Sterling Secure Proxy

Reverse Proxy Scenarios for Single Sign-On

Version 3.4

Sterling Secure Proxy

Reverse Proxy Scenarios for Single Sign-On

Version 3.4

Note

Before using this information and the product it supports, read the information in “Notices” on page 129.

This edition applies to version 3.4 of IBM Sterling Secure Proxy and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Configure a Single Sign-on Connection to an HTTP Server

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

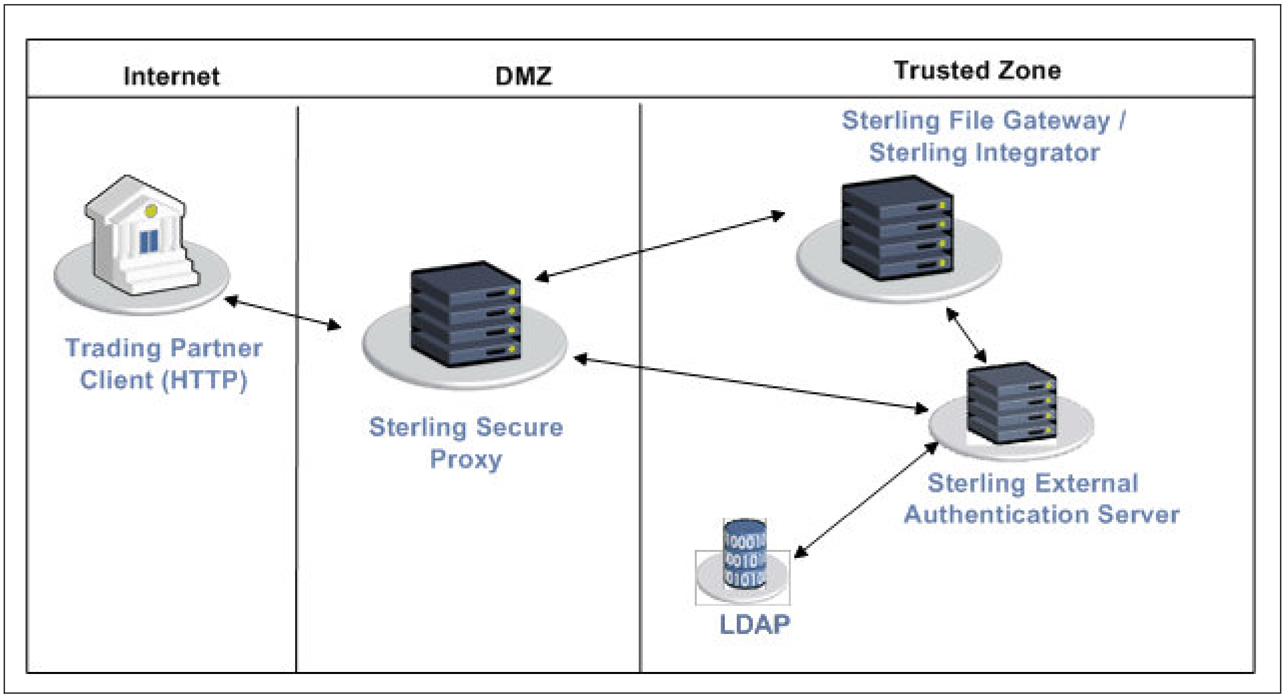
To support single sign-on, configure a Sterling Secure Proxy Login page and Sterling External Authentication Server to generate SSO tokens. Configuring SSO allows a trading partner to log on and use the same login session to connect to Sterling Secure Proxy and Sterling File Gateway. By default, Sterling External Authentication Server uses OpenSAML to create and manage SSO tokens. However, you can customize your environment to use a third-party application to generate tokens.

This topic describes how to configure the HTTP protocol in Sterling Secure Proxy between the trading partner and Sterling Secure Proxy and between Sterling Secure Proxy and Sterling File Gateway to enable authentication through Sterling External Authentication Server. It also describes how to configure Sterling External Authentication Server to issue tokens to authenticate the connection between Sterling Secure Proxy and Sterling File Gateway, without the need to log in again for this connection.

Flow of Data for Single Sign-On Configuration Between Sterling File Gateway and Sterling Secure Proxy

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 Sterling File Gateway 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, Sterling Secure Proxy, and Sterling File Gateway when Sterling External Authentication Server 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 Sterling Secure Proxy 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 Sterling Secure Proxy for authentication. You can optionally configure Sterling Secure Proxy to enforce client authentication and send the certificate to Sterling External Authentication Server for validation.
3. Sterling Secure Proxy presents a Login page to the trading partner, who provides his user ID and password. If the HTTP policy is configured to use basic authentication, Sterling Secure Proxy sends an unauthorized response and the browser displays the browser user ID/password prompt.
4. Sterling Secure Proxy sends either the user ID and password to Sterling External Authentication Server, and then validates this against information stored in LDAP.
5. If the credentials are valid, Sterling External Authentication Server creates an OpenSAML v2 token and Sterling Secure Proxy returns the a cookie associated with the token to the trading partner.
6. The trading partner sends an HTTP request to Sterling Secure Proxy and includes the cookie.
7. Sterling Secure Proxy checks for the cookie and validates the token using Sterling External Authentication Server.
8. Sterling Secure Proxy then connects to Sterling File Gateway and performs an SSL handshake. It then sends the HTTP request with the cookie from the trading partner to Sterling File Gateway.
9. Sterling File Gateway then validates the token against Sterling External Authentication Server and begins normal operation.

Configuration Considerations

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

- Only the HTTP, Sterling Connect:Direct®, FTP, and SFTP protocols support single sign-on connections.
- When Sterling Secure Proxy is configured to use SSO and the Sterling External Authentication Server user authentication profile is configured to return a mapped user ID, the mapped user ID, not the original user ID, and the SSO token are sent to the back-end system for user authentication.
- Each single sign-on user you create in Sterling File Gateway must be modified in the Sterling B2B Integrator User Accounts as an External user with the correct Authentication Host. Sterling Secure Proxy uses the specified *Authentication Host* to authenticate the user.
- The myFileGateway, FileGateway, and Sterling B2B Integrator dashboard users use application authentication in the HTTP policy.
- The Sterling B2B Integrator AS2 and WebDav users use basic authentication in the HTTP policy.
- Customize the Sterling Secure Proxy Login page-When you configure the basic scenario and select Application Authentication in the HTTP policy, you use the default Sterling Secure Proxy 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*.
- If you are using a load balancer to run multiple Sterling Secure Proxy engines, avoid login credential errors by configuring the load balancer to use persistence or "sticky connections." Refer to your load balancer documentation for details about configuring persistence.

Chapter 2. Configure the Basic Scenario to Enable a Connection to the myFileGateway Application

Procedure

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

Chapter 3. Configure Optional Features for SSO Using HTTP

Sterling Secure Proxy provides the following optional features and you can configure them as required for your environment. These features are available for SSO and non-SSO configurations. Refer to Protocol configuration information for instructions on how to configure the following features:

- Modify the HTTP connection requirement between Sterling Secure Proxy and inbound nodes by defining a specific IP address, a wildcard peer pattern, or an IP/subnet pattern
- Secure the outbound HTTP connection between Sterling Secure Proxy and Sterling File Gateway using SSL or TLS
- Authenticate an inbound certificate using Sterling External Authentication Server
- Define alternate nodes for failover support

Sterling External Authentication Server provides the ability to configure multifactor authentication. In addition to configuring client authentication in Sterling Secure Proxy, Sterling External Authentication Server can authenticate the IP address, certificate, password, and/or group access.

Chapter 4. Configure Advanced Features

Procedure

- 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 the SSO Attributes*.
- Configure Sterling B2B Integrator or Sterling File Gateway with additional pools-You use additional pools to support more than one Sterling External Authentication Server. Refer to *Configure Sterling B2B Integrator or Sterling File Gateway to use multiple Sterling External Authentication Servers*.
- Use a third-party application to configure tokens-The basic scenario uses Sterling External Authentication Server to configure and manage tokens. To use a third-party application to configure tokens, complete additional setup procedures. Refer to *Allow a Third-Party Provider to Create Tokens*.
- Configure a Single Sign-on connection to the Sterling File Gateway application-After you configure the basic SSO setup for myFileGateway, determine if internal company users require the ability to connect to the Sterling File Gateway application through Sterling Secure Proxy. Refer to *Add Single Sign-On Support for Sterling File Gateway*.
- Configure a Single Sign-on connection to other applications on Sterling B2B Integrator-This includes the Dashboard and Mailbox interfaces. Refer to *Configure Single Sign-On for Dashboard*.
- Configure a Single Sign-on connection to HTTP services on Sterling B2B Integrator that use Basic Authentication-This includes applications such as WebDAV and AS2. Refer to *Add Single Sign-On Support for Basic Authentication Applications on Sterling B2B Integrator*.
- Customize the Logon Portal-You use the default Logon Portal when you configure an HTTP adapter with Sterling Secure Proxy. To customize the Logon Portal, you can modify the Logon Portal pages and user messages, or you can configure Sterling Secure Proxy to use an external logon portal. Refer to *Customize the Logon Portal*.

Chapter 5. Basic Single Sign-On Scenario for myFileGateway

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

- Configure Sterling Secure Proxy to support basic single sign-on
- Use the default single sign-on configuration in Sterling External Authentication Server to manages OpenSAML v2 tokens
- Prepare Sterling File Gateway to support the single sign-on option
- Validate connections between the trading partner, Sterling Secure Proxy, and Sterling File Gateway

Chapter 6. Configure Sterling Secure Proxy for Basic Single Sign-On

Complete the following procedures to configure Sterling Secure Proxy for basic single sign-on:

- Create an SSO configuration.
- Create an Sterling Secure Proxy policy to support a single sign-on connection to Sterling File Gateway.
- Define a netmap to identify inbound and outbound connections.
- Define an HTTP adapter.

