IBM Sterling Secure Proxy

Field Definitions Guide

Version 3.3

Copyright

This edition applies to the 3.3 version of IBM Sterling Secure Proxy and to all subsequent releases and modifications until otherwise indicated in new editions.

Before using this information and the product it supports, read the information in *Notices* on page 87.

Licensed Materials - Property of IBM
IBM Sterling Secure Proxy
© Copyright IBM Corp. 2005, 2010. All Rights Reserved.
US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Sterling Secure Proxy Field Definitions 5

Engines Field Definitions 6
  SSP Engine Configuration - Basic 6
  SSP Engine Configuration - Advanced 6
Connect:Direct Protocol Field Definitions 7
  Connect:Direct Adapter Configuration - Basic 7
  Connect:Direct Adapter Configuration - Advanced 9
  Connect:Direct Adapter Definition - Properties 10
  Connect:Direct Netmap Definition. 10
  Connect:Direct Netmap Node Definition - Basic 11
  Connect:Direct Netmap Node Definition - Security 11
  Connect:Direct Netmap Node Definition - Advanced 13
Connect:Direct Policy Definition 14
  Connect:Direct Policy Configuration - Basic 14
  Connect:Direct Policy Configuration - Advanced 15
  Connect:Direct Policy Definition - Step Permissions. 16
FTP Protocol Field Definitions 16
  FTP Adapter Definition - Basic 16
  FTP Adapter Definition - Advanced. 17
  FTP Adapter Definition - Custom 18
  FTP Adapter Definition - Properties 18
  FTP Netmap Definition 20
  FTP Netmap Inbound Node Definition - Basic 20
  FTP Netmap Inbound Node Definition - Security 21
  FTP Netmap Inbound Node Definition- Advanced 23
  FTP Netmap Outbound Node Definition - Basic 23
  FTP Outbound Node Definition - Security. 24
  FTP Netmap Outbound Node Definition - Advanced 25
  FTP Policy Configuration - Basic 26
  FTP Policy Configuration - Advanced 26
HTTP Protocol Field Definitions. 27
  HTTP Adapter Configuration - Basic. 27
  HTTP Adapter Definition - Advanced 29
  HTTP Adapter Definition - Properties 30
  HTTP Netmap Definition 31
  HTTP Policy Configuration 38
SFTP Protocol Field Definitions. 40

- SFTP Adapter Configuration - Basic 40
- SFTP Adapter Configuration - Security 41
- SFTP Adapter Configuration - Advanced 42
- SFTP Adapter Definition - Properties 43
- SFTP Netmap Definition 44
- SFTP Policy Configuration - Basic 49
- SFTP Policy Configuration - Advanced 50

Monitoring Field Definitions 51
- Engine Status (All) 51
- Engine Detail 52

Credentials Field Definitions 52
- Trusted Certificate Store Configuration 52
- Trusted Certificate Configuration 53
- System Certificate Store Configuration 53
- System Certificate Configuration. 54
- Authorized User Key Store Configuration 55
- Authorized User Key Configuration 55
- Known Host Key Store Configuration 55
- Known Host Key Configuration 56
- Local User Key Store Configuration 56
- Local User Key Configuration 57
- Local Host Key Store Configuration 57
- Local Host Key Configuration 58
- User Store Configuration. 58

Advanced Menu Field Definitions 60
- Perimeter Servers Field Definitions. 60
- EA Server Configuration Field Definitions 64
- Connect:Direct Step Injection Configuration 66
- Password Policy Field Definitions 68

Single Sign-On Definitions. 69
- SSO Configuration - Basic 69
- SSO Configuration - Advanced 69
- SSO Configuration - Logon Portal. 69
- SSO Configuration - Properties. 70

System Menu Field Definitions 71
- CM Trusted Certificate Store Configuration 71
- CM Trusted Certificate Configuration 72
- CM System Certificate Store Configuration 72
- CM System Certificate Configuration 72
- CM User Configuration 73
- System Settings - Listeners 73
- System Settings - Security 74
- System Settings - Globals 74
- System Settings - Lock Manager 75

Single Sign-On Tokens Field Definitions in EA 76
- System Settings - SSO Tokens. 77

PeSIT Field Definitions 77
- PeSIT Adapter Configuration - Basic 77
- PeSIT Adapter Configuration - Advanced 78
- PeSIT Adapter Definition - Properties 80
- PeSIT Netmap Definition. 80
- PeSIT Netmap Node Definition - Basic 80

PeSIT Netmap Node Definition - Security 81
PeSIT Netmap Node Definition - Advanced 82
PeSIT Policy Configuration - Basic 84
PeSIT Policy Configuration - Advanced 84
PeSIT Policy Configuration - Transfer Direction 85

Notices **87**

Sterling Secure Proxy Field Definitions

This document provides screen-by-screen definitions and usage for each field in Sterling Secure Proxy. Use this document to:

- Look up a field by name using the Find function (Edit>Find or Ctrl+F).
- Look up a set of fields by screen / functionality using the bookmarks on the left.

For additional information, return to the main page of the
Sterling Secure Proxy Documentation Library.

Engines Field Definitions

Following are the field definitions for the engine screens. For more information, refer to the Manage SSP engines on the Sterling Secure Proxy Documentation Library.

SSP Engine Configuration - Basic

The SSP engine resides in the DMZ and runs the proxy adapters that handle client communication requests to servers in your trusted zone. Use this screen to specify basic information to configure an engine. You must obtain the engine host name and port from installation. Refer to the field definitions in the following table:

Field Name	Description
Engine Name	Engine Name identifies the name to assign the engine. It can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help identify the engine. Description can be up to 255 characters.
Engine Host	Engine Host is the host or IP address where the engine is running. Valid values are 1 to 255 alphanumeric characters. Special characters allowed are underscore (_), dash (-), colon (:), and period (.).
Engine Listen Port	Engine listen port is the port on which the engine listens for configuration information from CM. Valid values are 1–65535.

SSP Engine Configuration - Advanced

Use this screen to change advanced information about an engine, including logging for the engine, level of logging for the local perimeter server, and whether to use a user store other than the default. Refer to the field definitions in the following table. For more information, refer to Manage SSP engines on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Engine Logging	Engine Logging identifies the level of logging to write to the engine log file. Logging options include: ◆ ERROR writes only error messages to the log. ERROR is the default value. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to by Sterling Commerce Support.

Field Name	Description
Local Perimeter Server Logging Level	Level of logging to write to the local perimeter server log. Logging options include: ◆ ERROR writes only error messages to the log. ERROR is the default value. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to by Sterling Commerce Support.
Certicom Logging Level	Certicom Logging Level identifies the level of logging to write to the certicom log. Logging options include: ◆ ERROR writes only error messages to the log. ERROR is the default value. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to by Sterling Commerce Support.
User Store	User Store identifies the user store to use with this engine. It is the location where users who access the engine are defined. defUserStore is the default user store.

Connect:Direct Protocol Field Definitions

Following are the field definitions for the Connect:Direct protocol screens. For more information, see Connect:Direct proxy configuration on the Sterling Secure Proxy Documentation Library.

Connect:Direct Adapter Configuration - Basic

Use this screen to specify system-level communications information for Connect:Direct connections to and from SSP. Before you can click the Advanced or Properties tabs, you must specify Adapter Name and Listen Port and select a netmap to associate with the adapter.

Connect:Direct basic adapter fields are defined in the following table:

Field Name	Description
Name	Name identifies the name to assign to the adapter you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the adapter you create. Description can be up to 255 characters.
Type	Type identifies the protocol being used: Connect:Direct.

Field Name	**Description**
Listen Port	Listen Port identifies the port number to use to listen for inbound connections. Valid values include 1-65535.
Netmap	Netmap identifies the name of the netmap to associate with the adapter you are defining. If the netmap has not been created, click ⊕ to add the netmap.
Routing Type	Select the Routing Type to identify how inbound connections are routed to the server in the trusted zone. Routing options include: ◆ Standard— select Standard to direct connections to the outbound node specified in the SNODE Netmap Entry field. ◆ Certificate-based—select this option to use the certificate presented by the inbound PNODE to determine which outbound SNODE to connect to. Certificate-based routing uses External Authentication and requires that you configure a External Authentication server. ◆ PNODE-specified—select this option to route outbound connections based on information provided by the inbound PNODE. ◆ PNODE-specified, then Standard—select this option to route outbound connections based first on information provided by the inbound PNODE. If no routing information is presented by the PNODE, the connection is routed to the outbound node specified in the SNODE Netmap Entry field.
SNODE Netmap Entry	SNODE Netmap Entry identifies the name of the Connect:Direct server where the node connections are routed, after connecting to Sterling Secure Proxy. Select this value from a pull-down list.
Engine	Engine identifies the SSP server in the DMZ where traffic is first routed before being sent to the outbound secure Connect:Direct server. Select an engine from the list. You must define an engine before you can create an adapter.
Startup Mode	Startup Mode identifies how the adapter is started. **auto** starts the adapter as soon as it is pushed to the engine. **manual** requires that the adapter be manually started.

Connect:Direct Adapter Configuration - Advanced

Use this screen to specify additional communications information, and to specify the perimeter servers to use for this adapter.

Connect:Direct advanced adapter Configuration fields are defined in the following table.

Field Name	Description
Logging Level	Logging Level identifies the level of logging to write to the log file for the adapter. Logging options include: ◆ ERROR writes only error messages to the log. ERROR is the default value. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Maximum Sessions	Maximum Sessions identifies the maximum number of concurrent sessions that the adapter allows. Default=20.
Session Timeout	Session Timeout identifies the amount of time allowed, in seconds, between transmissions of TCP packets before a session is terminated. Default =90 seconds.
Http Ping Response	Http Ping Response identifies the response sent when an HTTP GET is received on the listen port. Provide this value to send a health check response to a third-party IP load balancer, such as Big IP. To test the response, ping the URL and port of the engine. For example if you configure an adapter on port 13640 and you want to get an HTTP 1.0 response, send a ping to http://ProxyServerURL:13640/. The value you supplied in the Http Ping Response field is returned. If you provide a value in this field, the value is displayed in a browser window. You can provide HTML syntax and text values.
Outbound Port Range	Outbound Port Range identifies the range of ports to use for the adapter. Valid values include a list of ports that are allowed with each value separated by a comma such as 1234, 2340, 16570 or a range of ports allowed, such as 16570 -17950.
External Authentication Server	External Authentication Server identifies the server to use. Select the server from the pull-down list. You must define an Sterling External Authentication Server before you can select the server from the list.
Perimeter Server Mapping - Inbound Perimeter Server	Select the perimeter server for the inbound connection in the Perimeter Server Mapping - Inbound Perimeter Server field. To use a remote perimeter server, you must define the server before you associate it with an inbound connection.
Perimeter Server Mapping - Outbound Perimeter Server	Select the perimeter server to use for the outbound connection in the Perimeter Server Mapping - Outbound Perimeter Server field. To use a remote perimeter server, you must define it before you can associate it with an outbound connection.
Perimeter Server Mapping - External Authentication Perimeter Server	Select the perimeter server to use for the EA connection in the Perimeter Server Mapping - External Authentication Perimeter Server field. To use a remote perimeter server, you must define it before you can associate it with an Sterling Secure Proxy connection.

Field Name	Description
Inbound and outbound sessions can have different levels of encryption	Inbound and outbound sessions can have different levels of encryption. This field allows the connections from the PNODE to SSP and from SSP to the SNODE to use different encryption methods. Set this option to enable a secure connection on the inbound session but use a nonsecure connection on the outbound session, or to use different protocols on the inbound and the outbound connection."

Connect:Direct Adapter Definition - Properties

Use this screen to edit properties associated with how the Connect:Direct protocol is implemented. Not all keys are not displayed. To change a default key value, type the key value and assign a value.

Property	Description
◆ failover.detection.enabled	Enables failover detection. Valid value=true | false. Default=false.
◆ failover.detection.mode	Determines the failover detection mode. ◆ continuous—Continuously polls the outbound node and EA server. continuous=default setting. ◆ Standard only—Polls the outbound node and EA server when a connection fails. Outbound and EA perimeter servers are always continuously polled regardless of this setting.
◆ failover.poll.interval	How many seconds between failover polling. Default=5.
◆ failover.ea.ping.profile	EA profile to use to extend the EA server healthcheck to the backend LDAP server.
◆ failover.debug	Enables debug logging for failover. Valid values are true | false. Default=false.
◆ load.balancer.addr	IP address of the load balancer. Define this property to suppress health check connections logging made by the load balancer.

Connect:Direct Netmap Definition

Use this screen to define the Connect:Direct netmap and all nodes allowed to connect through SSP. Connect:Direct netmap fields are defined in the following table.

Field Name	Description
Netmap Name	Netmap Name identifies the name to assign to the netmap you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).

Field Name	Description
Description	Description up to 255 characters to help identify the netmap you create.
Type	Protocol being used: HTTP, FTP, SFTP, or Connect:Direct.
Filter	Filter allows you to view a subset of available nodes. Use the wildcard characters, * and ?, to identify the nodes to display. Filters are case-sensitive. For example, the filter n* will display node1 but will not display Node1.

Connect:Direct Netmap Node Definition - Basic

Use this screen to define the minimum connection parameters for a Connect:Direct node. Define a node name, address, and port before you save the node definition. Connect:Direct netmap node basic fields are defined in the following table.

Field Name	Description
Node Name	Name of the node server you are configuring in Connect:Direct proxy. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Routing Name	Value used to select this SNODE as the outbound node during certificate-based routing. It must match the routing name returned by EA. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_). Set this field only if you are configuring certificate-based routing in EA.
Description	Assigns a description up to 255 characters to identify the node you create.
Connect:Direct Server Address	IP address or host name of the Connect:Direct server. Valid values are 1-200 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), colon (:), and underscore (_).
Connect:Direct Server Port	Port number of the Connect:Direct server. Valid values are 1-65535.
Policy	Policy you want to associate with the node you are creating. If a policy with the security attributes required has not been created, click ⊕ .
Step Injection	Function to associate with the node you are defining. If a step injection policy with the attributes required has not been created, click ⊕ .

Connect:Direct Netmap Node Definition - Security

Use this screen to define secure connection requirements for the node.

Field Name	Description
Use secure+	Enable Use secure+ to turn on the use of SSL/TLS to provide secure communications with transport protocols and to ensure that data is secured as it is transmitted across a single socket.

Field Name	Description
Verify Common Name	Enable Verify Common Name if your security environment requires that the common name in the certificate presented be verified. If you enable Verify Common Name, you must provide Certificate Common Name.
Certificate Common Name	Certificate Common Name identifies the common name value to validate. If the common name in the certificate does not match the value defined in this field, the session fails.
Enable Client Authentication	Enable Client Authentication on the inbound node connection to require that the SSP server authenticate the certificate presented by the inbound node connection.
Security Setting	Security Setting identifies the security protocol allowed for connections to this node. Options include: ◆ SSL - select this option to require SSL for the connection. ◆ TLS - select this option to require TLS for the connection. ◆ The PNODE host controls SSL Protocol - select this option to use the protocol specified at the PNODE.
Trust Store	Location where trusted CA certificates are stored. CA certificates verify that a certificate received from a server is signed by a trusted source.
CA Certificates/Trusted Root	CA Certificates/Trusted Root identifies the trusted certificate to use to authenticate the certificate presented by the client. You select a CA certificate or trusted root from the list of certificates stored in the trust store you selected in the Trust Store field. When a client presents a certificate to establish a secure connection, the trusted root certificate, located at the server, must match or be the entity who signed the certificate presented by the client during the SSL handshake.
Key Store	Key Store identifies the location where the keys and system certificates you want to use are stored.
Key/System Certificate	Certificate presented by SSP to the node to authenticate itself during the SSL handshake. Select the certificate to use for the node from the list that contains the key or system certificates stored in the key store selected in the Key Store field.
Available Cipher Suites	Available Cipher Suites is the list of ciphers that can be enabled to encrypt data transmitted during a secure SSL or TLS connection between Sterling Secure Proxy and a Connect:Direct node. Enable at least one cipher. To enable a cipher, highlight it and click Add. To enable multiple ciphers, highlight the ciphers to enable and click Add.
Selected Cipher Suites	Selected Cipher Suites identifies the ciphers you have enabled to encrypt data during a secure SSL or TLS connection. Ciphers are negotiated based on their location in the Selected Ciphers list. To reorder a cipher in the list, highlight it and click Up or Down.

Connect:Direct Netmap Node Definition - Advanced

Use this screen to change the logging level for a Connect:Direct node definition and the TCP timeout value to wait for a response as well as to identify a destination service name to use in an EA transaction and to configure nodes to use for failover support.

