Sterling Connect:Direct Secure Plus for z/OS

Implementation Guide

Version 5.2

Last updated: April 2014

Sterling Connect:Direct Secure Plus for z/OS

Implementation Guide

Version 5.2

Last updated: April 2014

Note

Before using this information and the product it supports, read the information in "Notices" on page 99.

This edition applies to Version 5 Release 2 of IBM Sterling Connect:Direct and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Sterling Connect:Direct Secure Plus for z/OS Overview

IBM® Sterling Connect:Direct® Secure Plus for z/OS® provides enhanced security for IBM Sterling Connect:Direct. It uses cryptography to secure data transmission with the security protocol you choose.

Configuration for a Secure Connection between z/OS and OpenVMS Nodes

This topic provides a detailed example for defining a remote node record in both a Sterling Connect:Direct Secure Plus for z/OS parameter file and a Sterling Connect:Direct Secure Plus for OpenMVS parameter file to set up a secure connection between the two nodes.

In this example, two nodes have set up records in their respective Sterling Connect:Direct Secure Plus parameter files:

- The Sterling Connect:Direct Secure Plus for z/OS node is named Q1A.ZOA.V4700 and is defined in a remote node record in the Sterling Connect:Direct Secure Plus for OpenVMS parameter file and in the network map.
- The Sterling Connect:Direct for OpenVMS node is named Q1A.ITAN.V3400 and is defined in a remote node record in the Sterling Connect:Direct Secure Plus for z/OS parameter file and the network map.

The Sterling Connect:Direct Secure Plus records are defined to allow each node to act as either the client (PNODE) or the server (SNODE), depending on which one initiates the session.

Records Settings in the z/OS Parameter File

In the Sterling Connect:Direct Secure Plus for z/OS parameter file, the local node record has the following settings:

- **Y** in the **Override** field
- **N** in the **Enable TLS** (or **SSL**) field
- **N** in the **Client Auth** field

The settings for the local node record have the following effects: Disabling Sterling Connect:Direct Secure Plus in the local node record means that the protocol and other settings for secure connections must be defined in each remote node record; enabling the **Override** parameter allows settings in remote node records to override those in the local node record; client authentication is not enabled for all remote nodes.

The remote node record defined for the OpenVMS node named Q1A.ITAN.V3400 in the z/OS Sterling Connect:Direct Secure Plus parameter file has the following settings:

- **Node Identification** is Q1A.ITAN.V3400. This value must correspond to the node name specified in the Sterling Connect:Direct Secure Plus for z/OS network map.
- **Override** is not applicable in the remote record and defaults to **N**.

- The TLS protocol is enabled for sessions to connect to this node.
- This OpenVMS node will not request client authentication of z/OS nodes with which it communicates.

The following **Secure+ Create/Update Panel - SSL/TLS Parameters** panel for Sterling Connect:Direct Secure Plus for z/OS illustrates the settings for the OpenVMS node named Q1A.ITAN.V3400 and commentary on the values set for the parameters.

The information in the bottom half of the screen pertains to the key certificate for the z/OS node. The OpenVMS remote node record for the z/OS node has enabled client authentication, as shown in Records Settings in the z/OS Remote Node Record for OpenVMS Parameter File. Therefore, when the z/OS node initiates the session, the OpenVMS node (the server) requests that the client send its ID certificate so that the OpenVMS node can authenticate the client by validating the key certificate defined on this panel (mfcert_a) against the key certificate specified in the Root Certificate file field (mfcert_a.txt) of the z/OS remote node record in the Sterling Connect:Direct Secure Plus for OpenVMS parameter file, as illustrated in Records Settings in the z/OS Remote Node Record for OpenVMS Parameter File. When the z/OS node is the server, it must send its public key, which is stored in the mfcert_a file, to the OpenVMS node during server authentication.

In this example, the z/OS key certificate resides in the default key database defined for the local node (indicated by *). If the certificate location does not default to the local node, the remote node definition must point to the absolute path. Definitions for the default key database are stored in the local node record. Certificate information identifying the z/OS node to remote nodes and remote nodes to the z/OS node is stored in the GSKKYMAN database. When certificates are exchanged, trading partners send the ID certificate portion of their keys to each other. In the z/OS system, this information must be imported into the GSKKYMAN database.

Note: In the OpenVMS system, fully qualified paths are always required for file locations.

The TLS ciphers previously selected are shown using the standard two-byte IBM convention for displaying ciphers (352F04050A09030601). The systems negotiate a cipher suite common to both the z/OS and OpenVMS nodes to encrypt information during the handshake and when actual data is being transmitted.

Records Settings in the z/OS Remote Node Record for OpenVMS Parameter File

The following example shows the remote node record that defines the Sterling Connect:Direct for z/OS node named Q1A.ZOA.V4700. The OpenVMS network map contains an adjacent (remote) node record with the exact same name.

```
                Node Name:    Q1A.ZOS.V4700
                Node type:    R
 1.              Protocol:    T
 2.  Client Authentication:    y
 3. Authentication timeout:    100
 4.Certificate common name:    mfsscert_a
 5.  Root Certificate file:    disk$data:[qaitan.q1a]mfcert_a.txt
 6.   Key Certificate file:    disk$data:[qaitan.q1a]2048sskeycert.txt
 7.            Passphrase:    ****
 8.         Cipher suites:  EXP_RC4_MD5,RC4_MD5,RC4_SHA,EXP_RC2_CBC_MD5,IDEA_CBC_SHA,
EXP_DES_CBC_SHA,DES_CBC_SHA,DES_CBC3A
```

When the OpenVMS node is the server, it requests that the client authenticate itself (Client Authentication = Y) and send its certificate common name (mfsscert_a) for an extra layer of authentication. The public key information for the z/OS node is stored in the Root Certificate file named mfcert_a.txt; its location is specified (disk$data:[qaitan.qla]).

The key certificate file contains the information that identifies the OpenVMS node to other nodes (disk$data:[qaitan.q1a]2048sskeycert.txt). In order for the OpenVMS system to access its private key to send information to the other node, the passphrase must be entered as well. The z/OS node validates this key certificate information against the information stored in its GSKYYMAN database.

The cipher suites are listed in the order of preference, and the first one that matches a cipher suite defined for the other node is used to establish a session.

Security Concepts

Cryptography is the science of keeping messages private. A cryptographic system uses encryption keys between two trusted communication partners. These keys encrypt and decrypt information so that the information is known only to those who have the keys.

There are two kinds of cryptographic systems: *symmetric-key* and *asymmetric-key*. Symmetric-key (or secret-key) systems use the same secret key to encrypt and decrypt a message. Asymmetric-key (or public-key) systems use one key (public) to encrypt a message and a different key (private) to decrypt it. Symmetric-key systems are simpler and faster, but two parties must somehow exchange the key in a secure way because if the secret key is discovered by outside parties, security is compromised. Asymmetric-key systems, commonly known as public-key systems, avoid this problem because the public key may be freely distributed, but the private key is never transmitted.

Cryptography provides information security as follows:

- **Authentication** verifies that the entity on the other end of a communications link is the intended recipient of a transmission.
- **Non-repudiation** provides undeniable proof of origin of transmitted data.
- **Data integrity** ensures that information is not altered during transmission.
- **Data confidentiality** ensures that data remains private during transmission.

  Sterling Connect:Direct Secure Plus enables you to implement multiple layers of security. Select from two security protocols to use to secure data during electronic transmission: Transport Layer Security (TLS) or Secure Sockets Layer protocol (SSL). Depending on the security needs of your environment, you can also validate certificates using the IBM® Sterling External Authentication Server application.

Sterling Connect:Direct also allows you to implement security and encryption as appropriate for your environment. For example, if your company has a universal policy you want to enforce, elect to encrypt all files at all times. To provide flexibility, allow a trading partner to override security settings by specifying any of the following conditions:

- Turning Sterling Connect:Direct Secure Plus for z/OS on or off for a particular session
- Specifying one or more ciphers for encryption instead of the default cipher suites
- Encrypting only the control block information contained in Function Management Headers (FMHs), such as a user ID, password, and filename, instead of the files being transferred if performance is a factor.

Security Protocols

Before you configure Sterling Connect:Direct Secure Plus for z/OS, determine the protocol you and your trading partners will use to secure communications sessions. For planning information, see SSL and TLS Prerequisites.

Transport Layer Security Protocol and Secure Sockets Layer Protocol

The TLS and the SSL protocols use certificates to exchange a session key between the node that initiates the data transfer process (the primary node, or PNODE) and the other node that is part of the communications session (the secondary node, or the SNODE). A certificate is an electronic document that associates a public key with an individual or other entity. It enables you to verify the claim that a given public key belongs to a given entity. Certificates can be self-issued or issued by a certificate authority (see Self-Signed and CA-Signed Certificates for details). When a certificate authority (CA) receives an application for a certificate, the CA validates the applicant's identity, creates a certificate, and then signs the certificate. You use the CA signature to authenticate CA-issued trading partner certificates. A certificate authority issues and revokes CA-issued certificates. Self-signed certificates are created and issued by the owner of the certificate, who must export the certificate in order to create a trusted root for the certificate and supply the trusted root of the self-signed certificate to the partner in a connection.

Levels of Security

The TLS and SSL protocols provide three levels of security:

- During the first level of authentication called server authentication, the site initiating the session (PNODE) requests a certificate from its trading partner (SNODE), during the initial handshake. The SNODE returns its ID certificate (read from its key certificate file) and the PNODE authenticates it using one or more trusted root certificates stored in a trusted root certificate file (the name and location of which are specified in the remote node record for that specific trading partner in the PNODE's Sterling Connect:Direct Secure Plus parameter file). Root certificates are signed by a trusted source—either a public certificate authority, such as Thawte, or by the trading partner acting as its own CA. If the ID certificate from the SNODE cannot be validated using any root certificate found in the trusted certificate file, or if the root certificate has expired, the

PNODE terminates the session. Sterling Connect:Direct writes entries to the statistics logs of both nodes, and the session is aborted.

- The second level of authentication is optional and is called client authentication. If this option is enabled in the SNODE's Sterling Connect:Direct Secure Plus parameter file definition for the PNODE, the SNODE will request a certificate from the PNODE, and authenticate it using the information in its trusted root certificate file. If this authentication fails, the SNODE terminates the session and Sterling Connect:Direct writes information about the failure to the statistics logs of both nodes.

  In order to perform this security check, the trading partner must have a key certificate file available at its site and the Sterling Connect:Direct server must have a trusted root file that validates the identity of either the Certificate Authority (CA) who issued the key certificate or the entity that created the certificate, if it is self-signed.
- The third authentication level is also optional and consists of validating the PNODE's certificate common name. When the security administrator enables client authentication, they can also specify the common name (CN) contained in the PNODE's ID certificate. During client authentication, the SNODE compares the common name it has specified for the PNODE in its Sterling Connect:Direct Secure Plus parameter file with the common name contained in the certificate sent by the PNODE. If the compare fails, that is, the information is not identical, the SNODE terminates the session, and Sterling Connect:Direct writes information about the failure to the statistics logs of both nodes.

Areas of Security

The SSL and TLS protocols provide data security in the following areas:

- Authentication—Certificates used in the SSL or TLS session are digitally signed by a CA through an established procedure to validate an applicant's identity or digitally signed by the certificate owner-issuer. The SSL or TLS protocol validates the digital signature of the certificate being used.
- Proof of data origin and data integrity validation—The certificate provides proof of origin of electronic transmission and encryption validates data integrity. Message digest (hashing) and encrypting the message digest ensure that the data is not altered.
- Data confidentiality—Cipher suites encrypt data and ensure that the data remains confidential. The sending node converts sensitive information to an unreadable format (encryption) before it is sent to the receiving node. The receiving node then converts the information back into a readable format (decryption).

TLS Features

Both the SSL protocol and the TLS protocol manage secure communication in a similar way. However, TLS provides a more secure method for managing authentication and exchanging messages, using the following features:

- While SSL provides keyed message authentication, TLS uses the more secure Key-Hashing for Message Authentication Code (HMAC) to ensure that a record cannot be altered during transmission over an open network such as the Internet.
- TLS defines the Enhanced Pseudorandom Function (PRF), which uses two hash algorithms to generate key data with the HMAC. Two algorithms increase

security by preventing the data from being changed if only one algorithm is compromised. The data remains secure as long as the second algorithm is not compromised.

- While SSL and TLS both provide a message to each node to authenticate that the exchanged messages were not altered, TLS uses PRF and HMAC values in the message to provide a more secure authentication method.
- To provide more consistency, the TLS protocol specifies the type of certificate that must be exchanged between nodes.
- TLS provides more specific alerts about problems with a session and documents when certain alerts are sent.
- If you are required to have a FIPS 140-2-validated solution, a FIPS-mode of operation is available in Sterling Connect:Direct for the TLS protocol.

Planning for System SSL in FIPS Mode

Beginning with IBM z/OS Version 1 Release 11, System SSL provides the capability to execute securely in FIPS 140-2 mode. To this end, System SSL can run in either "FIPS mode" or "non-FIPS mode." By default, System SSL runs in non-FIPS mode and must be configured to run in FIPS mode. While executing in FIPS mode, System SSL continues to take advantage of the CP Assist for Cryptographic Function (CPACF) when it is available. System SSL checks for the application of certain restrictions. For information about System SSL in FIPS Mode, see *z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08*.

Sterling Connect:Direct for z/OS can request for System SSL to be placed into FIPS mode with the appropriate System SSL API calls. The Sterling Connect:Direct for z/OS FIPS initialization parameter attempts to place System SSL into FIPS mode. This initialization parameter instructs Sterling Connect:Direct FTP+ to initiate FIPS mode by using the appropriate System SSL API call, gsk_fips_state_set. Sterling Connect:Direct FTP+ issues the SITA195I message to indicate a successful request. However, if the request is not successful, Sterling Connect:Direct FTP+ terminates until the problem is resolved. For more information about FIPS-mode errors, see Chapter 12, “Troubleshooting,” on page 79. For more information about the FIPS initialization parameter, see *IBM Sterling Connect:Direct for z/OS Administration Guide*. For more information about special considerations for FIPS-mode, see *IBM Sterling Connect:Direct for z/OS Release Notes.*

Secure Protocol and Security Mode

Connect:Direct for z/OS 5.2.00 and SecurePlus have implemented support for several new Secure protocols including SSLv3.0, TLSv1.0, TLSv1.1 and TLSv1.2 and a new mode called Security Mode. The Secure protocol and the Security mode work hand in hand and the mode will apply further restrictions as to Secure protocol can be used.

The SecurePlus Admin tool, SPAdmin, will allow multiple protocols to be enabled and depending on the needs and settings of the Remote Connect:Direct negotiate to the highest supported Secure protocol. For example, if the Local parameter record enables all Secure protocols if the Remote Connect:Direct has enabled TLSv1.2 then TLSv1.2 will be selected. However, if the Remote Connect:Direct has not enabled TLSv1.2 or does not support TLSv1.2 then the highest Secure protocol that Remote does support will be selected.

The Security mode restricts not only which Secure protocol that can be enabled and/or selected, if may also restrict cipher suite selection, certificate key strength and encryption algorithms. SPAdmin provides field level help for each Secure protocol and Security mode by pressing PF1 key while the cursor is positioned on the field.

FIPS mode requires the Secure protocol to be a minimum of TLSv1.0 and disables the use of SSLv3.0. FIPS mode also disables or ignores certain cipher suites.

SP800-131a in Transition Mode

SP800-131a is implemented in 2 modes, transition vs. strict mode. With SP800-131a Transition mode, the follow is recommended by is not enforced by SecurePlus:

- FIPS mode must be enabled - DES and RC2 cipher algorithms are disabled
- MD5 signature algorithms are disabled
- RSA and DSA certificates with key length less than 1024-bits are disabled
- Support for TLSV1.2 is enabled
- SSLV3, TLSV1.0 and TLSV1.1 are allowed but should be disabled
- Non-compliant TLS cipher suites are disabled

SP800-131a in Strict Mode

SP800-131a Strict mode will enforce these restrictions and if any parameter is outside of those parameter the SSL/TLS handshake will fail:

- FIPS mode must be enabled - DES, RC2 and two-key Triple DES cipher algorithms are disabled
- MD5 and SHA1 signature algorithms are disabled
- RSA and DSA certificates with key length less than 2048-bits are disabled
- EC certificates with key length less than 224-bits are disabled
- Protocol must be TLSV1.2
- SLV3, TLSV1.0, and TLSV1.1 are disabled

NSA Suite B 128bit Mode

The following restrictions apply to NSA Suite B in 128bit mode is enabled and further restricted in 192bit mode:

- Certificates must be ECC using elliptic curve secp256r1 or secp384r1
- Protocol must be TLSV1.2, all others are disabled
- Cipher algorithm must be AES-128
- Key exchange algorithm must be ECDH
- Digital signature algorithm must be ECDSA
- Hashing algorithm must be SHA256
- Cipher suites allowed for NSA Suite B 128 bit are:
  - TLS_ECDHE_ECDSA_W_AES_128_CBC_SHA256 (C023)
  - TLS_ECDHE_ECDSA_W_AES_128_GCM_SHA256 (C02B)

NSA Suite B 192bit Mode

- Certificates must be ECC using elliptic curve secp384r1
- Protocol must be TLSV1.2, all others are disabled
- Cipher algorithm must be AES-256
- Key exchange algorithm must be ECDH
- Digital signature algorithm must be ECDSA

- Hashing algorithm must be SHA384
- Cipher suites allowed for NSA Suite B 192 bit are
  - TLS_ECDHE_ECDSA_W_AES_256_CBC_SHA384 (C024)
  - TLS_ECDHE_ECDSA_W_AES_256_GCM_SHA384 (C02C)

Secure Cipher Suite

The Secure protocol and the Security mode affect which cipher suite is selectable during an SSL handshake. The order in which the SPAdmin tool presents the cipher suite is dependent on the Secure protocol and Security mode that is enabled. The table below illustrates which cipher suites are valid for each protocol and mode. The SPAdmin tool allows you to enable or select ten from the list. However, during the SSL handshake any selection that is not valid for the Secure protocol and Security mode selected are ignored. At least one cipher must be valid for the protocol and mode enabled in both the PNODE and SNODE list.

Cipher ID	Name	Deprecated	TLS 1.2	TLS 1.1	TLS 1.0	SSL 3.0	FIPS140-2 >= TLS1.0	SP800 - 131A TLS 1.2 Only	Suite B 128 TLS 1.2 Only	Suite B 192 TLS 1.2 Only	Kx	Au	Enc	Bits	Mac	Mac Bits	Mode Strength
0x0C02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384		X				X	X	X	X	ECDHE	ECDSA	AES_256_GCM	256	SHA384	384	2
0x0C024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		X				X	X			ECDHE	ECDSA	AES_256_CBC	256	SHA384	384	1
0x0C00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		X				X	X			ECDHE	ECDSA	AES_256_CBC	256	SHA	160	1
0x0C02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256		X				X	X	X		ECDHE	ECDSA	AES_128_GCM	128	SHA256	256	2
0x0C023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		X				X	X			ECDHE	ECDSA	AES_128_CBC	128	SHA256	256	1
0x0C009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		X				X	X			ECDHE	ECDSA	AES_128_CBC	128	SHA	160	1
0x0C007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA		X								ECDHE	ECDSA	RC4_128	128	SHA	160	0
0x0C008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA		X				X	X			ECDHE	ECDSA	3DES_EDE_CBC	168	SHA	160	1
0x0C006	TLS_ECDHE_ECDSA_WITH_NULL_SHA		X								ECDHE	ECDSA	NULL	0	SHA	160	0
0x0C030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		X				X	X			ECDHE	RSA	AES_256_GCM	256	SHA384	384	2
0x0C028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		X				X	X			ECDHE	RSA	AES_256_CBC	256	SHA384	384	1
0x0C014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		X				X	X			ECDHE	RSA	AES_256_CBC	256	SHA	160	1
0x0C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256		X				X	X			ECDHE	RSA	AES_128_GCM	128	SHA256	256	2
0x0C027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		X				X	X			ECDHE	RSA	AES_128_CBC	128	SHA256	256	1
0x0C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		X				X	X			ECDHE	RSA	AES_128_CBC	128	SHA	160	1
0x0C011	TLS_ECDHE_RSA_WITH_RC4_128_SHA		X								ECDHE	RSA	RC4_128	128	SHA	160	0
0x0C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA		X				X	X			ECDHE	RSA	3DES_EDE_CBC	168	SHA	160	1
0x0C010	TLS_ECDHE_RSA_WITH_NULL_SHA		X								ECDHE	RSA	NULL	0	SHA	160	0
0x0009D	TLS_RSA_WITH_AES_256_GCM_SHA384		X				X	X			RSA	RSA	AES_256_GCM	256	SHA384	384	2
0x0003D	TLS_RSA_WITH_AES_256_CBC_SHA256		X				X	X			RSA	RSA	AES_256_CBC	256	SHA256	256	1
0x00035	TLS_RSA_WITH_AES_256_CBC_SHA		X	X	X	X	X	X			RSA	RSA	AES_256_CBC	256	SHA	160	1
0x0009C	TLS_RSA_WITH_AES_128_GCM_SHA256		X				X	X			RSA	RSA	AES_128_GCM	128	SHA256	256	2
0x0003C	TLS_RSA_WITH_AES_128_CBC_SHA256		X				X	X			RSA	RSA	AES_128_CBC	128	SHA256	256	1
0x0002F	TLS_RSA_WITH_AES_128_CBC_SHA		X	X	X	X	X	X			RSA	RSA	AES_128_CBC	128	SHA	160	1
0x00005	TLS_RSA_WITH_RC4_128_SHA		X	X	X	X					RSA	RSA	RC4_128	128	SHA	160	0
0x00004	TLS_RSA_WITH_RC4_128_MD5			X	X	X					RSA	RSA	RC4_128	128	MD5	128	0
0x0000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA		X	X	X	X	X	X			RSA	RSA	3DES_EDE_CBC	168	SHA	160	1
0x00009	TLS_RSA_WITH_DES_CBC_SHA			X	X	X					RSA	RSA	DES_CBC	56	SHA	160	1
0x0003B	TLS_RSA_WITH_NULL_SHA256		X								RSA	RSA	NULL	0	SHA256	256	0
0x00002	TLS_RSA_WITH_NULL_SHA		X	X	X	X					RSA	RSA	NULL	0	SHA	160	0
0x00001	TLS_RSA_WITH_NULL_MD5			X	X	X					RSA	RSA	NULL	0	MD5	128	0
0x00000	TLS_RSA_WITH_NULL_NULL		X	X	X	X					RSA	NULL	NULL	0	NULL	0	0
0x00006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	X			X	X					RSA_EXPORT	RSA_EXPORT	RC2_CBC_40	40	MD5	128	1
0x00003	TLS_RSA_EXPORT_WITH_RC4_40_MD5	X			X	X					RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5	128	0
0x00062	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	X			X	X					RSA_EXPORT 1024	RSA_EXPORT 1024	DES_CBC	56	SHA	160	1
0x00064	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	X			X	X					RSA_EXPORT 1024	RSA_EXPORT 1024	RC4_56	56	SHA	160	0

Sterling Connect:Direct Access to System Resources for SSL or TLS

Before you can configure the Sterling Connect:Direct Secure Plus records to use the SSL or TLS protocol, you must ensure that the Sterling Connect:Direct components have access to the resources listed in the following table.

Component	Access to Resource
Sterling Connect:Direct	z/OS UNIX System Services or POSIX environment, must be installed and set up for Sterling Connect:Direct access.
	Access to the following APF-authorized IBM system libraries through the STEPLIB or LINKLST: • CEE.SCEERUN and CEE.SCEERUN2 (language environment) • CBC.SCLBDLL (C/C++ environment) • SYS1.SIEALNKE for IBM z/OS (System SSL Environment)
	For end-user server certificates with ICSF private key type: • The ICSF application must be running on the same environment as Sterling Connect:Direct. • The Crypto Hardware device and the ICSF application must be running and accessible by Sterling Connect:Direct.
Sterling Connect:Direct User ID (under which DTF runs)	Address space uses the maximum sockets (and other TCP/IP configurations) assigned by the UNIX System Services
	OMVS access
	A default UNIX directory
	UPDATE authority to the BPX.SERVER facility
SSL/TLS	Access to key database or key ring as follows: • gskkyman key database • RACF®, CA-ACF2, or CA-Top Secret key ring
	Access to the following APF-authorized IBM system library through the STEPLIB or LINKLST: • SYS1.SIEALNKE for IBM z/OS (System SSL Environment)
	Permission to read Sterling Connect:Direct key ring that is created using RACDCERT, as follows: • Define the IRR.DIGTCERT.LIST and IRR.DIGTCERT.LISTRING resources with universal access of **None**. • Grant the Sterling Connect:Direct User ID read access to the IRR.DIGTCERT.LIST and IRR.DIGTCERT.LISTRING resources in the FACILITY class. • Activate the FACILITY general resource class. • Refresh the FACILITY general resource class.

Component	Access to Resource
Sterling Connect:Direct User ID key database or key ring	Verification of other certificates requires access to the trusted root certificate of either: • A trusted CA certificate • Copy of a self-signed trusted certificate without private key
Sterling Connect:Direct Secure Plus Parameter file	Your node must have a remote node record in the parameter file of each of your trading partners that will use secure connections.

Sterling Connect:Direct Secure Plus Tools

Sterling Connect:Direct Secure Plus for z/OS consists of three components: the Administration Tool (Admin Tool), the parameter file, and the access file. The following sections describe these components and their purpose within Sterling Connect:Direct Secure Plus for z/OS.

Admin Tool

The Admin Tool enables you to configure and maintain the Sterling Connect:Direct Secure Plus environment. The Admin Tool is the only interface for creating and maintaining the Sterling Connect:Direct Secure Plus parameter file. Other operating system utilities and editing tools do not work.

