Sterling Secure Proxy®

Installation Guide

Version 3.1

Sterling Secure Proxy Installation Guide
Second Edition

Contents

Chapter 4 Install or Upgrade SSP on Windows   29

Chapter 5 Post Installation Tasks   39

Contents

Chapter 6 Upgrade SSP from Version 2.0.x to Version 3.x   51

Chapter 7 Install a Remote Perimeter Server   85

SSP Overview

Sterling Secure Proxy (SSP) acts as an application proxy between Connect:Direct nodes or between a client application and a Gentran Integration Suite (GIS). It provides a high level of data protection between external connections and your internal network. Define an inbound node definition for each trading partner connection from outside the company and an outbound node definition for every company server to which SSP will connect.

Following is an illustration of the SSP general proxy environment:
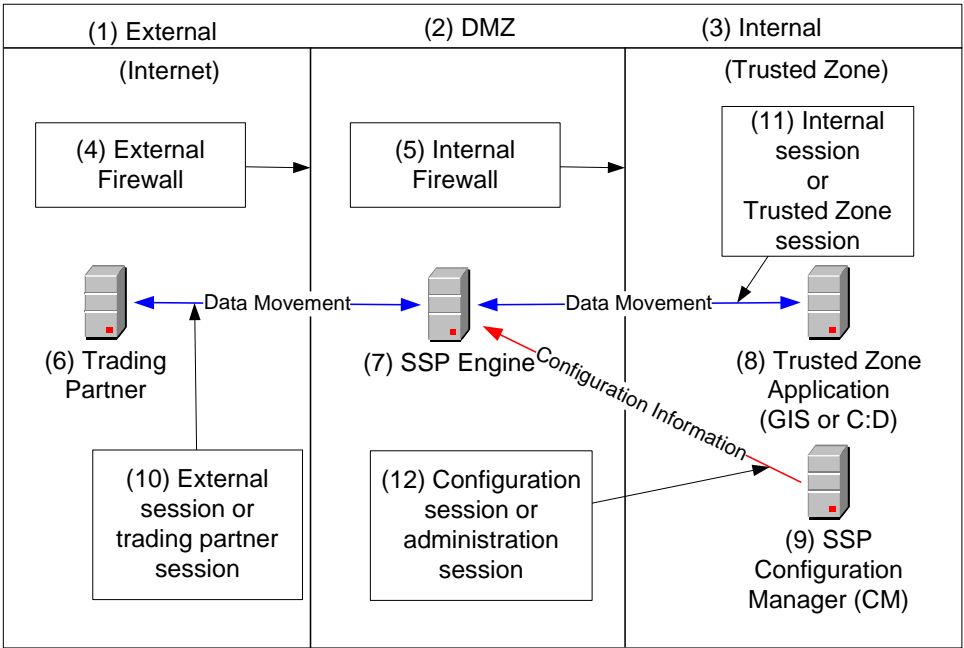
Configuration Overview

The SSP architecture requires that only the minimum amount of configuration information be stored in the DMZ. It includes two components: the Configuration Manager (CM) and an engine. Configuration data is stored at the CM, is encrypted, and does not require a database. The CM is installed on the internal or trusted network.

The engine resides in the DMZ and receives configuration data from CM. The engine stores engine properties on disk in the DMZ and the files are encrypted. The properties contain the minimum information required to accept and secure a connection from CM. It includes the IP address and port that the SSP engine listens on for the CM connection. It also includes the SSL key certificate, trusted certificate, and encryption cipher that will be used to secure the connection with CM.

When the engine is first started, it does not have configuration information. It listens on the configured IP address and port for a connection from CM, which tries to connect to the engine at a configurable interval. When CM connects to the engine, they negotiate an SSL session and secure the connection.

After the channel is secure, CM pushes the configuration to the engine. The engine reads the configuration and starts the appropriate proxy services. When you update a configuration in CM, it transfers the updates to the engine.

Following is a illustration of the SSP flow of a configuration push:
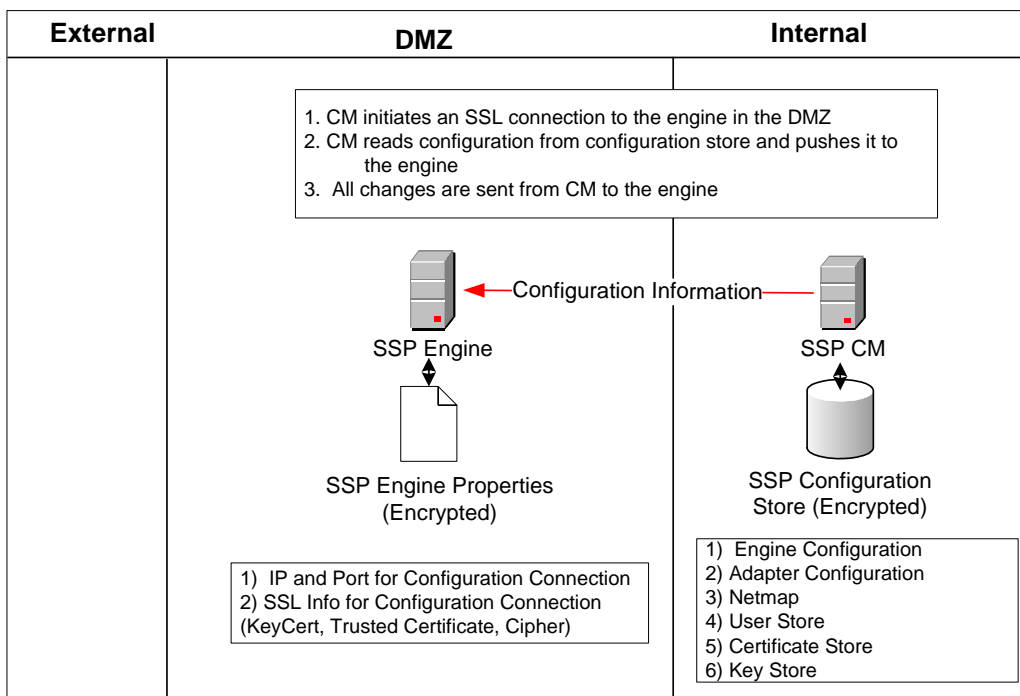
SSP Terminology

SSP architecture is described below:

SSP Engine—the engine resides in the DMZ and contains the minimum components necessary to manage communications sessions. The engine configuration (SSP engine properties) is created at CM and pushed to the engine. It is stored in active memory and is never stored on disk in the DMZ. No web services or UI ports are open in the DMZ.

Configuration Manager (SSP CM)—CM is installed in the trusted zone. Use this tool to configure your environment. When you save a configuration definition (SSP configuration store) at CM, it is pushed to an engine, using an SSL session. Configuration files are encrypted and stored on the computer where CM is installed.

Note: Only one CM should update an engine definition.

SSP configuration store—This file is encrypted on disk and contains the following information:

✦ The user store with information on user credentials

✦ The system certificate store with the certificates used for SSL/TLS sessions

✦ The key store with the SSH keys

✦ The engine configuration store with all configuration information for the engine

SSP engine properties file—These files are encrypted and contain the following information:

✦ The IP and port number to listen on for connections from CM

✦ SSL key certificate, trusted certificate, and encryption cipher used for the connection from CM

Web server—CM is installed with a web server. You open a browser and access CM through a Web page to configure SSP and monitor the engine activity. The web server is installed when you install CM.

Adapter—an adapter identifies the protocol allowed for connections from trading partners. You can accept connections from clients that use different protocols; however, you must define a different adapter for each protocol. A single engine can run multiple adapters. In an adapter definition, you identify the port on which to listen for connections, the netmap to use with the adapter, the security policy, and the routing method to use. If you are using External Authentication, you identify the EA server to use in the adapter definition. If you are using a remote server, you identify the server to use in the adapter definition.

Netmap—define a netmap to identify the trading partners authorized to communicate through SSP and the company servers where connections are made.

Policy—define a policy to identify the security features to implement for an inbound node definition or a Connect:Direct node definition.

Sterling External Authentication Server (EA)—a separately installed feature of SSP, EA allows you to validate digital certificates passed by the client or trading partner during SSL/TLS session requests. You can also validate certificates against one or more certificate revocation lists (CRLs),

---

and validate certificates based on the valid date range. See the Sterling External Authentication Server documentation for more information.

EA can be configured to validate certificates and authenticate users. The functions performed by EA are defined in an EA definition. EA performs one or more of the following functions:

✦ Certificate Validation

✦ Certificate Revocation List (CRL)

✦ Multi-factor Authentication

✦ Certificate Policy Enforcement

✦ LDAP Authentication

✦ User ID mapping—remote trading partners can be given IDs and passwords that do not provide access to internal systems; the ID and password presented by the trading partner is mapped to an ID and password that can then access the internal system

✦ TAM (Tivoli Access Manager) Authentication

✦ Generic Authentication

Before you can use EA with SSP, you must configure EA server definitions in SSP. Then, when configuring policies and protocol adapters, you select these server definitions. You can also select security features available in EA such as certificate authentication, user authentication, and user mapping. Refer to the Sterling External Authentication Server help for more information.

For more detailed information on SSP and its features, refer to the *Sterling Secure Proxy Configuration Guide*.

Before You Begin

System requirements for Sterling Secure Proxy vary with your business needs and system environment. Contributing factors include:

✦ Number of transactions processed

✦ Amount of data transferred

✦ Running Sterling Secure Proxy with or without perimeter servers

Review the requirements before you begin the installation tasks.

SSP UNIX and Linux System Requirements

You can install SSP on a UNIX or Linux operating system. This section identifies the system requirements for supported UNIX and Linux platforms. For each operating system, a JRE is installed with SSP.

Configuration information is maintained on both Configuration Manager (CM) and the engine. The space required to store configuration files depends on the size of the files you transmit and how long you maintain the files, as well as the level of logging you configure. The minimum space requirements in the following table identify the amount of space required if you turn on debugging.

SSP UNIX and Linux Host System Requirements

SSP requires the following minimum software RAM and disk space requirements on a UNIX or Linux host system:

Component	File Descriptor Size	RAM Minimum	Disk Space Minimum
CM	N/A	512 MB	2 GB
Engine	N/A	1 GB	2 GB
Remote Perimeter Server	2048 or greater (preferred setting is unlimited)	1 GB	2 GB

SSP UNIX or Linux Operating Systems Supported

SSP runs on multiple UNIX and Linux operating systems. The following table identifies the operating systems supported.

For a list of operating systems supported on a remote perimeter server, refer to *Remote Perimeter Server JDK and Patch Level Requirements in UNIX or Linux* on page 12.

Hardware	Operating System
HP Integrity system with Intel Itanium	HP-UX, version 11.23
HP PA-RISC	HP-UX, version 11.11
	HP-UX, version 11.23
IBM System p5 and IBM Power Systems	AIX 5L, version 5.3
Linux 64-bit	Red Hat Enterprise Linux Advanced Platform, version 5
x86-32bit	Red Hat Enterprise Linux Advanced Server, version 4
	Red Hat Enterprise Linux Advanced Platform, version 5
	SuSE SLES, version 9
	SuSE SLES, version 10
Solaris Intel system (x86)	Solaris, version 10
Sun SPARC system	Solaris, version 9
	Solaris, version 10
Sun x64 system with AMD Opteron processor	Solaris, version 10

Remote Perimeter Server JDK and Patch Level Requirements in UNIX or Linux

You can install and run a remote perimeter server on UNIX or Linux. It can reside on a different computer from CM or the engine. You must install a JDK, when you implement a perimeter server.

If you require a remote perimeter server, refer to the following table for the operating systems supported and the JDK and patch level requirements:

Hardware	Operating System	JDK and Patch Level Requirements
HP Integrity system with Intel Itanium	HP-UX, version 11.23 for IA64 (Itanium)	HP-UX JDK Build 1.5.0.08 Patch requirements as determined by the HPjconfig utility. Kernel parameters as determined by the HPjconfig utility.
HP PA-RISC	HP-UX, version 11.11 or HP-UX, version 11.23	HP-UX JDK Build 1.5.0.08 Patch requirements as determined by the HPjconfig utility. Kernel parameters as determined by the HPjconfig utility.

Hardware	Operating System	JDK and Patch Level Requirements
IBM System p5	AIX, version 5.3	IBM AIX build pap32devifx-20070725 (SR5a) Minimum IBM maintenance level: 5300-05
x86-32bit	Red Hat Enterprise Linux Advanced Server, version 4 and 5 (32-bit kernel only)	IBM 1.5.0 build pxi32devifx-20070806 (SR5a) Minimum kernel version:2.6.9-42.0.10.ELsmp (32-bit only) Minimum glibc version: 2.3.4-2.25
	SuSE SLES, version 9 (32-bit kernel only)	IBM 1.5.0 build pxi32devifx-20070806 (SR5a) Minimum kernel version: 2.6.5-7.283 (32-bit only) Minimum glibc version: 2.3.3-98.73
Sun SPARC System	Solaris, version 9 and 10	Sun JDK 1.5.0_11-b03 Minimum Solaris patch requirements are: 113096-03 111711-16 111712-16 112963-29 112785-58
Solaris Intel System (x86) Sun SPARC System Sun x64 System with AMD Opteron processor	Solaris, version 10 (global zone only)	Sun JDK 1.5.0_11-b03 Minimum Solaris patch requirements are: 120900-04 121133-02 119254-32 119578-30 118822-30 118833-24

Hardware Accelerator Board

SSP supports the cryptographic Sun Crypto Accelerator 10 hardware accelerator board.

Hardware Security Module (HSM) Requirements

If you plan to store certificates on a Hardware Security Module (HSM) appliance, SSP supports the following:

✦ Eracom ProtectServer Orange/Gold PCI

✦ Eracom ProtectServer Orange/Gold External

✦ nCipher nShield PCI

✦ nCipher netHSM

SSP Windows System Requirements

You can install SSP on Windows. This section identifies the system requirements for Windows supported platforms. A JRE is installed with SSP.

Configuration information is maintained on both CM and the engine. The space required to store configuration files depends on the size of the files you transmit and how long you maintain the files, as well as the level of logging you configure. The minimum space requirements in the table below identify the amount of space required if you turn on debugging.

If you determine that you require a remote perimeter server, use this information in this section to identify the operating system supported on a remote perimeter server. You must download a JDK and install it on the same computer.

SSP Windows Host System Requirements

SSP requires the following minimum RAM and disk space requirements on a Windows system:

Component	RAM Minimum	Disk Space Minimum
CM	512 MB	2 GB
Engine	1 GB	2 GB
Remote Perimeter Server	1 GB	2 GB

SSP-Supported Windows Operating Systems

SSP supports the following Windows operating systems:

✦   Windows Server 2003 Enterprise Edition Service Pack 1 (32-bit)

✦   Windows Vista Enterprise (32-bit)

Note: The remote perimeter server installation is not supported on Windows Vista Enterprise.

Remote Perimeter Server Requirements on Windows

You can run a perimeter server (PS) on Windows, on a different computer from CM or the engine. It supports different operating systems, patch levels, and JDK versions than SSP.

The PS on Windows supports JDS 1.5.0, also called JDK 5.0. When you download the JDK, it is identified as version 5.0.

If you require a remote PS, refer to the following table for the Windows platforms supported and the JDK and patch level requirements:

Remote PS-supported OS	JDK Requirements
Windows 2003 Server Enterprise Edition R2 (32-bit)	Sun JRE 1.5.0_11
Windows 2003 Server Standard Edition R2 (32-bit)	Sun JRE 1.5.0_11

Client Connections Supported

Sterling Secure Proxy supports the following client connections and security protocols:

Client	Protocol
Connect:Direct for z/OS (formerly OS/390) version 4.5 or later	Connect:Direct (SSL, TLS)
Connect:Direct for UNIX version 3.6.01 or later	Connect:Direct (SSL, TLS)
Connect:Direct for Windows version 4.2 or later	Connect:Direct (SSL, TLS)
Connect:Direct Select version 1.1 or later	Connect:Direct (SSL, TLS)
Connect:Direct for i5/OS version 3.6.00 or later	Connect:Direct (SSL, TLS)
Connect:Direct FTP+ version 1.0.08 or later	Connect:Direct (SSL, TLS)
Gentran Integration Suite (GIS) version 4.1 or later	FTP (SSL, TLS) HTTP (SSL, TLS) SSH Connect: Direct
cURL 7.12.1 or later with OpenSSL 0.9.7a or later	FTP (SSL, TLS) HTTP
OpenSSH 4.3p2	SSH
WS_FTP Professional 2007	FTP (SSL, TLS) SSH

Web Browsers Supported

Sterling Secure Proxy supports the following web browsers:

✦ Microsoft Internet Explorer 7.x or later
✦ Firefox 3.0 or later

Server Connections Supported

Sterling Secure Proxy supports the following server connections:

✦   Connect:Direct for z/OS (formerly OS/390) version 4.5.00 or later

✦   Connect:Direct for UNIX version 3.6.01 or later

✦   Connect:Direct for Windows version 4.2 or later

✦   Connect:Direct for i5/OS version 3.6.00 or later

✦   Connect:Direct Select version 1.1 or later

✦   Gentran Integration Suite (GIS) version 4.1 or later

Sterling Security Products Supported

SSP supports the following Sterling security products:

✦   Sterling Certificate Wizard 1.2.03 or later

✦   Sterling External Authentication Server 2.1.00 or later

Install or Upgrade SSP on UNIX or Linux

Before you install SSP, review the system requirements. Review the installation resources discussed in this section, and confirm that your system meets all requirements. Follow the procedures to install or upgrade SSP. Verify your installation by starting CM and the engine, and ensuring that they can communicate.

Review Resources for UNIX or Linux

Before installation, review any network and security-specific configuration details relevant for the hardware used to install CM and the engine. Consider details that are specific to your environment.

Refer to the following list of resources as you plan the use of network and security-related resources to install and configure SSP:

Installation or Configuration Resource	SSP Usage
TCP ports	Use available port numbers, in appropriate port ranges. The following SSP components require listening ports: ◆ CM ◆ Jetty web server ◆ Engine
Internet Explorer or FireFox	Access the CM logon screen from Internet Explorer or Firefox.
CM	Install CM in the trusted company zone. You can set up multiple engines with the same CM, but only one CM can be set up to control an engine. CM port handles listen requests from the Jetty web server. The default port number is 62366.
Jetty web server	The Jetty web server is installed when you install CM, and handles listen requests from the web browser. The web server port number is an element specified in the address bar when connecting to the logon screen. The default port number for the Jetty web server is 8443.

Installation or Configuration Resource	SSP Usage
SSP engine	The engine operates during production, and routes traffic.
	Install an engine in the DMZ. The default port number is 63366.
	If you install the engine on a computer with more than one Network Interface Card (NIC), specify the IP bind address of the card associated with that engine.
	Each engine requires a different license key and engine definition.
	When you define an engine in CM, you identify either the host name or the IP address in the definition. Create only one definition for each engine you install.
Remote perimeter server	A local perimeter server is installed when you install the engine. It manages communications between the engine and other nodes. You can install a remote perimeter server separately on another computer.
Sterling External Authentication Server	To provide another level of security by authenticating users or certificates, or mapping users, install Sterling External Authentication Server (EA). For more information, refer to the Sterling External Authentication Server documentation.
Default certificates	To secure communication, SSP is configured with default certificates that are exchanged between CM and the engine. Replace these certificates with your own after installation. Refer to Managing Certificates Between SSP Components in the *Sterling Secure Proxy Configuration Guide*.

