Configure and Troubleshoot MKA Using Secure Client 5

Contents

Introduction

This document describes the way in which you can configure MACsec encryption in an endpoint using Secure Client 5 as supplicant.

Prerequisites

Cisco recommends knowledge in these topics:

- Identity Services Engine
- 802.1x and Radius
- MACsec MKA encryption
- Secure Client version 5 (Formerly known as Anyconnect)

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) version 3.3

- Catalyst 9300 version 17.06.05
- Cisco Secure Client 5.0.4032

Background information

MACSec (Media Access Control Security) is a network security standard that provides encryption and protection for Ethernet frames at layer 2 of the OSI model (Data Link), defined by the IEEE as a standard denominated 802.1AE.

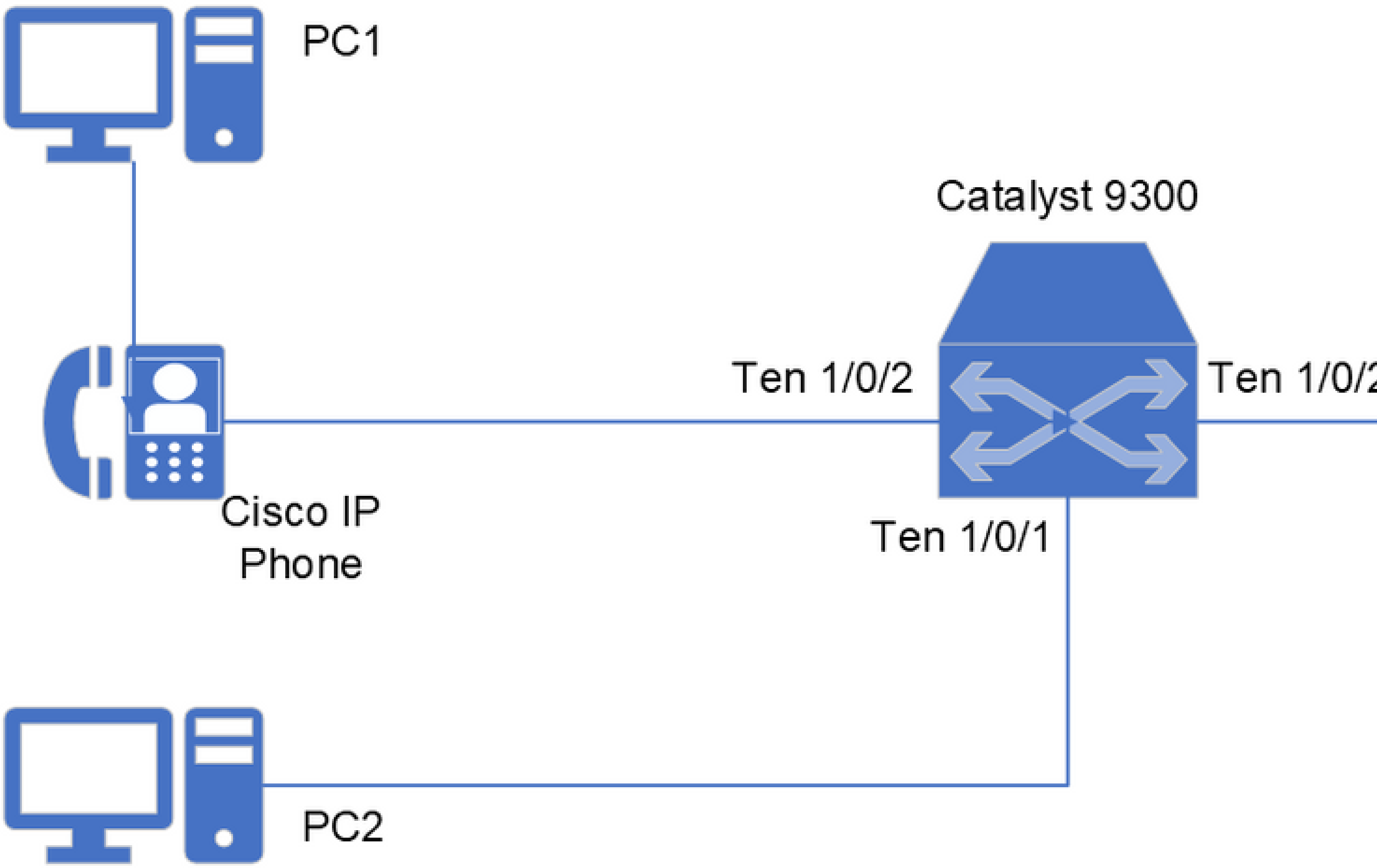
MACSec supplies this encryption in a point-to-point connection that can be switch-to-switch or switch-to-host connections, hence the coverage of this standard is limited to wired connections.

This standard encrypts the entire data except for the Source and Destination MAC address of frames that are transmitted in a layer 2 connection.

The MACsec Key Agreement (MKA) protocol is the mechanism from where MACsec peers are going to negotiate the security keys that are needed to secure the link.

Configure

Network Diagram



Note: This documentation considers that you have already a set-up of rules configured and working for Radius Authentication for the PCs devices and the Cisco IP phone. To setup a configuration from scratch, please refer to ISE Secure Wired Access Prescriptive Deployment Guide to review the configuration in Identity Services Engine and Switch for Identity-Based Network Access.

Setup of policies on ISE

The first task is to configure the corresponding authorization profiles that are applied for both PCs displayed in the preceding diagram (as well as the Cisco IP Phone).

In this hypothetical scenario, the PCs are going to use 802.1X protocol as the authentication method and the Cisco IP Phone uses Mac Address Bypass (MAB).

ISE communicates with the switch through Radius protocol about the attributes that the switch needs to enforce in the interface from where the endpoint is connected through a Radius session.

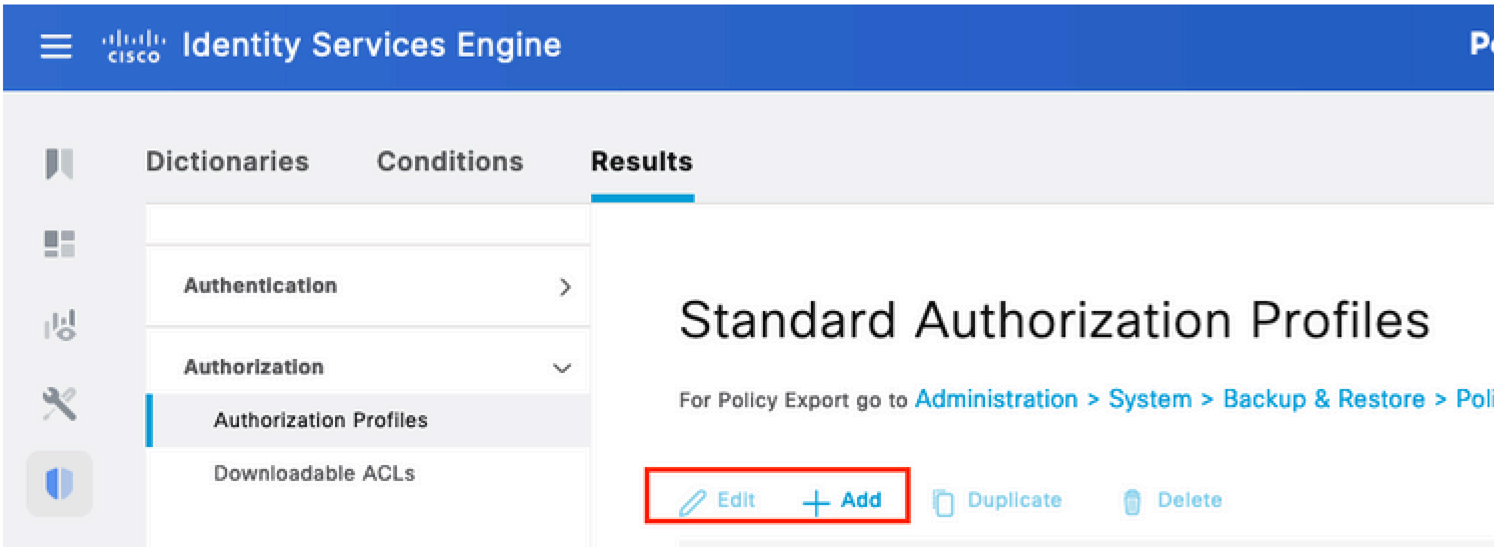
For MACsec encryption in hosts, the attribute required is cisco-av-pair = linksec-policy, which has these 3 possible values:

- **Should-not-Secure:** The switch does not perform MKA encryption in the interface where the Radius session is happening.
- **Must-Secure:** The switch needs to enforce encryption in the traffic linked with the Radius session, if the MKA session fails or has a timeout the connection is considered as authorization failure, there is a retrial of MKA session establishment.
- **Should-Secure:** The switch attempts to perform MKA encryption, if the MKA session linked to the Radius session is successful the traffic is encrypted, if the MKA fails or times out, the switch allows that unencrypted traffic linked to that Radius session.

Step 1. As considered in the previous information, in both PCs you can enforce a **should-secure** MKA policy to have flexibility in case a machine with no MKA capabilities connects to the interface Ten 1/0/1.

As an option you can configure a policy for PC2 that enforces a must-secure policy.

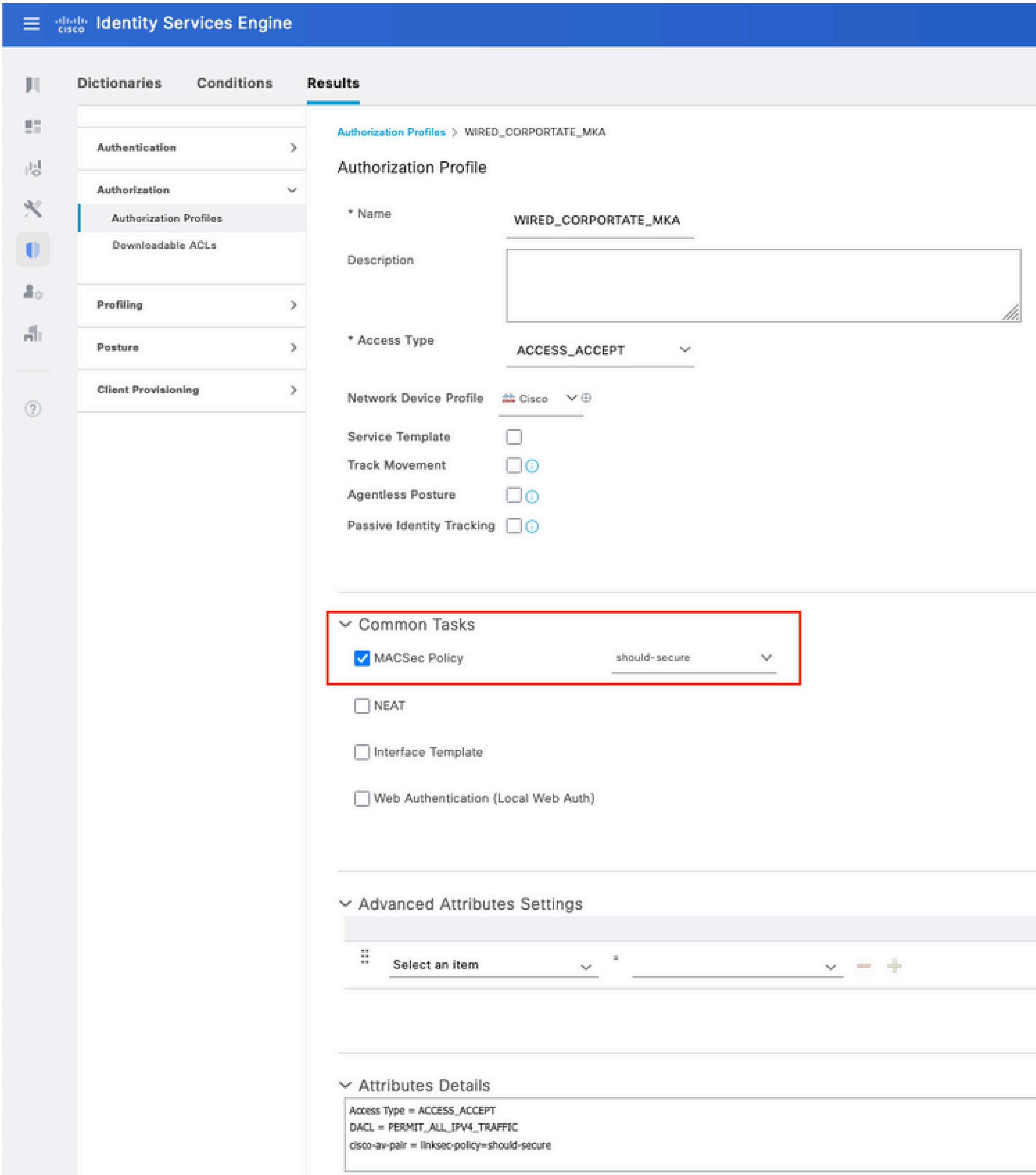
In this example configure the policy for the PCs as in **Policy** > **Policy Elements** > **Results** > **Authorization Profiles** then **+Add** or **Edit** an existing profile



Step 2. Complete or customize the fields required for the profile.

