

Sterling Connect:Direct Secure Plus for z/OS



Implementation Guide

Version 5.1.1

Sterling Connect:Direct Secure Plus for z/OS



Implementation Guide

Version 5.1.1

Note

Before using this information and the product it supports, read the information in "Notices" on page 185.

This edition applies to version 5.1.1 of IBM Sterling Connect:Direct Secure Plus for z/OS and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 1999, 2012.**

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

Contents

Chapter 1. Sterling Connect:Direct

Secure Plus for z/OS Overview 1

Security Concepts.	1
Security Protocols.	2
Transport Layer Security Protocol and Secure	
Sockets Layer Protocol	2
Station-to-Station Protocol	3
Planning for System SSL in FIPS Mode	4
Sterling Connect:Direct Secure Plus Tools	4
Administration Tool	4
Sterling Connect:Direct Secure Plus Parameter File	6
Access File	7
Sterling Control Center	7
Prerequisites	8
Expert Security Administrator	8
Sterling Connect:Direct ISPF Libraries in TSO	8
Security Requirements of Trading Partners	8
Implementation Plan for Sterling Connect:Direct	
Secure Plus	9
Worksheets	9
Sterling Connect:Direct Secure Plus for z/OS	
Documentation	9
Task Overview.	9

Chapter 2. Plan Your Implementation of the SSL or TLS Protocol 11

Transport Layer Security Protocol and Secure	
Sockets Layer Protocol.	11
TLS or SSL Protocol Processing.	12
Sterling Connect:Direct Secure Plus Data	
Exchange	12
Sterling Connect:Direct Access to System Resources	
for SSL or TLS	13
Self-Signed and CA-Signed Certificates	14
Terminology and Security Applications for SSL	
and TLS Certificates	15
General Requirements for Certificates.	18
Application-Specific Requirements.	18
Server Certificates and Sterling Connect:Direct.	18
Server Certificate	18
Setting Up Sterling Connect:Direct to Use	
Certificates	19

Chapter 3. Plan Your Implementation of the STS Protocol 21

STS Data Security	21
Encryption Options.	21
Summary of STS Protocol Processing	22
Authentication	22
Outbound Customer Data	23
Inbound Customer Data	23
Merged STS Security Settings	23
STS Process Override	24
Key Management for the STS Protocol	24

Public Key Exchange With Autoupdate	24
Key Update Frequency	25
Key File Management	25

Chapter 4. Using the SecurePlus Admin Tool and Populating the Parameter File. 27

Starting the Administration Tool	27
About the Admin Tool.	27
Protocol-Specific Parameters and Panels	29
Admin Tool Navigation	32
Admin Tool Help	32
Sterling Connect:Direct Secure Plus Configuration	33
Parameter File Creation	33
Node Configuration	34
Populating the Parameter File Using Quick Start	35
Manual Parameter File Creation	37

Chapter 5. Create the Parameter File Manually for the SSL or TLS Protocol . 39

Configuration Guidelines.	39
Adding the Local Node Record to the Parameter	
File Manually for the SSL or TLS Protocol	40
Adding a Remote Node Record to the Parameter	
File Manually for the SSL or TLS Protocol	47

Chapter 6. Create the Parameter File Manually for the STS Protocol 53

Configuration Guidelines.	53
Adding the Local Node Record to the Parameter	
File Manually for the STS Protocol.	54
Adding a Remote Node Record to the Parameter	
File Manually for the STS Protocol.	59

Chapter 7. Additional Configuration Options 67

Adding a Remote Node Record for the Sterling	
External Authentication Server	67
Establishing Secure TCP API Connections to a	
Sterling Connect:Direct Secure Plus-Enabled Server	70
Implementing Strong Password Encryption.	73
Disabling Strong Password Encryption	74
SPE Problem Troubleshooting	75

Chapter 8. Configure the Local Node Record Imported from the Network Map 79

Configuration Guidelines.	79
Configuring the Local Node Record for the SSL or	
TLS Protocol	80
Configuring the Local Node Record for the STS	
Protocol	86

Chapter 9. Configure Remote Node Records Imported from the Network Map	93
Configuration Guidelines	93
Configuring a Remote Node Record for the SSL or TLS Protocol	94
Configuring a Remote Node Record for the STS Protocol	97
Disabling Sterling Connect:Direct Secure Plus in a Remote Node Record	102

Chapter 10. Manage Keys for the STS Protocol	105
Exchanging STS Keys the First Time	105
Exporting STS Keys	106
Importing STS Keys from a File	107
Importing STS Keys Manually	110

Chapter 11. Enable and Validate Sterling Connect:Direct Secure Plus Operation	113
Saving and Submitting the Sterling Connect:Direct Secure Plus Parameter File	113
Preparing Sterling Connect:Direct for Secure Plus Operations	115
Parameter File Saving After the Initial Setup	115
Validating and Testing Connections by Session	115

Chapter 12. Override Settings in Sterling Connect:Direct Processes	117
PROCESS Statement Overrides for Sterling Connect:Direct Secure Plus Defaults	117
COPY Statement Overrides for Sterling Connect:Direct Secure Plus Defaults	118
Security Settings Override Examples	119
Secure Sessions Default Override	119
Non-Secure Sessions Default Override	119
Default Cipher Suite Override	119
Cipher Suite List Override of Single Default Cipher Suite	120
Control Block and Data Encryption Default Override	120
Sterling Connect:Direct Secure Plus Settings STS Protocol Override	120

Chapter 13. Maintain Sterling Connect:Direct Secure Plus	123
Parameter File Maintenance	123
Opening a Sterling Connect:Direct Secure Plus Parameter File	124
Viewing Information about the Parameter File	125
Saving Changes to Node Records Using the Save Active Option	126
Resecuring the Parameter File and Access File	126
Node Record Maintenance	127
Disabling Sterling Connect:Direct Secure Plus on an SSL or TLS Node	128

Disabling Sterling Connect:Direct Secure Plus on an STS Node	128
Changing the Cipher Suites	128
Changing the Encryption Algorithm Names	129
Inserting a Node	130
Deleting a Remote Node Record	130
STS Key Modification	131
Updating Keys in Node Records Configured for the STS Protocol	131
Resetting Keys in Remote Node Records Configured for STS	132

Chapter 14. Sterling Connect:Direct Secure Plus Statistics	133
SSL or TLS Statistics Record	133
SSL or TLS Extended Option Statistics Record	134
STS Statistics Record	135
STS Extended Option Statistics Records	137
Session Begin (SB) Record	138
Copy Step Start (CI) Record	138
Copy Termination (CT) Record	139

Chapter 15. Troubleshooting	141
------------------------------------	------------

Chapter 16. Certificate Parameter Definitions	147
RACF Application Certificate Parameter Definitions	147
GSSKYMANT Utility Certificate Parameter Definitions	149
CA-ACF2 Application Certificate Parameter Definitions	151
CA-Top Secret Application Certificate Parameter Definitions	154

Chapter 17. Configuration Worksheets	157
Local Node Security Feature Definition Worksheet	157
Remote Node Security Feature Definition Worksheet	158
.EASERVER Node Security Feature Definition Worksheet	160
.CLIENT Node Security Feature Definition Worksheet	160

Chapter 18. Test Sterling Connect:Direct Secure Plus with the STS Protocol	163
STS Protocol Test Procedure Overview	163
Accessing the Admin Tool	164
Definition Creation for Sterling Connect:Direct Secure Plus for Node A	164
Creating the Sterling Connect:Direct Secure Plus Local Node Record and Keys for Node A	164
Creating the Sterling Connect:Direct Secure Plus Remote Node Record and Keys for Node B	167
Exporting Node A's Public Keys	169
Saving the Sterling Connect:Direct Secure Plus Parameter File for Node A	170
Definition Creation for Sterling Connect:Direct Secure Plus for Node B	171

Creating the Sterling Connect:Direct Secure Plus Local Node Record and Keys for Node B	171
Creating the Sterling Connect:Direct Secure Plus Remote Node Record and Keys for Node A	172
Exporting the Public Keys of Node B	174
Importing the Public Keys from Node A	174
Saving the Sterling Connect:Direct Secure Plus Parameter File for Node B	175
Importing the Public Keys of Node B to Node A	176
Saving the Sterling Connect:Direct Secure Plus Parameter File for Node A	176
Updating Sterling Connect:Direct Network Maps for Node A and Node B	177
Modifying Sterling Connect:Direct Initialization Parameters	178
Restarting Sterling Connect:Direct	178

Verifying Sterling Connect:Direct Secure Plus is Enabled	178
Exchanging Data and Compare Results.	178

**Chapter 19. Configuration for a
Secure Connection between z/OS and
OpenVMS Nodes 181**

Records Settings in the z/OS Parameter File	181
Records Settings in the z/OS Remote Node Record for OpenVMS Parameter File	183

Notices 185

Index 189

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.

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 three security protocols to use to secure data during electronic transmission: Transport Layer Security (TLS), Secure Sockets Layer protocol (SSL), or Station-to-Station protocol (STS). 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*, and *Station-to-Station Protocol*.

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.

Station-to-Station Protocol

The Station-to-Station (STS) protocol is a three-pass variation of the basic Diffie-Hellman protocol. It enables you to establish a shared secret key between two nodes with mutual entity authentication. Nodes are authenticated using digital

signatures that sign and verify messages. When you use the STS protocol, you are responsible for generating and managing authentication and signature public keys and exchanging these keys with your trading partners.

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 15, "Troubleshooting," on page 141. 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*.

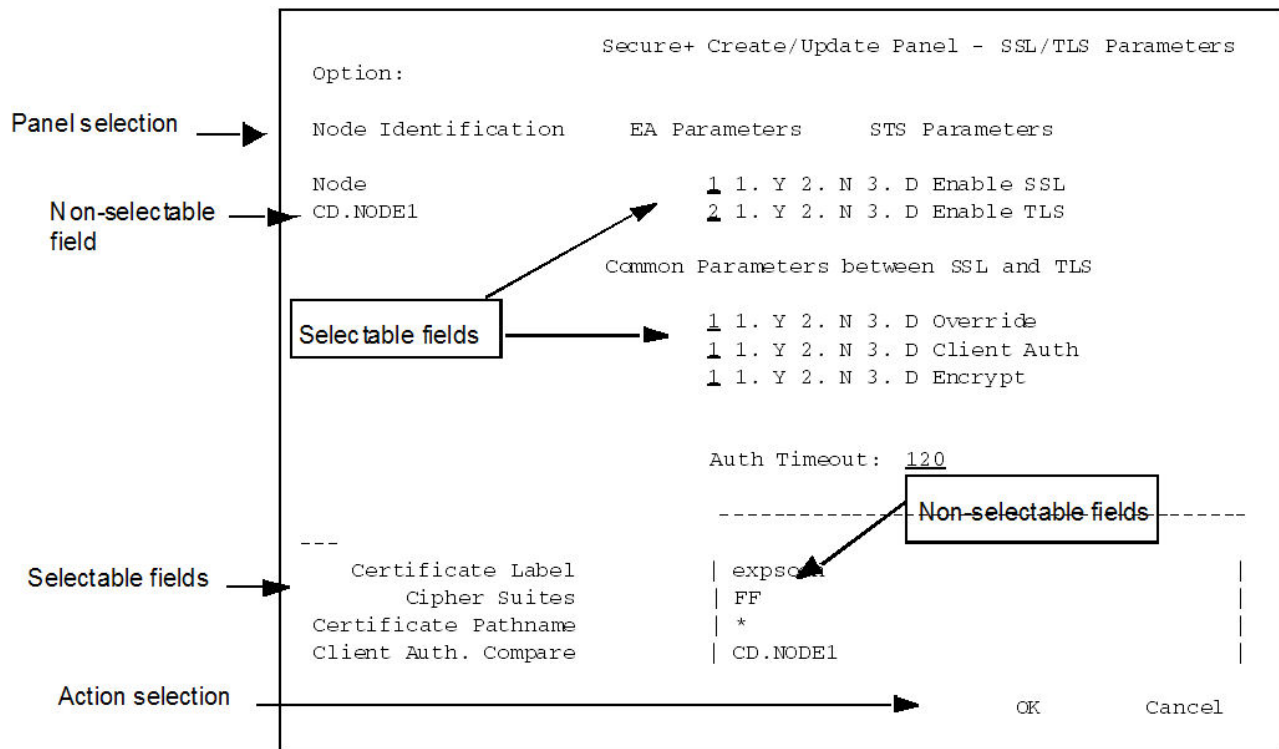
Sterling Connect:Direct Secure Plus Tools

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.

Administration 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.

Two interface modes are available for the Admin Tool: native ISPF or graphical user interface (GUI). Both of these modes are driven by ISPF, so the screen content and functionality are identical, but the elements of the interfaces are different. The following sample illustrates the native ISPF interface display of the Create/Update Panel for SSL/TLS parameters. If you use the native ISPF interface, 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.



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, and lastly, the STS Parameters panel used to disable that protocol.
- 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, such as the underlined value of 120 seconds next to the Auth Timeout 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.

GUI Interface

The GUI interface mode display uses command buttons, option buttons, and text boxes. To use the GUI mode, you must download an IBM workstation agent and change your ISPF settings (Option 0) to set up and use the workstation agent. See the IBM z/OS reference manuals for more information about downloading and using an IBM workstation agent. The following GUI interface sample illustrates the view when you customize Sterling Connect:Direct Secure Plus to display all parameters in a single panel.

The screenshot shows a window titled "MWATL1 - Secure+ Create/Update Panel - STS Parameters - SC.DUB.MWATL1". The main title bar reads "Secure+ Create/Update Panel - STS Parameters".

At the top, there is an "Option:" field. Below it are three tabs: "Node Identification", "EA Parameters", and "SSL/TLS Parameters".

The "Node" field contains "SC.DUB.MWATL1". To the right, there are radio button options for "Y", "N", and "D" for "Override", "Autoupdt", "Enable STS", "Signature", and "Encrypt".

The "Auth Timeout:" field contains "120". The "Algorithm" field contains "*".

Below these are two rows of buttons: "Create / Reset" for "Auth. Prev. Keys" and "Sig. Prev. Keys", each with an "Expire Date MDY" field.

Further down, there are "Create / Reset" buttons for "Auth. Pubkey" and "Sig. Pubkey", followed by their respective hexadecimal values: "0207.913A.6127.1F85.346D.6CB7.7B04.E6A8." and "0303.1A08.F439.8D0B.4AFD.7A8F.7C8E.AD88.". Below these are fields for "Algorithm Names" (containing "DESCBC56, TDESCBC112, IDEACBC128"), "Auth. Rmt. Key", and "Sig. Rmt. Key".

At the bottom, there are buttons for "Import Remote Keys", "Get Record", "OK", "Cancel", and "Enter".

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, or Station-to-Station Protocol, 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
Planning to use the STS protocol	Station-to-Station Protocol
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

Task	Reference
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
Setting up and testing local and remote node records for the STS protocol	Manual Creation of Parameter File for STS Local Node Record Imported from Network Map Configuration Remote Node Record Imported from Network Map Configuration Configuration Worksheets STS Protocol Test Procedures
Configuring special-purpose remote node records to perform one of the following functions: <ul style="list-style-type: none"> • 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
Managing STS keys	Key Management for STS
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
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 individual 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.

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 4.

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.

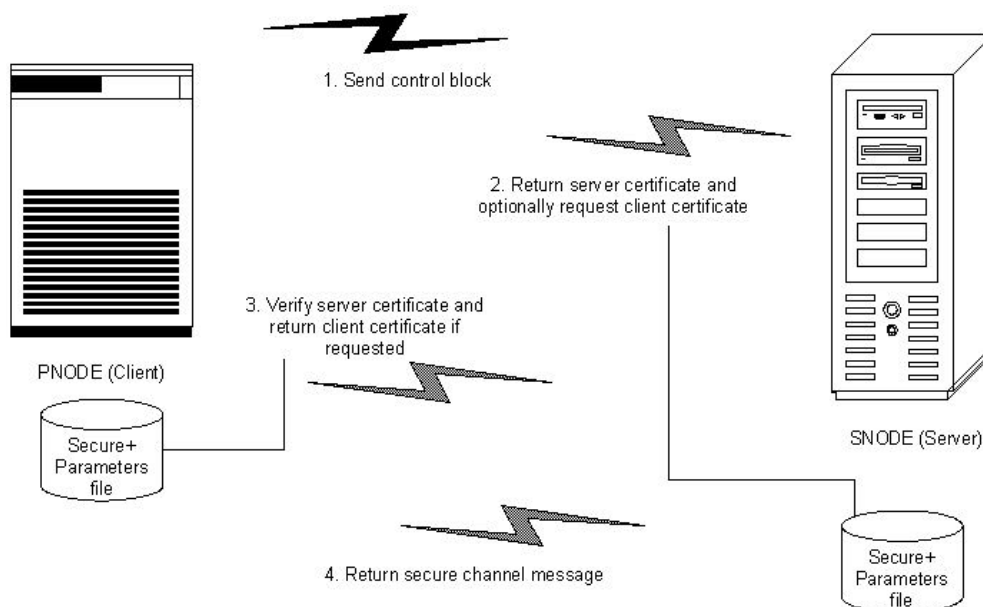
Note: You can implement the protocol you want to use for all data transfers or on a Process-by-Process basis. To specify a protocol each time you submit a Process, you must disable the protocol (but allow overrides) when you create the local and remote nodes in the Sterling Connect:Direct Secure Plus 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:



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 .

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

Component	Access to Resource
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • SYS1.SIEALNKE for IBM z/OS (System SSL Environment)
	Permission to read Sterling Connect:Direct key ring that is created using RACDCERT, as follows: <ul style="list-style-type: none"> • 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.
Sterling Connect:Direct User ID key database or key ring	Verification of other certificates requires access to the trusted root certificate of either: <ul style="list-style-type: none"> • 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.

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
CA-signed certificate	Not required to store the public key of trading partner	Must be purchased from third-party vendor
	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.	
	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.
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 GSKKMAN 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 <i>z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08</i> .
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 <i>z/OS V1R11.0 Cryptographic Services System Sockets Layer Programming SC24-5901-08</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • key.kdb = private key file • certreq.arm = Certificate Signing Request (CSR) file • cert.arm = public key file <p>The gskkyman utility loads currently available CA certificates to the key database.</p>
Resource Access Control Facility (RACF)	<p>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.</p> <p>The RACF utility does not assign default names to the files you generate with it.</p>

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. Plan Your Implementation of the STS Protocol

The Station-to-Station (STS) protocol is a three-pass variation of the basic Diffie-Hellman protocol. It enables you to establish a shared secret key between two nodes with mutual entity authentication. Nodes are authenticated using digital signatures that sign and verify messages.

In the STS protocol, each message is signed by the PNODE with its current authentication private key (and possibly its previous authentication private key) and verified by the SNODE using the corresponding public key of the PNODE. Each node uses two session keys to process control blocks: one for sending and the other for receiving. The encryption algorithms for control blocks and data copying functions are also determined. When strong authentication is completed successfully, control blocks are exchanged in an encrypted format for the entire session.

STS Data Security

The STS protocol provides data security in the following areas:

- Strong authentication—The STS protocol uses a digital signature for strong authentication. After you enable this feature, control blocks are signed and verified. A digital signature uniquely authenticates the node signing an electronic document much like a human signature uniquely identifies the person signing his or her name to a physical document.
- Proof of data origin and data integrity validation—The digital signature verifies the sender of the message. The digital signature feature also provides data integrity validation. If the digital signature is verified, then an uncorrupted message was transmitted.
- Data confidentiality—The data encryption feature ensures confidentiality of the data sent in a Sterling Connect:Direct transfer. Sensitive information is converted to an unreadable format (encryption) by the PNODE before it is sent to the SNODE. The SNODE then converts the information back into a readable format (decryption). In order for the encryption/decryption process to work, each of these communicating nodes must have the public key value of the other.

Encryption Options

Sterling Connect:Direct Secure Plus supports the following encryption algorithms:

- 56-bit DES using Cipher Block Chaining Mode (DESCBC56)
- 112-bit Triple DES in Cipher Block Chaining Mode (TDESCBC112)
- 128-bit IDEA in Cipher Block Chaining Mode (IDEACBC128)

Sterling Connect:Direct also gives you the ability to select what you want encrypted:

- Only the control block information contained in Function Management Headers (FMHs), such as a user ID, password, and filename
- Both control block information and the files being transferred

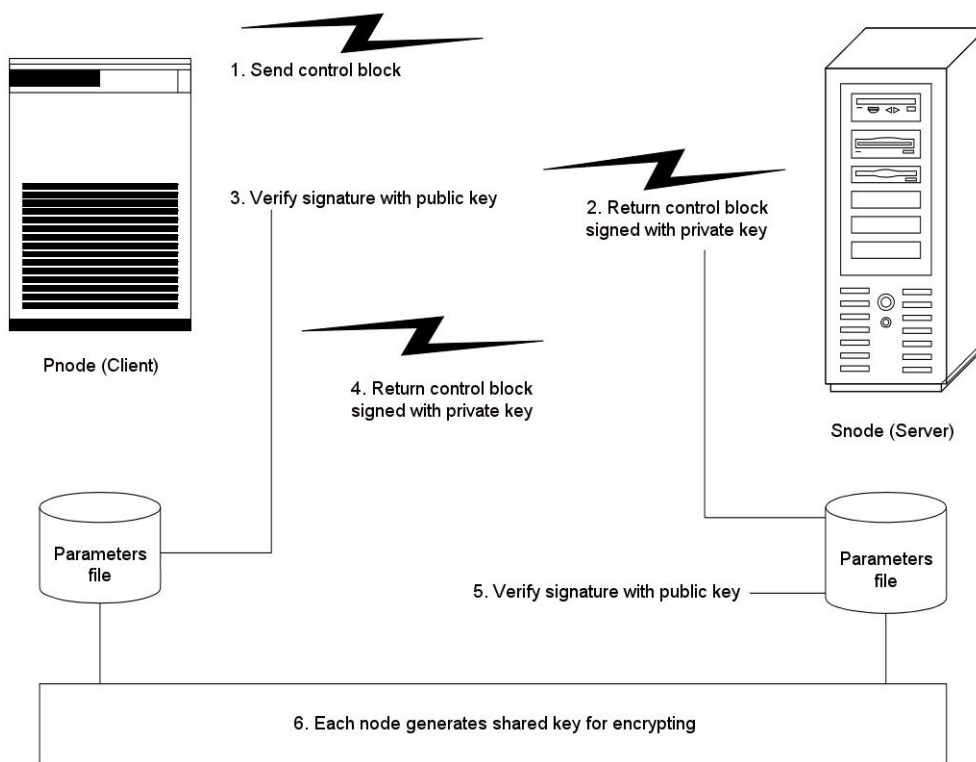
By restricting encryption to the control block information rather than both the preliminary FMH information exchanged during the handshake to set up the session and the actual data being transferred, CPU utilization will decrease dramatically.

Summary of STS Protocol Processing

Data exchange consists of three steps: authentication, sending data, and receiving data. The primary node (PNODE) initiates the data transmission, and the secondary node (SNODE) receives the data.

Authentication

The following figure illustrates the authentication process using the STS protocol:



The following steps occur during authentication:

1. The PNODE sends a control block to the trading partner (SNODE). Information for creating an encryption key for the PNODE is included. The SNODE confirms that it has a record defined in the Sterling Connect:Direct Secure Plus parameter file for the PNODE. If so, it retains the information for key encryption for processing later. If not, the session fails.
2. The SNODE sends a control block signed with its private authentication key. Information for creating an encryption key is included.
3. The PNODE verifies the signature of the SNODE using its public authentication key and returns a control block signed with its private authentication key.
4. The PNODE returns a control block signed with its private authentication key.
5. The SNODE verifies the signature using the public authentication key of the PNODE.