SSP Installation Checklist for UNIX or Linux

Use the following checklist to ensure that you complete all the tasks necessary to install SSP:

Installation Task	Procedure to Complete
Verify that your system meets the hardware and software requirements specified for this release.	*SSP UNIX and Linux System Requirements* on page 11.
Upgrade the engine, if you installed version 3.0 or later, or install SSP for the first time.	*Install or Upgrade the Engine on UNIX or Linux* on page 20.
If you install the engine on a computer with more than one Network Interface Card (NIC), specify the IP bind address of the NIC associated with that engine.	*Change the IP Address for an Engine* on page 22.
Upgrade CM, if you installed version 3.0 or later, or install CM for the first time.	*Install or Upgrade CM on UNIX or Linux* on page 22.

Installation Task	Procedure to Complete
Obtain a temporary license key and copy it to the appropriate directory.	*Obtain the Temporary License Key File for UNIX or Linux* on page 24.
Request and install a permanent license key.	*Obtain the Permanent License Key File for UNIX or Linux* on page 24.
Start the engine.	*Start the Engine on UNIX or Linux* on page 24.
Start and log onto CM.	*Start and Log On to CM on UNIX or Linux* on page 25.
Create an engine definition in CM.	*Create an Engine Definition* on page 26.
Verify the engine and CM connection.	*View Configured Engines* on page 27.
Obtain and check in certificates for the connection between CM and the Jetty web server.	*Manage Certificates between SSP Components* in the *Sterling Secure Proxy Configuration Guide.*
Obtain and check in certificates for the connection between the engine and CM.	*Manage Certificates between SSP Components* in the *Sterling Secure Proxy Configuration Guide.*
Determine if your environment requires a remote perimeter server.	*Configure Perimeter Servers to Manage SSP Communications* in the *Sterling Secure Proxy Configuration Guide.*
If required, install a remote perimeter server.	*Install a Remote Perimeter Server* on page 85.

About Passphrases

At installation, you define a passphrase for CM and the engine, which ensures that CM files are secure. A passphrase is six or more characters long and contains any combination of characters. The passphrase for CM is independent of the engine passphrase.

To start CM or the engine on UNIX or Linux, type the passphrase. You must type the passphrase at shutdown.

Note: You can change the passphrase for CM and the engine after installation. Ensure that you manage this information carefully because you need the current passphrase to operate the product. If you forget your passphrase, reinstall the product.

SSP Startup Worksheet for UNIX or Linux

Use the following worksheet to record the host name or IP address of CM and the engine, related listening ports, and the URL for the CM logon screen created at installation. You refer to this information to 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		
CM listen port		
Web server listen port		

URL to Connect to CM		

Engine	Defined at Installation	New
Host name or IP address		
Listen port		

Install or Upgrade the Engine on UNIX or Linux

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:

1. Take one of the following actions:

    ◆   If you download SSP from the Sterling Commerce Customer Center, navigate to the directory where you downloaded the engine installation file.

    ◆   If you download SSP from the ESD Portal, navigate to the directory where you downloaded the engine installation file.

◆ If you install SSP from the distribution media, mount the drive and navigate to the root directory.

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

Hardware	File
IBM System p5	SSP.V3101.AIX.bin
HP-UX Integrity system with Intel Itanium processor	SSP.V3101.HP-IA.bin
HP-UX PA-RISC series	SSP.V3101.HP.bin
RedHat or SuSE Linux	SSP.V3101.Linux.bin
Solaris SPARC system	SSP.V3101.SolarisSPARC.bin
Solaris Intel system (x86)	SSP.V3101.SolarisIntel.bin
Sun x 64 system with AMD Opteron processor	SSP.V3101.SolarisAMD.bin

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

2. Type the name of the appropriate file 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 **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**.

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.

Change the IP Address for an Engine

If you have multiple NICs on an engine, you can route traffic through the IP address associated with a NIC. For each NIC, perform this procedure to associate the IP address of the NIC with an engine.

> **Note:** Use the same IP address you define in this procedure as the IP address you define when you create an engine definition. Refer to *Create an Engine Definition* on page 26.

To specify the IP bind address of the NIC:

1. From a command line prompt, go to the /*install_dir*/bin directory, where *install_dir* is the engine installation directory.

2. Type the following command:

   ```
   ./configureAccepter.sh address=IPaddress
   ```

3. At the prompt, type the passphrase defined for the engine and press **Enter**.

Install or Upgrade CM on UNIX or Linux

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:

1. Take one of the following actions:
   - If you download SSP from the Sterling Commerce Customer Center, navigate to the directory where you downloaded the CM installation file.
   - If you download SSP from the ESD Portal, navigate to the directory where you downloaded the CM installation file.
   - If you install SSP from the distribution media, mount the drive and navigate to the root directory to locate the installation file.

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

Hardware	File
IBM System p5	SSPcm.V3101.AIX.bin
HP-UX Integrity system with Intel Itanium processor	SSPcm.V3101.HP-IA.bin

Hardware	File
HP-UX PA-RISC series	SSPcm.V3101.HP.bin
RedHat or SuSE Linux	SSPcm.V3101.Linux.bin
Solaris SPARC system	SSPcm.V3101.SolarisSPARC.bin
Solaris Intel system (x86)	SSPcm.V3101.SolarisIntel.bin
Sun x 64 system with AMD Opteron processor	SSPcm.V3101.SolarisAMD.bin

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

2. Type the name of the appropriate file 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.

Obtain a License Key File for UNIX or Linux

One license is required for each engine. You receive a temporary license key file in an e-mail after you order the product. The temporary key allows you to use SSP for a limited time. You receive a permanent license key after you provide information about the computer where the engine is installed.

If you upgrade SSP, you can continue to use your existing license. You are not required to complete these procedures.

Obtain the Temporary License Key File for UNIX or Linux

To obtain a temporary license key file:

1. Copy the temporary license key file from the Sterling Commerce e-mail to the *install_dir*/conf directory, where *install_dir* is the engine installation directory.

2. Rename the temporary license key file to **license.key**.

> *Caution:*   Do not edit the license.key file. Text editors insert extra information, which invalidates the key.

Obtain the Permanent License Key File for UNIX or Linux

To obtain a permanent license key file:

1. Obtain your IP address or host ID, and submit it to Sterling Commerce by replying to the e-mail that contained your temporary license key.

    The permanent license key file is delivered through e-mail in approximately 24 to 48 hours.

2. Make a copy of the original permanent license key file and keep it in a safe place.

3. Replace the temporary license key with the permanent license key file in the *install_dir*/conf directory.

4. Rename the permanent license key file to **license.key**.

> *Caution:*   Do not edit the license.key file. Text editors insert information into the file, which invalidates the key.

---

5. If the engine is running, stop and restart it.

Start the Engine on UNIX or Linux

To start the engine:

1. Navigate to the *install_dir*\bin directory, where *install_dir* is the engine installation directory, and type the following command:

```
./startEngine.sh
```

2. Type the passphrase defined for the engine and press **Enter**.

    You receive a message indicating the SSP engine is ready for service.

The engine runs in the foreground. To configure the engine to run in the background, refer to *Change the Startup Mode on UNIX or Linux* on page 41.

Start and Log On to CM on UNIX or Linux

The first time you log on to CM, you use a preconfigured user account. After you log on the first time, create a CM user account. Refer to *Manage User Accounts* in the *Sterling Secure Proxy Configuration Guide.*

To start CM:

1. Navigate to the *install_dir/*bin directory, where *install_dir* is the directory where CM is installed, and type the following command:

    ```
    ./startCM.sh
    ```

2. Type the passphrase defined for CM and press **Enter**.

    You receive the following messages indicating:

    ◆ The CM is ready for service.

    ◆ The URL to connect to the CM logon screen.

3. Record the URL to connect to the CM logon screen on the Startup Worksheet. Refer to *SSP Startup Worksheet for UNIX or Linux* on page 20.

To log onto CM:

1. Open Internet Explorer or Firefox.

2. Type the logon address in one of the following formats:

    ```
    https://hostname:port/SSPDashboard
    ```

    or

    ```
    https://ipaddress:port/SSPDashboard
    ```

    The following table describes the parameters in the logon address.

Parameter	Description
hostname or ipaddress	Name or IP address of the computer hosting the CM server.
port	Web server port number specified during CM installation. The default is 8443.

3. Do one of the following:

    ◆   From Internet Explorer, the following error message is displayed. Click **Continue to this website (not recommended)** to continue.

    > **Note:**   The error message *There is a problem with this website's security certificate* is displayed when you first access the URL to connect to CM. You click the **Continue to this website (not recommended)** link to connect to CM. Resolve this error by replacing the self-signed certificates with your CA certificate. For instructions, refer to the Internet Explorer documentation.

    ◆   From Firefox, the **Secure Connection Failed** message is displayed. Do the following:

    a. Click **Or you can add an exception**.
    b. Click **Add Exception**.
    c. Click **Get Certificate**.
    d. Click **Confirm Security Exception**.

    > **Note:**   SSP uses TCP/IP communications links between the web server and CM. When you install SSP, a default certificate is installed to allow you to communicate. Before you can begin production, you must import a secure certificate. Refer the *Sterling Secure Proxy Configuration Guide* for instructions.

4. On the log in screen, type admin in the User ID field and password in the Password field. Click **Log In**.

5. After you log on, create a CM user account. Refer to *Manage User Accounts* in the *Sterling Secure Proxy Configuration Guide.*

CM runs in the foreground. To configure CM to run in the background, refer to *Change the Startup Mode on UNIX or Linux* on page 41.

Create an Engine Definition

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	
		_____

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

To define an engine:

1. If necessary, 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.

5. Verify that the engine is running. Refer to *View Configured Engines* on page 27 for instructions.

View Configured Engines

Use the monitoring function in CM to view all configured engines.

To view configured engines:

1. Click Monitoring from the menu bar.

2. Click Engine Status (All). A list of all configured engines is displayed, including the status. Status is displayed as follows:

   ◆ 🟢 Engine is running

   ◆ 🔴 Engine is not running

   The following information is displayed for each engine:

   ◆ Engine Name

   ◆ Last Configuration Pushed

   ◆ Message

   ◆ CM Version

   ◆ Engine Version

Stop CM from UNIX or Linux

If you close the SSP web browser, CM continues to run.

To stop CM:

1. Log out of CM.

2. Navigate to the *install_dir/*bin directory, where *install_dir* is the directory where CM is installed.

3. Type the following command:

```
./stopCM.sh
```

4. At the prompt, type the passphrase defined for CM and press **Enter**.

5. At the administrator ID prompt, type the administrator ID and press **Enter**. The default administrator ID is admin.

6. At the password prompt, type the password and press **Enter.** The default password is password.

Stop the Engine from UNIX or Linux

To stop the engine:

1. Navigate to the *install_dir/*bin directory, where *install_dir* is the directory where the engine is installed.

2. Type the following command:

```
./stopEngine.sh
```

3. At the prompt, type the passphrase defined for the engine and press **Enter**.

Install or Upgrade SSP on Windows

Before you install SSP, review the system requirements. Review the installation resources discussed in this section, and confirm that your system meets all requirements. Follow the procedures to install or upgrade SSP. Verify your installation by starting CM and the engine, and ensuring that they can communicate.

Review Resources for Windows

Before installation, review any network and security-specific configuration details that are relevant for the hardware used to install CM and the engine. Consider details specific to your environment.

Refer to the following list of resources as you plan the use of network- and security-related resources for installing and configuring SSP:

Installation or Configuration Resource	SSP Usage
TCP Ports	Use available port numbers in appropriate port ranges. The following SSP components require listening ports: ◆ CM ◆ Jetty web server ◆ Engine
Internet Explorer or Firefox	Access the CM log in screen from Internet Explorer or Firefox.
SSP Configuration Manager (CM)	Install CM in the trusted company zone. You can set up multiple engines in the same CM, but only one CM can be set up to control an engine. The CM port handles listen requests from the web server. The default port number is 62366.
Web Server	The web server is installed when you install CM to handle listen requests from the web browser. The web server port number is an element specified in the address bar when connecting to the log in screen. The default port number for the web server is 8443.

Installation or Configuration Resource	SSP Usage
SSP Engine	Install an engine in the DMZ. The default port number is 63366.
	If you install the engine on a computer with more than one Network Interface Card (NIC), specify the IP bind address of the NIC associated with that engine.
	The engine operates during production to route traffic.
	Each engine requires a different license key and engine definition created in CM.
	When you define an engine, you identify either the host name or the IP address in the definition. Create only one definition for each engine you install.
Remote Perimeter Server	A local perimeter server is installed when you install the engine. It manages communications between the engine and other nodes. You can install a remote perimeter server on another computer.
Sterling External Authentication Server	To provide another level of security by authenticating users or certificates, or mapping users, install Sterling External Authentication Server (EA). For more information, refer to the Sterling External Authentication Server documentation.
Default certificates	To secure communication, SSP is configured with default certificates to exchange between CM and the engine. Replace these certificates with your own after installation. Refer to *Managing Certificates Between SSP Components* in the *Sterling Secure Proxy Configuration Guide*.

SSP Installation Checklist for Windows

Installing SSP requires you to complete several tasks. Use the following checklist to ensure that you complete all the tasks necessary for an installation:

Installation Task	Procedure to Complete
Verify that your system meets the hardware and software requirements specified for this release.	*SSP Windows System Requirements* on page 14.
Upgrade the engine, if you installed version 3.0 or later, or install SSP for the first time.	*Install or Upgrade the Engine on Windows* on page 32.
If you install the engine on a computer with more than one Network Interface Cards (NIC), specify the IP bind address of the NIC associated with that engine.	*Change the IP Address for an Engine on Windows* on page 33.
Upgrade CM, if you installed version 3.0 or later, or install CM for the first time.	*Install or Upgrade CM on Windows* on page 33.
Obtain a temporary license key and copy it to the appropriate directory.	*Install the Temporary License Key File on Windows* on page 34.

Installation Task	Procedure to Complete
Request and install a permanent license key.	*Obtain and Install the Permanent License Key File on Windows* on page 35.
Start the engine and CM.	*Start SSP as an Automatic Windows Service* on page 35.
Log onto CM.	*Log onto CM* on page 35.
Create an engine definition in CM.	*Create an Engine Definition* on page 37.
Verify the engine and CM connection.	*View Configured Engines* on page 37.
Obtain and check in certificates for the connection between CM and the Jetty web server.	Refer to Manage Certificates between SSP Components in the *SSP Configuration Guide*.
Obtain and check in certificates for the connection between the engine and CM.	Refer to Manage Certificates between SSP Components in the *SSP Configuration Guide*.
Determine if your environment requires a remote perimeter server.	Refer to Configure Perimeter Servers to Manage SSP Communications in the *SSP Configuration Guide*.
If required, install a remote perimeter server.	*Install a Remote Perimeter Server* on page 85.

About Passphrases

At installation, you define a passphrase for CM and the engine, which ensures that CM files are secure. A passphrase is six or more characters long and contains any combination of characters. The passphrase for CM is independent of the engine passphrase.

To start CM or the engine on UNIX or Linux, type the passphrase. You must type the passphrase at shutdown.

Note: You can change the passphrase for CM and the engine after installation. Ensure that you manage this information carefully because you need the current passphrase to operate the product. If you forget your passphrase, reinstall the product.

SSP Startup Worksheet for Windows

Use the worksheet provided to record the host name or IP address of CM and the engine, related 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 Windows

Use this procedure to install or upgrade the engine.

If you previously 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.

To install or upgrade an engine on Windows:

1. Take one of the following actions:

   ◆ If you download SSP from the Sterling Commerce Customer Center, navigate to the directory where you downloaded the engine installation file.

   ◆ If you download SSP from the ESD Portal, navigate to the directory where you downloaded the engine installation file.

   ◆ If you install SSP from the distribution media, navigate to the root directory of the distribution media.

2. Double-click the **SSP.V3101.Win.exe** file.

3. After the introduction, click **Next**.

4. Scroll down in the license agreement and read the 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. 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. You need this passphrase in the future.

   c. Retype the passphrase and 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. Click **Install**.

9. At the Installation Complete screen, click **Done**.

Change the IP Address for an Engine on Windows

If you have multiple Network Interface Cards (NIC) on an engine, you can route traffic through the IP addresses associated with them. For each NIC, perform this procedure to associate the IP address of the NIC with an engine.

Note: Use the same IP address you define in this procedure as the IP address you define when you create an engine definition. Refer to *Create an Engine Definition* on page 37.

To specify the IP bind address of the NIC:

1. From a command line prompt, go to the *install_dir*\\bin directory, where *install_dir* is the engine installation directory.

2. Type the following command:

```
configureAccepter address=IPaddress
```

3. At the prompt, type the passphrase defined for the engine and press **Enter**.

Install or Upgrade CM on Windows

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 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 CM on Windows:

1. Take one of the following actions:

    ◆   If you download SSP from the Sterling Commerce Customer Center, navigate to the directory where you downloaded the CM installation file.

    ◆   If you download the product from the ESD Portal, navigate to the directory containing the downloaded CM installation file.

    ◆   If you install the product from the distribution media, navigate to the root directory of the distribution media.

2. Double-click **SSPcm.V3101.Win.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**.

Obtain and Install a License Key File on Windows

One license is required for each engine. You receive a temporary license key file in an e-mail after you order the product. The temporary key allows you to use SSP for a limited time. You receive a permanent license key after you provide information about the computer where the engine is installed.

If you upgrade SSP, you can continue to use your existing license. You are not required to complete these procedures.

Install the Temporary License Key File on Windows

To install a temporary license key:

1. Copy the temporary license key file from the Sterling Commerce e-mail to the *install_dir/*conf directory, where *install_dir* is the directory where the engine is installed.

2. Rename the temporary license key file to **license.key**.

> *Caution:*   Do not edit the license.key file. Text editors insert extra information, which invalidates the key.

Obtain and Install the Permanent License Key File on Windows

To obtain and install a permanent license key:

1. Obtain your IP address or host ID, and submit it to Sterling Commerce by replying to the e-mail that contained your temporary license key.

    The permanent license key file is delivered through e-mail in approximately 24 to 48 hours.

2. Make a copy of the original permanent license key file and keep it in a safe place.

3. Replace the temporary license key with the permanent key in the *install_dir/*conf directory, where *install_dir* is the directory where the engine is installed.

4. Rename the permanent license key file to **license.key**.

> *Caution:*   Do not edit the license.key file. Text editors insert extra information, which invalidates the key.

5. If the engine is running, stop and restart the engine.

Start SSP as an Automatic Windows Service

Running SSP as a Windows service is a convenient method of starting the application. When you set it to do so, the application starts automatically when you start Windows. CM and the engine are defined as Windows services at installation but are not set as automatic services. You need to configure them if you want to enable this startup option.After you set up an automatic Windows service, SSP runs continuously in the background until you shut it down, or shut down Windows.

