

Sterling Secure Proxy®

Operations Guide

Version 3.2

Sterling Secure Proxy Operations Guide

Version 3.2 First Edition

(c) Copyright 2006-2009. Sterling Commerce, Inc. All rights reserved. Additional copyright information is located in the release notes.

STERLING COMMERCE SOFTWARE

*****TRADE SECRET NOTICE*****

THE STERLING :SECURE PROXY SOFTWARE (“STERLING COMMERCE SOFTWARE”) IS THE CONFIDENTIAL AND TRADE SECRET PROPERTY OF STERLING COMMERCE, INC., ITS AFFILIATED COMPANIES OR ITS OR THEIR LICENSORS, AND IS PROVIDED UNDER THE TERMS OF A LICENSE AGREEMENT. NO DUPLICATION OR DISCLOSURE WITHOUT PRIOR WRITTEN PERMISSION. RESTRICTED RIGHTS.

This documentation, the Sterling Commerce Software it describes, and the information and know-how they contain constitute the proprietary, confidential and valuable trade secret information of Sterling Commerce, Inc., its affiliated companies or its or their licensors, and may not be used for any unauthorized purpose, or disclosed to others without the prior written permission of the applicable Sterling Commerce entity. This documentation and the Sterling Commerce Software that it describes have been provided pursuant to a license agreement that contains prohibitions against and/or restrictions on their copying, modification and use. Duplication, in whole or in part, if and when permitted, shall bear this notice and the Sterling Commerce, Inc. copyright notice. As and when provided to any governmental entity, government contractor or subcontractor subject to the FARs, this documentation is provided with RESTRICTED RIGHTS under Title 48 52.227-19. Further, as and when provided to any governmental entity, government contractor or subcontractor subject to DFARs, this documentation and the Sterling Commerce Software it describes are provided pursuant to the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation.

These terms of use shall be governed by the laws of the State of Ohio, USA, without regard to its conflict of laws provisions. If you are accessing the Sterling Commerce Software under an executed agreement, then nothing in these terms and conditions supersedes or modifies the executed agreement.

Where any of the Sterling Commerce Software or Third Party Software is used, duplicated or disclosed by or to the United States government or a government contractor or subcontractor, it is provided with RESTRICTED RIGHTS as defined in Title 48 CFR 52.227-19 and is subject to the following: Title 48 CFR 2.101, 52.227-19, 227.7201 through 227.7202-4, FAR 52.227-14, and FAR 52.227-19(c)(1-2) and (6/87), and where applicable, the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation including DFAR 252.227-7013, DFAR 252,227-7014, DFAR 252.227-7015 and DFAR 252.227-7018, all as applicable.

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

Connect:Direct is a registered trademark of Sterling Commerce. Connect:Enterprise is a registered trademark of Sterling Commerce, U.S. Patent Number 5,734,820. Sterling Secure Proxy is a trademark of Sterling Commerce. Gentran Integration Suite is a registered trademark of Sterling Commerce. All Third Party Software names are trademarks or registered trademarks of their respective companies. All other brand or product names are trademarks or registered trademarks of their respective companies.

Sterling Commerce, Inc.

4600 Lakehurst Court Dublin, OH 43016-2000 *
614/793-7000

Contents

Chapter 1 SSP Overview	5
Configuration Overview	6
SSP Terminology.	7
Chapter 2 Manage Configuration Manager (CM)	9
Run CM on UNIX or Linux	9
Start CM on UNIX or Linux	9
Log On to CM on UNIX or Linux	9
Stop CM on UNIX or Linux	10
Run CM on Windows	10
Start CM as a Windows Service	11
Log on to CM on Windows	11
Change the Password for a CM User	11
Change the Listen Port on CM	12
Modify the Timeout Value for a CM Session	12
Modify the Listener Settings for CM	13
Modify Security Settings for CM	13
Modify the Logging Level for Sessions Between CM and the Web Server	14
Modify the Connection Settings for Sessions Between CM and the Web Server	14
Unlock a CM Component	15
Chapter 3 Manage an Engine	17
View Configured Engines	17
Stop an Engine	17
Stop an Engine from CM.	18
Stop an Engine Using a Script File from UNIX or Linux	18
Stop an Engine from Windows	18
Start an Engine on UNIX or Linux	18
Start an Engine on Windows	19
Configure the Refresh Interval Between CM and Engines	19
Update the Monitor Display of Engine Information	19
Manually Send a Configuration File to an Engine	20
Change the Listen Port for an Engine	20
Change the IP Address for an Engine	21

Chapter 4 Manage Adapters **23**

Monitor Configured Adapters	23
Stop an Adapter from CM	23
Start an Adapter from CM	24

Chapter 5 About Log Files **25**

Audit Log	25
Audit Log Parameters	26
Enable SysLog Support in the Audit Log	26
CM Audit Log Events	27
Engine Audit Log Events	27
Secure Proxy Log	27
Secure Proxy Log Parameters	27
Secure Proxy File Output	28
Node Logs	29
Certicom Logs	29
Perimeter Server Logs	30
SFTP Logs	31
Maverick Log	31
SFTP Adapter Log	31

Chapter 6 Start and Stop a Remote Perimeter Server **33**

Start and Stop a Remote Perimeter Server on UNIX or Linux	33
Start and Stop a Remote Perimeter Server on Windows	33

