



# MACsec Encryption

---

- [Prerequisites for MACsec Encryption, on page 1](#)
- [Restrictions for MACsec Encryption, on page 1](#)
- [Information about MACsec Encryption, on page 2](#)
- [How to Configure MACsec Encryption, on page 8](#)
- [Configuration Examples for MACsec Encryption, on page 21](#)
- [Feature Information for MACsec Encryption, on page 30](#)

## Prerequisites for MACsec Encryption

### Prerequisites for Certificate-Based MACsec

- 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.

## Restrictions for MACsec Encryption

- MACsec configuration is not supported on EtherChannel ports.
- Bidirectional Forwarding and Detection (BFD) is not supported on both MKA pre-shared keys (PSK) and MKA Extensible Authentication Protocol (EAP-TLS).
- The MACsec Cipher announcement is not supported for MACsec XPN Ciphers.
- Certificated based MACSec (EAP-TLS) is not supported if the access-session mode is configured as open.
- MACsec XPN Cipher Suites are not supported in MACsec connections.

- If the **dot1q tag vlan native** command is configured globally, the dot1x reauthentication will fail on trunk ports.
- MACsec with Precision Time Protocol (PTP) is not supported.
- MACsec is not supported on Locator ID Separation Protocol (LISP) interfaces and Cisco Software-Defined Access (SD-Access) solution.
- MACsec is not supported with Multicast VPN (mVPN).

## Information about MACsec Encryption

MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Catalyst switches support 802.1AE encryption with MACsec Key Agreement (MKA) on downlink ports for encryption between the switch and host device. The switch also supports MACsec encryption for switch-to-switch (inter-network device) security using both Cisco TrustSec Network Device Admission Control (NDAC), Security Association Protocol (SAP) and MKA-based key exchange protocol.



**Note** When switch-to-switch MACSec is enabled, all traffic is encrypted, except the EAP-over-LAN (EAPOL) packets.

Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional). Link layer security is supported on SAP-based MACsec.

**Table 1: MACsec Support on Switch Ports**

Connections	MACsec support
Switch-to-host	MACsec MKA encryption
Switch-to-switch	MACsec MKA encryption 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. MKA is supported on switch-to-host facing links (downlink) as well as switch-to-switch links (uplink). Host-facing links typically use flexible authentication ordering for handling heterogeneous devices with or without IEEE 802.1x, and can optionally use MKA-based MACsec encryption. 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.

## Recommendations for MACsec Encryption

This section lists the recommendations for configuring MACsec encryption:

- Use the confidentiality (encryption) offset as 0 in switch-to-host connections.
- Use Bidirectional Forwarding and Detection (BFD) timer value as 750 milliseconds for 10Gbps ports and 1.25 seconds for any port with speed above 10Gbps.

- Execute the **shutdown** command, and then the **no shutdown** command on a port, after changing any MKA policy or MACsec configuration for active sessions, so that the changes are applied to active sessions.
- Use Extended Packet Numbering (XPN) Cipher Suite for port speeds of 40Gbps and above.
- Set the connectivity association key (CAK) rekey overlap timer to 30 seconds or more.
- Do not use Cisco TrustSec Security Association Protocol (SAP) MACsec encryption for port speeds above 10Gbps.
- Do not enable both Cisco TrustSec SAP and uplink MKA at the same time on any interface.
- We recommend that you use MACsec MKA encryption.

## 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 the uplink. 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.

Starting with Cisco IOS XE Fuji 16.8.1, must-secure support for MKA uplink is enabled. MKA policy on a switch port can be configured in one of the following ways:

- **Must secure:** Once MACsec MKA is configured, all traffic must encrypt the packet. Unencrypted packets are dropped.

- Should secure: If the peer is configured for MACsec, the data traffic is encrypted, otherwise it is sent in clear text.




---

**Note** Must-secure mode is enabled by default.

---




---

**Note** Integrity check value (ICV) indicator in MACsec Key Agreement Protocol Data Unit is optional.

---

## MKA Policies

To enable MKA on an interface, a defined MKA policy should be applied to the 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

## Key Lifetime and Hitless Key Rollover

A MACsec key chain can have multiple pre-shared keys (PSK) each configured with a key id and an optional lifetime. A key lifetime specifies at which time the key expires. In the absence of a lifetime configuration, the default lifetime is unlimited. When a lifetime is configured, MKA rolls over to the next configured pre-shared key in the key chain after the lifetime is expired. Time zone of the key can be local or UTC. Default time zone is UTC.

