Configuring MACsec Encryption

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restriction for MACSec Encryption

- After applying the**switchport port-security mac-address forbidden x.x.x** command, the switch returns a message that it has reached the max limit of 0

Information About MACsec Encryption

This chapter describes how to configure Media Access Control Security (MACsec) encryption on the Catalyst switches. MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. The switch also supports MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional).

Note MACsec is not supported on switches running the NPE or the LAN base image.

All downlink ports on the switch can run Cisco TrustSec MACsec link layer switch-to-switch security.

Table 1: MACsec Support on Switch Ports

Interface	**Connections**	MACsec support
Switchports connected to other switches	Switch-to-switch	Cisco TrustSec NDAC MACsec

Cisco TrustSec and Cisco SAP are meant only for switch-to-switch links and are not supported on switch ports connected to end hosts, such as PCs or IP phones. Cisco NDAC and SAP are mutually exclusive with Network Edge Access Topology (NEAT), which is used for compact switches to extend security outside the wiring closet.

Media Access Control Security and MACsec Key Agreement

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP) framework. Only host facing links (links between network access devices and endpoint devices such as a PC or IP phone) can be secured using MACsec.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the client. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the client, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a client) using the current session key.

The MKA Protocol manages the encryption keys used by the underlying MACsec protocol. The basic requirements of MKA are defined in 802.1x-REV. The MKA Protocol extends 802.1x to allow peer discovery with confirmation of mutual authentication and sharing of MACsec secret keys to protect data exchanged by the peers.

The EAP framework implements MKA as a newly defined EAP-over-LAN (EAPOL) packet. EAP authentication produces a master session key (MSK) shared by both partners in the data exchange. Entering the EAP session ID generates a secure connectivity association key name (CKN). Because the switch is the authenticator, it is also the key server, generating a random 128-bit secure association key (SAK), which it sends it to the client partner. The client is never a key server and can only interact with a single MKA entity, the key server. After key derivation and generation, the switch sends periodic transports to the partner at a default interval of 2 seconds.

The packet body in an EAPOL Protocol Data Unit (PDU) is referred to as a MACsec Key Agreement PDU (MKPDU). MKA sessions and participants are deleted when the MKA lifetime (6 seconds) passes with no MKPDU received from a participant. For example, if a client disconnects, the participant on the switch continues to operate MKA until 6 seconds have elapsed after the last MKPDU is received from the client.

MKA Policies

To enable MKA on an interface, a defined MKA policy should be applied to the interface. Removing the MKA policy disables MKA on that interface. You can configure these options:

- Policy name, not to exceed 16 ASCII characters.
- Confidentiality (encryption) offset of 0, 30, or 50 bytes for each physical interface
- Replay protection. You can configure MACsec window size, as defined by the number of out-of-order frames that are accepted. This value is used while installing the security associations in the MACsec. A value of 0 means that frames are accepted only in the correct order.

Virtual Ports

You use virtual ports for multiple secured connectivity associations on a single physical port. Each connectivity association (pair) represents a virtual port, with a maximum of two virtual ports per physical port. Only one of the two virtual ports can be part of a data VLAN; the other must externally tag its packets for the voice VLAN. You cannot simultaneously host secured and unsecured sessions in the same VLAN on the same port. Because of this limitation, 802.1x multiple authentication mode is not supported.

The exception to this limitation is in multiple-host mode when the first MACsec supplicant is successfully authenticated and connected to a hub that is connected to the switch. A non-MACsec host connected to the hub can send traffic without authentication because it is in multiple-host mode. We do not recommend using multi-host mode because after the first successful client, authentication is not required for other clients.

Virtual ports represent an arbitrary identifier for a connectivity association and have no meaning outside the MKA Protocol. A virtual port corresponds to a separate logical port ID. Valid port IDs for a virtual port are 0x0002 to 0xFFFF. Each virtual port receives a unique secure channel identifier (SCI) based on the MAC address of the physical interface concatenated with a 16-bit port ID.