Ensure that in Common Tasks you have selected **MACSec Policy** and the corresponding policy to apply.

Scroll down and **Save** the configuration.



Authorization Profile

* Name: WIRED_CORPORTATE_MKA

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

☑ MACSec Policy: should-secure

□ NEAT

□ Interface Template

□ Web Authentication (Local Web Auth)

Advanced Attributes Settings

Select an item =

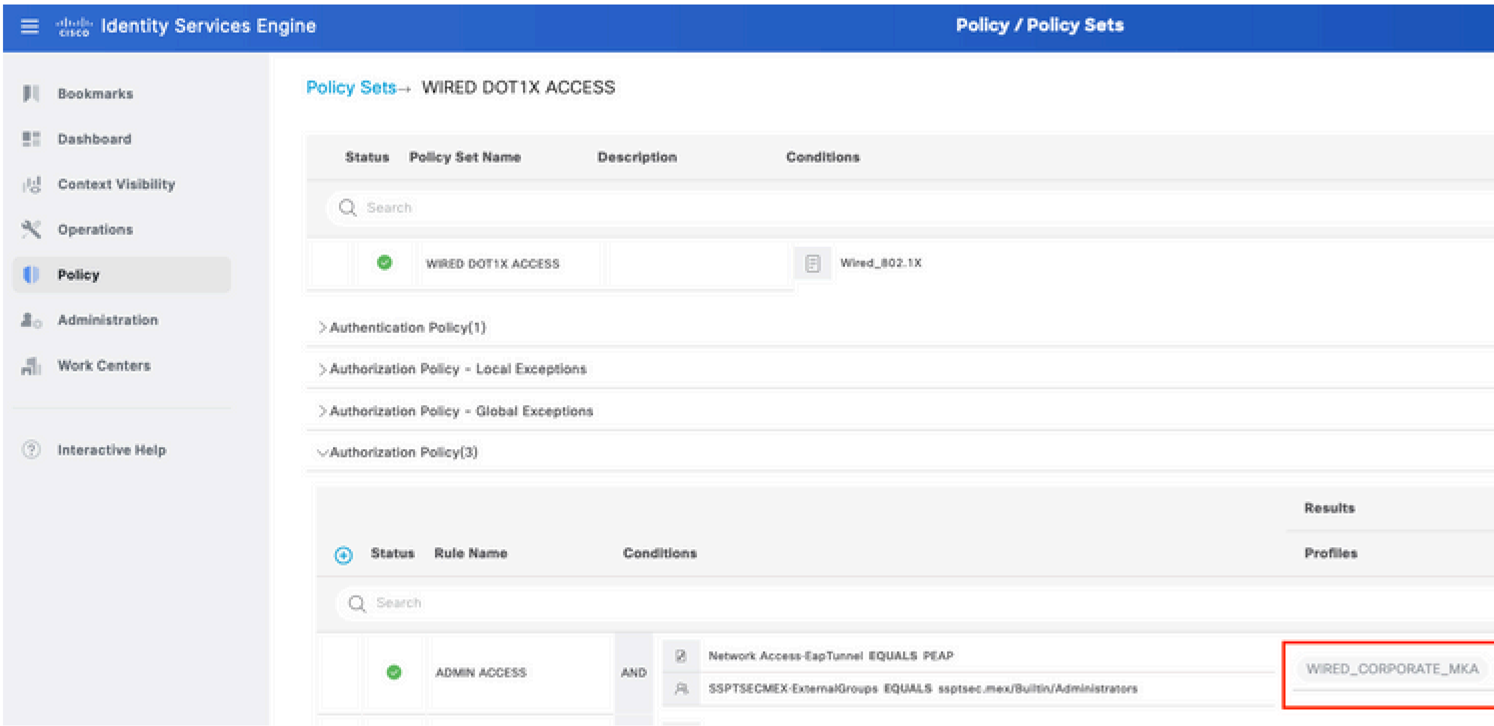
Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_IPV4_TRAFFIC
cisco-av-pair = linksec-policy=should-secure
```

Step 3. Assign the corresponding authorization profile to the authorization rules that are hit by the devices.

This action needs to be done in **Policy > Policy Sets > (Select Policy Set assigned) > Authorization Policy.**

Associate the authorization rule with the authorization profile with MACsec Settings. Scroll down **Save** your configuration**.**



Policy Sets→ WIRED DOT1X ACCESS

Status	Policy Set Name	Description	Conditions
✓	WIRED DOT1X ACCESS		Wired_802.1X

> Authentication Policy(1)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
∨ Authorization Policy(3)

Status	Rule Name	Conditions		Results Profiles
✓	ADMIN ACCESS	AND	Network Access-EapTunnel EQUALS PEAP SSPTSECMEX-ExternalGroups EQUALS ssptsec.mex/Builtin/Administrators	WIRED_CORPORATE_MKA

Setup of MKA in Catalyst 9300

Step 1. Configure a new MKA policy as this example suggests:

```
!
  mka policy MKA_PC
  key-server priority 0
  no delay-protection
  macsec-cipher-suite gcm-aes-128
  confidentiality-offset 0
  sak-rekey on-live-peer-loss
  sak-rekey interval 0
  no send-secure-announcements
  no include-icv-indicator
  no use-updated-eth-header
  no ssci-based-on-sci
!
```

Step 2. Enable MACsec encryption in the interface where the PCs are connected.

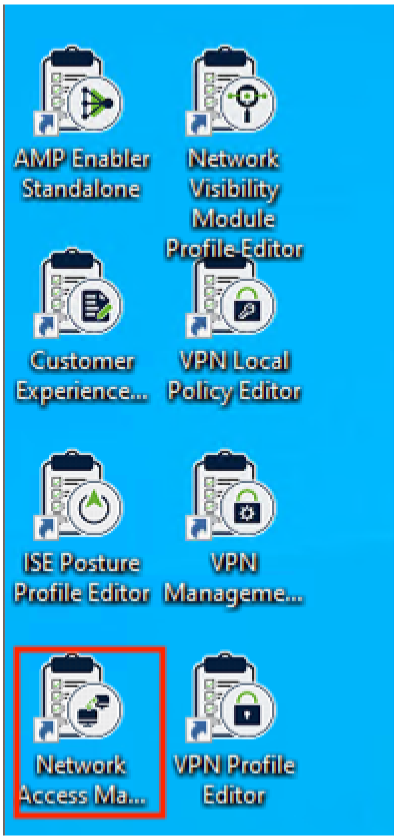
```
!
interface TenGigabitEthernet1/0/1
 macsec
 mka policy MKA_PC
!
```

> **Note**: For further information related to the commands and options in MKA configuration, please review the Security configuration guide corresponding the version of switch you use. In this scenario for this example, Security Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches)

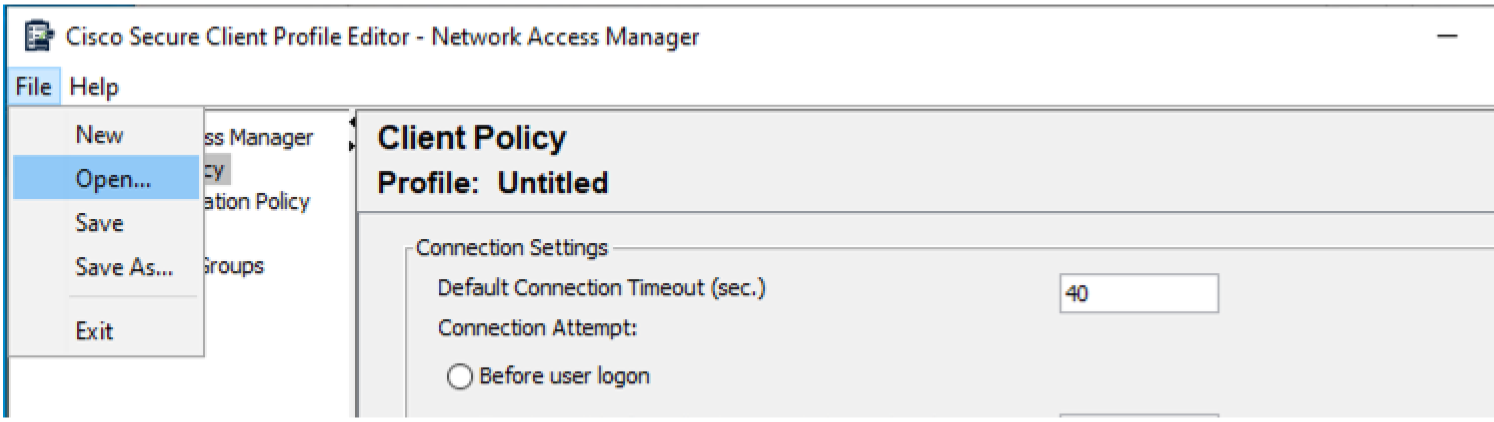
Setup of MKA using Network Access Manager Profile Editor.

Step 1. Download and open the Profile Editor from the Ciscoâ€™s download website that matches the version of Secure Client that you are using.

Once you have installed this program in your computer, proceed to open the **Cisco Secure Client Profile Editor â€“ Network Access Manager.**



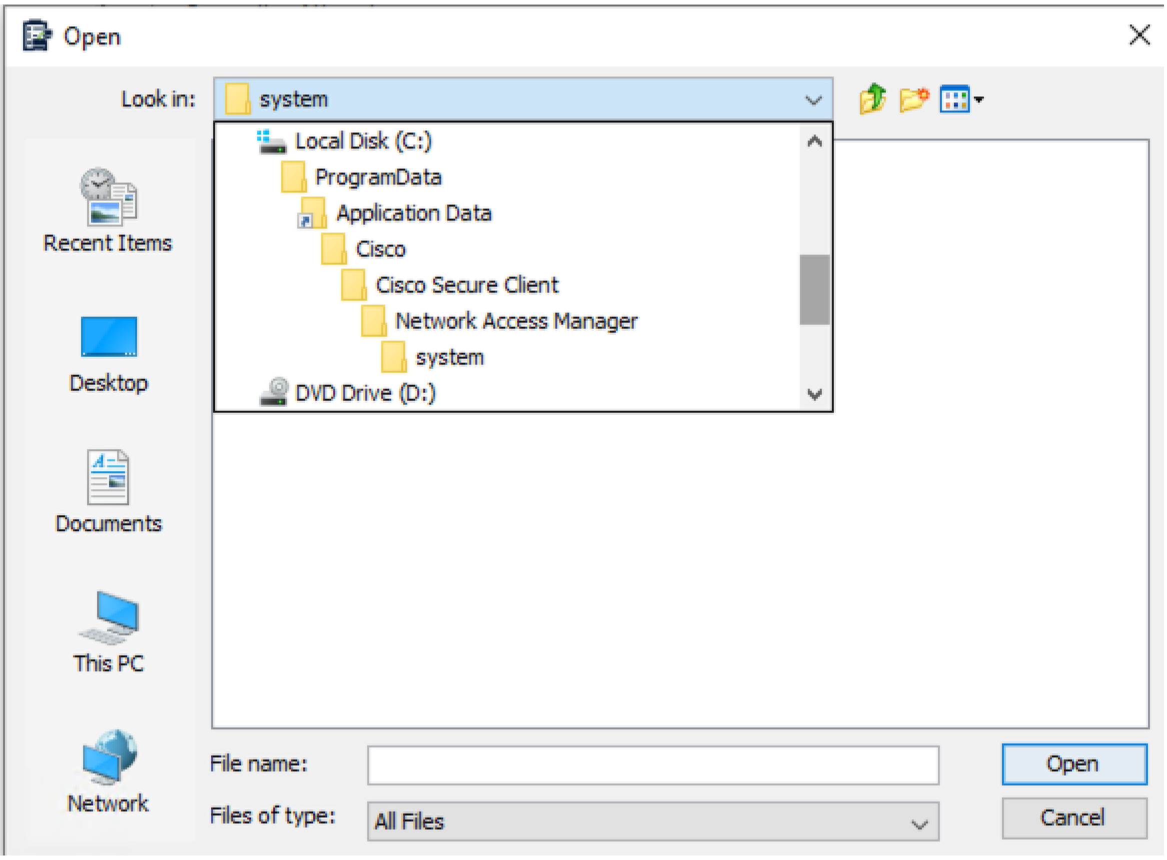
Step 2. Select the option **File** > **Open**.



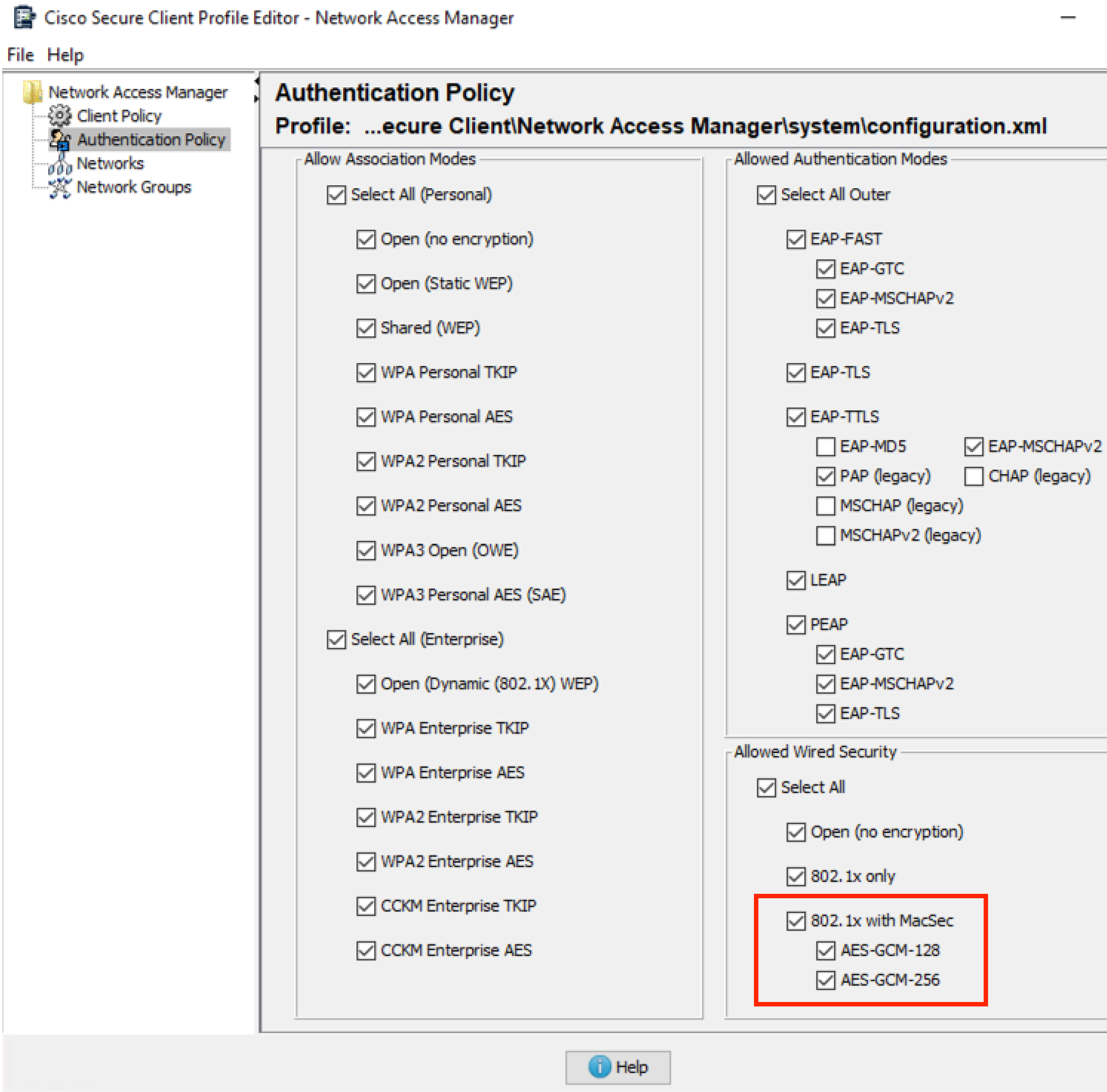
Client Policy
Profile: Untitled

Connection Settings
Default Connection Timeout (sec.) 40
Connection Attempt:
○ Before user logon

Step 3. Select the folder system that is being displayed in this image. Within this folder open the file named configuration.xml.



Step 4. Once the file has been loaded by the Profile Editor, select the option **Authentication Policy**, and ensure that the option related to 802.1x with MACSec is enabled.



Cisco Secure Client Profile Editor - Network Access Manager

Authentication Policy

Profile: ...ecure Client\Network Access Manager\system\configuration.xml

Allow Association Modes

- ☑ Select All (Personal)
  - ☑ Open (no encryption)
  - ☑ Open (Static WEP)
  - ☑ Shared (WEP)
  - ☑ WPA Personal TKIP
  - ☑ WPA Personal AES
  - ☑ WPA2 Personal TKIP
  - ☑ WPA2 Personal AES
  - ☑ WPA3 Open (OWE)
  - ☑ WPA3 Personal AES (SAE)
- ☑ Select All (Enterprise)
  - ☑ Open (Dynamic (802.1X) WEP)
  - ☑ WPA Enterprise TKIP
  - ☑ WPA Enterprise AES
  - ☑ WPA2 Enterprise TKIP
  - ☑ WPA2 Enterprise AES
  - ☑ CCKM Enterprise TKIP
  - ☑ CCKM Enterprise AES

Allowed Authentication Modes

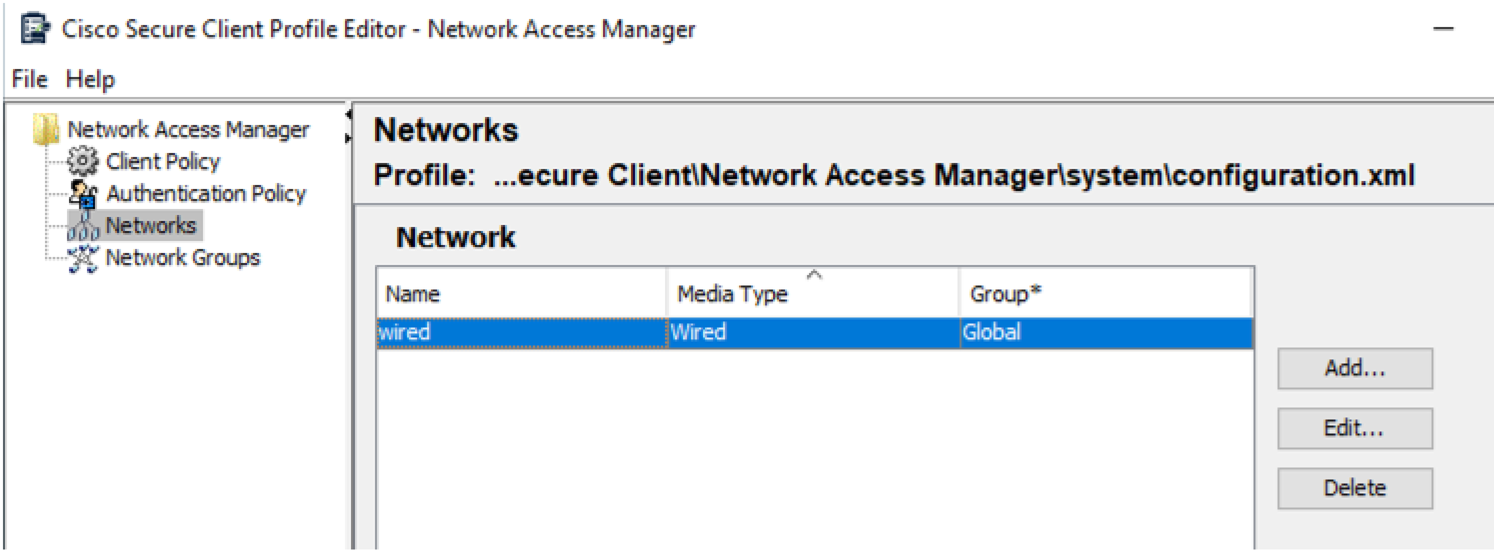
- ☑ Select All Outer
  - ☑ EAP-FAST
    - ☑ EAP-GTC
    - ☑ EAP-MSCHAPv2
    - ☑ EAP-TLS
  - ☑ EAP-TLS
  - ☑ EAP-TTLS
    - □ EAP-MD5
    - ☑ EAP-MSCHAPv2
    - ☑ PAP (legacy)
    - □ CHAP (legacy)
    - □ MSCHAP (legacy)
    - □ MSCHAPv2 (legacy)
  - ☑ LEAP
  - ☑ PEAP
    - ☑ EAP-GTC
    - ☑ EAP-MSCHAPv2
    - ☑ EAP-TLS

Allowed Wired Security

- ☑ Select All
  - ☑ Open (no encryption)
  - ☑ 802.1x only
  - ☑ 802.1x with MacSec
    - ☑ AES-GCM-128
    - ☑ AES-GCM-256

Step 5. Proceed to the section **Networks**, in this part you can **Add** a new profile for a wired connection or **Edit** the default wired profile that is installed with Secure Client 5.0 .

In this scenario, we are going to Edit the existing wired profile.



Networks

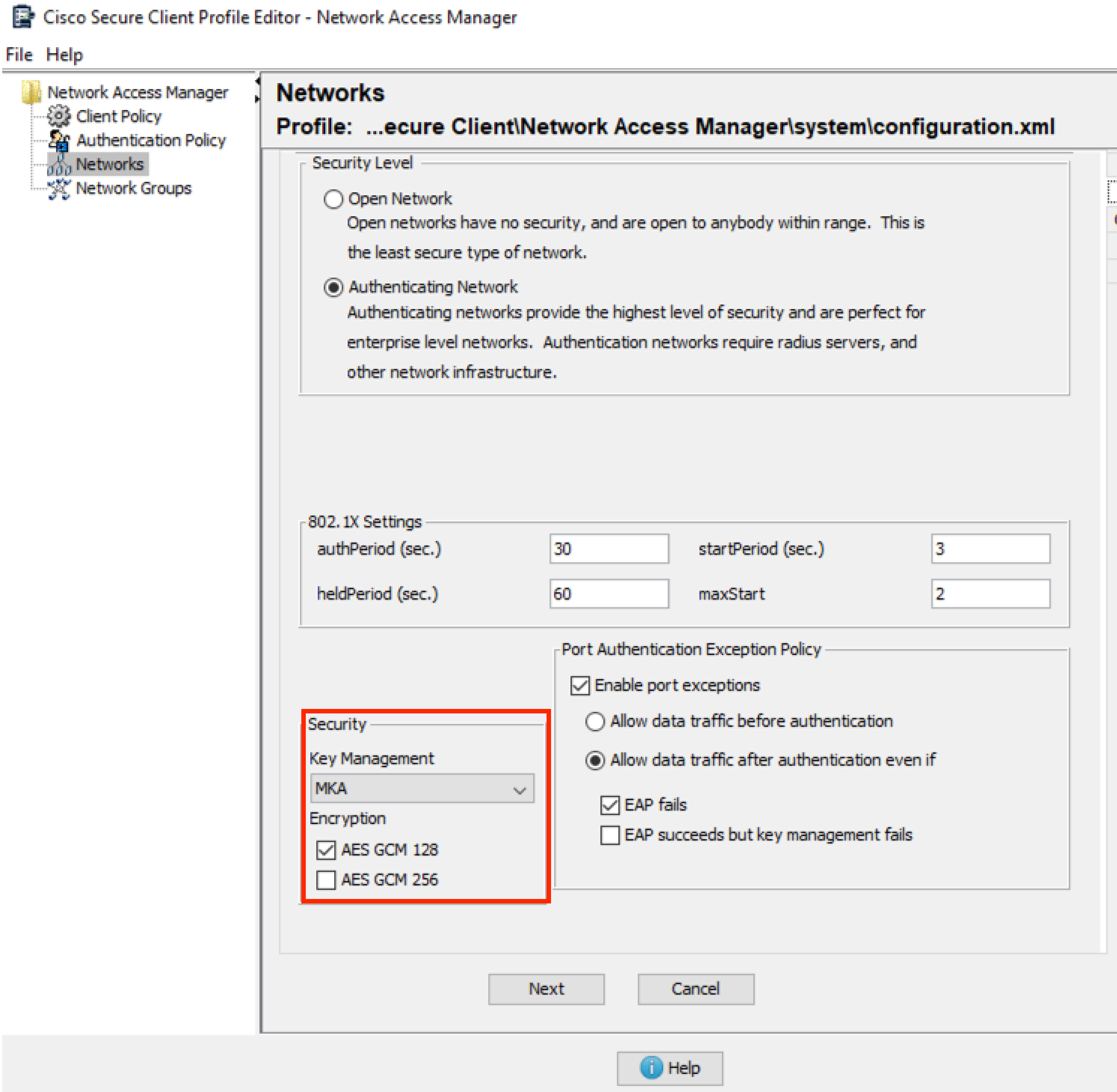
Profile: ...ecure Client\Network Access Manager\system\configuration.xml

Network

Name	Media Type	Group*
wired	Wired	Global

Step 6. Configure the profile. In the section **Security Level**, adjust the **Key Management** to use MKA followed by an encryption AES GCM 128.

Adjust the other parameters for the authentication dot1x and policies as well.



Cisco Secure Client Profile Editor - Network Access Manager

File Help

- Network Access Manager
  - Client Policy
  - Authentication Policy
  - Networks
  - Network Groups

Networks

Profile: ...ecure Client\Network Access Manager\system\configuration.xml

Security Level

○ Open Network

Open networks have no security, and are open to anybody within range. This is the least secure type of network.

● Authenticating Network

Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

Security

Key Management: MKA

Encryption

☑ AES GCM 128

☐ AES GCM 256

Port Authentication Exception Policy

☑ Enable port exceptions

○ Allow data traffic before authentication

● Allow data traffic after authentication even if

☑ EAP fails

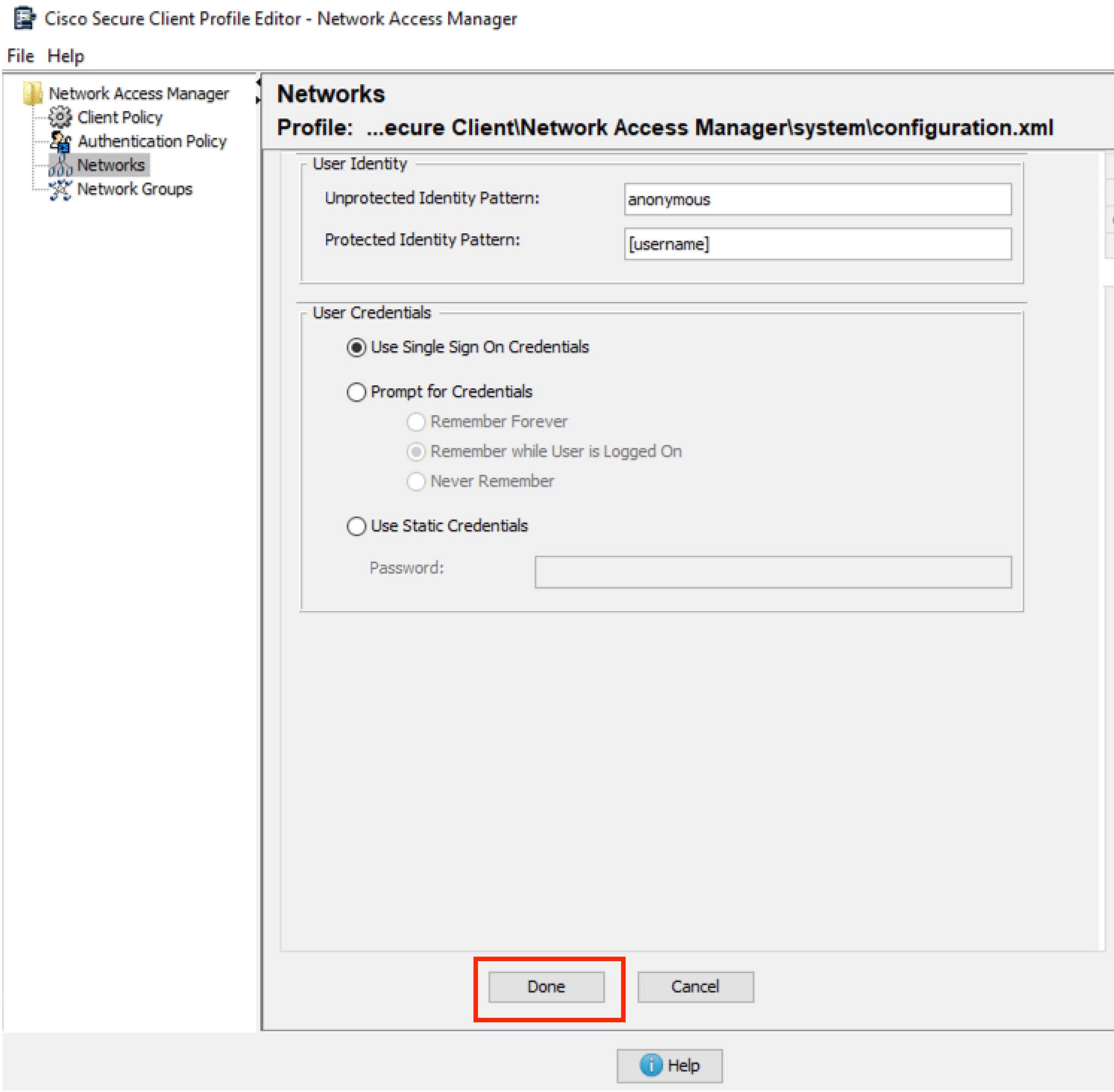
☐ EAP succeeds but key management fails

Step 7. Configure the remaining sections concerning **Connection Type**, **User Auth** and **Credentials.**

Those sections vary depending upon the authentication settings that you select in the **Security Level** section.