> **Note:** SSP uses the encrypted passphrases stored on your hard drive to start up CM and the engine. To avoid storing the encrypted passphrase on your hard drive, you can set up CM and the engine to run as console applications. This mode prompts you to type the passphrase at startup. For instructions, refer to *Change SSP Startup Mode in Windows* on page 44.

Refer to Microsoft Windows documentation for more information on configuring applications as an automatic Windows service.

Log onto CM

You access CM through a web browser.

To log onto CM:

1. Open Internet Explorer or Firefox.

2. Type the log in address in one of the following formats:

```
https://hostname:port/SSPDashboard
```

or

```
https://ipaddress:port/SSPDashboard
```

The following table describes the parameters used in the log in address:

Parameter	Description
hostname or ipaddress	Name or IP address of the computer hosting CM.
port	Web server port number specified during installation. Default is 8443.

3. Do one of the following:

◆ From Internet Explorer, the following error message is displayed. Click **Continue to this website (not recommended)**.

> **Note:** The error message *There is a problem with this website's security certificate* is displayed when you first access the URL to connect to CM. You click the **Continue to this website (not recommended)** link to connect to CM. Resolve this error by replacing the self-signed certificates with your CA certificate. For instructions, refer to the Internet Explorer documentation.

◆ From Firefox, the **Secure Connection Failed** message is displayed. Do the following:

a. Click **Or you can add an exception**.

b. Click **Add Exception**.

c. Click **Get Certificate**.

d. Click **Confirm Security Exception**.

> **Note:** SSP uses TCP/IP communications links between the web server and CM. When you install SSP, a default certificate is installed to allow you to communicate. Before you can begin production, you must import a secure certificate. Refer the *Sterling Secure Proxy Configuration Guide* for instructions.

4. On the log in screen, type admin for User ID, password for Password, and click **Log In**.

5. Once you are logged in, create a CM user account. Refer to Chapter 5, *Manage User Accounts and Passwords* in the *Sterling Secure Proxy Configuration Guide*.

Create an Engine Definition

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	
		_____

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

To define an engine:

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 *View Configured Engines* on page 37 for instructions.

View Configured Engines

Use the monitoring function in CM to view all configured engines.

To view configured engines:

1. Click Monitoring from the menu bar.

2. Click Engine Status (All). A list of all configured engines is displayed, including the status. Status is displayed as follows:

    ◆   Engine is running

    ◆   Engine is not running

    The following information is displayed for each engine:

    ◆   Engine Name

    ◆   Last Configuration Pushed

    ◆   Message

    ◆   CM Version

    ◆   Engine Version

Stop CM from Windows

If you close the web browser, CM continues to run. To stop CM:

1. Log out of CM.

2. Go to Windows services and stop the Sterling Secure Proxy Configuration Manager V3.1.01 application.

An alternative method to stop CM requires a passphrase with a script. For more information, refer to *Stop CM When Running as a Windows Console Application* on page 47.

Stop the Engine from Windows

If you close the web browser, the engine continues to run. To stop the engine, go to Windows services and stop the Sterling Secure Proxy Engine V3.1.01 application.

An alternative method to stop the engine requires a passphrase with a script. For more information, refer to *Stop the Engine When Running as a Windows Console Application* on page 47.

Post Installation Tasks

After you install CM and the engine, you can perform additional tasks to modify your system configuration. These tasks are optional.

SSP Post Installation Checklist

Use the following checklist to determine what post-installation tasks you want to complete:

Post Installation Task	Procedure to Complete
Stop an adapter	*Stop an Adapter from CM* on page 40.
Start an adapter	*Start an Adapter from CM* on page 40.
Stop the engine	*Stop the Engine from CM* on page 40.
Change the password for the administrator or CM user	Refer to the *Sterling Secure Proxy Configuration Guide.*
Create a new administrator for CM	Refer to the *Sterling Secure Proxy Configuration Guide.*
Install over an existing SSP installation	*Reinstall SSP* on page 41.
Change the engine startup mode in UNIX	*Change the Startup Mode on UNIX or Linux* on page 41.
Change the engine passphrase in UNIX	*Change the Engine Passphrase on UNIX or Linux* on page 42.
Change the CM passphrase in UNIX	*Change CM Passphrase on UNIX or Linux* on page 43.
Uninstall the engine in UNIX	*Uninstall the Engine from UNIX or Linux* on page 44.
Uninstall CM in UNIX	*Uninstall CM from UNIX or Linux* on page 44.
Change the engine startup mode in Windows	*Change SSP Startup Mode in Windows* on page 44.
Change the CM startup mode in UNIX	*Change the Startup Mode on UNIX or Linux* on page 41.
Change the CM startup mode in Windows	*Change SSP Startup Mode in Windows* on page 44.

Post Installation Task	Procedure to Complete
Stop the engine from a Windows console application	*Stop the Engine When Running as a Windows Console Application* on page 47.
Stop CM from a Windows console application	*Stop CM When Running as a Windows Console Application* on page 47.
Change the engine passphrase in Windows	*Change Engine Passphrase in Windows* on page 47.
Change CM Passphrase in Windows	*Change CM Passphrase in Windows* on page 48.
Uninstall the engine in Windows	*Uninstall the Engine from Windows* on page 49.
Uninstall CM in Windows	*Uninstall CM from Windows* on page 49.

Stop an Adapter from CM

To stop an adapter:

1. Click Monitoring from the menu bar.
2. Expand the Engine Status tree.
3. Click the engine where the adapter is running.
4. Select the adapter to stop and click Stop.

Start an Adapter from CM

To start an adapter:

1. Click Monitoring from the menu bar.
2. Expand the Engine Status tree.
3. Click the engine where the adapter is defined.
4. Select the adapter to start and click Start.

Stop the Engine from CM

To stop the engine from CM:

1. Click Monitoring from the menu bar.
2. Click Engine Status (All). A list of all configured engines is displayed. Engines that are running are indicated with the .

3. Select the engine that you want to stop.

4. Click Stop Engine.

5. Type the engine passphrase and click OK.

Reinstall SSP

When you remove CM or the engine, the configuration and log directories remain on your computer. When you reinstall SSP, it detects an existing installation, or the remaining files from a previous installation. You receive a prompt to either change your installation directory or install the product in the same directory as the existing configuration and log files.

For CM, the apps directory also remains on your computer when you remove the program. The apps/jetty/JettyConfigDef.xml file is not overwritten when updating an existing installation.

If you reinstall SSP and use the same directory, the passphrases and ports are already defined in the configuration files. If you use a different directory, you are prompted for this information. If you cancel the installation, some files may be written to the directory. Delete these files before you start a new installation.

Note: Back up all existing installation files before reinstalling SSP.

Change the Startup Mode on UNIX or Linux

In UNIX or Linux, CM and the engine run in the foreground and require that you provide a passphrase at startup. You can change the default startup mode for CM and the engine. This section describes configuration tasks for running CM and engine in the background without prompting for a passphrase. It also identifies configuration tasks to change the setup back to the default.

Set Up the Engine to Run in the Background on UNIX or Linux

To set up the engine to run in the background:

1. Navigate to the *install_dir*/bin directory, where *install_dir* is the directory where the engine is installed, and type the following command:

```
./enableBootstrap.sh
```

2. At the prompt, type the passphrase defined for the engine and press **Enter**.

3. From the same directory, type the following command:

```
./startEngine.sh
```

The engine starts up automatically in the background and does not prompt for a passphrase. You can determine if the engine is ready for service by viewing the message in the startEngine.out file in the *install_dir*/bin directory.

Set Up the Engine to Run in the Foreground on UNIX or Linux

After you configure the engine to run in the background, use this procedure to change back to starting the engine with a passphrase prompt and running the program in the foreground.

To set up the engine to run in the foreground, delete the **sb.enc** file from the *install_dir*/conf/system directory, where *install_dir* is the directory where the engine is installed.

Set Up CM to Run in the Background on UNIX or Linux

To set up CM to run in the background:

1. Navigate to the *install_dir*/bin directory, where *install_dir* is directory where CM is installed, and type the following command:

```
./enableBootstrap.sh
```

2. At the prompt, type the passphrase defined for CM and press **Enter.**

3. From the same directory, type the following command:

```
./startCM.sh
```

CM starts up automatically in the background without prompting for a passphrase. The startCM.out file in the *install_dir*/bin directory specifies the URL for connecting to the CM server log in screen and indicates whether CM is ready for service.

Set Up CM to Run in the Foreground on UNIX or Linux

After you configure CM to run in the background, use this procedure to change back to starting CM with a passphrase prompt and running the program in the foreground.

To change CM to run in the foreground, delete the **sb.enc** file from the *install_dir*/conf/system directory, where *install_dir* is the directory where CM is installed. This file contains the encrypted passphrase.

Change the Engine Passphrase on UNIX or Linux

You can change the passphrase defined for the engine at installation. To change the passphrase:

1. Navigate to the *install_dir*/bin directory, where *install_dir* is the directory where the engine is installed.

2. To stop the engine, type the following command and press **Enter**:

```
./stopEngine.sh
```

3. At the passphrase prompt, type the passphrase defined for the engine and press **Enter**.
4. Type the following command and press **Enter**:

```
./changePassphrase.sh
```

5. At the prompt, type the current passphrase and press **Enter**.
6. At the prompt, type a new passphrase with six or more characters and press **Enter**.
7. At the prompt, retype the new passphrase and press **Enter**.

    Your new passphrase is effective the next time you start the engine.

Change CM Passphrase on UNIX or Linux

You can change the passphrase defined for CM at installation.

To change the passphrase:

1. Navigate to the *install_dir*/bin directory, where *install_dir* is the directory where CM is installed.
2. To stop CM, type the following command and press **Enter**:

```
./stopCM.sh
```

3. At the prompt, type the passphrase defined for CM and press **Enter**.
4. At the administrator ID prompt, type the administrator ID and press **Enter**.
5. At the password prompt, type the password and press **Enter**.

    CM stops.
6. Type the following command, and press **Enter**.

```
./changePassphrase.sh
```

7. At the prompt, type the current passphrase and press **Enter**.
8. At the prompt, type a new passphrase with six or more characters and press **Enter**.
9. At the prompt, retype the new passphrase and press **Enter**.

    Your new passphrase is effective the next time you start CM.

Uninstall the Engine from UNIX or Linux

When you uninstall CM or the engine, configuration files and logs remain in the following directories: *install_dir/*conf and *install_dir/*logs.

To remove the engine:

1. Stop the engine.

2. Navigate to the *install_dir*/UninstallerData directory, where *install_dir* is the directory where the engine is installed.

3. Type the following command, and press **Enter**:

```
Uninstall_Sterling_Secure_Proxy_Engine_V3.1.01
```

4. Press **Enter**.

Uninstall CM from UNIX or Linux

To remove CM from your computer:

1. Stop CM.

2. Navigate to the *install_dir*/UninstallerData directory, where *install_dir* is the directory where CM is installed.

3. Type the following command, and press **Enter**:

```
Uninstall_Sterling_Secure_Proxy_Configuration_Manager_V3.1.01
```

4. Press **Enter**.

When you uninstall CM, configuration files and logs remain in the following directories: *install_dir/*conf, *install_dir/*logs, and apps/jetty/JettyConfigDef.xml.

Change SSP Startup Mode in Windows

In Windows, CM and the engine run in the background as a Windows service. This section provides instructions to change the default startup mode for the engine and CM. It describes tasks for starting up CM and the engine as console applications to run in the foreground.

Set Up CM to Require a Passphrase Prompt at Startup on Windows

When you install CM, the passphrase is saved in an encrypted file and the program starts as a Windows service without prompting you to type the passphrase. You can change the startup method to run the program in the foreground and require that a passphrase be provided at startup.

To configure CM to require a passphrase at startup, delete the **sb.enc** file from the *install_dir*\conf\system directory, where *install_dir* is the directory where CM is installed.

Set Up the Engine to Require a Passphrase Prompt at Startup on Windows

When you install the engine, the passphrase is saved in an encrypted file and the program starts as a Windows service without prompting you to type the passphrase. You can change the startup method to run the program in the foreground and require a passphrase at startup.

To change the startup method to require a passphrase at startup, delete the **sb.enc** file from the *install_dir*\conf\system directory, where *install_dir* is the directory where the engine is installed.

Start CM as Console Application on Windows

To start CM:

1. Click **Start** > **Run** > **Browse**.

2. Browse to the *install_dir*\bin directory, where *install_dir* is the directory where CM is installed

3. Double-click the following file:

```
startCM.bat
```

4. Click **OK**.

5. If prompted, type the passphrase defined for CM.

   You receive messages indicating:

   ◆ CM is ready for service.

   ◆ The URL to connect to the CM server.

6. Record the URL to connect to the CM server on the Startup Worksheet. Refer to *SSP Startup Worksheet for Windows* on page 31.

Start the Engine as a Console Application on Windows

To start the engine:

1. Click **Start** > **Run** > **Browse**.

2. Browse to the *install_dir*\bin directory, where *install_dir* is the directory where the engine is installed, and double-click the following file:

```
startEngine.bat
```

3. Click **OK**.

4. If prompted, type the passphrase defined for the engine.

    You receive a message indicating the engine is ready for service.

Note: When you run the engine as Windows service, the passphrase is encrypted and stored on your hard drive.

Set Up Windows Service for CM

To set up CM to start as a Windows service:

1. Click **Start** > **Run** > **Browse**.

2. Browse to the *install_dir*\bin directory, where *install_dir* is the directory where CM is installed, and double-click the following file:

    ```
    enableBootstrap.bat
    ```

3. Click **OK**.

4. At the prompt, type the CM passphrase and press **Enter.**

Note: When you run CM as Windows service, the passphrase is encrypted and stored on your hard drive.

Set up Windows Service for the Engine

To set up the engine to start as a Windows service:

1. Click **Start** > **Run** > **Browse**.

2. Browse to the *install_dir*\bin directory, where *install_dir* is the directory where the engine is installed, and double-click the following file:

    ```
    enableBootstrap.bat
    ```

3. Click **OK**.

4. At the prompt, type the engine passphrase and press **Enter**.

Note: When you run the engine as Windows service, the passphrase is encrypted and stored on your hard drive.

Stop the Engine When Running as a Windows Console Application

To shut down for planned maintenance or other reasons, complete the following steps.

To stop the engine:

1. Click **Start** > **Run** > **Browse**.
2. Browse to the *install_dir*\bin directory, where *install_dir* is the directory where the engine is installed, and double-click the following file:

```
stopEngine.bat
```

3. Click **OK**.
4. At the prompt, type the engine passphrase and press **Enter**.

Stop CM When Running as a Windows Console Application

To shut down for planned maintenance or other reasons, complete the following steps.

To stop CM:

1. Click **Start** > **Run** > **Browse**.
2. Browse to the *install_dir*\bin directory, where *install_dir* is the CM installation directory, and double-click the following file:

```
stopCM.bat
```

3. Click **OK**.
4. At the prompt, type the CM passphrase and press **Enter.**
5. At the administrator ID prompt, type the administrator ID and press **Enter**. The default administrator ID is admin.
6. At the password prompt, type the password and press **Enter.** The default password is password.

Change Engine Passphrase in Windows

You can change the passphrase that you defined for the engine at installation.

To change the passphrase:

1. Click **Start** > **Run** > **Browse**.

2. Browse to the *install_dir*\bin directory, where *install_dir* is the engine installation directory.

3. Double-click the following file:

```
stopEngine.bat
```

4. Click **OK**.

5. At the prompt, type the engine passphrase and press **Enter**.

   The engine stops.

6. Double-click the following file:

```
changePassphrase.bat
```

7. Click **OK**.

8. At the prompt, type the current passphrase and press **Enter.**

9. At the prompt, type the new passphrase and press **Enter.**

10. Retype the new passphrase and press **Enter.**

    Your new passphrase is effective the next time you start the engine.

Change CM Passphrase in Windows

You can change the passphrase defined for CM at installation.

To change the passphrase:

1. Click **Start** > **Run** > **Browse**.

2. Browse to the *install_dir*\bin directory, where *install_dir* is the CM installation directory.

3. To stop CM, double-click the following file:

```
stopCM.bat
```

4. Click **OK**.

5. At the prompt, type the CM passphrase and press **Enter.**

6. At the administrator ID prompt, type the administrator ID and press **Enter**.

7. At the password prompt, type the password and press **Enter.**

   CM stops.

8. Double-click the following file:

```
changePassphrase.bat
```

9. Click **OK**.

10. At the prompt, type the current passphrase and press **Enter.**

11. At the prompt, type the new passphrase and press **Enter.**

12. At the prompt, retype the new passphrase and press **Enter**.

    Your new passphrase is effective the next time you start CM.

Uninstall the Engine from Windows

When you uninstall the engine, configuration files and log files remain in the *install_dir*\conf and *install_dir*\logs directories. The file apps\jetty\JettyConfigDef.xml remains.

To remove the engine:

1. Stop the engine.

2. Click **Start** > **Programs** > **Sterling Secure ProxyV3.1.01.**

3. Click **Uninstall Engine**.

4. Click **Uninstall**.

5. Click **Done**.

Uninstall CM from Windows

When you uninstall CM, configuration files and logs files remain in the *install_dir*\conf and *install_dir*\logs directories.

To remove CM:

1. Stop CM.

2. Click **Start** > **Programs** > **SSP V3.1.01.**

3. Click **Uninstall Configuration Manager**.

4. Click **Uninstall**.

5. Click **Done**.

Upgrade SSP from Version 2.0.x to Version 3.x

Use the procedures in this section to upgrade SSP from version 2.0, 2.0.01 or 2.0.02 to version 3.x. To upgrade from version 3.0, follow the installation instructions.

SSP version 3.x uses a different architecture from version 2.0.x. It allows you to configure your environment using the Configuration Manager (CM). It then moves the configuration information to an Engine, to use during production. SSP version 2.0.x does not use an Engine or CM. Configuration and production occur on an SSP node, and data is stored in a database.

Before upgrading your environment, identify the configuration of your SSP version 2.0.x. Then, complete the procedures identified for each configuration. Configurations include:

✦ Single SSP environment—If you installed SSP on one node, refer to *Upgrade a Single SSP Node* on page 52.

✦ Clustered SSP environment—If you installed SSP on two or more nodes and all nodes use the same configuration information to provide high availability and secondary engines accept incoming requests if the primary engine is not available, refer to *Upgrade SSP Clustered Nodes* on page 56.

✦ Load balancing SSP environment—If you installed SSP version 2.0.x on two or more nodes and created a load balancing environment to provide redundancy and share the workload among multiple servers, refer to *Upgrade an SSP Loading Balancing Environment* on page 60 for instructions on how to upgrade this environment.

✦ Multiple SSP nodes environment—If you installed two or more SSP nodes and each node manages separate incoming requests, the configuration is unique for each node. Refer to *Upgrade a Multiple SSP Nodes Configuration* on page 64.

