Sterling Secure Proxy

Release Notes

Version 34

Last Updated: 4/28/14

Sterling Secure Proxy

Release Notes

Version 34

Last Updated: 4/28/14

Note
Before using this information and the product it supports, read the information in "Notices" on page 23.

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.

Contents

Release Notes 1
What's New in This Release 1
Support Requests Resolved for this Release 3
System Requirements 3
Sterling Secure Proxy UNIX and Linux System Requirements 3
Hardware Accelerator Board Requirements . . . 5
Hardware Security Module (HSM) Requirements 5
Sterling Secure Proxy Microsoft Windows System Requirements 5
Client Connections Supported 6
Web Browsers Supported by Configuration Manager 7
Server Connections Supported 7
IBM Security Products Supported 8
Cipher Suites Supported 8
Review Resources for UNIX or Linux 8
Special Considerations 9
Security Considerations 9
FIPS-Mode Considerations 10
Adapter Considerations 13
Logging Considerations 14
Configuration Manager (CM) Considerations . . 14
Engine Considerations 15
HSM Considerations 16
Perimeter Server Considerations 16
Single Sign-On Considerations 17
Upgrade Considerations 18
Sterling Connect:Direct Select Version 1.2.01 Considerations 18
Known Restrictions 19
Preparing for Production 20
Configure Sterling Secure Proxy to Interface with a Load Balancer 20
Modify the Node-Level TCP Timeout Value in a Sterling Connect:Direct Node 20
Remove the PKCS11 Security Provider 21

Notices 23

Release Notes

What's New in This Release

IBM® Sterling Secure Proxy version 3.4.1.8 has the following features and enhancements:

Version	Feature or Enhancement
Version 3.4.1.8	Enhances enablement by allowing rest clients within browsers or stand-alone java programs to interact with the IBM Sterling Secure Proxy Configuration Manager while performing create, update, and delete, as well as get Secure Proxy configuration objects and initiate configuration for related tasks. Refer to *IBM Sterling Secure Proxy Configuration Management REST APIs.*
	Adds ability to back out of the IBM Sterling Secure Proxy 3.4.1.8 upgrade. The format of configuration files in the IBM Sterling Secure Proxy Configuration Manager has changed due to the implementation of the new feature to allow the use of multiple SSP engines for one adapter configuration. IBM Sterling Secure Proxy 3.4.1.8 automatically creates a backup of the configuration file prior to starting that you can use to restore to a state prior to the upgrade. This backup does not occur during the upgrade process, but rather 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. Refer to *Restore CM State* in the documentation library for information about restoring or disabling the automatic backup feature.
	The SessionID is now used to associate login results of public key authentication and password-based authentication when using the IBM Sterling External Authentication Server. Audit files are available in the IBM Sterling External Authentication Server by accessing the `[SEAS_INSTALL]/logs/audit` directory.
	Enhances usability by allowing multiple SSP engines for one adapter configuration. Refer to *Sterling Connect:Direct Adapter Configuration - Basic* in the documentation library. Refer to *FTP Adapter Definition - Basic* in the documentation library. Refer to *HTTP Adapter Configuration* in the documentation library. Refer to *SFTP Adapter Configuration - Basic* in the documentation library.
	Enhances onboarding by allowing you to add wildcard entries when configuring entries for trading partner Connect DirectSterling Connect:Direct® nodes. This would allow for one wildcard entry to support many trading partner Connect Direct Nodes. Refer to *Sterling Connect:Direct Netmap Node Definition - Basic* in the documentation library.

Version	Feature or Enhancement
	Adds enhanced usability for Authorized User Key Configuration. SSH Authorized User Keys are sorted in alphabetical order to help you quickly locate the key you want to use.
	Enhances security by providing LDAP security authentication for Admin users using the IBM Sterling External Authentication Server. Refer to *CM User Configuration* in the documentation library.
Version 3.4.1.7	Enhances security by limiting SNodes that specific PNodes can communicate with by creating an Access Control List (ACL) for each PNode. Refer to *Create a Sterling Connect:Direct Netmap*.
	Adds 64-bit JRE support for zLinux (Red Hat and SuSE)
Version 3.4.1.0	Enhances security by providing FIPS 140-2 validated cryptographic modules for the HP-UX PA-RISC, HP-UX Itanium, AIX®, Solaris SPARC UNIX, Red Hat Linux, SuSE Linux, and Microsoft Windows platforms. Refer to *FIPS 140-2 Configuration*.
	Adds PeSIT adapter support for the transmission of messages. Allows users to enable or disable the transmission of messages in the PeSIT adapter policy. Refer to *Block PeSIT command from a PNODE* in the documentation library.
	User documentation is now available on a live IBM website. It provides improved search, by using Google search.
Version 3.3.01	Adds support for Apple Safari 3.2 and 4.0 on Microsoft Windows and Mac OS. Refer to *Client Connections Supported*.
	Adds support for Mozilla Firefox 3.5 on Microsoft Windows and Mac OS. Refer to *Client Connections Supported*.
	Adds 50 more IP addresses to IP address checking for the IBM Sterling Connect:Direct protocol. Refer to *Configure IP Address Checking (Netmap Check)* in the documentation library.
	Adds support for 64-bit JREs for Red Hat 5, AIX 5.3, Solaris 10, SuSE SLES 10, HP-UX 11.23 (PA-RISC and HP Itanium), and Microsoft Windows Server 2008 R2. Refer to *System Requirements*.