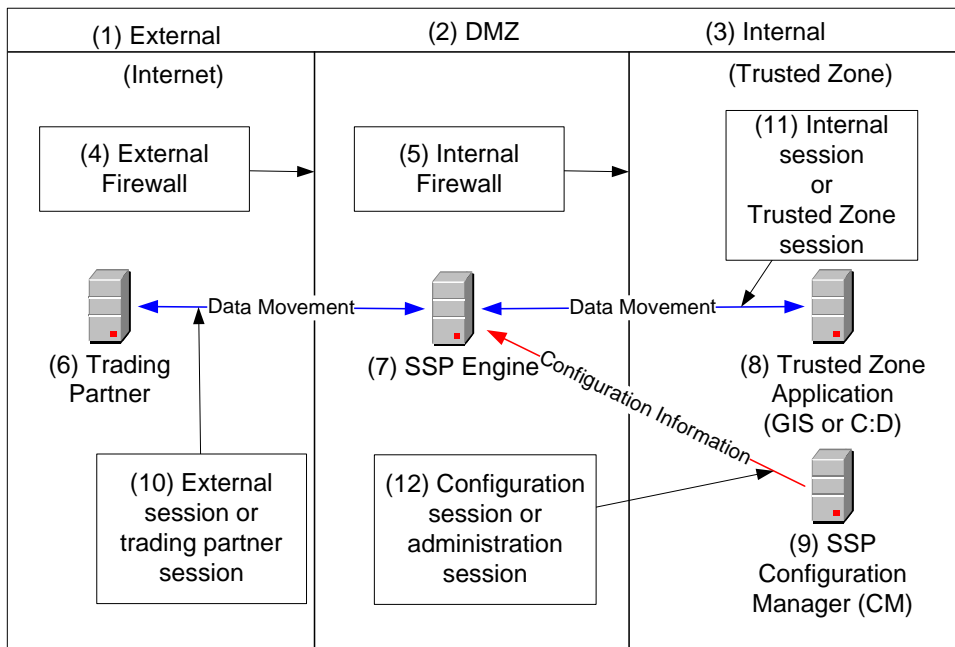
Chapter 7 Optional Tasks **35**

Obtain and Install a License Key File	35
Modify the Heap Size	36
Modify the Engine Heap Size on UNIX or Linux	36
Modify the CM Heap Size on UNIX or Linux	36
Modify the Engine Heap Size on Windows	36
Modify the CM Heap Size on Windows	36

SSP Overview

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

Following is an illustration of the SSP general proxy environment.



Configuration Overview

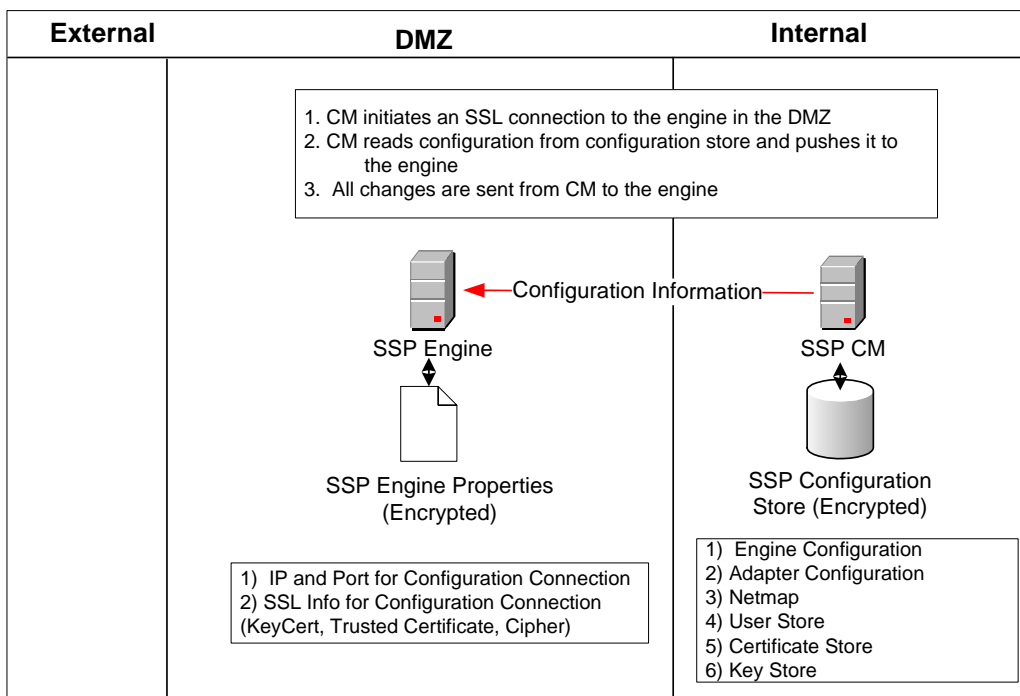
The SSP architecture requires that only the minimum amount of configuration information be stored in the DMZ. It includes two components: the Configuration Manager (CM) and an engine. Configuration data is stored at the CM, is encrypted, and does not require a database. The CM is installed on the internal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

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

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

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

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



SSP Terminology

SSP architecture is described below:

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

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

Note: Only one CM should update an engine definition.

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

- ◆ The user store with information on user credentials
- ◆ The system certificate store with the certificates used for SSL/TLS sessions
- ◆ The key store with the SSH keys
- ◆ The engine configuration store with all configuration information for the engine

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

- ◆ The IP and port number to listen on for connections from CM
- ◆ SSL key certificate, trusted certificate, and encryption cipher used for the connection from CM

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

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

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

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

Sterling External Authentication Server (EA)—A separately installed feature of SSP, EA allows you to validate digital certificates passed by the client or trading partner during SSL/TLS session requests. You can also validate certificates against one or more certificate revocation lists (CRLs), and validate certificates based on the valid date range. See the Sterling External Authentication Server documentation for more information.

