

Connect:Direct for Windows

Secure Plus Option Implementation Guide

Version 4.5

Sterling Commerce
An IBM Company

First Edition

(c) Copyright 1995-2009 Sterling Commerce, Inc. All rights reserved. Additional copyright information in Getting Started Guide.

STERLING COMMERCE SOFTWARE

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

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

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

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

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

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

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

Sterling Commerce, Inc.

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

Contents

Chapter 1 Overview 7

About Connect:Direct Windows Secure+ Option.....	7
Security Concepts	7
Secure Sockets Layer Protocol (SSL) and Transport Layer Security Protocol (TLS)	8
Station-to-Station Protocol (STS)	9
Secure+ Option Tools.....	10
Plan the Secure+ Option Configuration.....	12
About Key Management for the STS Protocol	13
Override STS Functions from the COPY Statement	14
Summary of Processing Using Secure+ Option	14
TLS and SSL Secure+ Option Data Exchange	15
STS Secure+ Option Data Exchange.....	15
Merge Secure+ Option Settings Using the STS Protocol.....	16
Connect:Direct Secure+ Option for Windows Documentation.....	18

Chapter 2 Set Up Secure+ 19

Set Up Secure+ Option	19
Initialize Secure+ Option	19
Start Secure+ Admin Tool	20
Prepare to Set Up Secure+ Option.....	20
Obtain a Certificate and Generate a Key Certificate File	20
Generate a Key Certificate File for a CA Certificate	21
Generate a Key Certificate File for a Self-Signed Certificate	21
Exchange Trusted Root Files with Trading Partners.....	22
Populate the Secure+ Option Parameters File.....	22

Chapter 3 Configure Nodes 23

Node Configuration Overview	23
Configure the Secure+ Option .Local Node Record	24
Customize Remote Node Records.....	26
Disable Secure+ Option for a Remote Node	26
Add Certificate Information and Trusted Root Information to a Remote Node Record	27
Add Self-Signed Certificate Information to a Remote Node Record	27
Enable or Disable Client Authentication	28

Contents

Enable or Disable External Authentication for a Remote Node	28
Identify the Cipher Suite to Use for Data Encryption	29
Define a Protocol for a Remote Node Record	29
Configure a Remote Node Record for the TLS or SSL Protocol	29
Configure a Remote Node for the STS Protocol	30
Manage STS Keys	33
Export Keys	34
Import Keys	34
Override STS Functions from the COPY Statement	35
Validate the Configuration	36
Configure External Authentication in the .SEAServer Record.....	36
Use the .Client Record to Prevent Non-Secure API Connections to a Secure+ Option-Enabled Server.....	37
Configure Strong Password Encryption	37
Disable Strong Password Encryption	38
Enable Strong Password Encryption.....	38
Reset Passwords When Strong Password Encryption Key and Password File are Out of Sync..	38
Decryption Failure	39
SPE License Key Considerations.....	39

Chapter 4 Automate Setup Using the CLI 41

Start and Set Up the Secure+ CLI.....	41
Use LCU Files to Encrypt Passwords for Use with the Secure+ CLI	42
Sample Scripts	42
Manage the Parameters File	43
Update the .Local Node Record	45
Manage Remote Node Records.....	48
Manage the Sterling External Authentication Server Record	55
Maintain the .Password File (Strong Password Encryption)	56
Manage STS Keys Using the CLI.....	56
Automatically Create STS Keys for Remote Node Records	57

Chapter 5 Maintain Secure+ 59

Secure+ Option Node List	59
View Secure+Option Parameters File Information	60
View Secure+ Option Node Record Change History.....	60
Disable Secure+ Option	60
Delete a Secure+ Option Remote Node Record	61
Resecure Secure+ Option Parameters and Access Files	61
Change Cipher Suites	62
Change STS Protocol Encryption Algorithms.....	62
Update Keys in an STS-Configured Node Record	63
Clear Keys in an STS-Configured Node Record	63

Chapter 6 View Statistics 65

View Statistics	65
-----------------------	----

Chapter 7 Audits	69
<hr/>	
Secure+ Option Parameters File Auditing	69
Secure+ Option Certificate Auditing	71
Chapter 8 Troubleshoot Secure+	73
<hr/>	
Troubleshooting.....	73
Chapter 9 Configuration Worksheets	77
<hr/>	
Local Node Security Feature Definition Worksheet.....	77
Remote Node Security Feature Definition Worksheet.....	77
Chapter 10 Certificate File Layout	79
<hr/>	
Certificate File Layout.....	79
Chapter 11 Test Secure+ with STS	83
<hr/>	
Set Up the Local and Remote Node Records for Testing	83
Exchange Public Keys.....	84
Export Keys	84
Import Keys	84
Validate the Configuration	36
Exchange Data and Verify Results.....	85
Chapter 12 Automation Scripts	87
<hr/>	
Automation Scripts	87
Automatically Add a Remote Node to a Connect:Direct Network	90
Configure Secure+ Option to Use the SSL or TLS Protocol.....	92
Chapter 13 Use LCU to Configure Encrypted Passwords	95
<hr/>	
Configure Encrypted Passwords Using the LCU.....	95
Create an LCU File.....	96

Contents

About Connect:Direct Windows Secure+ Option

Connect:Direct Secure+ Option for Windows provides enhanced security for Connect:Direct. It is available as a separate component. Connect:Direct Secure+ Option for Windows uses cryptography to secure data during transmission. You select the security protocol to use.

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 exchanged, 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.

Secure+ Option enables you to select one of 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 Sterling External Authentication Server application.

Connect:Direct provides alternative cryptographic solutions depending upon the protocol enabled. The protocols available depend upon the version of Secure+ Option installed. The following table identifies the protocols available in each version of Secure+ Option and the encryption algorithms available for each protocol:

Note: Beginning with version 4.4, the Connect:Direct Secure+ Option for Windows version number is the same as the Connect:Direct for Windows version number.

Secure+ Option Version	Protocol	Encryption Algorithms					
		ECC	IDEA	RC4	DES	Triple DES	AES
3.0	STS	x	x	x	x	x	
	SSL			x	x	x	
	TLS				x	x	
3.1 and 3.2	STS	x	x	x	x	x	
	SSL			x	x	x	x
	TLS				x	x	
4.4 and 4.5	STS	x	x	x	x	x	x
	SSL			x	x	x	x
	TLS				x	x	

Secure Sockets Layer Protocol (SSL) and Transport Layer Security Protocol (TLS)

The SSL and the TLS protocols use certificates to exchange a key between the node that initiates the data transfer (the primary node, or PNODE) and the node that receives the data (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. A certificate authority (CA) is the entity responsible for issuing and revoking these certificates. The CA validates an applicant's identity, creates a certificate, and then signs the certificate, thus vouching for an entity's identity.

The SSL and TLS protocols provide three levels of security:

- The first level of security is activated when a trading partner connects to a Connect:Direct server. After the initial handshake, the Connect:Direct server sends its digital certificate to the trading partner. The trading partner checks that it has not expired and that it has been issued by a certificate authority the trading partner trusts. The trading partner must have a trusted root file that identifies the certificate authority.

If the security fails on any one of these checks, the trading partner is notified that the site is not secure and the connection fails.

- The second level of security, called client authentication, requires that the trading partner send its own certificate. If enabled, the Connect:Direct server requests certificate information from the trading partner, after it returns its certificate information. If the client certificate is signed by a trusted source, the connection is established.

In order to perform this security check, the trading partner must have a key certificate file available at its site and the Connect:Direct server must have a trusted root file that validates the identity of the Certificate Authority (CA) who issued the key certificate.

- The third level of security requires that a certificate common name be verified. The Connect:Direct Secure+ Option for Windows server searches the certificate file it receives from the trading partner and looks for a matching certificate common name. If the server cannot find the certificate common name, communication fails.

- To communicate using the SSL or TLS protocol, you must have both an X.509 certificate and a private key. The SSL and TLS protocols provide data security in the following areas:
 - Strong authentication—Because the CA went through an established procedure to validate an applicant’s identity, users who trust the CA can be sure the key is held by the owner. The CA prevents impersonation, and provides a framework of trust in associating an entity with its public and private keys.
 - Proof of data origin and data integrity validation—The certificate provides proof of origin of electronic transmission and encryption validates data integrity. Encrypting the private key ensures that the data is not altered.
 - Data confidentiality—Cipher suites encrypt data and ensure that the data remains confidential. Sensitive information is converted to an unreadable format (encryption) by the PNODE before being sent to the SNODE. The SNODE then converts the information back into a readable format (decryption).
- 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.
- The Sterling External Authentication Server application enables you to validate certificates that are passed during an SSL or TLS session. Using the Sterling External Authentication Server application, you can configure certificate chain validation, including the option to validate certificates against one or more Certificate Revocation Lists (CRLs) that are stored on an LDAP server. You can also configure the Sterling External Authentication Server application to return attributes associated with the incoming certificate, such as group information, that are stored on an LDAP server. See the Sterling External Authentication Server Release Notes for installation information.

For more information on configuring Connect:Direct Secure+ Option for Windows for external authentication, see the related links in the Help.

Station-to-Station Protocol (STS)

The 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.

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 finishes successfully, control blocks are exchanged in an encrypted format for the entire session.

Providing 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 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

In a previous release of Secure+ Option, two versions of Secure+ Option were available for the STS protocol, based on government regulations regarding export laws. The difference in the versions is the encryption algorithms available.

The Limited Export version of Secure+ Option 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)

The Export version of Secure+ Option supports only the 56-bit DES using Cipher Block Chaining Mode (DESCBC56) encryption algorithm. You must specify if a trading partner uses the Export version of Secure+ Option in the parameters file.

Secure+ Option Tools

Secure+ Option consists of five components: the Secure+ Administration Tool (Secure+ Admin Tool), the parameters file, the access file, the Strong Password Encryption parameters file, and the Secure+ Command Line Interface (Secure+ CLI). The following sections describe these components and their function within Secure+ Option.

Note: Only one instance of the Secure+ Admin Tool or the Secure+ CLI may be used at a time because they access the same configuration file. Do not open these tools at the same time or multiple

copies of the same tool at the same time (two instances of Secure+ Admin or two instances of Secure+ CLI). Only the user who accessed the configuration file first will be able to save updates.

Administration Tool

The Secure+ Option Admin Tool enables you to configure and maintain the Secure+ Option environment. The Admin Tool is the only interface for creating and maintaining the Secure+ Option parameters file; operating system utilities and editing tools do not work.

Parameters File

The Secure+ Option parameters file contains information that determines the protocol and encryption method used during security-enabled Connect:Direct operations. To configure Secure+ Option, each site must have a parameters file that contains one local node record and at least one remote node record. The local node record defines the most commonly used security and protocol settings for the node at the site. Each remote node record defines the specific security and protocol used by a trading partner. You create a remote node record in the Secure+ Option parameters file for each Connect:Direct node that you communicate with.

At installation, a record named .SEAServer is created in the parameters file, which enables Connect:Direct Secure+ Option for Windows to interface with Sterling External Authentication Server during SSL/TLS sessions. External authentication is configured in this record and enabled/disabled in the local and remote node records.

For additional security, the parameters file is stored in an encrypted format. The information used for encrypting and decrypting the parameters file (and private keys) is stored in the Secure+ Option access file.

Access File

The Secure+ Option access file is generated automatically when you create the Secure+ Option parameters file for the first time. You type a passphrase when you first initialize Secure+ Option. This passphrase encrypts and decrypts the private keys in the Secure+ Option parameters file. Your Secure+ Option administrator must secure the access file. 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.

Strong Password Encryption Parameters File

Strong password encryption protects Connect:Direct passwords at rest on the Connect:Direct server using strong encryption. Strong password encryption parameters are stored in the parameters file (<CD installation directory>\Server\Secure+\Nodes\Password). This feature is enabled by default.

Secure+ Option Command Line Interface

The Java-based Secure+ Command Line Interface (Secure+ CLI) is provided to enable you to create customized scripts that automate implementing Secure+ Option. Sample Windows scripts are provided as models for your customized scripts. You can save these scripts with another name, modify them to reflect your environment, and distribute them throughout your enterprise. For more information about

using the Secure+ CLI, commands and parameter descriptions, and the scripts, see Automating the Setup of Secure+ Option Using the Secure+ CLI.

Plan the Secure+ Option Configuration

Before you configure the Connect:Direct environment for secure operations, first plan how you will use Secure+ Option. Configure the Secure+ Option environment, based on company needs or preferences.

General Planning for Secure+ Option

Since all remote nodes are automatically enabled with the protocol defined in the local node record, determine which protocol will be used by most trading partners. Then configure the local node with this protocol. If a trading partner is not using the protocol defined in the local node record, you must configure the remote node record for that trading partner with the protocol.

Secure+ Option uses two files to initiate TLS or SSL sessions: a trusted root certificate file and a key certificate file.

Note: Secure+ Option does not support server gated crypto (SGC) certificates.

- The trusted root certificate file verifies the identity of trusted sources who issue certificates. If you plan to use Secure+ Option communication with a trading partner, exchange trusted root file with the trading partner. The trading partner must identify the trusted root file used to validate trusted sources in a certificate when it configures its Secure+ Option parameters file.
- A key certificate file is required at all sending locations and describes the identity of the secure node. This file includes information about the certificate being exchanged and the private key that defines the server.

When a trading partner attempts to establish communications with a Connect:Direct node, the Connect:Direct node sends the public key certificate from the key certificate to the trading partner to verify its identity. The location of the key certificate file must be configured in the Secure+ Option parameters file. The private key in the key certificate file is never sent (disclosed) by Connect:Direct.

The following list summarizes the tasks associated with configuring Secure+ Option:

- Populate the parameters file at your site by importing the Connect:Direct network map. This task creates a local node record and remote node records.
 - Enable the TLS or SSL protocol in the local node record. Enabling the local node record configures remote nodes to default to the settings in the local node record. To enable TLS or SSL, activate the following options:
 - Identify the trusted root certificate file that authenticates the trusted authorities.
 - Identify the key certificate file.
- If you identify the trusted root file and the key certificate file to use for secure communications in the local node record, the trusted root file must define the identity of all CAs for all trading partners, and the root certificate associated with the key certificate file must include certificate and private key information for all certificates.
- Identify a cipher suite to use to encrypt data in both the sending and receiving node. After secure communication is established, Secure+ Option determines what cipher has been defined at both the sending and the receiving node and uses this cipher to encrypt

data before sending it. If more than one cipher is enabled, the preferences defined in the server parameters file determine the cipher suite used for the SSL protocol and the preferences defined in the client parameters file determine the cipher suite used for the TLS protocol.

- If you want to enable a second level of security, activate client authentication.
- If you want to enable common name checking, you must enable this feature in the remote node record.
- For remote nodes that are using the protocol defined in the local node record, configure the remote nodes to implement any of the following additional security features:
 - Activate client authentication.
 - Configure the remote node record of trading partners with the same cipher suites enabled by the trading partner because trading partners must use the same cipher suite to enable data encryption.
- If a trading partner uses a protocol that is different from the protocol defined in the local node record, define the protocol in the remote node record. The remote node record must identify the same protocol as that used by the trading partner. Otherwise, Connect:Direct Secure+ Option will fail.
- If a trading partner does not use Secure+ Option, disable Secure+ Option in that remote node record.

About 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 that node. In order to communicate with the trading partner, all four keys must be defined in the parameters file for both your configuration and the trading partner's configuration. Therefore, you and your trading partner must exchange keys.

For the initial configuration, you manually exchange keys. You export keys and send them to the trading partner. Then you import the keys you receive from the trading partner into the parameters file. After the initial exchange, you can automate the exchange of key information.

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.

Key Exchange Method

After you exchange keys with a trading partner, both partners should enable the automatic key update feature for easier key management. When automatic key update is enabled, the updated key is sent to the trading partner node during the authentication process and the remote node record is updated with the new key values. Both you and your trading partner must enable automatic key update in order to use this feature.

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.

Import Key File Management

Before you begin exchanging key files with a trading partner, you must consider how to manage key files. Secure+ Option 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:

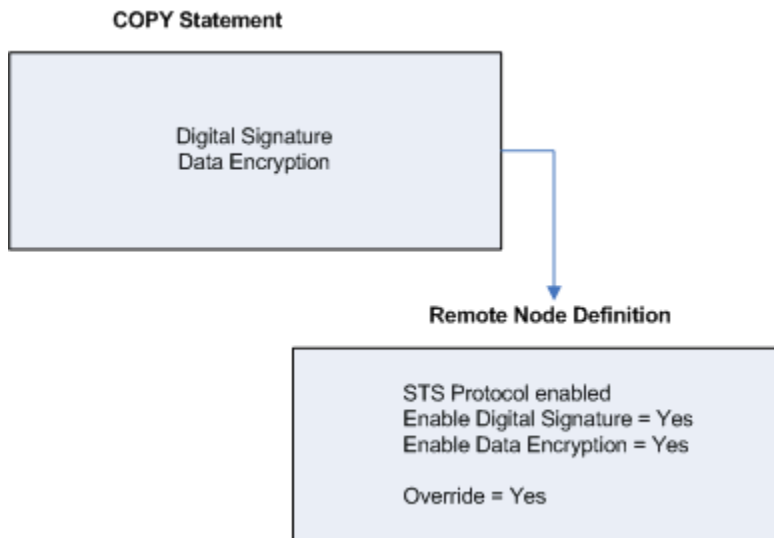
- Import the new key file immediately after receiving it from your trading partner and then delete the old key file.
- Rename the key file upon receipt or have your trading partner rename it before sending it.
- Create a directory for each remote node and store each key file separately in the associated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

It is not necessary to retain key files since the files are stored in the configuration file after you import them. However, saving the key files allows you to reconfigure the parameters file if a configuration is lost or if the node record is accidentally deleted.

Override STS Functions from the COPY Statement

When you configure a node to use the STS protocol, you can use the COPY statement in Connect:Direct to override the settings in the parameters file, if override is enabled. It is not always possible to disable digital signatures and data encryption. If either node enables these options, the options are used.

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



Summary of Processing Using Secure+ Option

After you configure Secure+ Option, you are ready to exchange data securely with other security-enabled Connect:Direct nodes. Your node must also be defined in the parameters file of your trading

partner. Data is securely exchanged between two nodes using the protocol defined in the parameters file.

