MKA configureren en oplossen met Secure Client 5

Inhoud

Inleiding

In dit document wordt beschreven hoe MACsec-codering in een eindpunt kan worden geconfigureerd met Secure Client 5 als aanvrager.

Voorwaarden

Cisco raadt kennis aan over deze onderwerpen:

- Identity Services-engine
- 802.1x en Radius
- MACsec MKA-codering
- Secure Client versie 5 (voorheen bekend als Anyconnect)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine (ISE) versie 3.3
- Catalyst 9300 versie 17.06.05
- Cisco Secure Client 5.0.4032

Achtergrondinformatie

MACSec (Media Access Control Security) is een netwerkbeveiligingsstandaard die codering en bescherming biedt voor Ethernet-frames op laag 2 van het OSI-model (Data Link), gedefinieerd door de 802.1AE IEEE-standaard.

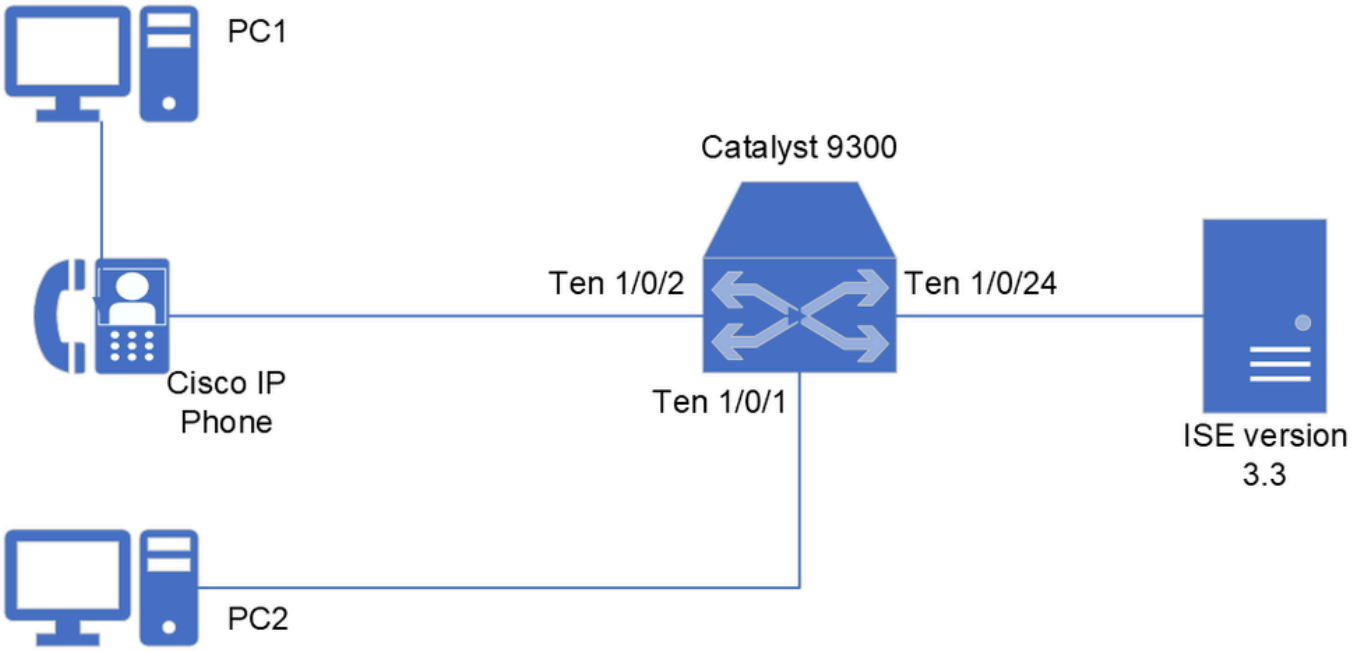
MACSec biedt deze codering in een point-to-point-verbinding die switch-naar-switch- of switch-naar-hostverbindingen kan zijn, dus de dekking van deze standaard is beperkt tot bekabelde verbindingen.

Deze standaard versleutelt de volledige gegevens, behalve het MAC-adres van de bron en bestemming van frames die worden verzonden in een laag 2-verbinding.