The Admin Tool uses a native ISPF interface. The following sample illustrates the native ISPF interface display of the Create/Update Panel for SSL/TLS parameters. You can change the ISPF settings (Option 0) for the action bar choices and point-and-shoot fields. Changing these settings to fit your personal preferences can enhance operation and navigation in the Admin Tool.

Note: The SPAdmin tool is not be able to open a Secure parameter file created in a previous release. See DGASCONV – Secure Parameter File Conversion Utility for more information.

Native ISPF User Interface

The Native ISPF User Interface uses the standard mouse method of pointing and clicking to position the cursor to select an item, or to access a different panel. You can also tab to move the cursor from field to field within a panel.

Panels that make up the Secure+ Admin tool can contain the following components:

- The Panel Selection bar lists the other panels you can access from the current panel. These panels are listed from left to right in the typical order you would enter information. For example, the first panel listed on the sample panel, Node Identification, contains basic information about the node that already exists in the network map, such as its node name and communication information (TCP/IP address). The Secure+ Create/Update Panel - SSL/TLS Parameters panel is the next panel used to enter protocol information for communicating with the current node, followed by the EA Parameter panel if External Authentication is implemented.
- A selectable field is one in which you can either enter new information or edit existing information. On the sample panel, the fields you can enter information are those related to enabling SSL or TLS and the common parameters. You enter information in the underlined area next to the selectable field.

- The other selectable fields on the Secure+ Create/Update Panel - SSL/TLS Parameters panel take you to different panels where you can continue entering information related to the enabled protocol. For example, to choose cipher suites, you would select Cipher Suites by moving the cursor to that label and pressing Enter. A new panel displays allowing you to select and prioritize the ciphers you want to use.
- Non-selectable fields contain reference information that is display-only, such as the node name, and existing certificate and cipher information.
- Action selection allows you to accept and save the information entered on the panel in the Sterling Connect:Direct Secure Plus parameter file or cancel. After you select an action, the panel which was displayed prior to the current panel, is redisplayed.

SPAdmin Navigations

Much work has been done to improve the user experience with the SPAdmin tool to allow all panel movement and configuration updates to be performed without the use of a mouse. There are many new line commands or fast path commands that can be entered from the command line (==>) to perform the function of the SPAdmin tool. All pull down menu options have been define fast path commands so that the pull down menu is not required to perform those function, example FO can be use perform the File Open function. The table below defines all of the menu option fast path commands.

Menu option	**Fast Path command**
File New	FN
Edit Create/Update	EM
File Open	FO
File Close	FC
File Info	FI
Save Active	FS
Save As	FA
File Exit	FE
Edit Create/Update	EM
Edit Delete Record	ED
Edit Options	EO
Help	HH
Help Custom	HC
Help TLS/SSL	HS

While in create, update or view mode edit of a Parameter file record, several fast path commands exist so that many of the point-n-shoot field s are not required. For example, OK can be entered from the command line to perform the OK point-n-shoot function.

Field Option	Fast Path command
Security Options	SEC
EA Parameters	EA
SSL/TLS Parameters	SSL

OK	OK
Cancel	CAN

Several point-n-shoot fields still exist, such as those listed below, and navigation to those can be made easier using the ISPF Option “Tab to point-and-shoot fields.” Using the TAB key you can jump easily from field to field within the SPAdmin tool. Make sure that the option you place the cursor on is the function you intend to update.

Listed below are some of the point-n-shoot fields:

- Certificate Label
- Cipher Suites
- Certificate Pathname
- Certificate Common Name
- External Auth Server Def
- External Auth Server Address
- External Auth Server Port

Sterling Connect:Direct Secure Plus Parameter File

The Sterling Connect:Direct Secure Plus parameter file contains information that determines the protocol and encryption method used during security-enabled Sterling Connect:Direct operations. To configure Sterling Connect:Direct Secure Plus, each site must have a parameter file that contains one local node record and a remote node record for each trading partner who uses Sterling Connect:Direct Secure Plus to perform a secure connection. The local node record defines the most commonly used security and protocol settings at the site and can be used as a default for one or more remote node records. Each remote node record defines the specific security and protocol used by a trading partner.

For additional security, the parameter file is stored in an encrypted format. The information used for encrypting and decrypting the parameter file (and private keys) is stored in the Sterling Connect:Direct Secure Plus access file.

Passwords are protected in the TCQ and AUTH files by encrypting them with Sterling Connect:Direct Secure Plus's proprietary "Polyalphabetic Substitution Cipher" which is a weak encryption. A stronger encryption algorithm, TDESCBC112, can be used if you add a .PASSWORD record to the Sterling Connect:Direct Secure Plus parameter file. After you create this record, enable the Strong Password Encryption (SPE) feature, and restart Sterling Connect:Direct Secure Plus, SPE protects Sterling Connect:Direct Secure Plus passwords stored in the TCQ and AUTH files with the stronger algorithm. For more information on using this feature, refer to Implementing Strong Password Encryption.

Access File

The Sterling Connect:Direct Secure Plus access file is generated automatically when you create the Sterling Connect:Direct Secure Plus parameter file for the first time. You type a passphrase when you first initialize Sterling Connect:Direct Secure Plus. This passphrase is used to generate the keys necessary to encrypt and decrypt the entries in the Sterling Connect:Direct Secure Plus parameter file. The passphrase itself is not retained.

Your Sterling Connect:Direct Secure Plus administrator must secure the access file. This requires full create and update capability. The Sterling Connect:Direct server must have read authority. To maintain a secure access file, the general user community should not have access permission.

This file can be secured with any available file access restriction tools. Availability of the access file to unauthorized personnel can compromise the security of data exchange.

Sterling Control Center

Once you have created your Sterling Connect:Direct Secure Plus parameter file, you can use IBM Sterling Control Center to perform the following functions when implementing the SSL or TLS protocol:

- Create and update a remote node
- Update the local node
- Add and update certificates
- Create an alias node
- Select cipher suites
- Delete a remote node

To perform these functions, you must have a Sterling Control Center user ID with Sterling Connect:Direct administration authority including privileges to read and write to the Sterling Connect:Direct Secure Plus parameter file.

For more information, see *Customizing Levels of Sterling Connect:Direct Functional Authority* in the *IBM Sterling Connect:Direct for z/OS Administration Guide*. For more information on how to perform these functions, see the documentation for Sterling Control Center.

Prerequisites

Before you configure Sterling Connect:Direct Secure Plus for z/OS, ensure that you complete the following tasks.

Expert Security Administrator

The instructions and information provided to assist you in implementing the SSL/TLS protocol assume that you have an expert z/OS security administrator who is familiar with the terms associated with digital certificates and has experience using the tools required to generate and manage certificates, including:

- UNIX System Services
- IBM ICSF application and Crypto Hardware device
- System security applications, for example, gskkyman, RACF, CA-Top Secret, or CA-ACF2
- Security terminology associated with digital certificates (see Terminology and Security Applications for SSL and TLS Certificates)
- Working knowledge of the Sterling Connect:Direct application and its environment

Sterling Connect:Direct ISPF Libraries in TSO

To ensure that you can perform Sterling Connect:Direct Secure Plus parameter file functions and generate the SAVE AS JCL for the Sterling Connect:Direct Secure Plus parameter file, you must allocate the same release of the following Sterling

Connect:Direct ISPF libraries in your TSO session before you try to perform Sterling Connect:Direct Secure Plus parameter file functions and generate and submit the Save As JCL as described in Sterling Connect:Direct Secure Plus Operation Enablement and Validation or the Save Active JCL as described in Sterling Connect:Direct Secure Plus Maintenance:

- $CD.SDGAISPC (must be allocated as SYSPROC)
- $CD.SDGALINK
- $CD.SDGAPENU
- $CD.SDGASENU
- $CD.SDGAMENU

If these required libraries have not been allocated, or have been allocated incorrectly, when you perform the save and submit procedure, the JCL for the SAVE AS job is not generated, and you have to repeat the configuration tasks. For more information on the required libraries and how to allocate them, see the *IBM Sterling Connect:Direct for z/OS Configuration Guide* and the *Program Directory for IBM Sterling Connect:Direct for z/OS*.

Security Requirements of Trading Partners

Security planning is a collaborative effort between you and your trading partners. You must know the expectations of your trading partners and plan your security implementation to meet these requirements. Consider the following guidelines for configuring communications sessions using the SSL or TLS protocol:

- You must acquire the certificates before you configure Sterling Connect:Direct Secure Plus.
- Determine whether you and your trading partner will use self-signed certificates or certificates signed by a Certificate Authority.
- Determine whether to use client authentication.
- Using the Sterling External Authentication Server application in conjunction with Sterling Connect:Direct Secure Plus to validate the other node's certificate for a secure session requires the following:
  - Using the TLS or SSL protocol for connections to the Sterling External Authentication Server
  - Enabling client authentication in remote node records so that the SNODE can validate the PNODE certificate
  - Exchanging certificates between Sterling Connect:Direct Secure Plus for z/OS and the Sterling External Authentication Server node

Implementation Plan for Sterling Connect:Direct Secure Plus

After you identify your security administrator and determine the security requirements of your trading partners, review SSL and TLS Prerequisites for protocol-specific configuration information.

Worksheets

Before you configure Sterling Connect:Direct Secure Plus for z/OS, complete the worksheets in Configuration Worksheets. Use this information to configure the local and remote nodes to use Sterling Connect:Direct Secure Plus for z/OS.

Sterling Connect:Direct Secure Plus for z/OS Documentation

The *IBM Sterling Connect:Direct Secure Plus for z/OS Implementation Guide* describes how to implement peer-to-peer security into Sterling Connect:Direct operations with Sterling Connect:Direct Secure Plus. This document includes information to plan, configure, and use Sterling Connect:Direct Secure Plus. The *IBM Sterling Connect:Direct Secure Plus for z/OS Implementation Guide* is for programmers and network operations staff who install and maintain Sterling Connect:Direct Secure Plus.

This guide assumes knowledge of Sterling Connect:Direct, including its applications, network, and environment and security policies and applications used in your environment.

Task Overview

The following table guides you to the information required to perform Sterling Connect:Direct Secure Plus tasks.

Task	Reference
Understanding Sterling Connect:Direct Secure Plus and assessing your security requirements	Sterling Connect:Direct Secure Plus for z/OS Overview
Planning to use the TLS or SSL protocol	SSL and TLS Prerequisites Certificate Parameter Definitions
Navigating the Secure+ Admin Tool and populating the parameter file	Admin Tool and Parameter File Usage Configuration for a Secure Connection between z/OS and OpenVMS Nodes
Setting up local and remote node records for the SSL or TLS protocol	Manual Creation of the SSL or TLS Parameter File Local Node Record Imported from Network Map Configuration Remote Node Record Imported from Network Map Configuration Configuration Worksheets Configuration for a Secure Connection between z/OS and OpenVMS Nodes
Configuring special-purpose remote node records to perform one of the following functions: • Validate certificates using the Sterling Authentication Server application • Block nonsecure TCP API connections • Secure passwords at rest within the Sterling Connect:Direct TCQ and AUTH files.	Additional Configuration Options
Saving the parameter file the first time after creating it and preparing Sterling Connect:Direct Secure Plus for operation	Sterling Connect:Direct Secure Plus Operation Enablement and Validation
Validating and testing connections by session	Sterling Connect:Direct Secure Plus Operation Enablement and Validation

Task	Reference
Performing exception processing by overriding Sterling Connect:Direct Secure Plus settings in the PROCESS statement	Override Settings in Sterling Connect:Direct Processes
Maintaining the Sterling Connect:Direct Secure Plus parameter file and indiividual remote nodes	Sterling Connect:Direct Secure Plus Maintenance
Viewing Sterling Connect:Direct Secure Plus statistics	Sterling Connect:Direct Secure Plus Statistics
Understanding error messages and resolving errors	Troubleshoot

Chapter 2. Plan Your Implementation of the SSL or TLS Protocol

Before you configure Sterling Connect:Direct Secure Plus, review the following concepts, requirements, terms, and tool descriptions to ensure that you have the resources and information necessary to implement the Transport Layer Security (TLS) protocol or Secure Sockets Layer (SSL) protocol.

For more information on using the TLS protocol and NIST with zOS, see the IBM publication **z/OS Cryptographic Services System SSL Programming (SC14-7495-00)**.

Transport Layer Security Protocol and Secure Sockets Layer Protocol

The Transport Layer Security protocol (TLS) and the Secure Sockets Layer (SSL) protocol use certificates to exchange a session key between the node that initiates the data transfer process (the primary node, or PNODE) and the other node that is part of the communications session (the secondary node, or the SNODE). A certificate is an electronic document that associates a public key with an individual or other entity. It enables you to verify the claim that a public key belongs to an entity. Certificates can be self-issued or issued by a certificate authority (CA). See Self-Signed and CA-Signed Certificates. When a CA receives an application for a certificate, it validates the applicant's identity, creates and signs certificate. A CA issues and revokes CA-issued certificates. Self-signed certificates are created and issued by the owner of the certificate, who must export the certificate in order to create a trusted root for the certificate and supply the trusted root of the self-signed certificate to the partner in a connection.

Sterling External Authentication Server validates certificates during an SSL or TLS session. Use the application to configure certificate chain validation, including the option to validate certificates against one or more Certificate Revocation Lists (CRLs) stored on an LDAP server. You can also configure the application to return attributes associated with the incoming certificate, such as group information, stored on an LDAP server. See *IBM Sterling External Authentication Server Implementation Guide* for information.

To use Sterling External Authentication Server, configure your application to connect to the host name and port where the Sterling External Authentication Server application resides and specify a certificate validation definition. See the instructions for creating the Sterling Connect:Direct Secure Plus parameter file manually or using the network map for the TLS or SSL protocols for instructions to create the remote node record for the Sterling External Authentication Server application (.EASERVER).

FIPS 140-2 Mode for the TLS Protocol

Enhanced security is available for Sterling Connect:Direct using System SSL FIPS mode available in IBM z/OS Version 1 Release 11 to meet FIPS 140-2 criteria. FIPS-mode operation is available only for the TLS protocol. For more information, see “Planning for System SSL in FIPS Mode” on page 6.

TLS or SSL Protocol Processing

After you configure Sterling Connect:Direct Secure Plus, you are ready to exchange data securely with other security-enabled Sterling Connect:Direct nodes. Data is securely exchanged between two nodes using the protocol defined in the parameter file.

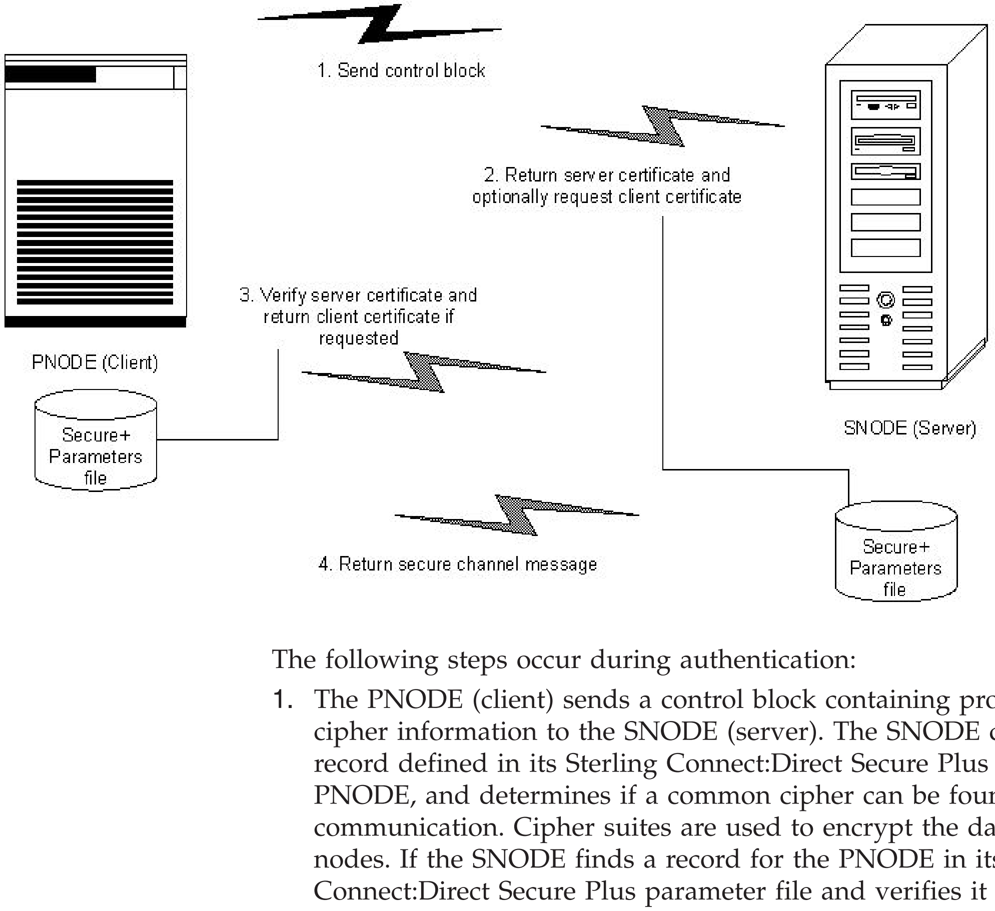
Note: You can implement the protocol you want to use for all data transfers or on a Process-by-Process basis. To specify a protocol each time you submit a Process, you must disable the protocol (but allow overrides) when you create the local and remote nodes in the Sterling Connect:Direct Secure Plus parameter file, and then specify it in the PROCESS statement using the SECURE parameter. For more information, see Override Settings in Sterling Connect:Direct Processes .

Sterling Connect:Direct Secure Plus Data Exchange

Data exchange consists of two processes: authentication and sending/receiving data. The TLS or SSL protocol data exchange process is described in the following sections.

Authentication

The following figure illustrates the authentication process using the TLS or SSL protocol:


1. Send control block
2. Return server certificate and optionally request client certificate
3. Verify server certificate and return client certificate if requested
4. Return secure channel message
PNODE (Client)
Secure+ Parameters file
SNODE (Server)
Secure+ Parameters file

The following steps occur during authentication:

1. The PNODE (client) sends a control block containing protocol (TLS or SSL) and cipher information to the SNODE (server). The SNODE confirms that it has a record defined in its Sterling Connect:Direct Secure Plus parameter file for the PNODE, and determines if a common cipher can be found and used for secure communication. Cipher suites are used to encrypt the data being sent between nodes. If the SNODE finds a record for the PNODE in its Sterling Connect:Direct Secure Plus parameter file and verifies it has a cipher defined in common with the PNODE, a common cipher is negotiated and the session continues.

2. The SNODE sends its ID certificate to the PNODE who confirms that it has a record defined in the Sterling Connect:Direct Secure Plus parameter file. Information for creating a public key is included. The PNODE verifies the ID certificate of the SNODE using the trusted root certificate file defined in its Sterling Connect:Direct Secure Plus parameter file, and generates a session key.
3. If client authentication is enabled on the SNODE, the SNODE requests an ID certificate from the PNODE. The PNODE sends its ID certificate defined in its Sterling Connect:Direct Secure Plus parameter file to the SNODE for verification against the trusted root certificate file specified in the SNODE's Sterling Connect:Direct Secure Plus parameter file. If a common name was also specified in the Sterling Connect:Direct Secure Plus parameter file for the PNODE, this name is used to verify the common name field of the PNODE's certificate.
4. The SNODE confirms that a secure environment is established and returns a secure channel message.

Customer Data Transmission

Once a Sterling Connect:Direct Secure Plus session has been established, all control blocks and customer data transmitted between the PNODE and SNODE are encrypted using the negotiated cipher.

Note: You can override certain security settings including what is encrypted during a session. If encrypting all data files is excessive in your environment, you can encrypt only the information necessary to establish a session and not the data files being transferred. For more information, see Control Block and Data Encryption Default Override .

Self-Signed and CA-Signed Certificates

Determining the type of certificate to use for secure communications sessions and the method to generate the certificate is challenging. Self-signed certificates and digital certificates issued by certificate authorities offer advantages and disadvantages. You may also be required to use both types of certificates, depending on the security requirements of your trading partners. The following table compares the advantages and disadvantages of self-signed and CA-signed certificates.

Note: When System SSL is in FIPS mode, the certificates and certificate store have FIPS requirements. For more information about FIPS requirements, see *z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08*

Type of Certificate	Advantages	Disadvantages
Self-signed certificate	No cost	Requires you to distribute your certificate, minus its private key, to each trading partner in a secure manner.
	Easy to generate	Difficult to maintain; anytime the certificate is changed, it must be distributed to all clients.
	Self-validated	Not validated by a third-party entity
	Efficient for small number of trading partners	Inefficient for large number of trading partners

Type of Certificate	Advantages	Disadvantages
CA-signed certificate	Not required to store the public key of trading partner The public key signed by the CA is exchanged at SSL negotiation and authenticated against the CA's Trusted Root Key, which is stored in the Trusted Root directory and the z/OS UNIX System Services key database or key ring of the Sterling Connect:Direct Secure Plus server.	Must be purchased from third-party vendor
	Tools used to generate certificates typically load the currently available CA certificates to the key database or key ring being generated, which means that you can connect your trading partner's certificates to the key ring to verify its trustworthiness.	
	Eliminates having to send your certificate to each trading partner	Trading partners must download digital CA-signed certificate used to verify the digital signature of trading partner public keys only if the CA certificate is not available
	Requires the remote client to store only the CA's digitally signed certificate (trusted key) in the Trusted Root directory	Must store the CA-signed certificate in the z/OS UNIX System Services key database or key ring and in the Trusted Root file
	No changes required on the trading partner's system if you recreate the CA signed certificate using the same CA	

Terminology and Security Applications for SSL and TLS Certificates

The following table defines the security terms associated with SSL and TLS certificates and applies them to communications sessions between a Sterling Connect:Direct PNODE (client) and SNODE (server). The terms are listed in alphabetical order.

Term	Definition
CA-Signed Certificate	Digital document issued by a certificate authority that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. An identity certificate issued by a CA is digitally signed with the private key of the certificate authority.

Term	Definition
Certificate Authority (CA)	An organization that issues digitally-signed certificates. The certificate authority authenticates the certificate owner's identity and the services that the owner is authorized to use, issues new certificates, renews existing certificates, and revokes certificates belonging to users who are no longer authorized to use them. The CA digital signature is assurance that anybody that trusts the CA can also trust that the certificate that it signs is an accurate representation of the certificate owner.
Certificate Signing Request (CSR)	Message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for further information.
Key Database	Database generated by the GSKKYMAN utility for creating and managing public and private keys and certificates. Typically, the files in this database are password-protected to ensure that they are inaccessible to unauthorized users. **Note:** If System SSL is in FIPS mode, a FIPS keybase is required. See *z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08*.
Key ring	File that contains public keys, private keys, trusted roots, and certificates. A key ring is a collection of certificates that identify a networking trust relationship (also called a trust policy) and are stored in a database. key rings are associated with specific user IDs, which can have more than one key ring. Key rings enable you to share key rings across multiple servers. **Note:** If System SSL is in FIPS mode, the key ring might have FIPS requirements. See *z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08*.
Private Key	String of characters used as the private, “secret” part of a complementary public-private key pair. The asymmetric cipher of the private key is used to sign outgoing messages and decrypt data that is encrypted with its complementary public key. Data that is encrypted with a Public Key can only be decrypted using its complementary Private Key. The private key is never transmitted.

Term	Definition
Public Key	String of characters used as the publicly distributed part of a complementary public-private key pair. The asymmetric cipher of the public key is used to confirm signatures on incoming messages and encrypt data for the session key that is exchanged between server and client during negotiation for an SSL/TLS session. The public key is part of the ID (public key) certificate. This information is stored in the key certificate file and read when authentication is performed.
Self-Signed Certificate	Digital document that is self-issued, that is, it is generated, digitally signed, and authenticated by its owner. Its authenticity is not validated by the digital signature and trusted key of a third-party certificate authority. To use self-signed certificates, you must exchange certificates with all your trading partners.
Session Key	Asymmetric cipher used by the client and server to encrypt data. It is generated by the SSL software.

System Security Applications

The following table describes some system security applications available for generating certificates. Review the documentation for your security application for detailed instructions for generating certificates. See Certificate Parameter Definitions, for more information on creating certificates using these tools.

Certificate Tool	Description
gskkyman	IBM utility for creating and managing digital certificates and public and private keys stored in a key database. Files created using the gskkyman utility have the following default names: • key.kdb = private key file • certreq.arm = Certificate Signing Request (CSR) file • cert.arm = public key file The gskkyman utility loads currently available CA certificates to the key database.
Resource Access Control Facility (RACF)	An IBM application that provides access control by identifying users to the system; verifying users of the system; authorizing access to protected resources; logging detected, unauthorized attempts to enter the system; and logging detected accesses to protected resources. The RACF utility can be used to create, store, and manage keys, digital self-signed or CA-signed certificates, and key rings. Because the RACF application can manage multiple key rings, certificates and key rings are added to the RACF database independently and then a certificate is associated with one or more key rings. For example, you can add the CA public key to your database and associate the certificates of your trading partners created by that CA with its public key. The RACF utility does not assign default names to the files you generate with it.

Certificate Tool	Description
Computer Associates Access Control Facility (CA-ACF2)	Security application, similar to the RACF application, that enables you to authenticate users and to protect a variety of z/OS resources. You can generate, administer, and process certificate requests, export keys, and manage key rings. The CA-ACF2 application does not assign default names to the files you generate with it.
CA-Top Secret	Security application, similar to the RACF application, that protects your mainframe computer systems and data by controlling access to resources and enables you to generate, administer, and process certificate requests, export keys, and manage key rings. The CA-Top Secret application does not assign default names to the files you generate with it.