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

- ◆ Certificate Validation
- ◆ Certificate Revocation List (CRL)
- ◆ Multi-factor Authentication
- ◆ Certificate Policy Enforcement
- ◆ LDAP Authentication
- ◆ User ID mapping—Remote trading partners can be given IDs and passwords that do not provide access to internal systems; the ID and password presented by the trading partner is mapped to an ID and password that can then access the internal system
- ◆ TAM (Tivoli Access Manager) Authentication
- ◆ Generic Authentication

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

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

Manage Configuration Manager (CM)

After you set up CM, use the procedures in this chapter to start and stop it, change the listen port defined at installation, modify the timeout value for a CM session, change the CM settings used to listen for secure connections, change the security information used during a secure connection from the web server to CM, modify the logging level for sessions between CM and the web server, modify session settings between CM and web server, or unlock a CM component.

Run CM on UNIX or Linux

You run CM by starting it and logging on.

Start CM on UNIX or Linux

To start CM on UNIX or Linux:

1. Navigate to the *install_dir/bin* directory, where *install_dir* is the CM installation directory.
2. Type the following command:

```
./startCM.sh
```

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

Note: You can change the startup method to run the engine in background mode and avoid the need to provide a passphrase. Refer to the *Sterling Secure Proxy Installation Guide* for instructions.

Log On to CM on UNIX or Linux

You log on and access the CM through a web browser.

To log on to CM from Windows:

1. Open Internet Explorer.
2. Type the logon address in one of the following formats:

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

or

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

Provide the following the information for your configuration:

Component	Description
hostname or ipaddress	Either the name or IP address of the computer where CM is installed.
port	The port defined for the web server at installation. The default value is 8443.

3. On the logon screen, type the user ID and password.
4. Click **Logon**.

Stop CM on UNIX or Linux

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

To stop CM on UNIX or Linux:

1. Log out of CM.
2. Navigate to the *install_dir/bin* directory, where *install_dir* is the directory where CM is installed.
3. Type the following command:

```
./stopCM.sh
```

4. Type the passphrase for CM.
5. Type the administrator user name and password.

Run CM on Windows

To run CM, first start the application and then log on.

Start CM as a Windows Service

CM is installed as a Windows service. Start CM from Windows Services.

Note: You can change CM to start up from a command line. You can also modify the startup to require that a passphrase be provided. Refer to the *Sterling Secure Proxy Installation Guide* for instructions.

Log on to CM on Windows

After starting CM, log on to the SSP dashboard and access CM through a web browser.

To log on to CM on Windows:

1. Open Internet Explorer.
2. Type the logon address in one of the following formats:

`https://hostname:port/SSPDashboard`

or

`https://ipaddress:port/SSPDashboard`

Type the following information for your configuration:

Component	Description
hostname or ipaddress	Either the name or IP address of the CM host system.
port	The port defined for CM at installation. The default value is 8443.

3. On the logon screen, type the user ID and password.
4. Click **Logon**.

Change the Password for a CM User

You configured users who can access the CM and defined a password for each user. If these user want change their CM password, provide them with the following procedure.

1. Open Internet Explorer.
2. Type the logon address as follows: `https://hostname:port/SSPDashboard` or `https://ipaddress:port/SSPDashboard`
3. On the logon screen, type the user ID and password.

4. Click **New Password**.
5. Type the new password in the New password and Confirm password fields.
6. Click **Confirm**.

Stop CM on Windows

If you close the web browser, CM continues to run. If you configure CM as a Windows service, the program is stopped when you shut down your computer, or you stop it through Windows Services.

Change the Listen Port on CM

Use this procedure to change the listen port. Stop CM before you change any information.

To change the listen port on UNIX, Linux, or Windows:

1. From a command line prompt, navigate to the *install_dir*\bin directory, where *install_dir* is the directory where CM is installed.
2. Type the following command:

```
configureaccepter port = nnnn
```

where *nnnn* is the port to listen on.

If the command is successful, a response similar to the following is displayed:

```
Acceptor configuration updated:  
name      = Secure  
secure    = true  
port      = nnnn  
address   = (default)  
timeout   = 30000  
enabled   = true
```

All changes to the listen accepters take effect the next time CM is started.

Modify the Timeout Value for a CM Session

By default, a CM session times out after 30 minutes. You can change the timeout value.

To change the CM session timeout value on UNIX, Linux, or Windows:

1. Open the web.xml file in the `install_dir\app\jetty\webservices\webapps\SSPDashboard\WEB-INF` directory.
2. Change the following parameter to identify the number of minutes to wait before a session is timed out.

```
<session-timeout>30</session-timeout>
```

3. Save the file.

Modify the Listener Settings for CM

When you install SSP, you define the IP address and port that CM uses to listen for secure connections from the engine.

To change the IP address and port used for secure connections:

1. Select System from the menu bar.
2. Click Actions > System Settings.
3. Change the values in the IPAddress and Secure Listener Port fields.
4. Click Save.

Modify Security Settings for CM

Use this procedure to modify the security information used during a secure connection from CM to the web server. You must export the certificate information and add it to the engine setup.

