



Configuring Cisco TrustSec Fibre Channel Link Encryption

This chapter provides an overview of the Cisco TrustSec Fibre Channel (FC) Link Encryption feature and describes how to configure and set up link-level encryption between switches.

This chapter includes the following topics:

- [Information About Cisco TrustSec FC Link Encryption section, page 32-177](#)
- [Guidelines and Limitations section, page 32-178](#)
- [Configuring Cisco TrustSec Fibre Channel Link Encryption section, page 32-179](#)
- [Configuring ESP Settings section, page 32-181](#)
- [Verifying Cisco TrustSec Fibre Channel Link Encryption Configuration section, page 32-185](#)

Information About Cisco TrustSec FC Link Encryption

Cisco TrustSec FC Link Encryption is an extension of the Fibre Channel-Security Protocol (FC-SP) feature and uses the existing FC-SP architecture to provide integrity and confidentiality of transactions. Encryption is now added to the peer authentication capability to provide security and prevent unwanted traffic interception. Peer authentication is implemented according to the FC-SP standard using the Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) protocol.



Note

Cisco TrustSec FC Link Encryption is currently only supported between Cisco MDS switches. This feature is not supported when you downgrade to software versions which do not have the Encapsulating Security Protocol (ESP) support.

This section includes the following topics:

- [Supported Modules section, page 32-177](#)
- [Cisco TrustSec FC Link Encryption Terminology section, page 32-178](#)
- [Support for AES Encryption section, page 32-178](#)

Supported Modules

The following modules are supported for the Cisco TrustSec FC Link Encryption feature:

- 1/2/4/8 Gbps 24-Port Fibre Channel switching module (DS-X9224-96K9)
- 1/2/4/8 Gbps 48-Port Fibre Channel switching module (DS-X9248-96K9)
- 1/2/4/8 Gbps 4/44-Port Fibre Channel switching module (DS-X9248-48K9)

Cisco TrustSec FC Link Encryption Terminology

The following Cisco TrustSec FC Link Encryption-related terms are used in this chapter:

- **Galois Counter Mode (GCM)**—A block cipher mode of operation providing confidentiality and data-origin authentication.
- **Galois Message Authentication Code (GMAC)**—A block cipher mode of operation providing only data-origin authentication. It is the authentication-only variant of GCM.
- **Security Association (SA)**—A connection that handles the security credentials and controls how they propagate between switches. The SA includes parameters such as salt and keys.
- **Key**—A 128-bit hexadecimal string that is used for frame encryption and decryption. The default value is zero.
- **Salt**—A 32-bit hexadecimal number that is used during encryption and decryption. The same salt must be configured on both sides of the connection to ensure proper communication. The default value is zero.
- **Security Parameters Index (SPI) number**—A 32-bit number that identifies the SA to be configured to the hardware. The range is from 256 to 4,294,967,295.

Support for AES Encryption

The Advanced Encryption Standard (AES) is the symmetric cipher algorithm that provides a high-level of security, and can accept different key sizes.

The Cisco TrustSec FC Link Encryption feature supports the 128-bit AES for security encryption and enables either AES-GCM or AES-GMAC for an interface. The AES-GCM mode provides encryption and authentication of the frames and AES-GMAC provides only the authentication of the frames that are being passed between the two peers.

Guidelines and Limitations

This section lists the guidelines for Cisco TrustSec FC Link Encryption:

- Ensure that Cisco TrustSec FC Link Encryption is enabled only between MDS switches. This feature is supported only on E-ports or the ISLs, and errors will result if non-MDS switches are used.
- Ensure that the peers in the connection have the same configurations. If there are differences in the configurations, a “port re-init limit exceeded” error message is displayed.
- Before applying the SA to the ingress and egress hardware of a switch interface, ensure that the interface is in the admin shut mode.

Configuring Cisco TrustSec Fibre Channel Link Encryption

This section includes the following topics:

- [Enabling Cisco TrustSec FC Link Encryption section, page 32-179](#)
- [Setting Up Security Associations section, page 32-179](#)
- [Setting Up Security Association Parameters section, page 32-180](#)

Enabling Cisco TrustSec FC Link Encryption

By default, the FC-SP feature and the Cisco TrustSec FC Link Encryption feature are disabled in all switches in the Cisco MDS 9000 Family.

You must explicitly enable the FC-SP feature to access the configuration and verification commands for fabric authentication and encryption. When you disable this feature, all related configurations are automatically discarded.