- When authentication is successful, each node generates a shared session encryption key for encrypting control blocks.

Outbound Customer Data

After communication is authenticated, the PNODE begins transmitting data.

- If data encryption is enabled, information for creating an encryption key is exchanged in the control blocks.
- If digital signature is enabled, the PNODE applies the signature algorithm to the data using its private signature key to ensure that the data was sent by the PNODE and has not been altered.
- If data compression is enabled, the PNODE compresses the data, based on settings defined in Sterling Connect:Direct.
- If data encryption is enabled, the PNODE encrypts the data with an encryption algorithm using a shared secret encryption key generated specifically for this transmission. The encryption algorithm is determined at authentication.

Inbound Customer Data

The SNODE receives the data.

- If data is encrypted, the SNODE decrypts the data using the encryption algorithm available for both the PNODE and the SNODE.
- If the data is compressed, the SNODE decompresses it.
- If digital signature is enabled, the SNODE verifies the origin and integrity of the data by applying a verification algorithm using the public digital signature key of the PNODE.

Merged STS Security Settings

When two nodes use the STS protocol to exchange secure data, Sterling Connect:Direct Secure Plus settings are exchanged during authentication. These settings are then merged and the resulting value for each security function is used for the Sterling Connect:Direct session. The result is based upon the values defined on the primary node (PNODE) and the secondary node (SNODE).

See Digital Signature and Algorithm for Encrypting Control Blocks to illustrate how the results of the merged PNODE and SNODE values is used to achieve the most secure connection.

Digital Signature

When Sterling Connect:Direct Secure Plus settings are merged, the most secure setting from either node is used for the digital signature feature. If either node enables the digital signature feature, digital signatures are used for the session. If both nodes disable digital signatures, digital signatures are not used. The following table shows the digital signature setting after the PNODE and SNODE values are merged:

PNODE Value	SNODE Value	Merged Results
Y	Y	Y
Y	N	Y
N	Y	Y
N	N	N

Algorithm for Encrypting Control Blocks

The algorithm that encrypts Sterling Connect:Direct control blocks used for strong authentication is the first algorithm ID in the PNODE list that is also in the SNODE list. If the nodes do not share a common algorithm, the copy function fails.

Data Encryption

The most secure setting from either node is used for data encryption. If the nodes do not share a common algorithm, the copy operation fails. The following table shows the setting after the PNODE and SNODE values are merged:

PNODE Value	SNODE Value	Merged Results
N	N	N
N	Y	First algorithm ID in the SNODE list that is in the PNODE list.
N	algorithm ID	SNODE algorithm ID if it is in the PNODE list.
Y	N Y algorithm ID	First algorithm ID in the PNODE list that is in the SNODE list.
algorithm ID	N Y algorithm ID	PNODE algorithm ID if it is in the SNODE list.

STS Process Override

When you configure a node to use the STS protocol, you can use the PROCESS or COPY statement in a Sterling Connect:Direct Process to override the settings in the parameter file, if override is enabled in the remote node record. Sterling Connect:Direct Secure Plus uses the most secure connection available. Therefore, if the remote node record enables digital signatures or encryption, the PNODE can not turn those options off by using the COPY statement override. For more information on overriding default settings in the parameter file, see Override Settings in Sterling Connect:Direct Processes.

Key Management for the STS Protocol

When you configure a remote node record to use the STS protocol, you generate unique authentication and signature public keys. In addition, your trading partner generates authentication and signature public keys for their node. In order to communicate with the trading partner, all four keys must be defined in the parameter file for both your configuration and the trading partner's configuration. Therefore, you and your trading partner must exchange these keys.

For the initial configuration, you manually exchange these keys. You export keys and send them to the trading partner. Then you import the keys you receive from the trading partner into the parameter file. After the initial exchange, you can automate the exchange of key information by defining the appropriate options in the remote node record.

If a remote node uses the STS protocol, you must decide how often to update keys and how to manage key files received from trading partners.

Public Key Exchange With Autoupdate

After you exchange keys with a trading partner, both partners can enable the automatic key update feature for easier key management. If both nodes enable the autoupdate function, the authentication and signature public key values are dynamically updated during authentication if the remote node supplies different

values. Both you and your trading partner must enable automatic key update in order to use this feature. Enabling autoupdate eliminates much of the work that has to be performed by the Sterling Connect:Direct Secure Plus administrator for maintaining the keys.

Key Update Frequency

Decide how frequently to update authentication and signature keys. The more frequently you update key values, the more secure your environment is. When you turn on automated key updates, you can update keys daily, because the updated keys are sent to the trading partners automatically and securely during authentication.

Key File Management

Before you begin exchanging key files with a trading partner, you must consider how to manage key files. Sterling Connect:Direct Secure Plus names exported key files based on the name of the target node; therefore, new key files that you receive from a trading partner have the same name as the old key file. To avoid overwriting an old key file with a new one, you manage key files in one of the following ways:

- Import the new key file immediately after receiving it from your trading partner and then delete the old key file.
- Rename the key file upon receipt or have your trading partner rename it before sending it.
- Create a directory for each remote node and store each key file separately in the associated directory.

See Key Management for STS, for instructions on importing and exporting keys.

Chapter 4. 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 Tool (Admin Tool) to set up and maintain a Sterling Connect:Direct Secure Plus operation.

To start the Secure+ Admin Tool:

Procedure

1. To start the Admin Tool, take one of the actions:
 - On the Connect:Direct Administrative Options Menu command line, type **S** and press Enter to select the Execute Secure Plus Commands option, and then type **SA** on the command line and press Enter.
 - 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**.

After the Admin Tool is initialized, the Secure+ Admin Tool: Main Screen is displayed.

```
File Edit Key Management Help
-----
Option ==>          Secure+ Admin Tool: Main Screen          Scroll CSR
                    Table Line Commands are:
E Export pub. key   H View History          D Delete node
U Update node      I Insert node
                   Secure
LC Node Name      Type 123C Override Encryption Signature ExtAuth Autoupd
-----
***** BOTTOM OF DATA *****
```

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 a field description and valid values for each field, according to the protocol to which they apply.

Field Name	Field Description	Valid Values
All Protocols		
LC	Line Command. For more information, see Node Record Maintenance.	E = Export public key H = View History D = Delete node U = Update node I = Insert node
Node Name	Displays the node record name.	Node name
Override (set in local node record)	Displays the status of override. When override is enabled in the local node record, values set in the the remote node record override the values set in the local node record.	Y = enabled N = disabled
Override (set in remote node record)	Displays the status of override. Enabling override in a remote node record allows values specified in 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
Type	Displays the current record type.	L = local node record R = remote node record A = alias record Alias is valid only for remote records.
Secure 1 2 3 C	Identifies the status of STS security. Indicates the status of SSL security. Indicates the status of TLS security. Identifies the status of client authentication. Client authentication is valid only for the SSL and TLS protocols.	Y=Yes N=No * = default to local node * is not a valid option in the local node record.
STS Protocol-Specific		
Override (set in remote node record for STS)	Displays the status of Override. Enabling Override in a remote node record that uses the STS protocol 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 in the STS protocol.	Y = enabled N = disabled * = default to local node
Signature	Identifies if digital signature is enabled in the STS protocol.	Y = enabled N = disabled * = default to local node

Field Name	Field Description	Valid Values
Autoupd	Indicates if the option to automatically update STS key values during communications is enabled.	Y = enabled N = disabled * = default to local
SSL and TLS Protocol-Specific		
ExtAuth	Identifies whether external authentication is enabled for the node. Valid only for the SSL or TLS protocol. For more information, see Adding a Remote Node Record for the Sterling External Authentication Server.	Y = enabled N = disabled * = default to local node

Protocol-Specific Parameters and Panels

The default Create/Update panel display has changed. In versions prior to 5.0, the information was divided into four panels for External Authentication (EA), SSL, TLS, and STS. In version 5.0, SSL and TLS were combined so that the panel selection bar shows three choices, as illustrated in the following Node Identification panel.

Secure+ Create/Update Panel - Node Identification

Option:

EA Parameters SSL/TLS Parameters STS Parameters

Node

2 1. Local
2. Remote

Alias

Names: TCP Information:
 IPaddr:
 Port:

Import Remote Keys Get Record OK Cancel

The Node Identification panel is the panel displayed when you create a record manually or when you want to display the Node Name and Type fields. The following tables list the Sterling Connect:Direct Secure Plus parameters according to the type of record (local or remote) to which they apply.

Node Identification Panel	Valid for Local Node Record?	Valid for Remote Node Record?
Node	Yes	Yes
Local/Remote	Yes	Yes
TCP Information/IP Address and Port	No	No

Node Identification Panel	Valid for Local Node Record?	Valid for Remote Node Record?
<p>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.</p>		
Alias Names	No	Yes

The following table describes the parameters displayed in the STS Parameters panel.

STS Parameters Panel	Valid for the Local Node Record?	Valid for the Remote Node Record?
Override	Yes. Valid for all protocols. Enable to allow turning security on or off in the PROCESS or COPY statement.	Yes. Enable to allow turning security on or off in the PROCESS or COPY statement. Consider the effects of settings for Signature and Encrypt when you set this parameter.
Autoupdt	Yes. Enable to allow automatic updates of keys used for the STS protocol.	Yes. Enable to allow automatic updates of keys used for the STS protocol.
Enable STS	Yes	Yes
Signature	Yes. Valid only for nodes that use the STS protocol.	Yes. Valid only for nodes that use the STS protocol.
Encrypt	Yes	Yes
Auth Timeout	Yes. Valid for all protocols.	Yes. Valid for all protocols.
Algorithm	Yes. Valid only for the STS protocol.	Yes. Valid only for the STS protocol.
Create/Reset Auth. Pubkey	Yes. Valid and required for all protocols.	Yes. Valid and required only for remote nodes that use the STS protocol.
Create/Reset Sig. Pubkey	Yes. Valid and required for all protocols.	Yes. Valid and required only for remote nodes that use the STS protocol.
Algorithm Names	Yes. Valid only for the STS protocol.	Yes. Valid only for the STS protocol.
Auth. Rmt.Key	Yes. Valid only for nodes that use the STS protocol.	Yes. Valid only for nodes that use the STS protocol.
Auth.Sig.Key	Yes. Valid only for nodes that use the STS protocol.	Yes. Valid only for nodes that use the STS protocol.
Import Remote Keys	Yes. Valid only for nodes that use the STS protocol.	Yes. Valid only for nodes that use the STS protocol.

Because the **Override**, **Encrypt**, and **Signature** parameters work together, review the following scenarios to determine the values to set for these parameters in a remote node record that uses the STS protocol.

Scenario	Setting for Override Parameter	Setting for Encrypt and Signature
All files must be encrypted and use signature.	Disable Override by setting to 2.	Enable Signature and Encrypt by setting to 1. If you disable Override, you cannot disable security in the PROCESS statement.
A few files must be encrypted and use signature.	Enable Override by setting to 1.	Disable Signature and Encrypt by setting to 2. You can change these settings in the COPY statement Process so that the individual files use encryption and signature. See Override Settings in Sterling Connect:Direct Processes .

The following table describes the parameters displayed in the EA Parameters panel.

Note: If you have configured an .EASERVER remote node record, the following fields are populated but unavailable from any record except the .EASERVER record: External Auth Server Def, External Auth Server Address, and External Auth Server Port. The External Auth field can be modified from any record.

EA Parameters	Valid for Local Node Record?	Valid for Remote Node Record?
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.

The following table describes the parameters displayed in the SSL/TLS Parameters panel. On this panel, you must enable only one protocol—either SSL or TLS—by entering a 1 next to the protocol you want to enable and a 2 next to the protocol to disable. Information common to both protocols is grouped under the Common Parameters heading followed by the certificate and cipher parameters related to the selected protocol selected.

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 4.

SSL/TLS Parameters Panel	Valid for the Local Node?	Valid for the Remote Node?
Enable SSL	Yes.	Yes.

SSL/TLS Parameters Panel	Valid for the Local Node?	Valid for the Remote Node?
Enable TLS	Yes.	Yes.
Override	Yes. Valid for all protocols.	Yes. Valid for all protocols to allow Sterling Connect:Direct Secure Plus settings to be overridden in a PROCESS statement. See Override Settings in Sterling Connect:Direct Processes .
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.
Encrypt	Yes.	Yes
Auth Timeout	Yes.	Yes.
Certificate Label	Yes. Valid only for the SSL or TLS protocol.	Yes. Valid only for the SSL or TLS protocol.
Cipher Suites	Yes. Valid only for the SSL or TLS protocol.	Yes. Valid only for the SSL or TLS protocol.
Certificate Pathname	Yes. Valid only for the SSL or TLS protocol.	Yes. Valid only for the SSL or TLS protocol. 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.
Client Auth. Compare	No	Yes. Requires the certificate common name of the local node certificate when client authentication is enabled. Valid only for the SSL or TLS protocol.

Admin Tool Navigation

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

Key	Function
PF8	Move forward
PF7	Move backward
PF12	Back up to a previous panel
PF3	Exit
Enter	To 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 position the cursor next to an option of an 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 .
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
<ul style="list-style-type: none"> • 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 .	<ul style="list-style-type: none"> • File is created automatically with a local node record and a record for each remote node in the network map that uses the TCP, UDT, or LU6.2 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.
<ul style="list-style-type: none"> • 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 .	<ul style="list-style-type: none"> • 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 .	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Adding the Local Node Record to the Parameter File Manually for the SSL or TLS Protocol Adding the Local Node Record to the Parameter File Manually for the STS Protocol Configure remote node records only for those trading partners who use Sterling Connect:Direct Secure Plus.	<ul style="list-style-type: none"> You define default settings for all protocols (TLS, SSL, STS) 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.	<ul style="list-style-type: none"> 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.

Scenario	How to Configure Node Records	Result
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.	<ul style="list-style-type: none"> • 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 the 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. With the **Secure+ Admin Tool Main Screen** open, select **File** on the action bar and press **Enter**.

```

File Edit Key Management Help
+-----+-----+
| 1. New | | Row 4 of 6
| 2. Open | Secure+ Admin Tool: Main Screen
| 3. Close | | Scroll CSR
| 4. Info... | |
| *. Rekey | Table Line Commands are:
| 6. Save Active | |
| 7. Save as... | H View History D Delete node
| 8. Unload | I Insert node
| 9. Exit | |
+-----+-----+
Secure
LC Node Name Type 123C Override Encryption Signature ExtAuth Autoupd
-----
***** BOTTOM OF DATA *****

```

2. Type **2** to select **Open** and press **Enter**.

```

Secure+ Admin Tool: File Selection

Enter file name for: INPUT SECURE PARM FILE

File
Name: $CD.SECURE.NETMAP Browse

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

```

3. Type the Sterling Connect:Direct network map file name prefix or partial prefix followed by an asterisk (*) 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**.

```

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.NETMAP
_ $CD.NETMAP.DATA
_ $CD.NETMAP.INDEX
***** Bottom of data *****

```

- 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:

```

File Edit Key Management Help
-----
Row 9 to 13 of 13
Q2A.ZOS.PARIS      Secure+ Admin Tool: Main Screen
Option ==>                               Scroll CSR

Table Line Commands are:

E Export pub. key      H View History        D Delete node
U Update node          I Insert node

Secure
LC Node Name          Type  123C  Override Encryption Signature ExtAuth Autoupd
-----
Q2A.ZOS.PARIS        L    NNNN   Y      N      N      N      N
Q3A.ZOS.PARIS        R    ***N   N      *      *      *      *
Q3B.ZOS.PARIS        R    ***N   N      *      *      *      *
SOL36SP              R    ***N   N      *      *      *      *
W2S.4200.CDWOPS8    R    ***N   N      *      *      *      *
***** BOTTOM OF DATA *****

```

- 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, refer to the following instructions for configuring the local and remote node records:

- Manual Creation of the SSL or TLS Parameter File
- Manual Creation of Parameter File for STS

Chapter 5. 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, STS) 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, EA Parameters, and STS Parameters. Allow overrides in the Local Node settings.
- Disable external authentication.
- Create keys for the STS protocol because this action also creates the key that encrypts the Sterling Connect:Direct Secure Plus parameter file.
- 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**

```

File Edit Key Management Help
-----
Option ==>          Secure+ Admin Tool: Main Screen          Scroll CSR

                    Table Line Commands are:
E Export pub. key   H View History          D Delete node
U Update node      I Insert node

                    Secure
LC Node Name      Type 123C Override Encryption Signature ExtAuth Autoupd
-----
***** BOTTOM OF DATA *****

```

2. On the **Edit** menu, select **1** to select **Create/Update Record** and press **Enter** to display the **Secure+ Create/Update - Node Identification** panel:

```

Option:          Secure+ Create/Update Panel - Node Identification
EA Parameters    SSL/TLS Parameters    STS Parameters

Node
                1 1. Local
                2 2. Remote

Alias
Names:          TCP Information:
                IPaddr:
                Port:

Import Remote Keys  Get Record          OK          Cancel

```

3. On the **Node Identification** panel:
 - a. Type a name for the local node in the **Node** field.
 - b. Type **1** next to the **Local** field.

- c. Leave the **TCP Information** fields (**IP addr** and **Port**) blank because they do not apply to the local node record.
 - d. Leave the **Alias Names** field blank because it is not valid for the local node.
4. Select **SSL/TLS Parameters** from the panel selection bar and press **Enter**.

```

Secure+ Create/Update Panel - SSL/TLS Parameters
Option:
Node Identification      EA Parameters      STS Parameters
Node                    2 1. Y 2. N 3. D Enable SSL SC.
OKC.PARIS1             2 1. Y 2. N 3. D Enable TLS

Common Parameters between SSL and TLS

1 1. Y 2. N 3. D Override
2 1. Y 2. N 3. D Client Auth
1 1. Y 2. N 3. D Encrypt

Auth Timeout: 120

Certificate Label      *
Cipher Suites          FF
Certificate Pathname   *
Client Auth. Compare

OK      Cancel

```

5. In the **SSL/TLS Parameters** panel:
- a. To disable the SSL protocol, type **2** beside the **Enable SSL** field.
 - b. To disable the TLS protocol, type **2** beside the **Enable TLS** field.
 - c. To enable the Override function, type **1** beside the **Override** field.
 - d. To disable the Client Authentication function, type **2** beside the **Client Auth** field.
 - e. To enable the default Encrypt function, type **1** beside the **Encrypt** field.
 - f. Modify the **Auth Timeout** value, if necessary, using the following table as a guide:

Field Name	Description	Valid Value
Auth Timeout	Identifies the maximum time, in seconds, that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.	0=No timeout. Sterling Connect:Direct waits indefinitely to receive the next message. Specify a time to prevent malicious entry from taking as much time as necessary to attack the authentication protocol. Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP:TIMER initialization parameter. The default is 120 seconds.

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 4.

- 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**.

Secure+ Create/Update Panel - SSL/TLS Parameters		
Option:	EA Parameters	STS Parameters
Node Identification		
Node	2 1. Y 2. N 3. D Enable SSL	
SC.OKC.PARIS1	2 1. Y 2. N 3. D Enable TLS	
Common Parameters between SSL and TLS		
	1 1. Y 2. N 3. D Override	
	2 1. Y 2. N 3. D Client Auth	
	1 1. Y 2. N 3. D Encrypt	
	Auth Timeout: 120	
Certificate Label	keylabel	
Cipher Suites	FF	
Certificate Pathname	*	
Client Auth. Compare		
	OK	Cancel

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 4.

- 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.

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 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.

0
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

```

- b. Type **1** by the cipher you want to enable and give the highest priority.
- c. Type **2** by the cipher you want to enable and place second in priority.
- d. 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.

- e. Press **F3** when you have enabled and ordered all necessary ciphers.

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.

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 **2** 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.

```

Secure+ Create/Update Panel - EA Parameters
Option:
Node Identification      SSL/TLS Parameters      STS Parameters
Node                    1 1. Y 2. N 3. D Override
SC.OKC.PARIS1          1 2 1. Y 2. N 3. D External Auth
External Auth Server Def THISISATEST
External Auth Server Address 10.20.201.2
External Auth Server Port 23234
OK                      Cancel

```

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

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node                    1 1. Y 2. N 3. D Override
SC.OKC.PARIS1          2 1. Y 2. N 3. D Autoupdt
                        2 1. Y 2. N 3. D Enable STS
                        2 1. Y 2. N 3. D Signature
                        2 1. Y 2. N 3. D Encrypt
Auth Timeout: 120
Algorithm *
Create / Reset Auth. Prev. Keys      Expire Date MDY
Create / Reset Sig. Prev. Keys      Expire Date MDY
Create / Reset Auth. Pubkey          *
Create / Reset Sig. Pubkey           *
Algorithm Names                      DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key                       0000
Sig. Rmt. Key                         0000
----- < > -----
Import Remote Keys  Get Record      OK      Cancel

```

11. In the **STS Parameters** panel:

- a. To disable the STS parameters, type **2** beside the following fields:
Autoupdt, **Enable STS**, **Signature**, and **Encrypt**.
- b. Type an asterisk (*) in the **Algorithm** field.

12. Generate the STS protocol authentication key, which is used to encrypt the parameter file:

- a. Select **Create/Reset Auth. Pubkey** and press **Enter** to display the **Generate Seed** screen.

Secure+ Admin Tool: Generate Seed	
2 1. Specify Value	Specify the seed value by typing it into the text field.
2. Sample Value	Generate a seed by processing text entered from the keyboard.
Random Number	
Seed:	

- b. Press **Enter** to accept the default value of **2-Sample Value**.
- c. When the following screen is displayed, edit or add data on any line and press **PF3** to save the information. Changing data creates a unique key value.

```

File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT          SYS06254.T160411.RA000.SSCHR1.R0207298          Columns 00001 00072
Command ==>                                           Scroll ==> PAGE
024: This process cannot proceed if the data in the edit file is unchanged.
==MSG> -Warning- The UNDO command is not available until you change
==MSG>          your edit profile using the command RECOVERY ON.
000001 262144
000002
000003 134217728
000004
000005 32
000006
000007 4
000008
000009 8589934592
000010
000011 131072
000012
000013 8388608
000014
000015 2097152
000016
000017 1073741824

```

- d. When the message *This is Loop 2 of 10* is displayed, type over data on any line and press **PF3** up to 10 times. This step is only necessary the first time you generate keys within the Secure+ Admin Tool for each parameter file. Repeating the process increases the randomness of keys.
- e. When the **Pass Phrase Generation** panel is displayed, type a string at least 32 characters long containing at least one uppercase character, one lowercase character, and one numeric value and press **Enter**.

Note: You do not need to remember the pass phrase.

Secure+ Create/Update Panel - STS Parameters			
Option:			
Node Identification	EA Parameters	SSL/TLS Parameters	
Node		1	1. Y 2. N 3. D Override
SC.OKC.PARIS1		2	1. Y 2. N 3. D Autoupdt
		2	1. Y 2. N 3. D Enable STS
Auth Timeout:	120	2	1. Y 2. N 3. D Signature
Algorithm	*	2	1. Y 2. N 3. D Encrypt
Create / Reset	Auth. Prev. Keys	Expire Date	MDY
Create / Reset	Sig. Prev. Keys	Expire Date	MDY
Create / Reset	Auth. Pubkey	----- < > -----	
Create / Reset	Sig. Pubkey	0203.093F.5D89.9024.5080.FE6D.7574.F55B.	
	Algorithm Names	*	
	Auth. Rmt. Key	DESCBC56,TDESCBC112,IDEACBC128	
	Sig. Rmt. Key	0000	

Import Remote Keys	Get Record	OK	Cancel

When the **Secure+ Create/Update Panel - STS Parameters** displays the message Seed generation complete, your public key for strong authentication has been generated and the **Create/Reset Auth. Pubkey field** is populated, as shown in the preceding illustration.