When you finish with the configurations select the option **Done.**

For this scenario we are using **Protected Extensible Authentication Protocol (PEAP)** with user credentials.


Cisco Secure Client Profile Editor - Network Access Manager

File Help

Networks

Profile: ...ecure Client\Network Access Manager\system\configuration.xml

User Identity

Unprotected Identity Pattern: anonymous

Protected Identity Pattern: [username]

User Credentials

● Use Single Sign On Credentials

○ Prompt for Credentials

○ Remember Forever

● Remember while User is Logged On

○ Never Remember

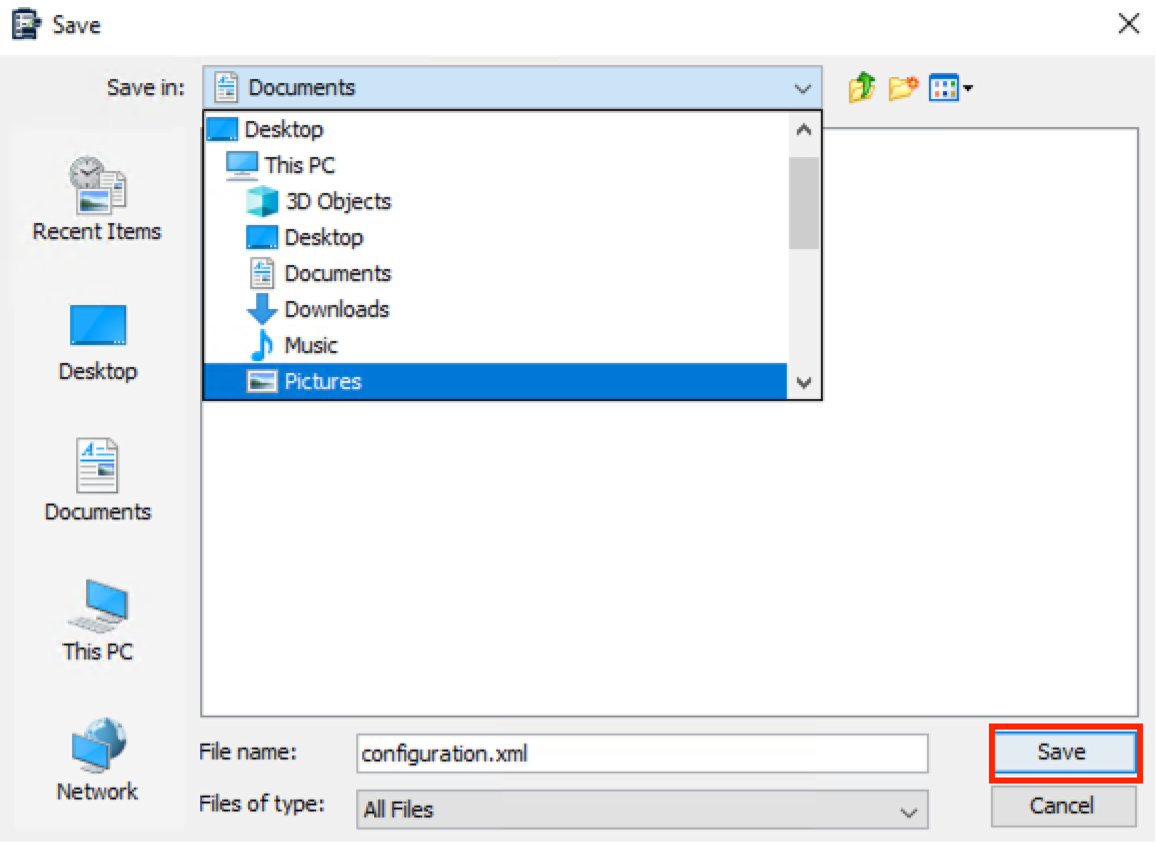
○ Use Static Credentials

Password:

Step 8. Navigate to the menu **File.** Proceed with **Save as** option.

Name the file as configuration.xml and save in a different folder from ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system.

In this example the file was saved in the Documents folder. **Save** the profile.


Save

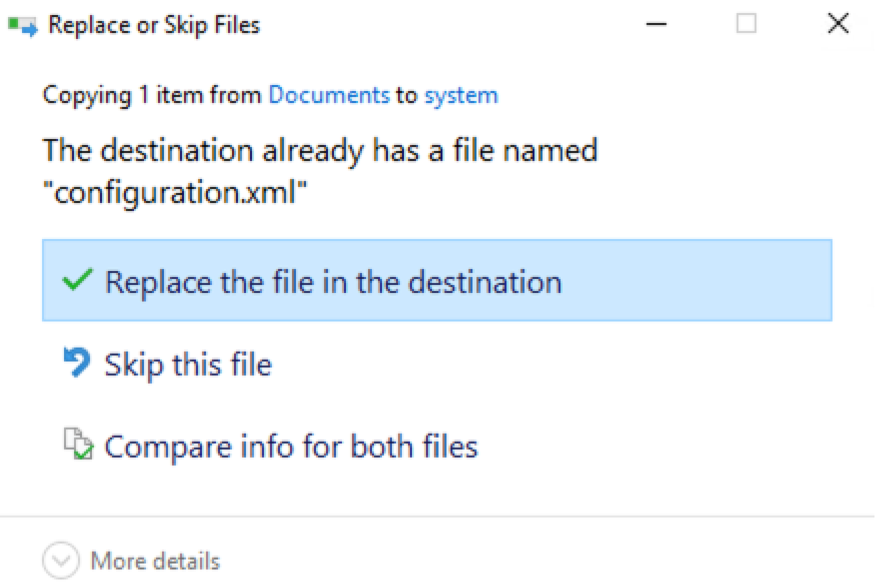
Save in: Documents

File name: configuration.xml

Files of type: All Files

Step 8. Proceed to the profile location, copy the file, and replace the file that is contained in the folder ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system.

Select the **Replace the file in destination** option.


Replace or Skip Files

Copying 1 item from Documents to system

The destination already has a file named "configuration.xml"

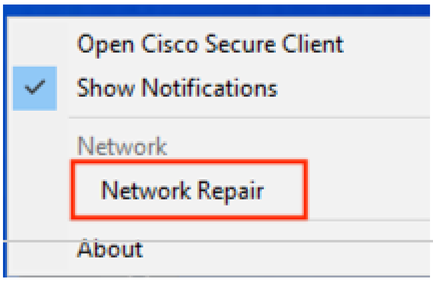
✓ Replace the file in the destination

Skip this file

Compare info for both files

Step 9. To load the profile modified in the Security Client 5.0, select with a right click the **Secure Client** icon located in the right lower taskbar of your Windows machine.

Perform a **Network Repair**.

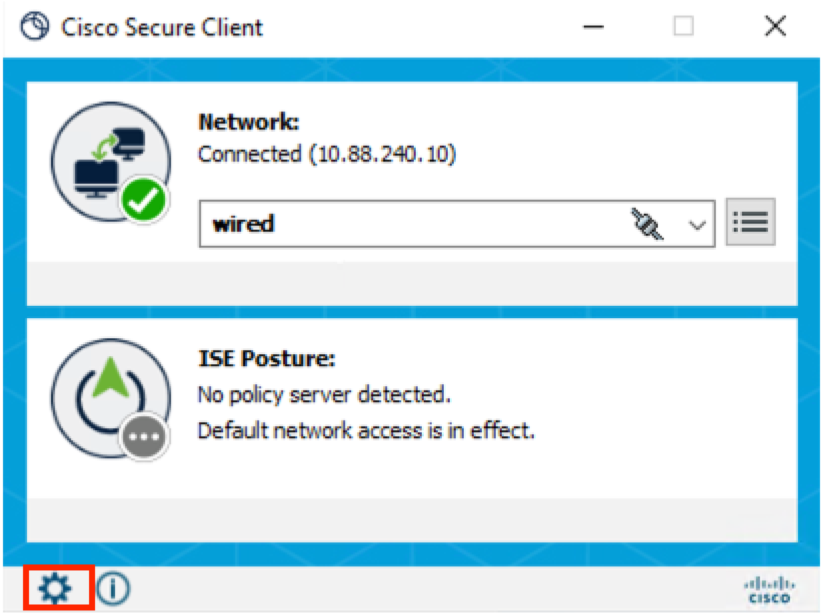


Note: All the networks configured through the profile editor have privileges of Administrator Network, hence the users are not able to customize/change the content that you configured using this tool.

Setup of MKA networks using Network Access Manager (optional).

Step 1. As an alternative to the MKA setup using the Profile Editor, you can add networks without the use of this tool.

From the Secure Client suite select the gear icon.



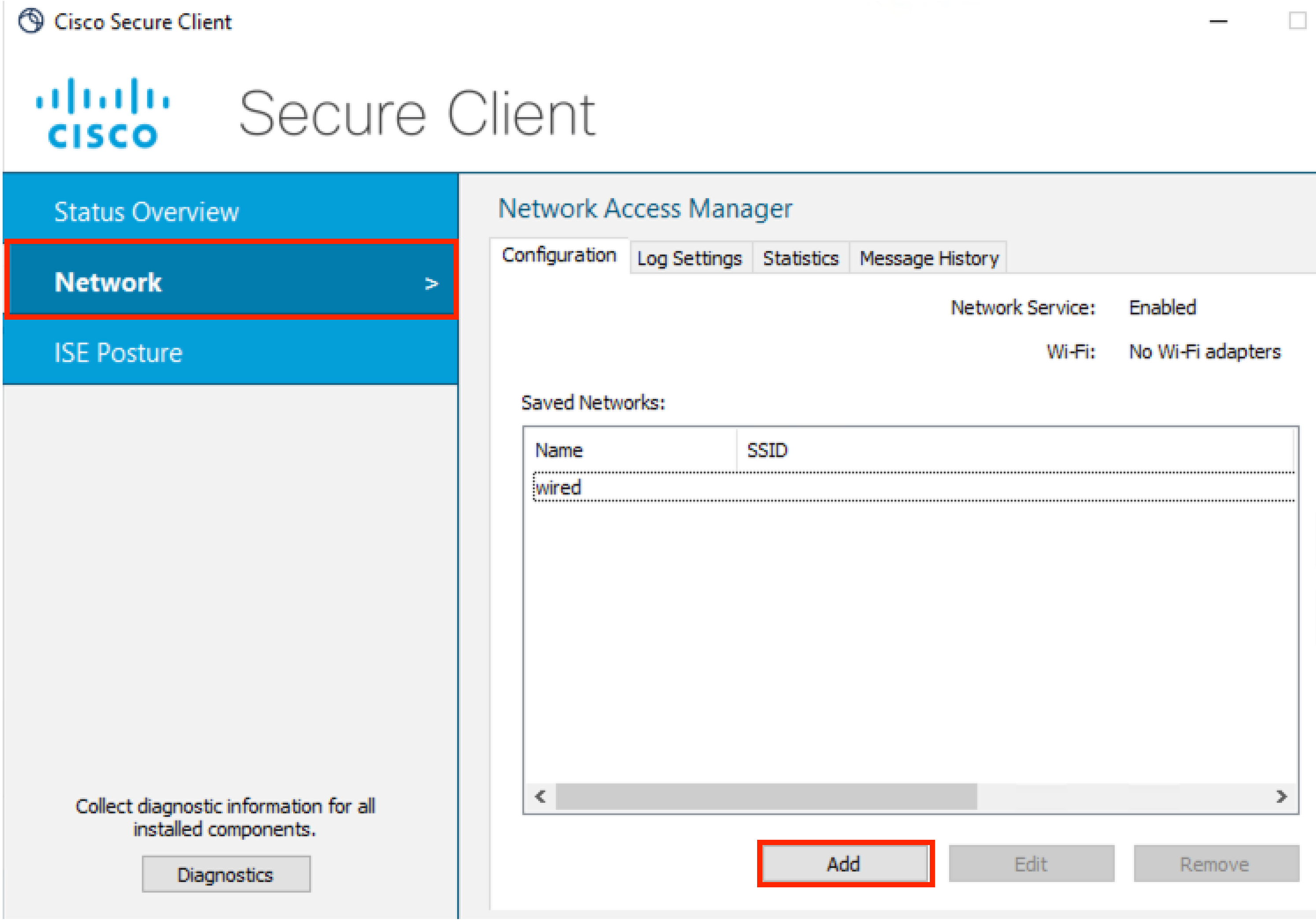
Network:
Connected (10.88.240.10)

wired

ISE Posture:
No policy server detected.
Default network access is in effect.

Step 2. In the new window displayed, select the option **Network.**

In the Configuration section select the option **Add** to ingress a network MKA capable with privileges User Network.



Network Service: Enabled

Wi-Fi: No Wi-Fi adapters

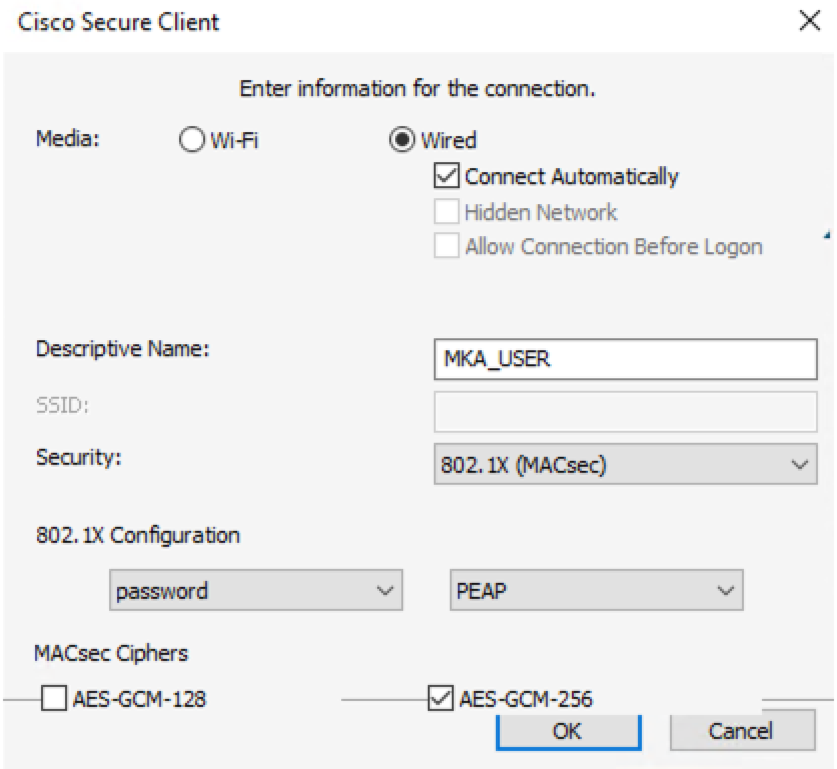
Saved Networks:

Name	SSID
wired	

Collect diagnostic information for all installed components.
Diagnostics
Add
Edit
Remove

Step 3. In the new configuration window, set up the characteristics of your connection and name the network.

When finished select the **OK** button.



Cisco Secure Client

Enter information for the connection.

Media: ○ Wi-Fi ● Wired

☑ Connect Automatically

□ Hidden Network

□ Allow Connection Before Logon

Descriptive Name: MKA_USER

SSID:

Security: 802.1X (MACsec)

802.1X Configuration

password PEAP

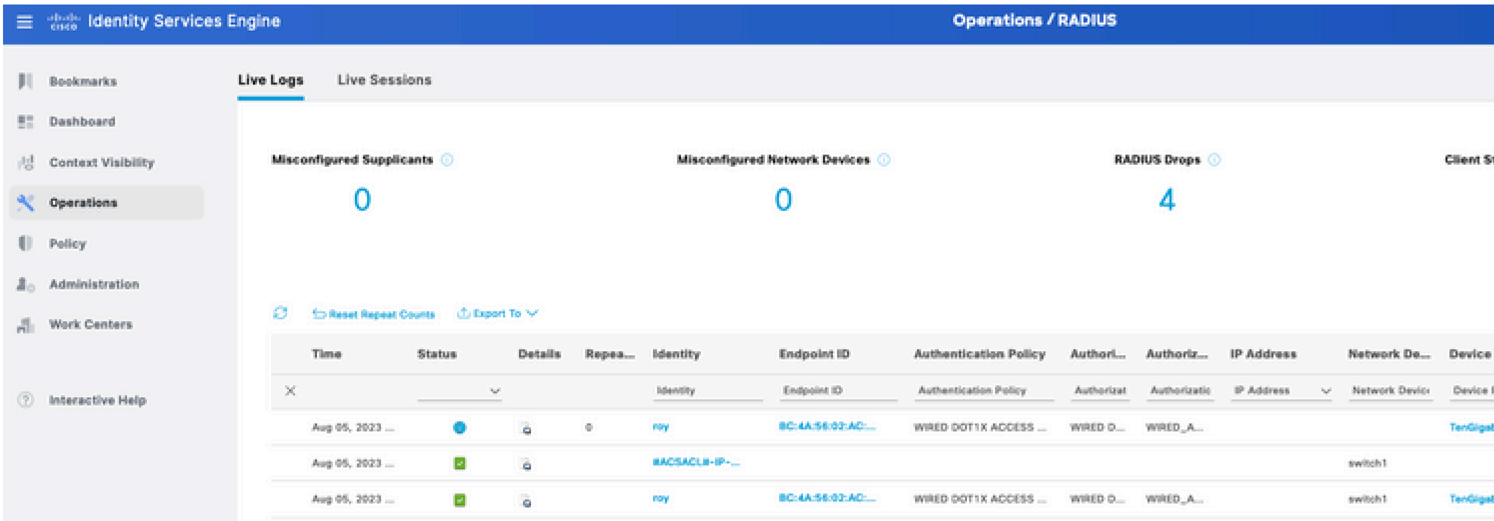
MACsec Ciphers

□ AES-GCM-128 ☑ AES-GCM-256

Verify

Validation on ISE

In ISE, upon the completion of the configuration of this flow, you see the device being authenticated and authorized in Livelogs.



Misconfigured Supplicants 0

Misconfigured Network Devices 0

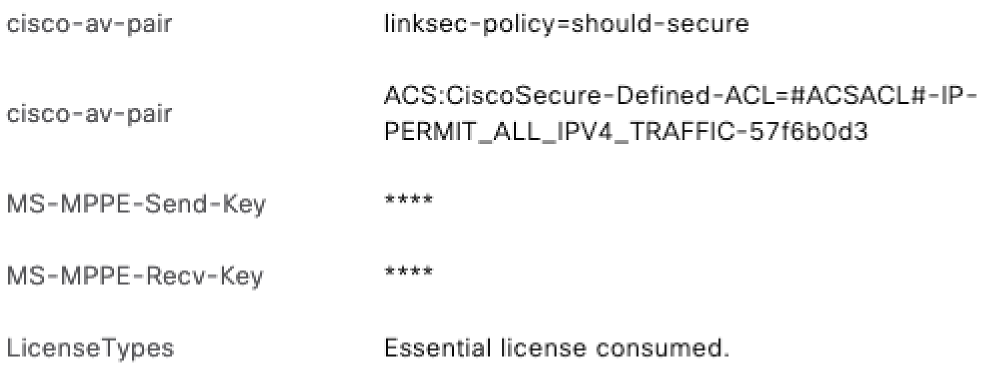
RADIUS Drops 4

Client S

Time	Status	Details	Repea...	Identity	Endpoint ID	Authentication Policy	Authori...	Authoriz...	IP Address	Network De...	Device
Aug 05, 2023 ...	●		0	roy	8C:4A:56:02:AC:...	WIRED DOT1X ACCESS ...	WIRED D...	WIRED_A...			TenGigal
Aug 05, 2023 ...	✓			#ACSACL#-IP-...						switch1	
Aug 05, 2023 ...	✓			roy	8C:4A:56:02:AC:...	WIRED DOT1X ACCESS ...	WIRED D...	WIRED_A...		switch1	TenGigal

Navigate in the **Details** of the authentication and the **Result** section.

The attributes set in the authorization profile are sent to the **Network Access Device (NAD)** as well as the consumption of one Essential license.

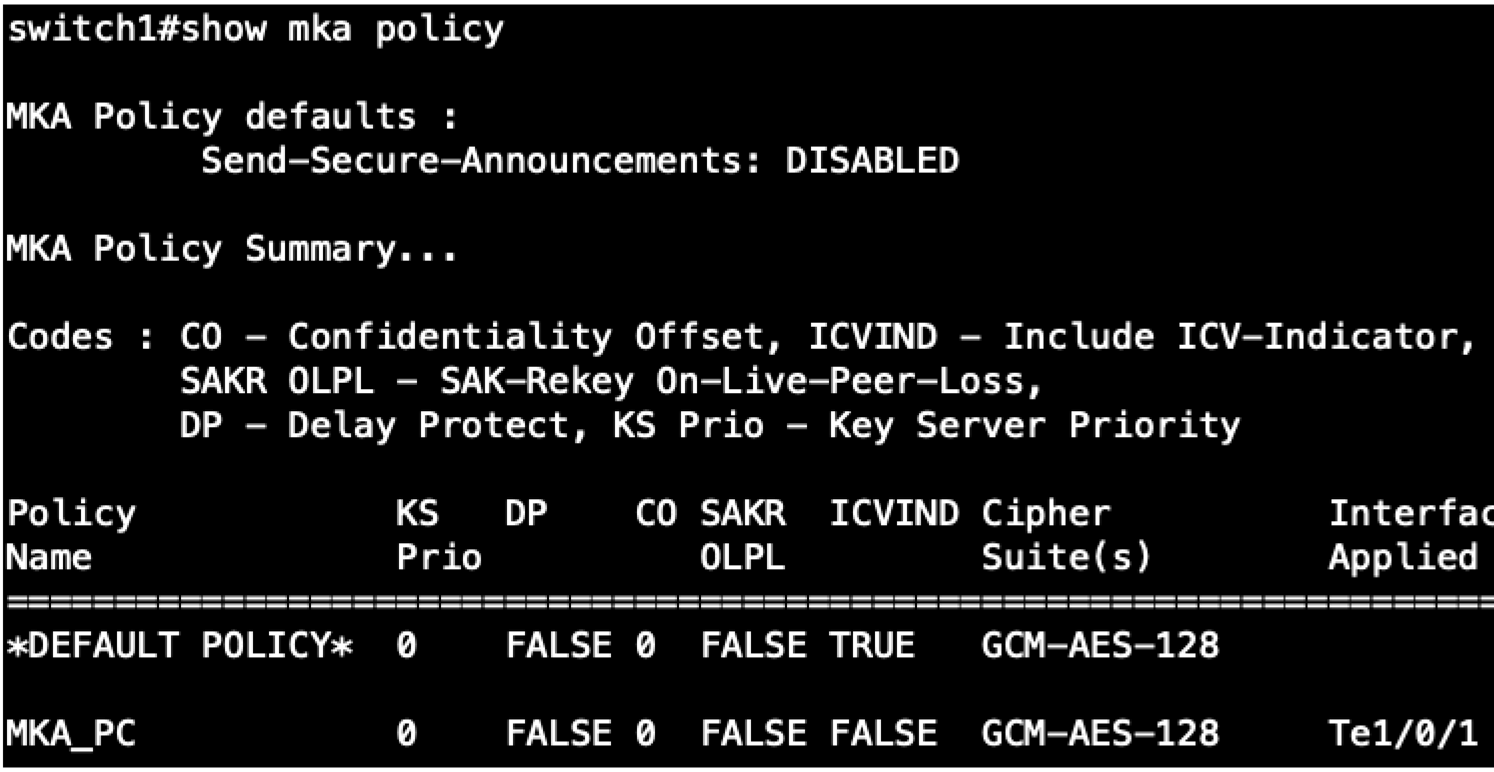


cisco-av-pair	linksec-policy=should-secure
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Essential license consumed.

Validation on the Catalyst switch.

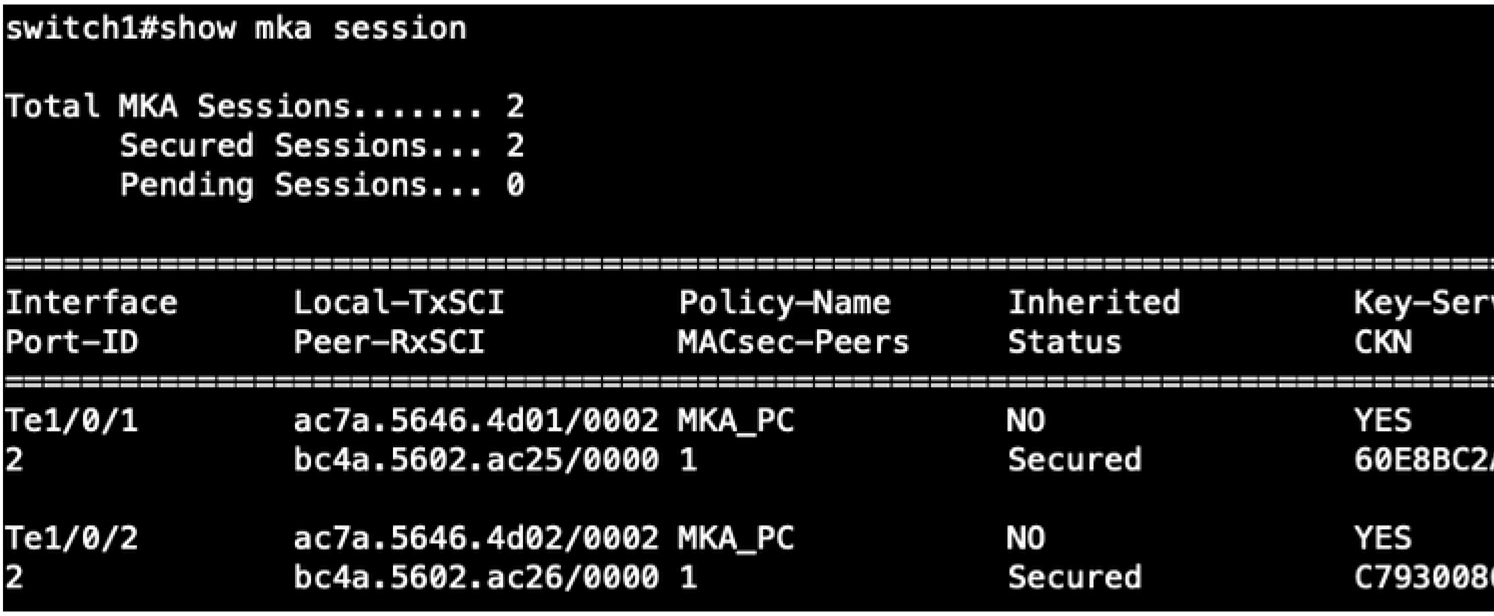
These commands can be used to validate the proper functionality of this solution.

