procedure describes how to enable the TLS or SSL protocol for the inbound connection to authenticate SSP to the trading partner initiating the connection. To require that SSP authenticate the trading partner, enable client authentication.

Before you can configure this option, you must obtain the necessary certificates and place them in the SSP Certificate Stores.

Before you add SSL/TLS support to the inbound connection, gather the following information:

Configuration Manager	Feature	Value
Inbound Node Name	Name of inbound node to add security to.	Select an inbound node definition.
Security Setting	Security protocol to use.	_____ (SSL v3 or TLS, SSL v2 or v3 with v3 Hello, SSL (any version) or TLS, SSL v2 or v3, TLS, or SSL v3)
Enable Client Authentication	Enable client authentication to require that the trading partner present its certificate for SSL or TLS client authentication?	_____ (Yes or No)
Trust Store	If client authentication is enabled, identify the trust store where the certificate used to verify the trading partner certificate is stored.	_____
CA Certificates/Trusted Root	Name of CA certificate/trusted root (if client authentication is enabled).	_____
Key Store	The database where the keys and system certificates you want to use are stored.	_____
Key/System Certificate	Name of SSP system certificate presented to the trading partner during the handshake.	_____
Available Cipher Suites Selected Cipher Suites	Select the ciphers to enable by moving them from the Available Ciphers to the Selected Ciphers field. TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_238_CBC_SHA, and TLS_RSA_WITH_3DES_EBE_CBC_SHA are enabled by default.	_____ _____ _____ _____

To enable the TLS or SSL protocol on the inbound connections:

1. Click **Configuration** from the menu bar.
2. Expand the Netmaps tree and select an HTTP netmap to modify.
3. Click the **Inbound Nodes** tab.
4. Select an inbound node to modify and click **Edit**.
5. Click the **Security** tab, and then click **Secure Connection** to enable security.

6. Select values for the following:
   - Security Setting
   - Key Store
   - Key/System Certificate
   - Available Cipher Suites
   - Selected Cipher Suites
7. To enable client authentication:
   a. Click **Enable Client Authentication**.
   b. Select the trust store where the CA certificate or trusted root certificate is stored.
   c. Select the CA Certificates/Trusted Root certificate to use.

   Note: Be sure to highlight the certificate to select it. If only one certificate is displayed in the field, it is not selected until you highlight it.

8. Click **OK**.
9. Click **Save**.

Establish a session initiated by an HTTPS client to SSP to test the configuration. If you can view the SSP login page, you have confirmed that the connections are working.

Variations to the Single Sign-On Configuration

This section provides instructions on the additional features you can configure by modifying the basic single sign-on scenario. Variations include:

- Customize the Open SAML v2.0 token attributes
- Allow a third-party provider to create tokens
- Customize token definitions created by EA
- Customize the login page

Customize the Open SAML v2.0 Token Attributes

To implement single sign-on, you use single sign-on attributes. When you configure the basic scenario, you use default attributes. You can customize these settings, including the name of the cookie containing the SSO token, HTTP 5header associated with a user ID, and the attributes associated with a token. Tokens can be generated with EA or with a third-party application. This procedure assumes you are using EA. Refer to *Allow a Third- Party Provider to Create Tokens* on page 22 for instructions on configuring an external application to generate tokens.

Before you customize this page, gather the following information:

Configuration Manager Field	Feature	Value
Name	Name to assign to the single sign-on configuration.	_____
Front End SSO Token Cookie Name (Inbound)	Name to assign the cookies associated with each token. This value must match the definition in SFG.	_____
Back End SSO User Header Name (Outbound)	The HTTP header name containing the user name that is sent to SFG.	_____
Back End SSO Token Cookie Name (Outbound)	Name to assign the cookies associated with each token. This value must match the definition in SFG.	_____

1. Click **Advanced** from the menu bar.
2. Do one of the following:
   - To create a new SSO configuration:
     a. Click **Actions>New SSO Configuration**.
     b. Type an SSO configuration name in the **Name** field.
   - To edit an existing SSO configuration:
     a. From the navigation menu, click **SSO Configurations**.
     b. Click the configuration to modify.
3. To customize the front-end definitions, edit the Front End SSO Token Cookie Name field.
4. To customize the back-end definitions, edit the following fields:
   - Back End SSO User Header Name
   - Back End SSO Token Cookie Name