The following topics describe what happens during a data exchange between two Connect:Direct nodes using Secure+ Option with the TLS or SSL protocol and with the STS protocol.

TLS and SSL Secure+ Option Data Exchange

Data exchange consists of three steps: authentication, sending data, and receiving data. The TLS or SSL protocol data exchange process is described in the following sections. The primary node initiates the data transmission, and the secondary node receives the data. The following description of processing depicts the PNODE as sending data and the SNODE as receiving data.

Authentication

The following steps occur during authentication:

1. The PNODE sends a control block to the SNODE. The SNODE confirms that it has a record defined in the Secure+ Option parameters file for the PNODE and determines the cipher suite to use for secure communication. If the SNODE finds a record for the PNODE and a common cipher suite can be negotiated, the session continues.
2. The SNODE sends its certificate back to the PNODE. Information for creating an encryption key is included. If client authentication is enabled, the SNODE also requests a certificate from the PNODE.
3. The PNODE verifies that the certificate of the SNODE is in its parameters file and generates a session key. If requested, it sends a client certificate to the SNODE for verification.
4. The SNODE confirms that a secure environment is established and returns a secure channel message.
5. The PNODE authenticates the SNODE and establishes communications.

Sending Customer Data

After communication is authenticated, the PNODE begins transmitting data.

- Information for encrypting data is exchanged in the control blocks.
- If data compression is enabled, the PNODE compresses the data.
- The PNODE encrypts the data with a cipher suite recognized by both communications nodes.

Receiving Customer Data

The SNODE receives the data.

- The SNODE decrypts the data using a cipher suite available for both the PNODE and the SNODE.
- If the data is compressed, the receiving node decompresses it.

STS Secure+ Option Data Exchange

Data exchange consists of three steps: authentication, sending data, and receiving data. The STS protocol data exchange process is described in the following sections. The primary node initiates the data exchange and the secondary node receives the data.

The following description of processing depicts the PNODE as sending data and the SNODE as receiving data.

Authentication

The following steps occur during authentication:

1. The PNODE sends a control block to the SNODE. Information for creating an encryption key for the PNODE is included. The SNODE confirms that it has a record defined in the Secure+ Option parameters 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.
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.
6. When authentication is successful, each node generates a shared session encryption key for encrypting control blocks.

Sending 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 SNODE 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.
- 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.

Receiving 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.

Merge Secure+ Option Settings Using the STS Protocol

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

The following topics describe the results of these merged values based on the PNODE and SNODE values.

Digital Signature

When Secure+ Option 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 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, authentication fails.

Auto Update Public Keys

If both nodes enable the auto update function, the authentication and signature public key values are dynamically updated during authentication if the remote node supplies different values. Enabling auto update eliminates much of the work that has to be performed by the Secure+ Option administrator.

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	The first algorithm ID in the SNODE list that is in the PNODE list.
N	Algorithm ID	The SNODE algorithm ID if it is in the PNODE list.
Y	N Y algorithm ID	The first algorithm ID in the PNODE list that is in the SNODE list.
algorithm ID	N Y algorithm ID	The PNODE algorithm ID if it is in the SNODE list.

Connect:Direct Secure+ Option for Windows Documentation

See the Connect:Direct release notes for your platform for a complete list of the product documentation.

About This Guide

The Connect:Direct Secure+ Option for Windows Implementation Guide describes how to implement point-to-point security into Connect:Direct operations with Secure+ Option. This document includes information to plan, install, configure, and use Secure+ Option.

The Connect:Direct Secure+ Option for Windows Implementation Guide is for programmers and network operations staff who install, configure, and maintain the Secure+ Option product.

This guide assumes knowledge of the Connect:Direct system, including its applications, network, and environment. If you are not familiar with the Connect:Direct system, refer to the Connect:Direct library of manuals.

Task Overview

The following table directs you to the information required to perform the tasks documented in the Connect:Direct Secure+ Option documentation, including chapter numbers in the printed documentation.

Task	For More Information See
Understanding Secure+ Option	About Connect:Direct Secure+ Option for Windows
Setting up Secure+ Option	Setting Up Secure+ Option
Automating the Set up of Secure+ Option	Automating the Setup of Secure+ Option Using the Secure + CLI
Testing Secure+ Option for STS	Testing Secure+ Option with the STS Protocol
Maintaining Secure+ Option	Maintaining Secure+ Option
Using scripts and the Secure+ CLI to automate implementation	Automating the Setup of Secure+ Option Using the Secure + CLI, and Automation Scripts
Viewing Secure+ Option statistics	Accessing Secure+ Option Statistics
Understanding error messages and resolving errors	Troubleshooting

Set Up Secure+ Option

Before you begin using Secure+ Option, you must configure nodes for secure operations.

You can install Secure+ Option using the Connect:Direct for Windows installation script. For more information on installing Secure+ Option, see the *Connect:Direct for Windows Getting Started Guide*.

Caution: After Secure+ Option is installed, the system administrator is responsible for securing access to the Secure+ Option Administration Tool, Secure+ CLI, and parameters files. The Secure+ administrator and Connect:Direct Server need full access to the Secure+ directory. No other users require access.

Intialize Secure+ Option

The first time you initialize the Secure+ Option Admin Tool, you must provide information to create the parameters file and access file for the associated Connect:Direct for Windows server node.

1. Click Start > Programs > Sterling Commerce Connect Direct v4.5.00 > CD Secure+ Admin Tool.

The Secure+ Admin Tool command shell window is displayed. The command shell starts the Secure+ Admin Tool and displays any program-generated error or trace messages.

Caution: Closing this shell when the Secure+ Admin Tool is open terminates the Admin Tool.

If this is the first installation of Secure+ Option, a message prompts you to initialize Secure+ Option.

2. Click OK. The Create new Parameters File dialog box is displayed.
3. Type the name of the associated local Connect:Direct node.
4. Type an alphanumeric string at least 32 characters long in the Passphrase field. Secure+ Option uses the passphrase to encrypt the Secure+ Option parameters and access files for greater security. You do not have to remember this passphrase value.
5. Click OK.

The Secure+ Option parameters file and access file are created, and the Secure+ Option Admin Tool window displays the local node record and the remote node record or records. When Secure+ Option is initialized, it is not functional because all of the parameters are disabled by default. You must configure the local node and remote node records before you can use Secure+ Option.

For more information on configuring these records, see *Configure Nodes*.

Start Secure+ Admin Tool

Use the Secure+ Option Administration Tool (Secure+ Admin Tool) to set up and maintain a Secure+ Option operation.

You can also use the Secure+ Option Command Line Interface (Secure+ CLI) to set up and manage Secure+ Option operations. See *Starting and Setting up the Secure+ CLI*.

Note: The parameters file is not dynamically updated. When multiple users update the parameters file, each user must close and reopen the file to display new records added by all sources.

1. Click Start > Programs.
2. Select Sterling Commerce Connect Direct v4.5.00 > CD Secure+ Admin Tool. The Secure+ Admin Tool Main Window is displayed.

The Secure+ Admin Tool starts and opens the Secure+ Option parameters file for the associated Connect:Direct node.

Prepare to Set Up Secure+ Option

Before you configure the Secure+ Option environment, perform the following setup procedures.

- Complete a worksheet for the local node record and a worksheet for each trading partner for whom you plan to enable Secure+ Option. Use the Local Node Security Feature Definition Worksheet to record the settings you plan to enable for the local node. For each trading partner, complete a Remote Node Security Feature Definition Worksheet and record the settings to enable Secure+ Option for the trading partner.
- Obtain a certificate and generate a key certificate file. A certificate is created by a trusted certificate authority (CA) or you can create a self-signed certificate. Generate a key certificate file by combining the certificate file and the private key file.
- Exchange trusted root certificate files with your trading partners
- Populate the Secure+ Option parameters file to include a record for each node running Secure+ Option. To communicate with a node running Secure+ Option, the node must have a record in the Connect:Direct network map and the Secure+ Option parameters file.

Obtain a Certificate and Generate a Key Certificate File

The TLS and the SSL security protocols use a secure server RSA X.509V3 certificate to authenticate a site for any node that accesses the site. Obtain a certificate (X509 ASN.1 Base64 format) from a CA

or create a self-signed certificate. Create a private key file (ASN.1/Base64 encoded PKCS8/PKCS5 v1.5 or “traditional SSLeay” format) using Sterling Certificate Wizard or any Web server software.

Secure+ Option looks for a key certificate file to authenticate a site. This file combines information from the certificate file and the private key file.

Certificate Wizard is a Sterling Commerce product that provides a way to create the files needed to obtain a certificate and create a key certificate file. It can be used to:

- Generate a certificate signing request (CSR) that you send to the CA to request a certificate.
- Generate a self-signed certificate and act as your own CA.
- Generate a private key file. A private key file is created when you generate the CSR or the self-signed certificate.
- Create a key certificate file that combines the certificate file with the private key file.

For information on installing Certificate Wizard, refer to the Sterling Certificate Wizard Release Notes. For information on using Certificate Wizard, refer to the Certificate Wizard online Help.

Generate a Key Certificate File for a CA Certificate

To generate a key certificate file from a certificate generated by a CA:

Note: While a key certificate may contain information about its intended use, such as e-mail, Secure+ Option does not use this information. It uses client or server authentication.

1. Generate a certificate signing request (CSR) and a private key using Certificate Wizard or any Web server software.
2. Send the CSR to the CA to request a certificate.
3. When you receive the certificate from the CA, generate a key certificate file using Certificate Wizard or a text editor. The key certificate file combines information from the certificate file that you received from the CA and the private key file you generated.

Generate a Key Certificate File for a Self-Signed Certificate

You can use Certificate Wizard to generate a key certificate file for a site that is authenticated with a self-signed certificate.

When Certificate Wizard generates a self-signed certificate, it creates a private key called `privkey.txt` and a trusted root file called `cert.crt`. The key certificate file combines information from the certificate file and the private key file. Certificate Wizard creates a key certificate file called `keycert.txt`.

1. Generate a self-signed certificate using Certificate Wizard.
2. Generate a key certificate file.
3. If necessary, copy the key certificate file to the Connect:Direct server.

Exchange Trusted Root Files with Trading Partners

When validating certificates, the trading partner must have a copy of the trusted root certificate file to verify the identity of the entity who issued your certificate, and you must have a copy of the trading partner's trusted root certificate file to validate the entity that issued the trading partner's certificate file.

Note: If the trading partner uses SSL for other secure communications, such as secure e-mail, the trading partner may already have a trusted root file for the CA used in the certificate.

To exchange trusted root files with a trading partner:

1. Obtain a copy of the trusted root file and copy it to the Secure+ Option directory on the Connect:Direct server.

You can maintain multiple trusted root files for each trading partner you need to verify, or you can maintain all trusted root file information in one file.

2. Do one of the following:
 - If you store all trusted root file information in one file, identify the location of this file in the local node record.
 - If you maintain a separate file for each trading partner, configure the name of each trading partner's trusted root file in the corresponding remote node record.

Populate the Secure+ Option Parameters File

To communicate with a trading partner using Secure+ Option, you define a node record for that partner in both the Connect:Direct network map and the Secure+ Option parameters file. To set up the Secure+ Option environment, you can populate the Secure+ Option parameters file from entries defined in an existing network map.

When you populate the parameters file from the network map, a record is automatically created in the parameters file for each node entry in the network map. Initially, Secure+ Option is disabled for each of the records created. You configure the local node record to activate Secure+ Option for all nodes in the parameters file.

1. From the Secure+ Admin Tool Main Window, click File > Sync with Netmap. The Available Netmaps dialog box is displayed.
2. Select the netmap to open and click Sync. The Select Netmap Entries to Add dialog box is displayed.
3. Click Add All. The Select Parameters File Entries to Delete dialog box is displayed.
4. Click Skip to close the parameters file without deleting any entries.

The Secure+ Option parameters file is populated and the Secure+ Admin Tool Main Window displays remote node records in the parameters file including the records you added from the network map.

Node Configuration Overview

When you import the network map records into the Secure+ Option parameters file, Secure+ Option parameters are disabled.

To configure the nodes for Secure+ Option, complete the following procedures:

- Configure the Secure+ Option .Local node record
 - Define the security options for the local node. Because TLS and SSL provide the strongest authentication with easy-to-maintain keys, configure the local node for one of these protocols. Determine which protocol is used by most trading partners and configure the local node with this protocol.
- Disable remote nodes that do not use Secure+ Option
- Customize a remote node for the following configurations:
 - To use a unique certificate file to authenticate a trading partner
 - To use a different self-signed certificate for client or server authentication
 - To identify a unique cipher suite used by a trading partner
 - To activate common name validation
 - To activate client authentication
 - To activate external authentication
- Configure all remote nodes that use a protocol that is not defined in the local node
 - When you configure the local node, all remote nodes are automatically configured to the protocol defined in the local node. If a trading partner uses a different protocol, you must turn on the protocol in the remote node record. For example, if you activate the TLS protocol in the .Local node record and a trading partner uses the SSL protocol, configure the SSL protocol in the remote node record for the trading partner.
- If you want to use Sterling External Authentication Server to validate certificates:
 - Update the .SEAServer record with the SEA Server host name and port
 - Enable TLS or SSL
 - Enable external authentication
 - Specify the certificate validation definition to use
- If you want to prevent non-secure API connections from communicating with a Secure+ Option enabled server:
 - Define a remote node called .Client

- Enable TLS or SSL
- Disable override

Configure the Secure+ Option .Local Node Record

Configure the .Local node record with the protocol used by most of your trading partners. Because remote node records can use the attributes defined in the .Local node record, defining the .Local node record with the most commonly used protocol saves time. After you define the protocol in the .Local node record, all remote nodes default to that protocol. Also, identify the trusted root file to be used to authenticate trading partners.

To configure the local node, refer to the Local Node Security Feature Definition Worksheet that you completed for the .Local node record security settings and complete the following procedure:

1. From the Secure+ Admin Tool Main Window, double-click the .Local record. The Edit Record dialog box displays the Security Options tab, the node name, and the type of node.
2. Set the following Security Options for the local node:
 - Enable TLS Protocol or Enable SSL Protocol
 - Enable Override
3. If necessary, change the time-out value in the Authentication Timeout box.

Refer to the following table for an explanation of the Security Options boxes:

Field Name	Field Definition	Valid Values
Node Name	Specifies the node record name.	.Local This is not an editable field.
Base Record	Specifies the name of the base record. If an alias record is selected, the base record name is displayed in this box.	Name of the local Connect:Direct node.
Type	Specifies the current record type.	Local for a local record and Remote for a remote record. This is not an editable field.
Disable Secure+	Disables Secure+ Option.	Default value is Disable Secure+. Note: If this option is selected, override is enabled, and no remote node definition exists for the remote node in the Secure+ Option parameters file, Secure+ Option is bypassed.
Enable TLS Protocol	Enables TLS protocol to ensure that data is securely transmitted.	The default value is Disable Secure+.
Enable SSL Protocol	Enables SSL protocol to ensure that data is securely transmitted.	The default value is Disable Secure+.
Enable STS Protocol	Enables STS protocol to ensure that data is securely transmitted.	The default value is Disable Secure+.

Field Name	Field Definition	Valid Values
Disable Override	Disables the ability to override values in the .Local node record with values in the remote node record.	The default value is Disable Override.
Enable Override	Enables override to allow values in the remote node record to override values in the .Local node record.	The default value is Disable Override.
Authentication Timeout	Specifies maximum time, in seconds, that the system waits to receive the Connect:Direct control blocks exchanged during the Secure + Option authentication process. If you specify a value of 0, 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 process.	A numeric value equal to or greater than 0, ranging from 0 to 3600. The default is 120 seconds.

4. Click the TLS/SSL Protocol tab. The TLS/SSL Options dialog box is displayed.
5. Type the location of the trusted root certificate file to use to authenticate trading partners in the Trusted Root Certificate File box or click Browse and locate the file.
6. Click Browse next to the Certificate File box, locate the key certificate file and double-click the file to select it. The Certificate Passphrase dialog box is displayed.
7. Type the passphrase you specified when you created the certificate in the Certificate Passphrase box.
8. Click OK. The Certificate File box is populated with the certificate file name and location.
9. To enable client authentication, click Yes in the Enable Client Authentication box.
10. To view information about the trusted root file and the certificate, click View Certificates.
11. Highlight the cipher suites to enable in the Available list and click Add.
12. If necessary, use the Up and Down buttons to reorder the cipher suites. Place the cipher suites in order of preference.
13. Click the External Authentication tab. The External Authentication dialog box is displayed.
14. Choose one of the following options:
 - To enable external authentication on the remote node, click Yes in the Enable External Authentication box.
 - To disable external authentication on the remote node, click No.
15. Type the Certificate Validation Definition character string defined in Sterling External Authentication Server.
16. Click OK to close the Edit Record dialog box and update the parameters file.

Customize Remote Node Records

After you configure the .Local node record, Secure+ Option enables the protocol and parameters that you configured for the local node for all remote node records. If all trading partners use the protocol and configuration defined in the .Local node record, you are now ready to begin using Secure+ Option.

However, even when a trading partner uses the same protocol as the one defined in the .Local node record, you may need to customize remote node records for the following configurations:

- Using a unique certificate file to authenticate a trading partner—During a TLS or SSL session, a certificate enables the PNODE to authenticate the SNODE. You identified a certificate in the .Local node record. If you want to use a unique certificate to authenticate a trading partner, you must identify this information in the remote node record.
- Using a self-signed certificate file to authenticate a trading partner—During a TLS or SSL session, a certificate enables the PNODE to authenticate the SNODE. If you want to use a self-signed certificate to authenticate a trading partner, you must identify this information in the remote node record.
- Activating client authentication—Client authentication requires that the SNODE validate the PNODE. If you want to enable client authentication, activate this feature in the remote node record. If you want another layer of security, you can activate the ability to validate the certificate common name.
- Identifying the cipher suite used by a trading partner—When configuring the TLS or SSL protocol, you enable cipher suites that are used to encrypt the transmitted data. When communicating with a trading partner, you and the trading partner must use the same cipher suite to encrypt data. If the trading partner does not enable a cipher suite that is enabled in your configuration, communication fails. If necessary, enable cipher suites in the remote node record.

If a trading partner uses a different protocol than the protocol defined in the .Local node record, you need to define the protocol in the remote node record. Refer to "Defining a Protocol for a Remote Node Record."

