Sterling Secure Proxy

Planning and Installation Guide

Version 34

Sterling Secure Proxy

Planning and Installation Guide

Version 34

Note
Before using this information and the product it supports, read the information in "Notices" on page 19.

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

Contents

Chapter 1. Plan a Sterling Secure Proxy Installation

Plan Your Sterling Secure Proxy Configuration

Before you are ready to configure IBM® Sterling Secure Proxy, plan how you will implement your proxy environment and determine what level of security is required to access the server in the trusted zone.

Determine the Communications Protocol

Sterling Secure Proxy supports four protocols. Identify the protocol required for your environment, as defined below:

- IBM Sterling Connect:Direct®—if you are using Sterling Secure Proxy to communicate between two Sterling Connect:Direct nodes or between a Sterling Connect:Direct node and an IBM Sterling B2B Integrator Sterling Connect:Direct server adapter, configure a Sterling Connect:Direct proxy adapter.
- FTP—configure an FTP reverse proxy adapter if you are using Sterling Secure Proxy to communicate between an FTP client and Sterling B2B Integrator.
- HTTP—configure an HTTP reverse proxy adapter if you are using Sterling Secure Proxy to communicate between an HTTP client and Sterling B2B Integrator.
- SFTP—configure an SFTP reverse proxy adapter if you are using Sterling Secure Proxy to communicate between an SSH client and Sterling Integrator.

Follow the instructions in the scenario chapters to configure Sterling Secure Proxy for a protocol. If you plan to use more than one protocol, completely test and configure one protocol before adding a configuration for another protocol.

Determine Validation Requirements for Inbound Nodes

Determine security policy requirements for inbound trading partners (inbound nodes) to Sterling Secure Proxy. Security options include:

- Require no authentication.
- Configure inbound node matching to allow only specific hosts to connect to Sterling Secure Proxy.
- Validate the user ID by comparing it to information stored in the Sterling Secure Proxy local user store. Validate the certificate by comparing it to information in the Sterling Secure Proxy local certificate store.
- Validate the trading partner (client) user ID and/or certificate using IBM Sterling External Authentication Server. Some of the validation methods that can be implemented using Sterling External Authentication Server include:
  - Query an LDAP or HTTP server to validate dates and signature on an inbound certificate
  - Authenticate user Common Name (CN) specified in the certificate of the inbound node or group name with which the CN is associated
  - Validate attributes of the certificate against information stored on LDAP server
  - Validate certificate against a certificate revocation list (CRL) stored on LDAP or HTTP server

– Authenticate the user ID and password submitted as logon credentials for the target server by comparing them against information stored on an LDAP or TAMS server and authorize access

Determine Requirements for Connection to Outbound Node

Identify requirements for connection to the Sterling B2B Integrator Server or Sterling Connect:Direct Node secure outbound node. Possible requirements include:

- Not requiring that the user ID and password be authenticated in Sterling Secure Proxy. The user ID and password provided by the trading partner is passed to the Sterling B2B Integrator or Sterling Connect:Direct server for authentication.
- Connecting to the Sterling B2B Integrator or Sterling Connect:Direct server (outbound node) using a user ID and password stored in the Sterling Secure Proxy netmap configuration.
- Connecting to the Sterling B2B Integrator or Sterling Connect:Direct server (outbound node) using information accessed from Sterling External Authentication Server. The Sterling External Authentication Server server determines whether an alternate user ID and password mapped to the trading partner (client) user ID should be used to connect to the outbound Sterling B2B Integrator or Sterling Connect:Direct server.

Set Up a Password Policy

You can identify security requirements for a group of users and then configure a password policy to define the security requirements. After you define a password policy, you can apply it to users who configure the Sterling Secure Proxy environment or to users who connect to the Sterling Secure Proxy engine and send files to a secure server.

Refer to *Manage User Accounts and Passwords* on the documentation library for instructions on defining a password policy and associating it with a user.

Set Up User Accounts to Configure the Sterling Secure Proxy Environment

You must create user accounts for users who will access the Sterling Secure Proxy Configuration Manager tool to configure the Sterling Secure Proxy environment. You can create operator users who have read-only access or define administrator users who have full access to Configuration Manager.