General Requirements for Certificates

The certificate for the Sterling Connect:Direct Secure Plus for z/OS server defined in the local node record has the following general requirements:

- X.509 version 3 end-user server certificate that can interpret digital signatures and can encrypt and decrypt data
- Must be defined to the key database or key ring
- Must be stored in the key database or key ring
- Must have a private key
- Must be valid and not expired
- Must be signed by a CA or self-signed
- Must be set as default in the key database or key ring

Application-Specific Requirements

In addition to the general requirements for certificates, see Certificate Parameter Definitions, for details on the minimum parameter definitions required for the security applications described in Terminology and Security Applications for SSL and TLS Certificates.

Server Certificates and Sterling Connect:Direct

To use the SSL or the TLS protocol to perform a secure connection, you must obtain a server certificate and set up Sterling Connect:Direct to use certificates.

Note: An optional feature provides the ability to monitor certificates and issue automatic and on-demand warnings when certificates expire and are soon to expire within a specified number of days. Refer to *Checking the Validity of Certificates Used by Sterling Connect:Direct Secure Plus* in the *IBM Sterling Connect:Direct for z/OS Administration Guide*.

Server Certificate

Certificates require key settings that define the type of security to implement at your site, including authentication, non-repudiation, data integrity, and data confidentiality, as described in Security Concepts. Although the security application that you use to create a digital certificate may use different terms to describe these security concepts (for example, digital signature, key encipherment, data encipherment, and non-repudiation), both self-signed certificates and certificate requests sent to a certificate authority must designate all these key usage items to ensure that Sterling Connect:Direct Secure Plus can use the certificates to perform the intended security functions.

You can use the following methods to obtain an X.509 version 3 server certificate:

- Your registration authority can contract with a formal certificate authority (CA) to obtain a server certificate. When you obtain the server certificate, you then import this certificate into the IBM System SSL toolkit key database or key ring.
- Your registration authority can create a self-signed private and public key using one of the system security applications described in Terminology and Security Applications for SSL and TLS Certificates.
- Using one of the system security applications described in Terminology and Security Applications for SSL and TLS Certificates, your registration authority can generate a certificate signing request (CSR) for submission to third-party Certificate Authority to obtain a CA-signed public key. You forward this certificate to a certificate authority to be signed. When you receive the signed certificate, you import this certificate into the IBM System SSL key database or key ring. Refer to the IBM documentation *IBM Cryptographic Services System Secure Sockets Layer Programming Guide and Reference* for details.

Setting Up Sterling Connect:Direct to Use Certificates

About this task

Before using the TLS or SSL protocol, you must set up Sterling Connect:Direct to use certificates.

Note: When System SSL is in FIPS mode, there might be additional requirements. See *z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08* .

To set up Sterling Connect:Direct to use certificates:

Procedure

1. Ensure that the local Sterling Connect:Direct node to be configured for the TLS or SSL protocol has either a key ring or a key database on the z/OS image that contains its certificate.
2. Record the following information on your local node record worksheet for use when you configure the local node record in the Sterling Connect:Direct Secure Plus parameter file:
   - Name of the key ring or full file name of the key database
   - Label of the certificate in your key ring or key database
   - Password used when the key database was created

   Note: Key rings do not use passwords.
3. If you are using a key database, issue the UNIX command **chmod 666** to ensure that Sterling Connect:Direct has permission to read from and write to the key database.

Chapter 3. Using the SecurePlus Admin Tool and Populating the Parameter File

Use the following information to familiarize yourself with the Sterling Connect:Direct Secure Plus administration tool and to determine whether to use Quickstart to populate the parameter file from the network map or populate the parameter file manually.

Note: You can only use the Quick Start option the first time you create a parameter file, and if your Sterling Connect:Direct TCP/IP netmap entries use standard IPV4 addresses.

Starting the Administration Tool

About this task

Use the Administration (Admin) Tool to set up and maintain a Sterling Connect:Direct Secure Plus operation.

Procedure

1. To start the Admin Tool, do one of the following:
   - From the Connect:Direct Administrative Options Menu, select **Secure+** from the action bar and press Enter. Type **1** to select Secure+ Admin Tool and press Enter.
   - On the Connect:Direct Administrative Options Menu command line, type **S** and press Enter to select the Executive Secure Plus Commands option, then type **SA** on the command line and press Enter.

   After the Admin Tool is initialized, the Secure+ Admin Tool: Main Screen is displayed.
2. To continue configuring Sterling Connect:Direct Secure Plus, refer to Sterling Connect:Direct Secure Plus Configuration.

About the Admin Tool

When you start the Secure+ Admin Tool and open a parameter file, the panel displays all node records that are defined in the parameter file including a summary of the attributes for each node, unless you have filtered the records by node name using **Options** on the **Edit** menu.

The following table describes the fields that are displayed on the Secure+ Admin Tool: Main Screen, including field descriptions and valid values for each field.

Field Name	Field Description	Valid Values

LC	Line Command. For more information, see Node Record Maintenance.	U = Update node
		I = Insert node
		H = View History
		V = View node
		D = Delete node

Field Name	Field Description	Valid Values
Node Name	Displays the node record name.	Node name

Type	Displays the current record type.	L = local node record
		R = remote node record
		A = alias record
		Note: Alias is valid only for remote records.

Secure+ Protocol	Displays the Secure+ protocol used.	Disabled * (default to local node) SSL TLSV10 TLSV11 TLSV12

Override	Displays the status of Override.
	Enabling Override in a remote node record allows values specified in the COPY statement or the PROCESS statement to override values set in the remote node record. For more information, see Override Settings in Sterling Connect:Direct Processes.
		Y = enabled
		N = disabled
		* = default to local node

Encryption	Indicates if data encryption is enabled.	Y = enabled
		N = disabled
		* = default to local node

External Auth	Identifies whether external authentication is enabled for the node.
	For more information, see Adding a Remote Node Record for the Sterling External Authentication Server.
		Y = enabled
		N = disabled
		* = default to local node

Client Auth	Identifies whether client authentication is enabled for the node.	Y = enabled
		N = disabled
		* = default to local node

Node-Specific Parameters

When you insert a node, in addition to entering the node name and Type (local or remote), you also must specify parameters on three additional screens that are accessed from the Secure+ Create Update Panel.

Security Options

The Security Options panel is displayed when you insert a node manually and select Security Options from the Create/Update panel. The following table lists the Sterling Connect:Direct Secure Plus parameters according to the type of record (local or remote) to which they apply.

Node Security Option	Valid for Local Node Record?	Valid for Remote Node Record?
Security Protocol	Yes	Yes
Security Mode	Yes	Yes
Enable Overrides	No	Yes
Alias Names	No	Yes
TCP Information	No	No
Note: When you create the Sterling Connect:Direct Secure Plus parameter file from the NETMAP, the TCP Information field is populated automatically; however, data in the TCP Information field of the remote record is not used to initiate Sterling Connect:Direct communications sessions. IP address and port number are acquired only from the NETMAP.		

EA Parameters

The following table describes the parameters displayed when you select EA Parameters from the Create/Update Panel:

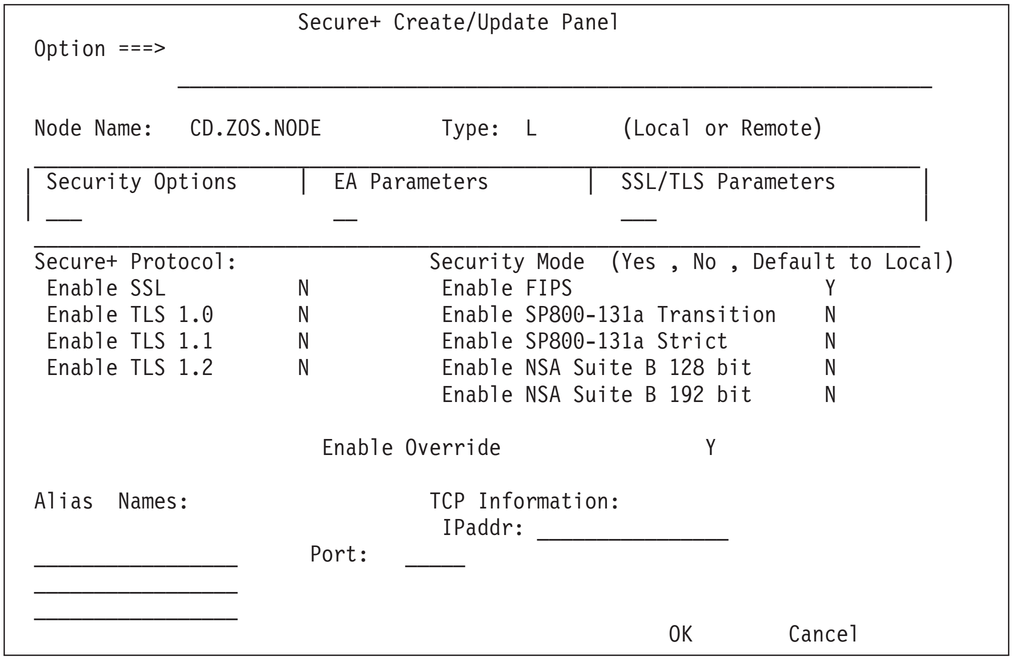
EA Parameters	Valid for Local Node Record?	Valid for Remote Node Record?
Enable External Auth	Yes. Not a good idea to enable this parameter in the local node record.	Yes. Valid only for .EASERVER remote node record.
External Auth Server Def	No	Yes. Valid only for .EASERVER remote node record.
External Auth Server Address	No	Yes. Valid only for .EASERVER remote node record.
External Auth Server Port	No	Yes. Valid only for .EASERVER remote node record.

SSL/TLS Parameters

The following table describes the parameters displayed when you select SSL/TLS Parameters from the Secure+: Create/Update panel.

Note: If System SSL is in FIPS mode, then TLS is the only supported protocol. See "Planning for System SSL in FIPS Mode" on page 6.

Table 1.



```
                      Secure+ Create/Update Panel
Option ===>
            ________________________________________________________________

Node Name:   CD.ZOS.NODE          Type:  L       (Local or Remote)
___________________________________________________________________________
| Security Options      |  EA Parameters        |  SSL/TLS Parameters      |
| ___                      __                       ___                    |
___________________________________________________________________________
Secure+ Protocol:                 Security Mode  (Yes , No , Default to Local)
 Enable SSL           N            Enable FIPS                     Y
 Enable TLS 1.0       N            Enable SP800-131a Transition    N
 Enable TLS 1.1       N            Enable SP800-131a Strict        N
 Enable TLS 1.2       N            Enable NSA Suite B 128 bit      N
                                   Enable NSA Suite B 192 bit      N

                        Enable Override               Y

Alias  Names:                     TCP Information:
                                   IPaddr: ________________
_________________      Port:   _____
_________________
_________________
                                                    OK        Cancel
```

SSL/TLS Parameters	Valid for the Local Node?	Valid for the Remote Node?
Enable Client Auth	Not a good idea to enable this parameter in the local node record.	Yes. Valid only for remote nodes that use the SSL or TLS protocol.
Enable Data Encrypt	Yes.	Yes

Admin Tool Navigation

Use the following standard function keys to navigate the Admin Tool:

Key	Function
PF8	Move forward
PF7	Move backward
PF12	Go back to the previous panel
PF3	Exit
Enter	Select an option

Admin Tool Help

You can access several types of Help information within the Secure+ Admin Tool as described in the following table:

Help	How to Access
General Help	From any Secure+ Admin Tool screen, select **Help** from the action bar and press **Enter**. Type **I** to select the general Help option.
Action Bar Help	Position the cursor on the action bar item and press **PF1**.
Screen and Panel-Level Help	Position the cursor in any uneditable part of the screen or panel and press **PF1**.

Help	How to Access
Field-Level Help	Position the cursor in the editable part of a field and press **PF1**.

Sterling Connect:Direct Secure Plus Configuration

You must configure Sterling Connect:Direct Secure Plus before you begin using it for secure communications. You create and save a Sterling Connect:Direct Secure Plus parameter file that contains a single local node record and a remote node record for every trading partner that uses Sterling Connect:Direct Secure Plus. The way you populate the parameter file depends on your environment. Parameter File Creation and Node Configuration describe two common scenarios and the most effective method of creating and populating the parameter file and configuring the local and remote nodes records for each scenario.

Parameter File Creation

The configuration procedures are based on the scenarios described in this section. Use the following table to help you decide how to create a Sterling Connect:Direct Secure Plus parameter file.

Scenario	Method to Create parameter file	Result
• First time to create a parameter file. • Large number of trading partners that use the same protocol.	Use Quickstart to copy the network map file and save it as the Sterling Connect:Direct Secure Plus parameter file. See Populating the Parameter File Using Quick Start .	• File is created automatically with a local node record and a record for each remote node in the network map that uses the TCP or UDT protocol. • Configure Sterling Connect:Direct Secure Plus for all remote node records, including trading partners that do not use Sterling Connect:Direct Secure Plus. • Sterling Connect:Direct Secure Plus protocols are disabled for all records created from the network map. • Establishes default settings for most parameters in the local node record.
• First time to create a parameter file. • Large number of trading partners. • Few trading partners use Sterling Connect:Direct Secure Plus.	Manually create a parameter file and add the local node record and remote node records. See Manual Parameter File Creation .	• You create the local node record and a record for each remote node that uses Sterling Connect:Direct Secure Plus. • Reduces the number of records to configure. • No default settings are established for parameters in the local node record. You must define all settings.

Node Configuration

After you create and populate the parameter file, you decide how to configure the local node record. The method that you use to configure the local node record then determines how you configure remote node records.

Use the following table to help you decide how to configure the local node:

Scenario	How to Configure Node Records	Result
Most trading partners use the same protocol.	Enable the most commonly used protocol in the local node record. Depending on the protocol, see the relevant procedure in Local Node Record Imported from Network Map Configuration .	• Enables the same protocol in all remote node records. • You have to modify only the records for remote nodes that do not use the settings for the local node.
Most trading partners do not use Sterling Connect:Direct Secure Plus.	Disable the Sterling Connect:Direct Secure Plus protocols in the local node record and enable the Override parameter. Depending on the protocol, see one of the following procedures: • Adding the Local Node Record to the Parameter File Manually for the SSL or TLS Protocol Configure remote node records only for those trading partners who use Sterling Connect:Direct Secure Plus.	• You define default protocol settings in the local node record so remote nodes can use default values. • You configure only those remote node records that use Sterling Connect:Direct Secure Plus.
Trading partners need to disable or enable security for a session.	Set OVERRIDE=Y in both the local and remote node records in the parameter files of both trading partners.	Either trading partner can disable or enable security for a particular session by setting the SECURE keyword in a Process or Copy statement. See Override Settings in Sterling Connect:Direct Processes for more information.
Some trading partners use Sterling Connect:Direct Secure Plus and the Sterling External Authentication Server application.	Disable external authentication in the local node record and enable the **Override** parameter. Create a .EASERVER remote record. See Adding a Remote Node Record for the Sterling External Authentication Server.	• You can enable external authentication only for those remote nodes that use it with Sterling Connect:Direct Secure Plus. • You can verify certificates exchanged during an SSL or TLS session using the Sterling External Authentication Server application.
Nonsecure TCP API connections are not allowed to connect to a Sterling Connect:Direct for z/OS server.	Create a .CLIENT remote node record and disable override. See Establishing Secure TCP API Connections to a Sterling Connect:Direct Secure Plus-Enabled Server.	• Communications from nonsecure connections is not allowed.

To see a scenario for setting up a secure connection between a Sterling Connect:Direct Secure Plus for OpenVMS node and a Sterling Connect:Direct for z/OS node, see Configuration for a Secure Connection between z/OS and OpenVMS Nodes. That topic provides a concrete example for defining a remote node record in both a Sterling Connect:Direct Secure Plus parameter file and a Sterling Connect:Direct Secure Plus for OpenMVS parameter file.

Populating the Parameter File Using Quick Start

About this task

The Quick Start option enables you to create a parameter file by importing information from the Sterling Connect:Direct network map and requires that you configure all remote node records, including those of trading partners that do not use Sterling Connect:Direct Secure Plus.

Note: You can only use the Quick Start option the first time you create a parameter file, and if your Sterling Connect:Direct TCP/IP netmap entries use standard IPV4 addresses.

To configure only the nodes that use Sterling Connect:Direct Secure Plus, refer to Manual Parameter File Creation.

To import node records to the Sterling Connect:Direct Secure Plus parameter file from the Sterling Connect:Direct network map.

Procedure

1. From the Secure+ Admin Tool: Main Screen, select **File** on the action bar and press Enter.
2. Type **2** to select **Open** and press Enter.
3. Type the Sterling Connect:Direct network map file name prefix or partial prefix followed by an asterisk (*) and select **Browse**. and press Enter.

   Note: You can also type the Sterling Connect:Direct network map file name and press **Enter**.
4. Type **S** next to the file name of the network map you want to use and press Enter.
5. When the Quick Start prompt screen is displayed, select **Yes** and press Enter.

   After a few seconds, the Secure+ Admin Tool: Main Screen displays nodes populated from the Sterling Connect:Direct network map.
6. Update the local and remote node records using the following procedures:
   - Local Node Record Imported from Network Map Configuration
   - Remote Node Record Imported from Network Map Configuration

Manual Parameter File Creation

If you determine that populating the parameter file manually is most efficient for your environment, see Manual Creation of the SSL or TLS Parameter File for configuring the local and remote node records.

Chapter 4. Create the Parameter File Manually for the SSL or TLS Protocol

If you communicate with a large group of trading partners, but only a few trading partners use Sterling Connect:Direct Secure Plus, you can manually create and populate the parameter file by creating a single local node record and a remote node record for each trading partner that uses Sterling Connect:Direct Secure Plus. This method minimizes the number of remote node records to configure in the parameter file.

For instructions on additional configuration options, see:

- Adding a Remote Node Record for the Sterling External Authentication Server
- Establishing Secure TCP API Connections to a Sterling Connect:Direct Secure Plus-Enabled Server

To validate and test a Sterling Connect:Direct Secure Plus connection between two business partners, see Validating and Testing Connections by Session.

Configuration Guidelines

When you use the manual method to populate the parameter file, you should disable all protocols and external authentication and allow override in the local node record. Review the Node Configuration Table to determine the configuration approach that best suits your needs, and use the following guidelines when you configure the local node record manually:

- Disable the Sterling Connect:Direct Secure Plus protocols (TLS/ SSL) in the local node record. Then configure each remote node record with the protocol used by that trading partner. To disable all protocols and the Sterling External Authentication Server application, you must change Default to Local Node settings in the following panels: SSL/TLS Parameters and EA Parameters. Allow overrides in the Local Node settings.
- Disable external authentication.
- For all environments, you must define required settings in the local node record, including certificate information used with the TLS or SSL protocol. You can also define optional settings in the local node record and use them in all remote node records.
- Read all warning and error messages. You can continue configuring the environment without resolving warning messages, but you may be unable to perform secure communications. You must resolve all errors before saving the parameter file.
- To enable secure connections using Sterling Connect:Direct Secure Plus, you must complete the procedures in Adding the Local Node Record to the Parameter File Manually for the SSL or TLS Protocol, Adding a Remote Node Record to the Parameter File Manually for the SSL or TLS Protocol, and Sterling Connect:Direct Secure Plus Operation Enablement and Validation.
- Before you start the Secure+ Admin Tool to add your local and remote node records, verify that you have allocated the ISPF libraries in your TSO session that are required to save the Sterling Connect:Direct Secure Plus parameter file (see Sterling Connect:Direct ISPF Libraries in TSO for details).

Adding the Local Node Record to the Parameter File Manually for the SSL or TLS Protocol

About this task

When you perform this procedure, refer to the Local Node Security Feature Definition Worksheet that you completed for the local node.

To add the local node record manually:

Procedure

1. Select **Edit** from the Secure+ Admin Tool Main Screen and press Enter.
2. On the **Edit** menu, select **1** for **Create/Update Record** and press Enter to display the Secure+ Create/Update panel:
3. On the Secure+ Create/Update panel:
   a. Type a name for the local node in the **Node** field.
   b. In the Type field, enter the type of node (local or remote).
4. Select **SSL/TLS Parameters** from the panel selection bar and press **Enter**.
5. In the **SSL/TLS Parameters** panel:
   a. To disable the Client Authentication function, type **N**beside the **Enable Client Auth** field.
   b. To enable the Data Encrypt function, type **Y** beside the **Enable Data Encrypt** field.
6. Specify the certificate label:
   a. Select the **Certificate Label** field and press **Enter**.

      Note: If System SSL is in FIPS Mode, the Certificate Label has FIPS requirements. See "Planning for System SSL in FIPS Mode" on page 6.
   b. Press **F8** to move to the editable portion of the panel containing the label field.
   c. This field is case sensitive; therefore, type the certificate label exactly as you defined it when you generated it using one of the security applications described in Configuration Worksheets and press **Enter**.
7. Identify where the certificate information is stored:
   a. Select the **Certificate Pathname** field and press **Enter**.

      Note: If System SSL is in FIPS Mode, the Certificate Pathname has FIPS requirements. See "Planning for System SSL in FIPS Mode" on page 6.
   b. Press **F8** to scroll to the editable portion of the panel containing the **Certificate Path** field.
   c. Type the UNIX path name of the key database (.kdb) or the security system key ring name that contains all certificates referred to in the parameter file.

      Note: This value is case sensitive. Type it exactly as it appears in the certificate file. Refer to the information in Local Node Security Feature Definition Worksheet.
   d. If you are using a key database:
      1) Press **F8** to scroll to the editable portion of the panel containing the password field.

2) Type the password used when the key database was created and press **Enter**.

   Note: This value is case sensitive. Ensure that you type it exactly as it appears in the certificate file. Refer to the information you recorded in Local Node Security Feature Definition Worksheet.

   Note: If you are using a key ring, leave the password field blank.

e. Click **OK**and press Enter.

8. To enable and prioritize cipher suites:

   Note: If System SSL is in FIPS mode, only certain ciphers are valid. See the *IBM Sterling Connect:Direct for z/OS Release Notes* for a list of valid FIPS-mode ciphers.

   a. Select **Security Options**.
   b. Type **Y** by the cipher you want to enable.
   c. Type **N** by the cipher you want to disable.
   d. Continue typing values next to the ciphers you want to enable or disable.
   e. Press **F3** when finished.

      Note: To identify the ciphers available, run a trace on the Sterling Connect:Direct system. Setting **debug=8C0000AE** in the initialization parameter file dynamically allocates DD R00000001. Available ciphers are listed in the trace DD. Turn global tracing off before you continue.

      Note: When the SSL or TLS environment is correctly set up and the cipher suites selected, the textual names in the Update Cipher Suites panel are set based on the protocol in effect.
   f. To enable override, type **Y**in the Enable Override field.
   g. Enter Alias Names.
   h. Enter TCP Information.
   i. Select **OK** and press Enter.
9. To disable the use of the Sterling External Authentication Server application:
   a. Select **EA Parameters** from the panel selection bar and press **Enter**.
   b. Type **N** in the **External Auth** field.

      The remaining external authentication fields are unavailable because they are valid only for the .EASERVER remote node record.

      Note: Values set for parameters that are displayed in multiple panels (Override, for example) are retained in a record after you set them the first time they are displayed.
10. Select **OK** and press **Enter** to display the values for the local node record.
11. Read all warning and error messages. Continue configuring the environment without resolving warning messages, but you must resolve errors before you save the parameter file.
12. After you configure the local node record, you can save and submit the parameter file using the procedures in Sterling Connect:Direct Secure Plus Operation Enablement and Validation, but if you have not added a remote node record, connections are not secure.

Adding a Remote Node Record to the Parameter File Manually for the SSL or TLS Protocol

About this task

Refer to the Remote Node Security Feature Definition Worksheet that you created for the remote node you are adding when you complete this procedure. The following procedure assumes that this remote node uses the SSL or TLS protocol and client authentication with Sterling Connect:Direct Secure Plus unless you want to override the Sterling Connect:Direct Secure Plus parameter settings from the PROCESS statement. For more information, see Override Settings in Sterling Connect:Direct Processes.

To add a remote node record manually for the SSL or TLS protocol:

Procedure

1. On the **Option** line type **I** (Insert Node) on the **Secure+ Admin Tool Main Screen** and press **Enter** to add a node. The **Secure+ Create/Update Panel** is displayed.
2. On the **Secure+ Create/Update Panel**:
   a. In the **Node Name** field, type the name for the remote node that corresponds to its name in the network map.
   b. Type **R** in the **Type** (Local or Remote) field.
3. Select **Security Options**.
4. To implement SSL, do one of the following, depending on whether you want to use SSL for all data transfers or on a Process-by-Process basis:
   - Type **Y** beside the **Enable SSL** field to enable the SSL protocol for this remote node.
   - Type **N** beside the **Enable SSL** field to disable the SSL protocol but enable it later in a PROCESS statement.
5. To implement TLS, do one of the following, depending on whether you want to use TLS for all data transfers or on a Process-by-Process basis:
   - Type **Y** beside the **Enable TLS** field to enable the TLS protocol for this remote node.
   - Type **N** beside the **Enable TLS** field to disable the TLS protocol but enable it later in a PROCESS statement.

   Note: If System SSL is in FIPS mode, TLS is the only supported protocol. See "Planning for System SSL in FIPS Mode" on page 6.