Version	Feature or Enhancement
Version 3.3	Adds single sign-on (SSO) support for the SFTP, FTP, and Sterling Connect:Direct protocols. Refer to the following in the documentation library: • *Configure a Single Sign-on Connection to an FTP Server* • *Configure a Single Sign-on Connection to an SFTP Server* • *Configure a Single Sign-on Connection to a Sterling Connect:Direct Server*
	Extended HTTP single sign-on (SSO) support allows trading partners to manage their passwords with a self-service mechanism. This change password functionality supports the recommended Sterling Secure Proxy, IBM Sterling External Authentication Server, and SSO configuration and does not use a third party external portal for password management. It improves interoperability between LDAP and Active Directory. Refer to *Customize the Logon Portal* in the documentation library.
	Improvements to the perimeter server installer. Refer to *Install a Remote Perimeter Server Overview* in the documentation library.
	Adds support for JAAS and RSA SecurID, through Sterling External Authentication Server. Refer to the following on the Sterling External Authentication Server documentation library: • *Create JAAS Authentication Definitions* • *Create RSA Authentication Definitions*

Support Requests Resolved for this Release

No support requests were resolved for Sterling Secure Proxy version 3.4.1.

System Requirements

Sterling Secure Proxy UNIX and Linux System Requirements

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

Sterling Secure Proxy UNIX and Linux Host System Requirements

Sterling Secure Proxy requires the following RAM and disk space requirements on a UNIX or Linux host system:

Component	File Descriptor Size	RAM Minimum	Disk Space Minimum
CM	N/A	512 MB	2 GB

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

Sterling Secure Proxy UNIX or Linux Operating Systems Supported

Sterling Secure Proxy supports the following UNIX and Linux operating systems:

Hardware	Operating System
HP Integrity system with Intel Itanium processor	HP-UX, version 11.23 and 11.31 Sterling Secure Proxy supports 64-bit JRE with this operating system.
HP 9000 (PA-RISC)	HP-UX, version 11.23 and 11.31 Sterling Secure Proxy supports 64-bit JRE with this operating system.
IBM System p5® and IBM Power Systems™	AIX 5L™, version 5.3 AIX 6, version 6.1 AIX 7, version 7.1 Sterling Secure Proxy supports 64-bit JRE with these operating systems.
x64/x86 64-bit	Red Hat Enterprise Linux Advanced Server, version 5 and 6 SuSE SLES, version 10 and 11 Sterling Secure Proxy supports 64-bit JRE with these operating systems.
x64/x86 32-bit	Red Hat Enterprise Linux Advanced Server, version 5 and 6 SuSE SLES, version 10 and 11
Sun SPARC system	Solaris, version 10 Sterling Secure Proxy supports 64-bit JRE with this operating system.
	VMware ESX and VMware vSphere with any UNIX or Linux operating system supported by Sterling Secure Proxy. Consider VMware configuration, administration, and tuning issues. Your VMware administrator must address these. IBM does not provide advice regarding VMware-specific issues.

Hardware	Operating System
x86 (Intel VT-x and AMD-V) 32-bit and 64-bit	Kernel-based Virtual Machine (KVM) with Red Hat Enterprise Linux Advanced Server, version 5.4. Consider KVM configuration, administration, and tuning issues. Your Red Hat administrator must address these. IBM does not provide advice regarding KVM-specific issues
zLinux 64-bit	Red Hat Enterprise Linux Advanced Server, version 5 and 6 SuSE SLES, version 10 and 11 Sterling Secure Proxy supports 64-bit JRE with these operating systems.

Perimeter Server Requirements in UNIX or Linux

You can install and run a remote perimeter server, on a different computer from CM or the engine. The perimeter server supports the UNIX or Linux platforms supported by Sterling Secure Proxy.

Hardware Accelerator Board Requirements

Sterling Secure Proxy supports the cryptographic Sun Crypto Accelerator 10 hardware accelerator board.

Hardware Security Module (HSM) Requirements

Hardware Security Module (HSM) appliance store certificates.

Sterling Secure Proxy supports the following types of HSM:

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

Sterling Secure Proxy Microsoft Windows System Requirements

A JRE is installed with Sterling Secure Proxy.

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

Sterling Secure Proxy Microsoft Windows Host System Requirements

Sterling Secure Proxy requires the following minimum RAM and disk space requirements on a Microsoft Windows system:

Component	RAM Minimum	Disk Space Minimum
CM	512 MB	2 GB

Component	RAM Minimum	Disk Space Minimum
Engine	1 GB	2 GB
Perimeter Server	1 GB	2 GB

Microsoft Windows Operating Systems Supported by Sterling Secure Proxy

Sterling Secure Proxy supports the following Microsoft Windows operating systems:

- Microsoft Windows Server 2003 Enterprise Edition Service Pack 1 (32-bit)
- Microsoft Windows Server 2008 R2 (64-bit). Sterling Secure Proxy supports 64-bit JRE with this operating system.
- Microsoft Windows Server 2012 (64-bit). Sterling Secure Proxy supports 64-bit JRE with this operating system.
- VMware ESX and VMware vSphere with any Microsoft Windows operating system supported by Sterling Secure Proxy. Consider VMware configuration, administration, and tuning issues. Your VMware administrator must address these. IBM does not provide advice regarding VMware-specific issues.

Perimeter Server Requirements on Microsoft Windows

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

- Microsoft Windows 2003 Server Enterprise Edition R2 (32-bit)
- Microsoft Windows 2003 Server Standard Edition R2 (32-bit)
- Microsoft Windows Server 2008 R2 (64-bit)
- Microsoft Windows Server 2012 (64-bit). Sterling Secure Proxy supports 64-bit JRE with this operating system.

Client Connections Supported

Sterling Secure Proxy is compatible with FTP, HTTP, or SSH-SFTP clients that comply with the relevant RFCs.