When customizing remote node records, refer to the Remote Node Security Feature Definition Worksheet you completed for each remote node.

Disable Secure+ Option for a Remote Node

If a trading partner is not using Secure+ Option, you must disable Secure+ Option for that remote node record.

Complete the procedure below to disable Secure+ Option for a remote node record:

1. Open the remote node record for which you want to disable Secure+ Option.
2. Click the Security Options tab.
3. Click the Disable Secure+ Option.
4. Click the Disable Override option.
5. Click OK to update the node record.

Add Certificate Information and Trusted Root Information to a Remote Node Record

You identified a certificate and a trusted root file to use for authentication when you defined the .Local node record. If you want to use a different certificate to authenticate a trading partner or a different trusted root file to validate the identity of the trusted source who issues certificates, you need to add that information to the remote node record.

Complete the following procedure to identify unique certificate information or trusted root information for a remote node record:

1. From the Secure+ Admin Tool Main Window, double-click the remote node record to open. The Edit Record dialog box is displayed.
2. Click the TLS/SSL Protocol tab.
3. Type the location of the trusted root certificate in the Trusted Root Certificate File box or click Browse and locate the file.
4. Click Clear Certificate to clear any associated certificate file from the remote node record.
5. Click Browse next to the Certificate File box, locate the key certificate file, and double-click the file to select it. The Certificate Passphrase dialog box is displayed.
6. Type the passphrase you specified when you created the certificate in the Certificate Passphrase box.
7. If you want to view trusted root files or key certificate files, click View Certificates.
8. Click OK.

Add Self-Signed Certificate Information to a Remote Node Record

If you want to use a self-signed certificate to authenticate a trading partner and this information has not been identified in the .Local node record, you need to add that information to the remote node record. First, obtain a copy of the trading partner's trusted root file and copy this file to a local drive. If you plan to perform server authentication, you must also send a copy of your trusted root certificate file to the trading partner.

Complete the following procedure to add self-signed certificate information to a remote node record:

1. From the Secure+ Admin Tool Main Window, double-click the remote node record to open. The Edit Record dialog box is displayed.
2. Click the TLS/SSL Protocol tab.
3. Type the location of the trading partner's self-signed certificate file in the Trusted Root Certificate File box or click Browse and locate the file.
4. Click OK.

Enable or Disable Client Authentication

Client authentication provides another level of security. If you activate client authentication, two levels of certificate validation occur. First, the PNODE validates the certificate from the SNODE. Then, the SNODE performs client authentication by validating the certificate from the PNODE. Within client authentication, you can enable a third level of security. If you provide a certificate common name during setup, the client authentication process first validates the certificate from the PNODE and then searches for the common name in the certificate file. If the SNODE cannot validate the PNODE certificate or locate the common name, communication fails. You must enable common name checking in the remote node record to use this function. It cannot be activated in the .Local node record.

If client authentication is enabled in the .Local node record, client authentication will be performed for all connections. If you want to disable client authentication for select trading partners, turn off this option in the remote node record.

Complete the following procedure to activate or deactivate client authentication for a remote node:

1. From the Secure+ Admin Tool main window, double-click the remote node record to open. The Edit Record dialog box is displayed.
2. Click the TLS/SSL Protocol tab.
3. To enable client authentication in a remote node record, click Yes in the Enable Client Authentication box.

Note: If client authentication is enabled in the .Local node record, it is automatically enabled in all remote node records.

4. To disable client authentication in the remote node record, click No in the Enable Client Authentication box.
5. To enable another level of security, type the certificate common name in the Certificate Common Name box.
6. Click OK to close the Edit Record dialog box and update the parameters file.

Enable or Disable External Authentication for a Remote Node

On a node-by-node basis, you can specify whether a remote node uses external authentication or if that remote node defaults to the external authentication setting in the .Local node record.

Complete the following procedure to configure a remote node for external authentication:

1. If necessary, open the remote node record. The Edit Record dialog box is displayed.
2. Click the External Authentication tab.
3. Choose one of the following options:
 - To enable external authentication on the remote node, click Yes in the Enable External Authentication box.

- To disable external authentication on the remote node, click No.
- To default to the external authentication setting defined in the .Local node record, click Default to Local Node.

Note: If external authentication is enabled in the .Local node record, it is automatically enabled in all remote node records.

4. Type the Certificate Validation Definition character string defined in Sterling External Authentication Server.
5. Click OK to close the Edit Record dialog box and update the parameters file.

Identify the Cipher Suite to Use for Data Encryption

Cipher suites encrypt the data you send to a trading partner. To encrypt data, Connect:Direct uses the cipher suite that is available for both the SNODE (trading partner) and the PNODE. If you want to specify a unique cipher suite for a trading partner, you can identify this information in the remote node record. Identifying a cipher suite ensures that the selected cipher suite is used for data encryption.

Complete the following procedure to identify the cipher suite used by a remote node.

1. If necessary, open the remote node record. The Edit Record dialog box is displayed.
2. Click the TLS/SSL Protocol tab.
3. Turn off Default to Local Node from the Cipher Suites section.
4. Highlight the cipher suite to use in the Available list and click Add.
5. If more than one cipher suite was selected, use the Up and Down buttons to reorder the cipher suites. Place the cipher suites in order of preference.
6. Click OK to close the Edit Record dialog box and update the parameters file.

Define a Protocol for a Remote Node Record

When you configured the .Local node record, all remote node records are automatically configured to use the same protocol. If a trading partner uses a different protocol, you define this protocol in the remote node record.

If you have not already done so, complete a Local Node Security Feature Definition Worksheet for each trading partner who plans to use a protocol not defined in the .Local node record.

Configure a Remote Node Record for the TLS or SSL Protocol

When the remote node record needs to be configured to use a different protocol (TLS or SSL) than is defined in the .Local node record, complete the following procedure:

1. From the Secure+ Admin Tool Main Window, double-click the remote node record to edit. The Edit Record window displays the Security Options tab, the node name, and the type of node.
2. Select the protocol to use by selecting Enable TLS Protocol or Enable SSL Protocol.
3. If necessary, change the time out value in the Authentication Timeout box.
4. Click the TLS/SSL Protocol tab.
5. Type the location of the trusted root certificate in the Trusted Root Certificate File box or click Browse and locate the file.
6. Click Clear Certificate to clear any associated certificate file from the remote node record.
7. Click Browse next to the Certificate File box, locate the key certificate file, and double-click the file to select it. The Certificate Passphrase dialog box is displayed.
8. Type the passphrase you specified when you created the certificate in the Certificate Passphrase box.
9. If you want to activate client authentication for the node, do the following:
 - Click Yes in the Enable Client Authentication box.
 - To enable another level of security, type the certificate common name in the Certificate Common Name box.
10. To identify the cipher suites that can be used by the remote node, do the following:
 - Turn off Default to Local Node from the Cipher Suites section.
 - Highlight the cipher suite to use in the Available list and click Add.
11. Click OK to close the Edit Record dialog box and update the parameters file.

Configure a Remote Node for the STS Protocol

When a trading partner uses the STS protocol, configure the remote node record to use the STS protocol, including creating signature and authentication keys and identifying the export version of Secure+ Option being used by the trading partner.

If you have not already done so, complete a Remote Node Security Feature Definition Worksheet for each trading partner who plans to use the STS protocol. Then use the procedures in this section to configure remote node records for the STS protocol.

After you create the keys for STS-enabled remote node records, you are responsible for managing them. The first time you use the STS protocol, you manually exchange keys with the trading partner. After you exchange keys for the first Secure+ Option enabled communication, you can then turn on the automatic key management function. The Public Key Auto Update function enables the public keys to be updated automatically during a communications session. This simplifies key management for ongoing communications.

If you activate the STS protocol for a remote node record, you can use the COPY statement in the Connect:Direct Process statements to override settings in the remote node records. Refer to "Overriding

STS Functions from the COPY Statement" for information about overriding remote node record settings.

Complete the following procedure to configure a remote node for the STS protocol:

1. Double-click the remote node to configure. The Edit Record dialog box displays the Security Options tab.
2. On the Security Options tab, click Enable STS Protocol.
3. If you want to allow the COPY statement to override values in the remote node, click Enable Override.
4. If necessary, change the value in the Authentication Timeout box.
5. Click the STS Protocol tab. The Edit Record dialog box displays STS Protocol information.
6. Set the STS Options as desired. Refer to the following table for an explanation of the options:

Field Name	Field Definition	Valid Values
Enable Digital Signatures	Enables or disables digital signatures.	Yes No Default to Local Node
Enable Public Key Auto Updates	Enables or disables automatic update of public keys during authentication. If this option is enabled for the PNODE and the SNODE, the public keys of the PNODE and SNDE are automatically exchanged during authentication. Auto update can only occur over a secure connection; therefore, the initial exchange of keys between two nodes must be done manually.	Yes No Default to Local Node
Limited Export Version	If a trading partner is using an earlier version of Secure+ Option, identifies the export version of Secure+ Option being used.	Yes No

Field Name	Field Definition	Valid Values
Enable Encryption	<p>Enables or disables data encryption during the copy operation.</p> <p>If Yes is selected, data encryption is enabled and the algorithm used depends on the merged value between the PNODE and SNODE. See Overriding STS Functions from the COPY Statement on page 14 for more information about the merged values for data encryption. See Data Encryption on page 20 for more information about the merged values for data encryption.</p> <p>If No is specified, data encryption is disabled.</p> <p>If Algorithm is specified and encryption is enabled, Algorithm must be populated and Enable STS Protocol must be enabled.</p> <p>If the remote node enables encryption, the local node cannot disable it.</p>	<p>Yes No Default to Local Node</p> <p>Algorithm name</p>
Encryption Algorithms	Lists acceptable data encryption algorithms when Copy file encryption is requested. List in order of preference, with the most-preferred algorithm first.	<p>Default to Local Node</p> <p>DESCBC56</p> <p>TDESCBC112</p> <p>IDEACBC128</p>

7. Click the Authentication Keys tab.
8. Click Generate Key to create the authentication keys for the node. The Generate Random Number Seed dialog box is displayed. If a previous key exists, a message is displayed, prompting you to save the previous key.
9. Do one of the following to generate a key:
 - Type an alphanumeric string at least 32 characters long in the Random Number Seed box and click OK. Secure+ Option uses the random number seed value to generate the authentication keys.
 - Click Sample Value, highlight all of the grid squares, and click OK to generate the random number seed.

The Authentication Keys window displays the populated Local Public Key box.
10. If you are replacing an older key and you save the old key as the previous key, type the expiration date for the public key in the Previous Key Pair Expiration Date box. Refer to the following table for a definition of the Authentication Keys boxes.

Field Name	Field Definition	Valid Values
Local Public Key	Public key used for authentication.	Generated by Secure+ Option.

Field Name	Field Definition	Valid Values
Previous Key Pair Expiration Date	Expiration date for previous authentication public keys. This eliminates the need to update Secure+ Option parameters 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, 00:00:00 is used.
Remote Public Key	Displays the imported value from the trading partner.	Imported from the trading partner.

11. Click the Signature Keys tab.
 12. Click Generate Key to create the signature keys for the node. The Generate Random Number Seed dialog box is displayed. If a previous key exists, a message is displayed, prompting you to save the previous key.
 13. Do one of the following to generate a key:
 - Type an alphanumeric string at least 32 characters long in the Random Number Seed box and click OK. Secure+ Option uses the random number seed value to generate the signature keys.
 - Click Sample Value, highlight all of the grid squares, and click OK to generate the random number seed.

The Signature Keys window displays the populated Public Key box.
 14. If necessary, type the expiration date for the public key in the Previous Key Pair Expiration Date box.
- Refer to the following table for the name, definition, and valid values for the Signature Keys boxes.

Field Name	Field Definition	Valid Values
Local Public Key	Public key used for digital signature.	Generated by Secure+ Option.
Previous Key Pair Expiration Date	Expiration date for previous digital signature public keys. This eliminates the need to update Secure+ Option parameters 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, 00:00:00 is used.
Remote Public Key	Displays the imported value from the trading partner.	Imported from the trading partner.

15. Click OK to close the remote node record and update the parameters file.

Manage STS Keys

When you define the STS protocol for a remote node, you must exchange keys with the trading partner before using Secure+ Option with that node.

To maintain the keys for the STS protocol, you perform the following procedures:

- Export keys to your trading partner
- Import keys from your trading partner

Export Keys

After you create signature and authentication keys for a node record, you must send this information to the trading partner. Export the information to a file that you can then send to the trading partner. Be sure that you export keys from the server associated with the local node.

Two ways of exporting keys are available. If you define several remote node records to use the STS protocol, you can create export key files for all remote node records at one time. If you want to export the key values for one remote node record, select the remote node record and export the selected remote node record key file.

To export the authentication and signature public key values for one or more remote node records:

1. Create a specific directory for storing the public key files.
2. If necessary, open the Secure+ Option parameters file. The Secure+ Admin Tool Main Window is displayed.
3. Do one of the following:
 - If you want to export the key files for all remote node records, select Export All Public Keys from the Key Management menu item.
 - If you want to export the key file for one or more remote node records, highlight the node records to export and click the Export Selection option of the Key Management menu item.

The Select Export Destination Directory dialog box is displayed.

4. Highlight the directory that you created in step 1 and click Select.

If you selected Export All Public Keys, a file with an `sxp` extension is created for all remote node records. If you exported the keys of a selected remote node record, one file is created for the remote node record. Each file is named after the corresponding remote node record.

Import Keys

Before you can communicate with a trading partner, you must obtain their key data and import the information into the parameters file.

To import the authentication and signature public key values sent to you by the trading partner administrator:

1. From the Secure+ Admin Tool Main Window, highlight the remote record to import the key from.
2. Click the Import Public Keys option of the Key Management menu item. The Select Import Source File dialog box is displayed.

3. Go to the directory that contains the signature and authentication key file for this remote node.
4. Highlight the `sxp` file for this node and click Import. The key is imported to the remote node record.
5. Ensure that the remote keys are imported by viewing the Remote Public Key box located in the Authentication Keys tab and Signature Keys tab.

Override STS Functions from the COPY Statement

After you set up the Secure+ Option environment, security is implemented each time that you use Connect:Direct with any node configured and enabled for Secure+ Option. You can, however, override some Secure+ Option functions from the COPY statement if you implemented the STS security protocol. This section tells you have to override the Secure+ Option features using the COPY statement.

Setting Secure+ Option Function Values from the COPY Statement

The SECURE COPY statement parameter enables you to set data encryption and digital signatures features from the Connect:Direct COPY statement. You can always enable these features from the COPY statement, but you cannot necessarily disable them from the COPY statement.

The SECURE parameter value specified in the COPY statement overrides the value specified in the Secure+ Option remote node record only if Enable Override is selected in that remote node record. After the security settings are merged between the PNODE and SNODE, 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.

If the override function is disabled in that remote node record and the values specified on the COPY statement are different from the values specified in the remote node record, the copy operation fails with a return code of 8 and message ID CSPA011E indicating the error.

The following table describes the SECURE parameters for the Connect:Direct COPY statement.

Parameter Name and Syntax	Parameter Description	Valid Values
<code>secure=(encrypt.data=valid value)</code> or <code>secure=(enc=valid value)</code>	Enables/disables Copy file encryption	Y N algorithm name DESCBC56 TDESCBC112 IDEACBC128 Default—Secure+ Option parameters file value
<code>secure=(signature=valid value)</code> or <code>secure=(sig=valid value)</code>	Enables/disables digital signature creation	Y N Default—Secure+ Option parameters file value

Note: Data encryption and digital signatures cannot necessarily be disabled from the COPY statement.

If both parameters are used from the COPY statement, the syntax is as follows:

```
secure=(enc=y,sig=y)
or
secure=(encrypt.data=y,signature=y)
```

The following sample Process, SECURE, copies the file README.TXT from the PNODE to the SNODE, renames it to VERIFY.TXT, and enables data encryption and digital signatures.

```
step1 copy
  from (
    file=/usr/ndm/bin/readme.txt
  )
  secure=(encrypt.data=y,signature=y)
  to (
    file=/usr/ndm/bin/verify.txt
    disp=(rpl)
  )
pend
```

Validate the Configuration

Perform this procedure to ensure that the nodes have been properly configured. The validation process checks each node to ensure that all necessary options have been defined and keys have been exchanged.

To validate the parameters file:

1. In the Secure+ Admin Tool, click File > Validate Secure+. The Secure+ Admin Tool - Validation Results window is displayed.

If the parameters file is not correctly configured, warning and error messages are displayed.

2. Read each warning message. To correct each warning or error reported, go back to the parameters file and make changes as needed.

Note: Warning messages do not always mean that the parameters file is incorrectly configured. Some warning messages are informational only.

3. Click Close to close the Validation Results window.

Configure External Authentication in the .SEAServer Record

At installation, a record named .SEAServer is created in the parameters file, which enables Connect:Direct Secure+ Option to interface with Sterling External Authentication Server (SEAS) during SSL/TLS sessions to validate certificates. SEAS properties are configured in this record and enabled/disabled in the local and remote node records.

Complete the following procedure to configure the server properties that will allow Connect:Direct for Windows to interface with Sterling External Authentication Server:

Note: The values specified for this procedure must match the values specified in Sterling External Authentication Server.

1. Double-click the record called .SEAServer.
2. Type the Host Name for SEAS.
3. Type the Port Number where SEAS is listening. The default is 61366.
4. Click OK to update the record.

Use the .Client Record to Prevent Non-Secure API Connections to a Secure+ Option-Enabled Server

Connect:Direct servers that use Secure+ Option support secure API connections. Client applications that use the API include Connect Control Center, Sterling Java API, Connect:Direct Requester, and Connect:Direct Browser User Interface. Client applications created using the Sterling Java API support secure API connections; client applications created using the Sterling SDK do not support secure API connections.

If a Connect:Direct server has Secure+ Option enabled, an API configuration that connects to this server uses the .Client node record to determine if it has the authority to connect to the server. The override settings in the .Client node record determine if the client application has the authority to connect to the server. When override is enabled in the .Client record, secure and non-secure API connections are allowed to connect to the Connect:Direct server. When override is disabled in the .Client record, all client connections must use the effective protocol configured in the .Client or .Local node record.

