Sterling Secure Proxy®

Installation Guide

Version 3.3.01

Sterling Commerce
An IBM Company

Sterling Secure Proxy Installation Guide
Version 3.3.01

First Edition

Sterling Commerce, Inc.
4600 Lakehurst Court Dublin, OH 43016-2000 *
614/793-7000

Contents

Chapter 1 System Requirements 7

System Requirements 7
SSP UNIX and Linux System Requirements 7
SSP UNIX and Linux Host System Requirements 7
SSP UNIX or Linux Operating Systems Supported 8
Perimeter Server Requirements in UNIX or Linux 8
Hardware Accelerator Board 8
Hardware Security Module (HSM) Requirements. 8
SSP Windows System Requirements 9
SSP Windows Host System Requirements 9
SSP-Supported Windows Operating Systems 9
Perimeter Server Requirements on Windows. 9
Client Connections Supported 9
Web Browsers Supported by CM 10
Server Connections Supported 10
Sterling Security Products Supported 11
Cipher Suites Supported 11
Review Resources for UNIX or Linux 11

Chapter 2 Install or Upgrade SSP on Windows 13

Install or Upgrade SSP on Windows 13
SSP Installation Checklist for Windows 13
SSP Startup Worksheet for Windows 14
Install or Upgrade the Engine on Windows 15
Install or Upgrade CM on Windows. 16
Obtain and Install a License Key File on Windows 16
Create an Engine Definition 16

Chapter 3 Install or Upgrade SSP on UNIX or Linux 19

Install or Upgrade SSP on UNIX or Linux 19
SSP Installation Checklist for UNIX or Linux. 19
SSP Startup Worksheet for UNIX or Linux 20
Install or Upgrade the Engine on UNIX or Linux 21

Install or Upgrade CM on UNIX or Linux 22
Obtain a License Key File for UNIX or Linux. 23
Create an Engine Definition 23

Chapter 4 Install a Remote Perimeter Server 25

Install a Remote Perimeter Server. 25
Perimeter Server Installation Prerequisites. 25
Perimeter Server Installation Guidelines 26
Install remote perimeter Server in a More Secure Network on UNIX or Linux . . 26
Install a remote perimeter Server in a Less Secure Network on UNIX or Linux . 27
Install remote perimeter Server in a More Secure Network in Windows. 29
Install remote perimeter Server in a Less Secure Network in Windows 30
Upgrade Perimeter Server in Windows, UNIX, or Linux 31
Restrict the Policy for a remote perimeter Server 31

Chapter 5 Upgrade SSP 35

Upgrade SSP from Version 2.0.x to Version 3.x 35
Upgrade a Single SSP Node. 36
Single Node File Conversion Illustration. 37
Pre-Upgrade Checklist 38
Upgrade Tasks 38
Upgrade SSP Clustered Nodes 40
Cluster Nodes File Conversion Illustration 42
Cluster Nodes Upgrade Checklist. 44
Upgrade an SSP Loading Balancing Environment 45
Load Balancing Nodes File Conversion Illustration 46
Load Balancing Nodes Upgrade Checklist 48
Upgrade a Multiple SSP Nodes Configuration 49
Multiple Node Environment File Conversion Illustration 50
Load Balancing Multiple Node Upgrade Checklist 52
Start and Log On to SSP Version 2.0.x. 53
Export SSP Version 2.0.x Information. 53
Stop Perimeter Server Version 2.0 54
Stop SSP Version 2.0.x. 54
Back Up Version 3.x Configuration Files. 55
Convert Files from SSP Version 2.0.x to Version 3.x 55
Validate an Export File 55
Convert Version 2.0.x Files With New Engine If No Warnings Are Found . . 56
Convert Version 2.0.x Files With Existing Engine If No Warnings Are Found 56
Convert Version 2.0.x Files and Ignore Warnings 57
Upgrade Script Options 58
Read the Upgrade Log File 59
Copy an Adapter 61
Validate the Converted Components in SSP Version 3.x 61
Validate an Engine Definition 61
Validate an Adapter 62
Validate a PS Definition for a PS in a More Secure Zone 62
Validate a PS Definition for a PS in a Less Secure Zone. 62
Validate the Connection Between Engines and CM 63

Maintain Changes to HTTP Properties 63
New Properties in Version 3.x HTTP Adapter. 65
Maintain Changes to FTP Properties 65
New FTP Adapter Properties in Version 3.x 66
Implement Property Changes Made to a Connect:Direct Adapter 66
Change How Many Times a User Can Attempt to Log In Before a Lock Occurs 67
Move Key Certificates Created in SSP 2.0.02 on the HSM 67

Chapter 1

System Requirements

System Requirements

System requirements vary with business needs and your system environment. Factors include number of transactions processed, amount of data transferred, and running SSP with a perimeter servers. Review the requirements before you begin the installation tasks.

SSP UNIX and Linux System Requirements

This section identifies the system requirements for UNIX and Linux platforms. A JRE is installed with SSP. Configuration information is maintained on Configuration Manager (CM) and the engine. The space to store configuration files depends on the files you transmit and how long you maintain them, as well as the level of logging. The minimum space in the following table identifies the space required if you turn on debugging.

