

Sterling Secure Proxy



Operations Guide

Version 34

Sterling Secure Proxy



Operations Guide

Version 34

Note

Before using this information and the product it supports, read the information in "Notices" on page 83.

This edition applies to version 3.3.01 of IBM Sterling Secure Proxy and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2006, 2013.**

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

Contents

Chapter 1. Start the Engine on UNIX or Linux	1
Start the Engine on UNIX or Linux	1
Start the Engine Using a Stored Passphrase	1
Start the Engine And Require a Passphrase	1
Chapter 2. Stop the Engine from UNIX or Linux	3
Chapter 3. Start the Engine on Microsoft Windows	5
Start the Engine on Microsoft Windows	5
Start the Engine as a Console Application on Microsoft Windows	5
Start Sterling Secure Proxy as an Automatic Microsoft Windows Service	5
Set Up the Engine to Require a Passphrase Prompt at Startup on Microsoft Windows	6
Set up the Engine to Start as a Microsoft Windows Service	6
Chapter 4. Stop the Engine from a Microsoft Windows Console Application . 7	7
Chapter 5. Stop the Engine from CM	9
Chapter 6. Stop the Engine from Microsoft Windows Services	11
Chapter 7. Start CM Without Providing a Passphrase at Startup on UNIX or Linux	13
Chapter 8. Start CM and Require a Passphrase at Startup on UNIX or Linux	15
Chapter 9. Log On to CM on UNIX or Linux	17
Chapter 10. Stop CM on UNIX or Linux	19
Chapter 11. Start CM from Microsoft Windows	21
Chapter 12. Log on to CM from Microsoft Windows	23
Chapter 13. Stop the Engine from Microsoft Windows	25

Chapter 14. Start and Stop a Remote Perimeter Server on UNIX or Linux	27
Chapter 15. Start and Stop a Remote Perimeter Server on Microsoft Windows	29
Chapter 16. Start and Stop Perimeter Servers	31
Start a Perimeter Server on UNIX or Linux	31
Stop a Perimeter Server on UNIX or Linux	31
Start Perimeter Servers in a Microsoft Windows Environment	31
Stop a Perimeter Server on Microsoft Windows	31
Chapter 17. The Configuration Manager 33	33
Restore CM State	33
Change the Password for a CM User	33
Change the CM Passphrase on UNIX or Linux	34
Change the CM Passphrase in Microsoft Windows	34
Change the Listen Port on CM	35
Modify the Listener Settings for CM	35
Modify Security Settings for CM	35
Modify Logging for Sessions Between CM and the Web Server	36
Modify Connection Settings for Sessions Between CM and the Web Server	36
Unlock a CM Component	36
Modify the Timeout Value for a CM Session	37
Uninstall CM from UNIX or Linux	37
Uninstall CM from Microsoft Windows	37
Chapter 18. Manage Configuration Definitions	39
Change the Logging Level for a Sterling Connect:Direct Node	39
Change the Logging Level for an Inbound Node	39
Change the Logging Level for an Outbound Node	39
Change the Logging Level for a Local Perimeter Server	40
Modify Properties in an Adapter Definition.	40
Chapter 19. Copy and Delete Engines, Adapters, Netmaps, Nodes, and Policies	41
Chapter 20. Copy an Engine, Adapter, Netmap, or Policy	43
Chapter 21. Copy a Node	45

Chapter 22. Delete an Engine, Adapter, Netmap, or Policy	47
Chapter 23. Delete an Inbound Node or Outbound Node	49
Chapter 24. Delete a Sterling Connect:Direct Node.	51
Chapter 25. Filter a Node List	53
Chapter 26. Manage Engines	55
View Configured Engines.	55
Change the Engine Passphrase on Microsoft Windows	55
Configure the Refresh Interval Between CM and Engines.	56
Update the Monitor Display of Engine Information	56
Manually Send a Configuration File to an Engine.	56
Change the Listen Port for an Engine.	57
Change the IP Address for an Engine.	57
Change the Logging Level for an Engine	58
Uninstall the Engine from UNIX or Linux	58
Uninstall the Engine from Microsoft Windows.	58
Chapter 27. Monitor Adapters	61
Monitor Configured Adapters	61
Stop an Adapter from CM	61
Start an Adapter from CM	61
Chapter 28. Modify Heap	63
Modify Engine Heap Size on UNIX or Linux	63
Modify Engine Heap Size on Microsoft Windows.	63
Modify the CM Heap Size on UNIX or Linux	64
Modify the CM Heap Size on Microsoft Windows	64
Chapter 29. Change Logging	65
Audit Log Overview	65

Audit Log Parameters	65
Enable SysLog Support in the Audit Log	66
CM Audit Log Events	66
Engine Audit Log Events.	66
Sterling Secure Proxy Log Overview	67
Sterling Secure Proxy Log Parameters	67
Sterling Secure Proxy File Output	68
Node Logs	68
Certicom Logs	68
Perimeter Server Log	69
Maverick Log.	70
SFTP Adapter Log	70

Chapter 30. Password Policy and Accounts.	73
Manage User Accounts and Passwords	73
Manage Password Policies	73
Create a Password Policy.	74
Edit a Password Policy	74
Copy a Password Policy	74
Delete a Password Policy.	75
Manage CM User Accounts	75
Create a CM User Account	76
Edit a CM User Account	76
Copy a CM User Account	76
Delete a CM User Account	77
Manage User Stores and User Accounts	77
Create a User Store.	77
Modify the User Account Locking Value in the User Store	78
Copy a User Store	78
Delete a User Store	79
Create an Engine User Account.	79
Add SSH Keys to a User Account	79
Edit an Engine User Account	80
Copy an Engine User Account	80
Delete an Engine User Account.	81

Notices	83
--------------------------	-----------

Chapter 1. Start the Engine on UNIX or Linux

Start the Engine on UNIX or Linux

About this task

When you install the Sterling Secure Proxy engine, you define a passphrase. It is required at startup. Use one of the following methods to start the Sterling Secure Proxy engine:

- Start the engine automatically, without interaction from the user.
- Require the user to type a passphrase at startup. It is masked and not visible as it is typed.

