

Sterling Secure Proxy



SFTP Reverse Proxy Scenarios

Version 34

Sterling Secure Proxy



SFTP Reverse Proxy Scenarios

Version 34

Note

Before using this information and the product it supports, read the information in "Notices" on page 51.

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

© **Copyright IBM Corporation 2006, 2012.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. SFTP Reverse Proxy Configuration	1	Chapter 15. Authenticate an Inbound Node by Comparing Both a Password and a Key to the Local User Store	31
Chapter 2. Complete and Test SFTP Configuration Scenarios.	3	Chapter 16. Provide User Mapping Using the Netmap	33
Chapter 3. Create a Basic SFTP Configuration	5	Chapter 17. Connect to the Outbound Server Using Credentials from the Netmap	35
Chapter 4. Create an SFTP Policy.	9	Chapter 18. Strengthen the SFTP User Authentication Using Sterling External Authentication Server	37
Chapter 5. Create an SFTP Netmap	11	Chapter 19. Authenticate the Inbound User ID and Password Using Sterling External Authentication Server	39
Chapter 6. Define the Adapter for the SFTP Connection	13	Chapter 20. Authenticate the Inbound User ID and Key Using Sterling External Authentication Server	41
Chapter 7. What You Defined with the Basic SFTP Configuration Scenario	15	Chapter 21. Strengthen the Outbound SFTP Connection With Sterling External Authentication Server User Mapping	43
Chapter 8. Variations on the Basic SFTP Configuration	17	Chapter 22. Connect to the Outbound SFTP Node Using Information Stored in LDAP	45
Chapter 9. Define SFTP Connection Requirements Between Sterling Secure Proxy and Inbound Nodes	19	Chapter 23. Test the Inbound and Outbound Connections	47
Chapter 10. Define Inbound Node Connection Definitions.	21	Chapter 24. Route an Outbound Connection to Alternate SFTP Servers	49
Chapter 11. Authenticate an Inbound SFTP Node Against Information Stored in the Local User Store.	23	Notices	51
Chapter 12. Add Local Authentication to the Inbound Node Using Password Information.	25		
Chapter 13. Authenticate an Inbound Node Using Key Information	27		
Chapter 14. Authenticate an Inbound Node by Comparing Either a Password or a Key to the Local User Store	29		

Chapter 1. SFTP Reverse Proxy Configuration

The SFTP configuration scenarios describe how to configure SFTP protocol connections to and from the engine.

Note: Configuration information must be available on the engine before communication sessions with Sterling B2B Integrator can be established.

Organization of the SFTP Configuration Scenarios

The first scenario instructs you on how to configure a basic configuration. Each successive scenario adds another security feature to the basic configuration. After adding a security feature, test the connection to ensure that you have correctly configured it. You determine your security needs and configure the security features applicable for your environment.

The following scenarios help you configure and test Sterling Secure Proxy for SFTP protocol connections to the SFTP server:

- Create a basic configuration
- Perform user authentication using the local user store
- Provide user mapping using the netmap

The remaining scenarios require Sterling External Authentication Server, an optional security feature of Sterling Secure Proxy that must be configured independently of Sterling Secure Proxy. After Sterling External Authentication Server is configured, you can update your basic security definitions to enable Sterling Secure Proxy to connect to the Sterling External Authentication Server to enforce the following advanced security features:


- Authenticate an inbound user using Sterling External Authentication Server
- Manage connection requirements to the outbound server using Sterling External Authentication Server

Additional procedures instruct you how to define alternate nodes for failover support.