The following clients have been tested and approved for interoperability with Sterling Secure Proxy:

Client	Protocol
Sterling Connect:Direct for z/OS® version 4.5 or later	Sterling Connect:Direct (SSL, TLS)
Sterling Connect:Direct for UNIX version 3.6.01 or later	Sterling Connect:Direct (SSL, TLS)
Sterling Connect:Direct for Microsoft Windows version 4.2 or later	Sterling Connect:Direct (SSL, TLS)
Sterling Connect:Direct Select version 1.1 or later	Sterling Connect:Direct (SSL, TLS)
Sterling Connect:Direct for i5/OS™ version 3.6.00 or later	Sterling Connect:Direct (SSL, TLS)
Sterling Connect:Direct FTP+ version 1.1.08 or later	Sterling Connect:Direct (SSL, TLS)

Client	Protocol
IBM Sterling B2B Integration version 4.1 or later	FTP (SSL, TLS) HTTP (SSL, TLS) SSH-SFTP Sterling Connect:Direct (SSL, TLS)
IBM Sterling Connect:Enterprise® Secure Client	FTP (SSL, TLS) SSH-SFTP HTTP - WebDAV (SSL)
IBM Sterling Connect:Express for z/OS version 4.2.2 or later	PeSIT
Sterling Connect:Express for UNIX version 1.4.4 or later	PeSIT
Sterling Connect:Express for Microsoft Windows version 3.0.5 or later	PeSIT
Microsoft Internet Explorer 7 and 8	HTTP - myFileGateway
Mozilla Firefox 3.5 or later	HTTP - myFileGateway
Apple Safari 3.2.3 and 4.0 on Microsoft Windows and Mac OS X (10.5.7 and 10.6.0)	HTTP - myFileGateway
cURL 7.12.1 or later with openSSL 0.9.7a or later	FTP (SSL, TLS) HTTP (SSL,TLS)
OpenSSH 4.3p2 or later	SSH
WS_FTP Professional 2007 or later	FTP (SSL, TLS) SSH-SFTP

Web Browsers Supported by Configuration Manager

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

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

Server Connections Supported

Sterling Secure Proxy supports the following server connections:

- Sterling Connect:Direct for z/OS version 4.5.00 or later
- Sterling Connect:Direct for UNIX version 3.6.01 or later
- Sterling Connect:Direct for Microsoft Windows version 4.2 or later
- Sterling Connect:Direct for i5/OS version 3.6.00 or later
- Sterling Connect:Direct Select version 1.1 or later
- Sterling B2B Integrator version 4.3.21 or later
- Sterling B2B Integrator version 5.0.03 or later
- IBM Sterling File Gateway version 1.1 with Sterling B2B Integrator Server version 4.3.22 or later (4.3.x)

- Sterling File Gateway version 2.0 with Sterling B2B Integrator version 5.0.03 or later

IBM Security Products Supported

Sterling Secure Proxy supports the following IBM security products:

- IBM Sterling Certificate Wizard 1.2.03 or later
- Sterling External Authentication Server 2.3.00 or later

Cipher Suites Supported

Sterling Secure Proxy supports the following cipher suites for the Sterling Connect:Direct, FTP, and HTTP protocols:

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

* FIPS Approved

Sterling Secure Proxy supports the following SSH ciphers in FIPS mode:

- AES 256-CBC
- AES 192-CBC
- AES 128-CBC
- 3DES-CBC

Sterling Secure Proxy supports the HMAC-SHA-1 SSH MAC algorithm in FIPS mode.

Review Resources for UNIX or Linux

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

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

Configuration Resource	Sterling Secure Proxy Usage
TCP ports	Use available port numbers, in appropriate port ranges. The following Sterling Secure Proxy components require listening ports: • CM • Jetty web server • Engine

Configuration Resource	Sterling Secure Proxy Usage
Internet Explorer or Firefox	Access the CM logon screen from Microsoft Internet Explorer or Mozilla Firefox.
CM	Install CM in the trusted company zone. You can set up multiple engines with the same CM, but only one CM can be set up to control an engine. CM port handles listen requests from the Jetty web server. The default port number is 62366.
Jetty web server	The Jetty web server is installed when you install CM, and handles listen requests from the web browser. The web server port number is an element specified in the address bar when connecting to the logon screen. The default port number for the Jetty web server is 8443.
Sterling Secure Proxy engine	The engine operates during production, and routes traffic. Install an engine in the DMZ. The default port number is 63366. If you install the engine on a computer with more than one Network Interface Card (NIC), specify the IP bind address of the card associated with that engine. When you define an engine in CM, you identify either the host name or the IP address in the definition. Create only one definition for each engine you install.
Perimeter server	A local perimeter server is installed when you install the engine. It manages communications between the engine and other nodes. You can install a remote perimeter server separately on another computer.
Sterling External Authentication Server	To provide another level of security by authenticating users or certificates, or mapping users, install Sterling External Authentication Server. For more information, refer to the Sterling External Authentication Server documentation library.
Default certificates	To secure communication, Sterling Secure Proxy is configured with default certificates that are exchanged between CM and the engine. Replace these certificates with your own after installation. Refer to *Manage Certificates Between Sterling Secure Proxy Components* on the documentation library.

Special Considerations

This section contains considerations in addition to the procedures contained in Sterling Secure Proxy documents.

Security Considerations

Refer to the following security considerations:

- If you use Sterling External Authentication Server, it uses strong, but limited, cryptography. To use stronger encryption, replace the default jurisdiction policy files with the Unlimited Strength Jurisdiction Policy Files 5.0, available from the

JCE provider. Refer to *Special Considerations* on the Sterling External Authentication Server documentation library.

- If you use Sterling Secure Proxy with Sterling Connect:Direct for UNIX version 3.7.00, you must use the TLS protocol for secure communications.
- Sterling Secure Proxy version 3.4.1 does not support the ENCRYPT.DATA=N feature for Sterling Connect:Direct. If a Sterling Connect:Direct node supports ENCRYPT.DATA=N and connects through Sterling Secure Proxy, a CSP068I warning message is written to the secureproxy.log. Copy steps that specify ENCTRYPT=N fail with a CSPA025E message.