The server starts in the background. All log messages are written to the `bin/startEngine.out` file.

Start the Engine Using a Stored Passphrase

About this task

To start the engine on UNIX or Linux without being prompted for a passphrase.

Procedure

1. Navigate to `install_dir/bin`, where `install_dir` is the directory where the engine is installed and type the following command: `./startEngine.sh`
2. At the prompt, type the passphrase defined during installation and press **Enter**. A message is displayed indicating the engine is ready for service.

Note: If the engine is running in the background, the message is not displayed. To view the message, go to the `startEngine.out` file.

Start the Engine And Require a Passphrase

About this task

To start the engine and require that a passphrase be typed at startup:

Procedure

1. Delete the `sb.enc` file from `install_dir/conf/system`.
2. Navigate to `install_dir/bin` and type the following command: `./startEngine.sh`
3. When prompted for a passphrase, type the passphrase defined at installation.

Chapter 2. Stop the Engine from UNIX or Linux

About this task

To stop the engine from the command line:

Procedure

1. Navigate to *install_dir/bin*, and type the following command: `./stopEngine.sh`
2. At the passphrase prompt, type the passphrase defined for the Engine.
A message is displayed indicating the engine is stopped.

Chapter 3. Start the Engine on Microsoft Windows

Start the Engine on Microsoft Windows

About this task

When you install the engine on Microsoft Windows, it is installed as a Microsoft Windows service and configured to start manually. By default, start Sterling Secure Proxy by starting the Sterling Secure Proxy Engine service from the Services application in Microsoft Windows. To start Sterling Secure Proxy automatically when you run Microsoft Windows, go to Microsoft Windows services and change the Sterling Secure Proxy Engine V3.4.1 application startup.

Start the Engine as a Console Application on Microsoft Windows

About this task

To start the engine:

Procedure

1. Click **Start > Run > Browse**.
2. Double-click the startEngine.bat file in the *install_dir\bin* directory.
3. Click **OK**.
4. If prompted, type the passphrase defined for the engine.
A message is displayed indicating the engine is ready for service.

Note: When you run the engine as a Microsoft Windows service, the passphrase is encrypted and stored.

Start Sterling Secure Proxy as an Automatic Microsoft Windows Service

About this task

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

Refer to Microsoft Windows documentation to configure Sterling Secure Proxy as an automatic Microsoft Windows service.

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

About this task

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

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

Set up the Engine to Start as a Microsoft Windows Service

About this task

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

Procedure

1. Click **Start > Run > Browse**.
2. Double-click the `enableBootstrap.bat` file in the `SSP_engine_install_dir\bin` directory:
3. Click **OK**.
4. At the prompt, type the engine passphrase and press **Enter**.

Note: When you run the engine as Microsoft Windows service, the passphrase is encrypted and stored.

Chapter 4. Stop the Engine from a Microsoft Windows Console Application

About this task

To stop the engine when it is running as a Microsoft Windows console application:

Procedure


1. Click **Start > Run > Browse**.
2. Double-click the stopEngine.bat file from the *install_dir\bin* directory.
3. Click **OK**.
4. At the prompt, type the engine passphrase and press **Enter**.

Chapter 5. Stop the Engine from CM

About this task

To stop the engine from CM:

Procedure

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**.

Chapter 6. Stop the Engine from Microsoft Windows Services

About this task

To stop the engine from Microsoft Windows services, go to Microsoft Windows services and stop the Sterling Secure Proxy Engine V3.4.1 application.

Chapter 7. Start CM Without Providing a Passphrase at Startup on UNIX or Linux

About this task

Use this method to start CM using a stored passphrase. The file called `sb.enc` is created during installation and must exist in the `ssp_install_dir/conf/system` directory.

To start CM automatically without the need to provide a passphrase, navigate to the `install_dir/bin` directory, and type the following command:

```
./startCM.sh
```

Chapter 8. Start CM and Require a Passphrase at Startup on UNIX or Linux

About this task

To start CM and require that a passphrase be provided:

Procedure

1. Navigate to *install_dir/conf/system* and delete the *sb.enc* file
2. Type the following command: `./startCM.sh`
3. Type the CM passphrase and press **Enter**.

Chapter 9. Log On to CM on UNIX or Linux

About this task

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

To sign in to CM:

Procedure

1. Open Microsoft Internet Explorer.
2. Type the sign in information in the following format. Refer to the table for a description:

`https://hostname or ipaddress:port/SSPDashboard`

Component	Description
hostname or ipaddress	Name or IP address of the computer where CM is installed.
port	Port defined for the web server at installation. Default= 8443.

3. On the sign-in screen, type the user ID and passphrase and click Sign In.

Chapter 10. Stop CM on UNIX or Linux

About this task

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

To stop CM on UNIX or Linux:

Procedure

1. Log out of CM.
2. Navigate to the *install_dir/bin* directory and type the following command:
`./stopCM.sh`
3. Type the passphrase for CM.
4. Type the administrator user name and passphrase.

Chapter 11. Start CM from Microsoft Windows

About this task

To start CM:

Procedure

1. Click **Start > Run > Browse**.
2. Browse to *install_dir*\bin, where *install_dir* is the CM installation directory
3. Double-click the startCM.bat file.
4. Click **OK**.
5. If prompted, type the passphrase defined for CM.
A message is displayed that CM is ready for service and identifying the URL used to connect to the CM server.
6. Record the URL to connect to the CM server on the Startup Worksheet.
7. Log on to CM From Microsoft Windows.