SSP UNIX and Linux Host System Requirements

SSP requires the following 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
Perimeter Server	2048 or greater (preferred setting: unlimited)	1 GB	2 GB

SSP UNIX or Linux Operating Systems Supported

SSP supports the following UNIX and Linux operating systems:

Hardware	Operating System
HP Integrity system with Intel Itanium processor	HP-UX, version 11.23 SSP supports 64-bit JRE with this operating system.
HP 9000 (PA-RISC)	HP-UX, version 11.23 SSP supports 64-bit JRE with this operating system.
IBM System p5 and IBM Power Systems	AIX 5L, version 5.3. SSP supports 64-bit JRE with this operating system.
x64/x86 64-bit	Red Hat Enterprise Linux Advanced Server, version 5 SuSE SLES, version 10 SSP supports 64-bit JRE with these operating systems.
x64/x86 32-bit	Red Hat Enterprise Linux Advanced Server, version 5 SuSE SLES, version 10
Sun SPARC system	Solaris, version 10 SSP supports 64-bit JRE with this operating system.
	VMware ESX and VMware vSphere with any UNIX or Linux operating system supported by SSP. Consider VMware configuration, administration, and tuning issues. Your VMware administrator must address these. Sterling Commerce does not provide advice regarding VMware-specific issues.
x86 (Intel VT-x and AMD-V) 32-bit and 64-bit	Kernel-based Virtual Machine (KVM) with Red Hat Enterprise Linux Advanced Server, version 5.4. Consider KVM configuration, administration, and tuning issues. Your Red Hat administrator must address these. Sterling Commerce does not provide advice regarding KVM-specific issues

Perimeter Server Requirements in UNIX or Linux

You can install and run a remote perimeter server (PS), on a different computer from CM or the engine. The PS supports the UNIX or Linux platforms supported by SSP.

Hardware Accelerator Board

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

Hardware Security Module (HSM) Requirements

SSP supports the following Hardware Security Module (HSM) appliance to store certificates:

- Safenet ProtectServer Gold
- Safenet ProtectServer External
- Thales nShield PCI

- Thales netHSM

SSP Windows System Requirements

This section identifies system requirements for Windows platforms. A JRE is installed with SSP.

Configuration information is maintained on both CM and the engine. How much is required to store configuration files depends on the size of the files and how long you maintain files, as well as the level of logging. The following table identifies the space required if you turn on debugging.

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
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 Server 2008 R2 (64-bit). SSP supports 64-bit JRE with this operating system.
- VMware ESX and VMware vSphere with any Windows operating system supported by SSP. Consider VMware configuration, administration, and tuning issues. Your VMware administrator must address these. Sterling Commerce does not provide advice regarding VMware-specific issues.

Perimeter Server Requirements on Windows

You can run a remote perimeter server (PS) on a different computer from CM or the engine. The PS supports the following Windows platforms:

- Windows 2003 Server Enterprise Edition R2 (32-bit)
- Windows 2003 Server Standard Edition R2 (32-bit)
- Windows Server 2008 R2 (64-bit)

Client Connections Supported

SSP is compatible with FTP, HTTP, or SSH-SFTP clients that comply with the relevant RFCs. The following clients have been tested and approved for interoperability with SSP:

Client	Protocol
Connect:Direct for z/OS (formerly OS/390) version 4.5 or later	Connect:Direct (SSL, TLS)

Client	Protocol
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 1.1.08 or later	Connect:Direct (SSL, TLS)
Sterling Integrator version 4.1 or later	FTP (SSL, TLS) HTTP (SSL, TLS) SSH-SFTP Connect: Direct (SSL, TLS)
Sterling Secure Client	FTP (SSL, TLS) SSH-SFTP HTTP - WebDAV (SSL)
Connect:Express for z/OS (formerly OS/390) version 4.2.2 or later	PeSIT
Connect:Express for UNIX version 1.4.4 or later	PeSIT
Connect:Express for Windows version 3.0.5 or later	PeSIT
Internet Explorer 7 and 8	HTTP - myFileGateway
Firefox 3.5	HTTP - myFileGateway
Safari 3.2.3 and 4.0 on Windows and Mac OS X (10.5.7 and 10.6.0)	HTTP - myFileGateway
cURL 7.12.1 or later with openSSL 0.9.7a or later	FTP (SSL, TLS) HTTP
OpenSSH 4.3p2 or later	SSH
WS_FTP Professional 2007 or later	FTP (SSL, TLS) SSH-SFTP

Web Browsers Supported by CM

Sterling Secure Proxy supports the following web browsers when using CM:

- Firefox 3.0 or later running on Windows
- Microsoft Internet Explorer 7

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 4.3.21 or later
- Sterling Integrator version 5.0.03 or later
- Sterling File Gateway (SFG) version 1.1 with GIS version 4.3.22 or later (4.3.x)
- Sterling File Gateway (SFG) version 2.0 with Sterling Integrator version 5.0.03 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 2.3.00 or later

Cipher Suites Supported

SSP supports the following cipher suites for the Connect:Direct, FTP, and HTTP protocols:

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_RSA_EXPORT_WITH_RC4_40_MD5
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

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:

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.

Configuration Resource	SSP Usage
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.
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.
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 library.
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 Manage Certificates Between SSP Components at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.

Chapter 2

Install or Upgrade SSP on Windows

Install or Upgrade SSP on Windows

Before you install SSP, review the system requirements. 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.

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 your system meets the hardware and software requirements specified for this release.	*System Requirements* on page 7
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 15
If you install the engine on a computer with more than one NIC, specify the IP bind address of the NIC associated with that engine.	Change the IP Address for an Engine. Click Manage SSP Engines on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
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 16.
Obtain a temporary license key and copy it to the appropriate directory.	*Sterling Commerce License Key Guide*
Request and install a permanent license key.	*Sterling Commerce License Key Guide*
Start the engine and CM.	Start the Engine on Windows. Click Start or Stop an SSP Component on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.

Installation Task	Procedure to Complete
Log onto CM.	Start the CM on Windows. Click Start or Stop an SSP Component on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
Create an engine definition in CM.	*Create an Engine Definition* on page 16.
Verify the engine and CM connection.	View the Engine and CM on Windows. Click Start or Stop an SSP Component on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
Check in certificates for the connection between the engine and CM	Manage Certificates Between SSP Components. Click Manage Certificates Between SSP Components on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
Determine if your environment requires a remote perimeter server.	Configure Perimeter Servers to Manage SSP Communications. Click Configure a Remote Perimeter Server on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
If required, install a remote perimeter server.	*Install a Remote Perimeter Server* on page 25.