✦ Move certificates used on an HSM device in SSP version 2.0.02. Release 2.0.02 supported the use of an HSM device. To use the HSM certificates created in version 2.0.02, complete the procedure, *Move Key Certificates Created in SSP 2.0.02 on the HSM* on page 83.

Upgrade a Single SSP Node

If you installed SSP version 2.0.x on one node, use the information in this section to upgrade your environment. The following diagram compares an SSP version 2.0.x single instance environment to SSP version 3.x.
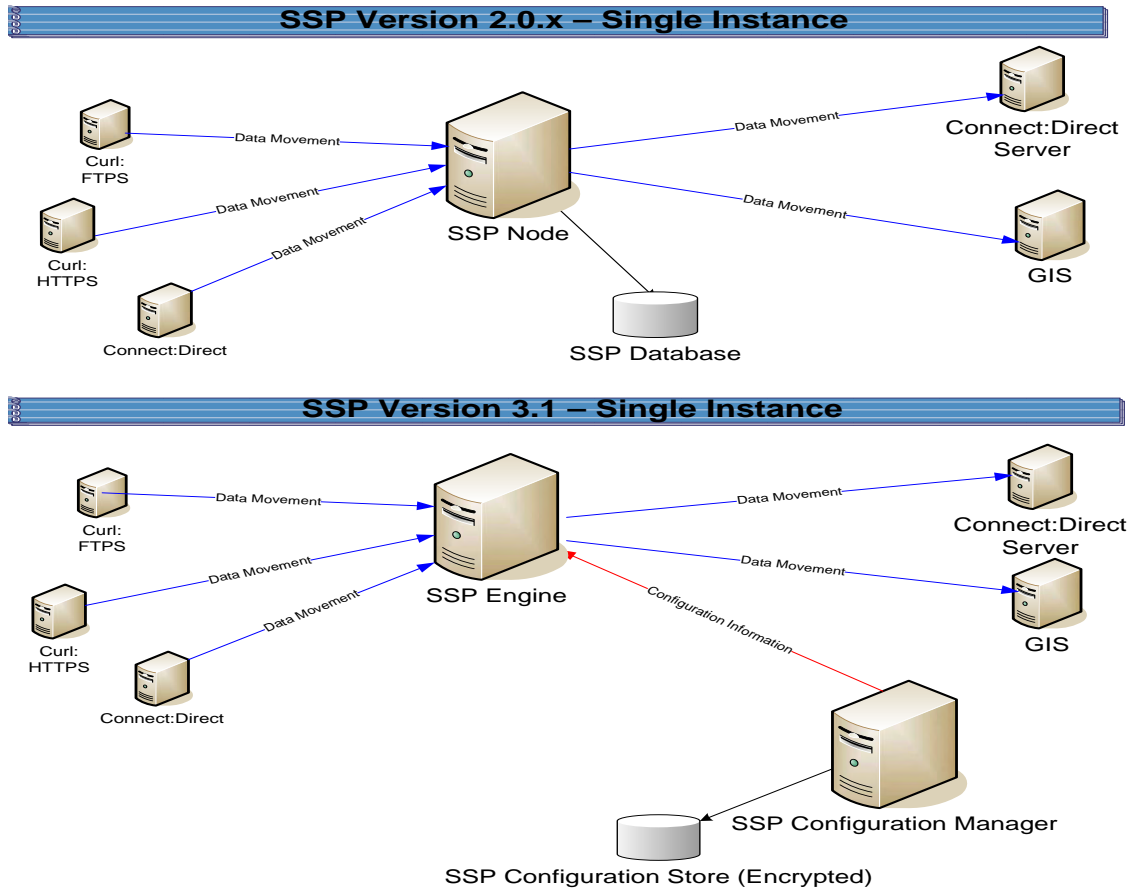
To upgrade a single node configuration created in version 2.0.x, first export information from SSP 2.0.x. Then, install an SSP version 3.x CM and engine. If you use remote perimeter servers (PS), install a new PS for each instance. Be sure to identify the settings used in version 2.0.x so that you can use this information when you install the new PS. To keep the existing remote PS configuration, install the new PS over the existing software. Then, run the upgrade script to convert the 2.0.x files to version 3.x. When you run the script, you define the engine to create and associate with the converted files. Refer to *Upgrade Tasks* on page 54.

Each exported object is renamed to identify the engine it is associated with. For example, if you created a Connect:Direct adapter in version 2.0.x called CDAdapter and you define the SSP node as engine1, the adapter is renamed to CDAdapter-engine1 when it is converted to SSP 3.x.

Single Node File Conversion Illustration

The following table illustrates how version 2.0.x objects are converted to version 3.x when you convert a single SSP instance. Each object name is converted to version 3.x.0. modified by adding the engine name to the end of it.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine1	No engine was defined in version 2.0.x. Each SSP node performed configuration and production tasks. The engine in version 3.x performs only production tasks.
ConnectAdapter1	ConnectAdapter1-engine1 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 STEPINJ_1-engine1	All information associated with a Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine1	
FTPAdapter1	FTPAdapter1-engine1	
HTTPNetmap1	HTTPNetmap1-engine1	
FTPNetmap1	FTPNetmap1-engine1	
HTTPPolicy1	HTTPPolicy1-engine1	
FTPPolicy1	FTPPolicy1-engine1	
Users	defUserStore	If you do not define a user store at conversion, a default is used. You can create one by using the -userstore argument at conversion.
System Certificates	dfltKeyStore	If you do not define a key store at conversion, a default is used. You can create one by using the -keystore argument at conversion
CA Certificates	dfltTrustStore	If you do not define a trust store at conversion, a default is used. You can create one by using the -truststore argument at conversion.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
Perimeter Server1	PerimeterServer1-engine1	
	EA_hostname_port-engine1	No EA object existed. It was defined as part of an adapter. If an EA server is defined in more than one adapter, using the same host and port, only the first instance is created and shared among the adapters.
	PASSWORDPOLICY-engine1	

Pre-Upgrade Checklist

Before you begin an upgrade, obtain the following information:

✦ Be sure the temporary license key for version 3.x is available on the computer where you will install the engine.

✦ If you use a remote perimeter server (PS), obtain the PS host name. If you install the PS in a less secure zone than the engine, obtain the host name and port number where the PS will be installed.

Upgrade Tasks

Complete the following tasks to upgrade a single instance of SSP:

Installation Task	Procedure to Complete or Information Needed
Start SSP version 2.0.x.	*Start and Log On to SSP Version 2.0.x* on page 68.
Export the SSP 2.0.x resources.	*Export SSP Version 2.0.x Information* on page 68.
Write down the export file name and password.	_____
Install the SSP 3.x Engine. **Note:** Install the engine but do not start it.	For UNIX or Linux, refer to *Install or Upgrade the Engine on UNIX or Linux* on page 20. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 32.
Install SSP 3.x CM.	For UNIX or Linux, refer to *Install or Upgrade CM on UNIX or Linux* on page 22. For Windows, refer to *Install or Upgrade CM on Windows* on page 34.
Obtain and install a license key.	For UNIX or Linux, refer to *Obtain a License Key File for UNIX or Linux* on page 23. For Windows, refer to *Obtain and Install a License Key File on Windows* on page 35.

Installation Task	Procedure to Complete or Information Needed
If you use an external perimeter server (PS), do the following: 1 Stop the version 2.0.x PS. 2 Install a version 3.x PS. 3 If SSP 2.0.x is installed on the same computer with the version 3.x engine, stop SSP 2.0.x.	*Stop Perimeter Server Version 2.0* on page 69. Chapter 7, *Install a Remote Perimeter Server*. *Stop SSP Version 2.0.x* on page 69.
Back up SSP version 3.x configuration files.	*Back Up Version 3.x Configuration Files* on page 70.
Run the upgrade script.	*Convert Files from SSP Version 2.0.x to Version 3.x* on page 70.
View the upgrade log to ensure that the conversion succeeded.	*Read the Upgrade Log File* on page 75.
Start and log on to CM.	For UNIX or Linux, refer to *Start and Log On to CM on UNIX or Linux* on page 25. For Windows, refer to *Log onto CM* on page 36.
Open the engine definition and verify the configuration.	*Validate an Engine Definition* on page 77.
Open the adapter definitions and verify each adapter configuration.	*Validate an Adapter* on page 77.
If you use a PS, validate the PS definition.	*Validate a PS Definition for a PS in a More Secure Zone* on page 78 or *Validate a PS Definition for a PS in a Less Secure Zone* on page 78.
If you changed any HTTP adapter property values, check the properties and make any necessary changes.	*Maintain Changes to HTTP Properties* on page 79.
If you made any changes to a Connect:Direct adapter properties in version 2.0.x, make the property changes in version 3.x.	*Implement Property Changes Made to a Connect:Direct Adapter* on page 82.
If you made any changes to FTP adapter properties in version 2.0.x, make the changes in version 3.x.	*Maintain Changes to FTP Properties* on page 81.
If you changed the log on attempts allowed in version 2.0.x, make the changes in version 3.x.	*Change How Many Times a User Can Attempt to Log In Before a Lock Occurs* on page 83.
Make sure that new FTP and HTTP adapter properties are correctly set.	*New FTP Adapter Properties in Version 3.x* on page 82 or *New Properties in Version 3.x HTTP Adapter* on page 80.
Start the engine.	Refer to *Start the Engine on UNIX or Linux* on page 24 or *Start SSP as an Automatic Windows Service* on page 36.
Verify that the engine can communicate with CM.	*Validate the Connection Between Engines and CM* on page 78.

Upgrade SSP Clustered Nodes

If you installed SSP version 2.0.x on two or more nodes and created a cluster environment to provide failover support, the configuration information at each node is the same and the nodes share a database. The following diagram compares an SSP version 2.0.x cluster environment to 3.x:
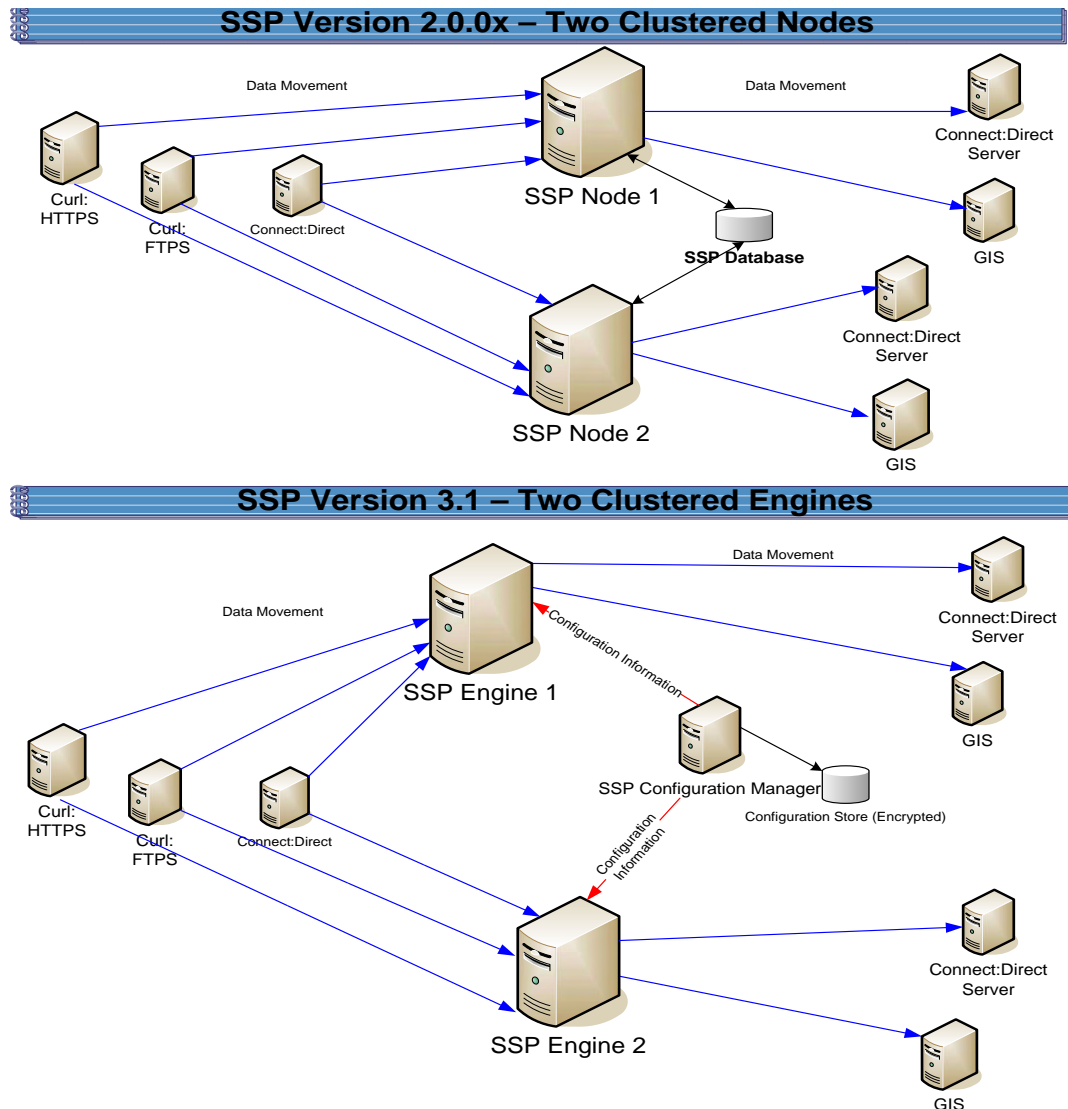
To upgrade a cluster configuration created in version 2.0.x, first export information from one SSP 2.0.x node. Then, install an SSP version 3.x CM. Install an engine for each cluster node in your environment. If you use remote perimeter servers (PS), install a new PS for each instance. To keep the existing configuration, install the new PS over the existing software. To install PS in a new location, be sure to identify the settings used in version 2.0.x so that you can use this information when you install the new PS. Then, run the upgrade script to convert the 2.0.x files to version 3.x. When you run the script, you define the primary engine to create and associate with the converted files. After you determine that the configuration is working on the primary engine, use CM to create additional engines needed in the cluster environment. For each additional engine, make a copy of the adapters and associate the copy with the engine you added.

Each object exported from version 2.0.x is renamed to identify the engine it is associated with. For example, if you created a Connect:Direct adapter in version 2.0.1 called CDAdapter and you define the SSP node1 as engine1, the adapter is renamed to CDAdapter-engine1 when it is converted.

Cluster Nodes File Conversion Illustration

The following table identifies how version 2.0.x objects are converted to version 3.x for a cluster environment. Each object name is converted to version 3.1.0. modified by adding the engine name to the end of it.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine1	No engine was defined in version 2.0.x. Each SSP node performed configuration and production tasks. The engine in version 3.x performs only production tasks.
ConnectAdapter1	ConnectAdapter1-engine1 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 CDSTEPINJ_1-engine1	All information associated with a Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine1	
FTPAdapter1	FTPAdapter1-engine1	
HTTPNetmap1	HTTPNetmap1-engine1	
FTPNetmap1	FTPNetmap1-engine1	
HTTPPolicy1	HTTPPolicy1-engine1	
FTPPolicy1	FTPPolicy1-engine1	
Users	defUserStore	If you do not define a user store at conversion, a default is used. You can create one by using the -userstore argument at conversion.
System Certificates	dfltKeyStore	If you do not define a key store at conversion, a default is used. You can create one by using the -keystore argument at conversion

Version 2.0.x Object	Converts to Version 3.x Object	Notes
CA Certificates	dfltTrustStore	If you do not define a trust store at conversion, a default is used. You can create one by using the -truststore argument at conversion.
Perimeter Server1	Perimeter Server1-engine1	
	EA_hostname_port-engine1	No EA object existed. It was defined as part of an adapter. If an EA server is defined in more than one adapter, using the same host and port, only the first instance is created.
	PASSWORDPOLICY-engine1	
	Engine called engine2	This engine is not created during the conversion. Use CM to define engine2.
ConnectAdapter1	ConnectAdapter1-engine2 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 CDSTEPINJ_1-engine1	This adapter is not created during the conversion. Use CM to copy ConnectAdapter1-engine1 and rename it ConnectAdapter1-engine2. The netmap, policy, and step injection object are reused.
HTTPAdapter1	HTTPAdapter1-engine2	This adapter is not created during the conversion. Use CM to copy HTTPAdapter1-engine1 and rename it to HTTPAdapter1-engine2.
FTPAdapter1	FTPAdapter1-engine2	This adapter is not created during the conversion. Use CM to copy FTPAdapter1-engine1 and rename it to FTPAdapter1-engine2.
HTTPNetmap1	HTTPNetmap1-engine1	The netmap created during conversion is reused.
FTPNetmap1	FTPNetmap1-engine1	The netmap created during conversion is reused.
HTTPPolicy1	HTTPPolicy1-engine1	The policy created during conversion is reused.
FTPPolicy1	FTPPolicy1-engine1	The policy created during conversion is reused.
Users	defUserStore	The same user store is used by engine 1 and engine 2.
System Certificates	dfltKeyStore	The same keystore is used by engine 1 and engine 2.
CA Certificates	dfltTrustStore	The same trust store is used by engine 1 and engine 2.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
PerimeterServer2	PerimeterServer2	Perimeter servers cannot be shared by engines. Install a new perimeter server and create a new perimeter server definition for the new engine.

Cluster Nodes Upgrade Checklist

Complete the procedures in the *Upgrade Tasks* on page 54 to begin the upgrade. Complete the following tasks to complete the cluster node upgrade:

Installation Task	Procedure to Complete or Information Needed
Install an SSP 3.x engine at each additional cluster node. **Note:** Do not start the engine.	For UNIX or Linux, refer to *Install or Upgrade the Engine on UNIX or Linux* on page 20. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 32.
Obtain and install a license key file for each engine.	For UNIX or Linux, refer to *Obtain a License Key File for UNIX or Linux* on page 23. For Windows, refer to *Obtain and Install a License Key File on Windows* on page 35.
Create an engine definition for each additional engine in the cluster.	*Create an Engine Definition* on page 26.
Using CM, make a copy of each adapter associated with the primary engine. Associate the adapter copy with the cluster engine you create. Repeat this for each additional node in the cluster.	*Copy an Adapter* on page 76.
Start all SSP cluster engines.	For UNIX or Linux, refer to *Start the Engine on UNIX or Linux* on page 24. For Windows, refer to *Start SSP as an Automatic Windows Service* on page 36
Verify that each cluster engine can communicate with CM.	*Validate the Connection Between Engines and CM* on page 78.