To enable FC-SP for a Cisco MDS switch, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# feature fcsp	Enables the FC-SP feature.
	switch(config)# no feature fcsp	Disables (default) the FC-SP feature in this switch.

Setting Up Security Associations

To perform encryption between the switches, a security association (SA) needs to be set up. An administrator manually configures the SA before the encryption can take place. The SA includes parameters such as keys and salt, that are required for encryption. You can set up to 2000 SAs in a switch.

To set up an SA between two switches, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# fcsp esp sa spi_number	Enters into SA submode for configuring SAs. The range of <i>spi_number</i> is from 256 to 4294967295.
Step 3	switch(config)# no fcsp esp sa spi_number	Deletes the SA between the switches. ¹

1. If the specified SA is currently programmed to the ports, this command returns an error saying that the SA is in use.

To determine which ports are using the SA, use the **show running-config fcsp** command. Refer to the “[Displaying Running System Information](#)” section on page 32-186.



Note

Cisco TrustSec FC Link Encryption is currently supported only on DHCHAP on and off modes.

Setting Up Security Association Parameters

To set up the SA parameters, such as keys and salt, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# fcsp esp sa <i>spi_number</i>	Enters into SA submode for configuring SAs. The range of <i>spi_number</i> is from 256 to 4294967295.
Step 4	switch(config-sa)# key <i>key</i>	Configures the key for the SA. Maximum size of <i>key</i> is 34.
Step 5	switch(config-sa)# no key <i>key</i>	Removes the key from the SA.
Step 6	switch(config-sa)# salt <i>salt</i>	Configures the salt for the SA. The range is from 0x0 to 0xffffffff.
Step 7	switch(config-sa)# no salt <i>salt</i>	Removes the salt for the SA.

To set up the SA parameters, such as keys and salt, using DCNM-SAN, follow these steps:

-
- Step 1** Expand **Switches > Security**, and then select **FC-SP (DHCHAP)**.
You see the FC-SP configuration in the Information pane.
 - Step 2** Click the **SA** tab.
You see the SA parameters for each switch.
 - Step 3** Click the **Create Row** icon.
You see the Create SA Parameters dialog box.
 - Step 4** Select the switches on which you want to perform an encryption.
 - Step 5** Select a value for the SP. The range is from 256 to 65536.
 - Step 6** Enter a value for the salt. Alternatively, click **Salt Generator** to select a value
 - Step 7** Enter a value for the key. Alternatively, click **Key Generator** to select a value.
 - Step 8** Click **Create** to save the changes.
-

To set up the SA parameters, such as keys and salt, using Device Manager, follow these steps:

-
- Step 1** Choose **Switches > Security**, and then select **FC-SP**.
You see the FC-SP configuration dialog box.
 - Step 2** Click the **SA** tab.
You see the SA parameters for each switch.
 - Step 3** Click **Create** to create new parameters.
You see the Create FC-SP SA dialog box.
 - Step 4** Select a value for the SP. The range is from 256 to 65536.
 - Step 5** Enter a value for the salt. Alternatively, click **Salt Generator** to select a value
 - Step 6** Enter a value for the key. Alternatively, click **Key Generator** to select a value.

Step 7 Click **Create** to save the changes.

Configuring ESP Settings

This section includes the following topics:

- [Configuring ESP on Ingress and Egress Ports section, page 32-181](#)
- [Configuring ESP Modes section, page 32-182](#)

Configuring ESP on Ingress and Egress Ports

Once the SA is created, you need to configure Encapsulating Security Protocol (ESP) on the ports. You should specify the egress and ingress ports for the encryption and decryption of packets between the network peers. The egress SA specifies which keys or parameters are to be used for encrypting the packets that leave the switch. The ingress SA specifies which keys or parameters are to be used to decrypt the packets entering that particular port.

This section covers the following topics:

- [Configuring ESP on Ingress Port section, page 32-181](#)
- [Configuring ESP on Egress Ports section, page 32-181](#)

Configuring ESP on Ingress Port

To configure SA to the ingress hardware, follow these steps:

Step 1	switch# config t	Enters the configuration mode.
Step 2	switch(config)# interface fc x/y	Configures the FC interface on slot <i>x</i> , port <i>y</i> .
Step 3	switch(config-if)# fcsp esp manual	Enters the ESP configuration submenu.
Step 4	switch(config-if)# ingress-sa spi_number	Configures the SA to the ingress hardware.
Step 5	switch(config-if)# no ingress-sa spi_number	Removes the SA from the ingress hardware. ¹

1. If SA is not configured in the ingress port, then running this command returns an error message.

Configuring ESP on Egress Ports

To configure SA to the egress hardware, follow these steps:

Step 1	switch# config t	Enters the configuration mode.
Step 2	switch(config)# interface fc x/y	Configures the FC interface on slot <i>x</i> , port <i>y</i> .
Step 3	switch(config-if)# fcsp esp manual	Enters the ESP configuration submenu.