Valid settings for API connections include TLS, SSL, or security disabled. An API configuration follows the same rules as other remote node connections with the following exceptions:

- API connections must use either the SSL or the TLS security protocol
- Certificate-based client authentication is not supported
- The local node is automatically overridden by settings in the .Client node definition

Since the local node is automatically overridden, Secure+ Option configurations that normally disable this setting will not be affected. In order to disable override and prevent API connections that are either nonsecure or that do not use the settings defined in the local node, configure the .Client node record and disable override.

To prevent non-secure connections to a Connect:Direct server with Secure+ Option enabled:

1. Double-click the remote node record called .Client.
2. Click the Disable Override option.
3. If necessary, configure the TLS or SSL protocol in this node, if it is not defined in the .Local node record. See "Configure a Remote Node Record for the TLS or SSL Protocol."

Note: The TLS or SSL protocol must be configured in either the .Client or the .Local node record.

4. Click OK to update the node record.

Configure Strong Password Encryption

This feature uses strong encryption to encrypt all Connect:Direct passwords stored on disk. This feature is enabled by default.

Disable Strong Password Encryption

To disable strong password encryption, do the following:

1. From the Secure+ Admin Tool main menu, select Edit > Password Encryption.
2. Click the No option for Enable Strong Password Encryption.
3. Click OK.

The following message displays: The Connect:Direct server must be restarted to update Strong Password Encryption.

Note: The change does not take effect until you restart Connect:Direct.

Enable Strong Password Encryption

To enable strong password encryption, do the following:

1. From the Secure+ Admin Tool main menu, select Edit > Password Encryption.
2. Click the Yes option for Enable Strong Password Encryption.
3. Click OK.

The following message displays: The Connect:Direct server must be restarted to update Strong Password Encryption.

Note: The change does not take effect until you restart Connect:Direct.

Reset Passwords When Strong Password Encryption Key and Password File are Out of Sync

If the Strong Password Encryption key stored in the .Password file becomes out of sync with the Strong Encryption key used to encrypt the passwords, you must reset all Strong Password Encryption passwords.

The .Password file can get out of sync if one of the following occurs:

- You restore the .Password file from a backup—The .Password file is updated each time the Connect:Direct server is started, so the backup will probably not contain the current parameters.
- The .Password file is deleted—The .Password file is recreated as needed, so the Strong Password Encryption key used to encrypt the passwords no longer exists.
- The .Password file is corrupt—The Strong Password Encryption key used to encrypt the passwords is not accessible.

To reset the passwords:

1. Delete the <CD installation directory>\Server\Secure+\Nodes\.password file.

2. Use the Requester to re-enter local user ID/password for any proxy records.
3. Use the Requester to manually delete all Processes in the TCQ.
4. Stop the Connect:Direct server.
5. Reset the message file database password by running the Connect:Direction Database Wizard.
6. Reset the SMTP password using the Change Notification Utility.
7. Start the Connect:Direct server.

Decryption Failure

If the Process KQV file fails decryption at startup or during runtime, the server places the Process in the Hold/Error queue to raise the visibility of the error.

SPE License Key Considerations

If your license key for Secure+ Option expires, strong password encryption is disabled and all passwords at rest are restored to their original values.

Automate Setup Using the CLI

Start and Set Up the Secure+ CLI

The following sections describe the commands and parameters used to start and set up the command line environment.

Start the Secure+ CLI

To start the Secure+ Command Line Interface:

1. Change to the following directory: C:\Program Files\Sterling Commerce\Connect Direct v4.5.00\Server\Secure+.
2. Enter the following command:

```
spcli.cmd
```

Control the Display of Commands

Set the following parameters to define how error messages are captured:

Parameter	Definition	Values
-li	Switch to enable the display of commands to the terminal.	y n
-lo	Switch to enable the display of output and error messages to the terminal.	y n
-le	Switch to enable the display of errors to STDERR.	y n
-e	Switch to tell the Secure+ CLI to exit when the return code is higher than 0 4 8 16 the specified number. If you do not include this parameter, Secure+ CLI continues to run even after an error has occurred.	
-p	The full path of the default parameters file directory. The parameters file in this directory is opened automatically.	
-h	Switch to display the usage of the Secure+ CLI.	

Control Help

The Help command determines what help information is displayed. You can list all the Secure+ CLI commands and display help for individual commands.

Command	Description
help	Displays all the Secure+ CLI commands.
help <command>	Displays help for the specified command.

Specify Delimiter Characters

Define the following commands to determine how error messages are captured:

Command	Definition	Values
Set begdelim= enddelim=	Defines beginning and ending character to use to enclose keywords that use blanks and other special characters.	Any character The default value is " (double quotes).

Use LCU Files to Encrypt Passwords for Use with the Secure+ CLI

The Secure+ CLI displays passwords in plain text. If your company security policy mandates that you use encrypted passwords, you can use the Local Connection Utility (LCU) to create an LCU file that contains non-encrypted information for encrypting the password and the encrypted password.

For more information on creating and using LCU files, see [Use the Local Connection Utility to Configure Encrypted Passwords](#).

Sample Scripts

The following scripts are provided as models for creating custom scripts to define your Secure+ Option environment and automate its implementation. To prevent any loss of data, you cannot run the scripts, but you can save them with a different name and modify them to suit your needs.

The sample scripts are available in the [Automation Scripts](#) topic. The scripts are designed to assist you as follows:

Windows Script	Explanation
spcust_sample1.cmd	An example of configuring Secure+ Option for the STS protocol with the Secure+ CLI. The example demonstrates the use of statically generated public keys to facilitate an automated mass implementation of Secure+ Option.
spcust_sample2.cmd	An example of configuring Secure+ Option for the STS protocol with the Secure+ CLI. The example demonstrates the use of statically generated public keys to facilitate the automated addition of a remote node to a Connect:Direct network. A script based on this sample is used to configure the existing nodes in the network map. The remote node itself is configured with a script based on spcust_sample1. In order for the operation to be successful, the two scripts must use the same seeds to generate keys.
spcust_sample3.cmd	An example of configuring Secure+ Option to use the SSL or TLS protocol with the Secure+ CLI. The example demonstrates the configuration of Secure+ Option with the trusted root file, key certificates, and ciphers.

The following list describes the tasks necessary to write and implement the script for a mass implementation of an initial installation that uses the STS protocol. Excerpts from the `spcust_sample1` sample script are provided for reference.

1. Use the `Create STSKeyPair` command to generate a passphrase-protected file (default name: `keypair`) in the format that is already in use for importing and exporting public keys. In this key pair file, the private key is encrypted, but the public key is not. The public key string can be cut and pasted into `spcust_samplex` scripts for setting the remote keys for remote nodes.
2. Distribute the key pair file along with the `SPCLI` script when you distribute the installation to additional sites.
3. Use the `Update LocalNode` command to set the current key pair to the key pair stored in the key pair file. When using the key pair file to set the local keys in local and remote nodes, you need the key pair file name and its passphrase, as shown in the following example from the `spcust_sample1` script:

```
StsAuthlocalkey=set
StsAuthKeyPairFile=keypairfile
StsAuthKeyPairFilePassphrase=secret
StsSiglocalkey=set
StsSigKeyPairFile=keypairfile
StsSigKeyPairFilePassphrase=secret
```

4. For each remote node, use the `Update RemoteNode` command to set the public key that was generated in step 1. Copy the public key string from the key pair file and paste it into the script on the lines where the remote keys of all the remote nodes are set, as shown in this example from the `spcust_sample1` script:

```
update remotenode name=*
STSAuthRemoteKey=public key string
STSSigRemoteKey=public key string
```

5. Use the `Update LocalNode` command to generate a new key pair and save the existing key pair as the previous key pair value. For example, in `spcust_sample1`, after the authentication and signature keys were set to the ones stored in the key pair file generated in step 1, the `Update LocalNode` command was used again, as shown in the following example:

```
update localnode
stsauthlocalkey=gen
stsauthkeyseedType=dynamic
STSPrevAuthKeyExpDateTime=2005:01:01-20:13:44
stssiglocalkey=gen
stssigkeyseedType=dynamic
STSPrevSigKeyExpDateTime=2005:01:01-20:13:45
;
```

Note: The Secure+ CLI script is called `spcli.cmd`. Each command within the script must be terminated with a semicolon (;). Use the `quit` command to exit the `spcli.cmd` script.

Manage the Parameters File

The following table describes commands used to manage and maintain the parameters file from the command line interface.

Command	Description	Parameter	Values
Init Parmfile	Creates the parameters file. Must be initialized before you can define nodes.	localnode=Name of the local node where the parameters file will be created.	local node name
		path=Location where the parameters file will be created.	directory location For example, d_dir/ndm/secure+/node
		passphrase=Arbitrary set of a string at least 32 characters that encrypts the parameters file.	characters long
Open parmfile	Opens a parameters file so that you can configure it.	path=Location where the parameters file will be created.	directory location For example, d_dir/ndm/secure+/node
Close parmfile	Closes the parameters file. After this command is issued, no more updates can be performed on the parameters file.	None	None
Validate parmfile	Validates the parameters file and ensures that it is a valid file.	None	None
Rekey parmfile	Recreates the parameters file if it becomes corrupted.	passphrase=Arbitrary set of characters that encrypts the parameters file.	passphrase, up to 32 characters long
Sync netmap	Imports remote node records defined in the Connect:Direct network map.	path=Location and name of the network map file.	location of network map file
		name=Name of the node in the network map. Use wildcard characters to resync more than one node at a time.	node name wildcard Wildcard values are: Asterisk (*)—any number of characters. Example: kps.* syncs up all nodes with a name that starts with kps. Question mark (?)—a single character. Example: k?s.* syncs up kas.* and kbs.*

Displaying Information

The following commands are available to display information:

Command	Description	Parameter
display info	Displays information about when the parameters file was last updated.	None
display all	Displays all nodes in the parameters file.	None
display localnode	Displays the values defined in the .Local node record.	None

Command	Description	Parameter
display remotenode	Displays the values defined in remote node records.	<p>name—The name of the node to display information about.</p> <p>Use wildcard characters to display information about a group of remote node records. The options are:</p> <p>Asterisk (*)—Indicates any number of characters. For example, kps.* displays all nodes with a name that starts with kps.</p> <p>Question mark (?)—Indicates a single character. For example: k?s.* displays kas.* and kbs.*.</p>
display client	Displays the values defined in the .Client node record.	None
display seaserver	Displays the values defined in the .SEAServer record.	None

Update the .Local Node Record

The update localnode command configures the protocol for the .Local node record.

The update localnode command has the following parameters:

Parameter	Values
protocol=Protocol to use in the .Local node record.	sts tls ssl disable
override=Identifies if values in the remote node can override values defined in the .Local node record.	y n
AuthTimeout=Specifies the maximum time, in seconds, 0–3600 seconds that the system waits to receive the Connect:Direct control blocks exchanged during the Secure+ Option authentication process.	
StsEnableSig=Enables digital signatures.	y n
StsEnableAutoUpdate=Enables automatic update of public keys during authentication.	y n
StsLimitExportVersion=Identifies if a trading partner is using an earlier version of Secure+ Option designated as an export version.	y n
StsEnableEnc=Enables data encryption during the copy operation.	<p>y n algorithm (that is, the actual text string, “algorithm,” which is not case-sensitive).</p> <p>If y is selected, data encryption is enabled and the algorithm used depends on the merged value between the PNODE and SNODE. If the remote node enables encryption, the local node cannot disable it.</p> <p>If this parameter is set to algorithm, the algorithm must be defined in the StsEnableEncAlg parameter.</p>

Parameter	Values
StsEnableEncAlg=Acceptable data encryption algorithms to use when the Copy file encryption is requested. List in order of preference, with the most-preferred algorithm first.	DESCBC56 TDESCBC112 IDEACBC128
StsEncAlgs=Acceptable data encryption algorithms to use when encrypting control data during secure communications. List in order of preference, with the most-preferred algorithm first.	DESCBC56 TDESCBC112 IDEACBC128 all null all—Makes all valid algorithms available for use. null—Clears any existing values from the node definition. To enable more than one algorithm, use parenthesis to enclose all algorithms listed and a comma to separate each algorithm. For example, to enable two algorithms define the following parameter: StsEncAlgs=(DESCBC56, TDESCBC112)
StsAuthLocalKey=Generates or clears the authentication keys for the node.	gen clear set gen—Generates the authentication key. If this parameter is defined as gen, the StsAuthKeySeed value must be defined. clear—Clears the authentication key value. If this command is defined as clear, the StsAuthKeysToClear must also be specified. set—Sets the value of the authentication key to the value that you define in the StsAuthKeySeed parameter.
StsAuthKeyPairFile=Key pair file that contains a pair of public and private keys.	key pair file name
StsAuthKeyPairFilePassphrase=The passphrase specified when the key pair file is created.	alphanumeric string LCU:filename Note: For more information on using LCU files to mask plain text passwords in the Secure+ CLI, see Using the Local Connection Utility to Configure Encrypted Passwords.
StsAuthPreservePrev=Determines which authentication key values are saved.	y n
StsAuthKeySeedType=Identifies what type of key seed will be generated.	dynamic static value dynamic—The key seed is generated by the system each time. It is not necessary to define a value for the StsAuthKeySeed parameter. value—The key seed is generated based on the value defined in the StsAuthKeySeed parameter and changes each time the key is generated, even when the StsAuthKeySeed parameter is unchanged. static—the key seed is generated based on the value defined in the StsAuthKeySeed parameter. If the value of StsAuthKeySeed is not changed, the same Auth key is generated.
StsAuthKeySeed=An alphanumeric string used to generate the authentication keys. This value is required when StsAuthKeySeedType is defined as static or value.	alphanumeric string at least 32 characters
StsAuthKeysToClear=Identifies the authentication keys to clear.	previous current both

Parameter	Values
StsPrevAuthKeyExpDateTime=Specifies the date and time that the previous authentication key expires.	yyyy:mm:dd-hh:mm:ss The default value is 30 days.
StsSigLocalKey=Creates the signature keys for the node.	gen clear set gen—Generates the key. If this parameter is defined as gen, the StsSigKeySeed value must be defined. clear—Clears the key value. If this command is defined as clear, the StsSigKeysToClear must also be specified. set—Sets the value of the key to the value that you define in the StsSigKeySeed parameter.
StsSigKeyPairFile=Key pair file that contains a pair of public and private keys.	key pair file name
StsSigKeyPairFilePassphrase=Passphrase specified when the key pair file is created.	alphanumeric string LCU:filename Note: For more information on using LCU files to mask plain text passwords in the Secure+ CLI, see Using the Local Connection Utility to Configure Encrypted Passwords.
StsSigPreserveKey=Determines if previous signature key values are saved.	current previous
StsSigKeySeed=Alphanumeric string used to generate the signature keys. This value is required when StsSigKeySeedType is defined as static or value.	alphanumeric string at least 32 characters
StsSigKeySeedType=Identifies what type of key seed will be generated.	dynamic static value dynamic—The key seed is generated by the system each time. It is not necessary to define a value for the StsSigKeySeed parameter. value—The key seed is generated based on the value defined in the StsSigKeySeed parameter and changes each time the key is generated, even when the StsSigKeySeed parameter is unchanged. static—The key seed is generated based on the value defined in the StsSigKeySeed parameter. If the value of StsSigKeySeed is not changed, the same Sig key is generated.
StsSigKeysToClear=Identifies the signature keys to clear.	previous current both
StsPrevSigKeyExpDateTime=The date and time that the previous signature key expires.	yyyy:mm:dd-hh:mm:ss The default value is 30 days
SslTlsTrustedRootCertFile=The location of the trusted root certificate file to use for client connections.	location null null—Clears any existing values from the node definition.
SslTlsCertFile=Identifies the location of the certificate file to use	location null null—Clears any existing values from the node definition.

Parameter	Values
SslTlsCertPassphrase=The passphrase specified when the certificate is created.	alphanumeric password assigned when the key was generated LCU:filename Note: For more information on using LCU files to mask plain text passwords in the Secure+ CLI, see Using the Local Connection Utility to Configure Encrypted Passwords.
SslTlsEnableClientAuth=Enables client authentication in a .Client node record.	y n
SslTlsEnableCipher=Specifies the cipher suites enabled	name of a cipher suite null all all—Enables all ciphers. null—Clears any existing values from the node definition.
SslTlsEnableFipsMode=Turns on Sterling Crypto-C module that provides a FIPS 140-2 validated cryptographic module.	y n
SslTlsSeaEnable=Enables certificate validation by Sterling External Authentication Server.	y n
SeaCertValDef=Character string defined in Sterling External Authentication Server (SEAS).	character string null null—Clears any existing values from the node definition.

Manage Remote Node Records

This section contains the commands and parameters used to create, update, display, and delete remote node records.

Create a Remote Node Record

The create remotenode command creates a remote node record and configures the protocol settings. The command has the following parameters:

Parameter	Values
model=Name of an existing node to use as a model to copy from.	name of a valid remote node
Name=Name for the remote node record.	name
protocol=Protocol to use in the node record.	sts tls ssl disable DefaultToLN
override=Identifies if values in the copy statement can override values defined in the remote node record.	y n DefaultToLN
AuthTimeout=Specifies the maximum time, in seconds, that the system waits to receive the Connect:Direct control blocks exchanged during the Secure+ Option authentication process.	0–3600. The default is 120 seconds.
StsEnableSig=Enables digital signatures.	y n DefaultToLN
StsEnableAutoUpdate=Enables automatic update of public keys during authentication.	y n DefaultToLN

Parameter	Values
StsLimitExportVersion=Identifies if a trading partner is using an earlier version of Secure+ Option designated as an export version.	y n
StsEnableEnc=Enables data encryption during the copy operation.	y n DefaultToLN algorithm (that is, the actual text string, "algorithm," which is not case-sensitive). If y is selected, data encryption is enabled and the algorithm used depends on the merged value between the PNODE and SNODE. If the remote node enables encryption, the local node cannot disable it. If this parameter is set to algorithm, the algorithm must be defined in the StsEnableEncAlg parameter.
StsEnableEncAlg=Acceptable data encryption algorithms to use when the Copy file encryption is requested. List in order of preference, with most-preferred algorithm first.	DESCBC56 TDESCBC112 IDEACBC128
StsEncAlgs=Acceptable data encryption algorithms to use when encrypting control data during secure communications. List in order of preference, with most-preferred algorithm first.	DESCBC56 TDESCBC112 IDEACBC128 All null all—Makes all valid algorithms available for use. null—Clears any existing values from the node definition. To enable more than one algorithm, use parenthesis to enclose all algorithms listed and a comma to separate each algorithm. For example, to enable two algorithms define the following parameter: StsEncAlgs=(DESCBC56, TDESCBC112)
StsAuthLocalKey=Generates, clears, or sets the authentication keys for the node.	gen clear set gen—Generates the authentication key. If this parameter is defined as gen, the StsAuthKeySeed value must be defined. clear—Clears the authentication key value. If this command is defined as clear, the StsAuthKeysToClear must also be specified. set—Sets the value of the authentication key to the value that you define in the StsAuthKeySeed parameter.
StsAuthKeySeedType=Identifies what type of key seed will be generated.	dynamic static value dynamic—The system generates the key seed each time. It is not necessary to define a value for the StsAuthKeySeed parameter. value—The key seed is generated based on the value defined in the StsAuthKeySeed parameter and changes each time the key is generated, even when the StsAuthKeySeed parameter is unchanged. static—The key seed is generated based on the value defined in the StsAuthKeySeed parameter. If the value of StsAuthKeySeed is not changed, the same Auth key is generated.
StsAuthKeyPairFile=Key pair file that contains a pair of public and private keys for authentication.	key pair file name
StsAuthKeyPairFilePassphrase=	alphanumeric string
Passphrase specified when the key pair file is created.	