Upgrade an SSP Loading Balancing Environment

If you installed SSP version 2.0.x on two or more nodes and created a load balancing environment to provide redundancy and share the workload among multiple servers, the configuration information at each node is the same but it is stored in different databases. The following diagram compares an SSP version 2.0.x load balancing environment to version 3.x.
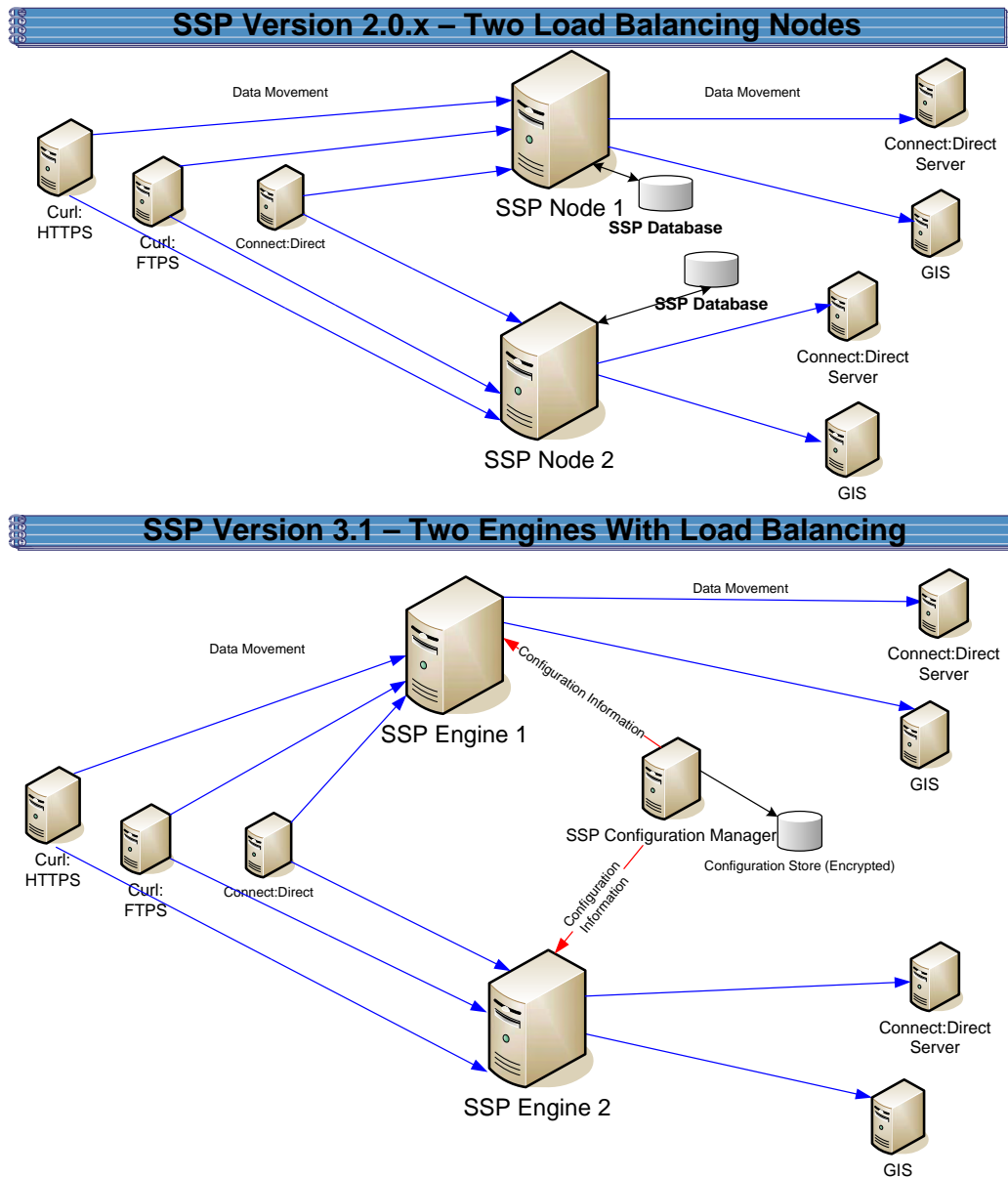
To upgrade a load balancing configuration, export information from each SSP 2.0.x node. Be sure to specify a unique engine name and export file for each node. Then, run the upgrade script for each node.

For each export file, exported objects are renamed to identify the engine it is associated with. For example, if you created a Connect:Direct adapter in version 2.0.x called CDAdapter and you define the SSP node1 as engine1, the adapter is renamed to CDAdapter-engine1 when it is converted. When you run the upgrade script again and specify the engine name as engine2, a new adapter definition is created and renamed CDAdapter-engine2.

Load Balancing Nodes File Conversion Illustration

The following table identifies how version 2.0.x objects are converted to version 3.x for a load balancing environment. For each engine defined, its objects are created from a unique database. Each object name is converted to version 3.x and modified by adding the engine name to the end of it.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine1	No engine was defined in version 2.0.x. Each SSP node performed configuration and production tasks. The engine in version 3.x performs only production tasks.
ConnectAdapter1	ConnectAdapter1-engine1 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 CDSTEPINJ_1-engine1	All information associated with a Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine1	
FTPAdapter1	FTPAdapter1-engine1	
HTTPNetmap1	HTTPNetmap1-engine1	
FTPNetmap1	FTPNetmap1-engine1	
HTTPPolicy1	HTTPPolicy1-engine1	
FTPPolicy1	FTPPolicy1-engine1	
Users	defUserStore	If you do not define a user store at conversion, a default is used. You can create one by using the -userstore argument at conversion.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
System Certificates	dfltKeyStore	If you do not define a key store at conversion, a default is used. You can create one by using the -keystore argument at conversion
CA Certificates	dfltTrustStore	If you do not define a trust store at conversion, a default is used. You can create one by using the -truststore argument at conversion.
PerimeterServer1	PerimeterServer1-engine1	
	EA_hostname_port-engine1	No EA object existed. It was defined as part of an adapter. If an EA server is defined in more than one adapter, using the same host and port, only the first instance is created.
	PASSWORDPOLICY-engine1	
	Engine called engine2	No engine was defined in version 2.0.x. Each SSP node was separately managed. In version 3.x, all engines can be managed by one CM.
ConnectAdapter1	ConnectAdapter1-engine2 CDNETMAP-ConnectAdapter1-engine2 CDPOLICY_1-engine2 CDSTEPINJ_1-engine2	All information associated with a Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object.
HTTPAdapter1	HTTPAdapter1-engine2	
FTPAdapter1	FTPAdapter1-engine2	
HTTPNetmap1	HTTPNetmap1-engine2	
FTPNetmap1	FTPNetmap1-engine2	
HTTPPolicy1	HTTPPolicy1-engine2	
FTPPolicy1	FTPPolicy1-engine2	
Users	defUserStore	The same user store is used by engine 1 and engine 2
System Certificates	dfltKeyStore	The same keystore is used by engine 1 and engine 2

| Version 2.0.x Object	Converts to Version 3.x Object	Notes
CA Certificates	dfltTrustStore	The same trust store is used by engine 1 and engine 2.
PerimeterServer2	PerimeterServer2-engine2	

Loading Balancing Nodes Upgrade Checklist

Complete the procedures in the *Upgrade Tasks* on page 54 to begin the upgrade. Perform the following procedures to complete the load balancing environment upgrade:

Installation Task	Procedure to Complete or Information Needed
Install an SSP 3.x engine at each additional load balancing location.	For UNIX or Linux, refer to *Install or Upgrade the Engine on UNIX or Linux* on page 20. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 32.
Obtain and install a license key file for each load balancing engine.	For UNIX or Linux, refer to *Obtain a License Key File for UNIX or Linux* on page 23. For Windows, refer to *Obtain and Install a License Key File on Windows* on page 35.
Export SSP version 2.0.x resources from each additional SSP node.	*Export SSP Version 2.0.x Information* on page 68.
Write down the export file name and password.	_____
Run the upgrade script and identify the name of the additional engine (node).	*Convert Files from SSP Version 2.0.x to Version 3.x* on page 70.
View the upgrade log to ensure that the conversion for the node succeeded.	*Read the Upgrade Log File* on page 75.
From CM, verify each load balancing engine definition.	*Validate an Engine Definition* on page 77.
Open the adapter definitions for each load balancing engine. Make sure that each adapter is correctly defined.	*Validate an Adapter* on page 77.
Start all SSP load balancing engines.	For UNIX or Linux, refer to *Start the Engine on UNIX or Linux* on page 24. For Windows, refer to *Start SSP as an Automatic Windows Service* on page 36.
Verify that the load balancing engine can communicate with CM.	*Validate the Connection Between Engines and CM* on page 78.

Upgrade a Multiple SSP Nodes Configuration

If you installed SSP version 2.0.x on multiple nodes and the configuration information for each node is unique, use the information in this section to identify how to upgrade your environment. The following diagram compares an SSP version 2.0.x multiple node environment to version 3.x:
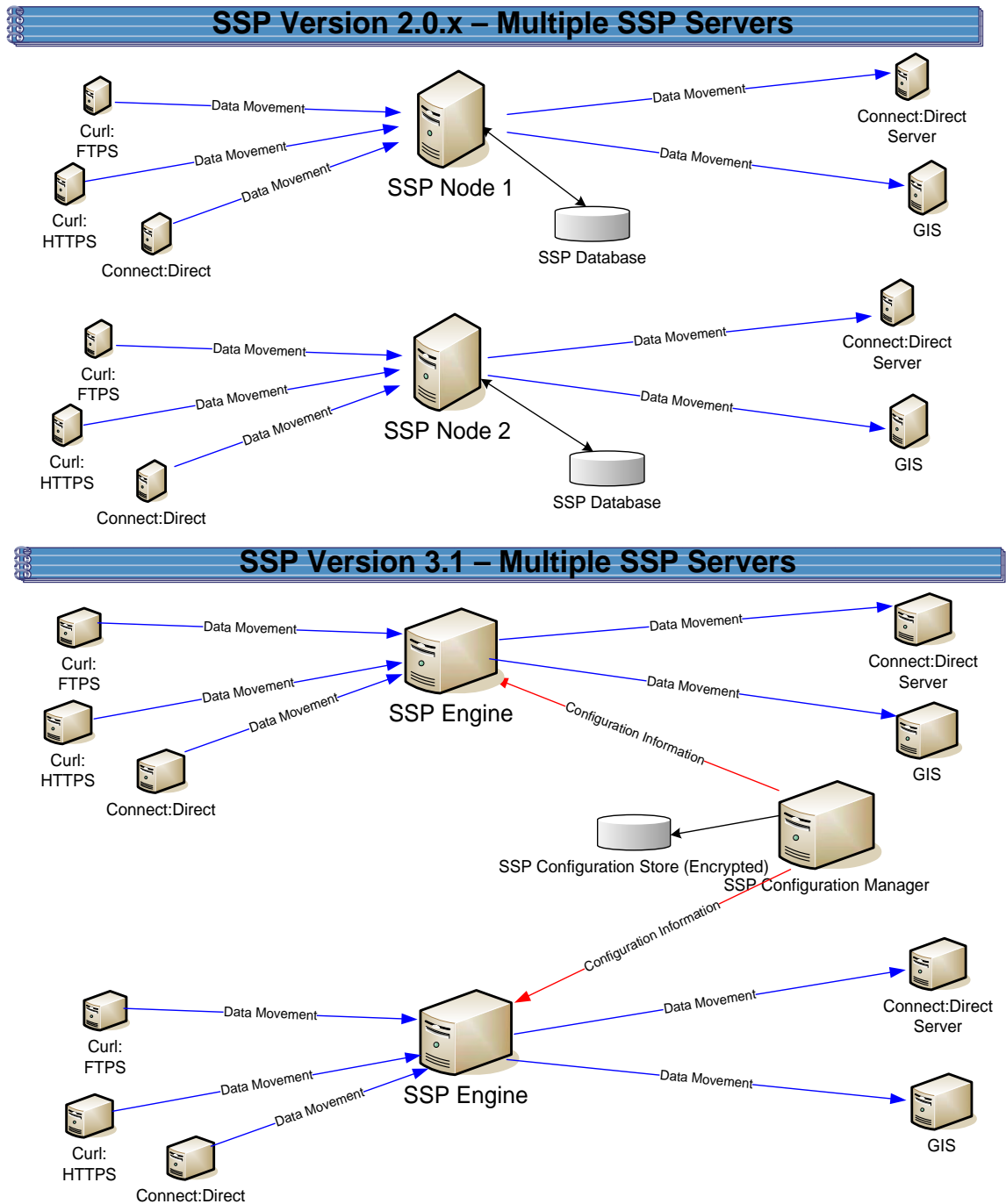
To upgrade the configuration created in version 2.0.x, export information from each node. Then, run the upgrade script at each node to convert the files to version 3.x. When you run the upgrade script, you define the engine to create and associate with the converted files. Be sure to define a unique engine name for each node.

Each exported object is renamed to identify the engine it is associated with. For example, if you created a Connect:Direct adapter in version 2.0.x called CDAdapter and you define the SSP node as engine1, the adapter is renamed to CDAdapter-engine1 when it is converted to SSP 3.x.

Multiple Node Environment File Conversion Illustration

The following table identifies how version 2.0.x objects are converted to version 3.x for a multiple node environment. For each engine defined, its objects are created from a unique database. Each object name is converted to version 3.x and modified by adding the engine name to the end of it.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine1	No engine was defined in version 2.0.x. Each SSP node was separately managed.
ConnectAdapter1	ConnectAdapter1-engine1 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 CDSTEPINJ_1-engine1	Each object name is modified by adding the engine name to the end of it in version 3.x. All information associated with a Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine1	
FTPAdapter1	FTPAdapter1-engine1	
HTTPNetmap1	HTTPNetmap1-engine1	
FTPNetmap1	FTPNetmap1-engine1	
HTTPPolicy1	HTTPPolicy1-engine1	
FTPPolicy1	FTPPolicy1-engine1	
Users	defUserStore	If you do not define a user store at conversion, a default is used. You can create one by using the -userstore argument at conversion.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
System Certificates	dfltKeyStore	If you do not define a key store at conversion, a default is used. You can create one by using the -keystore argument at conversion
CA Certificates	dfltTrustStore	If you do not define a trust store at conversion, a default is used. You can create one by using the -truststore argument at conversion.
PerimeterServer1	PerimeterServer1-engine1	
	EA_hostname_port-engine1	No EA object existed. It was defined as part of an adapter. If an EA server is defined in more than one adapter, using the same host and port, only the first instance is created.
	PASSWORDPOLICY-engine1	
	Engine called engine2	No engine was defined in version 2.0.x. Each SSP node was separately managed. In version 3.x, all engines can be managed by one CM.
ConnectAdapter1	ConnectAdapter1-engine2 CDNETMAP-ConnectAdapter1-engine2 CDPOLICY_1-engine2 CDSTEPINJ_1-engine2	Each object name is modified by adding the engine name to the end of it in version 3.x. All information associated with a Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine2	
FTPAdapter1	FTPAdapter1-engine2	
HTTPNetmap1	HTTPNetmap1-engine2	
FTPNetmap1	FTPNetmap1-engine2	
HTTPPolicy1	HTTPPolicy1-engine2	
FTPPolicy1	FTPPolicy1-engine2	

Version 2.0.x Object	Converts to Version 3.x Object	Notes
Users	defUserStore	The same user store is used by engine 1 and engine 2
System Certificates	dfltKeyStore	The same keystore is used by engine 1 and engine 2
CA Certificates	dfltTrustStore	The same trust store is used by engine 1 and engine 2.
PerimeterServer2	PerimeterServer2-engine2	

Load Balancing Multiple Node Upgrade Checklist

Complete the procedures in the *Upgrade Tasks* on page 54 to begin the upgrade. Perform the following procedures to complete the multiple node environment upgrade:

Installation Task	Procedure to Complete or Information Needed
Install an SSP 3.x engine at each additional server location.	For UNIX or Linux, refer to *Install or Upgrade the Engine on UNIX or Linux* on page 20. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 32.
Obtain and install a license key file for each additional engine.	For UNIX or Linux, refer to *Obtain a License Key File for UNIX or Linux* on page 23. For Windows, refer to *Obtain and Install a License Key File on Windows* on page 35.
Run the upgrade script at each additional engine.	Refer to *Convert Files from SSP Version 2.0.x to Version 3.x* on page 70.
View the upgrade log to ensure that the conversion succeeded.	*Read the Upgrade Log File* on page 75.
Start and log on to CM.	For UNIX or Linux, refer to *Start and Log On to CM on UNIX or Linux* on page 25. For Windows, refer to *Log onto CM* on page 36.
From CM, open the engine definition and verify the configuration.	*Validate the Converted Components in SSP Version 3.x* on page 77.
Open the adapter definitions. Make sure that each adapter is correctly defined.	*Validate an Adapter* on page 77.
Start the SSP engine.	For UNIX or Linux, refer to *Start the Engine on UNIX or Linux* on page 24. For Windows, refer to *Start SSP as an Automatic Windows Service* on page 36
Verify that the engines can communicate with CM.	*Validate the Connection Between Engines and CM* on page 78.

Start and Log On to SSP Version 2.0.x

To start and log on to SSP version 2.0.x:

1. Do one of the following:

   ◆ To start SSP on UNIX or Linux:

      a. Change the directory to *install_dir*/bin.

      b. Type **run.sh**.

      c. **Enter** the passphrase that you supplied during installation.

   ◆ To start SSP on Windows, double-click the SSP icon on your Windows desktop.

   When startup is complete, a message such as the following is displayed: *Open your Web browser to http://host:port/dashboard*, where *host:port* is the IP address and port number where SSP is installed.

2. Open a browser window and type the URL address for SSP version 2.0.x.

3. Type the user ID and password in the **User ID** and **Password** fields. The default values are proxy_admin and password.

Export SSP Version 2.0.x Information

To move configuration information defined in SSP version 2.0.x to version 3.x, first export the resource files from version 2.0.x.

To export SSP version 2.0.x resource files:

1. From the Deployment menu, select **Import/Export**.

2. Next to **Export Resources**, click **Go!**

3. With **XML Document** selected, click **Next**.

4. With **No** selected, click **Next**.

5. With **Standard** selected as the export type, click **Next**.

6. Select all of the resources to export and click **Next**. Resource types include:

   ◆ Accounts

   ◆ Proxy Policies

   ◆ Perimeter Servers

   ◆ Digital Certificates

   ◆ Proxy Netmaps

   ◆ Service Configurations

7. Select Users as the account type to export and click **Next**.

8. To export all users, click the double-right arrows to move all users to the To Be Exported column. Click **Next**.

9. To export all permission definitions, click the double-right arrows to move all permission definitions to the To Be Exported column. Click **Next**.

10. Select CA Digital Certificates and System Certificates to export all digital certificates. Click **Next**.

11. To export all CA digital certificates, click the double-right arrows to move all certificates to the To Be Exported column. Click **Next**.

12. To export all system certificates, click the double-right arrows to move all certificates to the To Be Exported column. Click **Next**.

13. To export all proxy policies, click the double-right arrows to move all policies to the To Be Exported column. Click **Next**.

14. To export all netmaps, click the double-right arrows to move all netmaps to the To Be Exported column. Click **Next**.

15. To export all perimeter servers, click the double-right arrows to move all items to the To Be Exported column. Click **Next**.

16. To export all service configurations (adapters), click the double-right arrows to move all items to the To Be Exported column. Click **Next**.