Chapter 2. Complete and Test SFTP Configuration Scenarios

About this task

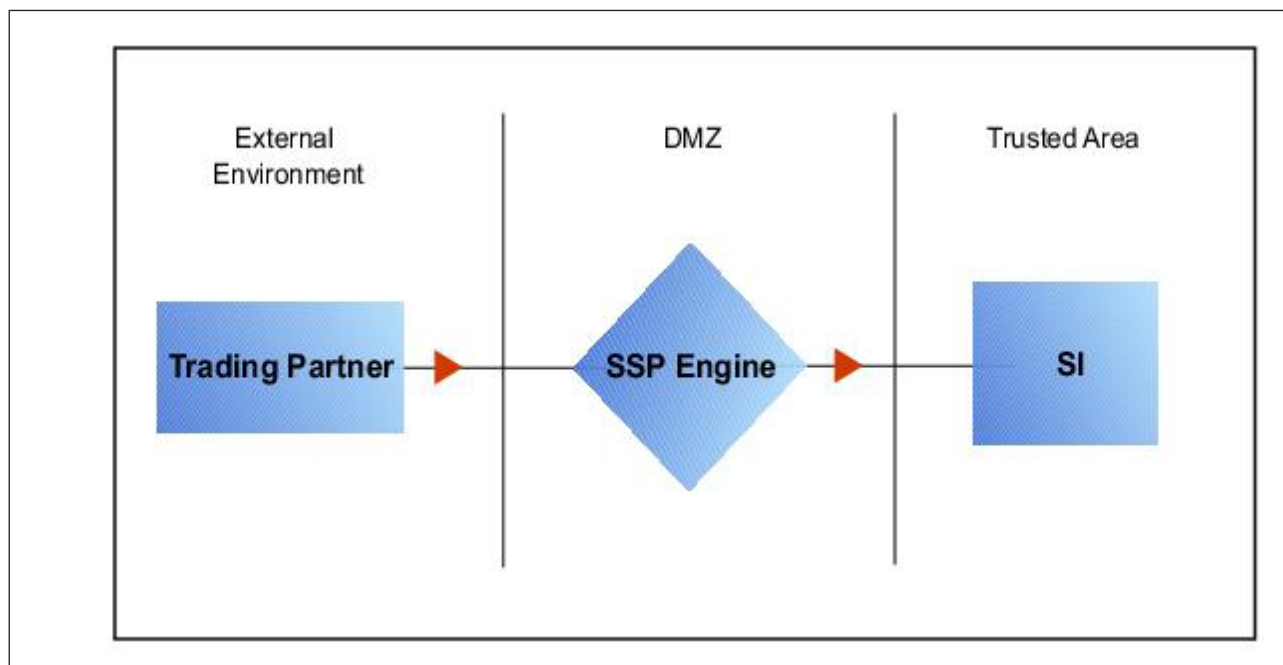
Work through the sequence of SFTP configuration scenarios in the order in which they are presented to add and test security features. Be sure to test each feature before you add the next feature to the configuration. Before you move Sterling Secure Proxy into production, ensure that you have configured and tested all of the security features you need for your environment.

Note: As you complete each task, provide all required information. If information is not provided or is incorrect, the following error icon is displayed:  . To view more information about the error, hover over the icon.

Chapter 3. Create a Basic SFTP Configuration

This scenario contains all the information and tools to configure Sterling Secure Proxy to establish a basic connection from a trading partner to the SFTP server as shown in the following diagram. You are configuring the minimum requirements to allow you to test the connections and ensure that communications sessions can be established between the inbound node and Sterling Secure Proxy, and to the outbound SFTP node. The basic configuration requires that Sterling Secure Proxy present its key to the inbound node for authentication and that the SFTP server present its key to Sterling Secure Proxy for authentication. It does not configure user authentication. After you create and test the basic SFTP configuration and all connections are working, you then add user authentication.

You accept default values when configuring this scenario. As a result, user credentials presented by the inbound node are used to connect to the outbound SFTP server.



After you configure the basic SFTP configuration, validate it by initiating an SFTP connection from the trading partner. For more information on testing the configuration, see *Test the Inbound and Outbound Connections*.

Complete the following tasks to define a basic SFTP configuration:

- Create a policy
- Define inbound and outbound connections in a netmap
- Define an SFTP adapter

Basic SFTP Configuration Worksheet

Before you configure Sterling Secure Proxy for SFTP connections, gather the information on the Basic SFTP Configuration Worksheet. You use this information as you configure a basic SFTP connection for Sterling Secure Proxy. After you configure Sterling Secure Proxy for SFTP connections, validate the configuration by initiating an SFTP connection from the inbound node.

Create a basic policy. The default authentication method is password authentication. However, the password is not authenticated in the basic configuration because you do not select an authentication mechanism. Instead, it is passed through to the outbound node for authentication. In a later SFTP configuration scenario, you add the configuration information needed to authenticate an inbound node.

Configuration Manager Field	Feature	Value
Policy Name	Name of policy.	

Create a netmap that contains connection information for the nodes connecting to and from Sterling Secure Proxy: the trading partner (inbound node) and the Sterling B2B Integrator SFTP server (outbound node). For the outbound node, you must identify the host name and IP address to connect to the node as well as the known host key to use for server authentication and the ciphers or message authentication codes (MACs) to use to encrypt the data. You also associate the basic policy you create with the inbound node.

Note: You must have SSH keys to authenticate Sterling Secure Proxy to the inbound node (local host keys) and to authenticate the outbound SFTP server to Sterling Secure Proxy (known host keys). Create a key store for the keys and check the keys into the key store. Refer to *Manage Local Host Key Stores and Keys* for instructions on creating a local host key store and add a key to the key store. Refer to *Manage Known Host Key Stores and Keys* for instructions on creating the known host key store and importing the key. If Sterling Secure Proxy is required by the SFTP server to present its user key for authentication, you must have SSH keys for the local user for this authentication exchange. Refer to *Manage Local User Key Stores and Keys* for instructions on creating the local host key store and importing the key.

Configuration Manager Field	Feature	Value
Netmap Name	Netmap name.	
Inbound Node Name	Inbound Trading Partner Information Trading partner name (name to assign to inbound node definition).	No spaces allowed.