You can Key rolls over to the next key within the same key chain by configuring a second key in the key chain and configuring a lifetime for the first key. When the lifetime of the first key expires, it automatically rolls over to the next key in the list. If the same key is configured on both sides of the link at the same time, then the key rollover is hitless, that is, key rolls over without traffic interruption.

On all participating devices, the MACsec key chain must be synchronised by using Network Time Protocol (NTP) and the same time zone must be used. If all the participating devices are not synchronized, the connectivity association key (CAK) rekey will not be initiated on all the devices at the same time.




---

**Note** The lifetime of the keys need to be overlapped in order to achieve hitless key rollover.

---

## 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. See [Example: Displaying MKA Information, on page 24](#) for further information.

## Key Lifetime and Hitless Key Rollover

A MACsec key chain can have multiple pre-shared keys (PSK) each configured with a key id and an optional lifetime. A key lifetime specifies at which time the key expires. In the absence of a lifetime configuration, the default lifetime is unlimited. When a lifetime is configured, MKA rolls over to the next configured pre-shared

key in the key chain after the lifetime is expired. Time zone of the key can be local or UTC. Default time zone is UTC.

You can Key rolls over to the next key within the same key chain by configuring a second key in the key chain and configuring a lifetime for the first key. When the lifetime of the first key expires, it automatically rolls over to the next key in the list. If the same key is configured on both sides of the link at the same time, then the key rollover is hitless, that is, key rolls over without traffic interruption.

On all participating devices, the MACsec key chain must be synchronised by using Network Time Protocol (NTP) and the same time zone must be used. If all the participating devices are not synchronized, the connectivity association key (CAK) rekey will not be initiated on all the devices at the same time.



**Note** The lifetime of the keys need to be overlapped in order to achieve hitless key rollover.

## MACsec, MKA and 802.1x Host Modes

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

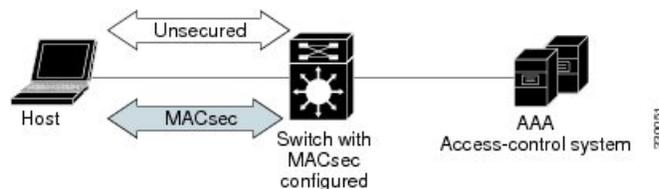


**Note** Switch-to-host connection is not supported on downlink ports in Cisco IOS XE Everest 16.5.1a. Support will be added in future releases.

### Single-Host Mode

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

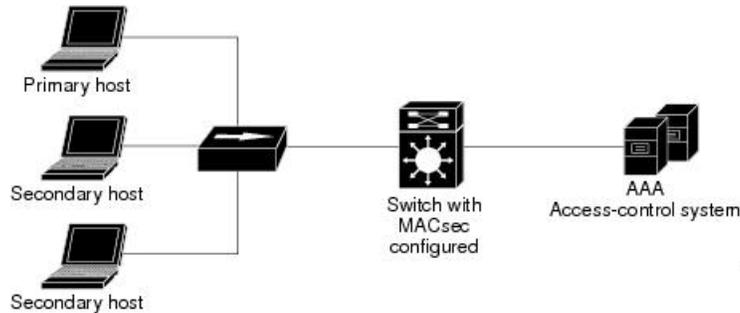
**Figure 1: MACsec in Single-Host Mode with a Secured Data Session**



### Multiple Host Mode

In standard (not 802.1x REV) 802.1x multiple-host mode, a port is open or closed based on a single authentication. If one user, the primary secured client services client host, is authenticated, the same level of network access is provided to any host connected to the same port. If a secondary host is a MACsec supplicant, it cannot be authenticated and traffic would not flow. A secondary host that is a non-MACsec host can send traffic to the network without authentication because it is in multiple-host mode. The figure shows MACsec in Standard Multiple-Host Unsecure Mode.

Figure 2: MACsec in Multiple-Host Mode - Unsecured



**Note** Multi-host mode is not recommended because after the first successful client, authentication is not required for other clients, which is not secure.