   Note: If you attempt to set both SSL and TLS to 1 (or Y for Enabled), a warning displays indicating that the Enable SSL setting was changed to 2 (disabled) because you can only enable one protocol at a time for a particular node.
6.
   a. In the **Alias Names** field, type any alternative name for this remote node that uses the same Sterling Connect:Direct Secure Plus parameters. This alias name must also exist as a valid remote node entry in the network map.
   b. Leave the **TCP Information** fields (**IP addr** and **Port**) blank because Sterling Connect:Direct always obtains the IP address and port for a remote node from the network map.

c. Take one of the following actions, depending on whether you want to use the Sterling Connect:Direct Secure Plus parameter settings override feature.
   - To enable the Sterling Connect:Direct Secure Plus parameter settings override feature in the PROCESS or COPY statement, type **1** beside the **Override** field. For more information, see Override Settings in Sterling Connect:Direct Processes.
   - To disable the Sterling Connect:Direct Secure Plus parameter settings override feature, type **2** beside the **Override** field.

d. To enable client authentication:
   1) Type **1** beside the **Client Auth** field.
   2) To have the common certificate name verified during the authentication process, select **Client Auth. Compare** and when the next panel displays, type the certificate common name of the local node certificate and press **Enter**. To not have the name verified, leave this field blank by not selecting the **Client Auth. Compare** field. If the common name is not entered, the client name verification process is not performed but client authentication is.

      Note: This value is case-sensitive. Type it exactly as it appears in the certificate file.

e. Take one of the following actions, depending on what information you want to encrypt:
   - Type **1** beside the **Encrypt** field to encrypt all information sent during the handshake to set up communication sessions and the actual files being transferred.
   - Type **2** beside the **Encrypt** field to encrypt only the control block information sent during the handshake to set up communication sessions and not the actual files being transferred.
   - Type **3** beside the **Encrypt** field to default to the local node's specification of Encrypt.

7. To change the list of ciphers enabled for this remote node record:

   Note: If System SSL is in FIPS mode, only certain ciphers are valid. See the *IBM Sterling Connect:Direct for z/OS Release Notes* for a list of valid FIPS-mode ciphers.

   a. Select the **Cipher Suites** field and press **Enter** to display the **Update Cipher Suites** panel.
   b. Type **1** by the cipher you want to enable and give the highest priority.
   c. Continue typing numbers next to the ciphers you want to enable, in order of priority.

      The ciphers you enable appear in the order of priority in the **Enabled Cipher-Suites** list.
   d. Press **F3** when you have enabled and ordered all necessary ciphers.

8. To specify the certificate label:
   a. Select the **Certificate Label** field and press **Enter**.
   b. Press **F8** to move to the editable portion of the panel containing the label field.
   c. This field is case sensitive; therefore, type the label of the certificate exactly as you defined it when you generated it using one of the security applications described in Configuration Worksheets, or type an asterisk (*) to specify the same label as the local node record, and press **Enter**.

Note: The Certificate Pathname field is automatically set to '*' (Default to Local) in the Remote Node record. You are not allowed to update this field for a remote node.

9. Select **EA Parameters** and press **Enter**.

   In the **EA Parameters** panel:

10. Type **3** beside the **Override** field because it is not relevant to External Authentication.
11. Take one of the following actions, depending on whether the remote node validates client certificates using the Sterling External Authentication Server application.
    - Type **1** beside the **External Auth** field if this remote node uses the Sterling External Authentication Server application.
    - Type **2** beside the **External Auth** field if the remote node does not use the Sterling External Authentication Server application.
    - Type **3** beside the **External Auth** field if the remote node's use of the Sterling External Authentication Server defaults to the Local Node's setting.

      The remaining EA parameters are unavailable because they are valid only for the .EASERVER remote node record.
12. Select **OK** and press **Enter** to save and close this remote node record.
13. Read all warning and error messages. You can continue configuring the environment without resolving warning messages, but you must resolve all errors before you save the parameter file.
14. Take one of the following actions:
    - To configure an .EASERVER remote node record, continue with Adding a Remote Node Record for the Sterling External Authentication Server
    - To configure a .CLIENT remote node record, continue with Establishing Secure TCP API Connections to a Sterling Connect:Direct Secure Plus-Enabled Server.
    - If you have no other remote node records to configure, continue with the procedures in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.

Chapter 5. Additional Configuration Options

You can configure special-purpose remote node records to perform the following functions:

- Validate certificates using Sterling External Authentication Server (TLS and SSL)
- Block nonsecure TCP API connections (TLS and SSL)
- Secure passwords at rest within the Sterling Connect:Direct TCQ and AUTH files (all protocols)

With the SSL and TLS protocols, you can validate certificates using the Sterling External Authentication Server application. To use Sterling External Authentication Server, configure your application to connect to the host name and port where the Sterling External Authentication Server application (.EASERVER) resides. Specify a certificate validation definition. For configuration instructions, see "Adding a Remote Node Record for the Sterling External Authentication Server."

Use only secure TCP API connections to connect to a Sterling Connect:Direct for z/OS server. To block nonsecure TCP API connections, define a .CLIENT remote node record, disable override, and identify SSL or TLS as the protocol to use for secure TCP API connections. For configuration instructions, see Establishing Secure TCP API Connections to a Sterling Connect:Direct Secure Plus-Enabled Server.

In Sterling Connect:Direct, passwords can be used in Sterling Connect:Direct when Processes are submitted, during API signons. and when the AUTH file is maintained. You can use Strong Password Encryption SPE) to secure passwords at rest within the Sterling Connect:Direct TCQ and AUTH files. See Implementing Strong Password Encryption.

Adding a Remote Node Record for the Sterling External Authentication Server

About this task

To verify certificates using Sterling External Authentication Server, create a remote node record for the Sterling External Authentication (EA) Server in the Sterling Connect:Direct Secure Plus parameter file. Before you begin, complete the .EASERVER Node Security Feature Definition Worksheet.

To add a remote node record for the Sterling External Authentication Server:

Procedure

1. Select **Edit** from the **Secure+ Admin Tool Main Screen** and press **Enter**
2. On the **Edit** menu, type **1** to select **Create/Update Record** and press **Enter**.
3. On the Secure Plus: Create/Update Panel:
   a. Type **.EASERVER** in the **Node Name** field.
   b. Type **R** beside the **Type** field.
   c. Select **EA Parameters** and press **Enter**.
   d. Type * beside the **Override** field because it is not relevant to External Authentication.
   e. Type **N**beside the **External Auth** field.

4. On the**EA Parameters** screen:
   a. Type information from the worksheet for the .EASERVER record in the following fields:

Field	Description
External Auth Server Def	Name of the certificate validation definition configured on the Sterling External Authentication Server that defines how to validate certificates. This field is case sensitive.
External Auth Server Address	IP address of server for Sterling External Authentication Server
External Auth Server Port	Port number to connect to the Sterling External Authentication Server.

   Note: After you create the .EASERVER remote node record, the **External Auth Server Def**, **External Auth Server Address**, and **External Auth Server Port** fields are populated in the EA Parameters panel of all Sterling Connect:Direct Secure Plus parameter file records, but the only field that can be modified from a record other than the .EASERVER record is the **Enable External Auth** field.

   b. Select **SSL/TLS Parameters** in the panel selection bar and press **Enter**.
5. To enable client authentication, Type **Y** beside the **Enable Client Auth** field.
6. To specify the certificate label:
   a. Select the **Certificate Label** field and press **Enter**.
   b. Press **F8** to move to the editable portion of the label field.
   c. This field is case-sensitive, therefore, type the label of the certificate exactly as you defined it when you generated it using one of the security applications described in Configuration Worksheets, or type an asterisk (*) to specify the same label as the local node, and press **Enter**.

   Note: The Certificate Pathname field is automatically set to '*' (Default to Local) in the Remote Node record. You are not allowed to update this field for a remote node.
7. To enable ciphers:

   Note: If System SSL is in FIPS mode, only certain ciphers are valid. See the *IBM Sterling Connect:Direct for z/OS Release Notes* for a list of valid FIPS-mode ciphers.
   a. Select **Security Options** and press **Enter**.
   b. Type **Y** by the cipher you want to enable.
   c. Continue typing **Y** or **N** next to the ciphers you want to enable or disable.
   d. Press **OK** when you have enabled all necessary ciphers.
8. Select **OK** and press **Enter** to save and close this remote node record.
9. Read all warning and error messages. You can configure the environment without resolving warning messages, but you must resolve errors before you save the parameter file.
10. Press **Cancel** to display current settings for the EA node.
11. Save the parameter file using the procedure in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.

Establishing Secure TCP API Connections to a Sterling Connect:Direct Secure Plus-Enabled Server

About this task

Sterling Connect:Direct servers that use Sterling Connect:Direct Secure Plus allow you to allow secure TCP API connections or block nonsecure TCP API connections. Nonsecure API applications include Sterling Connect:Direct CICS® Option, batch interface, ISPF IUI, z/OS Console interface, and Interconnect Option (ICO). Secure API applications can include Sterling Control Center and IBM Sterling Connect:Direct Browser User Interface.

Note: To run Sterling Connect:Direct Secure Plus using a nonsecure API connection, set the S+.CMD.ENFORCE.SECURE.CONNECTION parameter to NO. See *Global Initialization Parameters*, in the *IBM Sterling Connect:Direct for z/OS Administration Guide*. In addition, specify OVERRIDE=YES in step 4 in the following procedure.

To prevent nonsecure TCP API connections, define a remote node record called .CLIENT and disable override. Additionally, identify the protocol to use for secure API connections. Defining a remote node called .CLIENT and disabling override prevents nonsecure connections to the Sterling Connect:Direct server without disabling override settings in the local node record.

If you define a .CLIENT record and disable override, also configure batch interface and ISPF IUI programs in Sterling Connect:Direct to use the SNA protocol. These programs are nonsecure TCP API connections.

An API configuration follows the same rules as other remote node connections with the following exceptions:

- API connections use either the SSL or the TLS security protocol.
- The Sterling Connect:Direct server supports TCP and defines a TCP API port for these connections. Refer to *IBM Sterling Connect:Direct for z/OS Administration Guide* for instructions on setting up TCP API support on the server.
- Settings in the .CLIENT node definition automatically override the local node.

To configure a .CLIENT remote node record when Sterling Connect:Direct Secure Plus is enabled:

Procedure

1. From the **Secure+ Admin Tool Main Screen**, select **Edit** and press **Enter** to display the **Edit** menu.
2. On the **Edit** menu, type **1** to select **Create/Update Record** and press **Enter**.
3. On the **Secure+ Create/Update** panel:
   a. Type .**CLIENT** in the **Node Name** field.

      Note: You must name this node .CLIENT in order for Sterling Connect:Direct to read this node and allow secure TCP API connections.

   b. Type **R** next to the **Type** field.
   c. Select **EA Parameters** and press **Enter**.
4. In the **EA Parameters** panel:

   a. Type **N** beside the **Enable External Auth** field to disable it. The remaining EA parameters are unavailable because they are valid only for the .EASERVER remote node record.
   b. Select **SSL/TLS Parameters** and press **Enter**.
5. Take one of the following actions, depending on whether you want to use the Sterling Connect:Direct Secure Plus parameter settings override feature:

   Note: If System SSL is in FIPS mode, TLS is the only supported protocol. See “Planning for System SSL in FIPS Mode” on page 6.
   a. Type **N** beside the **Enable Client Auth** field to disable it.
   b. Click **Security Options**.
6. The remaining fields are not valid for the .CLIENT record.
7. Click **OK** and press **Enter** to save and close the .CLIENT node record.
8. Save the parameter file using the procedure in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.
9. Ensure that the ISPF IUI and batch interface connections define SNA as the connection protocol.

   Note: If the .CLIENT node record disables the Override function, ISPF IUI and must use the SNA protocol.

Implementing Strong Password Encryption

To implement the Strong Password Encryption (SPE), you add an SPE record to the Sterling Connect:Direct Secure Plus parameter file in the same way you would any remote node record. After you go through the following procedure and restart Sterling Connect:Direct Secure Plus for z/OS, the SPE feature will be in effect.

About this task

To add an SPE record to the Sterling Connect:Direct Secure Plus parameter file and enable the SPE feature:

Procedure

1. Select **Edit** from the Secure+ Admin Tool Main Screen and press Enter.
2. On the **Edit** menu, select **1** to display the Secure+ Create/Update Panel and press**Enter**.
3. On the Secure+ Create/Update panel:
   a. Type **.password** in the **Node Name** field.
   b. Type **L** next to the **Type** field.
   c. Press **Enter** to display the **Secure+ Create/Update Panel - SPE Parameters** screen.
4. On the **SPE Parameters** panel, type **1** next to the **Enable SPE** field.

   Press **Enter** to enable SPE and finish creating the SPE record by clicking **OK**.
5. Save the parameter file using the procedure in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.
6. Restart Sterling Connect:Direct Secure Plus for z/OS.
7. To verify that Sterling Connect:Direct Secure Plus for z/OS initialization is complete along with the SPE feature, after you restart Sterling Connect:Direct Secure Plus for z/OS, review the task output for the following messages interspersed with the other initialization messages:

```
SITA460I  Strong Password Encryption Initiated; CONNECT.CD.AUTH
SITA462I  Strong Password Encryption Completed; CONNECT.CD.AUTH
SITA460I  Strong Password Encryption Initiated; CONNECT.CD.TCQ
SITA462I  Strong Password Encryption Completed; CONNECT.CD.TCQ
```

Note: These messages display even if no .PASSWORD record exists and no encryption is possible. If you return to the Secure+ Create/Update Panel - SPE Parameters screen where you enabled SPE, you should see (SPE currently in use) displayed to confirm that SPE has indeed been implemented.

Disabling Strong Password Encryption

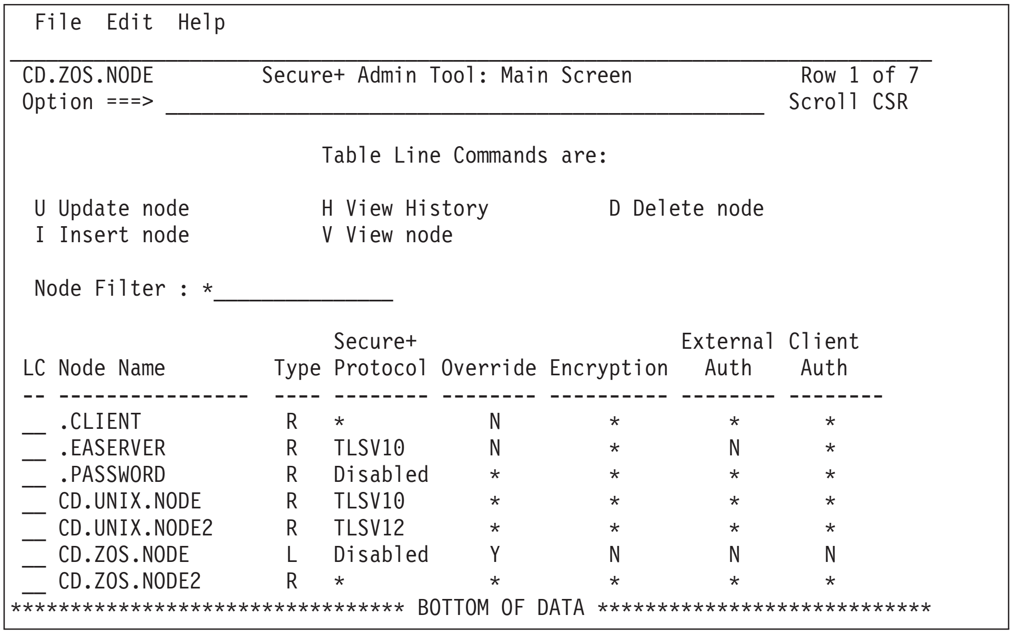
About this task

If the Strong Password Encryption feature was backed out inappropriately by deleting the .PASSWORD record while at the same time passwords existed in the TCQ and AUTH files in the SPE format, you will see one of the messages listed in the following section, SPE Problem Troubleshooting. Follow the procedure in this section, restart Sterling Connect:Direct Secure Plus for z/OS, and then enable the SPE feature again.

To disable the SPE feature:

Procedure

1. Start the Secure+ Admin Tool to display the **Secure+ Admin Tool: Main Screen**, which displays the nodes populated from the Sterling Connect:Direct Secure Plus for z/OS network map along with other records in the Sterling Connect:Direct Secure Plus parameter file.



```
  File  Edit  Help
______________________________________________________________________________
 CD.ZOS.NODE         Secure+ Admin Tool: Main Screen            Row 1 of 7
 Option ===> __________________________________________________  Scroll CSR

                          Table Line Commands are:

  U Update node           H View History          D Delete node
  I Insert node           V View node

  Node Filter : *_______________

                           Secure+                            External Client
 LC Node Name         Type Protocol Override Encryption   Auth    Auth
 -- ----------------  ---- -------- -------- ---------- -------- --------
 __ .CLIENT            R   *           N         *         *       *
 __ .EASERVER          R   TLSV10      N         *         N       *
 __ .PASSWORD          R   Disabled    *         *         *       *
 __ CD.UNIX.NODE       R   TLSV10      *         *         *       *
 __ CD.UNIX.NODE2      R   TLSV12      *         *         *       *
 __ CD.ZOS.NODE        L   Disabled    Y         N         N       N
 __ CD.ZOS.NODE2       R   *           *         *         *       *
********************************* BOTTOM OF DATA ****************************
```

2. Type **U** next to the **.PASSWORD** record and press **Enter** to display the **Secure+ Create/Update Panel - SPE Parameters** screen.
3. On the **SPE Parameters** panel, type **2** next to the **Enable SPE** field and press **Enter**.
4. Save the parameter file using the procedure in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.
5. Restart Sterling Connect:Direct Secure Plus for z/OS.

SPE Problem Troubleshooting

If the Strong Password Encryption key stored in the .PASSWORD record is out of sync with the SPE key used to encrypt the passwords, errors can occur and you must reset all SPE passwords and reimplement the SPE feature.

The .PASSWORD record can get out of sync if one of the following occurs:

- You restore the .PASSWORD record from a backup of the Sterling Connect:Direct Secure Plus parameter file—The .PASSWORD record is updated and a new encryption key generated each time the Sterling Connect:Direct Secure Plus for z/OS server is restarted, so the backup will probably not contain the current parameters.
- The .PASSWORD record is deleted outside of Sterling Connect:Direct and Sterling Connect:Direct Secure Plus—The .PASSWORD record is recreated as needed, so the SPE key used to encrypt the passwords no longer exists.
- The .PASSWORD record is corrupt—The SPE encryption key used to encrypt the passwords is not accessible.

The following tables identify errors you may experience when using the SPE feature, along with solutions to fix each issue.

Condition: Because of SPE errors, Sterling Connect:Direct Secure Plus for z/OS either initializes with a SITA461I message or does not initialize at all with a SITA463E message.

Error	Cause	Action
SITA461I SITA463E	SPE-formatted passwords exist In the TCQ and/or AUTH files, but Sterling Connect:Direct Secure Plus has not been enabled.	Sterling Connect:Direct for z/OS has not been set up to run with Sterling Connect:Direct Secure Plus for z/OS. Add the SECURE.DSN=*filename* parameter to the initialization parameters, where *filename* is the name of the Sterling Connect:Direct Secure Plus parameter file. Restart Sterling Connect:Direct Secure Plus for z/OS. To see more detailed information about individual errors related to the general failure, see the ESTAE trace output.
	• SPE-formatted passwords exist In the TCQ and/or AUTH files, but there is no .PASSWORD record in the Sterling Connect:Direct Secure Plus parameter file. • SPE-formatted passwords exist in the TCQ and/or AUTH files, but the .PASSWORD record in the Sterling Connect:Direct Secure Plus parameter file has OLD encryption keys. This can only occur if an old Sterling Connect:Direct Secure Plus parmfile is restored with a backup that contains old keys.	Reset all passwords in the TCQ and AUTH files by performing these actions: • Select the AUTH file record in the AUTH file. Provide a new password and blank out all unusable data. • In the TCQ file, delete all Processes and resubmit. To see more detailed information about individual errors related to the general failure, see the ESTAE trace output.

Condition: You encounter errors while trying to maintain the AUTH file.

Error	Cause	Action
SAFB023W SAFF016W SAFC016W SAFE016W	While inserting and updating users through the IUI (INSERT/UPDATE/SELECT/ DELETE USER RECORD screen), Sterling Connect:Direct Secure Plus for z/OS could not read or record passwords.The .PASSWORD record does not contain the correct encryption key pair. The Sterling Connect:Direct Secure Plus parameter file may have been restored with an old copy of the .PASSWORD record.	1. Disable the SPE feature. 2. Restart Sterling Connect:Direct Secure Plus for z/OS. 3. Enable the SPE feature again. 4. Restart Sterling Connect:Direct Secure Plus for z/OS. To see more detailed information about individual errors related to the general failure, see the ESTAE trace output.

Chapter 6. Configure the Local Node Record Imported from the Network Map

The following procedures assume that you populated the parameter file by importing the network map. The Quick Start method creates a remote node record in the parameter file for each remote node record in the network map and a local node record. Using the Quick Start method to populate the parameter file is most efficient if you have a large number of trading partners that use the same protocol. You can enable that protocol in the local node record and because the remote node records are set automatically to Default to Local Node, they inherit the settings of the local node.

Depending on how you configure the local node record, you may or may not need to modify the remote node records. You must disable the Sterling Connect:Direct Secure Plus protocols in the records for all remote nodes that do not use Sterling Connect:Direct Secure Plus, and update all remote node records that use a protocol that is different from the protocol defined in the local node record.

Use the following procedures to configure the local node record imported from the network map for the SSL and TLS protocols:

- Configuring the Local Node Record for the SSL or TLS Protocol

Configuration Guidelines

Observe the following guidelines when you configure node records imported from the network map:

- Sterling Connect:Direct Secure Plus protocols are disabled initially for all records created from the network map when you use Quick Start to populate the parameter file.
- Before you start the Secure+ Admin Tool to configure the local node record, you may want to save and submit the parameter file to verify that you can generate the SAVE AS JCL. If you are unable to generate the JCL for the SAVE AS job, verify that you have allocated the ISPF libraries in your TSO session that are required to save the Sterling Connect:Direct Secure Plus parameter file (see Saving and Submitting the Sterling Connect:Direct Secure Plus Parameter File).
- To enable secure connections using Sterling Connect:Direct Secure Plus for z/OS, you must complete the following procedures:
  - Configuring the Local Node Record for the SSL or TLS Protocol
  - Relevant procedures in Remote Node Record Imported from Network Map Configuration
  - Procedures in Sterling Connect:Direct Secure Plus Operation Enablement and Validation
- Read all warning and error messages. You can continue configuring the environment without resolving warning messages, but you may be unable to perform secure communications. You must resolve all errors before saving the parameter file.

Configuring the Local Node Record for the SSL or TLS Protocol

About this task

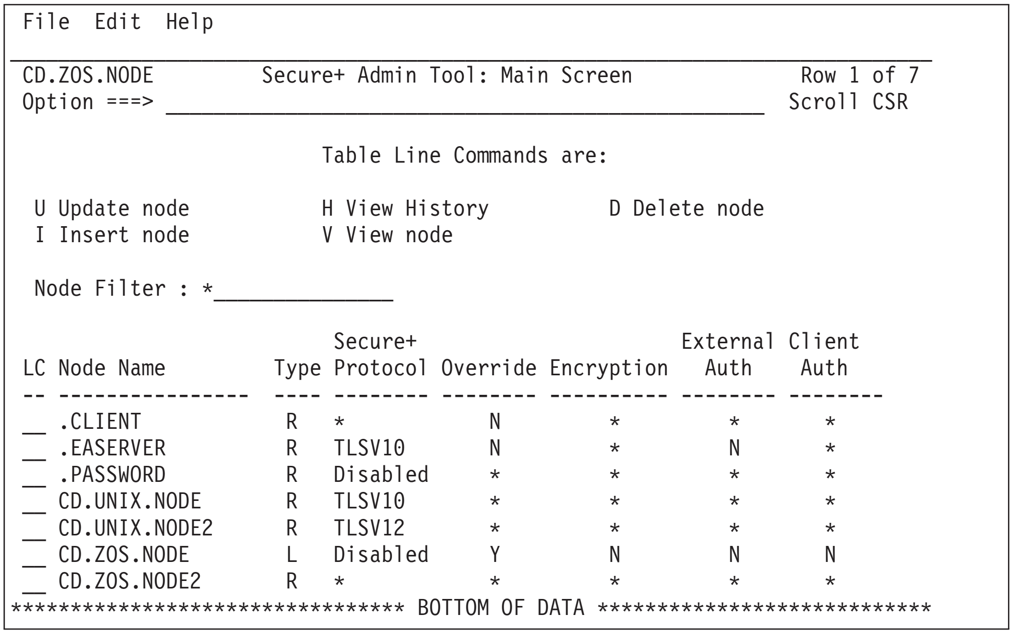
All Sterling Connect:Direct Secure Plus protocols are disabled when you import the network map. This procedure updates the local node record for the SSL (or TLS) protocol and enables the **Override** parameter. Remember that all options set for the local node are inherited by all remote node records.

To update the local node record for the SSL (or TLS) protocol:

Procedure

1. From the Sterling Connect:Direct Secure Plus Admin Main screen, type **U** next to the local node record and press **Enter** to display the **Secure+ Create/Update Panel** and the current values for the selected node.

   Note: When you import the network map, the system enables **Overrride** in the local node record automatically, as shown in the following illustration.



```
 File  Edit  Help
______________________________________________________________________________
 CD.ZOS.NODE         Secure+ Admin Tool: Main Screen              Row 1 of 7
 Option ===> __________________________________________________  Scroll CSR

                          Table Line Commands are:

  U Update node           H View History          D Delete node
  I Insert node           V View node

  Node Filter : *_______________

                           Secure+                              External Client
 LC Node Name         Type Protocol Override Encryption   Auth    Auth
 -- ---------------- ---- -------- -------- ---------- -------- --------
 __ .CLIENT            R   *            N        *          *       *
 __ .EASERVER          R   TLSV10       N        *          N       *
 __ .PASSWORD          R   Disabled     *        *          *       *
 __ CD.UNIX.NODE       R   TLSV10       *        *          *       *
 __ CD.UNIX.NODE2      R   TLSV12       *        *          *       *
 __ CD.ZOS.NODE        L   Disabled     Y        N          N       N
 __ CD.ZOS.NODE2       R   *            *        *          *       *
******************************** BOTTOM OF DATA ****************************
```

2. Select **SSL/TLS Parameters** in the panel selection line and press **Enter** to display the **SSL/TLS Parameters** panel.
3. To select the protocol you want to enable, type **Y** beside the Secure+ Protocol you want to enable, or **N**beside the protocol you want to disable.