Configuration Manager Field	Feature	Value
Peer Address Pattern	Host name/IP address pattern.	*
		Specifying * for this value allows all inbound nodes configured on the SFTP server as trading partners to connect to the SFTP server. To define a more specific node definition, see Define SFTP Connection Requirements Between Sterling Secure Proxy and Inbound Nodes.
Policy	Name of policy you create. (Select it from the pull-down list.)	
Outbound SFTP Server Connection		
Outbound Node Name	Outbound SFTP server node name.	
Primary Destination Address	Host name/IP address of SFTP server.	
Primary Destination Port	Port number to connect to SFTP server.	
Known Host Key Store	Name of the key store where the known host key is stored.	
Known Host Key	Location and name of the public key presented to Sterling Secure Proxy by the outbound SFTP server during authentication.	

Create an SFTP adapter that defines information necessary to establish SFTP connections to and from Sterling Secure Proxy. When you configure the adapter, select the basic netmap and outbound SFTP server in the netmap definition and the local host key that Sterling Secure Proxy presents to its clients.

Configuration Manager Field	Feature	Value
Adapter Name	Adapter name.	
Listen Port	Listen port to use for inbound connections.	
Netmap	Netmap to associate with the adapter.	
Standard Routing Node	Name of the outbound node corresponding to the Sterling B2B Integrator server where inbound connections are routed.	
Engine	Engine to run on.	

Configuration Manager Field	Feature	Value
Startup Mode	How the adapter is started.	<p>auto starts the adapter as soon as it is pushed to the engine.</p> <p>manual requires that the adapter be manually started.</p>
Local Host Key Store	Name of the key store where the local host key is stored.	
Local Host Key	Location and name of the private part of the key presented by Sterling Secure Proxy to the inbound connection during authentication.	
Available Cipher Suites	Cipher suites to enable.	
Selected Cipher Suites	(Be sure to match the configuration of the SFTP client.)	
Available Cipher Suites	Cipher suites to enable.	
Selected Cipher Suites	(Be sure to match the configuration of the SFTP client.)	
Available Key Exchange	Key exchange to enable.	
Selected Key Exchange	(Be sure to match the configuration of the SFTP client.)	

Chapter 4. Create an SFTP Policy

About this task

The SFTP policy defines how you impose controls to authenticate a trading partner trying to access an SFTP server over the public Internet. The basic policy does not enable any security features. You add user authentication to the policy definition in later scenarios.

To define a policy:

Procedure

1. Click **Configuration** from the menu bar.
2. Click **Actions > New Policy > SFTP Policy**.
3. Specify a name for the policy in the **Policy Name** field.
4. Click **Save**.

Chapter 5. Create an SFTP Netmap

About this task

You define inbound connection information for your external trading partners and outbound connection information for the SFTP server Sterling Secure Proxy connects to. These values are stored in a netmap. The netmap is associated with a policy and an adapter.

The SFTP protocol requires that the server authenticate itself to the client.

- Inbound connection-Server authentication for the inbound connection requires that Sterling Secure Proxy use its private key to verify its identity to the inbound connection. Before you can configure authentication of Sterling Secure Proxy, you must configure a local host key store and add the private key to the local host key store. You must also send the public key to the inbound trading partner. Refer to *Manage Local Host Key Stores and Keys* for instructions. The keys used to authenticate Sterling Secure Proxy to the inbound node connection are configured in the adapter definition.
- Outbound connection-Server authentication for the outbound connection requires that the SFTP server present its public key to Sterling Secure Proxy. Sterling Secure Proxy must use the public key to validate the server connection. Before you can configure authentication of the SFTP server, you must configure a known host key store and add the public key received from the SFTP server to this key store. Refer to *Manage Known Host Key Stores and Keys* for instructions.

For authentication of the SFTP server connection, you must determine what ciphers are allowed for encryption and what MACs are allowed for message integrity protection. These MACs and ciphers must also include the required settings from the inbound nodes, the outbound node, and all keys checked into the key stores. You also determine the order of preference for both the ciphers and the MACs. Communicate with the SFTP server administrator to ensure that your configuration matches the SFTP server configuration.

Before you begin this procedure, create a policy to associate with the netmap.

To create a netmap and define inbound and outbound nodes:

Procedure

1. Click **Configuration** from the menu bar.
2. Click **Actions > New Netmap > SFTP Netmap**.
3. Type a name for the netmap in the **Netmap Name** field.
4. To define an inbound node definition:
 - a. Click **New**.
 - b. Specify the following values:
 - **Inbound Node Name**
 - **Peer Address Pattern**
 - **Policy**
 - c. Click **OK**.
5. To define an outbound node definition:

- a. Click the **Outbound Nodes** tab and click **New**.
 - b. Specify the following values:
 - **Outbound Node Name**
 - **Primary Destination Address**
 - **Primary Destination Port**
 - **Known Host Key Store**
 - **Known Host Key**
 - c. Click the **Security** tab.
 - d. Specify the following values:
 - **Available Cipher Suites**
 - **Available MAC Suites**
 - **Available Key Exchange**
 - e. If necessary, reorder the selected cipher suites, MAC suites, and key exchanges.
 - f. Click **OK**.
6. Click **Save**.