13. Generate the signature key, which is part of the key pair used to encrypt the parameter file:
 - a. Select **Create/Reset Sig. Pubkey** and press **Enter**.
 - b. Press **Enter** to accept the default value (**2-Sample Value**).

Secure+ Create/Update Panel - STS Parameters			
Option:			
Node Identification	EA Parameters	SSL/TLS Parameters	
Node		1	1. Y 2. N 3. D Override
SC.OKC.PARIS1		2	1. Y 2. N 3. D Autoupdt
		2	1. Y 2. N 3. D Enable STS
Auth Timeout:	120	2	1. Y 2. N 3. D Signature
Algorithm	*	2	1. Y 2. N 3. D Encrypt
Create / Reset	Auth. Prev. Keys	Expire Date	MDY
Create / Reset	Sig. Prev. Keys	Expire Date	MDY
Create / Reset	Auth. Pubkey	----- < > -----	
Create / Reset	Sig. Pubkey	0203.093F.5D89.9024.5080.FE6D.7574.F55B.	
	Algorithm Names	0201.C2DB.B318.1B91.3A11.7FD3.3553.37EA.	
	Auth. Rmt. Key	DESCBC56,TDESCBC112,IDEACBC128	
	Sig. Rmt. Key	0000	

Import Remote Keys	Get Record	OK	Cancel

When the **Secure+ Create/Update Panel - STS Parameters** displays the message Seed generation complete, your public key for digital signature has been generated and the **Create/Reset Sig. Pubkey field** is populated, as shown in the preceding illustration.

14. Select **OK** and press **Enter** to display the values for the local node record.

15. 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.
16. 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. Select **Edit** from the **Secure+ Admin Tool Main Screen** and press **Enter** to display the **Edit** menu. Settings for configured node records are displayed.

```

File Edit Key Management Help
-----
                                Row 1 of 1
Option ==>>                Secure+ Admin Tool: Main Screen                Scroll CSR

                                Table Line Commands are:

E Export pub. key            H View History                D Delete node
U Update node                I Insert node

                                Secure
LC Node Name                Type  123C  Override Encryption Signature ExtAuth Autoupd
-----
MYLOCAL                    L    NNNN   Y      N      N      N      N
***** BOTTOM OF DATA *****

```

2. On the **Edit** menu, type **1** to select **Create/Update Record** and press **Enter**.

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.

Secure+ Create/Update Panel - Node Identification			
Option:			
EA Parameters	SSL/TLS Parameters	STS Parameters	
Node	1. Local 2. Remote		
Alias Names:	TCP Information: IPaddr: Port:		
Import Remote Keys	Get Record	OK	Cancel

3. On the **Node Identification** panel:
 - a. In the **Node** field, type the name for the remote node that corresponds to its name in the network map.
 - b. Type **2** next to the **Local/Remote** field.
 - c. 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.
 - d. 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.
4. Select **SSL/TLS Parameters** from the panel selection bar and press **Enter**.

Secure+ Create/Update Panel - SSL/TLS Parameters	
Option:	
Node Identification	EA Parameters STS Parameters
Node	1 1. Y 2. N 3. D Enable SSL
REMOTE01	2 1. Y 2. N 3. D Enable TLS
	Common Parameters between SSL and TLS
	2 1. Y 2. N 3. D Override
	1 1. Y 2. N 3. D Client Auth
	2 1. Y 2. N 3. D Encrypt
	Auth Timeout: 120
Certificate Label	----- * FF * -----
Cipher Suites	
Certificate Pathname	
Client Auth. Compare	
	OK Cancel

- a. To implement SSL, take one of the following actions, depending on whether you want to use SSL for all data transfers or on a Process-by-Process basis:
 - Type **1** beside the **Enable SSL** field to enable the SSL protocol for this remote node.
 - Type **2** beside the **Enable SSL** field to disable the SSL protocol but enable it later in a PROCESS statement.
- b. To implement TLS, take one of the following actions, depending on whether you want to use TLS for all data transfers or on a Process-by-Process basis:
 - Type **1** beside the **Enable TLS** field to enable the TLS protocol for this remote node.
 - Type **2** 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 4.

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.

- 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.

- f. To modify the value for the **Auth Timeout** field, use the following table as a guide:

Field	Description	Valid Values
Auth Timeout	Identifies the maximum time, in seconds, that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.	0=No timeout. Sterling Connect:Direct waits indefinitely to receive the next message. Specify a time to prevent malicious entry from taking as much time as necessary to attack the authentication protocol. Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP:TIMER initialization parameter. The default is 120 seconds.

5. 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.

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 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.

7. Select **STS Parameters** and press **Enter**.

Secure+ Create/Update Panel - STS Parameters			
Option:			
Node Identification	EA Parameters	SSL/TLS Parameters	
Node		1	1. Y 2. N 3. D Override
SC.OKC.PARIS1		2	1. Y 2. N 3. D Autoupdt
		2	1. Y 2. N 3. D Enable STS
Auth Timeout: 120		2	1. Y 2. N 3. D Signature
Algorithm *		2	1. Y 2. N 3. D Encrypt
Create / Reset	Auth. Prev. Keys		Expire Date MDY
Create / Reset	Sig. Prev. Keys		Expire Date MDY
Create / Reset	Auth. Pubkey	----- < > -----	
Create / Reset	Sig. Pubkey	*	
	Algorithm Names	DESCBC56,TDESCBC112,IDEACBC128	
	Auth. Rmt. Key		
	Sig. Rmt. Key		
Import Remote Keys		Get Record	OK Cancel

8. In the **STS Parameters** panel:
 - a. To disable the STS protocol, type **2** in the following fields: **Autoupdt**, **Enable STS**, **Signature**, and **Encrypt**.
 - b. Type an asterisk (*) in the **Algorithm** field.
9. Select **EA Parameters** and press **Enter**.

Secure+ Create/Update Panel - EA Parameters			
Option:			
Node Identification	SSL/TLS Parameters	STS Parameters	
Node		1	1. Y 2. N 3. D Override
SC.OKC.PARIS1		2	1. Y 2. N 3. D External Auth
External Auth Server Def	THISISATEST		
External Auth Server Address	10.20.201.2		
External Auth Server Port	23234		
		OK	Cancel

- 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.
 - To configure records for remote nodes that use STS, continue with Adding a Remote Node Record to the Parameter File Manually for the STS Protocol.
 - 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 6. Create the Parameter File Manually for the STS 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. However, because the local node record that you create manually does not specify meaningful default settings (all settings are default to local node), you must configure all parameters.

See *Override Settings in Sterling Connect:Direct Processes* for information about overriding remote node record settings when executing a particular Process.

In addition to configuring local and remote node records, you must also perform the procedures to manage keys used with the STS protocol. See *Key Management for STS*, for instructions.

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 configure the local node record to define the default settings for all protocols. Review the table in *Parameter File Creation* to determine the configuration approach that best suits your needs, and use the following guidelines to configure node records manually:

- Disable external authentication.
- Because you are configuring only those nodes that use Sterling Connect:Direct Secure Plus, disable the Sterling Connect:Direct Secure Plus protocols (TLS, SSL, STS) in the local node record. Then configure each remote node record with the protocol used by that trading partner.
- 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 STS Protocol*, *Adding a Remote Node Record to the Parameter File Manually for the STS Protocol*, and *Sterling Connect:Direct Secure Plus Operation Enablement and Validation*.
- You must perform the additional tasks in *Key Management for STS*.
- 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 Sterling Connect:Direct Secure Plus parameter file.
- See *Override Settings in Sterling Connect:Direct Processes* for information about overriding remote node record settings.
- 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 STS Protocol

About this task

Refer to the Local Node Security Feature Definition Worksheet that you completed for the local node when you perform this procedure.

To add the local node record manually:

Procedure

1. Select **Edit** from the **Secure+ Admin Tool Main Screen** and press **Enter** to display the **Edit** menu.

```

File Edit Key Management Help
-----
Option ==>>          Secure+ Admin Tool: Main Screen          Scroll CSR

                        Table Line Commands are:
E Export pub. key      H View History          D Delete node
U Update node          I Insert node

                        Secure
LC Node Name          Type 123C Override Encryption Signature ExtAuth Autoupd
-----
***** BOTTOM OF DATA *****
  
```

2. On the **Edit** menu, type **1** to select **Create/Update Record** and press **Enter** to display the **Secure+ Create/Update Node Identification** panel.

```

Option:              Secure+ Create/Update Panel - Node Identification
EA Parameters        SSL/TLS Parameters      STS Parameters

Node
1 1. Local
2. Remote

Alias
Names:              TCP Information:
                   IPaddr:
                   Port:

Import Remote Keys   Get Record                OK          Cancel
  
```

3. In the **Node Identification** panel:
 - a. Type a name for the local node in the **Node** field.
 - b. To add the local node record, type **1** next to the **Local/Remote** field.

- c. Leave the **TCP Information** fields (**IP address** and **Port**) blank because they are not valid for the local node record.
- d. Leave the **Alias Names** field blank because it is not valid for the local node.
- e. Select **STS Parameters** and press **Enter**.

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
MYLOCAL
Auth Timeout: 120
Algorithm *
Create / Reset Auth. Prev. Keys      Expire Date MDY
Create / Reset Sig. Prev. Keys      Expire Date MDY
Create / Reset Auth. Pubkey *
Create / Reset Sig. Pubkey *
Algorithm Names DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key 0000
Sig. Rmt. Key  0000
----- < > -----
Import Remote Keys  Get Record      OK      Cancel

```

- 4. In the **STS Parameters** panel:
 - a. Type **1** beside the **Override** field.
 - b. Disable Sterling Connect:Direct Secure Plus by typing **2** beside the following fields: **Autoupdt**, **Enable STS**, **Signature**, and **Encrypt**.
 - c. If necessary, change the values for the **Auth Timeout** and **Algorithm** fields using the following table as a guide:

Field Name	Description	Valid Values
Auth Timeout	Identifies the maximum time, in seconds, that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.	0=No timeout. Sterling Connect:Direct waits indefinitely to receive the next message. Specify a time to prevent malicious entry from taking as much time as necessary to attack the authentication protocol. Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP.TIMER initialization parameter. The default is 120 seconds.

Field Name	Description	Valid Values
Algorithm	Specifies the data encryption algorithm used. Also set Encrypt to Yes .	* = Use first algorithm in list DESCBC56 TDESCBC112 IDEACBC128

5. Generate the authentication key for the STS protocol:

- a. Select **Create/Reset Auth. Pubkey** and press **Enter** to display the **Generate Seed** screen.

```
Secure+ Admin Tool: Generate Seed

2 1. Specify Value      Specify the seed value by typing it
                        into the text field.
   2. Sample Value     Generate a seed by processing text
                        entered from the keyboard.

Random Number
Seed:
```

- b. Press **Enter** to accept the default value of **2-Sample Value**.

```
File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT      SYS06254.T160411.RA000.SSCHR1.R0207298      Columns 00001 00072
Command ==>                               Scroll ==> PAGE
024: This process cannot proceed if the data in the edit file is unchanged.
==MSG> -Warning- The UNDO command is not available until you change
==MSG>      your edit profile using the command RECOVERY ON.
000001 262144
000002
000003 134217728
000004
000005 32
000006
000007 4
000008
000009 8589934592
000010
000011 131072
000012
000013 8388608
000014
000015 2097152
000016
000017 1073741824
```

- c. Edit or add data on any line and press **PF3**. Changing data creates a unique key value.
- d. If the message *This is Loop 2 of 10* is displayed, type over data on any line and press **PF3** up to 10 times. This step is only necessary the first time you generate keys within the Sterling Connect:Direct Secure Plus Admin Tool for each parameter file. Repeating the process increases the randomness of keys.

- e. When the **Pass Phrase Generation** panel is displayed, type a string at least 32 characters long containing at least one uppercase character, one lowercase character, and one numeric value and press **Enter**.

Note: You do not need to remember this number.

Secure+ Create/Update Panel - STS Parameters			
Option:			
Node Identification	EA Parameters	SSL/TLS Parameters	
Node		1	1. Y 2. N 3. D Override
MYLOCAL		2	1. Y 2. N 3. D Autoupdt
		2	1. Y 2. N 3. D Enable STS
	Auth Timeout: 120	2	1. Y 2. N 3. D Signature
	Algorithm *	2	1. Y 2. N 3. D Encrypt
Create / Reset	Auth. Prev. Keys		Expire Date MDY
Create / Reset	Sig. Prev. Keys		Expire Date MDY
Create / Reset	Auth. Pubkey	----- < > -----	
Create / Reset	Sig. Pubkey	0203.093F.5D89.9024.5080.FE6D.7574.F55B.	
	Algorithm Names	*	
	Auth. Rmt. Key	DESCBC56,TDESCBC112,IDEACBC128	
	Sig. Rmt. Key	0000	

Import Remote Keys	Get Record	OK	Cancel

When the Sterling Connect:Direct Secure Plus Create/Update Panel displays the message Seed generation complete, your public key for strong authentication has been generated and the **Create/Reset Auth. Pubkey** field is populated, as shown in the preceding illustration.

6. To generate the signature key:
 - a. Select **Create/Reset Sig. Pubkey** and press **Enter**.
 - b. Press **Enter** to accept the default value (**2-Sample Value**).

Secure+ Create/Update Panel - STS Parameters			
Option:			
Node Identification	EA Parameters	SSL/TLS Parameters	
Node		1	1. Y 2. N 3. D Override
MYLOCAL		2	1. Y 2. N 3. D Autoupdt
		2	1. Y 2. N 3. D Enable STS
	Auth Timeout: 120	2	1. Y 2. N 3. D Signature
	Algorithm *	2	1. Y 2. N 3. D Encrypt
Create / Reset	Auth. Prev. Keys		Expire Date MDY
Create / Reset	Sig. Prev. Keys		Expire Date MDY
Create / Reset	Auth. Pubkey	----- < > -----	
Create / Reset	Sig. Pubkey	0201.C2DB.B318.1B91.3A11.7FD3.3553.37EA.	
	Algorithm Names	*	
	Auth. Rmt. Key	DESCBC56,TDESCBC112,IDEACBC128	
	Sig. Rmt. Key	0000	

Import Remote Keys	Get Record	OK	Cancel

When the Sterling Connect:Direct Secure Plus Create/Update Panel - STS Parameters displays the message *Seed generation complete*, your public key for digital signature has been generated and the **Create/Reset Sig. Pubkey** field is populated, as shown in the preceding illustration.

7. Select **EA Parameters** and press **Enter**.
8. In the **EA Parameters** panel:
 - a. Type **2** beside the **External Auth** field to disable it. The remaining External Authentication fields are available only from 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.

- b. Select **SSL/TLS Parameters** and press **Enter**.

Secure+ Create/Update Panel - SSL/TLS Parameters		
Option:	EA Parameters	STS Parameters
Node Identification		
Node	2 1. Y 2. N 3. D	Enable SSL
MYLOCAL	2 1. Y 2. N 3. D	Enable TLS
Common Parameters between SSL and TLS		
	1 1. Y 2. N 3. D	Override
	2 1. Y 2. N 3. D	Client Auth
	1 1. Y 2. N 3. D	Encrypt
	Auth Timeout: 120	
Certificate Label	* _____	
Cipher Suites	FF	
Certificate Pathname	* _____	
Client Auth. Compare	_____	
OK Cancel		

9. In the **SSL/TLS Parameters** panel:
 - a. Type **2** beside the **Enable SSL** and **Enable TLS** fields to disable those protocols.
 - b. Type **1** beside the **Override** field.
 - c. Type **2** beside the **Client Auth** field because it is not valid for the STS protocol.
 - d. Type **1** beside the **Encrypt** field.
 - e. Leave the remaining fields as they are because they are not valid for the STS protocol.
10. Select **OK** and press **Enter**.
11. From the **Create/Update** panel, press **Cancel** to display the settings for the local node record.
12. Read all warning and error messages. Continue configuring the environment without resolving warning messages, but you must resolve 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.

Adding a Remote Node Record to the Parameter File Manually for the STS Protocol

About this task

Configure a remote node record for each trading partner that uses the STS protocol. Refer to the Remote Node Security Feature Definition Worksheet that you created for a remote node that uses the STS protocol when you complete this procedure.

To add a remote node record manually for the STS protocol:

Procedure

1. Select **Edit** from the **Secure+ Admin Tool Main Screen** and press **Enter** to display the **Edit** menu.

```

File Edit Key Management Help
-----
                                Row 1 of 1
Option ==>          Secure+ Admin Tool: Main Screen          Scroll CSR

                                Table Line Commands are:

E Export pub. key      H View History          D Delete node
U Update node          I Insert node

                                Secure
LC Node Name          Type 123C Override Encryption Signature ExtAuth Autoupd
-----
MYLOCAL              L   NNNN   Y           N           N           N           N
***** BOTTOM OF DATA *****

```

2. On the **Edit** menu, type **1** to select **Create/Update Record** and press **Enter** to display the **Secure+ Create/Update Node Identification** panel.

```

Option:          Secure+ Create/Update Panel - Node Identification

EA Parameters          SSL/TLS Parameters          STS Parameters

Node
                    2 1. Local
                    2 2. Remote

Alias
Names:             TCP Information:
                   IPaddr:
                   Port:

Import Remote Keys    Get Record           OK           Cancel

```

3. In the **Node Identification** panel:

- a. Type a name for the node in the **Node** field.
- b. Type **2** next to the **Local/Remote** field.
- c. 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.
- d. 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.
- e. Select **STS Parameters** and press **Enter**.

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
REMOTE01                1 1. Y 2. N 3. D Override
                        2 1. Y 2. N 3. D Autoupdt
                        2 1. Y 2. N 3. D Enable STS
                        2 1. Y 2. N 3. D Signature
                        2 1. Y 2. N 3. D Encrypt
Auth Timeout: 120
Algorithm *
Create / Reset Auth. Prev. Keys      Expire Date MDY
Create / Reset Sig. Prev. Keys      Expire Date MDY
Create / Reset Auth. Pubkey *
Create / Reset Sig. Pubkey *
Algorithm Names DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key 0000
Sig. Rmt. Key  0000
----- < > -----
Import Remote Keys  Get Record      OK      Cancel

```

4. Because the **Override**, **Encrypt**, and **Signature** parameters work together, use the following table to determine the values to set in this remote node record:

Scenario	Setting for Override Parameter	Setting for Encrypt and Signature
All files must be encrypted and use signature.	Disable Override by setting to 2.	Enable Signature and Encrypt by setting to 1.
A few files must be encrypted and use signature.	Enable Override by setting to 1.	Disable Signature and Encrypt by setting to 2. You can change these settings in the COPY statement Process so that the individual files use encryption and signature. See Override Settings in Sterling Connect:Direct Processes. For additional information, see the <i>IBM Sterling Connect:Direct Process Language Reference Guide</i> .

In the **STS Parameters** panel, set values for the fields listed in the following table to enable the STS protocol:

Field	Description	Valid Values
Enable STS	Enables or disables using the STS protocol for Sterling Connect:Direct Secure Plus. Note: To specify that the session for a particular Process is to be secure using STS, disable STS by specifying 2 but enable the remote node to override the default of non-secure sessions by specifying YES for the OVERRIDE field. See Override Settings in Sterling Connect:Direct Processes .	1 = Enable STS 2 = Disable STS 3 = Default to local node
Autoupdt	Allows STS keys to be automatically updated when the values change.	1=Yes 2=No 3=Default to local node
Override	Enables or disables the following security override functions on a session-by-session basis: <ul style="list-style-type: none"> Allow values in the COPY statement to override values in the remote node record. Allow the STS protocol to be turned on or off for a particular session overriding the security default in the remote node record. 	1=Yes 2=No 3=Default to local node
Signature	Enables digital signatures for use with the STS protocol.	1=Yes 2=No 3=Default to local node
Encrypt	Enables data encryption with the STS protocol, during the COPY operation. If you activate this feature, you must also populate the Algorithm field. Note: If the SNODE enables encryption, the PNODE cannot disable it.	1=Yes 2=No 3=Default to local node. This is not a valid value for the local node definition.

5. Generate the authentication key as follows:
 - a. Select **Create /Reset Auth. Pubkey** and press **Enter** to display the **Generate Seed** screen.

Secure+ Admin Tool: Generate Seed	
2 1. Specify Value	Specify the seed value by typing it into the text field.
2. Sample Value	Generate a seed by processing text entered from the keyboard.
Random Number Seed:	

- b. Press **Enter** to accept the default value of **2-Sample Value**.
 - c. When the following screen is displayed, edit or add data on any line and press **PF3** to save the information. Changing data creates a unique key value.

```

File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT          SYS06254.T160411.RA000.SSCHR1.R0207298          Columns 00001 00072
Command ==>                               Scroll ==> PAGE
024: This process cannot proceed if the data in the edit file is unchanged.
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 262144
000002
000003 134217728
000004
000005 32
000006
000007 4
000008
000009 8589934592
000010
000011 131072
000012
000013 8388608
000014
000015 2097152
000016
000017 1073741824

```

- d. When the **Pass Phrase Generation** panel is displayed, type a string at least 32 characters long containing at least one uppercase character, one lowercase character, and one numeric value and press **Enter**.

Note: You do not need to remember the pass phrase.

When the Sterling Connect:Direct Secure Plus Create/Update Panel - STS Parameters displays the message Seed generation complete, your public key for strong authentication has been generated and the **Create/Reset Auth. Pubkey** field is populated, as shown in the following illustration.

- 6. To generate the signature key:
 - a. Select **Create/Reset Sig. Pubkey** and press **Enter**.
 - b. Press **Enter** to accept the default value (**2-Sample Value**).