SSP Startup Worksheet for Windows

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

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

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

URL to Connect to CM

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

Install or Upgrade the Engine on Windows

Use this procedure to install or upgrade the engine.

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

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

To install or upgrade an engine on Windows:

1. Navigate to the directory where you downloaded the SSP installation file for Windows.
2. Double-click the SSP.V3301.Windows.zip file to extract the SSP engine, CM, and perimeter server installation files for Windows.
3. Take one of the following actions:
   - To install the engine on Windows Server 2003 (32-bit), double-click **SSP.V3301.Win.exe**.
   - To install the engine on Windows Server 2008 (64-bit), double-click **SSP.V3301.Win_X64.exe**.
4. After the introduction, click **Next**.
5. Scroll down in the license agreement and read the agreement. Click the radio button to accept the terms and click **Next**.
6. Accept the default directory, or click **Choose** to navigate to a different directory. For an upgrade, change to the directory where the previous version is installed. Click **Next**.
7. To continue a new installation:
   a. Accept the default value **63366** for the engine listen port or specify a different port. Record the engine listen port on the Startup Worksheet and click **Next.**
   b. Type a passphrase. Retype the passphrase and click **Next**.
8. To continue an upgrade, specify the directory where the previous version is installed and press **Next**. A prompt indicates the Sterling Secure Proxy installation already exists.
9. Review the pre-installation summary. Click **Install**.
10. At the Installation Complete screen, click **Done**.

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 ports are maintained as well as configuration, log files, and adapter definitions.

To install or upgrade CM on Windows:

1. Navigate to the directory where you extracted the CM installation files from the archive in the previous procedure.
2. Take one of the following actions:
   - To install the CM on Windows Server 2003 (32-bit), double-click **SSPcm.V3301.Win.exe**.
   - To install the CM on Windows Server 2008 (64-bit), double-click **SSPcm.V3301.Win_X64.exe**.
3. After the introduction, click **Next**.
4. At the end of the license agreement, click the radio button to accept the terms and click **Next**.
5. Accept the default directory, or click **Choose** to navigate to a different directory. For an upgrade, change to the directory where the previous version is installed. Click **Next**.
6. Perform the following steps to continue a new installation:
   a. Accept the default value **62366** for the CM listen port or specify a different port. Record the CM listen port on the Startup Worksheet. Click **Next.**
   b. Type a passphrase. Retype the passphrase and click **Next**.
   c. Accept the default value of **8443** for the web server listen port or specify a different port. Record the web server listen port on the Startup Worksheet. Click **Next**.
7. To continue an upgrade, specify the directory where the previous version is installed and press **Next**. A prompt displays the directory and a message indicating that the Sterling Secure Proxy installation already exists.
8. Review the pre-installation summary before continuing. Click **Install**.
9. At the Installation Complete screen, click **Done**.

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. Refer to the Sterling Secure Proxy License Key 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	
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 Manage SSP Engines on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.for instructions.

Chapter 3

Install or Upgrade SSP on UNIX or Linux

Install or Upgrade SSP on UNIX or Linux

Before you install SSP, review the system requirements. 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.

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 requirements specified for this release.	*System Requirements* on page 7.
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 21.
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. Click Manage SSP Engines on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
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.
Obtain a temporary license key and copy it to the appropriate directory.	*Obtain a License Key File for UNIX or Linux* on page 23
Start the engine.	Start the Engine on UNIX or Linux. Click Start or Stop an SSP Component on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
Run CM.	Run CM on UNIX or Linux. Click Manage Engines on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.

Installation Task	Procedure to Complete
Create an engine definition in CM.	*Create an Engine Definition* on page 23
Verify the engine and CM connection.	Manage SSP Engines. Click Manage SSP Engines on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
Check in certificates for the connection between the engine and CM.	Manage Certificates Between SSP Components. Click Manage Certificates Between SSP Components on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
Determine if your environment requires a remote perimeter server.	Configure Perimeter Servers to Manage SSP Communications. Click Configure a Remote Perimeter Server on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
If required, install a remote perimeter server.	*Install a Remote Perimeter Server* on page 25

SSP Startup Worksheet for UNIX or Linux

Use the following worksheet to record the host name or IP address of CM and the engine, listening ports, and the URL for the CM sign-in screen. You refer to this information to use the application and set up your environment.

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

CM	Value at Installation
Host name or IP address	
CM listen port	
Web server listen port	

URL to Connect to CM

Engine	Value at Installation
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. Navigate to the directory where you downloaded the SSP installation file.

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

Hardware	File
IBM System p5 and IBM Power System	SSP.V3301.AIX.bin
HP Integrity system with Intel Itanium processor	SSP.V3301.HP-IA.bin
HP 9000 (PA-RISC)	SSP.V3301.HP.bin
x64/x86 Linux (32-bit) x64/x86 Linux (64-bit)	SSP.V3301.Linux.bin SSP.V3301.Linux_X64.bin
Sun SPARC system	SSP.V3301.SolarisSPARC.bin

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

2. Type the following command to retrieve the SSP engine, CM, and perimeter server installation files from the archive:

```
tar xvf SSP installation file
```

3. Type the name of the engine installation file for your platform and press **Enter**.
4. Read the terms of the license agreement. At the end of the agreement, type **Y** at the prompt.
5. For a new installation, perform the following steps:
   a. When prompted for the installation location, press **Enter** to accept the default directory or specify a different directory.
   b. Accept the default value **63366** for the engine listen port or specify a different port. Record the engine listen port on the Startup Worksheet, and press **Enter**.
   c. Type a passphrase and press **Enter**. You need this passphrase in the future.
   d. Retype the passphrase and press **Enter**.

6. For an upgrade, perform the following steps:
   a. Specify the directory where the previous version is installed and press **Enter**. A prompt displays the directory and a message indicating that the Sterling Secure Proxy installation already exists.
   b. Type **C** to continue.
7. Review the pre-installation summary, and press **Enter**.
8. Press **Enter**. The command prompt is displayed.

