Enable MACsec Using Cisco Catalyst SD-WAN Manager

Table 1: Feature History

Feature Name	Release Information	Feature Description
Enabling MACsec using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	With this feature, you can enable MACsec using Cisco Catalyst SD-WAN Manager for Cisco Catalyst SD-WAN devices on the service side. With MACsec enabled using Cisco Catalyst SD-WAN Manager, communication between devices in the service VPN is protected, thus enhancing security for the service VPN.

Information About Enabling MACsec Using Cisco SD-WAN Manager

MACsec is an IEEE 802.1AE standards-based Layer 2 hop-by-hop encryption that provides data confidentiality and integrity for media access independent protocols. MACsec helps improve security at branches and between the branches. When MACsec is enabled using Cisco SD-WAN Manager, communication between the devices in the service VPN is protected, thus enhancing security in the service VPN.

MACsec, 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. Only network access devices and endpoint devices such as a PC or IP phone is secured using MACsec. The 802.1AE encryption with MKA is supported on downlink ports for encryption between the routers or switches and host devices. MACsec encrypts all data except for the source and destination MAC addresses of an ethernet packet.

Supported Devices for MACsec in Cisco Catalyst SD-WAN

Table 2: Supported Devices for MACsec

Devices	Minimum Supported Releases
• Cisco Catalyst C8500-12X Router • Cisco Catalyst C8500-12X4QC Router • Cisco Catalyst C8500-20x6C Router • Cisco Catalyst C8500L-8S4X Router	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1
• Cisco 4461 Integrated Services Router (ISR4461) K9 built-in 1G and 10G ports with NIM-2GE-CU-SFP • C8300-2N2S-4T2X built-in 10G ports, and also with C-NIM-1X • C-NIM-4X and C-NIM-1X on C8300 Series • C-NIM-8T & C-NIM-8M & C-NIM-2T on C8300/C8200/C8200L Series	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1

Note The Integrated Services Router platform is compatible with all MACsec scenarios in Cisco Catalyst SD-WAN.

Benefits of Enabling MACsec in Cisco Catalyst SD-WAN

- Support for Point-to-Multipoint (P2MP) deployment models.
- Support for multiple P2P and P2MP deployments on the same physical interface.
- Support for 128- and 256-bit Advanced Encryption Standard–Galois Counter Mode (AES-GCM) encryption for data packets.
- Support for 128- and 256-bit Advanced Encryption Standard-Cipher-based Message Authentication Code (AEC-CMAC) encryption for control packets.
- Support for VLAN tag in the clear option to enable Carrier Ethernet Service Multiplexing.

- Support for coexisting of MACsec and Non-MACsec sub interfaces.
- Support for configurable Extensible Authentication Protocol over LAN (EAPoL) destination address.
- Support for configurable option to change the EAPoL Ethernet type.
- Support for configurable replay protection window size to accommodate packet reordering in the service provider network.

Prerequisites for Enabling MACsec in Cisco Catalyst SD-WAN

- MACsec requires MACsec license. For more information, see https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8500-series-edge-platforms/datasheet-c78-744089.html?oid=dstetr023042#Licensing
- Layer 2 transparent Ethernet Services must be present.
- The service provider network must provide a MACsec Layer 2 Control Protocol transparency such as, Extensible Authentication Protocol over LAN (EAPoL).

Restrictions for Enabling MACsec in Cisco Catalyst SD-WAN

- MACsec is supported up to the line rate on each interface. However, the forwarding capability may be limited by the maximum system forwarding capability.
- To configure port-channel, ensure that you configure MACsec at each interface of the link bundle.
- You cannot configure MACsec on the native sub interface. However, you can configure MACsec on the main interface using the **macsec dot1q-in-clear 1**.
- If the MKA session becomes inactive because of key unwrap failure, reconfigure the pre-shared key-based MKA session using MACsec configuration commands on the respective interfaces to bring the MKA session up.
- MACsec-configured on physical interface with Ethernet Virtual Circuits (EVC) is not supported. The EAPoL frames get dropped in such cases.
- When **macsec dot1q-in-clear** is enabled, the native VLAN is not supported.

Configure MACsec Enablement in Cisco SD-WAN Manager Using a CLI Template

Use the CLI templates to configure MACsec feature in Cisco Catalyst SD-WAN Manager. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

1. Enable MACsec feature from the global configuration mode in Cisco Catalyst SD-WAN Manager.

   ```
   key chain key_chain_name macsec
    key connectivity_association_key_name
     key-string connectivity_association_key
   ```

2. Configure MKA.

   The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys.