Refer to *Manage User Accounts and Passwords* on the documentation library for instructions on defining Configuration Manager users.

Set Up Users for Inbound Connections

Depending upon your configuration, you may need to create a user account for a trading partner who plans to connect to the Sterling Secure Proxy engine to transfer files to Sterling B2B Integrator or Sterling Connect:Direct server to authenticate the user ID and password in the Sterling Secure Proxy local user store.

Refer to *Manage User Accounts and Passwords* on the documentation library for instructions to define inbound users.

Determine Security Requirements for Communications

When you install CM and an engine, a secure communications channel is required to communicate. By default, the SSL communication is configured using a single key for both the engine and the system where the web server and CM are installed.

To secure the communication between these components, replace the factory certificates. Refer to *Manage Certificates Between Sterling Secure Proxy Components* on the documentation library for instructions.

Configure a Sterling External Authentication Server

An advanced method of user and certificate authentication is provided through an optional IBM product named Sterling External Authentication Server. If you plan to use this tool to authenticate users or certificates, you must configure a Sterling External Authentication Server.

Refer to *Configure Sterling Secure Proxy for Sterling External Authentication Server* on the documentation library for instructions on configuring a Sterling External Authentication Server.

Configure a Remote Perimeter Server

A local perimeter server (internal) is installed with Sterling Secure Proxy and will be used to manage communications. You can install a remote perimeter server if you want an additional perimeter server.

Refer to *Configure Perimeter Servers to Manage Sterling Secure Proxy Communications* on the documentation library for sample implementations of the remote perimeter server and for instructions on configuring a remote perimeter server. Refer to *Install a Remote Perimeter Server Overview* for instructions on installing a remote perimeter server.

Chapter 2. Install Sterling Secure Proxy Perimeter Servers

Install a Remote Perimeter Server Overview

Sterling Secure Proxy uses perimeter servers to increase security between internal and external communications. A local perimeter server (internal) is installed with Sterling Secure Proxy. The local mode server is useful in environments that do not require a DMZ solution.

To configure your environment so that your firewall only allows connections established from inside a more secure environment, install a remote perimeter server in a DMZ. You configure the remote perimeter servers within Sterling Secure Proxy. After you install and configure a remote perimeter server, you map how the perimeter server is used: inbound, outbound, or External Authentication. For more information, refer to

- *Configure Perimeter Servers to Manage Sterling Secure Proxy Communications*
- *Configure a Remote Perimeter Server*

Perimeter Server Installation Prerequisites

Prior to installing and configuring a perimeter server on a remote system, you must complete the following tasks and gather the required information:

- Install CM and the engine.
- Go to the directory that contains the downloaded perimeter server installer files.
- Obtain the IP address for both the remote perimeter server computer and the engine computer.
- If you plan to install the perimeter server in a less secure network zone than the Sterling Secure Proxy engine, open the port for connections from the engine to the remote perimeter server computer on which you plan to install your perimeter server.
- If you plan to install the perimeter server in a more secure network zone than the Sterling Secure Proxy engine, open the port for connections from the remote perimeter server computer on which you plan to install your perimeter server to the engine.

Perimeter Server Installation Guidelines

When you install a perimeter server, follow these guidelines:

- Each perimeter server is limited to two TCP/IP addresses: internal interface and external interface. Internal interface is the TCP/IP address that the perimeter server uses to communicate with the engine. External interface is the TCP/IP address that the perimeter server uses to communicate with trading partners.

  To use additional TCP/IP addresses, install additional perimeter servers.
- To install an additional perimeter server on a computer with an existing instance, install the new perimeter server in unique installation directory.
- To upgrade an existing perimeter server, install a new instance of perimeter server in the installation directory of the existing perimeter server.
- The combination of internal TCP/IP address and port must be unique for all perimeter servers installed on one computer.

- If a perimeter server is installed using the wildcard address, then all ports must be unique.
- If a perimeter server is installed using the wildcard address, then its port is not available for use by service adapters that use the server or any other perimeter server on that computer.
- The internal and external interface may use the same TCP/IP address. However, the port used by the perimeter server is not available to the service adapters that use the server.