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

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

Hardware	File
IBM System p5 and IBM Power System	SSPcm.V3301.AIX.bin
HP Integrity system with Intel Itanium processor	SSPcm.V3301.HP-IA.bin
HP 9000 (PA-RISC)	SSPcm.V3301.HP.bin
x86 Linux (32-bit) x64 Linux (64-bit)	SSPcm.V3301.Linux.bin SSPcm.v3301.Linux_X64.bin
Sun SPARC system	SSPcm.V3301.SolarisSPARC.bin

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

2. Type the name of the CM installation file for your platform and press **Enter**.
3. Read the terms of the license agreement. At the end of the agreement, type **Y** at the prompt.
4. For a new installation, perform the following steps:
   a. When prompted for the installation location, press **Enter** to accept the default directory or specify a different directory.
   b. Accept the default value **62366** for the CM listen port, or specify a different port. Record the CM listen port on the Startup Worksheet, and press **Enter**.
   c. Type a passphrase and press **Enter**. You need this passphrase in the future.

   d. Retype the passphrase and press **Enter**.
   e. Accept the default value of **8443** for the web server listen port or specify a different port. Record the web server listen port on the Startup Worksheet, and press **Enter**.

5. For an upgrade, perform the following steps:
   a. Specify the directory where the previous version is installed and press **Enter**. A prompt displays the directory and a message indicating that the Sterling Secure Proxy installation already exists.
   b. Type **C** to continue.
6. Review the pre-installation summary, and press **Enter.**
7. Press **Enter**. The command prompt is displayed.
8. If you previously configured a single sign on HTTP adapter, open property tag and you will find the url used for SSP3.2 was not removed. I was told it should be in SSO object.

Obtain a License Key File for UNIX or Linux

One license is required for each engine. You receive a temporary license key file 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 use your existing license. You are not required to complete these procedures. Refer to the Sterling Secure Proxy License Key Guide for instructions to obtain a temporary key and a permanent key.

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	
Engine Host	IP address of the engine	
Engine Listen Port	Port number of the engine	

To define an engine:

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

- Engine Listen Port

4. Click **Save**.

   Verify that the engine is running. Click Manage SSP Engines on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.

Chapter 4

Install a Remote Perimeter Server

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 Configure a Remote Perimeter Server on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.

Perimeter Server Installation Prerequisites

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

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

Perimeter Server Installation Guidelines

When you install a perimeter server, follow these guidelines:

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

  To use additional TCP/IP addresses, install additional perimeter servers.
- To install an additional perimeter server on a computer with an existing instance, install the new perimeter server in unique installation directory.
- To upgrade an existing perimeter server, install a new instance of perimeter server in the installation directory of the existing perimeter server.
- The combination of internal TCP/IP address and port must be unique for all perimeter servers installed on one computer.
  - If a perimeter server is installed using the wildcard address, then all ports must be unique.
  - If a perimeter server is installed using the wildcard address, then its port is not available for use by service adapters that use the server or any other perimeter server on that computer.
  - The internal and external interface may use the same TCP/IP address. However, the port used by the perimeter server is not available to the service adapters that use the server.

Install remote perimeter Server in a More Secure Network on UNIX or Linux

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

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

Platform	Installation File Name
IBM System p5 and IBM Power system	PS.V3301.AIX.bin
HP Integrity system with Intel Itanium processor	PS.V3301.HP-IA.bin
HP 9000 (PA-RISC)	PS.V3301.HP.bin
x64/x86 Linux (32-bit) x64/x86 Linux (64-bit)	PS.V3301.Linux.bin PS.V3301.Linux_X64.bin
Sun SPARC system	PS.V3301.SolarisSPARC.bin

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

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

   If you type quit, the installation program will terminate.

5. Read the License Agreement information. Press Enter to page through the license agreement. When you are prompted to accept the License Agreement, press Y or y. The Choose Installation Folder screen is displayed.
6. Press Enter to accept the default installation folder, or type the absolute path name of the directory where the perimeter server will be installed.
7. Confirm that the installation directory is correct by typing Y or y. The Network Zone screen is displayed.
8. Type 2 to install the perimeter server in a more secure network. The installation program displays a list of network interfaces available on the perimeter server host.
9. Select the network interface for the perimeter server to use to communicate with the SSP engine, or press Enter if a specific interface address is not required.
10. Type the port number of the local port the perimeter server will use to communicate with the SSP engine. Specify a port number greater than or equal to 1024. If a specific port is not required, press Enter.

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

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

Install a remote perimeter Server in a Less Secure Network on UNIX or Linux

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

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

Platform	Installation File Name
IBM System p5 and IBM Power System	PS.V3301.AIX.bin
HP Integrity system with Intel Itanium processor	PS.V3301.HP-IA.bin
HP 9000 (PA-RISC)	PS.V3301.HP.bin

Platform	Installation File Name
x64/x86 Linux (32-bit) x64/x86 Linux (64-bit)	PS.V3301.Linux.bin PS.V3301.Linux_X64.bin
Sun SPARC system	PS.V3301.SolarisSPARC.bin

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

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

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

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

Install remote perimeter Server in a More Secure Network in Windows

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

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

Platform	Installation File Name
Windows Server 2003 Enterprise Edition Service Pack 1 (32-bit)	PS.V3301.Win.exe
Windows Server 2008 R2 (64-bit)	PS.V3301.Win_X64.exe

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

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

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

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

When the perimeter server is installed, the installation program displays an Installation Complete message.

14. Click Done to exit the installation.
15. Change to the installation directory.
16. Do one of the following:
    - Run startPSService.cmd to start the perimeter server.
    - Configure the perimeter server service to start automatically as a Windows Service at system startup.

Install remote perimeter Server in a Less Secure Network in Windows

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

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

Platform	Installation File Name
Windows Server 2003 Enterprise Edition Service Pack 1 (32-bit)	PS.V3301.Win.exe
Windows Server 2008 R2 (64-bit)	PS.V3301.Win_X64.exe

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

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

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

The installation program displays a list of network interfaces available on the perimeter server host.

