Connect:Direct® Secure+ Option
HP NonStop

Implementation Guide

Version 3.5

Sterling Commerce
An IBM Company

Connect:Direct Secure+ Option HP NonStop Implementation Guide
Version 3.5
First Edition

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

Preface

Chapter 1 About Connect:Direct Secure+ Option HP NonStop

Chapter 2 Setting Up Connect:Direct Secure+ Option HP NonStop

Chapter 3 Maintaining Secure+ Option

Preface

The *Connect:Direct Secure+ Option HP NonStop Implementation Guide* describes how to implement point-to-point security into Connect:Direct operations with Secure+ Option. This document includes information to plan, configure, and use Secure+ Option. The *Connect:Direct Secure+ Option HP NonStop Implementation Guide* is for network operations staff who maintain Connect:Direct Secure+ Option HP NonStop.

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 guides you to the information required to perform Secure+ Option tasks:

Task	Reference
Understanding Secure+ Option	Chapter 1, *About Connect:Direct Secure+ Option HP NonStop*
Setting up Secure+ Option	Chapter 2, *Setting Up Connect:Direct Secure+ Option HP NonStop* Appendix A, *Understanding the Certificate File Layout*
Maintaining Secure+ Option	Chapter 3, *Maintaining Secure+ Option*
Viewing Secure+ Option statistics	Chapter 4, *Accessing Secure+ Option Statistics and Troubleshooting*
Understanding error messages and resolving errors	Chapter 4, *Accessing Secure+ Option Statistics and Troubleshooting*

Chapter 1

About Connect:Direct Secure+ Option HP NonStop

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

This chapter describes:

- Security concepts
- Secure Sockets Layer Protocol (SSL) and Transport Layer Security Protocol (TLS)
- Secure+ Option tools
- Planning the Secure+ Option configuration

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.

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.
- **Data integrity** ensures that information is not altered during transmission.
- **Data confidentiality** ensures that data remains private during transmission.

Connect:Direct Secure+ Option HP NonStop enables you to select Transport Layer Security (TLS) or Secure Sockets Layer protocol (SSL) to secure data during electronic transmission.

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

The SSL and the TLS protocols use certificates to create and exchange session keys that are used to encrypt and hash all messages and data exchanged between the two Connect:Direct nodes, ensuring both confidentiality and data integrity. 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.

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 sender before being sent to the receiver. The receiver 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 which must be exchanged between nodes.
- TLS provides more specific alerts about problems with a session, and documents when certain alerts are sent.

The SSL and TLS protocols provide three levels of security:

- The first level of security is called server authentication and occurs at the beginning of every Secure+ session. When a PNODE (the client) connects to an SNODE (the server), the Connect:Direct server sends its digital certificate to the client. The client checks that the server's certificate has not expired, that it has been issued by a Certificate Authority the client trusts, and that it is being used by the server for which it has been issued. The client node must have a trusted root certificate file that identifies the Certificate Authority and can authenticate the server's certificate.

  If the security fails on any one of these checks, the session 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.
- The second level of security is called client authentication, and is optional. If enabled in the server's Secure+ configuration, the server will request that the client send its own digital certificate to the server. The server then authenticates the client's certificate with a trusted root certificate configured in the server.
- The third level of security, also optional, is Common Name validation. When client authentication is enabled in the server's Secure+ configuration,, a common name can also be specified. When the server receives the client's digital certificate, it compares the common name value defined in the server to the common name field in the client's certificate. If they do not match, the session fails.

Secure+ Option Tools

Connect:Direct Secure+ Option HP NonStop consists of two components: the Administration Tool (Admin Tool) and the parameters file.

- Administration Tool (Admin Tool)—use this tool 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. Access the Administration Tool from the main panel of the automated installation and management system (AIMS) tool. The AIMS tool is a full-screen, block-mode interface for configuring and starting Connect:Direct Secure+ Option HP NonStop as well as Connect:Direct HP NonStop.
- Parameters File (SPNodes)—this file contains information that determines the protocol and encryption method used during security-enabled Connect:Direct operations.

Planning the Connect:Direct HP NonStop Configuration

In order to use Secure+ Option, you must create a parameters file that defines a local node record and an adjacent node record for each trading partner that is defined in the Connect:Direct network map file. When you first create the parameters file, Secure+ Option is disabled for all nodes. You configure each node that uses Secure+ Option.

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

- During the first part of the SSL handshake, the PNODE's (client's) trusted root certificate file is used to authenticate the end-user certificate provided by the SNODE (the server). If the SNODE (the server), has enabled client authentication, the PNODE provides its end-user certificate, which is, in turn, authenticated by the trusted root certificate stored on the SNODE.
- The key certificate file contains the end-user certificate issued to you following submission of a CSR (certificate signing request). It also contains the private key generated during the creation of the CSR. When a trading partner attempts to establish communications with a Connect:Direct node, each Connect:Direct node sends the certificate portion of its key certificate file to the trading partner, who verifies (authenticates) the certificate using a trusted root certificate. The location of the key certificate file must be configured in the Secure+ Option parameters file.

Use one of the following methods to configure an environment to use Secure+ Option:

- Define parameters for each adjacent node record that will use Secure+ Option and set the following values:
  - Enable the protocol to use for secure communications: SSL or TLS

    Note: To create the most secure environment, use the TLS protocol.

  - Identify the cipher suite to use to ensure data confidentiality

    A common cipher suite be configured in the parameters file of both the client (PNODE) and server (SNODE). After initial communication has been established, Secure+ Option determines a common cipher and uses this cipher to encrypt all messages and data exchanged between the two nodes. If more than one cipher is enabled, the preferences defined in the server’s Secure+ Option parameters file determine the cipher suite used for the SSL protocol, and the preferences defined in the client’s parameters file determine the cipher suite used for the TLS protocol.

  - Identify the trusted root certificate file that will authenticate the end-user certificate sent by the adjacent node during the SSL handshake.

  - Identify the key certificate file and passphrase used to decrypt the private key
  - As an option, enable client authentication. This option requires that, when your node is acting as the server (SNODE) during an SSL handshake, the client (PNODE) must provide its end-user certificate to you for authentication. To enable an additional level of security, identify the certificate common name. If you provide a certificate common name, the client authentication process first validates the certificate from the client, then attempts to match the common name with the common name in the certificate. If the server (SNODE) cannot validate the client's (PNODE's) certificate or the common name value does not match the certificate's common name, communication fails.

- The definition of the local node record is not used during Secure+ communication. However, if you have a large environment, you can define default values in the local node record. Then set all adjacent nodes that use Secure+ Option to default to the values defined in the local node. This method allows you to set the values one time in the local node and turn on these options in one step in each adjacent node record. If you use this method, you can define the protocol, cipher suite, trusted root certificate file, and key certificate file in the local node record. You must set all adjacent node records to default to the settings in the local node record.

  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 key certificate file must include certificate and private key information for all certificates.

The adjacent node record must identify the same protocol as that used by the trading partner or the Connect:Direct Secure+ Option HP NonStop session will not be established.

Chapter 2

Setting Up Connect:Direct Secure+ Option HP NonStop

This chapter provides information for performing the following tasks:

- Preparing to Set Up Secure+ Option
- Creating the Secure+ Option Parameters File

Preparing to Set Up Secure+ Option

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

- Complete a configuration worksheet for each trading partner

  Complete the *Node Security Feature Definition Worksheet* on page 14 for each trading partner for whom you plan to enable Secure+ Option.
- Obtain a certificate and generate a key certificate file

  Before configuring Connect:Direct Secure+ Option HP NonStop, obtain a certificate and generate a private key 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.
- Transfer the key certificate file to the Connect:Direct HP NonStop server
- Exchange trusted root certificate files with your trading partners
- Change the file access rights of the trusted root file and the key certificate file

Obtaining a Certificate and Generating 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 from a CA or create a self-signed certificate. Create a private key file using Certificate Wizard or any Web server software. Secure+ Option uses a key certificate file to authenticate a site. This file combines information from the certificate file and the private key file. For more information about certificates, see Appendix A, *Understanding the Certificate File Layout*.

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.

- 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.

To install Certificate Wizard, refer to the *Certificate Wizard* Installation Card. To use Certificate Wizard, refer to the Online Help. To generate a key certificate file, refer to *Generating a Key Certificate File for a CA Certificate* or *Generating a Key Certificate File for a Self-Signed Certificate*.

Generating a Key Certificate File for a CA Certificate

Complete the following steps to generate a key certificate file from a certificate generated by a CA:

1. Generate a certificate signing request (CSR) and a private key. Use Certificate Wizard or any Web server software to generate the CSR and the private key file.
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.

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 and server authentication.

Generating a Key Certificate File for a Self-Signed Certificate

Complete the following steps to generate a key certificate file for a site that is authenticated with a self-signed certificate:

1. Generate a self-signed certificate using Certificate Wizard. Certificate Wizard performs the following tasks when it generates a self-signed certificate:
    - Creates a private key called privkey.txt
    - Creates the trusted root file called cert.crt
2. Generate a key certificate file. 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.

Transferring the Key Certificate File to the HP NonStop System

Once you generate the key certificate file, the file must be moved to the HP NonStop system. Use one of the following methods to transfer the file:

- Use FTP client in binary mode to transfer the key certificate file to the SECUREPL subvolume. Use a destination name for the file that conforms to the Tandem file naming convention such as KEYCERT1.
- Use Connect:Direct to copy the file to the HP NonStop node. Do not translate the file. Define the file as odd unstructured.

Exchanging 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 CA who issued your certificate and you must have a copy of the trading partner’s trusted root certificate file to validate the CA who issued the trading partner’s certificate file. Obtain a copy of the trusted root file and copy it to the SECUREPL subvolume on the Connect:Direct HP NonStop server.

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.

Changing File Access Rights for the Key Certificate File and the Trusted Root File

After you copy the key certificate file and the trusted root file to the Connect:Direct HP NonStop server, you must change the file access rights. The Connect:Direct administrator and all userids under which Connect:Direct Processes may run must have read access to the certificate files. For example, the following commands change the file access rights to a file called TRUSTED1 and another file called KEYCERT1:

```
‘fup secure TRUSTED1, “NCNC”’
‘fup secure KEYCERT1, “NCNC”’
```

Node Security Feature Definition Worksheet

Use this worksheet to record configuration information for Connect:Direct Secure+ Option HP NonStop. For each trading partner, define an adjacent node record. Make a copy of the worksheet for each adjacent node that you are configuring for Secure+ operations.