Install Remote Perimeter Server in a More Secure Network on UNIX or Linux

About this task

To install a perimeter server in a more secure network than your Sterling Secure Proxy server:

Procedure

1. Navigate to the directory containing the downloaded perimeter server installer file for your platform.

Platform	Installation File Name
IBM System p5 and IBM Power system	PS.V3410.AIX.bin
HP Integrity system with Intel Itanium processor	PS.V3410.HP-IA.bin
HP 9000 (PA-RISC)	PS.V3410.HP.bin
x64/x86 Linux (32-bit)	PS.V3410.Linux.bin
x64/x86 Linux (64-bit)	PS.V3410.Linux_X64.bin
Sun SPARC system	PS.V3410.SolarisSPARC.bin

2. Copy the perimeter server installation file for your platform to your home directory or base directory. If you are using FTP to copy the file, make sure your session is set to binary mode.
3. To begin the installation, type the installation file name and press **Enter**.

   The installation program displays the Introduction screen.
4. Press **Enter** to continue the installation.

   If you type `quit`, the installation program will terminate.
5. Read the License Agreement information. Press **Enter** to page through the license agreement. When you are prompted to accept the License Agreement, press `Y` or `y`. The Choose Installation Folder screen is displayed.
6. Press **Enter** to accept the default installation folder, or type the absolute path name of the directory where the perimeter server will be installed.
7. Confirm that the installation directory is correct by typing `Y` or `y`. The Network Zone screen is displayed.
8. Type `2` to install the perimeter server in a more secure network. The installation program displays a list of network interfaces available on the perimeter server host.

9. Select the network interface for the perimeter server to use to communicate with the Sterling Secure Proxy engine, or press **Enter** if a specific interface address is not required.
10. Type the port number of the local port the perimeter server will use to communicate with the Sterling Secure Proxy engine. Specify a port number greater than or equal to 1024. If a specific port is not required, press **Enter**.

    The installation program displays a list of network interfaces available on the perimeter server host.
11. Select the network interface for the perimeter server to use to communicate with the backend server, or press **Enter** if a specific interface address is not required.
12. Type the hostname or IP address of the Sterling Secure Proxy engine host that will be connected to this perimeter server.
13. Type the port number the Sterling Secure Proxy engine will listen on for requests from the perimeter server.
14. Verify the Post-Installation Summary information, and press **Enter**.

    When the perimeter server is installed, the installation program displays an Installation Complete message.
15. Press **Enter** to exit the installation.
16. Change to the installation directory.
17. Type `startupPS.sh` to start the perimeter server.

Install a Remote Perimeter Server in a Less Secure Network on UNIX or Linux

About this task

To install a perimeter server in a less secure network than your Sterling Secure Proxy server:

Procedure

1. Navigate to the directory containing the downloaded perimeter server installer file for your platform.

Platform	Installation File Name
IBM System p5 and IBM Power System	PS.V3410.AIX.bin
HP Integrity system with Intel Itanium processor	PS.V3410.HP-IA.bin
HP 9000 (PA-RISC)	PS.V3410.HP.bin
x64/x86 Linux (32-bit)	PS.V3410.Linux.bin
x64/x86 Linux (64-bit)	PS.V3410.Linux_X64.bin
Sun SPARC system	PS.V3410.SolarisSPARC.bin

2. Copy the perimeter server installation file for your platform to your home directory or base directory. If you are using FTP to copy the file, make sure your session is set to binary mode.
3. To begin the installation, type the installation file name and press **Enter**.

   The installation program displays the Introduction screen.

4. Press **Enter** to continue the installation.

   If you type `quit`, the installation program will terminate.
5. Read the License Agreement information. Press **Enter** to page through the license agreement. When you are prompted to accept the License Agreement, press Y or `y`. The Choose Installation Folder screen is displayed.
6. Press **Enter** to accept the default installation folder, or type the absolute path name of the directory where the perimeter server will be installed.
7. Confirm that the installation directory is correct by typing Y or `y`. The Network Zone screen is displayed.
8. Type 1 to install the perimeter server in a less secure network. The installation program displays a list of network interfaces available on the perimeter server host.
9. Select the network interface for the perimeter server to use to communicate with the Sterling Secure Proxy engine, or press **Enter** if a specific interface address is not required.
10. Type the port number of the local port the perimeter server will listen on for requests from the Sterling Secure Proxy engine. Specify a port number greater than or equal to 1024. Press **Enter**. The installation program displays a list of network interfaces available on the perimeter server host.
11. Select the network interface for the perimeter server to use to communicate with trading partners, or press **Enter** if a specific interface address is not required.
12. Verify the Post-Installation Summary information, and press **Enter**.