17. Type the passphrase defined during the version 2.0.x installation twice and click **Next**.

18. Click **Finish** to export the resources and create the export file.

19. To view the export report, click **View Export Report**. Make sure that all resources were successfully exported.

20. Click **Download Export data (.xml** or **.jar)** to save the export file.

21. Click **Return**.

Stop Perimeter Server Version 2.0

To stop a version 2.0 perimeter server:

1. Change the directory to /*install_dir*/bin where *install_dir* is the location where the PS is installed.

2. Type **stopPs.sh** and press **Enter**.

Stop SSP Version 2.0.x

To stop SSP version 2.0.x:

1. If necessary, open SSP version 2.0.x. Refer to *Start and Log On to SSP Version 2.0.x* on page 68.

2. From the Administration menu, select **System Tools>Troubleshooter**.

3. Click **Stop the System** and wait for shutdown to complete.

Back Up Version 3.x Configuration Files

Before you upgrade version 2.0.x files to version 3.x, first back up the version 3.x configuration files. Back up the folder called /*install_dir*/conf/ on the computer where CM is installed.

Convert Files from SSP Version 2.0.x to Version 3.x

After you export the resource files from SSP version 2.0.x, run the upgrade script. The script first validates the objects in the file. If an object is not valid, a warning is generated and written to the upgrade log. It then performs a dependency check to ensure that items associated with an object are available in the export file. For example, if you exported an HTTP adapter that uses SSL, the dependency check searches for the certificate used in the HTTP secure communications. If it is not available, a dependency warning is generated and written to the upgrade log. The script then converts the objects to version 3.x syntax and imports the objects into CM.

Run the script using one or more of the following modes:

✦ Validation (-v)—reads the export file and generates a list of warnings that will occur if the file is converted. It does not convert the objects.

✦ Default—validates the export file and determines if it can be converted. It then performs a dependency check. If no validation or dependency warnings are generated, the objects are converted. If warnings occur, the file is not converted and warnings are written to the upgrade log.

✦ Ignore warning (-w)—validates the export file and performs a dependency check. Objects are then converted. Any dependency or validation warnings are written to the upgrade log.

✦ Dependency check (-d)—validates the export file and determines if it can be converted. It then performs a dependency check. If no validation warnings are generated, the objects are converted. It ignores dependency warnings and writes them to the upgrade log.

✦ Overwrite (-o)—converts an export file and if an object already exists in the version 3.x configuration, it overwrites the object with the new information. All other modes ignore an object that already exists.

Validate an Export File

Complete this procedure to validate an export file and write warnings that will occur at conversion to the upgrade log. This procedure does not convert the objects to version 3.x.

To validate an export file:

1. From the /*install_dir*/bin directory, where *install_dir* is the CM installation directory, type the following command and press **Enter**: Refer to *Upgrade Script Options* on page 73 for a description of the parameters:

```
./sspUpgrade export_file engine_name -v
```

2. Type the passphrase defined at installation for SSP version 2.0.x and press **Enter**.

3. Type the passphrase defined when you installed CM.

Convert Version 2.0.x Files With New Engine If No Warnings Are Found

Complete this procedure to convert objects from SSP version 2.0.x to version 3.x and create a new engine. You identify the name of the engine to create and the engine host and port as well as the version 2.0.x file to convert on the command line.

The upgrade script reads the export file and determines if objects are valid. It then performs a dependency check to determine if any item referenced by an exported object is missing. If any object is not valid or if a dependency check warning is generated, the files are not converted. If the objects are valid, an engine is created with the values you specify. Then, objects are converted to version 3.x format and associated with the engine.

To convert the version 2.0.x export file version 3.x and create a new engine, if no warnings are generated:

1. From the /*install_dir*/bin directory, where *install_dir* is the CM installation directory, type the following command and press **Enter**. Refer to *Upgrade Script Options* on page 73 for a description of the parameters.

```
./sspUpgrade export_file_name engine_name -enginehost enginehostvalue -engineport
engineportvalue
```

2. Do one of the following:

   ◆ If you have not backed up the /*install_dir*/conf/ folder, type n and press **Enter** to stop the script. After you perform the backup, perform this procedure again.

   ◆ Type y and press **Enter** to continue.

3. Type the passphrase defined at installation for SSP version 2.0.x and press **Enter**.

4. Type the passphrase defined when you installed CM 3.x and press **Enter**.

Convert Version 2.0.x Files With Existing Engine If No Warnings Are Found

Complete this procedure to convert an export file from SSP version 2.0.x to version 3.xand associate converted files with an engine that is already defined in version 3.x. You identify the name of the engine to associate the converted objects with on the command line.

The upgrade script reads the export file and determines if objects are valid. It then performs a dependency check to determine if any item referenced by an exported object is missing. If any object is not valid or if a dependency check warning is generated, the files are not converted. If the objects are valid, they are converted to version 3.x format and associated with the engine you specified.

To convert the version 2.0.x export file to version 3.x, if no warnings are generated, and associate them with an engine that is already defined in version 3.x:

1. From the /*install_dir*/bin directory where *install_dir* is the CM installation directory, type the following command and press **Enter**:

```
./sspUpgrade export_file_name engine_name
```

2. Do one of the following:

   ◆ If you have not backed up the /*install_dir*/conf/ folder, type n and press **Enter** to stop the script. After you perform the backup, perform this procedure again.

   ◆ Type y and press **Enter** to continue.

3. Type the passphrase defined at installation for SSP version 2.0.x and press **Enter**.

4. Type the passphrase defined when you installed CM3.xand press **Enter**.

Convert Version 2.0.x Files and Ignore Warnings

Complete this procedure to convert an export file from SSP version 2.0.x to version 3.x and ignore warnings.

Caution: We strongly recommend that you resolve warnings before converting files to the version 3.x format. Converting files with warnings may prevent adapters from working. If you convert files that contain warnings or dependencies to version 3.x, be sure to resolve the warnings. Then, open and save the engine definition to ensure that the changes are pushed to the engine.

The script first reads the export file and determines if objects are valid. It then performs a dependency check to determine if any item referenced by an exported object is missing. The -w option allows the files to be converted to version 3.x format, even if validation warnings occur. The -d option allows the files to be converted to version 3.x format, even if dependency warnings occur. All warnings are written to the upgrade log.

To convert the export file even if warnings occur:

1. From a command line prompt, go to the /*install_dir*/bin directory, where *install_dir* is the CM installation directory.

2. Do one of the following:
    *   To convert the export file even if validation or dependency warnings occur, type the following command:

```
./sspUpgrade export_file_name engine_name -enginehost value -engineport value -w
```

    *   To convert the export file even if dependency warnings occur, type the following command:

```
./sspUpgrade export_file_name engine_name -enginehost value -engineport value -d
```

> **Note:** To associate converted files with an engine that is already defined in version 3.x, you do not have to specify an enginehost and engineport value on the command line.

3. Do one of the following:
    *   If you have not backed up the /*install_dir*/conf/ folder, type n and press **Enter** to stop the script. After you perform the backup, start over with this procedure.
    *   Press **Enter** to continue.
4. Type the passphrase defined at installation for SSP version 2.0.x and press **Enter**.
5. Type the passphrase defined when you installed CM and press **Enter**.

Upgrade Script Options

Following are the arguments to use when running the upgrade script:

Argument	Description	Required
export_file_name	The name assigned to the file you exported from version 2.0.x.	Y
engine_name	The engine name where the resources should be copied.	Y
	◆ If this engine has not been created, the upgrade script creates it and assigns it the default values. It then adds all the resources to the engine definition. If you do not define the -enginehost and -engineport parameters, use CM to complete the engine definition. If you provide a value for the parameters called enginehost and engineport, the engine is configured as part of the upgrade procedure and is ready for use.	
	◆ If the engine name already exists in version 3.x, all components in the export file are added to the engine definition.	
-enginehost *hostvalue*	The engine host name.The default is defaultEngineHost.	

Argument	Description	Required
-engineport *portvalue*	The engine port used to communicate with CM and inbound nodes. The default value is 63366.	
-userstore *userStoreName*	The name of the user store where user definitions are added. If no user store is specified, definitions are added to the default user store, called defUserStore.	
-truststore *trustStoreName*	The name of the trust store where trusted certificates are added. If no trust store is specified, trusted certificates are added to the default trust store, called dfltTrustStore.	
-keystore *keyStoreName*	The name of the keystore where key certificates are added. If no keystore is specified, key certificates are added to the default key store, called dfltKeyStore.	
-conf	An alternate location to copy the files after they are converted. The directory must already exist and must contain the key file needed to encrypt the files. The default directory is ../conf.	
-help or -h	To view help for the command.	
Following are the options to identify how the script is implemented:		
	If no option is defined, the upgrade process validates the parameters in the export file and performs a dependency check to determine if items referenced by an exported object are available. If any validation or dependency warnings are identified, the upgrade is stopped. If any object being upgraded already exists in CM, it is not replaced.	
-v	Performs a validation to make sure that the 2.0.x export file can be converted to version 3.x format without warnings. However, the file is not converted. Any warnings are written to a log file. Use this option to identify warnings and fix them before you move the information into version 3.x.	
-d	Converts the export file, even when dependency warnings occur. A dependency check determines if any item referenced by an exported object is missing. Dependency check warnings are written to the log. If a validation warning occurs, the upgrade process is stopped, and no files are updated.	
-w	Converts the export file, even when validation or dependency warnings occur. Be sure to resolve any warnings before you begin sending data through SSP.	
-o	If an item already exists, overwrites the item with the new information.	

Read the Upgrade Log File

After you run the upgrade script, make sure that the upgrade is successful. Read the upgrade log located in the *Engineinstall_dir*logs folder in the Engine installation directory.

Following is a sample log message:

```
21 Apr 2009 13:09:30,746 5281 [main] WARN
com.sterlingcommerce.hadrian.tools.gis.conversion.GISConverter - General
warning(s)occurred, upgrade process stopped.
```

A message includes the following information:

Field	Description	Sample Message Text
Date and timeStamp	The date when the message is written.	21 Apr 2009 13:09:30
Process ID	An ID assigned to the message.	746 5281
Message type	The type of message written: INFO or WARN. Use the WARN messages to troubleshoot a conversion problem.	WARN
Program module	The module that generated the warning.	com.sterlingcommerce. hardrian.tools.gis. conversionGISConverter
Message text	A description of the informational message or warning.	General warning(s) occurred, upgrade process stopped.

Following are some of the warning messages that are written to the upgrade log. Use the messages to troubleshoot any problems that occur:

Warning Message	Description
DEPENDENCY CHECK WARNING: Netmap inbound node *nodename* is missing key certificate *certificatename*	The key certificate referenced in the netmap inbound node is missing. If you specify the -d argument on the command line, the items available in the export file will be converted to version 3.x and can be used. However, you must import the certificate into SSP 3.x before you are ready for a production environment.
Warning	A problem occurred when an item was converted to the version 3.x format.
GENERAL WARNING: Engine host and/or port is not provided for newengine, using default values.	You did not define a host and port argument for the engine you created. You must use CM to update the Engine before you are ready for production. Refer to *Validate the Converted Components in SSP Version 3.x* on page 77.
General warning(s) occurred. Upgrade process stopped.	Warnings cause the upgrade process to stop. If you want the upgrade process to continue even when warnings occur, use the -w argument.

Warning Message	Description
Upgrade process begins saving configuration with warnings	The -w argument was used on the command line.
WARN:General warning (s) ignored	The -w argument was used on the command line. Even though a warning occurred the conversion continues. Be sure to validate your configuration before you move to a production environment.
Upgrade is completed successfully.	The export file was successfully converted to version 3.x format.
Validation of C:\source\temp\ssp2.0.2export\ exportfile.xml is completed	The export file has been validated.
General exception(s) occurred.	The export was stopped because a warning occurred.

Copy an Adapter

When you upgrade a cluster environment, you define multiple engines. One engine is the primary engine and performs the main workload. Each additional engine performs the work, if the primary engine is unavailable. Configuration information must be the same at all engines in the cluster. Engines can share configuration files for netmaps, policies, user stores, trust stores, and keystores. They cannot share adapter configuration files because each adapter is associated with one engine.

To ensure that information is the same at each engine, create a copy of each adapter defined at the primary node. Then, associate the copy of the adapter with the new engine.

To copy an adapter definition and associate it with a secondary engine:

1. If necessary, select Configuration from the menu bar.

2. Expand the Adapters tree and select the adapter to copy.

3. Select Actions > Copy Selected.

   A new item is created and renamed to Copyof*Adapter,* where *AdapterName* is the name of the original adapter.

4. Rename the adapter. Be sure to remove the name of the primary engine and replace it with the name of the engine you are configuring.

5. From the Engine drop-down list, select the name of the engine you are configuring.

6. Click Save.

7. Repeat this process for every adapter that you want to use with this engine.

Sterling Secure Proxy Installation Guide

Validate the Converted Components in SSP Version 3.x

After you run the upgrade script, the converted items are now available in SSP version 3.x. Before using SSP 3.x, open the engine, adapters, and any remote perimeter servers and validate the definitions.

Validate an Engine Definition

When you run the upgrade script, you identified an engine in the engine name parameter. If the upgrade was successful, an engine definition is now available in SSP 3.x.

✦ If you specified the -enginehost and -engineport arguments in the upgrade script, the engine is ready to use. Use this procedure to validate the engine definition to make sure that the host and port values are correct.

✦ If you did not specify the -enginehost and -engineport arguments in the upgrade command, an engine is defined but it does not have a valid host and port value. Use this procedure to define the host and port associated with the engine.

If necessary, gather the following information and use it as you configure 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 validate an engine definition:

1. If necessary, click Configuration from the menu bar.

2. Expand the Engines tree and click the engine to validate.

3. Check the following values and change them as needed:

    ◆ Engine Host

    ◆ Engine Listen Port

4. Click Save.

Validate an Adapter

When you perform an upgrade, version 2.0.x adapters are converted to version 3.x. Before you begin using the adapters in a version 3.x production environment, open each adapter and validate the settings.

To view an adapter definition:

1. If necessary, select Configuration from the menu bar.
2. Expand the Adapters tree and select the adapter to view.
3. View the configuration for the adapter. If necessary, modify the configuration.

   Refer to the online help for a description of each field and valid values.
4. Click Save.
5. Click OK.

Validate a PS Definition for a PS in a More Secure Zone

To validate a perimeter server definition when the PS is in a more secure zone:

1. From CM, click Advanced from the menu bar.
2. Click the Perimeter Servers tree to expand it.
3. Click More Secure Zone to view the more secure PS definitions.
4. Click the more secure PS to validate.
5. Make sure that the Proxy Local Listen Port is correctly defined.
6. Click Save.

Validate a PS Definition for a PS in a Less Secure Zone

To validate a perimeter server definition when the PS is in a less secure zone:

1. From CM, click Advanced from the menu bar.
2. Click the Perimeter Servers tree to expand it.
3. Click Less Secure Zone to view the less secure PS definitions.
4. Click the less secure PS to validate.
5. Make sure that the Perimeter Server Host and Perimeter Server Port are correct.
6. Click Save.

Validate the Connection Between Engines and CM

After you ensure that the engine definition is valid, use the following procedure to make sure that the engine can connect to CM.

To validate engine connections:

1. Click Monitoring from the menu bar.

2. Click Engine Status (All). A list of all configured engines is displayed, including the status. Status is displayed as follows:

   ◆ Engine is running

   ◆ Engine is not running

3. Make sure that the engine is running.

Maintain Changes to HTTP Properties

You had the ability to modify the following properties for version 2.0.x HTTP adapters in the *install_dir*/properties/httpproxy.properties file:

✦ Common exploits that are blocked for an adapter (blockexploit)

✦ Commands allowed (http.commands.allowed)

✦ Commands prohibited (http.commands.prohibited)

✦ Maximum length of an HTTP header in an incoming HTTP request (httpMaxHeaderFieldLength)

✦ Maximum number of HTTP headers allowed in the incoming HTTP request (httpMaxNumHeaderFields)

Modified properties are not maintained when you convert to version 3.x

Note: In 2.0.x, the properties applied to all HTTP adapters. In version 3.x, properties are defined for each adapter.

To maintain HTTP property changes in version 3.x:

1. Write down the changes you made to HTTP properties in version 2.0.x:

   Exploit to Block:_____

   Additions to methods allowed:_____

   Additions to prohibited methods:_____

   Maximum length of an HTTP header:_____

   Maximum number of HTTP headers allowed:_____

2. Open CM version 3.x.

3. From the Configuration navigation panel, expand the Adapters tree and click the adapter to modify.

4. On the HTTP Adapter Configuration panel, click the Properties tab.

5. To edit an existing value, type the new value in the Value field.

6. To delete an item, click the radio button to the left of an item and click Delete.

7. To add a new item, click New.

8. Modify one of the properties as required:

   ◆ To add a block common exploits value, type block.exploit.strings.*n* as the Key value, where *n* is a unique number appended to the block.exploit.strings key. Be sure that you increment the number and do not duplicate an existing key. Type the value to block in the Value field.

   ◆ To add an HTTP command allowed, type http.commands.allowed in the Key value. Type the commands to allow in the Value field.

   ◆ To add an HTTP command prohibited, type http.commands.prohibited in the Key value. Type the commands to prohibit in the Value field.

   ◆ To modify the maximum header fields length allowed, type httpMaxHeaderFieldLength in the Key value. Type the maximum header length in the Value field.

   ◆ To modify the maximum number of header fields allowed, type httpMaxNumHeaderField in the Key value. Type the maximum header value in the Value field.

9. Click OK.

10. Click Save.

11. Repeat steps 3 through 10 for each adapter you want to update.

New Properties in Version 3.x HTTP Adapter

New properties are defined in version 3.x for the HTTP adapter. These properties have default values that may change the behavior of an adapter. If necessary, change one or more of these properties for your environment. Properties include:

✦ max.ps.client.threads—Maximum number of threads in the pool used during a connection with a client. Default value is 10.

✦ max.ps.server.threads—Maximum number of threads in the pool used during a connection with a server. Default value is 10.

Maintain Changes to FTP Properties

You had the ability to modify the following FTP adapter properties for version 2.0.x in the *install_dir*/properties/httpproxy.properties file:

✦ Commands allowed in the ftp.commands.allowed string

✦ Commands prohibited in the ftp.commands.prohibited string

Modified values for these properties are not maintained when you convert to version 3.x.

Note: In 2.0.x, the properties applied to all HTTP adapters. In version 3.x, properties are defined for each adapter.

To maintain FTP property changes in version 3.x:

1. Write down the changes you made to FTP properties in version 2.0.x.:

    Additions to methods allowed:_____

    Additions to prohibited methods:_____

2. Open CM version 3.x.

3. From the Configuration navigation panel, expand the Adapters tree and click the FTP adapter to modify.

4. On the FTP Adapter Configuration panel, click the Properties tab.

5. To edit an existing value, type the new value in the Value field.

6. To delete an item, click the radio button to the left of an item and click Delete.

7. To add a new item, click New.

8. Modify one of the properties as required:

    ◆ To add an FTP command allowed, type ftp.commands.allowed in the Key value. Type the command to allow in the Value field.