Chapter 7. Create an SSO Configuration

About this task

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

- Provide a value for each Sterling Secure Proxy 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.

Configuration Manager Field	Feature	Value
Name	SSO configuration file.	
Default Landing Page	Identify the Sterling File Gateway application to connect to.	/myfilegateway

To define an SSO configuration:

Procedure

1. Click **Advanced** from the menu bar.
2. Click **Actions** > **New SSO Configuration**.
3. On the **Basic** tab, type a configuration name in the **Name** field.
4. Type the fully qualified host name that the trading partner will use to connect to myFileGateway in the **Fully Qualified Host Name** field.
5. Click on the **Advanced** tab.
6. Type `/myfilegateway` in the **Default Landing Page** field.
7. If this is for an unsecure connection (HTTP, rather than HTTPS), you must uncheck the **SSO Cookie Secure Flag**.
8. Click **Save**.

Chapter 8. Create an HTTP Policy to Support a Single-Sign On Connection

About this task

To create an HTTP policy to support a single sign-on connection to Sterling File Gateway

Procedure

1. Select **Application Authentication** in the **User Authentication Type** field. The values, `Through External Authentication` and `SSO token from External Authentication`, are selected by default.
2. If the trading partner uses a non-browser client, select **Basic Authentication** in the **User Authentication Type** field. .
3. Enable **Through External Authentication** and enable **SSO token from External Authentication**.
4. Type the definition you defined in Sterling External Authentication Server in the **External Authentication Profile** field.

   For more information about configuring the HTTP policy, refer to *HTTP Reverse Proxy Configuration*.

Chapter 9. Create an HTTP Netmap to Support a Single Sign-On Connection to myFileGateway

About this task

To create an HTTP netmap to support a single sign-on connection to myFileGateway:

Procedure

1. Configure the inbound node information for your external trading partners. Select the policy defined for SSO in the preceding section.
2. Configure the outbound node information for your Sterling File Gateway server.

Chapter 10. Define the HTTP Reverse Proxy Adapter Used for the Single Sign-On Connection

About this task

To create an HTTP adapter to support a single sign-on connection to myFileGateway:

Procedure

1. Specify standardRouting for the **Routing Type** field.
2. Specify the netmap you created for the single sign-on connection to **SFG for the Netmap** field.
3. Specify the SSO configuration you created for the single sign-on connection to Sterling File Gateway for the **SSO Configuration** field.
4. Specify your Sterling External Authentication Server in the **External Authentication Server** field.

Results

For more information about configuring the HTTP policy, refer to *HTTP Reverse Proxy Configuration*.

Chapter 11. Configure Sterling External Authentication Server to Support Single Sign-On

To allow an SSO connection between a trading partner and Sterling Secure Proxy to route traffic to Sterling File Gateway, you configure OpenSAML v2.0 tokens in Sterling External Authentication Server. You can authenticate an inbound connection against information stored in an LDAP database by configuring Sterling External Authentication Server to define how the connection is authenticated. The Sterling External Authentication Server definition determines which options are enabled. Refer to the Sterling External Authentication Server documentation library for instructions on configuring an Sterling External Authentication Server definition.

The Sterling External Authentication Server generates and manages tokens. A default configuration called SEAS-SAML is enabled when you install Sterling External Authentication Server. If you use the default configuration, Sterling External Authentication Server is the identity provider, token signing keys are automatically generated, and the token expires after 15 minutes. Use the default configuration when you configure basic single sign-on. To customize Sterling External Authentication Server for single sign-on, refer to *Customize Token Definitions Created by Sterling External Authentication Server*.

Chapter 12. Prepare Sterling File Gateway to Support Single Sign-On on UNIX or Linux

About this task

Before you enable single sign-on between a trading partner and Sterling File Gateway, when using Sterling Secure Proxy, you modify the Sterling File Gateway installation. The files required to enable SSO are installed with Sterling External Authentication Server. To prepare Sterling File Gateway to support SSO on UNIX or Linux:

Procedure

1. From the Sterling External Authentication 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 Sterling File Gateway server, where *EA_install_dir* is the location of the Sterling External Authentication Server installation.

   Note: If you use FTP to copy the files to the Sterling File Gateway server, be sure to transfer the .jar files in binary mode (TYPE I).
2. On the Sterling File Gateway server, move to the *SFG_install_dir*/properties directory, where *SFG_install_dir* is the Sterling File Gateway installation directory.
3. Type the following commands to copy the SSO properties files to the Sterling File Gateway server, where *base_dir* is the location where you copied the files in step 1:

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

4. Stop Sterling File Gateway if it is running.
5. In the server.properties_seas-sso_ext file, uncomment the following line and replace <SI_install> with the actual installation path for Sterling File Gateway:

   ```
   # seas-sso=<SI_install>/properties/seas-sso/1.0/seas-sso.properties
   ```
6. In the server.properties_seas-auth_ext file, uncomment the following line and replace <SI_install> with the actual installation path for Sterling File Gateway:

   ```
   # seas-auth=<SI_install>/properties/seas-auth/1.0/seas-auth.properties
   ```
7. 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
```

8. From the *SFG_install_dir*/jar/seas-sso/1.0 directory, create a subdirectory named `private`.
9. Move to the /private directory.
10. Type the following command to copy the jar files to the /private directory on the Sterling File Gateway server:

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

Chapter 13. Modify Sterling File Gateway to Support Single Sign-On on UNIX or Linux

About this task

Before Sterling File Gateway supports single sign-on from an Sterling Secure Proxy environment, you must modify properties. Do not make changes directly to the properties files. Instead, make changes to customer_overrides.properties to prevent custom settings from being overwritten when you apply patches. The customer_overrides.properties file is not changed during upgrades or patches. If the customer_overrides.properties file is not present, you must create it. Refer to the Sterling B2B Integrator customer_overrides.properties topic for more information.

To modify Sterling File Gateway to enable single-sign on:

Procedure

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 single sign-on:
      - 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
      - security.SSO_FORWARD_URL.FILEGATEWAY.LOGOUT= /Signon/logout
      - security.SSO_FORWARD_URL.FILEGATEWAY.TIMEOUT= /Signon/timeout
      - security.SSO_FORWARD_URL.FILEGATEWAY. VALIDATION_FAILED=/ Signon/validationerror
      - security.SSO_FORWARD_URL.AFT.LOGOUT=/Signon/logout
      - security.SSO_FORWARD_URL.AFT.TIMEOUT=/Signon/timeout
      - security.SSO_FORWARD_URL.AFT.VALIDATION_FAILED=/Signon/ validationerror

   b. Add the following values to configure single sign-on for the Sterling B2B Integrator Dashboard:
      - security.SSO_FORWARD_URL.WS.LOGOUT=/Signon/logout
      - security.SSO_FORWARD_URL.DASHBOARD.LOGOUT=/Signon/logout
      - security.SSO_FORWARD_URL.WS.TIMEOUT=/Signon/timeout
      - security.SSO_FORWARD_URL.DASHBOARD.TIMEOUT=/Signon/ timeout
      - security.SSO_FORWARD_URL.WS.TIMEOUT=/Signon/timeout
      - security.SSO_FORWARD_URL.DASHBOARD.TIMEOUT=/Signon/ timeout

      Note: To access dashboard using SSO, browser must request this URI:

```
/dashoard/sso.jsp
```

Default Landing Page should also be set to

```
/dashoard/sso.jsp
```

For Dashboard/B2BConsole:

```
neo-struts-ui.url.ws.sso=http://SSPhost:port/ws/
neo-struts-ui.url.dash.sso=http://SSPhost:port/dashboard/
```

c. Add the following values to access Mailbox (MBI) using single sign-on:
   - security.SSO_FORWARD_URL.MAILBOX.LOGOUT=/Signon/logout
   - security.SSO_FORWARD_URL.MAILBOX.TIMEOUT=/Signon/timeout
   - security.SSO_FORWARD_URL.MAILBOX.VALIDATION_FAILED=/Signon/validationerror

d. Add the following values to access AFT or MyAFT using single sign-on:
   - security.SSO_FORWARD_URL.AFT.LOGOUT=/Signon/logout
   - security.SSO_FORWARD_URL.AFT.TIMEOUT=/Signon/timeout
   - security.SSO_FORWARD_URL.AFT.VALIDATION_FAILED=/Signon/validationerror
   - security.SSO_FORWARD_URL.MYAFT.LOGOUT=/Signon/logout
   - security.SSO_FORWARD_URL.MYAFT.TIMEOUT=/Signon/timeout
   - security.SSO_FORWARD_URL.MYAFT.VALIDATION_FAILED=/Signon/validationerror

e. Add the following values to access an unknown source using single sign-on:
   - security.SSO_FORWARD_URL.LOGOUT=/Signon/logout
   - security.SSO_FORWARD_URL.TIMEOUT=/Signon/timeout
   - security.SSO_FORWARD_URL.VALIDATION_FAILED=/Signon/validationerror

f. Add the following connection parameters to configure the Sterling File Gateway connection to Sterling External Authentication Server:
   - seas-sso.EA_HOST=IP address or host name of Sterling External Authentication Server
   - seas-sso.EA_PORT=listen port of Sterling External Authentication Server

     Specify the appropriate secure or clear listen port from the Sterling External Authentication Server configuration.
   - seas-sso.EA_PS_NAME=perimeter server used to connect to Sterling External Authentication Server

     Specify *local* if you do not use a perimeter server to connect to Sterling External Authentication Server.
   - seas-sso.EA_SECURE_CONNECTION=`trueorfalse`

     `true` sets connections to Sterling External Authentication Server 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. Look up the system certificate names in Sterling B2B Integrator by navigating to **Trading Partner** > **Digital Certificates** > **System**.
   - seas-sso.EA_TRUSTED_CERT[1]=name of the trusted certificate used for secure connections to Sterling External Authentication Server. Look up the

trusted certificate names in Sterling B2B Integrator by navigating to **Trading Partner** > **Digital Certificates** > **Trusted**.

If you use chained certificates and each certificate of the chain is checked in individually, you must define each of the certificates in the chain in Sterling External Authentication Server. For each certificate, define a separate value, using the seas-sso.EA_TRUSTED_CERT(#) parameter. For example, for the first certificate, configure the parameter, seas-sso.EA_TRUSTED_CERT[1]; for the second certificate, define seas-sso.EA_TRUSTED_CERT[2], until all certificates in the chain are defined in Sterling External Authentication Server. The order you configure the certificates in Sterling External Authentication Server does not have to match the definitions in Sterling B2B Integrator .

Note: Additional fields can be added if you wish to override the defaults shown below:

```
## SEAS-SSO Configuration
## HTTP cookie containing the SSO token
seas-sso.SSO_TOKEN_COOKIE=SSOTOKEN
## Maximum time to wait for making EA connections and receiving responses
seas-sso.SSO_TIMEOUT=30
seas-sso.SSO_TIMEOUT_UNITS=seconds
## Whether to keep persistent connections to EA
seas-sso.PERSISTENT_EA_CONNECTIONS=true
## Maximum number of EA connections
seas-sso.MAX_EA_CONNECTIONS=1
```

3. Save and close the file.
4. Stop and restart Sterling File Gateway to use the new values.

Chapter 14. Prepare Sterling File Gateway to Support Single Sign-On on Microsoft Windows

About this task

Before you enable single sign-on between a trading partner and Sterling File Gateway, when using Sterling Secure Proxy, you modify the Sterling File Gateway installation. The files required to enable SSO are installed with Sterling External Authentication Server. To prepare Sterling File Gateway to support SSO on Microsoft Windows:

Procedure

1. From the Sterling External Authentication Server, copy the files from the *EA_install_dir*\lib\sterling\sfg-sso-plugin directory to a location that is accessible by the Sterling File Gateway server.

   Note: If you use FTP to copy the files to the Sterling File Gateway server, be sure to transfer the .jar files in binary mode (TYPE I).
2. On the Sterling File Gateway server, move to the *SFG_install_dir*\properties directory.
3. Type the following commands to copy the SSO security.properties files *to the Sterling File Gateway 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 .
copy base_dir\sfg-sso-plugin\properties\authentication_policy.properties_seas-auth_ext.in .
copy base_dir\sfg-sso-plugin\properties\servers.properties_seas-sso_ext .
copy base_dir\sfg-sso-plugin\properties\servers.properties_seas-auth_ext .
```

4. Stop Sterling File Gateway if it is running.
5. In the server.properties_seas-sso_ext file, uncomment the following line and replace <SI_install> with the actual installation path for Sterling File Gateway:

   ```
   # seas-sso=<SI_install>\properties\seas-sso\1.0\seas-sso.properties
   ```
6. In the server.properties_seas-auth_ext file, uncomment the following line and replace <SI_install> with the actual installation path for Sterling File Gateway:

   ```
   # seas-auth=<SI_install>\properties\seas-auth\1.0\seas-auth.properties
   ```
7. From the *SFG_install_dir*\bin directory, type the following commands:

```
install3rdParty.cmd seas-sso 1.0 -j base_dir\sfg-sso-plugin\seas-sso.jar
install3rdParty.cmd seas-sso 1.0 -p base_dir\sfg-sso-plugin\properties\seas-sso.properties
install3rdParty.cmd seas-auth 1.0 -p base_dir\sfg-sso-plugin\properties\seas-auth.properties
```

8. From the *SFG_install_dir*\jar\seas-sso\1.0 directory, create a subdirectory named `private`.
9. Go to the \private directory.
10. Type the following command to copy the jar files to the Sterling File Gateway server:

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

Chapter 15. Modify Sterling File Gateway to Support Single Sign-On on Microsoft Windows

About this task

Before Sterling File Gateway is configured to support single sign-on from an Sterling Secure Proxy 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. If the customer_overrides.properties file is not present, you must create it. Refer to the Sterling B2B Integrator customer_overrides.properties topic for more information.

To modify Sterling File Gateway to enable single sign-on:

Procedure

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 single sign-on:

```
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
security.SSO_FORWARD_URL.FILEGATEWAY.LOGOUT=\Signon\logout
security.SSO_FORWARD_URL.FILEGATEWAY.TIMEOUT=\Signon\timeout
security.SSO_FORWARD_URL.FILEGATEWAY.VALIDATION_FAILED=\Signon\validationerror
security.SSO_FORWARD_URL.AFT.LOGOUT=\Signon\logout
security.SSO_FORWARD_URL.AFT.TIMEOUT=\Signon\timeout
security.SSO_FORWARD_URL.AFT.VALIDATION_FAILED=\Signon\validationerror
```

   b. Add the following values to configure single sign-on for the Sterling B2B Integrator Dashboard:
      - security.SSO_FORWARD_URL.WS.LOGOUT=\Signon\logout
      - security.SSO_FORWARD_URL.DASHBOARD.LOGOUT=\Signon\logout
      - security.SSO_FORWARD_URL.WS.TIMEOUT=\Signon\timeout
      - security.SSO_FORWARD_URL.DASHBOARD.TIMEOUT=\Signon\timeout
      - security.SSO_FORWARD_URL.WS.TIMEOUT=\Signon\timeout
      - security.SSO_FORWARD_URL.DASHBOARD.TIMEOUT=\Signon\timeout

      Note: To access dashboard using SSO, browser must request this URI:

      ```
      /dashoard/sso.jsp
      ```

      Default Landing Page should also be set to

      ```
      /dashoard/sso.jsp
      ```

      For Dashboard/B2BConsole:

      ```
      neo-struts-ui.url.ws.sso=http://SSPhost:port/ws/
      neo-struts-ui.url.dash.sso=http://SSPhost:port/dashboard/
      ```

   c. Add the following values to access Mailbox (MBI) using single sign-on:

- security.SSO_FORWARD_URL.MAILBOX.LOGOUT=\Signon\logout
- security.SSO_FORWARD_URL.MAILBOX.TIMEOUT=\Signon\timeout
- security.SSO_FORWARD_URL.MAILBOX.VALIDATION_FAILED=\Signon\validationerror

d. Add the following values to access AFT or MyAFT using single sign-on:
   - security.SSO_FORWARD_URL.AFT.LOGOUT=\Signon\logout
   - security.SSO_FORWARD_URL.AFT.TIMEOUT=\Signon\timeout
   - security.SSO_FORWARD_URL.AFT.VALIDATION_FAILED=\Signon\validationerror
   - security.SSO_FORWARD_URL.MYAFT.LOGOUT=\Signon\logout
   - security.SSO_FORWARD_URL.MYAFT.TIMEOUT=\Signon\timeout
   - security.SSO_FORWARD_URL.MYAFT.VALIDATION_FAILED=\Signon\validationerror

e. Add the following values to access an unknown source using single sign-on:
   - security.SSO_FORWARD_URL.LOGOUT=\Signon\logout
   - security.SSO_FORWARD_URL.TIMEOUT=\Signon\timeout
   - security.SSO_FORWARD_URL.VALIDATION_FAILED=\Signon\validationerror

f. Add the following connection parameters to configure the Sterling File Gateway connection to Sterling External Authentication Server:
   - seas-sso.EA_HOST=IP address or host name of Sterling External Authentication Server
   - seas-sso.EA_PORT=listen port of Sterling External Authentication Server

     Specify the appropriate secure or clear listen port from the Sterling External Authentication Server configuration.
   - seas-sso.EA_PS_NAME=perimeter server used to connect to Sterling External Authentication Server

     Specify *local* if you do not use a perimeter server to connect to Sterling External Authentication Server.
   - seas-sso.EA_SECURE_CONNECTION=`true` or `false`

     `true` sets connections to Sterling External Authentication Server 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. Look up the system certificate names in Sterling B2B Integrator by navigating to **Trading Partner** > **Digital Certificates** > **System**.
   - seas-sso.EA_TRUSTED_CERT[1]=name of the trusted certificate used for secure connections to Sterling External Authentication Server. Look up the trusted certificate names in Sterling B2B Integrator by navigating to **Trading Partner** > **Digital Certificates** > **Trusted**.

     If you use chained certificates and each certificate of the chain is checked in individually, you must define each of the certificates in the chain in Sterling External Authentication Server. For each certificate, define a separate value, using the seas-sso.EA_TRUSTED_CERT(#) parameter. For example, for the first certificate, configure the parameter, seas-sso.EA_TRUSTED_CERT[1]; for the second certificate, define seas-sso.EA_TRUSTED_CERT[2], until all certificates in the chain are defined in Sterling External Authentication Server. The order you configure the certificates in Sterling External Authentication Server does not have to match the definitions in Sterling B2B Integrator .