Field Name	Description
Logging level	Logging level identifies the level of logging at which to write to the node log file. Logging options include: ◆ NONE turns logging off. NONE is the default value. ◆ ERROR writes only error messages to the log. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
TCP Timeout	TCP Timeout identifies the number of seconds to wait for a TCP/IP request or response before ending the session. Default=90.
Destination Service Name	Destination Service Name identifies the name of the service that is passed to Sterling External Authentication Server (EA) for use in authenticating services. If no value is provided, the SNODE name is used as the service name.
Alternate Destinations - Node	Alternate Destinations Node 1 identifies the node name or IP address and port to use to connect to an alternate Connect:Direct outbound server, if a connection to the primary node cannot be made. Up to three alternate destination nodes can be defined for each outbound node. To use different security and Sterling External Authentication Server definitions for the alternate destination node, first configure an outbound node definition for the alternate node in the netmap. Then, open the primary outbound node definition and select the alternate node name from the drop-down list in the Alternate Destinations - Node 1 field. To use the security and Sterling External Authentication Server definition defined in the primary outbound node for an alternate destination node, you do not have to define the alternate node in the netmap. Select IP Address/Port from the drop down list and then provide a value in the IP Address and Port fields. Define up to three alternate node names.
Alternate Destinations - IP Address	Alternate Destinations Address identifies the IP address to use to connect to an alternate destination node, if a connection to the primary node cannot be made. Up to three alternate destination nodes can be selected. Valid values are 1-200 alphanumeric characters and special characters: underscore (_), dash (-), colon (:), and period (.). If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and EA definition from the primary node is used for the connection.

Field Name	Description
Alternate Destinations - Port	Alternate Destinations Port identifies the port to use to connect to an alternate destination node if a connection to the primary node cannot be made. Up to three alternate destination nodes can be selected. Valid values are 1-65535. If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and EA definition from the primary outbound node is used for the connection.

Connect:Direct Policy Definition

Use the screen and the tabs to define the Connect:Direct policy and define how you impose controls to authenticate a trading partner. For more information, see Connect:Direct proxy configuration on the Sterling Secure Proxy Documentation Library.

Connect:Direct Policy Configuration - Basic

Use the fields on this tab to define the policy name, the protocol being used, and the action to take if a protocol violation occurs. Connect:Direct Policy Basic fields are defined in the following table.

Field Name	Description
Policy Name	Policy Name identifies the name to assign to the policy you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the policy you create. Description can be up to 255 characters.
Type	Type identifies the protocol being used: Connect:Direct.
Protocol Error Action	Protocol Error Action identifies the action to perform if Sterling Secure Proxy detects protocol violations during a communications session. Valid values are: ◆ NONE - select this option to disable checking of protocol errors. ◆ IGNORE - select this option to ignore protocol errors. ◆ WARN - select this option if you want Sterling Secure Proxy to write an error message to the log but continue the session when protocol errors are detected. ◆ ABORT - select this option to terminate a communications session when protocol errors are detected.
Check IP Address	Turn on Check IP Address to ensure that the IP address of the system connecting to the Connect:Direct adapter matches the address of that node in the netmap.

Connect:Direct Policy Configuration - Advanced

Use this tab to specify the type of user authentication for inbound access requests. For Certificate Authentication and User Authentication through External Authentication, you must install and configure EA. For more information, see Connect:Direct Proxy Configuration on the Sterling Secure Proxy Documentation Library.

Connect:Direct Policy Configuration - Advanced fields are defined in the following table.

Field Name	Description
Certificate Authentication - External Authentication Certificate Validation	Turn on External Authentication Certificate Validation to validate information presented in certificates received from trading partners using EA.
Certificate Authentication - External Authentication Profile	External Authentication Profile identifies the name of the Certificate Validation Definition you defined in the EA. You must enable certificate validation before you can provide a profile. Valid values are 1-255 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
User Authentication - Through External Authentication	Turn on this option to send an incoming user ID and password to Sterling External Authentication Server for validation.
User Authentication - External Authentication Profile	If you enabled user authentication through EA, identify the certificate authentication profile you defined in EA in the External Authentication Profile field. Valid values are 1-255 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
User Authentication - Through Local User Store	User Authentication Through Local User Store validates the user ID and password of the inbound node using information defined in the user store. You must add the user to the user store in order to successfully use this method.
User Mapping - Internal User ID	User Mapping - Internal User ID is enabled in the policy and determines what user ID and password is used to connect to the Connect:Direct server in the secure environment. For the user ID and password to successfully access the Connect:Direct server, a user definition must be defined at the server. User mapping options include: ◆ Pass-through for PNODE—Uses the user ID and password supplied by the PNODE to connect to the Connect:Direct server in the secure zone. To successfully connect to the Connect:Direct server, the user ID and password must be defined at the server. ◆ Replace SNODEID with UserId mapped in External Authentication—Maps the user ID provided by the inbound SNODE to a value defined in External Authentication and uses the EA-supplied value to connect to the SNODE. If you select this option, both the SNODE ID and the submitter ID are replaced with a new value. Do not select this option if you have enabled secure point of entry checking in Connect:Direct. ◆ Replace SubmitterID with UserId mapped in External Authentication—Maps the submitter ID provided by the inbound PNODE to a value defined in External Authentication and uses the EA-supplied value to connect to the SNODE. ◆ SSO token from External Authentication—Uses a token from Sterling External Authentication Server to authenticate the user to the server.

Connect:Direct Policy Definition - Step Permissions

Use this tab to block Connect:Direct tasks from being performed on a node. Connect:Direct Policy Definition - Step Permissions fields are defined in the following table.

Field Name	Description
Runjob step allowed	Allows runjob steps to be performed on the PNODE.
Runtask step allowed	Allows runtask steps to be performed on the PNODE.
Copy step allowed	Allows copy steps to be performed on the PNODE.
Submit step allowed	Allows submit steps to be performed on the PNODE

FTP Protocol Field Definitions

Following are the field definitions for the FTP protocol screens. For more information, see FTP Reverse Proxy Configuration on the Sterling Secure Proxy Documentation Library.

FTP Adapter Definition - Basic

Use this tab to specify basic communications information for FTP connections to and from Sterling Secure Proxy. Before you can click the Advanced or Properties tabs, you must specify Adapter Name and Listen Port. Refer to the field definitions in the following table.

Field Name	Description
Adapter Name	Adapter Name identifies the name to assign to the adapter you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the adapter you create. Description can be up to 255 characters.
Type	Type identifies the protocol being used as FTP.
Listen Port	Port number to use to listen for inbound connections. Valid values are between 1-65535.
Netmap	Netmap identifies the name of the netmap to associate with the adapter you are defining. If the netmap has not been created, click ⊕ to add the netmap.
Standard Routing Node	Standard Routing Node identifies the name of the FTP secure server where the inbound node connections are routed after connecting to Sterling Secure Proxy.

Field Name	Description
Engine	Engine identifies the SSP server in the DMZ where traffic is first routed before being sent to the outbound secure Connect:Direct server. Select an engine from the list. You must define an engine before you can create an adapter.
Startup Mode	Startup Mode identifies how the adapter is started. **auto** starts the adapter as soon as it is pushed to the engine. **manual** requires that the adapter be manually started.

FTP Adapter Definition - Advanced

Use this screen to specify additional communications information and to specify the perimeter servers to use for this adapter. FTP advanced adapter fields are defined in the following table.

Field Name	Description
Logging Level	Logging Level identifies the level of logging at which to write to the adapter log file. Logging options include: ◆ ERROR writes only error message to the log. ◆ WARN writes error messages and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Maximum Sessions	Maximum Sessions identifies the maximum number of sessions that the adapter allows. Default=20.
Session Timeout	Session Timeout identifies the amount of time allowed, in minutes, between TCP packets before a session is terminated. Default=3 minutes.
Outbound Port Range	Port range to use for connections on the client data channel, when the client submits a PORT command. If no value is specified, any available port is used.
Active Data Outbound Port Range	Active Data Outbound Port Range identifies the port range to use to listen for connections on the client data channel, when the client submits a PORT command. If no value is specified, any available port is used.
Passive Data Listening Port Range	Passive Data Listening Port Range identifies the port range used to listen for connections on the data channel when the client issues a PASV command. If no value is specified, any available port is used.
Passive NAT Address	Passive NAT Address identifies the IP address sent to the FTP client in response to a PASV command. Define this value if the client cannot directly connect to the proxy, such as when using a remote perimeter server or static network address translation (NAT). The default value is the remote perimeter server address. If you are using a remote external perimeter server with the FTP reverse proxy adapter, identify the name or IP address of the computer running the external perimeter server.

Field Name	Description
External Authentication Server	External Authentication Server identifies the server where EA is installed. Select the EA server from list. You must define the EA server before you select it from the list.
Use IP from PASV Response	Enable this option to use the IP address from the PASV response for outbound data connections. Otherwise, the IP address in the PASV response is ignored and the connection is made to the same IP Address as the initial command connection.
Perimeter Server Mapping - Inbound Perimeter Server	Select the perimeter server to use for the inbound connection in the Perimeter Server Mapping - Inbound Perimeter Server field. You must define the remote perimeter server before you can associate it with an inbound connection.
Perimeter Server Mapping - Outbound Perimeter Server	Select the perimeter server to use for the outbound connection in the Perimeter Server Mapping - Outbound Perimeter Server field. You must define the remote perimeter server before you can associate it with an outbound connection.
Perimeter Server Mapping - External Authentication Perimeter Server	Select the perimeter server to use for the EA connection in the Perimeter Server Mapping - External Authentication Perimeter Server field. You must define the remote perimeter server before you can associate it with an EA connection.

FTP Adapter Definition - Custom

Use this screen to define a custom banner to display for a server greeting banner and a login banner. Refer to the field definitions in the following table.

Field Name	Description
Server Greeting Banner Text	Text to display when a user successfully connects to the server. For example, type Welcome to my ftp site. If no text is provided in this field, the default banner, 220 FTP Server ready, is displayed. Valid values are 0-4000 alphanumeric characters.
Login Banner Text	Identify the text to display as a login message for an FTP proxy adapter. If no banner text is provided, the default banner, 230 User %user logged in, is displayed. Valid values are 0-4000 alphanumeric characters.

FTP Adapter Definition - Properties

Use this screen to edit properties associated with how the FTP protocol is implemented. The keys are not displayed. To change a default key value, type the key value as defined in the following table and assign a value to the key. New adapter properties that are not pre-defined must be added by user.

Properties fields are defined in the following table.

Field Name	Description
Key	Key identifies properties that you can change for an adapter. Available keys include:

Field Name	Description	
	◆ max.ps.server.threads	Maximum number of threads in the pool used during a connection with a server. Default=10.
	◆ ftp.ssl.pbsz.required	Identifies whether the SSL command, PBSZ, is required. Valid values include Y|Yes|y|No|N|n. Default=Y. Set this property to N for certain clients, like Tumbleweed, that do not send a PBSZ command during an SSL session.
	◆ ftp.commands.prohibited	Identifies the FTP commands that cannot be used when an FTP client initiates a connection.
	◆ ftp.ssl.prot.required	Identifies whether the SSL command, PROT, is required. Valid values include Y|Yes|y|No|N|n. Default=Y. Set this property to N for certain clients, like Tumbleweed, that do not send a PROT command during an SSL session.
	◆ max.ps.client.threads	Maximum number of threads in the pool used during a connection with a client. Default=10.
	◆ ftp.commands.allowed	Identifies the FTP commands that can be used when an FTP client initiates a connection.
	◆ ftp.max.command.length	Maximum length allowed for a client command. Default=1024. The command length is unlimited if this parameter is set to 0. If this length is exceeded, an error is logged and the connection is closed.
	◆ ftp.max.response.length	Maximum length allowed for a server ftp response. Default=4096. The server ftp length is unlimited if the parameter is set to 0. If this length is exceeded, an error is logged and the connection is closed. **Note:** Set this parameter to 0 when communicating with a z/OS FTP server.
	◆ failover.detection.enabled	Enables failover detection. Valid value=true | false. Default=false.
	◆ failover.detection.mode	Determines the failover detection mode. ◆ continuous—Continuously polls the outbound node and EA server. continuous=default setting. ◆ Standard only—Polls the outbound node and EA server when a connection fails. Outbound and EA perimeter servers are always continuously polled regardless of this setting.
	◆ failover.poll.interval	Seconds between failover polling. Default=5.
	◆ failover.ea.ping.profile	EA profile to use to extend the EA server healthcheck to the backend LDAP server.

Field Name	Description	
	◆ failover.debug	Enables debug logging for failover. Valid values are true | false. Default=false.
	◆ load.balancer.addr	IP address of the load balancer. Define this property to suppress health check connections logging made by the load balancer.
Value	Value to assign to a property key. See Key for a list of properties you can modify.	

FTP Netmap Definition

Use this screen to define the FTP netmap. Click Inbound Nodes to add connection information for external trading partners. Click Outbound Nodes to add connection information for internal FTP server.

FTP Adapter Definition - Netmap Definition fields are defined in the following table.

Note: You must define a netmap, at least one inbound node, and at least one outbound node before you can save the netmap. If you exit the application before all three elements are defined, you lose the netmap definition.

Field Name	Description
Netmap Name	Netmap Name identifies the name to assign to the netmap you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the netmap you create. Description can be up to 255 characters.
Type	Type identifies the protocol being used as FTP.
Filter	Filter allows you to view a subset of available inbound or outbound nodes. Use the wildcard characters, * and ?, to identify the nodes to display. Filters are case sensitive. For example, the filter i* will display inboundnode1 but will not display InboundNode1.

FTP Netmap Inbound Node Definition - Basic

Use this screen to define the minimum FTP connection requirements for an external trading partner.

Refer to the field definitions in the following table.

Field Name	Description
Inbound Node Name	Inbound Node Name is the name associated with the inbound node connection. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the inbound node you create. Description can be up to 255 characters.
Peer Address Pattern	Peer Address Pattern identifies the pattern to allow for the inbound connections to SSP. Valid values are alphanumeric characters and the following special characters: dash (-), underscore (_), colon (:), period (.), dollar sign ($), forward slash (/), exclamation mark (!), tilde (~), asterisk (*), open parenthesis ("), close parenthesis (") semicolon (;), question mark (?), at (@), and comma (,). You can define one of the following types of patterns: ◆ Wildcard validates incoming DNS names. If a wildcard pattern is provided, Sterling Secure Proxy performs a reverse lookup on the incoming IP address and the DNS name is compared to the wildcard patterns. Wildcard characters allowed are ? and *. For example, *.a.com allows a connection from b.a.com but not from b.b.com. ◆ IP/Subnet validates incoming IP addresses. Use the format IP-address/num-bits where IP-address identifies an IP address template and num-bits identifies the number of leading (highest-order) bits in the template that are significant. An IP match is performed by comparing the leading (highest-order) num-bits of the incoming IP address against num-bits of the template. For example, 10.20.0.0/16 searches for a match to the first 16 bits. All IP addresses beginning with 10.20.* are allowed. 10.0.0.0/8 searches for a match to the first 8 bits. All addresses beginning with 10.* are allowed. 0.0.0.0/0 searches for a match the first zero bits. All IP addresses are allowed.
Policy	Policy is a list of policies you have created. Select the policy you want to associate with the inbound node you are creating. If a policy with the security attributes required has not been created, click ⊕.

FTP Netmap Inbound Node Definition - Security

Use this screen to define secure connection requirements for an external trading partner. Refer to the field definitions in the following table.

Field Name	Description
Secure Connection	Enable Secure Connection to turn on the use of SSL/TLS to provide secure communications with transport protocols and to ensure that data is secured as it is transmitted across a single socket.

Field Name	Description
Security Setting	Security Setting identifies the security protocol allowed for connections to this node. Options include: ◆ SSL v3 or TLS—sends a TLS Hello and accept SSLv3 or TLS ◆ SSL v2 or v3 with v3 Hello—sends an SSLv3 Hello and accept SSLv3 or SSLv2 ◆ SSL (any version) or TLS—sends an SSL v2 Hello and accept SSLv3, SSLv2, or TLS ◆ SSL v2 or v3—sends SSLv2 Hello and accept SSLv3 or SSLv2 ◆ TLS—sends TLS Hello and accept TLS only ◆ SSL v3—sends SSLv3 Hello and accept SSLv3 only
Enable Client Authentication	Enable Client Authentication on the inbound node connection to require that the SSP server authenticate the certificate presented by the inbound node connection.
Trust Store	Location where trusted CA certificates are stored. CA certificates verify that a certificate received from a server is signed by a trusted source.
CA Certificates/Trusted Root	CA Certificates/Trusted Root identifies the trusted certificate to use to authenticate the certificate presented by the client. You select a CA certificate or trusted root from the list of certificates stored in the trust store you selected in the Trust Store field. When a client presents a certificate to establish a secure connection, the trusted root certificate located at the server must match or be the entity who signed the certificate presented by the client during the SSL handshake.
Key Store	Location where the key certificates you want to use are stored.
Key/System Certificate	Certificate presented by SSP to the node to authenticate itself during the SSL handshake. Select the certificate to use for the node from the list that contains the key or system certificates stored in the key store selected in the Key Store field.
Available Cipher Suites	List of ciphers that can be enabled to encrypt data transmitted during a secure SSL or TLS connection. Enable at least one cipher. To enable a cipher, highlight it and click Add. To enable multiple ciphers, highlight them and click Add.
Selected Cipher Suites	Selected Cipher Suites identifies the ciphers you have enabled to encrypt data during a secure SSL or TLS connection. A cipher suite is negotiated during a secure channel connection between a client and a server. Ciphers are negotiated based on their location in the Selected Ciphers list. To reorder a cipher in the list, highlight it and click Up or Down.
Clear Control Channel	Enable Clear Control Channel to allow an inbound or outbound node to use an unencrypted control channel for commands after the SSL or TLS handshake is complete. The data channel for file transfers is still be encrypted.

