



Configuring MACsec Encryption

- [Finding Feature Information, on page 1](#)
- [Information About MACsec Encryption, on page 1](#)
- [Configuring MKA and MACsec, on page 8](#)
- [Configuring MACsec MKA using PSK, on page 11](#)
- [Configuring MACsec MKA using EAP-TLS, on page 13](#)
- [Configuring Cisco TrustSec MACsec, on page 27](#)
- [Configuration Examples for Configuring MACsec Encryption, on page 32](#)

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 <https://cfng.cisco.com/>. An account on Cisco.com is not required.

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-TLS) or Pre Shared Key (PSK) framework.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the MKA peer, 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 MKA peer) 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). The switch acts as the authenticator for both uplink and downlink; and acts as the key server for downlink. It generates a random secure association key (SAK), which is sent 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 MKA peer disconnects, the participant on the switch continues to operate MKA until 6 seconds have elapsed after the last MKPDU is received from the MKA peer.



Note Integrity check value (ICV) indicator in MKPDU is optional. ICV is not optional when the traffic is encrypted.

EAPoL Announcements indicate the use of the type of keying material. The announcements can be used to announce the capability of the supplicant as well as the authenticator. Based on the capability of each side, the largest common denominator of the keying material could be used.

Prior to Cisco IOS XE Fuji 16.8.1a, should-secure was supported for MKA and SAP. With should-secure enabled, if the peer is configured for MACsec, the data traffic is encrypted, otherwise it is sent in clear text. Starting with Cisco IOS XE Fuji 16.8.1a, must-secure support is enabled on both the ingress and the egress. Must-secure is supported for MKA and SAP. With must-secure enabled, only EAPoL traffic will not be encrypted. The rest of the traffic will be encrypted. Unencrypted packets are dropped.



Note Must-secure mode is enabled by default.

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 (Catalyst 3560cx) Switch 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.



Note If you are using 1G SFP modules for inter switch connection, change system MTU to 1550 byte to ensure support of MACsec overhead.

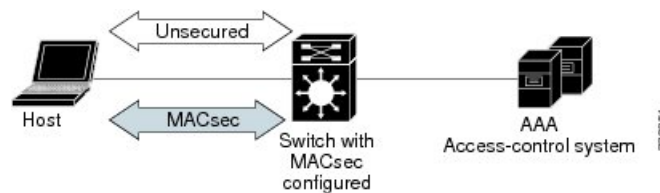
MACsec, MKA and 802.1x Host Modes

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

```

Information About MACsec MKA using EAP-TLS

MACsec MKA is supported on switch-to-switch links. Using IEE 802.1X Port-based Authentication with Extensible Authentication Protocol (EAP-TLS), you can configure MACsec MKA between device uplink ports. EAP-TLS allows mutual authentication and obtains an MSK (master session key) from which the connectivity association key (CAK) is derived for MKA operations. Device certificates are carried, using EAP-TLS, for authentication to the AAA server.

Prerequisites for MACsec MKA using EAP-TLS

- Ensure that you have a Certificate Authority (CA) server configured for your network.
- Generate a CA certificate.

- Ensure that you have configured Cisco Identity Services Engine (ISE) Release 2.0.
- Ensure that both the participating devices, the CA server, and Cisco Identity Services Engine (ISE) are synchronized using Network Time Protocol (NTP). If time is not synchronized on all your devices, certificates will not be validated.
- Ensure that 802.1x authentication and AAA are configured on your device.

Limitations for MACsec MKA using EAP-TLS

- MKA is not supported on port-channels.
- Cisco Catalyst 3560-CX Switches do not support MACSec MKA configuration on EtherChannels.
- MKA is not supported with High Availability and local authentication.
- MKA/EAPTLS is not supported for promiscuous PVLAN Primary port.
- While configuring MACsec MKA using EAP-TLS, MACsec secure channels encrypt counters does not increment before first Rekey.

Cisco TrustSec Overview

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)	<p>Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption.</p> <p>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.</p> <p>This feature is only available between TrustSec hardware-capable devices.</p>
Endpoint Admission Control (EAC)	<p>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).</p>

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.
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.
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

Configuring MKA and MACsec

Default MACsec MKA Configuration

MACsec is disabled. No MKA policies are configured.

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 <i>policy name</i>	Identify an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters.
Step 3	confidentiality-offset <i>Offset value</i>	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 <i>frames</i>	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 relay-policy
Switch(config-mka-policy)# confidentiality-offset 0
Switch(config-mka-policy)# replay-protection window-size 300
Switch(config-mka-policy)# end
```