Parameter	Values
StsAuthKeySeed=An alphanumeric string used to generate the authentication keys. This value is required when StsAuthKeySeedType is defined as static or value.	alphanumeric string at least 32 characters long
StsAuthRemoteKey=The authentication keys used to authenticate the remote node or clear to clear the value of the remote key.	key value clear key value—The value assigned to the authentication key. clear—Clears the value of the authentication key. If clear is specified, the StsAuthKeysToClear must also be specified.
StsAuthKeysToClear=Identifies the authentication keys to clear.	previous current both
StsPrevAuthKeyExpDateTime=Identifies the date and time that the previous authentication key expires.	yyyy:mm:dd-hh:mm:ss
StsSigLocalKey=Creates the signature keys for the node.	gen clear set gen—Generates the key. If this parameter is defined as gen, the StsSigKeySeed value must be defined. clear—Clears the key value. If this command is defined as clear, the StsSigKeysToClear must also be specified. set—Sets the value of the key to the value that you define in the StsSigKeySeed parameter.
StsPrevSigKeyExpDateTime=The date and time that the previous signature key expires.	yyyy:mm:dd-hh:mm:ss
StsSigKeySeedType=Identifies what type of key seed will be generated.	dynamic static value dynamic—The key seed is generated by the system each time. It is not necessary to define a value for the StsSigKeySeed parameter. static—The key seed is generated based on the value defined in the StsSigKeySeed parameter and changes each time the key is generated, even when the StsSigKeySeed parameter is unchanged. value—The key seed is generated based on the value defined in the StsSigKeySeed parameter. If the value of StsSigKeySeed is not changed, the same Sig key is generated.
StsSigKeySeed=An alphanumeric string used to generate the signature keys. This value is required when StsSigKeySeedType is defined as static or value.	alphanumeric string at least 32 characters long
StsSigRemoteKey=The signature key used to authenticate the remote node or clear to clear the value of the remote key.	key value clear key value—The value assigned to the key. clear—Clears the value of the key. If clear is specified, the StsSigKeysToClear must also be specified.
StsSigKeyPairFile=Key pair file that contains a pair of public and private keys.	key pair file name
StsSigKeyPairFilePassphrase=Passphrase specified when the key pair file is created.	alphanumeric string

Parameter	Values
StsSigKeysToClear=Identifies the signature keys to clear.	previous current both
SslTlsTrustedRootCertFile=Location of the trusted root certificate file to use for client connections.	location null null—Clears any existing values from the node definition.
SslTlsCertFile=Identifies the location of the certificate file to use	location null null—Clears any existing values from the node definition.
SslTlsCertPassphrase=Passphrase specified when the certificate is created.	alphanumeric password assigned when the key was generated.
SslTlsEnableClientAuth=Enables client authentication in a .Client node record.	y n DefaultToLN DefaultToLN—Defaults to the setting specified in the .Local node record
SslTlsSeaEnable=Enables certificate validation by Sterling External Authentication Server.	y n DefaultToLN DefaultToLN—Defaults to the setting specified in the .Local node record
SeaCertValDef=Character string defined in Sterling External Authorization Server.	character string null null—clears any existing values from the node definition
SslTlsCertCommonName=The certificate common name defined in the certificate	name null null—Clears any existing values from the node definition.
SslTlsEnableCipher=The cipher suites enabled	name of a cipher suite all null all—Enable all ciphers. null—Clears any existing values from the node definition.

Update the Remote Node Record

The update remotenode command creates a remote node record and configures the protocol settings. The command has the following parameters:

Parameter	Values
Name=Name for the remote node record.	remote node name wildcard Use wildcard characters to update a group of remote node records. The options are: Asterisk (*)—Any number of characters. Example: kps.* displays remote nodes with a name that starts with kps. Question mark (?)—Single character. Example: k?s.* displays kas.* and kbs.*
protocol=The protocol to use in the node record.	sts tls ssl disable DefaultToLN
override=Identifies if values in the copy statement can override values defined in the remote node record.	y n DefaultToLN

Parameter	Values
AuthTimeout=Specifies the maximum time, in seconds, 0–3600 seconds that the system waits to receive the Connect:Direct control blocks exchanged during the Secure+ Option authentication process.	
StsEnableSig=Enables digital signatures.	y n DefaultToLN
StsEnableAutoUpdate=Enables automatic update of public keys during authentication.	y n DefaultToLN
StsLimitExportVersion=Identifies If a trading partner is using an earlier version of Secure+ Option designated as an export version.	y n
StsEnableEnc=Enables data encryption during the copy operation.	y n algorithm DefaultToLN <p>y—Enable data encryption. If y is selected, data encryption is enabled and the algorithm used depends on the merged value between the PNODE and SNODE. If the remote node enables encryption, the local node cannot disable it.</p> <p>n—Disable data encryption</p> <p>DefaultToLN—Use the values defined in the .Local node record.</p> <p>algorithm—The text string, “algorithm,” which is not case-sensitive. If this parameter is set to algorithm, the algorithm must be defined in the StsEnableEncAlg parameter.</p>
StsEnableEncAlg—Acceptable data encryption algorithms to use when the Copy file encryption is requested. List in order of preference, with most-preferred algorithm first.	DESCBC56 TDESCBC112 IDEACBC128
StsAuthLocalKeygenerates, clears, or sets the authentication keys for the node.	gen clear set <p>gen—Generates the authentication key. If this parameter is defined as gen, the StsAuthKeySeed value must be defined.</p> <p>clear—Clears the authentication key value. If this command is defined as clear, the StsAuthKeysToClear must also be specified.</p> <p>set—Sets the value of the authentication key to the value that you define in the StsAuthKeySeed parameter.</p>
StsEncAlgs=Acceptable data encryption algorithms to use when encrypting control data during secure communications. List in order of preference, with most-preferred algorithm first.	DESCBC56 TDESCBC112 IDEACBC128 All null <p>All—Sets all valid algorithms available for use.</p> <p>null—Clears any existing values from the node definition.</p> <p>To enable more than one algorithm, use parenthesis to enclose all algorithms listed and a comma to separate each algorithm. For example, to enable two algorithms define the following parameter: StsEncAlgs=(DESCBC56, TDESCBC112)</p>
StsAuthPreserveKey=Determines if the previous authentication key values are saved.	y n current previous
StsAuthKeysToClear=Identifies the authentication keys to clear.	current previous both

Parameter	Values
StsAuthKeySeedType=Identifies what type of key seed will be generated.	dynamic static value dynamic—The system generates the key seed each time. It is not necessary to define a value for the StsAuthKeySeed parameter. value—The key seed is generated based on the value defined in the StsAuthKeySeed parameter and changes each time the key is generated, even when the StsAuthKeySeed parameter is unchanged. static—The key seed is generated based on the value defined in the StsAuthKeySeed parameter. If the value of StsAuthKeySeed is not changed, the same authentication key is generated.
StsAuthKeySeed=An alphanumeric string used to generate the authentication keys. This value is required when StsAuthKeySeedType is defined as static or value.	an alphanumeric string at least 32 characters long
StsAuthRemoteKey=Authentication keys used to authenticate the remote node or clear to clear the value of the remote key.	key value clear key value—Value assigned to the authentication key. clear—Clear the value of the authentication key. If clear is specified, the StsAuthKeysToClear must also be specified.
StsPrevAuthKeyExpDate=Date and time that the previous authentication key expires.	yyyy:mm:dd-hh:mm:ss The default value is 30 days
StsAuthKeyPairFile=Key pair file that contains a pair of public and private keys.	key pair file name
StsAuthKeyPairFilePassphrase=Passphrase specified when the key pair file is created.	alphanumeric string
StsSigLocalKey=Creates the signature keys for the node.	gen clear set gen—Generates the key. If this parameter is defined as gen, the StsSigKeySeed value must be defined. clear—Clears the key value. If this command is defined as clear, the StsSigKeysToClear must also be specified. set—Sets the value of the key to the value that you define in the StsSigKeySeed parameter.
StsSigPreserveKey=Determines if previous signature key values are saved.	current previous
StsSigKeySeedType=Identifies what type of key seed will be generated.	dynamic static value dynamic—The key seed is generated by the system each time. It is not necessary to define a value for the StsSigKeySeed parameter. value—The key seed is generated based on the value defined in the StsSigKeySeed parameter and changes each time the key is generated, even when the StsSigKeySeed parameter is unchanged. static—The key seed is generated based on the value defined in the StsSigKeySeed parameter. If the value of StsSigKeySeed is not changed, the same Signature key is generated.

Parameter	Values
StsSigKeySeed=Alphanumeric string used to generate the signature keys. This value is required when StsSigKeySeedType is defined as static or value.	alphanumeric string at least 32 characters long
StsPrevSigKeyExpDateTime=Date and time that the previous signature key expires.	yyyy:mm:dd-hh:mm:ss The default value is 30 days
StsSigRemoteKey=Signature key used to authenticate the remote node or clear to clear the value of the remote key.	key value clear key value—The value assigned to the key. clear—Clears the value of the key. If clear is specified, the StsSigKeysToClear must also be specified.
StsSigKeysToClear=Identifies the signature keys to clear.	previous current both
StsSigKeyPairFile=Key pair file that contains a pair of public and private keys.	key pair file name
StsSigKeyPairFilePassphrase=Passphrase specified when the key pair file is created.	alphanumeric string
SslTlsTrustedRootCertFile=Location of the trusted root certificate file to use for client connections.	location null null—Clears any existing values from the node definition.
SslTlsCertFile=Identifies the Location of the certificate file to use.	location null null—Clears any existing values from the node definition.
SslTlsCertPassphrase=Passphrase specified when the certificate is created.	alphanumeric password assigned when the key was generated.
SslTlsEnableClientAuth=Enables client authentication in a .Client node record.	y n DefaultToLN DefaultToLN—Defaults to the setting specified in the .Local node record
SslTlsSeaEnable=Enables certificate validation by Sterling External Authentication Server.	y n DefaultToLN DefaultToLN—Defaults to the setting specified in the .Local node record
SslTlsCertCommonName=Certificate common name defined in the certificate	name null null—Clears any existing values from the node definition.
SeaCertValDef=Character string defined in Sterling External Authorization Server.	character string null null—clears any existing values from the node definition
SslTlsEnableCipher=Cipher suites enabled	name of a cipher suite null all all enables all ciphers. null—Clears any existing values from the node definition.

Display a Remote Node Record

The display remotenode command displays information about one or more remote node records. The command has the following parameter:

Parameter	Values
name=Name of the remote node record to display information about.	node name wildcard value To display information about more than one remote node record, use wildcard characters. Use wildcard characters to display information about a group of remote node records. The options are: Asterisk (*)—Any number of characters. Example: kps.* displays remote nodes with a name that starts with kps. Question mark (?)—A single character. Example: k?s.* displays kas.* and kbs.*.

Delete a Remote Node Record

The delete remotenode command deletes one or more remote node records. The command has the following parameter:

Parameter	Values
name=Name of the remote node record to display information about. Use wildcard characters to delete a group of remote node records.	remote node name wildcard value To display information about more than one remote node record, use wildcard characters. Use wildcard characters to display information about a group of remote node records. The options are: Asterisk (*)—Any number of characters. Example: kps.* displays remote nodes with a name that starts with kps. Question mark (?)—A single character. Example: k?s.* displays kas.* and kbs.*.

Manage the Sterling External Authentication Server Record

This section contains the commands and parameters used to update and display the .SEAServer record.

Update the Sterling External Authentication Server Record

The update seaserver command configures properties for Sterling External Authentication Server (SEAS) in the .SEAServer record that is created at installation. The command has the following parameters:

Parameter	Values
Protocol=Protocol to use in the .SEAServer record.	sts tls ssl disable DefaultToLN
SeaHost=External authentication host name defined in SEAS.	host name null null—Clears any existing values from the node definition
AuthTimeout=Specifies the maximum time, in seconds, that the system waits to receive the Connect:Direct control blocks exchanged during the Secure+ Option authentication process.	0–3600 seconds

Parameter	Values
Override=Identifies if values in the copy statement can override values y n DefaultToLN defined in the remote node record.	
SeaPort=External authentication server port number (listening) defined in SEAS.	port number 61366

Display the Sterling External Authentication Record

The display SEAServer command displays information about the .SEAServer record.

Maintain the .Password File (Strong Password Encryption)

This section contains the commands and parameters used to update and display the .Password file through the Connect:Direct Secure+ CLI.

Update the .Password File

The **Update Password** command enables or disables strong password encryption. The update goes into effect after you start the Connect:Direct server. The command has one parameter, SpeEnable, which can be set to Y or N to enable or disable strong password encryption. Following is an example:

```
Update Password
    SpeEnable=<Y>
;
```

If you enable or disable strong password encryption, the server displays the following warning:

The Connect:Direct Server must be restarted to update Strong Password Encryption.

Display the .Password File

The **Display Password** command displays the strong password encryption setting.

The **Display All** command displays the strong password encryption setting and .Password history.

Manage STS Keys Using the CLI

The commands and parameters in this section describe how to create, export, and import STS keys.

Create an STS Key Pair

The create STSKeypair command creates a key pair of public and private keys. The only required parameter is passphrase. The command has the following parameters:

Parameter	Values
KeyPairFile= File in which to store the encrypted key pair.	Valid file name. The default value is keypair.

Parameter	Values
passphrase=Arbitrary set of characters.	a string LCU:filename Note For more information on using LCU files to mask plain text passwords in the Secure+ CLI, see Appendix E, Using the Local Connection Utility to Configure Encrypted Passwords.
KeySeedType=Type of key seed to generate.	dynamic static dynamic—The key seed is generated by the system each time. static—The key seed is generated based on the value defined in the KeySeed parameter. If the value of KeySeed is not changed, the same key pair is generated.
KeySeed=Alphanumeric string at least 32 characters long used to generate the key pair. This parameter is required when static is specified for KeySeedType.	key seed value, at least 32 characters long
StsLimitExportVersion=Identifies If a trading partner is using an earlier version of Secure+ Optionn designated as an export version.	y n

Export STS Keys

The export STSKeys command allows you to export STS keys. The command has the following parameters.

Parameter	Values
dir=Directory in which to export the key file.	valid directory name
name=Name of the remote node record to export keys for. Use wildcard characters to export information about a group of remote node records.	remote node name wildcard Wildcard options are: Asterisk (*)—Any number of characters. For example, kps.* exports all nodes with a name that starts with kps. Question mark (?)—A single character. For example, k?s.* exports kas.* and kbs.*.

Import STS Keys

The import STSKeys command allows you to import STS keys. The command has the following parameter:

Parameter	Values
path=The directory and name of the file that contains the public keys.	valid path value

Automatically Create STS Keys for Remote Node Records

Before you can begin using Secure+ Option and the STS protocol for secure communications, you must exchange keys with the trading partner. To facilitate automatic configuration, you can now generate unique keys for a trading partner without the initial exchange of keys.

For information on using scripts to automatically update STS keys, see the Sample Scripts and Automation Scripts topics.

To create unique keys for the STS protocol and eliminate the need to exchange keys manually with a trading partner:

1. In the .Local node record for both locations, configure the same previous authentication key and the same previous digital signature key.
2. In the .Local node records, configure unique keys in the current authentication and current digital signature keys.
3. Configure every remote node record with the following information:
 - The same current authentication public key
 - The same current signature public key
4. Turn on auto update of public keys.

Turning on auto update causes the public keys in the remote node records to be automatically updated to the value in the current authentication field and the current signature public key field from the remote node.

Completing the procedure results in the following activity:

- When the first connection between the local and remote node occurs, STS authentication is performed based on the values defined in the previous authentication key.
- If authentication is successful, enabling auto update causes each node to automatically import the public authentication key and public signature key from the remote node record from control information exchanged on the communications link. It also updates the remote node record in the local parameters file.
- For subsequent connections, the newly imported keys are used for authentication.

Secure+ Option Node List

After you set up node records in Secure+ Option, you can view all of the nodes and their attributes from the Secure+ Admin Tool Main Window. From the Node Name list, you can view the record of an individual node by double-clicking on a node name.

The following table shows all the fields in the Node Name List:

Field Name	Description	Valid Values
Node Name	Displays the node record name.	.Local remote node name .client
Type	Displays the current record type.	L—Local record R—Remote record
Secure+	Displays the status of Secure+ Option	N—Disabled TLS—TLS protocol SSL—SSL protocol STS—STS protocol *—Default to local node
Override	Displays the status of override. Enable override in the local node to allow remote node records to override the settings in the local node record. If the STS protocol is enabled, enabling override in a remote node allows the values in the COPY statement to override key values in the remote node record.	Y—Enabled N—Disabled *—Default to local node
CipherSuites	Displays the TLS or SSL cipher suites that are enabled for the node record.	Varies, based on the cipher suites enabled.
ClientAuth	Displays the status of client authentication. If the TLS or SSL protocol is used, enabling client authentication means the SNODE verifies the identity of the PNODE.	Y—enabled N—Disabled *—Default to local node
Encryption	Indicates if encryption is enabled in the STS protocol.	Y—Enabled N—Disabled

Field Name	Description	Valid Values
Signature	Identifies if digital signature is enabled in the STS protocol.	Y—Enabled N—Disabled *—Default to local node
LimExpr	Identifies if the Limited Export version is being used by a remote node.	Y—Enabled N—Disabled *—Default to local node
AutoUpdate	Indicates if the option to automatically update key values during communication is enabled.	Y—enabled N—disable *—default to local node
Base Record	Displays the name of the base record for the alias records.	