In standard (not 802.1x REV) 802.1x multiple-domain mode, a port is open or closed based on a single authentication. If the primary user, a PC on data domain, is authenticated, the same level of network access is provided to any domain connected to the same port. If a secondary user is a MACsec supplicant, it cannot be authenticated and traffic would no flow. A secondary user, an IP phone on voice domain, that is a non-MACsec host, can send traffic to the network without authentication because it is in multiple-domain mode.

## Multiple-Domain Mode

In standard (not 802.1x REV) 802.1x multiple-domain mode, a port is open or closed based on a single authentication. If the primary user, a PC on data domain, is authenticated, the same level of network access is provided to any domain connected to the same port. If a secondary user is a MACsec supplicant, it cannot be authenticated and traffic would no flow. A secondary user, an IP phone on voice domain, that is a non-MACsec host, can send traffic to the network without authentication because it is in multiple-domain mode.

## 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.

## 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>
Network Device Admission Control (NDAC)	<p>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.</p>
Security Association Protocol (SAP)	<p>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.</p>
Security Group Tag (SGT)	<p>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.</p>

Cisco TrustSec Feature	Description
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

## How to Configure MACsec Encryption

### Configuring MKA and MACsec

#### Default MACsec MKA Configuration

MACsec is disabled. No MKA policies are configured.

#### Configuring an MKA Policy

##### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enter global configuration mode.
<b>Step 2</b>	<code>mka policy <i>policy name</i></code>	Identify an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters.

	Command or Action	Purpose
		<p><b>Note</b> The default MACsec cipher suite in the MKA policy will always be "GCM-AES-128". If the device supports both "GCM-AES-128" and "GCM-AES-256" ciphers, it is highly recommended to define and use a user defined MKA policy to include both 128 and 256 bits ciphers or only 256 bits cipher, as may be required.</p>
<b>Step 3</b>	<code>key-server priority</code>	<p>Configure MKA key server options and set priority (between 0-255).</p> <p><b>Note</b> When value of key server priority is set to 255, the peer can not become the key server.</p>
<b>Step 4</b>	<code>include-icv-indicator</code>	Enables the ICV indicator in MKPDU. Use the <b>no</b> form of this command to disable the ICV indicator — <b>no include-icv-indicator</b> .
<b>Step 5</b>	<code>macsec-cipher-suite gcm-aes-128</code>	Configures cipher suite for deriving SAK with 128-bit encryption.
<b>Step 6</b>	<code>confidentiality-offset Offset value</code>	<p>Set the Confidentiality (encryption) offset for each physical interface</p> <p><b>Note</b> Offset Value can be 0, 30 or 50. If you are using Anyconnect on the client, it is recommended to use Offset 0.</p>
<b>Step 7</b>	<code>end</code>	Returns to privileged EXEC mode.
<b>Step 8</b>	<code>show mka policy</code>	Verify your entries.

### Example

This example configures the MKA policy:

```
Switch(config)# mka policy mka_policy
Switch(config-mka-policy)# key-server priority 200
Switch(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Switch(config-mka-policy)# confidentiality-offset 30
Switch(config-mka-policy)# end
```

## Configuring Switch-to-host MACsec Encryption

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

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch>enable	Enables privileged EXEC mode. Enter the password if prompted.
<b>Step 2</b>	<b>configureterminal</b> <b>Example:</b> Switch>configure terminal	Enters the global configuration mode.
<b>Step 3</b>	<b>interface interface-id</b>	Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.
<b>Step 4</b>	<b>switchport access vlanvlan-id</b>	Configure the access VLAN for the port.
<b>Step 5</b>	<b>switchport mode access</b>	Configure the interface as an access port.
<b>Step 6</b>	<b>authentication event linksec fail action authorize vlan vlan-id</b>	(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.
<b>Step 7</b>	<b>authentication host-mode multi-domain</b>	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.
<b>Step 8</b>	<b>authentication linksec policy must-secure</b>	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> .
<b>Step 9</b>	<b>authentication port-control auto</b>	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.
<b>Step 10</b>	<b>authentication periodic</b>	Enable or Disable Reauthentication for this port .
<b>Step 11</b>	<b>authentication timer reauthenticate</b>	Enter a value between 1 and 65535 (in seconds). Obtains re-authentication timeout value from the server. Default re-authentication time is 3600 seconds.
<b>Step 12</b>	<b>authentication violation protect</b>	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