Chapter 12. Log on to CM from Microsoft Windows

About this task

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

To log on to CM:

Procedure

1. Open Microsoft Internet Explorer.
2. Type the logon in the following format. Refer to the table for a description of the components:
`https://hostname or ipaddress:port/SSPDashboard`
3. Type the following information for your configuration:

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

4. On the logon screen, type the user ID and passphrase.
5. Click **Logon**.

Chapter 13. Stop the Engine from Microsoft Windows

About this task

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

To stop the engine on Microsoft Windows, go to Microsoft Windows services and stop the Sterling Secure Proxy Engine V3.4.1 application.

Chapter 14. Start and Stop a Remote Perimeter Server on UNIX or Linux

Procedure

1. To start a remote perimeter server on UNIX or Linux:
 - a. Change to the directory where the perimeter server is installed.
 - b. Type `startupPSService.sh`.
2. To stop a remote perimeter server on UNIX or Linux:
 - a. Change to the directory where the perimeter server is installed.
 - b. Type `stopPs.sh`.

Chapter 15. Start and Stop a Remote Perimeter Server on Microsoft Windows

About this task

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

Procedure

1. To start a perimeter server from the command line on Microsoft Windows:
 - a. Change to the directory where the perimeter server is installed.
 - b. Type `startPSService.cmd`.
2. To stop a perimeter server from a command line on Microsoft Windows:
 - a. Change to the directory where the perimeter server is installed.
 - b. Type `stopPs.cmd`.

Chapter 16. Start and Stop Perimeter Servers

Start a Perimeter Server on UNIX or Linux

About this task

To start a perimeter server on UNIX or Linux:

Procedure

1. Change the directory to `/install_dir/bin` where `install_dir` is the directory where the perimeter server is installed.
2. Type `startupPs.sh` and press **Enter**.

Stop a Perimeter Server on UNIX or Linux

About this task

To stop a perimeter server:

Procedure

1. Change the directory to `/install_dir/bin` where `install_dir` is the directory where the perimeter server is installed.
2. Type `stopPs.sh` and press **Enter**.

Start Perimeter Servers in a Microsoft Windows Environment

About this task

To start a perimeter server:

Procedure

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

Stop a Perimeter Server on Microsoft Windows

About this task

The remote perimeter server is installed as a Microsoft Windows service. You can stop the remote perimeter server using the Microsoft Windows service option or you can stop the perimeter server from the command line.

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

Procedure

1. Change the directory to `install_dir\bin` where `install_dir` is the directory where the perimeter server is installed.
2. Type `stopPSService.cmd`.

Chapter 17. The Configuration Manager

Restore CM State

About this task

IBM® Sterling Secure Proxy 3.4.1.8 and above automatically creates a backup of the configuration file prior to starting. There is currently no functionality to remove or manage backed-up directories and unnecessary backup files should be removed that you no longer need. The backup does not occur during the upgrade process, it occurs when you run the IBM Sterling Secure Proxy Configuration Manager after the 3.4.1.8 upgrade. It is recommended that you perform a manual backup prior to the upgrade process.

To restore the Configuration Manager to a previous state, complete the following steps:

Procedure

1. By default, the backup directory is located in [CM_INSTALL]/CM-BACKUPyyyyymmddmss. To select a different backup directory, select a new directory in [CM_INSTALL]/conf/system/sysGlobal.xml. A new field, backupDir is added and allows you to specify a new backup directory.

Note: If using a new backup directory, the backup files are placed in [backupDir]/CM-BACKUP-yyyyymmddmss.

2. Copy the [BACKUP_DIR]/apps to [CM_INSTALL]/conf
3. Copy the the [BACKUP_DIR]/apps to [CM_INSTALL]/conf >[BACKUP_DIR]/apps to [CM_INSTALL]/app
4. Restart the IBM Sterling Secure Proxy Configuration Manager.
5. To utilize a different backup directory for startup and backup processing, make the following changes in [CM_INSTALL]conf/system/sysGlobal.xml and replace **/your-back-dir** with the backup directory to be used by the IBM Sterling Secure Proxy Configuration Manager to backup CM configuration files during startup.

```
<sysGlobalDef <threadCount>5</threadCount>
<logLevel>INFO</logLevel>
<maxAllowedLoginAttempts>0</maxAllowedLoginAttempts>
<loginLockoutDelayTime>10</loginLockoutDelayTime>
<backupDir><![CDATA[/your-back-dir]]&gt;</backupDir>
<name>sysGlobal</name>
<verStamp>1</verStamp>
</sysGlobalDef>
```

Note: To disable the automatic backup feature, modify the sysGlobal.xml in [CM_INSTALL]/conf/system and change the enableConfigBackup parameter from "true" to "false".

Change the Password for a CM User

About this task

Configured users can access the CM and define a password for each user. To change the user's CM password, complete the following procedure.

Procedure

1. Open Microsoft 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**.

Change the CM Passphrase on UNIX or Linux

About this task

To change the passphrase defined for CM at installation.

Procedure

1. Navigate to `install_dir/bin`, where `install_dir` is the CM installation directory.
2. To stop CM, type the following command and press **Enter**:
`./stopCM.sh`
3. Type the passphrase defined for CM and press **Enter**.
4. At the administrator ID prompt, type the administrator ID and press **Enter**.
5. At the password prompt, type the password and press **Enter**. CM stops.
6. Type the following command, and press **Enter**.
`./changePassphrase.sh`
7. Type the current passphrase and press **Enter**.
8. Type a new passphrase and press **Enter**. Retype the new passphrase and press **Enter**.
Your new passphrase is effective the next time you start CM.

Change the CM Passphrase in Microsoft Windows

About this task

To change the passphrase defined for CM at installation:

Procedure

1. Click **Start > Run > Browse**.
2. Browse to the `install_dir\bin` directory, where `install_dir` is the CM installation directory.
3. To stop CM, double-click the following file:
`stopCM.bat`
4. Click **OK**.
5. Type the CM passphrase and press **Enter**.
6. At the administrator ID prompt, type the administrator ID and press **Enter**.
7. At the password prompt, type the password and press **Enter**.
CM stops.
8. Double-click the following file:
`changePassphrase.bat`
9. Click **OK**.