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: <pre>Switch> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Switch# <code>configure terminal</code>	Enters global configuration mode.
Step 3	interface <i>interface-id</i>	Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.
Step 4	switchport access vlan <i>vlan-id</i>	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 <i>vlan-id</i>	(Optional) Specify that the switch processes authentication link-security failures resulting from unrecognized user 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 <i>should secure</i> .
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 <i>policy name</i>	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

	Command or Action	Purpose
Step 15	<code>dot1x pae authenticator</code>	Configure the port as an 802.1x port access entity (PAE) authenticator.
Step 16	<code>spanning-tree portfast</code>	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	<code>end</code> Example: <code>Switch(config)# end</code>	Returns to privileged EXEC mode.
Step 18	<code>show authentication session interface interface-id</code>	Verify the authorized session security status.
Step 19	<code>show authentication session interface interface-id details</code>	Verify the details of the security status of the authorized session.
Step 20	<code>show macsec interface interface-id</code>	Verify MacSec status on the interface.
Step 21	<code>show mka sessions</code>	Verify the established mka sessions.
Step 22	<code>copy running-config startup-config</code> Example: <code>Switch# copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Configuring MACsec MKA using PSK

SUMMARY STEPS

1. `configure terminal`
2. `key chain key-chain-name macsec`
3. `key hex-string`
4. `key-string { [0/6/7] pwd-string | pwd-string }`
5. `lifetime local [start timestamp {hh::mm::ss | day | month | year}] [duration seconds | end timestamp {hh::mm::ss | day | month | year}]`
6. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.

	Command or Action	Purpose
Step 2	key chain <i>key-chain-name</i> macsec	Configures a key chain and enters the key chain configuration mode.
Step 3	key <i>hex-string</i>	Configures a unique identifier for each key in the keychain and enters the keychain's key configuration mode. Note For 128-bit encryption, use 32 hex digit key-string.
Step 4	key-string { [0/6/7] <i>pwd-string</i> <i>pwd-string</i> }	Sets the password for a key string. Only hex characters must be entered.
Step 5	lifetime local [<i>start timestamp</i> { <i>hh::mm::ss</i> <i>day</i> <i>month</i> <i>year</i> }] [duration <i>seconds</i> <i>end timestamp</i> { <i>hh::mm::ss</i> <i>day</i> <i>month</i> <i>year</i> }]	Sets the lifetime of the pre shared key.
Step 6	end	Returns to privileged EXEC mode.

Example

Following is an indicative example:

```
Switch(config)# Key chain keychain1 macsec
Switch(config-key-chain)# key 1000
Switch(config-keychain-key)# cryptographic-algorithm gcm-aes-128
Switch(config-keychain-key)# key-string 12345678901234567890123456789012
Switch(config-keychain-key)# lifetime local 12:12:00 July 28 2016 12:19:00 July
28 2016
Switch(config-keychain-key)# end
```

Configuring MACsec MKA on an Interface using PSK

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **macsec network-link**
4. **mka policy** *policy-name*
5. **mka pre-shared-key** *key-chain* *key-chain name*
6. **macsec replay-protection window-size** *frame number*
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	<code>interface <i>interface-id</i></code>	Enters interface configuration mode.
Step 3	<code>macsec network-link</code>	Enables MACsec on the interface.
Step 4	<code>mka policy <i>policy-name</i></code>	Configures an MKA policy.
Step 5	<code>mka pre-shared-key key-chain <i>key-chain name</i></code>	Configures an MKA pre-shared-key key-chain name. Note The MKA pre-shared key can be configured on either physical interface or sub-interfaces and not on both.
Step 6	<code>macsec replay-protection window-size <i>frame number</i></code>	Sets the MACsec window size for replay protection.
Step 7	<code>end</code>	Returns to privileged EXEC mode.

Example

Following is an indicative example:

```
Switch(config)# interface GigabitEthernet 0/0/0
Switch(config-if)# mka policy mka_policy
Switch(config-if)# mka pre-shared-key key-chain key-chain-name
Switch(config-if)# macsec replay-protection window-size 10
Switch(config-if)# end
```

What to do next

It is not recommended to change the MKA policy on an interface with MKA PSK configured when the session is running. However, if a change is required, you must reconfigure the policy as follows:

1. Disable the existing session by removing `macsec network-link` configuration on each of the participating node using the **no macsec network-link** command
2. Configure the MKA policy on the interface on each of the participating node using the **mka policy policy-name** command.
3. Enable the new session on each of the participating node by using the **macsec network-link** command.