	Command or Action	Purpose
		are connected to that port. If not configured, the default is to shut down the port.
<b>Step 13</b>	<b>mka policy</b> <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 <b>mka policy</b> global configuration command).
<b>Step 14</b>	<b>dot1x pae authenticator</b>	Configure the port as an 802.1x port access entity (PAE) authenticator.
<b>Step 15</b>	<b>spanning-tree portfast</b>	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
<b>Step 16</b>	<b>end</b> <b>Example:</b> <code>Switch(config)#end</code>	Returns to privileged EXEC mode.
<b>Step 17</b>	<b>show authentication session interface</b> <i>interface-id</i>	Verify the authorized session security status.
<b>Step 18</b>	<b>show authentication session interface</b> <i>interface-id</i> details	Verify the details of the security status of the authorized session.
<b>Step 19</b>	<b>show macsec interface</b> <i>interface-id</i>	Verify MacSec status on the interface.
<b>Step 20</b>	<b>show mka sessions</b>	Verify the established mka sessions.
<b>Step 21</b>	<b>copy running-config startup-config</b> <b>Example:</b> <code>Switch#copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## Configuring MACsec MKA using PSK

Beginning in privileged EXEC mode, follow these steps to configure MACsec MKA policies using a Pre Shared Key (PSK).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <code>Device&gt; enable</code>	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>key chain <i>key-chain-name</i> macsec</b> <b>Example:</b> Device(config)# <b>key chain keychain1 macsec</b>	Configures a key chain and enters the key chain configuration mode.
<b>Step 4</b>	<b>key <i>hex-string</i></b> <b>Example:</b> Device(config-key-chain)# <b>key 1000</b>	Configures a unique identifier for each key in the keychain and enters the keychain's key configuration mode.  <b>Note</b> For 128-bit encryption, use any value between 1 and 32 hex digit key-string. For 256-bit encryption, use 64 hex digit key-string.
<b>Step 5</b>	<b>cryptographic-algorithm {<i>aes-128-cmac</i> / <i>aes-256-cmac</i>}</b> <b>Example:</b> Device(config-key-chain)# <b>cryptographic-algorithm aes-128-cmac</b>	Set cryptographic authentication algorithm with 128-bit or 256-bit encryption.
<b>Step 6</b>	<b>key-string { [0/6/7] <i>pwd-string</i> / <i>pwd-string</i> }</b> <b>Example:</b> Device(config-key-chain)# <b>key-string 12345678901234567890123456789012</b>	Sets the password for a key string. Only hex characters must be entered.
<b>Step 7</b>	<b>lifetime local [<i>start timestamp</i> {<i>hh::mm::ss</i> / <i>day</i> / <i>month</i> / <i>year</i>}] [<b>duration</b> <i>seconds</i>   <i>end timestamp</i> {<i>hh::mm::ss</i> / <i>day</i> / <i>month</i> / <i>year</i>}]</b> <b>Example:</b> Device(config-key-chain)# <b>lifetime local 12:12:00 July 28 2016 12:19:00 July 28 2016</b>	Sets the lifetime of the pre shared key.
<b>Step 8</b>	<b>end</b> <b>Example:</b> Device(config-key-chain)# <b>end</b>	Exits key chain configuration mode and returns to privileged EXEC mode.

## Configuring MACsec MKA on an Interface using PSK

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>interface-id</i>	Enters interface configuration mode.
<b>Step 3</b>	<b>macsec network-link</b>	Enables MACsec on the interface.
<b>Step 4</b>	<b>mka policy</b> <i>policy-name</i>	Configures an MKA policy.
<b>Step 5</b>	<b>mka pre-shared-key key-chain</b> <i>key-chain name</i>	Configures an MKA pre-shared-key key-chain name.  <b>Note</b> The MKA pre-shared key can be configured on either physical interface or sub-interfaces and not on both.
<b>Step 6</b>	<b>macsec replay-protection window-size</b> <i>frame number</i>	Sets the MACsec window size for replay protection.
<b>Step 7</b>	<b>end</b>	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