Note: Additional fields can be added if you wish to override the defaults shown below:

```
## SEAS-SSO Configuration
## HTTP cookie containing the SSO token
seas-sso.SSO_TOKEN_COOKIE=SSOTOKEN
## Maximum time to wait for making EA connections and receiving responses
seas-sso.SSO_TIMEOUT=30
seas-sso.SSO_TIMEOUT_UNITS=seconds
## Whether to keep persistent connections to EA
seas-sso.PERSISTENT_EA_CONNECTIONS=true
## Maximum number of EA connections
seas-sso.MAX_EA_CONNECTIONS=1
```

3. Save and close the file.
4. Stop and restart Sterling File Gateway to use the new values.

Chapter 16. Verify That Sterling File Gateway is Configured for Single Sign-On

About this task

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

Procedure

1. Start Sterling File Gateway.
2. View the authentication.log and security.log to make sure the Sterling File Gateway files are updated. If the update was successful, log files display the success messages.
   - Authentication.log file displays the following messages:

```
ALL 000000000000 GLOBAL_SCOPE SSOAuthenticationPolicy SI 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 PLUGIN: Plug-in initialized
     ```

Chapter 17. Verify the Sterling Secure Proxy Connections

About this task

To verify that the engine can receive and initiate communications sessions after configuring the basic single sign-on environment:

Procedure

Establish a connection between an HTTP client and the HTTP reverse proxy adapter to ensure that the Sterling File Gateway Login page is displayed.

Results

If you can view the Sterling File Gateway home page, you have confirmed that the connections are working. You are ready to add SSL or TLS support to the inbound connection. For more information about configuring the HTTP policy, refer to *HTTP Reverse Proxy Configuration*.

Chapter 18. Configure Advanced Features for SSO Using HTTP

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 the SSO Cookie Attributes*.
- Configure Sterling B2B Integrator or Sterling File Gateway with additional pools—You use additional pools to support more than one Sterling External Authentication Server. Refer to Configure Sterling Secure Proxy or Sterling File Gateway to use multiple Sterling External Authentication Servers.
- Use a third-party application to configure tokens—The basic scenario uses Sterling External Authentication Server to configure and manage tokens. To use a third-party application to configure tokens, complete additional setup procedures. Refer to *Allow a Third-Party Provider to Create Tokens*.
- Configure a Single Sign-on connection to the Sterling File Gateway Application—After you configure the basic SSO setup for myFileGateway, determine if internal company users require the ability to connect to the Sterling File Gateway application through Sterling Secure Proxy. Refer to Add Single Sign-On Support for Sterling File Gateway.
- Configure a Single Sign-on connection to other applications on Sterling B2B Integrator—This includes the Dashboard and Mailbox interfaces. Refer to *Configure Single Sign-On for Sterling File Gateway Dashboard*.
- Configure a Single Sign-on connection to HTTP services on Sterling B2B Integrator that use Basic Authentication—This includes applications such as WebDAV and AS2. Refer to *Add Single Sign-On Support for Basic Authentication Applications on Sterling B2B Integrator*.
- Customize the Logon Portal—You use the default Logon Portal when you configure an HTTP adapter with Sterling Secure Proxy. To customize the Logon Portal, you can modify the Logon Portal pages and user messages, or you can configure Sterling Secure Proxy to use an external logon portal. Refer to *Customize the Logon Portal*.

Chapter 19. Customize the SSO Cookie Attributes

About this task

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 header associated with a user ID, and the attributes associated with a token. Tokens can be generated with Sterling External Authentication Server or with a third-party application. This procedure assumes you are using Sterling External Authentication Server. Refer to *Allow a Third-Party Provider to Create Tokens* for instructions on configuring an external application to generate tokens.

Before you customize this page, gather the following information:

- Provide a value for each Sterling Secure Proxy 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.

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 Sterling File Gateway.	
Back End SSO User Header Name (Outbound)	The HTTP header name containing the user name that is sent to Sterling File Gateway.	
Back End SSO Token Cookie Name (Outbound)	Name to assign the cookies associated with each token. This value must match the definition in Sterling File Gateway.	

Procedure

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. To customize the front-end definitions, edit the **Front End SSO Token Cookie Name** field.
5. 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 these settings on the Sterling File Gateway and Sterling B2B Integrator system:

```
## HTTP header containing the SSO user
security.SSO_USER_HEADER=SM_USER
## SEAS-SSO Configuration
## HTTP cookie containing the SSO token
seas-sso.SSO_TOKEN_COOKI
```

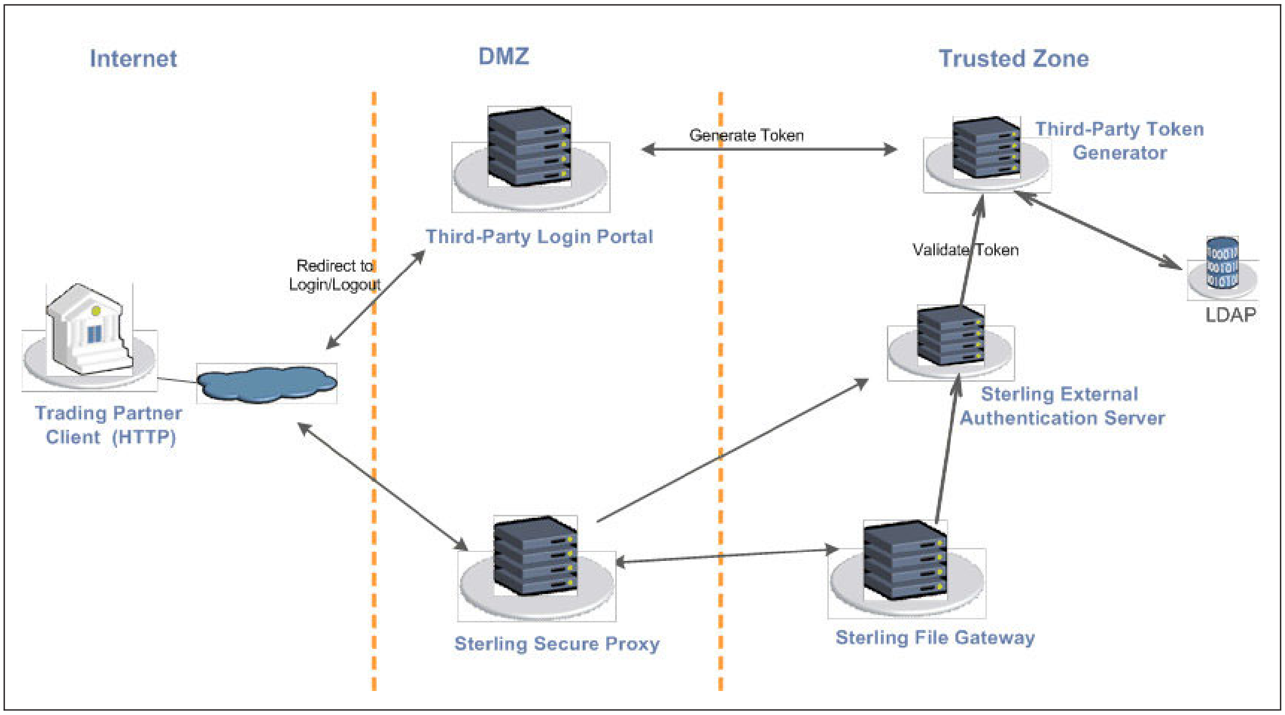
Refer to the Sterling File Gateway documentation for instructions.

6. Click **Save**.

Chapter 20. Allow a Third-Party Provider to Create Tokens

You used the default OpenSAML token generation definition when you configured the basic single sign-on definition. The default configuration uses Sterling External Authentication Server to manage tokens. To use a third-party application for token generation, you must modify the SSO Token setup in Sterling External Authentication Server.

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



Chapter 21. Configure Sterling External Authentication Server to Enable a Third-Party Provider to Create Tokens

About this task

You can configure Sterling External Authentication Server to validate a token generated by a third-party login application using a custom class. You must first verify that a custom class exists that Sterling External Authentication Server can use to verify tokens generated by the third-party application. Refer to the Sterling External Authentication Server documentation library for more information.

Before you configure Sterling External Authentication Server to enable a third-party application to create tokens, gather the following information:

- Provide a value for each Sterling Secure Proxy 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.

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 Sterling External Authentication Server and enable a third-party application to generate tokens:

Procedure

1. Log on to Sterling External Authentication Server.
2. Select **Manage** > **System Settings**.
3. From the System Settings dialog, click the **SSO Token** tab.
4. To configure a token manager other than Sterling External Authentication Server, select **Custom from the Token Manager** field.
5. Type the class name in the **Class name** field.
6. To change how long a token can be used before it expires, type a new value in the **Token Expiration Period** field.
7. Click **OK**.

Chapter 22. Customize Sterling Secure Proxy to Use a Login Portal of a Third-Party Application

About this task

You can configure Sterling Secure Proxy to redirect connections to a third-party login portal for authentication and SSO token generation. Before doing this, you should verify that a custom class exists that Sterling External Authentication Server can use to verify tokens generated by the third-party application. Before you configure Sterling Secure Proxy to enable the login page of a third-party application, gather the following information:

- Provide a value for each Sterling Secure Proxy 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.

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

To configure the SSO Configuration in Sterling Secure Proxy:

Procedure

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. Click the **Logon Portal** tab.
5. Select the **External portal** option.
6. To identify the URL of the application being used to generate tokens, type the URL in the **External Application Login URL** field.

Chapter 23. Customize Token Definitions Created by Sterling External Authentication Server

About this task

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. Refer to the Sterling External Authentication Server documentation library for more information.

Before you customize token definitions, gather the following information:

- Provide a value for each Sterling Secure Proxy 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.

Configuration Manager Field	Feature	Value
Named Identity Provider	Prefix appended to generated tokens to identify the provider. **Note:** If you change the provider name, any outstanding tokens are invalid.	
Token Signing Key	Alias of the key certificate to sign the token.	
Token Expiration Period	How long a token is valid. Default is 15 minutes.	

To customize the token configuration in Sterling External Authentication Server:

Procedure

1. Log on to Sterling External Authentication Server.
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**.

Chapter 24. Configure Sterling B2B Integrator or Sterling File Gateway to Use Multiple Sterling External Authentication Servers

About this task

If you are implementing single sign-on for HTTP with Basic Authentication, or for protocols other than HTTP, and you need to support additional Sterling External Authentication Servers, add the following parameters for each additional Sterling External Authentication Server pool configuration to the customer_overrides.properties file located in the *install_dir*\properties directory.

Note: The Sterling File Gateway and myFileGateway applications always use the default SSO_POOL Sterling External Authentication Server connection to validate SSO tokens, regardless of which Authentication Host is selected for the user. Additional Sterling External Authentication Server connection pools may only be used for HTTP Basic Auth applications, FTP, SFTP, and Sterling Connect:Direct.

- authentication_policy.authentication_n.className= com.sterlingcommerce.seas.gis.sso.plugin.SeasAuthentication
- authentication_policy.authentication_n.display_name = name to be used on the Sterling B2B Integrator/Sterling File Gateway user administration UI. Use something different than the default Sterling External Authentication Server Server Authentication, which is used by the default SSO_POOL. This is the Authentication Host name that is selected when you configure external User Accounts to use this pool.
- authentication_policy.authentication_n.enabled=true
- seas-auth.authentication_n.profile = userAuth
- seas-auth.authentication_n.ea_pool=unique name for your pool other than the default SSO_POOL, which shares the Sterling External Authentication Server connection pool with the Sterling File Gateway SSO configuration

  Note: Change the "n" in the above example to a number greater than 1 to avoid overwriting the default SSO_POOL, which is shared with the FileGateway and myFileGateway SSO configuration. Also, make sure you avoid using a number already in use for LDAP authentication. Define a unique number for each entry.

To use another connection pool instead of the default SSO_POOL, configure the Sterling External Authentication Server connection of the pool with the following parameters, where *pool* is the pool name defined in the preceding section:

- seas-auth.*pool*.EA_HOST=IP address or host name of Sterling External Authentication Server
- seas-auth.*pool*.EA_PORT=listen port of Sterling External Authentication Server
- seas-auth.*pool*.EA_PS_NAME=perimeter server used to connect to Sterling External Authentication Server
- seas-auth.*pool*.EA_SECURE_CONNECTION=enables a secure Sterling External Authentication Server
- *true* sets connections to Sterling External Authentication Server as secure and *false* sets the connection as clear. If this parameter is true, you must also define the Sterling External Authentication Server_SYSTEM_CERT and Sterling External Authentication Server_TRUSTED_CERT[1].

- seas-auth.*pool*.EA_SYSTEM_CERT=name of the system certificate in the system certificate store, if the connection is secure
- seas-auth.*pool*.EA_TRUSTED_CERT[1]=name of the trusted certificate used by Sterling External Authentication Server for secure connections
- seas-auth.*pool*.TIMEOUT=maximum time to wait for making Sterling External Authentication Server connections and receiving responses
- seas-auth.*pool*.TIMEOUT_UNITS=unit of time to use, minutes or seconds, for seas-auth.*pool*.TIMEOUT parameter
- seas-auth.*pool*.PERSISTENT_EA_CONNECTIONS=whether to keep persistent connections to Sterling External Authentication Server

  true sets connections to Sterling External Authentication Server as persistent and *false* sets the connections as not persistent.
- seas-auth.*pool*.MAX_EA_CONNECTIONS=maximum number of Sterling External Authentication Server connections

Note: Additional fields can be added if you wish to override the defaults shown below:

```
## SEAS-SSO Configuration
## HTTP cookie containing the SSO token
seas-sso.SSO_TOKEN_COOKIE=SSOTOKEN
## Maximum time to wait for making Sterling External Authentication
Server connections and receiving responses
seas-sso.SSO_TIMEOUT=30
seas-sso.SSO_TIMEOUT_UNITS=seconds
## Whether to keep persistent connections to Sterling External Authentication
Server
seas-sso.PERSISTENT_EA_CONNECTIONS=true
## Maximum number of Sterling External Authentication
Server connections
seas-sso.MAX_EA_CONNECTIONS=1
```

All of the primary Sterling External Authentication Server connection properties on the SSO plug-in can be prefixed by "ALT_" and suffixed by ".<n>" to specify alternate Sterling External Authentication Servers.

These are the connection properties for the primary Sterling External Authentication Server:

- EA_HOST=IP address or host name of Sterling External Authentication Server (required)
- EA_PORT=port of Sterling External Authentication Server (default = 61365)
- EA_PS_NAME=name of perimeter server to connect to Sterling External Authentication Server (default = local)
- EA_SECURE_CONNECTION=whether connection to Sterling External Authentication Server is secure: true/false (default = false)
- EA_CIPHER_SUITE[1]=cipher suite #1, if secure connection (defaulted if not specified)
- EA_CIPHER_SUITE[2]=cipher suite #2, if secure connection (defaulted if not specified)
- ::
- EA_CIPHER_SUITE[n]=cipher suite #n, if secure connection (defaulted if not specified)
- EA_SYSTEM_CERT=name of system certificate for secure connection to Sterling External Authentication Server (default = OpsKey)

- EA_TRUSTED_CERT[1]=name of trusted certificate used by Sterling External Authentication Server for secure connections (required if secure connection; either the public certificate of the Sterling External Authentication Server, or the CA root that issued Sterling External Authentication Server's certificate)
- EA_TRUSTED_CERT[2]=name of trusted certificate used by Sterling External Authentication Server for secure connections (optional; intermediate certificate in Sterling External Authentication Server's certificate chain)
- ::
- EA_TRUSTED_CERT[n]=name of trusted certificate used by Sterling External Authentication Server for secure connections (optional; intermediate certificate in Sterling External Authentication Server's certificate chain)

The suffix ".<n>" indicates the alternate order, starting with 1. There is no limit to the number of alternates.

For example, if you have two alternate Sterling External Authentication Servers, configure the following properties:

```
# Alternate Sterling External Authentication Server #1
ALT_EA_HOST.1 = <address of alternate Sterling External Authentication Server #1>
ALT_EA_PORT.1 = <port of alternate Sterling External Authentication Server #1>
ALT_EA_PS_NAME.1 = <perimeter server for alternate Sterling External Authentication Server #1>
ALT_EA_SECURE_CONNECTION.1 = true
ALT_EA_CIPHER_SUITE[1].1 = TLS_RSA_WITH_AES_128_CBC_SHA
ALT_EA_CIPHER_SUITE[2].1 = TLS_RSA_WITH_AES_256_CBC_SHA
ALT_EA_CIPHER_SUITE[3].1 = TLS_RSA_WITH_3DES_EDE_CBC_SHA
ALT_EA_SYSTEM_CERT.1 = <system certificate for alternate Sterling External Authentication Server #1>
ALT_EA_TRUSTED_CERT.1 = <trusted certificate for alternate Sterling External Authentication Server #1>