Note: This procedure does not include all steps necessary to configure security settings for CM. Refer to Chapter 15, *Manage Certificates Between SSP Components* in the Configuration Guide for instructions on how to configure security settings.

To modify security settings for CM:

1. Select System from the menu bar.
2. Click Actions > System Settings.
3. Click the Security tab.
4. Change the values in the Key/System Certificate and Cipher Suites fields.
5. Click Save.

Modify the Logging Level for Sessions Between CM and the Web Server

Use this procedure to modify the logging level for sessions between CM and the web server. To modify the logging level:

1. Select System from the menu bar.
2. Click Actions > System Settings.
3. Click the Globals tab.
4. Modify the logging level. Logging levels include:
 - ◆ NONE turns logging off.
 - ◆ ERROR writes only error messages to the log.
 - ◆ WARN writes error and warning messages to the log.
 - ◆ INFO writes error and informational messages to the log. INFO is the default value.
 - ◆ DEBUG writes all messages to the log including debugging messages. Use this logging level when instructed to turn it on by Sterling Support.
5. Click Save.

Modify the Connection Settings for Sessions Between CM and the Web Server

Use this procedure to modify the connection settings for sessions between CM and the web server. To modify connection settings:

1. Select System from the menu bar.
2. Click Actions > System Settings.
3. Click the Globals tab.
4. Modify one or more of the following values:
 - ◆ Listen backlog
 - ◆ Accept timeout
 - ◆ SSL handshake timeout
 - ◆ Connect timeout
 - ◆ Read timeout
5. Click Save.

Unlock a CM Component

Use the Lock Manager to unlock CM components. A component may become locked if it is already being edited by another user or if the browser is closed without logging out of CM.

To unlock a CM component:

1. Select System from the menu bar.
2. Click Lock Manager.
3. In the show field, select the component to unlock.
4. To limit the list, select the protocol used in the component.
5. Click Unlock Selected.

Manage an Engine



You can perform one or more of the following activities on an engine: view configured engines to determine if an engine is running, stop or start an engine, change how often CM polls an engine to determine its status, immediately poll an engine for status information, manually push a configuration file to an engine, and change the listen port defined at installation on an engine.

View Configured Engines

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

To view configured engines:

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

- ◆  Engine is running
- ◆  Engine is not running

The following information is displayed for each engine:


- ◆ Engine Name
- ◆ Last Pushed
- ◆ Message
- ◆ CM Ver
- ◆ Eng. Ver

Stop an Engine

You can stop the engine from CM or using a script from the command line.

Stop an Engine from CM

To stop the engine from CM:

1. Click Monitoring from the menu bar.
2. Click Engine Status (All). A list of all configured engines is displayed. Engines that are running are indicated with the .
3. Select the engine that you want to stop.
4. Click Stop Engine.
5. Type the engine passphrase and click OK.

Stop an Engine Using a Script File from UNIX or Linux

To stop the engine from UNIX or Linux:

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

```
./stopEngine.sh
```

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

Stop an Engine from Windows

To stop the engine, go to Windows services and stop the SSP Engine V3.2.00 application.

Start an Engine on UNIX or Linux

To start the engine on UNIX or Linux:

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

```
./startEngine.sh
```

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

Note: You can change the startup method to run the engine in background mode and avoid the need to provide a passphrase. Refer to the *Sterling Secure Proxy Installation Guide* for instructions.

Start an Engine on Windows

When you install the Sterling Secure Proxy engine, it is installed as a Windows service. By default, you must start the application by starting the SSP Engine service. Start the service from the Services application in Windows.

The engine is installed as a Windows service and is configured to be started manually. If you want the application to start automatically whenever you run Windows, go to the Windows services and change the Sterling Secure Proxy Engine V3.2.00 application startup method.

Note: You can change the startup method to run the engine from a command line. You can also modify the startup to require that a passphrase be provided. Refer to the *Sterling Secure Proxy Installation Guide* for instructions on modifying the startup method.

Configure the Refresh Interval Between CM and Engines

The Engine Status Page provides information on engines, including when configuration files were pushed to the engine, the version of the configuration files at CM and at the engine. CM polls engines every 30 seconds and updates the information displayed in the Monitoring display. Use this procedure to change how often engines are polled.

To change how often CM polls its engines for status information:

1. Click Monitoring from the menu bar.
2. Click Engine Status (All). A list of all configured engines is displayed.
3. Type the value in seconds to identify how often to poll engines in the Refresh Interval (secs) field.
4. Click Save.

Note: The new polling interval is not implemented immediately. The previous polling interval must expire before the new value is implemented. For example, if the polling interval is set to 50 seconds and you change the value to 15 seconds, the new value of 15 seconds is implemented after 50 seconds.

Update the Monitor Display of Engine Information

The Engine Status Page provides information on engines, including when configuration files were pushed to the engine, the version of the configuration files at CM and at the engine. The CM polls engines every 30 seconds and updates the information displayed in the Monitoring display. Use this procedure to immediately poll all engines and update the information displayed.

To poll all engines and obtain configuration information:

1. Click Monitoring from the menu bar.
2. Click Engine Status (All). A list of all configured engines is displayed.
3. Click Refresh.

Manually Send a Configuration File to an Engine

Adapters are configured at CM. The configuration is then sent to the engine the next time CM polls it. The version of the configuration file saved at the engine and the version at CM is displayed. The version should be the same at the engine and CM. If not, you can either wait for CM to poll the engine or you can manually push the configuration file to the engine. The engine must be running in order to push a configuration file.