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
REMOTE01                1 1. Y 2. N 3. D Override
                        2 1. Y 2. N 3. D Autoupdt
                        2 1. Y 2. N 3. D Enable STS
Auth Timeout: 120      2 1. Y 2. N 3. D Signature
Algorithm *            2 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys      Expire Date MDY
Create / Reset Sig. Prev. Keys      Expire Date MDY

Create / Reset Auth. Pubkey | ----- < > -----
Create / Reset Sig. Pubkey | 0203.093F.5D89.9024.5080.FE6D.7574.F55B.
Algorithm Names            | 0203.C2DB.B318.1B91.3A11.7FD3.3553.37EA.
Auth. Rmt. Key             | DESCBC56,TDESCBC112,IDEACBC128
Sig. Rmt. Key              | 0000
                           | -----
Import Remote Keys        Get Record        OK        Cancel

```

When the Sterling Connect:Direct Secure Plus Create/Update Panel - STS Parameters displays the message Seed generation complete, your public key for digital signature has been generated and the **Create/Reset Sig. Pubkey** field is populated, as shown in the preceding illustration.

7. Set values in one or more of the following fields as required:

Field Name	Field Description	Valid Values
Algorithm	Specifies the data encryption algorithm used. Also set Encrypt to Yes .	* = Use first algorithm in the Algorithm Names list below DESCBC56 TDESCBC112 IDEACBC128
Create / Reset Auth. Prev. Keys Expire Date	Identifies the expiration date, including the time, for previous authentication public keys used with the STS protocol. This value eliminates the need to update Sterling Connect:Direct Secure Plus parameter file across all nodes in the network simultaneously when public keys for the local node are changed. Authentication Previous Keys are intended to be the most recently active keys prior to the current keys becoming active. To create previous keys, click Create . To clear the keys and any related expiration date, click Reset . The previous key is checked if an operation using the current key fails, and any expiration date for the previous key has not expired.	Format— You must enter both a date and time. Must match the date format specified in the Sterling Connect:Direct server's DATEFORM parameter (for more information, see the DATEFORM parameter in <i>Global Initialization Parameters</i> , in the <i>IBM Sterling Connect:Direct for z/OS Administration Guide</i>). If connected to the Sterling Connect:Direct server, the current date format is displayed after the Expire Date fields and will be either MDY, DMY, YMD, or YDM. If the server cannot be logged on to, the default DATEFORM of MDY is used. For examples of valid date and time formats, see the Help panel.
Create / Reset Sig. Prev. Keys Expire Date	Identifies the expiration date and time for previous digital signature public keys used with the STS protocol. This value eliminates the need to update Sterling Connect:Direct Secure Plus parameter file across all nodes in the network simultaneously when public keys for the local node are changed. Signature Previous Keys are intended to be the most recently active keys prior to the current keys becoming active. To create previous keys, click Create . To clear the keys and any related expiration date, click Reset . The previous key is checked if an operation using the current key fails, and any expiration date for the previous key has not expired.	Format— You must enter both a date and time. Must match the date format specified in the Sterling Connect:Direct server's DATEFORM parameter (for more information, see the DATEFORM parameter in <i>Global Initialization Parameters</i> , in the <i>IBM Sterling Connect:Direct for z/OS Administration Guide</i>). If connected to the Sterling Connect:Direct server, the current date format is displayed after the Expire Date fields and will be either MDY, DMY, YMD, or YDM. If the server cannot be logged on to, the default DATEFORM of MDY is used. For examples of valid date and time formats, see the Help panel.

Field Name	Field Description	Valid Values
Algorithm Names	Lists the acceptable data encryption algorithms to use when copy file encryption is requested. Listed in order of preference, with the most-preferred algorithm listed first.	DESCBC56 TDESCBC112 IDEACBC128
Import Remote Keys (on the Action selection line at the bottom of the panel)	Imports keys from the remote trading partner for both the Authorization and Signature functions in the STS protocol.	The name of the key file to import.
Auth Timeout	Identifies the maximum time, in seconds, that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.	0=No timeout. Sterling Connect:Direct waits indefinitely to receive the next message. Specify a time to prevent malicious entry from taking as much time as necessary to attack the authentication protocol. Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP.TIMER initialization parameter. The default is 120 seconds.
Get Record	Opens another node record.	The name of an existing node record.

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

9. In the **EA Parameters** panel:

- a. Type **3** beside the **Override** field because it is not relevant to Sterling External Authentication Server.
- b. Type **2** beside the **External Auth** field to disable it. The remaining External Authentication fields are available only from 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.

- c. Select **SSL/TLS Parameters** in the panel selection line and press **Enter**.

Secure+ Create/Update Panel - SSL/TLS Parameters

Option:

Node Identification	EA Parameters	STS Parameters
Node	2 1. Y 2. N 3. D	Enable SSL
REMOTE01	2 1. Y 2. N 3. D	Enable TLS

Common Parameters between SSL and TLS

1 1. Y 2. N 3. D	Override
2 1. Y 2. N 3. D	Client Auth
1 1. Y 2. N 3. D	Encrypt

Auth Timeout: 120

Certificate Label	*
Cipher Suites	FF
Certificate Pathname	*
Client Auth. Compare	

OK Cancel

10. In the **SSL/TLS Parameters** panel:
 - a. Type **2** beside the **Enable SSL** and **Enable TLS** fields to disable those protocols.
 - b. Type **1** beside the **Override** field.
 - c. Type **2** beside the **Client Auth** field because it is not valid for the STS protocol.
 - d. Type **1** beside the **Encrypt** field.
 - e. Leave the remaining fields as they are because they are not valid for the STS protocol.
11. Select **OK** and press **Enter** to display the updated values.
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 saving the parameter file.
13. Take one of the following actions:
 - To configure records for remote nodes that use a protocol other than STS, continue with the procedure, *Adding a Remote Node Record to the Parameter File Manually for the SSL or TLS Protocol*.
 - 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 7. 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. In the **Node Identification** panel:
 - a. Type **.EASERVER** in the **Node** field.
 - b. Type **2** beside the **Local/Remote** field.

Note: Leave the **TCP Information** fields (**IP addr** and **Port**) blank because you define them in the EA Parameters panel.

- c. Select **EA Parameters** and press **Enter**.

Secure+ Create/Update Panel - EA Parameters		
Option:		
Node Identification	SSL/TLS Parameters	STS Parameters
Node	1 1. Y 2. N 3. D Override	
SC.OKC.PARIS1	2 1. Y 2. N 3. D External Auth	
External Auth Server Def	CertValidateDef	
External Auth Server Address	10.20.201.2	
External Auth Server Port	23234	
		OK Cancel

4. In the **EA Parameters** panel:
 - a. Type **3** beside the **Override** field because it is not relevant to External Authentication.
 - b. Type **2** beside the **External Auth** field.
 - c. 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.

- d. Select **SSL/TLS Parameters** in the panel selection bar and press **Enter**.
5. In the **SSL/TLS Parameters** panel, enable Sterling Connect:Direct Secure Plus by typing **1** beside the **Enable TLS** or **Enable SSL** field. Select the other protocol you are not using for Sterling External Authentication Server connections and type **2** beside the **Enable TLS** or **Enable SSL** field. and press **Enter**.

Note: If System SSL is in FIPS mode, TLS is the only supported protocol. See "Planning for System SSL in FIPS Mode" on page 4.

6. To enable client authentication:
 - a. Type **1** beside the **Client Auth** field.
 - b. To verify the common certificate name during authentication, select **Client Auth. Compare**. 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.

7. To enable and define the priority of 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 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 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.

9. Select **OK** and press **Enter** to save and close this remote node record.
10. 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.
11. Press **Cancel** to display current settings for the the EA node.

```

File Edit Key Management Help
-----
                                         Row 1 of 1
Secure+ Admin Tool: Main Screen
Option ==>                               Scroll CSR

Table Line Commands are:
E Export pub. key      H View History      D Delete node
U Update node         I Insert node

Secure
LC Node Name          Type 123C Override Encryption Signature ExtAuth Autoupd
-----
.EASERVER             R   NYNY   N       N       N       Y       N
***** BOTTOM OF DATA *****
  
```

12. 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**.

Secure+ Create/Update Panel - Node Identification			
Option:			
EA Parameters	SSL/TLS Parameters	STS Parameters	
Node	1. Local 2. Remote		
Alias Names:	TCP Information: IPaddr: Port:		
Import Remote Keys	Get Record	OK	Cancel

3. On the **Node Identification** panel:
 - a. Type **.CLIENT** in the **Node** 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 **2** next to the **Local/Remote** field.

Note: 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. Also, leave the **Alias Names** field blank.

- c. Select **EA Parameters** in the panel selection bar and press **Enter**.

Secure+ Create/Update Panel - EA Parameters			
Option:			
Node Identification	SSL/TLS Parameters	STS Parameters	
Node	2 1. Y 2. N 3. D Override		
.CLIENT	2 1. Y 2. N 3. D External Auth		
External Auth Server Def			
External Auth Server Address			
External Auth Server Port			
		OK	Cancel

4. In the **EA Parameters** panel:
 - a. Type **2** beside the **Override** field to disable override for the **.CLIENT** remote node record.

Note: To allow nonsecure API connections, type **1** to enable overrides.

- b. Type **2** beside the **External Auth** field to disable it. The remaining EA parameters are unavailable because they are valid only for the .EASERVER remote node record.
 - c. Select **SSL/TLS Parameters** from the panel selection bar 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 4.

- Type **1** beside the **Enable TLS** (or **Enable SSL**) field to enable the desired protocol for this remote node.
 - Type **3** beside the **Enable TLS** (or **Enable SSL**) field to default to the local node setting.
- a. Type **2** beside the **Client Auth** field to disable it.
 - b. Change the value in the **Auth Timeout** field, if necessary, using the following table:

Field	Description	Valid Values
Auth Timeout	Identifies the maximum time, in seconds, that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.	0=No timeout. Sterling Connect:Direct waits indefinitely to receive the next message. 120 = Default. Specify a time to prevent malicious entry from taking as much time as necessary to attack the authentication protocol. Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP.TIMER initialization parameter.

- 6. Select **STS Parameters** in the panel selection bar and press **Enter**.

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
.CLIENT                1 1. Y 2. N 3. D Override
                        2 1. Y 2. N 3. D Autoupdt
                        2 1. Y 2. N 3. D Enable STS
                        2 1. Y 2. N 3. D Signature
Auth Timeout: 120      2 1. Y 2. N 3. D Encrypt
Algorithm *            2 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys      Expire Date MDY
Create / Reset Sig. Prev. Keys      Expire Date MDY

Create / Reset Auth. Pubkey *
Create / Reset Sig. Pubkey *
Algorithm Names DESCBC56, TDESCBC112, IDEACBC128
Auth. Rmt. Key 0000
Sig. Rmt. Key  0000

----- < > -----
Import Remote Keys  Get Record      OK      Cancel

```

- 7. In the **STS Parameters** panel:

- a. Disable the STS protocol by typing **2** beside the following fields:
Autoupdt, **Enable STS**, **Signature**, and **Encrypt**.
- b. Type an asterisk (*) beside the **Algorithm** field.
The remaining fields are not valid for the .CLIENT record.
8. Click **OK** and press **Enter** to save and close the .CLIENT node record.
9. Save the parameter file using the procedure in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.
10. 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** to display the **Edit** menu.
2. On the **Edit** menu, select **1** to select **Create/Update Record** and press **Enter** to display the **Secure+ Create/Update Node Identification** panel.
3. On the **Node Identification** panel:
 - a. Type **.password** in the **Node** field.
 - b. Type **2** next to the **Local** field.

Secure+ Create/Update Panel - Node Identification		
Option:		
EA Parameters	SSL/TLS Parameters	STS Parameters
Node		
.password	2 1. Local	
	2. Remote	
Alias		
Names:	TCP Information:	
	IPaddr:	
	Port:	
Import Remote Keys	Get Record	OK Cancel

- c. Press **Enter** to display the **Secure+ Create/Update Panel - SPE Parameters** screen.

- On the **SPE Parameters** panel, type **1** next to the **Enable SPE** field.

Secure+ Create/Update Panel - SPE Parameters

Option:

Option	Node	Enable SPE
.PASSWORD		1 1. Y 2. N Enable SPE (SPE not currently in use)

----- < > -----

Password Public Key | *
Algorithm Names | TDESCBC112

OK Cancel

Press **Enter** to enable SPE and finish creating the SPE record by clicking **OK**.

- Save the parameter file using the procedure in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.
- Restart Sterling Connect:Direct Secure Plus for z/OS.
- 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

- 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 Key Management Help							
SC.DUB.DOVER1 Secure+ Admin Tool: Main Screen						Row 1 of 7	
Option ==>						Scroll CSR	
Table Line Commands are:							
E Export pub. key		H View History		D Delete node			
U Update node		I Insert node					
Secure							
LC	Node Name	Type	123C	Override	Encryption	Signature	ExtAuth Autoupd
.CLIENT		R	NNNN	Y	N	N	N
.EASERVER		R	N*YN	N	N	N	N
.PASSWORD		R	Y***	*	*	*	*
SC.DUB.DOVER1		L	NNNN	Y	N	N	N
SC.DUB.DOVER2		R	NNYN	Y	N	N	N
SC.DUB.DOVER3		R	NNYN	Y	N	N	N
SC.DUB.DOVER4		R	NYNY	Y	N	N	N
***** BOTTOM OF DATA *****							

- Type **U** next to the **.PASSWORD** record and press **Enter** to display the **Secure+ Create/Update Panel - SPE Parameters** screen.
- On the **SPE Parameters** panel, type **2** next to the **Enable SPE** field and press **Enter**.

Option:		Secure+ Create/Update Panel - SPE Parameters	
Node			
.PASSWORD		2 1. Y 2. N	Enable SPE (SPE not currently in use)
Password Public Key	Algorithm Names	* TDESCBC112	
		----- < > -----	
		OK	Cancel

- Save the parameter file using the procedure in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.
- 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	<p>SPE-formatted passwords exist In the TCQ and/or AUTH files, but Sterling Connect:Direct Secure Plus has not been enabled.</p> <ul style="list-style-type: none"> • 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. 	<p>Sterling Connect:Direct for z/OS has not been set up to run with Sterling Connect:Direct Secure Plus for z/OS. Add the <code>SECURE.DSN=<i>filename</i></code> parameter to the initialization parameters, where <i>filename</i> 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.</p> <p>Reset all passwords in the TCQ and AUTH files by performing these actions:</p> <ul style="list-style-type: none"> • 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. <p>To see more detailed information about individual errors related to the general failure, see the ESTAE trace output.</p>

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.	<ol style="list-style-type: none"> 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. <p>To see more detailed information about individual errors related to the general failure, see the ESTAE trace output.</p>

Chapter 8. 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, TLS, and STS protocols:

- Configuring the Local Node Record for the SSL or TLS Protocol
- Configuring the Local Node Record for the STS 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.
- You must create keys for the STS protocol because this action also creates the key that encrypts the Sterling Connect:Direct Secure Plus 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 or Configuring the Local Node Record for the STS 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, enables the **Override** parameter, and verifies that the selected and STS protocols are disabled. 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 **Override** in the local node record automatically, as shown in the following illustration.

```
File Edit Key Management Help
-----
Row 9 to 13 of 13
Q2A.ZOS.PARIS      Secure+ Admin Tool: Main Screen
Option ==>                               Scroll CSR
Table Line Commands are:
E Export pub. key   H View History     D Delete node
U Update node       I Insert node

LC Node Name      Type  Secure
-----
      123C  Override Encryption Signature ExtAuth Autoupd
-----
u Q2A.ZOS.PARIS   L    NNNN    Y      N      N      N      N
Q3A.ZOS.PARIS   R    ***N    N      *      *      *      *
Q3B.ZOS.PARIS   R    ***N    N      *      *      *      *
SOL36SP          R    ***N    N      *      *      *      *
W2S.4200.CDWOPS8 R    ***N    N      *      *      *      *
***** BOTTOM OF DATA *****
```

2. In the **STS Parameters** panel, verify that the following STS protocol parameters are disabled: **Autoupdt**, **Enable STS**, **Signature**, and **Encrypt**.


```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
Q2A.ZOS.PARIS          1 1. Y 2. N 3. D Override
                       2 1. Y 2. N 3. D Autoupdt
                       2 1. Y 2. N 3. D Enable STS
Auth Timeout: 120      2 1. Y 2. N 3. D Signature
Algorithm *            2 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys      Expire Date
Create / Reset Sig. Prev. Keys      Expire Date

Create / Reset Auth. Pubkey | *
Create / Reset Sig. Pubkey | *
Algorithm Names             | DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key              |
Sig. Rmt. Key               |
----- < > -----
Import Remote Keys      Get Record      OK      Cancel

```

3. Generate the STS protocol authentication key, which is part of the key pair that is used to encrypt the parameter file:
 - a. Select **Create/Reset Auth. Pubkey** and press **Enter** to display the **Generate Seed** screen.

```

Secure+ Admin Tool: Generate Seed

2 1. Specify Value      Specify the seed value by typing it
                       into the text field.
2. Sample Value        Generate a seed by processing text
                       entered from the keyboard.

Random Number
Seed:

```

- b. Press **Enter** to accept the default value of **2-Sample Value**.
- c. When the following screen is displayed, edit or add data on any line and press **PF3** to save the information. Changing data creates a unique key value.

```

File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT          SYS06254.T160411.RA000.SSCHR1.R0207298          Columns 00001 00072
Command ==>                               Scroll ==> PAGE
024: This process cannot proceed if the data in the edit file is unchanged.
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 262144
000002
000003 134217728
000004
000005 32
000006
000007 4
000008
000009 8589934592
000010
000011 131072
000012
000013 8388608
000014
000015 2097152
000016
000017 1073741824

```

- d. When the message *This is Loop 2 of 10* is displayed, type over data on any line and press **PF3** up to 10 times. This step is only necessary the first time you generate keys within the Sterling Connect:Direct Secure Plus Admin Tool for each parameter file. Repeating the process increases the randomness of keys.
- e. When the **Pass Phrase Generation** panel is displayed, type a string at least 32 characters long containing at least one uppercase character, one lowercase character, and one numeric value and press **Enter**.

Note: You do not need to remember the pass phrase.

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
Q2A.ZOS.PARIS          1 1. Y 2. N 3. D Override
                       2 1. Y 2. N 3. D Autoupdt
Auth Timeout: 120      2 1. Y 2. N 3. D Enable STS
Algorithm *            2 1. Y 2. N 3. D Signature
                       2 1. Y 2. N 3. D Encrypt
Create / Reset Auth. Pubkey 0203.093F.5D89.9024.5080.FE6D.7574.F55B.
Create / Reset Sig. Pubkey
Algorithm Names         DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key
Sig. Rmt. Key
----- < > -----
Import Remote Keys      Get Record              OK              Cancel

```

When the Sterling Connect:Direct Secure Plus Create/Update Panel - STS Parameters displays the message Seed generation complete, your public key for strong authentication has been generated and the **Create/Reset Auth. Pubkey field** is populated, as shown in the preceding illustration.

4. Generate the signature key, which is part of the key pair used to encrypt the parameter file:
 - a. Select **Create/Reset Sig. Pubkey** and press Enter.
 - b. Press **Enter** to accept the default value (**2-Sample Value**).

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
Q2A.ZOS.PARIS          1 1. Y 2. N 3. D Override
                       2 1. Y 2. N 3. D Autoupdt
                       2 1. Y 2. N 3. D Enable STS
                       2 1. Y 2. N 3. D Signature
                       2 1. Y 2. N 3. D Encrypt
Auth Timeout: 120
Algorithm *
Create / Reset Auth. Prev. Keys      Expire Date
Create / Reset Sig. Prev. Keys      Expire Date
Create / Reset Auth. Pubkey          ----- < > -----
Create / Reset Sig. Pubkey          0203.093F.5D89.9024.5080.FE6D.7574.F55B.
Algorithm Names                     0201.C2DB.B318.1B91.3A11.7FD3.3553.37EA.
Auth. Rmt. Key                      DESCBC56,TDESCBC112,IDEACBC128
Sig. Rmt. Key                       0000
                                     0000
Import Remote Keys      Get Record      OK      Cancel

```

When the Sterling Connect:Direct Secure Plus Create/Update Panel - STS Parameters displays the message Seed generation complete, your public key for digital signature has been generated and the **Create/Reset Sig. Pubkey** field is populated, as shown in the preceding illustration.

5. Select **SSL/TLS Parameters** in the panel selection line and press **Enter** to display the **SSL/TLS Parameters** panel.

```

Secure+ Create/Update Panel - SSL/TLS Parameters
Option:
Node Identification      EA Parameters      STS Parameters
Node
Q2A.ZOS.PARIS          1 1. Y 2. N 3. D Enable SSL
                       2 1. Y 2. N 3. D Enable TLS
Common Parameters between SSL and TLS
2 1. Y 2. N 3. D Override
1 1. Y 2. N 3. D Client Auth
1 1. Y 2. N 3. D Encrypt
Auth Timeout: 120
Certificate Label
Cipher Suites
Certificate Pathname
Client Auth. Compare
-----
*
FF
*
-----
OK      Cancel

```

6. To select the protocol you want to enable, type **1** beside the **Enable SSL** or **Enable TLS** field. Type **2** beside the other field to disable the other protocol.

Note: If System SSL is in FIPS mode, TLS is the only supported protocol. See “Planning for System SSL in FIPS Mode” on page 4.

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.

7. Type **1** in the **Override** field and **2** in the **Client Auth** field.
8. Take one of the following actions 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.
9. Update the value for the **Auth Timeout** field, if necessary Refer to the following table:

Field	Description	Valid Values
Auth Timeout	Identifies the maximum time, in seconds, that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.	<p>0=No timeout. Sterling Connect:Direct waits indefinitely to receive the next message.</p> <p>Specify a time to prevent malicious entry from taking as much time as necessary to attack the authentication protocol. Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP.TIMER initialization parameter.</p> <p>The default is 120 seconds.</p>

10. 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 4.
 - 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**.
11. 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 4.
 - 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.

12. 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.

```

More:      +
More:      +

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

0
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

```

- b. Type **1** by the cipher suite you want to enable and give the highest priority.
- c. Type **2** 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=8C000AE** 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.

13. Select **EA Parameters** and press **Enter**.
14. 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.
15. 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.
16. 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.

Configuring the Local Node Record for the STS 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 STS protocol, enables the **Override** parameter, and verifies that the TLS and SSL protocols are disabled. Remember that all options set for the local node are inherited by all remote node records.

To update the local node record imported from the network map:

Procedure

1. Type **U** next to the local node record and press **Enter**. The **Secure+ Create/Update Panel** displays the current values for the selected node.

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

File Edit Key Management Help							
							Row 9 to 13 of 13
Q2A.ZOS.PARIS				Secure+ Admin Tool: Main Screen			Scroll CSR
Option ==>							
Table Line Commands are:							
E Export pub. key		H View History		D Delete node			
U Update node		I Insert node					
Secure							
LC	Node Name	Type	123C	Override	Encryption	Signature	ExtAuth Autoupd
u	Q2A.ZOS.PARIS	L	NNNN	Y	N	N	N N
	Q3A.ZOS.PARIS	R	***N	N	*	*	* *
	Q3B.ZOS.PARIS	R	***N	N	*	*	* *
	SOL36SP	R	***N	N	*	*	* *
	W2S.4200.CDWOPS8	R	***N	N	*	*	* *
***** BOTTOM OF DATA *****							

2. In the **STS Parameters** panel:

- a. Type **1** beside the **Enable STS** field to enable the STS protocol.
- b. Set values in one or more of the following fields to configure the STS protocol parameters:

Field Name	Field Description	Valid Values
Autoupdt	Allows STS keys to be automatically update when the values change.	1=Yes 2=No 3=Default to local node.
Override	Allows settings in a remote node record to override settings in the local node record.	1=Yes 2=No 3=Default to local node.
Signature	Enables digital signatures for use with the STS protocol.	1=Yes 2=No 3=Default to local node. This is not a valid value for the local node definition.
Encrypt	Enables data encryption with the STS protocol, during the copy operation. If you activate this feature, you must also populate Algorithm . If the SNODE enables encryption, the PNODE cannot disable it.	1=Yes 2=No 3=Default to local node. This is not a valid value for the local node definition.
Algorithm	Specifies the data encryption algorithm used. Also set Encrypt to Yes .	* = Use first algorithm in list DESCBC56 TDESCBC112 IDEACBC128
Sig. Prev. Keys Expire Date	Identifies the expiration date for previous digital signature public keys used with the STS protocol. This value eliminates the need to update Sterling Connect:Direct Secure Plus parameter files across all nodes in the network simultaneously when public keys for the local node are changed.	Format YYYY/MM/DD HH:MM:SS If time is not specified, 00:00:01 is used.
Auth. Pubkey	Generates the public key used for strong authentication with the STS protocol.	Generated by Sterling Connect:Direct Secure Plus. See step 3 in Configuring the Local Node Record for the SSL or TLS Protocol .
Sig. Pubkey	Generates the public key used for digital signature with the STS protocol.	Generated by Sterling Connect:Direct Secure Plus. See step 5 in Configuring the Local Node Record for the SSL or TLS Protocol .