FTP Netmap Inbound Node Definition- Advanced

Use this screen to specify the level at which to log information on this inbound connection. FTP Netmap Inbound Node Definition - Advanced fields are defined in the following table.

Field Name	Description
Logging Level	Logging Level identifies the level of logging to write to the log file for the inbound node. Logging options include the following: ◆ NONE turns logging off. NONE is the default value. ◆ ERROR writes only error messages to the log. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.

FTP Netmap Outbound Node Definition - Basic

Use this screen to define the minimum connection requirements for your internal FTP server.

FTP Netmap Outbound Node Definition - Basic fields are defined in the following table.

Field Name	Description
Outbound Node Name	Name of the outbound server in the secure zone which is the destination of the communications session. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description up to 255 characters to help identify the outbound node you create.
Primary Destination Address	IP address or host name to use to connect to the Connect:Direct outbound server. Valid values are 1-200 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), colon (:), and underscore (_).
Primary Destination Port	Primary Destination Port identifies the port to use to connect to the secure Connect:Direct server. Valid values are 1-65535.

FTP Outbound Node Definition - Security

Use this screen to define the secure connection requirements for your internal FTP server. FTP Netmap Inbound Node Definition - Security fields are defined in the following table.

Field Name	Description
Secure Connection	Enable Secure Connection to turn on the use of SSL/TLS to provide secure communications with transport protocols and to ensure that data is secured as it is transmitted across a single socket.
Security Setting	Security protocol allowed for connections to this node. Options include: ◆ SSL v3 or TLS - select this option to send an TLS Hello and accept SSLv3 or TLS ◆ SSL v2 or v3 with v3 Hello - select this option to send an SSLv3 Hello and accept SSLv3 or SSLv2 ◆ SSL (any version) or TLS - select this option to send an SSL v2 Hello and accept SSLv3, SSLv2, or TLS ◆ SSL v2 or v3 - select this option to send SSLv2 Hello and accept SSLv3 or SSLv2 ◆ TLS - select this option to send TLS Hello and accept TLS only ◆ SSL v3 - select this option to send SSLv3 Hello and accept SSLv3 only
Trust Store	Location where trusted CA certificates are stored. CA certificates verify that a certificate received from a server is signed by a trusted source.
CA Certificate /Trusted Root	CA Certificate/Trusted Root identifies the trusted certificate to use to authenticate the certificate presented by the client. You select a CA certificate or trusted root from the list of certificates stored in the trust store you selected in the Trust Store field. When a client presents a certificate to establish a secure connection, the trusted root certificate, located at the server, must match or be the entity that signed the certificate presented by the client during the SSL handshake.
Key Store	Key Store identifies the location where the key certificates you want to use are stored.
Key/System Certificate	Certificate presented by SSP to the node to authenticate itself during the SSL handshake. Select the certificate to use for the node from the list that contains the key or system certificates stored in the key store selected in the Key Store field.
Available Cipher Suites	Ciphers that can be enabled to encrypt data transmitted during a secure SSL or TLS connection. Enable at least one cipher. To enable a cipher, highlight the cipher in the Available Cipher Suites dialog and click Add. To enable multiple ciphers, highlight the ciphers to enable and click Add.
Selected Cipher Suites	Cipher you have enabled to encrypt data during a secure SSL or TLS connection. A cipher suite is negotiated during a secure channel connection between a client and a server. Ciphers are negotiated based on their location in the Selected Ciphers list. To reorder a cipher in the list, highlight the cipher to reorder and click the Up or Down button.
Clear Control Channel	Enable Clear Control Channel to allow an inbound or outbound node to use an unencrypted control channel for commands after the SSL or TLS handshake is complete. The data channel for file transfers will still be encrypted.

FTP Netmap Outbound Node Definition - Advanced

Use this screen to define advanced parameters for your internal FTP server. Refer to the field definitions in the following table.

Field Name	Description
Logging Level	Logging Level identifies the level of logging to write to the log file for the outbound node. Logging options include: ◆ NONE turns logging off. ◆ ERROR writes only error message to the log. ◆ WARN writes error messages and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Destination Service Name	Destination Service Name identifies a destination server that can be accessed by the outbound node, when using EA to map a user ID and password. Valid values are 1-255 alphanumeric characters and certain special characters. The following special characters are not allowed: ! @ # % ^ * ( ) + ? , < > { } [ ] | ; " '
User ID	User ID identifies the user ID to use to connect to the secure outbound server, if the policy is defined to required that the user ID and password from the netmap be used. Valid values are 1-255 alphanumeric characters and certain special characters. The following special characters are not allowed: ! @ # % ^ * ( ) + ? , < > { } [ ] | ; " '
Password	Password to use to connect to the secure outbound server, if the policy is defined to require the user ID and password from the netmap. Valid values are 1-255 alphanumeric characters and certain special characters. The following special characters are not allowed: , " '
Alternate Destinations - Node	Alternate Destinations Node 1 identifies the node name or IP address and port to use to connect to an alternate Connect:Direct outbound server if a connection to the primary node cannot be made. Up to three alternate destination nodes can be defined for each outbound node. To use different security and EA definitions for the alternate destination node, first configure an outbound node definition for the alternate node in the netmap. Then, open the primary outbound node definition and select the alternate node name from the drop-down list in the Alternate Destinations - Node 1 field. To use the security and EA definition defined in the primary outbound node for an alternate destination node, you do not have to define the alternate node in the netmap. Select IP Address/Port from the drop down list and then provide a value in the IP Address and Port fields. Define up to three alternate node names.
Alternate Destinations - IP Address	Alternate Destinations Address identifies the IP address to use to connect to an alternate destination node, if a connection to the primary node cannot be made. Up to three alternate destination nodes can be selected. Valid values are 1-200 alphanumeric characters and special characters: underscore (_), dash (-), colon (:), and period (.). If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and EA definition from the primary node is used for the connection.

Field Name	Description
Alternate Destinations - Port	Alternate Destinations Port identifies the port to use to connect to an alternate destination node, if a connection to the primary node cannot be made. Up to three alternate destination nodes can be selected. Valid values are 1-65535. If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and EA definition from the primary outbound node is used for the connection.

FTP Policy Configuration - Basic

Use this screen to define how you impose controls to authenticate a trading partner trying to access your FTP server. FTP Policy Configuration - Basic fields are defined in the following table.

Field Name	Description
Policy Name	Name to assign to the policy you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description up to 255 characters to help identify the policy you create.
Type	Protocol being used as FTP.

FTP Policy Configuration - Advanced

Use this tab to specify the type of user authentication to use for inbound access requests. For Certificate Authentication and User Authentication through External Authentication, you must have installed and configured EA. You can also use this screen to map an incoming user ID and password to a different user ID and password to present to the internal server.

FTP Policy Configuration - Advanced fields are defined in the following table.

For more information, see FTP Reverse Proxy Configuration on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Certificate Authentication - External Authentication Certificate Validation	Turn on External Authentication Certificate Validation to validate information presented in certificates received from trading partners using EA.
Certificate Authentication - External Authentication Profile	External Authentication Profile identifies the name of the Certificate Validation Definition you defined in EA. You must enable certificate validation before you can provide a profile.

Field Name	**Description**
User Authentication - Through External Authentication	Turn on User Authentication through External Authentication to send an incoming user ID and password to EA for validation.
User Authentication - External Authentication Profile	If you enabled user authentication through EA, identify the certificate authentication profile you defined in EA in the External Authentication Profile field.
User Authentication - Through Local User Store	User Authentication Through Local User Store validates the user ID and password of the inbound node using information defined in the user store. You must add the user to the user store in order to successfully use this method.
User Mapping - Internal User ID	Determines what user ID and password is used to attach to the outbound node in the secure environment. User mapping options include: ◆ Pass-through—Uses the user ID and password supplied by the inbound node to connect to the outbound node in the secure zone. To successfully connect to the outbound node, the user ID and password provided by the client must be valid at the target server. ◆ From External Authentication—Uses a user ID and password from EA to connect to the outbound node. To successfully connect using this option, the user ID and password must be defined in the LDAP database and must be valid at the target server. ◆ From Netmap—Uses the user ID and password defined in the netmap to connect to the outbound node. To successfully connect using this option, define the user ID and password to use to connect to the target server in the outbound node definition. ◆ SSO token from External Authentication—Uses a token from EA to authenticate the user to the outbound node.

HTTP Protocol Field Definitions

Following are the field definitions for the HTTP protocol screens. For more information, see HTTP reverse proxy configuration on the Sterling Secure Proxy Documentation Library.

HTTP Adapter Configuration - Basic

Use this tab to specify basic communications information for HTTP connections. Before you can click the Advanced or Properties tabs, you must specify Adapter Name and Listen Port. Refer to the field definitions in the following table.

Field Name	Description
Adapter Name	Name to assign to the adapter you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description up to 255 characters to help identify the adapter you create.
Type	Type identifies the protocol being used as HTTP.
Listen Port	Port number to use to listen for inbound connections. Default=13640. Valid values include 1-65535.
Netmap	Name of the netmap to associate with the adapter you are defining. If the netmap has not been created, click ⊕ to add the netmap.
Routing Type	Select the Routing Type to identify how inbound connections are routed to the HTTP server in the trusted zone. For HTTP connections to an outbound node, select standardRouting. Select noRouting to use this HTTP adapter only as a change password portal and prevent any outbound connections to the secure zone.
Standard Routing Node	Standard Routing Node identifies the name of the HTTP secure server where the inbound node connections are routed, after connecting to SSP. Select this value from a pull-down list.
Support HTML Rewrite	Enable Support HTML Rewrite to rewrite URLs within the HTML returned by the outbound node. HTML Rewrite must also be defined and enabled on the netmap.
Engine	Engine identifies the SSP server in the DMZ where the adapter listens for inbound connections and routes the connection to an outbound node. Select an engine from the list. You must define an engine before you can create an adapter.
Startup Mode	Startup Mode identifies how the adapter is started. **auto** starts the adapter as soon as it is pushed to the engine. **manual** requires that the adapter be manually started.

HTTP Adapter Definition - Advanced

Use this screen to specify additional communications information, and to specify the perimeter servers to use for this adapter. HTTP Adapter Definition - Advanced fields are defined in the following table.

Field Name	Description
Logging Level	Logging Level identifies the level of logging to write to the log file for the adapter. Logging options include: ◆ ERROR writes only error message to the log. ◆ WARN writes error messages and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Maximum Sessions	Maximum Sessions identifies the maximum number of sessions that the adapter allows. Default=20.
Session Timeout	Session Timeout identifies the amount of time allowed, in minutes, between TCP packets before a session is terminated. Default=3 minutes.
HTTP Ping Response	HTTP Ping Response identifies the response to send when an HTTP GET is received on the listen port. Provide this value To perform a health check response to a third-party IP load balancer, such as Big IP. If you provide a value in this field, the value is displayed in a browser window. You can provide HTML syntax and text values in this field. To test the response, ping the URL that you define in the HTTP Ping URI field and port of the engine. For example if you configure an adapter on port 13640 and you want to get an HTTP 1.0 response, send a ping to http://ProxyServerURL:13640/<*HTTP Ping URI*>. The value you supplied in the HTTP Ping Response field is returned. If you provide a value in this field, the value is displayed in a browser window. You can provide HTML syntax and text values.
HTTP Ping URI	HTTP Ping URI identifies the URI to monitor for incoming requests from an inbound node. If SSP receives a request for this URI, it returns the ping response, provided in the HTTP Ping Response field.
Outbound Port Range	Outbound Port Range identifies the range of ports to use for the adapter. Valid values include a list of ports that are allowed with each value separated by a comma such as 1234, 2340, 16570 or a range of ports allowed, such as 16570 -17950.
SSO Configuration	Select the SSO configuration to use for this adapter. This field is required if the adapter supports the use of single sign-on tokens.
External Authentication Server	External Authentication Server (EA) identifies the server where EA is installed. Select the EA server from the pull-down list. You must define an EA server before can select the server from the list.

Field Name	Description
Perimeter Server Mapping - Inbound Perimeter Server	Select the perimeter server to use for the inbound connection in the Perimeter Server Mapping - Inbound Perimeter Server field. To use a remote perimeter server, you must define the remote perimeter server before you can associate it with an inbound connection.
Perimeter Server Mapping - Outbound Perimeter Server	Select the perimeter server to use for the outbound connection in the Perimeter Server Mapping - Outbound Perimeter Server field. To use a remote perimeter server, you must define the remote perimeter server before you can associate it with an outbound connection.
Perimeter Server Mapping - External Authentication Perimeter Server	Select the perimeter server to use for the EA connection in the Perimeter Server Mapping - External Authentication Perimeter Server field. To use a remote perimeter server, you must define the remote perimeter server before you can associate it with an EA connection.

HTTP Adapter Definition - Properties

Use this screen to edit properties associated with how the HTTP protocol is implemented. HTTP Adapter Definition - Properties fields are defined in the following table.

Field Name	Description	
Key	Properties that you can change for an adapter. Available keys include:	
	◆ http.commands.allowed	HTTP method allowed. Commands that are allowed by default include GET, HEAD, PUT, POST, TRACE, OPTIONS, and DELETE. WebDAV methods allowed are PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, and UNLOCK. To identify more than one allowed method, separate each value with a comma.
	◆ http.commands.prohibited	HTTP methods, such as DELETE, MOVE, that are prohibited. By default, CONNECT is prohibited. To identify more than one prohibited method, separate each value with a comma.
	◆ httpMaxHeaderFieldLength	Maximum length allowed for any HTTP header in the incoming HTTP request. Default=8192.
	◆ httpMaxNumHeaderFields	Identifies the maximum number of HTTP headers allowed in the incoming HTTP request. The default value is 1024.
	◆ max.html.rewrite.threads	Maximum number of threads in the pool used to service rewriting URLs in the HTML pages coming from the backend HTTP Server. The default is 10. **Note:** This parameter is not displayed. If you want to change its value, you must type the field in the Key field and the new value in the Value field.

Field Name	Description	
	◆ max.ps.client.threads	Maximum threads in the pool used during a connection with a client. Default value is 10.
	◆ max.ps.server.threads	Maximum threads in the pool used during a connection with a server. Default value is 10.
	◆ html.rewrite.threads	Number of threads used in the thread pool for HTML rewrite processing. Default is 10.
	◆ html.rewrite.threads.queue.size	Buffer size used to queue the request for HTML rewrite processing. **Note:** This parameter is not displayed. If you want to change its value, you must type the field in the Key field and the new value in the Value field.
	◆ failover.detection.enabled	Enables failover detection. Valid value=true | false. Default=false.
	◆ failover.detection.mode	Determines the failover detection mode. ◆ continuous—Continuously polls the outbound node and EA server. Default setting. ◆ Standard only—Polls the outbound node and EA server when a connection fails. Outbound and EA perimeter servers are always continuously polled regardless of this setting.
	◆ failover.poll.interval	How many seconds between failover polling. Default=5.
	◆ failover.ea.ping.profile	Identifies a EA profile to use to extend the EA server healthcheck to the backend LDAP server.
	◆ failover.debug	Enables debug logging for failover. Valid values are true | false. Default=false.
	◆ load.balancer.addr	IP address of the load balancer. Define this property to suppress health check connections logging made by the load balancer.
Value	Value to assign to a property key. See Key for a list of properties you can modify.	

HTTP Netmap Definition

Use this screen to define the HTTP netmap. The netmap includes inbound and outbound node definitions, and HTML rewrite definitions.

- HTTP Netmap Inbound Node Definition- Basic—Click Inbound Nodes to add connection information for your external trading partner.
- HTTP Netmap Outbound Node Definition - Basic—Click Outbound Nodes to add connection information for your internal Connect:Direct server.
- HTML Rewrite Definition—Click HTML Rewrite to reroute an incoming URL request.

HTTP Netmap Definition fields are defined in the following table.

Note: You must define a netmap, at least one inbound node, and at least one outbound node before you can save the netmap. If you exit the application before all three elements are defined, you lose the netmap definition.

Field Name	Description
Netmap Name	Name to assign to the netmap you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description up to 255 characters to help identify the netmap you create.
Type	Protocol being used as HTTP.
Filter	Filter allows you to view a subset of available inbound or outbound nodes. Use the wildcard characters, * and ?, to identify the nodes to display. Filters are case-sensitive. For example, the filter i* will display inboundnode1 but will not display InboundNode1.

HTTP Netmap Inbound Node Definition- Basic

Use this screen to define the minimum HTTP connection requirements for an external trading partner. HTTP Netmap Inbound Node Definition - Basic fields are defined in the following table.

Field Name	Description
Inbound Node Name	Inbound Node Name is the name associated with the inbound node connection. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the inbound node you create. Description can be up to 255 characters.

