Sterling Connect:Direct Secure Plus Enhancements

Contents

Chapter 1. Sterling Connect:Direct Secure Plus Enhancements Overview

Overview

The IBM® Sterling Connect:Direct® Secure Plus Enhancements document supplements the documentation for IBM Sterling Connect:Direct for Microsoft Windows and IBM Sterling Connect:Direct for UNIX.

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

- Turning Sterling Connect:Direct Secure Plus on or off for a particular session
- Specifying one or more cipher suites to use for encryption instead of the default cipher suites
- Encrypting only the control block contained in Function Management Headers (FMHs), which includes session information, instead of the files being transferred if performance is a factor.

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

Note: This document assumes you are very familiar with the Sterling Connect:Direct Process language. To see the complete documentation, see the *IBM Sterling Connect:Direct Process Language Reference Guide*.

Requirements to Use Overrides

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

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

Processing Hierarchy

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

- The Sterling Connect:Direct Secure Plus parameter file is the default and base of the hierarchy.
- The PROCESS statement overrides the Sterling Connect:Direct Secure Plus parameter file.
- The SUBMIT statement overrides the PROCESS statement.
- Each COPY statement overrides the effective settings of the session established by the Sterling Connect:Direct Secure Plus parameter file and PROCESS or SUBMIT overrides for the duration of the COPY statement.

Data Encryption Feature

The data encryption feature allows the encryption of only the control block information in Function Management Headers (FMHs). FMHs include the user ID, password, and file name for all of the files that are sent to a particular trading partner or for one particular file. CPU utilization decreases dramatically because data encryption is restricted to the control block information rather than both the preliminary FMH information exchanged during the handshake to set up the session and the files that are transferred. By default, the Enable Data Encryption option is set to yes. This option encrypts both the information necessary to establish a session and the data transferred during the session.

After you set up the default encryption option you want to use on a general basis in the Sterling Connect:Direct Secure Plus parameter file definitions, you can override the default option through individual PROCESS, SUBMIT, and COPY statements.

Encrypt Only Security Handshake Information

To define the default encryption definition for a local or remote note, you must edit that node's record in the Sterling Connect:Direct Secure Plus parameter file for each site. By default if security is turned on, the system encrypts both the data that is being transferred and the information necessary to set up the session.

Note: To override the encryption option that is defined in the Sterling Connect:Direct Secure Plus parameter file, see the ENCRYPT.DATA option for the SECURE keyword in “Sterling Connect:Direct Secure Plus Override Features” on page 3.

Adjust Data Encryption Settings by Using SPAdmin

About this task

To change the default behavior to encrypt only the security handshake information by using the Secure Plus Administrator tool, follow this procedure.

Note: To override the encryption option that is defined in the Sterling Connect:Direct Secure Plus parameter file, see the ENCRYPT.DATA option for the SECURE keyword in “Sterling Connect:Direct Secure Plus Override Features” on page 3.

Procedure

1. Open the local or remote node record.
2. Click the **TLS/SSL Protocol** tab.
3. Click **No** for the Enable Data Encryption option on the **TLS/SSL Options** dialog box.
4. Click **OK** to update the node record.

Adjust Data Encryption Settings by Using Secure Plus CLI

To change the default behavior to encrypt only the security handshake information by using the Secure Plus command line interface, use the ssltlsenableenc parameter. This parameter is a part of the update localnode, create remotenode and update remotenode commands. You can enable or disable the data encryption feature with the ssltlsenableenc parameter by setting it to yes or no:

- ssltlsenableenc=y - Setting the parameter to yes encrypts both the control block information that is contained in FMHs and the file data that is transferred. This is the default setting.
- ssltlsenableenc=n - Setting the parameter to no encrypts only the control block information that is contained in FMHs, and does not encrypt the file data. This option enhances performance and can be used if the file data is not considered sensitive in nature.