MACsec and Stacking

A Device stack master running MACsec maintains the configuration files that show which ports on a member switch support MACsec. The stack master performs these functions:

- Processes secure channel and secure association creation and deletion
- Sends secure association service requests to the stack members.
- Processes packet number and replay-window information from local or remote ports and notifies the key management protocol.
- Sends MACsec initialization requests with the globally configured options to new switches that are added to the stack.
- Sends any per-port configuration to the member switches.

A member switch performs these functions:

- Processes MACsec initialization requests from the stack master.
- Processes MACsec service requests sent by the stack master.
- Sends information about local ports to the stack master.

In case of a stack master changeover, all secured sessions are brought down and then reestablished. The authentication manager recognizes any secured sessions and initiates teardown of these sessions.

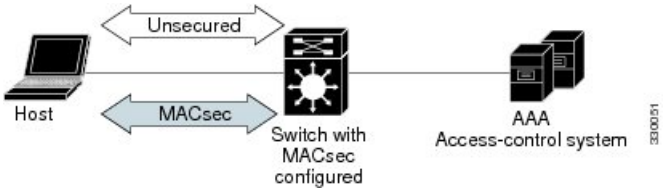
MACsec, MKA and 802.1x Host Modes

You can use MACsec and the MKA Protocol with 802.1x single-host mode or Multi Domain Authentication (MDA) mode. Multiple authentication mode is not supported.

Single-Host Mode

The figure shows how a single EAP authenticated session is secured by MACsec by using MKA

Figure 1: MACsec in Single-Host Mode with a Secured Data Session



MKA Statistics

Some MKA counters are aggregated globally, while others are updated both globally and per session. You can also obtain information about the status of MKA sessions.

This is an example of the**show mka statistics** command output:

```
SWitch# show mka statistics
MKA Global Statistics
======================
MKA Session Totals
Secured..................... 32
Reauthentication Attempts.. 31

Deleted (Secured)........... 1
Keepalive Timeouts......... 0

CA Statistics
Pairwise CAKs Derived...... 32
Pairwise CAK Rekeys........ 31
Group CAKs Generated....... 0
Group CAKs Received........ 0

SA Statistics
SAKs Generated............. 32
SAKs Rekeyed............... 31
SAKs Received.............. 0
SAK Responses Received..... 32


MKPDU Statistics
MKPDUs Validated & Rx...... 580
"Distributed SAK"..... 0
"Distributed CAK"..... 0
MKPDUs Transmitted......... 597
"Distributed SAK"..... 32
"Distributed CAK"..... 0

MKA Error Counter Totals
========================
Bring-up Failures................... 0
Reauthentication Failures........... 0
```

```
SAK Failures
SAK Generation................... 0
Hash Key Generation............. 0
SAK Encryption/Wrap............. 0
SAK Decryption/Unwrap........... 0

CA Failures
Group CAK Generation............ 0
Group CAK Encryption/Wrap....... 0
Group CAK Decryption/Unwrap..... 0
Pairwise CAK Derivation......... 0
CKN Derivation.................. 0
ICK Derivation.................. 0
KEK Derivation.................. 0
Invalid Peer MACsec Capability.. 2

MACsec Failures
Rx SC Creation................... 0
Tx SC Creation................... 0
Rx SA Installation............... 0
Tx SA Installation............... 0

MKPDU Failures
MKPDU Tx......................... 0
MKPDU Rx Validation.............. 0
MKPDU Rx Bad Peer MN............. 0
MKPDU Rx Non-recent Peerlist MN.. 0
```

Configuring MKA and MACsec

Default MACsec MKA Configuration

MACsec is disabled. No MKA policies are configured.

Related Topics

Configuring MACsec on an Interface, on page 6
Configuring an MKA Policy, on page 5
Example: Configuring MACsec on an Interface, on page 17

Configuring an MKA Policy

SUMMARY STEPS

1. **configure terminal**
2. **mka policy** *policy name*
3. **confidentiality-offset** *Offset value*
4. **replay-protection window-size** *frames*
5. **end**
6. **show mka policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mka policy** *policy name*	Identify an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters.
Step 3	**confidentiality-offset** *Offset value*	Set the Confidentiality (encryption) offset for each physical interface **Note** Offset Value can be 0, 30 or 50. If you are using Anyconnect on the client, it is recommended to use Offset 0.
Step 4	**replay-protection window-size** *frames*	Enable replay protection, and configure the window size in number of frames. The range is from 0 to 4294967295. The default window size is 0. Entering a window size of 0 is not the same as entering the **no replay-protection command**. Configuring a window size of 0 uses replay protection with a strict ordering of frames. Entering **no replay-protection** turns off MACsec replay-protection.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show mka policy**	Verify your entries.