Field Name	Description
Peer Address Pattern	Peer Address Pattern identifies the pattern to allow for the inbound connections to SSP. Valid values are alphanumeric characters and the following special characters: dash(-), underscore(_), colon(:), period(.), dollar sign($), forward slash(/), exclamation mark(!), tilde(~), asterisk(*), open parenthesis '(', close parenthesis ')' semicolon(;), question mark(?), at(@), and comma(,). You can define one of the following types of patterns: ◆ Wildcard validates incoming DNS names. If a wildcard pattern is provided, SSP performs a reverse lookup on the incoming IP address and the DNS name is compared to the wildcard patterns. Wildcard characters allowed are ? and *. For example, *.a.com allows a connection from b.a.com but not from b.b.com ◆ IP/Subnet validates incoming IP addresses. Use the format IP-address/num-bits where IP-address identifies an IP address template and num-bits identifies the number of leading (highest-order) bits in the template that are significant. An IP match is performed by comparing the leading (highest-order) num-bits of the incoming IP address against num-bits of the template. For example, 10.20.0.0/16 searches for a match to the first 16 bits. All IP addresses beginning with 10.20.* are allowed. 10.0.0.0/8 searches for a match to the first 8 bits. All addresses beginning with 10.* are allowed. 0.0.0.0/0 searches for a match the first zero bits. All IP addresses are allowed.
Policy	Policy is a pull-down list of policies you have created. Select the policy you want to associate with the inbound node you are creating. If a policy with the security attributes required has not been created, click ⊕.

HTTP Netmap Inbound Node Definition- Security

Use this screen to define secure connection requirements for an external trading partner.

HTTP Netmap Inbound Node Definition - Security fields are defined in the following table.

Field Name	Description
Secure Connection	Enable Secure Connection to turn on the use of SSL/TLS to provide secure communications with transport protocols and to ensure that data is secured as it is transmitted across a single socket.

Field Name	Description
Security Setting	Security Setting identifies the security protocol allowed for connections to this node. Options include: ◆ SSL v3 or TLS - select this option to send an TLS Hello and accept SSLv3 or TLS ◆ SSL v2 or v3 with v3 Hello - select this option to send an SSLv3 Hello and accept SSLv3 or SSLv2 ◆ SSL (any version) or TLS - select this option to send an SSL v2 Hello and accept SSLv3, SSLv2, or TLS ◆ SSL v2 or v3 - select this option to send SSLv2 Hello and accept SSLv3 or SSLv2 ◆ TLS - select this option to send TLS Hello and accept TLS only ◆ SSL v3 - select this option to send SSLv3 Hello and accept SSLv3 only
Enable Client Authentication	Enable Client Authentication on the inbound node connection to require that the SSP server authenticate the certificate presented by the inbound node connection.
Trust Store	Location where trusted CA certificates are stored. CA certificates verify that a certificate received from a server is signed by a trusted source.
CA Certificates/Trusted Root	CA Certificates/Trusted Root identifies the trusted certificate to use to authenticate the certificate presented by the client. You select a CA certificate or trusted root from the list of certificates stored in the trust store you selected in the Trust Store field. When a client presents a certificate to establish a secure connection, the trusted root certificate, located at the server, must match or be the entity who signed the certificate presented by the client during the SSL handshake.
Key Store	Key Store identifies the location where the key certificates you want to use are stored.
Key/System Certificate	Certificate presented by SSP to the node to authenticate itself during the SSL handshake. Select the certificate to use for the node from the list that contains the key or system certificates stored in the key store selected in the Key Store field.
Available Cipher Suites	Available Cipher Suites provides a list of ciphers that can be enabled to encrypt data transmitted during a secure SSL or TLS connection. Enable at least one cipher. To enable a cipher, highlight the cipher in the Available Cipher Suites dialog and click Add. To enable multiple ciphers, highlight the ciphers to enable and click Add.
Selected Cipher Suites	Selected Cipher Suites identifies the ciphers you have enabled to encrypt data during a secure SSL or TLS connection. A cipher suite is negotiated during a secure channel connection between a client and a server. Ciphers are negotiated based on their location in the Selected Ciphers list. To reorder a cipher in the list, highlight the cipher to reorder and click the Up or Down button.

HTTP Netmap Inbound Node Definition- Advanced

Use this screen to specify what level to log information on this inbound connection.

Field Name	Description
Node Logging Level	Node Logging Level identifies the level of logging to write to the log file for the inbound node. Logging options include: ◆ NONE turns logging off. ◆ ERROR writes only error messages to the log. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.

HTTP Netmap Outbound Node Definition - Basic

Use this screen to define the minimum connection requirements for your internal HTTP server.

Field Name	Description
Outbound Node Name	Outbound Node Name identifies the name of the outbound server in the secure zone which is the destination of the communications session. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the outbound node you create. Description can be up to 255 characters.
Primary Destination Address	Primary Destination Address identifies the IP address or host name to use to connect to the outbound server. Valid values are 1-200 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), colon (:), and underscore (_).
Primary Destination Port	Primary Destination Port identifies the port to use to connect to the outbound server. Valid values are 1-65535.

HTTP Netmap Outbound Node Definition - Security

Use this screen to define the secure connection requirements for your internal HTTP server. Refer to the field definitions in the following table.

Field Name	Description
Secure Connection	Enable Secure Connection to turn on the use of SSL/TLS to provide secure communications with transport protocols and to ensure that data is secured as it is transmitted across a single socket.

Field Name	Description
Security Setting	Security Setting identifies the security protocol allowed for connections to this node. Options include: ◆ SSL v3 or TLS - select this option to send an TLS Hello and accept SSLv3 or TLS ◆ SSL v2 or v3 with v3 Hello - select this option to send an SSLv3 Hello and accept SSLv3 or SSLv2 ◆ SSL (any version) or TLS - select this option to send an SSL v2 Hello and accept SSLv3, SSLv2, or TLS ◆ SSL v2 or v3 - select this option to send SSLv2 Hello and accept SSLv3 or SSLv2 ◆ TLS - select this option to send TLS Hello and accept TLS only ◆ SSL v3 - select this option to send SSLv3 Hello and accept SSLv3 only
Trust Store	Location where trusted CA certificates are stored. CA certificates verify that a certificate received from a server is signed by a trusted source.
CA Certificate/Trusted Root	CA Certificate/Trusted Root identifies the trusted certificate to use to authenticate the certificate presented by the client. You select a CA certificate or trusted root from the list of certificates stored in the trust store you selected in the Trust Store field. When a client presents a certificate to establish a secure connection, the trusted root certificate, located at the server, must match or be the entity who signed the certificate presented by the client during the SSL handshake.
Key Store	Key Store identifies the location where the key certificates you want to use are stored.
Key/System Certificate	Certificate presented by SSP to the node to authenticate itself during the SSL handshake. Select the certificate to use for the node from the list that contains the key or system certificates stored in the key store selected in the Key Store field.
Available Ciphers	Available Ciphers provides a list of ciphers that can be enabled to encrypt data transmitted during a secure SSL or TLS connection. Enable at least one cipher. To enable a cipher, highlight the cipher in the Available Cipher Suites dialog and click Add. To enable multiple ciphers, highlight the ciphers to enable and click Add.
Selected Ciphers	Selected Ciphers identifies the ciphers you have enabled to encrypt data during a secure SSL or TLS connection. A cipher suite is negotiated during a secure channel connection between a client and a server. Ciphers are negotiated based on their location in the Selected Ciphers list. To reorder a cipher in the list, highlight the cipher to reorder and click the Up or Down button.

HTTP Netmap Outbound Node Definition - Advanced

Use this screen to define advanced parameters for your internal HTTP server. HTTP Netmap Outbound Node Definition - Advanced fields are defined in the following table.

For more information, see HTTP reverse proxy configuration on the Sterling Secure Proxy Documentation Library.

Field Name	**Description**
Node Logging Level	Node Logging Level identifies the level of logging to write to the log file for the outbound node. Logging options include: ◆ NONE turns logging off. ◆ ERROR writes only error messages to the log. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Destination Service Name	Destination Service Name identifies a destination server that can be accessed by the outbound node, when using EA to map a user ID and password. Valid values are 1-255 alphanumeric characters and certain special characters. The following special characters are not allowed: ! @ # % ^ * ( ) + ? , < > { } [ ] | ; " '
User ID	User ID identifies the user ID to use to connect to the secure outbound server, if the policy is defined to required that the user ID and password from the netmap be used. Valid values are 1-255 alphanumeric characters and certain special characters. The following special characters are not allowed: ! @ # % ^ * ( ) + ? , < > { } [ ] | ; " '
Password	Password to use to connect to the secure outbound server, if the policy is defined to required that the user ID and password from the netmap be used. Valid values are 1-255 alphanumeric characters and certain special characters. The following special characters are not allowed: , " '
Alternate Destinations - Node	Alternate Destinations Node 1 identifies the node name or IP address and port to use to connect to an alternate outbound server, if a connection to the primary node cannot be made. Up to three alternate destination nodes can be defined for each outbound node. To use different security and EA definitions for the alternate destination node, first configure an outbound node definition for the alternate node in the netmap. Then, open the primary outbound node definition and select the alternate node name from the drop-down list in the Alternate Destinations - Node 1 field. To use the security and EA definition defined in the primary outbound node for an alternate destination node, you do not have to define the alternate node in the netmap. Select IP Address/Port from the drop down list and then provide a value in the IP Address and Port fields."
Alternate Destinations - IP Address	Alternate Destinations Address identifies the IP address to use to connect to an alternate destination node, if a connection to the primary node cannot be made. Up to three alternate destination nodes can be selected. Valid values are 1-200 alphanumeric characters and special characters: underscore (_), dash (-), colon (:), and period (.). If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and EA definition from the primary node is used for the connection.

Field Name	Description
Alternate Destinations - Port	Alternate Destinations Port identifies the port to use to connect to an alternate destination node, if a connection to the primary node cannot be made. Up to three alternate destination nodes can be selected. Valid values are 1-65535. If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and EA definition from the primary outbound node is used for the connection.

HTML Rewrite Definition

Use this screen to rewrite URLs in the HTML presented by your internal HTTP server and route requests to the HTTP Reverse Proxy Adapter. Click New to define a new Server-Proxy URL pair. HTML Rewrite Definition fields are defined in the following table.

Field Name	Description
Support HTML Rewrite	Enable Support HTML Rewrite to replace HTML values that route connections to an internal server with a values that route connections to SSP.
Server URL	Server URL identifies the URL of the internal HTTP server. Because the inbound node does not have access to the internal HTTP server, you must identify the proxy URL to replace the server URL with.
Proxy URL	Proxy URL identifies the URL of the HTTP Reverse Proxy adapter where the inbound connection is routed instead of to the server URL.

HTTP Policy Configuration

Use this screen and tabs to define how you authenticate a trading partner to access an HTTP server.

HTTP Policy Configuration- Basic

Use this screen to define basic authentication information. HTTP Policy Configuration - Basic fields are defined in the following table.

Field Name	Description
Policy Name	Policy Name identifies the name to assign to the policy you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the policy you create. Description can be up to 255 characters.
Type	Type identifies the protocol being used as HTTP.

HTTP Policy Configuration- Advanced

Use this tab to specify the type of user authentication to use for inbound access requests. For Certificate Authentication and User Authentication through External Authentication, you must have installed and configured EA. HTTP Policy Configuration - Advanced fields are defined in the following table.

Field Name	Description
External Authentication Profile	External Authentication Profile identifies the name of the certificate validation definition you defined in the EA. You must enable certificate validation before you can provide a profile.
User Authentication Type	User authentication to enable. To enable single sign-on, select Application Authentication for browser based clients and basic authentication for non-browser based clients.
Through External Authentication	Turn on User Authentication through External Authentication to send an incoming user ID and password to EA for validation.
External Authentication Profile	If you enabled user authentication through EA, identify the certificate authentication profile you defined in EA.
Through Local User Store	Validates the user ID and password of the inbound node using information defined in the user store. You must add the user to the user store to successfully use this method.
Internal User ID	User ID and password used to attach to the server in the secure environment. For the user ID and password presented to the GIS server to successfully access the server, a user definition must be defined at the GIS server. User mapping options include: ◆ User ID/Password passed through from client—Uses the user ID and password supplied by the inbound node to connect to the server in the secure zone. To successfully connect to the server, the user ID and password must be defined in the user store at the server. ◆ User ID/Password From External Authentication—Uses a user ID and password from EA to connect to the server. To successfully connect using this option, the user ID and password must be defined in the LDAP database. ◆ User ID/Password from netmap—Uses the user ID and password defined in the netmap to connect to the outbound server. To successfully connect using this option, define the user ID and password to use in the outbound node definition. ◆ SSO token from External Authentication—Uses a token from Sterling External Authentication Server to authenticate the user to the server.
Block Common Exploit Strings	Enable this option to scan inbound URI queries for any of the defined strings. If a match is found, the request is rejected and the connection is closed. Default blocked strings include: --, |, ', \, <?, \u0000. To modify the common exploits that are blocked, modify the strings.

SFTP Protocol Field Definitions

Following are the field definitions for the SFTP protocol screens. For more information on configuring an SFTP Adapter, see SFTP Reverse Proxy Configuration on the Sterling Secure Proxy Documentation Library.

SFTP Adapter Configuration - Basic

Use this screen to specify system-level communications information for SFTP connections to and from Sterling Secure Proxy. Refer to the field definitions in the following table.

Field Name	Description
Adapter Name	Adapter Name identifies the name to assign to the adapter you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the adapter you create. Description can be up to 255 characters.
Type	Type identifies the protocol being used as SFTP.
Listen Port	Port number to use to listen for inbound connections. Valid values are between 1-65535.
Netmap	Netmap identifies the name of the netmap to associate with the adapter you are defining. If the netmap has not been created, click ⊕ to add the netmap.
Standard Routing Node	Standard Routing Node identifies the name of the SFTP outbound node where the inbound node connections are routed, after connecting to SSP. Select this value from a pull-down list.
Engine	Engine identifies the SSP server in the DMZ where the adapter will listen for inbound connections to be routed to the outbound node. Select an engine from the list. You must define an engine before you can create an adapter.
Startup Mode	Startup Mode identifies how the adapter is started. **auto** starts the adapter as soon as it is pushed to the engine. **manual** requires that the adapter be manually started.
Local Host Key Store	Local Host Key Store identifies the local host key store you created to store local host keys. Select the local host key store that contains the local host key to use to authenticate SSP to the inbound node connections.
Local Host Key	Local Host Key identifies the local host key you have added to the key store. Select the local host key from the drop-down list that will used to authenticate SSP to the inbound node connections. If you make changes to the local host key, you must restart the adapter before the change is recognized.

SFTP Adapter Configuration - Security

Use this screen to specify security information for SFTP connections to and from Sterling Secure Proxy. Refer to the field definitions in the following table.

Field Name	Description
Available Cipher Suites	Available Cipher Suites provides a list of ciphers that can be enabled to encrypt data transmitted during a secure SSH connection. Enable at least one cipher. To enable a cipher, highlight the cipher in the Available Cipher Suites dialog and click Add. To enable multiple ciphers, highlight the ciphers to enable and click Add.
Selected Cipher Suites	Selected Cipher Suites identifies the ciphers you have enabled to encrypt data during a secure connection. A cipher suite is negotiated during a secure channel connection between a client and a server. Ciphers are negotiated based on their location in the Selected Ciphers list. To reorder a cipher in the list, highlight the cipher to reorder and click the Up or Down button. If you make changes to the selected cipher suites, you must restart the adapter before the change is recognized. **Note:** If you define multiple SFTP adapters on an engine, all adapters must define a common set of ciphers. Unintended results may occur if this parameter is defined differently.
Available MAC Suites	Available MAC Suites provides a list of MACs that can be enabled to provide message integrity protection. Enable at least one MAC. To enable a MAC, highlight the MAC in the Available MAC Suites dialog and click Add. To enable multiple MACs, highlight the MACs to enable and click Add.
Selected MAC Suites	Selected MAC Suites identifies the MACs you have enabled to provide message integrity protection. MACs are negotiated based on their location in the Selected MAC Suites list. To reorder a MAC in the list, highlight the MAC to reorder and click the Up or Down button. If you make changes to the selected MAC suites, you must restart the adapter before the change is recognized. **Note:** If you define multiple SFTP adapters on an engine, all adapters must define a common set of MACs. Unintended results may occur if this parameter is defined differently.
Available Key Exchange	Identifies the available key exchanges you can configure for an SFTP adapter.
Selected Key Exchange	Identifies the key exchanges that have been configured. Key exchanges are used in the order in which they are selected in this field. To reorder a key exchange in the list, highlight the exchange to reorder and click the Up or Down button.

SFTP Adapter Configuration - Advanced

Use this screen to specify additional communications information, and to specify the perimeter servers to use for this adapter. Refer to the field definitions in the following table.