View Secure+Option Parameters File Information

To view information about the Secure+ Option parameters file:

1. Open the Secure+ Admin Tool.
2. Click File > Info. The following fields are displayed in the File Information dialog box.

Field Name	Description
Current File	The name of the parameters file opened.
Number of Records	The number of nodes defined in the parameters file.
Number of Updates	How many times the parameters file has been updated.
Last 3 Updates	The name of the last three nodes updated.

View Secure+ Option Node Record Change History

To view the history of changes to a Secure+ Option node record:

1. From the Secure+ Option Admin Tool Main Window, double-click the node record name.
2. Click the Security Options tab.
The history of changes is displayed in the Update History field.

Disable Secure+ Option

You can use this procedure to disable all nodes in a configuration or one remote node.

1. Do one of the following:

- To disable all nodes in a configuration, open the local node record.
 - To disable one node, open the remote node record for that node.
2. Click the Security Options tab.
 3. Click Disable Secure+.
 4. Click OK to update the node record.
- Note:** In order to continue Connect:Direct operations with Secure+ Option disabled, both trading partners must disable Secure+ Option.

Delete a Secure+ Option Remote Node Record

If a remote node record is no longer defined in the network map, you can remove it from the parameters file. The following procedure deletes nodes that are defined in the Secure+ Option parameters file but not in the selected network map.

Caution: Do not delete the remote node record that is named for the Connect:Direct node. It is the base record for the .Local node record. You cannot delete the .Local node record.

1. From the Secure+ Admin Tool Main Window, click File > Sync with Netmap.
2. Click the network map to use from the pulldown list.
3. Click OK.
4. Click Skip to move through the Select Netmap Entries to the Add dialog box.
5. To delete node records, do one of the following:
 - To delete selected node records, highlight the remote nodes to delete and click Delete Selection.
 - To delete all remote node records not found in the network map, click Delete All.

Resecure Secure+ Option Parameters and Access Files

Routinely, or if your access file is compromised, perform the following steps to resecure Secure+ Option:

Caution: Do not type a new passphrase if an error occurs. If an error occurs while you are resecuring the files, restore the node records from the ACFSave directory. This directory is created after the Rekey Secure+ feature is executed.

1. From the Secure+ Admin Tool Main Window, click File > Rekey Secure+. The Rekey Secure+ dialog box is displayed.
2. Type an alphanumeric string of at least 32 characters in the Passphrase field. Secure+ Option uses the passphrase to re-encrypt the Secure+ Option parameters and access files. You do not have to remember this passphrase value.

3. Click OK to accept the new passphrase. The Secure+ Option decrypts and re-encrypts the parameters file and access file.

Change Cipher Suites

When you activate the TLS or SSL protocol for a node, cipher suites are used to encrypt the data being transmitted. The same cipher suite must be used at both ends of the transmission. Secure+ Option searches the enabled cipher suite list at both nodes and locates the first cipher suite that is common for communications at both the SNODE and the PNODE.

You enable the cipher suites in the preferred order, or enter them randomly and order them using the following procedure:

1. If necessary, open the Secure+ Option Admin Tool.
2. Double-click the node you want to edit.
3. Click the TLS/SSL Protocol tab.
4. If you are configuring a remote node, turn off Default to Local Node in the Cipher Suites section.
5. To modify cipher suites, do one of the following:
 - To enable a cipher suite, highlight it in the Available list and click Add.
 - To remove a cipher suite, highlight it in the Enabled list and click Remove.
 - To change a cipher suite's priority, highlight the cipher suite and click Up or Down until it is in the correct priority position.
6. Click OK.

Change STS Protocol Encryption Algorithms

When you activate the STS protocol for a node, it uses algorithms to encrypt the data being transmitted. The same algorithms must be used at both ends of the transmission.

Secure+ Option searches the enabled algorithm list and locates the first algorithm that is common for communications at both ends. You can enable the algorithms in the preferred order, or enter them randomly and order them using the following procedure:

1. If necessary, start the Secure+ Admin Tool.
2. Double-click the node you want to edit.
3. Click the STS Options tab.
4. Turn off Default to Local Node in the Encryption Algorithms section.
5. To modify algorithms, do one of the following:
 - To enable an algorithm, highlight it in the Available list and click Add.
 - To remove an algorithm, highlight it in the Enabled list and click Remove.

- To change the priority of an algorithm, highlight the item and click Up or Down until it is in the correct priority position.
6. Click OK.

Update Keys in an STS-Configured Node Record

To maintain communications with a trading partner when updating your keys, you must maintain a copy of the previous keys until your trading partner receives the updated keys.

If you and your trading partner both enable the Public Key Auto Updates feature in the parameters file, Secure+ Option uses the existing keys to establish a session and then creates new keys during authentication. The parameters files for you and your trading partner are automatically updated with the new key values.

To update signature and authentication keys:

1. Open the Secure+ Admin Tool.
2. Double-click the node record to update.
3. Click the STS Protocol tab.
4. Click the tab for the type of new keys you want to generate: Authentication Keys or Signature Keys.
5. Click Generate Key to create new public keys. A message asks if you want to save the current key pair as previous.
6. Click Yes to save the current key pair as the previous. The Generate Random Number Seed dialog box is displayed.
7. Do one of the following to generate a key:
 - Type an alphanumeric string of at least 32 characters in the Random Number Seed field and click OK. Secure+ Option uses the random number seed value to generate the authentication keys.
 - Click Sample Value, highlight all of the grid squares, and click OK to generate the random number seed.

The Public Keys window displays the populated Public Key field.

8. If necessary, type the expiration date in the Previous Key Pair Expiration Date field.
9. Click OK to save the changes to the parameters file.

Clear Keys in an STS-Configured Node Record

To clear the keys in an STS-configured node record:

1. Open the Secure+ Admin Tool.

2. Double-click the node record to update with key information.
3. Click the STS Protocol tab.
4. Click the tab for the type of new keys you want to clear: Authentication Keys or Signature Keys.
5. Click Clear Key.
6. Click the appropriate button for the type of keys to clear: Current, Previous, Both, or Cancel.

View Statistics

Connect:Direct logs statistics for Connect:Direct Process activity. The Connect:Direct statistics include Secure+ Option information for a Process. Connect:Direct information is included in the Process statistics information only when you attach to a Connect:Direct server.

Connect:Direct Requester Select Statistics

Use the Select Statistics function of Connect:Direct Requester to view the information about a Connect:Direct Process, including statistics information about a particular Process. If Secure+ Option is enabled, you view Secure+ Option fields by scrolling to the bottom of the Statistics Detail dialog box. Secure+ Option statistics are displayed in the Session Start Record (SSTR) and Copy Termination Record (CTRC).

For more information on using Connect:Direct Requester to view statistics information, see the Connect:Direct for Windows Help or the *Connect:Direct for Windows System Guide*.

The Secure+ Option fields and valid values available using the Select Statistics function of the Connect:Direct Requester are shown in the following table:

Field Name	Description	Valid Values
Secure+ Enabled	Specifies whether Secure+ Option is enabled.	Y N
Secure+ Protocol	Which protocol is enabled.	SSL 3.0 STS 1.0 TLS 1.0
Cipher Suite	Displays the cipher suite used during a session. cipher suite name, for example:	SSL_RSA_EXPORT_WITH_RC4_40_MD5
PNode Cipher List	Specifies the encryption algorithms available for the PNODE during the session.	IDEACBC128 TDESCBC112 DESCBC56
PNode Cipher	Specifies the preferred data encryption as specified in the Secure+ Option parameters file of the PNODE.	Y N algorithm name
SNode Cipher List	Specifies the encryption algorithms available for the SNODE during the session as specified in the Secure+ Option parameters file of the SNODE.	IDEACBC128 TDESCBC112 DESCBC56

Field Name	Description	Valid Values
SNode Cipher	Specifies the preferred data encryption algorithm as defined in the Secure+ Option parameters file of the SNODE.	Y N algorithm name
Control Block Cipher	Specifies the algorithm used for encrypting control blocks. This value is determined during authentication when the PNODE and SNODE are merged.	IDEACBC128 TDESCBC112 DESCBC56
Copy Data Cipher	Specifies the encryption method used for encrypting data. The value is determined after the values in the SNODE and the PNODE are merged.	IDEACBC128 TDESCBC112 DESCBC56
PNODE Signature Enabled	Indicates whether digital signatures are enabled for the PNODE. This value is obtained from the Secure + Option parameters file settings. If the COPY statement overrides the Secure+ Option parameters file, the value from the COPY statement is used.	Y N
SNODE Signature Enabled	Indicates whether digital signatures are enabled for the SNODE. This value is obtained from the Secure + Option parameters file settings.	Y N
Signature Enabled	Identifies the digital signature value used for a copy operation. In the Session Start record, this value is the result of the merged value between the PNODE and SNODE. In the Copy Termination record, if the COPY statement overrides the parameters file value, the merged value depends on the value supplied in the COPY statement. (The unprocessed value from the COPY statement is recorded in the Signature Enabled field of the PNODE).	Y N
Current Signature Verified	Indicates whether the current digital signature was verified.	Y N
Previous Signature Verified	Indicates whether the previous digital signature was verified.	Y N

Connect:Direct CLI Select Statistics Detail

When you use the CLI Select Statistics function to view the information about a Connect:Direct Process, you see statistics information about a particular Process. The Connect:Direct fields are shown in bold in the following samples.

Session Start (SSTR) Record

The following sample Session Start Record (SSTR) displays the output of an SSL session:

```
Record Id      => SSTR
Process Name   =>
Process Number => 0
Submitter Id  =>
Start Time    => 15:23:20
Stop Time     => 15:23:21
Stat Log Time => 15:23:21
Stat Log Date => 10/16/2009
Start Date    => 10/16/2009
Stop Date     => 10/16/2009
```

```

SNODE          => JKTIB8100
Completion Code => 0
Message Id     => LSMI004I
Message Text   => PNODE session started - remote node &NODE
Secure+ Protocol => SSL 3.0
SSL Cipher Suites => SSL_RSA_WITH_RC4_128_MD5
-----

```

Copy Termination (CTRC) Record

The Copy Termination Record (CTRC) sample below uses the SSL protocol:

```

Record Id      => CTRC
Process Name   => XX           Stat Log Time => 15:26:32
Process Number => 195          Stat Log Date => 10/16/2009
Submitter Id  => user1
Start Time    => 15:23:47    Start Date    => 10/16/2009
Stop Time     => 15:26:32    Stop Date     => 10/16/2009
SNODE        => DLAS8100
Completion Code => 0
Message Id    => SCPA000I
Message Text  => Copy operation successful.
COPY DETAILS: Ckpt=> Y Lkfl=> N Rstr=> N XLat=> N Scmp=> N Ecmp=> N
From node    => S
Src File     => D:\long path
Dest File    => D:\long path
Src CCode    => 0           Dest CCode    => 0
Src Msgid    => SCPA000I    Dest Msgid    => SCPA000I
Bytes Read   => 23592960    Bytes Written => 23592960
Records Read => 1024        Records Written => 1024
Bytes Sent   => 23791420    Bytes Received => 23791420
RUs Sent     => 30721       RUs Received  => 30721
Secure+ Protocol => SSL 3.0
SSL Cipher Suites => SSL_RSA_WITH_RC4_128_MD5
-----

```

Connect:Direct CLI Select Process Detail

When you use the CLI select process command to view information about a Connect:Direct Process, you see statistics about a Process. The following sample Select Process Detail uses the STS protocol. If Secure+ Option is not enabled, no Secure+ information is displayed:

```

Process Name   => XX           Class         => 32
Process Number => 197          Priority      => 10
Submitter Node => DALLAS       PNode        => DALLAS
Submitter     => user1       SNode        => DALLAS
Retain Process => N
Submit Time   => 15:55:55    ScheduleTime =>
Submit Date   => 10/19/2009 ScheduleDate  =>
Queue        => EXEC
Process Status => EX
Message Text  =>
Function     => COPY
Step Name    => TWO
Type        => Send
File Bytes   => 3202560       File Recs    => 0
Xmit Bytes   => 3247926       Xmit Buffers => 0
Secure+ Protocol => STS 1.0
Ctrl Block Cipher => TDESCB112
Copy Data Cipher => IDEACBC128
Signature Enabled => Y
-----

```

Secure+ Option Parameters File Auditing

The Secure+ Option Administration Tool (Secure+ Admin Tool) and the Secure+ Option Command Line Interface (Secure+ CLI) log changes made to the Secure+ Option parameters file.

The following events are logged:

- Application Startup
- Init Parmfile
- Open Parmfile
- Sync Netmap
- Rekey Parmfile
- Create Node
- Update Node
- Delete Node

The parameters file logging feature has the following operational characteristics:

- The logging feature is always enabled and cannot be disabled.
- If errors occur when the log is being updated, the application terminates.
- Each log entry contains a timestamp, user ID, and a description of the action/event.
- When an existing node is updated, any changed fields are reported.
- When a node is created or deleted, the values of all non-empty fields are reported.
- Any commands that modify a node are logged.

Accessing Parameters File Audit Logs

The parameters file audit logs are stored in a dedicated directory, `..\secure+\log`. The log file naming convention is `SP[YYYY][MM][DD].001` (using local time), and the contents of a log file are limited to a single calendar date. You can view these log files using any text editor. Log files are not deleted by Secure+ Option.

Parameters File Audit Log Entries

Each audit log has the following header:

```
[YYYYMMDD][HH:MM:SS:mmm][userid]
```

When a parameter file is created or opened, an ID is generated that associates the change with the node being updated, as shown in the following:

```
[YYYYMMDD][HH:MM:SS:mmm][userid][ParmFileID]
```

The following fields may appear in a create, update, or delete audit record.

Field Name	Description
Name	Name of the node
BaseRecord	Name of the base record
Type	Record type of local, remote, or alias
Protocol	Enables Secure+ Option protocol
Override	Enables overriding the current node
AuthTimeOut	Authentication timeout
StsEnableSig	Enable STS signatures
StsEnableAutoUpdate	Enable STS auto update remote public keys
StsEnableEnc	Enable STS copy encryption stream
StsEncAlgs	Enable STS control block encryption streams
StsAuthLocalKey	STS authentication local public key
StsAuthRemoteKey	STS authentication remote public key
StsPrevAuthKey	STS authentication previous private key (masked)
StsPrevAuthKeyExpDateTime	STS authentication previous private key expiration date
StsSigLocalKey	STS signature local public key
StsSigRemoteKey	STS signature remote public key
StsPrevSigKey	STS signature previous private key (masked)
StsPrevSigKeyExpDateTime	STS signature previous private key expiration date
SslTlsTrustedRootCertFile	Pathname to trusted roots file
SslTlsCertFile	Pathname to key certificate file
SslTlsCertPassphrase	Key certificate passphrase (masked)
SslTlsEnableClientAuth	Enable client authentication
SslTlsCertCommonName	Common name of the remote certificate to verify
SslTlsEnableCipher	List of SSL/TLS cipher suites
SslTlsSeaEnable	Enable external authentication
SeaCertValDef	External authentication validation definition
SeaHost	External authentication host name
SeaPort	External Authentication port number

Parameters File Audit Log Error Reporting

Errors are reported for the following logging functions: open log, write log, and lock log. If an error occurs during one of these functions, an error message is displayed and the application is terminated. The lock function times out after 30 seconds. Typically, Secure+ Admin Tool or the Secure+ CLI hold the lock for less than one second per update.

Secure+ Option Certificate Auditing

In an SSL/TLS session, audit information about the identity certificate and its signing certificate is logged in the statistics log in the Session Start (SSTR) and Copy Termination (CTRC) records. The audit information is included in the response data from a Select Statistics command in the SSTR and CTRC records.

In an SSL/TLS session, the PNODE (client) always logs the audit information. The SNODE (server) only logs the information when client authentication is enabled. For logging to occur, the session handshake must succeed and progress to the point of logging the SSTR and CTRC records.

Certificate Audit Log Entries

The audit consists of the subject name and serial number of the identity and its signing certificate. The identity certificate also contains an issuer attribute, which is identical to the signing certificate subject name. Although many signing certificates may exist between the identity and final root certificate, the audit includes only the last two certificates in a chain: an intermediate certificate and an end certificate.

In the SSTR and CTRC records, the CERT contains the common name and serial number of the key certificate, and the CERI contains the common name of the issuer and the serial number of an intermediate or root CA. They may also contain the certificate serial number, for example:

```
CERT=(/C=US/ST=MA/L=Marshfield/O=test.org/OU=Dev/CN=Test ID/SN=99c0ce01382e6c83) |
CERI=(/C=US/ST=MA/L=Marshfield/O=test.org/CN=root CA/SN=da870666bbfb5538)
```

Secure+ Option certificate audits may contain the following fields:

Field Name	Abbreviation	Max Lengths (RFC 2459)
Common Name	CN	64
Country	C	2
Locality	L	128
State	ST	128
Organization	O	64
Organization Unit	OU	64
Email Address	emailAddress	128
Serial Number	SN	128 (estimated)

Accessing Certificate Audit Logs

Certificate audit information located in the SSTR and CTRC records cannot be accessed directly using Connect:Direct Requester or Connect:Direct Browser User Interface. To access certificate information, you can issue a query directly to the database or use an SDK-based or JAI-based program to issue a Select Statistics command. The response to the Select Statistics command contains the AuditInfo field of the statistics records, including the SSTR and CTRC records. This field contains certificate audit information.