Node Name: ____

Node Type: Local Adjacent

Configured Security Functions

TLS protocol enabled: Yes _____ No ______

SSL protocol enabled: Yes _____ No ______

Secure+ disabled: Yes _____ No ______

Default to settings defined in local node: Yes _____ No ______

Trusted Root Certificate File:_______________________________________

Certificate File: ____

Cipher Suite(s) Enabled:____

____

____

____

Client Authentication enabled: Yes _____ No ______

Certificate Common Name, if enabled:_______________________________

Creating the Secure+ Option Parameters File

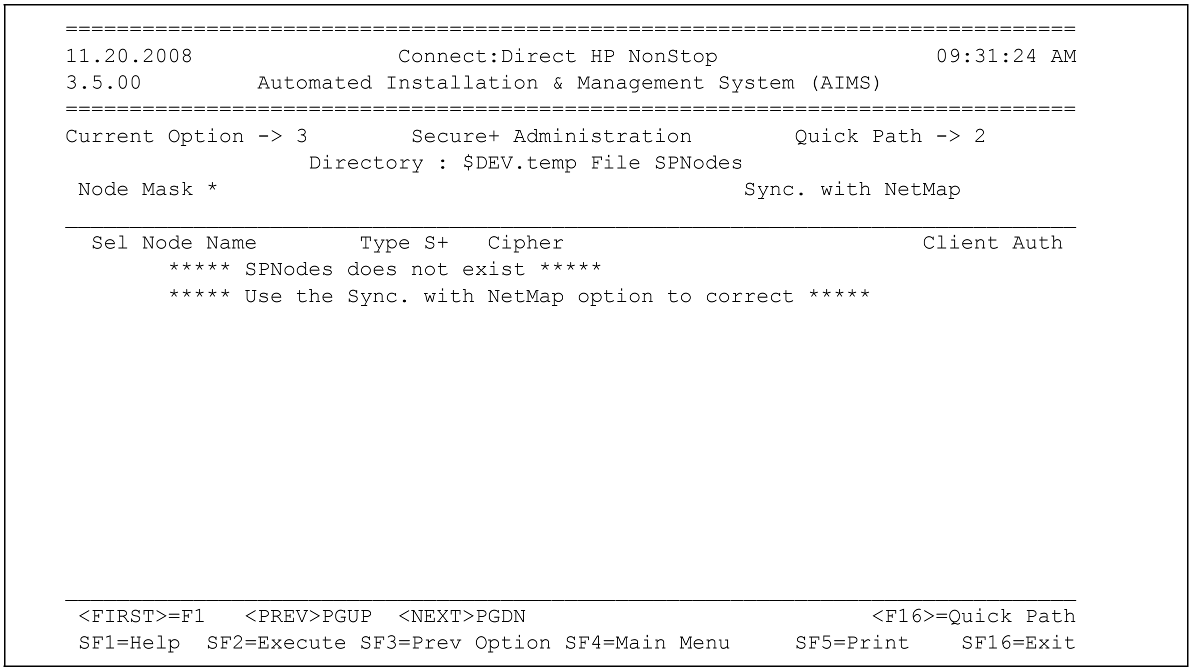
To use Secure+ Option for secure communication, you create a parameters file by importing node definitions defined in the Connect:Direct network map. This section provides the following procedures for starting Secure+ Option and creating a parameters file:

- Starting the Secure+ Option Administration Tool
- Populating the Secure+ Option Parameters File (SPNODES File)

Note: For information on starting and using the menu-driven system called AIMS, see the chapter on installing and configuring Connect:Direct HP NonStop in the *Connect:Direct HP NonStop Installation Guide.*

Starting the Secure+ Option Administration Tool

To start the Secure+ Option Administration Tool, from the Main Menu panel, press **F3** to begin the Connect:Direct Secure+ Option HP NonStop installation. The Secure+ Administration panel is displayed:



```
===============================================================================
11.20.2008              Connect:Direct HP NonStop                 09:31:24 AM
3.5.00         Automated Installation & Management System (AIMS)
===============================================================================
Current Option -> 3       Secure+ Administration        Quick Path -> 2
                   Directory : $DEV.temp File SPNodes
 Node Mask *                                        Sync. with NetMap
_______________________________________________________________________________
  Sel Node Name        Type S+   Cipher                            Client Auth
        ***** SPNodes does not exist *****
        ***** Use the Sync. with NetMap option to correct *****













_______________________________________________________________________________
 <FIRST>=F1   <PREV>PGUP  <NEXT>PGDN                          <F16>=Quick Path
 SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

The Secure+ Option Admin Tool starts and opens the Secure+ Option parameters file for the associated Connect:Direct node. The first time you use Secure+ Option, no parameters file exists. You must create the parameters file. Refer to *Populating the Secure+ Option Parameters File (SPNODES File)* in the next section.

Populating the Secure+ Option Parameters File (SPNODES 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, populate the Secure+ Option parameters file from entries defined in an existing network map using the Sync with NetMap function.

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.

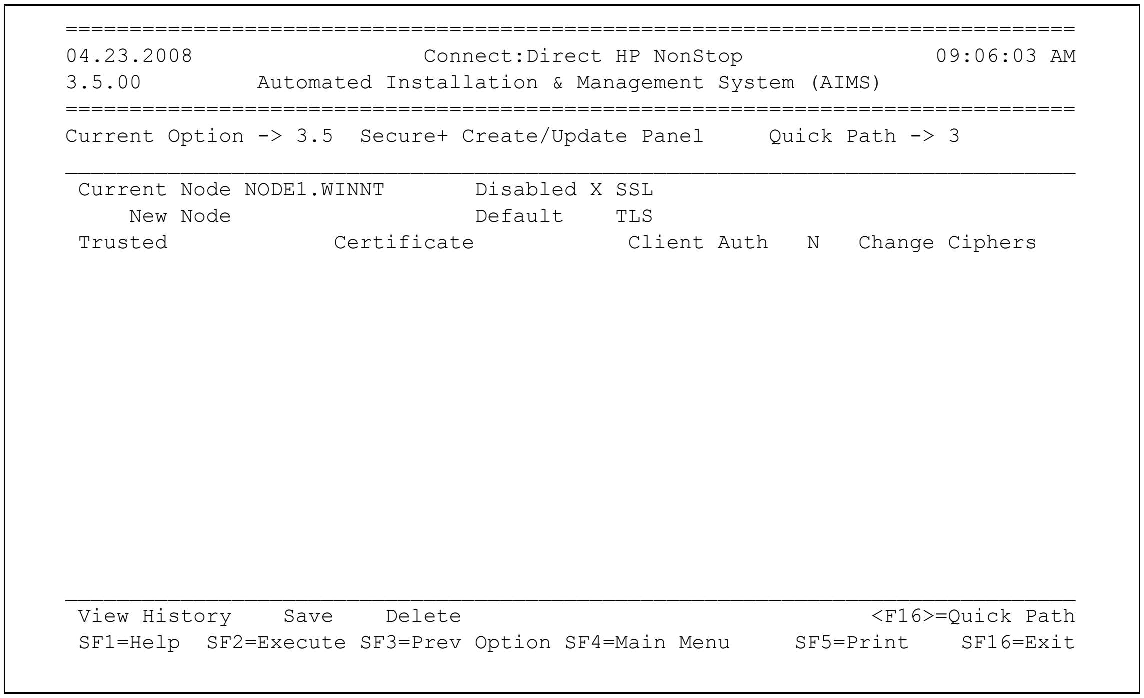
Perform the following step to populate the Secure+ Option parameters file with node entries defined in the Connect:Direct network map:

1. From the Secure+ Administration panel, type an x in the **Sync. with NetMap** field and press **SF2**.

Configuring Nodes for Secure+ Option

When you import the network map records into the Secure+ parameters file, Secure+ Option is disabled. You should have determined how you want to configure your environment in *Planning the Connect:Direct HP NonStop Configuration* on page 9. Complete the following procedure to configure a local or adjacent node record:

1. From the Secure+ Administration panel, tab to the node record to configure. Type an x next to the node to configure and press **SF2**. The Secure+ Create/Update Panel panel is displayed:



```
================================================================================
04.23.2008                  Connect:Direct HP NonStop               09:06:03 AM
3.5.00         Automated Installation & Management System (AIMS)
================================================================================
Current Option -> 3.5  Secure+ Create/Update Panel     Quick Path -> 3
________________________________________________________________________________
 Current Node NODE1.WINNT       Disabled X SSL
     New Node                   Default    TLS
 Trusted             Certificate            Client Auth   N   Change Ciphers










________________________________________________________________________________
 View History    Save    Delete                                <F16>=Quick Path
 SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

2. If you want to add a node that is not yet defined in the parameters file:
   a. Type the new node name in the **New Node** field.
   b. Type an x in the **Save** field.
   c. Press **SF2**.
   d. Type an x next to the node you added and press **SF2** to return to the Secure+ Update/Create panel.

3. Clear the x from the **Disabled** field to turn off this option. This is the default value.
4. Type an x next to the security option to activate for the node. You can only activate one of the following options for each node:
   - TLS—select this option to activate the TLS protocol for the node.
   - SSL—select this option to activate the SSL protocol for the node.
   - Default—select this option in adjacent nodes to use the settings defined in the local node record. This option is only valid for adjacent node records.

Note: When SSL is selected, the SSL handshake may still "negotiate up" to TLS for the Secure+ session, depending on which SSL toolkits are being used on the client and server.

Cipher suites are negotiated in the following manner:

- TLS—the first cipher configured on the server (SNODE) takes precendence.
- SSL—the first cipher configured on the client (PNODE) takes precedence.

This is only an issue if both nodes have multiple ciphers in one another's remote node definitions. Usually, a single cipher is configured in a remote node definition.

Caution: To create the most secure environment, use the TLS protocol.

Refer to the following table for an explanation of the fields on the Secure+ Create/Update Panel panel:

Field Name	Field Definition	Valid Values
Current Node	Specifies the node record name.	This is not an editable field.
New Node	Defines a new adjacent node record.	Any valid node name. **Note**: Usually new nodes are first added to the netmap, then imported to the SPNODES file using the "SYNC with Netmap" option. You can use the "New Node" feature to create a pseudo node and then refer to it using the adjacent node's SECURE parameter, thus grouping nodes with the same security characteristics together.
Disabled	Disables Secure+ for the selected node.	Selected or deselected. Default value is selected.
SSL	Enables the SSL protocol for this node to ensure that data is securely transmitted.	Selected or deselected. Default value is deselected.
Default	Allows the selected adjacent node record to use the protocol values defined in the local node record.	Selected or deselected. Default value is deselected. This option is only valid for adjacent node records.
TLS	Enables the TLS protocol for this node to ensure that data is securely transmitted.	Selected or deselected. Default value is deselected.