   Note: If System SSL is in FIPS mode, TLS is the only supported protocol. See "Planning for System SSL in FIPS Mode" on page 6.

   Note: If you attempt to set both SSL and TLS to 1 (or Y for Enabled), a warning displays indicating that the Enable SSL setting was changed to 2 (disabled) because you can only enable one protocol at a time for a particular node.
4. Type **Y** in the **Enable Override** field.
5. On the EA Parameters screen, type **N** next to the Enable External Auth field.

6. On the Security Options screen, do one of the following depending on the Encrypt option you want to implement:
   a. To encrypt both the control block information and the files being transferred, type **1** beside the **Encrypt** field.
   b. To encrypt only the control block information used to establish the session, type **2** beside the **Encrypt** field.
   c. To default to the local node record, type **3** beside the **Encrypt** field.
7. If necessary, update the certificate label:
   a. Select the **Certificate Label** field and press **Enter**.

      Note: If System SSL is in FIPS Mode, the Certificate Label has FIPS requirements. See "Planning for System SSL in FIPS Mode" on page 6.
   b. Press **F8** to move to the editable portion of the panel containing the label field.
   c. This field is case sensitive; type the certificate label exactly as you defined it when you generated it and press **Enter**.
8. If necessary, update the location where the certificate information is stored:
   a. Select the **Certificate Pathname** field and press **Enter** to display the **Certificate Pathname** panel.

      Note: If System SSL is in FIPS Mode, the Certificate Pathname has FIPS requirements. See "Planning for System SSL in FIPS Mode" on page 6.
   b. Press **F8** to scroll to the **Certificate Path Name** field.
   c. Type the UNIX path name of the key database (.kdb) or the security system key ring name that contains all the certificates referred to in the parameter file.

      Note: This value is case sensitive. Ensure that you type it exactly as it appears in the certificate file. Refer to the information you recorded in Local Node Security Feature Definition Worksheet.
   d. If you are using a key database:
      1) Press **F8** to scroll to the password field.
      2) Type the password used when the key database was created and press **Enter**.

         Note: This value is case sensitive. Ensure that you type it exactly as it appears in the certificate file. Refer to the information you recorded in Local Node Security Feature Definition Worksheet .

         Note: If you are using a key ring, leave the password field blank.
9. To update the enabled cipher suites:

   Note: If System SSL is in FIPS mode, only certain ciphers are valid. See the *IBM Sterling Connect:Direct for z/OS Release Notes* for a list of valid FIPS-mode ciphers.
   a. Select the **Cipher Suites** field and press **Enter** to display the **Update Cipher Suites** panel.
   b. Type **Y** by the cipher suite you want to enable and give the highest priority.
   c. Type **N** by the cipher suite you want to enable and place second in priority.

d. Continue typing numbers next to the cipher suites you want to enable, in order of priority.

   The cipher suites you enable appear in the order of priority in the **Enabled Cipher-Suites** list.

e. Press **F3** when you have enabled and ordered all necessary cipher suites.

   Note: If you do not know what cipher suites are available, run a trace on the Sterling Connect:Direct system. Setting **debug=8C0000AE** in the initialization parameter file dynamically allocates DD R00000001. Available cipher suites are listed in the trace DD. Turn global tracing off before you continue.

10. Select **EA Parameters** and press **Enter**.

11. Verify that External Authentication (**External Auth**) is disabled (set to **2**). The remaining external authentication fields are unavailable because they are valid only for the .EASERVER remote node record.

12. Read all warning and error messages. You can continue configuring the environment without resolving warning messages, but you may be unable to perform secure communications. You must resolve all errors before you can save the parameter file.

13. After you configure the local node record, you can save and submit the parameter file using the procedures in Sterling Connect:Direct Secure Plus Operation Enablement and Validation, but if you have not added a remote node record, connections are not secure.

Chapter 7. Configure Remote Node Records Imported from the Network Map

The following procedures assume that you populate the parameter file by importing the network map. The Quick Start method creates a remote node record in the parameter file for each remote node record in the network map and a local node record. Using the Quick Start method to populate the parameter file is most efficient if you have a large number of trading partners that use the same protocol. You can enable that protocol in the local node record and because the remote node records are set automatically to Default to Local Node, they inherit the settings of the local node.

Depending on how you configured the local node record, you may or may not need to modify the remote node records. You must disable the Sterling Connect:Direct Secure Plus protocols in the records for all remote nodes that do not use Sterling Connect:Direct Secure Plus, and update all remote node records that use a protocol that is different from the protocol defined in the local node record.

Use the following procedures to modify remote node records imported from the network map for the SSL and TLS protocols, and to disable all protocols for a remote node:

- Configuring a Remote Node Record for the SSL or TLS Protocol
- Disabling Sterling Connect:Direct Secure Plus in a Remote Node Record

Your environment may have one or both of the following requirements:

- Blocking nonsecure TCP API connections
- Verifying certificates using the Sterling External Authentication Server application

For instructions on configuring these special-purpose remote node records for the TLS and SSL protocol, see the following procedures:

- Establishing Secure TCP API Connections to a Sterling Connect:Direct Secure Plus-Enabled Server
- Adding a Remote Node Record for the Sterling External Authentication Server

Configuration Guidelines

Observe the following guidelines when you configure node records imported from the network map:

- Sterling Connect:Direct Secure Plus protocols are disabled for all records created from the network map when you use Quick Start to populate the parameter file.
- For all environments, define required settings in the local node record. If desired, you can define optional settings in the local node record and use them in all remote node records.
- To enable secure connections using Sterling Connect:Direct Secure Plus for z/OS, you must complete the relevant procedure for configuring the local node record in Local Node Record Imported from Network Map Configuration, the relevant procedures in this chapter, and the procedures in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.

- Read all warning and error messages. You can continue configuring the environment without resolving warning messages, but you may be unable to perform secure communications. You must resolve all errors before saving the parameter file.

Configuring a Remote Node Record for the SSL or TLS Protocol

About this task

After you configure the local node, you can configure remote node records. When you import the network map file, you create a remote node record in the parameter file for each remote node record in the network map. Depending on how you configured the local node record, you may or may not need to update the remote node records.

- If you disabled the Sterling Connect:Direct Secure Plus protocols in the local node record, Sterling Connect:Direct Secure Plus is disabled for all remote node records. You must update all remote node records that use Sterling Connect:Direct Secure Plus to identify which protocol is used by the trading partner.
- If you enabled a protocol in the local node record, that protocol is enabled in all remote node records. You must disable the Sterling Connect:Direct Secure Plus protocols in the records for all remote nodes that do not use Sterling Connect:Direct Secure Plus, and update all remote node records that use a protocol that is different from the protocol defined in the local node record.

Note: To override security functions for a particular session, you can use the SECURE parameter in the PROCESS statement. For more information, see Override Settings in Sterling Connect:Direct Processes.

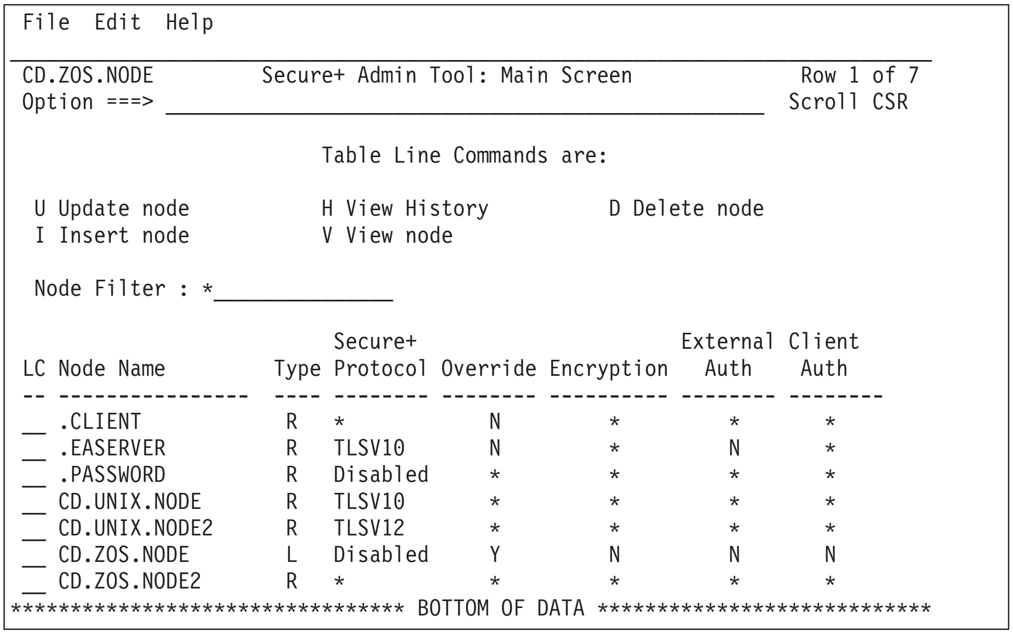
The following procedure assumes that you enabled the SSL (or TLS) protocol in the local node record, this remote node uses the SSL (or TLS) protocol, and that you need to modify some SSL (or TLS) parameters for this remote node record.

To update a remote node record for the SSL (or TLS) protocol:

Procedure

1. Type **U** next to the remote node record to update and press **Enter** to display the current values for the selected node in the Secure+ Create/Update Panel - **SSL/TLS Parameters** panel.

   Note: An asterisk in a field on the Secure+ Admin Main Screen indicates the value **Default to Local Node**. If the TLS protocol is enabled in the Local Node record, **Y** appears in the third position instead of the second position in the Secure 123C column below.



```
 File  Edit  Help
______________________________________________________________________________
 CD.ZOS.NODE         Secure+ Admin Tool: Main Screen              Row 1 of 7
 Option ===> __________________________________________________  Scroll CSR

                          Table Line Commands are:

  U Update node           H View History         D Delete node
  I Insert node           V View node

  Node Filter : *_______________

                           Secure+                         External Client
 LC Node Name        Type Protocol Override Encryption   Auth    Auth
 -- ---------------- ---- -------- -------- ---------- -------- --------
 __ .CLIENT           R   *           N         *         *       *
 __ .EASERVER         R   TLSV10      N         *         N       *
 __ .PASSWORD         R   Disabled    *         *         *       *
 __ CD.UNIX.NODE      R   TLSV10      *         *         *       *
 __ CD.UNIX.NODE2     R   TLSV12      *         *         *       *
 __ CD.ZOS.NODE       L   Disabled    Y         N         N       N
 __ CD.ZOS.NODE2      R   *           *         *         *       *
********************************* BOTTOM OF DATA ****************************
```

2. Select **EA Parameters** and press **Enter**.
3. In the **EA Parameters** panel:
   a. Specify a value for the External Authentication parameter, if required, using the following table as a guide:

Field	Description	Valid Values
External Auth	Allows validating certificates for secure sessions using Sterling External Authentication Server.	1=Yes 2=No 3=Default to local node

   b. Select **SSL/TLS Parameters** in the panel selection line and press **Enter**.
4. Take one of the following actions depending on the protocol you are implementing:
   - If you defined default SSL settings in the local node record that this remote node record uses, verify that the **Enable TLS** field is disabled (set to **2**) or set to **Default to Local Node** (**3**). If you do not need to change any other settings, continue with step 10.
   - If you defined default TLS settings in the local node record that this remote node record uses, verify that the **Enable SSL** field is disabled (set to **2**) or set to **Default to Local Node** (**3**). If you do not need to change any other settings, continue with step 10.

   Note: If System SSL is in FIPS mode, TLS is the only supported protocol. See "Planning for System SSL in FIPS Mode" on page 6.

   Note: If you attempt to set both SSL and TLS to **1** (or **Y** for Enabled), a warning displays indicating that the **Enable SSL** setting was changed to **2** (disabled) because you can only enable one protocol at a time for a particular node.
   - To modify SSL (or TLS) protocol settings in a remote node record, continue with step 7.

5. Take one of the following actions, depending on what information you want to encrypt:
   - Type **1** beside the **Encrypt** field to encrypt all information sent during the handshake to set up communication sessions and the actual files being transferred.
   - Type **2** beside the **Encrypt** field to encrypt only the control block information sent during the handshake to set up communication sessions and not the actual files being transferred.
6. Take one of the following actions, depending on whether you want to use the Sterling Connect:Direct Secure Plus parameter settings override feature.
   - To enable the Sterling Connect:Direct Secure Plus parameter settings override feature in the PROCESS or COPY statement, type **1** beside the **Override** field. For more information, see Override Settings in Sterling Connect:Direct Processes.
   - To disable the Sterling Connect:Direct Secure Plus parameter settings override feature, type **2** beside the **Override** field.
7. To change the list of cipher suites enabled for a remote node record:

   Note: If System SSL is in FIPS mode, only certain ciphers are valid. See the *IBM Sterling Connect:Direct for z/OS Release Notes* for a list of valid FIPS-mode ciphers.
   a. Select the **Cipher Suites** field and press **Enter**. The **Update Cipher Suites** panel is displayed.
   b. Type **1** by the cipher suite you want to enable and give the highest priority.
   c. Continue typing numbers next to the cipher suites you want to enable, in order of priority.

      The cipher suites you enable appear in the order of priority in the **Enabled Cipher-Suites** list.
   d. Press **F3** when you have enabled and ordered all necessary cipher suites.
8. To enable client authentication:
   a. Type **1** beside the **Client Auth** field.
   b. To have the common certificate name verified during the authentication process, select **Client Auth. Compare** and when the next panel displays, type the certificate common name of the local node certificate and press **Enter**. To not have the name verified, leave this field blank by not selecting the **Client Auth. Compare** field. If the common name is not entered, the client name verification process is not performed but client authentication is.

      Note: This value is case-sensitive. Type it exactly as it appears in the certificate file.
9. To specify the certificate label:
   a. Select the **Certificate Label** field and press **Enter**.
   b. Press **F8** to move to the editable portion of the panel containing the label field.
   c. This field is case sensitive; therefore, type the label of the certificate exactly as you defined it when you generated it using one of the security applications described in Configuration Worksheets, or type an asterisk (*) to specify the same label as the local node record, and press **Enter**.

Note: The Certificate Pathname field is automatically set to '*' (Default to Local) in the Remote Node record. You are not allowed to update this field for a remote node.

10. Select **OK** and press **Enter** to display the updated values.
11. Read all warning and error messages. You can continue configuring the environment without resolving warning messages, but you must resolve all errors that occur before you can save the parameter file.
12. Save the parameter file using the instructions in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.

Disabling Sterling Connect:Direct Secure Plus in a Remote Node Record

About this task

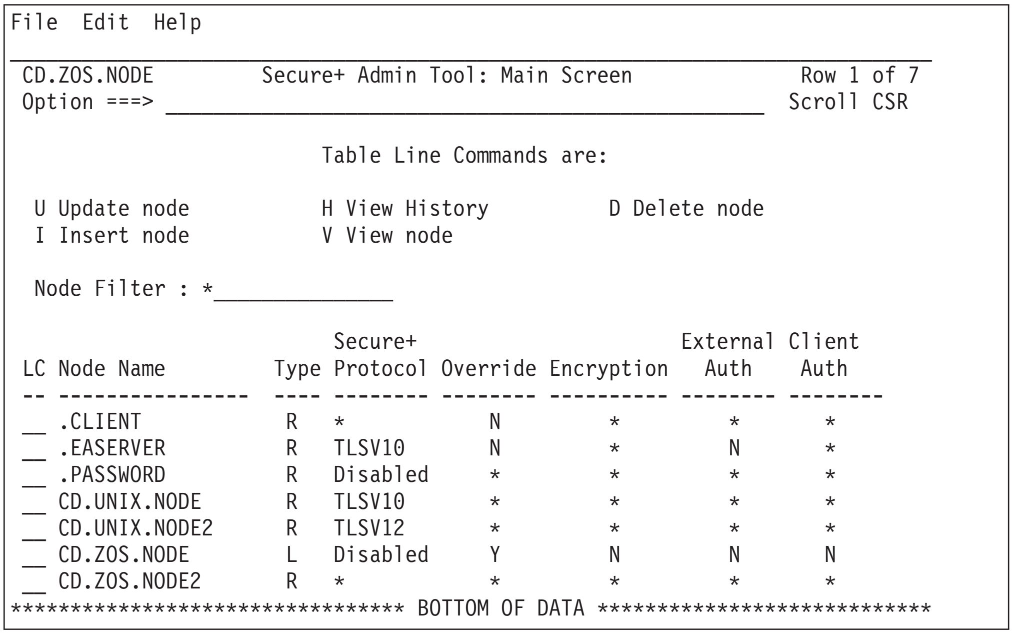
If you have remote nodes that do not use Sterling Connect:Direct Secure Plus, then you must disable all protocols for those node.

To disable all protocols in a remote node record imported from the network map:

Procedure

1. Type **U** next to the remote node record to update and press **Enter** to display the current values for the selected node.

   Note: An asterisk in a field on the Secure+ Admin Main Screen indicates the value **Default to Local Node**.



```
File  Edit  Help
______________________________________________________________________________
 CD.ZOS.NODE         Secure+ Admin Tool: Main Screen              Row 1 of 7
 Option ===> __________________________________________________  Scroll CSR

                          Table Line Commands are:

  U Update node           H View History          D Delete node
  I Insert node           V View node

  Node Filter : *_______________

                           Secure+                           External Client
 LC Node Name        Type Protocol Override Encryption   Auth    Auth
 -- ---------------- ---- -------- -------- ---------- -------- --------
 __ .CLIENT           R   *            N         *         *       *
 __ .EASERVER         R   TLSV10       N         *         N       *
 __ .PASSWORD         R   Disabled     *         *         *       *
 __ CD.UNIX.NODE      R   TLSV10       *         *         *       *
 __ CD.UNIX.NODE2     R   TLSV12       *         *         *       *
 __ CD.ZOS.NODE       L   Disabled     Y         N         N       N
 __ CD.ZOS.NODE2      R   *            *         *         *       *
********************************* BOTTOM OF DATA ****************************
```

2. Select **EA Parameters** and press **Enter**.
3. In the **EA Parameters** panel, disable the External Authentication parameter by typing **2** beside the **External Auth** field, if necessary. The remaining external authentication parameters are unavailable because they are valid only for the .EASERVER remote node record.
4. Select **SSL/TSL Parameters** in the panel selection line and press **Enter**.

5. If necessary, disable the SSL and TLS protocols by typing **2** beside the **Enable SSL** and **Enable TLS** fields, if necessary.
6. Select **OK** and press **Enter** to display the updated values.
7. Read all warning and error messages. You can continue configuring the environment without resolving warning messages, but you may be unable to perform secure communications. You must resolve all errors before saving the parameter file.
8. Save the parameter file using the instructions in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.

Chapter 8. Enable and Validate Sterling Connect:Direct Secure Plus Operation

After you initially configure the local and remote nodes for Sterling Connect:Direct Secure Plus for z/OS , save and submit the parameter file and prepare Sterling Connect:Direct for operation. As a final step, validate and test connections between you and your business partners to establish secure communications and then test to make sure you can change your security defaults for a session.

During normal maintenance after you make changes to the parameter file, you can use the Save Active option to dynamically save updates without having to restart Sterling Connect:Direct. See Saving Changes to Node Records Using the Save Active Option.

If Sterling Connect:Direct is running and Sterling Connect:Direct Secure Plus is enabled, you must use the Save Active option. Otherwise, you must use the Save As option. (When Sterling Connect:Direct Secure Plus is enabled, the Sterling Connect:Direct Secure Plus parameter file is open and Sterling Connect:Direct cannot perform the Save As option since that option deletes, redefines, and reloads the parameter file.)

Saving and Submitting the Sterling Connect:Direct Secure Plus Parameter File

About this task

This procedure assumes that you have verified that the following required Sterling Connect:Direct ISP libraries (all of the same release) have been allocated in your TSO session:

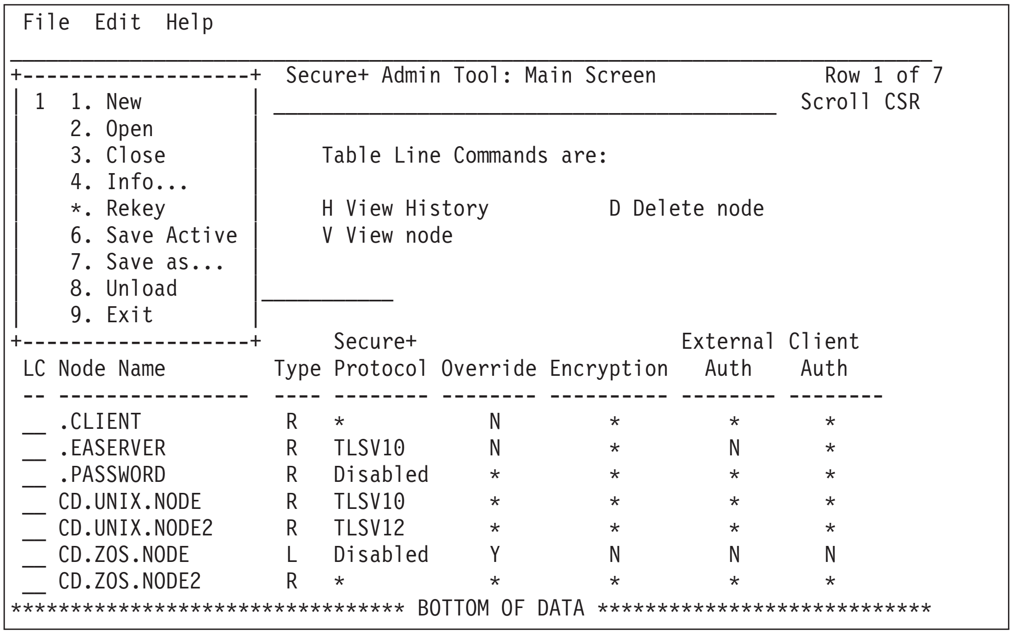
- $CD.SDGAISPC (must be allocated as SYSPROC)
- $CD.SDGALINK
- $CD.SDGAPENU
- $CD.SDGASENU
- $CD.SDGAMENU

If these required libraries have not been allocated, or have been allocated incorrectly, when you perform this procedure, the JCL for the SAVE AS job is not generated, and you have to repeat the procedures to configure the local and remote nodes. For information on how to allocate these libraries, see *IBM Sterling Connect:Direct for z/OS Configuration Guide* and *Program Directory for IBM Sterling Connect:Direct for z/OS*.

To save the Sterling Connect:Direct Secure Plus parameter file:

Procedure

1. From the Sterling Connect:Direct Secure Plus Admin Tool: Main Screen, select **File** and press **Enter**.



```
 File  Edit  Help
_____________________________________________________________________________
+-------------------+  Secure+ Admin Tool: Main Screen             Row 1 of 7
| 1  1. New         | __________________________________________  Scroll CSR
|    2. Open        |
|    3. Close       |     Table Line Commands are:
|    4. Info...     |
|    *. Rekey       |     H View History          D Delete node
|    6. Save Active |     V View node
|    7. Save as...  |
|    8. Unload      |___________
|    9. Exit        |
+-------------------+      Secure+                      External Client
 LC Node Name         Type Protocol Override Encryption   Auth    Auth
 -- ---------------- ---- -------- -------- ---------- -------- --------
 __ .CLIENT            R   *            N         *         *        *
 __ .EASERVER          R   TLSV10       N         *         N        *
 __ .PASSWORD          R   Disabled     *         *         *        *
 __ CD.UNIX.NODE       R   TLSV10       *         *         *        *
 __ CD.UNIX.NODE2      R   TLSV12       *         *         *        *
 __ CD.ZOS.NODE        L   Disabled     Y         N         N        N
 __ CD.ZOS.NODE2       R   *            *         *         *        *
********************************* BOTTOM OF DATA ****************************
```

2. Type **7** to select **Save As**.
3. Type the file name you want to use for the Sterling Connect:Direct Secure Plus parameter file and press **Enter**. (You will use this same file name in step 1 when you add this information as a parameter to the Sterling Connect:Direct initialization parameter file to tell Sterling Connect:Direct where security information is located.)

   CAUTION:
   The default Save As file name is the name of the last file that you opened. When you create the Sterling Connect:Direct Secure Plus parameter file from the Sterling Connect:Direct network map, you risk overwriting the network map file with the Sterling Connect:Direct Secure Plus parameter file if you do not change the name in this field. If the file specified here exists, you will be prompted that it will be deleted, redefined, and built anew if you select OK.
4. On the **Save As** information panel, type site-specific job card information, allocation information, STEPLIB DSNs, and Access file Dsname, using the library names created when you saved the parameter file.

   CAUTION:
   For the Access file Dsname, you must not use the same name specified for the Sterling Connect:Direct Secure Plus parameter file. However, the Access file and Sterling Connect:Direct Secure Plus parameter file act as a pair and one is not any good without the other. To more easily track the files if necessary, it is recommended that at least the first two qualifiiers match. For example, you could use $CD.SECURE.PARM and $CD.SECURE.ACCESS for the names of the related Sterling Connect:Direct Secure Plus parameter and access files.
5. Type **3** to select **Submit** and press **Enter** to save your parameter file. (If you need to change anything later, type 2 to edit the JCL before submitting the job. Edit the JCL and then submit the job.)