   ```
   mka policy policyname
   ```

3. Configure MACsec and MKA on an interface.

   ```
   interface GigabitEthernet interface
   macsec
   mka policy policyname
   mka pre-shared-key key-chain [keychainname|fallback-key]
   ```

Here's the complete configuration example for configuring and enabling MACsec in Cisco Catalyst SD-WAN Manager:

```
key chain mka-keychain128 macsec
 key 10
interface TenGigabitEthernet0/0/5
 vrf forwarding 20
 ip address 60.60.60.2 255.255.255.0
 ip mtu 1468
 speed 1000
 mka pre-shared-key key-chain mka-keychain128
 macsec
```

Verify MACsec Enablement in Cisco SD-WAN Manager

Verify MACsec Keychains

The following is a sample output from the **show mka keychains** command that displays the list of MACsec keychains configured on a Cisco IOS XE Catalyst SD-WAN device. It shows information that displays a list of keychain name, key number and the associated interface.

```
Device# show mka keychains

MKA PSK Keychain(s) Summary...

Keychain         Latest CKN                                                    Interface(s)
Name              Latest CAK                                                       Applied

=============================================================================================
mka-keychain128  10                                                             Te0/0/5

                 <HIDDEN>
```

Verify Default MACsec Policy

The following is a sample output from the **show mka default-policy detail** command that displays the default MACsec policy configured on a Cisco IOS XE Catalyst SD-WAN device. Use this command to retrieve detailed information about the default policy, including its name, cipher suite, key agreement protocol, and

other parameters. The additional keywords (detail, sessions, sessions detail) provide more specific information about the default policy or its active sessions.

```
Device# show mka default-policy detail
MKA Policy Configuration ("*DEFAULT POLICY*")
=========================
MKA Policy Name...........*DEFAULT POLICY*
Key Server Priority.......0
Confidentiality Offset....0
Delay Protect.............FALSE
SAK-Rekey On-Peer-Loss....0
SAK-Rekey Interval........0
Send Secure Announcement..DISABLED
Include ICV Indicator.....TRUE
SCI Based SSCI............FALSE
Use Updated Ethernet Hdr..NO
Cipher Suite(s)........ GCM-AES-128
                        GCM-AES-256

Applied Interfaces...
```

The following is a sample output from the **show mka default-policy sessions** command.

```
Device# show mka default-policy sessions
Summary of All Active MKA Sessions with MKA Policy "*DEFAULT POLICY*"...

=============================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

=============================================================================================
Te0/0/5         e8d3.22d3.2085/000d  *DEFAULT POLICY*  NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10
```

The following is a sample output from the **show mka default-policy sessions detail** command.

```
Device# show mka default-policy sessions detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI.............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 10
Member Identifier (MI)... DE832E171DCC70441E997F96
Message Number (MN)...... 80
EAP Role................. NA
Key Server............... NO
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
```

```
SAK Rekey Time.......... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                       MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                            Priority  Installed
  ----------------------------------------------------------------------------------------
  811368FD2F9F9CC82C1894C8  379101      a03d.6e5d.037f/0045  0         YES            0

Potential Peers List:
  MI                       MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                            Priority  Installed
  ----------------------------------------------------------------------------------------

Dormant Peers List:
  MI                       MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                            Priority  Installed
  ----------------------------------------------------------------------------------------


MKA Detailed Status for MKA Session
===================================
Status: INITIALIZING - Searching for Peer (Waiting to receive first Peer MKPDU)

Local Tx-SCI............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 11
Member Identifier (MI)... 6758F1CA5F050202DC742B03
Message Number (MN)...... 79
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... *DEFAULT POLICY*
```

```
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 0
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------
```

Verify MACsec Policies

The following is a sample output from the **show mka policy** command that displays the MACsec policies configured on a Cisco IOS XE Catalyst SD-WAN device. You can specify a specific policy name to view its details, or use the keywords detail or sessions to provide additional information about the policies or their active sessions.

```
Device# show mka policy MKA-128
MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
================================================================================
MKA-128           0    FALSE 0  FALSE TRUE   GCM-AES-128     Te0/0/5
```

Verify Active MACsec Sessions

The following is a sample output from the **show mka sessions** command that displays the active MACsec sessions on a Cisco IOS XE Catalyst SD-WAN device. You can use this command to display information about the sessions, including their interface, Policy-Name and Macsec Peers etc. The additional keywords such as **detail**, interface **TenGigabitEthernet** offer more specific details about the sessions or sessions associated with a particular interface.

```
Device# show mka sessions
Total MKA Sessions....... 1
      Secured Sessions... 1
```

```
      Pending Sessions... 0

=============================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server
Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN
=============================================================================================
Te0/0/5         e8d3.22d3.2085/000d  MKA-128           NO                 NO
13              a03d.6e5d.037f/0045  1                 Secured            10
```