# Alternate Sterling External Authentication Server #2
ALT_EA_HOST.2 = <address of alternate Sterling External Authentication Server #2>
ALT_EA_PORT.2 = <port of alternate Sterling External Authentication Server #2>
ALT_EA_PS_NAME.2 = <perimeter server for alternate Sterling External Authentication Server #2>
ALT_EA_SECURE_CONNECTION.2 = true
ALT_EA_CIPHER_SUITE[1].2 = TLS_RSA_WITH_AES_128_CBC_SHA
ALT_EA_CIPHER_SUITE[2].2 = TLS_RSA_WITH_AES_256_CBC_SHA
ALT_EA_CIPHER_SUITE[3].2 = TLS_RSA_WITH_3DES_EDE_CBC_SHA
ALT_EA_SYSTEM_CERT.2 = <system certificate for alternate Sterling External Authentication Server #2>
ALT_EA_TRUSTED_CERT.2 = <trusted certificate for alternate Sterling External Authentication Server #2>
```

If you are using customer.overrides.properties, prefix the properties with "seas-sso." or with "seas-auth.<*pool_name*>.", depending on whether you are configuring the Sterling External Authentication Server SSO plug-in or authenticator.

Chapter 25. Configure Single Sign-On for Sterling File Gateway

After you configure single sign-on for myFileGateway, determine if internal company users require access to Sterling File Gateway through Sterling Secure Proxy.

Complete the following procedures to configure Sterling Secure Proxy for basic single sign-on for Sterling File Gateway:

- *Create an SSO Configuration for Sterling File Gateway*
- *Create an HTTP Policy to Support SSO for Sterling File Gateway*
- *Define the HTTP Netmap for Sterling File Gateway*
- *Configure HTML Rewrite*
- *Configure an HTTP Adapter for Sterling File Gateway*
- *Create User Accounts in Sterling File Gateway*
- *Verify the Sterling Secure Proxy Connections*

Chapter 26. Create an SSO Configuration for Sterling File Gateway

About this task

To configure SSO for internal users:

Procedure

1. Make a copy of the myFileGateway SSO configuration.
2. Rename the copy to identify the configuration as a Sterling File Gateway definition.
3. Change the field called **Default Landing Page** to connect to /filegateway. Refer to *Create an SSO Configuration* for more information.

Results

Note: You can also use the included Welcome Page, which includes links to Sterling File Gateway and myFileGateway and can be customized to include other applications.

Chapter 27. Create an HTTP Policy to Support SSO for Sterling File Gateway

About this task

To create an HTTP policy to support a single sign-on connection to Sterling File Gateway:

Procedure

1. Select Application Authentication in the User Authentication Type field. The values, `Through External Authentication` and `SSO token from External Authentication`, are selected by default.
2. Type the definition you defined in Sterling External Authentication Server in the **External Authentication Profile** field.

   For more information about configuring the HTTP policy, refer to *HTTP Reverse Proxy Configuration*.

Chapter 28. Define the HTTP Netmap for Sterling File Gateway

Procedure

1. Make a copy of the myFileGateway HTTP netmap.
2. Rename the copy to identify the configuration as a Sterling File Gateway definition.
3. Configure the inbound node definitions for the nodes that need to connect to Sterling File Gateway. Configure the outbound node definition to support the connection to Sterling File Gateway.
4. Change the values as needed. Refer to *Create an HTTP Netmap to Support a Single Sign-On Connection to myFileGateway* for more information.

Chapter 29. Configure HTML Rewrite for SSO

About this task

HTML rewriting allows you to replace the URL links returned by an HTTP server to the Sterling Secure Proxy server by configuring how the URL links from the server will be mapped to the URL links in Sterling Secure Proxy. If the HTTP server has web pages with links to other web pages, you must map the URL connections in order for the links to work. You must configure HTML rewrite in order for the Sterling File Gateway application to function correctly.

Certain pages on the dashboard use javascript to create URL dynamically using a back-end host name literal. To change this host name to the proxy host name, you add another entry to the HTML rewrite. Use the third entry in the table below as an example.

Note: HTML rewrite may not work for arbitrary javascripts that dynamically create URL at the client side.

To configure this environment, use the following table to help you identify the rewrite values to define in the netmap definition:

- Provide a value for each Sterling Secure Proxy 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.

Server URL	**Proxy URL**
http(s)://*<fully qualified DNS name for the SFG_host>*:*<port>*	http(s)://*<fully qualified DNS name for the proxy_host>*:*<adapter1_port>*
http(s)://*<SFG_ipaddress>*:*<port>*	http(s)://*<proxy_ipaddress>*:*<port>*
http(s)://*<fully qualified DNS name for the SFG_host>*	http(s)://*<fully qualified DNS name for the proxy_host>*
<fully qualified DNS name for the SI_host>	*<fully qualified DNS name for the proxy host>*

To configure HTML rewrite:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the netmap definition you created.
3. On the HTTP Netmap Nodes panel, click the **HTML Rewrite** tab.
4. Click **New**.
5. Enable the **Support HTML Rewrite** field.
6. Type the URL path for the outbound server in the **Server URL** field.
7. Type the URL path for the proxy in the **Proxy URL** field.
8. Click **Save**.
9. Repeat steps 4 through 8 for all HTML Rewrite options you want to configure.
10. To reorder the HTML rewrite definitions:

   a. Click the radio button beside the URL routing definition to reorder.
   b. Click **Move Up** or **Move Down** until the item is in the correct order.
11. Click **Save**.
12. Test the configuration to ensure that single sign-on and HTML rewrite to the Sterling File Gateway server is configured correctly.

Chapter 30. Configure an HTTP Adapter for Sterling File Gateway

Procedure

1. Make a copy of the myFileGateway HTTP adapter.
2. Rename the copy to identify the configuration as a Sterling File Gateway configuration.
3. Enable Support HTML Rewrite.
4. Specify the SSO configuration and HTTP netmap configurations you created for Sterling File Gateway. Refer to *Define the HTTP Reverse Proxy Adapter Used for the Single Sign-On Connection* for more information.

Chapter 31. Create User Accounts in Sterling File Gateway

About this task

User accounts work with permissions to provide security for your organization. These features make it possible to regulate which users have access to each module in Sterling File Gateway and what functions each user can perform. To create a user account:

Procedure

1. From Sterling File Gateway, select **Tools** > **B2B Console**.
2. From within Sterling File Gateway, select **Accounts** > **User Accounts** > **Create a new Account**.
3. Complete the steps in the wizard. Supply the following information about the user:
   - **Authentication type (external)**
   - **User ID**
   - **Password** (For the default user policy, the password must be six characters or more and contain at least two of the following characters: (number, capital letter, !, @, #, $, %, ^, &, *)
   - **Confirm Password**
   - **Policy (Default User Policy)**
   - **SSH Authorized User Key**
   - **Session Timeout (in minutes)**
   - **Accessibility (Dashboard UI)**
   - **Dashboard Theme (Default)**
4. Select one or more of the following groups to assign the user to, based on their job responsibilities:
   - **Sterling File Gateway Integration Architects**
   - **Sterling File Gateway Operators**
   - **Sterling File Gateway Route Provisioners**
   - **Sterling File Gateway System Administrators**

   Note: Do not assign the myFileGateway user to the trading partner group. Otherwise, the user will not be able to login to the Sterling File Gateway application.

   Note: For full Sterling File Gateway functionality, each of these groups must have at least one user. By default, the following users are created during installation: fg_sysadmin, fg_architect, fg_provisioner, and fg_operator. One user can belong to multiple groups.

   Note: To create the equivalent of fg_sysadmin, assign all the Sterling File Gateway groups listed above and the Sterling B2B Integrator Admin group to the user.
5. Supply the following information for the user:
   - **Given Name**
   - **Surname**

- **E-mail**
- **Pager**
- **Preferred Language (English, Japanese)**
- **Manager ID**
- **Identity**

6. Review and confirm the user to create the new user account.

Chapter 32. Verify That Sterling File Gateway is Configured for Single Sign-On

About this task

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

Procedure

1. Start Sterling File Gateway.
2. View the authentication.log and security.log to make sure the Sterling File Gateway files are updated. If the update was successful, log files display the success messages.
   - Authentication.log file displays the following messages:

```
ALL 000000000000 GLOBAL_SCOPE SSOAuthenticationPolicy SI 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 PLUGIN: Plug-in initialized
     ```

Chapter 33. Configure Single Sign-On for Sterling B2B Integrator Dashboard

After you configure single sign-on for myFileGateway, determine if internal company users require access to Sterling B2B Integrator dashboard through Sterling Secure Proxy.

Complete the following procedures to configure Sterling Secure Proxy for basic single sign-on for dashboard:

- *Create an SSO Configuration for Sterling B2B Integrator Dashboard*
- Create an *HTTP Policy to Support SSO for Sterling B2B Integrator Dashboard*
- *Define the HTTP Netmap for Sterling B2B Integrator Dashboard*
- *Configure HTML Rewrite for Sterling B2B Integrator Dashboard*
- *Configure an HTTP Adapter for Sterling B2B Integrator Dashboar*d
- *Create User Accounts in Sterling B2B Integrator*
- *Verify the Sterling Secure Proxy Connections*

Chapter 34. Create an SSO Configuration for Sterling B2B Integrator Dashboard

About this task

To configure SSO for dashboard users:

Procedure

1. Make a copy of the myFileGateway SSO configuration.
2. Rename the copy to identify the configuration as a Sterling B2B Integrator dashboard definition.
3. Change the field called **Default Landing Page** to connect to /dashboard/sso.jsp. Refer to *Create an SSO Configuration* for more information.

Results

Note: You can also select the Welcome Page as the Default Landing Page when you configure the SSO configuration.

Chapter 35. Create an HTTP Policy to Support SSO for Sterling B2B Integrator Dashboard

About this task

To create an HTTP policy to support a single sign-on connection to Sterling B2B Integrator Dashboard:

Procedure

1. Select **Application Authentication** in the **User Authentication Type** field. The values, `Through External Authentication` and `SSO token from External Authentication`, are selected by default.
2. Type the definition you defined in Sterling External Authentication Server in the **External Authentication Profile** field.

   For more information about configuring the HTTP policy, refer to *HTTP Reverse Proxy Configuration*.

Chapter 36. Define the HTTP Netmap for Sterling B2B Integrator Dashboard

Procedure

1. Make a copy of the myFileGateway HTTP netmap.
2. Rename the copy to identify the configuration as a Sterling B2B Integrator dashboard definition.
3. Configure the inbound node definitions for the nodes that need to connect to dashboard. Configure the outbound node definition to support the connection to dashboard.
4. Change the values as needed. Refer to *Create an HTTP Netmap to Support a Single Sign-On Connection to myFileGateway* for more information.

Chapter 37. Configure HTML Rewrite for Sterling B2B Integrator Dashboard

About this task

HTML rewriting allows you to replace the URL links that refer to the Sterling B2B Integrator server in the HTML pages returned by the HTTP server with the links pointing to Sterling Secure Proxy. When the user clicks on these links, the HTTP requests come back to Sterling Secure Proxy. You must configure HTML rewrite in order for the dashboard application to function correctly.

Certain pages on the dashboard use javascript to create URL dynamically using a back-end host name literal. To change this host name to the proxy host name, you add another entry to the HTML rewrite. Use the fourth entry in the table below as an example.

Note: HTML rewrite may not work for arbitrary javascripts that dynamically create URL at the client side.

To configure this environment, use the following table to help you identify the rewrite values to define in the netmap definition:

- Provide a value for each Sterling Secure Proxy 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.

Server URL	Proxy URL
http(s)://*<fully qualified DNS name for the SI_host>*:*<port>*	http(s)://*<fully qualified DNS name for the proxy_host>*:*<adapter1_port>*
http(s)://*<SI_ipaddress>*:*<port>*	http(s)://*<fully qualified DNS name for the proxy_host>*:*<adapter1_port>*
http(s)://*<fully qualified DNS name for the SI_host>*:	http(s)://*<fully qualified DNS name for the proxy_host>*:
http(s)://*<fully qualified DNS name for the SI_host>*	http(s)://*<fully qualified DNS name for the proxy_host>*
<fully qualified DNS name for the SI_host>	*<fully qualified DNS name for the proxy host>*

Note: Ensure that the Destination Address field in the outbound node has the fully qualified DNS name of the Sterling B2B Integrator host. If not, the URLs in the HTML pages that reference the Sterling B2B Integrator host will not match the host URL entered for the HTML rewrite.

To configure HTML rewrite:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the netmap definition you created.
3. On the HTTP Netmap Nodes panel, click the **HTML Rewrite** tab.

4. Click **New**.
5. Enable the **Support HTML Rewrite** field.
6. Type the URL path for the outbound server in the **Server URL** field.
7. Type the URL path for the proxy in the **Proxy URL** field.
8. Click **Save**.
9. Repeat steps 4 through 8 for all HTML Rewrite options you want to configure.
10. To reorder the HTML rewrite definitions:
    a. Click the radio button beside the URL routing definition to reorder.
    b. Click **Move Up** or **Move Down** until the item is in the correct order.
11. Click **Save**.