Example

This example configures the MKA policy *relay-policy*:

```
Switch(config)# mka policy replay-policy
Switch(config-mka-policy)# confidentiality-offset 0
Switch(config-mka-policy)# replay-protection window-size 300
Switch(config-mka-policy)# end
```

Related Topics

Default MACsec MKA Configuration, on page 5
Example: Configuring MACsec on an Interface, on page 17

Configuring MACsec on an Interface

Follow these steps to configure MACsec on an interface with one MACsec session for voice and one for data:

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** *interface-id*
4. **switchport access vlan***vlan-id*
5. **switchport mode access**
6. **macsec**
7. **authentication event linksec fail action authorize vlan** *vlan-id*
8. **authentication host-mode multi-domain**
9. **authentication linksec policy must-secure**
10. **authentication port-control auto**
11. **authentication periodic**
12. **authentication timer reauthenticate**
13. **authentication violation protect**
14. **mka policy** *policy name*
15. **dot1x pae authenticator**
16. **spanning-tree portfast**
17. **end**
18. **show authentication session interface** *interface-id*
19. **show authentication session interface** *interface-id* details
20. **show macsec interface** *interface-id*
21. **show mka sessions**
22. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id*	Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.
Step 4	**switchport access vlan***vlan-id*	Configure the access VLAN for the port.
Step 5	**switchport mode access**	Configure the interface as an access port.
Step 6	**macsec**	Enable 802.1ae MACsec on the interface.
Step 7	**authentication event linksec fail action authorize vlan** *vlan-id*	(Optional) Specify that the switch processes authentication link-security failures resulting from unrecognized user

	Command or Action	Purpose
		credentials by authorizing a restricted VLAN on the port after a failed authentication attempt.
Step 8	**authentication host-mode multi-domain**	Configure authentication manager mode on the port to allow both a host and a voice device to be authenticated on the 802.1x-authorized port. If not configured, the default host mode is single.
Step 9	**authentication linksec policy must-secure**	Set the LinkSec security policy to secure the session with MACsec if the peer is available. If not set, the default is *should secure*.
Step 10	**authentication port-control auto**	Enable 802.1x authentication on the port. The port changes to the authorized or unauthorized state based on the authentication exchange between the switch and the client.
Step 11	**authentication periodic**	Enable or Disable Reauthentication for this port .
Step 12	**authentication timer reauthenticate**	Enter a value between 1 and 65535. Obtains re-authentication timeout value from the server.
Step 13	**authentication violation protect**	Configure the port to drop unexpected incoming MAC addresses when a new device connects to a port or when a device connects to a port after the maximum number of devices are connected to that port. If not configured, the default is to shut down the port.
Step 14	**mka policy** *policy name*	Apply an existing MKA protocol policy to the interface, and enable MKA on the interface. If no MKA policy was configured (by entering the **mka policy** global configuration command), you must apply the MKA default policy to the interface by entering the **mka default-policy** interface configuration command
Step 15	**dot1x pae authenticator**	Configure the port as an 802.1x port access entity (PAE) authenticator.
Step 16	**spanning-tree portfast**	Enable spanning tree Port Fast on the interface in all its associated VLANs. When Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes
Step 17	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 18	**show authentication session interface** *interface-id*	Verify the authorized session security status.