Field Name	Description
Logging Level	Level of logging to write to the log file for the adapter. Logging options include: ◆ ERROR writes only error messages to the log. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Maximum Sessions	Maximum number of sessions that the adapter allows. The default is 20. If you make changes to the maximum sessions, you must restart the adapter before the change is recognized.
Session Timeout	Amount of time allowed, in minutes, between TCP packets before a session is terminated. The default is 3 minutes. If you make changes to the session timeout, you must restart the adapter before the change is recognized.
Pre-Authentication Banner Text	The remote software version to send when an inbound connection is made. The text is sent to the client before server authentication is performed. Valid values are 0-255 alphanumeric and special characters. The default value is SSHD_Maverick.
Post-Authentication Banner Text	Text displayed when an inbound connection is made. It is sent to the client after server authentication is performed. Valid values are 0-4000 alphanumeric and special characters. No default value is defined.
External Authentication Server	Server where EA is installed. Select the EA server from the pull-down list. You must define an EA server before can select the server from the list.
Compression	Compression method to use to compact files before they are transmitted and is negotiated with the client. Compression methods include none or Zlib. The default is none. If you make changes to the compression value, you must restart the adapter before the change is recognized. If you select Zlib, both Zlib and None are supported. **Note:** If you define multiple SFTP adapters on an engine, you must set compression to the same value for each adapter. Unintended results may occur if this parameter is defined differently.
Outbound Port Range	Range of ports to use for the adapter. Valid values include a list of ports separated by commas, such as 1234, 2340, 16570, or a range of ports, such as 16570 -17950.
Perimeter Server Mapping - Inbound Perimeter Server	The perimeter server to use for the inbound connection in the Perimeter Server Mapping - Inbound Perimeter Server field. To use a remote perimeter server, you must define the remote perimeter server before you can associate it with an inbound connection. If you make changes to the inbound perimeter server, you must restart the adapter before the change is recognized.

Field Name	**Description**
Perimeter Server Mapping - Outbound Perimeter Server	The perimeter server to use for the outbound connection in the Perimeter Server Mapping - Outbound Perimeter Server field. To use a remote perimeter server, you must define the remote perimeter server before you can associate it with an outbound connection. If you make changes to the outbound perimeter server, you must restart the adapter before the change is recognized.
Perimeter Server Mapping - External Authentication Perimeter Server	Select the perimeter server to use for the EA connection in the Perimeter Server Mapping - External Authentication Perimeter Server field. To use a remote perimeter server, you must define the remote perimeter server before you can associate it with an EA connection. If you make changes to the EA perimeter server, you must restart the adapter before the change is recognized.

SFTP Adapter Definition - Properties

Use this screen to edit the default values assigned to properties used to determine how the SFTP protocol is implemented. The keys are not displayed. To change a default key value, type the key value as defined in the following table and assign a value to the key.

Field Name	**Description**	
Key	Key identifies properties that you can change for an adapter. Available keys include:	
	◆ max.ps.client.threads	Maximum number of threads in the pool used during a connection with a client. Default is 10.
	◆ max.ps.server.threads	Maximum number of threads in the pool used during a connection with a server. Default is 10.
	◆ sftp_invalidadapter	Identifies how many users can perform an unsuccessful log in attempt before all log in attempts to the adapter fail.
	◆ sftp_rekeycount	Identifies how many packets are transmitted before a key renegotiation is performed. The default is 20.000.
	◆ sftp_threadpoolsize	A tuning parameter that defines the minimum thread pool size.
	◆ sftp_selectorthreads	A tuning parameter to determine how backend threads are managed.
	◆ sftp_maxchannels	Identifies the maximum channels allowed for an SFTP server thread. The default is 3.
	◆ sftp_acceptthreads	Identifies how many threads are available to accept inbound client connections. The default value is 50.
	◆ sftp_connectthreads	Identifies how many threads are available for permanent connect threads. When existing SSH connections make socket connections through port forwarding, these threads manage the asynchronous connection process. The default value is 50.

Field Name	Description	
	◆ sftp_xferthreadpools	Identifies how many threads are available for permanent transfers. This thread asynchronously performs the IO for the socket. The default value is 50.
	◆ sftp_maxauthentications	Identifies how many authentication attempts can be established before the SFTP server closes the connection. This parameter does not lock out a user. The default is 10.
	◆ sftp_maxPacketLength	Identifies the maximum SFTP packet size supported. The default is 65535.
	◆ sftp_jce_enable	Enables only the JCE ciphers. Value values are: true or false. If this property is set to true, only the AES256-CBC, AES192-CBC, AES128-CBC, 3DES-CBC, and BLOWFISH-CBC ciphers and the HMAC-SHA1 and HMAC-MD5 MACs are supported. If you modify the property, you must restart the engine before the change is enabled.
	◆ failover.detection.enabled	Enables failover detection. Valid value=true | false. Default=false.
	◆ failover.detection.mode	Determines the failover detection mode. ◆ continuous—Continuously polls the outbound node and EA server. Default setting. ◆ Standard only—Polls the outbound node and EA server when a connection fails. Outbound and EA perimeter servers are always continuously polled regardless of this setting.
	◆ failover.poll.interval	How many seconds between failover polling. Default=5.
	◆ failover.ea.ping.profile	Identifies a EA profile to use to extend the EA server healthcheck to the backend LDAP server.
	◆ failover.debug	Enables debug logging for failover. Valid values are true | false. Default=false.
	◆ load.balancer.addr	IP address of the load balancer. Define this property to suppress health check connections logging made by the load balancer.
Value	Value identifies the value to assign to a property key. See Key for a list of properties you can modify.	

SFTP Netmap Definition

Use this screen to define the SFTP netmap. Click Inbound Nodes to add connection information for your external trading partner. Click Outbound Nodes to add connection information for your internal SFTP server. Refer to the field definitions in the following table.

Note: You must define a netmap, at least one inbound node, and at least one outbound node before you can save the netmap. If you exit the application before all three elements are defined, you lose the netmap definition.

Field Name	Description
Netmap Name	Netmap Name identifies the name to assign to the netmap you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the netmap you create. Description can be up to 255 characters.
Type	Type identifies the protocol being used as SFTP.
Filter	Filter allows you to view a subset of available inbound or outbound nodes. Use the wildcard characters, * and ?, to identify the nodes to display. Filters are case-sensitive. For example, the filter i* will display inboundnode1 but will not display InboundNode1.

SFTP Netmap Inbound Node Definition - Basic

Use this screen to define the minimum SFTP connection requirements for an external trading partner. Refer to the field definitions in the following table.

Field Name	Description
Inbound Node Name	Inbound Node Name assigns a name to the inbound node connection. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the inbound node you create. Description can be up to 255 characters.

Field Name	Description
Peer Address Pattern	Peer Address Pattern identifies the pattern to allow for the inbound connections to SSP. Valid values are alphanumeric characters and the following special characters: dash(-), underscore(_), colon(:), period(.), dollar sign($), forward slash(/), exclamation mark(!), tilde(~), asterisk(*), open parenthesis '(', close parenthesis ')' semicolon(;), question mark(?), at(@), and comma(,). You can define one of the following patterns: ◆ Wildcard validates incoming DNS names. If a wildcard pattern is provided, SSP performs a reverse lookup on the incoming IP address and the DNS name is compared to the wildcard patterns. Wildcard characters allowed are ? and *. For example, *.a.com allows a connection from b.a.com but not from b.b.com ◆ IP/Subnet validates incoming IP addresses. Use the format *IP-address*/*num-bits* where IP-address identifies an IP address template and num-bits identifies the number of leading bits in the template that are significant. An IP match is performed by comparing the leading num-bits of the incoming IP address against num-bits of the template. For example, 10.20.0.0/16 searches for a match to the first 16 bits. All IP addresses beginning with 10.20.* are allowed. 10.0.0.0/8 searches for a match to the first 8 bits. All addresses beginning with 10.* are allowed. 0.0.0.0/0 allows connections from all IP addresses.
Policy	Policy is a pull-down list of policies you have created. Select the policy you want to associate with the inbound node you are creating. If a policy with the security attributes required has not been created, click ⊕.

SFTP Netmap Inbound Node Definition- Advanced

Use this screen to specify what level to log information on this inbound connection. Refer to the field definitions in the following table.

Field Name	Description
Node Logging Level	Node Logging Level identifies the level of logging to write to the log file for the inbound node. Logging options include: ◆ NONE turns logging off. NONE is the default value. ◆ ERROR writes only error messages to the log. ERROR is the default value. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.

SFTP Netmap Outbound Node Definition - Basic

Use this screen to define the minimum connection requirements for your internal SFTP server. Refer to the field definitions in the following table.

Field Name	Description
Outbound Node Name	Name of an outbound SFTP server in the secure zone. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description to help you identify the outbound node you create. Description can be up to 255 characters.
Primary Destination Address	IP address or host name to use to connect to the SFTP outbound server. Valid values are 1-200 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), colon (:), and underscore (_).
Primary Destination Port	Port to use to connect to the secure SFTP server. Valid values are 1-65535.
Known Host Key Store	Key store you created to store the public keys of GIS servers. Select the known host key store that contains the known host key to use to authenticate the outbound GIS server that you are defining in the outbound node definition.
Known Host Key	Known host keys you added to the key store. Select the known host key from the drop-down list used to authenticate the GIS server to SSP.

SFTP Netmap Outbound Node Definition - Security

Use this screen to define the secure connection requirements for your internal SFTP server. Refer to the field definitions in the following table.

Field Name	Description
Available Cipher Suites	Available Cipher Suites provides a list of ciphers that can be enabled to encrypt data transmitted during a secure SSH connection. Enable at least one cipher. To enable a cipher, highlight the cipher in the Available Cipher Suites dialog and click Add. To enable multiple ciphers, highlight the ciphers to enable and click Add.
Selected Cipher Suites	Selected Cipher Suites identifies the ciphers you have enabled to encrypt data during a secure connection. A cipher suite is negotiated during a secure channel connection between a client and a server. Ciphers are negotiated based on their location in the Selected Ciphers list. To reorder a cipher in the list, highlight the cipher to reorder and click the Up or Down button. To remove a cipher from the selected list, highlight the cipher and click Remove.
Available MAC Suites	Available MAC Suites provides a list of MACs that can be enabled to provide message integrity protection. Enable at least one MAC. To enable a MAC, highlight the MAC in the Available MAC Suites dialog and click Add. To enable multiple MACs, highlight the MACs to enable and click Add.

Field Name	Description
Selected MAC Suites	Selected MAC Suites identifies the MACs you have enabled to provide message integrity protection. MACs are negotiated based on their location in the Selected MAC Suites list. To reorder a MAC in the list, highlight the MAC to reorder and click the Up or Down button. To remove a MAC from the selected list, highlight the cipher and click Remove.
Available Key Exchange	The available key exchanges you can configure for an SFTP outbound node.
Selected Key Exchange	Identifies the key exchanges that have been configured. Key exchanges are used in the order in which they are selected in this field. To reorder a key exchange in the list, highlight the exchange to reorder and click the Up or Down button.

SFTP Netmap Outbound Node Definition - Advanced

Use this screen to define advanced parameters for your internal SFTP server. Refer to the field definitions in the following table.

Field Name	Description
Node Logging Level	Node Logging Level identifies the level of logging to write to the log file for the outbound node. Logging options include: ◆ NONE turns logging off. NONE is the default value. ◆ ERROR writes only error message to the log. ◆ WARN writes error messages and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Destination Service Name	Destination Service Name identifies a destination service accessed by the outbound node. This value can be sent to the EA to use when authenticating a user for access to specific services on the GIS server. The following special characters are not allowed: ! @ # % ^ * ( ) + ? , < > { } [ ] | ; " '
User ID	User ID to use to connect to the outbound server, if the policy is defined to require that the user ID and password from the netmap be used. Valid values are 1-255 alphanumeric characters and certain special characters. The following special characters are not allowed: ! @ # % ^ * ( ) + ? , < > { } [ ] | ; " '
Password	Password to use to connect to the outbound server, if the policy is defined to require that the user ID and password from the netmap be used. Valid values are 1-255 alphanumeric characters and certain special characters. The following special characters are not allowed: , " '
Local User Key Stores	Local User Key Stores identifies the name of the key store where the key to authenticate SSP to the outbound connection is stored. Select the local user key store from a drop-down list.

Field Name	Description
Local User Key	Local User Key identifies the local user key to use to authenticate SSP to the outbound connection. Select the local user key from the drop-down list.
Compression	Compression identifies the compression method to use to compact files before they are transmitted to the outbound node. Compression methods include none or Zlib.
Alternate Destinations - Node	Alternate Destinations Node identifies the node name or IP address and port to use to connect to an alternate SFTP outbound server if a connection to the primary node cannot be made. Up to three alternate destination nodes can be defined for each outbound node. To use different security and advanced definitions for the alternate destination node connection, first configure an outbound node definition for the alternate node in the netmap. Then, open the primary outbound node definition and select the alternate node name in the Alternate Destinations - Node field. To use the security and advanced definition defined in the primary outbound node for an alternate destination node connection, you do not have to define the alternate node in the netmap. Select IP Address/Port and then provide a value in the IP Address and Port fields.
Alternate Destinations - IP Address	Alternate Destinations - IP Address identifies the IP address to use to connect to an alternate destination node, if a connection to the primary node cannot be made. Up to three alternate destination nodes can be defined. Valid values are 1-200 alphanumeric characters and special characters: underscore (_), dash (-), colon (:), and period (.). If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and advanced definition from the primary node is used for the connection.
Alternate Destinations - Port	Alternate Destinations Port identifies the port to use to connect to an alternate destination node if a connection to the primary node cannot be made. Up to three alternate destination nodes can be defined. Valid values are 1-65535. If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and advanced definition from the primary outbound node is used for the connection.

SFTP Policy Configuration - Basic

Use this screen to define how you impose controls to authenticate a trading partner trying to access your SFTP server. Refer to the field definitions in the following table.

Field Name	Description
Policy Name	Policy Name identifies the name to assign to the policy you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the policy you create. Description can be up to 255 characters.
Type	Type identifies the protocol being used as SFTP.

SFTP Policy Configuration - Advanced

Use this tab to specify the type of user authentication to use for inbound access requests. For Certificate Authentication and User Authentication through External Authentication, you must have installed and configured EA. You can also use this screen to map an incoming user ID and password to a different user ID and password to present to the internal server.

Field Name	**Description**
Required Authentication Method	Required Authentication Methods identifies the method to use to authenticate the inbound node connection. Valid values include: ◆ Password - to require that the inbound node password be authenticated against information stored in the local user store or in EA. ◆ Key - to require that the inbound node present a key authenticated against information stored in the local user store or in EA. ◆ Password and Key - to require that the password and the key presented by the inbound node be authenticated against information stored in the local user store or in EA. ◆ Password or Key - to require that the inbound node connection present either a password or a key authenticated against information stored in the local user store.
User Authentication Mechanism - Through External Authentication	Turn on the option to send an incoming user ID and password to EA for validation.
User Authentication Mechanism - User Authentication Profile	If you enabled user authentication through EA, identify the user authentication profile you defined in EA.
User Authentication Mechanism - Key Authentication Profile	If you enabled key authentication through EA, identify the key authentication profile you defined in EA.
User Authentication Mechanism - Through Local User Store	Validates the user ID and password and/or the public key of the inbound node using information defined in the user store. You must add the user to the user store in order to successfully use this method.

Field Name	Description
User Mapping - Internal User ID	User Mapping - Internal User ID is enabled in the policy and determines what user ID and password is used to attach to the SFTP server in the secure environment. User mapping options include: ◆ Pass-Through—Uses the user ID and password supplied by the inbound node to connect to the SFTP server in the secure zone. To successfully connect to the SFTP server, the user ID and password must be defined in the user store at the server. ◆ External Authentication—Uses a user ID and password and/or key from EA to connect to the SFTP server. To successfully connect using this option, the user ID and password must be valid at the target server. ◆ Netmap—Uses the user ID and password and private key defined in the netmap to connect to the SFTP server. To successfully connect using this option, define the user ID and password and key to use to connect to the SFTP server in the outbound node definition. ◆ SSO token from External Authentication—Uses a token from Sterling External Authentication Server to authenticate the user to the server.

Monitoring Field Definitions

Following are the field definitions for the monitoring screens.

Engine Status (All)

Adapters are configured at CM and then pushed to the engine. The Engine Status Page for all Engines provides information on the engines that are configured including when configuration files were pushed to the engine, the version of the configuration file at CM and at the engine. You can also use the engine status page to manually push a configuration to an engine and to stop an engine.

Field Name	Description
Refresh Interval (secs)	How often CM polls the engine to obtain updates and how often the display is refreshed. The Engine Status window is not a real time display. The default polling interval is 30 seconds.
Engine Name	Name of the engine for which information is displayed.
Last Pushed	Date and time when the last configuration file was sent to the engine.
Message	Message returned from the engine.
CM Ver	Version of the configuration file stored at CM.
Engine Ver	Version of the configuration file stored at the engine. If the CM Ver and the Engine Ver do not match, manually push the configuration.

Field Name	Description
Refresh	Click Refresh to manually update the display.
Stop Engine	Select an engine from the list and click Stop Engine to stop the engine.
Push Config	Select an engine from the list and click Push Config to manually push the adapter configuration from CM to the engine.

Engine Detail

The Engine Detail Page provides information on an engine that has been configured including adapters that are configured at the engine, the type of adapter and the port where it is configured. You can also use this tab to stop an adapter.

Field Name	Description
Poll Interval (secs)	Poll Interval (secs) identifies how often to refresh the display.
Refresh	Click Refresh to manually update the display.
Adapter Name	Adapter lists the adapters that are configured at the engine.
Type	Type identifies the type of adapter that is configured at the engine.
Port	Port identifies the port where the adapter is configured.
Message	Message displays the last message that was returned from the engine.
Action	Action allows you to start or stop an adapter. Click Stop to stop the adapter. If the adapter is not running, click Start to start the adapter.