Chapter 38. Configure an HTTP Adapter for Sterling B2B Integrator Dashboard

Procedure

1. Make a copy of the myFileGateway HTTP adapter.
2. Rename the copy to identify the configuration as a Sterling B2B Integrator dashboard configuration.
3. Enable Support HTML Rewrite.
4. Specify the SSO configuration and HTTP netmap configurations you created for dashboard. Refer to *Define the HTTP Reverse Proxy Adapter Used for the Single Sign-On Connection* for more information.

Chapter 39. Create User Accounts in Sterling B2B Integrator

About this task

User accounts work with permissions to provide security for your organization. These features make it possible to regulate which users have access to each module in Sterling B2B Integrator and what functions each user can perform. To create a user account:

Procedure

1. Select **Accounts** > **User Accounts** > **Create a new Account**.
2. Complete the steps in the wizard. Supply the following information about the user:
   - **Authentication type (external)**
   - **User ID**
   - **Authentication Host—**Select a host that corresponds to the seas_auth.authentication-*n* configuration maintained in the customer_overrides.properties file described in the previous section.
   - **Password** (For the default user policy, the password must be six characters or more and contain at least two of the following characters. (number, capital letter, !, @, #, $, %, ^, &, *)
   - **Confirm Password**
   - **Policy (Default User Policy)**
   - **SSH Authorized User Key**
   - **Session Timeout** (in minutes)
   - **Accessibility (Dashboard UI)—**This adds the user to the Dashboard Users group.
   - **Dashboard Theme** (Default)
3. Select one or more groups to assign the user to, based on their job responsibilities.
4. Supply the following information for the user:
   - **Given Name**
   - **Surname**
   - **E-mail**
   - **Pager**
   - **Preferred Language (English, Japanese)**
   - **Manager ID**
   - **Identity**
5. Review and confirm the user to create the new user account.

Chapter 40. Verify the Sterling Secure Proxy Connections

About this task

To verify that the engine can receive and initiate communications sessions after configuring the basic single sign-on environment:

Procedure

1. Establish a connection between an HTTP client and the HTTP reverse proxy adapter to ensure that the Sterling Secure Proxy Login page is displayed.
2. If you can view the dashboard home page, you have confirmed that the connections are working. If the Default Landing Page in your SSO configuration is the Welcome page, you will see a Welcome page with links to back-end applications, such as myFileGateway and the dashboard. Click on the dashboard link to see the dashboard home page and confirm that the connections are working. You can change the Default Landing Page to /dashboard/sso.jsp to skip the Welcome page and go right to the dashboard.

Results

You are ready to add SSL or TLS support to the inbound connection. For more information, refer to *HTTP Reverse Proxy Configuration*.

Chapter 41. Create an HTTP Policy to Support a Single-Sign On Connection

About this task

To create an HTTP policy to support a single sign-on connection to a basic authentication application:

Procedure

1. Select Basic Authentication in the User Authentication Type field. Enable **Through External Authentication** and enable **SSO token from External Authentication**.
2. Type the definition you defined in Sterling External Authentication Server in the **External Authentication Profile** field.

   For more information about configuring the HTTP policy, refer to *HTTP Reverse Proxy Configuration*.

Chapter 42. Add Single Sign-On Support for Basic Authentication Applications on Sterling B2B Integrator

After you configure single sign-on for myFileGateway, determine if users require access to Sterling B2B Integrator applications that use basic authentication, such as AS2 or WebDAV.

Complete the following procedures to configure Sterling Secure Proxy for basic single sign-on for basic authentication applications on Sterling B2B Integrator.

- *Create an SSO Configuration for a Basic Authentication Application*
- *Create an HTTP Policy to Support a Single-Sign On Connection*
- *Define the HTTP Netmap for a Basic Authentication Application*
- *Configure an HTTP Adapter for a Basic Authentication Application*
- *Create Basic Authentication Application User Accounts in Sterling B2B Integrator*
- *Verify the Sterling Secure Proxy Connections*

Chapter 43. Create an SSO Configuration for a Basic Authentication Application

Procedure

1. To configure SSO for basic authentication application users, make a copy of the myFileGateway SSO configuration.
2. Rename the copy to identify the configuration as a definition for the application, such as AS2.
3. Change the field called **Default Landing Page** to connect to the application, such as /as2. Refer to *Create an SSO Configuration* for more information.

Chapter 44. Define the HTTP Netmap for a Basic Authentication Application

Procedure

1. Make a copy of the myFileGateway HTTP netmap.
2. Rename the copy to identify the configuration as a definition for the application, such as AS2. Configure the inbound node definitions for the nodes that need to connect to the application.
3. Configure the outbound node definition to support the connection to the application.
4. Change the values as needed. Refer to *Create an HTTP Netmap to Support a Single Sign-On Connection to myFileGateway* for more information.

   Usually, applications that use basic authentication, such as AS2 and WebDAV, do not require HTML rewrite.

Chapter 45. Configure an HTTP Adapter for a Basic Authentication Application

Procedure

1. Make a copy of the myFileGateway HTTP adapter.
2. Rename the copy to identify the configuration as a basic authentication application configuration, such as AS2 or WebDAV.
3. Specify the SSO configuration and HTTP netmap configurations you created for the application. Refer to *Define the HTTP Reverse Proxy Adapter Used for the Single Sign-On Connection* for more information.

Chapter 46. Create Basic Authentication Application User Accounts in Sterling B2B Integrator

User accounts work with permissions to provide security for your organization. These features make it possible to regulate which users have access to each module in Sterling B2B Integrator and what functions each user can perform. For more information, refer to *Create User Accounts in Sterling B2B Integrator.*

Chapter 47. Verify the Sterling Secure Proxy Connections

About this task

To verify that the engine can receive and initiate communications sessions after configuring the basic single sign-on environment:

Procedure

1. Establish a connection between an HTTP client and the HTTP reverse proxy adapter to ensure that the browser user ID/password prompt is displayed.
2. For applications that use basic authentication, the Default Landing Page is the back-end application URL. If the Default Landing Page in your SSO configuration is the Welcome page, you will see a Welcome page with links to back-end applications, such as myFileGateway, AS2, and WebDAV. Click on the application link to see the application home page and confirm that the connections are working. You can change the Default Landing Page to the URI of the application, such as /as2, to skip the Welcome page and go right to the application.

Results

You are ready to add SSL or TLS support to the inbound connection. For more information about configuring the HTTP policy, refer to *HTTP Reverse Proxy Configuration*.

Chapter 48. Customize the Logon Portal

Sterling Secure Proxy provides a self-service Logon Portal that allows Sterling File Gateway users to manage and change their passwords. The Logon Portal is separately licensed and includes verification of the new password, password expiration notification, display of password policy, and welcome and logon screens. You can also configure Sterling Secure Proxy to use an external logon portal.

To support the Logon Portal, configure the HTTP protocol in Sterling Secure Proxy for SSO.

This topic describes how to configure the Sterling Secure Proxy Logon Portal for the HTTP protocol.

Before you complete the Logon Portal configuration, be aware of the following considerations:

- Sterling Secure Proxy SSO must be properly configured before you can use the change password functionality of the Logon Portal.
- Configure Active Directory or LDAP to allow the trading partner to change his password.
- Comments are included in the default Logon Portal .html pages to simplify editing. Remove all of these comments after you edit the pages to minimize security risks.

Chapter 49. Common User Tasks Managed by the Logon Portal

You can configure the Logon Portal to skip the Welcome page. You cannot configure the sequence of any other Logon Portal pages presented to the user. The following Logon Portal workflows are described below:

- *Workflow When the User Initiates a Password Change*
- *Workflow When a User Password is Expired or Must Change*
- *Workflow When the User Provides Invalid Logon Credentials*
- *Workflow When a User Account is Locked*
- *Workflow When the User Cannot Change Password*

Workflow When the User Initiates a Password Change

In this scenario, the trading partner decides to change his password.

When a user connects to Sterling File Gateway, Sterling Secure Proxy presents a Login page. The user provides user credentials. If the credentials are valid, a Welcome page is displayed. The user can change his password or continue to the HTTP application. If the user selects Change Password, he can view the password policy or change his password.

To change a password, the user must follow the restrictions defined in the password policy. However, the user will not be locked out of Sterling Secure Proxy if he does not define a valid new password.

Note: The setting to allow the trading partner to change his password is in the Sterling External Authentication Server group profile. This profile is specified in the HTTP policy configuration.

Workflow When a User Password is Expired or Must Change

In this scenario, the trading partner's password has expired or must be changed.

When a user connects to Sterling File Gateway, Sterling Secure Proxy presents a Login page. The user provides user credentials. If the credentials are valid, a Change Password page is displayed and a user message is presented indicating that the password is expired or must be changed. The user can change his password or view the password policy. If the user successfully changes his password, a Welcome page is displayed. If the user fails to successfully change his password, a Change Password page is displayed with an error message.

Note: The setting to allow the trading partner to change his password is in the Sterling External Authentication Server group profile. This profile is specified in the HTTP policy configuration.

Workflow When the User Provides Invalid Logon Credentials

In this scenario, the trading partner enters an invalid user ID or password.

When a user connects to Sterling File Gateway, Sterling Secure Proxy presents a Login page. The user provides invalid user credentials. A Login page is displayed with a customizable error message.

Workflow When a User Account is Locked

In this scenario, the trading partner enters a valid user ID and password, but the account is locked.

When a user connects to Sterling File Gateway, Sterling Secure Proxy presents a Login page. The user provides user credentials for a locked account. A Login page is displayed with a customizable error message.

Workflow When the User Cannot Change Password

In this scenario, the trading partner enters a valid user ID and password, but the user is not allowed to change the password.

When a user connects to Sterling File Gateway, Sterling Secure Proxy presents a Login page. The user provides user credentials for an account that is not allowed to change the password. A Login page is displayed with a customizable error message.

Note: The setting to allow the trading partner to change his password is in the Sterling External Authentication Server group profile. This profile is specified in the HTTP policy configuration.