    When the perimeter server is installed, the installation program displays an Installation Complete message.
13. Press **Enter** to exit the installation.
14. Change to the installation directory.
15. Type `startupPS.sh` to start the perimeter server.

Install Remote Perimeter Server in a More Secure Network in Windows

About this task

To install a perimeter server in a more secure network in a Windows environment:

Procedure

1. Navigate to the directory containing the downloaded perimeter server installer file for your platform.

Platform	Installation File Name
Windows Server 2003 Enterprise Edition Service Pack 1 (32-bit)	PS.V3410.Win.exe
Windows Server 2008 R2 (64-bit)	PS.V3410.Win_X64.exe

2. Copy the perimeter server installation file for your platform to the Windows server. If you are using FTP to copy the file, be sure your session is set to binary mode.
3. To begin the installation, run the perimeter server installation .exe file.

   The installation program displays the Introduction screen.
4. Click **Next** to continue the installation.

5. Read the License Agreement information, accept the terms of the License Agreement, and click **Next**. The Choose Installation Folder screen is displayed.
6. Click **Next** to accept the default installation folder, click **Choose** to navigate to an installation folder, or type the absolute path name of the directory where the perimeter server will be installed and click **Next**.

   The Network Zone screen is displayed.
7. Select the Perimeter Server in a more-secure zone button, and click **Next**. The installation program displays a list of network interfaces available on the perimeter server host.
8. Select the network interface for the perimeter server to use to communicate with the Sterling Secure Proxy engine, or click **Next** if a specific interface address is not required.
9. Type the port number of the local port the perimeter server will use to communicate with the Sterling Secure Proxy engine. Specify a port number greater than or equal to 1024. If a specific port is not required, click **Next**.

   The installation program displays a list of network interfaces available on the perimeter server host.
10. Select the network interface for the perimeter server to use to communicate with the backend server, or click **Next** if a specific interface address is not required.
11. Type the hostname or IP address of the Sterling Secure Proxy engine host that will be connected to this perimeter server.
12. Type the port number the Sterling Secure Proxy engine will listen on for requests from the perimeter server, and click **Next**.
13. Verify the Pre-Installation Summary, and click **Next**.

    When the perimeter server is installed, the installation program displays an Installation Complete message.
14. Click **Done** to exit the installation.
15. Change to the installation directory.
16. Do one of the following:
    - Run startPSService.cmd to start the perimeter server.
    - Configure the perimeter server service to start automatically as a Windows Service at system startup.

Install Remote Perimeter Server in a Less Secure Network in Microsoft Windows

About this task

To install a perimeter server in a less secure network in a Microsoft Windows environment:

Procedure

1. Navigate to the directory containing the downloaded perimeter server installer file for your platform.

Platform	Installation File Name
Microsoft Windows Server 2003 Enterprise Edition Service Pack 1 (32-bit)	PS.V3410.Win.exe

Platform	Installation File Name
Microsoft Windows Server 2008 R2 (64-bit)	PS.V3410.Win_X64.exe

2. Copy the perimeter server installation file for your platform to the Microsoft Windows server. If you are using FTP to copy the file, be sure your session is set to binary mode.
3. To begin the installation, run the perimeter server installation .exe file.

   The installation program displays the Introduction screen.
4. Click **Next** to continue the installation.
5. Read the License Agreement information, accept the terms of the License Agreement, and click **Next**. The Choose Installation Folder screen is displayed.
6. Click **Next** to accept the default installation folder, click **Choose** to navigate to an installation folder, or type the absolute path name of the directory where the perimeter server will be installed and click **Next**.

   The Network Zone screen is displayed.
7. Select the Perimeter Server in a less-secure zone button, and click **Next**. The installation program displays a list of network interfaces available on the perimeter server host.
8. Select the network interface for the perimeter server to use to communicate with the Sterling Secure Proxy engine, or click **Next** if a specific interface address is not required.
9. Type the port number of the local port the perimeter server will listen on for requests from the Sterling Secure Proxy engine. Specify a port number greater than or equal to 1024. Click **Next**.