Configuring MACsec MKA using EAP-TLS

To configure MACsec with MKA on point-to-point links, perform these tasks:

- Configure Certificate Enrollment
 - Generate Key Pairs
 - Configure SCEP Enrollment
 - Configure Certificates Manually

- Configure an Authentication Policy
- Configure EAP-TLS Profiles and IEEE 802.1x Credentials
- Configure MKA MACsec using EAP-TLS on Interfaces

Remote Authentication

Generating Key Pairs

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>crypto key generate rsa label <i>label-name</i> general-keys modulus <i>size</i></code>	Generates a RSA key pair for signing and encryption. You can also assign a label to each key pair using the label keyword. The label is referenced by the trustpoint that uses the key pair. If you do not assign a label, the key pair is automatically labeled <Default-RSA-Key>. If you do not use additional keywords this command generates one general purpose RSA key pair. If the modulus is not specified, the default key modulus of 1024 is used. You can specify other modulus sizes with the modulus keyword.
Step 3	<code>end</code>	Returns to privileged EXEC mode.
Step 4	<code>show authentication session interface <i>interface-id</i></code>	Verifies the authorized session security status.
Step 5	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Configuring Enrollment using SCEP

Simple Certificate Enrollment Protocol (SCEP) is a Cisco-developed enrollment protocol that uses HTTP to communicate with the certificate authority (CA) or registration authority (RA). SCEP is the most commonly used method for sending and receiving requests and certificates.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>crypto pki trustpoint <i>server name</i></code>	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 3	<code>enrollment url <i>url name pem</i></code>	Specifies the URL of the CA on which your device should send certificate requests.

	Command or Action	Purpose
		<p>An IPv6 address can be added in the URL enclosed in brackets. For example: http:// [2001:DB8:1:1::1]:80.</p> <p>The pem keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.</p>
Step 4	rsa keypair <i>label</i>	<p>Specifies which key pair to associate with the certificate.</p> <p>Note The rsakeypair name must match the trust-point name.</p>
Step 5	serial-number none	The none keyword specifies that a serial number will not be included in the certificate request.
Step 6	ip-address none	The none keyword specifies that no IP address should be included in the certificate request.
Step 7	revocation-check <i>crl</i>	Specifies CRL as the method to ensure that the certificate of a peer has not been revoked.
Step 8	auto-enroll <i>percent regenerate</i>	<p>Enables auto-enrollment, allowing the client to automatically request a rollover certificate from the CA.</p> <p>If auto-enrollment is not enabled, the client must be manually re-enrolled in your PKI upon certificate expiration.</p> <p>By default, only the Domain Name System (DNS) name of the device is included in the certificate.</p> <p>Use the percent argument to specify that a new certificate will be requested after the percentage of the lifetime of the current certificate is reached.</p> <p>Use the regenerate keyword to generate a new key for the certificate even if a named key already exists.</p> <p>If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable: “! RSA key pair associated with trustpoint is exportable.”</p> <p>It is recommended that a new key pair be generated for security reasons.</p>
Step 9	crypto pki authenticate <i>name</i>	Retrieves the CA certificate and authenticates it.
Step 10	exit	Exits global configuration mode.
Step 11	show crypto pki certificate <i>trustpoint name</i>	Displays information about the certificate for the trust point.

Configuring Enrollment Manually

If your CA does not support SCEP or if a network connection between the router and CA is not possible. Perform the following task to set up manual certificate enrollment:

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>crypto pki trustpoint <i>server name</i></code>	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 3	<code>enrollment url <i>url name pem</i></code>	Specifies the URL of the CA on which your device should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: <code>http:// [2001:DB8:1:1::1]:80</code> . The pem keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.
Step 4	<code>rsa keypair <i>label</i></code>	Specifies which key pair to associate with the certificate.
Step 5	<code>serial-number none</code>	The none keyword specifies that a serial number will not be included in the certificate request.
Step 6	<code>ip-address none</code>	The none keyword specifies that no IP address should be included in the certificate request.
Step 7	<code>revocation-check <i>crl</i></code>	Specifies CRL as the method to ensure that the certificate of a peer has not been revoked.
Step 8	<code>exit</code>	Exits Global Configuration mode.
Step 9	<code>crypto pki authenticate <i>name</i></code>	Retrieves the CA certificate and authenticates it.
Step 10	<code>crypto pki enroll <i>name</i></code>	Generates certificate request and displays the request for copying and pasting into the certificate server. Enter enrollment information when you are prompted. For example, specify whether to include the device FQDN and IP address in the certificate request. You are also given the choice about displaying the certificate request to the console terminal. The base-64 encoded certificate with or without PEM headers as requested is displayed.
Step 11	<code>crypto pki import <i>name certificate</i></code>	Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate. The device attempts to retrieve the granted certificate via TFTP using the same filename used to send the request, except the extension is changed from “.req” to “.crt”. For

	Command or Action	Purpose
		usage key certificates, the extensions “-sign.crt” and “-encr.crt” are used. The device parses the received files, verifies the certificates, and inserts the certificates into the internal certificate database on the switch. Note Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If your CA ignores the usage key information in the certificate request, only import the general purpose certificate. The router will not use one of the two key pairs generated.
Step 12	<code>exit</code>	Exits global configuration mode.
Step 13	<code>show crypto pki certificate <i>trustpoint name</i></code>	Displays information about the certificate for the trust point.
Step 14	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Enabling 802.1x Authentication and Configuring AAA

Procedure

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	<code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>aaa new-model</code>	Enables AAA.
Step 4	<code>dot1x system-auth-control</code>	Enables 802.1X on your device.
Step 5	<code>radius server <i>name</i></code>	Specifies the name of the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode.
Step 6	<code>address <i>ip-address</i> auth-port <i>port-number</i> acct-port <i>port-number</i></code>	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
Step 7	<code>automate-tester username <i>username</i></code>	Enables the automated testing feature for the RADIUS server. With this practice, the device sends periodic test authentication messages to the RADIUS server. It looks for a RADIUS response from the server. A success

	Command or Action	Purpose
		message is not necessary - a failed authentication suffices, because it shows that the server is alive.
Step 8	<code>key string</code>	Configures the authentication and encryption key for all RADIUS communications between the device and the RADIUS server.
Step 9	<code>radius-server deadtime minutes</code>	Improves RADIUS response time when some servers might be unavailable and skips unavailable servers immediately.
Step 10	<code>exit</code>	Returns to global configuration mode.
Step 11	<code>aaa group server radius group-name</code>	Groups different RADIUS server hosts into distinct lists and distinct methods, and enters server group configuration mode.
Step 12	<code>server name</code>	Assigns the RADIUS server name.
Step 13	<code>exit</code>	Returns to global configuration mode.
Step 14	<code>aaa authentication dot1x default group group-name</code>	Sets the default authentication server group for IEEE 802.1x.
Step 15	<code>aaa authorization network default group group-name</code>	Sets the network authorization default group.

Configuring EAP-TLS Profile and 802.1x Credentials

Procedure

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>eap profile profile-name</code>	Configures EAP profile and enters EAP profile configuration mode.
Step 4	<code>method tls</code>	Enables EAP-TLS method on the device.
Step 5	<code>pki-trustpoint name</code>	Sets the default PKI trustpoint.
Step 6	<code>exit</code>	Returns to global configuration mode.
Step 7	<code>dot1x credentials profile-name</code>	Configures 802.1x credentials profile and enters dot1x credentials configuration mode.
Step 8	<code>username username</code>	Sets the authentication user ID.
Step 9	<code>pki-trustpoint name</code>	Sets the default PKI trustpoint.

	Command or Action	Purpose
Step 10	end	Returns to privileged EXEC mode.