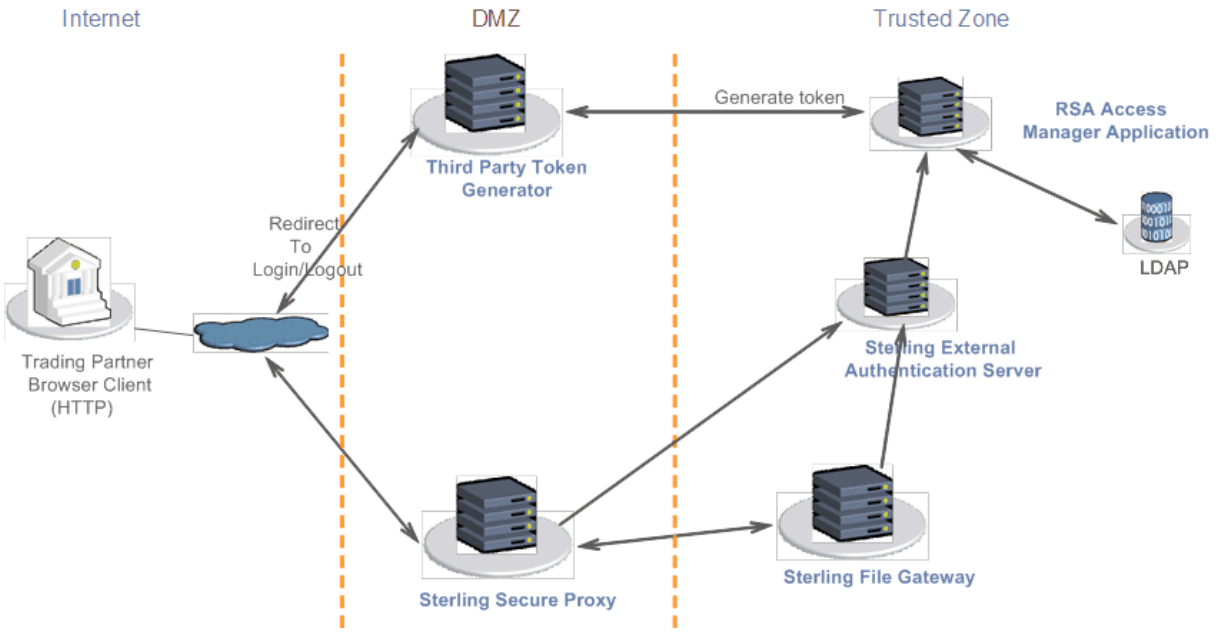
   Note: The values defined in the back-end fields must match the settings defined in SFG. Refer to the Sterling File Gateway documentation for instructions.
5. Click Save.
6. Create a copy of the folder *ssp_install_dir*\Signon\.

   Making a copy of the folder prevents the custom attributes you created from being overwritten if you upgrade the software or apply a patch.

Allow a Third- Party Provider to Create Tokens

You used the default token generation definition when you configured the basic single sign-on definition. The default configuration uses EA to create tokens. To use a third-party application for token generation, you must modify the single sign-on attributes to configure an external application. You must also modify the SSO Token setup in EA.

The following diagram illustrates the flow using a third-party application for token generation.



Configure EA to Enable a Third-Party Provider to Create Tokens

Before you configure EA to enable a third-party application to create tokens, gather the following information:

Configuration Manager Field	Feature	Value
Token Manager	The application that creates the tokens.	Custom
Class Name	Name of the Java class that implements the token manager interface.	_____
Token Expiration Period	How long a token is valid. Default is 15 minutes.	_____

To configure EA and enable a third-party application to generate tokens:

1. Log on to EA.
2. Select **Manage>System Settings**.

3. From the System Settings dialog, click the **SSO Token** tab.
4. To configure a token manager other than EA, select **Custom** from the Token Manager drop-down box.
5. Provide the class name in the **Class name** field.
6. To change the how long a token can be used before it expires, type a new value in the **Token Expiration Period** field.
7. Click **OK**.