### Generating Key Pairs

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>crypto key generate rsa label <i>label-name</i> general-keys modulus <i>size</i></b>	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.
<b>Step 3</b>	<b>end</b>	Returns to privileged EXEC mode.
<b>Step 4</b>	<b>show authentication session interface <i>interface-id</i></b>	Verifies the authorized session security status.
<b>Step 5</b>	<b>copy running-config startup-config</b>	(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
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>crypto pki trustpoint</b> <i>server name</i>	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
<b>Step 3</b>	<b>enrollment url</b> <i>url name pem</i>	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: http://[2001:DB8:1:1::1]:80.  The pem keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.
<b>Step 4</b>	<b>rsakeypair</b> <i>label</i>	Specifies which key pair to associate with the certificate.  <b>Note</b> The <b>rsakeypair</b> name must match the trust-point name.
<b>Step 5</b>	<b>serial-number none</b>	The <b>none</b> keyword specifies that a serial number will not be included in the certificate request.
<b>Step 6</b>	<b>ip-address none</b>	The <b>none</b> keyword specifies that no IP address should be included in the certificate request.
<b>Step 7</b>	<b>revocation-check crl</b>	Specifies CRL as the method to ensure that the certificate of a peer has not been revoked.
<b>Step 8</b>	<b>auto-enroll</b> <i>percent regenerate</i>	Enables auto-enrollment, allowing the client to automatically request a rollover certificate from the CA.  If auto-enrollment is not enabled, the client must be manually re-enrolled in your PKI upon certificate expiration.  By default, only the Domain Name System (DNS) name of the device is included in the certificate.  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.  Use the regenerate keyword to generate a new key for the certificate even if a named key already exists.

	Command or Action	Purpose
		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.”  It is recommended that a new key pair be generated for security reasons.
<b>Step 9</b>	<b>crypto pki authenticate</b> <i>name</i>	Retrieves the CA certificate and authenticates it.
<b>Step 10</b>	<b>exit</b>	Exits global configuration mode.
<b>Step 11</b>	<b>show crypto pki certificate</b> <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
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>crypto pki trustpoint</b> <i>server name</i>	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
<b>Step 3</b>	<b>enrollment url</b> <i>url name pem</i>	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: http://[2001:DB8:1:1::1]:80.  The pem keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.
<b>Step 4</b>	<b>rsakeypair</b> <i>label</i>	Specifies which key pair to associate with the certificate.
<b>Step 5</b>	<b>serial-number none</b>	The <b>none</b> keyword specifies that a serial number will not be included in the certificate request.
<b>Step 6</b>	<b>ip-address none</b>	The <b>none</b> keyword specifies that no IP address should be included in the certificate request.

	Command or Action	Purpose
<b>Step 7</b>	<code>revocation-check crl</code>	Specifies CRL as the method to ensure that the certificate of a peer has not been revoked.
<b>Step 8</b>	<code>exit</code>	Exits Global Configuration mode.
<b>Step 9</b>	<code>crypto pki authenticate <i>name</i></code>	Retrieves the CA certificate and authenticates it.
<b>Step 10</b>	<code>crypto pki enroll <i>name</i></code>	<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>
<b>Step 11</b>	<code>crypto pki import <i>name certificate</i></code>	<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><b>Note</b> 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>
<b>Step 12</b>	<code>exit</code>	Exits global configuration mode.
<b>Step 13</b>	<code>show crypto pki certificate <i>trustpoint name</i></code>	Displays information about the certificate for the trust point.

	Command or Action	Purpose
Step 14	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## 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.

# Configuring Cisco TrustSec MACsec

## 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.
- Before changing the configuration from MKA to Cisco TrustSec SAP and vice versa, we recommend that you remove the interface configuration.

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface <i>interface-id</i></b>  <b>Example:</b> Switch(config)# <b>interface tengigabitethernet 1/1/2</b>	<b>Note</b> Enters interface configuration mode.
<b>Step 3</b>	<b>cts manual</b>  <b>Example:</b> Switch(config-if)# <b>cts manual</b>	Enters Cisco TrustSec manual configuration mode.