Credentials Field Definitions

Following are the field definitions for the Credentials screens. For more information on configuring certificates, see Configure SSL/TLS Certificates for Trading Partners on the Sterling Secure Proxy Documentation Library.

Trusted Certificate Store Configuration

The Trusted Certificate Stores dialog shows you the name and description of the selected Trusted Certificate Store. The certificates that are in the store are displayed in a table, with a radio button indicating the active certificate. From this screen, you can change the active certificate. You can also add, edit, copy or delete a certificate. Refer to the field definitions in the following table.

Field Name	Description
Trusted Certificate Store Name	Trusted Certificate Store Name identifies the name to assign to the certificate store you create. The name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the certificate store you create. Description can be up to 255 characters.

Trusted Certificate Configuration

Use this screen to update a certificate currently in the trust store or to create a new certificate in the trust store. Refer to the field definitions in the following table.

Field Name	Description
Enable Certificate	Check Enable Certificate to allow the certificate to be used to authorize a secure communications session.
Trusted Certificate Name	Trusted Certificate Name identifies the name to associate with the trusted certificate you are adding to the certificate store. Trusted Certificate Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the certificate you create. Description can be up to 255 characters.
Import from file	Import from file identifies the location and certificate to import to the certificate definition. Use the Browse button to locate the file.
Certificate Data	Certificate Data displays the contents of the certificate that you imported.

System Certificate Store Configuration

The System Certificate Stores dialog shows you the name and description of the selected System Certificate Store. The private keys that are in the store are displayed in a table, with a radio button indicating the active key. From this screen, you can change the active key. You can also add, edit, copy or delete a key. Refer to the field definitions in the following table.

Field Name	Description
System Certificate Store Name	System Certificate Store Name identifies the name to assign to the certificate store you create. The name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the certificate store you create. Description can be up to 255 characters.

System Certificate Configuration

Use this screen to update a software key or HSM key. Click the Software Keys tab to update a software key currently in the trust store or create a new key in the key store. Click the HSM Keys tab to view an HSM key currently in the trust store or change the description of an HSM key.

For additional information on configuring HSM keys, see Store Certificates on a Hardware Security Module (HSM) on the Sterling Secure Proxy Documentation Library.

Software Keys

From the Software Keys tab, you can add or update a software key. Refer to the field definitions in the following table:

Field Name	Description
Enable Certificate	Check Enable Certificate to allow the certificate to be used to authorize a secure communications session.
System Certificate Name	System Certificate Name identifies the name to associate with the system certificate you are adding to the certificate store. The name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the certificate you create. Description can be up to 255 characters.
Import from File	Import from file identifies the location and certificate to import to the certificate definition. Use the Browse button to locate the file.
Certificate Data	Certificate Data displays the contents of the certificate that you imported.

HSM Keys

From the HSM Keys tab, you can view an HSM key currently in the trust store or modify the description of an HSM key. Refer to the field definitions in the following table:

Field Name	Description
Enable Certificate	Check Enable Certificate to allow the certificate to be used to authorize a secure communications session.
System Certificate Name	Name of the HSM certificate you are viewing. This information cannot be edited.
Description	Description to help you identify the certificate you view. Description can be up to 255 characters. You can edit the HSM key description.
Certificate Data	Contents of the certificate that you imported. This information cannot be edited.

Authorized User Key Store Configuration

The Authorized User Key Store dialog shows you the name and description of the selected Authorized User Key Store. The keys that are in the store are displayed in a table with a radio button indicating the active key. For more information on configuring SSH keys, see Manage SSH Keys on the Sterling Secure Proxy Documentation Library.

From this screen, you can change the active key. You can also add, edit, copy or delete a key. Refer to the field definitions in the following table.

Field Name	Description
Authorized User Key Store Name	Authorized User Key Store Name identifies the name to assign to the key store you create. Authorized User Key Store Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the user key store you create. Description can be up to 255 characters.

Authorized User Key Configuration

Use this screen to update a key currently in the Authorizes User Key Store or to create a new key in the store. Refer to the field definitions in the following table.

For more information on configuring SSH keys, see Manage SSH Keys on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Enable Key	Check Enable Key to allow the key to authorize a user.
Authorized User Key Name	Authorized User Key Name identifies the name to associate with the key you are adding to the Key Store. Authorized User Key Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the user key you create. Description can be up to 255 characters.
Import from file	Import from file identifies the location and key to import to the key definition. Use the Browse button to locate the file.
Key Data	Key Data displays the contents of the key that you imported.

Known Host Key Store Configuration

The Know Host Key Store dialog shows you the name and description of the selected Known Host Key Store. The keys that are in the store are displayed in a table with a radio button indicating the active key. From this screen, you can change the active key. You can also add, edit, copy or delete a key. Refer to the field definitions in the following table.

For more information on configuring SSH keys, see Manage SSH Keys on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Known Host Key Store Name	Known Host Key Store Name identifies the name to assign to the key store you create. Authorized User Key Store Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the user key store you create. Description can be up to 255 characters.

Known Host Key Configuration

Use this screen to update a key currently in the Known Host User Key Store or to create a new key in the store. Refer to the field definitions in the following table.

For more information on configuring SSH keys, see Manage SSH Keys on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Enable Key	Check Enable Key to allow the key to be used to authorize a user.
Known Host Key Name	Known Host Key Name identifies the name to associate with the key you are adding to the Key Store. Known Host Key Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the user key you create. Description can be up to 255 characters.
Import from file	Import from file identifies the location and key to import to the key definition. Use the Browse button to locate the file.
Key Data	Key data displays the contents of the key that you imported.

Local User Key Store Configuration

The Local User Key Store dialog shows you the name and description of the selected Local User Key Store. The keys that are in the store are displayed in a table with a radio button indicating the active key. From this screen, you can change the active key. You can also add, edit, copy or delete a key. Refer to the field definitions in the following table.

Field Name	Description
Local User Key Store Name	Local User Key Store Name identifies the name to assign to the key store you create to store keys used to authenticate SSP to the inbound connection. Local User Key Store Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the user key store you create. Description can be up to 255 characters.

Local User Key Configuration

Use this screen to update a key currently in the Local User Key Store or to create a new key in the store. Refer to the field definitions in the following table.

Field Name	Description
Enable Key	Check Enable Key to allow the key to be used to authorize a user.
Local User Key Name	Local User Key Name identifies the name to assign to the key you create. This field can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the user key you create. Description can be up to 255 characters.
Password	Password to use to access the key. Password can be up to 255 alphanumeric characters and does not allow comma (,), double quotes (“), or single quotes (‘).
Confirm Password	Confirm Password requires that you retype the password value.
Import From File	Import from File identifies the location and key to import to the key definition. Use the Browse button to locate the file.
Key Data	Key Data displays the contents of the key that you imported.
Routing Name	The value that EA will return to map to this key.

Local Host Key Store Configuration

The Local Host Key Store dialog shows you the name and description of the selected Local Host Key Store. The keys that are in the store are displayed in a table with a radio button indicating the active key. From this screen, you can change the active key. You can also add, edit, copy or delete a key. Refer to the field definitions in the following table.

Field Name	Description
Local Host Key Store Name	Local Host Key Store Name identifies the name to assign to the key store you create. Local Host Key Store Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the key store you create. Description can be up to 255 characters.

Local Host Key Configuration

Use this screen to update a key currently in the Local Host Key Store or to create a new key in the store. Refer to the field definitions in the following table.

Field Name	Description
Enable Key	Check Enable Key to allow the key to be used to authorize a user.
Local Host Key Name	Local Host Key Name identifies the name to associate with the key you are adding to the Key Store. Local Host Key Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the user key you create. Description can be up to 255 characters.
Password	Password to use to access the key. Password can be up to 255 alphanumeric characters and does not allow comma (,), double quotes (“), or single quotes (‘).
Confirm Password	Confirm Password requires that you retype the password value.
Import From File	Import From File identifies the location and key to import to the key definition. Use the Browse button to locate the file.
Key Data	Key data displays the contents of the key that you imported.

User Store Configuration

The User Store is a file that contains user accounts. A default user store called defUserStore is available with the product. If desired, you can create additional user stores. The user account is locked if the user fails to type the correct login credentials, the number of times defined in the user lockout threshold. The default value is 3. If an error occurs when connecting to a server, such as EA, this is not considered a login credentials error.

Use this screen to add a user store or modify the default user store. Refer to the field definitions in the following table.

Field Name	Description
User Store Name	User Store Name identifies the name to assign to the user store you create. User Store Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_). A default user store is provided called defUserStore.
Description	Description assigns a description to help you identify the user store you create. Description can be up to 255 characters.
User Lockout Duration	User Lockout Duration identifies how long a user is unable to access SSP, after too many incorrect logon attempts. The default value is 300 seconds.
User Lockout Threshold	User Lockout Threshold identifies how many unsuccessful logon attempts are allowed before a user is locked out.

User Configuration - Basic

The User Configuration allows you to define users who are allowed to access Sterling Secure Proxy. Use this screen to define the basic requirements for user access to SSP. Refer to the field definitions in the following table.

Field Name	Description
User Name	Name to assign to the user you configure. User Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the user you create. Description can be up to 255 characters.
Password	Password that the user must provide to access SSP. It can be up to 28 alphanumeric characters and cannot include commas (,), double quotes (“), or single quotes (‘). The length of the password required is defined in the password policy configuration.
Confirm Password	Retype the password value required by the user.
Password Policy ID	Password policy to associate with the user you are configuring. You must configure a password policy before you can associate it with a user. Select a Password Policy ID from the pull-down list.
User Active	Identifies that the user can communicate with SSP. Disable this option to prevent a user from accessing SSP.
First Name	First name of the user. Optional.
Last Name.	Last Name of the user. Optional.
Email Address	Email address of the user. Optional.
Pager	Pager number for the user. Optional.
Manager ID	Manager information for the user.

User Configuration - Advanced

The User Configuration Advanced tab allows you to associate SSH keys with a user definition. Refer to the field definitions in the following table.

Field Name	Description
SSH Authorized User Key Store	Select an SSH Authorized User Key Store to associate with the user from the drop-down list.
SSH Authorized User Key	Select the SSH Authorized User Keys to associate with the user from the drop-down list.

Advanced Menu Field Definitions

Following are the field definitions for the Advanced menu screens.

Perimeter Servers Field Definitions

From the Advanced menu, you can configure remote perimeter servers that you want to use with a Sterling Secure Proxy engine. Identify if the perimeter server is installed in a more secure zone or a less secure zone and then configure the perimeter server. For additional information on configuring perimeter servers, see Configure Perimeter Servers on the Sterling Secure Proxy Documentation Library.

Less Secure Zone PS Configuration - Basic

Use this screen to configure a remote perimeter server in a less secure zone. Refer to the field definitions in the following table.

Field Name	Description
Perimeter Server Name	Name to assign to the perimeter server you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description to help you identify the perimeter server you create. Description can be up to 255 characters.
Perimeter Server Host	DNS name or TCP/IP address where the DMZ perimeter server is installed.
Perimeter Server Port	Port number that the DMZ perimeter server monitors for connections. This is the port number you specified when installing your perimeter server in the DMZ.

Less Secure Zone PS Configuration - Advanced

Use this screen to edit advanced properties associated with a remote perimeter server installed in a less secure zone. Refer to the field definitions in the following table.

Field Name	**Description**
Perimeter Server Outbound Low Water Mark	Lowest outbound connection buffer size. This is the low water mark. The default is 150 KB. When SSP sends data to a trading partner faster than the trading partner can receive it, the excess data accumulates inside perimeter services in the outbound connection buffer. When the buffer size reaches the High Outbound Connection value, perimeter services stops sending data through that connection until enough of the excess data has been sent that the outbound connection buffer size drops to the Low Outbound Connection value. For example, if you set the High Outbound Connection value to 500 KB and the Low Outbound Connection value to 250 KB, perimeter services will stop sending data when the outbound connection buffer size reaches 500 KB and will resume sending data when the outbound connection buffer size drops to 250 KB.
Perimeter Server Outbound High Watermark	Highest outbound connection buffer size. This is the high water mark. The default is 250 KB. When SSP sends data to a trading partner faster than the trading partner can receive it, the excess data accumulates inside perimeter services in the outbound connection buffer. When the buffer size reaches the Perimeter Server High Outbound Connection value, perimeter services stops sending data through that connection until enough of the excess data has been sent that the outbound connection buffer size drops to the Perimeter Server Low Outbound Connection value. For example, if you set the Perimeter Server High Outbound Connection value to 500 KB and the Perimeter Server Low Outbound Connection value to 250 KB, perimeter services will stop sending data when the outbound connection buffer size reaches 500 KB and will resume sending data when the outbound connection buffer size drops to 250 KB.
Perimeter Server Inbound Low Water Mark	Lowest inbound connection buffer size. This is the low watermark. The default is 150 KB. When a trading partner sends data faster than SSP can process it, the excess data accumulates inside perimeter services in the inbound connection buffer. When the buffer size reaches the High Inbound Connection value, perimeter services stops receiving data for that connection until enough of the excess data has been processed that the inbound connection buffer size drops to the Low Inbound Connection value. For example, if you set the High Inbound Connection value to 500 KB and the Low Inbound Connection value to 250 KB, perimeter services will stop receiving data when the inbound connection buffer size reaches 500 KB and will resume receiving data when the inbound connection buffer size drops to 250 KB.

Field Name	**Description**
Perimeter Server Inbound High Water Mark	Highest inbound connection buffer size. This is the high watermark. The default is 250 KB. When a trading partner sends data faster than SSP can process it, the excess data accumulates inside perimeter services in the inbound connection buffer. When the buffer size reaches the Perimeter Server High Inbound Connection value, perimeter services stops receiving data for that connection until enough of the excess data has been processed that the inbound connection buffer size drops to the Perimeter Server Low Inbound Connection value. For example, if you set the Perimeter Server High Inbound Connection value to 500 KB and the Perimeter Server Low Inbound Connection value to 250 KB, perimeter services will stop receiving data when the inbound connection buffer size reaches 500 KB and will resume receiving data when the inbound connection buffer size drops to 250 KB.
Proxy Local Interface	Network interface SSP uses to connect to the perimeter server. The default is *, which allows the operating system to make the selection. You can specify any IP address or DNS name of an interface which exists on this machine.
Proxy Local Port	Port number to use for the local end of the socket to the perimeter server. The default is 0, which allows the operating system to select any free port. Valid values are 1–65,535.
Perform DNS Resolution	Place where DNS resolution occurs. The default is At Local Host. ◆ At Local Host — The DNS name is resolved at the local host where SSP is installed. ◆ At Perimeter Server Host — The DNS name is resolved at the perimeter server host.

More Secure Zone PS Configuration - Basic

Use this screen to configure a remote perimeter server in a more secure zone. Refer to the field definitions in the following table.

Field Name	**Description**
Perimeter Server Name	Perimeter Server Name identifies the name to assign to the perimeter server you create. Valid values are 1–150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description for the perimeter server to help identify the perimeter server you create. Description can be up to 255 characters.
Proxy Local Listen Port	Port number that the perimeter server monitors for connections. This is the port number you specified when installing your perimeter server. Valid values are 1–65,535.

More Secure Zone PS Configuration - Advanced

Use this screen to edit the default properties associated with a perimeter server installed in a more secure zone. Refer to the field definitions in the following table.

Field Name	Description
Perimeter Server Outbound Low Water Mark	Lowest outbound connection buffer size. This is the low water mark. The default is 150 KB. When SSP sends data to a trading partner faster than the trading partner can receive it, the excess data accumulates inside perimeter services in the outbound connection buffer. When the buffer size reaches the High Outbound Connection value, perimeter services stops sending data through that connection until enough of the excess data has been sent that the outbound connection buffer size drops to the Low Outbound Connection value. For example, if you set the High Outbound Connection value to 500 KB and the Low Outbound Connection value to 250 KB, perimeter services will stop sending data when the outbound connection buffer size reaches 500 KB and will resume sending data when the outbound connection buffer size drops to 250 KB.
Perimeter Server Outbound High Watermark	Highest outbound connection buffer size. This is the high water mark. The default is 250 KB. When SSP sends data to a trading partner faster than the trading partner can receive it, the excess data accumulates inside perimeter services in the outbound connection buffer. When the buffer size reaches the Perimeter Server High Outbound Connection value, perimeter services stops sending data through that connection until enough of the excess data has been sent that the outbound connection buffer size drops to the Perimeter Server Low Outbound Connection value. For example, if you set the Perimeter Server High Outbound Connection value to 500 KB and the Perimeter Server Low Outbound Connection value to 250 KB, perimeter services will stop sending data when the outbound connection buffer size reaches 500 KB and will resume sending data when the outbound connection buffer size drops to 250 KB.
Perimeter Server Inbound Low Water Mark	The lowest inbound connection buffer size. This is the low watermark. The default is 150 KB. When a trading partner sends data faster than SSP can process it, the excess data accumulates inside perimeter services in the inbound connection buffer. When the buffer size reaches the High Inbound Connection value, perimeter services stops receiving data for that connection until enough of the excess data has been processed that the inbound connection buffer size drops to the Low Inbound Connection value. For example, if you set the High Inbound Connection value to 500 KB and the Low Inbound Connection value to 250 KB, perimeter services will stop receiving data when the inbound connection buffer size reaches 500 KB and will resume receiving data when the inbound connection buffer size drops to 250 KB.