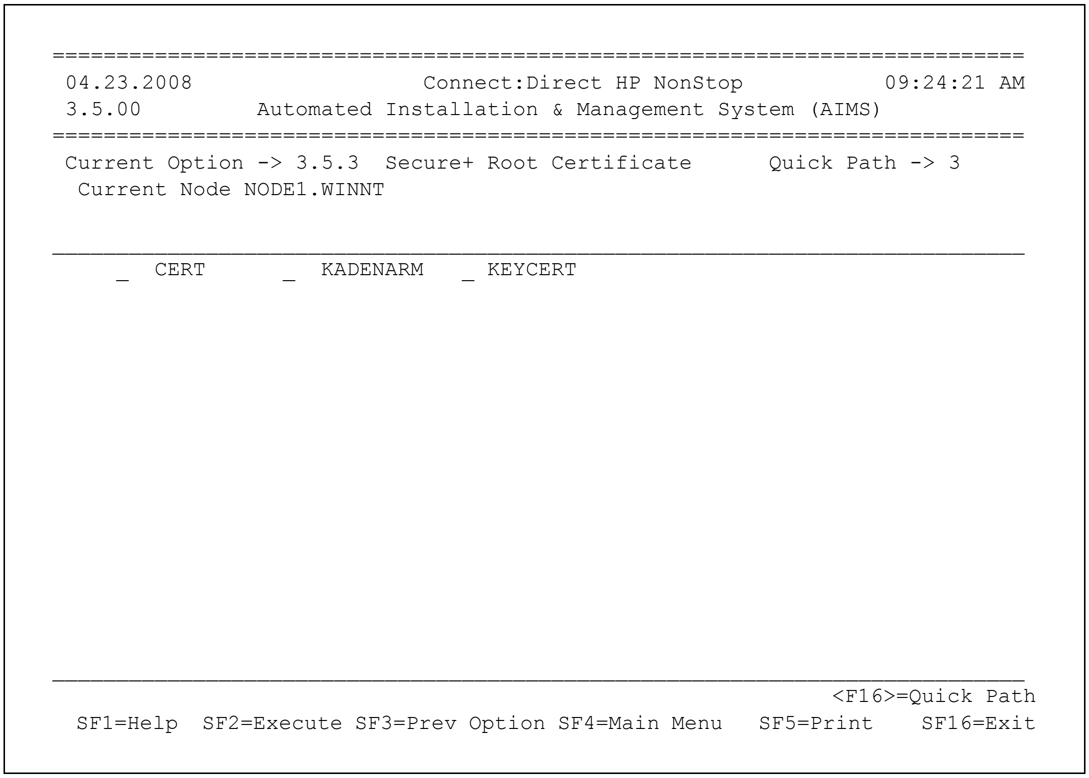
Field Name	Field Definition	Valid Values
Trusted	Opens another panel and identifies the trusted root certificate file to use for a node or deselects a trusted root certificate file.	Valid location and file name of a trusted root certificate file.
Certificate	Opens another panel and identifies the key certificate file to use for a node or deselects a key certificate file.	Select this option and identify the key certificate file.
Client Auth	Opens another panel and turns on or turns off client authentication.	Y | N
Change Ciphers	Opens the Secure+ Cipher panel and defines the cipher suite to use to perform secure communication.	Selected or deselected. Default value is deselected.

5. If you selected TLS or SSL in step 3, define the security options. Refer to *Defining SSL or TLS Options* on page 18.
6. Press **SF2** to save the settings.

Defining SSL or TLS Options

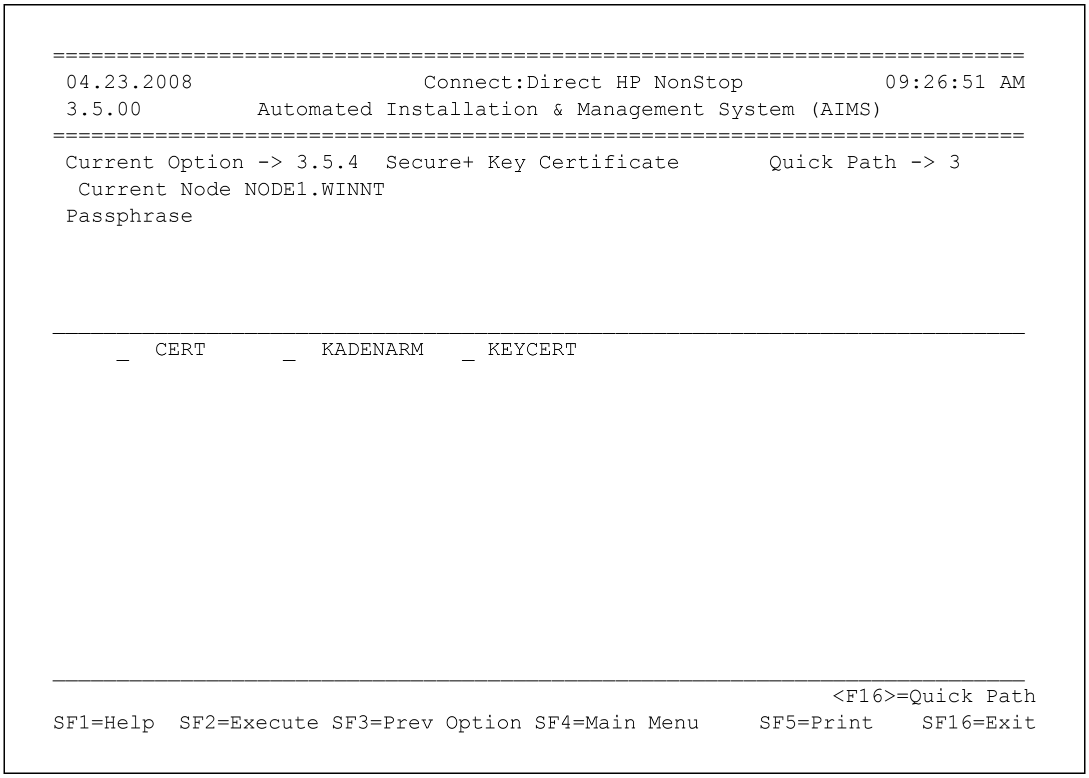
If you enable the TLS or SSL protocol for a node, you must also define the security options. Complete the following procedure to define the SSL or TLS security options:

1. To identify the trusted root certificate file, perform the following actions:
   a. From the Secure+ Create/Update panel, type an x in the **Trusted** field and press **SF2**. The Secure+ Root Certificate panel is displayed:



```
============================================================================
 04.23.2008                  Connect:Direct HP NonStop          09:24:21 AM
 3.5.00         Automated Installation & Management System (AIMS)
============================================================================
 Current Option -> 3.5.3  Secure+ Root Certificate      Quick Path -> 3
  Current Node NODE1.WINNT

____________________________________________________________________________
     _  CERT       _  KADENARM   _ KEYCERT















____________________________________________________________________________
                                                              <F16>=Quick Path
  SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu   SF5=Print    SF16=Exit
```

   b. Type an x next to the trusted root certificate file to use.
   c. Press **SF2** to save these settings and return to the Secure+ Create/Update panel.
2. To identify the key certificate file, perform the following actions:
   a. Type an x in the **Certificate** field and press **SF2**. The Secure+ Key Certificate panel is displayed:

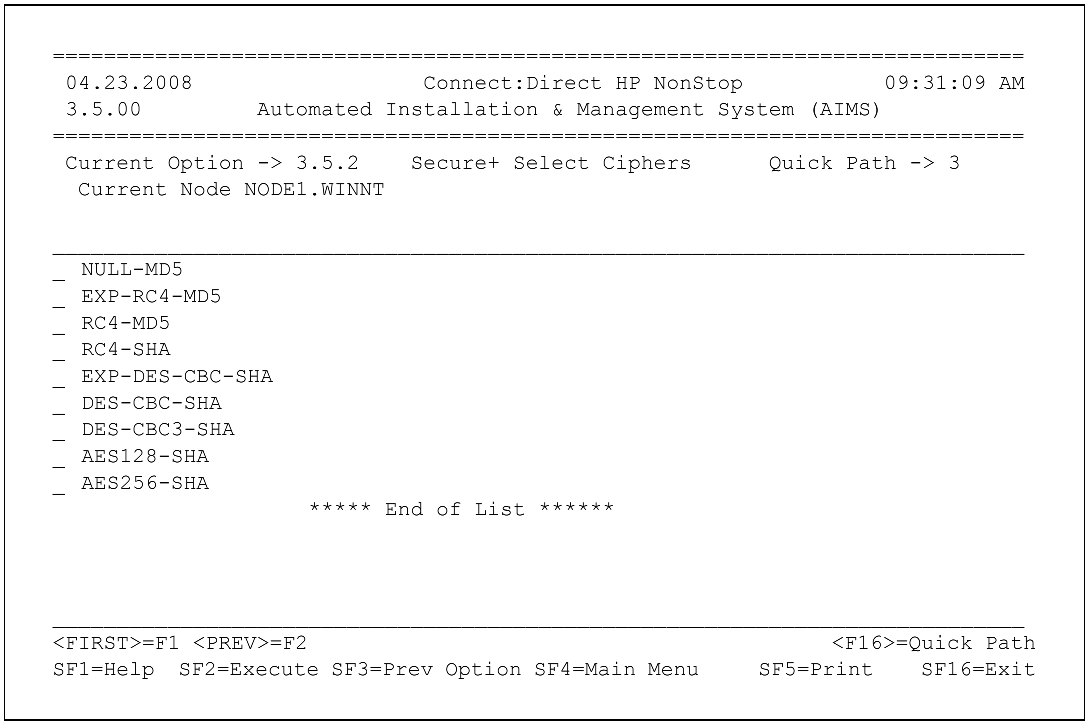


```
============================================================================
 04.23.2008                  Connect:Direct HP NonStop          09:26:51 AM
 3.5.00         Automated Installation & Management System (AIMS)
============================================================================
 Current Option -> 3.5.4  Secure+ Key Certificate       Quick Path -> 3
  Current Node NODE1.WINNT
 Passphrase



____________________________________________________________________________
     _  CERT       _  KADENARM   _ KEYCERT












____________________________________________________________________________
                                                               <F16>=Quick Path
SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

   b. Type the passphrase for the key certificate file that you select in the **Passphrase** field.
   c. Type an x next to the key certificate file to use.
   d. Press **SF2** to save these settings and return to the Secure+ Create/Update panel. If the passphrase does not match the passphrase defined in the key certificate file, an error is displayed. Resolve any errors before continuing.

3. To identify the cipher to use to encrypt data for the node, perform the following actions:

   a. Place an x in the **Change Ciphers** field and press **SF2**. The Secure+ Select Ciphers panel is displayed:



```
============================================================================
 04.23.2008                  Connect:Direct HP NonStop           09:31:09 AM
 3.5.00         Automated Installation & Management System (AIMS)
============================================================================
 Current Option -> 3.5.2    Secure+ Select Ciphers      Quick Path -> 3
  Current Node NODE1.WINNT


____________________________________________________________________________
_ NULL-MD5
_ EXP-RC4-MD5
_ RC4-MD5
_ RC4-SHA
_ EXP-DES-CBC-SHA
_ DES-CBC-SHA
_ DES-CBC3-SHA
_ AES128-SHA
_ AES256-SHA
                    ***** End of List ******



____________________________________________________________________________
<FIRST>=F1 <PREV>=F2                                         <F16>=Quick Path
SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

   b. Type an x next to the cipher that you want to enable. You can enable more than one cipher, but only one cipher is negotiated for use in a Secure+ session.

   c. Press **SF2** to save the settings and return to the Secure+ Create/Update panel.

   d. After selecting the ciphers, you can reorder them. To reorder ciphers, type new numbers by the ciphers to identify the order of preference.