Field Name	Field Description	Valid Values
Algorithm Names	Lists the acceptable data encryption algorithms to use when copy file encryption is requested. Listed in order of preference, with the most-preferred algorithm listed first.	DESCBC56 TDESCBC112 IDEACBC128 Not used with the TLS or SSL protocol.
Import Remote Keys	Imports keys from the remote trading partner for both the Authorization and Signature functions in the STS protocol.	The name of the key file to import.
Auth. Prev. Keys Expire Date	Identifies the expiration date for previous authentication public keys used with the STS protocol. This value eliminates the need to update Sterling Connect:Direct Secure Plus parameter files across all nodes in the network simultaneously when public keys for the local node are changed.	Format YYYY/MM/DD HH:MM:SS If time is not specified, 00:00:01 is used.
Auth Timeout	Identifies the maximum time, in seconds, that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.	0=No timeout. Sterling Connect:Direct waits indefinitely to receive the next message. Specify a time to prevent malicious entry from taking as much time as necessary to attack the authentication protocol. Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP.TIMER initialization parameter. The default is 120 seconds.


```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node                    Node              1 1. Y 2. N 3. D Override
Q2A.ZOS.PARIS          2 1. Y 2. N 3. D Autoupdt
                        2 1. Y 2. N 3. D Enable STS
                        Auth Timeout: 120 2 1. Y 2. N 3. D Signature
                        Algorithm      * 2 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys      Expire Date
Create / Reset Sig. Prev. Keys      Expire Date

Create / Reset Auth. Pubkey
Create / Reset Sig. Pubkey
Algorithm Names      DESCBC56, TDESCBC112, IDEACBC128
Auth. Rmt. Key      0000
Sig. Rmt. Key      0000

Import Remote Keys      Get Record      OK      Cancel

```

3. Generate the authentication key for use with the STS protocol:

- a. Select **Create/Reset Auth. Pubkey** and press **Enter** to display the **Generate Seed** screen.

```

Secure+ Admin Tool: Generate Seed

2 1. Specify Value      Specify the seed value by typing it
                        into the text field.
2. Sample Value      Generate a seed by processing text
                        entered from the keyboard.

Random Number
Seed:

```

- b. Press **Enter** to accept the default value of **2-Sample Value**. The following screen is displayed.

```

File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT      SYS06254.T160411.RA000.SSCHR1.R0207298      Columns 00001 00072
Command ==>      Scroll ==> PAGE
024: This process cannot proceed if the data in the edit file is unchanged.
==MSG> -Warning- The UNDO command is not available until you change
==MSG>      your edit profile using the command RECOVERY ON.
000001 262144
000002
000003 134217728
000004
000005 32
000006
000007 4
000008
000009 8589934592
000010
000011 131072
000012
000013 8388608
000014
000015 2097152
000016
000017 1073741824

```

- c. Edit or add data on any line and press **PF3**. Changing data creates a unique key value.
- d. If the message *This is Loop 2 of 10* is displayed, type over data on any line and press **PF3** up to 10 times. This step is only necessary the first time you generate keys within the Sterling Connect:Direct Secure Plus Admin Tool for each parameter file. Repeating the process increases the randomness of keys.
- e. When the **Pass Phrase Generation** panel is displayed, type a string at least 32 characters long containing at least one uppercase character, one lowercase character, and one numeric value and press **Enter**.

Note: You do not need to remember the pass phrase

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
Q2A.ZOS.PARIS          1 1. Y 2. N 3. D Override
                        2 1. Y 2. N 3. D Autoupdt
                        2 1. Y 2. N 3. D Enable STS
                        2 1. Y 2. N 3. D Signature
                        2 1. Y 2. N 3. D Encrypt
Auth Timeout: 120
Algorithm *
Create / Reset Auth. Prev. Keys      Expire Date
Create / Reset Sig. Prev. Keys      Expire Date
Create / Reset Auth. Pubkey          ----- < > -----
Create / Reset Sig. Pubkey          0303.ADB4.2924.EADD.FF27.4B7F.B248.E1CA
Algorithm Names                     DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key                      0000
Sig. Rmt. Key                       0000
-----
Import Remote Keys      Get Record      OK      Cancel

```

When the Sterling Connect:Direct Secure Plus Create/Update Panel displays the message Seed generation complete, your public key for strong authentication has been generated and the **Create/Reset Auth. Pubkey** field is populated.

- 4. To generate the signature key:
 - a. Select **Create/Reset Sig. Pubkey** and press **Enter**.
 - b. Press **Enter** to accept the default value (**2-Sample Value**).

Secure+ Create/Update Panel - STS Parameters			
Option:			
Node Identification	EA Parameters	SSL/TLS Parameters	
Node		1 1. Y 2. N 3. D Override	
Q2A.ZOS.PARIS		2 1. Y 2. N 3. D Autoupdt	
		2 1. Y 2. N 3. D Enable STS	
	Auth Timeout: 120	2 1. Y 2. N 3. D Signature	
	Algorithm *	2 1. Y 2. N 3. D Encrypt	
Create / Reset	Auth. Prev. Keys		Expire Date
Create / Reset	Sig. Prev. Keys		Expire Date
Create / Reset	Auth. Pubkey	----- < > -----	
Create / Reset	Sig. Pubkey	0203.093F.5D89.9024.5080.FE6D.7574.F55B.	
	Algorithm Names	0201.C2DB.B318.1B91.3A11.7FD3.3553.37EA.	
	Auth. Rmt. Key	DESCBC56,TDESCBC112,IDEACBC128	
	Sig. Rmt. Key	0000	
		0000	
Import Remote Keys	Get Record	OK	Cancel

When the Sterling Connect:Direct Secure Plus Create/Update Panel displays the message Seed generation complete, your public key for digital signature has been generated and the **Create/Reset Sig. Pubkey** field is populated, as shown in the preceding illustration.

5. Select **EA Parameters** and press **Enter**.
6. In the **EA Parameters** panel, type **2** beside the **Enable External Auth** field. The remaining external authentication fields are unavailable because they are valid only for the .EASERVER remote node record.
7. Select **OK** and press **Enter** to display the updated values.
8. 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.
9. 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 9. 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, TLS, and STS protocols, and to disable all protocols for a remote node:

- Configuring a Remote Node Record for the SSL or TLS Protocol
- Configuring a Remote Node Record for the STS 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.
- You must create keys for remote nodes that use the the STS protocol.
- 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 - **STS 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 Key Management Help
-----
Row 9 to 13 of 13
Q3B.ZOS.PARIS Secure+ Admin Tool: Main Screen
Option ==> Scroll CSR

Table Line Commands are:
E Export pub. key H View History D Delete node
U Update node I Insert node

Secure
LC Node Name Type 123C Override Encryption Signature ExtAuth Autoupd
-----
Q2A.ZOS.PARIS L NYNN Y N N N N
Q3A.ZOS.PARIS R ***N N * * * *
u Q3B.ZOS.PARIS R ***N N * * * *
SOL36SP R ***N N * * * *
***** BOTTOM OF DATA *****

```

2. In the **STS Parameters** panel:
 - a. Verify that the following parameters are disabled (set to **2**): **Override**, **Autoupdt**, **Enable STS**, **Signature**, and **Encrypt**, or set to **Default to Local Node (3)**.
 - b. Verify that the following fields are set to **Default to Local Node (3)**: **Create/Reset Auth. Pubkey**, and **Create/Reset Sig. Pubkey**.

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification EA Parameters SSL/TLS Parameters
Node 1 1. Y 2. N 3. D Override
Q3B.ZOS.PARIS 2 1. Y 2. N 3. D Autoupdt
Auth Timeout: 120 2 1. Y 2. N 3. D Enable STS
Algorithm * 2 1. Y 2. N 3. D Signature
3 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys Expire Date
Create / Reset Sig. Prev. Keys Expire Date

Create / Reset Auth. Pubkey *
Create / Reset Sig. Pubkey *
Algorithm Names DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key 0000
Sig. Rmt. Key 0000

Import Remote Keys Get Record OK Cancel

```

- c. 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 4.

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.

Configuring a Remote Node Record for the STS Protocol

About this task

After you configure the local node, you can configure remote node records. When you imported the network map file, you created 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 record.

- If you disabled Sterling Connect:Direct Secure Plus 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 **COPY** or **PROCESS** statement. For more information, see **Override Settings in Sterling Connect:Direct Processes** .

- You must perform additional tasks for those nodes that use the STS protocol. Refer to Key Management for STS.

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

To update a remote node record for the STS protocol:

Procedure

1. Type **U** next to the remote node record to update and press **Enter**. The **Secure+ Create/Update Panel** displays the current values for the selected node.

```

File Edit Key Management Help
-----
Row 9 to 13 of 13
Q3B.ZOS.PARIS      Secure+ Admin Tool: Main Screen
Option ==>>>                                           Scroll CSR

Table Line Commands are:
E Export pub. key      H View History      D Delete node
U Update node          I Insert node

Secure
LC Node Name          Type  123C  Override Encryption Signature ExtAuth Autoupd
-----
Q2A.ZOS.PARIS        L   YNNN   Y      Y      Y      N      Y
Q3A.ZOS.PARIS        R   ***N   N      *      *      *      *
u Q3B.ZOS.PARIS      R   ***N   N      *      *      *      *
SOL36SP              R   ***N   N      *      *      *      *
W2S.4200.CDWOPS8    R   ***N   N      *      *      *      *
***** BOTTOM OF DATA *****

```

2. In the **STS Parameters** panel:
 - a. Review the following table to determine the values to set for the **Override**, **Encrypt**, and **Signature** parameters because these parameters work together.

Scenario	Setting for Override Parameter	Setting for Encrypt and Signature
All files must be encrypted and use signature.	Disable Override by setting to 2.	Enable Signature and Encrypt by setting to 1. Note: If you disable Override, you cannot disable security in the PROCESS statement.

Scenario	Setting for Override Parameter	Setting for Encrypt and Signature
A few files must be encrypted and use signature.	Enable Override by setting to 1.	Disable Signature and Encrypt by setting to 2. You can override these settings in a COPY statement so that the individual files use encryption and signature. See Override Settings in Sterling Connect:Direct Processes. For a complete description of the SECURE parameter, see the <i>IBM Sterling Connect:Direct Process Language Reference Guide</i> .

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node
Q3B.ZOS.PARIS          1 1. Y 2. N 3. D Override
                       2 1. Y 2. N 3. D Autoupdt
                       2 1. Y 2. N 3. D Enable STS
Auth Timeout: 120      2 1. Y 2. N 3. D Signature
Algorithm *            2 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys      Expire Date
Create / Reset Sig. Prev. Keys      Expire Date

Create / Reset Auth. Pubkey
Create / Reset Sig. Pubkey
Algorithm Names
Auth. Rmt. Key
Sig. Rmt. Key
----- < > -----
DESCBC56,TDESCBC112,IDEACBC128
0000
0000

Import Remote Keys      Get Record      OK      Cancel

```

b. Set values for the parameters listed in the following table to enable the STS protocol:

Field	Description	Valid Values
Enable STS	Enables or disables using the STS protocol for Sterling Connect:Direct Secure Plus.	1 = Enable STS 2 = Disable STS 3 = Default to local node
Autoupdt	Allows STS keys to be automatically updated when the values change.	1=Yes 2=No 3=Default to local node
Override	Activating override in a remote node record that uses the STS protocol enables the values in the COPY statement to override values in the remote node record.	1=Yes 2=No 3=Default to local node

Field	Description	Valid Values
Signature	Enables digital signatures for use with the STS protocol.	1=Yes 2=No 3=Default to local node
Encrypt	Enables data encryption with the STS protocol during the COPY operation. If you activate this feature, you must also populate the Algorithm field. If the SNODE enables encryption, the PNODE cannot disable it.	1=Yes 2=No 3=Default to local node. This is not a valid value for the local node definition.
Algorithm	Specifies the data encryption algorithm used. Also set Encrypt to Yes .	* = Use first algorithm in list DESCBC56 TDESCBC112 IDEACBC128
Auth Timeout	Identifies the maximum time, in seconds, that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.	0=No timeout. Sterling Connect:Direct waits indefinitely to receive the next message. Specify a time to prevent malicious entry from taking as much time as necessary to attack the authentication protocol. Set the value equal to or greater than the value set for the Sterling Connect:Direct TCP.TIMER initialization parameter. The default is 120 seconds.

3. Generate the authentication key for use with the STS protocol:
 - a. Select **Create/Reset Auth. Pubkey** and press **Enter**. to display the **Generate Seed** screen.

Secure+ Admin Tool: Generate Seed	
2 1. Specify Value	Specify the seed value by typing it into the text field.
2. Sample Value	Generate a seed by processing text entered from the keyboard.
Random Number Seed:	

- b. Press **Enter** to accept the default value of **2-Sample Value**.
- c. When the following screen is displayed, edit or add data on any line and press **PF3** to save the information. Changing data creates a unique key value.

```

File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT          SYS06254.T160411.RA000.SSCHR1.R0207298          Columns 00001 00072
Command ==>                               Scroll ==> PAGE
024: This process cannot proceed if the data in the edit file is unchanged.
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 262144
000002
000003 134217728
000004
000005 32
000006
000007 4
000008
000009 8589934592
000010
000011 131072
000012
000013 8388608
000014
000015 2097152
000016
000017 1073741824

```

4. Generate the signature key:
 - a. Select **Create/Reset Sig. Pubkey** and press **Enter**.
 - b. Press **Enter** to accept the default value (**2-Sample Value**).
5. Set values for one or more of the following parameters as required:

Field Name	Field Description	Valid Values
Sig. Prev. Keys Expire Date	Identifies the expiration date for previous digital signature public keys used with the STS protocol. This value eliminates the need to update Sterling Connect:Direct Secure Plus parameter files across all nodes in the network simultaneously when public keys for the local node are changed.	Format YYYY/MM/DD HH:MM:SS If time is not specified, 00:00:01 is used.
Algorithm Names	Lists the acceptable data encryption algorithms to use when copy file encryption is requested. Listed in order of preference, with the most-preferred algorithm listed first.	DESCBC56 TDESCBC112 IDEACBC128
Import Remote Keys	Imports keys from the remote trading partner for both the Authorization and Signature functions in the STS protocol.	The name of the key file to import.
Auth. Prev. Keys Expire Date	Identifies the expiration date for previous authentication public keys used with the STS protocol. This value eliminates the need to update Sterling Connect:Direct Secure Plus parameter files across all nodes in the network simultaneously when public keys for the local node are changed.	Format YYYY/MM/DD HH:MM:SS If time is not specified, 00:00:01 is used.
Get Record	Opens another node record.	The name of an existing node record.

6. Select **EA Parameters** and press **Enter**.
7. Verify that the **External Auth** field is disabled (set to **2**) or set to **Default to Local Node (3)**.

8. Select **SSL/TLS Parameters** and press **Enter**.
9. Verify that the **Enable SSL**, **Enable TLS**, and the **Client Auth** fields are set to **Default to Local Node (3)** or disabled (2).
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 may be unable to perform secure communications. You must resolve all errors before saving the parameter file.
12. Save the parameter file using the procedure 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 in the **Secure+ Create/Update Panel - STS Parameters** panel.

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

File Edit Key Management Help							
							Row 9 to 13 of 13
Q3B.ZOS.PARIS		Secure+ Admin Tool: Main Screen				Scroll CSR	
Option ==>							
Table Line Commands are:							
E Export pub. key	H View History		D Delete node				
U Update node	I Insert node						
Secure							
LC	Node Name	Type	123C	Override	Encryption	Signature	ExtAuth Autoupd
	Q2A.ZOS.PARIS	L	NYNN	Y	N	N	N N
	Q3A.ZOS.PARIS	R	***N	N	*	*	* *
u	Q3B.ZOS.PARIS	R	***N	N	*	*	* *
	SOL36SP	R	***N	N	*	*	* *
	W2S.4200.CDWOPS8	R	***N	N	*	*	* *
***** BOTTOM OF DATA *****							

2. In the **STS Parameters** panel:
 - a. Disable (set to 2) the following parameters: **Override**, **Autoupdt**, **Enable STS**, **Signature**, and **Encrypt**, if necessary.
 - b. Verify that the following fields are set to Default to Local Node (*): **Create/Reset Auth. Pubkey**, and **Create/Reset Sig. Pubkey**.

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node                    1 1. Y 2. N 3. D Override
Q3B.ZOS.PARIS          2 1. Y 2. N 3. D Autoupdt
                        2 1. Y 2. N 3. D Enable STS
                        Auth Timeout: 120
                        Algorithm      *      2 1. Y 2. N 3. D Signature
                        2 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys      Expire Date
Create / Reset Sig. Prev. Keys      Expire Date

Create / Reset Auth. Pubkey      *
Create / Reset Sig. Pubkey      *
Algorithm Names      DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key      0000
Sig. Rmt. Key      0000

----- < > -----

Import Remote Keys      Get Record      OK      Cancel

```

3. Select **EA Parameters** and press **Enter**.
4. 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.
5. Select **SSL/TSL Parameters** in the panel selection line and press **Enter**.
6. If necessary, disable the SSL and TLS protocols by typing **2** beside the **Enable SSL** and **Enable TLS** fields, if necessary.
7. Select **OK** and press **Enter** to display the updated values.
8. 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.
9. Save the parameter file using the instructions in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.

Chapter 10. Manage Keys for the STS Protocol

For nodes that use the STS protocol, you are responsible for managing the keys that you create. When you configure a remote node record to use the STS protocol, you must exchange keys with the trading partner before you can use Sterling Connect:Direct Secure Plus to establish a secure connection with that node. The first time you use the STS protocol, you manually exchange keys with each trading partner. After you exchange keys for the first communications session with Sterling Connect:Direct Secure Plus, if you have enabled the Autoupdate parameter, then the STS public keys are updated automatically for subsequent communications sessions, which simplifies key management for ongoing communications.

To manage the keys for the STS protocol, perform the following tasks:

- Export keys to your trading partner
- Import keys from your trading partner
- Validate the Sterling Connect:Direct Secure Plus parameter file

Exchanging STS Keys the First Time

About this task

The first time you exchange STS keys with your trading partners that use the STS protocol, you must perform the following steps on both systems where Sterling Connect:Direct Secure Plus is installed.

To exchange STS keys the first time:

Procedure

1. Open the remote node records for the trading partners that use the STS protocol and ensure that the **Enable STS** parameter is set to **1** on both systems where Sterling Connect:Direct Secure Plus is installed.

Note: The STS protocol must be enabled in the remote node record to export the STS keys to a file.

2. Export your STS keys using the procedure Exporting STS Keys.
3. Open the remote record again and disable Sterling Connect:Direct Secure Plus by typing **2** beside the **Enable STS** field in the **STS Parameters** panel.

Note: You must disable Sterling Connect:Direct Secure Plus until you have transferred your keys to your trading partner, imported keys from the remote trading partner, and enabled Sterling Connect:Direct Secure Plus because your sessions will fail if you have enabled the STS protocol but you have not exchanged keys.

4. Save the parameter file.
5. To ensure the integrity of the export file that contains your STS keys, create a Sterling Connect:Direct Secure Plus for z/OS Process to transfer the export key file to your trading partner.

Note: If you are sending the export key file to a non-mainframe node, you must send it in binary format.

3. Type the name of this export file or use the default name.

Secure+ Admin Tool: File Selection		
Enter file name for: Secure Export Prefix		
File Name:	USERID.secure.export	Browse
File System Type:	1 1. MVS 2. HFS	Cancel

4. Type **1** to select MVS™ as the file type or type **2** to select **HFS** and press **Enter**. The **Secure+ Create/Update Panel** displays the message *Export Successful*.
5. To ensure the integrity of the export file that contains your STS keys, create a Sterling Connect:Direct Secure Plus for z/OS Process to transfer your export key file to your trading partner.

Note: If you are sending the export key file to a non-mainframe node, you must send it in binary format.

Importing STS Keys from a File

About this task

When you receive the STS key file from the administrator of the remote node (trading partner), you must import it to the Sterling Connect:Direct Secure Plus parameter file. This example illustrates how to import the remote node key file named USERID.SECURE.EXPQ3A.#CSGPRO.#D390.

To import the authentication and digital signature public key values:

Procedure

1. From the **Secure+ Admin Tool: Main Screen**, select **Key Management** and press **Enter**.
2. Perform one of the following actions:
 - Type **1** to select **Import Public Keys** and press **Enter**. This option imports keys from your trading partner for all nodes in the parameter file.
 - Type **U** next to the node for which you want to import keys.

LC	Node Name	Type	Secure 123C	Override	Encryption	Signature	ExtAuth	Autoupd
AIX3601SP		R	***N	N	*	*	*	*
CSG.PROD390		L	NNNN	Y	N	N	N	N
Q1A.ZOS.PARIS		R	***N	N	*	*	*	*
Q1E.ZOS.PARIS		R	***N	N	*	*	*	*
Q1G.ZOS.PARIS		R	***N	N	*	*	*	*
Q2A.ZOS.PARIS		R	***N	N	*	*	*	*
Q3A.ZOS.PARIS		R	Y***	N	N	N	*	N
W2S.4200.CDWOPS8		R	***N	N	*	*	*	*

- Type the file name prefix or partial prefix followed by an asterisk (*), select **Browse**, and press **Enter**, or type the complete file name that you received from your trading partner, as shown in the following illustration.

```

Secure+ Admin Tool: File Selection

Enter file name for: Secure Import File

File Name:      USERID.SECURE.EXPQ3A.#CSGPRO.#D390      Browse
File System Type:
1 1. MVS  2. HFS                                          Cancel

```

- Type **S** next the file to import, (ensure that the file extension of the import file includes the node name) and press **Enter**.

```

Secure+ Admin Tool: File Selection                               Row 1 of 1

Option: _____ Scroll CSR

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

LC Filename or Directory
s USERID.SECURE.EXPQ3A.#CSGPRO.#D390
***** Bottom of data *****

```

The message *2 entries imported from othernote* is displayed on the **Secure+ Admin Tool: Main Screen**, indicating that both the authentication and the digital signature public keys have been imported.

```

File Edit Key Management Help
-----
Row 7 of 10
CSG.PROD390 Secure+ Admin Tool: Main Screen
024: 2 entries imported from Q3A.ZOS.PARIS

Table Line Commands are:
E Export pub. key H View History D Delete node
U Update node I Insert node

Secure
LC Node Name Type 123C Override Encryption Signature ExtAuth Autoupd
-----
Q3A.ZOS.PARIS R Y*** N N N * N
W2S.4200.CDWOPS8 R ***N N * * * *
135.71.104.3 R ***N N * * * *
199.0.91.45 R ***N N * * * *
***** BOTTOM OF DATA *****

```

- Type **U** next to the remote node record name and press **Enter** to verify that the remote public keys are imported. If the keys have been imported, the keys are displayed in the **Auth. Rmt. Key** and the **Sig. Rmt. Key** fields.

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification EA Parameters SSL/TLS Parameters
Node 1 1. Y 2. N 3. D Override
Q3A.ZOS.PARIS 2 1. Y 2. N 3. D Autoupdt
Auth Timeout: 120 2 1. Y 2. N 3. D Enable STS
Algorithm * 2 1. Y 2. N 3. D Signature
2 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys Expire Date
Create / Reset Sig. Prev. Keys Expire Date

Create / Reset Auth. Pubkey | 0303.1C2E.630C.E557.4F27.B1BB.358F.BB3A.
Create / Reset Sig. Pubkey | 0206.4C8C.575F.5956.35D8.C91F.EB0E.CAE8.
Algorithm Names | DESCBC56,TDESCBC112,IDEACBC128
Auth. Rmt. Key | 0200.0A7E.686B.49FC.B1E1.1BC3.E844.BA5B.
Sig. Rmt. Key | 0301.46C6.20A2.0F09.70F0.9C7D.E401.DE1A.

Import Remote Keys Get Record OK Cancel

```

After you and your trading partner have imported each other's keys, you can verify that you have imported the keys correctly by displaying the STS Parameters panel for the remote node record on each system and validating that the key values have the correspondence illustrated in the following table. See the STS Parameters panels preceding and following this table for the data used to illustrate the correspondence.