FIPS-Mode Considerations

Certificates used for FIPS-mode sessions must have be signed with a FIPS-approved message digest, such as SHA-1. If a certificate is signed with an unapproved message digest, such as MD5, it will fail session authentication when FIPS mode is enabled. This applies to the entire certificate chain. The certificate is validated in both key certificate files and trusted root certificate files.

Note: When FIPS-mode is enabled, you will not receive an error when you check in or import certificates that are not signed with a FIPS-approved message digest.

Ensure that the certificates that your FIPS-mode trading partners use are signed with the SHA-1 message digest.

SSL Certificates and SSH keys used for FIPS-mode sessions must have a minimum key length of 1024.

Note: Sterling Secure Proxy only uses TLS regardless of the SSL protocol selected in the configuration.

FIPS 140-2 Mode Configuration

Sterling Secure Proxy, which is FIPS 140-2 validated, provides you with a FIPS solution. FIPS-mode operation is available only for the TLS protocol.

When you enable FIPS mode for Sterling Secure Proxy, the list of cipher suites is unchanged; all ciphers are listed. You must select at least one FIPS-approved cipher. For a list of the FIPS-approved cipher suites, see *Cipher Suites Supported*.

If no FIPS-approved ciphers are selected, Sterling Secure Proxy will terminate the SSL connection and log an error message.

When you enable FIPS compliance, the setting is global. All communication sessions must use FIPS-approved cipher suites and certificates. This includes all communication between the following components:

- Configuration Manager and Sterling Secure Proxy Engine
- Sterling Secure Proxy Engine and Sterling External Authentication Server Server
- Sterling External Authentication Server and LDAP
- Sterling External Authentication Server and Sterling B2B Integrator (through a user exit)
- Sterling External Authentication Server GUI and Sterling External Authentication Server

Enabling FIPS-Mode

To enable FIPS-mode, complete the following procedure on the Sterling Secure Proxy engine, the Configuration Manager, and Sterling External Authentication Server:

Procedure

1. Stop the application.
2. From the `<install_dir>/bin` directory, open the `security.properties` file in a text editor.
3. Change the `FIPS_MODE` parameter to true.
4. Save the `security.properties` file.
5. Restart the application.

   Note: In FIPS-mode, Sterling Secure Proxy only uses TLS regardless of the SSL protocol selected in the configuration.

Disabling FIPS-Mode

To disable FIPS mode, complete the following procedure on the Sterling Secure Proxy engine, the Configuration Manager, and Sterling External Authentication Server:

Procedure

1. Stop the application.
2. From the *<install_dir>*/bin directory, open the security.properties file in a text editor.
3. Change the FIPS_MODE parameter to false.
4. Save the security.properties file.
5. Restart the application.

FIPS Certificate List Report

When FIPS is enabled, Sterling Secure Proxy restricts certificate usage to certificates that are FIPS-compliant. If a non-compliant certificate is used while FIPS-mode is enabled, Sterling Secure Proxy produces an error when a secure connection using that certificate is attempted.

The following scripts examine the keystore and truststores for FIPS-compliant certificates and key certificates and generate a report:

- listCerts.sh and listCerts.bat – Sterling Secure Proxy Engine
- listCmCerts.sh and listCmCerts.bat – Sterling Secure Proxy Configuration Manager

The scripts produce a list of certificates that match the criteria specified on the command line.

Script Syntax

The syntax for both scripts is the same:

`<script> [passphrase=<passphrase>] [criteria]`

The *<passphrase>* is the passphrase specified during system installation. If it is not specified, the script prompts for it.

The *criteria* can be a combination of any or none of the following:

Parameter	Description	Default Value
Type=[keyCerts | trustedCerts | both]	The type of certificates to list	both
Fips[=true | false]	List FIPS-compliant or non-compliant certificates	(ignore FIPS criteria)
Expired[=true | false]	List expired/unexpired certificates	(ignore expiration)
ExpireDays=*days*	List certificates expiring in the specified number of days or less	(ignore expiration)
keyAlg=*algorithm*	List certificates using the specified key algorithm	(ignore key algorithm)
keyLength=*bits*	List certificates with public key lengths equal to the specified number of bits	(ignore public key length)
"keyLength < *bits*"	List certificates with public key lengths less than the specified number of bits	(ignore public key length)
"keyLength <= *bits*"	List certificates with public key lengths less than or equal to the specified number of bits	(ignore public key length)
"keyLength > *bits*"	List certificates with public key lengths greater than the specified number of bits	(ignore public key length)
"keyLength >= *bits*"	List certificates with public key lengths greater than or equal to the specified number of bits	(ignore public key length)
"keyLength != *bits*"	List certificates with public key lengths not equal to the specified number of bits	(ignore public key length)

If no criteria is specified, all certificates are listed.

All command line parameters and values are case-insensitive. For example, *fips=true* is equivalent to *Fips=TRUE*.

Note: You can run listCmCerts while the Sterling Secure Proxy Configuration Manager is running.