Chapter 6. Define the Adapter for the SFTP Connection

About this task

An SFTP adapter definition specifies both the system-level communications information necessary to establish SFTP connections to and from Sterling Secure Proxy and the local host key used to validate Sterling Secure Proxy to an inbound connection. Because the SFTP protocol requires that Sterling Secure Proxy present its key to the inbound node for authentication, you must configure the adapter with the local host key store and the local host key to present to the inbound connection. Before you can configure the adapter, create a local host key store and a local host key. Refer to *Manage Local Host Key Stores and Keys* for instructions.

You must also determine what ciphers are allowed for encryption and what MACs are allowed for message integrity protection, as well as the order of preference for both the ciphers and the MACs. Communicate with the administrator of the inbound node to ensure that your configurations match.

You can create multiple adapter definitions.

Before you begin this procedure, create the following definitions:

- A netmap to associate with the adapter
- An engine definition to associate with the adapter. Refer to *Install or Upgrade Sterling Secure Proxy on UNIX or Linux* or *Install or Upgrade Sterling Secure Proxy on Microsoft Windows* for instructions.

To define an SFTP adapter:

Procedure

1. Click **Configuration** from the menu bar.
2. Click **Actions > New Adapter > SFTP Reverse Proxy**.
3. Specify values for the following:
 - **Adapter Name**
 - **Listen Port**
 - **Netmap**
 - **Standard Routing Node**
 - **Engine**
 - **Local Host Key Store**
 - **Local Host Key**
4. Click the **Security** tab.
5. Specify values for the following fields:
 - **Available Cipher Suites**
 - **Available MAC Suites**
 - **Available Key Exchange**
6. If necessary, reorder the selected cipher suites, MAC suites, or key exchange algorithms.

Note: If you change one of the following values, you must restart the adapter before the change takes effect: listen port, local host key, selected cipher suites, selected MAC suites, key exchange, compression, maximum sessions, session timeout, inbound perimeter server, outbound perimeter server, or external authentication perimeter server.

7. Click **Save**.

Chapter 7. What You Defined with the Basic SFTP Configuration Scenario

Creating secure connections to SFTP servers on behalf of nodes external to your trusted zone requires that you organize information about the trading partners and the SFTP server in a policy, a netmap, and an adapter definition. You created these items when you defined the Basic SFTP Configuration. Be sure to test the Basic SFTP Configuration before you configure additional security features. Refer to *Test the Inbound and Outbound Connections* for information about testing the SFTP reverse proxy configurations outlined in this scenario.

As you add complexity to your security configurations using the procedures in the remaining scenarios, you modify these items to configure more complex authentication measures.

Chapter 8. Variations on the Basic SFTP Configuration

After you confirm that the communications sessions you established using the basic SFTP configuration were successful, you may want to validate sessions using other types of inbound trading partner definitions before adding complexity to the security configuration. To ensure that you can validate and troubleshoot problems, you should test one variation at a time by changing the configuration, initiating a connection, and verifying the result.

You can modify the inbound trading partner node definitions as follows:

- Define a specific IP address
- Define a wildcard peer pattern
- Define an IP/subnet pattern

Chapter 9. Define SFTP Connection Requirements Between Sterling Secure Proxy and Inbound Nodes

You define connection requirements between Sterling Secure Proxy and inbound nodes by defining inbound node definitions. Refer to your company security requirements to determine how tightly to define the parameters that an inbound node must provide to allow a connection.

You can create inbound node definitions to allow only one individual inbound connection, or you can identify a pattern of IP addresses and create an inbound definition to allow inbound connections matching the pattern to connect to Sterling Secure Proxy. Methods of defining inbound nodes are as follows:

- Create an entry for an individual inbound node and define the inbound node IP address to connect to Sterling Secure Proxy. Only connections from that IP address are allowed. A single IP Address must be specified as a subnet pattern where all bits are matched, such as 11.22.33.44/32. Sterling Secure Proxy also supports individual host names. They must match the value returned by a reverse DNS lookup.
- Create an inbound node entry that allows all nodes that match an IP/Subnet address pattern. Patterns include:
 - Match the first 16 bits of an IP address pattern. For example, 10.20.0.0/16 allows all IP addresses that begin with 10.20.* to connect to Sterling Secure Proxy.
 - Match the first 8 bits of an IP address pattern. For example, 10.0.0.0/8 allows all IP addresses that begin with 10.* to connect to Sterling Secure Proxy.
- Define an inbound node entry that allows all inbound nodes that match a wildcard host name pattern. When a connection is attempted and you have defined a wildcard host name pattern definition, a reverse DNS lookup is performed on the IP address of the inbound connection. The DNS name is compared to the wildcard pattern. Wildcard patterns include:
 - Asterisk (*) enables a match on any number of characters. For example, *.a.com allows a connection from b.a.com but not from a.bc.com. Using only the * allows all inbound nodes to successfully connect to Sterling Secure Proxy.
 - Question mark (?) enables a match on one character. For example, a?.com allows a connection from a.b.com but not from a.bc.com.

