Sterling Commerce
Product Documentation

Connect:Direct® for z/OS Versions 4.7.02 and 4.8.01

Strong Password Encryption Guide

Sterling Commerce
An IBM Company

Connect:Direct for z/OS Strong Password Encryption Guide

First Edition

Sterling Commerce, Inc.

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

Contents

Connect:Direct for z/OS Strong Password Encryption Guide

The *Connect:Direct for z/OS Strong Password Encryption Guide* document supplements Connect:Direct version 4.7 and 4.8 documentation. The Strong Password Encryption (SPE) feature was originally released with PUT 4702 in May 2009 and release with PUT 4801 in October 2009. See the *Maintenance Notes* for the PUT 4702 and PUT 4801 maintenance package for complete instructions on how to apply the code to the base release. The *Maintenance Notes* also include a complete description of all other features and fixes included in that maintenance package. For more directions on how to locate this information, see *Customer Center Portal User Name and Password* on page 12 and *Obtaining Product Updates* on page 12.

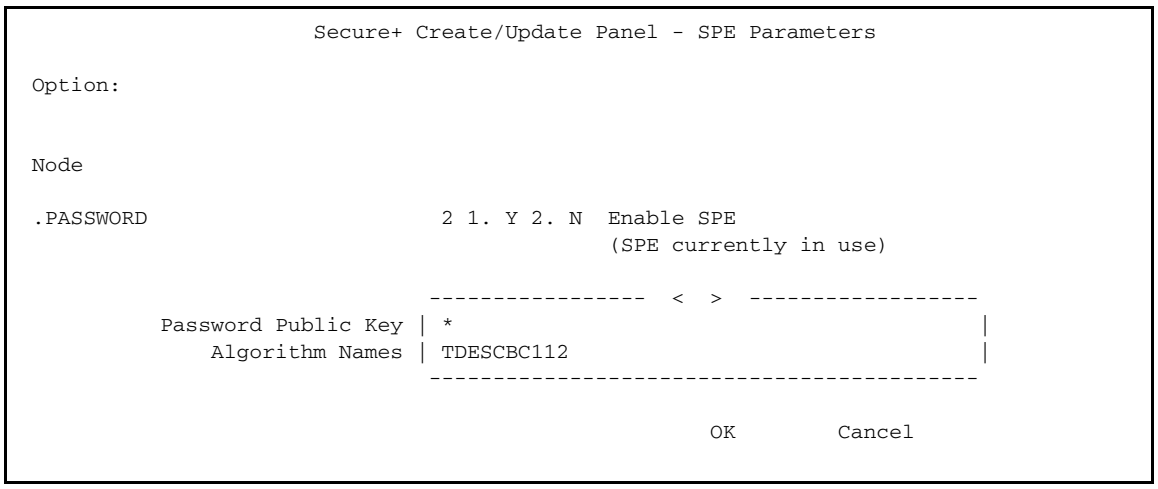
For information on the entire documentation set for base release, see *Connect:Direct Documentation* on page 13.

Using Strong Password Encryption to Enhance Security

Passwords can be used in Connect:Direct in the following circumstances:

- When Processes are submitted
- During API signons
- When the AUTH file is maintained

You can use Strong Password Encryption (SPE) to secure passwords at rest within the Connect:Direct TCQ and AUTH files. SPE uses the TDESCBC112 encryption algorithm of Connect:Direct Secure+ Option so if you have the Secure+ Option component installed and configured, and then take the necessary steps to enable the SPE feature (see *Implementing Strong Password Encryption* on page 7), SPE will be in effect. To confirm that SPE is in effect, you can return to the Secure+ Create/Update Panel - SPE Parameters screen and make sure you see the message, (SPE currently in use).