```
switch1#show mka policy
```



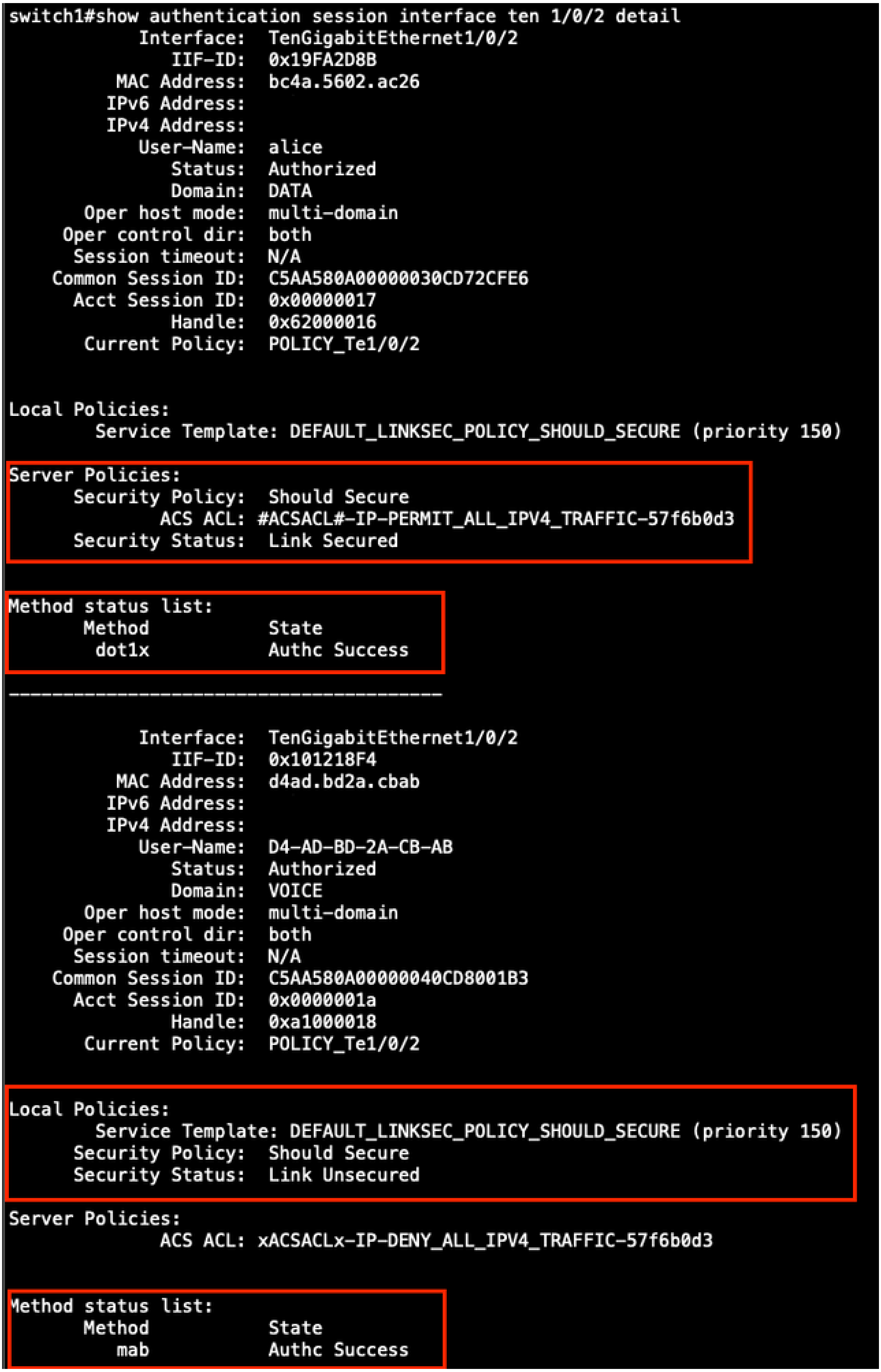
```
switch1#show mka policy