Applying the 802.1x MACsec MKA Configuration on Interfaces

To apply MACsec MKA using EAP-TLS to interfaces, perform the following task:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i>	Identifies the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.
Step 3	macsec network-link	Enables MACsec on the interface.
Step 4	authentication periodic	Enables reauthentication for this port.
Step 5	authentication timer reauthenticate interval	Sets the reauthentication interval.
Step 6	access-session host-mode multi-domain	Allows hosts to gain access to the interface.
Step 7	access-session closed	Prevents preauthentication access on the interface.
Step 8	access-session port-control auto	Sets the authorization state of a port.
Step 9	dot1x pae both	Configures the port as an 802.1X port access entity (PAE) supplicant and authenticator.
Step 10	dot1x credentials profile	Assigns a 802.1x credentials profile to the interface.
Step 11	dot1x supplicant eap profile <i>name</i>	Assigns the EAP-TLS profile to the interface.
Step 12	service-policy type control subscriber <i>control-policy name</i>	Applies a subscriber control policy to the interface.
Step 13	exit	Returns to privileged EXEC mode.
Step 14	show macsec interface	Displays MACsec details for the interface.
Step 15	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Local Authentication

Configuring the EAP Credentials using Local Authentication

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	aaa new-model	Enables AAA.
Step 4	aaa local authentication default authorization default	Sets the default local authentication and default local authorization method.
Step 5	aaa authentication dot1x default local	Sets the default local username authentication list for IEEE 802.1x.
Step 6	aaa authorization network default local	Sets an authorization method list for local user.
Step 7	aaa authorization credential-download default local	Sets an authorization method list for use of local credentials.
Step 8	exit	Returns to privileged EXEC mode.

Configuring the Local EAP-TLS Authentication and Authorization Profile

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	aaa new-model	Enables AAA.
Step 4	dot1x credentials <i>profile-name</i>	Configures the dot1x credentials profile and enters dot1x credentials configuration mode.
Step 5	username <i>name</i> password <i>password</i>	Sets the authentication user ID and password.
Step 6	exit	Returns to global configuration mode.
Step 7	aaa attribute list <i>list-name</i>	(Optional) Sets the AAA attribute list definition and enters attribute list configuration mode.
Step 8	aaa attribute type linksec-policy must-secure	(Optional) Specifies the AAA attribute type.

	Command or Action	Purpose
Step 9	<code>exit</code>	Returns to global configuration mode.
Step 10	<code>username name aaa attribute list name</code>	(Optional) Specifies the AAA attribute list for the user ID.
Step 11	<code>end</code>	Returns to privileged EXEC mode.

Configuring Enrollment using SCEP

Simple Certificate Enrollment Protocol (SCEP) is a Cisco-developed enrollment protocol that uses HTTP to communicate with the certificate authority (CA) or registration authority (RA). SCEP is the most commonly used method for sending and receiving requests and certificates.

Procedure

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>crypto pki trustpoint server name</code>	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	<code>enrollment url url name pem</code>	Specifies the URL of the CA on which your device should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: <code>http://[2001:DB8:1:1::1]:80</code> . The pem keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.
Step 5	<code>rsa keypair label</code>	Specifies which key pair to associate with the certificate. Note The rsa keypair name must match the trust-point name.
Step 6	<code>serial-number none</code>	The none keyword specifies that a serial number will not be included in the certificate request.
Step 7	<code>ip-address none</code>	The none keyword specifies that no IP address should be included in the certificate request.
Step 8	<code>revocation-check crl</code>	Specifies CRL as the method to ensure that the certificate of a peer has not been revoked.
Step 9	<code>auto-enroll percent regenerate</code>	Enables auto-enrollment, allowing the client to automatically request a rollover certificate from the CA.

	Command or Action	Purpose
		<p>If auto-enrollment is not enabled, the client must be manually re-enrolled in your PKI upon certificate expiration.</p> <p>By default, only the Domain Name System (DNS) name of the device is included in the certificate.</p> <p>Use the percent argument to specify that a new certificate will be requested after the percentage of the lifetime of the current certificate is reached.</p> <p>Use the regenerate keyword to generate a new key for the certificate even if a named key already exists.</p> <p>If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable: “! RSA key pair associated with trustpoint is exportable.”</p> <p>It is recommended that a new key pair be generated for security reasons.</p>
Step 10	crypto pki authenticate <i>name</i>	Retrieves the CA certificate and authenticates it.
Step 11	exit	Exits global configuration mode.
Step 12	show crypto pki certificate <i>trustpoint name</i>	Displays information about the certificate for the trust point.