10. Type the current passphrase and press **Enter**.
11. Type the new passphrase and press **Enter**. Retype the new passphrase and press **Enter**.
Your new passphrase is effective the next time you start CM.

Change the Listen Port on CM

About this task

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

Procedure

1. Stop CM.
2. Navigate to `install_dir\bin`, where *install_dir* is the CM installation directory.
3. Type the following command:

```
configureaccepter port = nnnnn
```

where `nnnn` is the port to listen on.

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 accepters take effect the next time CM is started.

Modify the Listener Settings for CM

About this task

When you install Sterling Secure Proxy, 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:

Procedure

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

About this task

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 *Manage Certificates Between Sterling Secure Proxy Components* to configure security settings.

To modify security settings for CM:

Procedure

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 Logging for Sessions Between CM and the Web Server

About this task

To modify the logging level for sessions between CM and the web server:

Procedure

1. Select **System** from the menu bar.
2. Expand the **System Settings** tree and click **CMSystemSettings**.
3. Click the **Globals** tab.
4. Modify the logging level.
5. Click **Save**.

Modify Connection Settings for Sessions Between CM and the Web Server

About this task

To modify the connection settings for sessions between CM and the web server:

Procedure

1. Select **System** from the menu bar.
2. Click **Actions > System Settings**.
3. Click the **Globals** tab.
4. Modify one or more of the connection values.
5. Click **Save**.

Unlock a CM Component

About this task

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:

Procedure

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**.

Modify the Timeout Value for a CM Session

About this task

When you configure your environment using CM, a session times out if it is idle for 30 minutes. To change the CM session timeout value on UNIX, Linux, or Microsoft Windows:

Procedure

1. Open the web.xml file in the *install_dir*\apps\jetty\webservices\webapps\SSPDashboard\WEB-INF directory.
2. Change the following parameter to identify how many minutes before a session time out.
`<session-timeout>30</session-timeout>`

Uninstall CM from UNIX or Linux

About this task

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

If you uninstall CM on HP-UX, the /jre directory remains. You must delete it manually.

To remove CM:

Procedure

1. Stop CM.
2. Navigate to the *SSPCM_install_dir*/UninstallerData directory.
3. Type the following command and press **Enter**:
`Uninstall_Sterling_Secure_Proxy_Configuration_Manager_V3.4.1`

Uninstall CM from Microsoft Windows

About this task

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

To remove CM:

Procedure

1. Stop CM.
2. Click **Start** > **Programs** > IBM Sterling Secure Proxy Vx.x.x.x
3. Click **Uninstall Configuration Manager**.
4. Click **Uninstall**.
5. Click **Done**.

Chapter 18. Manage Configuration Definitions

Change the Logging Level for a Sterling Connect:Direct Node

About this task

When you configure a Sterling Connect:Direct® node, the logging level is set to None and no log is created.

To change the logging level for a Sterling Connect:Direct node so that a log is created:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Netmaps tree and select the netmap that contains the node to modify.
3. Select a node and click **Edit**.
4. Click the **Advanced** tab.
5. Select the logging level in the **Logging level** field.
6. Click **Save**.

Change the Logging Level for an Inbound Node

About this task

When you configure an inbound node for the HTTP, FTP, or SFTP protocol, the logging level for the node is set to None and no log is created for the node.

To change the logging level for an inbound HTTP, FTP, or SFTP node:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Netmaps tree and select the netmap where the inbound node to modify is defined.
3. Select the inbound node to modify and click **Edit**.
4. Click the **Advanced** tab.
5. Select the logging level in the **Logging level** field.
6. Click **Save**.

Change the Logging Level for an Outbound Node

About this task

When you configure an outbound node for the HTTP, FTP, or SFTP protocol, the logging level is set to None and no log is created for the node.

To change the logging level for an outbound HTTP, FTP, or SFTP node:

Procedure

1. From the **Configuration** navigation panel, click Netmap to expand the list of netmaps.
2. Click the netmap where the outbound node to modify is defined.
3. Click the **Outbound Node** tab.
4. Select an outbound node to modify and click **Edit**.
5. Click the **Advanced** tab.
6. Select the logging level in the **Logging level** field.
7. Click **Save**.

Change the Logging Level for a Local Perimeter Server

About this task

When you configure an engine, the logging level for the local perimeter server is set to Error by default. Error logging level writes all error messages for the local perimeter server to the log.

To change the logging level for a local perimeter server:

Procedure

1. If necessary, click **Configuration** from the menu bar.
2. Expand the Engines tree and click the engine to modify.
3. Click the **Advanced** tab.
4. Select the logging level in the **Local Perimeter Server Logging Level** field.
5. Click **Save**.

Modify Properties in an Adapter Definition

About this task

Adapters are configured with default settings. Perform this procedure to modify a property. For FTP and HTTP adapters, the properties and default values are displayed. To change a property, type a new value for the property key. For SFTP and Sterling Connect:Direct adapters, the properties are not displayed. Refer to the field level help for a description of the properties. To change a property, type the property name and its key value.

To modify an adapter property:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Adapters tree and click the adapter to modify.
3. Click the **Properties** tab.
4. Click **New** to add a new property definition.
5. For each property, specify values for the following:
 - Key
 - Value
6. Click **Save**.

Chapter 19. Copy and Delete Engines, Adapters, Netmaps, Nodes, and Policies

After you create an engine, adapter, netmap, node, or policy, you can copy or delete it as necessary. For nodes, you can filter the list to view only those nodes that meet your requirements. Use the following procedures to copy or delete an engine, adapter, netmap, node, or policy:

- *Copy an Engine, Adapter, Netmap, or Policy*
- *Copy a Node*
- *Copy a Sterling Connect:Direct Node*
- *Delete an Engine, Adapter, Netmap, or Policy*
- *Delete an Inbound Node or Outbound Node*
- *Delete a Sterling Connect:Direct Node*

Chapter 20. Copy an Engine, Adapter, Netmap, or Policy

About this task

To quickly create an adapter, netmap, or policy, you can copy an existing definition and make the changes necessary to create a new item.