10. Select the network interface for the perimeter server to use to communicate with trading partners, or click Next if a specific interface address is not required.
11. Verify the Pre-Installation Summary information, and click Next.

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

Upgrade Perimeter Server in Windows, UNIX, or Linux

To upgrade an existing instance of perimeter server:

1. Run the perimeter server installation program.
2. Read and accept the License Agreement.
3. On the Installation Folder screen, select the installation directory of the existing perimeter server.

   The installation program detects the existing perimeter server installation and displays an update message.
4. Select the option to update the existing installation.

   The installation program will use the configuration information of the existing installation to configure the updated installation.
5. Verify the Pre-Installation Summary information and complete the installation.
6. 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:nnnn", "connect";
// For each target FTP Server
//
// permission java.net.SocketPermission "ftphost:nn", "connect";
// Control connection.
// permission java.net.SocketPermission"
ftphost:lowPort-highPort", "connect"; // Passive data connections.
// For each target HTTP Server//
//
permission java.net.SocketPermission "htttphost:nnn", "connect";
// For each target C:D snode
//
// permission java.net.SocketPermission "snode:nnnn", "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 remote_perimeter.properties file located in the perimeter server installation directory. Set the value of restricted to true as shown below:

```
restricted=true
```

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. Remove the comment markers from 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. Run uninstallPSService.cmd to uninstall the existing perimeter server Windows service.

   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.

Chapter 5

Upgrade SSP

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.

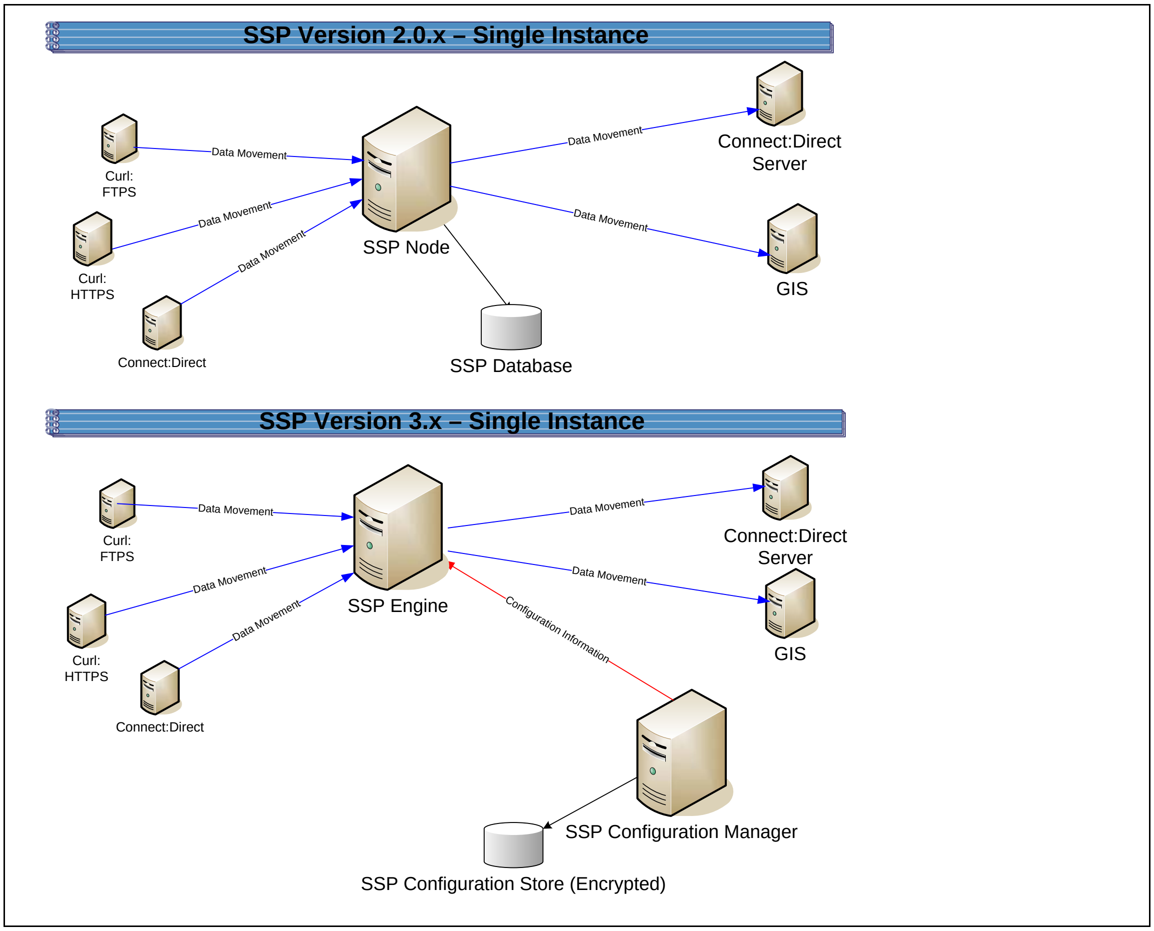
SSP version 3.x uses a different architecture from version 2.0.x. It allows you to configure your environment using the Configuration Manager (CM). It then moves the configuration information to an Engine, to use during production. SSP version 2.0.x does not use an Engine or CM. Configuration and production 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 36.
- 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 40.
- 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 45 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 49.
- 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 67.

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 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 38.