   The installation program displays a list of network interfaces available on the perimeter server host.
10. Select the network interface for the perimeter server to use to communicate with trading partners, or click **Next** if a specific interface address is not required.
11. Verify the Pre-Installation Summary information, and click **Next**.

    When the perimeter server is installed, the installation program displays an Installation Complete message.
12. Click **Done** to exit the installation.
13. Change to the installation directory.
14. Do one of the following:
    - Run startPSService.cmd to start the perimeter server.
    - Configure the perimeter server service to start automatically as a Microsoft Windows Service at system startup.

Chapter 3. Install Sterling Secure Proxy on Microsoft Windows

Install or Upgrade Sterling Secure Proxy on Microsoft Windows

Before you install Sterling Secure Proxy, review the system requirements. Confirm that your system meets all requirements. Follow the procedures to install or upgrade Sterling Secure Proxy.

Sterling Secure Proxy Startup Worksheet for Microsoft Windows

Use the worksheet to record the host name or IP address of CM and the engine, listen ports, and the URL for the CM log in screen. You refer to this information when you use the application and set up your environment. If you change this information, use this worksheet to record your changes.

Note: When assigning ports, check that ports are not used by other software.

CM	Defined at Installation	New
Host name or IP address of CM		
CM listen port		
Web server listen port		
URL to Connect to CM		

Engine	Defined at Installation	New
Host name or IP address of the engine		
Engine listen port		

Install or Upgrade the Engine on Microsoft Windows

About this task

Use this procedure to install or upgrade the engine.

If you installed version 3.0 or later, you can upgrade to this version by installing over the existing files. If you install this version in the same directory, the passphrases and port definitions are maintained as well as configuration and log files. All adapter definitions created in the previous version can be used in the new installation.

At installation, define a passphrase for CM and the engine, to ensure that files are secure. A passphrase is six or more characters and contains any characters. The passphrase for CM is independent of the engine passphrase. To start CM or the engine, type the passphrase. You type the passphrase at shutdown.

To install or upgrade an engine on Microsoft Windows:

Procedure

1. Navigate to the directory where you downloaded the Sterling Secure Proxy installation file for Microsoft Windows.
2. Double-click the Sterling Secure Proxy.V3410.Windows.zip file to extract the Sterling Secure Proxy engine, CM, and perimeter server installation files for Microsoft Windows.
3. Take one of the following actions:
   - To install the engine on Microsoft Windows Server 2003 (32-bit), double-click SSP.V3410.Win.exe.
   - To install the engine on Microsoft Windows Server 2008 (64-bit), double-click SSP.V3410.Win_X64.exe.
4. After the introduction, click **Next**.
5. Scroll down in the license agreement and read the agreement. Click the radio button to accept the terms and click **Next**.
6. Accept the default directory, or click **Choose** to navigate to a different directory. For an upgrade, change to the directory where the previous version is installed. Click **Next**.
7. To continue a new installation:
   a. Accept the default value 63366 for the engine listen port or specify a different port. Record the engine listen port on the Startup Worksheet and click **Next**.
   b. Type a passphrase. Retype the passphrase and click **Next**.
8. To continue an upgrade, specify the directory where the previous version is installed and press **Next**. A prompt indicates the Sterling Secure Proxy installation already exists.
9. Review the pre-installation summary. Click **Install**.
10. At the Installation Complete screen, click **Done**.
11. If you are upgrading Sterling Secure Proxy and HSM was enabled, you must run the setupHSM script after the upgrade to reenable HSM. Refer to the setupHSM command in the documentation library for more information.

Install or Upgrade CM on Microsoft Windows

About this task

Use this procedure to install or upgrade CM.

If you previously installed version 3.0 or later of CM, you can upgrade to this version by installing over the existing files. If you install this version in the same directory, the passphrases and ports are maintained as well as configuration, log files, and adapter definitions.