Node Record	Parameter and Value	Node Record	Parameter and Value
Q3A.ZOS.PARIS	Create / Reset Auth. Pubkey= 0303.1C2E.630C.E557. 4F27.B1BB.358F.BB3A.	CSG.PROD390	Auth. Rmt. Key= 0303.1C2E.630C.E557. 4F27.B1BB.358F.BB3A.
Q3A.ZOS.PARIS	Create / Reset Sig. Pubkey= 0206.4C8C.575F.5956. 35D8.C91F.EB0E.CAE8.	CSG..PROD390	Sig. Rmt. Key= 0206.4C8C.575F.5956. 35D8.C91F.EB0E.CAE8.

Node Record	Parameter and Value	Node Record	Parameter and Value
CSG.PROD390	Create / Reset Auth. Pubkey 0303.1C2E.630C.E557. 4F27.B1BB.358F.BB3A.	Q3A.ZOS.PARIS	Auth.Rmt. Key= 0303.1C2E.630C.E557. 4F27.B1BB.358F.BB3A.
CSG.PROD390	Create / Reset Sig. Pubkey= 0206.4C8C.575F.5956. 35D8.C91F.EB0E.CAE	Q3A.ZOS.PARIS	Sig. Rmt. Key= 0206.4C8C.575F.5956. 35D8.C91F.EB0E.CAE

```

Secure+ Create/Update Panel - STS Parameters
Option:
Node Identification      EA Parameters      SSL/TLS Parameters
Node                    Node                1 1. Y 2. N 3. D Override
CSG.PROD390             2 1. Y 2. N 3. D Autoupdt
                        2 1. Y 2. N 3. D Enable STS
                        Auth Timeout: 120
                        Algorithm      *      2 1. Y 2. N 3. D Signature
                        2 1. Y 2. N 3. D Encrypt

Create / Reset Auth. Prev. Keys      Expire Date
Create / Reset Sig. Prev. Keys      Expire Date

Create / Reset Auth. Pubkey | ----- < > -----
Create / Reset Sig. Pubkey | 0200.0A7E.686B.49FC.B1E1.1BC3.E844.BA5B.
Algorithm Names            | 0301.46C6.20A2.0F09.70F0.9C7D.E401.DE1A.
Auth. Rmt. Key             | DESCBC56,TDESCBC112,IDEACBC128
Sig. Rmt. Key              | 0303.1C2E.630C.E557.4F27.B1BB.358F.BB3A.
                          | 0206.4C8C.575F.5956.35D8.C91F.EB0E.CAE8.
                          | -----

Import Remote Keys      Get Record      OK      Cancel

```

Importing STS Keys Manually

About this task

If you do not have a key file from which to import, but you have a hard copy printout of the keys, you must type the keys into the parameter file.

To type keys into the parameter file:

Procedure

1. Locate an existing export file.
2. Create a data set with DCB= LRECL=255 BLKSIZE=23200 RECFM=VB and copy the export file from step 1 into this data set.

Note: This step provides a guide for preallocation of the file. If you get the error *Import fails with "024 0 entries imported"* when the file is preallocated with this DCB information, do not specify DCB information. Use the DCB information defined in the input file. If you preallocate the file and the error message is displayed, delete the preallocated file and reallocate the file with larger lrecl and blksize values.

3. Using the **DGA#ADR2** display tool, display the existing export file in readable format to create a temporary data set.
4. Use the **REPRO** command on the temporary data set to copy the data into the data set created in step 2.

Note: You can also cut the data from the temporary data set and paste it into the new data set.

5. Edit the new data set, and change the **auth.pubkey** and **sig.pubkey** data according to the key file. Also change the export and import node names to match exactly the names of your local and remote nodes.
6. Import the new data set as an export file into your parameter file using the procedure described in Importing STS Keys from a File.

Chapter 11. 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 Key Management Help
-----+-----
2 1. New
   2. Open
   *. Close
   4. Info...
   *. Rekey
   *. Save Active
   7. Save as...
   *. Unload
   9. Exit
-----+-----
Secure+ Admin Tool: Main Screen
                                     Scroll CSR

Table Line Commands are:
H View History           D Delete node
I Insert node

Secure
-----+-----
LC Node Name      Type  123C  Override  Encryption  Signature  ExtAuth  Autoupd
-----+-----
.CLIENT           R     NNNN   Y         N           N           N         N
.EASERVER         R     N*YN   N         N           N           N         N
SC.OKC.PARIS1    L     NNNN   Y         N           N           N         N
SC.REMOTE01      R     NNYN   Y         N           N           N         N
SC.REMOTE02      R     NYNN   Y         N           N           N         N
SC.REMOTE03      R     NYNY   Y         N           N           N         N
***** 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 qualifiers 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 4.

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, SSL, or STS).
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=TLS|SSL|STS** in the PROCESS statement.
9. After you valid and test your connections by session, save the parameter files and restart Sterling Connect:Direct.

Chapter 12. 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 STS keys and algorithms or 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 Statment 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, TLS, or STS) 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 4.

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

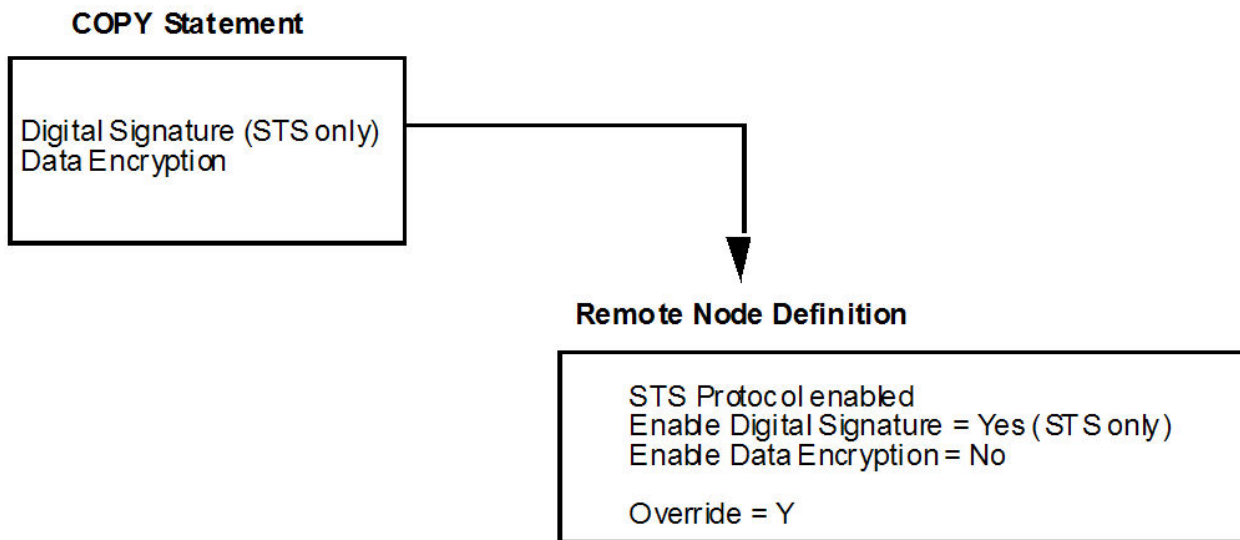
```
SECURE=OFF|STS|SSL|TLS  
or  
SECURE=ENCRYPT.DATA=Y|N  
or  
SECURE = (OFF | SSL | TLS | STS, ENCRYPT.DATA=Y|N)  
or  
SECURE = (OFF | SSL | TLS | STS,<cipher_suite>|(cipher_suite_list),ENCRYPT.DATA=Y|N)
```

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 digital signatures (in the case of an STS environment) or encryption, the **PNODE** cannot turn those options off using the **COPY** statement override.

The following illustration shows how the **COPY** statement overrides the security functions set in a remote node record:



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
```

In an STS environment, you can also specify the algorithm to use for encryption and whether to enable digital signatures, as the following syntax example shows:

```
SECURE = (ENCRYPT.DATA=Y|N|algorithm name,SIGNATURE=Y|N)  
or  
SECURE = ENC=Y|N|algorithm name,SIG=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:

```
SSL0FF 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:

```
SSL0N 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.

Sterling Connect:Direct Secure Plus Settings STS Protocol Override

The business partners agreed by default all sessions are none-secure and chose STS as the default protocol when secure transfers are required. Both partners specified the following configuration in their Sterling Connect:Direct Secure Plus parameter files:

- Disabled the STS protocol in the remote node record
- Specified **OVERRIDE=Y** in both the Local and Remote Node records

To enable data encryption and digital signatures in the following example, **SAMPLE**, and override the default non-secure connection, they use the following COPY statement, which copies the data set **TEST.INPUT.DATASET** from the PNODE to the SNODE (**THE.OTHER.NODE**) and renames it to **TEST.OUTPUT.DATASET**.


```
SAMPLE PROCESS SNODE=THE.OTHER.NODE SECURE=STS
*
COPYFILE COPY FROM ( PNODE
                        DSN='TEST.INPUT.DATASET'
                        DISP=SHR
                    )
TO ( SNODE
     DSN='TEST.OUTPUT.DATASET'
     DISP=(NEW.CATLG)
   )
  SECURE=(ENC=Y,SIG=Y)
```


Chapter 13. 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 Key Management Help								
1	1. New							Row 1 of 6
	2. Open							Secure+ Admin Tool: Main Screen
	3. Close							Scroll CSR
	4. Info...							
	*. Rekey							Table Line Commands are:
	6. Save Active							H View History
	7. Save as...							D Delete node
	8. Unload							I Insert node
	9. Exit							
LC	Node Name	Type	123C	Override	Encryption	Signature	ExtAuth	Autoupd
	.CLIENT	R	NNNN	Y	N	N	N	N
	.EASERVER	R	N*YN	N	N	N	N	N
	SC.OKC.PARIS	L	NNNN	Y	N	N	N	N
	SC.REMOTE1	R	NNYN	Y	N	N	N	N
	SC.REMOTE2	R	NYNN	Y	N	N	N	N
	SC.REMOTE3	R	NYNY	Y	N	N	N	N
***** 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.PARMPFILE                               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 MVS.

LC Filename or Directory
S $CD.PARMPFILE
_ $CD.PARMPFILE.DATA
_ $CD.PARMPFILE.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.PARMFIL
|      | $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:CSPA000I	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

After you start the Secure+ Admin Tool, the main screen is displayed:

```

File Edit Key Management Help
-----
Q2A.ZOS.PARIS          Secure+ Admin Tool: Main Screen          Row 9 to 13 of 13
Option ===>                                                    Scroll CSR

                          Table Line Commands are:

E Export pub. key      H View History          D Delete node
U Update node          I Insert node

                          Secure
LC Node Name          Type 123C Override Encryption Signature ExtAuth Autoupd
-----
Q2A.ZOS.PARIS         L  NNNN  Y      N      N      N      N
Q3A.ZOS.PARIS         R  ***N  N      *      *      *      *
Q3B.ZOS.PARIS         R  ***N  N      *      *      *      *
SOL36SP               R  ***N  N      *      *      *      *
W2S.4200.CDWOPS8     R  ***N  N      *      *      *      *
***** BOTTOM OF DATA *****

```

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

- **E—Export** allows you to export the STS keys for the selected STS node only. For more information on exporting STS keys for all nodes or a single node, see *Exporting STS Keys (STS nodes only)*.
- **U—Update** allows you to perform the following functions:
 - Disabling Sterling Connect:Direct Secure Plus on an SSL or TLS Node (all nodes)
 - Changing the Cipher Suites (TLS or SSL nodes only)
 - Changing the Encryption Algorithm Names (STS nodes only)
- **H—History** lists the individual dates including the time the selected node was updated.
- **I—Insert** allows you to create a new remote node record. For more information, see *Inserting a Node*.
- **D—Delete** 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 **2** beside the **Enable SSL** and **Enable TLS** fields. Select **OK** and press **Enter**.
3. To reselect the same node, type **U** next to the node to update and press **Enter**. Select **STS Parameters** in the panel selection line and press **Enter**. Type **2** beside the **Enable STS** field.
4. Select **OK** and press **Enter**.
5. 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.

Disabling Sterling Connect:Direct Secure Plus on an STS Node

To disable Sterling Connect:Direct Secure Plus on an STS node:

Procedure

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

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.

0
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.

Changing the Encryption Algorithm Names

About this task

When you activate the STS protocol for a node, it uses algorithms to encrypt the data being transmitted. A common algorithm must exist on both endpoints of the transmission.

Sterling Connect:Direct Secure Plus searches the enabled algorithm list and locates the first algorithm that is common for communications at both nodes.

To enable algorithms for a node record:

Procedure

1. From the **Secure+ Admin Tool Main Screen**, type **U** next to the node to update.
The **Algorithm Names** field specifies the algorithms being used. They are listed from left to right in priority order.
2. Edit or rearrange the algorithm names by typing over the existing names.
3. Select **OK** and press **Enter**.
4. 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. If you are creating a node record for the SSL or TLS protocol, go to step 4 and proceed from there. If you are creating a node record for the STS protocol, go to step 4 and proceed from there.
4. After you finish the procedure and saved 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.

STS Key Modification

If you are using STS protocol with Sterling Connect:Direct Secure Plus, you periodically need to update and clear keys. This section provides the following procedures for modifying key files for Sterling Connect:Direct Secure Plus.

- Updating keys in node records configured for STS
- Resetting keys in node records configured for STS

Updating Keys in Node Records Configured for the STS Protocol

About this task

In order to maintain communications with a trading partner when you update your keys, you must maintain a copy of the previous keys until your trading partner receives the updated keys. You must perform this procedure for both the local node record and remote nodes that use the STS protocol.

To update your signature and authentication keys:

Procedure

1. From the **Secure+ Admin Tool Main Screen**, type **U** next to the node record name (local or remote) to update and press **Enter**.
2. From the **Secure+ Create/Update Panel - STS Parameters** panel select **Create Auth. Prev. Keys**.

Sterling Connect:Direct Secure Plus copies the current authentication keys to previous keys and assigns an expiration date of 30 days from the time that you generated the previous key value. Only the expiration date and time are displayed on the screen. The previous keys are stored internally.

3. To change the expiration date, position your cursor in the date field and change any of the information.
4. Select **Create Sig. Prev. Keys**.

Sterling Connect:Direct Secure Plus copies the current signature keys to previous keys and assigns an expiration date of 30 days from the time that you generated this previous key value. Only the expiration date and time are displayed on the screen. The previous keys are stored internally.

5. To change the expiration date, position your cursor in the date field and change any of the information.
6. Select **Create Auth. Pubkey** and press **Enter**.
7. On the **Generate Seed** screen, type **2** to select **Sample Value** and press **Enter**.
8. Change some of the text by typing over it. Press **PF3**.

When the **Secure+ Create/Update Panel** displays the message *Seed generation complete*, your public key for strong authentication is created.

9. Select **Create Sig. Pubkey** and press **Enter**.
10. On the **Generate Seed** screen, type **2** to select **Sample Value** and press **Enter**.
11. Change the text by typing over it. Changing the text creates a secure key value. Press **PF3**.

When the **Secure+ Create/Update Panel** displays the message *Seed generation complete*, your public key for digital signatures is created.

12. Select **OK** and press **Enter**.
13. Save the Sterling Connect:Direct Secure Plus parameter file using the procedure in Sterling Connect:Direct Secure Plus Operation Enablement and Validation.

Resetting Keys in Remote Node Records Configured for STS

About this task

To reset the keys in remote node records to default to the settings in the local node record.

Procedure

1. From the **Secure+ Admin Tool Main Screen**, type **U** next to the node to update and press **Enter**.
2. From the **Secure+ Create/Update Panel - STS Parameters**, select **Reset Auth. Pubkey** and press **Enter**.

This step resets the public key used for strong authentication to the default value in the local node record.

3. From the **Secure+ Create/Update Panel - STS Parameters**, select **Reset Sig. Pubkey** and press **Enter**.

This step resets the public key used for the digital signature to the default value in the local node record.

Chapter 14. 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

```



```

=====
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 => 1                     Comp Code  => 00000000
                                           Comp Msg   => SSPA001I

Userid      => $CD
Primary     => CD.OS390.V40000        Step Name  =>
Submitted DSN=> $CD.CD.PROCESS(SUB1)
-----

```

```

-----
Function    => COPY                  Start Time => 10:26:35
Process Name => STATSAMP              Stop Time  => 10:26:39
Process Num => 338                   Comp Code  => 00000000
                                           Comp Msg   => SCPA000I

Userid      => $CD
Secondary   => SC.OS390.V40000        Step Name  => COPYFIL1
-----

```

```

From ( Pnode
Dsn=$CD.SECURE.TESTFILE)
    recs => 0                        blkS => 157
    I/O BYTES => 5,000,000
    VTAM BYTES => 5,000,314
    Cmpr Perc => 0.0%
Digital Signature enabled = Yes
    VOL=SER=> USER05
To ( Snode
Dsn=$CD.SECURE.RESTART.OUT1)
    recs => 0                        blkS => 157
    I/O BYTES => 5,000,000
    VTAM BYTES => 5,000,314
    Cmpr Perc => 0.0%
Digital Signature enabled = No
Merged Signature enabled = Yes
Merged Encryption enabled = No
Verified Signature = Curr
    VOL=SER=> USER02

```

The following fields are included for the Sterling Connect:Direct Secure Plus for z/OS statistics for the copy function:

Field	Description	Valid Values
Digital Signature enabled	Specifies whether digital signature are enabled in the Sterling Connect:Direct Secure Plus parameter file. This information is displayed in the statidtics separately for the PNODE and SNODE.	Yes No
Merged Signature enabled	Specifies the resulting value of the merge between the PNODE and the SNODE Sterling Connect:Direct Secure Plus parameter files and the COPY statement parameters for digital signature.	Yes No
Merged Encryption enabled	Specifies the resulting value of the merge between the PNODE and the SNODE Sterling Connect:Direct Secure Plus parameter files and the COPY statement parameters for data encryption.	Algorithm ID No
Verified Signature	Specifies whether the current or previous key verified the digital signature of digital signature is enabled for the session. This information is displayed only if the merged signature value is Yes .	Curr Prev

STS Extended Option Statistics Records

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

Note: You must type * in the **RECORD** field of the **Select Statistics Extended Options** screen to ensure that the complete information is displayed.

A description of the fields follows the samples.

```
=====
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 => 10:26:35
                                           Start Date => 05/04/2003

Process Name => STATSAMP
Process Num => 338                    Comp Code  => 00000000
                                           Comp Msg   => SVTM055I

Userid      => $CD
Primary Node => CD.OS390.V40000
Secondary Node CD.OS390.V40000        ALT.NODE => CD.DALLAS.OFFICE
Submitter Node CD.OS390.V40000

Pnode Signature Enabled = No
Snode Signature Enabled = No
Merged Signature Enabled = No
Pnode Encrypt.Data Algorithms...
IDEACBC128
TDESCBC112
DESCBC56
Snode Encrypt.Data Algorithms...
IDEACBC128
TDESCBC112
DESCBC56
System Data Encryption = IDEACBC128
-----
```

```
-----
Function    => COPY STEP START        Time       => 10:26:35
Process Name => STATSAMP              Process Num => 338
Primary Node => CD.OS390.V40000      Secondary Node => SC.OS390.V40000

Pnode Signature Enabled = No
Snode Signature Enabled = No
Merged Signature Enabled = No
Pnode Encryption Enabled = No
Snode Encryption Enabled = No
Encryption Enabled = No
-----
```

```
-----
Function    => COPY                    Start Time => 10:26:35
Process Name => STATSAMP              Stop Time  => 10:26:39
Process Num => 338                    Comp Code  => 00000000
                                           Comp Msg   => SCPA000I

Userid      => $CD
Secondary   => SC.OS390.V40000        Step Name  => COPYFIL1
-----
```