The following is a sample output from the **show mka sessions detail** command.

```
Device# show mka sessions detail
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI.............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 10
Member Identifier (MI)... DE832E171DCC70441E997F96
Message Number (MN)...... 134
EAP Role................. NA
Key Server............... NO
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... MKA-128
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------
  811368FD2F9F9CC82C1894C8  379154      a03d.6e5d.037f/0045  0         YES            0
```

```
Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------


MKA Detailed Status for MKA Session
===================================
Status: INITIALIZING - Searching for Peer (Waiting to receive first Peer MKPDU)

Local Tx-SCI..... e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 11
Member Identifier (MI)... 6758F1CA5F050202DC742B03
Message Number (MN)...... 133
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... MKA-128
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 0
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------
```

```
Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------
```

View MACsec Statistics

The following is a sample output from the **show mka statistics** command that displays MACsec statistics on a Cisco IOS XE Catalyst SD-WAN device for eg CAK, SAK and MKPDU statistics. When used with the keyword interface **TenGigabitEthernet**, it provides statistics specifically for that interface.

```
Device# show mka statistics interface TenGigabitEthernet 0/0/5
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.............. 0
   SAKs Rekeyed................ 0
   SAKs Received............... 1
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics
   MKPDUs Validated & Rx... 229
      "Distributed SAK".. 1
      "Distributed CAK".. 0
   MKPDUs Transmitted...... 231
      "Distributed SAK".. 0
      "Distributed CAK".. 0
```

View Summary of MKA Sessions

The following is a sample output from the **show mka summary** command that displays a summary of MACsec-related information on a Cisco IOS XE Catalyst SD-WAN device. It includes details about the MACsec feature such as the global MKA configuration, default policy, and the number of active sessions.

```
Device# show mka summary
Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

=============================================================================================
Te0/0/5         e8d3.22d3.2085/000d  MKA-128           NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10


MKA Global Statistics
=====================
```

```
MKA Session Totals
   Secured..................... 18
   Fallback Secured............ 0
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 17
   Keepalive Timeouts......... 0

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

SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 0
   SAKs Received............... 18
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics
   MKPDUs Validated & Rx...... 374465
      "Distributed SAK"..... 18
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 384191
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures................ 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 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... 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 ICV Verification............. 0
   MKPDU Rx Fallback ICV Verification..... 0
   MKPDU Rx Validation................... 0
```

```
   MKPDU Rx Bad Peer MN.................. 0
   MKPDU Rx Non-recent Peerlist MN........ 0
SAK USE Failures
   SAK USE Latest KN Mismatch............. 0
   SAK USE Latest AN not in USE........... 0
```

View Hardware-related Information about MACsec

The following is a sample output from the **show macsec hw detail** command that displays detailed hardware-related information about MACsec on a Cisco IOS XE Catalyst SD-WAN device. It provides information about the hardware capabilities and configurations related to MACsec.

```
Device# show macsec hw detail
MACsec Capable Interface         RxSA Inuse
-----------------------------------------------
 TenGigabitEthernet0/0/5       :        1


Other Debug Statistics
Interface TenGigabitEthernet0/0/5 HMAC:
RxOctets              0  RxUcastPkts           0  RxMcastPkts           0
RxBcastPkts           0  RxDiscards            0  RxErrors              0
TxOctets              0  TxUcastPkts           0  TxMcastPkts           0
TxBcastPkts           0  TxErrors              0
LMAC:
RxOctets           5595  RxUcastPkts          22  RxMcastPkts           9
RxBcastPkts           0  RxDiscards            0  RxErrors              0
TxOctets           1710  TxUcastPkts          15  TxMcastPkts           0
TxBcastPkts           0  TxErrors              0
```