The following example was generated using a database query.

```
'2009-05-21 14:50:27', 2, 'SSTR', 'CAEV', '', 0, '2009-05-21 14:50:26',
'2009-05-21
```

```

14:50:27', '', '', 'JLYON-XP.4500', 0,
'MSGI=LSMI004I|SBST=(&NODE=JLYON-XP.4500)|PNOD=JLYON-XP.4500|CSPE=Y|CSPP=TLsv1|
CSPS=
TLS_RSA_WITH_AES_256_CBC_SHA|
CERT=(/C=US/ST=MA/L=Marshfield/O=test.org/OU=Dev/
CN=Example Test ID/SN=a9febbeb4f59d446)|
CERI=(/C=US/ST=MA/L=Marshfield/O=test.org/OU=Dev/CN=Example
IntermediateCA/SN=a69634a8a7830268)|STSD=2|TZDI=-14400|
'2009-05-21 14:50:28', 2, 'CTRC', 'CAPR', 'SAMPLE', 1, '2009-05-21 14:50:27',
'2009-05-21 14:50:28', 'JLYON-XP.4500', 'jlyon', 'JLYON-XP.4500', 0,
'MSGI=SCPA000I|LCCD=0|LMSG=SCPA000I|OCCD=0|OMSG=SCPA000I|PNAM=SAMPLE|PNUM=1|
SNAM=STE
P1|SBND=JLYON-XP.4500|SBID=jlyon|PNOD=JLYON-XP.4500|SNOD=JLYON-XP.4500|LNOD=P|
FROM=P
XLAT=N|ECZI=N|ECMP=N|SCMP=N|OERR=N|CKPT=Y|LKFL=N|RSTR=N|RUSZ=65535|PACC=|SACC=|
PPMN
|=|SFIL=C:\Program Files\Sterling Commerce\Connect Direct
v4.5.00\Server\Process\Sample.html|SDS1=|SDS2=|SDS3=
|SFSZ=0|SBYR=861|SRCR=1|SBYX=863|SRUX=1|SNVL=-1|SVOL=|DFIL=C:\Program Files
\Sterling
Commerce\Connect Direct v4.45.00\Server\Process\Verify.html|PPMN=|DDS1=R|DDS2=|
DDS3=
|DBYW=861|DRCW=1|DBYX=863|DRUX=1|DNVL=0|DVOL=|CSPE=Y|CSPP=TLsv1|
CSPS=TLS_RSA_WITH_AES
S_256_CBC_SHA|CERT=(/C=US/ST=MA/L=Marshfield/O=test.org/OU=Dev/CN=Example Test
ID/SN=a9febbeb4f59d446)|CERI=(/C=US/ST=MA/L=Marshfield/O=test.org/OU=Dev/
CN=Example Intermediate CA/SN=a69634a8a7830268)
|PCRC=N|ETMC=60|ETMK=10|ETMU=0|STSD=2|TZDI=-14400|'

```

Certificate Audit Log Error Reporting

If an error occurs when the subject name is extracted from the identity (CERT) or issuer's (CERI) certificates, the following message ID is logged:

```
CERT=(MSGI=CSPA310E)|CERI=(MSGI=CSPA310E)
```

Only the message ID is displayed with the CERT or CERI tokens; the standard Connect:Direct error function is not used. After the error occurs, the session continues.

Troubleshoot Secure+

Troubleshooting

Use the following table to help troubleshoot problems with Secure+ Option.

Problem	Possible Cause	Solution
Secure+ Option features are enabled in the parameters file, but the statistics record indicates that these functions are disabled.	The Connect:Direct network maps do not contain entries for the PNODE and SNODE.	Verify that the netmap entries for both the PNODE and the SNODE exist.
Running a Process with a remote node fails with an authentication error.	Unique public/private key pairs are generated for the remote node record and the .Local node record is set to Enable Override=N.	Change the .Local node record to Enable Override=Y.
The Secure+ Option parameter, ENCRYPT.DATA, specified from the COPY statement causes the copy step to fail with error message CSPA080E.	The algorithm name used in the COPY statement is not in the supported algorithm list for both nodes.	Verify that the algorithm name in the COPY statement is in the supported algorithm list for both nodes.
Secure+ Option is installed, but error message CSPA001E occurs on non-Secure+ Option transfers.	Remote node records do not exist.	<ul style="list-style-type: none"> A remote node record must exist for every node in the netmap. Use the Sync with Netmap feature to create any missing nodes. Disable Secure+ Option by clicking Disable Secure+ in the .Local node record.
Signature verification fails with error message CSPA002E.	Configuration settings missing or incorrect.	<ul style="list-style-type: none"> If this is a non-Secure node, make sure the remote node record has Disable Secure+ selected. Check the Secure+ Option settings for the node.
Signature verification fails with error message CSPA003E, CSPA004E, or CSPA005E.	<ul style="list-style-type: none"> Configuration settings missing or incorrect. A security attack in progress. 	<ul style="list-style-type: none"> Correct the STS settings for the remote node. Execute standard operating procedure for investigating security violation.

Problem	Possible Cause	Solution
Signature verification fails with error message CSPA007E.	Expired Signature Key Pair. Date exceeded or keys have been changed.	If Auto Update is disabled, check the expiration date for the signature key pair for both nodes. Check the update history log on both nodes for the last change to the record. Verify that the signature public key is correct for both nodes.
Running a Process with a remote node fails with an authentication error, CSPA008E.	Authentication Key Pair Expiration Date exceeded or keys have been changed.	If Auto Update is disabled, check the authentication previous key pair expiration date for both nodes. Check the update history log on both nodes for the last change to the record. Verify the authentication public key is correct for both nodes.
Strong authentication fails with the error, CSPA010E.	<ul style="list-style-type: none"> The time allowed for strong authentication expired. A security attack in progress. 	<ul style="list-style-type: none"> Increase the timeout value. Execute standard operating procedure for investigating security violation.
Secure+ Option session fails with the error, CSPA011E.	An illegal attempt to override Secure+ Option parameters.	<ul style="list-style-type: none"> Turn on Enable Override in the remote node record to allow the COPY statement to override the node settings. Check the COPY statement and remove the override statements.
Secure+ Option session fails with the error, CSPA014E.	Secure+ Option cannot read the remote node definition.	Check the remote node definition settings.
Secure+ Option session fails with the error, CSPA016E.	Secure+ Option is not enabled in the local node definition.	Make sure Secure+ Option is enabled for the local node.
Secure+ Option session fails with the error, CSPA019E.	Error generating digital signature.	<ul style="list-style-type: none"> Resubmit the Process. Call Sterling Commerce Customer Support.
Secure+ Option session fails with the error, CSPA077E.	The COPY statement requested Secure+ Option parameters but Secure+ Option is not configured.	Remove the SECURE= parameter from the COPY statement.
Secure+ Option session fails with the error, CSPA079E.	Invalid encryption algorithm identified in COPY statement.	Change the ENC.DATA parameter and specify one of the following values: Y, N, IDEACBC128, TDESCBC112, or DESCBC56 and resubmit the Process.
Secure+ Option session fails with the error, CSPA080E.	No common algorithms are available for both nodes.	Verify the algorithm list for both nodes contains at least one common algorithm name.
Secure+ Option session fails with the error, CSPA091E.	Session attempted but remote node is not configured.	Make sure both nodes are defined and Enable STS Protocol is selected for the remote node record.

Problem	Possible Cause	Solution
Secure+ Option session fails with the error, CSPA200E.	Both nodes are not configured for the same protocol.	<ul style="list-style-type: none"> • Check the protocol setting at both sites and verify that the same protocol is configured at each site. • If necessary, edit the remote node record and activate the STS protocol.
Secure+ Option session fails with the error, CSPA202E.	SSL or TLS protocol handshake failed.	Edit the cipher suite list and add a cipher suite used by the trading partner.
Secure+ Option session fails with the error, CSPA203E or CSPA204E.	The SSL or TLS protocol could not validate the server's certificate.	Make sure the certificate information is typed into the node record.
Secure+ Option session fails with the error, CSPA205E.	A trading partner is not using TCP/IP for communication.	Make sure that both ends of the communication use TCP/IP.
Secure+ Option session fails with the error, CSPA206E.	The SSL or TLS protocol could not validate the server's certificate.	Make sure the certificate information is entered into the node record.
Secure+ Option session fails with the error, CSPA208E.	The common name in the certificate received does not match the Secure + Option configuration.	Make sure the certificate common name is spelled correctly and uses the same case as that in the certificate.
Secure+ Option session fails with the error, CSPA209E.	The certificate has expired or is invalid.	Obtain a new certificate and reconfigure the node record.
Secure+ Option session fails with the error, CSPA210E.	The COPY statement attempts to override settings in the STS protocol.	If desired, change the Process statement and remove the COPY override options.
Secure+ Option session fails with the error, CSPA211E.	The remote trading partner failed to send a certificate.	Notify the trading partner that a certificate is required.
Secure+ Option session fails with the error, CSPA280E.	The trusted root certificate could not be loaded.	Check the local node configuration and make sure the location of the trusted root certificate is correctly identified.
Secure+ Option session fails with the error, CSPA281E.	The trusted root certificate is empty.	Check the local node configuration and make sure the location of the trusted root certificate is correctly identified.
Secure+ Option session fails with the error, CSPA282E.	The user certificate file cannot be loaded.	Check the local node configuration and make sure the location of the user certificate file is correctly identified.
Secure+ Option session fails with the error, CSPA303E.	The parameters files have not been initialized.	Run the Admin Tool to initialize the parameters files.
Secure+ Option session fails with the error, CSPA309E.	The SSL library failed during the handshake.	Examine all related errors to determine the cause of the failure.
Secure+ Option session fails with the error, CSPA311E.	Certificate validation failed.	Verify that the root certificate is properly configured. An alternate certificate may be required.

Configuration Worksheets

Local Node Security Feature Definition Worksheet

Record the security definitions for the local Connect:Direct node.

Local Node Name

Configured Security Functions

- Enable TLS protocol (Yes | No)
- Enable SSL protocol (Yes | No)
- Authorization Timeout
- Trusted Root Certificate File location
- Certificate File
- Certificate Passphrase
- Cipher Suite(s) Enabled

External Authentication

- Enable External Authentication (Yes | No)
 - Certificate Validation Definition
-

Remote Node Security Feature Definition Worksheet

Make a copy of this worksheet for each remote node defined in the Secure+ Option parameters file that you are configuring for Secure+ Option operations. Record the security feature definitions for a remote node record on this worksheet.

Remote Node Name

Security Options

- Protocol defined in the .Local node record (TLS | SSL)
 - Is the remote node using the protocol defined in the .Local node record? (Y | N)
 - If you answered No to the question above, identify the protocol to use for the Remote Node (TLS | SSL)
 - Enable TLS protocol (Y | N)
 - Enable SSL protocol (Y | N)
 - Enable STS protocol (Y | N)
 - To use the same protocol defined in the local node, select Default to Local Node.
 - Enable Override (Y | N)
- Note:** To use the COPY statement to override settings in the parameters file for STS-enabled nodes, set Enable Override for the remote node. The COPY statement cannot override settings in SSL-enabled or TLS-enabled remote nodes.
- Authorization Timeout

TLS or SSL Protocol Functions

- Trusted Root Certificate File location
- Certificate File
- Certificate Passphrase
- Cipher Suite(s) Enabled
- Enable Client Authentication (Y | N | Default to local node)
- Certificate Common Name)

Note: If you want to add a second level of security, enable client authentication for the remote node and type the certificate common name.

External Authentication

- Enable External Authentication (Y | N | Default to local node)
 - Certificate Validation Definition
-

Certificate File Layout

Certificate File Layout

The SSL and TLS security protocols use a secure server RSA X.509V3 certificate to authenticate your site to any client that accesses the server and provides a way for the client to initiate a secure session. When you obtain a certificate file from a certificate authority or create a self-signed certificate, a trusted root certificate file and key file are created.

Secure+ Option uses two certificate files to initiate TLS or SSL sessions: a trusted root certificate file and a key certificate file.

When you obtain a root certificate from a certificate authority, you receive a trusted root certificate file. To configure Secure+ Option, add the name and location of the trusted root certificate file to the node record using the Secure+ Admin Tool.

A sample trusted root certificate file called `trusted.txt` is installed in the `Secure+\certificates` directory when you install Secure+ Option. Use any text editor to add or delete certificate information to this file. In simple configurations, only one trusted root certificate file is used. In more sophisticated configurations, you may associate individual certificate files with one or more node records.

When you use a certificate signing request (CSR) tool, such as the Certificate Wizard, you do not need to change the contents of the key certificate file. This is created for you by the Certificate Wizard.

If you set up your own PKI infrastructure, you may chain more than two certificates, including a CA root certificate, one or more intermediate CA certificates, and an identity certificate. You can create chained certificates using one of the following methods:

- Using the Local Key Certificate File—In a chain of two certificates, the local key certificate file contains a private key and an identity certificate. In a longer chain, the key certificate file contains the private key and the identity key, followed by the intermediate CA certificates.
- Using the Remote Trusted File— In a chain of two certificates, the remote trusted file contains the CA root certificate. In a longer chain, the remote trusted file contains the CA root certificate and all the intermediate CA certificates.

General Object Format

All objects are formatted in the Privacy Enhanced Mail (PEM) style, beginning with a line in the following format:

```
-----BEGIN <object>-----
```

and ending with a line in this format:

```
-----END <object>-----
```

In the above examples, <object> is a placeholder for the name of the object type: CERTIFICATE or ENCRYPTED PRIVATE KEY.

Certificate Format

A certificate is encoded as a general object with the identifier string CERTIFICATE or X.509 CERTIFICATE. The base64 data encodes a Bit Error Rate (BER)-encoded X.509 certificate. This is the same format used for PEM. Anyone who provides or understands PEM-format certificates can accommodate the certificate format. For example, VeriSign commonly fulfills certificate requests with certificates in this format, SSLeay supports them, and SSL servers understand them. Most browsers support this format for importing root CA certificates.

Private Key Format

A private key is encoded as a general object with the identifier string ENCRYPTED PRIVATE KEY. The base64 data encodes a BER-encoded PKCS#8 Private Key object. The passphrase associated with the Private Key is required for Secure+ Option and is stored in the Secure+ Option parameters file. Additional encryption is used to prevent the passphrase from being discovered.

Sample Certificate Files

In the sample user certificate below, a private key is followed by the server certificate, which is followed by the root certificate.

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICDAaBgkqhkiG9w0BBQMwDQIIIfYyAEFKaEECAQUEggHozdmGz7zbC1mcJ2r
.
.
.
IGpupStY5rLqqQ5gwLn45UWgzy6DM96CQg6+Dyn0N9d1M51Ig2wlnUwE8vI=
-----END ENCRYPTED PRIVATE KEY-----
User/Server Certificate
-----BEGIN CERTIFICATE-----
MIICUDCCAdoCBDAmltYwDQYJKoZIhvcNAQEEBQAwwY8xCzAJBgNVBAYTAlVTMRMw
.
.
.
iKlsPBRbNdq5cNIuIfPS8emrYMs=
-----END CERTIFICATE-----
// Final Root Certificate (optional)
-----BEGIN CERTIFICATE-----
MIICUDCCAdoCBDAmltYwDQYJKoZIhvcNAQEEBQAwwY8xCzAJBgNVBAYTAlVTMRMw
.
.
.
iKlsPBRbNdq5cNIuIfPS8emrYMs=
-----END CERTIFICATE-----
```

In the sample root certificate below, the trusted.txt file contains a list of trusted root certificates.

```
RSA Commercial CA - exp. Dec 31, 2003
-----BEGIN CERTIFICATE-----
MIICUDCCAdoCBDAmltYwDQYJKoZIhvcNAQEEBQAwwY8xCzAJBgNVBAYTAlVTMRMw
.
.
.
```



```
iKlsPBRbNdq5cNIuIfPS8emrYMs=  
-----END CERTIFICATE-----  
RSA Commercial CA - exp. Dec 31, 2010  
-----BEGIN CERTIFICATE-----  
MIICUDCCAdoCBDaMltYwDQYJKoZIhvcNAQEEBQAwwY8xCzAJBgNVBAYTAlVTMRMw  
.  
.  
iKlsPBRbNdq5cNIuIfPS8emrYMs=  
-----END CERTIFICATE-----
```

Test Secure+ with STS

Set Up the Local and Remote Node Records for Testing

Before using the STS protocol in a production environment, test the installation to ensure Secure+ Option is operational.

The parameters file is initially populated with two node records: the .Local record and a remote record for the associated Connect:Direct node. The remote record for this local node is created to support loopback (PNODE=SNODE) processing to test Secure+ Option. To test the Secure+ Option installation, you need to configure the sample .Local node record and remote node record.

1. Click Start > Programs > Sterling Commerce Connect Direct v4.5.00>Secure+ Option Admin Tool.
2. To configure the .Local node record, double-click .Local. The Edit Record dialog box opens to the Security Options tab.
3. Change the Security Options values (for the local or remote node record) as follows:

Field	Local Node Setting	Remote Node Setting
Secure+ Protocol	Enable STS Protocol	Enable STS Protocol
Node or Copy Statement Override	Enable Override	Default to Local Node
Authentication Timeout	90	90

4. Click the STS Protocol tab. The Edit Record - STS Protocol window displays the STS Options.
5. On the STS Options tab, click the following values:

Field	Local Node Setting	Remote Node Setting
Enable Digital Signatures	Yes	Default to Local Node
Enable Public Key Auto Updates	No	Default to Local Node
Enable Encryption	Yes	Default to Local Node

6. Click the Authentication Keys tab.
7. Generate the authentication keys as follows:
 - Click the Generate Key button. The Generate Random Number Seed dialog box is displayed.

- Type an alphanumeric string of at least 32 characters in the Random Number Seed field and click OK.
8. Click the Signature Keys tab.
 9. Generate the signature keys as follows:
 - Click the Generate Key button. The Generate Random Number Seed dialog box is displayed.
 - Type an alphanumeric string of at least 32 characters in the Random Number Seed field and click OK.

The Secure+ Option Admin Tool generates the Signature keys and populates the Local Public Key field.
 10. Click OK to save the changes.

Exchange Public Keys

To complete the setup for testing the STS protocol, you need to exchange public keys. In a production environment, you create and configure a remote node for each trading partner. Then you export keys from the remote node and send this information to the trading partner. Finally, you import keys that the trading partner sends to you into the remote node record.

Export Keys

The first step to exchange keys is to export the keys of the remote node. Exporting keys copies the public keys to a file that can be sent to the trading partner.

To export the remote node key:

1. Create a specific directory for storing the public key files.
2. From the Secure+ Admin Tool Main Window, highlight the remote node record. Then click Key Management > Export Selection. The Select Export Destination Directory dialog box is displayed.
3. Click Select and save the key file to the directory you created in step 1. A file with an `sxp` extension is created for the remote node entry for this local node. The file is named after the local node.

Import Keys

When you are ready to import keys, have your trading partner send this file to your production environment. However, for test purposes, use the information you exported from the Export Keys process.

1. From the Secure+ Admin Tool Main Window, highlight the remote node record and click Key Management > Import Public Keys. The Select Import Source File dialog box is displayed.
2. Go to the directory where you saved the `sxp` file.

3. Highlight the `sxp` file for this node and click Import. The key is imported to the remote node record.
4. Ensure that the remote keys are imported by viewing the Remote Public Key field located in the Authentication Keys tab and Signature Keys tab.

Note: The remote node public keys are not displayed in the `.Local` node record, but are displayed in the base remote node record.

Validate the Configuration

Perform this procedure to ensure that the nodes have been properly configured. The validation process checks each node to ensure that all necessary options have been defined and keys have been exchanged.

To validate the parameters file:

1. In the Secure+ Admin Tool, click File > Validate Secure+. The Secure+ Admin Tool - Validation Results window is displayed.

If the parameters file is not correctly configured, warning and error messages are displayed.

2. Read each warning message. To correct each warning or error reported, go back to the parameters file and make changes as needed.

Note: Warning messages do not always mean that the parameters file is incorrectly configured. Some warning messages are informational only.

3. Click Close to close the Validation Results window.

Exchange Data and Verify Results

To exchange data and verify the results, submit the sample Process that is provided with `Connect:Direct`.

To verify the success of the sample Process and review the Secure+ Option statistics for the session, refer to *Connect:Direct for Windows Getting Started Guide*.

Automation Scripts

The following scripts are provided as models for creating custom scripts to define your Secure+ Option environment and automate the implementation of it. To prevent any loss of data, you cannot run the scripts, but you can save them with a different name and modify them to suit your needs.

Automate Secure+ Option Implementation for the STS Protocol

The two sample scripts in this section illustrate using the Secure+ CLI to automate a mass implementation of Secure+ Option and add a remote node, respectively. Both scripts illustrate using statically generated public keys.

Use Statically Generated Public Keys for Automated Mass Implementation

The `spcust_sample1` script demonstrates a mass implementation of Secure+ Option using statically generated public keys.