Chapter 50. Configuration Considerations for Logon Portal

- Sterling Secure Proxy SSO must be properly configured before you can use the change password functionality of the Logon Portal.
- Configure Active Directory or LDAP to allow the trading partner to change his password.
- Comments are included in the default Logon Portal .html pages to simplify editing. Remove all of these comments after you edit the pages to minimize security risks.

Chapter 51. Organization of Logon Portal Customization Scenarios

When you first configure Sterling Secure Proxy for HTTP, you use the default Login page, Welcome page, Change Password Page, Logout page, and Password Policy Page.

This document provides instructions on how to customize an Sterling Secure Proxy Logon Portal.

- *Customize the Login Page*
- *Customize the Welcome Page*
- *Configure Sterling Secure Proxy to Skip the Welcome Page*
- *Customize the Change Password Page*
- *Customize the Logout Page*
- *Customize Password Policy Page*
- *Customize User Messages*
- *Configure the Forgot Your User ID or Password Page*
- *Configure Sterling Secure Proxy to Use External Logon Portal*

Chapter 52. Customize the Login Page

About this task

The default Login page is a simple page with no logo information and prompts the user to provide a user ID and password. The default page also contains a link if the user forgets his user ID or password.

You can customize the Login page to define how you want the page to look and what information to include on the page. You customize this page by modifying the labels or replacing the entire page.

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

- Provide a value for each Sterling Secure Proxy 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.

Configuration Manager Field	Feature	Value
Name	Name to assign to the Sterling Secure Proxy configuration	
Sterling Secure Proxy Internal Portal		
• Login Page	Custom page to display for the Sterling Secure Proxy single sign-on login.	
• Login Directory Name	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 Sterling Secure Proxy Login page. This value is sent to the browser as part of the content-type header 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 Sterling Secure Proxy Login page:

Procedure

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. On the **Logon Portal** tab, select **SSP Internal Portal**.
5. Change one or more of the following fields to customize the Login page:

- **Login Page**
- **Login Directory Name**
- **Login Page Charset**
- **Login Page Media Type**

6. Click **Save**.
7. If you want to change the text or graphics on the Login page, 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="#{ssoMsgTitle}";
   var ssoMsgType="#{ssoMsgType}";
   var ssoMsgOnly="#{ssoMsgOnly}";
   ```
8. If you modify the login .html file, create a copy of the \install_dir\\Signon directory.

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

Chapter 53. Customize the Welcome Page

About this task

The default Welcome page is a simple page with no logo information that provides links to the Logout page and the Change Password page. The default page does not include links to back-end applications.

You can customize the Welcome page to define how you want the page to look and what information to include on the page. You customize this page by modifying the labels or replacing the entire page.

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

- Provide a value for each Sterling Secure Proxy 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.

Configuration Manager Field	Feature	Value
Name	Name to assign to the Sterling Secure Proxy configuration	
Sterling Secure Proxy Internal Portal		
• Welcome Page	Custom page to display for the Sterling Secure Proxy single sign-on welcome.	
• Login Directory Name	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 Sterling Secure Proxy Login page. This value is sent to the browser as part of the content-type header 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 Sterling Secure Proxy Welcome page:

Procedure

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. On the **Logon Portal** tab, select **SSP Internal Portal**.
5. Change one or more of the following fields to customize the Login page:

- **Welcome Page**
- **Login Directory Name**
- **Login Page Charset**
- **Login Page Media Type**

6. Click **Save**.
7. If you want to change the text or graphics on the Welcome page, open the \install_dir\\signon directory and modify the welcome .html file as required.

   Add the URLs for back-end applications in the welcome.html as required.

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

   ```
   var ssoMsgText="#{ssoMsgText}";
   var ssoMsgTitle="#{ssoMsgTitle}";
   var ssoMsgType="#{ssoMsgType}";
   var ssoMsgOnly="#{ssoMsgOnly}";
   ```
8. If you modify the welcome .html file, create a copy of the \install_dir\\Signon directory.

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

Chapter 54. Configure Sterling Secure Proxy to Skip the Welcome Page

About this task

You can configure Sterling Secure Proxy so that a user is directed to the back-end application instead of the Welcome page after logging in. You can configure this behavior by modifying the SSO configuration.

To configure Sterling Secure Proxy to skip the Welcome page:

Procedure

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. On the **Advanced** tab, type the URL for the back-end application in the **Default Application URL** field. You can use the relative URL, such as /myfilegateway, or full URL.
5. Click **Save**.

Chapter 55. Customize the Change Password Page for HTTP SSO

About this task

The default Change Password page is a simple page with no logo information that prompts the user to provide his user ID, existing password, and new password. The default page provides a link to the Password Policy page.

You can customize the Change Password page to define how you want the page to look and what information to include on the page. You customize this page by modifying the labels or replacing the entire page.

Before you modify the Change Password page, gather the following information:

- Provide a value for each Sterling Secure Proxy 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.

Configuration Manager Field	Feature	Value
Name	Name to assign to the Sterling Secure Proxy configuration	
Sterling Secure Proxy Internal Portal		
• Change Password Page	Custom page to display for the Sterling Secure Proxy single sign-on Change Password page.	
• Login Directory Name	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 Sterling Secure Proxy Login page. This value is sent to the browser as part of the content-type header 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 Sterling Secure Proxy Change Password page:

Procedure

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. On the **Logon Portal** tab, select **SSP Internal Portal**.
5. Change one or more of the following fields to customize the Change Password page:
   - **Change Password Page**
   - **Login Directory Name**
   - **Login Page Charset**
   - **Login Page Media Type**
6. Click **Save**.
7. If you want to change the text or graphics on the Change Password page, open the \install_dir\\signon directory and modify the change password .html file as required.

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

   ```
   var ssoMsgText="#{ssoMsgText}";
   var ssoMsgTitle="#{ssoMsgTitle}";
   var ssoMsgType="#{ssoMsgType}";
   var ssoMsgOnly="#{ssoMsgOnly}";
   ```
8. If you modify the change password .html file, create a copy of the \install_dir\\Signon directory.

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

Chapter 56. Customize the Logout Page

About this task

The default Logout page is a simple page with no logo information. You can configure Sterling Secure Proxy to use the Login page in place of the Logout page.

You can customize the Logout page to define how you want the page to look and what information to include on the page. You customize this page by modifying the labels or replacing the entire page.

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

- Provide a value for each Sterling Secure Proxy 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.

Configuration Manager Field	Feature	Value
Name	Name to assign to the Sterling Secure Proxy configuration	
Sterling Secure Proxy Internal Portal		
• Logout Page	Custom page to display for the Sterling Secure Proxy single sign-on Logout page. If you want to use the Login page as the Logout page, specify the Login page here.	
• Login Directory Name	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 Sterling Secure Proxy Login page. This value is sent to the browser as part of the content-type header 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 Sterling Secure Proxy Logout page:

Procedure

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. On the **Logon Portal** tab, select **SSP Internal Portal**.

5. Change one or more of the following fields to customize the Logout page:
   - **Logout Password Page**
   - **Login Directory Name**
   - **Login Page Charset**
   - **Login Page Media Type**
6. Click **Save**.
7. If you want to change the text or graphics on the Logout page, open the \install_dir\signon directory and modify the logout .html file as required.

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

   ```
   var ssoMsgText="#{ssoMsgText}";
   ```

   ```
   var
   ssoMsgTitle="#{ssoMsgTitle}";
   ```

   ```
   var ssoMsgType="#{ssoMsgType}";
   ```

   ```
   var
   ssoMsgOnly="#{ssoMsgOnly}";
   ```
8. If you modify the logout .html file, create a copy of the *install_dir*\Signon directory.

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

Chapter 57. Customize Password Policy Page

The Password Policy page is a simple page with no logo information that displays the password policy.

Sterling Secure Proxy obtains the password policy dynamically from Active Directory or IBM Tivoli using Sterling External Authentication Server. If you update the password policy, the Password Policy page displays the new password policy.

Chapter 58. Customize User Messages

About this task

You can customize user messages that display on the Logon Portal pages. You customize these messages by modifying the messageBundle.properties file, located in the Signon/resources directory.

By default, messages are associated with specific events. For example, if a logon attempt fails because the user password has expired, the logon page displays a message alerting the user that the password has expired. For security reasons, you might use the same general error message for all logon failures.

To customize user messages:

Procedure

1. From the *SSP_install_dir*\Signon\resources directory, open the messageBundle.properties file in a text editor.
2. Modify the message text for all user messages you want to customize.
3. Save the messageBundle.properties file.
4. Restart Sterling Secure Proxy.

Chapter 59. Configure the Forgot Your User ID or Password Page

About this task

You can configure the Forgot Your User ID or Password page to display a customized user message. You customize this user message by editing the Login page .html file.

Procedure

1. To customize the Forgot Your User ID or Password page, 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="#{ssoMsgTitle}";
   var ssoMsgType="#{ssoMsgType}";
   var ssoMsgOnly="#{ssoMsgOnly}";
   ```
2. If you modify the logout .html file, create a copy of the \install_dir\\Signon directory.

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

Chapter 60. Configure Sterling Secure Proxy to Use External Logon Portal

About this task

You can configure Sterling Secure Proxy to use an external logon portal.

Before you configure an external logon portal, gather the following information:

- Provide a value for each Sterling Secure Proxy 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.

Configuration Manager Field	Feature	Value
Name	Name to assign to the Sterling Secure Proxy configuration	
External Portal • External Application Login URL	URL of external login portal.	

To configure Sterling Secure Proxy to use the external logon portal:

Procedure

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. On the **Logon Portal** tab, select **External Portal**.
5. Type the URL of the external login portal in the **External Application Login URL** field.
6. Click **Save**.

Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2012. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2012.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce™, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Printed in USA