Configuring Enrollment Manually

If your CA does not support SCEP or if a network connection between the router and CA is not possible. Perform the following task to set up manual certificate enrollment:

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint <i>server name</i>	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	enrollment url <i>url name pem</i>	<p>Specifies the URL of the CA on which your device should send certificate requests.</p> <p>An IPv6 address can be added in the URL enclosed in brackets. For example: http:// [2001:DB8:1:1::1]:80.</p>

	Command or Action	Purpose
		The pem keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.
Step 5	rsa keypair <i>label</i>	Specifies which key pair to associate with the certificate.
Step 6	serial-number none	The none keyword specifies that a serial number will not be included in the certificate request.
Step 7	ip-address none	The none keyword specifies that no IP address should be included in the certificate request.
Step 8	revocation-check <i>crl</i>	Specifies CRL as the method to ensure that the certificate of a peer has not been revoked.
Step 9	exit	Exits Global Configuration mode.
Step 10	crypto pki authenticate <i>name</i>	Retrieves the CA certificate and authenticates it.
Step 11	crypto pki enroll <i>name</i>	<p>Generates certificate request and displays the request for copying and pasting into the certificate server.</p> <p>Enter enrollment information when you are prompted. For example, specify whether to include the device FQDN and IP address in the certificate request.</p> <p>You are also given the choice about displaying the certificate request to the console terminal.</p> <p>The base-64 encoded certificate with or without PEM headers as requested is displayed.</p>
Step 12	crypto pki import <i>name certificate</i>	<p>Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate.</p> <p>The device attempts to retrieve the granted certificate via TFTP using the same filename used to send the request, except the extension is changed from “.req” to “.crt”. For usage key certificates, the extensions “-sign.crt” and “-encr.crt” are used.</p> <p>The device parses the received files, verifies the certificates, and inserts the certificates into the internal certificate database on the switch.</p> <p>Note Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If your CA ignores the usage key information in the certificate request, only import the general purpose certificate. The router will not use one of the two key pairs generated.</p>
Step 13	exit	Exits Global Configuration mode.

	Command or Action	Purpose
Step 14	<code>show crypto pki certificate <i>trustpoint name</i></code>	Displays information about the certificate for the trust point.
Step 15	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Configuring EAP-TLS Profile and 802.1x Credentials

Procedure

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>eap profile <i>profile-name</i></code>	Configures EAP profile and enters EAP profile configuration mode.
Step 4	<code>method tls</code>	Enables EAP-TLS method on the device.
Step 5	<code>pki-trustpoint <i>name</i></code>	Sets the default PKI trustpoint.
Step 6	<code>exit</code>	Returns to global configuration mode.
Step 7	<code>dot1x credentials <i>profile-name</i></code>	Configures 802.1x credentials profile and enters dot1x credentials configuration mode.
Step 8	<code>username <i>username</i></code>	Sets the authentication user ID.
Step 9	<code>pki-trustpoint <i>name</i></code>	Sets the default PKI trustpoint.
Step 10	<code>end</code>	Returns to privileged EXEC mode.

Applying the 802.1x MKA MACsec Configuration on Interfaces

To apply MKA MACsec using EAP-TLS to interfaces, perform the following task:

Procedure

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>interface <i>interface-id</i></code>	Identifies the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.

The **show macsec status interface *interface-id*** displays MACsec status information for the given interface.

```
Device# show macsec status interface te0/1/2
```

```
Capabilities:
Ciphers Supported:      GCM-AES-128 GCM-AES-256
Cipher:                 GCM-AES-128
Confidentiality Offset: 0
Replay Window:         64
Delay Protect Enable:   FALSE
Access Control:         must-secure

Transmit SC:
  SCI:                  74A2E6254C220012
  Transmitting:         TRUE
Transmit SA:
  Next PN:              412
  Delay Protect AN/nextPN: 99/0

Receive SC:
  SCI:                  74A2E62544130013
  Receiving:            TRUE
Receive SA:
  Next PN:              64
  AN:                   0
  Delay Protect AN/LPN: 0/0
```

The **show access-session interface *interface-id* details** displays detailed information about the access session for the given interface.

```
Device# show access-session interface te1/0/1 details
```

```
Interface: TenGigabitEthernet1/0/1
  IIF-ID: 0x17298FCD
  MAC Address: f8a5.c592.13e4
  IPv6 Address: Unknown
  IPv4 Address: Unknown
  User-Name: DOT1XCRED
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-host
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 00000000000000BB72E8AFA
  Acct Session ID: Unknown
  Handle: 0xc3000001
  Current Policy: MUSTS_1

Local Policies:
  Security Policy: Must Secure
  Security Status: Link Secured

Server Policies:

Method status list:
  Method      State
  dot1xSup    Authc Success
  dot1x       Authc Success
```