You can define more than one inbound node definition and use a combination of the node definition methods. Order the definitions from most specific to least specific. When an inbound node connection is attempted, Sterling Secure Proxy compares the IP address of the inbound node to the first inbound node definition. If it matches, a connection is established. If it does not match, Sterling Secure Proxy checks the next inbound node definition until a match is found. If no match is found, the connection is terminated.

Inbound SFTP Connection Definition - Worksheet

Use the following worksheet to identify the information needed to configure inbound node definitions specific inbound nodes or groups of inbound nodes that match a pattern.

Define Inbound Trading		
Configuration Manager Field	Partner Information	Value
<p>Note: If you define a single node and definitions for multiple nodes using pattern matching, order the definitions from most specific to least specific. Sterling Secure Proxy processes them in the order in which they are listed.</p>		
Inbound Node Name	Trading Partner Name	
Policy	Policy to associate with the inbound trading partner	
For a Single Node		
Peer Address Pattern	IP address/32 or hostname	
	<p>Create an entry for an individual inbound node and define the inbound node IP address that can connect to Sterling Secure Proxy. Only connections from that IP address will be allowed. Sterling Secure Proxy supports host name. An example definition is a.b.com.</p> <p>A single IP address must be specified as a subnet pattern where all bits are matched, such as 11.22.33.44/32.</p>	
For Multiple IP Addresses Using IP/Subnet Pattern		
Peer Address Pattern	Peer Address IP/Subnet	Pattern Options
For Multiple Nodes Using Wildcard Peer Address Pattern to Validate Inbound DNS		
Peer Address Pattern	Wildcard Peer Address	Pattern

Chapter 10. Define Inbound Node Connection Definitions

About this task

This procedure instructs you how to modify the basic SFTP configuration to add inbound node definitions for a group of nodes with similar information, and definitions that limit access to one specific inbound node. It assumes that you have already configured an adapter. Gather a list of all inbound trading partners, including names and IP addresses.

To define inbound connection definitions:

Procedure

1. Identify patterns that can be used to define groups of inbound nodes.
2. Decide if you need to define a trading partner connection for any individual IP addresses, to increase security.
3. Click **Configuration** from the menu bar.
4. Expand the **Netmaps** tree and click the netmap to modify.
5. Click **New** to add a new inbound node definition.
6. Using the information you defined on the Inbound Connection Definition Worksheet, provide the following information and click **Save**:
 - **Inbound Node Name**
 - **Peer Address Pattern**
 - **Policy**
7. Repeat step 6 for every group of connections and for every individual IP address connection you want to define.
8. If necessary, reorder the node definitions in the netmap. Order definitions from most specific to least specific since they will be evaluated in order.
 - a. Click the radio button beside the inbound node definition to move.
 - b. Click **Move Up** or **Move Down** until the node definition is in the correct order.
9. Click **OK**.
10. Click **Save**.

Chapter 11. Authenticate an Inbound SFTP Node Against Information Stored in the Local User Store

The Create a Basic SFTP Configuration scenario does not authenticate the inbound node. For additional security, you may configure the authentication method to use for the inbound node. You can choose from the following user authentication methods:

- Authenticate the password presented by the inbound node against information stored in the local user store.
- Authenticate the key presented by the inbound node against information stored in the authorized user key store.
- Authenticate either the password or the key presented by the inbound node using information stored in the local user store or the authorized user key store.
- Authenticate both the password and the key presented by the inbound node using information stored in the local user store and the authorized user key store.
- Authenticate a password using information stored in the Sterling External Authentication Server.

The following scenarios build on the Create a Basic SFTP Configuration scenario by adding user authentication of the inbound node using information from the local user store. Determine which authentication method you want to enable and then complete the procedure to implement it. Refer to *Strengthen the SFTP User Authentication Using Sterling External Authentication Server* for instructions on configuring user authentication using Sterling External Authentication Server.

Add Local Authentication to an Inbound Node Worksheet

Before you add user authentication to the inbound connection you created in the Basic Configuration scenario, gather the information on the Add Local Authentication to an Inbound Node Worksheet. Use this information as you configure user authentication for the inbound connection.

Configuration Manager Field	Feature	Value
Policy Name	Name of policy associated with the inbound node.	
Required Authentication Method	Method to use for the inbound node. Options include: <ul style="list-style-type: none">• Password• Key• Password and Key• Password or Key	
Internal User ID	The source to use to for the internal user ID.	Pass-Through or Netmap
Name	Name to assign to the user you create.	

Configuration Manager Field	Feature	Value
Password	If you are authenticating the user-supplied password, identify the password value to use to validate the inbound password.	
Confirm Password		

Chapter 12. Add Local Authentication to the Inbound Node Using Password Information

About this task

This scenario builds on the Basic SFTP Configuration by adding user authentication to the inbound connection. It compares a password presented by the inbound node to information defined in the local user store. You must add the password information to the local user store before you can test this scenario. Refer to *Manage CM User Accounts* for instructions.