   CAUTION:
   Closing the JCL without submitting the job loses all of the changes you made to the parameter file.

6. Research any return code other than zero before closing the parameter file or exiting the Admin Tool.

Preparing Sterling Connect:Direct for Secure Plus Operations

About this task

After you set up the Sterling Connect:Direct Secure Plus environment, you must prepare Sterling Connect:Direct to use Sterling Connect:Direct Secure Plus.

To set up Sterling Connect:Direct to run with Sterling Connect:Direct Secure Plus:

Procedure

1. Add the following parameter to the Sterling Connect:Direct for z/OS initialization parameters: **SECURE.DSN=filename**, where **filename** is the name of the Sterling Connect:Direct Secure Plus parameter file for that node.
2. If you are operating in a CD/Plex environment, add the **SECURE.SSL.Path.Prefix=prefix** parameter, where **prefix** is the prefix location of the key database or key ring that contains the certificates for the TLS or SSL protocol.
3. Restart Sterling Connect:Direct on that node.
4. To verify that Sterling Connect:Direct Secure Plus for z/OS initialization is complete, after you restart Sterling Connect:Direct with SECURE.DSN, review the started task output for the following messages: *SITA028I Secure+ initialization* and *SITA165I Secure+ initialization complete*, if you are using the TLS or SSL protocol.

What to do next

See "Planning for System SSL in FIPS Mode" on page 6.

Parameter File Saving After the Initial Setup

After you save the Sterling Connect:Direct Secure Plus parameter file the first time using the **Save As** option, you must stop Sterling Connect:Direct before using the **Save As** option again, and then restart Sterling Connect:Direct.

When you are maintaining Sterling Connect:Direct Secure Plus for z/OS and want to save your changes without recycling Sterling Connect:Direct, use the Save Active option. For more information, see Saving Changes to Node Records Using the Save Active Option.

Validating and Testing Connections by Session

About this task

To validate and test a connection between two business partners, follow this general procedure. After you confirm that the secure connection has been established and that you can change your default security settings for a session, you can finalize the settings in the Sterling Connect:Direct Secure Plus parameter file of each business partner, save the files, and begin transferring data.

Procedure

1. For the selected protocol, make sure all prerequisites outside of Sterling Connect:Direct Secure Plus have been taken care of, such as the obtaining of server certificates and exchanging of keys.
2. Make sure each node is defined in the partner's network map.
3. For both the local and remote nodes, specify the protocol to be used when a secure connection is required (TLS or SSL).
4. For the selected protocol, make sure to define all settings required for a successful connection in the local and remote node records in the parameter files.
5. Perform the procedures in this chapter, namely, Saving and Submitting the Sterling Connect:Direct Secure Plus Parameter File, and Preparing Sterling Connect:Direct for Secure Plus Operations.
6. To test the connection, perform a file transfer between the two partners.

   Once you have successfully performed a file transfer using a secure connection, you are ready to finalize the parameter files.
7. Take one of the following actions, depending on whether you want to make your sessions default to secure or non-secure:
   - To have your sessions default to secure, specify **OVERRIDE=Y** in both the local and remote node records in the parameter files of both business partners.
   - To have your sessions default to non-secure, specify **OVERRIDE=Y** in both the local and remote node records in the parameter files of both business partners. Disable the selected protocol in the remote node record.
8. To test changing your security defaults for a session, take one of the following actions depending on whether you want to make your sessions default to secure or non-secure. For a complete description of the **SECURE** parameter and how to use it in the PROCESS statement, see the *IBM Sterling Connect:Direct Process Language Reference Guide*. Also, see Security Settings Override Examples.
   - To make a session non-secure, specify SECURE=OFF in the PROCESS statement preceding the COPY statement to transfer the file.
   - To make a session secure, specify SECURE=OFF|SSL|TLS|TLS11|TLS12 in the PROCESS statement.
9. After you valid and test your connections by session, save the parameter files and restart Sterling Connect:Direct.

Chapter 9. Override Settings in Sterling Connect:Direct Processes

After you configured Sterling Connect:Direct Secure Plus, security is either turned on or off each time that you use Sterling Connect:Direct with a node defined in the Sterling Connect:Direct Secure Plus parameter file. However, you can override some default security settings in a remote node record from a Sterling Connect:Direct Process using the SECURE parameter in the PROCESS or COPY statement.

To allow a business partner to override the default security setting of whether security is turned on or off for another business partner and to choose the protocol for the remote node, the following conditions must be in place:

- Each business partner agrees all sessions are secure or non-secure as the default
- Each business partner agrees to allow the override of the Sterling Connect:Direct Secure Plus parameters by specifying **OVERRIDE=Y** for both the local and remote nodes in their Sterling Connect:Direct Secure Plus parameter file.
- The remote node definition in each Sterling Connect:Direct Secure Plus parameter file specifies the parameters necessary for a secure session even if the protocol is disabled including all information necessary for exchanging and validating each partner's identity. All parameters related to a protocol are defined, such as SSL/TLS cipher suites and key databases.
- Sterling Connect:Direct Secure Plus is active on both nodes.

Once the Sterling Connect:Direct Secure Plus parameter files for both business partners have been set up properly, you can override the default security settings on a Process-by-Process basis to perform exception processing.

For a complete description of the SECURE parameter and how to use it in the PROCESS or COPY statement, see the *IBM Sterling Connect:Direct Process Language Reference Guide.*

PROCESS Statement Overrides for Sterling Connect:Direct Secure Plus Defaults

The first statement in all Sterling Connect:Direct Processes is the PROCESS statement which defines the attributes of a Process. The SECURE keyword in the PROCESS statement allows you to perform one or more of the following functions:

- Turn on security when non-secure sessions are the default
- Select the protocol (SSL or TLS) when non-secure sessions are the default
- Specify one or more cipher suites to override the default cipher suites defined in the Sterling Connect:Direct Secure Plus parameter file
- Turn off security when secure sessions are the default (if **OVERRIDE=Y** is specified in the Remote Node record settings in the Sterling Connect:Direct Secure Plus parameter file).
- Encrypt only the control block information contained in Function Management Headers (FMHs), such as a user ID, password, and filename. (The default is to encrypt both the control block information and the data being transferred.)

Note: If System SSL is in FIPS mode, TLS is the only supported protocol. See "Planning for System SSL in FIPS Mode" on page 6.

The following syntax example shows the options available for the SECURE keyword:

```
SECURE=OFF|SSL|TLS|TLS11|TLS12
or
SECURE=ENCRYPT.DATA=Y|N
or
SECURE = (OFF|SSL|TLS|TLS11|TLS12, ENCRYPT.DATA=Y|N)
or
SECURE = (OFF|SSL|TLS|TLS11|TLS12,<cipher_suite>|(cipher_suite_list),ENCRYPT.DATA=Y|N)
```

If you use multiple **SECURE** subparameters, **ENCRYPT.DATA** must be the last (or only) value specified on the **SECURE=** parameter.

COPY Statement Overrides for Sterling Connect:Direct Secure Plus Defaults

By using the COPY statement's SECURE parameter in a Sterling Connect:Direct Process to override the settings in the Sterling Connect:Direct Secure Plus parameter file and enabling the override feature in the remote node record, you can disable security for a particular file transfer. Sterling Connect:Direct Secure Plus uses the most secure connection available. Therefore, if the remote node record enables encryption, the PNODE cannot turn those options off using the COPY statement override.

After the security settings of the PNODE and SNODE are merged, the strongest setting is always used. Therefore, the value specified from the COPY statement cannot disable data encryption or digital signatures if the SNODE has enabled them.

In an SSL or TLS environment, the following syntax example shows the options available for the SECURE keyword in a COPY statement (for the destination file that you are copying to):

```
SECURE = ENCRYPT.DATA=Y|N
or
SECURE = ENC=Y|N
```

Security Settings Override Examples

These examples illustrate how business partners use the SECURE parameter to override the security defaults for a particular session.

Secure Sessions Default Override

The business partners agree by default all sessions are secure and choose SSL as the default protocol. Both partners enable the SSL protocol in the Sterling Connect:Direct Secure Plus parameter files and specify **OVERRIDE=Y** in both the Local and Remote Node records.

To override the default and make a particular session non-secure, they use the following PROCESS statement:

```
SSLOFF PROCESS SNODE=OTHERBP SECURE=OFF
```

Non-Secure Sessions Default Override

The business partners agree by default all sessions are non-secure. When a secure communication line is required for a particular session, the non-secure default is overridden and the SSL protocol used. The Remote Node records specify **OVERRIDE=Y**, but the SSL protocol is not enabled in the Sterling Connect:Direct Secure Plus parameter files. However, all other parameters required to perform the handshake to establish an SSL session are defined in the Remote Node records. To specify that the session for this PROCESS is to be secure using SSL, the business partners use the following PROCESS statement:

```
SSLON PROCESS SNODE=OTHERBP SECURE=SSL
```

Default Cipher Suite Override

The business partners agreed by default all sessions are secure and chose TLS as the default protocol. Both partners specified the following configuration in their Sterling Connect:Direct Secure Plus parameter files:

- Enabled the TLS protocol
- Specified **OVERRIDE=Y** in both the Local and Remote Node records
- Selected **TLS_RSA_WITH_RC4_128_MD5** as the cipher suite to use when executing Processes

To override the default cipher suite and use **TLS_RSA_WITH_3DES_EDE_CBC_SHA** when executing a particular Process, they use the following PROCESS statement:

```
NEWCIPHER PROCESS SNODE=OTHERBP SECURE=(TLS,TLS_RSA_WITH_3DES_EDE_CBC_SHA)
```

Cipher Suite List Override of Single Default Cipher Suite

The business partners agreed by default all sessions are secure and chose TLS as the default protocol. Both partners specified the following configuration in their Sterling Connect:Direct Secure Plus parameter files:

- Enabled the TLS protocol
- Specified **OVERRIDE=Y** in both the Local and Remote Node records
- Selected **TLS_RSA_WITH_RC4_128_MD5** as the cipher suite to use when executing Processes

To override the default protocol and use a list of other TLS cipher suites when executing a particular Process, they use the following PROCESS statement:

```
NEWCIPHERS PROCESS SNODE=OTHERBP SECURE=(TLS,(TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_AES_128_SHA,TLS_RSA_AES_256_SHA,TLS_RSA_WITH_DES_CBC_SHA) )
```

Control Block and Data Encryption Default Override

The business partners agreed by default to encrypt all information sent during the handshake to set up communication sessions and the actual files being transferred. Both partners specified the following configuration in their Sterling Connect:Direct Secure Plus parameter files:

- Specified **ENCRYPT=Y** in both the Local and Remote Node records
- Specified **OVERRIDE=Y** in both the Local and Remote Node records

To not go through the expense of encrypting and decrypting data being transferred, they use the following PROCESS statement when transferring a particular file:

```
ENCNO PROCESS SNODE=OTHERBP SECURE=ENCRYPT.DATA=N
```

In this scenario, both business partners are more concerned with increasing throughput and using less CPU while protecting the information being exchanged to establish the session.

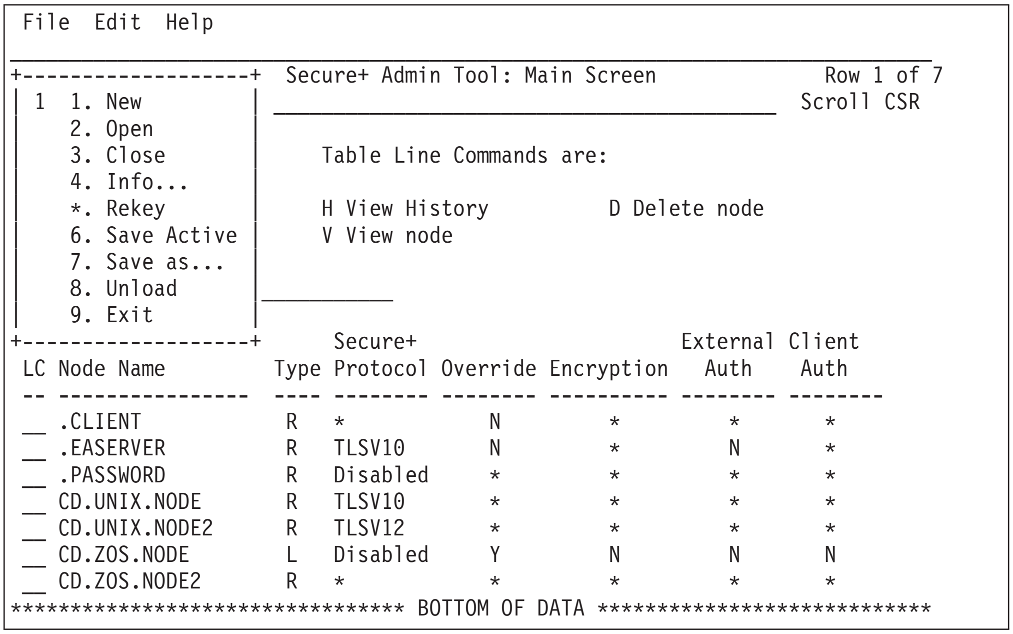
Chapter 10. Maintain Sterling Connect:Direct Secure Plus

After you set up the Sterling Connect:Direct Secure Plus environment, you will need to maintain both the Sterling Connect:Direct Secure Plus parameter file and the records it contains whenever changes in your system or a trading partner's environment require updates. For SSL and TLS node records, you can also use Sterling Control Center to display and modify information, and to delete nodes.

After you make changes, refer to Saving Changes to Node Records Using the Save Active Option to put the updates in effect immediately.

Parameter File Maintenance

The File Menu on the Secure+ Admin Tool: Main Screen contains options for maintaining the parameter file. To open this menu, select **File** from the action bar and press **Enter**. The following panel sample shows the available options when a parameter file is already open.



```
 File  Edit  Help
______________________________________________________________________________
+-------------------+  Secure+ Admin Tool: Main Screen              Row 1 of 7
| 1  1. New         | ___________________________________________  Scroll CSR
|    2. Open        |
|    3. Close       |     Table Line Commands are:
|    4. Info...     |
|    *. Rekey       |     H View History          D Delete node
|    6. Save Active |     V View node
|    7. Save as...  |
|    8. Unload      |___________
|    9. Exit        |
+-------------------+     Secure+                           External Client
 LC Node Name        Type Protocol Override Encryption   Auth    Auth
 -- ----------------  ---- -------- -------- ---------- -------- --------
 __ .CLIENT           R   *            N        *         *       *
 __ .EASERVER         R   TLSV10       N        *         N       *
 __ .PASSWORD         R   Disabled     *        *         *       *
 __ CD.UNIX.NODE      R   TLSV10       *        *         *       *
 __ CD.UNIX.NODE2     R   TLSV12       *        *         *       *
 __ CD.ZOS.NODE       L   Disabled     Y        N         N       N
 __ CD.ZOS.NODE2      R   *            *        *         *       *
********************************* BOTTOM OF DATA ****************************
```

The following options are available on the File menu:

- 1—New checks if any current table record has been modified and prompts to save, and then the table will be reset to empty. To create a new parameter file, select the **Create/Update** option on the **Edit** Menu or the **Insert** node table line command (see Inserting a Node).
- 2—**Open** displays the File Selection panel which allows you select the parameter file you want to open. For more information, see Opening a Sterling Connect:Direct Secure Plus Parameter File.
- 3—**Close** shuts the File menu allowing you to select options from the Secure+ Admin Tool. Main Screen.
- 4—**Info** displays general information about the Sterling Connect:Direct Secure Plus parameter file, such as the version of Sterling Connect:Direct Secure Plus

that you are using, the name of the parameter file, and the number of remote node records it contains. For more information, see Viewing Information about the Parameter File.

- Rekey is not an active option. However, for more information on how to regenerate the keys required to encrypt and decrypt the entries in the parameter file, see Resecuring the Parameter File and Access File.
- 6—**Save Active** allows you to dynamically update records in the parameter file without bringing Sterling Connect:Direct down. For more information, see Saving Changes to Node Records Using the Save Active Option.
- 7—**Save as** is the option you use the first time you save the parameter file. Subsequently Sterling Connect:Direct must be down to use this option which saves updates to the parameter file and you have to submit the job which restarts Sterling Connect:Direct. For more information, see Saving and Submitting the Sterling Connect:Direct Secure Plus Parameter File.
- 8—**Unload** retrieves information from the Sterling Connect:Direct Secure Plus parameter file and displays it as an ISPF TMP data set on your screen.
- 9—**Exit** takes you out of the Secure+ Admin Tool and displays the **Connect:Direct Administrative Options Menu**.

Opening a Sterling Connect:Direct Secure Plus Parameter File

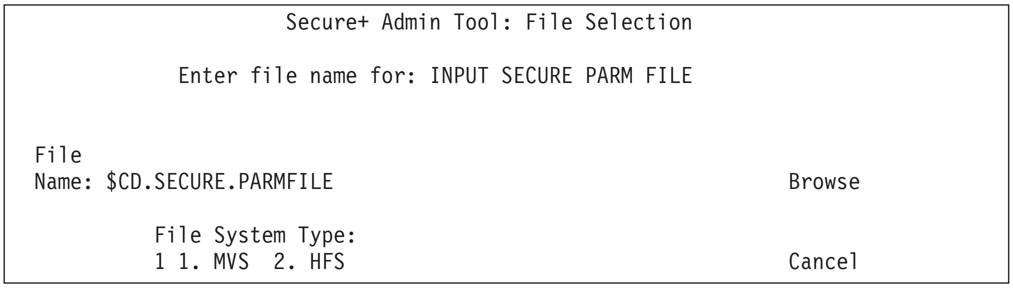
About this task

Before you can modify node records, you must open the parameter file that contains these records.

To open a Sterling Connect:Direct Secure Plus parameter file:

Procedure

1. With the **Secure+ Admin Tool Main Screen** open, select **File** and press **Enter**:
2. Type **2** to select **Open** and press **Enter** to display the file selection screen:



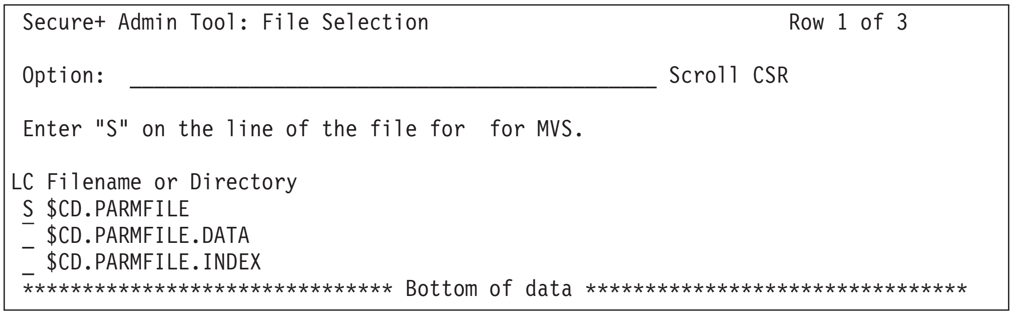
```
                        Secure+ Admin Tool: File Selection

               Enter file name for: INPUT SECURE PARM FILE


   File
   Name: $CD.SECURE.PARMFILE                                       Browse

             File System Type:
             1 1. MVS  2. HFS                                      Cancel
```

3. Type the parameter file name prefix or partial prefix followed by an asterisk (*), select **Browse,** and press **Enter**. The following screen is displayed:



```
  Secure+ Admin Tool: File Selection                           Row 1 of 3

  Option:  ____________________________________________ Scroll CSR

  Enter "S" on the line of the file for  for MVS.

 LC Filename or Directory
  S $CD.PARMFILE
  _ $CD.PARMFILE.DATA
  _ $CD.PARMFILE.INDEX
  ****************************** Bottom of data ********************************
```

Note: You can also type the complete parameter file name and press **Enter**.

4. Type **S** next to the file name to open and press **Enter**. The **Secure+ Admin Tool: Main Screen** displays nodes populated from the parameter file you opened. See Node Record Maintenance for more information on this panel and how to select the available options.

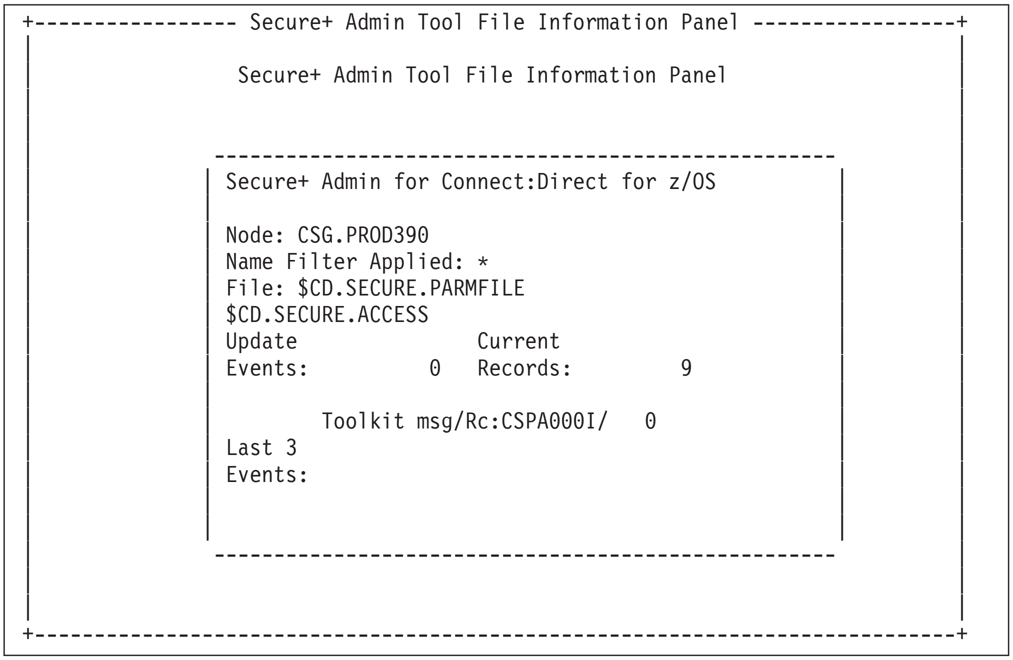
Viewing Information about the Parameter File

About this task

To view information about the Sterling Connect:Direct Secure Plus parameter file:

Procedure

1. Open the Admin Tool.
2. Select **File** and press Enter.
3. Type **4** to select **Info**. The **File Information** Panel is displayed:



```
+----------------- Secure+ Admin Tool File Information Panel -----------------+
|                                                                             |
|                  Secure+ Admin Tool File Information Panel                  |
|                                                                             |
|                                                                             |
|                ----------------------------------------------------         |
|               | Secure+ Admin for Connect:Direct for z/OS          |        |
|               |                                                    |        |
|               | Node: CSG.PROD390                                  |        |
|               | Name Filter Applied: *                             |        |
|               | File: $CD.SECURE.PARMFILE                          |        |
|               | $CD.SECURE.ACCESS                                  |        |
|               | Update              Current                        |        |
|               | Events:          0   Records:         9            |        |
|               |                                                    |        |
|               |         Toolkit msg/Rc:CSPA000I/   0               |        |
|               | Last 3                                             |        |
|               | Events:                                            |        |
|               |                                                    |        |
|               |                                                    |        |
|                ----------------------------------------------------         |
|                                                                             |
|                                                                             |
+-----------------------------------------------------------------------------+
```

The fields in the **File Information Panel** are described in the following table:

Field Name	**Description**
Node	The name of the local node for the parameter file that is open.
Admin Version	The version of Secure+ Admin Tool being used.
Name Filter Applied	Name of the filter used to determine which remote node records to display.
File	The name of the current parameter file and the access file.
Update Events	Number of updates to the parameter file.
Current® Records	Total number of remote node records.
Toolkit msg/Rc:CSPA0001	Message ID of the last Toolkit call.
Last 3 Events	List of the last 3 updates.

Saving Changes to Node Records Using the Save Active Option

About this task

The **Save Active** option on the Secure+ Admin Tool **File** menu enables you to dynamically save changes to all records in an existing Sterling Connect:Direct Secure Plus parameter file.

You must use the **Save As** option the first time you create the parameter file. This option deletes, defines, and reloads the Sterling Connect:Direct Secure Plus parameter file. See Saving and Submitting the Sterling Connect:Direct Secure Plus Parameter File.

Note: Sterling Connect:Direct Secure Plus for z/OS must be running in order to use the **Save Active** option. Any changes made to node records take effect immediately.

To save the Sterling Connect:Direct Secure Plus parameter file and put any changes made in effect immediately:

Procedure

1. Open the Admin Tool.
2. Select **File** and press **Enter**.
3. Type **6** to select **Save Active**.
4. Read all warning and error messages. You can continue without resolving warning messages, but you must resolve all errors before you save the parameter file.

   CAUTION:
   Because Sterling Connect:Direct Secure Plus for z/OS cannot restrict multiple users from attempting to apply updates to the same parameter file, measures should be in place to ensure that only one user is accessing a particular parameter file at one time. If precautions are not taken, updates will be lost and conflicts among multiple user interfaces will occur.

Resecuring the Parameter File and Access File

About this task

Routinely, or if your passphrase is compromised, you should resecure the Sterling Connect:Direct Secure Plus parameter and access files. You must open a parameter file before you perform this procedure.