```

From ( Pnode
Dsn=$CD.SECURE.TESTFILE)
    recs => 0                               blks => 157
    I/O BYTES => 5,000,000
    VTAM BYTES => 5,000,314
    Cmpr Perc => 0.0%
Digital Signature enabled = Yes
    VOL=SER=> USER05
To ( Snode
Dsn=$CD.SECURE.RESTART.OUT1)
    recs => 0                               blks => 157
    TYPE => LRGSAM
    I/O BYTES => 5,000,000
    VTAM BYTES => 5,000,314
    Cmpr Perc => 0.0%
Digital Signature enabled = No
Merged Signature enabled = Yes
Merged Encryption enabled = No
Verified Signature = Curr
    VOL=SER=> USER02

```

Session Begin (SB) Record

The following fields are included for the Sterling Connect:Direct extended option statistics in the Session Begin record:

Field	Description	Valid Values
Pnode Signature Enabled	Specifies whether digital signatures are enabled in the Sterling Connect:Direct Secure Plus parameter file of the PNODE.	Yes No
Snode Signature Enabled	Specifies whether digital signatures are enabled in the Sterling Connect:Direct Secure Plus parameter file of the SNODE.	Yes No
Merged Signature Enabled	Specifies the resulting value of the merge between the PNODE and SNODE Sterling Connect:Direct Secure Plus parameter files for digital signature.	Yes No
Pnode Encrypt.Data Algorithms	Specifies the available encryption algorithms of the PNODE. The algorithms are displayed in the priority order set by the Sterling Connect:Direct Secure Plus administrator of the PNODE.	Algorithm ID List
Snode Encrypt.Data Algorithms	Specifies the available encryption algorithms of the SNODE. The algorithms are displayed in the priority order set by the Sterling Connect:Direct Secure Plus administrator of the SNODE.	Algorithm ID List
System Data Encryption	Specifies the algorithm used for encrypting Sterling Connect:Direct control blocks during security-enabled transfers.	Algorithm ID

Copy Step Start (CI) Record

The following fields are included for the Sterling Connect:Direct extended option statistics in the Copy Step Start record shown in STS Extended Option Statistics Records.

Field	Description	Valid Values
Pnode Signature Enabled	Specifies whether digital signature is enabled in the Sterling Connect:Direct Secure Plus parameter file of the PNODE.	Yes No
Snode Signature Enabled	Specifies whether digital signature is enabled in the Sterling Connect:Direct Secure Plus parameter file of the SNODE.	Yes No
Merged Signature Enabled	Specifies the resulting value of the merge between the PNODE and SNODE Sterling Connect:Direct Secure Plus parameter files for digital signature.	Yes No
Pnode Encryption Enabled	Specifies whether data encryption is enabled in the Sterling Connect:Direct Secure Plus parameter file of the PNODE.	Yes No
Snode Encryption Enabled	Specifies whether data encryption is enabled in the Sterling Connect:Direct Secure Plus parameter file of the SNODE.	Yes No
Encryption Enabled	Specifies the resulting value of the merge between the PNODE and SNODE Sterling Connect:Direct Secure Plus parameter files for data encryption.	Algorithm ID No

Copy Termination (CT) Record

The following fields are included for the Sterling Connect:Direct extended option statistics in the Copy Termination record as shown in STS Extended Option Statistics Records.

Field	Description	Valid Values
Digital Signature enabled	Specifies whether digital signatures are enabled in the Sterling Connect:Direct Secure Plus parameter file. This information is displayed in the statistics separately for the PNODE and the SNODE.	Yes No
Merged Signature enabled	Specifies the resulting value of the merge between the PNODE and SNODE Sterling Connect:Direct Secure Plus parameter files <i>and</i> the COPY statement parameters for digital signature.	Yes No
Merged Encryption enabled	Specifies the resulting value of the merge between the PNODE and SNODE Sterling Connect:Direct Secure Plus parameter files <i>and</i> the COPY statement parameters for data encryption.	Algorithm ID No
Verified Signature	Specifies whether the current or previous key verified the digital signature if digital signature is enabled for the session. This information is displayed only if the merged signature value is Yes .	Curr Prev

Chapter 15. 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: <ul style="list-style-type: none"> • 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
<p>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.</p> <p>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.</p>	<p>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.</p>	<p>Take the appropriate action to generate or obtain a new certificate.</p>
<p>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.</p> <p>Note: A message will not contain the node name if the certificate did not have one associated with it.</p>	<p>The warning message will appear based on the validation check controlled by the following initialization parameters, CHECK.CERT.EXPIRE.</p>	<p>Take the appropriate action to generate or obtain a new certificate.</p>
<p>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.</p> <p>Note: A message will not contain the node name if the certificate did not have one associated with it.</p>	<p>The most likely cause of this is the certificate does not exist in the Key database or Key ring.</p>	<p>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.</p>
<p>The following message is received when an SSL or TLS Process is run:</p> <p>SSL or TLS handshake failure, reason=GSK_ERROR_SOCKET_CLOSED.</p>	<p>The trading partners have not enabled a matching cipher suite.</p>	<p>Update the remote node record for the trading partner to enable a cipher suite recognized by the trading partner and resubmit the Process.</p>
<p>The following message is received:</p> <p>CSPA202E SSL handshake failure, reason=GSK_ERROR_BAD_CERTIFICATE.</p>	<p>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.</p> <p>This error is common if you use self-signed certificates because the remote Sterling Connect:Direct system does not have the CA certificate.</p>	<p>Verify that each trading partner can validate the certificates of other trading partners and resubmit the Process.</p> <p>Ensure that the remote node record for the trading partner has enabled the correct protocol.</p>

Problem	Possible Cause	Solution
<p>The following error is received from the SNODE:</p> <p>CSPA202E SSL or TLS handshake failure, reason= GSK_ERROR_UNKNOWN_ERROR.</p>	<p>A conflict within the IBM System SSL toolkit occurred because a certificate being processed did not use version 3 of the toolkit.</p>	<p>Ensure that all certificates and CA certificates are using version 3.</p>
<p>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.</p>	<p>The Sterling Connect:Direct network maps do not contain entries for the PNODE and SNODE.</p> <p>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.</p>	<p>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.</p>
<p>Sterling Connect:Direct Secure Plus parameters specified from the copy statement cause the copy step to fail with message CSPA077E.</p>	<p>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.</p>	<p>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.</p>
<p>An error occurs in ESTAE with a bad return code (RC=3) when running a Process with a remote node and the Process fails.</p>	<p>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.</p>	<p>Verify that the remote node definitions on both sites accurately state the Sterling Connect:Direct Secure Plus Export information.</p>
<p>Running a Process with a remote node fails with an authentication error.</p>	<p>Unique public/private key pairs are generated for the remote node record and the local node record is set to OVERRIDE=N.</p>	<p>Change the local node record to OVERRIDE=Y or do not use unique public/private key pairs in the remote node record.</p>
<p>The Save Active option is not selectable.</p>	<p>You can only use the Save Active function once each time you open the Sterling Connect:Direct Secure Plus parameter file.</p>	<p>Reopen the Sterling Connect:Direct Secure Plus parameter file to use the Save Active function or use the Save As function.</p>
<p>The text entry fields on the Create/Update panel of the Secure+ Admin Tool are not visible.</p>	<p>The CUA attributes in your ISPF profile are not set correctly.</p>	<p>Change the value for Normal Text entry in the CUA attributes of the ISPF profile to uscore in the Highlight column.</p>
<p>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.</p>	<p>The algorithm name used in the COPY statement is not in the supported algorithm list for both nodes.</p>	<p>Verify that the algorithm name in the copy statement is in the supported algorithm list for both nodes.</p>

Problem	Possible Cause	Solution
<p>A Process including a COPY statement with a SECURE parameter was submitted and failed. The following CSPA011E error message is displayed:</p> <p>Illegal attempt to override Sterling Connect:Direct Secure Plus parameters</p>	<p>You attempted to use the SECURE parameter in a COPY statement for the STS protocol but did not specify OVERRIDE=Y in the remote node record to enable the security override feature.</p>	<p>Take one of the following actions:</p> <ul style="list-style-type: none"> 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. <p>See Override Settings in Sterling Connect:Direct Processes.</p>
<p>An SSL or TLS session was attempted with a Sterling Connect:Direct system that does not implement SSL or TLS.</p>	<p>The trading partner does not have the protocol enabled.</p>	<p>Request that the trading partner configure its node for the correct protocol or disable Sterling Connect:Direct Secure Plus for the node.</p>
<p>Either the CSPA203E error message or the CSPA204E message is displayed:</p> <p>SSL or TLS send failure, rc=&RC, rsn=&RSN or</p> <p>SSL or TLS receive failure, rc=&RC, rsn=&RSN.</p>	<p>The client cannot validate the server's certificate.</p>	<p>Ensure that client authentication is turned on and certificate information is defined in the remote node record.</p>
<p>The following CSPA205E error message is displayed: SSL or TLS support requires the TCP/IP protocol.</p>	<p>One of the trading partners is not using TCP/IP for communications.</p>	<p>Determine which trading partner does not have TCP/IP enabled and change the configuration of that trading partner.</p>
<p>The following CSPA200E error message is displayed: Sterling Connect:Direct Secure Plus version mismatch.</p>	<p>You are attempting to use the SSL or TLS protocol to securely communicate with a trading partner that does not have the protocol enabled.</p>	<p>Change the configuration of the remote node record to enable the correct protocol.</p>
<p>The following CSPA206E error message is displayed: Remote certificate is invalid.</p>	<p>The root certificate was not found.</p>	<p>Check the parameter file configuration and ensure that the correct certificate is identified in the remote node record.</p>
<p>The following CSPA207E error message is displayed: Root certificate not found.</p>	<p>The remote certificate could not be validated.</p>	<p>Check the parameter file configuration and ensure the correct key database file is identified in the remote node record.</p>
<p>The following SITA1901 error message is displayed: Sec+ Init failed. Secure=No. Override=No.</p>	<p>The local node record has all Sterling Connect:Direct Secure Plus protocols disabled and has override set to no.</p>	<p>Either enable the appropriate protocol in the remote node record or enable override=yes in the local node record.</p>

Problem	Possible Cause	Solution
<p>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.</p>	<p>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.</p>	<p>Take one of the following actions:</p> <ul style="list-style-type: none"> • 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. <p>See Override Settings in Sterling Connect:Direct Processes.</p>
<p>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.</p>	<p>You attempted to use the SECURE parameter in a PROCESS statement but did not include an equal sign after the SECURE keyword.</p>	<p>Correct the PROCESS statement syntax by inserting an equal sign and resubmit the Process.</p>
<p>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.</p>	<p>You attempted to use the SECURE parameter in a PROCESS statement but the syntax was faulty.</p>	<p>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 <i>Sterling Connect:Direct Process Language Reference Guide</i>.</p>
<p>System initialization failed, and the following SITA196E error message is displayed: FIPS Mode Requested but SECURE.DSN parameter is not specified.</p>	<p>You specified the FIPS initialization parameter as YES, but you did not specify the SECURE.DSN parameter to enable Sterling Connect:Direct Secure Plus.</p>	<p>Update the initialization parameters and restart IBM Sterling Connect:Direct.</p>
<p>System initialization failed, and the following error message is displayed: Connect;Direct FIPS keyword requires z/OS release 1.11 or later.</p>	<p>Your current, active z/OS release level does not support FIPS mode for System SSL.</p>	<p>Either update the FIPS initialization parameter to NO or execute Sterling Connect:Direct on the appropriate release level of z/OS.</p>
<p>Sterling Connect:Direct was terminated, and the following error message is displayed: Secure+ Severe FIPS Mode Error, &var1.</p>	<p>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:</p> <ul style="list-style-type: none"> • KEY database (not FIPS-mode) • Random number generation failure • RSA or DSA keypair generation failure • gsk_perform_kat API failure 	<p>Contact IBM Support or correct the error and restart Sterling Connect:Direct.</p>

Chapter 16. Certificate Parameter Definitions

This topic describes the certificate parameter definitions for certificates created by the RACF application, GSKKYMANT 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.	<p>HANDSHAKE (Required): Indicates that digital signature and key encipherment are enabled.</p> <p>DOCSIGN (Optional): Indicates that non-repudiation is enabled.</p> <p>DATAENCRYPT (Optional): Indicates that data encipherment is enabled.</p> <p>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.</p>
X.509 Subject's Distinguished Name Issuer's Name	<p>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.</p> <p>Note: Self-signed certificates display the same information in the Issuer Name and Subject Name parameters.</p>	<p>The following fields, which must be enclosed in single quotes, are attributes of the Issuer's Name parameter and the Subject's Name parameter:</p> <p>CN=Common Name of the certificate in single quotes, for example, 'RACF SELF SIGN COMMON'</p> <p>T='Title of person creating certificate'</p> <p>OU='Organizational Unit associated with the person creating the certificate'</p> <p>O='Organization for which the certificate is being created'</p> <p>L='Locality (city) of the entity for which the certificate is created'</p> <p>SP='State/Province of the locality'</p> <p>C='Country of the locality'</p>
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.	1024
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

GSSKYMANT Utility Certificate Parameter Definitions

This table describes the minimum parameter definitions required for Sterling Connect:Direct Secure Plus for z/OS. Consult the GSKKYMANT 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.

GSSKYMANT 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

GSKKMAN 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.	rsaEncryption
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.	1024
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.	<p>The following fields, which must be enclosed in single quotes, are attributes of the Issuer's Name parameter and the Subject's Name parameter:</p> <p>CN=Common Name of the certificate in single quotes, for example, 'RACF SELF SIGN COMMON'</p> <p>T='Title of person creating certificate'</p> <p>OU='Organizational Unit associated with the person creating the certificate'</p> <p>O='Organization for which the certificate is being created'</p> <p>L='Locality (city) of the entity for which the certificate is created'</p> <p>SP='State/Province of the locality'</p> <p>C='Country of the locality'</p>
Size	Specifies the size of the private encryption key in bits.	1024
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.	<p>HANDSHAKE (Required): Indicates that digital signature and key encipherment are enabled.</p> <p>DOCSIGN (Optional): Indicates that non-repudiation is enabled.</p> <p>DATAENCRYPT (Optional): Enables the certificate to be used to.</p> <p>CERTSIGN: Indicates the certificate can sign other digital certificates and CRLs.</p> <p>Note: Do not specify CERTSIGN. Only Certificate Authority (Issuer) certificates should have keyCertSign and cRLSign indicators.</p>

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.	1024
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 17. 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 4 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 4.	Yes ____ No ____
SSL protocol enabled:	Yes ____ No ____
STS protocol enabled:	Yes ____ No ____
Configured Security Functions	
Override enabled:	Yes ____
Encryption enabled:	Yes ____ No ____
Autoupd enabled: Applies only to STS	Yes ____
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 4.	_____ 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 4.	_____ Valid only for SSL or TLS
Password: Valid only for certificates created in a gskkyman database; leave blank for key rings.	_____

Local Node Name: _____	
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 <i>IBM Sterling Connect:Direct for z/OS Release Notes</i> for a list of valid FIPS-mode ciphers.	_____
Enable Digital Signatures: Applies only to STS	Yes ____ No ____
Create Public Auth and Sig Key: Applies to all protocols	Yes ____ No ____
Algorithm Names: Applies only to STS	_____
Algorithms Enabled Applies only to STS	__ DES __ TDES __ IDEA
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 ____
STS protocol enabled	Yes ____ No ____
Enable Override: When override is enabled in a remote node record, <ul style="list-style-type: none"> • Values in the COPY statement override values in the remote node record that uses the STS protocol • Values in the PROCESS statement override values in the remote node record that uses any 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 ____
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)

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.	
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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.	_____
STS Protocol Functions	
If you enabled the STS protocol, set one or more of the following functions:	
Enable Digital Signatures:	Yes ____ No ____
Enable Public Key Auto Updates:	Yes ____ No ____
Note: If the trading partner uses an earlier version of Sterling Connect:Direct Secure Plus, you need identify the version of Sterling Connect:Direct Secure Plus the partner is using.	
Algorithm Names:	_____
Algorithms Enabled:	__ DES __ TDES __ IDEA

.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 ____

Remote Node Name:	.CLIENT (Required)
Note: The node name must be defined as .CLIENT to allow secure connections.	
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 ____

Chapter 18. Test Sterling Connect:Direct Secure Plus with the STS Protocol

This topic describes the steps for testing Sterling Connect:Direct Secure Plus with the STS protocol. To test an STS configuration and verify that Sterling Connect:Direct Secure Plus is working as intended, you must install and set up Sterling Connect:Direct and Sterling Connect:Direct Secure Plus on two different nodes. You can define two new test nodes as described in the following procedures (Node A and Node B) or you can use two existing nodes. Each node must be defined in the partner's Sterling Connect:Direct network map. These existing nodes can be two nodes within your enterprise or you can coordinate testing with a trading partner.

For the initial setup and testing, define *only* the minimum required fields for both nodes as described in the procedures in this section. Specific settings are provided to create nodes to test.

STS Protocol Test Procedure Overview

The following list summarizes the order of the tasks necessary to test Sterling Connect:Direct Secure Plus with the STS protocol.

1. Define Sterling Connect:Direct Secure Plus for Node A
 - a. Create the Sterling Connect:Direct Secure Plus local node record and keys
 - b. Create the Sterling Connect:Direct Secure Plus remote node record (Node B) and keys
 - c. Export the public keys of Node A for Node B
 - d. Save the parameter file
2. Define Sterling Connect:Direct Secure Plus for Node B
 - a. Create the Sterling Connect:Direct Secure Plus local node record and keys
 - b. Create the Sterling Connect:Direct Secure Plus remote node record (Node A) and keys
 - c. Export the public keys of Node B for Node A
 - d. Import the public keys from Node A to Node B
 - e. Save the parameter file
3. Import public keys from Node B to Node A
4. Save the parameter file for Node A
5. Update Sterling Connect:Direct network maps for Node A and Node B
6. Add the **SECURE.DSN=filename** parameter to the Sterling Connect:Direct for z/OS initialization parameter file of Node A and Node B (where filename is the name of the Sterling Connect:Direct Secure Plus parameter file for that node)
7. Restart Sterling Connect:Direct (Node A and Node B)
8. Verify that Sterling Connect:Direct Secure Plus is enabled (Node A and Node B)
9. Exchange data and compare results
 - a. Send data from Node A to Node B
 - b. Review statistics records for transaction

Accessing the Admin Tool

Before you begin

Use the **Secure+ Admin Tool** to set up Sterling Connect:Direct Secure Plus to test an STS installation.

To access the Admin tool, from the **Connect:Direct Administrative Options Menu**, type **SA** and press **Enter**.

Definition Creation for Sterling Connect:Direct Secure Plus for Node A

Defining Sterling Connect:Direct Secure Plus for Node A involves:

- Creating the Sterling Connect:Direct Secure Plus local node record and generating the public keys
- Creating the Sterling Connect:Direct Secure Plus remote node record and generating the public keys
- Exporting the public keys of Node A
- Saving the parameter file

Creating the Sterling Connect:Direct Secure Plus Local Node Record and Keys for Node A

To create the local node record:

Procedure

1. From the **Secure+ Admin Tool: Main Screen**, select **Edit** and press **Enter**.
2. Type **1** to select **Create/Update Record** and press **Enter** to display the **Node Identification** panel.

Secure+ Create/Update Panel - Node Identification		
Option:		
EA Parameters	SSL/TLS Parameters	STS Parameters
Node NODEA	1 1. Local 2. Remote	
Alias Names:	TCP Information: IPaddr: Port:	
Import Remote Keys	Get Record	OK Cancel

3. To define values for Node A:
 - a. Select each of the panels listed in the following table.
 - b. Type the sample values in the fields listed for each panel.Fields that are either not valid for the STS protocol or for the type of record being configured are identified and should be left blank.

Panel	Field	Value
Node Identification	Node	Name of Node A (NODEA for this example)
	Local/Remote	Local (1)
	TCP Information	Not valid for local node
	Alias Names	Not valid for local node
STS Parameters	Auth Timeout	90
	Autoupdt	No (2)
	Override	Yes (1)
	Enable STS	Yes (1)
	Signature	Yes (1)
	Encrypt	Yes (1)
	Algorithm	* to provide access to all available algorithms defined in the local node record
EA Parameters	Enable Auth	No (2)
SSL/TLS Parameters	Enable SSL	No (2)
	Enable TLS	No (2)
	Client Auth	No (2)

4. When you finish setting the sample values, select **STS Parameters** and press **Enter**.
5. Generate the authentication key for the STS protocol:
 - a. Select **Create / Reset Auth. Pubkey** and press **Enter** to display the **Generate Seed** screen.

Secure+ Admin Tool: Generate Seed	
2 1. Specify Value	Specify the seed value by typing it into the text field.
2. Sample Value	Generate a seed by processing text entered from the keyboard.
Random Number Seed:	

- b. Press **Enter** to accept the default value (**2 - Sample Value**).
- c. On the **Command Prompt** screen, select **OK** and press **Enter**.
- d. When the following screen is displayed, if the message *This is Loop 2 of 10* is displayed, type over data on any line and press **PF3** up to 10 times. This step is only necessary the first time you generate keys within the Secure+ Admin Tool for each parameter file. Repeating the process increases the randomness of keys.
- e. Press **PF3** to save the information.

```

File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT          SYS06254.T160411.RA000.SSCHR1.R0207298          Columns 00001 00072
Command ==>                               Scroll ==> PAGE
024: This process cannot proceed if the data in the edit file is unchanged.
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 262144
000002
000003 134217728
000004
000005 32
000006
000007 4
000008
000009 8589934592
000010
000011 131072
000012
000013 8388608
000014
000015 2097152
000016
000017 1073741824

```

- f. When the **Pass Phrase Generation** panel is displayed, type a string at least 32 characters long containing at least one uppercase character, one lowercase character, and one numeric value and press **Enter**.

Note: You do not need to remember this number.

When the **Secure+ Create/Update Panel** displays the message *Seed generation complete*, your public key for strong authentication is created, as illustrated in the following sample.

```

Secure+ Create/Update Panel - Node Identification
Option:
EA Parameters          SSL/TLS Parameters      STS Parameters
Node
NODEB                  1 1. Local
                      2. Remote
Alias
Names:                 TCP Information:
                      IPaddr:
                      Port:

Import Remote Keys    Get Record           OK           Cancel

```

- 6. Select **Create Sig. Pubkey** and press **Enter**.
- 7. Press **Enter** to accept the default value (2 - **Sample Value**).
When the message *Seed generation complete* is displayed on the **Secure+ Create/Update Panel**, your public key for digital signature is created.
- 8. Select **OK** and press **Enter**. The node field clears.

Creating the Sterling Connect:Direct Secure Plus Remote Node Record and Keys for Node B

To create the remote node record:

Procedure

1. From the **Secure+ Admin Tool: Main Screen**, select **Edit** and press **Enter**.
2. Type **1** to select **Create/Update Record** and press **Enter** to display the **Node Identification** panel.

Secure+ Create/Update Panel - Node Identification			
Option:			
EA Parameters	SSL/TLS Parameters	STS Parameters	
Node NODEB	1 1. Local 2. Remote		
Alias Names:	TCP Information: IPaddr: Port:		
<input type="button" value="Import Remote Keys"/> <input type="button" value="Get Record"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>			

3. Select each of the panels listed in the following table and type the sample values in the fields listed for each panel. Fields that are either not valid for the STS protocol or for the type of record being configured should be left blank.

Panel	Field	Value
Node Identification	Node	Name of Node B (NODEB for this example)
	Local/Remote	Remote (2)
	TCP Information	Leave blank because Sterling Connect:Direct gets IP address information from the network map
	Alias Names	Leave blank
STS Parameters	Auth Timeout	90
	Autoupdt	Default to local (3)
	Override	Default to local (3)
	Enable STS	Default to local (3)
	Signature	Default to local (3)
	Encrypt	Default to local (3)
	Algorithm	* to provide access to all available algorithms defined in the local node record
EA Parameters	Enable Auth	Default to local (3)
SSL/TLS Parameters	Enable SSL	No (2)
	Enable TLS	No (2)
	Client Auth	No (2)

4. Select **STS Parameters** and press **Enter** when you finish setting these values.
5. Generate the authentication key for the STS protocol:
 - a. Select **Create / Reset Auth. Pubkey** and press **Enter**.

```
Secure+ Admin Tool: Generate Seed

2 1. Specify Value      Specify the seed value by typing it
                           into the text field.
   2. Sample Value     Generate a seed by processing text
                           entered from the keyboard.

Random Number
Seed:
```

- b. Press **Enter** to accept the default value (**2 - Sample Value**).
- c. On the **Command Prompt** screen, select **OK** and press **Enter**.
- d. When the following panel is displayed, if the message *This is Loop 2 of 10* is displayed, type over data on any line and press **PF3** up to 10 times. This step is only necessary the first time you generate keys within the Secure+ Admin Tool for each parameter file. Repeating the process increases the randomness of keys.
- e. Press **PF3** to save the information.

```
File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT      SYS06254.T160411.RA000.SSCHR1.R0207298      Columns 00001 00072
Command ==>                                     Scroll ==> PAGE
024: This process cannot proceed if the data in the edit file is unchanged.
==MSG> -Warning- The UNDO command is not available until you change
==MSG>          your edit profile using the command RECOVERY ON.
000001 262144
000002
000003 134217728
000004
000005 32
000006
000007 4
000008
000009 8589934592
000010
000011 131072
000012
000013 8388608
000014
000015 2097152
000016
000017 1073741824
```

- f. When the **Pass Phrase Generation** panel is displayed, type a string at least 32 characters long containing at least one uppercase character, one lowercase character, and one numeric value and press **Enter**.

Note: You do not need to remember this number.

When the **Secure+ Create/Update Panel** displays the message *Seed generation complete*, your public key for strong authentication is created.

6. Select **Create Sig. Pubkey** and press **Enter**.

7. On the **Generate Seed** screen, press **Enter** to accept the default value (**2 - Sample Value**).
8. Change some of the text by typing over it and press **PF3**.
On the **Secure+ Create/Update Panel**, the message *Seed generation complete* is displayed when your public key for digital signature is created.
9. Select **OK** and press **Enter**.
10. Select **Cancel** and press **Enter** to return to the **Secure+ Admin Tool: Main Screen** and display the two node records you defined.