MKA Policy defaults :
         Send-Secure-Announcements: DISABLED

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          Interfac
Name                Prio           OLPL         Suite(s)        Applied
=========================================================================
*DEFAULT POLICY*    0     FALSE 0  FALSE TRUE   GCM-AES-128

MKA_PC              0     FALSE 0  FALSE FALSE  GCM-AES-128     Te1/0/1
```

```
switch1#show mka session
```



```
switch1#show mka session

Total MKA Sessions....... 2
      Secured Sessions... 2
      Pending Sessions... 0

=============================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Ser
Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
=============================================================================
Te1/0/1        ac7a.5646.4d01/0002 MKA_PC           NO                YES
2              bc4a.5602.ac25/0000 1                Secured           60E8BC2

Te1/0/2        ac7a.5646.4d02/0002 MKA_PC           NO                YES
2              bc4a.5602.ac26/0000 1                Secured           C793008
```

```
switch1#show authentication session interface <interface_ID> detail
```



```
switch1#show authentication session interface ten 1/0/2 detail
            Interface:  TenGigabitEthernet1/0/2
               IIF-ID:  0x19FA2D8B
          MAC Address:  bc4a.5602.ac26
         IPv6 Address:
         IPv4 Address:
            User-Name:  alice
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  C5AA580A00000030CD72CFE6
      Acct Session ID:  0x00000017
               Handle:  0x62000016
       Current Policy:  POLICY_Te1/0/2


Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
      Security Policy:  Should Secure
              ACS ACL: #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
      Security Status:  Link Secured