Sterling Connect:Direct Secure Plus Override Features

Sterling Connect:Direct Secure Plus allows you to perform exception processing by using one or more of the following override functions:

- Turn on security when non-secure sessions are the default
- Select the protocol when no-secure sessions are the default
- Specify one or more cipher suites to override the default cipher suites defined in the Sterling Connect:Direct Secure Plus parameter file
- Turn off security when secure sessions are the default (if OVERRIDE=Y is specified in the remote node record settings in the parameter file)
- Encrypt only the FMH control block information, which includes the user ID and password

Overriding Sterling Connect:Direct Secure Plus Defaults in a PROCESS or SUBMIT Statement

The SECURE keyword in both PROCESS and SUBMIT statements lets you specify options to override defaults in the Sterling Connect:Direct Secure Plus parameter file. For an environment where security is turned on by default, you can turn off security for a particular Process.

Conversely, you can use the SECURE keyword to turn on security for a specific session by selecting a protocol (SSL, TLS, or STS) when non-secure sessions are the default. You can also select one or more cipher suites and the type of encryption you want performed.

Syntax

The following syntax example shows the options available for the SECURE keyword for both the PROCESS and SUBMIT statements:

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

Keyword Descriptions

The following table describes these options in more detail.

Parameter	Description
OFF	If the remote node in the Sterling Connect:Direct Secure Plus parameter file specifies OVERRIDE=Y for this node, attempts to start the session as a non-secure session. The session will be successfully established if: • The SNODE has no remote node entry for this node in its Sterling Connect:Direct Secure Plus parameter file. • The SNODE's remote node entry in its Sterling Connect:Direct Secure Plus parameter file for this node specifies that all Sterling Connect:Direct Secure Plus protocols are disabled. • The SNODE's remote node entry in its Sterling Connect:Direct Secure Plus parameter file for this node specifies OVERRIDE=Y. • The Sterling Connect:Direct Secure Plus parameter file specifies data encryption be disabled and is configured for SSL,TLS, or STS.
SSL ¦ TLS ¦ STS	If the remote node in the Sterling Connect:Direct Secure Plus parameter file specifies OVERRIDE=Y, attempts to start the session as a secure session using the specified protocol. The session will be successfully established if: • The SNODE's remote node entry in its Sterling Connect:Direct Secure Plus parameter file for this node specifies that the specified protocol is to be used. • The SNODE's remote node entry in its Sterling Connect:Direct Secure Plus parameter file for this node specifies OVERRIDE=Y.

Parameter	Description
,Cipher Suite	Must be used in conjunction with the SSL | TLS | STS option. Specifies the cipher suite for Sterling Connect:Direct to use when executing the Process overriding the protocol and cipher suite defined in the Sterling Connect:Direct Secure Plus parameter file, for example, RSA_WITH_3DES_EDE_CBC_SHA. If the remote node in the Sterling Connect:Direct Secure Plus parameter file specifies OVERRIDE=Y for this node, attempts to start the session using the protocol and cipher suite provided. The session is established if: • The appropriate protocol and cipher suite are specified as a pair in the PROCESS/SUBMIT statement. • The SNODE's remote entry in its Sterling Connect:Direct Secure Plus parameter file for this node specifies a matching protocol and at least one matching cipher suite from the PNODE list. • The SNODE's remote entry in its Sterling Connect:Direct Secure Plus parameter file for this node specifies OVERRIDE=Y. (This only applies to overriding the protocol–not the cipher suite.)

Parameter	Description
,(Cipher suite list)	Must be used in conjunction with the SSL | TLS | STS option. Specifies a list of cipher suites for Sterling Connect:Direct to use when executing the Process overriding the protocol and cipher suites defined in the Sterling Connect:Direct Secure Plus parameter file. If the remote node in the Sterling Connect:Direct Secure Plus parameter file specifies OVERRIDE=Y for this node, attempts to start the session using the protocol and one of the cipher suites provided. The session is established if: • The appropriate protocol and cipher suites are specified as a pair in the PROCESS/SUBMIT statement. • The SNODE's remote entry in its Sterling Connect:Direct Secure Plus parameter file for this node specifies a matching protocol and at least one matching cipher suite from the PNODE list. • The SNODE's remote entry in its Sterling Connect:Direct Secure Plus parameter file for this node specifies OVERRIDE=Y. (This only applies to overriding the protocol–not a cipher suite.) The cipher suite list must be enclosed in parentheses and each cipher suite separated by a comma or space, for example, (RSA_AES_128_SHA, RSA_AES_256_SHA, RSA_WITH_DES_CBC_SHA)
,ENCRYPT.DATA=Y|N or ENC=Y|N	Depending on the option chosen, encrypts both the control block information contained in Function Management Headers (FMHs) and the files being transferred (ENC=Y) or encrypts only the FMHs (ENC=N). The type of encryption chosen will be performed if: • The SNODE's remote node entry in its Sterling Connect:Direct Secure Plus file for this node specifies OVERRIDE=Y. • ENCRYPT.DATA must be the last (or only) value specified on the SECURE= parameter. • Both sides of the connection support ENCRYPT.DATA= for SSL/TLS.