	Command or Action	Purpose
Step 4	<p><b>sap pmk</b> <i>key</i> [<b>mode-list</b> <i>mode1</i> [<i>mode2</i> [<i>mode3</i> [<i>mode4</i>]]]]</p> <p><b>Example:</b></p> <pre>Switch(config-if-cts-manual)# <b>sap pmk</b> 1234abcdef <b>mode-list</b> <b>gcm-encrypt no-encap</b></pre>	<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"> <li>• <i>key</i>—A hexadecimal value with an even number of characters and a maximum length of 32 characters.</li> </ul> <p>The SAP operation mode options:</p> <ul style="list-style-type: none"> <li>• <b>gcm-encrypt</b>—Authentication and encryption</li> </ul> <p><b>Note</b> Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.</p> <ul style="list-style-type: none"> <li>• <b>gmac</b>—Authentication, no encryption</li> <li>• <b>no-encap</b>—No encapsulation</li> </ul>
Step 5	<p><b>no propagate sgt</b></p> <p><b>Example:</b></p> <pre>Switch(config-if-cts-manual)# <b>no</b> <b>propagate sgt</b></pre>	<p>Use the <b>no</b> form of this command when the peer is incapable of processing a SGT. The <b>no propagate sgt</b> command prevents the interface from transmitting the SGT to the peer.</p>
Step 6	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Switch(config-if-cts-manual)# <b>exit</b></pre>	<p>Exits Cisco TrustSec 802.1x interface configuration mode.</p>
Step 7	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config-if)# <b>end</b></pre>	<p>Returns to privileged EXEC mode.</p>
Step 8	<p><b>show cts interface</b> [<i>interface-id</i>   <b>brief</b>   <b>summary</b>]</p>	<p>(Optional) Verify the configuration by displaying TrustSec-related interface characteristics.</p>
Step 9	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Device#<b>copy running-config startup-config</b></pre>	<p>(Optional) Saves your entries in the configuration file.</p>

# Configuration Examples for MACsec Encryption

## Configuring Switch-to-host MACsec Encryption

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch>enable	Enables privileged EXEC mode. Enter the password if prompted.
<b>Step 2</b>	<b>configureterminal</b> <b>Example:</b> Switch>configure terminal	Enters the global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>interface-id</i>	Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.
<b>Step 4</b>	<b>switchport access vlan</b> <i>vlan-id</i>	Configure the access VLAN for the port.
<b>Step 5</b>	<b>switchport mode access</b>	Configure the interface as an access port.
<b>Step 6</b>	<b>authentication event linksec fail action</b> <b>authorize vlan</b> <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.
<b>Step 7</b>	<b>authentication host-mode multi-domain</b>	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.
<b>Step 8</b>	<b>authentication linksec policy must-secure</b>	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> .
<b>Step 9</b>	<b>authentication port-control auto</b>	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.
<b>Step 10</b>	<b>authentication periodic</b>	Enable or Disable Reauthentication for this port .

	Command or Action	Purpose
Step 11	<b>authentication timer reauthenticate</b>	Enter a value between 1 and 65535 (in seconds). Obtains re-authentication timeout value from the server. Default re-authentication time is 3600 seconds.
Step 12	<b>authentication violation protect</b>	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 13	<b>mka policy</b> <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 <b>mka policy</b> global configuration command).
Step 14	<b>dot1x pae authenticator</b>	Configure the port as an 802.1x port access entity (PAE) authenticator.
Step 15	<b>spanning-tree portfast</b>	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 16	<b>end</b> <b>Example:</b> <code>Switch(config)#end</code>	Returns to privileged EXEC mode.
Step 17	<b>show authentication session interface</b> <i>interface-id</i>	Verify the authorized session security status.
Step 18	<b>show authentication session interface</b> <i>interface-id</i> details	Verify the details of the security status of the authorized session.
Step 19	<b>show macsec interface</b> <i>interface-id</i>	Verify MacSec status on the interface.
Step 20	<b>show mka sessions</b>	Verify the established mka sessions.
Step 21	<b>copy running-config startup-config</b> <b>Example:</b> <code>Switch#copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## 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 gil/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 gil/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
```