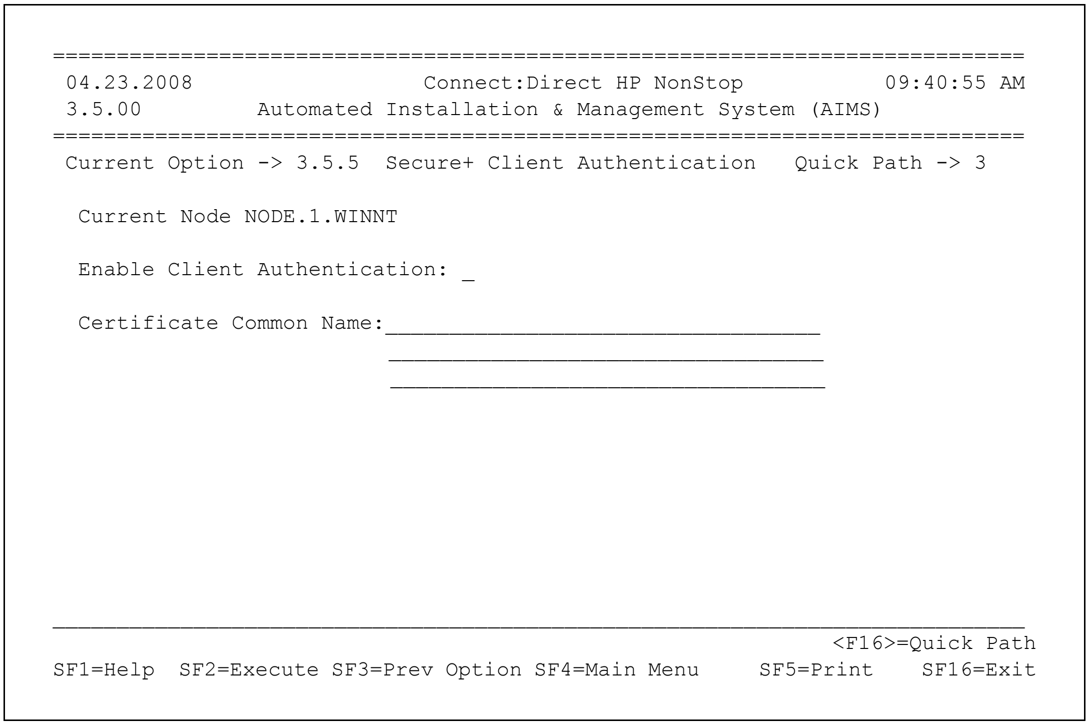
Note: If you place a 1 next to more than one cipher, ciphers are reordered from bottom to top.

   e. Press **SF2** to save the cipher selected and to reorder the ciphers. This also returns you to the Secure+ Administration panel.

4. To activate client authentication, perform the following actions:

   a. Type an x in the **Client Auth** field and press **SF2**. The Secure+ Client Authentication panel is displayed:

   Note: This option is only valid for a remote node record.



```
===========================================================================
 04.23.2008                 Connect:Direct HP NonStop          09:40:55 AM
 3.5.00        Automated Installation & Management System (AIMS)
===========================================================================
 Current Option -> 3.5.5  Secure+ Client Authentication   Quick Path -> 3

  Current Node NODE.1.WINNT

  Enable Client Authentication: _

  Certificate Common Name:__________________________________
                          __________________________________
                          __________________________________









___________________________________________________________________________
                                                             <F16>=Quick Path
SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

   b. Type an x in the **Enable Client Authentication** field.

   c. If you want to enable another level of security, type the trading partner's certificate common name in the **Certificate Common Name** field.

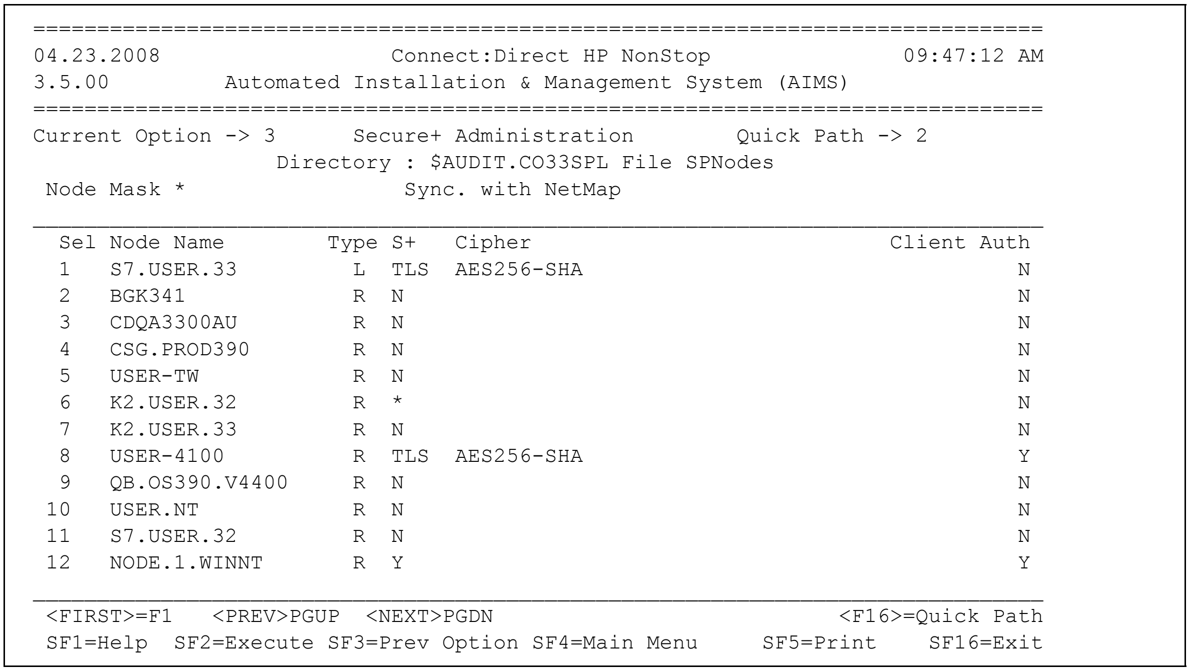
   d. Press **SF2** to save the client authentication definitions and return to the Secure+ Update/Create panel.

   Note: To deactivate client authentication, clear the x from the Client Authentication field and press **SF2** to save the settings.

5. To save the changes, place an x in the **Save** field and press **SF2** to update the node record in the parameters file.

Secure+ Administration Panel Information

Once you configure adjacent nodes to use Secure+ Option, the Secure+ Administration panel displays the nodes defined in the parameters file with information about each node. Below is a sample of the Secure+ Administration panel populated with nodes:



```
===============================================================================
04.23.2008                  Connect:Direct HP NonStop               09:47:12 AM
3.5.00         Automated Installation & Management System (AIMS)
===============================================================================
Current Option -> 3      Secure+ Administration        Quick Path -> 2
                   Directory : $AUDIT.CO33SPL File SPNodes
 Node Mask *                 Sync. with NetMap
_______________________________________________________________________________
  Sel Node Name        Type S+   Cipher                            Client Auth
  1   S7.USER.33         L  TLS  AES256-SHA                                  N
  2   BGK341             R  N                                                N
  3   CDQA3300AU         R  N                                                N
  4   CSG.PROD390        R  N                                                N
  5   USER-TW            R  N                                                N
  6   K2.USER.32         R  *                                                N
  7   K2.USER.33         R  N                                                N
  8   USER-4100          R  TLS  AES256-SHA                                  Y
  9   QB.OS390.V4400     R  N                                                N
 10   USER.NT            R  N                                                N
 11   S7.USER.32         R  N                                                N
 12   NODE.1.WINNT       R  Y                                                Y
_______________________________________________________________________________
 <FIRST>=F1   <PREV>PGUP  <NEXT>PGDN                           <F16>=Quick Path
 SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

Following is a description of the fields displayed on the Secure+ Administration panel:

Field Name	Field Definition	Valid Values
Node Mask	Allows you to type filtering information to display a list of node names that match the filter information. For example, to display all nodes beginning with Loc1, type Loc1*.	Any alpha numeric characters and the * character as a wildcard character.
Sync. with NetMap	Creates a parameters file with values defined in the Connect:Direct network map.	x = selected
Node Name	Specifies the node record name.	This is not an editable field.

Type	Displays the current record type.	L = local node record.
		R = adjacent node record.

S+	Displays the status of Secure+.	N = Secure+ Option is disabled. TLS = TLS protocol is enabled for this node. SSL = SSL protocol is enabled for this node. * = node values default to the values defined in the local node record.