To copy a configured engine, adapter, netmap, or policy:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand an Engine, Adapter, Netmap, or Policy tree and click the item to copy.
3. Select **Actions > Copy Selected**.

A new item is created and renamed to *CopyofItemName* where *ItemName* is the name of the original item you created.

4. Modify the item as necessary.
5. Click **Save**.

Chapter 21. Copy a Node

About this task

To quickly create an inbound or outbound node definition, you can copy an existing definition and make the changes necessary to create a new one.

To copy a node:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Netmaps tree and click the netmap where the node is defined.
3. Click the radio button beside the node to copy and click **Copy**.

A new node is created and renamed to *CopyofItemName* where *ItemName* is the name of the original node you created.

4. Modify the node definition as necessary.
5. Click **Save**.

Chapter 22. Delete an Engine, Adapter, Netmap, or Policy

About this task

If you determine that an engine, adapter, netmap, or policy is no longer needed, you can delete it. Before you can delete the item, you must remove any references to it in other items. For example, if a netmap is associated with an adapter definition, it cannot be deleted.

To delete a configured engine, adapter, netmap, or policy:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand an Engine, Adapter, Netmap, or Policy tree and click the item to delete.
3. Select **Actions > Delete Selected**.
4. Click **Delete**.

Chapter 23. Delete an Inbound Node or Outbound Node

About this task

If you determine that a node definition is no longer needed, you can delete it.

To delete a node:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Netmaps tree and click the netmap where the node is defined.
3. Select a node to delete and click **Delete**.
4. Click **Save**.

Chapter 24. Delete a Sterling Connect:Direct Node

About this task

If you determine that a node definition is no longer needed, you can delete it.

To delete a Sterling Connect:Direct node:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Netmap tree and click the Sterling Connect:Direct netmap to where the node is defined.
3. Select the node to delete and click **Delete**.
4. Click **Save**.

Chapter 25. Filter a Node List

About this task

If you define a large set of inbound or outbound nodes, all of the nodes cannot be displayed on the main page. To view a subset of all available inbound nodes or outbound nodes, use the filter function. You can filter the list to display nodes that match the criteria you specify.

To filter a list:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Netmap tree and click the netmap to modify.
3. To filter an outbound node list:
 - a. Click the **Outbound Node** tab.
 - b. Type filter criteria to limit the list. For example, type HTTP* to view all node definitions that begin with HTTP.
4. To filter an inbound node list:
 - a. Click the **Inbound Node** tab.
 - b. Type filter criteria to limit the list.

Note: Filters are case sensitive.

Chapter 26. Manage Engines

View Configured Engines



About this task

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

To view configured engines:

Procedure

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

	Engine is running
	Engine is not running

The following information is displayed for each engine:

- Engine Name
- Last Configuration Pushed
- Message
- CM Version
- Eng. Version

Change the Engine Passphrase on Microsoft Windows

About this task

To change the passphrase defined for the engine at installation:

Procedure

1. Click **Start > Run > Browse**.
2. Double-click the following file in the *install_dir\bin* directory:
stopEngine.bat
3. Click **OK**.
4. Type the engine passphrase and press **Enter**.
The engine stops.
5. Double-click the following file:
changePassphrase.bat
6. Click **OK**.
7. Type the current passphrase and press **Enter**.
8. Type the new passphrase and press **Enter**. Retype the new passphrase and press **Enter**.

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

Configure the Refresh Interval Between CM and Engines

About this task

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

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

Procedure

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

About this task

Use the Engine Status Page for 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 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:

Procedure

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

About this task

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, either wait for CM to poll the engine or manually push the configuration file to the engine. The engine must be running 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:

Procedure

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

About this task

You can change the listen port defined at installation on Microsoft Windows, UNIX, or Linux. Stop the engine before you change the listen port. Refer to *Change the Engine Passphrase on UNIX or Linux* for instructions.

To change the listen port on an engine:

Procedure

1. From *install_dir/bin*, where *install_dir* is the engine installation, type the following command:

```
configureAcceptor port=nnnn
```

2. Type the system passphrase.

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
```

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

Change the IP Address for an Engine

About this task

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 *Install or Upgrade Sterling Secure Proxy on UNIX or Linux* or *Install or Upgrade Sterling Secure Proxy on Microsoft Windows* for instructions.

To specify the IP bind address of the NIC card:

Procedure

1. From *\install_dir\bin*, where *install_dir* is the engine directory, type the following command:

```
configureAcceptor address=IPaddress
```

2. 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
```

Change the Logging Level for an Engine

About this task

When you configure an engine, the logging level for the engine is set to Error by default. Error logging level writes all error messages for the engine to the log.

To change the logging level for an engine:

Procedure

1. Click **Configuration** from the menu bar.
2. Highlight the engine to modify.
3. Click the **Advanced** tab.
4. Select the logging level in the **Engine Logging Level** field.
5. Click **Save**.

Uninstall the Engine from UNIX or Linux

About this task

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

If you uninstall CM or the engine on HP-UX, the */jre* directory remains. You must delete it manually.

To remove the engine:

Procedure

1. Stop the engine.
2. Navigate to the *SSPEngine_install_dir/UninstallerData* directory.
3. Type the following command, and press **Enter**:
`Uninstall_Sterling_Secure_Proxy_Engine_V3.4.1`

Uninstall the Engine from Microsoft Windows

About this task

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

To remove the engine:

Procedure

1. Stop the engine.
2. Click **Start > Programs > Sterking Secure Proxy V3.4.1**.
3. Click **Uninstall Engine**.
4. Click **Uninstall**.
5. Click **Done**.

Chapter 27. Monitor Adapters

Monitor Configured Adapters

About this task

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

To view and monitor adapters:

Procedure

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

About this task

To stop an adapter from CM:

Procedure

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

About this task

To start an adapter:

Procedure

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**.