	Command or Action	Purpose
Step 19	**show authentication session interface** *interface-id* details	Verify the details of the security status of the authorized session.
Step 20	**show macsec interface** *interface-id*	Verify MacSec status on the interface.
Step 21	**show mka sessions**	Verify the established mka sessions.
Step 22	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Default MACsec MKA Configuration, on page 5
Example: Configuring MACsec on an Interface, on page 17

Information About Cisco TrustSec

The table below lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

Cisco TrustSec Feature	Description
802.1AE Tagging (MACsec)	Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption. Between MACsec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices. This feature is only available between TrustSec hardware-capable devices. **Note** This feature is not supported on Catalyst 2960x.
Endpoint Admission Control (EAC)	EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).

Cisco TrustSec Feature	Description
Network Device Admission Control (NDAC)	NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption. **Note** This feature is not supported on Catalyst 2960x.
Security Group Access Control List (SGACL)	A Security Group Access Control List (SGACL) associates a Security Group Tag with a policy. The policy is enforced upon SGT-tagged traffic egressing the TrustSec domain.
Security Association Protocol (SAP)	After NDAC authentication, the Security Association Protocol (SAP) automatically negotiates keys and the cipher suite for subsequent MACSec link encryption between TrustSec peers. SAP is defined in IEEE 802.11i. **Note** This feature is not supported on Catalyst 2960x.
Security Group Tag (SGT)	An SGT is a 16-bit single label indicating the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet.
SGT Exchange Protocol (SXP)	Security Group Tag Exchange Protocol (SXP). With SXP, devices that are not TrustSec-hardware-capable can receive SGT attributes for authenticated users and devices from the Cisco Identity Services Engine (ISE) or the Cisco Secure Access Control System (ACS). The devices can then forward a sourceIP-to-SGT binding to a TrustSec-hardware-capable device will tag the source traffic for SGACL enforcement.

When both ends of a link support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a security association (SA).

Depending on your software version and licensing and link hardware support, SAP negotiation can use one of these modes of operation:

- Galois Counter Mode (GCM)—authentication and encryption
- GCM authentication (GMAC)— GCM authentication, no encryption
- No Encapsulation—no encapsulation (clear text)
- Null—encapsulation, no authentication or encryption

Related Topics

Configuring Cisco TrustSec MACsec, on page 11

Configuring Cisco TrustSec MACsec

Related Topics

Information About Cisco TrustSec , on page 9

Configuring Cisco TrustSec Credentials on the Switch

To enable Cisco TrustSec features, you must create Cisco TrustSec credentials on the switch to use in other TrustSec configurations. Beginning in privilege EXEC mode, follow these steps to configure Cisco TrustSec credentials.

SUMMARY STEPS

1. **cts credentials id** *device-id* **password** *cts-password*
2. **show cts credentials**
3. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cts credentials id** *device-id* **password** *cts-password* **Example:** `Switch# cts credentials id trustsec password mypassword`	Specifies the Cisco TrustSec credentials for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. • **id** *device-id*—Specifies a Cisco TrustSec device ID for the switch. The device-id argument has a maximum length of 32 characters and is case sensitive • **password** *cts-password*—Specifies the Cisco TrustSec password for the device.
Step 2	**show cts credentials** **Example:** `Switch# show cts credentials`	(Optional) Displays Cisco TrustSec credentials configured on the switch.
Step 3	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Example

To delete the Cisco TrustSec credentials, enter the **clear cts credentials** privileged EXEC command.

This example shows how to create Cisco TrustSec credentials.

```
Switch# cts credentials id trustsec password mypassword
CTS device ID and password have been inserted in the local keystore. Please make
sure that the same ID and password are configured in the server database.

Switch# show cts credentials
CTS password is defined in keystore, device-id = trustsec
```

What to do next

Before you configure Cisco TrustSec MACsec authentication, you should configure Cisco TrustSec seed and non-seed devices. For 802.1x mode, you must configure at least one seed device, that device closest to the access control system (ACS). See this section in the Cisco TrustSec Configuration Guide:http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html

Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1x Mode

Before you begin

You enable Cisco TrustSec link layer switch-to-switch security on an interface that connects to another Cisco TrustSec device. When configuring Cisco TrustSec in 802.1x mode on an interface, follow these guidelines:

- To use 802.1x mode, you must globally enable 802.1x on each device. For more information 802.1x, see the Configuring IEEE 802.1x Port-Based Authentication chapter.
- If you select GCM as the SAP operating mode, you must have a MACsec encryption software license from Cisco. MACsec is supported on Catalyst 3850 and 3650 universal IP Services and IP Base licenses . It is not supported with the NPE license or with a LAN base service image.