Field Name	Field Definition	Valid Values
Cipher	Displays the first cipher that is enabled for the node record.	NULL-MD5 EXP-RC4-MD5 RC4-MD5 RC4-SHA EXP-DES-CBC-SHA DES-CBC-SHA DES-CBC3-SHA AES128-SHA AES256-SHA

Client Auth	Displays the status of client authentication. Enabling client authentication requires the trading partner node to submit its own certificate to authenticate its identity to the Connect:Direct server node.	Y = enabled
		N = disabled

Chapter 3

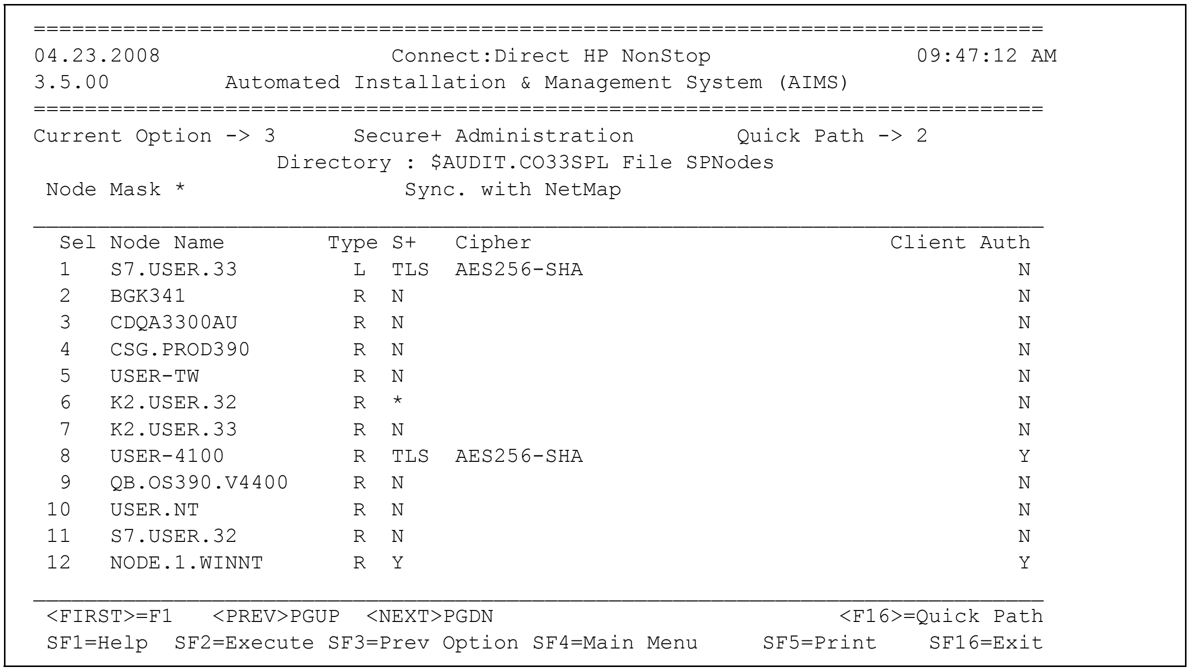
Maintaining Secure+ Option

After you set up the Secure+ Option environment, you must perform additional maintenance tasks as needed. This chapter provides procedures for performing the following Secure+ Option maintenance tasks:

- Viewing the Secure+ Node List
- Viewing Secure+ Option Node Record Change History
- Modifying a Secure+ Option Configuration

Viewing the Secure+ Node List

After you set up node records in Secure+ Option, you can view all of the nodes and their attributes from the Secure+ Administration panel. Below is a sample of the node list. Refer to *Secure+ Administration Panel Information* on page 22 for a description of the fields.



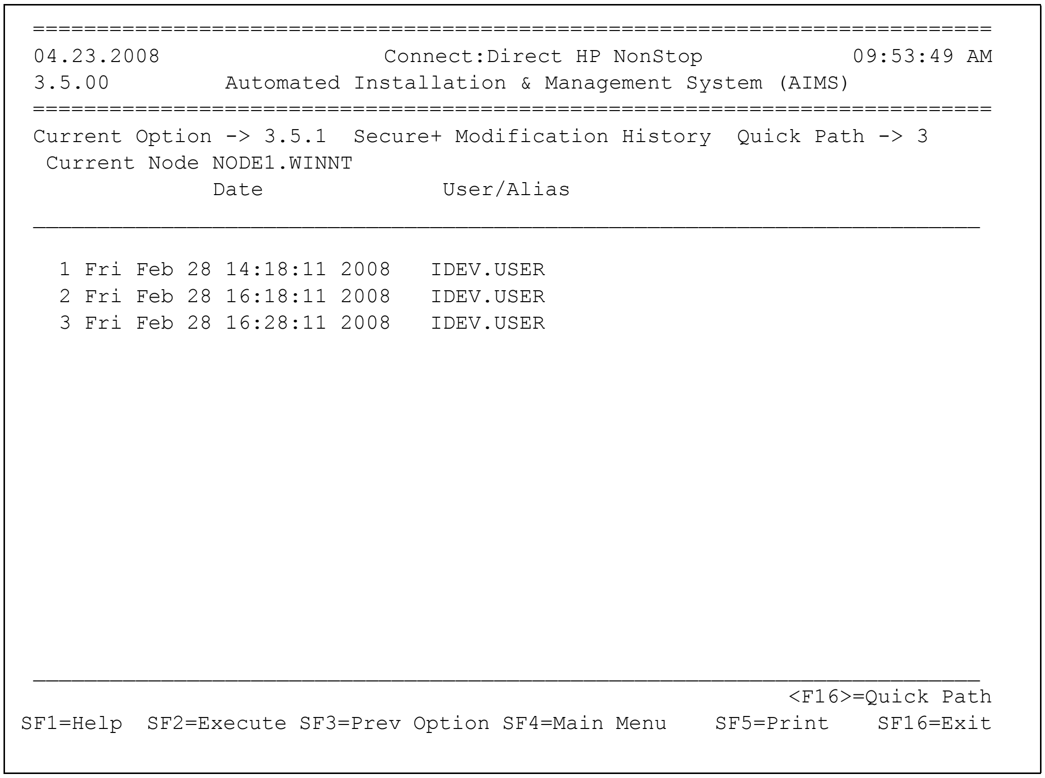
```
===============================================================================
04.23.2008                 Connect:Direct HP NonStop               09:47:12 AM
3.5.00         Automated Installation & Management System (AIMS)
===============================================================================
Current Option -> 3      Secure+ Administration       Quick Path -> 2
                   Directory : $AUDIT.CO33SPL File SPNodes
 Node Mask *                  Sync. with NetMap
_______________________________________________________________________________
  Sel Node Name         Type S+   Cipher                              Client Auth
   1   S7.USER.33          L  TLS  AES256-SHA                                   N
   2   BGK341              R  N                                                 N
   3   CDQA3300AU          R  N                                                 N
   4   CSG.PROD390         R  N                                                 N
   5   USER-TW             R  N                                                 N
   6   K2.USER.32          R  *                                                 N
   7   K2.USER.33          R  N                                                 N
   8   USER-4100           R  TLS  AES256-SHA                                   Y
   9   QB.OS390.V4400      R  N                                                 N
  10   USER.NT             R  N                                                 N
  11   S7.USER.32          R  N                                                 N
  12   NODE.1.WINNT        R  Y                                                 Y
_______________________________________________________________________________
 <FIRST>=F1   <PREV>PGUP  <NEXT>PGDN                          <F16>=Quick Path
 SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

To display a Secure+ Option node record, type an x in the **Sel** field and press **SF2**.

Viewing Secure+ Option Node Record Change History

Secure+ Option keeps a record of when a parameters file has been modified and who modified it. Perform the following steps to view a history of changes made to a node record:

1. From the Admin Tool, type an x in the **Sel** field and press **SF2** to open a Secure+ Option node record.
2. Type an x in the **View History** field at the bottom of the panel and press **SF2**. The Secure+ Modification History panel is displayed:



```
 ============================================================================
 04.23.2008                  Connect:Direct HP NonStop            09:53:49 AM
 3.5.00         Automated Installation & Management System (AIMS)
 ============================================================================
 Current Option -> 3.5.1  Secure+ Modification History  Quick Path -> 3
  Current Node NODE1.WINNT
               Date              User/Alias
 ___________________________________________________________________________

   1 Fri Feb 28 14:18:11 2008   IDEV.USER
   2 Fri Feb 28 16:18:11 2008   IDEV.USER
   3 Fri Feb 28 16:28:11 2008   IDEV.USER