To add support for password authentication:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and select the policy to modify.
3. Click the **Advanced** tab.
4. Select **Password** as the **Required Authentication Method**.
5. Enable the **User Authentication Mechanism: Through Local User Store** option.
6. Click **Save**.

Chapter 13. Authenticate an Inbound Node Using Key Information

About this task

This scenario builds on the Basic SFTP Configuration by adding inbound user authentication using a key. This authentication method requires that credentials for the Sterling B2B Integrator server be defined in the netmap since only the password can be passed through to the Sterling B2B Integrator server. You must add the key information to the user definition before you can test this scenario. Refer to *Add SSH Keys to a User Account* for instructions.

To add support for key authentication:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and select a policy.
3. Click the **Advanced** tab.
4. Select **Key** as the **Required Authentication Method**.
5. Enable the **User Authentication Method: Through Local User Store** option.
6. In the **Internal User ID** field, select **Netmap**.
7. Click **Save**.
8. Expand the netmap tree and open the netmap to edit.
9. Click the **Outbound Nodes** tab.
10. Select the outbound node to edit and click **Edit**.
11. Click the **Advanced** tab.
12. Type the user ID and password or key to use to connect to the outbound Sterling B2B Integrator server.
13. Click **OK**.
14. Click **Save**.

Chapter 14. Authenticate an Inbound Node by Comparing Either a Password or a Key to the Local User Store

About this task

This scenario builds on the Basic SFTP Configuration by adding support for either key or password authentication of the inbound connection. The inbound node may present a key or a password. Only one must be authenticated for a communications session to be established. This authentication method requires that credentials for the Sterling B2B Integrator server be defined in the netmap, since only a password can be passed through to the Sterling B2B Integrator server.

You must add the password and key information to the user definition in the local user store before you can test this scenario. Refer to *Create an Engine User Account* for instructions on creating a user account and assigning a password. Refer to *Add SSH Keys to a User Account* for instructions on adding a key to a user account definition.

To add support for either password or key authentication:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and select a policy.
3. Click the **Advanced** tab.
4. Select **Password or Key** as the **Required Authentication Method**.
5. Enable the **User Authentication Mechanism: Through Local User Store** option.
6. In the **Internal User ID** field, select **Netmap**.
7. Click **Save**.
8. Expand the netmap tree and open the netmap to edit.
9. Click the **Outbound Nodes** tab.
10. Select the outbound node to edit and click **Edit**.
11. Click the **Advanced** tab.
12. Type the user ID and password to use to connect to the outbound Sterling B2B Integrator server.
13. Click **OK**.
14. Click **Save**.

Chapter 15. Authenticate an Inbound Node by Comparing Both a Password and a Key to the Local User Store

About this task

This scenario builds on the Basic SFTP Configuration by adding support for both key and password authentication of the inbound connection. The inbound node must present both a key and a password and both must be authenticated for a communications session to be established.

You must add the password and key information to the user definition in the local user store before you can test this scenario. Refer to *Create an Engine User Account* for instructions on creating a user account and assigning a password. Refer to *Add SSH Keys to a User Account* for instructions on adding a key to a user account definition.

To add support for password and key authentication:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and select a policy.
3. Click the **Advanced** tab.
4. Select **Password and Key** as the **Required Authentication Method**.
5. Enable the **User Authentication Method: Through Local User Store** option.
6. In the **Internal User ID** field, select **Pass-through**.
7. Click **Save**.
8. After you configure user authentication using both key and password information, validate the configuration by establishing a session initiated by an SFTP client to an SFTP server.

Chapter 16. Provide User Mapping Using the Netmap

This scenario builds on the Basic SFTP Configuration by enabling the use of different user credentials for the outbound connection to the SFTP server.

If you configure this option, the credentials presented by the inbound trading partner are not used to connect to the SFTP server. Credentials stored in the netmap are used to connect to the SFTP server. This method prevents trading partners from accessing the actual credentials used to connect to the internal SFTP server.

After you configure the use of alternate credentials to connect to the SFTP server using information from the netmap, test the configuration by establishing a session initiated by an SFTP client to a SFTP server. Refer to *Test the Inbound and Outbound Connections* for more information on testing the configuration described in this scenario.

Provide User Mapping Using the Netmap - Worksheet

In this scenario, edit the netmap and the policy you created in the basic configuration to strengthen the outbound connection by providing user credentials and a mapping method to use to secure the outbound connection to the SFTP server.

Collect the following information so you can match the Sterling Secure Proxy configuration with the SFTP server configuration. Use the information on this worksheet as you edit the outbound node definition, and be sure to select the netmap and policy you created in the Basic Configuration.

Configuration Manager Field	Feature	Value
Netmap	Name of netmap to modify.	
Policy	Name of policy to modify.	
User ID	User ID to connect to the SFTP server (Defined at the SFTP server).	
Password	Password to connect to the SFTP server (Defined at the SFTP sever).	
Local User Key Stores	The name of the key store where the key to authenticate Sterling Secure Proxy to the outbound connection is stored.	
Local User Key	The local user key to use to authenticate Sterling Secure Proxy to the outbound connection.	