To resecure the Sterling Connect:Direct Secure Plus parameter file and access file:

Procedure

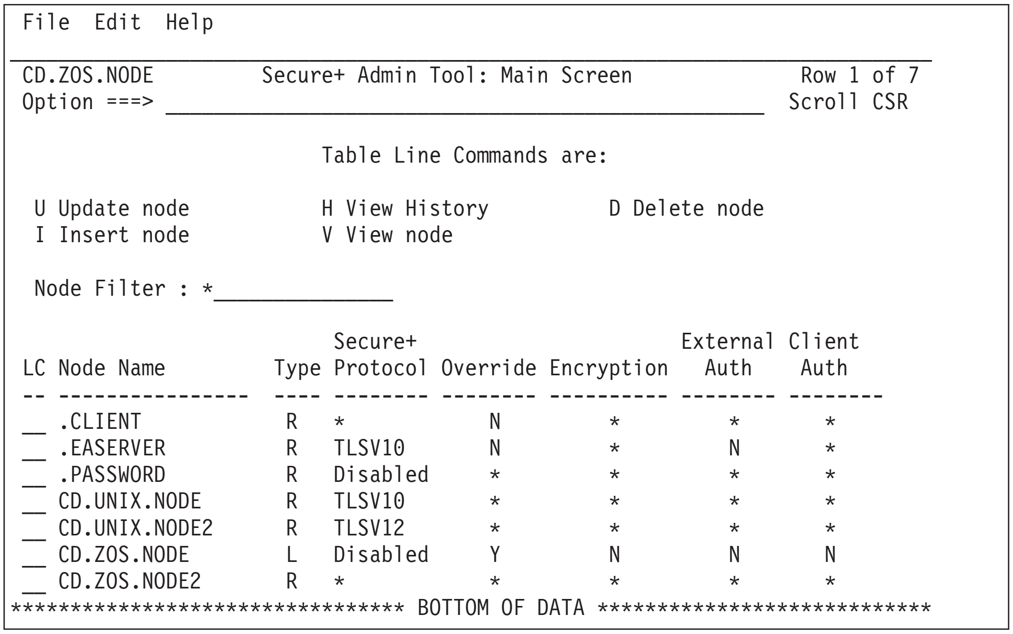
1. From the **Secure+ Admin Tool Main Screen**, select **File** and press **Enter**.
2. Type **7** to select **Save As** and press **Enter**.
3. If any warning messages are displayed, read them and press **F3** to close the warning panel.
4. On the **File Selection** panel, the file name of the parameter file that you have open is displayed. Press **Enter**.
5. At the confirmation prompt, select **OK**. The old parameter file is deleted and a new parameter file with the same name is created.

6. On the **Save As** screen, type **2** to select **Edit**, then select **Make Pass Phrase** and press **Enter**.
7. Select **OK** to confirm that you want to create a new passphrase.
8. Type a 32-byte string, using uppercase, lowercase, numeric, and alphabetic characters.
9. On the **Save As** panel, type **3** to select **Submit** and press **Enter**.
10. Select **OK** to submit the job.
11. When the *Job Submitted* message is displayed, press **Enter**.
12. Verify that the job completed with a return code of zero before closing the parameter file or exiting the **Secure+ Admin Tool**. Research any return codes other than zero.

Node Record Maintenance

When you start the Secure Plus Admin Tool, the main screen is displayed.

Secure Plus Admin Tool Main Screen



```
 File  Edit  Help
_____________________________________________________________________________
 CD.ZOS.NODE         Secure+ Admin Tool: Main Screen              Row 1 of 7
 Option ===> __________________________________________________  Scroll CSR

                          Table Line Commands are:

  U Update node           H View History          D Delete node
  I Insert node           V View node

  Node Filter : *_______________

                           Secure+                      External Client
 LC Node Name         Type Protocol Override Encryption   Auth    Auth
 -- ----------------  ---- -------- -------- ---------- -------- --------
 __ .CLIENT            R   *            N         *         *       *
 __ .EASERVER          R   TLSV10       N         *         N       *
 __ .PASSWORD          R   Disabled     *         *         *       *
 __ CD.UNIX.NODE       R   TLSV10       *         *         *       *
 __ CD.UNIX.NODE2      R   TLSV12       *         *         *       *
 __ CD.ZOS.NODE        L   Disabled     Y         N         N       N
 __ CD.ZOS.NODE2       R   *            *         *         *       *
********************************* BOTTOM OF DATA *****************************
```

The following table line commands are available to use on the nodes displayed:

- **U Update node** allows you to perform the following functions:
  - Disabling Sterling Connect:Direct Secure Plus on an SSL or TLS Node
  - Changing the Cipher Suites
- **I Insert node** allows you to create a new remote node record. For more information, see Inserting a Node.
- **H View History** lists the individual dates including the time the selected node was updated.
- **V View node** allows you to view the remote node record.
- **D Delete node** allows you to delete the selected node. For more information, see Deleting a Remote Node Record.

Disabling Sterling Connect:Direct Secure Plus on an SSL or TLS Node

To disable Sterling Connect:Direct Secure Plus on a SSL or TLS node:

Procedure

1. From the **Secure+ Admin Tool Main Screen**, type **U** next to the SSL or TLS node to update and press **Enter**. The **Secure+ Create/Update Panel** displays the information for the selected node.
2. Type **N** beside the **Enable SSL** and **Enable TLS** fields. Select **OK** and press **Enter**.
3. Select **OK** and press **Enter**.
4. Save the Sterling Connect:Direct Secure Plus parameter file using the procedure in Saving Changes to Node Records Using the Save Active Option.

   Note: To continue Sterling Connect:Direct operations with Sterling Connect:Direct Secure Plus disabled, *both* trading partners must disable Sterling Connect:Direct Secure Plus.

Changing the Cipher Suites

About this task

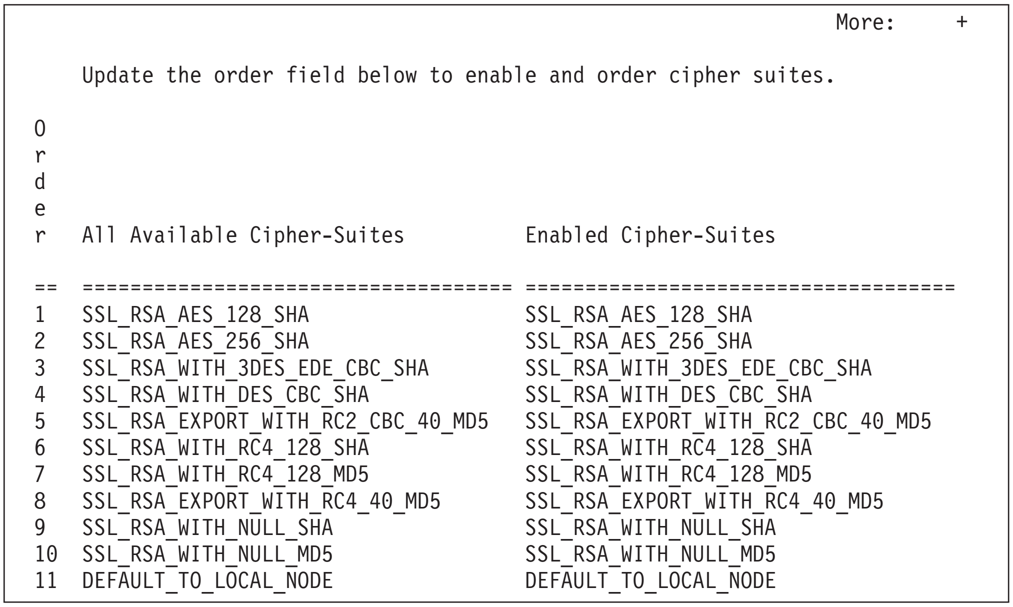
When you activate the SSL or the TLS protocol for a node, cipher suites are used to encrypt transmitted data. The same cipher suite must be defined at both ends of the transmission. Sterling Connect:Direct Secure Plus searches the enabled cipher suite list and locates the first cipher suite that is common for communications at both the PNODE and the SNODE. It then uses this cipher suite to encrypt data. You defined cipher suites when you configured the local node record.

Note: If System SSL is in FIPS mode, only certain ciphers are valid. See the *IBM Sterling Connect:Direct for z/OS Release Notes* for a list of valid FIPS-mode ciphers.

To change the cipher suites enabled for a node and the priorities assigned to them:

Procedure

1. From the **Secure+ Admin Tool Main Screen**, type **U** next to the node to update.
2. On the **Create/Update** Panel, select the **Cipher Suites** field and press **Enter** to display the **Update Cipher Suites** panel.



```
                                                                  More:     +

      Update the order field below to enable and order cipher suites.

  O
  r
  d
  e
  r   All Available Cipher-Suites          Enabled Cipher-Suites

  ==  ==================================== ====================================
  1   SSL_RSA_AES_128_SHA                  SSL_RSA_AES_128_SHA
  2   SSL_RSA_AES_256_SHA                  SSL_RSA_AES_256_SHA
  3   SSL_RSA_WITH_3DES_EDE_CBC_SHA        SSL_RSA_WITH_3DES_EDE_CBC_SHA
  4   SSL_RSA_WITH_DES_CBC_SHA             SSL_RSA_WITH_DES_CBC_SHA
  5   SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5   SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
  6   SSL_RSA_WITH_RC4_128_SHA             SSL_RSA_WITH_RC4_128_SHA
  7   SSL_RSA_WITH_RC4_128_MD5             SSL_RSA_WITH_RC4_128_MD5
  8   SSL_RSA_EXPORT_WITH_RC4_40_MD5       SSL_RSA_EXPORT_WITH_RC4_40_MD5
  9   SSL_RSA_WITH_NULL_SHA                SSL_RSA_WITH_NULL_SHA
  10  SSL_RSA_WITH_NULL_MD5                SSL_RSA_WITH_NULL_MD5
  11  DEFAULT_TO_LOCAL_NODE                DEFAULT_TO_LOCAL_NODE
```

The list on the left side contains all available cipher suites. The active cipher suites are listed on the right side of the screen and are assigned a numerical order in the **Order** column on the left side of the screen.

3. Take one or more of the following actions as needed:
   - Type **1** by the cipher you want to enable and give the highest priority. Type **2** by the cipher suite you want to enable and place second in priority. Continue typing numbers next to the ciphers you want to enable, in order of priority. The ciphers you enable appear in the order of priority in the **Enabled Cipher-Suites** list.
   - To deactivate a cipher suite, clear the number in the **Order** field and press **Enter**.
   - To change the order of a cipher suite, type new numbers in the **Order** fields of the cipher suites to reorder and press **Enter**.
4. Press **PF3** to save the new enabled cipher-suite list and return to the **Secure+ Create/Update Panel**.
5. Save the parameter file using the procedure described in Saving Changes to Node Records Using the Save Active Option.

Inserting a Node

About this task

The **Insert** node option follows the same procedure as creating a remote node manually using the **Edit** menu.

To create a remote node:

Procedure

1. To create a remote node, type **I** next to any node on the **Secure+ Admin Tool Main Screen** and press **Enter**.
2. Type the name of the existing remote node that corresponds to its name in the network map and enter the rest of the information on the **Node Identification** panel. The **Secure+ Create/Update Panel** is displayed.

3. After you finish the procedure and save the record by selecting **OK** and pressing **Enter** , save the parameter file using the procedure described in Saving Changes to Node Records Using the Save Active Option.

Deleting a Remote Node Record

If you remove a remote node record from the network map in Sterling Connect:Direct, you can also remove it from the Sterling Connect:Direct Secure Plus parameter file. This process deletes nodes from the Sterling Connect:Direct Secure Plus parameter file.

About this task

Note: If you have implemented the Strong Password Encryption feature, you cannot use the **Delete** node table line command to delete the.PASSWORD record. To determine if SPE is in effect, see Disabling Strong Password Encryption for instructions on how to access the SPE Parameters screen. You will see either the message, *SPE not currently in use* or *SPE currently in use* on that panel. If SPE is not in use, you can delete the **.PASSWORD** record; otherwise, follow the procedure to disable SPE, and then reinitialize Sterling Connect:Direct. This initialization with SPE disabled will remove any SPE encryption that has been previously applied.

To delete a remote node record:

Procedure

1. Type **D** next to the node to delete and press **Enter**.

   The Sterling Connect:Direct Secure Plus **Confirmation Prompt** displays the message *Are you sure you want to delete 'selected node'?*.
2. Select **OK** and press **Enter** to delete the record.
3. Save the Sterling Connect:Direct Secure Plus parameter file using the procedure in Saving Changes to Node Records Using the Save Active Option.

Chapter 11. Sterling Connect:Direct Secure Plus Statistics

Sterling Connect:Direct logs statistics for Sterling Connect:Direct Process activity. The Sterling Connect:Direct statistics include Sterling Connect:Direct Secure Plus information for a Process.

The following samples of Sterling Connect:Direct Process statistics records contain information for Sterling Connect:Direct Secure Plus support. For information about viewing Sterling Connect:Direct for z/OS Process statistics, refer to the *IBM Sterling Connect:Direct for z/OS User's Guide*.

SSL or TLS Statistics Record

When you use the **Select Statistics** command to view the information about a Sterling Connect:Direct Process that uses SSL or TLS security, you see a screen similar to the following. (Be sure to use the Display option by typing **D** on the CMD line to see the detailed version of the SELECT STATISTICS report.) The Sterling Connect:Direct Secure Plus fields are in bold. A description for the fields follows the samples.

```
===============================================================================
CD.OS390.V40000                 SELECT STATISTICS                    05/04/2010
===============================================================================
_______________________________________________________________________________
Function     => PROCESS SUBMIT          Start Time => 19:30:00
Process Name => OS3903                  Stop Time  => 19:30:00
Process Num  => 1                       Comp Code  => 00000000
                                        Comp Msg   => SSPA001I
Userid       => JWHITE
Primary Node => SC.DUB.JWHITE           Step Name  =>
Submitted DSN=> JWHITE.NDM.PROCESS.LIB(OS3903)
_______________________________________________________________________________
Function     => COPY                    Start Time => 19:30:14
Process Name => OS3903                  Stop Time  => 19:30:14
Process Num  => 1                       Comp Code  => 00000000
                                        Comp Msg   => SCPA000I
Userid       => JWHITE
Secondary Node => SC.DUB.JWHITE         Step Name  => PUSH01
Other addr   => 10.20.201.2
Other port   => 04399

V2 Buffer Size            => 65,536
Negotiated V2 Buffer Size => 65,536
TCP Buffer Size Used      => 262,144
Session Protocol =   TCP
CRC Requested
CRC Not Performed

TLS Enabled         => Yes
TLS Ciphersuite     => TLS_RSA_AES_256_SHA
Subject => (SN=47:b2:1a:10:00:0e:07:72/C=US/ST=a/L=t/O=g/CN=mikey3/)
Issuer  => (C=US/ST=a/L=t/O=g/CN=mikey3/)

***** CHECKPOINTED;    Interval => 1,000
From ( Pnode
 Dsn=>JWHITE.TCPIP.DATA.FILE)
         recs => 0                     blks => 1
    I/O BYTES => 266
   VTAM BYTES => 53
    Cmpr Perc => 80.1%
```

```
       VOL=SER=> USER17
To   ( Snode
 Dsn=>JWHITE.FTST.AA1030B)
         recs => 0                     blks => 1
    I/O BYTES => 266
   VTAM BYTES => 53
    Cmpr Perc => 80.1%
       VOL=SER=> WRKPK3
```

The following statistics are displayed for the copy function:

Field	Description	Valid Values
TLS (or SSL) Enabled	Specifies whether TLS (or SSL) x.509 certificate use is enabled.	Yes No
TLS (or SSL) Ciphersuite	Specifies the cipher suite used in the session and whether the Process defined an override. **Note:** If **ENCRYPT.DATA=N** was in effect, **NONE** appears in this field.	Any valid cipher suite
Subject	Specifies the subject name on the certificate.	Any valid subject name
Issuer	Specifies the issuer name on the certificate.	Any valid issuer name

SSL or TLS Extended Option Statistics Record

When you use the **Select Statistics** command with the extended option enabled to view the information about a Sterling Connect:Direct Process that uses SSL or TLS security, you see a screen similar to the following. The Sterling Connect:Direct Secure Plus fields are in bold. A description for the fields follows the sample.

```
 ===============================================================================
 CD.OS390.V40000                 SELECT STATISTICS                    05/04/2010
 ===============================================================================


 _______________________________________________________________________________
 Function     => PROCESS SUBMIT            Start Time => 10:26:32
 Process Name => STATSAMP                  Stop Time  => 10:26:32
 Process Num  => 338                       Comp Code  => 00000000
                                                    Comp Msg   => SSPA001I
 Userid       => $CD
 Primary      => CD.OS390.V40000           Step Name  =>
 Submitted DSN=> $CD.CD.PROCESS(SUB1)
 _______________________________________________________________________________
Function     => Session Begin          Start Time => 19:30:14
                                       Start Date => 2008.11.17

Process Name => OS3903
Process Num  => 1                      Comp Code  => 00000000
                                       Comp Msg   => SVTM055I

Userid       => JWHITE
Primary Node   => SC.DUB.JWHITE
Secondary Node => SC.DUB.JWHITE2
Submitter Node => SC.DUB.JWHITE3

TLS Enabled         => Yes
TLS Ciphersuite => TLS_RSA_AES_256_SHA
Subject => (SN=47:b2:1a:10:00:0e:07:72/C=US/ST=a/L=t/O=g/CN=mikey3/)
Issuer  => (C=US/ST=a/L=t/O=g/CN=mikey3/)

Session Protocol =   TCP
Socket for Origin      => 04199  ; 10.20.201.2
Socket for Destination => 04399  ; 10.20.201.2
Bind Attempts => 0
Remote Node Communications Address => 10.20.201.2
________________________________________________________________________________
Function     => COPY                   Start Time => 19:30:14
Process Name => OS3903                 Stop Time  => 19:30:14
Process Num  => 1                      Comp Code  => 00000000
                                       Comp Msg   => SCPA000I
Userid       => JWHITE
Secondary Node => SC.DUB.JWHITE        Step Name  => PUSH01
Other addr   => 10.20.201.2
Other port   => 04399

V2 Buffer Size            => 65,536
Negotiated V2 Buffer Size => 65,536
TCP Buffer Size Used      => 262,144
Session Protocol =   TCP
CRC Requested
CRC Not Performed

TLS Enabled         => Yes
TLS Ciphersuite => TLS_RSA_AES_256_SHA
Subject => (SN=47:b2:1a:10:00:0e:07:72/C=US/ST=a/L=t/O=g/CN=mikey3/)
Issuer  => (C=US/ST=a/L=t/O=g/CN=mikey3/)

***** CHECKPOINTED;    Interval => 1,000
From ( Pnode
 Dsn=>JWHITE.TCPIP.DATA.FILE)
        recs => 0                      blks => 1
    I/O BYTES => 266
   VTAM BYTES => 53
    Cmpr Perc => 80.1%
       VOL=SER=> USER17
To   ( Snode
 Dsn=>JWHITE.FTST.AA1030B)
        recs => 0                      blks => 1
    I/O BYTES => 266
   VTAM BYTES => 53
    Cmpr Perc => 80.1%
       VOL=SER=> WRKPK3
```

The following fields are included for the Sterling Connect:Direct for z/OS extended option statistics:

Field	Description	Valid Values
TLS (or SSL) Enabled	Specifies whether TLS (or SSL) x.509 certificate use is enabled.	Yes No
TLS (or SSL) Ciphersuite	Specifies the cipher suite used in the session and whether the Process defined an override.	Any valid cipher suite
Subject	Specifies the subject name on the certificate.	Any valid subject name
Issuer	Specifies the issuer name on the certificate.	Any valid issuer name

Chapter 12. Troubleshooting

Use the following table to help troubleshoot problems with Sterling Connect:Direct Secure Plus:

Note: For all errors related to Strong Password Encryption, see SPE Problem Troubleshooting.

Problem	Possible Cause	Solution
System initialization failed, and the following SITA196E error message is displayed: FIPS Mode Requested but SECURE.DSN parameter is not specified.	You specified the FIPS initialization parameter as YES, but you did not specify the SECURE.DSN parameter to enable Sterling Connect:Direct Secure Plus.	Update the initialization parameters and restart Sterling Connect:Direct.
System initialization failed, and the following error message is displayed: Connect;Direct FIPS keyword requires z/OS release 1.11 or later.	Your current, active z/OS release level does not support FIPS mode for System SSL.	Either update the FIPS initialization parameter to NO or execute Sterling Connect:Direct on the appropriate release level of z/OS.
Sterling Connect:Direct was terminated, and the following error message is displayed: Secure+ Severe FIPS Mode Error, &var1.	During operation of a TLS FIPS mode request, a severe error occurred causing Sterling Connect:Direct to terminate with a U4079 abend due to one of the following: • KEY database (not FIPS-mode) • Random number generation failure • RSA or DSA keypair generation failure • gsk_perform_kat API failure	Contact IBM Support or correct the error and restart Sterling Connect:Direct .
The following message is received at startup: SITA166I or SITA167I Secure+ SSL or TLS initialization failed. rc=00000134, rs=NO DFLT UNIX PATH.	The Sterling Connect:Direct system does not have a default directory created for it in UNIX system services. The DLL files and other facilities related to SSL or TLS require the presence of a default UNIX directory.	Contact your z/OS system programmer.
The following message is received at startup: SITA166I Secure+ SSL or TLS initialization failed. rc=000000002, rs=GSK_KEYFILE_OPEN_ FAILED.	The Sterling Connect:Direct Secure Plus parameter file, with the SECURE.SSL.PATH.PREFIX initialization parameter, specifies a nonexistent key database, the key database has incorrect file permissions, OR the PASSWORD typed IS INCORRECT.	Correct the name specified in the initialization parameter or the Sterling Connect:Direct Secure Plus parameter file, the UNIX permissions, or the password.

Problem	Possible Cause	Solution
The following message is received at startup or when Sterling Connect:Direct performs a certificate validation check and discovers a certificate that will soon expire: CSPA600W WARNING Cert: &cert for Node: &node expires: &date. The named certificate will expire on the specified date. **Note:** A message will not contain the node name if the certificate did not have a Sterling Connect:Direct Secure Plus parameter file record associated with it.	The warning message will appear based on the validation check controlled by the following initialization parameters, CHECK.CERT.EXPIRE, CHECK.CERT.WARN.DAYS and CHECK.CERT.EXPIRE.TIME.	Take the appropriate action to generate or obtain a new certificate.
The following message is received at startup or when Sterling Connect:Direct performs a certificate validation check and discovers that a certificate has expired: CSPA601E ERROR Cert: &cert for Node: &node expired on: &date. The named certificate has expired on the specified date. **Note:** A message will not contain the node name if the certificate did not have one associated with it.	The warning message will appear based on the validation check controlled by the following initialization parameters, CHECK.CERT.EXPIRE.	Take the appropriate action to generate or obtain a new certificate.
The following message is received at startup or when Sterling Connect:Direct performs a certificate validation check and discovers a certificate it cannot validate: CSPA607W WARNING Cert: &cert for Node: &node does not exist. The Certificate Expiration Validation function has obtained a Certificate label for the Secure Parmfile however that certificate can not be retrieved. **Note:** A message will not contain the node name if the certificate did not have one associated with it.	The most likely cause of this is the certificate does not exist in the Key database or Key ring.	Ensure that the Certificate exist and that the Secure Parmfile entry specifies the correct label name. The label is case sensitive and must match exactly.
The following message is received when an SSL or TLS Process is run: SSL or TLS handshake failure, reason= GSK_ERROR_SOCKET_CLOSED.	The trading partners have not enabled a matching cipher suite.	Update the remote node record for the trading partner to enable a cipher suite recognized by the trading partner and resubmit the Process.
The following message is received: CSPA202E SSL handshake failure, reason=GSK_ERROR_BAD_ CERTIFICATE.	The certificate is not valid on the system issuing GSK_ERROR_BAD_CERT. This error occurs if the certificate is not validated on any local trusted CA certificate. This error is common if you use self-signed certificates because the remote Sterling Connect:Direct system does not have the CA certificate.	Verify that each trading partner can validate the certificates of other trading partners and resubmit the Process. Ensure that the remote node record for the trading partner has enabled the correct protocol.

Problem	Possible Cause	Solution
The following error is received from the SNODE: CSPA202E SSL or TLS handshake failure, reason= GSK_ERROR_UNKNOWN_ERROR.	A conflict within the IBM System SSL toolkit occurred because a certificate being processed did not use version 3 of the toolkit.	Ensure that all certificates and CA certificates are using version 3.
Sterling Connect:Direct Secure Plus features are enabled in the Sterling Connect:Direct Secure Plus parameter file, but the statistics record indicates that these functions are disabled.	The Sterling Connect:Direct network maps do not contain entries for the PNODE and SNODE. The node that you are connecting with is a V1 flow (such as LU0 or Netex). Sterling Connect:Direct Secure Plus is not supported for V1 flows because of reliance on XDR support.	Verify that the network map entries for both the PNODE and the SNODE exist, and use a V2 protocol such as LU6.2 ,TCP/IP, or UDT. Check for the existence of the extended statistics record for Session Begin (the SB record). This record is only created in V2 flows. The absence of this record indicates V1 flows were used.
Sterling Connect:Direct Secure Plus parameters specified from the copy statement cause the copy step to fail with message CSPA077E.	The node that you are connecting with is a V1 flow (such as LU0 or Netex). Sterling Connect:Direct Secure Plus is not supported for V1 flows because of reliance on XDR support.	Check for the existence of the extended statistics record for Session Begin (the SB record). This record is only created in V2 flows. The absence of this record indicates V1 flows were used.
An error occurs in ESTAE with a bad return code (RC=3) when running a Process with a remote node and the Process fails.	The value for Sterling Connect:Direct Secure Plus Export version is incorrect in the remote node definitions for one or both of the nodes. If one node is EXPORT and the other node is NOT EXPORT, the elliptic curves that enable you to create keys and generate Diffie-Hellman shared secrets are not correct.	Verify that the remote node definitions on both sites accurately state the Sterling Connect:Direct Secure Plus Export information.
Running a Process with a remote node fails with an authentication error.	Unique public/private key pairs are generated for the remote node record and the local node record is set to OVERRIDE=N.	Change the local node record to OVERRIDE=Y or do not use unique public/private key pairs in the remote node record.
The **Save Active** option is not selectable.	You can only use the Save Active function once each time you open the Sterling Connect:Direct Secure Plus parameter file.	Reopen the Sterling Connect:Direct Secure Plus parameter file to use the Save Active function or use the Save As function.
The text entry fields on the **Create/Update** panel of the Secure+ Admin Tool are not visible.	The CUA attributes in your ISPF profile are not set correctly.	Change the value for **Normal Text entry** in the CUA attributes of the ISPF profile to **uscore** in the **Highlight** column.
The Sterling Connect:Direct Secure Plus parameter, ENCRYPT.DATA specified from the copy statement causes the copy step to fail with an error message CSPA080E.	The algorithm name used in the COPY statement is not in the supported algorithm list for both nodes.	Verify that the algorithm name in the copy statement is in the supported algorithm list for both nodes.