Note: Only one CM can be used to configure an engine. If you attempt to send configuration files to an engine from more than one CM, you generate configuration errors.

To manually send the configuration file to an engine:

1. Click Monitoring from the menu bar.
2. Click Engine Status (All). A list of all configured engines is displayed.
3. Select the engine where you want to push a configuration.
4. Click Push Config.

Change the Listen Port for an Engine

Use this procedure to change the listen port defined for an engine at installation on Windows, UNIX, or Linux. Be sure to stop the engine before you change the listen port. Refer to *Stop an Engine* on page 17 for instructions.

To change the listen port on an engine:

1. From a command line prompt, go to the bin folder in the *install_dir* directory where *install_dir* is the directory where the engine is installed.
2. Type the following command:

```
configureAcceptor port=nnnn
```

3. Type the system passphrase.

If the command is successful, a response similar to the following is displayed:

```

Accepter configuration updated:
name      = Secure
secure    = true
port      = nnnn
address   = (default)
timeout   = 30000
enabled   = true

```

All changes to the listen acceptor ports take effect the next time the engine is started.

Change the IP Address for an Engine

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

Note: After you change the IP address for an engine, create an engine definition that uses the same IP address. Refer to *Create an Engine Definition* in the *Sterling Secure Proxy Installation Guide*.

To specify the IP bind address of the NIC card:

1. From a command line prompt, go to the `\install_dir\bin` directory where `install_dir` is the engine installation directory.
2. Type the following command:

```
configureAcceptor address=IPaddress
```

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

If the command is successful, a response similar to the following is displayed:

```

Accepter configuration updated:
name      = Secure
secure    = true
port      = nnnn
address   = (default)
timeout   = 30000
enabled   = true

```

Manage Adapters

After you configure adapters and are in a production environment, use the procedures in this chapter to monitor adapter activity and stop or start an adapter.

Monitor Configured Adapters

Use the monitoring function in CM to view and monitor adapters configured for an engine.

To view and monitor adapters:

1. Click Monitoring from the menu bar.
2. Expand the Engine Status (All) tree.
3. Click the engine where the adapters you want to monitor is running.

The following information about each adapter is displayed:

- ◆ Adapter Name
- ◆ Type
- ◆ Port
- ◆ Message

Stop an Adapter from CM

To stop an adapter from CM:

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

Start an Adapter from CM

To start an adapter:

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

About Log Files

SSP provides multiple log files including an audit log, secure proxy log, node logs, perimeter server log, SFTP log, and Certicom log.

Audit Log

The audit log contains messages about system operations and events. You view the log for information about suspected misuse, and identify the user, application, or remote trading partner responsible for the misuse. The audit log provides proof that SSP functions and events occurred. It identifies the occurrence of malicious attack attempts. It can provide proof to resolve disputes with customers or legal entities, and prevent the payment of penalties for legal or service level agreement violations.

An audit log is created for both the CM and the engine in the *install_dir/logs/audit* directory and is named *auditlog.xml*. An audit log record can also be sent to a syslog daemon to be routed elsewhere for other processing.

Audit log records are formatted in XML and are written to a file with an *.inc* suffix. Another file with suffix *.xml* contains an XML prolog and epilog information. The two files together make up one version of the audit log.

When an audit log file reaches a predefined size, it is archived and saved as *auditlog1.xml*. If archive files have already been created, each archive file is renamed. For example, when a new archive file is created, a log called *auditlog3.xml* is renamed to *auditlog4.xml* and *auditlog2.xml* is renamed to *auditlog3.xml*. You configure the maximum number of archive files to maintain.

Audit log settings are configured in the *log.properties* file located in the *install_dir/bin* directory.

Audit Log Parameters

You can modify the following parameters for an audit log in the `log.properties` file:

Parameter	Description
<code>audit.log.filename</code>	The location and file name to assign to an audit log. The default value is <code>../logs/audit/auditlog.xml</code> .
<code>audit.log.maxfilesize</code>	The number of files allowed in an audit log. When the <code>maxfilesize</code> is reached, the audit log is closed and a new log is opened. The default audit log file size is 500KB.
<code>audit.log.maxbackupindex</code>	The number of archive files to maintain. If the number of archive files identified in this parameter is exceeded, the oldest archive file is deleted. The default value is 100.
<code>audit.log.file.routing</code>	Determines if the audit log is written to a file. <code>y</code> = write the log to a file. <code>y</code> is the default setting. <code>n</code> = do not create an audit log file. Note: If you configure the audit log to write to the <code>syslog</code> daemon, this parameter can be set to <code>n</code> . Otherwise, an audit log is written to a file, regardless of the value of this parameter.
<code>audit.log.syslog.routing</code>	Determines if the audit log is written to <code>syslog</code> . <code>y</code> = write the log to <code>syslog</code> . <code>n</code> = do not write the audit log to <code>syslog</code> . <code>n</code> is the default setting. You must configure a valid <code>syslogd.port</code> and <code>syslogd.host</code> in order to write to <code>syslog</code> .
<code>audit.log.syslog.facility</code>	The facility number to associate with audit log messages. The default value is 18.