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:

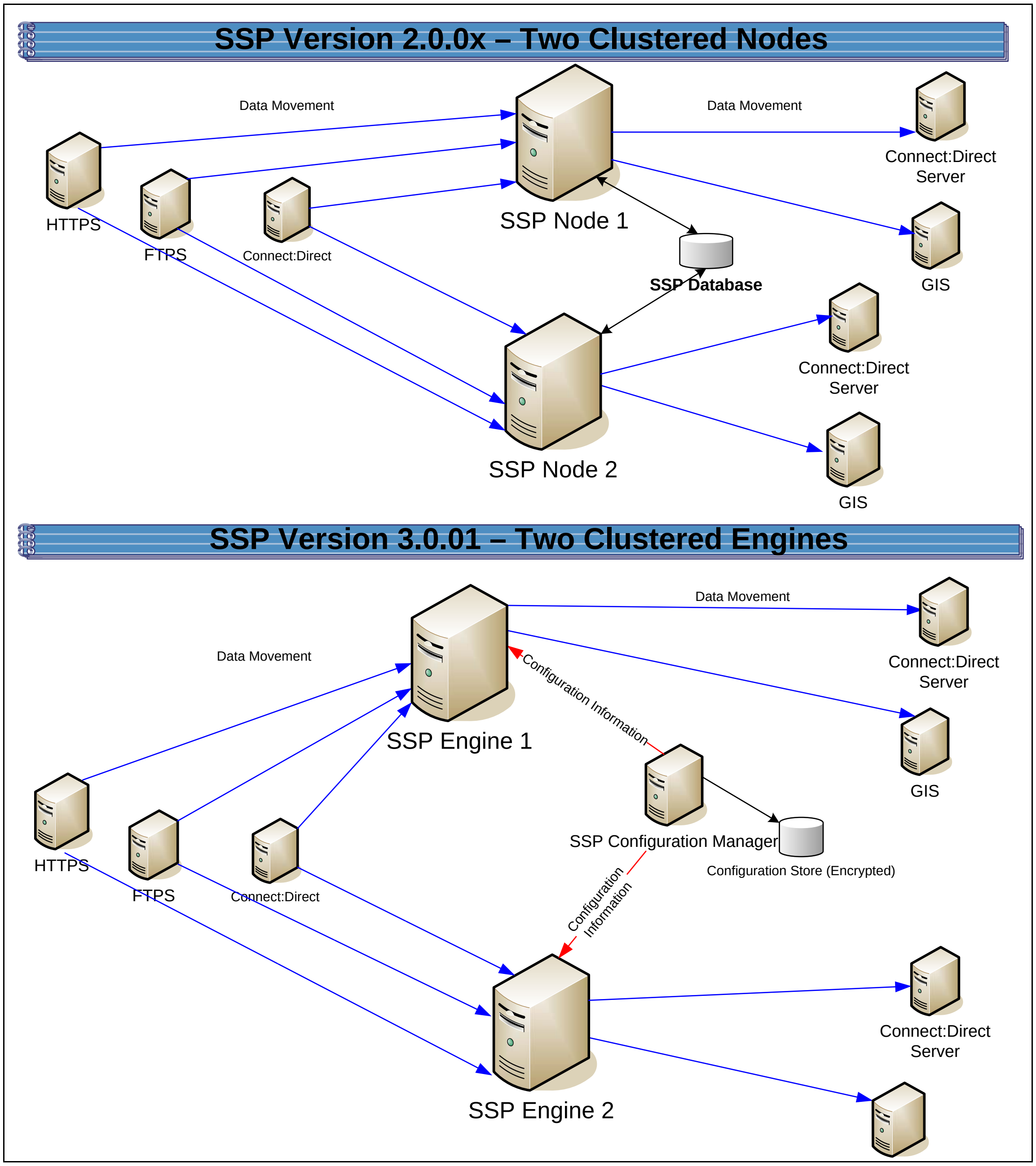
Installation Task	Procedure to Complete or Information Needed
Start SSP version 2.0.x.	*Start and Log On to SSP Version 2.0.x* on page 53.
Export the SSP 2.0.x resources.	*Export SSP Version 2.0.x Information* on page 53.
Write down the export file name and password.	
Install the SSP 3.x Engine. **Note:** 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 21. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 15.
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 16.
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 16.

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.	*Stop Perimeter Server Version 2.0* on page 54.
2 Install a version 3.x PS.	*Install a Remote Perimeter Server* on page 25
3 If SSP 2.0.x is installed on the same computer with the version 3.x engine, stop SSP 2.0.x.	*Stop SSP Version 2.0.x* on page 54.
Back up SSP version 3.x configuration files.	*Back Up Version 3.x Configuration Files* on page 55.
Run the upgrade script.	*Convert Files from SSP Version 2.0.x to Version 3.x* on page 55.
View the upgrade log to ensure that the conversion succeeded.	*Read the Upgrade Log File* on page 59.
Start and log on to CM.	For UNIX or Linux, refer to *Run CM on UNIX or Linux* on page 307. For Windows, refer to *Run CM on Windows* on page 309.Click Start or Stop an SSP Component on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
Open the engine definition and verify the configuration.	*Validate an Engine Definition* on page 61.
Open the adapter definitions and verify each adapter configuration.	*Validate an Adapter* on page 62.
If you use a PS, validate the PS definition.	*Validate a PS Definition for a PS in a More Secure Zone* on page 62 or *Validate a PS Definition for a PS in a Less Secure Zone* on page 62.
If you changed any HTTP adapter property values, check the properties and make any necessary changes.	*Maintain Changes to HTTP Properties* on page 63.
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 66.
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 65.
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 67.
Make sure that new FTP and HTTP adapter properties are correctly set.	*New FTP Adapter Properties in Version 3.x* on page 66 or *New Properties in Version 3.x HTTP Adapter* on page 65.

Installation Task	**Procedure to Complete or Information Needed**
Start the engine.	Refer to *Start and Stop Configuration Manager and the Engine* on page 305.Click Start or Stop an SSP Component on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
Verify that the engine can communicate with CM.	*Validate the Connection Between Engines and CM* on page 63.

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.x. 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.

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	Perimeter servers cannot be shared by engines. Install a new perimeter server and create a new perimeter server definition for the new engine.