Customize SSP to Accept Tokens Generated by a Third-Party Application

Before you configure SSP to enable a third-party application to create tokens, gather the following information:

Configuration Manager Field	Feature	Value
Name	Name to assign to the single sign-on file.	_____
Front End External Application Login URL	External login portal URL where the user is authenticated and a token is generated.	_____

To configure the token attributes in SSP:

1. Click Advanced from the menu bar.
2. Do one of the following:
   - To create a new SSO configuration:
     a. Click **Actions>New SSO Configuration**.
     b. Type an SSO configuration name in the **Name** field.
   - To edit an existing SSO configuration:
     a. From the navigation menu, click **SSO Configurations**.
     b. Click the configuration to modify.
3. Click the **Advanced** tab.
4. To identify the URL of the application being used to generate tokens, type the URL in the **External Application Login URL** field.
5. Click **Save**.

Customize Token Definitions Created by EA

You used the default token definition when you configured the basic single sign-on definition. To customize the token definition, complete the following procedure. You can modify the named identity provider, the token signing key, or how long a token can be used before it expires.

Before you enable a third-party application to create tokens, gather the following information:

Configuration Manager Field	Feature	Value
Named Identity Provider	The prefix appended to generated tokens to identify the provider. **Note:** If you change the identity provider name, any outstanding tokens are invalid.	_____
Token Signing Key	Alias of the key certificate used to sign the token.	_____
Token Expiration Period	How long a token is valid.	_____

To customize the token configuration in EA:

1. Log on to EA.
2. Select **Manage>System Settings**.
3. From the System Settings dialog, click the **SSO Token** tab.
4. Customize one or more of the following definitions:
   - Named Identity Provider
   - Token Signing Key
   - Token Expiration Period
5. Click **OK**.

Customize the Login Page

You used the default login page definition when you configured basic single sign-on. The default configuration uses a simple login page with no logo information and prompts the user to provide a user ID and password.

You can customize a login page to define how a page looks and what information to include on the page. Customize this page by modifying the labels or replacing the entire page.

Before you modify the login page, gather the following information:

Configuration Manager Field	Feature	Value
Name	Name of the single sign-on configuration.	_____
Internal Token Attributes		
◆ Application Login Page	Custom page displayed for the single sign-on log in.	_____
◆ Login Directory ID	Custom directory in the engine installation directory where the HTML files that support single sign-on are stored.	_____
◆ Login Page Charset	Character encoding used to create the SSP login page. This value is sent to the browser as part of the content-type header when with the login page.	_____
◆ Login Page Media Type	Media type value sent to the browser in the content-type header with the login page. Default is text/html.	_____

To customize the SSP login page:

1. Click **Advanced** from the menu bar.
2. To create a new SSO configuration:
   a. Click **Actions>New SSO Configuration**.
   b. Type an SSO configuration name in the **Name** field.
3. To edit an existing SSO configuration:
   a. From the navigation menu, click **SSO Configurations**.
   b. Click the configuration to modify.
4. Change one or more of the following fields as necessary to update the login page:
   - Application Login Page
   - Login Directory ID
   - Login Page Charset
   - Login Page Media Type
5. Click **Save**.

6. To change the text or graphics on the login page:
   a. Open the *install_dir*\Signon directory and modify the login.html file as required.

Note: If you modify the login.html file, do not modify the following lines:

```
var ssoMsgText = "#{ssoMsgText}";
var ssoMsgTitle= "#{ssoMsgTtle}";
var ssoMsgType = "#{ssoMsgType}";
var ssoMsgOnly = "#{ssoMsgOnly}";
```

   b. Create a copy of the folder, *install_dir*\Signon directory.

Single Sign-On Field Definitions in SSP

This section provides SSP field definitions for unique dialogs and fields added to support single sign-on connections between SSP and Sterling File Gateway. For field definitions of the standard HTTP dialogs, refer to HTTP Protocol Field Definitions in the *Sterling Secure Proxy Configuration Guide*.

HTTP Adapter Definition - Properties

Use this tab to edit properties associated with how the HTTP protocol is implemented. Refer to the *Sterling Secure Proxy Configuration Guide* for an explanation of the standard fields on this dialog box. Below is an explanation of the key you define to configure single sign-on:

Field Name	Description
Key	A key to support single sign-on. Modify the following property to define the server URL: ◆ default.app.url—defines the server application URL. To support the myFilegateway application, define this key as myfilegateway.

HTTP Policy Configuration - Advanced

Use this tab to specify the user authentication to use for inbound access requests. Refer to the *Sterling Secure Proxy Configuration Guide* for an explanation of the standard fields on this dialog box. Below is an explanation of the HTTP policy fields you define to configure single sign-on:

Field Name	Description
User Authentication Type	User authentication to enable. To enable single sign-on, select Application Authentication for browser based clients and basic authentication for non-browser based clients.