Chapter 28. Modify Heap

Modify Engine Heap Size on UNIX or Linux

About this task

If you determine that your system is running slowly, you can change the heap size on either the engine or the configuration manager (CM) to improve performance. When you install the Sterling Secure Proxy engine, the heap size is set to a default size of 512MB. To modify the engine heap size on UNIX or Linux:

Procedure

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

Note: You can change the heap size for the engine by setting a `MAXHEAP` environmental variable. Refer to the documentation for your UNIX or Linux operating system for information about configuring environmental variables.

Note: You can override the heap size for the engine by specifying the heap size when you invoke the engine from a script:

```
startEngine.sh 1024m
```

Modify Engine Heap Size on Microsoft Windows

About this task

If you determine that your system is running slowly, you can change the heap size on either the engine or the configuration manager (CM) to improve performance. When you install the Sterling Secure Proxy engine, the heap size is set to a default size of 512MB. If you run the engine as a Microsoft Windows service, modify the engine heap size as follows:

Procedure

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.
4. If you start the engine from a Command Prompt, do the following:
 - a. From the *install_dir\bin* directory, open the `startEngine.bat` file.
 - b. Modify the `MAXHEAP` parameter to the preferred value:
`MAXHEAP=512m`
 - c. Save the file.

Note: You can change the heap size for the engine by setting a `MAXHEAP` environmental variable. You can configure the `MAXHEAP` environmental variable from a Command Prompt:

```
set MAXHEAP=2048m
```

Note: You can override the heap size for the engine by specifying the heap size when you invoke the engine from a Command Prompt:

```
startEngine.bat 1024m
```

Modify the CM Heap Size on UNIX or Linux

About this task

When you install the CM, the heap size is set to 536870912 (512 MB). If your system is slow, you can modify the heap size to improve performance. To modify the CM heap size on UNIX or Linux:

Procedure

1. From the *install_dir/bin* directory, open the startCM.sh file.
 2. Modify the MAXHEAP parameter.
 3. Save the file.
-

Modify the CM Heap Size on Microsoft Windows

About this task

When you install the CM, the heap size is set to 536870912 (512 MB). If your system is slow, you can modify the heap size to improve performance. If you run the CM as a Microsoft Windows service, modify the CM heap size as follows:

Procedure

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=536870912`
3. Save the file.
4. If you run the CM from a Command Prompt, do the following:
 - a. From the *install_dir\bin* directory, open the startCM.bat file.
 - b. Modify the MAXHEAP parameter to the preferred value:
`MAXHEAP=512m`
 - c. Save the file.

Chapter 29. Change Logging

Audit Log Overview

The audit log contains messages about system operations and events. 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 Sterling Secure Proxy 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 called `auditlog.xml` is created for both CM and the engine in the `install_dir/logs/audit` directory. An audit log record can be sent to a syslog daemon to be routed elsewhere for 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>	Number of archive files to maintain. If the number 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. y = write the log to a file. y is the default setting. n = do not create an audit log file. Note: If you configure the audit log to write to the syslog daemon, this parameter can be set to n. Otherwise, an audit log is written to a file, regardless of the value of this parameter.

Parameter	Description
audit.log.syslog.routing	Determines if the audit log is written to syslog. y = write the log to syslog. n = do not write the audit log to syslog. n is the default setting. Configure a valid syslogd.port and syslogd.host in order to write to syslog.
audit.log.syslog.facility	Facility number to associate with audit log messages. The default value is 18.

Enable SysLog Support in the Audit Log

About this task

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
syslogd.enable	Enables syslog daemon support. y = enabled. n = disabled. n is the default setting.
syslogd.host	Name or IP address of the syslog host. The default value is the local host.
syslogd.port	UDP port where the syslog 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 Sterling 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 Sterling Connect:Direct protocols.
- Outbound login successes and failures for the FTP, HTTP, and SFTP protocols.

Sterling Secure Proxy Log Overview

Use the secure proxy log to troubleshoot Sterling Secure Proxy issues. Sterling 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 Sterling 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. Sterling Secure Proxy log settings are configured in the `log.properties` file located in the `install_dir/bin` directory.

Sterling 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>	Determines if the Sterling Secure Proxy log is written to a file. <ul style="list-style-type: none">• <code>y</code> = write the log to a file. This value is the default.• <code>n</code>=do not create a log file. <p>Note: If you configure the Sterling Secure Proxy log to be written to the syslog 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>
<code>proxy.log.filename</code>	The location and file name to assign to a log. The default value is <code>../logs/secureproxy.log</code> .
<code>proxy.log.maxfilesize</code>	The maximum file size allowed for a Sterling 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.
<code>proxy.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 10.
<code>proxy.log.level</code>	The logging level for the Sterling Secure Proxy log. The default value is <code>INFO</code> . This value can be set using CM.
<code>proxy.log.syslog.routing</code>	Determines if the Sterling Secure Proxy log is written to syslog. <ul style="list-style-type: none">• <code>y</code> = write the log to syslog.• <code>n</code> = do not write the debug log to syslog. This is the default setting. <p>Configure a valid <code>syslogd.port</code> and <code>syslogd.host</code> in order to write to syslog.</p>
<code>proxy.log.syslog.facility</code>	Facility number to associate with Sterling Secure Proxy log messages. Default=17.

Sterling Secure Proxy File Output

Following are the fields in a Sterling 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 AcceptorThread:Secure
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.

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. Default= <code>../logs/certicom.log</code> .

Parameter	Description
certicom.log.maxfilesize	Maximum file size allowed for a certicom log. When the maximum is reached, the log is closed and a new log is opened. Default=100MB.
certicom.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 1.
certicom.log.level	Logging level for the certicom log. The default value is ERROR.
certicom.log.syslog.routing	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. Configure a valid syslogd.port and .host in order to write to syslog.
certicom.log.syslog.facility	Facility number to associate with Certicom log messages. Default=17.