  If you select GCM without the required license, the interface is forced to a link-down state.

Beginning in privilege EXEC mode, follow these steps to configure Cisco TrustSec switch-to-switch link layer security with 802.1x:

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **cts dot1x**
4. **sap mode-list***mode1* [*mode2* [*mode3* [*mode4*]]]
5. **exit**
6. **end**
7. **show cts interface** [*interface-id* | **brief** I**summary**]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface tengigabitethernet 1/1/2`	**Note** Enters interface configuration mode.
Step 3	**cts dot1x** **Example:** `Switch(config-if)# cts dot1x`	Configures the interface to perform NDAC authentication.
Step 4	**sap mode-list***mode1* [*mode2* [*mode3* [*mode4*]]] **Example:** `Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap`	(Optional) Configures the SAP operation mode on the interface. The interface negotiates with the peer for a mutually acceptable mode. Enter the acceptable modes in your order of preference. Choices for *mode* are: • **gcm-encrypt**—Authentication and encryption **Note** Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption. • **gmac**—Authentication, no encryption • **no-encap**—No encapsulation • **null**—Encapsulation, no authentication or encryption **Note** If the interface is not capable of data link encryption, no-encap is the default and the only available SAP operating mode. SGT is not supported. **Note** Although visible in the CLI help, the timer reauthentication and propagate sgt keywords are not supported.
Step 5	**exit** **Example:** `Switch(config-if-cts-dot1x)# exit`	Exits Cisco TrustSec 802.1x interface configuration mode.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show cts interface** [*interface-id* | **brief** I**summary**]	(Optional) Verify the configuration by displaying TrustSec-related interface characteristics.

	Command or Action	Purpose
Step 8	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Example

This example shows how to enable Cisco TrustSec authentication in 802.1x mode on an interface using GCM as the preferred SAP mode:

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap

Switch(config-if-cts-dot1x)# exit
Switch(config-if)# end
```

Related Topics

Cisco TrustSec Switch-to-Switch Link Security Configuration Example, on page 20

Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode

Before you begin

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, Cisco TrustSec encapsulation or encryption is not performed.
- If you select GCM as the SAP operating mode, you must have a MACsec Encryption software license from Cisco. If you select GCM without the required license, the interface is forced to a link-down state.
- These protection levels are supported when you configure SAP pairwise master key (sap pmk):
  - SAP is not configured—no protection.
  - **sap mode-list gcm-encrypt gmac no-encap**—protection desirable but not mandatory.
  - **sap mode-list gcm-encrypt gmac**—confidentiality preferred and integrity required. The protection is selected by the supplicant according to supplicant preference.
  - **sap mode-list gmac**—integrity only.
  - **sap mode-list gcm-encrypt**—confidentiality required.
  - **sap mode-list gmac gcm-encrypt**—integrity required and preferred, confidentiality optional.

Beginning in privileged EXEC mode, follow these steps to manually configure Cisco TrustSec on an interface to another Cisco TrustSec device:

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **cts manual**
4. **sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]]
5. **no propagate sgt**
6. **exit**
7. **end**
8. **show cts interface** [*interface-id* | **brief** | **summary**]
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface tengigabitethernet 1/1/2`	**Note** Enters interface configuration mode.
Step 3	**cts manual** **Example:** `Switch(config-if)# cts manual`	Enters Cisco TrustSec manual configuration mode.
Step 4	**sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]] **Example:** `Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap`	(Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode. • *key*—A hexadecimal value with an even number of characters and a maximum length of 32 characters. The SAP operation mode options: • **gcm-encrypt**—Authentication and encryption **Note** Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption. • **gmac**—Authentication, no encryption • **no-encap**—No encapsulation • **null**—Encapsulation, no authentication or encryption

	Command or Action	Purpose
		Note If the interface is not capable of data link encryption, **no-encap** is the default and the only available SAP operating mode. SGT is not supported.
Step 5	**no propagate sgt** **Example:** `Switch(config-if-cts-manual)# no propagate sgt`	Use the **no** form of this command when the peer is incapable of processing a SGT. The **no propagate sgt** command prevents the interface from transmitting the SGT to the peer.
Step 6	**exit** **Example:** `Switch(config-if-cts-manual)# exit`	Exits Cisco TrustSec 802.1x interface configuration mode.
Step 7	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	**show cts interface** [*interface-id* | **brief** | **summary**]	(Optional) Verify the configuration by displaying TrustSec-related interface characteristics.
Step 9	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Example

This example shows how to configure Cisco TrustSec authentication in manual mode on an interface:

```
Switch# configure terminal
Switch(config)# interface tengiigabitethernet 1/1/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

Related Topics

Cisco TrustSec Switch-to-Switch Link Security Configuration Example, on page 20

Configuration Examples

Example: Configuring MACsec on an Interface

Configuring MACsec on an Interface

```
Device(config)# interface GigabitEthernet1/0/25
Device(config-if)# switchport access vlan 10
Device(config-if)# switchport mode access
Device(config-if)# macsec
Device(config-if)# authentication event linksec fail action authorize vlan 2
Device(config-if)# authentication host-mode multi-domain
Device(config-if)# authentication linksec policy must-secure
Device(config-if)# authentication port-control auto
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate
Device(config-if)# authentication violation protect
Device(config-if)# mka policy replay-policy
Device(config-if)# dot1x pae authenticator
Device(config-if)# spanning-tree portfast
Device(config-if)# end
```

```
Device# show authentication session interface gigabitethernet6/0/36

Interface MAC Address Method Domain Status Fg Session ID
--------------------------------------------------------------------------
Gi6/0/36 001b.214c.a98c dot1x DATA Auth 020000D4000019440E54D478
Gi6/0/36 001b.0cdb.bdd8 mab  VOICE Auth 020000D400000FB2001687B2


Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
N - Waiting for AAA to come up
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker

Runnable methods list:
Handle Priority Name
16 5 dot1x
19 10 mab
23 15 webauth
```

```
Device# show authentication session interface gigabitethernet6/0/36 details


Interface: GigabitEthernet6/0/36
IIF-ID: 0x1062E8000000AB0
MAC Address: 001b.214c.a98c
IPv6 Address: Unknown
```

```
IPv4 Address: 16.0.0.21
User-Name: D_MustSecure
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Session timeout: 200s (local), Remaining: 187s
Timeout action: Reauthenticate
Common Session ID: 020000D4000019440E54D478
Acct Session ID: 0x000019D8
Handle: 0x86000996
Current Policy: POLICY_Gi6/0/36

Local Policies:
Idle timeout: 60 sec
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
Vlan Group: Vlan: 16

Security Policy: Must Secure
Security Status: Link Secured
SGT Value: 0

Method status list:
Method State
dot1x Authc Success

----------------------------------------
Interface: GigabitEthernet6/0/36
IIF-ID: 0x100200000000120
MAC Address: 001b.0cdb.bdd8
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: 00-1B-0C-DB-BD-D8
Status: Authorized
Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
Session timeout: 200s (local), Remaining: 177s
Timeout action: Reauthenticate
Common Session ID: 020000D400000FB2001687B2
Acct Session ID: 0x000019DB

Handle: 0x0A000006
Current Policy: POLICY_Gi6/0/36

Local Policies:
Idle timeout: 60 sec
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
Vlan Group: Vlan: 116
Security Policy: Must Not Secure
Security Status: Link Unsecure

Method status list:
Method State
dot1x Stopped
mab Authc Success

Device# show macsec interface gigabitethernet6/0/3615
MACsec is enabled
Replay protect : enabled
```

```
Replay window : 0
Include SCI : yes
Use ES Enable : no
Use SCB Enable : no
Admin Pt2Pt MAC : forceTrue(1)
Pt2Pt MAC Operational : no
Cipher : GCM-AES-128
Confidentiality Offset : 0

Capabilities
Identifier :
Name :
ICV length : 16
Data length change supported: yes
Max. Rx SA : 16
Max. Tx SA : 16
Max. Rx SC : 8
Max. Tx SC : 8
Validate Frames : strict
PN threshold notification support : Yes
Ciphers supported : GCM-AES-128

Transmit Secure Channels
SCI : B000B43A70A40002
SC state : notInUse(2)
Elapsed time : 00:05:25
Start time : 7w0d
Current AN: 1
Previous AN: 0
Next PN: 0
SA State: notInUse(2)
Confidentiality : no
SAK Unchanged : no
SA Create time : 2d18h
SA Start time : 7w0d
SC Statistics
Auth-only Pkts : 0
Auth-only Bytes : 0
Encrypt Pkts : 308
Encrypt Bytes : 0
SA Statistics
Auth-only Pkts : 0
Encrypt Pkts : 182

Port Statistics

Receive Secure Channels
SCI : 001B214CA98C0000
SC state : notInUse(2)
Elapsed time : 00:05:25
Start time : 7w0d
Current AN: 1
Previous AN: 0
Next PN: 0
RX SA Count: 0
SA State: notInUse(2)
SAK Unchanged : no
SA Create time : 2d18h
SA Start time : 7w0d
SC Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 495
Valid bytes 0
```

```
Late pkts 0
Uncheck pkts 0
Delay pkts 0
UnusedSA pkts 0
NousingSA pkts 0
Decrypt bytes 0
SA Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 146
UnusedSA pkts 0
NousingSA pkts 0

Port Statistics
#
```