Script Output

The scripts write all output to the screen. Each certificate entry is displayed in the following format:

```
Certificate name: <name>
Certificate store: <keystore name>
Subject: <subject DN>
Issuer: <issuer DN>
Serial number: <serial number>
Expires on: <expiration date>
Signature algorithm: <algorithm>
Public key algorithm: <algorithm>
Public key length: <number of bits>
```

Example from listCmCerts:

```
========================================================================
Certificate name: factory
Certificate store: C:\cvsprojs\sspfips\dist\conf\system\keystore
```

```
Subject: CN=Sterling Secure Proxy Factory Certificate, OU=Development, O=Sterling Commerce, L=Irving,
         ST=Texas, C=US
Issuer: CN=Sterling Secure Proxy Factory Certificate, OU=Development, O=Sterling Commerce, L=Irving,
         ST=Texas, C=US
Serial number: 1
Expires on: Fri Dec 01 09:54:13 CST 2017
Signature algorithm: SHA1withRSA
Public key algorithm: RSA
Public key length: 1024
================================================================================
Certificate name: factory
Certificate store: C:\cvsprojs\sspfips\dist\conf\system\truststore
Subject: CN=Sterling Secure Proxy Factory Certificate, OU=Development, O=Sterling Commerce, L=Irving,
         ST=Texas, C=US
Issuer: CN=Sterling Secure Proxy Factory Certificate, OU=Development, O=Sterling Commerce, L=Irving,
        ST=Texas, C=US
Serial number: 1
Expires on: Fri Dec 01 09:54:13 CST 2017
Signature algorithm: SHA1withRSA
Public key algorithm: RSA
Public key length: 1024
================================================================================
Certificate name: sspDefaultKeyCert
Certificate store: dfltKeyStore
Subject: EMAILADDRESS=ssp_engine@stercomm.com, CN=ssp engine, OU=Development, O=Sterling commerce,
         L=Irving, ST=Texas, C=US
Issuer: EMAILADDRESS=ssp_engine@stercomm.com, CN=ssp engine, OU=Development, O=Sterling commerce,
        L=Irving, ST=Texas, C=US
Serial number: 0
Expires on: Wed Nov 03 20:59:42 CDT 2032
Signature algorithm: SHA1withRSA
Public key algorithm: RSA
Public key length: 1024
================================================================================
Certificate name: sspDefaultTrustedCert
Certificate store: dfltTrustStore
Subject: EMAILADDRESS=cms@stercomm.com, CN=Configuration Manager, OU=Development, O=Sterling Commerce,
         L=Irving, ST=Texas, C=US
Issuer: EMAILADDRESS=cms@stercomm.com, CN=Configuration Manager, OU=Development, O=Sterling Commerce,
        L=Irving, ST=Texas, C=US
Serial number: 0
Expires on: Wed Nov 03 21:02:28 CDT 2032
Signature algorithm: SHA1withRSA
Public key algorithm: RSA
Public key length: 1024
```

Differences Between listCerts and listCmCerts

The listCmCerts script is the same as the listCerts script, except that in addition to listing certificates in the system keystore and truststore, internal communication certificates, it lists certificates in the CM certificate stores, adapter key certificates and partner trusted certificates.

Adapter Considerations

Refer to the following adapter considerations when configuring or editing an adapter definition:

- If a Sterling Connect:Direct adapter is stopped while one or more sessions are active, the adapter is not restarted until the listen time-out interval expires. To determine if an adapter has active sessions, view the proxy log file.

- If you configure a Sterling Connect:Direct adapter and you do not provide a value for the Ping Response field, the message displayed when a user connects to the host or port has changed to Server Ready. The old message displayed was SecureProxy.
- If you change one of the following values on an SFTP adapter, you must restart the adapter before the change takes effect: listen port, local host key, selected cipher suites, selected MAC suites and selected key exchange algorithms, compression, maximum sessions, session time-out, inbound perimeter server, outbound perimeter server, or external authentication perimeter server.
- If you change the perimeter server mapped to an adapter, you must stop and restart the adapter and the perimeter server before the change is enabled.

Logging Considerations

Refer to the following consideration when viewing log files:

- To check the CM or engine log file on Microsoft Windows, use the Notepad application. WordPad will not open the log file because the file is locked by the application. If you want to use WordPad, copy the file before opening it.
- A connection time-out with a remote node causes a listen time-out exception in an Sterling Secure Proxy log.
- CM uses the log4j tool to log messages. The configuration file that controls the CM log is called `log4j.properties`. By default, the logging level is set to INFO and includes warning, error, and informational messages. You can change the log level to DEBUG but this is not recommended because DEBUG generates a large amount of logs and may affect system performance.
- To configure the CM log to write debug messages, open the `log4j.properties` file located in *install_dir /conf* where *install_dir* is the location of the CM installation.
- To write debug messages for the Jetty web server, add the following statements:

```
# GUI log4j
log4j.logger.sspdashboard=DEBUG,R,stdout
log4j.logger.sspjsf=DEBUG,R,stdout
log4j.logger.com.sterlingcommerce.sspgui.web=DEBUG,R,stdout
log4j.logger.com.sterlingcommerce.csp.gui.web=DEBUG,R,stdout
log4j.logger.com.sterlingcommerce.hadrian.client.gui=DEBUG,R,stdout
```

- To write debug messages for CM, add the following statements:

```
#CM log4j
log4j.logger.com.sterlingcommerce.component.configurator=DEBUG,R,stdout
log4j.logger.com.sterlingcommerce.hadrian.system=DEBUG,R,stdout
log4j.logger.com.sterlingcommerce.component.accepter.csap.impl.AccepterImpl=INFO,R,stdout
log4j.logger.com.sterlingcommerce.component.dispatcher.XmlConversionFilter=INFO,R,stdout
```

Configuration Manager (CM) Considerations

Refer to the following considerations when configuring CM:

- Configure an engine with only one CM. If you use more than one CM, the engine accepts only the CM configuration with a higher version number than its own and with the engine name defined at the first connection.
- If you configure CM to use a port already in use by another application, CM will not start.
- If you upgrade CM from version 3.2 to version 3.3.01 or later, information about Configuration Manager from version 3.2 is maintained in the new installation to allow the CM from version 3.2 to continue to work for both engines. If you want to change the url used to connect to the server in version 3.3.01 or later, click the Advanced menu. Then select the SSO Configuration to modify. Modify the value

in the *Default Landing Page* field. You must also delete the `default.app.url` property defined in the adapter on the Properties tab; otherwise, the property overrides the value defined in the SSO Configuration.