When you restart Connect:Direct, Connect:Direct generates a encryption key pair and performs a password conversion of the TCQ and AUTH files. Each time you restart Connect:Direct, a new encryption key pair is generated and applied to passwords in the TCQ and AUTH files. Connect:Direct performs internal validation checks to ensure the passwords are usable and encrypted in the proper manner, but in the event of an error during the encryption process, you will see either a SITA461I or SITA463E message, *Strong Password Encryption Error,* when you try to initialize Connect:Direct. To see more detailed information about individual errors related to the general failure, see the ESTAE trace output and *Troubleshooting Possible SPE Problems* on page 10.

If SPE has been enabled properly, when a Process is submitted, passwords contained in the Process are encrypted before it is written to the TCQ file. If the Process is submitted using the Extended Submit Facility (ESF), passwords remain in the non-SPE format until Connect:Direct can process the ESF submit via product initialization or ESF timer services. When the ESF can be established, Strong Password Encryption will be performed and the TCQ file updated.

Once SPE has been implemented, passwords in the TCQ and AUTH files will be in the SPE format and will be unusable if SPE is inappropriately disabled by deleting the .PASSWORD record. The SPAdmin tool does not allow you to use the Delete node table line command to delete the .PASSWORD record. To disable SPE properly, see *Disabling Strong Password Encryption* on page 9. Follow that procedure and then reinitialize Connect:Direct. This initialization with SPE disabled will convert the passwords in the TCQ and AUTH to the non-SPE encryption format.

In the event that this process of converting to and from the SPE format should fail, all passwords in the TCQ and AUTH files will be unusable by Connect:Direct. The Connect:Direct administrator must then reset the passwords. For more information, see *Troubleshooting Possible SPE Problems* on page 10.

Documentation Updates

This section describes updates to the base release 4.7 and 4.8 Connect:Direct documentation.

Connect:Direct Secure+ Option for z/OS Implementation Guide

Add the following information to reflect the new Strong Password Encryption feature.

Chapter 1, About Connect:Direct Secure+ Option

Replace the *Parameters File* section.

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 a remote node record for each trading partner who uses Secure+ Option to perform a secure connection. The local node record defines the most commonly used security and protocol settings at the site and can be used as a default for one or more remote node records. Each remote node record defines the specific security and protocol used by a trading partner.

For additional security, the 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.

To protect Connect:Direct passwords in the TCQ and AUTH files, you can add a .PASSWORD record to the Secure+ Option parameters file. After you create this record, enable the Strong Password Encryption (SPE) feature, and restart Connect:Direct, SPE protects Connect:Direct passwords stored in the TCQ and AUTH files and sent in Connect:Direct Processes. For more information on using this feature, refer to *Implementing Strong Password Encryption*.

Chapter 4, Using the Secure+ Admin Feature and Populating the Parameters File

Add this section to the end of this chapter.

Implementing Strong Password Encryption

To implement the Strong Password Encryption (SPE), you add an SPE record to the Secure+ Option parameters file in the same way you would any remote node record. After you go through the following procedure and restart Connect:Direct, the SPE feature will be in effect.

To add an SPE record to the Secure+ Option parameters file and enable the SPE feature:

1. Select **Edit** from the **Secure+ Admin Tool Main Screen** and press **Enter** to display the **Edit** menu.
2. On the **Edit** menu, select **1** to select **Create/Update Record** and press **Enter** to display the **Secure+ Create/Update Node Identification** panel.

3. On the Node Identification panel:
   a. Type **.password** in the **Node** field.
   b. Type **2** next to the **Local** field.

```
                    Secure+ Create/Update Panel - Node Identification

Option:

EA Parameters           SSL Parameters    TLS Parameters     STS Parameters

Node
.password               2 1. Local
                          2. Remote

Alias
Names:                  TCP Information:
                          IPaddr:
                          Port:
 Import Remote Keys     Get Record                OK        Cancel
```

   c. Press **Enter** to display the **Secure+ Create/Update Panel - SPE Parameters** screen.
4. On the **SPE Parameters** panel, type **1** next to the **Enable SPE** field.

```
                   Secure+ Create/Update Panel - SPE Parameters

Option:


Node

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

                               -----------------  <  >  ------------------
          Password Public Key | *                                         |
              Algorithm Names | TDESCBC112                                |
                               -------------------------------------------

                                                    OK        Cancel
```

   Press **Enter** to enable SPE and finish creating the SPE record by clicking **OK**.
5. Save the parameters file using the procedure in Chapter 12, *Enable and Validate Secure+ Operation*.
6. Restart Connect:Direct.