    ◆ To add an FTP command prohibited, type ftp.commands.prohibited in the Key value. Type the command to prohibit in the Value field.

9. Click OK.

10. Click Save.

11. Repeat steps 3 through 10 for each adapter you want to update.

New FTP Adapter Properties in Version 3.x

New FTP adapter properties are defined in version 3.x. These properties have default values that may change the behavior of an adapter. If necessary, change one or more of the following properties for your environment:

✦ max.ps.server.threads—Maximum number of threads in the pool used during a connection with a server. Default value is 10.

✦ ftp.ssl.pbsz.required—Identifies whether the SSL command, PBSZ, is required. Valid values include Y|Yes|y|No|N|n. The default is Y.

✦ ftp.ssl.prot.required—Identifies whether the SSL command, PROT, is required. Valid values include Y|Yes|y|No|N|n. The default is Y.

✦ max.ps.client.threads—Maximum number of threads in the pool used during a connection with a client. Default value is 10.

✦ ftp.max.command.length—Maximum length allowed for a client command. The default is 1024. The command length is unlimited if this parameter is set to 0. If this length is exceeded, an error is logged and the connection is closed.

✦ ftp.max.response.length—Maximum length allowed for a server ftp response. The default is 4096. The server ftp length is unlimited if the parameter is set to 0. If this length is exceeded, an error is logged and the connection is closed. Set this parameter to 0 when communicating with a z/OS FTP server.

Implement Property Changes Made to a Connect:Direct Adapter

You had the ability to modify properties for a Connect:Direct adapter in Version 2.0.x. If you made changes, they are not maintained when you upgrade to version 3.x. Properties that may be modified include:

✦ CDSP|BreadCrumbAddress=granted—By default, this property is set to *granted* to allow information to be added to messages and identify the presence of a proxy in a communications session. You may have changed this value to *denied* to prevent proxy information from being added to a message.

✦ CDSP|BreadCrumbAddressTransparentContent=wishboneHoast—Identifies the string that is placed in the Connect:Direct FMH message if BreadCrumbAddress is set to *denied*. If BreadCrumbAddress is set to *granted*, information about the adapter is placed in the FMH message.

To implement Connect:Direct property changes in version 3.x:

1. Identify the changes you made in version 2.0.x. Write down the changes below:

   Connect:Direct property changes:_____

2. Open CM version 3.x.

3. From the Configuration navigation panel, expand the Adapters tree and click the Connect:Direct adapter to modify.

4. On the Connect:Direct Adapter Configuration panel, click the Properties tab.

5. Click New.

6. Type the property string in the Key field and the value in the Value field.

7. Click OK.

8. Click Save.

Change How Many Times a User Can Attempt to Log In Before a Lock Occurs

You can modify the lock out parameter for HTTP and FTP in SSP 2.0.x to change how many consecutive times a user can attempt to log in before being locked out. Any changes made to this parameter are not maintained when you upgrade to version 3.x. In addition, version 3.x changes the behavior of a user lockout. In version 2.0.x, the user remained locked out until you unlocked the account. In version 3.x, you define a lockout duration. When the lockout duration elapses, starting from the last failed login attempt, the user can then access SSP. For each user store that you define, you must identify the lockout duration and the user lockout threshold.

To change how many times a user can attempt to log in before a lock occurs and how long to lock out a user:

1. Write down the value you assigned to log in attempts allowed in SSP version 2.0.x. This value is defined in the maxConsecutiveAuthAttempts property in the ftpproxy.properties and httpproxy.properties files located in the *install_dir*/properties directory.

   Value of Log In Attempts Allowed:_____

2. Open CM version 3.x.

3. Click Credentials on the menu bar.

4. Expand the User Store tree and click the user store where user definitions are defined. The default user store is defUserStore.

5. Set the user attempts allowed in the User Lockout Threshold field.

6. Identify how long a user is locked out in the User Lockout Duration field.

7. Click Save.

Move Key Certificates Created in SSP 2.0.02 on the HSM

If you used HSM to store certificates in SSP version 2.0.02 and you want to use these certificates in SSP version 3.1, complete this procedure.

Use one of the following procedures to convert HSM key certificates from SSP 2.0.02 to SSP 3.x.

To convert HSM key certificates from an SSP 2.0.02 installation:

1. Type RemoveSystemCert -l and redirect the output of the script to a file. This command lists the system certificates stored in version 2.0.02 and writes them to the file. Remove the lines from the top of the file up to the first "PrivateKeyInfo for ID" line.

2. Export the configuration into an XML file. Refer to *Export SSP Version 2.0.x Information* on page 68.

3. Stop SSP.

To convert HSM key certificates from an SSP 3.1installation:

1. Install the SSP 3.1 engine on the same computer where SSP 2.0.02 is installed. For UNIX or Linux, refer to *Install or Upgrade the Engine on UNIX or Linux* on page 20. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 32.

2. Type the following command to enable HSM support:

```
setupHSM -enable hsm=hardwaredevicename path = locationofHSMSoftware
```

    Refer to *Chapter 4, Store System Certificate on a Hardware Security Module (HSM)* in the *Sterling Secure Proxy Configuration Guide* for more information on the command parameters.

3. Start the engine. For UNIX or Linux, refer to *Start the Engine on UNIX or Linux* on page 24. For Windows, refer to *Start SSP as an Automatic Windows Service* on page 36

4. Install CM. For UNIX or Linux, refer to *Install or Upgrade CM on UNIX or Linux* on page 22. For Windows, refer to *Install or Upgrade CM on Windows* on page 34.

5. Create an engine definition on CM. Make sure that the engine shows on monitoring screen as running. Refer to *Validate an Engine Definition* on page 77.

6. Stop CM.

7. Type the following command at CM to obtain the HSM keys and add them to the CM database. Identify the file that you created in step 2 on page 84 in the file parameter.

```
manageKeyCerts -loadHSM file=filecreatedfromversion2.0.02HSM
```

    The *file* is the name of the file created in step 1 on page 84.

    Refer to *Chapter 4, Store System Certificate on a Hardware Security Module (HSM)* in the *Sterling Secure Proxy Configuration Guide* for more information on the command parameters.

8. Type the following command at CM:

```
sspUpgrade export_file_name engine_name -enginehost value -engineport value -d
```

    Specify the engine name and the -d option to ignore dependencies. The -d option is required to ensure that the script runs successfully. The *export_file_name* is the name of the file created in step 2 on page 84.

Install a Remote Perimeter Server

SSP uses perimeter servers to increase security between internal and external communications. A local perimeter server (internal) is installed with SSP. 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 SSP. 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 the *Sterling Secure Proxy Configuration Guide*.

Remote 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.

✦ On the remote computer, install a JDK version that the perimeter server supports.

Caution: Do not use spaces in the name of the JDK installation directory.

✦ Obtain access to the SSP installation distribution media, or go to the ESD download directory that contains the ps_200*x*.jar file.

✦ Obtain the IP address for both the remote perimeter server computer and the engine computer.

✦ Open the port for connections from the engine to the remote perimeter server computer on which you plan to install your perimeter server.

Remote 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 a perimeter server on a computer with an existing instance, install the new perimeter server in a different installation directory.

✦ 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

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

1. Do one of the following:

   ◆ To download the product from the ESD Portal, navigate to the directory containing the downloaded ps_200*x*.jar file

   ◆ To install the product from the distribution media, mount the drive and navigate to the remote_perimeter_server directory of the distribution media to locate the ps_200*x*.jar file.

2. Copy the installation files 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 absolute path to the following jar file:

```
/absolutePath/jre/bin/java –jar /absolutePath/ps_200x.jar
```

The program verifies the operating system and required patch level and the location and version of the JRE.

4. Enter the full path name of the installation directory.

5. If an installation exists in the directory you specify, you can update it using the same settings. Answer the question:

```
There is an existing install at that location, update it while keeping existing
settings?
```

If yes, the installation proceeds without additional input.

> **Note:** To change any of the settings, use a new directory, or delete the old installation before performing the new installation. You cannot overwrite an existing installation, and you cannot use an existing directory that contains an invalid installation.

6. Confirm that the installation directory is correct.

   The program verifies the amount of available disk space.

7. Answer No to the question, "Is this server in a less secure network than the integration server?"

8. Answer the question:

```
Will this server need to operate on specific network interfaces?
```

If yes, the program returns a list of the network interfaces available on your host. Select the interfaces for the server to use.

   a. Enter the TCP/IP address or DNS name on which the engine listens for the connection from this server.

   b. Verify the TCP/IP address or DNS name.

9. Enter the port on which the engine listens for the connection from this server. The port number must be greater than or equal to 1024.

10. Enter the local port that the perimeter server will use for the connection to the engine. The port number must be greater than or equal to 1024. However, specify a port of zero if you want the operating system to select any unused port.

11. Verify the port.

    When the perimeter server is installed, the following message is displayed:

```
Installation of Perimeter Service is finished
```

12. Change to the installation directory.

13. Type startupPs.sh to start the perimeter server.

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

To install a perimeter server in a less secure network in a UNIX or Linux environment:

1. Do one of the following:

   ◆ To download the product from the ESD Portal, navigate to the directory containing the downloaded ps_200*x*.jar file

   ◆ To install the product from the distribution media, mount the drive and navigate to the remote_perimeter_directory of the distribution media to locate the ps_200*x*.jar file.

2. Copy the installation files from the installation distribution media 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 absolute path to the following jar file:

   ```
   /absolutePath/jre/bin/java -jar /absolutePath/ps_200x.jar
   ```

   The program verifies the operating system and required patch level and the location and version of the JRE.

4. Enter the full path name of the installation directory.

5. If an installation exists in the directory you specify, you can update it using the same settings. Answer the question:

   ```
   There is an existing install at that location, update it while keeping existing
   settings?
   ```

   If yes, the installation proceeds without additional entries.

Note:	To change any of the settings, use a new directory or delete the old installation before installing the new one. You cannot overwrite an existing installation, and you cannot use an existing directory that contains an invalid installation.

6. Confirm that the installation directory is correct.

   The program verifies the amount of available disk space.

7. Answer Yes to the question, "Is this server in a less secure network than the integration server?"

8. Answer the question:

   ```
   Will this server need to operate on specific network interfaces?
   ```

If yes, a list of the network interfaces available on your host displays. Select the interfaces for the server to use, and complete the following steps.

    a. Enter the TCP/IP address or DNS name that the internal interface is to use to communicate with the engine. Press Enter to use a wildcard for this address.

    b. Verify the TCP/IP address or DNS name for the internal interface.

    c. Enter the TCP/IP address or DNS name for the external interface to use to communicate with trading partners. Press Enter to use a wildcard for this address.

    d. Verify the TCP/IP address or DNS name for the external interface.

9. Enter the port on which the perimeter server will listen for the connection from the engine. The port number must be greater than or equal to 1024.

10. Verify the port. When the perimeter server is installed, the following message is displayed:

```
Installation of Perimeter Service is finished
```

11. Change to the installation directory.

12. Type startupPs.sh to start the perimeter server.

Install Remote Perimeter Server in a More Secure Network in Windows

To install a perimeter server in a Windows environment:

1. Close all open Windows programs.

2. Do one of the following:

    ◆ To download the product from the ESD Portal, navigate to the directory containing the downloaded ps_200*x*.jar file.

    ◆ To install the product from the distribution media, mount the drive and navigate to the remote_perimeter_server directory of the distribution media to locate the ps_200*x*.jar file.

3. Open a DOS command window.

4. Copy the installation files to your home directory or base directory. If you are using FTP to copy the file, be sure your session is set to binary mode.

5. To begin the installation, enter the absolute path to the following jar file:

```
\absolutePath\jre\bin\java -jar \absolutePath\ps_200x.jar
```

The program verifies the operating system and required patch level and the location and version of the JRE.

6. Enter the name for the installation directory and press **Enter**.

7. If an installation exists in the directory you specify, you can update it using the same settings. Answer the following question:

```
There is an existing install at that location, update it while keeping existing
settings?
```

If yes, the installation proceeds without additional input.

> **Note:** To change any of the settings, use a new directory or delete the old installation before installing the new one. You cannot overwrite an existing installation, and you cannot use an existing directory that contains an invalid installation.

The program verifies the amount of available disk space.

8. Answer No to the question: Is this server in a less secure network than the integration server?

9. Answer the following question:

```
Will this server need to operate on specific network interfaces?
```

If yes, the network interfaces available on your host are displayed. Select the interfaces for the server to use.

a. Enter the TCP/IP address or DNS name on which the engine listens for the connection from this server and press **Enter**.

b. Verify the TCP/IP address or DNS name, or press **Enter** to use a wildcard address.

10. Enter the port on which the engine will listen for the connection from this server. The port number must be greater than or equal to 1024.

11. Enter the local port that the perimeter server will use for the connection to Sterling Secure Proxy. The port number must be zero or a number greater than or equal to 1024. Specify zero if you want the operating system to select any unused port.

12. Verify the port.

13. When installation is complete, change to the installation directory.

14. Type installPS.cmd to install this perimeter server as a Windows Service.

15. Type startPSService.cmd to start the perimeter server.

Install Remote Perimeter Server in a Less Secure Network in Windows

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

1. Close all open Windows programs.

2. Do one of the following:

   * If you download the product from the ESD Portal, navigate to the directory containing the downloaded ps_200*x*.jar file.

   * If you install the product from the distribution media, mount the drive and navigate to the remote_perimeter_server directory to locate the ps_200*x*.jar file.

3. Open a DOS command window.

4. Copy the installation files to your home directory or base directory. If you are using FTP to copy the file, be sure your session is set to binary mode.

5. To begin the installation, enter the absolute path to the following jar file:

```
\absolutePath\jre\bin\java -jar \absolutePath\ps_200x.jar
```

   The program verifies the operating system and required patch level and the location and version of the JRE.

6. Enter the name for the installation directory.

7. If an installation exists in the directory you specify, you can update it using the same settings. Answer the following question:

```
There is an existing install at that location, update it while keeping existing
settings?
```

   If you answer yes, the installation proceeds without additional input.

Note:	To change any of the settings, use a new directory or delete the old installation before installing the new one. You cannot overwrite an existing installation, and you cannot use an existing directory that contains an invalid installation.

   The program verifies the amount of available disk space.

8. Answer Yes to the question: Is this server in a less secure network than the integration server?

9. Answer the question:

```
Will this server need to operate on specific network interfaces?
```

   If you answer yes, a list of network interfaces available on your host displays. Select the interfaces for the server to use, and complete the following steps.

   a. Enter the TCP/IP address or DNS name for the internal interface to use to communicate with the integration server (Sterling Secure Proxy). Press **Enter** to use a wildcard for this address.

   b. Verify the TCP/IP address or DNS name for the internal interface.

   c. Type the TCP/IP address or DNS name for the external interface to use to communicate with trading partners. Press Enter to use a wildcard for this address.

   d. Verify the TCP/IP address or DNS name for the external interface.

10. Type the port on which the perimeter server will listen for the connection from the server (Sterling Secure Proxy). The port number must be greater than or equal to 1024.

11. Verify the port.

12. When the installation is complete, change to the installation directory.

13. Type installPS.cmd to install this perimeter server as a Windows service.

14. Type startPSService.cmd to start the perimeter server.

Restrict the Policy for a Remote Perimeter Server

To limit perimeter server activity:

1. Install a remote perimeter server. Select the option to indicate that the perimeter server is in a more-secure network zone.

2. Edit the restricted.policy file located in the installation directory. The following is a sample restricted.policy file.

```
// Standard extensions get all permissions by default
grant codeBase "file:${{java.ext.dirs}}/*" {
permission java.security.AllPermission;
};
grant {
// Grant all permissions needed for basic operation.
permission java.util.PropertyPermission "*", "read";
permission java.security.SecurityPermission "putProviderProperty.*";
permission java.io.FilePermission "-", "read,write";
permission java.io.FilePermission ".", "read";
// Needed to allow lookup of network interfaces.
permission java.net.SocketPermission "*", "resolve";
};
grant {
// Adjust for your local network requirements.
// Needed to connect out for the persistent connection
permission java.net.SocketPermission "localhost:12002", "connect";
// For each target FTP Server
//
// permission java.net.SocketPermission "ftphost:21", "connect";
// Control connection.
// permission java.net.SocketPermission"
ftphost:lowPort-highPort", "connect"; // Passive data connections.
// For each target HTTP Server//
//
permission java.net.SocketPermission "htttphost:443", "connect";
// For each target C:D snode
//
// permission java.net.SocketPermission "snode:1364", "connect";
};
```

Edit the grant section, highlighted above, to define your local network requirements. Add a permission line for each back-end server Sterling Secure Proxy server can access.

Commented examples are provided for each type of back-end server that Sterling Secure Proxy supports.

> **Note:** Do not edit the grant sections called grant codeBase or Grant all permissions needed for basic operations.

3. To turn on restrictions in a UNIX installation, edit the startupPs.sh file located in the perimeter server *install_dir* installation directory. Uncomment the following line:

```
#POLICY="-Djava.security.manager -Djava.security.policy==restricted.policy"
```

Restrictions will take effect the next time you start this perimeter server.

4. To turn on and activate restrictions in Windows:

   a. Edit the installPS.cmd file located in the perimeter server installation directory. Uncomment the following line:

   ```
   rem set POLICY="-Djava.security.manager
   -Djava.security.policy==restricted.policy"
   ```

   b. Run `stopPSService.cmd` to stop the current perimeter server.

   c. If you installed the Windows service for the perimeter server, run `uninstallPSService.cmd` to uninstall the existing perimeter server.

   d. Run `installPS.cmd` to install the modified version of the Windows service.

   e. Run startPSService.cmd to run the restricted perimeter server.

   > **Note:** If the perimeter server attempts to access restricted network resources, the connection is rejected and logged in the perimeter server log.