Chapter 17. Connect to the Outbound Server Using Credentials from the Netmap

About this task

To increase security for connections to the server in the trusted zone, you can use the netmap to prevent the user ID and password, or the key provided by the trading partner, from being used to connect to the server. If you configure this option, the inbound node uses one set of credentials to connect to Sterling Secure Proxy and uses information stored in the netmap to connect to the outbound server.

Before you configure this option:

- Ensure that a user ID and password or key are defined for the outbound connection on the SFTP server
- Obtain the user ID and password.

To configure validation for the outbound connection using credentials stored in the netmap:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and click the netmap to modify.
3. Click the **Outbound Nodes** tab.
4. Select the outbound node to modify and click **Edit**.
5. Click the **Advanced** tab.
6. Type the values to use to connect to the SFTP server:
 - **User ID**
 - **Password**
 - **Local User Key Stores**
 - **Local User Key**
7. Click **Save**.
8. Expand the **Policies** tree and click the policy to modify.
9. On the **Policy Configuration** panel, click the **Advanced** tab.
10. From the **User Mapping: Internal User ID** list, select **Netmap**.
11. Click **Save**.

Chapter 18. Strengthen the SFTP User Authentication Using Sterling External Authentication Server

This scenario builds on the basic SFTP configuration by adding user and password authentication or user and key authentication using information defined in Sterling External Authentication Server. To provide a more advanced method of securing the SFTP connection, use Sterling External Authentication Server.

Authenticate an Inbound SFTP User or Key Using Sterling External Authentication Server

You can authenticate an inbound connection against information stored in an LDAP database by configuring Sterling External Authentication Server to define how the connection is authenticated. The Sterling External Authentication Server definition determines the options that are enabled. Sterling External Authentication Server will return a user ID, password, and routing name for a local user key stored on Sterling Secure Proxy. Refer to Sterling External Authentication Server documentation library for the functions that can be performed in Sterling External Authentication Server.

Authenticate an Inbound SFTP User or Key Using Sterling External Authentication Server Worksheet

Use the following worksheet to identify the information needed to authenticate a trading partner user ID, password, or key using Sterling External Authentication Server. Update the policy you created in the Basic Configuration for this scenario.

Configuration Manager Field	Feature	Value
Policy Name	Name of policy associated with the inbound node.	
Required Authentication Method	Method to use to authenticate the inbound node. Options include: <ul style="list-style-type: none">• Password• Key• Password and Key• Password or Key	
User Authentication Mechanism - Through External Authentication	Enable this option because you will validate user information using Sterling External Authentication Server.	
User Authentication Profile	If you are authenticating a user ID and password, type the name of the profile defined in Sterling External Authentication Server used to authenticate the user.	

Configuration Manager Field	Feature	Value
Key Authentication Profile	If you are authenticating the user ID and key, type the name of the profile defined in Sterling External Authentication Server to authenticate the key.	

Chapter 19. Authenticate the Inbound User ID and Password Using Sterling External Authentication Server

About this task

To authenticate the user ID and password provided by the inbound node against information stored in an LDAP database, you must configure Sterling External Authentication Server. After you configure Sterling External Authentication Server to enable user authentication, use this procedure to configure Sterling Secure Proxy to use the authentication method you defined.

Before you configure Sterling Secure Proxy, obtain the name of the Sterling External Authentication Server definition and ensure that the Sterling External Authentication Server connection has been configured.

To configure authentication of an inbound node password using Sterling External Authentication Server:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and click the policy to modify.
3. On the **Policy Configuration** panel, click the Advanced tab.
4. Select **Password** or **Password or Key** in the **Required Authentication Method** field.
5. Enable **User Authentication Mechanism - Through External Authentication** and type the name of the user authentication definition you defined in Sterling External Authentication Server in the **User Authentication Profile** field.
6. Deselect the **Through Local User Store** option.
7. Click **Save**.

Results

You can now associate this policy with a inbound node for which you want to perform user authentication using Sterling External Authentication Server.

Chapter 20. Authenticate the Inbound User ID and Key Using Sterling External Authentication Server

About this task

To authenticate key information about the inbound node against information stored in an LDAP database, you must configure Sterling External Authentication Server. After configuring Sterling External Authentication Server, use this procedure to configure Sterling Secure Proxy to use the authentication method you defined.

Before you configure Sterling Secure Proxy, obtain the name of the Sterling External Authentication Server definition and ensure that the Sterling External Authentication Server connection has been configured.

To configure authentication of an inbound node password using Sterling External Authentication Server:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and click the policy to modify.
3. On the **Policy Configuration** panel, click the **Advanced** tab.
4. Select **Key in the Required Authentication Method** field.
5. Enable **Key Authentication Mechanism - Through External Authentication** and type the name of the key authentication definition you defined in Sterling External Authentication Server in the **Key Authentication Profile** field.
6. Deselect the **Through Local User Store** option.
7. Click **Save**.