- When you access CM with a browser, a session time-out occurs, if the session is idle for 30 minutes. The Monitoring screen is periodically refreshed, which prevents a session time-out. If the Monitoring screen is displayed as the active application and is not minimized, it does not time out. If you select Monitoring and then minimize the application, a time-out occurs. After a time-out, you may have to login to CM again. Enforce desktop security to prevent unauthorized access to CM.
- When you configure a node in a netmap, complete all required fields before you copy a policy or add a new policy. Otherwise, an error message is generated.
- When you configure an adapter, complete all required fields before you copy or create a netmap. Otherwise, an error message is generated.
- If you are using Mozilla Firefox, do not open two login sessions on a computer; otherwise, the second login page is blank.
- If you use Mozilla Firefox as your browser and you clear the cache while using CM, restart the browser. Otherwise, it may display unpredictable results.
- If you use Mozilla Firefox as your browser and you upgrade Sterling Secure Proxy, clear the cache before you use CM. Otherwise, it may display unpredictable results.
- If you do not store the certificate in the trusted store and you are using Mozilla Firefox, you receive an error message. Adding the CM certificate to the trusted store prevents this error.

Engine Considerations

Refer to the following considerations when configuring or editing an engine definition:

- When you configure an engine, you identify either the host name or the IP address in the definition. Define only one engine definition for each engine you install.
- To run two engines that use different network interface cards (NICs) on one computer, install the engine and use the `configureAcceptor` script to change the IP address and port to listen on. Create an engine definition for each NIC card and make sure that the IP address in the engine definition is the same as the one specified in the script. If you want the engine's local perimeter server to use a specific NIC for adapter traffic, you must edit the `perimeter.properties` file and change the `localmode.interface` parameter to the desired IP address. Refer to the documentation library.
- When the engine is installed on Solaris 10 and you use SSL or TLS, the `AES_256` and `DES40` ciphers fail. To enable these ciphers, refer to *Remove the PKCS11 Security Provider*.
- The default session limit is 20 and allows only about six users with browser sessions. If you use an application such as myFileGateway, Sterling File Gateway, or Dashboard, change this limit.
- If you get the following out of memory error, the engine does not have enough memory to create new threads. This error could result in an abnormal termination.

  ```
  java.lang.OutOfMemoryError: unable to create new native thread
  at java.lang.Thread.start0(Native Method)
  at java.lang.Thread.start (Thread.java:574)
  ```

  Take one or more of the following actions:

– If you have more physical memory on the Sterling Secure Proxy server, install and configure another engine on the server and move some adapters to the new engine. Refer to *Planning and Installation* and *Other Configuration Options* on the documentation library for instructions.
– Decrease the size of the thread pool defined for SFTP adapters. For each adapter definition, change the following parameters to the same value:
  - `sftp_acceptthreads` - Identifies how many threads are available to accept inbound client connections. The default value is 50.
  - `sftp_connectthreads` - Identifies how many threads are available for permanent connect threads. When existing SSH connections make socket connections through port forwarding, these threads manage the asynchronous connection process. The default value is 50.
  - `sftp_xferthreadpools` - Identifies how many threads are available for permanent transfers. This thread asynchronously performs the IO for the socket. The default value is 50.

    Refer to *SFTP Adapter Definition - Properties*in the documentation library for instructions on changing these values.
– Make more memory available for a Java process and increase the maximum number of threads allowed. Refer to your operating system documentation.

HSM Considerations

Refer to the following considerations when configuring or installing an HSM:

- If you run the **`manageKeyCerts -list`** command, as documented in the and it takes a long time to run or appears to lock, perform the following steps to correct the problem:
  1. Open the `install_dir/bin/security.properties` file on the CM computer, where `install_dir` is the location of the CM installation.
  2. Insert the following line: `DEF_KEYSTORE_TYPE=JKS`
  3. Save the file.
- If you upgrade from Sterling Secure Proxy version 3.1.0 and HSM was enabled, you must run the `setupHSM` script after the upgrade to re-enable HSM.

Perimeter Server Considerations

Refer to the following considerations when configuring or editing a perimeter server definition:

- If you change the perimeter server associated with an adapter, stop and restart the adapter to implement the change.
- If you change a more secure perimeter server configuration, you may need to restart the engine that uses the perimeter server before the changes are enabled.
- For a perimeter server installed in a less secure zone, the value of the parameter called restricted in the `remote_perimeter.properties` is set to false by default. Do not change it.
- Before changing a remote perimeter server configuration, first stop all adapters that are using that perimeter server. If you save changes to a perimeter server definition without stopping the adapters that use the perimeter server, errors may occur, the adapters are stopped, and any sessions that are active are stopped. You will be unable to restart these adapters. First stop and restart the remote perimeter server that is used by the adapter and then restart the adapters.

- To change the listen port, outbound port range, or perimeter server that a Sterling Connect:Direct adapter uses, stop the adapter, make the necessary changes, and enable the adapter.
- If you experience a connection failure, refer to the perimeter server log for additional error information.
- Some configuration issues exist when using two NIC cards configured with one remote perimeter server. When configuring client software, be sure to identify the correct IP address based on the definition of the external network interface.

  When configuring the client software, make sure to use the IP address defined for the external network interface. When using the host name, make sure the host name refers to the IP address specified during the network interface configuration. If not, use the IP address only.
- If you change the value of a Sterling External Authentication Server perimeter server in an adapter from local to a more secure configuration, restart the perimeter server or the Sterling Secure Proxy engine.
- The `remote_perimeter.properties` file should not be modified except in special circumstances. If you have modified this file and are upgrading your perimeter server from Sterling Secure Proxy 3.1.01 Perimeter Server to Sterling Secure Proxy 3.4.1 Perimeter Server, the changes are overwritten. If it is necessary to keep the modifications to this file, save the `remote_perimeter.properties` file to a safe location for future reference before upgrading.