Step 4	<code>switch(config-if)# egress-sa spi_number</code>	Configures the SA to the egress hardware.
Step 5	<code>switch(config-if)# no egress-sa spi_number</code>	Removes the SA from the egress hardware. ¹

1. If SA is not configured in the egress port, then running this command returns an error message.

**Note**

To apply the SA to the ingress and egress hardware of an interface, the interface needs to be in the admin shut mode.

Configuring ESP Modes

Configure the ESP settings for the ports as GCM to enable message authentication and encryption or as GMAC to enable message authentication.

The default ESP mode is AES-GCM.

This section covers the following topics:

- [Configuring AES-GCM section, page 32-182](#)
- [Configuring AES-GMAC section, page 32-182](#)

Configuring AES-GCM

To configure the AES-GCM mode, follow these steps:

	Command	Purpose
Step 1	<code>switch# config t</code>	Enters the configuration mode.
Step 2	<code>switch(config)# interface fc x/y</code>	Configures the FC interface on slot <i>x</i> , port <i>y</i> .
Step 3	<code>switch(config-if)# fcsp esp manual</code>	Enters the ESP configuration submode to configure the ESP settings on each port.
Step 4	<code>switch(config-if-esp)# mode gcm</code>	Sets the GCM mode for the interface.

Configuring AES-GMAC

To configure AES-GMAC mode, follow these steps:

	Command	Purpose
Step 1	<code>switch# config t</code>	Enters the configuration mode.
Step 2	<code>switch(config)# interface fc x/y</code>	Configures the FC interface on slot <i>x</i> , port <i>y</i> .
Step 3	<code>switch(config-if)# fcsp esp manual</code>	Enters the ESP configuration submode to configure the ESP settings on each port.
Step 4	<code>switch(config-if-esp)# mode gmac</code>	Sets the GMAC mode for the interface.
Step 5	<code>switch(config-if-esp)# no mode gmac</code>	Removes the GMAC mode from the interface and applies the default AES-GCM mode.



Note The ESP modes are set only after a SA is configured to either the ingress or the egress hardware. If SA has not been configured, ESP is turned off and encapsulation does not occur.



Note An ESP mode change always needs a port flap because the change is not seamless if it is done after you configure the port; although the configurations are not rejected.

To configure ESP settings, follow these steps:

-
- Step 1** Expand **Switches > Security**, and then select **FC-SP (DHCHAP)**.
You see the FC-SP configuration in the Information pane.
 - Step 2** Click the **ESP Interfaces** tab.
You see the Interface details for each switch.
 - Step 3** Click the **Create Row** icon.
You see the Create ESP Interfaces dialog box.
 - Step 4** Select the switches on which you want to perform an encryption.
 - Step 5** Enter an interface for the selected switch.
 - Step 6** Select the appropriate ESP mode for the encryption.
 - Step 7** Enter the appropriate egress port for the encryption.
 - Step 8** Enter the appropriate ingress port for the encryption.
 - Step 9** Click **Create** to save the changes.
-

To configure ESP settings using Device Manager, follow these steps:

-
- Step 1** Expand **Switches > Security**, and then select **FC-SP**.
You see the FC-SP configuration dialog box.
 - Step 2** Click the **ESP Interfaces** tab.
You see the Interface details for each switch.
 - Step 3** Click **Create**.
You see the Create FC-SP ESP Interfaces dialog box.
 - Step 4** Enter an interface for any switch for encryption. Alternatively, you can select values from the available interfaces for the selected switch.
 - Step 5** Select the appropriate ESP mode for the encryption.
 - Step 6** Enter the appropriate egress port for the encryption.
 - Step 7** Enter the appropriate ingress port for the encryption.
 - Step 8** Click **Create** to save the changes.
-

Configuring ESP Using ESP Wizard

You can configure and set up link-level encryption between switches using ESP wizard. You can configure an existing Inter-Switch Link (ISL) as a secure ISL or edit an existing secure ingress SPI and egress SPI using this wizard.