To install or upgrade CM on Microsoft Windows:

Procedure

1. Navigate to the directory where you extracted the CM installation files from the archive in the previous procedure.
2. Take one of the following actions:

- To install the CM on Microsoft Windows Server 2003 (32-bit), double-click SSPcm.V3410.Win.exe.
- To install the CM on Microsoft Windows Server 2008 (64-bit), double-click SSPcm.V3410.Win_X64.exe.

3. After the introduction, click **Next**.
4. At the end of the license agreement, click the radio button to accept the terms and click **Next**.
5. Accept the default directory, or click **Choose** to navigate to a different directory. For an upgrade, change to the directory where the previous version is installed. Click **Next**.
6. Perform the following steps to continue a new installation:
   a. Accept the default value 62366 for the CM listen port or specify a different port. Record the CM listen port on the Startup Worksheet. Click **Next**.
   b. Type a passphrase. Retype the passphrase and click **Next**.
   c. Accept the default value of 8443 for the web server listen port or specify a different port. Record the web server listen port on the Startup Worksheet. Click **Next**.
7. To continue an upgrade, specify the directory where the previous version is installed and press **Next**. A prompt displays the directory and a message indicating that the Sterling Secure Proxy installation already exists.
8. Review the pre-installation summary before continuing. Click **Install**.
9. At the Installation Complete screen, click **Done**.
10. If you are upgrading Sterling Secure Proxy and HSM was enabled, you must run the setupHSM script after the upgrade to reenable HSM. Refer to the setupHSM command in the documentation library for more information.

Create an Engine Definition - Microsoft Windows

About this task

The engine resides in the DMZ and runs the proxy adapters that manage client communication requests to servers in your trusted zone. perform this function, the engine receives configuration information from CM. Use CM to create an engine definition that contains configuration information for the engine.

Before you configure the engine, gather the following information that you will need to configure the engine. After you configure the engine, validate the configuration by ensuring that CM can view the engine.

CM Field	Feature	Value
Engine Name	Name of the engine	
Engine Host	IP address of the engine	
Engine Listen Port	Port number of the engine	

To define an engine:

Procedure

1. If necessary, select Configuration from the menu bar.
2. Click **Actions** > **New Engine**.
3. Specify the following values:

- **Engine Name**
- **Engine Host**
- **Engine Listen Port**

4. Click **Save**.
5. Verify that the engine is running. Refer to *Start and Stop Sterling Secure Proxy* on the documentation library for instructions.

Chapter 4. Install Sterling Secure Proxy on UNIX

Install or Upgrade Sterling Secure Proxy on UNIX or Linux

Before you install Sterling Secure Proxy, review the system requirements. Confirm that your system meets all requirements. Follow the procedures to install or upgrade Sterling Secure Proxy.

Verify your installation by starting CM and the engine, and ensuring that they can communicate.

Install or Upgrade the Engine on UNIX or Linux

About this task

Use this procedure to install or upgrade the engine.

If you previously installed version 3.0 or later of the engine, you can upgrade to this version by installing over the existing files. If you upgrade the engine, the passphrases and port definitions are maintained as well as configuration and log files. All adapter definitions created in the previous version can be used in the new installation.

To install or upgrade an engine on UNIX or Linux:

Procedure

1. Navigate to the directory where you downloaded the Sterling Secure Proxy installation file.

   Refer to the following table to identify the file to install the engine on your operating system:

Hardware	File
IBM System p5 and IBM Power System	SSP.V3410.AIX.bin
HP Integrity system with Intel Itanium processor	SSP.V3410.HP-IA.bin
HP 9000 (PA-RISC)	SSP.V3410.HP.bin
x64/x86 Linux (32-bit)	SSP.V3410.Linux.bin
x64/x86 Linux (64-bit)	SSP.V3410.Linux_X64.bin
Sun SPARC system	SSP.V3410.SolarisSPARC.bin

   Note: Log on to the UNIX system with the privileges required to install software.
2. Type the following command to retrieve the Sterling Secure Proxy engine, CM, and perimeter server installation files from the archive:

   `tar xvf` *`SSP installation file`*
3. Type the name of the engine installation file for your platform and press **Enter**.
4. Read the terms of the license agreement. At the end of the agreement, type `Y` at the prompt.