Related Topics

Configuring MACsec on an Interface, on page 6
Configuring an MKA Policy, on page 5
Default MACsec MKA Configuration, on page 5

Cisco TrustSec Switch-to-Switch Link Security Configuration Example

This example shows the configuration necessary for a seed and non-seed device for Cisco TrustSec switch-to-switch security. You must configure the AAA and RADIUS for link security. In this example, ACS-1 through ACS-3 can be any server names and cts-radius is the Cisco TrustSec server.

Seed Device Configuration:

```
Switch(config)#aaa new-model
Switch(config)#radius server ACS-1
Switch(config-radius-server)#address ipv4 10.5.120.12 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-2
Switch(config-radius-server)#address ipv4 10.5.120.14 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-3
Switch(config-radius-server)#address ipv4 10.5.120.15 auth-port 1812 acct-port
 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#aaa group server radius cts-radius
Switch(config-sg-radius)#server name ACS-1
Switch(config-sg-radius)#server name ACS-2
Switch(config-sg-radius)#server name ACS-3
Switch(config-sg-radius)#exit
Switch(config)#aaa authentication login default none
Switch(config)#aaa authentication dot1x default group cts-radius
Switch(config)#aaa authorization network cts-radius group cts-radius
Switch(config)#aaa session-id common
```

```
Switch(config)#cts authorization list cts-radius
Switch(config)#dot1x system-auth-control

Switch(config)#interface gi1/1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#cts dot1x
Switch(config-if-cts-dot1x)#sap mode-list gcm-encrypt gmac

Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)#interface gi1/1/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#cts manual
Switch(config-if-cts-dot1x)#sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
gmac
Switch(config-if-cts-dot1x)#no propagate sgt
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)#radius-server vsa send authentication
Switch(config)#end
Switch#cts credentials id cts-36 password trustsec123
```

Non-Seed Device:

```
Switch(config)#aaa new-model
Switch(config)#aaa session-id common
Switch(config)#dot1x system-auth-control

Switch(config)#interface gi1/1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#shutdown
Switch(config-if)#cts dot1x
Switch(config-if-cts-dot1x)#sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)#interface gi1/1/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#shutdown
Switch(config-if)#cts manual
Switch(config-if-cts-dot1x)#sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
gmac
Switch(config-if-cts-dot1x)#no propagate sgt
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)#radius-server vsa send authentication
Switch(config)#end
Switch(config)#cts credentials id cts-72 password trustsec123
```

Related Topics

Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1x Mode, on page 12
Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode, on page 14