Field Name	Description
Perimeter Server Inbound High Watermark	The highest inbound connection buffer size. This is the high watermark. The default is 250 KB. When a trading partner sends data faster than SSP can process it, the excess data accumulates inside perimeter services in the inbound connection buffer. When the buffer size reaches the Perimeter Server High Inbound Connection value, perimeter services stops receiving data for that connection until enough of the excess data has been processed that the inbound connection buffer size drops to the Perimeter Server Low Inbound Connection value. For example, if you set the Perimeter Server High Inbound Connection value to 500 KB and the Perimeter Server Low Inbound Connection value to 250 KB, perimeter services will stop receiving data when the inbound connection buffer size reaches 500 KB and will resume receiving data when the inbound connection buffer size drops to 250 KB.
Proxy Local Interface	The network interface is used by SSP to listen for connections form the perimeter server. The default is *, which means SSP will listen on all available interfaces. You can specify any IP address or DNS name of an interface which exists on this machine.
Perform DNS Resolution	Perform DNS Resolution identifies where the DNS resolution occurs. The default is At Local Host. ◆ At Local Host—DNS name is resolved at the local host where SSP is installed ◆ At Perimeter Server Host—DNS name is resolved at the perimeter server host.

EA Server Configuration Field Definitions

To use EA to authenticate users or certificates, you must install an EA server and configure the EA server in Sterling Secure Proxy. Refer to the field definitions in the following table.

For additional information on configuring perimeter servers, see Configure SSP for External Authentication on the Sterling Secure Proxy Documentation Library.

SSP EA Server Configuration - Basic

Use this screen to configure an EA server. Refer to the field definitions in the following table.

Field Name	Description
EA Server Name	Name to assign to the EA server definition you create. Valid values are 1–150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description to help you identify the EA server definition you create. Description can be up to 255 characters.

Field Name	Description
EA Server Address	IP address or host name to use to connect to the EA server. Valid values are 1-200 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), colon (:), and underscore (_).
EA Server Port	Port number to use to connect to the EA server. Valid values include 1-65535.
Outbound Port Range	Range of ports to use to connect to the EA server. Valid values include a list of ports that are allowed with each value separated by a comma such as 1234, 2340, 16570 or a range of ports allowed, such as 16570 -17950.

SSP EA Server Configuration - Security

Use this screen to define secure connection requirements for an EA server definition. Refer to the field definitions in the following table.

Field Name	Description
Use Secure Connection	Enable Use Secure Connection to turn on the use of SSL/TLS to provide secure communications with transport protocols and to ensure that data is secured as it is transmitted across a single socket.
Security Setting	Security protocol allowed for connections to the EA server. Options include: ◆ SSL—select this option to require SSL for the connection ◆ TLS—select this option to require TLS for the connection
Trust Store	Location where the system and CA certificates are stored. System and CA certificates are used during a secure connection to verify that a certificate received from a server is signed by a trusted source.
CA /Trusted Certificates	The trusted certificate to use to authenticate the certificate presented by EA. You select a CA certificate or trusted root from the list of certificates stored in the trust store you selected in the Trust Store field. When EA presents a certificate to establish a secure connection, the trusted root certificate, located at the SSP server, must match or be the entity who signed the certificate presented by EA during the SSL handshake.
Key Store	Location where the keys and system certificates you want to use are stored.
Key/System Certificate	Certificate presented by SSP to the node to authenticate itself during the SSL handshake. Select the certificate to use for the node from the list that contains the certificates stored in the key store you selected in the Key Store field.
Cipher Suites	List of ciphers that can be enabled to encrypt data transmitted during a secure SSL or TLS connection between SSP and an EA server. Enable at least one cipher.

SSP EA Server Configuration - Advanced

Use the advanced tab for an EA server definition to allow failover support for an EA server. If failover support is configured and a connection to the primary EA server cannot be configured, SSP connects to the first alternate server. If a connection to the first alternate EA server cannot be made, SSP connects to the second alternate server. Refer to the field definitions in the following table.

Note: If a connection to the primary EA server is established but the connection is closed because a secure handshake could not be performed, SSP does not attempt a failover connection. This failure is not a connection failure.

Field Name	Description
Alternate EA Server	EA server name to use to connect to an alternate EA server, if a connection to the primary EA server cannot be made. Up to three alternate EA servers can be defined for each EA server. The servers are used in sequence 1, 2, 3. You must first configure each EA server. Then you can identify alternate EA servers to use if an EA server is not available by selecting a server definition from the list.

Connect:Direct Step Injection Configuration

Use this screen to create a step injection function. Use the Step Injection Advanced tab to define the functions implemented with the step injection you define.

Step injection allows you to insert Connect:Direct Process statements into the communications session with the SNODE independent of the PNODE Process statements. These injected statements can provide real-time notification of file delivery, invoke applications, submit operating system jobs, and submit other Connect:Direct Processes, all without the need to provide an exit program on the SNODE or without changing the PNODE Process. The PNODE receives no indication that these steps have executed. However, execution results of these steps are logged in the statistics file of the SNODE.

Connect:Direct Step Injection Configuration - Basic

Use this tab to create a step injection function.

Connect:Direct Step Injection Configuration - Basic fields are defined in the following table.

Field Name	Description
Step Injection Name	Step Injection Name identifies the name to assign to the step injection policy you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description assigns a description to help you identify the step injection function you create. Description can be up to 255 characters.

Connect:Direct Step Injection - Advanced

Use this tab to define the functions implemented the step injection.

Connect:Direct Step Injection Configuration - Advanced fields are defined in the following table.

Field Name	Description
Copy on success	Enable Copy on success to copy information to the SNODE at the end of a successful step. Information that can be copied includes certificate information, metadata returned by Sterling External Authentication Server associated with the entity represented by the certificate, and Process information such as a file name or step name.
Copy identifying information	If you enable Copy on success, identify what information to copy to the SNODE. Options include: ◆ Copy All Information to copy all information about the session to the SNODE ◆ Copy Certificate Information to copy only certificate information to the SNODE ◆ Copy Session Information to copy only session information to the SNODE
Session information output file	Session information output file identifies the name of the file where information about the successful session is written.
Tcp timeout for copy	Tcp timeout for copy identifies the number of seconds to wait for a TCP/IP request or response before ending the session.
Execute on success	Enable this option to execute an operating system command, program, or Submit Connect:Direct Process on the SNODE at the end of a successful step.
Step selection	If you enable Execute on success, identify the type of step to execute: Runtask, Runjob, or Submit.
Step parameter	Step parameter provides a place to type the step parameters. Refer to the Connect:Direct Process Information on the Sterling Commerce Customer Center for information on step parameters.
Tcp timeout for step	Tcp timeout for step identifies the number of seconds to wait for a TCP/IP request or response before ending the session.
Copy on failure	Enable this option to copy session-specific data to the SNODE at the end of a failed step.
Copy identifying information	If you enable Copy on failure, identify the information to copy to the SNODE. Options include: ◆ Copy All Information—to copy all information about the session to the SNODE ◆ Copy Certificate Information—to copy only certificate information to the SNODE ◆ Copy Session Information—to copy only session information to the SNODE
Session information output file	Session information output file identifies the name of the file where information about the failed session is to be written.
Tcp timeout for copy	Tcp timeout for copy identifies the number of seconds to wait for a TCP/IP request or response before ending the session.
Execute on failure	Enable Execute on failure to execute an operating system command, program, or Submit Connect:Direct Process on the SNODE at the end of a failed step.

Field Name	Description
Step selection	If you enable Execute on failure, identify the type of step to execute: Runtask, Runjob, or Submit.
Step parameter	Step parameter provides a place to type the step parameters. Refer to the Connect:Direct process Guide for information on step parameters.
Tcp timeout for step	Tcp timeout for step identifies the number of seconds to wait for a TCP/IP request or response before ending the session.

Password Policy Field Definitions

The Password Policy tab is used to define password policies, a set of security decisions that you make and apply to different user accounts according to security policies in your company. After you create a password policy, you can associate it with a user definition.

For additional information, refer to Manage User Accounts on the Sterling Secure Proxy Documentation Library.

Password Policy Field Definitions

Following are the password policy field definitions.

Field	Description
Password Policy Name	Name that displays in the user interface when a reference is made to the password policy.
Description	Description to help you identify the password policy you create. Description can be up to 255 characters.
Days Valid	Number of days that a user password is valid. The user is prompted to change the password when this time period expires. The default is 0, which means the password never expires. You can change this number to any number you want. There is no maximum value. The expiration count down starts the first time a user logs in to SSP after a password is assigned to the user account.
Minimum Length	Minimum length that the password must be. This field is required. Valid values are any numerals. The default value is 6. If no policy is applied, SSP enforces a minimum length of 6.
Maximum Length	How long the password can be.This field is required. Valid values are any numerals. This number must be set to at least the same number as the minimum length. The default value is 28
Kept in History	How many passwords to keep in the PWD_HISTORY table in the file for a user. Values store in history cannot be used when defining a new password value. After this number of passwords is exceeded, the oldest password is removed from the table and can be re-used by the user. The default value is 5.
Must contain special characters	The password must contain at least one special character, such as numeral, capital letter, !, @, #, $, %, ^, &, or *.

Single Sign-On Definitions

Following are definitions of the single sign-on fields in SSP for connections between SSP and Sterling File Gateway. For more information, see Configure single sign-on connection for HTTP on the Sterling Secure Proxy Documentation Library.

SSO Configuration - Basic

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

Field Name	Description
Name	Name of the SSO configuration.
Description	Description of the SSO configuration.
Fully Qualified Host name the Trading Partner connects to	External-facing or client-facing fully qualified DNS name the trading partner connects to.
SSO Cookie Domain	Domain that the trading partner connects to. The browser sends the cookie with requests which match this domain. If more than one server need to share this cookie, enter the domain that is common to these servers.

SSO Configuration - Advanced

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

Field Name	Description
Default Application URL	Defines the server application URL. To support the myFilegateway application, set this field to myfilegateway.
SSO Cookie Secure Flag	When the secure flag of the cookie is enabled, the browser will only send it over a secure channel. Default is enabled.

SSO Configuration - Logon Portal

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

Field Name	Description
Front End SSO Token Cookie Name	Cookie name used by SSP when communicating with the client. If an external authentication SSO server is used, this name must match the cookie name used by the external SSO authentication server.
Login Page	Name of the page that is displayed when a trading partner logs in and single sign-on is configured. Default is login.html.
Change Password Page	Name of the page that is used to change a trading partner's password. Default is changepw.html.
Welcome Page	Name of the page that is displayed after a trading partner logs in. Default is welcome.html.
Logout Page	Name of the page that is displayed when a trading partner logs out. Default is logout.html.
Login Directory ID	Directory where the HTML files are stored. This directory is created below the installation directory. Default is Signon.
Login Page Charset	Character encoding sent as part of the content-type header to the browser with the login page. Default is UTF-8.
Login Page Media Type	Media type value sent to the browser in the content-type header with the login page. Default is text/html.
External Application Login URL	External URL where SSP redirects any HTTP requests, when a third-party application is used to create the token.
Back End SSO User Header Name	HTTP header used to send the user ID to the SFG server application. Default = SM_USER.
Back End SSO Token Cookie Name	Cookie name used to send the token to SFG or the application defined in the outbound node. The default is the same as the name of the front-end cookie name.

SSO Configuration - Properties

Use this tab to define properties for a single sign-on session. Not all properties are automatically displayed. To change a default key value, type the key value as defined in the following table and assign a value to the key.

Field Name	Description
login.form.password.field.name	Field name of the password on the single sign-on login page. Default=password.
login.form.userid.field.name	Field name of the user ID on the on the single sign-on login page. Default is user.
sso.login.command	Field name of the log in command. Default=login.

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

System Menu Field Definitions

Following are the field definitions for the System menu.

CM Trusted Certificate Store Configuration

The CM Trusted Certificate Stores dialog shows you the name and description of the CM Trusted Certificate Store. The certificates that are in the store are displayed in a table. These certificates are used to authenticate an SSL or TLS secure communications session with the web server and the engine. From this screen, you can view the active certificate. Refer to the field definitions in the following table.

For additional information on configuring certificates, see Configure SSL/TLS Certificates for Trading Partners on the Sterling Secure Proxy Documentation Library.

Field Name	Description
CM Trusted Certificate Store Name	Name of the certificate store you are viewing.
Description	Description to help you identify the certificate store you create. Description can be up to 255 characters.

CM Trusted Certificate Configuration

Use this screen to view a certificate currently in the trust store. Refer to the field definitions in the following table.

For additional information on configuring certificates, see Configure SSL/TLS Certificates for Trading Partners on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Enable Certificate	This field is disabled.
CM Trusted Certificate Name	Name of the trusted certificate you are viewing.
Description	Description to help you identify the certificate you are viewing.
Import from file	This field is disabled.
Certificate Data	Contents of the certificate.

CM System Certificate Store Configuration

The CM System Certificate Stores dialog shows you the name and description of the selected System Certificate Store. The private keys that are in the store are displayed in a table. From this screen, you can change the active key. You can also add, edit, copy or delete a key. Refer to the field definitions in the following table.

For additional information on configuring certificates, see Configure SSL/TLS Certificates for Trading Partners on the Sterling Secure Proxy Documentation Library.

Field Name	Description
CM System Certificate Store Name	Name of the certificate store you are viewing.
Description	Description to help you identify the certificate store you are viewing.

CM System Certificate Configuration

Use this screen to view a key currently in the trust store. Refer to the field definitions in the following table.

For additional information on configuring certificates, see Configure SSL/TLS Certificates for Trading Partners on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Enable Certificate	This field is disabled.
CM System Certificate Name	Name associated with the system certificate you are viewing in the certificate store.
Description	Description to identify the certificate you are viewing.

Field Name	Description
Password	This field is disabled.
Confirm Password	This field is disabled.
Import From File	This field is disabled.
Certificate Data	Contents of the certificate that you are viewing.

CM User Configuration

The CM User Configuration tab is used to create accounts for users who will access CM. You can assign roles to users based on how they will use CM. The operator role has read-only access to CM. The administrator role has full access to all of the configuration options available in CM.

Refer to Manage Configuration Manager on the Sterling Secure Proxy Documentation Library.

Field Name	Description
User Name	User you define to allow access to CM. User Name can be up to 150 characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description to help you identify the CM user you create. Up to 255 characters.
Password	Password required by the user to access CM. Up to 255 alphanumeric characters and does not allow comma (,), double quotes (“), or single quotes (‘).
Confirm Password	Retype the password value.
User role	Role allowed by the user you create. The Operator role has read-only access to CM; whereas, the Admin role has full access to create and edit all of the configuration options available in CM. Admin is the default user role value
Policy ID	Password policy to associate with the user you configure. Configure a password policy before you can associate it with a user. Select a Password Policy ID from the pull-down list.
Requires change	Requires that the user change the default password after the initial log in. A prompts is displayed to the user.

System Settings - Listeners

System Settings - Listeners identifies the IP address and ports that CM uses to listen for secure connections. Refer to Manage Configuration Manager on the Sterling Secure Proxy Documentation Library.

Field Name	Description
IPAddress	IP address at CM to use to listen for secure connections.

Field Name	Description
Port	Port at CM to use to listen for secure connections.

System Settings - Security

System Settings - Security identifies the security information used during a secure connection from CM to the engine. Setting up the internal certificate, using this screen, does not completely configure internal certificates. We recommend that you use the scripts provided to set up the internal certificates.

For additional information on configuring certificates, refer to Configure SSL/TLS Certificates for Trading Partners on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Protocol	Identifies that TLS is used to secure the connection. TLS is the only protocol that can be used for the connection between CM and the web server. This is a read-only field.
Key store file	Location where the keys and system certificates you want to use are stored.
Key/System Certificate	Certificate presented by the web server to CM to authenticate itself during the TLS handshake. Select the certificate to use from the list of key or system certificates stored in the key store selected in the Key Store field.
Cipher Suites	List of ciphers that can be enabled to encrypt data transmitted during a secure connection between CM and the web server. Enable at least one cipher.

System Settings - Globals

System Settings - Global identifies the system settings for sessions between CM and the web server. Use this panel to modify the default settings. For additional information, refer to Manage Configuration Manager on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Logging level	Level of logging to write to the log file for CM. Logging options include: ◆ NONE turns logging off. ◆ ERROR writes only error messages to the log. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. INFO is the default value. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.

Field Name	Description
Listen backlog	Number of client connections allowed in a queue before connections are refused. Valid values range from 0 to 2147483.
Accept timeout	Number of seconds that the accepter listens before a timeout occurs. The default is 30. Valid values range from 0 to 2147483.
SSL handshake timeout	How many seconds are allowed for an SSL handshake. If the SSL handshake does not occur during this time, the session is terminated. This parameter ensures that a connecting client authenticates within a fixed amount of time. The default is 30 seconds. Valid values range from 0 to 2147483.
Connect timeout	How many seconds are allowed for an outbound connection from the server before a timeout occurs, if the connection is not accepted. Valid values range from 0 to 2147483.
Read timeout	How many seconds elapse before a read operation times out, if unsuccessful. Valid values range from 0 to 2147483.