```
REM spcust_sample1.cmd contains an example of configuring
REM Secure+ with the Secure+ CLI. The example demonstrates
REM the use of statically generated public keys to facilitate
REM an automated mass rollout of Secure+.
REM
REM Variables
REM The return code.
REM spcli.cmd returns the highest return code of the commands
REM it executed. Possible return codes and their meanings are
REM 0 success
REM 4 warning
REM 8 error
REM 16 fatal error
set cdInstallDir=
set spDir=%cdInstallDir%\Server\Secure+
pushd "%spDir%"
REM Main script
REM
echo.
echo This script has been prevented from running because it will alter
echo the configuration of Secure+. Before removing this warning and its
echo exit call, please modify the script so that it carries out only
echo desired modifications to the configuration of Secure+.
echo.
goto :EOF
```

```

all :initCustom
call :invokeCLI
call :terminateCustom
REM End of main script
goto :EOF
REM
REM Functions
REM
REM Custom initialization logic written by customer.
REM :initCustom
REM Customer adds custom initialization code here.
echo Init custom...
echo.
REM del /F "%spDir%\Nodes"
REM End ofinitCustom
goto :EOF
REM Invoke CLI to configure Secure+.
:invokeCLI
set tempFile=clicmds.txt
echo ;
>%tempFile%
echo ; -- Create a new parmfile
>>%tempFile%
echo ;
>>%tempFile%
echo init parmfile
>>%tempFile%
echo localnode=KCHEN-TW-4500
>>%tempFile%
echo path="%spDir%\Nodes"
>>%tempFile%
echo passphrase=12345678901234567890123456789012
>>%tempFile%
echo ;
>>%tempFile%
echo display info
>>%tempFile%
echo ;
>>%tempFile%
echo ;
>>%tempFile%
echo ; -- Synch with netmap
>>%tempFile%
echo ;
>>%tempFile%
echo sync netmap
>>%tempFile%
echo path=v4.3.00\KCHEN-TW-4500
>>%tempFile%
echo name=*
>>%tempFile%
echo ;
>>%tempFile%
echo ;
>>%tempFile%
echo ; -- Update localnode, enable protocol and add keys.
>>%tempFile%
echo ;
>>%tempFile%
echo update localnode
>>%tempFile%
echo protocol=sts
>>%tempFile%
echo override=y
>>%tempFile%
echo STSEnableSig=y
>>%tempFile%
echo STSEnableEnc=y
>%tempFile%
echo STSEnableAutoUpdate=y

```



```

>>%tempFile%
echo stsAuthlocalkey=set
>>%tempFile%
echo StsAuthKeyPairFile=keypairfile
>>%tempFile%
echo StsAuthKeyPairFilePassphrase=secret
>%tempFile%
echo stsSiglocalkey=set
>>%tempFile%
echo StsSigKeyPairFile=keypairfile
>>%tempFile%
echo StsSigKeyPairFilePassphrase=secret
>>%tempFile%
echo ;
>>%tempFile%
echo ;
>>%tempFile%
echo ; -- Display localnode
>>%tempFile%
echo ;
>>%tempFile%
echo display localnode
>>%tempFile%
echo ;
>>%tempFile%
echo ;
>>%tempFile%
echo ; -- Update remotenode records
>>%tempFile%
echo ;
>>%tempFile%
echo update remotenode
>>%tempFile%
echo name=*
>>%tempFile%
echo STSAuthRemoteKey=0200.5F8E.F736.1E38.85C7.2BD0.E312.BD4D.FBC5.A2D3.8E1F
>>%tempFile%
echo
STSSigRemoteKey=0200.5F8E.F736.1E38.85C7.2BD0.E312.BD4D.FBC5.A2D3.8E1F
>>%tempFile%
echo ;
>>%tempFile%
echo ;
>>%tempFile%
echo ; -- Verify localnode does not have remote keys
>>%tempFile%
echo ;
>>%tempFile%
echo display localnode
>>%tempFile%
echo ;
>>%tempFile%
echo ;
>>%tempFile%
echo ; -- Verify all remote nodes have remote pub keys set
>>%tempFile%
echo ;
>>%tempFile%
echo display remotenode
>>%tempFile%
echo name=*
>>%tempFile%
echo ;
>>%tempFile%
echo ;
>>%tempFile%
echo ; -- Update localnode, enable protocol and add keys.
>>%tempFile%
echo ;
>>%tempFile%

```

```

echo update localnode
>>%tempFile%
echo stsauthlocalkey=gen
  >>%tempFile%
echo stsauthkeyseedType=dynamic
>>%tempFile%
echo STSPrevAuthKeyExpDateTime=2005:01:01-20:13:44
>>%tempFile%
  echo stssiglocalkey=gen
  >>%tempFile%
echo stssigkeyseedType=dynamic
>>%tempFile%
  echo STSPrevSigKeyExpDateTime=2005:01:01-20:13:45
  >>%tempFile%
echo ;
>>%tempFile%
  echo display localnode;
>>%tempFile%
  echo ; -- Validate parmfile
  >>%tempFile%
echo ;
>>%tempFile%
  echo validate parmfile
  >>%tempFile%
echo ;
>>%tempFile%
echo quit;
>>%tempFile%
call "%spDir%\spcli.cmd" -e 8 -li y < %tempFile%
  set RC=%ERRORLEVEL%
  del %tempFile%
  REM End of invokeCLI
goto :EOF
REM Custom termination logic written by customer.
REM :terminateCustom
REM Customer adds custom termination code here.
REM For example, E-mail standard out log for review.
REM Send error messages to system monitoring facility.
echo.
echo Custom Terminating with errorlevel of %RC%
echo.
REM End of terminateCustom
goto :EOF
popd

```

Automatically Add a Remote Node to a Connect:Direct Network

The `spcust_sample2` script illustrates how to automate adding a remote node to a Connect:Direct network.

```

@echo off
REM spcust_sample2.cmd contains an example of configuring
REM Secure+ with the Secure+ CLI. The example demonstrates
REM the use of statically generated public keys to
REM facilitate the automated addition of a new node to a
REM Connect:Direct network. In this example, the name of
REM the new node is cd-ultra3600.
REM A script based on this sample is used to
REM figure the existing nodes in the new node's Netmap.
REM The new node itself is configured with a script based REM
on spcust_sample1.cmd. In order for the addition to be
REM successful, the two scripts must use the same seeds
REM to generate keys.
REM
REM Variables
REM The return code.

```

```

REM spcli.cmd returns the highest return code of the commands
REM it executed. Possible return codes and their meanings are
REM 0 success
REM 4 warning
REM 8 error
REM 16 fatal error
set cdInstallDir=
set spDir=%cdInstallDir%\Server\Secure+
pushd "%spDir%"
REM Main script
echo This script has been prevented from running because it will alter
echo The configuration of Secure+. Before removing this warning and its
echo exit call, please modify the script so that it carries out only
echo desired modifications to the configuration of Secure+.
goto :EOF
call :initCustom
call :invokeCLI
call :terminateCustom
REM End of main script
goto :EOF
REM Functions
REM Custom initialization logic written by customer.
:initCustom
REM Customer adds custom initialization code here.
echo Init custom...
echo.
REM End of initCustom
goto :EOF
REM Invoke CLI to configure Secure+.
invokeCLI
set tempFile=clicmds.txt
echo ;
>%tempFile%
echo ;
>>%tempFile%
echo ; -- Synch with netmap
>>%tempFile%
echo ;
>>%tempFile%
echo sync netmap
>>%tempFile%
echo path=v4.5.00\KCHEN-TW-4500
>>%tempFile%
echo name=*
>>%tempFile%
echo ;
>>%tempFile%
echo ;
>>%tempFile%
echo ; -- Update remotenode records
>>%tempFile% echo ;
>>%tempFile%
echo update remotenode
>>%tempFile%
echo name=salmon3600
>>%tempFile%
echo stsAuthlocalkey=set
>>%tempFile%
echo StsAuthKeyPairFile=keypairfile
>>%tempFile%
echo StsAuthKeyPairFilePassphrase=secret
>>%tempFile%
echo stsSiglocalkey=set
>>%tempFile%
echo StsSigKeyPairFile=keypairfile
>>%tempFile%
echo StsSigKeyPairFilePassphrase=secret
>>%tempFile%
echo STSAuthRemoteKey=0200.5F8E.F736.1E38.85C7.2BD0.E312.BD4D.FBC5.A2D3.8E1F
>>%tempFile%

```

```

echo STSSigRemoteKey=0200.5F8E.F736.1E38.85C7.2BD0.E312.BD4D.FBC5.A2D3.8E1F
>>%tempFile%
echo ;
>>%tempFile%
echo display remotenode name=salmon3600
>>%tempFile%
echo ;
>>%tempFile%
echo validate parmfile
>>%tempFile%
echo ;
>>%tempFile%
echo quit;
>>%tempFile%
call "%spDir%\spcli.cmd" -p "%spDir%\Nodes" -e 8 -li y < %tempFile%
set RC=%ERRORLEVEL%
del %tempFile%
REM End of invokeCLI
goto :EOF
REM Custom termination logic written by customer.
:terminateCustom
REM Customer adds custom termination code here.
REM For example, E-mail standard out log for review.
REM Send error messages to system monitoring facility.
echo Custom Terminating with errorlevel of %RC%
REM End of terminateCustom
goto :EOF
popd

```

Configure Secure+ Option to Use the SSL or TLS Protocol

The spcust_sample3 script demonstrates using the Secure+ CLI to configure Secure+ Option to use the SSL or TLS protocol with the trusted root file, key certificates, and ciphers.

```

@echo off
REM spcust_sample3.cmd contains an example of configuring
REM Secure+ to use SSL or TLS protocols with the Secure+ CLI.
REM The example demonstrates the configuration of Secure+
REM with the trusted root and key certificates and ciphers
REM Variables
REM The return code.
REM spcli.cmd returns the highest return code of the commands
REM it executed. Possible return codes and their meanings are
REM 0 success
REM 4 warning
REM 8 error
REM 16 fatal error
echo ; -- Create a new parmfile
>>%tempFile%
echo ;
>>%tempFile%
echo init parmfile
>>%tempFile%
echo localnode=KCHEN-TW
>>%tempFile%
echo path="%spDir%\Nodes"
>>%tempFile%
echo passphrase=12345678901234567890123456789012
>>%tempFile%
echo ;
>>%tempFile%
echo display info
>>%tempFile%
echo ;
>>%tempFile%
echo ;

```

```

>>%tempFile%
echo ; -- Synch with netmap
  >>%tempFile%
set cdInstallDir= set spDir=%cdInstallDir%\Server\Secure+
  pushd "%spDir%"
REM Main script This script has been prevented from running because it will alter
The configuration of Secure+. Before removing this warning and its
  exit call, please modify the script so that it carries out only
  desired modifications to the configuration of Secure+.
goto :EOF
call :initCustom
  call :invokeCLI
  call :terminateCustom
REM End of main script
goto :EOF
  REM Functions
REM Custom initialization logic written by customer.
  :initCustom
  REM Customer adds custom initialization code here.
  echo Init custom...
echo.
REM del /F "%spDir%\Nodes"
  REM End ofinitCustom
goto :EOF
REM Invoke CLI to configure Secure+.
  REM :invokeCLI
set tempFile=clicmds.txt
echo ;
>%tempFile%
echo ;
>>%tempFile%
echo sync netmap
>>%tempFile%
echo path=v4.5.00\KCHEN-TW-4500
>>%tempFile%
  echo name=*
  >>%tempFile%
echo ;
>>%tempFile%
echo ;
  >>%tempFile%
echo ; -- Update localnode, enable protocol and add keys.
  >>%tempFile%
  echo ;
>>%tempFile%
  echo update localnode
>>%tempFile%
echo override=n
>>%tempFile%
echo protocol=tls
>>%tempFile%
echo SSLTLSTRUSTEDROOTCERTFILE="%spDir%\Certificates\trusted.txt"
  >>%tempFile%
echo SSLTLSCERTFILE="%spDir%\Certificates\keycert.txt"
>>%tempFile%
  echo SSLTLSCERTPASSPHRASE=athena
>>%tempFile%
echo SSLTLENABLECIPHER=all >>%tempFile%
  echo ;
>>%tempFile%
  echo ;
>>%tempFile%
echo ; -- Display localnode
  >>%tempFile%
echo ;
  >>%tempFile%
echo display localnode
  >>%tempFile%
echo ;
  >>%tempFile%

```

```
echo validate parmfile
>>%tempFile%
echo ;
>>%tempFile%
echo quit;
>>%tempFile%
call "%spDir%\spcli.cmd" -e 8 -li y < %tempFile%
set RC=%ERRORLEVEL%
del %tempFile%
    REM End of invokeCLI
goto :EOF
REM Custom termination logic written by customer.
:terminateCustom
REM Customer adds custom termination code here.
    REM For example, E-mail standard out log for review.
    REM Send error messages to system monitoring facility.
    echo.
    echo Custom Terminating with errorlevel of %RC%
    echo.
    REM End of terminateCustom
goto :EOF
popd
```

Use LCU to Configure Encrypted Passwords

Configure Encrypted Passwords Using the LCU

The Secure+ CLI displays passwords in plain text. If you need to encrypt passwords for use with the Secure+ CLI, use the Local Connection Utility (LCU) to create an LCU file that contains non-encrypted information used to encrypt the password and the encrypted password, such as a keycert passphrase. You can then refer to this file when prompted for passwords.

LCU Files

The following example shows how to specify when an LCU file is used in place of a plain-text password:

```
C:\...\...\Connect Direct v4.5.00\Common Utilities>lcu -f C:\SomeDir\MyLCU.dat
*****
*          Connect:Direct Java Client Connection Utility          *
*                               Version 4.5.00                    *
*-----*
* Copyright (c) 1999, 2009 Sterling Commerce Inc.                *
* All Rights Reserved.                                           *
*****
Node:
>JLYON-XP.4500
API Address: <Enter> = 'JLYON-XP'
>
API Port: <Enter> = '1363'
>
User Name:
>SomeValue
Password:
> Confirm Password:
>
Saving file: C:\SomeDir\MyLCU.dat
C:\...\...\Connect Direct v4.5.00\Server\Secure+>SPCLI
...
SPCLI> Create STSKeyPair
KeyPairFile=C:\SomeDir\StsKeyPairFile.dat
Passphrase=LCU:C:\SomeDir\MyLCU.dat;
SPCG670I rc=0 Create stskeypair command successful.
SPCLI> Update RemoteNode
Name=JLYON-XP.4500
StsAuthLocalKey=set
StsAuthKeyPairFile=C:\SomeDir\StsKeyPairFile.dat
StsAuthKeyPairFilePassphrase=LCU:C:\SomeDir\MyLCU.dat
SPCG470I rc=0 Update remote node "JLYON-XP.4500" command successful.
```

The use of the LCU syntax “LCU:” indicates that what follows is an LCU filename and not a passphrase. The pathname of the LCU file can be a relative path, a relative path to the bin directory, or a full path. If LCU:filename contains spaces, it must be enclosed in quotation marks: “LCU:filename”. The default name of the LCU file is cddef.bin. After the cddef.bin file is created, you can rename it as needed.

LCU files can be used to provide encrypted passwords for the following commands and parameters:

Command	Parameter
Update LocalNode	StsAuthKeyPairFilePassphrase
	StsSigKeyPairFilePassphrase
	SslTlsCertPassphrase
Create RemoteNode	StsAuthKeyPairFilePassphrase
	StsSigKeyPairFilePassphrase
	SslTlsCertPassphrase
Update RemoteNode	StsAuthKeyPairFilePassphrase
	StsSigKeyPairFilePassphrase
	SslTlsCertPassphrase
Create STSKeyPair	Passphrase
Update Client	SslTlsCertPassphrase
Update SEAServer	SslTlsCertPassphrase

Create an LCU File

To create an LCU file:

- Type the following command to run the LCU utility:

```
lcu.bat
```
- As you are prompted, enter values for the following parameters:
 - Node
 - API Address
 - API Port
 - User Name
 - Password
 - Confirm Password
- The cd.def file is created.