Sterling Secure Proxy

Sterling Connect:Direct Proxy Single Sign-on Configuration

Version 34

Sterling Secure Proxy

Sterling Connect:Direct Proxy Single Sign-on Configuration

Version 34

Note
Before using this information and the product it supports, read the information in "Notices" on page 27.

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

Sterling Secure Proxy can be used as a proxy with Sterling B2B Integrator and Sterling File Gateway and supports a single sign-on connection for Sterling Connect:Direct® connections. Single sign-on (SSO) bypasses the normal user authentication process in Sterling B2B Integrator and instead trusts that Sterling Secure Proxy has authenticated the user.

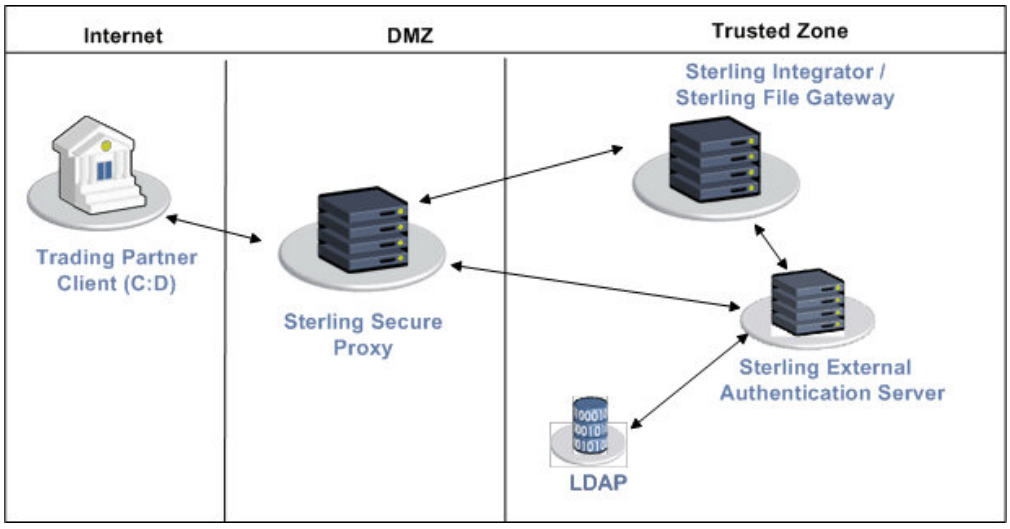
To support single sign-on, configure Sterling External Authentication Server to generate SSO tokens. Configuring SSO allows a trading partner to log on and use the same login session to connect to Sterling Secure Proxy and Sterling B2B Integrator. By default, Sterling External Authentication Server uses 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 Sterling Connect:Direct protocol in Sterling Secure Proxy between the trading partner and Sterling Secure Proxy and between Sterling Secure Proxy and Sterling B2B Integrator to enable authentication through Sterling External Authentication Server. It describes how to configure Sterling External Authentication Server to issue tokens to authenticate the connection between Sterling Secure Proxy and Sterling B2B Integrator. It also describes how to configure a self-service Change Password Portal for external trading partners.

Flow of Data for Single Sign-On Configuration Between Sterling B2B Integrator 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 B2B Integrator 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 B2B Integrator when Sterling External Authentication Server is used to generate and manage tokens:

1. The trading partner requests a connection to Sterling B2B Integrator.
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 sends an authentication request to the trading partner, who provides his user ID and password.
4. Sterling Secure Proxy sends the user ID and password to Sterling External Authentication Server and then validates it against information stored in LDAP.
5. If the credentials are valid, Sterling External Authentication Server creates an OpenSAML v2 token and returns the token to Sterling Secure Proxy.
6. Sterling Secure Proxy connects to Sterling B2B Integrator and performs an SSL handshake. Sterling Secure Proxy then sends the request with the token from Sterling External Authentication Server to Sterling B2B Integrator.
7. Sterling B2B Integrator 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.
- The Sterling Secure Proxy Change Password Portal requires an HTTP adapter, which is an optional, licensed component of Sterling Secure Proxy, and a license for the Change Password Portal. Refer to Configure Change Password Portal instructions to configure this feature.
- 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.

Organization of Single Sign-On Scenarios

The scenarios describe how to configure single sign-on between Sterling Secure Proxy and trading partners and between Sterling Secure Proxy and Sterling B2B Integrator.