Perimeter Server Log

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
perimeter.log.file.routing	Determines if the perimeter log is written to a file. y = write the log to a file. y is the default setting. n = do not create a perimeter log file. 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.
perimeter.log.filename	The location and file name to assign to a perimeter server log. Default=../logs/perimeter.log.
perimeter.log.maxfilesize	The maximum size allowed in a perimeter server log. When the maxfilesize is reached, the perimeter server log is closed and a new log is opened. Default=100MB.
perimeter.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. Default=1.
perimeter.log.level	The logging level for the perimeter log. The default value is ERROR. This value can be set using CM.
perimeter.log.syslog.routing	Determines if the perimeter log is written to syslog. y = write the log to syslog. n = do not write the log to syslog. This is the default setting. You must configure a valid syslogd.port and syslogd.host in order to write to syslog.

Parameter	Description
perimeter.log.syslog.facility	Facility number to associate with the log messages. Default=17.

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. Default=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. Default=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 Sterling Secure Proxy.

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
<code>sftp.log.enable</code>	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.

Field	Description
sftp.log.filename	Location and file name to assign to an SFTP adapter log. Default=../logs/sftp.adapter- <i>adaptername</i> .log where adaptername is the name assigned to the adapter in Sterling Secure Proxy.
sftp.log.maxfilesize	The maximum size of an SFTP log file before archiving it and creating a new file. Default=50MB.
sftp.log.maxbackupindex	The number of backup files to maintain. Default=10.

Chapter 30. Password Policy and Accounts

Manage User Accounts and Passwords

Two types of user accounts can be created in Sterling Secure Proxy: CM user accounts and Sterling Secure Proxy engine user accounts. CM user accounts control access to the Sterling Secure Proxy user interface. Engine user accounts control which users can send data through Sterling Secure Proxy. Password policies can be associated with both a CM user account and engine user account to help enforce your company's security policies. Some of the options in the password policy do not apply to engine users. CM user accounts also include role-based security to provide varying levels of access to users within the organization. Sterling Secure Proxy can be configured to perform user authentication based on information defined in a user account.

Use the information in the following topics to manage password policies and user accounts:

- *Manage Password Policies*
- *Manage CM User Accounts*
- *Manage User Stores and User Accounts*

Manage Password Policies

Password policies are sets of security decisions you make and apply to different user accounts according to security policies in your company. These choices include items such as the number of days a password is valid and the maximum and minimum length of a password.

Use password policies to streamline security operations when adding new users. Instead of adding individual policies for each user, you create one password policy and apply it to all users who require the same access.

A password policy is applied to a new user or when the password is changed on an existing user.

You can apply a password policy only to internal user accounts. This provides you the greatest flexibility in maintaining security policies.

For example, a password policy named Test may have the following password settings:

- Valid for 10 days
- Requires a minimum of 10 characters and maximum of 20 characters
- Requires default password change after the initial log in
- Maintains three passwords in history so the user cannot reuse them
- Must use at least two special characters

In this example, the system administrator gives the user a user name and password. The user logs in to Sterling Secure Proxy and is prompted to change the password. If the user fails to provide a password with at least 10 and no more than 20 characters, or without at least two special characters, Sterling Secure Proxy

prompts the user for corrections. After all conditions in the password policy are met, the new password is saved and the user is allowed access.

Each user account can have only one password policy associated with it, but one password policy can be applied to multiple user accounts.

Create a Password Policy

About this task

You create a password policy to assign to user accounts. You do not have to associate a password policy with a user account, but doing so helps manage your security by streamlining your security operations. A user account can have only one password policy.

To create a password policy:

Procedure

1. Click **Advanced** from the menu bar.
2. Click **Actions > New Password Policy**.
3. Specify values for the following:
 - **Password Policy Name** (no spaces allowed)
 - **Days Valid**
 - **Minimum Length**
 - **Maximum Length**
 - **Keep in History**
4. To enforce the policy of using at least two special characters in passwords, enable **Must contain special characters**.
5. Click **Save**.

Results

You can now edit and delete password policies and assign them to user accounts.

Edit a Password Policy

About this task

To edit a password policy:

Procedure

1. Click **Advanced** from the menu bar.
2. Expand the **Password Policies** tree.
3. Click the password policy to edit.
4. Edit the values you want to change. You cannot edit the policy name.
5. Click **Save**.

Copy a Password Policy

About this task

To copy a password policy:

Procedure

1. Click **Advanced** from the menu bar.
2. Expand the **Password Policies** tree.
3. Click the password policy to copy.
4. Click **Actions > Copy Selected**.
5. Type a name for the new policy.
6. Edit any values you want to change.
7. Click **Save**.

Delete a Password Policy

About this task

To delete a password policy:

Procedure

1. If the password policy is associated with a user:
 - a. Click **Credentials** from the menu bar.
 - b. Expand the **User Stores** tree.
 - c. Select the user store that contains the user definition.
 - d. Select the user to edit and click **Edit**.
 - e. Remove the password policy to delete from the **Password Policy ID field**.
 - f. Click **OK**.
 - g. Click **Save**.
2. Click **Advanced** from the menu bar.
3. Expand the **Password Policies** tree and click the password policy to delete.
4. Click **Actions > Delete Selected**.
5. Click **Delete**.

Manage CM User Accounts

CM accounts are assigned a user role: Admin or Operator. Admin users can create and update user accounts and have full access to all configuration options in CM. Operator users have read-only access to accounts and cannot access system functions. Operator users can, however, change their passwords from the login screen.

In addition to role-based security, you can assign password policies to user accounts. Use the default CM user account called admin access CM to create user accounts.

This section includes the following procedures:

- *Create a CM User Account*
- *Edit a CM User Account*
- *Copy a CM User Account*
- *Delete a CM User Account*

Create a CM User Account

About this task

To create a CM user account:

Procedure

1. Click **System** from the menu bar.
2. Click **Actions > New CM User**.
3. Specify the following values for the user account:
 - **User Name** (no spaces allowed)
 - **Password**
 - **Confirm Password**
4. Select the user role to assign to the user account from the User role list: Admin or Operator.
5. To enforce a password policy for this account, select a password policy from the list.
6. To require that the user change the password after the first logon, enable **Password Requires change**.
7. Click **Save**.