To configure ESP using ESP wizard, follow these steps:

Step 1 Right-click **Tools > Security > FC-SP ESP Link Security** to launch the ESP wizard from DCNM-SAN.

Step 2 Select the appropriate ISL to secure or edit security.



Note Only ISLs with FC-SP port mode turned on and available on ESP-capable switches or blades are displayed.

Step 3 Create new Security Associations (SAs).

You can create a new SA for each switch or use the existing SAs. You can click **View Existing SA** to view the existing SAs.



Note The existing list of SAs displays all existing SAs for a switch. The wizard runs only when a pair of switches have a common SA. The wizard checks for this requirement when you select **Next** and a warning message is displayed if a pair of switches do not have a common SA. You must create a common SA on the pair of the switches to run this wizard.

Step 4 Specify the Egress port, Ingress port, and ESP mode for the selected ISL.

The Egress and Ingress ports are auto populated with SPIs of the SAs common to a pair of switches in case of a secured ISL.

In this scenario, the mode is disabled and you cannot edit the modes for a secured ISL.



Note You can modify an existing ESP configuration provided the selected ISLs are enabled.

Step 5 Review your configuration.

Step 6 Click **Finish** to start the configuration for the ESP setup. You can view the status of the configuration in the status column.

Changing Keys for Switches

After the SA is applied to the ingress and egress ports, you should change the keys periodically in the configuration. The keys should be changed sequentially to avoid traffic disruption.

As an example, consider that a security association has been created between two switches, Switch1 and Switch2. The SA is configured on the ingress and egress ports as shown in the following example:

```
switch# config t
switch(config)# interface fc1/1
```

```
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 256
switch(config-if)# egress-sa 256
```

To change the keys for these switches, follow these steps:

Step 1 Add a new SA on Switch1 and Switch2.

```
switch# config t
switch(config)# fcsp esp sa 257
switch(config-sa)# key 0xAC9EF8BC8DB2DBD2008D184F794E0C38
switch(config-sa)# salt 0x1234
```

Step 2 Configure the ingress SA on Switch1.

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 257
```

Step 3 Configure the ingress and the egress SA on Switch2.

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 257
switch(config-if)# egress-sa 257
```

Step 4 Configure the egress SA on Switch1.

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# egress-sa 257
```

Step 5 Remove the previously configured ingress SA from both the switches.

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# no ingress-sa 256
```

Verifying Cisco TrustSec Fibre Channel Link Encryption Configuration

You can view information about the Cisco TrustSec FC Link Encryption feature using the **show** commands in DCNM-SAN or Device Manager.


```

interface fc8/48
  fcsp off
  fcsp esp manual
  ingress-sa 300
  ingress-sa 301
  egress-sa 300

```

Displaying FC-SP Interface Statistics

Use the **show fcsp interface statistics** command to show all statistics related to DHCHAP and ESP for an interface. The ESP statistics shown depend on the ESP supported by the port ASIC.

```

switch# show fcsp interface fc3/31 statistics

fc7/41:
  fcsp authentication mode:SEC_MODE_ON
  ESP is enabled
  configured mode is: GMAC
  programmed ingress SA: 256, 257
  programmed egress SA: 256
  Status:Successfully authenticated
  Authenticated using local password database
  Statistics:
  FC-SP Authentication Succeeded:17
  FC-SP Authentication Failed:3
  FC-SP Authentication Bypassed:0
  FC-SP ESP SPI Mismatched frames:0
  FC-SP ESP Auth failed frames:0

```

Displaying FC-SP Interface Statistics

You can view the statistics data that displays the Encapsulating Security Protocol-ESP Security Parameter (SPI) mismatches and Interface-Encapsulating Security Protocol authentication failures information using DCNM-SAN.

To view the ESP statistics for an interface, follow these steps:

-
- Step 1** Expand **Interfaces > FC Physical**, and then select **FC-SP**.
You see the FC-SP configuration in the Information pane.
 - Step 2** Click the **FC-SP** tab.
You see view the FC-SP statistics data in the Information pane.
 - Step 3** Click **Refresh** to refresh the statistics data.
-

Displaying FC-SP Interface Statistics Using Device Manager

To view the ESP statistics for an interface using Device Manager, follow these steps:

-
- Step 1** Choose **Security > FC Physical**, and then select **FC-SP**.
You see the FC-SP configuration in the Information pane.
- Step 2** Click the **Statistics** tab.
You see the statistics in the Information pane.
- Step 3** Click **Refresh** to refresh the statistics data.
-