Configuring Cisco TrustSec MACsec

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 <i>device-id</i> password <i>cts-password</i> 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. <ul style="list-style-type: none"> • id <i>device-id</i>—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 <i>cts-password</i>—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: Switch# 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 3560cx universal IP base and IP services 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-listmode1 [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 <i>interface-id</i>	Note Enters interface configuration mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Switch(config)# interface tengigabitethernet 1/1/2</pre>	
Step 3	<p>cts dot1x</p> <p>Example:</p> <pre>Switch(config-if)# cts dot1x</pre>	Configures the interface to perform NDAC authentication.
Step 4	<p>sap mode-list<i>mode1</i> [<i>mode2</i> [<i>mode3</i> [<i>mode4</i>]]]</p> <p>Example:</p> <pre>Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap</pre>	<p>(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.</p> <p>Choices for <i>mode</i> are:</p> <ul style="list-style-type: none"> • gcm-encrypt—Authentication and encryption <p>Note Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.</p> <ul style="list-style-type: none"> • gmac—Authentication, no encryption • no-encap—No encapsulation • null—Encapsulation, no authentication or encryption <p>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.</p> <p>Note Although visible in the CLI help, the timer reauthentication and propagate sgt keywords are not supported.</p>
Step 5	<p>no propagate sgt</p> <p>Example:</p> <pre>Switch(config-if-cts-dot1x)# no propagate sgt</pre>	The switch (Catalyst 3560cx) does not support SGT tagging. This command disables propagation of SGT tag on the CTS link. It is mandatory that for the peer switch also to have "no propagate sgt" configured for the traffic to flow properly over the CTS link.
Step 6	<p>exit</p> <p>Example:</p> <pre>Switch(config-if-cts-dot1x)# exit</pre>	Exits Cisco TrustSec 802.1x interface configuration mode.
Step 7	<p>end</p> <p>Example:</p> <pre>Switch(config-if)# end</pre>	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	show cts interface [<i>interface-id</i> brief summary]	(Optional) Verify the configuration by displaying TrustSec-related interface characteristics.
Step 9	copy running-config startup-config Example: Switch# 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)# no propagate sgt
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# end
```

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**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> 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 <i>key</i> [mode-list <i>mode1</i> [<i>mode2</i> [<i>mode3</i> [<i>mode4</i>]]]] Example: Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap	<p>(Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode.</p> <ul style="list-style-type: none"> • <i>key</i>—A hexadecimal value with an even number of characters and a maximum length of 32 characters. <p>The SAP operation mode options:</p> <ul style="list-style-type: none"> • gcm-encrypt—Authentication and encryption <p>Note Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.</p> <ul style="list-style-type: none"> • gmac—Authentication, no encryption • no-encap—No encapsulation • null—Encapsulation, no authentication or encryption

	Command or Action	Purpose
		<p>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.</p>
Step 5	<p>no propagate sgt</p> <p>Example:</p> <pre>Switch(config-if-cts-manual)# no propagate sgt</pre>	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	<p>exit</p> <p>Example:</p> <pre>Switch(config-if-cts-manual)# exit</pre>	Exits Cisco TrustSec 802.1x interface configuration mode.
Step 7	<p>end</p> <p>Example:</p> <pre>Switch(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 8	<p>show cts interface [<i>interface-id</i> brief summary]</p>	(Optional) Verify the configuration by displaying TrustSec-related interface characteristics.

Example

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

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 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
```

Configuration Examples for Configuring MACsec Encryption

Example: Configuring MACsec on an Interface

Configuring MACsec on an Interface

```
Switch(config)# interface GigabitEthernet1/0/25
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# macsec
Switch(config-if)# authentication event linksec fail action authorize vlan 2
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication linksec policy must-secure
```



```
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate
Switch(config-if)# authentication violation protect
Switch(config-if)# mka policy replay-policy
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch# show authentication session interface gigabitethernet1/0/5
```

```
Interface MAC Address Method Domain Status Fg Session ID
-----
Gi1/0/5 88f0.7788.9205 dot1x VOICE Auth 1E0000010000001300030B0F
Gi1/0/5 000c.2923.6ff1 dot1x DATA Auth 1E0000010000001400030D80
```

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
7 5 dot1x
21 10 mab
```

```
19 15 webauth
```

```
Switch# show authentication session interface gigabitethernet1/0/5 details
```