5. For a new installation, perform the following steps:
   a. When prompted for the installation location, press **Enter** to accept the default directory or specify a different directory.
   b. Accept the default value 63366 for the engine listen port or specify a different port. Record the engine listen port on the Startup Worksheet, and press **Enter**.
   c. Type a passphrase and press **Enter**. You need this passphrase in the future.
   d. Retype the passphrase and press **Enter**.
6. For an upgrade, perform the following steps:
   a. Specify the directory where the previous version is installed and press **Enter**. A prompt displays the directory and a message indicating that the Sterling Secure Proxy installation already exists.
   b. Type `C` to continue.
7. Review the pre-installation summary, and press **Enter**.
8. Press **Enter**. The command prompt is displayed.
9. If you are upgrading Sterling Secure Proxy and HSM was enabled, you must run the setupHSM script after the upgrade to reenable HSM. Refer to the setupHSM command in the documentation library for more information.

Install or Upgrade CM on UNIX or Linux

About this task

Use this procedure to install or upgrade CM.

If you previously installed version 3.0 or later of CM, you can upgrade to this version by installing over the existing files. After you upgrade, the passphrases and port definitions from the previous version are maintained as well as configuration and log files. All previously defined adapter definitions can be used in the new installation.

To install or upgrade CM on UNIX or Linux:

Procedure

1. Navigate to the directory where you extracted the CM installation file from the archive in the previous procedure.

   Refer to following table to identify the file to use to install CM on your operating system:

Hardware	File
IBM System p5 and IBM Power System	SSPcm.V3410.AIX.bin
HP Integrity system with Intel Itanium processor	SSPcm.V3410.HP-IA.bin
HP 9000 (PA-RISC)	SSPcm.V3410.HP.bin
x86 Linux (32-bit)	SSPcm.V3410.Linux.bin
x64 Linux (64-bit)	SSPcm.V3410.Linux_X64.bin
Sun SPARC system	SSPcm.V3410.SolarisSPARC.bin

Note: Log on to the UNIX system with the privileges required to install software.

2. Type the name of the CM installation file for your platform and press **Enter**.
3. Read the terms of the license agreement. At the end of the agreement, type `Y` at the prompt.
4. For a new installation, perform the following steps:
   a. When prompted for the installation location, press **Enter** to accept the default directory or specify a different directory.
   b. Accept the default value 62366 for the CM listen port, or specify a different port. Record the CM listen port on the Startup Worksheet, and press **Enter**
   c. Type a passphrase and press **Enter**. You need this passphrase in the future.
   d. Retype the passphrase and press **Enter**.
   e. Accept the default value of `8443` for the web server listen port or specify a different port. Record the web server listen port on the Startup Worksheet, and press **Enter**.
5. For an upgrade, perform the following steps:
   a. Specify the directory where the previous version is installed and press **Enter**. A prompt displays the directory and a message indicating that the Sterling Secure Proxy installation already exists.
   b. Type `C` to continue.
6. Review the pre-installation summary, and press **Enter**.
7. Press **Enter**. The command prompt is displayed.
8. If you previously configured a single sign on HTTP adapter, open property tab and you will find the url used for SSP3.2 was not removed.
9. If you are upgrading Sterling Secure Proxy and HSM was enabled, you must run the setupHSM script after the upgrade to reenable HSM. Refer to the setupHSM command in the documentation library for more information.

Create an Engine Definition - UNIX

About this task

The engine resides in the DMZ and runs the proxy adapters that handle client communication between clients and servers in your trusted zone. The engine receives configuration information from CM. You create an engine definition using CM.

Before you configure the engine, gather the following information. After you create the engine definition, validate the configuration by ensuring that CM can view it.

CM Field	Feature	Value
Engine Name	Name of the engine	
Engine Host	IP address of the engine	
Engine Listen Port	Port number of the engine	

To define an engine:

Procedure

1. Click **Configuration** from the menu bar.
2. Click **Actions** > **New Engine**.
3. Specify the following values:
   - **Engine Name**
   - **Engine Host**
   - **Engine Listen Port**
4. Click **Save**.

   Verify that the engine is running. Refer to *View Configured Engines* and *Manage Sterling Secure Proxy* on the documentation library for instructions.

Notices

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

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

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

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

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

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

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

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

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

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

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

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

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

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

Printed in USA