Enable SysLog Support in the Audit Log

To route audit log content to a `syslog` in a UNIX or Linux environment, configure the following parameters in the `log.properties` file:

Parameter	Description
<code>syslogd.enable</code>	Enables <code>syslog</code> daemon support. <code>y</code> = enabled. <code>n</code> = disabled. <code>n</code> is the default setting.
<code>syslogd.host</code>	Name or IP address of the <code>syslog</code> host. The default value is the local host.
<code>syslogd.port</code>	UDP port where the <code>syslog</code> host receives log messages. The default is 514.

CM Audit Log Events

Following are the configuration events that are written to the CM audit log:

- ◆ A list of all fields when you create a new configuration object.
- ◆ Modify fields when you update a configuration object.
- ◆ A list of all fields when you delete an object.
- ◆ All fields of a configuration pushed to an engine.

Engine Audit Log Events

Following are the configuration events that are written to the engine audit log:

- ◆ All fields of an initial engine configuration received from CM.
- ◆ Changed fields from an engine configuration update from CM.
- ◆ Inbound connections received for all protocols.
- ◆ Inbound handshakes completed for the FTP, HTTP, and Connect:Direct protocols.
- ◆ Inbound login successes and failures for the FTP, HTTP, and SFTP protocols.
- ◆ Outbound connections established for all protocols.
- ◆ Outbound handshakes completed for the FTP, HTTP, and Connect:Direct protocols.
- ◆ Outbound login successes and failures for the FTP, HTTP, and SFTP protocols.

Secure Proxy Log

Use the secure proxy log to troubleshoot SSP issues. Secure proxy logs are created for the CM and the engine. The file is called `secureproxy.log` at the engine and `cms.log` at CM.

When a secure proxy log file reaches a predefined size, the current log is archived and the file name is changed to `secureproxy.log.1`. If archive files already exist, each archive file is renamed. For example, a log called `secureproxy.log.3` is renamed to `secureproxy.log.4` and a log `secureproxy.log.2` is renamed `secureproxy.log.3`. The maximum number of archive files to maintain is configured. Secure proxy log settings are configured in the `log.properties` file located in the `install_dir/bin` directory.

Secure Proxy Log Parameters

Following are the parameters that can be modified for a secure proxy log in the `log.properties` file:

Parameter	Description
<code>proxy.log.file.routing</code>	<p>Determines if the secure proxy log is written to a file.</p> <p><code>y</code> = write the log to a file. <code>y</code> is the default setting. <code>n</code> = do not create a log file.</p> <p>Note: If you configure the secure proxy log to be written to the <code>syslog</code> daemon, this parameter can be set to <code>n</code>. Otherwise, a debug log is written to a file, regardless of the value of this parameter.</p>

Parameter	Description
proxy.log.filename	The location and file name to assign to a log. The default value is <code>../logs/secureproxy.log</code> .
proxy.log.maxfilesize	The maximum file size allowed for a secure proxy log. When the maximum file size is reached, the debug log is closed and a new log is opened. The default log file size is 50MB.
proxy.log.maxbackupindex	The number of archive files to maintain. If the number of archive files identified in this parameter is exceeded, the oldest archive file is deleted. The default value is 10.
proxy.log.level	The logging level for the secure proxy log. The default value is INFO. This value can be set using CM.
proxy.log.syslog.routing	Determines if the secure proxy log is written to syslog. y = write the log to syslog. n is the default setting. n = do not write the debug log to syslog. You must configure a valid <code>syslogd.port</code> and <code>syslogd.host</code> in order to write to syslog.
proxy.log.syslog.facility	The facility number to associate with secure proxy log messages. The default value is 17.

Secure Proxy File Output

Following are the fields in a secure proxy log:

Field	Format	Description
Date	dd-mm-yyyy where dd = day, mm = month, and yyyy = year.	The date the message was logged.
Time	hh:mm:ss:mss where hh = hours, mm = minutes, ss = seconds, mss = milliseconds.	The time the message was logged.
Session id	A 72-digit number	A number assigned to the session.
Name of component issuing log msg	"{" + name + "}"	The component that issues the message such as <code>AccepterThread:Secure</code>
Logging level	ERROR, WARN, INFO, DEBUG	The type of logging that is written to the log.
Msg text	a text string	An explanation of the error message.

Node Logs

You can turn on node level logging to log sessions for a specific node. The node-level logs are named `secureproxy-<netmapName>.<nodeName>.log` where *netmapName* is the name of the netmap and *nodeName* is the name of the node for which activity is being logged. Refer to the Sterling Secure Proxy Configuration Guide for more information.

When the sessions for a node end, the node-level log file for the session is closed. A new session appends to the end of the node log file. Both inbound and outbound nodes log both sides of the connection. Enabling logging on one of the nodes captures end-to-end session events.

Certicom Logs

Use the Certicom log to troubleshoot communications issues when using SSL or TLS. The file is called `certicom.log`.

Following are the parameters that can be modified for a Certicom log in the `log.properties` file:

Parameter	Description
<code>certicom.log.file.routing</code>	Determines if the certicom log is written to a file. y = write the log to a file. y is the default setting. n = do not create a log file. Note: If you configure the log to be written to the syslog daemon, this parameter can be set to n. Otherwise, a log is written to a file, regardless of the value of this parameter.
<code>certicom.log.filename</code>	The location and file name to assign to a log. The default value is <code>../logs/certicom.log</code> .
<code>certicom.log.maxfilesize</code>	The maximum file size allowed for a certicom log. When the maximum file size is reached, the log is closed and a new log is opened. The default log file size is 100MB.
<code>certicom.log.maxbackupindex</code>	The number of archive files to maintain. If the number of archive files identified in this parameter is exceeded, the oldest archive file is deleted. The default value is 1.
<code>certicom.log.level</code>	The logging level for the certicom log. The default value is ERROR.
<code>certocm.log.syslog.routing</code>	Determines if the certicom log is written to syslog. y = write the log to syslog. n is the default setting. n = do not write the debug log to syslog. You must configure a valid <code>syslogd.port</code> and <code>syslogd.host</code> in order to write to syslog.
<code>certicom.log.syslog.facility</code>	The facility number to associate with Certicom proxy log messages. The default value is 17.