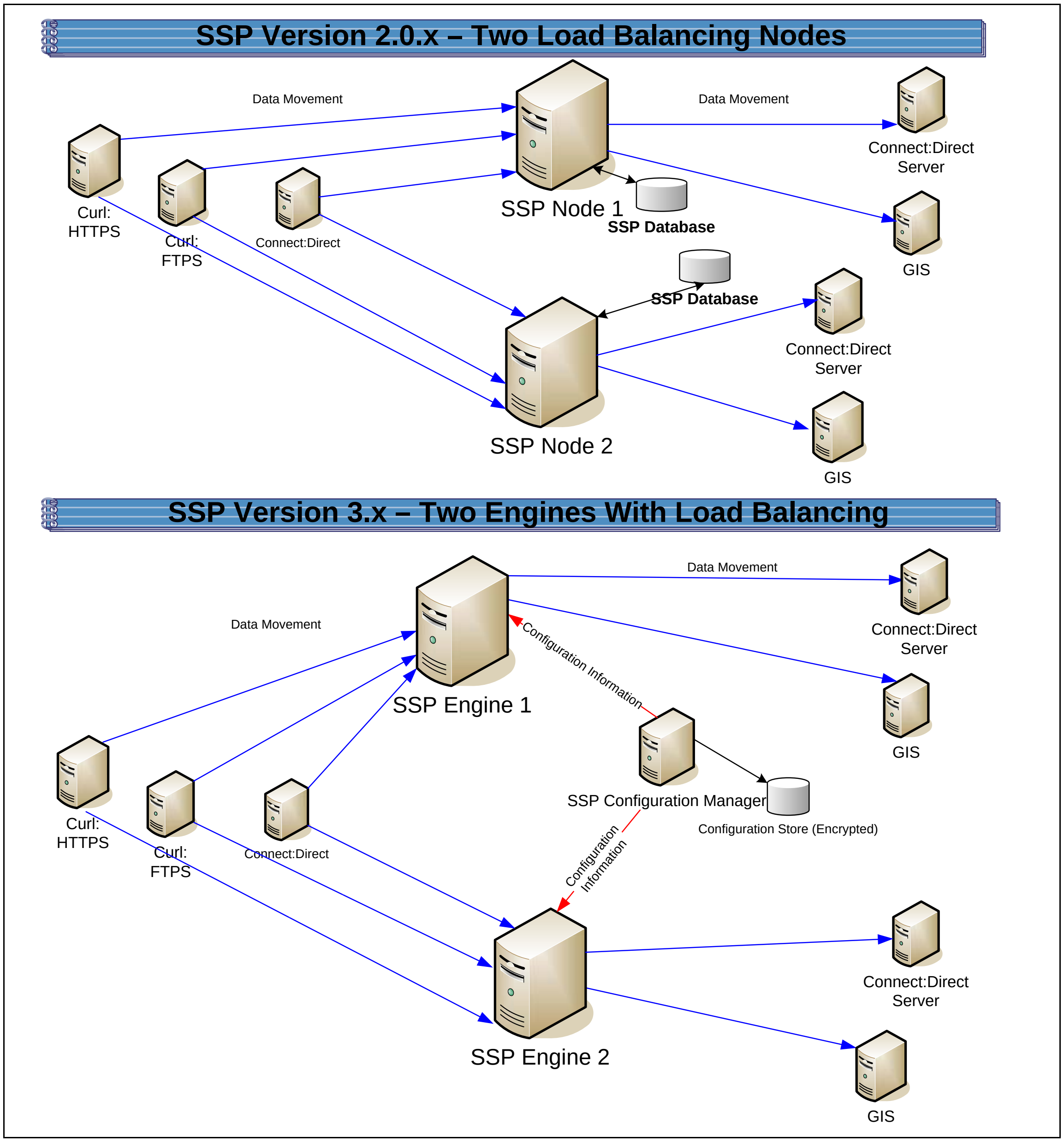
Cluster Nodes Upgrade Checklist

Complete the procedures in the *Upgrade Tasks* on page 38 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 21. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 15.
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 16.
Create an engine definition for each additional engine in the cluster.	*Create an Engine Definition* on page 23.
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 61.
Start all SSP cluster engines.	For UNIX or Linux, refer to *Create an Engine Definition* on page 23. For Windows, refer to *Create an Engine Definition* on page 16
Verify that each cluster engine can communicate with CM.	*Validate the Connection Between Engines and CM* on page 63.

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 to add 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.
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
CA Certificates	dfltTrustStore	The same trust store is used by engine 1 and engine 2.
PerimeterServer2	PerimeterServer2-engine2	