7. To verify that Connect:Direct Secure+ Option initialization is complete along with the SPE feature, after you restart Connect:Direct, review the started task output for the following messages interspersed with the other initialization messages:

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

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

Disabling Strong Password Encryption

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

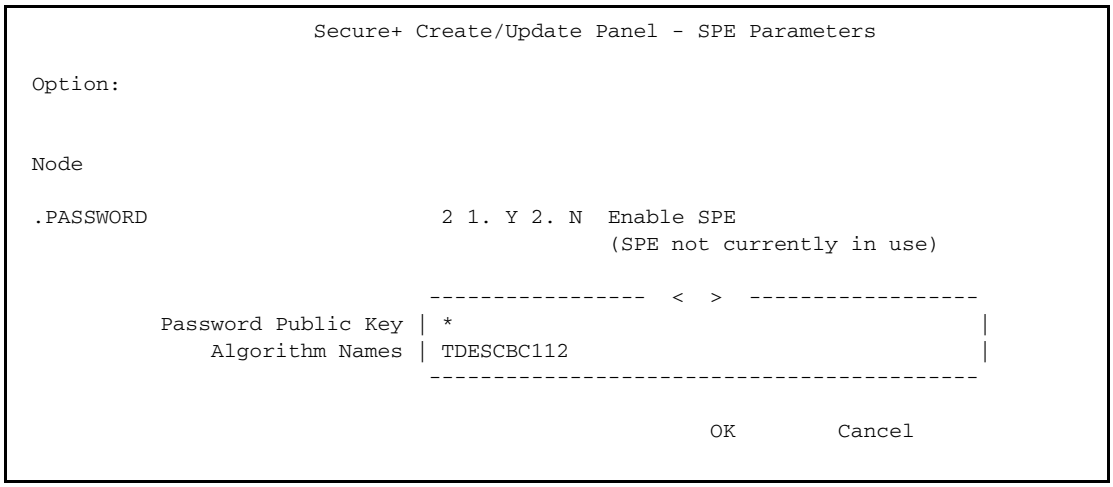
To disable the SPE feature:

1. Start the Secure+ Admin Tool to display the **Secure+ Admin Tool: Main Screen**, which displays the nodes populated from the Connect:Direct network map along with other records in the Secure+ Option parameters file.

```
  File  Edit  Key Management  Help
-------------------------------------------------------------------------------
                                                                      Row 1 of 7
 SC.DUB.DOVER1        Secure+ Admin Tool: Main Screen
 Option ===>                                                          Scroll CSR

                          Table Line Commands are:

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

                           Secure
LC Node Name         Type  123C  Override Encryption Signature ExtAuth Autoupd
-- ----------------  ---- ------ -------- ---------- --------- ------- -------
   .CLIENT            R    NNNN     Y         N          N        N       N
   .EASERVER          R    N*YN     N         N          N        N       N
   .PASSWORD          R    Y***     *         *          *        *       *
   SC.DUB.DOVER1      L    NNNN     Y         N          N        N       N
   SC.DUB.DOVER2      R    NNYN     Y         N          N        N       N
   SC.DUB.DOVER3      R    NNYN     Y         N          N        N       N
   SC.DUB.DOVER4      R    NYNY     Y         N          N        N       N
****************************** BOTTOM OF DATA ********************************
```

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

3. On the **SPE Parameters** panel, type **2** next to the **Enable SPE** field and press **Enter**.



4. Save the parameters file using the procedure in Chapter 12, *Enable and Validate Secure+ Operation*.
5. Restart Connect:Direct.