Perimeter Server Logs

Perimeter server log information is written to a log file called `perimeter.log`. The default maximum size for the perimeter log is 100 MB.

When a log file reaches a predefined size, the current log is renamed and a new log is created. For example, an older log called `perimeter.log1` is renamed to `perimeter.log2` and the log `perimeter.log2` becomes `perimeter.log3`.

Perimeter server log parameters are defined in the `log.properties` file. You can change one or more of the following parameters:

Parameter	Description
<code>perimeter.log.file.routing</code>	<p>Determines if the perimeter log is written to a file.</p> <p>y = write the log to a file. y is the default setting.</p> <p>n = do not create a perimeter log file.</p> <p>Note: If you configure the perimeter log to be written to the syslog daemon, this parameter can be set to n. Otherwise, a perimeter log is written to a file, regardless of the value of this parameter.</p>
<code>perimeter.log.filename</code>	The location and file name to assign to a perimeter server log. The default value is <code>../logs/perimeter.log</code> .
<code>perimeter.log.maxfilesize</code>	The maximum size allowed in a perimeter server log. When the <code>maxfilesize</code> is reached, the perimeter server log is closed and a new log is opened. The default log file size is 100MB.
<code>perimeter.log.maxbackupindex</code>	The number of archive files to maintain. If the number of archive files identified in this parameter is exceeded, the oldest archive file is deleted. The default value is 1.
<code>perimeter.log.level</code>	The logging level for the perimeter log. The default value is <code>ERROR</code> . This value can be set using <code>CM</code> .
<code>perimeter.log.syslog.routing</code>	<p>Determines if the perimeter log is written to syslog.</p> <p>y = write the log to syslog.</p> <p>n = do not write the log to syslog. n is the default setting.</p> <p>You must configure a valid <code>syslogd.port</code> and <code>syslogd.host</code> in order to write to syslog.</p>
<code>perimeter.log.syslog.facility</code>	The facility number to associate with the perimeter log messages. The default value is 17.

SFTP Logs

If you configure SSP for an SFTP environment, two additional logs are maintained: a Maverick log and an SFTP adapter log.

Maverick Log

The Maverick toolkit is used to manage communications in an SFTP environment. All of the protocol messages generated by the Maverick toolkit are written to a log file called `maverick.log`. If you have problems in an SFTP environment, view this log to help troubleshoot the issue. File routing and syslog routing for a Maverick log are controlled by the `proxy.log.file.routing` and `proxy.log.syslog.routing` settings.

The default size of the `maverick.log` file is 100MB. The maverick log is set up to maintain one archive file so that when the `maverick.log` files reaches 100MB, a new file is created, and the archive file is renamed to `maverick.log.1`.

Following are the properties for the maverick log that you can change in the `log.properties` file:

Field	Description
<code>maverick.log.filename</code>	The location and file name to assign to a maverick server log. The default is <code>../logs/maverick.log</code> .
<code>maverick.log.maxfilesize</code>	The maximum size of a maverick log file before archiving it and creating a new file. The default size is 100MB.
<code>maverick.log.maxbackupindex</code>	The number of backup files to maintain. The default value is 1.
<code>maverick.log.level</code>	The logging level to write to the maverick log file. Available options include: NONE, ERROR, WARN, INFO, and DEBUG. The default value is INFO.

SFTP Adapter Log

A log is maintained for SFTP adapter activity. The file is called `sftp.adapter-<adapterName>.log` where *adapterName* is the name of the adapter as configured in SSP.

The SFTP adapter log is set up to maintain 10 archive files. When the log files reaches 50MB, a new file is created and the archive file is renamed to `sftp.adapterAdapterA.log.1`. If older versions exist, they will be renamed first. For example, an older log called `sftp.adapter<adapterName>.log` is renamed to `sftp.adapter<adapterName>.log1` and the `sftp.adapter<adapterName>.log 2` is renamed `sftp.adapter<adapterName>.log 3`. The maximum number of versions to keep is configured in the `log.properties` file.

Following are the properties for the SFTP log that you can change in the log.properties file:

Field	Description
sftp.log.enable	Identifies if SFTP adapter messages are written to a separate log. Valid values are true false The default value is false. If this parameter is set to true, the adapter log information is written to the log file.
sftp.log.filename	The location and file name to assign to an SFTP adapter log. The default value is ../logs/sftp.adapter- <i>adaptername</i> .log where <i>adaptername</i> is the name assigned to the adapter in SSP.
sftp.log.maxfilesize	The maximum size of an SFTP log file before archiving it and creating a new file. The default size is 50MB.
sftp.log.maxbackupindex	The number of backup files to maintain. The default value is 10.

Start and Stop a Remote Perimeter Server

Use the procedures in this chapter to start and stop a remote perimeter server.