Method status list:
       Method           State
        dot1x           Authc Success

----------------------------------------

            Interface:  TenGigabitEthernet1/0/2
               IIF-ID:  0x101218F4
          MAC Address:  d4ad.bd2a.cbab
         IPv6 Address:
         IPv4 Address:
            User-Name:  D4-AD-BD-2A-CB-AB
               Status:  Authorized
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  C5AA580A00000040CD8001B3
      Acct Session ID:  0x0000001a
               Handle:  0xa1000018
       Current Policy:  POLICY_Te1/0/2


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

Server Policies:
              ACS ACL: xACSACLx-IP-DENY_ALL_IPV4_TRAFFIC-57f6b0d3


Method status list:
       Method           State
          mab           Authc Success
```

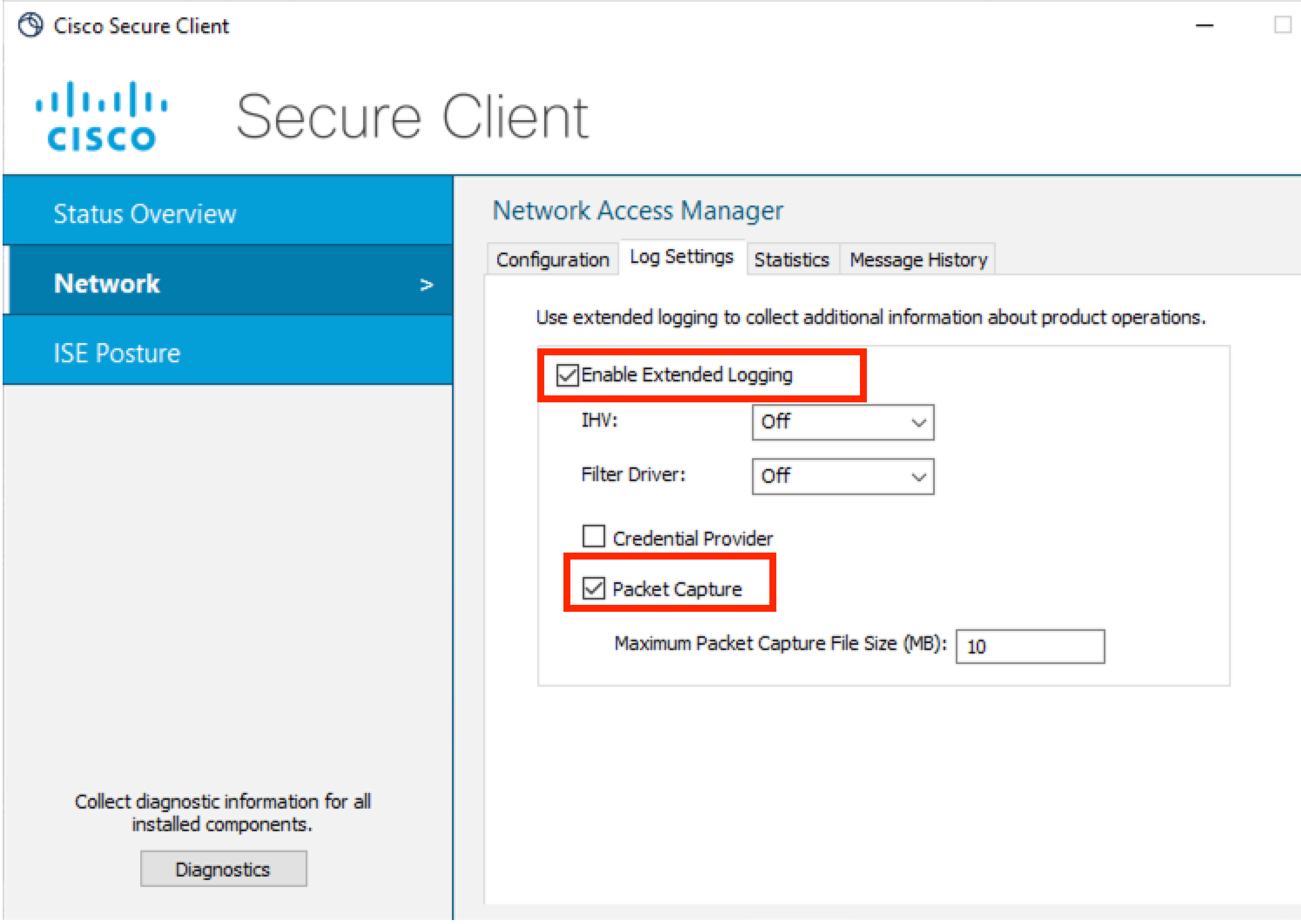
Validation on Secure Client.

The authentication is successful with the profile that you created with MACsec encryption. If you click in th

: This section covers the troubleshooting part related to MKA problems that can emerge. If you face an authentication or authorization failure, please refer to [ISE Secure Wired Access Prescriptive Deployment Guide - Troubleshooting] to investigate further as this guide assumes the authentications are working fine without MACsec encryption.

Cisco Secure Endpoint

- Enable DART module in the Secure Endpoint suite.
- In this menu, enable Extended Logging to gather more data about the user MKA connection. You can additionally enable a packet capture that is contained in the DART bundle.



Network Access Manager

Log Settings

Use extended logging to collect additional information about product operations.

☑ Enable Extended Logging

IHV: Off

Filter Driver: Off

□ Credential Provider

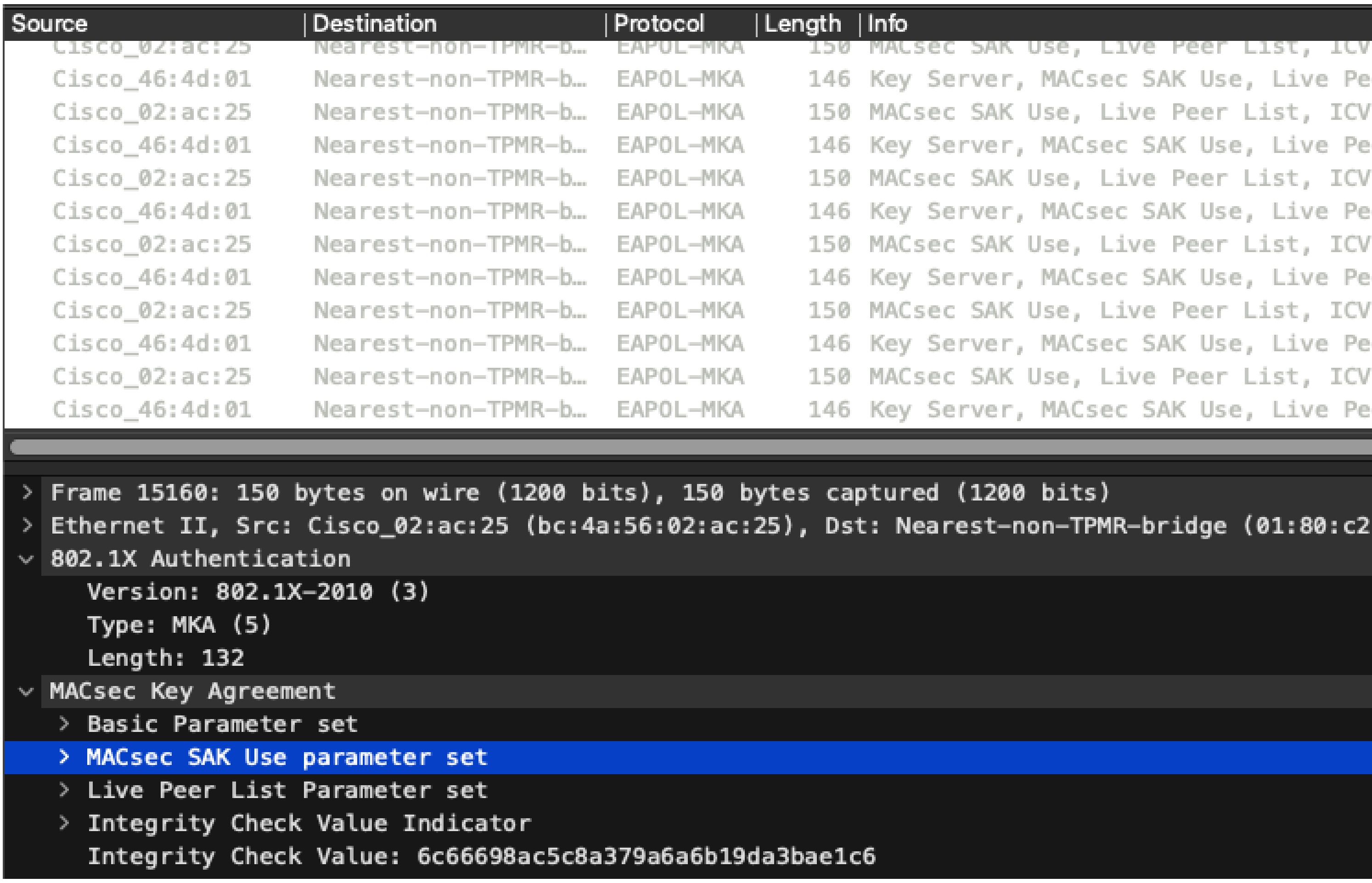
☑ Packet Capture

Maximum Packet Capture File Size (MB): 10

Collect diagnostic information for all installed components.

- Collect DART bundle to proceed with analysis of configuration.xml and Network access Manager. Refer to the documentation [Run DART to Gather Data for Troubleshooting]

This example displays how the packets are seen as the information between the host and the switch is encrypted :



```
Source            Destination           Protocol    Length  Info
Cisco_02:ac:25    Nearest-non-TPMR-b…   EAPOL-MKA   150 MACsec SAK Use, Live Peer List, ICV
Cisco_46:4d:01    Nearest-non-TPMR-b…   EAPOL-MKA   146 Key Server, MACsec SAK Use, Live Pe
Cisco_02:ac:25    Nearest-non-TPMR-b…   EAPOL-MKA   150 MACsec SAK Use, Live Peer List, ICV
Cisco_46:4d:01    Nearest-non-TPMR-b…   EAPOL-MKA   146 Key Server, MACsec SAK Use, Live Pe
Cisco_02:ac:25    Nearest-non-TPMR-b…   EAPOL-MKA   150 MACsec SAK Use, Live Peer List, ICV
Cisco_46:4d:01    Nearest-non-TPMR-b…   EAPOL-MKA   146 Key Server, MACsec SAK Use, Live Pe
Cisco_02:ac:25    Nearest-non-TPMR-b…   EAPOL-MKA   150 MACsec SAK Use, Live Peer List, ICV
Cisco_46:4d:01    Nearest-non-TPMR-b…   EAPOL-MKA   146 Key Server, MACsec SAK Use, Live Pe
Cisco_02:ac:25    Nearest-non-TPMR-b…   EAPOL-MKA   150 MACsec SAK Use, Live Peer List, ICV
Cisco_46:4d:01    Nearest-non-TPMR-b…   EAPOL-MKA   146 Key Server, MACsec SAK Use, Live Pe
Cisco_02:ac:25    Nearest-non-TPMR-b…   EAPOL-MKA   150 MACsec SAK Use, Live Peer List, ICV
Cisco_46:4d:01    Nearest-non-TPMR-b…   EAPOL-MKA   146 Key Server, MACsec SAK Use, Live Pe
```

```
> Frame 15160: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
> Ethernet II, Src: Cisco_02:ac:25 (bc:4a:56:02:ac:25), Dst: Nearest-non-TPMR-bridge (01:80:c2
v 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: MKA (5)
    Length: 132
v MACsec Key Agreement
  > Basic Parameter set
  > MACsec SAK Use parameter set
  > Live Peer List Parameter set
  > Integrity Check Value Indicator
    Integrity Check Value: 6c66698ac5c8a379a6a6b19da3bae1c6
```

From the DART bundle, we can find useful information for the authentication 802.1X and the MKA session in the log named **NetworkAccessManager.txt.**

This information is displayed in a successful Authentication with MKA encryption.