Troubleshooting Possible SPE Problems

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

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

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

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

Condition: Because of SPE errors, Connect:Direct either initializes with a SITA461I message or does not initialize at all with a SITA463E message.

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

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

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

Chapter 16, Troubleshooting

Add this note to the beginning of the chapter.

Note: For all errors related to Strong Password Encryption, see *Troubleshooting Possible SPE Problems*.

Connect:Direct for z/OS Installation Guide

Add the following information to reflect the new Strong Password Encryption feature.

Appendix D, Initialization and License Key Error

Add this note to the beginning of the *Initialization Errors* section.

Note: For all initialization errors related to Strong Password Encryption, see *Troubleshooting Possible SPE Problems* in the *Connect:Direct Secure+ Option for z/OS Implementation Guide*.

Customer Center Portal User Name and Password

The Customer Center portal offers you a single location to administer everything associated with your Sterling Commerce products and services. It provides quick access to online tools, on-demand applications, community forums, product information, industry news, support updates, and support case management.

To log into the Customer Center, go to http://customer.sterlingcommerce.com. If you do not have a Customer Center user name and a password, click the Join Now link and follow the instructions for new users. If you have a Customer Center account, define a new password the first time you log on.

Obtaining Product Updates

Product updates and update summaries, including issues resolved for previous versions of Sterling Control Center, are available on the Sterling Commerce Customer Center Web site.

To obtain product updates:

1. Log on to your Customer Center Web site.
2. Click **Support Center**.
3. From the **Product Support** menu on the left navigation bar, click **Connect > Product Updates & Downloads >** Connect:Direct.
4. Locate the updates for your product and platform and click **View/Download**.

Connect:Direct Documentation

The Connect:Direct documentation is available on the product media or the documentation CD-ROM. You can view or download documentation from the Sterling Commerce Customer Center Web site at http://customer.sterlingcommerce.com. You need a Customer Center user name and password. See *Obtaining Product Updates* on page 12 for instructions on obtaining your user name and password.

Access to PDF files requires the latest version of Adobe Acrobat Reader, which you can download at www.adobe.com. You can search for a specific word or phrase in the text of an open PDF document or a set of PDF documents in a specified location. See the Adobe Acrobat Reader Help for instructions on using the Search feature. The search lists all instances of the specified string.

The Connect:Direct documentation consists of:

- *Connect:Direct for z/OS Administration Guide*
- *Connect:Direct for z/OS User's Guide*
- *Connect:Direct for z/OS Installation Guide*
- *Connect:Direct for z/OS Quick Reference*
- *Connect:Direct for z/OS CICS Administration and User's Guide*
- Connect:Direct *for z/OS Facilities Guide*
- *Connect:Direct Secure+ Option for z/OS Implementation Guide*
- *Sterling External Authentication Server Help*
- *Understanding Connect:Direct Processes*
- *Connect:Direct Compatibility and Connectivity Chart*
- *Connect:Direct for z/OS File Agent Configuration Guide and Help*

Documentation for the following supplemental products is available on additional distribution media and from links in the Documentation Library on the Sterling Commerce Customer Center Web site:

- Connect:Direct Browser User
- Sterling Certificate Wizard
- Sterling External Authentication Server

After you log in to the Customer Center web site and click **Support Center**, use the Self Support Tool, Documentation Library to access additional documentation links.

The latest updates to and information on Connect:Direct Processes are available on the Managed File Transfer (MFT) Documentation > Connect:Direct Documentation web page in Customer Center.

The *Connect:Direct Compatibility and Connectivity Chart* contains the latest information about currently supported versions and platforms of Connect:Direct and their compatibility and connectivity. This document is available as a PDF file on the Connect:Direct Documentation web page.