Problem	Possible Cause	Solution
A Process including a COPY statement with a SECURE parameter was submitted and failed. The following CSPA011E error message is displayed: Illegal attempt to override Sterling Connect:Direct Secure Plus parameters	You attempted to use the SECURE parameter in a COPY statement but did not specify OVERRIDE=Y in the remote node record to enable the security override feature.	Take one of the following actions: • Remove the SECURE= parameter from the COPY statement and resubmit the Process. • Change the OVERRIDE setting in the remote node record in the parameter file and make sure all other necessary protocol settings are specified. Resubmit the Process including the SECURE= parameter. See Override Settings in Sterling Connect:Direct Processes.
An SSL or TLS session was attempted with a Sterling Connect:Direct system that does not implement SSL or TLS.	The trading partner does not have the protocol enabled.	Request that the trading partner configure its node for the correct protocol or disable Sterling Connect:Direct Secure Plus for the node.
Either the CSPA203E error message or the CSPA204E message is displayed: SSL or TLS send failure, rc=&RC, rsn=&RSN or SSL or TLS receive failure, rc=&RC, rsn=&RSN.	The client cannot validate the server's certificate.	Ensure that client authentication is turned on and certificate information is defined in the remote node record.
The following CSPA205E error message is displayed: SSL or TLS support requires the TCP/IP protocol.	One of the trading partners is not using TCP/IP for communications.	Determine which trading partner does not have TCP/IP enabled and change the configuration of that trading partner.
The following CSPA200E error message is displayed: Sterling Connect:Direct Secure Plus version mismatch.	You are attempting to use the SSL or TLS protocol to securely communicate with a trading partner that does not have the protocol enabled.	Change the configuration of the remote node record to enable the correct protocol.
The following CSPA206E error message is displayed: Remote certificate is invalid.	The root certificate was not found.	Check the parameter file configuration and ensure that the correct certificate is identified in the remote node record.
The following CSPA207E error message is displayed: Root certificate not found.	The remote certificate could not be validated.	Check the parameter file configuration and ensure the correct key database file is identified in the remote node record.
The following SITA1901 error message is displayed: Sec+ Init failed. Secure= No. Override=No.	The local node record has all Sterling Connect:Direct Secure Plus protocols disabled and has override set to no.	Either enable the appropriate protocol in the remote node record or enable override=yes in the local node record.

Problem	Possible Cause	Solution
A Process was submitted and failed. The following CSPA078E error message is displayed: Invalid specification of SECURE= on PROCESS statement. SECURE= cannot be specified in a non-Sterling Connect:Direct Secure Plus environment or when the Remote Node record in the Sterling Connect:Direct Secure Plus Parmfile does not specify OVERRIDE=Y.	You attempted to use the SECURE parameter in a PROCESS statement but did not specify OVERRIDE=Y in the remote node record to enable the security override feature.	Take one of the following actions: • Remove the SECURE= parameter from the PROCESS statement and resubmit the Process. • Change the OVERRIDE setting in the remote node record in the parameter file and make sure all other necessary protocol settings are specified. Resubmit the Process including the SECURE= parameter. See Override Settings in Sterling Connect:Direct Processes.
The submit within a Process failed with a reason code of 8. The following SCBI514E or SSUB267E error message is displayed: Equal sign required after SECURE keyword. The SECURE keyword in the PROCESS must be followed by an equal sign.	You attempted to use the SECURE parameter in a PROCESS statement but did not include an equal sign after the SECURE keyword.	Correct the PROCESS statement syntax by inserting an equal sign and resubmit the Process.
The submit within a Process failed with a reason code of 8. The following SCBI515E or SSUB268E error message is displayed: A parsing error occurred on the SECURE keyword when processing the SECURE keyword on the PROCESS statement.	You attempted to use the SECURE parameter in a PROCESS statement but the syntax was faulty.	Correct the PROCESS statement and resubmit the Process. For a complete description of the SECURE parameter and how to use it in the PROCESS statement, see the see the *Sterling Connect:Direct Process Language Reference Guide*.
System initialization failed, and the following SITA196E error message is displayed: FIPS Mode Requested but SECURE.DSN parameter is not specified.	You specified the FIPS initialization parameter as YES, but you did not specify the SECURE.DSN parameter to enable Sterling Connect:Direct Secure Plus.	Update the initialization parameters and restart IBM Sterling Connect:Direct.
System initialization failed, and the following error message is displayed: Connect;Direct FIPS keyword requires z/OS release 1.11 or later.	Your current, active z/OS release level does not support FIPS mode for System SSL.	Either update the FIPS initialization parameter to NO or execute Sterling Connect:Direct on the appropriate release level of z/OS.
Sterling Connect:Direct was terminated, and the following error message is displayed: Secure+ Severe FIPS Mode Error, &var1.	During operation of a TLS FIPS mode request, a severe error occurred causing Sterling Connect:Direct to terminate with a U4079 abend due to one of the following: • KEY database (not FIPS-mode) • Random number generation failure • RSA or DSA keypair generation failure • gsk_perform_kat API failure	Contact IBM Support or correct the error and restart Sterling Connect:Direct.

Chapter 13. Certificate Parameter Definitions

This topic describes the certificate parameter definitions for certificates created by the RACF application, GSKKYMAN utility, CA-ACF2 application, and CA-ACF2 application.

RACF Application Certificate Parameter Definitions

To avoid some problems associated with CA-signed and self-signed certificates, refer to the following information about certificate parameter definitions required to use Sterling Connect:Direct Secure Plus for z/OS. Minimum parameter definitions for certificates generated with the RACF, gskkyman, CA-ACF2, and CA-Top Secret security applications are provided.

If you plan to use FIPS mode, see *z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08* for more information about System SSL and FIPS mode.

You may also want to record the parameter definitions you configure for certificates on the worksheets provided for the local and remote node records in Configuration Worksheets.

This table describes the minimum parameter definitions required for Sterling Connect:Direct Secure Plus for z/OS. When two parameters are listed in the same row, the first parameter name is used when you create a certificate and the second parameter name is its equivalent, which is used when you display information about the certificate. Consult the RACF documentation for detailed information about all the certificate parameters and commands.

RACF Parameter	Description	Value Used for Sterling Connect:Direct Secure Plus
User ID	Security ID used to start the Sterling Connect:Direct Job or Started Task.	RACF-defined ID
Label	Certificate label. LABEL keywords are case and blank sensitive; therefore, the values specified for these keywords must be exact.	Information that identifies the certificate, for example, CD Secure Plus **Note:** Specify the exact value in the **Certificate Label** field in the Local Node record of the Sterling Connect:Direct Secure Plus parameter file.
Status	Status of the certificate.	Status=TRUST All certificates used by Sterling Connect:Direct Secure Plus for z/OS must be Trusted.
NOTBEFORE Start Date	Specifies the local date and time from which the certificate is valid.	Must be a valid date and time

RACF Parameter	**Description**	**Value Used for Sterling Connect:Direct Secure Plus**
NOTAFTER End Date	Specifies the local date and time after which the certificate is no longer valid. All certificates used in the SSL/TLS handshake, including issuer certificates, must not be expired.	Must be a valid date and time
Key Usage	Facilitates identification and key exchange during SSL/TLS security handshakes.	HANDSHAKE (**Required**): Indicates that digital signature and key encipherment are enabled. DOCSIGN (Optional): Indicates that non-repudiation is enabled. DATAENCRYPT (Optional): Indicates that data encipherment is enabled. CERTSIGN: Indicates the certificate can sign other digital certificates and CRLs. **Note:** Do not specify CERTSIGN. Only Certificate Authority (Issuer) certificates should have keyCertSign and cRLSign indicators.
X.509 Subject's Distinguished Name Issuer's Name	Specifies the distinguished name of the issuer that issued or signed a certificate. The name identifies the trusted certificate of the issuer or CA that signed the server certificate. The name identifies the trusted certificate of the issuer or CA that signed the server certificate. The CA or entity certificate with that name must be available within the key database or Keyring. The Issuer Name keywords are case and blank sensitive. **Note:** Self-signed certificates display the same information in the Issuer Name and Subject Name parameters.	The following fields, which must be enclosed in single quotes, are attributes of the Issuer's Name parameter and the Subject's Name parameter: CN=Common Name of the certificate in single quotes, for example, 'RACF SELF SIGN COMMON' T=*'Title of person creating certificate'* OU=*'Organizational Unit associated with the person creating the certificate'* O=*'Organization for which the certificate is being created'* L=*'Locality (city) of the entity for which the certificate is created'* SP=*'State/Province of the locality'* C=*'Country of the locality'*
X.509 Subject's Distinguished Name Subject's Name	Specifies the certificate's subject distinguished name. It identifies the certificate. This name can identify certificates that may have issued or signed other certificates and can match to other certificates Issuer's Name.	

RACF Parameter	Description	Value Used for Sterling Connect:Direct Secure Plus
Private Key Size	Specifies the size of the private key expressed in decimal bits. Key size of 1024 provides a secure encryption. A larger size provides a more secure encryption but requires more CPU to encrypt.	
Private Key Type	Specifies how the private key should be stored for future use. Type can be none, non-ICSF, or ICSF. If Type= none, the certificate does not have a private key.	If ICSF is specified, see Sterling Connect:Direct Access to System Resources for SSL or TLS for requirements.
Ring Name	Specifies the name of the keyring that a certificate is connected with.	If you use a key ring, the exact value in this field must be specified in the **Certificate Pathname** field for the Local Node record in the Sterling Connect:Direct Secure Plus parameter file.
Usage	Specifies how this certificate should be used in a keyring for the USERID of the person submitting a batch job or signed on to TSO.	PERSONAL
Default	Specifies that the certificate is the default certificate. Only one certificate can be the default certificate. Define the end-user server certificate of the local Sterling Connect:Direct node as the default.	YES

GSSKYMAN Utility Certificate Parameter Definitions

This table describes the minimum parameter definitions required for Sterling Connect:Direct Secure Plus for z/OS. Consult the GSKKYMAN documentation for detailed information about all the certificate parameters and commands. If you plan to use FIPS mode, see *z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08* for more information about System SSL and FIPS mode.

GSKKYMAN Parameter	Description	Value Required for Sterling Connect:Direct Secure Plus Option
Label	Certificate label. LABEL keywords are case and blank sensitive; therefore, the values specified for these keywords must be exact.	Information to identify the certificate, for example, CD Secure Plus **Note:** Specify the exact Label value in the **Certificate Label** field in the local node record of the Sterling Connect:Direct Secure Plus parameter file.
Version	X.509 certificates with version number 3 are supported.	3
Trusted	Specifies the certificate status.	Yes

GSKKYMAN Parameter	Description	Value Required for Sterling Connect:Direct Secure Plus Option
Effective Date	Specifies the local date and time from which the certificate is valid.	Must be a valid date and time
Expiration Date	Specifies the local date and time after which the certificate is no longer valid. All certificates used in the SSL/TLS handshake, including issuer certificates, must not be expired.	Must be a valid date and time
keyUsage	Facilitates identification and key exchange during SSL/TLS security handshakes.	Digital Signature (**Required**) Non-repudiation Key encipherment Data encipherment
Issuer Name	Specifies the distinguished name of the Issuer that issued or signed a certificate. The name identifies the trusted certificate of the issuer or CA that signed the server certificate. The CA or entity certificate with that name must be available within the key database or keyring. The Issuer Name keywords are case and blank sensitive. Self-signed certificates have the same Issuer name and Subject name.	
Certificate Subject Name	Specifies the certificate's subject distinguished name. It identifies the certificate. This name can identify certificates that may have issued or signed other certificates and can match to other certificates Issuer's Name.	The following fields are attributes of the Certificate Subject Name parameter: CN=Common Name of the certificate in single quotes, for example, ‘RACF SELF SIGN COMMON' T=*'Title of person creating certificate'* OU=*'Organizational Unit associated with the person creating the certificate'* O=*'Organization for which the certificate is being created'* L=*'Locality (city) of the entity for which the certificate is created'* SP=*'State/Province of the locality'* C=*'Country of the locality'*

GSKKYMAN Parameter	Description	Value Required for Sterling Connect:Direct Secure Plus Option
Public Key Algorithm	Specifies the algorithm used to encrypt data.	
Public Key Size	Specifies the size of the public key expressed in decimal bits. Key size of 1024 provides a secure encryption. A larger size provides a more secure encryption but requires more CPU to encrypt.	
Key database password	Specifies the password used when you created a key database file.	When you specify a gskkyman key database file name in the **Certificate Pathname** field for the local node record, you must specify the key database password in the **Certificate Pathname Pass Phrase** field**.**

CA-ACF2 Application Certificate Parameter Definitions

This table describes the minimum parameter definitions required for Sterling Connect:Direct Secure Plus for z/OS. Consult the CA-ACF2 documentation for detailed information about all the certificate parameters and commands.

CA-ACF2 Parameter	Description	Value Used by Sterling Connect:Direct Secure Plus Option
ACID	Security ID used to start the Sterling Connect:Direct Job or Started Task.	CA-ACF2 defined ID
Label	Certificate label. LABEL keywords are case and blank sensitive; therefore, the values specified for these keywords must be exact.	Information that identifies the certificate, for example, CD Secure Plus **Note:** Specify the exact value in the **Certificate Label** field in the Local Node record of the Sterling Connect:Direct Secure Plus parameter file.

CA-ACF2 Parameter	Description	Value Used by Sterling Connect:Direct Secure Plus Option
Subjsdsn	Specifies the subject's distinguished name. It identifies the certificate. This name can identify certificates that may have issued or signed other certificates and can match to other certificates Issuer's Name.	The following fields, which must be enclosed in single quotes, are attributes of the Issuer's Name parameter and the Subject's Name parameter: CN=Common Name of the certificate in single quotes, for example, 'RACF SELF SIGN COMMON' T=*'Title of person creating certificate'* OU=*'Organizational Unit associated with the person creating the certificate'* O=*'Organization for which the certificate is being created'* L=*'Locality (city) of the entity for which the certificate is created'* SP=*'State/Province of the locality'* C=*'Country of the locality'*
Size	Specifies the size of the private encryption key in bits.	
Active	Specifies the local date and time from which the certificate is valid.	Must be a valid date and time
Expire	Specifies the local date and time after which the certificate is no longer valid. All certificates used in the SSL/TLS handshake, including issuer certificates, must not be expired.	Must be a valid date and time
Keyusage	KeyUsage certificate extension, of which one or more of the following values might be coded.	HANDSHAKE (**Required**): Indicates that digital signature and key encipherment are enabled. DOCSIGN (Optional): Indicates that non-repudiation is enabled. DATAENCRYPT (Optional): Enables the certificate to be used to. CERTSIGN: Indicates the certificate can sign other digital certificates and CRLs. **Note:** Do not specify CERTSIGN. Only Certificate Authority (Issuer) certificates should have keyCertSign and cRLSign indicators.

CA-ACF2 Parameter	Description	Value Used by Sterling Connect:Direct Secure Plus Option
KEYRING	Specifies the record key of a KEYRING record to which the certificate is associated.	If you use a keyring, the value in this field must be specified in the **Certificate Label** field for the Local Node record in the Sterling Connect:Direct Secure Plus parameter file.
RINGNAME	Specifies the ring name of a KEYRING record to which the certificate information is associated.	If you use a keyring, the value in this field must be specified in the **Certificate Pathname** field for the Local Node record in the Sterling Connect:Direct Secure Plus parameter file.
USAGE	Specifies how this certificate should be used in a keyring for the USERID of the person submitting a batch job or signed on to TSO.	PERSONAL
DEFAULT	Specifies that the certificate is the default certificate. Only one certificate can be the default certificate. Define the end-user server certificate of the local Sterling Connect:Direct node as the default.	YES

CA-Top Secret Application Certificate Parameter Definitions

This table describes the minimum parameter definitions required for Sterling Connect:Direct Secure Plus for z/OS. Consult the CA-ACF2 documentation for detailed information about all the certificate parameters and commands.

CA-Top Secret Parameter	Description	Value Used for Sterling Connect:Direct Secure Plus Option
SUBJECTDSN	Specifies the subject's distinguished name. It identifies the certificate. This name can identify certificates that may have issued or signed other certificates and can match to other certificates Issuer's Name.	The following fields, which must be enclosed in single quotes, are attributes of the Issuer's Name parameter and the Subject's Name parameter: CN='Common Name of the certificate in single quotes,' for example, 'RACF SELF SIGN COMMON' T=*'Title of person creating certificate'* OU=*'Organizational Unit associated with the person creating the certificate'* O=*'Organization for which the certificate is being created'* L=*'Locality (city) of the entity for which the certificate is created'* SP=*'State/Province of the locality'* C=*'Country of the locality'* UID=*'userid'*
UID	Security ID used to start the Sterling Connect:Direct Job or Started Task.	CA-Top Secret defined ID
NBDATE/ NBTIME	Specifies the local date and time from which the certificate is valid.	Must be a valid date and time
NADATE/ NATIME	Specifies the local date and time after which the certificate is no longer valid. All certificates used in the SSL/TLS handshake, including issuer certificates, must not be expired.	Must be a valid date and time
KEYSIZE	Specifies the size of the private encryption key in bits.	
LABLCERT	Certificate label. LABEL keywords are case and blank sensitive; therefore, the values specified for these keywords must be exact. This parameter is specified when you associate a certificate with an ACID.	Information to identify the certificate, for example, CD Secure Plus **Note:** Specify the exact value in the **Certificate Label** field in the Local Node record of the Sterling Connect:Direct Secure Plus parameter file.

CA-Top Secret Parameter	Description	Value Used for Sterling Connect:Direct Secure Plus Option
ICSF	If Private Key type is ICSF, the private key is stored in the ICSF PKDS (public key data set). Access to the private key then requires that the ICSF application be executing and Sterling Connect:Direct have access authority to the ICSF application	If ICSF is specified, see Sterling Connect:Direct Access to System Resources for SSL or TLS for requirements.
TRUST | NOTRUST	Specifies the status of the certificate when you associate a certificate with an ACID.	TRUST
KEYRING	Specifies the key ring being added to the user's ACID.	If you use a keyring, the value in this field must be specified in the **Certificate Label** field for the Local Node record in the Sterling Connect:Direct Secure Plus parameter file.
LABLRING	Specifies the label to be associated with the keyring being added to the user, which is used as the identifier of the digital certificate.	If you use a keyring, the value in this field must be specified in the **Certificate Pathname** field for the Local Node record in the Sterling Connect:Direct Secure Plus parameter file.
DEFAULT	Specifies how this certificate should be used in a keyring for the USERID of the person submitting a batch job or signed on to TSO.	PERSONAL
USAGE	Specifies that the certificate is the default certificate. Only one certificate can be the default certificate. Define the end-user server certificate of the local Sterling Connect:Direct node as the default.	YES

Chapter 14. Configuration Worksheets

Use the worksheets in this topic to record the configuration information for Sterling Connect:Direct Secure Plus for z/OS .

Local Node Security Feature Definition Worksheet

Record the security feature definitions for the Sterling Connect:Direct Secure Plus local node record on this worksheet. Refer to this worksheet as you configure the local node record. If you plan to use FIPS mode, see "Planning for System SSL in FIPS Mode" on page 6 and *z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08*.

Local Node Name:____	
TLS protocol enabled: **Note:** If System SSL is in FIPS mode, TLS is the only supported protocol. See "Planning for System SSL in FIPS Mode" on page 6.	Yes _____ No ______
SSL protocol enabled:	Yes _____ No ______
Configured Security Functions	
Override enabled:	Yes _____
Encryption enabled:	Yes _____ No ______
Authorization Timeout: Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP.TIMER initialization parameter.	_________(Numeric value equal to or greater than 0 seconds)
Certificate Label (label specified when the certificate was generated using one of the security applications; may be called LABLCERT): **Note:** If System SSL is in FIPS Mode, the Certificate Label has FIPS requirements. See "Planning for System SSL in FIPS Mode" on page 6.	____ Valid only for SSL or TLS
Certificate Pathname: key database or key ring **Note:** If System SSL is in FIPS Mode, the Certificate Pathname has FIPS requirements. See "Planning for System SSL in FIPS Mode" on page 6.	____ Valid only for SSL or TLS
Password: Valid only for certificates created in a gskkyman database; leave blank for key rings.	_________________________________
Cipher Suite(s) to Enable: Applies only to SSL and TLS **Note:** If System SSL is in FIPS mode, only certain ciphers are valid. See the *IBM Sterling Connect:Direct for z/OS Release Notes* for a list of valid FIPS-mode ciphers.	____

Local Node Name:____	
Enable External Authentication: Applies only to SSL and TLS	Yes _____ No ______

Remote Node Security Feature Definition Worksheet

Record the security feature definitions for a remote node record on this worksheet. Make a copy of this worksheet for each remote node defined in the Sterling Connect:Direct Secure Plus parameter file that you are configuring for Sterling Connect:Direct Secure Plus operations. Refer to this worksheet when you configure a remote node record.

Remote Node Name:	____
Security Options	
TLS protocol enabled:	Yes _____ No ______
SSL protocol enabled:	Yes _____ No ______
Enable Override: When override is enabled in a remote node record, values in the PROCESS statement override values in the remote node record that uses either protocol.	Yes _____ No ______ Default to local node ______
Encryption enabled:	Yes _____ No ______
Enable External Authentication: Valid only for SSL or TLS	Yes _____ No ______ Default to local node ______
TLS or SSL Protocol Functions	
If you enabled the TLS or SSL protocol and you did not define this information in the local node record, set one or more of the following functions:	
Certificate Label: Label specified when the certificate was generated using one of the security applications; may be called LABLCERT.	____ You can type an asterisk (*) to default to the local node record.
Cipher Suite(s) Enabled:	____
Ask the trading partner which cipher suites are enabled. Circle all applicable cipher suites.	
• SSL_RSA_WITH_AES_128_SHA • SSL_RSA_WITH_AES_256_SHA • SSL_ RSA_WITH_3DES_EDE_CBC_SHA • SSL_RSA_WITH_DES_CBC_SHA • SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5 • SSL_RSA_WITH_RC4_40_SHA • SSL_RSA_WITH_RC4_128_MD5 • SSL_RSA_EXPORT_WITH_RC4_40_MD5 • SSL_RSA_WITH_NULL_SHA • SSL_RSA_WITH_NULL_MD5	• TLS_RSA_WITH_AES_128_SHA • TLS_RSA_WITH_AES_256_SHA • TLS_(or TLS_) RSA_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_DES_CBC_SHA • TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 • TLS_RSA_WITH_RC4_40_SHA • TLS_RSA_WITH_RC4_128_MD5 • TLS_RSA_EXPORT_WITH_RC4_40_MD5 • TLS_RSA_WITH_NULL_SHA • TLS_RSA_WITH_NULL_MD5

Certificate Pathname key database or key ring	____ You can type an asterisk (*) to default to the local node record.
To add a second level of security by enabling Client Authentication, set the following two options:	
Enable Client Authentication:	Yes _____ No ______
If client authentication is enabled, specify the certificate common name of the local node certificate in the **Client Auth. Compare** field.	____

.EASERVER Node Security Feature Definition Worksheet

Use the following worksheet to record information to configure the remote node record for .EASERVER node. Refer to this worksheet when you configure the .EASERVER remote node record.

Remote Node Name:	**.EASERVER (Required)**
TLS protocol enabled:	**Yes _____ No ______**
SSL protocol enabled	Yes _____ No ______
Note: You must enable either SSL or TLS to communicate with the Sterling External Authentication server.	
External Auth Server Def	____ Name of the certificate validation definition configured on the Sterling External Authentication Server that defines how to validate certificates. This parameter is case sensitive.
External Auth Server Address	____ IP address of server for the Sterling External Authentication Server application
External Auth Server Port	____ Number of the port to use to connect to the Sterling External Authentication Server
Client Authentication enabled:	Yes _____
Client Authentication Common Name: If client authentication is enabled, specify the certificate common name of the local node certificate in the **Client Auth. Compare** field.	____
Certificate Label:	____ You can type an asterisk (*) in the Certificate Label field to default to the local node record.
Certificate Pathname key database or key ring	____ You can type an asterisk (*) in the Certificate Pathname field to default to the local node record.

.CLIENT Node Security Feature Definition Worksheet

Record the security feature definitions for a remote node record named .CLIENT that you create to allow secure connections. Refer to this worksheet when you configure the .CLIENT node record.

Remote Node Name:	**.CLIENT (Required)**
Note: The node name must be defined as .CLIENT to allow secure connections.	
Security Options	
Autoupd enabled:	Yes _____ No ______
TLS protocol enabled:	Yes _____ No ______
SSL protocol enabled:	Yes _____ No ______
Enable Override:	Yes _____ No ______
ISPF IUI and Batch Interface Options	
ISPF IUI protocol defined as SNA:	Yes _____ No ______
Batch interface protocol defined as SNA	Yes _____ No ______

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.

Index

Product Number: 5655-X01

Printed in USA