```
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: PORT (1) net: RECV (status: UP, AUTO) (portMsg.c 709)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: 8021X (2) RECEIVED SUCCESS (dot1x_util.c 326)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) current state = AUTHENTICATING (dot1x_sm.c 323)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) S_enterStateAux called with state = AUTHENTICATIN
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) staying in 802.1x state: AUTHENTICATING (dot1x_sm
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: 8021X (2) smTimer: sec=30 (dot1x_util.c 454)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) eap_type<0>, lengths<4,1496> (dot1x_proto.c 90)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: 8021X (2) smTimer: paused (dot1x_util.c 484)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: EAP (0) Received EAP-Success. (eap_auth_client.c 835)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: EAP (0) tlsAuthOnAuthEnd: clear TLS session (eap_auth_tls_c
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: EAP (0) tlsAuthOnAuthEnd: successful authentication, save p
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: EAP (3) new credential list saved (eapRequest.c 1485)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: EAP (3) EAP status: AC_EAP_STATUS_EAP_SUCCESS (eapMessage.c
%csc_nam-7-DEBUG_MSG: %[tid=9028]: EAP-CB: EAP status notification: session-id=1, handle=04B2DD44, statu
%csc_nam-7-DEBUG_MSG: %[tid=9028]: EAP-CB: sending EapStatusEvent...
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: PORT (2) EAP response received. <len:400> <res:2> (dot1x_pr
%csc_nam-7-DEBUG_MSG: %[tid=2716]: EAP: ...received EapStatusEvent: session-id=1, EAP handle=04B2DD44, s
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: 8021X (2) smTimer: activated (dot1x_util.c 503)
%csc_nam-6-INFO_MSG: %[tid=2716]: EAP: Eap status AC_EAP_STATUS_EAP_SUCCESS.
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) current state = AUTHENTICATING (dot1x_sm.c 323)
%csc_nam-7-DEBUG_MSG: %[tid=2716]: EAP: processing EapStatusEvent in the subscriber
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) dot1x->eapSuccess is True (dot1x_sm.c 352)
%csc_nam-7-DEBUG_MSG: %[tid=2716]: Auth[wired:user-auth]: Enabling fast reauthentication
```

```
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) SUCCESS (dot1x_sm.c 358)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) S_enterStateAux called with state = AUTHENTICATED
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) S_enterStateAux calling sm8Event8021x due to auth
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: 8021X (2) smTimer: disabled (dot1x_util.c 460)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: MKA (0) NASP: dot1xAuthSuccessEvt naspStopEapolAnnouncement
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: NASP (0) >> NASP: naspStopEapolAnnouncement (nasp.c 900)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: NASP (0) << NASP: naspStopEapolAnnouncement.  err = 0 (nasp
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: 8021X (2) dot1x->config.useMka = 1 (dot1x_main.c 829)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: INF (2) >> MKA: StartSession (mka.c 511)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: MKA (2) MKA: bUseMka = 1, bUseMacSec = 1706033334, MacsecSu
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: MKA (2) >> MKA: InitializeContext (mka.c 1247)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: INF (2) MKA: Changing state to Unconnected (mka.c 1867)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: INF (2) MKA: Changing Sak State to Idle (mka.c 1271)
%csc_nam-7-DEBUG_MSG: %[tid=2716]: Auth[wired:user-auth]: Fast reauthentication enabled on authenticatio
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: MKA (2) << MKA: InitializeContext (mka.c 1293)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: MKA (2) MKA: Changing state to Need Server (mka.c 1871)
%csc_nam-7-DEBUG_MSG: %[tid=2716]: Auth[wired:user-auth]: Sending NOTIFICATION__SUCCESS to subscribers
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: INF (2) >> MKA: CreateKeySet (mka.c 924)
%csc_nam-7-DEBUG_MSG: %[tid=2716]: Network auth request NOTIFICATION__SUCCESS
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: NASP (0) >> NASP: naspGetNetCipherSuite (nasp.c 569)
%csc_nam-6-INFO_MSG: %[tid=9028][comp=SAE]: MKA (2) MKA: Key length is 16 bytes (mka.c 954)
%csc_nam-7-DEBUG_MSG: %[tid=2716]: Auth[wired:user-auth]: Finishing authentication
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: MKA (2) MKA: MyMac (mka.c 971)
%csc_nam-7-DEBUG_MSG: %[tid=2716]: Auth[wired:user-auth]: Authentication finished
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: API (1) event: STATUS - AC_PORT_STATUS_EAP_SUCCESS (portWor
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: API (1) event: complete (portWorkList.c 130)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: API (1) event: STATUS - AC_PORT_STATUS_MKA_UNCONNECTED (por
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: API (1) event: complete (portWorkList.c 130)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: API (1) event: STATUS - AC_PORT_STATUS_MKA_NEED_SERVER (por
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: API (1) event: complete (portWorkList.c 130)
%csc_nam-7-DEBUG_MSG: %[tid=8140][comp=SAE]: NET (0) SscfCallback(1): SSCF_NOTIFICATION_CODE_SEND_PACKET
%csc_nam-7-DEBUG_MSG: %[tid=8140][comp=SAE]: NET (0) CIMD Event: evtSeq#=0 msg=4 ifIndex=1 len=36 (cimdE
%csc_nam-7-DEBUG_MSG: %[tid=8140][comp=SAE]: NET (1) cdiEvt:(3,0) dataLen=4 (cimdEvt.c 358)
%csc_nam-7-DEBUG_MSG: %[tid=8140][comp=SAE]: NET (1) cdiEvt:(3,1) dataLen=102 (cimdEvt.c 358)
%csc_nam-7-DEBUG_MSG: %[tid=8140][comp=SAE]: NET (1) netEvent(1): Recv queued (netEvents.c 91)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: PORT (1) net: RECV (status: UP, AUTO) (portMsg.c 709)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: MKA (2) >> MKA: EapolInput (mka.c 125)
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: MKA (2) MKA: MKPDU In (mka.c 131)
```

Cisco IOS Troubleshooting

These commands can be implemented in the **Network Access Device (NAD)** to review the MKA encryption between the platform and the supplicant.

For further information on the commands, review the corresponding configuration guide of the platform used as NAD.

```
#show authentication session interface <interface_ID> detail
#show mka summary
#show mka policy
#show mka session interface <interface_ID> detail
#show macsec summary
#show macsec interface <interface_ID>
#debug mka events
#debug mka errors
#debug macsec event
#debug macsec error
```

These are debugs of one successfull MKA connection to a host. You can use this as a reference comes up :

```
%LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/1, changed state to down
Macsec interface TenGigabitEthernet1/0/1 is UP
MKA-EVENT: Create session event: derived CKN 9F0DC198A9728FB3DA198711B58570E4, len 16
MKA-EVENT EC000025: SESSION START request received...
NGWC-MACSec: pd get port capability is invoked
MKA-EVENT: New MKA Session on Interface TenGigabitEthernet1/0/1 with Physical Port Number 9 is using the
MKA-EVENT: New VP with SCI AC7A.5646.4D01/0002 on interface TenGigabitEthernet1/0/1
MKA-EVENT: Created New CA 0x80007F30A6B46F20 Participant on interface TenGigabitEthernet1/0/1 with SCI A
%MKA-5-SESSION_START: (Te1/0/1 : 2) MKA Session started for RxSCI bc4a.5602.ac25/0000, AuditSessionID C5
MKA-EVENT: Started a new MKA Session on interface TenGigabitEthernet1/0/1 for Peer MAC bc4a.5602.ac25 wi
MKA-EVENT bc4a.5602.ac25/0000 EC000025: FSM (Init MKA Session) - Successfully derived CAK.
MKA-EVENT bc4a.5602.ac25/0000 EC000025: Successfully initialized a new MKA Session (i.e. CA entry) on in
MKA-EVENT bc4a.5602.ac25/0000 EC000025: FSM (Derive KEK/ICK) - Successfully derived KEK...
MKA-EVENT bc4a.5602.ac25/0000 EC000025: FSM (Derive KEK/ICK) - Successfully derived ICK...
MKA-EVENT bc4a.5602.ac25/0000 EC000025: New Live Peer detected, No potential peer so generate the first
MKA-EVENT bc4a.5602.ac25/0000 EC000025: >> FSM - Generate SAK for CA with CKN 9F0DC198 (Latest AN=0, Old
MKA-EVENT bc4a.5602.ac25/0000 EC000025: Generation of new Latest SAK succeeded (Latest AN=0, KN=1)...
MKA-EVENT bc4a.5602.ac25/0000 EC000025: >> FSM - Install RxSA for CA with CKN 9F0DC198 on VP with SCI AC
MKA-EVENT bc4a.5602.ac25/0000 EC000025: Clean up the Rx for dormant peers
MACSec-IPC: send_xable send msg success for switch=1
MACSec-IPC: blocking enable disable ipc req
MACSec-IPC: watched boolean waken up
MACSec-IPC: geting switch number
MACSec-IPC: switch number is 1
MACSec-IPC: create_tx_sc send msg success
Send create_tx_sc to IOMD successfully
alloc_cache called TxSCI: AC7A56464D010002 RxSCI: BC4A5602AC250000
Enabling replication for slot 1 vlan 330 and the ref count is 1
MACSec-IPC: vlan_replication send msg success
Added replication for data vlan 330
MACSec-IPC: geting switch number
MACSec-IPC: switch number is 1
MACSec-IPC: create_rx_sc send msg success
Sent RXSC request to FED/IOMD
MACSec-IPC: geting switch number
MACSec-IPC: switch number is 1
MACSec-IPC: install_rx_sa send msg success
Sent ins_rx_sa to FED and IOMD
MKA-EVENT bc4a.5602.ac25/0000 EC000025: Requested to install/enable new RxSA successfully (AN=0, KN=1 SC
%LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan330, changed state to up
MKA-EVENT bc4a.5602.ac25/0000 EC000025: Sending SAK for AN 0 resp peers 0 cap peers 1
MKA-EVENT bc4a.5602.ac25/0000 EC000025: SAK Wait Timer started for 6 seconds.
MKA-EVENT bc4a.5602.ac25/0000 EC000025: (KS) Received new SAK-Use response to Distributed SAK for AN 0,
MKA-EVENT bc4a.5602.ac25/0000 EC000025: (KS) All 1 peers with the required MACsec Capability have indica
MKA-EVENT: Reqd to Install TX SA for CA 0x80007F30A6B46F20 AN 0 CKN 9F0DC198 - on int(TenGigabitEthernet
MKA-EVENT bc4a.5602.ac25/0000 EC000025: >> FSM - Install TxSA for CA with CKN 9F0DC198 on VP with SCI AC
MACSec-IPC: geting switch number
MACSec-IPC: switch number is 1
MACSec-IPC: install_tx_sa send msg success
MKA-EVENT bc4a.5602.ac25/0000 EC000025: Before sending SESSION_SECURED status - SECURED=false, PREVIOUSL
MKA-EVENT bc4a.5602.ac25/0000 EC000025: Successfully sent SECURED status for CA with CKN 9F0DC198.
MKA-EVENT: Successfully updated the CKN handle for interface: TenGigabitEthernet1/0/1 with 9F0DC198 (if_
%MKA-5-SESSION_SECURED: (Te1/0/1 : 2) MKA Session was secured for RxSCI bc4a.5602.ac25/0000, AuditSessio
MKA-EVENT: MSK found to be same while updating the MSK and EAP Session ID in the subblock
MKA-EVENT bc4a.5602.ac25/0000 EC000025: After sending SESSION_SECURED status - SECURED=true, PREVIOUSLY_
```

Identity Services Engine (ISE) Troubleshooting

The troubleshooting related to this feature is limited to the delivery of the cisco-av-pair attribute **linksec-policy=should-secure.**

Ensure that the authorization result is sending that information to the Radius session linked to the switchports where the devices are being connected.

For further authentication analysis on ISE refer to Troubleshoot and Enable Debugs on ISE

Common Problems

Cipher mismatch

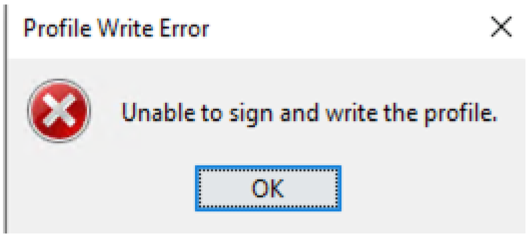
This log can be seen in the MKA debugs in the NAD.

```
MKA-4-MKA_MACSEC_CIPHER_MISMATCH: (Te1/0/1 : 30) Lower strength MKA-cipher than macsec-cipher for RxSCI
```

The first thing to verify in this scenario is that the ciphers configured in the MKA policy in the switch and in the Secure Client profile match.

For the case of AES-GCM-256 encryption, these requirements need to be met as per the documentation Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5

Inability to save the configuration.xml.



Profile Write Error

Unable to sign and write the profile.

This problem related to Profile Write Error is solved by saving the configuration.xml (as described earlier) named Setup of MKA using Network Access Manager Profile Editor.

The error is related that the file configuration.xml in used cannot be modified, hence you need to save the file in another location to proceed next with the replacement of the profiles.

Related information

- Configuring MACsec Encryption
- Configuring MACsec Switch to Host with Cat9k & ISE