 ___________________________________________________________________________
                                                             <F16>=Quick Path
SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu    SF5=Print    SF16=Exit
```

Refer to the following table for an explanation of the fields.

Field Name	Field Definition
Current Node	Displays the name of the node opened.
Date	Displays the date and time the node record was updated.
User/Alias	Displays the Tandem user ID used to make the change to the record.

Modifying a Secure+ Option Configuration

After using Secure+ Option, it may be necessary to modify a configuration. This section provides the following procedures for modifying Secure+ Option information:

- Disabling Secure+ Option
- Disabling SSL or TLS Options
- Deleting a Secure+ Option adjacent node record

Disabling Secure+ Option

You can use this procedure to disable Secure+ Option in an adjacent node record. Perform the following steps to disable Secure+ Option for a node record:

1. From the Main AIMS panel, press **F3**. The Secure+ Administration panel is displayed.
2. Type an x next to the node record to disable and press **SF2**. The Secure+ Create/Update Panel panel is displayed.
3. Clear the x from the protocol to turn off this option.
4. Type an x next to the **Disabled** option.
5. To save the changes, type an x in the **Save** field and press **SF2** to update the node record.

Note: In order to continue Connect:Direct operations with Secure+ disabled, *both* trading partners must disable Secure+ Option.

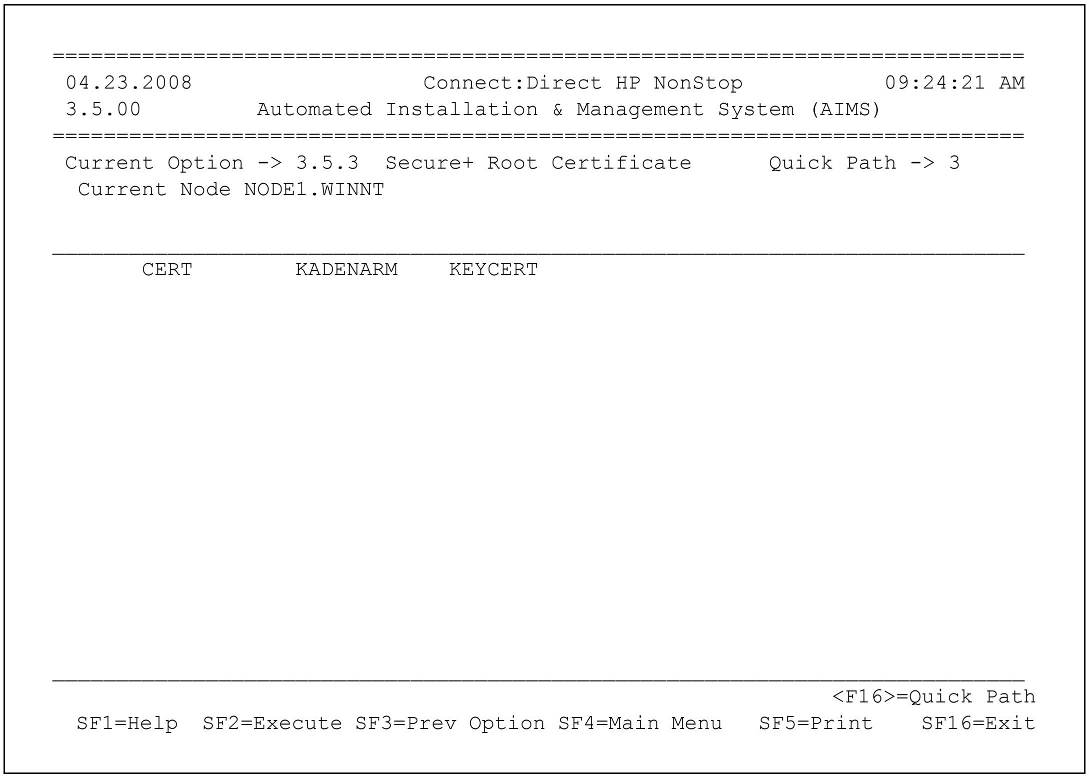
Disabling SSL or TLS Options

If you enable the TLS or SSL option, you defined security options. Complete the following procedure to disable an SSL or TLS option:

1. From the Main AIMS panel, press **F3**. The Secure+ Administration panel is displayed.
2. Type an x next the node record to disable and press **SF2**. The Secure+ Create/Update Panel panel is displayed.

3. To deselect a trusted root certificate file, perform the following actions:

   a. From the Secure+ Create/Update panel, type an x in the **Trusted** field and press **SF2**. The Secure+ Root Certificate panel is displayed:



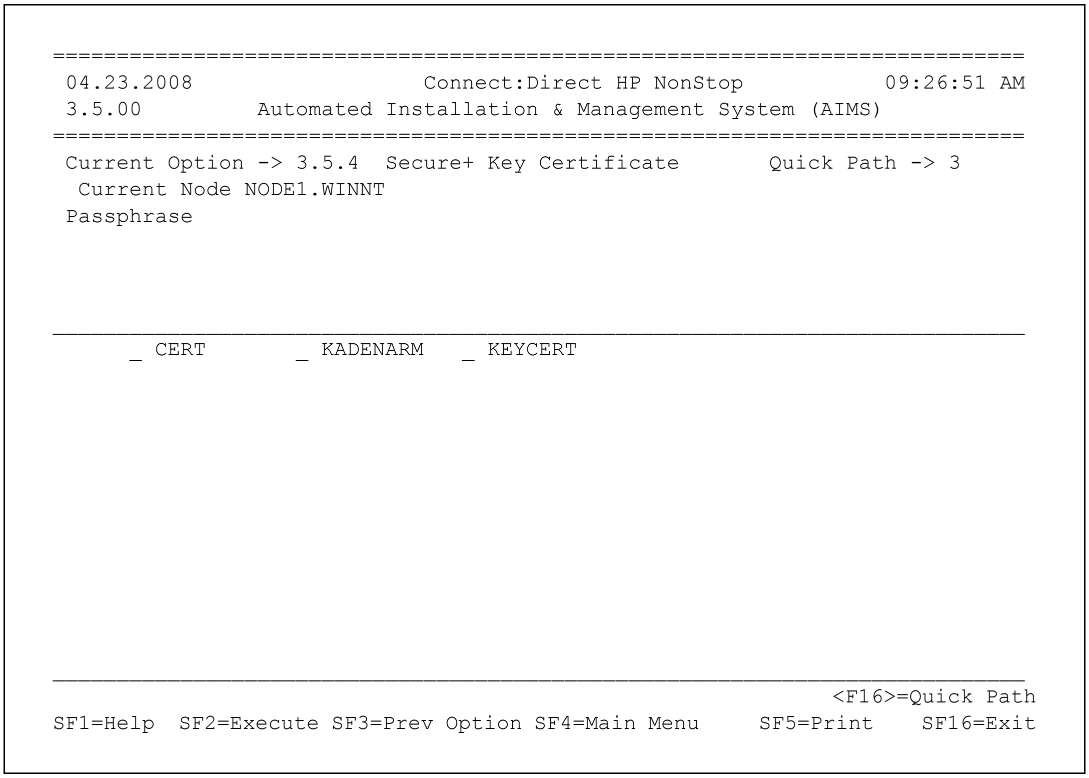
```
============================================================================
 04.23.2008                  Connect:Direct HP NonStop          09:24:21 AM
 3.5.00         Automated Installation & Management System (AIMS)
============================================================================
 Current Option -> 3.5.3  Secure+ Root Certificate      Quick Path -> 3
  Current Node NODE1.WINNT

____________________________________________________________________________
        CERT        KADENARM    KEYCERT















____________________________________________________________________________
                                                              <F16>=Quick Path
  SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu   SF5=Print    SF16=Exit
```

   b. Clear the x from any selected file.

   c. Press **SF2** to save these settings and return to the Secure+ Create/Update panel.

4. To deselect a key certificate file, perform the following actions:

   a. Type an x in the **Certificate** field and press **SF2**. The Secure+ Key Certificate panel is displayed:



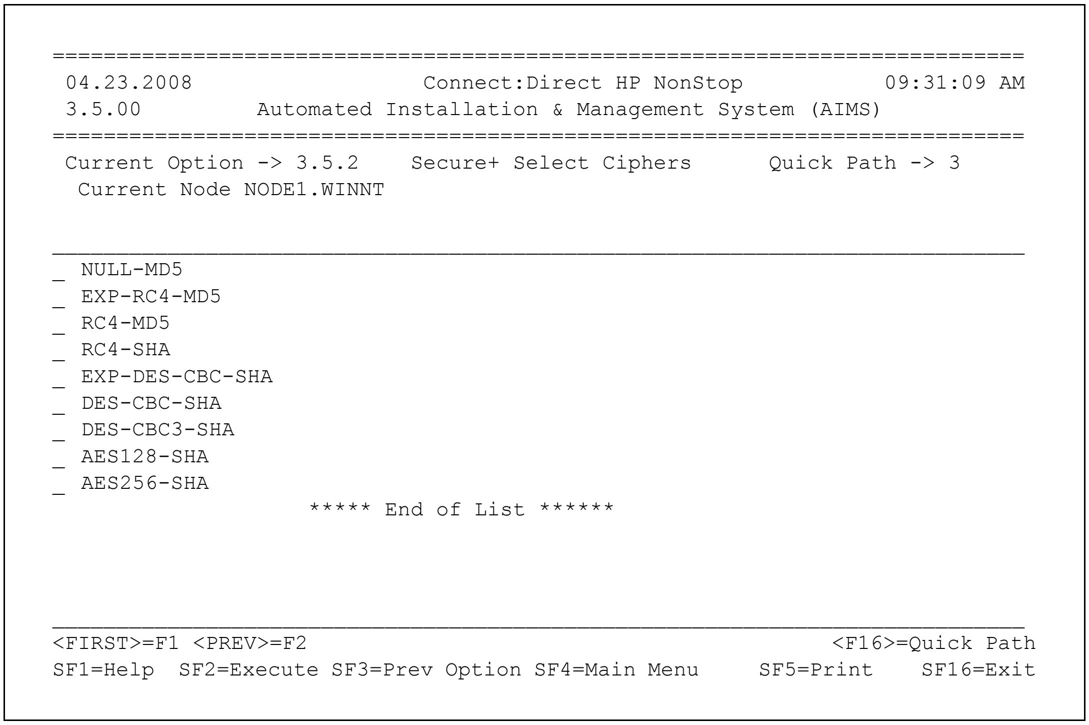
```
=============================================================================
 04.23.2008                 Connect:Direct HP NonStop          09:26:51 AM
 3.5.00         Automated Installation & Management System (AIMS)
=============================================================================
 Current Option -> 3.5.4  Secure+ Key Certificate       Quick Path -> 3
  Current Node NODE1.WINNT
 Passphrase



_____________________________________________________________________________
      _ CERT        _ KADENARM    _ KEYCERT











_____________________________________________________________________________
                                                              <F16>=Quick Path
SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

   b. Clear the x next to any key certificate file to deselect it.

   c. Press **SF2** to save these settings and return to the Secure+ Create/Update panel.

5. To deselect a cipher used to encrypt data for the node, perform the following actions:

   a. From the Secure+ Update/Create panel, place an x in the **Change Ciphers** field and press **SF2**. The Secure+ Select Ciphers panel is displayed:



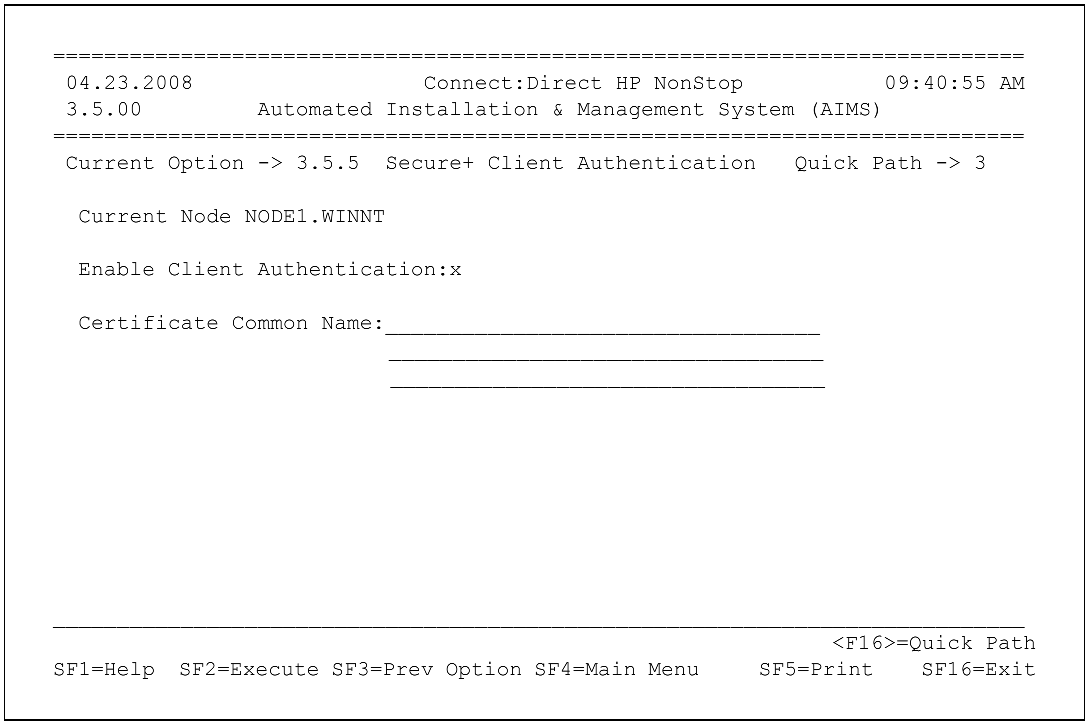
```
============================================================================
 04.23.2008                  Connect:Direct HP NonStop           09:31:09 AM
 3.5.00         Automated Installation & Management System (AIMS)
============================================================================
 Current Option -> 3.5.2    Secure+ Select Ciphers      Quick Path -> 3
  Current Node NODE1.WINNT


____________________________________________________________________________
_ NULL-MD5
_ EXP-RC4-MD5
_ RC4-MD5
_ RC4-SHA
_ EXP-DES-CBC-SHA
_ DES-CBC-SHA
_ DES-CBC3-SHA
_ AES128-SHA
_ AES256-SHA
                    ***** End of List ******



____________________________________________________________________________
<FIRST>=F1 <PREV>=F2                                          <F16>=Quick Path
SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

   b. Clear the x next to the cipher to disable.

   c. Press **SF2** to save the settings and return to the Secure+ Create/Update panel.

6. To deactivate client authentication, perform the following actions:

   a. From the Secure+ Create/Update panel, type an x in the **Client Auth** field and press **SF2**. The Secure+ Client Authentication panel is displayed:



```
============================================================================
 04.23.2008                  Connect:Direct HP NonStop          09:40:55 AM
 3.5.00         Automated Installation & Management System (AIMS)
============================================================================
 Current Option -> 3.5.5  Secure+ Client Authentication   Quick Path -> 3

  Current Node NODE1.WINNT

  Enable Client Authentication:x

  Certificate Common Name:__________________________________
                          __________________________________
                          __________________________________









____________________________________________________________________________
                                                             <F16>=Quick Path
SF1=Help  SF2=Execute SF3=Prev Option SF4=Main Menu     SF5=Print    SF16=Exit
```

   b. Clear the x in the **Client Authentication** field.

   c. Press **SF2** to save the client authentication definitions and return to the Secure+ Update/Create panel.

7. To save the changes, type an x in the **Save** field and press **SF2** to update the node record in the parameters file.

Deleting a Secure+ Option Adjacent Node Record

Perform the following steps to delete an adjacent node record from the parameters file:

1. From the Main AIMS panel, press **F3**. The Secure+ Administration panel is displayed.
2. Type an x next the node record to delete and press **SF2**. The Secure+ Create/Update panel is displayed.
3. Type an x next to the **Delete** option.
4. Clear the x from the **Save** field.
5. Press **SF2** to update the node record.

Caution: Do *not* delete the local node record.

Chapter 4

Accessing Secure+ Option Statistics and Troubleshooting

Connect:Direct logs statistics for Connect:Direct Process activity. If Connect:Direct Secure+ Option is enabled, Connect:Direct statistics include Secure+ Option information for a Process.

This chapter provides samples of Connect:Direct Process statistics records for Secure+ Option.

Secure+ Option Statistics Record Information

When a Connect:Direct session uses SSL or TLS for secure transmission, information is logged to the statistics file. The statistics information can be viewed from NDMCOM.

Fields are included in the Connect:Direct Process statistics records to provide Secure+ Option information about the Process. Secure+ information is included in the Process statistics information only when you attach to a Secure+ server.

Select Statistics Output

Secure+ Option statistics are recorded in the PROCSTART, STEPSTART, and STEPEND records. Following is a sample Select Statistics report with Secure+ Option statistics in bold:

```
SEL STAT STARTT(,12:55)
================================================================================
3.5.00                   S E L E C T    S T A T I S T I C S
================================================================================
Date    => 06.26.2008  Time      => 12:55:44.89   PROCESS - SUBMIT
Pnumber => 3814        Node      => NSTOP.TEST.350   PlexClass =>
Pname   => NSTOP350    Submitter => S7.TEST.35       DEV.USER
Rtncd   => 0           Message ID=> SSRV101I          Feedback  => 0
File    => \ESCAPE.$DEV.JSPROC.NSTOP35
  SSRV101I: (RC=0, FDBK="0")
Process submitted successfully. Process number : 3814
File name    : \ESCAPE.$DEV.JSPROC.NSTOP35
Process name : NSTOP350    Submit time : 06/26/2008 12:55:44.89
_______________________________________________________________________________
Date    => 06.26.2008  Time      => 12:55:56.48   PROCESS - PROCSTART
Pnumber => 3814        Snode     => NSTOP.TEST.350   Xnode     => P
Pname   => NSTOP350    Submitter => S7.TEST.35       DEV.USER
Class   => 1           PlexClass =>                   CRC Check => OFF
LU Name => \ESCAPE.TCP32D
Portnum => 17132       TCPNAME   => \ESCAPE.$ZSAM1
IPaddr  =>             fd00:0:0:20a0::34
Secure+ Protocol>  TLSv1
Cipher Suite>  AES256-SHA
Remote Cert Name>  sterling
_______________________________________________________________________________
Date    => 06.26.2008  Time      => 12:55:57.18   PROCESS - STEPSTART
Pnumber => 3814        Snode     => NSTOP.TEST.350   Xnode     => P
Pname   => NSTOP350    Submitter => S7.TEST.35       DEV.USER
Function=> COPY        Step Name => NSTP5PSH
From Pnode  DSN= \ESCAPE.$DEV.JSDATA.EDIT02
To   Snode  DSN= $DEV.JSDATA.NONSTOP5
Secure+ Protocol>  TLSv1
Cipher Suite>  AES256-SHA
Remote Cert Name>  sterling
________________________________________________________________________________
Date    => 06.26.2008  Time      => 12:55:58.05   PROCESS - STEPEND
Pnumber => 3814        Xlate     =>                   Start Date=> 06.26.2008
Pname   => NSTOP350    Compress  => NO                End Date  => 06.26.2008
Msgid   => SCPA000I    Restart   => NO                Start Time=> 12:55:57.15
Rtncd   => 0           Link Stat => OK                End time  => 12:55:58.01
FDBK    => 0           Snode     => NSTOP.TEST.350   Direction => SENDING
Step    => NSTP5PSH    Submitter => S7.TEST.35       DEV.USER
From Pnode  DSN= \ESCAPE.$DEV.JSDATA.EDIT02
     FILE SIZE=> 23334
     I/O Bytes=> 20000           Xmit Bytes=> 20508           RUsize=>8740
     I/O Recs => 254             Xmit RUs  => 3               Comp%=> 0.00
To   Snode  DSN= $DEV.JSDATA.NONSTOP5
     I/O Bytes=> 20000           Xmit Bytes=> 20508
     I/O Recs => 254             Xmit RUs  =>                 Comp%=> 0.00
                                 Bytes/Sec => 83333.3
Secure+ Protocol>  TLSv1
Cipher Suite>  AES256-SHA
Remote Cert Name>  sterling
  SCPA000I: (RC=0, FDBK="0")
Copy operation successful.
A copy operation completed successfully.

SYSTEM ACTION:

RESPONSE:      None.
```

Select Process Display

When Secure+ Option is enabled for a node, all Copy statements executed on the node display Connect:Direct Secure+ Option parameter settings. When you specify that detail be displayed on the Select Process command, the name of the enabled protocol is displayed along with the negotiated cipher suite. Following is a sample Select Process display:

```
CD.14.>sel proc detail
===============================================================================
3.5.00                    S E L E C T    P R O C E S S
===============================================================================
Process Name    => S75CRC   Submitter=> NSTOP.TEST.350      DEV.USER
Process Number  => 36105      Snode    => S7.TEST.35   Queue   => Exec
Submitter Class => NONE       PlexClass=>                  Priority=> 10
Process File    => \ESCAPE.$AUDIT.TEMP1.PUSHPULE           Retain  =>
Executing LU    => \ESCAPE.$TCP.#L06
CRC Check       => OFF
Execution Class => 0          State    => Exec Prc+PC\Rcv FMH72
FILE SIZE => 3133440
Secure+ Protocol>  TLSv1
Cipher Suite>  AES256-SHA
Remote Cert Name>  sterling
```

Following are the Secure+ Option fields and valid values displayed in a Select Process or Select Statistics report:

Field Name	Field Description	Valid Values
Secure+ Protocol	Specifies which protocol is enabled.	SSL 3.0 | TLS 1.0
Cipher Suite	Specifies the ciphers available for the TLS or SSL session as identified in the parameters (SPNODES) file.	NULL-MD5 EXP-RC4-MD5 RC4-MD5 RC4-SHA EXP-DES-CBC-SHA DES-CBC-SHA DES-CBC3-SHA AES128-SHA AES256-SHA
Remote Cert Name	Specifies the name of the key certificate file used for a remote node.	User-specified

Troubleshooting

Use the following table to help troubleshoot errors generated by AIMS when configuring Secure+ Option:

Error Message	Possible Cause	Solution
Error Opening NetMap file <netmap filename>	Cannot locate the network map file.	Verify the location of the network map file or create it, if necessary.
Error Opening/creating <Secure+ directory>:SPNODES file, error <guardian error>	General disk problems or security access problems.	Ensure that you have the rights to modify the file.
Error Reading local node from NetMap file <netmap filename>	Cannot locate the local node in the network map.	Create a local node in the network map file.
No Local node LOCAL.NODE in NetMap file <netmap filename>	Cannot locate the local node in the network map.	Create a local node in the network map file.
Error Inserting <node name> into SPNode file, err=<guardian error>	General disk problems or security access problems.	Ensure that you have the rights to modify the file.
Error Reading Node <node name> from SPNode file, err=<guardian error>	General disk problems or security access problems.	Ensure that you have the rights to modify the file.
Error positioning in NetMap file <netmap filename>, err=<guardian error>	General disk problems or security access problems.	Ensure that you have the rights to modify the file.
Error Reading Node <node name> from SPNode file, err=<guardian error>	General disk problems or security access problems.	Ensure that you have the rights to modify the file.
SPNode does not exist or is corrupt	The network map definitions have not been imported.	Use the Sync. With NetMap option to recreate an SPNode file.
Node record does not exist	You have not defined the settings for the Local node record.	Use the Administration tool to define settings for the local node record.

Appendix A

Understanding the Certificate File Layout

The SSL and TLS security protocols use a secure server RSA X.509V3 certificate to authenticate your site for any client that accesses the server, and provides a way for the client to initiate a secure session. You obtain a certificate from a certificate authority (CA) or you can create a self-signed certificate. When you obtain a certificate file, a trusted root certificate file, certificate file, and private key are created. You create a key certificate file by combining information about the certificate and the private key file. This appendix describes the layout of the trusted root certificate file and the certificate key file.

Certificate Files

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

When you obtain a certificate from a certificate authority, you receive a trusted root certificate file. Give a copy of this file to any trading partner with whom you will communicate, using Secure+ Option.

A sample trusted root certificate file is provided in this chapter. 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.

User certificates are a set of certificates that describe a chain and include a certificate for the server and a certificate for each certificate authority. The user certificates are detailed in the certificate key file. The server certificate must be identified first in the certificate key file and the root certificate authority must be listed last in the file. The private key for the server certificate must also be defined in the file.

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

Formats

The formats discussed in this section apply to the certificate files used with Secure+ Option. The formats are illustrated in the sample certificate files on page 39.

General Object Format

All objects are formatted in the PEM style. Below is a sample object format:

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

and end with:

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

In this sample, <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 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 and SSL servers understand them. Both Netscape and Microsoft 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+ and is stored in the Secure+ parameters file. Additional encryption is used to prevent the passphrase from being discovered.

Sample Certificate Files

In the following sample user certificate, a private key is followed by the server certificate, and then the root certificate.

Sample User Certificate

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICCDAaBgkqhkiG9w0BBQMwDQQIIfYyAEFKaEECAQUEggHozdmgGz7zbC1mcJ2r
.
.
.
IGpupStY5rLqqQ5gwLn45UWgzy6DM96CQg6+Dyn0N9d1M5lIg2wlnUwE8vI=
-----END ENCRYPTED PRIVATE KEY-----

User/Server Certificate
-----BEGIN CERTIFICATE-----
MIICUDCCAdoCBDaM1tYwDQYJKoZIhvcNAQEEBQAwgY8xCzAJBgNVBAYTAlVTMRMw
.
.
.
iKlsPBRbNdq5cNIuIfPS8emrYMs=
-----END CERTIFICATE-----

// Final Root Certificate (optional)
-----BEGIN CERTIFICATE-----
MIICUDCCAdoCBDaM1tYwDQYJKoZIhvcNAQEEBQAwgY8xCzAJBgNVBAYTAlVTMRMw
.
.
.
iKlsPBRbNdq5cNIuIfPS8emrYMs=
-----END CERTIFICATE-----
```

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

Sample Root Certificate

```
RSA Commercial CA - exp. Dec 31, 2008
-----BEGIN CERTIFICATE-----
MIICUDCCAdoCBDaM1tYwDQYJKoZIhvcNAQEEBQAwgY8xCzAJBgNVBAYTAlVTMRMw
.
.
.
iKlsPBRbNdq5cNIuIfPS8emrYMs=
-----END CERTIFICATE-----

RSA Commercial CA - exp. Dec 31, 2010
-----BEGIN CERTIFICATE-----
MIICUDCCAdoCBDaM1tYwDQYJKoZIhvcNAQEEBQAwgY8xCzAJBgNVBAYTAlVTMRMw
.
.
.
iKlsPBRbNdq5cNIuIfPS8emrYMs=
-----END CERTIFICATE-----
```

Glossary

A

Adjacent Node Record

An entry in the parameters file that defines the security settings used to communicate with a trading partner. An adjacent node record must be defined for every trading partner you communicate with.

Administration Tool (Admin Tool)

The Secure+ Option tool that enables configuring and maintaining the Secure+ Option environment. This is the only tool you can use to configure and maintain Secure+ Option.

Asymmetric Keys

A separate but integrated user key pair comprised of one public key and one private key. Each key either encrypts information or decrypts information but does not perform both functions.

Authentication

The process of verifying that a particular name really belongs to a particular entity.

C

Certificate

A document obtained from a certificate authority by generating a certificate signing request (CSR) that contains specific information in

a specific format about the requester. It typically contains (1) distinguished name and public key of the server or client; (2) distinguished name and digital signature of the certificate authority; (3) period of validity (certificates expire and must be renewed); and (4) administrative and extended information. The certificate authority analyzes the CSR fields, validates the accuracy of the fields, generates a certificate, and sends it to the requester.

Certificate Authority (CA)

A company responsible for verifying and processing certificate requests, and issuing and managing certificates. The CA you choose should be one that your trading partners trust. You must meet the requirements for the CA you choose.

Certificate Revocation List

A list of certificates that have been revoked.

Certificate Signing Request

An output file sent through E-mail to a certificate authority to request an X.509 certificate.

Cipher Suite

A cryptographic algorithm that enables you to encrypt and decrypt files and messages.

Cipher Text

Data that is encrypted. Cipher text is unreadable until it is converted into plain text (decrypted) with a key.

Client

The entity that initiates a communication session. See also Primary Node.

Client Authentication

An optional level of security that requires the client or PNODE to authenticate its identity to the server by sending its certificate. The SNODE must request a certificate before the client sends it.

Configuration File

A file that contains instructions and definitions upon which the system bases its processing.

D

Data Confidentiality

Ensuring that data remains private during transmission.

Decryption

Any process to convert cipher text back into plain text.

Digital Certificate

A specifically formatted document that allows you to authenticate or identify yourself to a Web browser, an E-mail reader, a secure server, or a client. It contains information on who you are, your relevant details, and who issued the certificate. A certificate can be tied to an E-mail address, a Web server or a company, and in each case the certificate is used for different things. A basic E-mail certificate allows you to prove that you are who you say you are. It also allows you to store more information about yourself such as your place of work or telephone contact details. The certificate also contains your public key.

Data Integrity

Ensuring that information is not altered during transmission.

Digital Signature

Processing using public and private keys to verify participant identity in the exchange of electronic information. A digital signature uniquely authenticates the person *signing* an electronic document much like a human signature uniquely identifies the person who signs a physical document. Because a private key is unique to each person, a value encrypted using the sender's private key and subsequently decrypted using the sender's public key authenticates the senders's identity.

E

Encryption

Any process that converts plain text into cipher text.

Encryption Algorithm

The set of mathematical logic that encrypts or decrypts data.

F

FTP

Internet application and network protocol for transferring files between host computers. File transfer protocol.

I

Integrity

Assurance that data is not modified (by unauthorized persons) during storage or transmittal.

K

Key Certificate File

A file stored on the client that contains an encrypted message to identify the client and enable client/server authentication during secure FTP connections.

Keys

A collection of bits, usually stored in a file, which encrypts or decrypts a message.

L

Local Node Record

The base record in a parameters file that defines the Connect:Direct HP NonStop server. It includes the most commonly used settings at a site and is the central node through which all communication is filtered.

Depending upon how each adjacent node record is configured, trading partner node records may use settings that are defined in the local node record.

N

Network Map (Netmap)

The file that identifies all valid Connect:Direct HP NonStop nodes in a network including a local node record and an adjacent node record for each trading partner. The network map also defines the rules or protocols used by each node when communicating with the local Connect:Direct HP NonStop node.

P

Passphrase

Similar to a password but can be any characters, including spaces. A passphrase is stronger than a password, although not many programs support the use of a passphrase.

Password

A character-limited word or phrase that establishes identity to allow access to a system. Generally, a password is composed of letters, numbers, special characters, or a combination of these characters.

Primary Node (PNODE)

The node that submits the Connect:Direct HP NonStop Process to the secondary node (Snode). In every communication, you must have a PNODE and an SNODE.

Private Key

The secret key of a public-private key cryptography system. This key enables you to *sign* outgoing messages and decrypt incoming messages.

Proof of Data Origin

A method of verifying the identity of the sender and that information is not altered during an electronic exchange.

Public Key

The public key of a public-private key cryptography system. This key confirms *signatures* on incoming messages or encrypts a file or message so that only the holder of the private key can decrypt the file or message. A public key is disseminated freely to clients and servers via certificates signed by a certificate authority (CA).

S

Secondary Node (SNODE)

The Connect:Direct node that interacts with the primary node (PNODE) during Connect:Direct HP NonStop Process execution and is the non-controlling node. Every Process has one secondary node and one primary node.

Secure Sockets Layer (SSL)

A protocol that provides secure communications with transport protocols, including FTP, over TCP/IP. It is an open, non-proprietary Internet protocol that is widely adopted as standard. SSL ensures point-to-point security, meaning that the data is secured as it is transmitted across a single socket.

Self-Signed Certificate

A self-generated certificate that identifies your organization. It is often used during the period between your request and receipt of a certificate from a public certificate authority. If self-signed certificates are used, the trusted root signing certificate must be installed in the client manually.

Server

The location that receives communication from a client.

Session Key

Cryptography key intended to encrypt data for a limited period of time, typically only for a single communications session between a pair of entities. When the session is over, the key is discarded and a new one established when a new session takes place.

T

Third-Party Certificate

A certificate, other than those that are preconfigured for the application, that identifies an organization. If third-party certificates are used by the server, the corresponding trusted certificate must be installed in the client manually.

Transport Layer Security (TLS)

A protocol that provides secure communications with transport protocols, including FTP, over TCP/IP. It is an open, non-proprietary Internet protocol that is widely adopted as standard. TLS ensures point-to-point security, meaning that the data is secured as it is transmitted across a single socket.

Both the SSL protocol and the TLS protocol manage secure communication in a similar way. However, TLS provides a more standard, more secure method for managing authentication and exchanging messages. TLS uses Key-Hashing for Message Authentication Code (HMAC), to ensure that a record cannot be altered while traveling over an open network such as the Internet. TLS defines the Enhanced Pseudorandom Function (PRF), used to generate key data, with the HMAC and uses two hash algorithms to guarantee security. 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 exposed.

Trusted Root Certificate File

A file stored in a local directory on the client that contains a list of trusted sources. During FTP connections, the client compares the server certificate, or vice versa, to the trusted root certificate file to determine if the server certificate was signed by a trusted source. The client can establish a secure FTP connection if a trusted source signed the server certificate.

U

Unsecure Connection

A connection that has no security.

X

X.509 CertificateV3

Public key certificate specification developed as part of the X.500 directory specification, and often used in public key systems.

Index