Overriding the Data Encryption Setting in a COPY Statement

By using the COPY statement's SECURE parameter in a Sterling Connect:Direct Process to override the data encryption setting in the Sterling Connect:Direct Secure Plus parameter file or Process statement and enabling the override feature in the remote node record, you can disable data encryption for a particular file transfer. The control block information is always encrypted if Sterling Connect:Direct Secure Plus is enabled.

Note: The SECURE parameter along with the CKPT and COMPRESS parameters can be placed in between the FROM and TO clauses or after them but cannot be divided between the clauses. You can also place these parameters outside these clauses at the end of the COPY statement.

Syntax for SECURE Keyword in TLS/SSL

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

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

Syntax for SECURE Keyword in STS

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

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

Note: The behavior of ENCRYPT.DATA for STS is unchanged. For more information, see the *IBM Sterling Connect:Direct Process Language Reference Guide*.

Chapter 2. Override Security Setting in Process Statement Examples

Disable Security when Default is Secure Sessions Example

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

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

```
tlsoff process snode=othertp secure=off
```

Enable TLS when Default is Non-Secure Sessions Example

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

```
tlson process snode=othertp secure=tls
```

Override Default Cipher Suite Example

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

- Enabled the TLS protocol
- Specified OVERRIDE=Y in both the Local and Remote Node records
- Selected RSA_WITH_RC4_128_MD5 as the cipher suite to use when executing Processes

To override the default cipher suite and use RSA_WITH_3DES_EDE_CBC_SHA when executing a particular Process, use the following PROCESS statement:

```
newcipher process snode=othertp secure=(TLS,RSA_WITH_3DES_EDE_CBC_SHA)
```

Note: The SNODE's remote node entry in the Sterling Connect:Direct Secure Plus parameter file for the PNODE must specify TLS_RSA_WITH_3DES_EDE_CBC_SHA in addition to TLS_RSA_WITH_RC4_128_MD5.

Replace Single Default Cipher Suite with a Cipher List Example

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

- Enabled the TLS protocol
- Specified OVERRIDE=Y in both the Local and Remote Node records
- Selected RSA_WITH_RC4_128_MD5 as the cipher suite to use when executing Processes

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

```
newciphers process snode=othertp
secure=(TLS,(RSA_WITH_3DES_EDE_CBC_SHA,RSA_AES_128_SHA,
RSA_AES_256_SHA,RSA_WITH_DES_CBC_SHA) )
```

Note: The SNODE's remote node entry in the Sterling Connect:Direct Secure Plus parameter file for the PNODE must specify at least one of the cipher suites specified in the PROCESS statement override.

Elect to Not Encrypt Data File Example

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

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

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

```
encno process snode=othertp secure=(encrypt.data=n)
```

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

Override Settings in STS Example

The trading partners agreed by default all sessions are none-secure and chose STS as the default protocol when secure transfers are required. However, all parameters required to perform the handshake to establish an STS session are defined in the Remote Node records. Both partners specified the following configuration in their Sterling Connect:Direct Secure Plus parameter files:

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

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

```
sample process snode=the.other.node secure=sts
*
copyfile copy from (pnode file=test.input)
              to   (snode file=test.output)
              secure=(enc=y,sig=y)
              pend
```