Start and Stop a Remote Perimeter Server on UNIX or Linux

To start a remote perimeter server on UNIX or Linux:

1. Change to the directory where the perimeter server is installed.
2. Type `startupPs.sh`.

To stop a remote perimeter server on UNIX or Linux:

1. Change to the directory where the perimeter server is installed.
2. Type `stopPs.sh`.

Start and Stop a Remote Perimeter Server on Windows

You can start a perimeter server from a Windows service or from the command line.

To start a perimeter server from the command line on Windows:

1. Change to the directory where the perimeter server is installed.
2. Type `startPSService.cmd`.

You can stop a perimeter server from a Windows service or from the command line.

To stop a perimeter server from a command line on Windows:

1. Change to the directory where the perimeter server is installed.
2. Type `stopPs.cmd`.

Optional Tasks

Use the procedures in this chapter to obtain a license file or change the heap size to improve performance.

Obtain and Install a License Key File

If your license key is close to its expiration date, you need to request a new key. To obtain and install a license key file:

1. Obtain your IP address or host ID information.
2. Log on to the Sterling Commerce Customer Support Web site.

Note: You must have a Support on Demand user name and password for access to information and services provided on the Sterling Commerce Customer Support Web site. If you are a new user, click the new account setup under New User. Your user account and will be sent to you within one business day.

3. From the support menu, select Connect > Key Request.
4. Complete the Connect Key Request form and submit it to Sterling Commerce.
5. When you receive the new license key, make a copy of the file and keep it in a safe place.
6. Replace the existing license key with the new license key file in the *install_dir/conf* directory, where *install_dir* is the directory used to install the engine.
7. Rename the new license key file to **license.key**.
8. If the engine is running, stop and restart it.

Modify the Heap Size

When you install the engine and the CM, the heap size is set to 512 MB on the engine and 256 MB on CM. If you determine that your system is running slow, modify the heap size to improve performance.

Modify the Engine Heap Size on UNIX or Linux

To modify the engine heap size on UNIX or Linux:

1. From the *install_dir/bin* directory, open the `startEngine.sh` file.
2. Modify the `MAXHEAP` parameter to the preferred value:
3. Save the file.

Modify the CM Heap Size on UNIX or Linux

To modify the CM heap size on UNIX or Linux:

1. From the *install_dir/bin* directory, open the `startCM.sh` file.
2. Modify the `MAXHEAP` parameter to the preferred value:
3. Save the file.

Modify the Engine Heap Size on Windows

If you run the engine as a Windows service, modify the engine heap size as follows:

1. From the *install_dir\bin* directory, open the `SSPEngine$.lax` file.
2. Modify the following parameter to the preferred value:

```
lax.nl.java.option.java.heap.size.max=536870912
```

3. Save the file.

If you run the engine from the command line, modify the engine heap size as follows:

1. From the *install_dir\bin* directory, open the `startEngine.bat` file.
2. Modify the `MAXHEAP` parameter to the preferred value:
3. Save the file.

Modify the CM Heap Size on Windows

If you run the engine as a Windows service, modify the CM heap size as follows:

1. From the *install_dir\bin* directory, open the `SSPcm$.lax` file.

2. Modify the following parameter to the preferred value:

```
lax.nl.java.option.java.heap.size.max=268435456
```

3. Save the file.

If you run the CM from the command line, modify the CM heap size as follows:

1. From the *install_dir*\bin directory, open the startCM.bat file.
2. Modify the following parameter to the preferred value:

```
MAXHEAP=256m
```

3. Save the file.

A

Adapter
 defined 7
 start from CM 24

Audit log 25

C

Change
 CM user password 11
 logging level for inbound node 30

CM
 change user password 11
 logon on UNIX or Linux 9
 modify the timeout value for a session 12
 run on UNIX or Linux 9
 start from a Windows Service 11
 start on UNIX or Linux 9
 stop on UNIX or Linux 10

D

Definition
 Sterling External Authentication Server 7

Definition, Sterling Secure Proxy 5

E

EA, defined 7

Engine
 audit log events 27
 change the listen port 35
 start on UNIX or Linux 18
 start on Windows 19
 stop from CM 18
 stop on Windows 18

H

Heap size, modify 36

I

Illustration, Sterling Secure Proxy 5

L

Listen port
 for engine, change 35

Logon
 to CM on UNIX or Linux 9
 to CM on Windows 11

M

Maverick log 31

Modify
 connection settings 14
 connection settings for CM 14
 logging level for CM session 14
 the CM heap size 36
 the engine heap size 36
 the heap size 36
 timeout value for a CM session 12

N

Netmap, defined 7

Node logs 29

O

Obtain a license key file 35

P

Password
 change for CM user 11

Perimeter server logs 30

Policy, defined 7

R

Run

- CM on UNIX or Linux 9
- CM on Window 10
- CM on Windows 10

S

SFTP adapter log 31

SFTP logs 31

SSP architecture 6

SSP configuration store, defined 7

SSP engine properties file, defined 7

SSP engine, defined 7

SSP flow diagram 6

Start

- an engine on UNIX or Linux 18
- CM from a Windows service 11
- CM on UNIX or Linux 9

Sterling External Authentication Server (EA), defined 7

Sterling Secure Proxy

- defined 5
- illustration 5

Stop

- an engine from UNIX or Linux 18
- an engine on Windows 18
- CM on UNIX or Linux 10

System settings

- globals 14
- lock manager 15

T

Timeout

- modify for CM session 12

Timeout value for a CM session, modify the 12

U

Unlock

- a CM component 15

V

View configured engines 19

W

Web server, defined 7