Chapter 2. Configure the Basic Scenario to Enable a Connection to Sterling B2B Integrator

About this task

Configure the basic scenario to allow you to quickly become operational using single sign-on to connect to a Sterling Connect:Direct Server Adapter in Sterling B2B Integrator. After you complete this scenario, test the connection to ensure that you have correctly configured it. You then have a basic configuration and can begin operation.

Chapter 3. Configure Advanced Features

About this task

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

- 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, you complete additional setup procedures. Refer to *Allow a Third-Party Provider to Create Tokens for Sterling Connect:Direct*.
- Customize the OpenSAML v2 tokens-You use the default token generation definition when you configure the basic single sign-on definition. To customize the token definition, you can modify the named identity provider, the token signing key, or how long a token can be used before it expires. Refer to *Customize Token Definitions Created by Sterling External Authentication Server for Sterling Connect:Direct*.
- Configure Sterling B2B Integrator or Sterling File Gateway with additional pools-You use additional pools to support more than one Sterling External Authentication Server server. *Refer to Configure Sterling B2B Integrator or Sterling File Gateway to use multiple Sterling External Authentication Server servers for Sterling Connect:Direct*.

Chapter 4. Configure Optional Features

Sterling Secure Proxy provides optional security features and you can configure them as required for your environment.

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 also authenticate the IP address, certificate, password, and/or group access. Refer to the Sterling External Authentication Server documentation library for instructions.

Sterling Secure Proxy provides a Change Password Portal that allows trading partners to manage their own passwords. This feature requires the HTTP adapter, which is an optional, licensed component of Sterling Secure Proxy. Refer to *Configure Change Password Portal for Sterling Connect:Direct* for instructions on how to configure this feature.

Worksheets

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

- 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.

Chapter 5. Basic Single Sign-on Scenario

Complete the following tasks to define a Sterling Connect:Direct configuration between a trading partner and Sterling Secure Proxy and between Sterling Secure Proxy and Sterling B2B Integrator to support a single sign-on connection to a Sterling Connect:Direct Server Adapter:

- Configure Sterling Secure Proxy to support basic single sign-on.
- Use the default single sign-on configuration in Sterling External Authentication Server to manage OpenSAML v2 tokens.
- Prepare Sterling B2B Integrator to support the single sign-on option.
- Validate the connections between the trading partner, Sterling Secure Proxy, and Sterling B2B Integrator.

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 a Sterling Connect:Direct policy to support a single sign-on connection to Sterling B2B Integrator.
- Define a Sterling Connect:Direct netmap to identify inbound and outbound connections.
- Define a Sterling Connect:Direct adapter.

Chapter 7. Configure Sterling External Authentication Server to Support Single Sign-On

About this task

To allow an SSO connection between a trading partner and Sterling Secure Proxy to route traffic to Sterling B2B Integrator, 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 Sterling External Authentication Server Server documentation library for instructions on configuring an Sterling External Authentication Server definition.

The Sterling External Authentication Server 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 for Sterling Connect:Direct*.

Chapter 8. Prepare Sterling B2B Integrator to Support Single Sign-On

Before you enable single sign-on between a trading partner and Sterling B2B Integrator, when using Sterling Secure Proxy, you modify the Sterling B2B Integrator installation. The files required to enable SSO are installed with Sterling External Authentication Server.

Modify Sterling B2B Integrator to Support Single Sign-On

About this task

Before Sterling B2B Integrator 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 B2B Integrator 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.
3. Add the following parameters to configure the connection to Sterling External Authentication Server:
   - `seas-sso.EA_HOST`=IP address or host name of Sterling External Authentication Server server
   - `seas-sso.EA_PORT`=listen port of Sterling External Authentication Server server

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

4. Save and close the file.
5. Stop and restart Sterling B2B Integrator to use the new values.

Change Sterling B2B Integrator User Accounts Single Sign-On

About this task

After you install and configure the SSO plug-in and restart Sterling B2B Integrator, the Sterling B2B Integrator User Accounts page presents additional choices for Authentication Type. To enable SSO for a user account, select an authentication method of External and then select the appropriate Sterling External Authentication Server server for Authentication Host. The default is SEAS Authentication. Additional choices are available only if you define other Sterling External Authentication Server Connection pools in addition to the default SSO_POOL.

Verify the Sterling Secure Proxy Connections for Sterling Connect:Direct SSO

About this task

After you configure the basic single sign-on environment, to verify that the engine can receive and initiate communications sessions, establish a connection between a Sterling Connect:Direct server and the Sterling Connect:Direct Proxy adapter.