View MACsec Summary

The following is a sample output from the **show macsec summary** command that displays a summary of MACsec information on the device, including MACsec capable interfaces, installed Secure Channels (SC), and MACsec enabled interfaces with their associated receive SC and VLAN.

```
Device# show macsec summary
MACsec Capable Interface                Extension              Installed Rx SC
-------------------------------------------------------------------------------
 TenGigabitEthernet0/0/0                 One tag-in-clear
 TenGigabitEthernet0/0/1                 One tag-in-clear
 TenGigabitEthernet0/0/2                 One tag-in-clear
 TenGigabitEthernet0/0/3                 One tag-in-clear
 TenGigabitEthernet0/0/4                 One tag-in-clear
 TenGigabitEthernet0/0/5                 One tag-in-clear                1
 TenGigabitEthernet0/0/6                 One tag-in-clear
 TenGigabitEthernet0/0/7                 One tag-in-clear
 TenGigabitEthernet0/1/0                 One tag-in-clear
 TenGigabitEthernet0/1/1                 One tag-in-clear
 TenGigabitEthernet0/1/2                 One tag-in-clear
 TenGigabitEthernet0/1/3                 One tag-in-clear
 FortyGigabitEthernet0/2/0               One tag-in-clear
 FortyGigabitEthernet0/2/4               One tag-in-clear
 FortyGigabitEthernet0/2/8               One tag-in-clear
 GigabitEthernet0                        One tag-in-clear
 SDWAN System Intf IDB                   One tag-in-clear
 SDWAN vmanage_system IDB                One tag-in-clear
 LIIN0                                   One tag-in-clear
 LI-Null0                                One tag-in-clear
 Loopback65528                           One tag-in-clear
 Loopback65529                           One tag-in-clear
 SR0                                     One tag-in-clear
 Tunnel1                                 One tag-in-clear
```

```
 VoIP-Null0                              One tag-in-clear

 MACsec Enabled Interface         Receive SC   VLAN
-----------------------------------------------------
 TenGigabitEthernet0/0/5       :        1         0
```

The following is a sample output from the **show macsec mka-request-notify** command that displays information about MACsec (Media Access Control Security) enabled interfaces, including the counts of Control Plane (CR) transmit and delete Secure Channels (SC), transmit Security Associations (SA), receive SC, and delete SAs, as well as the MKA (MACsec Key Agreement) notification count on the interface "TenGigabitEthernet0/0/5.

```
Device# show macsec mka-request-notify
MACsec Enabled Interface         CR_TX_SC  DEL_TX_SC  INST_TX_SA  CR_RX_SC  DEL_RX_SC
INST_RX_SA  DEL_RX_SA  MKA_NOTIFY
-------------------------------------------------------------------------------------------------
 TenGigabitEthernet0/0/5       :       18        17        18        18         0
18           11         0
```

The following is a sample output from the **show macsec post** command.

```
Device# show macsec post
 MACsec Capable Interface                          POST Result
-------------------------------------------------------------
 TenGigabitEthernet0/0/0                             NONE
 TenGigabitEthernet0/0/1                             NONE
 TenGigabitEthernet0/0/2                             NONE
 TenGigabitEthernet0/0/3                             NONE
 TenGigabitEthernet0/0/4                             NONE
 TenGigabitEthernet0/0/5                             NONE
 TenGigabitEthernet0/0/6                             NONE
 TenGigabitEthernet0/0/7                             NONE
 TenGigabitEthernet0/1/0                             NONE
 TenGigabitEthernet0/1/1                             NONE
 TenGigabitEthernet0/1/2                             NONE
 TenGigabitEthernet0/1/3                             NONE
 FortyGigabitEthernet0/2/0                           NONE
 FortyGigabitEthernet0/2/4                           NONE
 FortyGigabitEthernet0/2/8                           NONE
```

Verify MACsec Configuration and Status

The following is a sample output from the **show macsec status interface** command that displays the MACsec configuration and status for interface TenGigabitEthernet 0/0/5. It shows the supported ciphers, selected cipher, replay window size, transmit and receive Secure Channel Identifiers (SCIs), and the next expected packet numbers for transmission and reception

```
Device# show macsec status interface TenGigabitEthernet 0/0/5
Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256 GCM-AES-XPN-128 GCM-AES-XPN-256
  Cipher:                   GCM-AES-128
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure
  Include-SCI:              TRUE

 Transmit SC:
  SCI:                      E8D322D32085000D
  Transmitting:             TRUE
 Transmit SA:
  Next PN:                  10002
  Delay Protect AN/nextPN:  NA/0
```

```
 Receive SC:
  SCI:                      A03D6E5D037F0045
  Receiving:                TRUE
 Receive SA:
  Next PN:                  10077
  AN:                       1
  Delay Protect AN/LPN:     0/0
```

Configuration Example for MACsec Enablement in Cisco SD-WAN Manager

The following example displays the configuration for MACsec configured on Cisco Catalyst C8500 platforms.

```
key chain mka-keychain128 macsec
 key 10
interface TenGigabitEthernet0/0/5
 vrf forwarding 20
 ip address 60.60.60.2 255.255.255.0
 ip mtu 1468
 speed 1000
 mka pre-shared-key key-chain mka-keychain128
 macsec
```