```
*DEFAULT POLICY* 0      FALSE  TRUE  0    0    GCM-AES-128
p1                1      FALSE  TRUE  0    0    GCM-AES-128
p2                2      FALSE  TRUE  0    0    GCM-AES-128  Gi1/0/1
```

The following is a sample output from the **show mka policy *policy-name*** command:

```
Device# show mka policy p2
```

```
MKA Policy Summary...
```

Policy Name	KS Priority	Delay Protect	Replay Protect	Window Size	Conf Offset	Cipher Suite(s)	Interfaces Applied
p2	2	FALSE	TRUE	0	0	GCM-AES-128	Gi1/0/1

The following is a sample output from the **show mka policy *policy-name* detail** command:

```
Device# show mka policy p2 detail
```

```
MKA Policy Configuration ("p2")
```

```
=====
MKA Policy Name..... p2
Key Server Priority.... 2
Confidentiality Offset. 0
Send Secure Announcement..DISABLED
Cipher Suite(s)..... GCM-AES-128
```

```
Applied Interfaces...
  GigabitEthernet1/0/1
```

The following is a sample output from the **show mka statistics interface *interface-name*** command:

```
Device# show mka statistics interface GigabitEthernet 1/0/1
```

```
MKA Statistics for Session
```

```
=====
Reauthentication Attempts.. 0
```

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

```
SA Statistics
  SAKs Generated..... 1
  SAKs Rekeyed..... 0
  SAKs Received..... 0
  SAK Responses Received.. 1
```

```
MKPDU Statistics
  MKPDUs Validated & Rx... 89585
    "Distributed SAK".. 0
    "Distributed CAK".. 0
  MKPDUs Transmitted..... 89596
    "Distributed SAK".. 1
    "Distributed CAK".. 0
```

The following is a sample output from the **show mka summary** command:

```
Device# show mka summary
```

```
Total MKA Sessions..... 1
```



```

Invalid Peer MACsec Capability... 0
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

```

The following is a sample output from the **show macsec interface** command:

```
Device# show macsec interface HundredGigE 2/0/4
```

```

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
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
                   GCM-AES-256
                   GCM-AES-XPB-128
                   GCM-AES-XPB-256

Access control : must secure

Transmit Secure Channels
SCI : 3C5731BBB5850475
SC state : inUse(1)
Elapsed time : 7w0d
Start time : 7w0d
Current AN: 0
Previous AN: -
Next PN: 149757
SA State: inUse(1)
Confidentiality : yes
SAK Unchanged : yes
SA Create time : 00:04:41
SA Start time : 7w0d
SC Statistics
Auth-only Pkts : 0
Auth-only Bytes : 0
Encrypted Pkts : 0
Encrypted Bytes : 0
SA Statistics
Auth-only Pkts : 0
Auth-only Bytes : 0

```

```

Encrypted Pkts : 149756
Encrypted Bytes : 16595088

Port Statistics
Egress untag pkts 0
Egress long pkts 0

Receive Secure Channels
SCI : 3C5731BBB5C504DF
SC state : inUse(1)
Elapsed time : 7w0d
Start time : 7w0d
Current AN: 0
Previous AN: -
Next PN: 149786
RX SA Count: 0
SA State: inUse(1)
SAK Unchanged : yes
SA Create time : 00:04:39
SA Start time : 7w0d
SC Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 0
Late pkts 0
Uncheck pkts 0
Delay pkts 0
UnusedSA pkts 0
NousingSA pkts 0
Validated Bytes 0
Decrypted Bytes 0
SA Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 149784
Late pkts 0
Uncheck pkts 0
Delay pkts 0
UnusedSA pkts 0
NousingSA pkts 0
Validated Bytes 0
Decrypted Bytes 16654544

Port Statistics
Ingress untag pkts 0
Ingress notag pkts 631726
Ingress badtag pkts 0
Ingress unknownSCI pkts 0
Ingress noSCI pkts 0
Ingress overrun pkts 0

```

## Feature Information for MACsec Encryption

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

**Table 2: Feature Information for MACsec Encryption**

<b>Feature Name</b>	<b>Releases</b>	<b>Feature Information</b>
MACsec Encryption	Cisco IOS XE Everest 16.5.1a	MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Catalyst switches support 802.1AE encryption with MACsec Key Agreement (MKA) encryption between the switch and host device.