Note: Configuration files must be available on the engine for communication sessions to be established.

This procedure enables you to verify that the engine can:

- Establish a Sterling Connect:Direct session initiated by a trading partner using a Sterling Connect:Direct server
- Initiate an outbound session to an Sterling B2B Integrator Sterling Connect:Direct Server Adapter on behalf of the Sterling Connect:Direct server connection

To verify the communications sessions:

Procedure

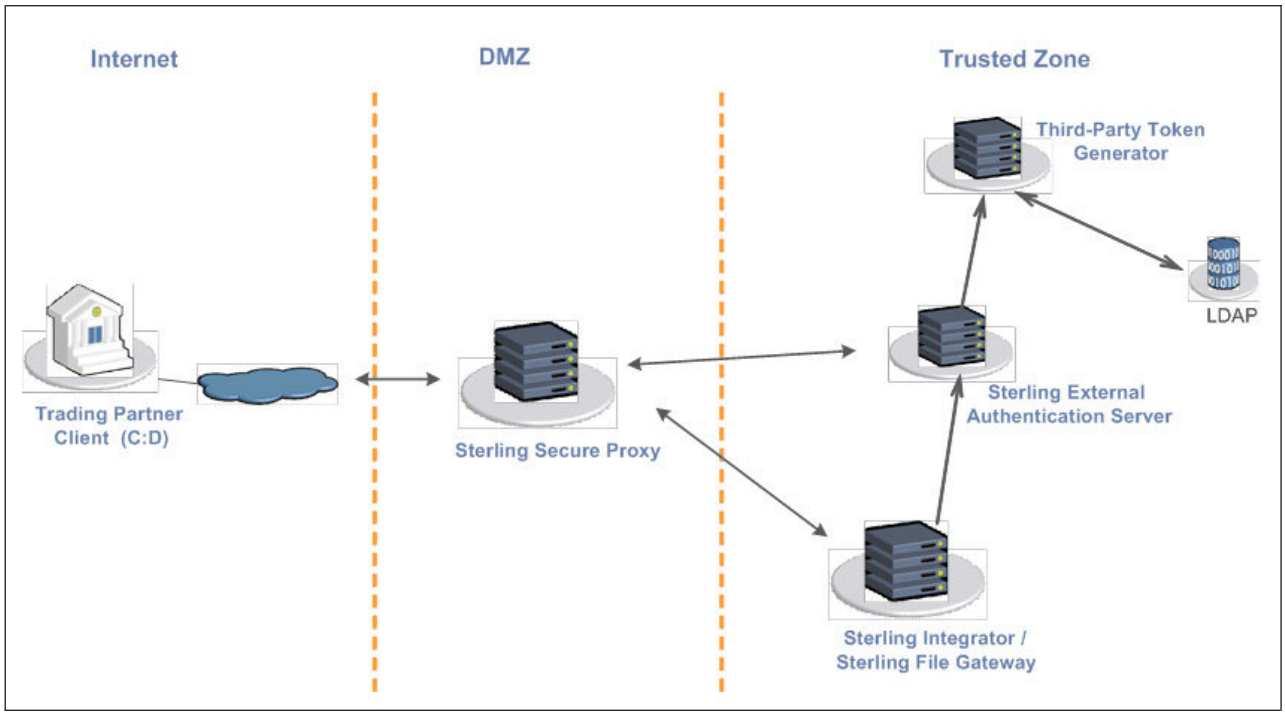
1. Make sure the engine is running.
2. Submit a Sterling Connect:Direct Process where the SNODE is the Sterling Connect:Direct Proxy adapter. The SNODE ID and password must match the user ID and password stored in LDAP and the user ID must be defined in Sterling B2B Integrator as an external user with the correct Authentication Host.
3. View the Sterling Connect:Direct server statistics to verify the Sterling Connect:Direct session.

Chapter 9. Allow a Third-Party Provider to Create Tokens

About this task

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.



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

About this task

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

Configuration Manager Field	Feature	Value
Token Manager	The application that creates the tokens.	Custom

Configuration Manager Field	Feature	Value
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 10. 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.

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	The prefix appended to generated tokens to identify the provider. **Note:** If you change the identity provider name, any outstanding tokens are invalid.	
Token Signing Key	Alias of the key certificate used to sign the token.	
Token Expiration Period	How long a token is valid. 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 11. 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 Server 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 server
- seas-auth.*pool*.EA_PORT=listen port of Sterling External Authentication Server 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 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.

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