Field Name	Description
Internal User ID	User ID and password used to authenticate at SFG. Four options are available. Refer to the Field Descriptions in the Configuration Guide for a description of the options used in environments other than single sign-on. To enable single sign-on, select the following option: SSO token from External Authentication—Enables single sign-on and uses a token generated by EA to connect to the SFG server.

SSO Configuration - Basic

Use this tab to define single sign-on attributes. Below is an explanation of the SSO Configuration fields you can customize to configure single sign-on:

Field Name	Description
Name	Name of the SSO configuration.
Description	Description of the SSO configuration.
Application Login Page	Name of the page that is displayed when a trading partner logs in and single sign-on is configured. Default is login.html.
Login Directory ID	Directory where the HTML files are stored. This directory is created below the installation directory. Default is Signon.
Login Page Charset	Character encoding sent as part of the content-type header to the browser with the login page. Default is UTF-8.
Login Page Media Type	Media type value sent to the browser in the content-type header with the login page. Default is text/html.

SSO Configuration - Advanced

Use this tab to define advanced single sign-on attributes. Below is an explanation of the fields you define to configure single sign-on:

Field Name	Description
Front End SSO Token Cookie Name	External URL where SSP redirects any HTTP requests, when a third-party application is used to create tokens.
External Application Login URL	External URL where SSP redirects any HTTP requests, when a third-party application is used to create the token.
Back End SSO User Header Name	HTTP header used to send the user ID to the SFG server application. Default = SM_USER.
Back End SSO Token Cookie Name	Cookie name used to send the token to SFG or the application defined in the outbound node. The default is the same as the name of the front-end cookie name.

SSO Configuration - Properties

Use this tab to define properties for a single sign-on session. Not all properties are automatically displayed. If you Below is an explanation of the Property fields you can customize:

Field Name	Description
login.form.password.field.name	Field name of the password on the single sign-on login page. Default is password.
login.form.userid.field.name	Field name of the user ID on the on the single sign-on login page. Default is user.
sso.login.command	Field name of the log in command. Default is login.
sso.logout.command	Command used in the URLS specified in security.properties_filegateway_ext file for logout. For example, the logout command in SSO_FORWARD_URL.MYFILEGATEWAY.LOGOUT= /Signon/logout) is logout. Default is logout.
sso.validation.err.command	Command used to specify validation errors in the URL specified in the security.properties_filgateway_ext file. Default is validationerror.
sso.timeout.command	Command used to specify timeout in the URLs specified in security.properties_filegateway_ext file. For example, the value is specified as timeout in the SSO_FORWARD_URL.MYFILEGATEWAY.TIMEOUT= /Signon/timeout) command. Default is timeout.
sso.req.prefix	Prefix used in the URLs specified in the security.properties_filegateway_ext file in Sterling File Gateway. For example, the prefix in SSO_FORWARD_URL.FILEGATEWAY.LOGOUT= /Signon/logout is Signon. Default is Signon.
sso.token.validation.interval	If multiple HTTP requests are made on the same TCP connection, SSP validates the token first if the interval between the last validation and the current request is more than the value specified in this property.

Single Sign-On Tokens Field Definitions in EA

This section provides EA field definitions for unique dialogs added to support single sign-on connections between SSP and Sterling File Gateway. For field definitions of the standard EA dialogs, refer to the *Sterling External Authentication Server Implementation Guide*.

Use the System Settings - SSO Tokens tab to customize single sign-on attributes in EA. A default configuration is shipped with the product. Below is an explanation of the fields you can customize:

Field Name	Description
Token Manager	To configure a token manager other than EA, select custom in the Token Manager field. Default is SEAS-SAML and uses EA to manage tokens.
Identity Provider Name	The prefix appended to generated tokens. Select Identity Provider Name and type the prefix to identify the provider. **Note:** If you change the identity provider name, any outstanding tokens are invalidated.
Token Signing Key	To generate the token signing key using a certificate alias, enable Certificate alias and type the certificate alias.
Token Expiration Period	Defines how long a token can be used before it expires. Default is 15 minutes.
Additional Properties	This field is reserved for future development.
Class name	The java class name that the EA directs every SSO token request to.