```

File Edit Key Management Help
-----
                                Row 1 of 2
Option ==>          Secure+ Admin Tool: Main Screen          Scroll CSR

                                Table Line Commands are:
E Export pub. key      H View History          D Delete node
U Update node          I Insert node

                                Secure
LC Node Name          Type 123C Override Encryption Signature ExtAuth Autoupd
-----
NODEA                  L   YNNN   Y      Y      Y      N      N
NODEB                  R   *NNN   *      *      *      *      *
***** BOTTOM OF DATA *****

```

Exporting Node A's Public Keys

To export the local node authentication and digital signature public key values to the remote node you are testing with:

Procedure

1. From the **Secure+ Admin Tool: Main Screen**, select **Key Management** and press **Enter**.
2. Type **2** to select **Export Public Keys** and press **Enter**.

Note: If warning messages are displayed, read them. Press **PF3** to continue.

```

                                Secure+ Admin Tool: File Selection

                                Enter file name for: INPUT SECURE PARM FILE

File
Name: $CD.SECURE.EXPORT                                Browse

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

```

3. Press **Enter** to accept the default file name and MVS file system type.
4. Select **OK** and press **Enter**.
The **Secure+ Admin Tool: Main Screen** displays the message *Export Successful*.

Saving the Sterling Connect:Direct Secure Plus Parameter File for Node A

About this task

When you save the Sterling Connect:Direct Secure Plus parameter file you created for Node A, the access file is also created.

To save the parameter 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**.

Note: If warning messages are displayed, read them. Press **PF3** to continue.

The **File Selection** screen is displayed.

3. Press **Enter** to accept the default file name or type a file name of your choice.
4. Type your site-specific job card information, allocation information, STEPLIB DSNs, and Access file Dsname as in the following example, using the library names created in your installation.

Site-dependent
job card information



Site-dependent
Allocation information



Site-dependent
STEPLIB DSNs



Access file Dsname



```
Secure+ Admin Tool: "Save As" information
(Or press PF3/PF12 to cancel)

What do you want to do with the generated JCL?
_ 1. Browse 2. Edit 3. Submit Make Pass Phrase
   Job statement information. Verify before proceeding.

====> //$CDA JOB (ACCOUNT),NAME,MSGCLASS=,NOTIFY=$CD
====> /** SECOND JCL
====> /** THIRD JCL
====> /** FOURTH JCL

Mgmt. Class _____ Volume Serial _____
Sig. Class _____
Data Class _____

Product Load library information. Verify before proceeding.

====> /** FIRST STEPLIB
====> /** SECOND STEPLIB
====> /** THIRD STEPLIB
====> Access file Dsname (long names may need quotation)
      _____
```

5. Type **3** to select **Submit** and press **Enter** to save your parameter file.
6. After the job is submitted, a screen similar to the following is displayed:

```
JOB $CDA(JOB01111) SUBMITTED
***
```

7. Press **Enter** to return to the **Secure+ Admin Tool: Main Screen**.
8. Verify that you get a return code of **0** (zero). Research any return code other than zero to determine the cause of the error condition.
9. Press **PF3** to return to the **Connect:Direct Administrative Options Menu**.

Defintion Creation for Sterling Connect:Direct Secure Plus for Node B

Defining Sterling Connect:Direct Secure Plus for Node B involves:

- Creating the Sterling Connect:Direct Secure Plus local node record and generating the public keys
- Creating the Sterling Connect:Direct Secure Plus remote node record and generating the public keys
- Exporting the public keys of Node B
- Importing the public keys from Node A
- Saving the parameter file

Creating the Sterling Connect:Direct Secure Plus Local Node Record and Keys for Node B

About this task

At the second location you are using to test your setup of Sterling Connect:Direct Secure Plus, you must configure a local node record for Node B.

To configure Node B as the local node.

Procedure

1. Start the **Secure+ Admin Tool**.
2. From the **Secure+ Admin Tool: Main Screen**, select **Edit** and press **Enter**.
3. Type **1** to select Create/Update Record and press **Enter** to display the **Secure+ Create/Update Panel - Node Identification** panel.
4. Select each of the panels listed in the following table and type the sample values in the fields listed for each panel. Fields that are either not valid for the STS protocol or for the type of record being configured are identified and should be left blank.

Panel	Field	Value
Node Identification	Node	Name of Node B (NODEB for this example)
	Local/Remote	Local (1)
	TCP Information	Leave blank because Sterling Connect:Direct gets IP address information from the network map
	Alias Names	Leave blank
STS Parameters	Auth Timeout	90
	Autoupdt	No (2)
	Override	Yes (1)
	Enable STS	Yes (1)
	Signature	Yes (1)
	Encrypt	Yes (1)
	Algorithm	* to provide access to all available algorithms defined in the local node record
EA Parameters	Enable Auth	No (2)

Panel	Field	Value
SSL/TLS Parameters	Enable SSL	No (2)
	Enable TLS	No (2)
	Client Auth	No (2)

5. Select **Create Auth. Pubkey** and press **Enter**.
6. On the **Generate Seed** screen, press **Enter** to accept the default value (**2 - Sample Value**).
7. On the **Command Prompt** screen, select **OK** and press **Enter**.
8. When the message *This is Loop 2 of 10* is displayed, type over the data on any line and press **F3** up to 10 times. This is only necessary the first time you generate keys within the Secure+ Admin Tool for each parameter file, and it increases the randomness of your keys.
9. Press **F3** to save the changes.
10. When the **PassPhrase Generation** panel is displayed, type a 32-byte character string with uppercase, lowercase, numeric, and alphabetic characters. Press **Enter**.

Note: You do not need to remember this number.

When the message *Seed generation complete* is displayed on the **Secure+ Create/Update Panel**, your public key for authentication is created.

11. Select **Create Sig. Pubkey** and press **Enter**.
12. On the **Generate Seed** screen, press **Enter** to accept the default value (**2 - Sample Value**).
When the message *Seed generation complete* is displayed On the **Secure+ Create/Update Panel**, your public key for digital signature is created.
13. Select **OK** and press **Enter**. The node field clears.

Creating the Sterling Connect:Direct Secure Plus Remote Node Record and Keys for Node A

To configure a remote node record for Node A on Node B:

Procedure

1. From the **Secure+ Admin Tool: Main Screen**, select **Edit** and press **Enter**.
2. Type **1** to select **Create/Update Record** and press **Enter** to display the **Node Identification** panel.
3. Select each of the panels listed in the following table and type the sample values in the fields listed for each panel. Fields that are either not valid for the STS protocol or for the type of record being configured should be left blank.

Panel	Field	Value
Node Identification	Node	Name of Node A (NODEA for this example)
	Local/Remote	Remote (2)
	TCP Information	Leave blank because Sterling Connect:Direct gets IP address information from the network map
	Alias Names	Leave blank

Panel	Field	Value
STS Parameters	Auth Timeout	90
	Autoupdt	Default to local (3)
	Override	Default to local (3)
	Enable STS	Default to local (3)
	Signature	Default to local (3)
	Encrypt	Default to local (3)
	Algorithm	* to provide access to all available algorithms defined in the local node record
EA Parameters	Enable Auth	Default to local (3)
SSL/TLS Parameters	Enable SSL	No (2)
	Enable TLS	No (2)
	Client Auth	No (2)

4. Select **STS Parameters** and press **Enter** when you finish setting these values.
5. Select **Create Auth. Pubkey** and press **Enter**.
6. On the **Generate Seed** screen, press **Enter** to accept the default value (2 - **Sample Value**).
7. On the **Command Prompt** screen, select **OK** and press **Enter**.
8. When the message *This is Loop 2 of 10* is displayed, type over the data on any line and press **F3** up to 10 times. This is only necessary the first time you generate keys within the Secure+ Admin Tool for each parameter file, and it increases the randomness of your keys.
9. Press **F3** to save the changes.
10. When the **PassPhrase Generation** panel is displayed, type a 32-byte character string with uppercase, lowercase, numeric, and alphabetic characters. Press **Enter**.

Note: You do not need to remember this number.

When the message *Seed generation complete* is displayed on the **Secure+ Create/Update Panel**, your public key for authentication is created.

11. Select **Create Sig. Pubkey** and press **Enter**.
12. On the **Generate Seed** screen, press **Enter** to accept the default value (2 - **Sample Value**).
13. Change some of the text by typing over it. Press **PF3**.
On the **Secure+ Create/Update Panel**, the message *Seed generation complete* is displayed. Your public key for digital signatures is created.
14. Select **OK** and press **Enter**.
15. Select **Cancel** and press **Enter** to return to the **Secure+ Admin Tool: Main Screen**. Your screen should have two nodes populated, as shown in the following example.

```

File Edit Key Management Help
-----
Option ==>> Secure+ Admin Tool: Main Screen Row 1 of 2
                                                    Scroll CSR

Table Line Commands are:
E Export pub. key      H View History      D Delete node
U Update node         I Insert node

LC Node Name          Type  123C  Override Encryption Signature ExtAuth Autoupd
-----
NODEA                 R   *NNN   *      *      *      *      *
NODEB                 L   YNNN   Y      Y      Y      N      N
***** BOTTOM OF DATA *****

```

Exporting the Public Keys of Node B

To export the Node B public keys for Node A:

Procedure

1. From the **Secure+ Admin Tool: Main Screen**, select **Key Management** and press **Enter**.
2. Type **2** to select **Export Public Keys** and press **Enter**.

Note: If warning messages are displayed, read them. Press **PF3** to continue.

3. Press **Enter** to accept the default file name and MVS file system type.
On the **Secure+ Create/Update Panel**, the message *Export Successful* is displayed.

Importing the Public Keys from Node A

To import your authentication and digital signature public key values from the remote node you are testing with (Node A):

Procedure

1. From the **Secure+ Admin Tool: Main Screen**, select **Key Management** and press **Enter**.
2. Type **1** to select **Import Public Keys** and press **Enter**.
3. Type the file name prefix or partial prefix followed by an asterisk (*), select **Browse** and press **Enter**.
4. Type **S** next to the export file name with an extension for this node name (for example, \$CD.SECURE.EXPORT.#NODEB) and press **Enter**.

The message *2 entries imported from NODEA* is displayed on the **Secure+ Admin Tool: Main Screen**, indicating that both the authentication and the digital signature public keys have been imported.

5. Type **U** next to NODEA and press **Enter** to ensure that you now have keys for the remote (RMT).

Saving the Sterling Connect:Direct Secure Plus Parameter File for Node B

About this task

When you save the Sterling Connect:Direct Secure Plus parameter file you created for Node B, the access file is also created.

To save the parameter file for Node B:

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. Press **Enter** to accept the default file name.
4. Type your site-specific job card information, allocation information, STEPLIB DSNs, and Access file Dsname as in the following example, using the library names created in your installation.

```
Secure+ Admin Tool: "Save As" information
(Or press PF3/PF12 to cancel)

What do you want to do with the generated JCL?
- 1. Browse 2. Edit 3. Submit Make Pass Phrase
  Job statement information. Verify before proceeding.

=====> //SCDA JOB (ACCOUNT),NAME,MSGCLASS= ,NOTIFY=$CD
=====> /* SECOND JCL
=====> /* THIRD JCL
=====> /* FOURTH JCL

Mgmt. Class _____ Volume Serial _____
Sfg. Class _____
Data Class _____

Product Load library information. Verify before proceeding.

=====> /* FIRST STEPLIB
=====> /* SECOND STEPLIB
=====> /* THIRD STEPLIB
Access file Dsname (long names may need quotation)
=====> _____
```

5. Type **3** to select **Submit** and press **Enter** to save your parameter file.
6. After the job is submitted, a screen similar to the following is displayed:

```
JOB $CDA(JOB01111) SUBMITTED
***
```

7. Press **Enter** to return to the **Secure+ Admin Tool: Main Screen**.
8. Verify that you get a return code of **0** (zero). Research any return code other than zero to determine the cause of the error condition.
9. Press **PF3** to return to the **Connect:Direct Administrative Options Menu**.

Importing the Public Keys of Node B to Node A

To import the authentication and digital signature public keys from Node B:

Procedure

1. Start the **Secure+ Admin Tool**.
2. From the **Secure+ Admin Tool: Main Screen**, select **File** and press **Enter**.
3. Type **2** to select **Open** and press **Enter**.
4. Type the complete file name of the parameter file that you created for Node A and press **Enter**.
5. Select **Key Management** and press **Enter**.
6. Type **1** to select **Import Public Keys** and press **Enter**.
7. Type the file name prefix or partial prefix followed by an asterisk (*), select **Browse**, and press **Enter**.
8. Type **S** next to the export file name with an extension for this node name (for example, \$CD.SECURE.EXPORT.#NODEA) and press **Enter**.

The message *2 entries imported* from NODEB is displayed on the **Secure+ Admin Tool: Main Screen**, indicating that both the authentication and the digital signature public keys have been imported.

9. Type **U** next to NODEB and press **Enter** to ensure that you now have keys for the remote node record (RMT).

Saving the Sterling Connect:Direct Secure Plus Parameter File for Node A

To save the Node A parameter 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. Press **Enter** to accept the default file name.
4. Type your site-specific job card information, allocation information, STEPLIB DSNs, and Access file Dsname as in the following example, using the library names created in your installation.

Site-dependent
job card information

Site-dependent
Allocation information

Site-dependent
STEPLIB DSNs

Access file Dsname

```

Secure+ Admin Tool: "Save As" information
(Or press PF3/PF12 to cancel)

What do you want to do with the generated JCL?
_ 1. Browse 2. Edit 3. Submit Make Pass Phrase
Job statement information. Verify before proceeding.

=====> //SCDA JOB (ACCOUNT),NAME,MSGCLASS= ,NOTIFY=$CD
=====> /* SECOND JCL
=====> /* THIRD JCL
=====> /* FOURTH JCL

Mgmt. Class _____ Volume Serial _____
Sfg. Class _____
Data Class _____

Product Load library information. Verify before proceeding.

=====> /* FIRST STEPLIB
=====> /* SECOND STEPLIB
=====> /* THIRD STEPLIB
Access file Dsname (long names may need quotation)
=====> _____

```

5. Type 3 to select **Submit** and press **Enter** to save your parameter file.
6. After the job submits, a screen similar to the following is displayed:

```

JOB $CDA(JOB01111) SUBMITTED
***

```

7. Press **Enter** to return to the **Secure+ Admin Tool: Main Screen**.
8. Verify that you get a return code of 0 (zero). Research any return code other than zero to determine the cause of the error condition.
9. Press **PF3** to return to the **Connect:Direct Administrative Options Menu**.

Updating Sterling Connect:Direct Network Maps for Node A and Node B

About this task

If you used existing nodes for testing, this step is not necessary. If you created new test nodes (Node A and Node B), update Sterling Connect:Direct network maps (netmaps) that you created during the initial installation of Sterling Connect:Direct Secure Plus for z/OS.

To add these test nodes to the Sterling Connect:Direct network map:

Procedure

1. Update the network map of Node A to add Node B.
2. Update the network map of Node B to add Node A.

Note: Refer to the *IBM Sterling Connect:Direct for z/OS Administration Guide* for specific instructions for updating the Sterling Connect:Direct network map.

Modifying Sterling Connect:Direct Initialization Parameters

For both nodes, add the parameter **SECURE.DSN=filename** to the Sterling Connect:Direct for z/OS initialization parameters, where **filename** is the name of the Sterling Connect:Direct Secure Plus parameter file for that node.

Restarting Sterling Connect:Direct

Restart Sterling Connect:Direct for both nodes.

Verifying Sterling Connect:Direct Secure Plus is Enabled

When you have successfully finished the preceding procedures, verify that Sterling Connect:Direct Secure Plus is enabled. The following message is displayed:

Before you begin

```
SITTA028I Secure+ Initialization Complete
```

Exchanging Data and Compare Results

To verify installation of Sterling Connect:Direct Secure Plus and test the configuration created in the preceding procedures:

Procedure

1. Create and run the following sample Sterling Connect:Direct Process to send data from Node A to Node B.

```
SAMPLE PROCESS SNODE=NODEB
*
COPYFILE COPY FROM ( PNODE          -
                      DSN='TEST.INPUT.DATASET' -
                      DISP=SHR           -
                      )                 -
TO ( SNODE            -
     DSN='TEST.OUTPUT.DATASET' -
     DISP=(NEW,CATLG)         -
     )                         -
SECURE=(ENC=Y,SIG=Y)
```

2. Review the statistics record for the transaction to verify the success of the sample Process by selecting the extended record type for session begin (SB), as shown in the following sample record.

```
Function      => Session Begin           Start Time => 18:49:58
                                           Start Date => 04/28/2003
Process Name => SAMPLE
Process Num  => 7                         Comp Code  => 00000000
                                           Comp Msg   => SVTM055I
Userid      => $CD
Primary Node => NODEA
Secondary Node NODEB
Submitter Node SC.MVS.$CD3
              Pnode Signature Enabled = Yes
              Snode Signature Enabled = Yes
              Merged Signature Enabled = Yes
              Pnode Encrypt.Data Algorithms...
                DESCBC56
                TDESCBC112
                IDEACBC128
              Snode Encrypt.Data Algorithms...
                TDESCBC112
                DESCBC56
                IDEACBC128
              System Data Encryption   = DESCBC56
```

Chapter 19. 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.
- **Auth Timeout** is set to the two-minute default to identify the maximum time that the system waits to receive Sterling Connect:Direct control blocks exchanged during the authentication protocol.

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.

```

Secure+ Create/Update Panel - SSL/TLS Parameters
Option:
Node Identification      EA Parameters      STS Parameters
Node                    2 1. Y 2. N 3. D Enable SSL
Q1A.ITAN.V3400=remote node 1 1. Y 2. N 3. D Enable TLS
                    name
Common Parameters between SSL and TLS
                    2 1. Y 2. N 3. D Override ==> Override parm (N/A)
                    1 1. Y 2. N 3. D Client Auth
                    1 1. Y 2. N 3. D Encrypt

Auth Timeout: 120

Certificate Label      -----
Cipher Suites          | mfcert_a ==> certificate for z/OS node
Certificate Pathname   | 352F04050A09030601 ==> z/OS cipher suites
Client Auth. Compare   | * ==> default to path in local node rec
                    -----

OK                      Cancel

```

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 GSKKMAN 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 GSKKMAN 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.q1a]).

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.

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 2013. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2013.

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

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

Index

A

- Access File, defined 7
- Accessing the Secure+ Admin Tool 164
 - Admin Tool
 - function keys defined 32
 - Main screen, description 27
 - starting and using 27
- algorithms, changing 129
- Autoupdate, public keys 24

C

- certificates
 - application-specific requirements 18
 - CA-signed
 - advantages and disadvantages 15
 - CA-ACF2 parameter
 - definitions 151
 - CA-Top Secret parameter
 - definitions 154
 - parameter definitions for GSSKMAN 149
 - RACF parameter definitions 147
 - general requirements 18
 - methods to obtain 19
 - obtain for SSL and TLS 18
 - security applications for
 - generating 17
 - terminology 15
 - types 14
- cipher suites, changing 128
- client authentication
 - defined 2
 - processing 13
- configuring a remote node record for SSL
 - importing the network map 94
- configuring a remote node record for STS
 - importing the network map 97
- Copy Step Start statistics record, fields defined 138
- Copy Termination statistics record, fields defined 139

D

- Data confidentiality, defined 21
- Data encryption
 - supported encryption algorithms 21
- data security, using STS 21
- Digital signature, merged settings 23

E

- exchanging STS keys, initial exchange 105
- External authentication, defined 1

F

- FIPS mode
 - System SSL planning 4

G

- guidelines
 - configuring parameter file manually 39
 - configuring parameter file manually for STS 53
 - configuring remote node records
 - imported from the network 93
 - configuring the local node record
 - imported from the network map 79

I

- implementation of SSL and TLS,
 - planning 11
- importing STS keys 107
 - manually 110
- importing the network map
 - configuring remote node records 93
 - configuring the local node record for SSL 80
 - configuring the local node record for STS 86
 - disabling Sterling Connect:Direct Secure Plus 102

K

- Key update frequency 25
- Keyfile management, defined 25
- Keys
 - planning implementation 24

L

- local and remote nodes, configuration scenarios 34
- local node record
 - adding manually for SSL protocol 40
 - adding manually for STS 54
- Local Node Security Feature Definition Worksheet 157

M

- Merged Secure Plus settings
 - using the STS Protocol 23

O

- OpenVMS
 - configuring node record for Sterling Connect:Direct 181

- overriding remote node values in a PROCESS statement 28, 31, 34, 49, 96

P

- parameter file
 - methods to populate 33
- parameters file
 - opening 124
 - resecuring 126
 - save and submit 113
 - scenarios for creating 33
 - viewing information about 125
- preparing for Secure Plus
 - configuration 27
- preventing nonsecure API connections,
 - configuring remote node record for SSL 70
- PROCESS statement
 - overriding security function values for all protocols 117
 - overriding values in a remote node record 28
 - Sterling Connect:Direct Secure Plus examples 119
- Proof of data origin, defined 21
- protocol-specific panels, parameters displayed 29
- Public keys
 - resetting in remote node records 132

Q

- Quickstart
 - populating Sterling Connect:Direct Secure Plus parameter file 35

R

- remote node record
 - adding for external authentication server 67
 - adding manually for SSL protocol 47
 - adding manually for STS 59
 - deleting 131
- Remote Node Security Feature Definition Worksheet 158
- Resetting, keys in remote node records 132

S

- saving remote node records
 - save action option 126
- Secure+ Admin Tool
 - types of Help 32
- Session Begin statistics record, fields defined 138

- SSL and TLS protocol
 - system resource requirements for Sterling Connect:Direct 13
- SSL protocol
 - create local node record manually 40
 - data security 3
 - defined 2
- Station-to-station protocol (STS)
 - defined 3, 21
 - functions, overriding from the COPY statement 24
 - keys
 - exporting 106
 - importing 107
 - managing overview 24
 - summary of processing 22
 - statistics record
 - SSL and TLS extended option 134
 - viewing for SSL 133
 - viewing for STS 135
 - viewing for STS extended option 137
- Sterling Connect:Direct
 - Prepare for Sterling Connect Direct Secure Plus 115
 - set up to use certificates 19
- Sterling Connect:Direct for OpenVMS
 - configuring node record 181
- Sterling Connect:Direct for z/OS
 - configuring node record 181
- Sterling Connect:Direct Process
 - use to send export key file 107
- Sterling Connect:Direct Secure Plus
 - maintaining 123
- Sterling Connect:Direct Secure Plus
 - parameter file
 - populating using Quickstart 35
- Sterling Connect:Direct Secure Plus
 - parameters
 - type of record valid for 29
- Sterling External Authentication Server
 - application, function 11
- Sterling External Authentication Server,
 - configuring remote record 67
- STS
 - adding local node record
 - manually 54
 - resetting keys 132
 - updating keys 131
- Summary
 - processing using Sterling Connect:Direct Secure Plus 12

T

- TLS
 - additional security features 3
 - levels of security 2
 - overview 2
 - protocol, defined 2
- Troubleshooting
 - Sterling Connect:Direct Secure Plus 141
- turning security on and off 117

U

- Updating, keys 24

W

- Worksheets
 - .CLIENT node 160
 - .EASERVER node 160
 - local node definition 157
 - remote node definition 158

Z

- z/OS
 - configuring node record for Sterling Connect:Direct 181



Product Number: 5655-X01

Printed in USA