```
Interface: GigabitEthernet1/0/5
MAC Address: 88f0.7788.9205
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: CP-9971-SEP88F077889205
Status: Authorized
Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
Session timeout: N/A
Common Session ID: 1E0000010000001300030B0F
Acct Session ID: Unknown
Handle: 0xC0000006
Current Policy: POLICY_Gi1/0/5
```

Local Policies:

```
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure
```

Server Policies:

Method status list:

Method State

```

dot1x Authc Success

-----
Interface: GigabitEthernet1/0/5
MAC Address: 000c.2923.6ff1
IPv6 Address: Unknown
IPv4 Address: 172.30.30.50
User-Name: dataMustSecure
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Session timeout: N/A
Common Session ID: 1E0000010000001400030D80
Acct Session ID: Unknown
Handle: 0x22000007
Current Policy: POLICY_Gil/0/5

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Security Status: Link Secured

Server Policies:

Method status list:
Method State

dot1x Authc Success

Switch#
Switch# show macsec interface gigabitethernet1/0/5
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 : 8
Max. Tx SA : 8
Max. Rx SC : 4
Max. Tx SC : 4
Validate Frames : strict
PN threshold notification support : Yes
Ciphers supported : GCM-AES-128

Transmit Secure Channels
SCI : 547C69B687850002
SC state : inUse(1)
Elapsed time : 16:36:44
Start time : 7w0d
Current AN: 0

```

```
Previous AN: -
Next PN: 0
SA State: inUse(1)
Confidentiality : no
SAK Unchanged : no
SA Create time : 00:09:21
SA Start time : 7w0d
SC Statistics
Auth-only Pkts : 0
Auth-only Bytes : 0
Encrypt Pkts : 52960
Encrypt Bytes : 0
SA Statistics
Auth-only Pkts : 0
Encrypt Pkts : 52960

Port Statistics

Receive Secure Channels
SCI : 000C29236FF10000
SC state : inUse(1)
Elapsed time : 16:36:44
Start time : 7w0d
Current AN: 0
Previous AN: -
Next PN: 0
RX SA Count: 0
SA State: inUse(1)
SAK Unchanged : no
SA Create time : 00:09:19
SA Start time : 7w0d
SC Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 9914
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 9914
UnusedSA pkts 0
NousingSA pkts 0

Port Statistics

Switch#
```

Configuration Examples for MACsec MKA using EAP-TLS

Example: Enrolling the Certificate

```
Configure Crypto PKI Trustpoint:
```

Example: Enabling 802.1x Authentication and AAA Configuration

```

crypto pki trustpoint POLESTAR-IOS-CA
  enrollment terminal
  subject-name CN=ASR1000x1@polestar.com, C=IN, ST=KA, OU=ENG,O=Polestar
  revocation-check none
  rsa-keypair mkaioscarsa
  storage nvram:
!
```

Manual Installation of Root CA certificate:

```
crypto pki authenticate POLESTAR-IOS-CA
```

Example: Enabling 802.1x Authentication and AAA Configuration

```

aaa new-model
dot1x system-auth-control
radius server ISE
  address ipv4 <ISE ipv4 address> auth-port 1645 acct-port 1646
  automate-tester username dummy
  key dummy123
  radius-server deadtime 2
!
aaa group server radius ISEGRP
  server name ISE
!
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

Example: Configuring EAP-TLS Profile and 802.1X Credentials

```

eap profile EAPTLS-PROF-IOSCA
  method tls
  pki-trustpoint POLESTAR-IOS-CA
!

dot1x credentials EAPTLSCRED-IOSCA
  username asr1000@polestar.company.com
  pki-trustpoint POLESTAR-IOS-CA
!
```

Example: Applying 802.1X, PKI, and MACsec Configuration on the Interface

```

interface TenGigabitEthernet0/1
  macsec network-link
  authentication periodic
  authentication timer reauthenticate <reauthentication interval>
  access-session host-mode multi-host
  access-session closed
  access-session port-control auto
  dot1x pae both
  dot1x credentials EAPTLSCRED-IOSCA
  dot1x supplicant eap profile EAPTLS-PROF-IOSCA
  service-policy type control subscriber DOT1X_POLICY_RADIUS
```

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 gil1/1/2
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)# no propagate sgt
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# interface gil1/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt gmac
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit
```

```
Switch(config)# radius-server vsa send authentication
Switch(config)# exit
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 gil/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 gil/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
gmac
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit

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