Single Sign-On Considerations

Refer to the following considerations when configuring single sign-on for Sterling File Gateway:

- Sterling File Gateway does not support Mozilla Firefox.
- To prevent a token created for one application from accessing a different application, define a unique Sterling External Authentication Server for each application. For example, if you configure myFileGateway and Sterling File Gateway, configure one server for Sterling File Gateway and another one for myFileGateway. Each external user in Sterling File Gateway must then be assigned to their respective Authentication Host (Sterling External Authentication Server).
- If you configure SSO in Sterling Secure Proxy version 3.2, a Signon directory is created to store SSO files. When you upgrade to version 3.3.01 or later, the Signon directory is backed up. A message is displayed at the end of the installation indicating the where the information is backed up. Compare the contents of the backup Signon directory and the newly-installed Signon directory to ensure that all changes are applied to the new Signon directory.
- If you upgrade from version 3.2 to version 3.3.01 or later and you configured single sign-on, you must update the **Fully Qualified host name the Trading Partner connects to** field in the SSO Configurations object. This field did not exist in version 3.2 but it is required in version 3.3.01 or later.
- If you upgrade from version 3.2 to 3.4, unsecure HTTP connections using single sign-on will fail until the SSO configuration is edited so that the SSO Cookie Secure Flag is disabled. To edit the SSO Cookie Secure Flag, you must first define the Fully Qualified Host Name in order to navigate to the Advanced tab, but this will not affect HTTP sessions that use SSO.
- When you connect through Sterling Secure Proxy to the Sterling B2B Integrator Dashboard or the Sterling B2B Integrator B2B console applications, you may experience some UI presentation issues, including Manage Layout functionality and some Calendar pop-ups. In addition, Webstart applications do not function correctly through Sterling Secure Proxy.

Upgrade Considerations

Refer to the following considerations when upgrading:

- When you upgrade Sterling Secure Proxy to version 3.4.1, a new script, `convertKey`, located in the `<install dir>/bin` directory, automatically runs and converts the `sb.enc` file and the `idmb.enc` file to the new version. The `convertKey` script creates a new `idmb2.enc` file to replace the `idmb.enc` file. If the `sb.enc` file already exists, the script overwrites the file.
- After you upgrade Sterling Secure Proxy to version 3.4.1, you can run the `convertKey` script manually, although you do not need to. The system handles the file conversion automatically.

Sterling Connect:Direct Select Version 1.2.01 Considerations

Sterling Connect:Direct Select version 1.2.01 processes zero length messages in a different way than version 1.2.00 and is reported as an issue in the Sterling Secure Proxy testing database. Therefore, it will not work as configured with Sterling Secure Proxy version 3.1.x or later. To use Sterling Connect:Direct Select version 1.2.01 with Sterling Secure Proxy, turn off empty SSL records.

In a Microsoft Windows installation, first determine how the Sterling Secure Proxy engine is running and then modify the appropriate file. To turn off empty SSL records in a Microsoft Windows installation running as a Microsoft Windows service:

1. Open the **SSPEngine$.lax** file in the *install_dir\bin* directory, where *install_dir* is the location of the Sterling Secure Proxy engine.
2. Add the parameter, `-DDisableSSLEmptyRecords=true`, to the following section, as shown:

```
 lax.nl.java.option.additional=-DDisableSSLEmptyRecords=true -server
-Dorg.apache.commons.logging.Log=org.apache.commons.logging.impl.Log4JLogger
-Dcom.sterlingcommerce.cspssh.logging.SSHLogger.logger=logrp
-Dcom.sterlingcommerce.cspssh.stats=false -DvendorFile=vendor.properties
-DPsPlatformFactory=com.sterlingcommerce.csp.perimeter.platform.SSPPlatformFactor
y -Dhadrian.root.dir=.. -Djava.net.preferIPv4Stack=true
```

To turn off empty SSL records in a Microsoft Windows installation running as a console application:

1. Open the `startEngine.bat` file.
2. Add the parameter, `qq=-DDisableSSLEmptyRecords=true`, to the following section, as shown:

```
set qq=-DDisableSSLEmptyRecords=true
"C:\installSSP\gabuild\jre\bin\java.exe" %qq% -server
```

To turn off empty SSL records in a UNIX or Linux installation:

1. Open the `startEngine.sh` file.
2. Add the parameter, `QQ=-DDisableSSLEmptyRecords=true`, to the following section, as illustrated:

```
QQ=-DDisableSSLEmptyRecords=true
"if test ! -s "${DIST_DIR}/conf/system/sb.enc"
then
"${JAVA_HOME}/bin/java" ${QQ} -server
-Xmx${MAXHEAP} -cp ${CLASSPATH} ${F} ${B} ${C}
-DvendorFile=vendor.properties
-DPsPlatformFactory=com.sterlingcommerce.csp.perimeter.platform.SSPPlatformFactor
y -Dhadrian.root.dir=${DIST_DIR} -Djava.net.preferIPv4Stack=true
com.sterlingcommerce.hadrian.Main
else
```

```
nohup "${JAVA_HOME}/bin/java" ${QQ} -server
-Xmx${MAXHEAP} -cp ${CLASSPATH} ${F} ${B} ${C}
-DvendorFile=vendor.properties
-DPsPlatformFactory=com.sterlingcommerce.csp.perimeter.platform.SSPPlatformFactor
y -Dhadrian.root.dir=${DIST_DIR} -Djava.net.preferIPv4Stack=true
com.sterlingcommerce.hadrian.Main >startEngine.out &
```

Known Restrictions

Sterling Secure Proxy version 3.4.1 has the following restrictions:

- The AES cipher suites do not work with Microsoft Internet Explorer 7.
- If you use Apple Safari 4.0.4 with Sterling Secure Proxy, you must add the following line to the startEngine script: `"-Dcom.certicom.tls.record.maximumPaddingLength=0"`.
- The only cipher suites supported with Apple Safari 4.0.4 are: TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_RC4_128_MD5, TLS_RSA_WITH_DES_CBC_SHA, TLS_RSA_EXPORT_WITH_RC4_40_MD5, and TLS_RSA_WITH_3DES_EDE_CBC_SHA.
- If you configure an SFTP adapter to use JCE with the property sftp_jce_enable=true, only the AES256-CBC, AES192-CBC, AES128-CBC, ARCFOUR, ARCFOUR-128, ARCFOUR-256, 3DES-CBC,and BLOWFISH-CBC ciphers and the HMAC-SHA1 and HMAC-MD5 MACs are supported.
- The arcfour SSH ciphers `ARCFOUR. ARCFOUR-128`. and ARCFOUR-256 only work with JCE.
- If you modify the property called `sftp_jce_enable` in an SFTP adapter, you must restart the engine before the change is enabled.
- Using JCE for SFTP must be consistent across all SFTP adapters running on an engine. You cannot mix JCE and non-JCE SFTP adapters.
- The only cipher suites supported with SSLv2 are: TLS_RSA_WITH_RC4_128_MD5 and TLS_RSA_EXPORT_WITH_RC4_40_MD5.
- When using WS_FTP Professional, only version 2007 or later is supported.
- If problems occur with WS_FTP Professional version 2007, upgrade to version 2007.11.12 or later.
- When connecting to Sterling Secure Proxy using WS_FTP Professional for SSH-SFTP, if the password and public key are both required for authentication, configure WS_FTP Professional to present the public key first or the connection will fail.
- If you use Mozilla Firefox with Sterling Secure Proxy, do not open multiple tabs. Opening multiple tabs may cause unexpected results.
- If you use Apple Safari and Microsoft Internet Explorer on the same workstation to access Sterling File Gateway, you must clear the browser cache on both browsers when you switch from one browser to the other.
- Enhanced failover support, RSA SecurID, single sign-on, and logon portal functionality do not apply to the PeSIT protocol.
- Sterling Connect:Direct control block encryption–Sterling Secure Proxy Connect:Direct Adapter does not support disabling data encryption and encrypting only the control block information contained in Function Management Headers (FMHs), such as a user ID, password, and filename. Sessions that require disabling data encryption will fail.
- If you use an Eracom HSM device and enable FIPS mode, you may encounter a delay completing SSL handshakes.

Preparing for Production

Configure Sterling Secure Proxy to Interface with a Load Balancer

If you configure a Sterling Connect:Direct or HTTP environment, you can define an HTTP ping response to perform a health check, such as when using a load balancer tool. If you define these options, you can create a configuration for a BigIP connection and perform different levels of security checks.

Following are some possible scenarios for configuring tools like BigIP to monitor the status of the HTTP or Sterling Connect:Direct proxy adapter. The scenarios are presented in increasing order of security.

- Simple health check - In this scenario the monitoring agent makes a TCP connection to the listening port of the adapter and immediately disconnects. A successful connection indicates that the adapter is running. This health check has the least effect on performance.
- Medium health check - The monitoring agent sends an HTTP GET request with a specific URI. If the information matches the ping URI specified in the HTTP Reverse Proxy adapter, the adapter responds with the configured ping response. This allows the monitoring agent to determine that the adapter is alive and responsive.
- Comprehensive health check - The request from the monitoring agent is sent all the way to the Sterling B2B Integrator HTTP server using the HTTP proxy adapter. To allow this connection, either the URI of the GET request sent by the monitoring agent should not match the ping URI specified in the adapter configuration, or the ping URI in the adapter configuration should be empty. In either case, the adapter passes the request to the Sterling B2B Integrator server or to another Sterling Secure Proxy in the chain, depending upon the configuration. It is the responsibility of the monitoring agent and the backend server to ensure that the ping URI and response match.

Modify the Node-Level TCP Timeout Value in a Sterling Connect:Direct Node

About this task

TCP timeout identifies the maximum number of seconds Sterling Secure Proxy waits for a TCP buffer when communicating with a Sterling Connect:Direct node. For inbound sessions, this field is used after the first buffer is received from the remote node and the connecting node is identified. For outbound sessions from the proxy, this field is used from the start of the session. The default value is 90 seconds. Use this procedure to modify the TCP timeout value.

To modify the TCP timeout value in a Sterling Connect:Direct node:

Procedure

1. From the Configuration navigation panel, click **Netmap** to expand the list of available netmaps.
2. Click the netmap where the node is defined.
3. Click the radio button beside the node you want to modify and click **Edit**.
4. Click the **Advanced** tab.
5. Change the value in the **TCP timeout** field.

6. Click **OK**.
7. Click **Save**.

Remove the PKCS11 Security Provider

About this task

If the Sterling Secure Proxy engine is installed on Solaris 10 and you need to communicate using SSL or TLS with the AES_256 or DES40 cipher, you must remove the PKCS11 security provider from the java.security file.

Use the following procedure to remove the PKCS11 security provider:

Procedure

1. Open the *install_dir*/jre/lib/security/java.security file where *install_dir* is the directory where SSP is installed.

   The first two entries in the file are displayed below:

```
security.provider.1=sun.security.pkcs11.SunPKCS11 ${java.home} /lib/security/sunpkcs11-solaris.cfg
security.provider.2=sun.security.provider.Sun
```

2. Comment out the first entry for security.provider.1.
3. Make a copy of the second entry and renumber it to security.provider.1. Following is a sample of the new line:

   ```
   security.provider.1=sun.security.provider.Sun
   ```

   Leave the second entry as security.provider.2=sun.security.provider.Sun. Although the first two entries are the same, you do not have to renumber all security provider lines.
4. Save and close the java.security file.

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® 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.

Product Number: 5725-D03

Printed in USA