Results

You can now associate this policy with a inbound node for which you want to perform key authentication using Sterling External Authentication Server.

Chapter 21. Strengthen the Outbound SFTP Connection With Sterling External Authentication Server User Mapping

This scenario builds on the basic SFTP configuration by adding user or key mapping using information defined in Sterling External Authentication Server. To provide a more advanced method of securing an SFTP connection, use Sterling External Authentication Server to map a user ID and password or user key presented by the inbound node to login credentials stored in Sterling External Authentication Server. The mapped login credentials are used to connect to the outbound server in the secure zone.

Manage SFTP User Mapping Using Sterling External Authentication Server

For a higher level of security when connecting to the outbound server, use information stored in an LDAP database to connect to the outbound server. To use information in an LDAP database, you configure Sterling External Authentication Server. You can use Sterling External Authentication Server to map a user ID, password, or key provided by an inbound connection to a user ID, password, or key that is not exposed to the external node.

Perform User Mapping Using Sterling External Authentication Server in an SFTP Environment Worksheet

Use this worksheet to identify the information needed to authenticate a trading partner user ID, password, or key using Sterling External Authentication Server. Update the policy you created in the Basic Configuration for this scenario.

Configuration Manager Field	Feature	Value
Policy Name	Name of policy associated with the inbound node.	
Internal User ID	The source to use to for the internal user ID.	Sterling External Authentication Server

Chapter 22. Connect to the Outbound SFTP Node Using Information Stored in LDAP

About this task

If you store user credentials in an LDAP database, use this procedure to configure Sterling Secure Proxy to use these credentials to connect to the secure outbound server.

Before you configure this option:

- Configure a SSH key authentication definition in Sterling External Authentication Server and obtain the name of the Sterling External Authentication Server definition.
- Configure the Sterling External Authentication Server to allow connections from Sterling Secure Proxy.
- Ensure that the public keys for Sterling Secure Proxy have been sent to the Sterling External Authentication Server and imported into the Sterling External Authentication Server trust store.
- Configure Sterling Secure Proxy for user authentication through Sterling External Authentication Server. Refer to *Strengthen the SFTP User Authentication Using Sterling External Authentication Server* .

To configure the use of a password or a key from the LDAP database:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and click the policy to modify.
3. On the **Policy Configuration** panel, click the **Advanced** tab.
4. Select **From External Authentication** in the **User Mapping:Internal User ID** field.
5. Click **Save**.

Chapter 23. Test the Inbound and Outbound Connections

About this task

To verify that the engine can receive and initiate communications sessions, you have to establish a connection between an SFTP client and the engine, initiate a session from the engine to the SFTP server in the trusted zone, and review the Sterling Secure Proxy audit log for the results.

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

This procedure enables you to verify that the engine can:

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

To verify the communications sessions:

Procedure

1. Make sure the engine is running.
2. Initiate a client session to the SFTP server in your trusted zone from a trading partner.
3. View the log file at the client to ensure that the connection from the inbound node to Sterling Secure Proxy was successful.
4. View the log file of the engine to ensure that the connection to Sterling Secure Proxy was successful.

Chapter 24. Route an Outbound Connection to Alternate SFTP Servers

About this task

When you configure an SFTP adapter, you define a primary SFTP server to connect to. For each outbound node definition, you can identify a maximum of three alternate outbound nodes to connect to if the primary SFTP server is not available.

Two methods of configuring alternate SFTP server routing are available.

- Select an SFTP server from the drop-down list. To configure this method, you first configure an outbound node definition in the netmap for each alternate SFTP server. Each alternate connection uses the security and advanced settings defined for the outbound node in the netmap.
- Select IP address/port from the drop-down list and enter values for the IP address and port. If you use this method, you do not have to define the alternate outbound nodes in the netmap. Each alternate connection uses the security and advanced settings defined in the primary node definition.

If you configure alternate SFTP server definitions in the outbound node definition, when a connection to the primary outbound node is unsuccessful Sterling Secure Proxy tries to connect to the alternate node you defined as Node 1. If the connection to the first alternate node is unsuccessful, Sterling Secure Proxy tries to connect to the second alternate node, Node 2. If this connection is unsuccessful, Sterling Secure Proxy tries to connect to the third alternate, Node 3. If the connection to this node is unsuccessful, the inbound connection is aborted.

To configure alternate outbound connections:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Netmap** tree and click the netmap to modify.
3. Click the **Outbound Nodes** tab.
4. Select the outbound node to modify and click **Edit**.
5. Click the **Advanced** tab.
6. To identify an alternate node that is defined in the netmap and use the security settings defined in the alternate node definition, select the outbound node name from the drop-down list.
7. To configure an alternate node that is not in the netmap and use the security setting defined in the primary node definition:
 - a. Select from the drop-down list in the **Address/Port Alternate Destinations Node** field.
 - b. Provide the **IP Address Port** number for the alternate outbound node.
8. Click **OK**.
9. Click **Save** to save the netmap updates.

Notices

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

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

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

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

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

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

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

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

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

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



Printed in USA