Index

A

Adapter
  copy 76
  defined 9
  start from CM 40
  stop from CM 40
  validate 77

B

Back up, version 3.x files 70

Background mode, run engine in 41

C

Change
  CM passphrase, UNIX or Linux 43
  CM passphrase, Windows 48
  engine passphrase, UNIX or Linux 42
  startup mode, UNIX or Linux 41
  startup mode, Windows 44

Checklist, post installation 39

Clustered nodes
  file conversion 57
  file conversion, illustration 57
  upgrade checklist 59

Configuration Manager
  change passphrase, UNIX or Linux 43
  change startup mode 41
  install or upgrade on UNIX 20
  logon, Windows 35
  run in background, UNIX or Linux 42
  run in foreground, UNIX or Linux 42
  start adapter from 40
  start as console application, Windows 45
  start, UNIX or Linux 25
  stop adapter from 40
  stop engine from 40
  stop from UNIX or Linux 28
  stop, Windows 38
  uninstall, UNIX or Linux 44

Configuration Manager (continued)
  uninstall, Windows 49
  upgrade or install on Windows 33
  validate connection to engines 78

Convert
  files from version 2.0.x to 3.0.01 70
  version 2.0.x files for existing engine, ignore
    warnings 72
  version 2.0.x files for new engine 71
  version 2.0.x files, if no warnings 71
  version 2.0.x files, ignore warnings 72

Copy, adapter 76

Create engine definition 26, 37

D

Definition of Sterling Secure Proxy 7

E

EA, defined 9

Engine
  associate with NIC card 22
  associate with NIC Card, Windows 33
  change passphrase, UNIX or Linux 42
  convert files for existing engine 72
  convert files for new engine 71
  convert files, ignore warnings 72
  create definition 26
  install or upgrade on UNIX or Linux 20
  require passphrase at startup, Windows 45
  run in background, UNIX or Linux 41
  run in the foreground, UNIX or Linux 42
  start as console application, Windows 45
  stop from CM 40
  stop from UNIX or Linux 28
  stop from Windows 38
  stop from Windows console application 47
  validate connection to CM 78
  view configured 37

Sterling Secure Proxy Installation Guide

V

W

Third Party Software

doc_ssp3.1.01

Portions of the Sterling Commerce Software may include products, or may be distributed on the same storage media with products, ("Third Party Software") offered by third parties ("Third Party Licensors"). Sterling Commerce Software may include Third Party Software covered by the following copyrights: Copyright © 2002-2005 Andy Clark. Copyright © 1999-2007 The Apache Software Foundation. Copyright © 2007 Brice Burgess. Copyright © 2002, 2003, 2004 Certicom Corp. Copyright © 2000-2004 Jason Hunter & Brett McLaughlin. Copyright © 1998-2005 International Business Machines Corporation (ibm.com). Contains JMX™ Technology. Copyright 1999-2004 © Intalio, Inc, and others. Copyright © 2004-2007 QoS.ch. Copyright © 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). Copyright © 2001 Zero G Software, Inc. All rights reserved by all listed parties.

The Sterling Commerce Software is distributed on the same storage media as certain Third Party Software covered by the following copyrights: Copyright © 1999-2004 The Apache Software Foundation. Copyright © 1999-2008 Hewlett-Packard Company. Copyright ©2005, Michael Glad and Pawel Vesolv. Copyright © 2003 MortBay Consulting Pty., Ltd. (Australia) and others. Copyright © 1994-2008 Sun Microsystems, Inc. Copyright © S.E. Morris (FISH) 2003-04. All rights reserved by all listed parties.

Certain components of the Sterling Commerce Software are distributed on the same storage media as certain Third Party Software not listed above. Additional Third Party Software information for such components of the Sterling Commerce Software is located in the file *readme.txt* located in the root directory of the DVD.

As set forth below, certain of the Third Party Licensors assert the following terms to their respective products. Such terms shall only apply as to the specific Third Party Licensor product and not to those portions of the product derived from other Third Party Licensor products or to this software product as a whole. Those portions of the Sterling Commerce Software which include, or are distributed on the same storage media with, the Third Party Software where use, duplication, or disclosure by the United States government or a government contractor or subcontractor, are provided with RESTRICTED RIGHTS under Title 48 CFR 2.101, 12.212, 52.227-19, 227.7201 through 227.7202-4, DFAR 252.227-7013(c) (1) (ii) and (2), DFAR 252.227-7015(b)(6/95), DFAR 227.7202-3(a), FAR 52.227-14(g)(2)(6/87), and FAR 52.227-19(c)(2) and (6/87)as applicable.

The Sterling Commerce Software and the related documentation are licensed either "AS IS" or with a limited warranty, as set forth in the Sterling Commerce license agreement. Other than any limited warranties provided, NO OTHER WARRANTY IS EXPRESSED AND NONE SHALL BE IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR USE OR FOR A PARTICULAR PURPOSE. The applicable Sterling Commerce entity reserves the right to revise this publication from time to time and to make changes in the content hereof without the obligation to notify any person or entity of such revisions or changes.

Except as otherwise set forth below, the Third Party Software is provided "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. FURTHER, IF YOU ARE LOCATED OR ACCESSING THIS SOFTWARE IN THE UNITED STATES, ANY EXPRESS OR IMPLIED WARRANTY REGARDING TITLE OR NON-INFRINGEMENT ARE DISCLAIMED.

THE APACHE SOFTWARE FOUNDATION

The Sterling Commerce Software is distributed with or on the same storage media as the following software products: Commons-el version 1.0 and Xerces version 2.0.2 (collectively, "Apache 1.1 Software").   Apache 1.1 Software is free software which is distributed under the terms of the following license:

License Version 1.1

Copyright 1999-2000, 2002 The Apache Software Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgement: "This product includes software developed by the Apache Software Foundation (http://www.apache.org)." Alternatively, this acknowledgement may appear in the software itself, if and whenever such third-party acknowledgements normally appear.
4. The names "BSF", "log4j", "Xerces "Xalan", "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without specific prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without the prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMIPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTIBILITY, AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTIAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. The BSF software was originally created by Sanjiva Weeranwarana and others at International Business Machines Corporation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>

The preceding license only applies to the Apache 1.1 Software and does not apply to the Sterling Commerce Software or to any other Third Party Software.

THE APACHE SOFTWARE FOUNDATION SOFTWARE

The Sterling Commerce Software is also distributed with or on the same storage media

as the following software products (or components thereof): Hivemind, Apache HTTP Client, Commons Logging, Apache Jakarta Commons Beanutils, Apache Jakarta ORO, Apache Log4J, and Apache Xalan 2.7.0, (collectively, "Apache 2.0 Software"). Apache 2.0 Software is free software which is distributed under the terms of the Apache License Version 2.0. A copy of License Version 2.0 is found in the following files for the individual pieces of the Apache 2.0 Software in the *install_dir/*lib/thirdparty directory:

> hivemind.license.txt
> http_client.license.txt
> commons_logging.licnese.txt
> commons_beanutils.license.txt
> oro.license.txt
> log4j.license.txt
> xalan.license.txt

Unless otherwise stated in a specific directory, the Apache 2.0 Software was not modified. Neither the Sterling Commerce Software, modifications, if any, to Apache 2.0 Software, nor other Third Party Code is a Derivative Work or a Contribution as defined in License Version 2.0. License Version 2.0 applies only to the Apache 2.0 Software which is the subject of the specific directory file and does not apply to the Sterling Commerce Software or to any other Third Party Software. License Version 2.0 includes the following provision:

"Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License."

CASTOR SOFTWARE

Copyright 1999-2004 (C) Intalio Inc., and others. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "ExoLab" must not be used to endorse or promote products derived from this Software without prior written permission of Intalio Inc. For written permission, please contact info@exolab.org.

4. Products derived from this Software may not be called "Castor" nor may "Castor" appear in their names without prior written permission of Intalio Inc. Exolab, Castor and Intalio are trademarks of Intalio Inc.

5. Due credit should be given to the ExoLab Project (http://www.exolab.org/).

THIS SOFTWARE IS PROVIDED BY INTALIO AND CONTRIBUTORS ""AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTALIO OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH   DAMAGE.

GETOPT SOFTWARE

The Getopt Software and is distributed WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

GETOPT.JAR SOFTWARE
The Sterling Commerce Software is distributed on the same storage media as the GETOPT.JAR software (Copyright © 1998-2002 Aaron M. Renn (arenn@urbanophile.com) ("Getopt Software") and the Crypt.jar software (Copyright ©2005, Michael Glad and Pawel Vesolv) ("Crypt.jar Software"). The Getopt Software and the Crypt.jar Software are both independent from and not linked or compiled with the Sterling Commerce Software. The Getopt Software and the Crypt.jar Software are free software products which can be distributed and/or modified under the terms of the GNU Library Public License as published by the Free Software Foundation, version 2, or the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License or any later version. A copy of the GNU Lesser General Public License is provided in the getopt.license.txt file in the *install_dir/*lib/thirdparty directory where Sterling Secure Proxy is installed. This license only applies to the Getopt.jar Software and the Crypt.jar Software and does not apply to the Sterling Commerce Software, or any other Third Party Software.

Sterling Commerce has not modified the Getopt.jar Software. Source code for the Getopt.jar Software is located at: http://www.urbanophile.com/arenn/hacking/download.html.
The Getopt.jar Software is distributed WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

HEWLETT PACKARD

The Sterling Commerce Software is distributed on the same storage media as the Hewlett-Packard Software which contains HP-UX Java Runtime Environment for the Java 2 Platform Standard Edition, version 5.0.14 for HP 9000 PA-RISC and HP-UX Integrity, Copyright © 1999-2007 Hewlett-Packard Development Company (collectively the "HP JRE Software"). All Rights Reserved. Additional license information is located in the file <install_dir>/lib/thirdparty/hp_jre.license.txt and applies only to the HP JRE Software and not to the Sterling Commerce Software or to any other Third Party Software. The HP JRE Software includes the following notice: "Some third-party code

embedded or bundled with the [HP JRE] Software is licensed to you under terms and conditions as set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions contained in the "AS IS" Warranty Statement shall apply to all code distributed as part of or bundled with the [HP JRE] Software."

US Government Rights Notice. Confidential Computer Software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and12.212, Commercial Computer Software, Computer Software documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

You will only find the JRE license information for the HP JRE Software in the specified directory if the Sterling Software and Third Party Software are installed on a HEWLETT PACKARD system.

IBM

The Sterling Commerce Software is distributed on the same storage media as the IBM software which contains Java 2 Runtime Environment 1.5.0 for AIX, Copyright © 1996-2005 IBM Corporation (collectively "IBM JRE Software"). All Rights Reserved. Other copyright acknowledgements may be found in the 'Notices' file in the IBM JRE Software.

U.S. Government Users Restricted Rights- Use, duplication or disclosure restricted by the GSA ADP Schedule Contract with the IBM Corporation.

You will only find the JRE license information for the IBM JRE Software in the specified directory if the Sterling Software and Third Party Software are installed on an IBM system.

JASPER REPORTS

Copyright © 2001-2004 Teodor Danciu (teodord@users.sourceforge.net) All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by Teodor Danciu (http://jasperreports.sourceforge.net)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The name "JasperReports" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact teodord@users.sourceforge.net.

5. Products derived from this software may not be called "JasperReports", nor may "JasperReports" appear in their name, without prior written permission of Teodor Danciu.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JAVASSIST SOFTWARE

The Sterling Commerce Software is distributed on the same storage media as the Javassist Software (Copyright © 1999-2005 Shigeru Chiba) ("Javasist Software. The Javasisst Software is independent from and not linked or compiled with the Sterling Commerce Software. The Javassist Software is a free software product which can be distributed and/or modified under the terms of the Mozilla Public Licensed version 1.1 as published by The Mozilla Organization.

A copy of the Mozilla Public License is provided at javassist.license.txt file in the *install_dir*/lib/thirdparty directory where Sterling Secure Proxy is installed. This license only applies to the Javassist Software and does not apply to the Sterling Commerce Software, or any other Third Party Software.

The Javassist Software is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the license for the specific language governing rights and limitations under the license. Original Code is the Javassist Software 3.0 and the Initial Developer of the Original Code is Shigeru Chiba.

Sterling Commerce has not made any modifications to the Javasisst Software. Source code for the Javassist Software is located at http://downloads.sourceforge.net/jboss/javassist-3.0.zip?use_mirror=voxel. In the event the source code is no longer available from the website referenced herein, please contact Sterling Commerce support for assistance.

THE JAVASISST SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES THAT JAVASISST SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING.

JDOM SOFTWARE

The Sterling Commerce Software is distributed on the same storage media as the JDOM Software. The JDOM Software is a free software product which is distributed subject to the

following license (which applies only to the JDOM Software and not to the Sterling Commerce Software or any other Third Party Software):

Copyright (C) 2000-2004 Jason Hunter & Brett McLaughlin.
 All rights reserved.

 Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

 1. Redistributions of source code must retain the above copyright
    notice, this list of conditions, and the following disclaimer.

 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

 3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <request_AT_jdom_DOT_org>.

 4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management <request_AT_jdom_DOT_org>.

 In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following:
    "This product includes software developed by the
     JDOM Project (http://www.jdom.org/)."
 Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

 THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
 OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

 This software consists of voluntary contributions made by many
 individuals on behalf of the JDOM Project and was originally
 created by Jason Hunter <jhunter_AT_jdom_DOT_org> and
 Brett McLaughlin <brett_AT_jdom_DOT_org>. For more information on the JDOM Project, please see <http://www.jdom.org/>.

JETTY SOFTWARE

The Sterling Commerce Software is distributed with or on the same storage media as the Jetty Software, which is subject to the following license:

From http://jetty.mortbay.org/jetty/LICENSE.html:

<div align="center">

Jetty License
$Revision: 3.7$

</div>

Preamble:

The intent of this document is to state the conditions under which the Jetty Package may be copied, such that the Copyright Holder maintains some semblance of control over the development of the package, while giving the users of the package the right to use, distribute and make reasonable modifications to the Package in accordance with the goals and ideals of the Open Source concept as described at http://www.opensource.org.

It is the intent of this license to allow commercial usage of the Jetty Package, so long as the source code is distributed or suitable visible credit given or other arrangements made with the copyright holders.

Definitions:

• "Jetty" refers to the collection of Java classes that are distributed as a HTTP server with servlet capabilities and associated utilities.

• "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

• "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.

• "Copyright Holder" is whoever is named in the copyright or copyrights for the package. Mort Bay Consulting Pty. Ltd. (Australia) is the "Copyright Holder" for the Jetty Package.

• "You" is you, if you're thinking about copying or distributing this Package.

• "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

• "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

0. The Jetty Package is Copyright © Mort Bay Consulting Pty. Ltd. (Australia) and others. Individual files in this Package may contain additional copyright notices. The javax.serviet packages are copyright Sun Microsystems Inc.

1.   The Standard Version of the Jetty package is available from http://jetty.mortbay.org.

2.   You may make and distribute verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you include this license and all of the original copyright notices and associated disclaimers.

3.   You may make and distribute verbatim copies of the compiled form of the Standard Version of this Package without restriction, provided that you include this license.

4.   You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

5.   You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a)   Place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b)   Use the modified Package only within your corporation or organization.

c)   Rename any non-standard classes so the names do not conflict with standard classes, which must also be provided, and provide a separate manual page for each non-standard class that clearly documents how it differs from the Standard Version.

d)   Make other arrangements with the Copyright Holder.

6.   You may distribute modifications or subsets of this Package in source code or compiled form, provided that you do at least ONE of the following:

a)   Distribute this license and all original copyright messages, together with instructions (in the about dialog, manual page or equivalent) on where to get the complete Standard Version.

b)   Accompany the distribution with the machine-readable source of the Package with your modifications. The modified Package must include this license and all of the original copyright notices and associated disclaimers, together with instructions on where to get the complete Standard Version.

c)   Make other arrangements with the Copyright Holder.

7.   You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you meet the other distribution requirements of this license.

8.   Input to or the output produced from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.

9.   Any program subroutines supplied by you and linked into this Package shall not be considered part of this Package.

10.   The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

11.   This license may change with each release of a Standard Version of the Package. You may choose to use the license associated with version you are using or the license of the latest Standard Version.

12.   THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

13.   If any superior law implies a warranty, the sole remedy under such shall be, at the Copyright Holders option either a) return of any price paid or b) use or reasonable endeavours to repair or replace the software.

14.   This license shall be read under the laws of Australia.

The End

This license was derived from the Artistic license published on http://www.opensource.com

JQMODAL

The Sterling Commerce Software is distributed on the same storage media as the JQMODAL Software. The JQMODAL Software is a free software product which is distributed subject to the following license (which applies only to the JMODAL Software and not to the Sterling Commerce Software or any other Third Party Software):

Copyright (c) 2007 Brice Burgess.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,

TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

NEKO SOFTWARE
The Sterling Commerce Software is distributed on the same storage media as the Neko Software.
The Neko Software is a free software product which is distributed subject to the following license
(which applies only to the Neko Software and not to the Sterling Commerce Software or any
other Third Party Software):
(C) Copyright 2002-2005, Andy Clark. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

3. The end-user documentation included with the redistribution,
   if any, must include the following acknowledgment:
     "This product includes software developed by Andy Clark."
   Alternately, this acknowledgment may appear in the software itself, if and wherever such third-
party acknowledgments normally appear.

4. The names "CyberNeko" and "NekoHTML" must not be used to endorse or promote products
derived from this software without prior written permission. For written permission, please
contact andyc@cyberneko.net.

5. Products derived from this software may not be called "CyberNeko", nor may "CyberNeko"
appear in their name, without prior written permission of the author.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR OTHER CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY,
OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY
OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SLF4 Software
The Sterling Commerce Software is distributed on the same storage media as the SLF4J code,
Copyright © 2004-2007QOS.ch. All Rights Reserved. ("SLF4J Software"). The SLF4J Software
is distributed subject to the following license:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMIPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,ARISING FROM , OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SUN MICROSYSTEMS

SUN, Sun Microsystems, the Sun logo, Solaris, Java, Jini, Forte, J2SE, and iPlanet and all related trademarks, service marks logos and other brand designations that are referred to or displayed in the Sterling Commerce Software or the related documentation are trademarks or registered trademarks of Sun Microsystems, Inc. The Sterling Commerce Software is distributed on the same storage media as the JAVA (tm) 2 Runtime Environment (J2RE) Standard Edition, Version 5.0 for Solaris-Sparc, Solaris-i586 and Linux-i586, Copyright © 2008 Sun Microsystems, Inc. (collectively "Sun JRE Software"). All Rights Reserved.

The license terms for the Sun JRE Software are located at <install_dir>/lib/thirdparty/sun_jre.license.txt. The Sun JRE Software includes the following notice: "Additional copyright notices and license terms applicable to portions of the Sun JRE Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party open source/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Sun JRE Software in this distribution."

The Sun JRE Software license terms also require the inclusion of the following notice: "This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at http://oss.software.ibm.com/ico4j/."

If [Sun JRE] Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in [Sun JRE] Software and accompanying documentation will be only as set forth in this agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

You will only find the JRE license information for Sun JRE Software in the specified directory if the Sterling Software and Third Party Software are installed on a SUN Solaris system, a Microsoft Windows system, a Red Hat Linux system, or a SUSE Linux system.

Such licenses only apply to the Sun product which is the subject of such directory and does not apply to the Sterling Commerce Software or to any other Third Party Software

The Sterling Commerce Software is also distributed on the same storage media as NetBeans IDE 5.5 software, Copyright © 1999-2006 Sun Microsystems, Inc. All Rights Reserved. ("NetBeans Software"). Sterling Commerce has not made any additions or changes to the NetBeans Software. The Sterling Commerce Software is not a derivative work of the NetBeans Software. The Sterling Commerce Software is not a Contribution as defined in the Common Public License – v 1.0.

The source code for the NetBeansSoftware is available at netbeans.org.

The NetBeans source code is available from Sterling Commerce under the Common Public License - v 1.0. Contact Sterling Commerce Customer Support in the event that the source code for the NetBeans Software is no longer available at the above-listed site.   A copy of the Common Public License – v 1.0 is provided at netbeans.license.txt file located in *the install_dir*/lib/thirdparty directory where Sterling Secure Proxy is installed. This license applies only to the NetBeans Software and does not apply to the Sterling Commerce Software or any other Third Party Licensor Software.