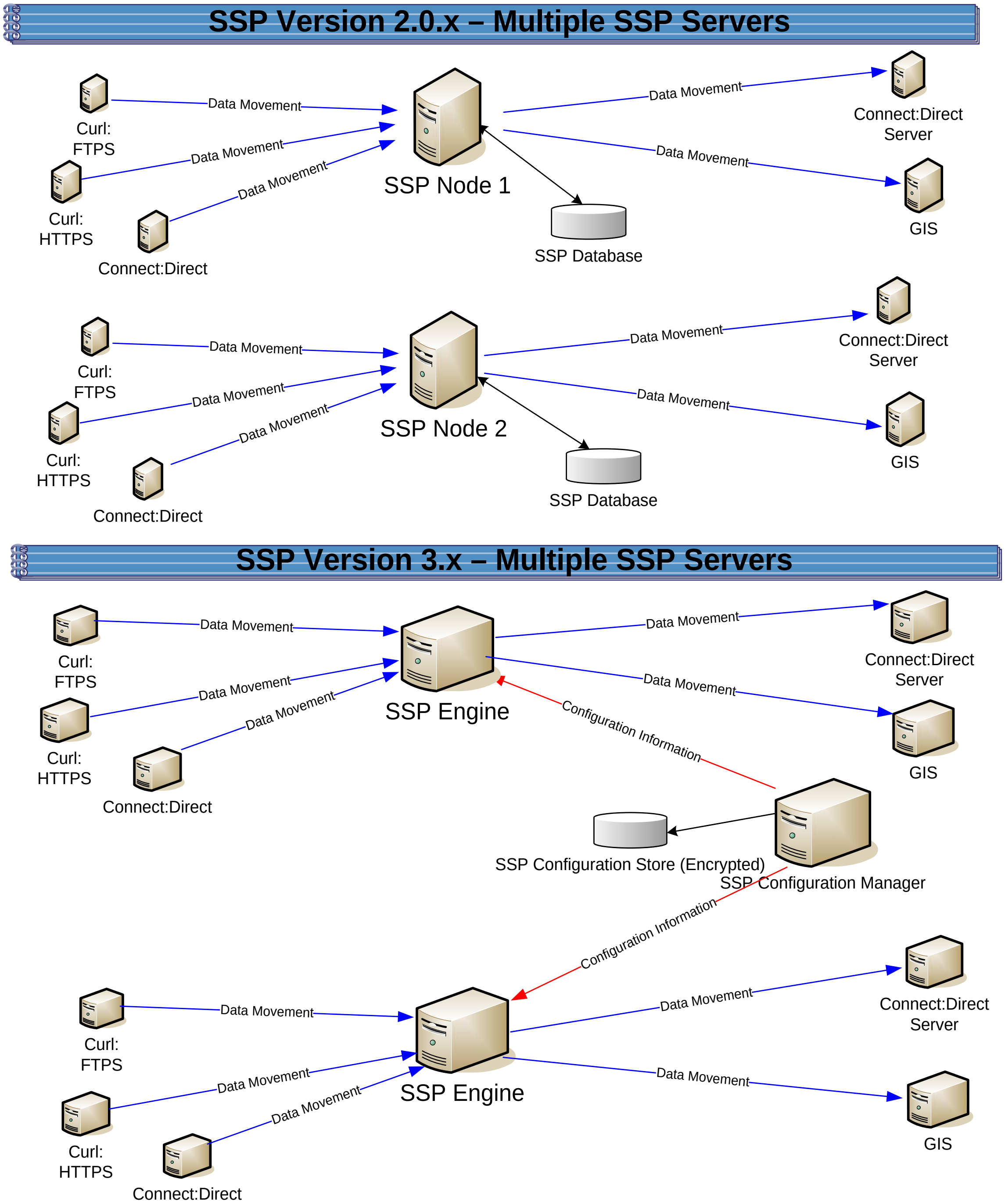
Load Balancing Nodes Upgrade Checklist

Complete the procedures in the *Upgrade Tasks* on page 38 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 21. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 15.
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 16.
Export SSP version 2.0.x resources from each additional SSP node.	*Export SSP Version 2.0.x Information* on page 53.
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 55.
View the upgrade log to ensure that the conversion for the node succeeded.	*Read the Upgrade Log File* on page 59.
From CM, verify each load balancing engine definition.	*Validate an Engine Definition* on page 61.
Open the adapter definitions for each load balancing engine. Make sure that each adapter is correctly defined.	*Validate an Adapter* on page 62.
Start all SSP load balancing engines.	For UNIX or Linux, refer to *Create an Engine Definition* on page 23. For Windows, refer to *Create an Engine Definition* on page 16.
Verify that the load balancing engine can communicate with CM.	*Validate the Connection Between Engines and CM* on page 63.

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	
Users	defUserStore	The same user store is used by engine 1 and engine 2

Version 2.0.x Object	Converts to Version 3.x Object	Notes
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 38 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, *Install or Upgrade the Engine on UNIX or Linux* on page 21. For Windows, *Install or Upgrade the Engine on Windows* on page 15.
Obtain and install a license key file for each additional engine.	*Sterling Commerce License Key Guide*.
Run the upgrade script at each additional engine.	*Convert Files from SSP Version 2.0.x to Version 3.x* on page 55.
View the upgrade log to ensure that the conversion succeeded.	*Read the Upgrade Log File* on page 59.
Start and log on to CM.	For UNIX or Linux, refer to *Run CM on UNIX or Linux* on page 307. For Windows, refer to *Run CM on Windows* on page 309.Click Start or Stop an SSP Component on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
From CM, open the engine definition and verify the configuration.	*Validate the Converted Components in SSP Version 3.x* on page 61.
Open the adapter definitions. Make sure that each adapter is correctly defined.	*Validate an Adapter* on page 62.
Start the SSP engine.	*Create an Engine Definition* on page 23.
Verify that the engines can communicate with CM.	*Validate the Connection Between Engines and CM* on page 63.

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 53.
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 58 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 58 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. ◆ 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.	Y
-enginehost *hostvalue*	The engine host name.The default is defaultEngineHost.	
-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.	

Argument	Description	Required
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 2010 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 2010 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

Field	Description	Sample Message Text
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 61.
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.
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 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 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.

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	

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

To validate an engine definition:

1. 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 3.x. Before you use 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 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.x, 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 53.
3. Stop SSP.

To convert HSM key certificates from an SSP 3.x installation:

1. Install the SSP 3.x 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 21. For Windows, refer to *Install or Upgrade the Engine on Windows* on page 15.
2. Type the following command to enable HSM support:

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

   Refer to *Store System Certificates on a Hardware Security Module (HSM)* on page 283 for more information on the command parameters.

   Refer to Store System Certificates on a Hardware Security Module (HSM) on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm.
3. Start the engine. For UNIX or Linux, refer to *Create an Engine Definition* on page 23. For Windows, refer to *Create an Engine Definition* on page 16
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 16.
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 61.
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 68 in the file parameter.

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

   The *file* is the name of the file created in step 1 on page 67.

   Refer to *Store System Certificates on a Hardware Security Module (HSM)*Store System Certificates on a Hardware Security Module (HSM) on the Documentation Library at www.sterlingcommerce.com/Documentation/SSP33/HomePage.htm 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 68.