System Settings - Lock Manager

Lock Manager allows you to unlock CM components.For additional information, see Manage Configuration Manager on the Sterling Secure Proxy Documentation Library.

Field Name	Description
show	A drop-down list of all components that you can select and unlock. Available options include: ◆ All Objects—select All Objects to view all objects that are locked. ◆ Engines—select Engines to view all engines that are locked. ◆ Adapters—select Adapters to view locked adapters. You can filter this list and select Connect:Direct, HTTP, FTP, or SFTP to view only locked adapters of a specific protocol ◆ Netmaps—select Netmaps to view locked netmap. You can filter this list and select Connect:Direct, HTTP, FTP, or SFTP to view only locked netmaps of a specific protocol ◆ Policies—select Policies to view locked policies. You can filter this list and select Connect:Direct, HTTP, FTP, or SFTP to view only locked policies of a specific protocol ◆ EA Servers—select EA Servers to view all EA servers that are locked. ◆ Perimeter Servers—select Perimeter Servers to view all perimeter servers that are locked. ◆ Password Policies—select Password Policies to view all password policies that are locked. ◆ Step Injections—select Step Injections to view all step injection objects that are locked. ◆ Key Stores—select Key Stores to view all key stores that are locked. ◆ User Stores—select User Stores to view all user stores that are locked. ◆ CM Users—select CM Users to view all CM users whose account is locked.
Name	Name of the object that is locked.
Object	Type of object that is locked.
Protocol	Protocol of the locked object.
Locked By	The user ID that locked the object.
Lock Time	When the object was locked.
Expiration	When the lock expires.

Single Sign-On Tokens Field Definitions in EA

This section describes field definitions that support single sign-on connections between SSP and Sterling File Gateway. For field definitions of the standard EA dialogs, refer to the Sterling External Authentication Server Documentation Library.

System Settings - SSO Tokens

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

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

PeSIT Field Definitions

Following are definitions of the fields contained on the PeSIT protocol dialogs in SSP.

PeSIT Adapter Configuration - Basic

Use this screen to specify system-level communications information for PeSIT/Connect:Express connections to and from SSP. Before you can click the Advanced or Properties tabs, you must specify Adapter Name and Listen Port and select a netmap to associate with the adapter.

Refer to the field definitions in the following table. For more information, refer to PeSIT Proxy Configuration on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Name	Name to assign to the adapter you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description to help you identify the adapter you create. Description can be up to 255 characters.
Type	Protocol being used: PeSIT.

Field Name	Description
Listen Port	Port number to use to listen for inbound connections. Valid values include 1-65535.
Netmap	Netmap to associate with adapter.
Routing Type	Select the Routing Type to identify how inbound connections are routed to the server in the trusted zone. Routing options include: ◆ Standard (Default)—select Standard to direct connections to the outbound node specified in the SNODE Netmap Entry field. ◆ Certificate-based—select this option to use the certificate presented by the inbound PNODE to determine which outbound SNODE to connect to. Certificate-based routing uses External Authentication and requires that you configure External Authentication server. ◆ PNODE-specified—select this option to route outbound connections based on information provided by the inbound PNODE. ◆ PNODE-specified, then Standard—select this option to route outbound connections based first on information provided by the inbound PNODE. If the routing information presented by the PNODE is not configured in the netmap, the connection is routed to the outbound node specified in the SNODE Netmap Entry field.
SNODE Netmap Entry	Name of the Connect:Express server where the node connections are routed, after connecting to SSP. Select this value from a pull-down list. **Note:** Only nodes defined with an IP address are outbound nodes, and are shown in the list.
Engine	Engine identifies the SSP server in the DMZ where the adapter will listen for inbound connections to be routed to the outbound node. Select an engine from the list. You must define an engine before you can create an adapter.
Startup Mode	Identifies how the adapter is started. **auto** (Default) starts the adapter as soon as the configuration is pushed to the engine. **manual** requires that the adapter be manually started.

PeSIT Adapter Configuration - Advanced

Use this screen to specify additional communications information, and to specify the perimeter servers to use for this adapter. Refer to the field definitions in the following table. For more information, refer to PeSIT Proxy Configuration on the Sterling Secure Proxy Documentation Library.

Field Name	Description
Logging Level	Level of logging to write to the log file for the adapter. Logging options include: ◆ ERROR writes only error messages to the log. ERROR is the default value. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Maximum Sessions	Maximum number of concurrent sessions that the adapter allows. The default is 20.
Session Timeout	Amount of time allowed, in minutes, between transmissions of TCP packets before a session is terminated. The default is 3 minutes.
Http Ping Response	Response sent when an HTTP GET is received on the listen port. Provide this value to send a health check response to a third-party IP load balancer, such as Big IP. To test the response, ping the URL and port of the engine. For example, if you configure an adapter on port 13640 and you want to get an HTTP 1.0 response, send a ping to http://ProxyServerURL:13640/. The value you supplied in the Http Ping Response field is returned. If you provide a value in this field, the value is displayed in a browser window. You can provide HTML syntax and text values.
Outbound Port Range	Range of ports to use for the adapter. Valid values include a list of ports that are allowed with each value separated by a comma such as 1234, 2340, 16570, or a range of ports allowed, such as 16570-17950.
External Authentication Server	Sterling External Authentication Server to use. Select the server from the pull-down list. You must define an EA server before you can select the server from the list.
Perimeter Server Mapping - Inbound Perimeter Server	Select the perimeter server to use for the inbound connection. To use a remote perimeter server, you must define the remote perimeter server before you can associate it with an inbound connection.
Perimeter Server Mapping - Outbound Perimeter Server	Select the perimeter server to use for the outbound connection. To use a remote perimeter server, you must define the it before you can associate it with an outbound connection.
Perimeter Server Mapping - External Authentication Perimeter Server	Select the perimeter server to use for the EA connection. To use a remote perimeter server, you must define it before you can associate it with an Sterling External Authentication Server connection.
Inbound and outbound sessions can have different levels of encryption	Enable this field to allow the connections from the PNODE to SSP and from SSP to the SNODE to use different encryption methods. Set this option to enable a secure connection on the inbound session but use a non-secure connection on the outbound session or to use different protocols on the inbound and the outbound connection.

PeSIT Adapter Definition - Properties

Edit properties to change how the PeSIT protocol is implemented. The SsslHeaderBytesUsed key is used for specific SSL links. Change or add the key when instructed to do so by Sterling support. Valid values are false or true.For more information, refer to PeSIT Proxy Configuration on the Sterling Secure Proxy Documentation Library.

PeSIT Netmap Definition

Use the netmap definition to define secure connection requirements for the node. Refer to the field definitions in the following table.

Field Name	Description
Netmap Name	Name to assign to the netmap you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description to help you identify the netmap you create. Description can be up to 255 characters.
Type	Protocol being used: HTTP, FTP, SFTP, PeSIT, or Connect:Direct.
Filter	Filter allows you to view a subset of available nodes. Use the wildcard characters, * and ?, to identify the nodes to display. Filters are case-sensitive. For example, the filter n* will display node1 but will not display Node1.
Move Up Move Down	Use Move Up and move Down to arrange the node list from more specific to less Specific IP address if you are mixing IP addresses and Patterns

PeSIT Netmap Node Definition - Basic

Define connection parameters for a PeSIT Connect:Express node. Define a node name, address, and port before you save the node definition. Refer to the field definitions in the following table.

Field Name	Description
Node Name	Name of the Connect:Express/PeSIT node you are configuring in PeSIT proxy. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Routing Name	A value used to select this SNODE as the outbound node during certificate-based routing. It must match the routing name returned by EA. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_). Set this field only if you are configuring certificate-based routing in EA.
Description	Description to help you identify the node you create. It can be up to 255 characters.

Field Name	Description
PeSIT Server Address	IP address or host name of the Connect:Express/PeSIT node. Valid values are 1-200 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), colon (:), and underscore (_). You can also define one of the following types of patterns: ◆ Wildcard validates incoming DNS names. If a wildcard pattern is provided, SSP performs a reverse lookup on the incoming IP address and the DNS name is compared to the wildcard patterns. Wildcard characters allowed are ? and *. For example, *.a.com allows a connection from b.a.com but not from b.b.com. ◆ IP/Subnet validates incoming IP addresses. Use the format IP-address/num-bits where IP-address identifies an IP address template and num-bits identifies the number of leading (highest-order) bits in the template that are significant. An IP match is performed by comparing the leading (highest-order) num-bits of the incoming IP address against num-bits of the template. For example, 10.20.0.0/16 searches for a match to the first 16 bits. All IP addresses beginning with 10.20.* are allowed. 10.0.0.0/8 searches for a match to the first 8 bits. All addresses beginning with 10.* are allowed. 0.0.0.0/0 searches for a match to the first zero bits. All IP addresses are allowed. **Note:** When you use a pattern, you are configuring an inbound only node. The Routing Name and PeSIT Server Port are used for outbound only, and these fields are disabled.
PeSIT Server Port	Port number of the Connect:Express/PeSIT node. Valid values are 1 - 65535. If the server address is a pattern, this field can be left blank.
Policy	Policy you want to associate with the node you are creating. If a policy with the security attributes required has not been created, click (+).

PeSIT Netmap Node Definition - Security

Use these fields to define secure connection requirements for the node. Refer to the field definitions in the following table.

Field Name	Description
Use SSL	Enable SSL to turn on the use of SSL/TLS to provide secure communications with transport protocols and to ensure that data is secured as it is transmitted across a single socket.
Verify Common Name	Enable Verify Common Name if your security environment requires that the common name in the certificate presented be verified. If you enable Verify Common Name, you must provide Certificate Common Name.
Certificate Common Name	Common name value to validate. If the common name in the certificate does not match the value defined in this field, the session fails.
Enable Client Authentication	Enable Client Authentication on the inbound node connection to require that the inbound node authenticate the certificate presented by the SSP server.

Field Name	Description
Security Setting	Security protocol allowed for connections to this node. Options include: ◆ SSL V3 or TLS (Default) - select this option to require SSL V3 or TLS for the connection. ◆ TLS - select this option to require TLS for the connection. ◆ SSL V3 - select this option to require SSL V3 for the connection.
Trust Store	Database where the system and CA certificates are stored. System and CA certificates are used during a secure connection to verify that a certificate received from a server is signed by a trusted source.
CA Certificates/Trusted Root	Trusted certificate to use to authenticate the certificate presented by the client. You select a CA certificate or trusted root from the list of certificates stored in the trust store you selected in the Trust Store field. When a client presents a certificate to establish a secure connection, the trusted root certificate, located at the server, must match or be the entity who signed the certificate presented by the client during the SSL handshake.
Key Store	Database where the keys and system certificates you want to use are stored.
Key/System Certificate	Certificate presented by SSP to the node to authenticate itself during the SSL handshake, or presented by the Connect:Express server to authenticate itself to the SSP server. Select the Key/System Certificate to use for the node from the list, that contains the certificates stored in the key store selected in the Key Store field.
Available Cipher Suites	List of ciphers that can be enabled to encrypt data transmitted during a secure SSL or TLS connection between SSP and a Connect:Express node. Enable at least one cipher. To enable a cipher, highlight it and click Add. To enable multiple ciphers, highlight the ciphers to enable and click Add.
Selected Cipher Suites	Ciphers you enabled to encrypt data during a secure SSL or TLS connection. Ciphers are negotiated based on their location in the Selected Ciphers list. To reorder a cipher in the list, highlight it and click Up or Down.

PeSIT Netmap Node Definition - Advanced

Change the logging level for a PeSIT node definition, identify a destination service name to use in an EA transaction, and configure nodes to use for failover support. Refer to the field definitions in the following table.

Field Name	Description
Logging level	The level of logging to write to the node log file. Logging options include: ◆ NONE turns logging off. NONE is the default value. ◆ ERROR writes only error messages to the log. ◆ WARN writes error and warning messages to the log. ◆ INFO writes error, warning, and informational messages to the log. ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Commerce Support.
Destination Service Name	Name of the service that is passed to Sterling External Authentication Server (EA) for use in authenticating services. If no value is provided, the SNODE name is used as the service name.
Logon ID	ID to use to connect to the outbound server if the policy is requires that the credentials from the netmap be used. Valid values are 1-8 alphanumeric characters and certain special characters. The following special characters are not allowed: ! @ # % ^ * ( ) + ? , < > { } [ ] |; " '
Password	Password to use to connect to the outbound server if the policy requires that credentials from the netmap be used. Valid values are 1-8 alphanumeric characters and certain special characters. The following special characters are not allowed: , " '
Alternate Destinations - Node	Node name or IP address and port to use to connect to an alternate Connect:Express/PeSIT outbound node if a connection to the primary node cannot be made. Up to three alternate destination nodes can be defined for each outbound node. To use different security and Sterling External Authentication Server definitions for the alternate destination node, first configure an outbound node definition for the alternate node in the netmap. Then, open the primary outbound node definition and select the alternate node name from the drop-down list in the Alternate Destinations - Node 1 field. To use the security and Sterling External Authentication Server definition defined in the primary outbound node for an alternate destination node, you do not have to define the alternate node in the netmap. Select IP Address/Port from the drop-down list and then provide a value in the IP Address and Port fields. Define up to three alternate node names. **Note:** Only nodes with an IP address are outbound nodes and shown in the list.
Alternate Destinations - IP Address	IP address to use to connect to an alternate destination node if a connection to the primary node cannot be made. Up to three alternate destination nodes can be selected. Valid values are 1-200 alphanumeric characters and special characters: underscore (_), dash (-), colon (:), and period (.). If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and EA definition from the primary node is used for the connection.

Field Name	Description
Alternate Destinations - Port	Port to use to connect to an alternate destination node if a connection to the primary node cannot be made. Up to three alternate destination nodes can be selected. Valid values are 1-65535. If you provide an IP address and port as an alternate destination and a connection to the alternate node is attempted, the security and EA definition from the primary outbound node is used for the connection.

PeSIT Policy Configuration - Basic

Use this screen to define how you impose controls to authenticate an inbound node. A trading partner trying to access your Connect:Express server will need a stronger policy than a Connect:Express server trying to access a PeSIT node.

Field Name	Description
Policy Name	Name to assign to the policy you create. Valid values are 1-150 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
Description	Description up to 255 characters to help you identify the policy you create.
Type	Protocol being used: PeSIT.
Protocol Error Action	Action to perform if SSP detects protocol violations during a communications session. Valid values are: ◆ NONE (Default)—select this option to disable checking of protocol errors. ◆ IGNORE—select this option to ignore protocol errors. ◆ WARN—select this option if you want SSP to write an error message to the log but continue the session when protocol errors are detected. ◆ ABORT—select this option to terminate a communications session when protocol errors are detected.

PeSIT Policy Configuration - Advanced

Use this tab to specify the type of PNODE authentication for inbound access requests. For Certificate Authentication and LogonID Authentication through External Authentication, you must install and configure EA. Refer to the field definitions in the following table.

Field Name	Description
Certificate Authentication - External Authentication Certificate Validation	Turn on External Authentication Certificate Validation to validate information presented in certificates received from trading partners using EA.

Field Name	Description
Certificate Authentication - External Authentication Profile	Name of the Certificate Validation Definition you defined in the EA. You must enable certificate validation before you can provide a profile. Valid values are 1-255 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
LogonID Authentication - Through External Authentication	Turn on this option to send an incoming PNODE LogonID and password to EA for validation.
LogonID Authentication - External Authentication Profile	If you enabled LogonID authentication through EA, identify the certificate authentication profile you defined in EA in this field. Valid values are 1-255 alphanumeric characters with no spaces. Special characters allowed are period (.), dash (-), and underscore (_).
LogonID Authentication - Through Local User Store	Validates the PNODE LogonID and password of the inbound node using information defined in the user store. You must add the PNODE LogonID to the user store in order to successfully use this method.
LogonID Mapping - Internal logon ID	Enable this option in the policy to determine what PNODE LogonID and password is used to connect to the Connect:Express server in the secure environment. For the PNODE LogonID and password to successfully access the Connect:Express server, a PNODE definition must be defined at the server. PNODE mapping options include: ◆ **Pass-through for PNODE** (Default)—uses the LogonID and password supplied by the PNODE to connect to the Connect:Express server in the secure zone. To successfully connect to the Connect:Express server, the LogonID and password must be defined at the server. ◆ **Replace LogonID with LogonID mapped in External Authentication**—maps the LogonID provided by the inbound PNODE to a value defined in External Authentication and uses the EA-supplied value to connect to the SNODE. ◆ **Replace LogonID with Netmap LogonID**—maps the LogonID provided by the inbound PNODE to a value defined in the netmap and uses the netmap value to connect to the SNODE.

PeSIT Policy Configuration - Transfer Direction

Use the transfer direction fields to block a transfer direction for this node. Refer to the field definitions in the following table.

Field Name	Description
Receive a file allowed (SELECT)	Allows the PNODE to request reception of a file. Disable this option to block PeSIT SELECT commands from the PNODE.
Send a file allowed (CREATE)	Allows the PNODE to request transmission of a file. Disable this option to block PeSIT CREATE commands from the PNODE.

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.

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 ficticious 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 2010. Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. 2010.

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

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: *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, Microsoft Windows NT, and the Microsoft 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.