Edit a CM User Account

About this task

To edit a CM user account:

Procedure

1. Click **System** from the menu bar.
2. Expand the **CM Users** tree.
3. Select the user account to edit.
4. Edit the user properties as needed. The **User Name** cannot be edited.
5. Click **Save**.

Copy a CM User Account

About this task

You can copy a CM user account to create a new user account.

To copy an account:

Procedure

1. Click **System** from the menu bar.
2. Expand the **CM Users** tree.
3. Select the user account to copy and Click **Actions > Copy Selected**.
4. Type a name for the account.
5. Edit the user properties as needed.
6. Click **OK**.
7. Click **Save**.

Delete a CM User Account

About this task

You can delete a CM user account as needed to maintain the security of Sterling Secure Proxy.

To delete a user account:

Procedure

1. Click **System** from the menu bar.
2. Expand the **CM Users** tree.
3. Select the user account to delete.
4. Click **Actions > Delete Selected**.

Manage User Stores and User Accounts

Create user accounts for users who need to access Sterling Secure Proxy for file transfer. You can create Sterling Secure Proxy user accounts in the default user store, `defUserStore`, or you can create a new user store to manage groups of users.

For users who communicate using the SSH protocol and who use multiple keys to authorize users, identify the key store where keys are stored and the user record containing the key.

Before you begin:

- If you plan to use password policies for user accounts, configure the password policies prior to configuring user accounts.
- If you plan to perform local user authentication using SSH keys for SFTP inbound connections, import SSH keys into the SSH key stores. For more information on importing keys into the SSH key stores, see *Manage SSH Keys for SFTP Transactions*.

This section includes the following procedures:

- *Create a User Store*
- *Copy a User Store*
- *Delete a User Store*
- *Create an Engine User Account*
- *Add SSH Keys to a User Account*
- *Edit an Engine User Account*
- *Copy an Engine User Account*
- *Delete an Engine User Account*

Create a User Store

About this task

To create a user store:

Procedure

1. Click **Credentials** from the menu bar.
2. Click **Actions > New User Store**.

3. Specify a user store name in the **User Store Name** field.
4. If desired, change the default values for the following fields:
 - **User Lockout Duration**
 - **User Lockout Threshold**
5. Click **New** to add a user account to the user store. You must create at least one user account in the user store before you can save it.
6. Specify the following values for the user account:
 - **User Name**
 - **Password**
 - **Confirm Password**
7. To enforce a password policy for this account, select a password policy from the list.
8. If desired, provide the following information for the user:
 - **First Name**
 - **Last Name**
 - **Email Address**
 - **Pager**
 - **Manager ID**
9. Click **OK**.
10. Click **Save**.

Modify the User Account Locking Value in the User Store

About this task

A user account is locked if the user tries to log in to Sterling Secure Proxy and is unsuccessful, the number of times defined in the User Lockout Threshold field. A login is unsuccessful if the user provides an invalid user ID or password. Internal errors, such as a failure by Sterling External Authentication Server to connect to LDAP server, is not a login failure.

To modify the user account locking value:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** in the left navigation bar.
3. Click the user store name to open.
4. Change the default value for the **User Lockout Threshold** field.
5. Click **OK**.
6. Click **Save**.

Copy a User Store

About this task

To copy a user store:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** tree.

3. Select the user store to copy.
4. Click **Actions > Copy Selected**.
5. Type a name for the new user store.
6. Edit the properties as needed.
7. Click **Save**.

Delete a User Store

About this task

To delete a user store:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** tree.
3. Select the user store to delete. The default user store cannot be deleted.
4. Click **Actions > Delete Selected**.
5. Click **Delete**.

Create an Engine User Account

About this task

Create a user account to provide access to the engine. To create an engine user account:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** tree.
3. Click the user store to which you want to add a user account.
4. Click **New**.
5. Specify the following values for the user account:
 - **User Name** (no spaces allowed)
 - **Password**
 - **Confirm Password**
6. To enforce a password policy for this account, select a password policy from the list.
7. Click **OK**.
8. Click **Save**.

Add SSH Keys to a User Account

About this task

To perform local user authentication for a user account that will be used to access Sterling Secure Proxy for SFTP connections, you can associate SSH keys with that account.

To add SSH keys to a user account:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** tree.
3. Click the user store to where the user account is stored.
4. Select the user account to add the SSH key to and click **Edit**.
5. Click the **Advanced** tab.
6. Select an **SSH Authorized User Key Store** from the list or click **+** to create a new User Key Store. Refer to *Create a User Store*.
7. Select the **SSH Authorized User Keys** that can be used by this user. Use **Shift + Ctrl** to select multiple keys.
8. Click **OK**.
9. Click **Save**.

Edit an Engine User Account

About this task

To edit an engine user account:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** tree.
3. Click the user store to edit.
4. Select the user account to edit and click **Edit**.
5. Edit the user properties.
6. Click **OK**.
7. Click **Save**.

Copy an Engine User Account

About this task

You can copy an engine user account to create a new user account.

To copy an account:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** tree.
3. Click the user store that contains the user account to copy.
4. Select the user account to copy and click **Copy**.
5. Type a name for the account.
6. Edit the user properties as needed.
7. Click **OK**.
8. Click **Save**.

Delete an Engine User Account

About this task

You can delete a user account as needed to maintain the security of Sterling Secure Proxy.

To delete a user account:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** tree.
3. Click the user store that contains the user account to delete.
4. Select the user account to delete.
5. Click **Delete**.
6. Click **Save**.

Notices

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

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

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

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

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

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

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

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

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

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

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

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

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

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

© IBM 2014. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2014.

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

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



Printed in USA