Het MACsec Key Agreement (MKA)-protocol is het mechanisme van waaruit MACsec-peers gaan onderhandelen over de beveiligingssleutels die nodig zijn om de koppeling te beveiligen.

Configureren

Netwerkdiagram



Opmerking: in deze documentatie wordt ervan uitgegaan dat u regels hebt geconfigureerd en werkt voor Radius-verificatie voor de pc-apparaten en de Cisco IP-telefoon. Raadpleeg de ISE Secure Wired Access Prescriptive Deployment Guide om een geheel nieuwe configuratie in te stellen om de configuratie in Identity Services Engine en Switch voor Identity-Based Network Access te bekijken.

Opzetten van beleid op het gebied van ISE

De eerste taak is het configureren van de bijbehorende autorisatieprofielen die worden toegepast op beide pc's (evenals de Cisco IP Phone) die in het vorige diagram worden weergegeven.

In dit hypothetische scenario zullen de pc's het 802.1X-protocol gebruiken als de verificatiemethode en de Cisco IP Phone gebruikt Mac Address Bypass (MAB).

ISE communiceert met de switch via het Radius-protocol over de attributen die de switch moet afdwingen in de interface van waaruit het eindpunt is verbonden via een Radius-sessie.

Voor MACsec-codering in hosts is het vereiste attribuut cisco-av-pair = linksec-policy, dat deze 3 mogelijke waarden heeft:

- Moet-niet-beveiligd: de switch voert geen MKA-codering uit in de interface waar de Radius-

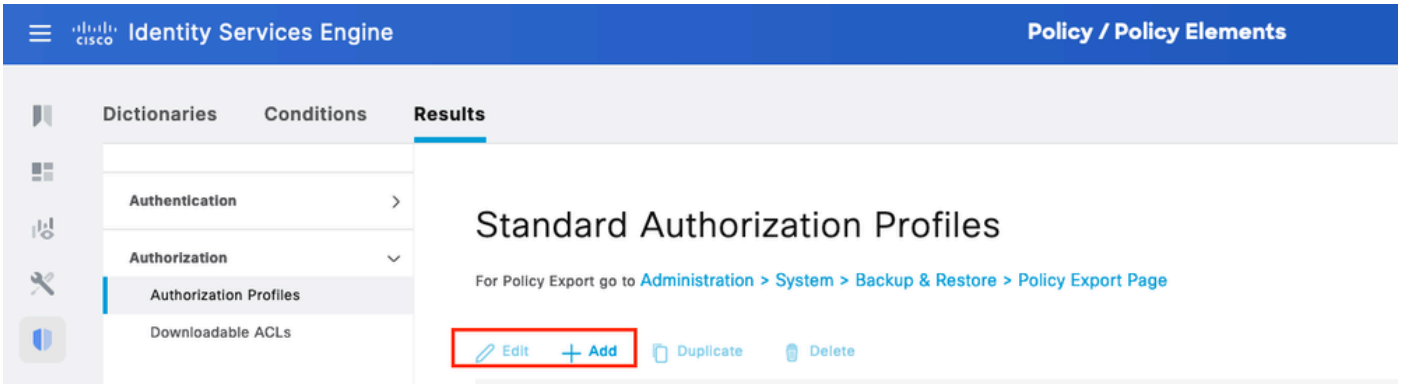
sessie plaatsvindt.

- Must-Secure: De switch moet codering afdwingen in het verkeer dat is gekoppeld aan de Radius-sessie. Als de MKA-sessie mislukt (of een time-out heeft), wordt de verbinding beschouwd als een autorisatiefout en wordt een andere poging gedaan om de MKA-sessie tot stand te brengen.
- Should-Secure: De switch probeert MKA-codering uit te voeren. Als de MKA-sessie gekoppeld aan de Radius-sessie succesvol is, wordt het verkeer versleuteld. Als de MKA uitvalt of uitvalt, staat de switch toe dat ongecodeerd verkeer wordt gekoppeld aan die Radius-sessie.

Stap 1. In beide pc's moet een must-secure MKA-beleid worden afgedwongen om flexibiliteit te hebben in het geval dat een machine zonder MKA-mogelijkheden verbinding maakt met de interface Ten 1/0/1.

Als optie kunt u een beleid voor pc2 configureren dat een beleid afdwingt dat moet worden beveiligd.

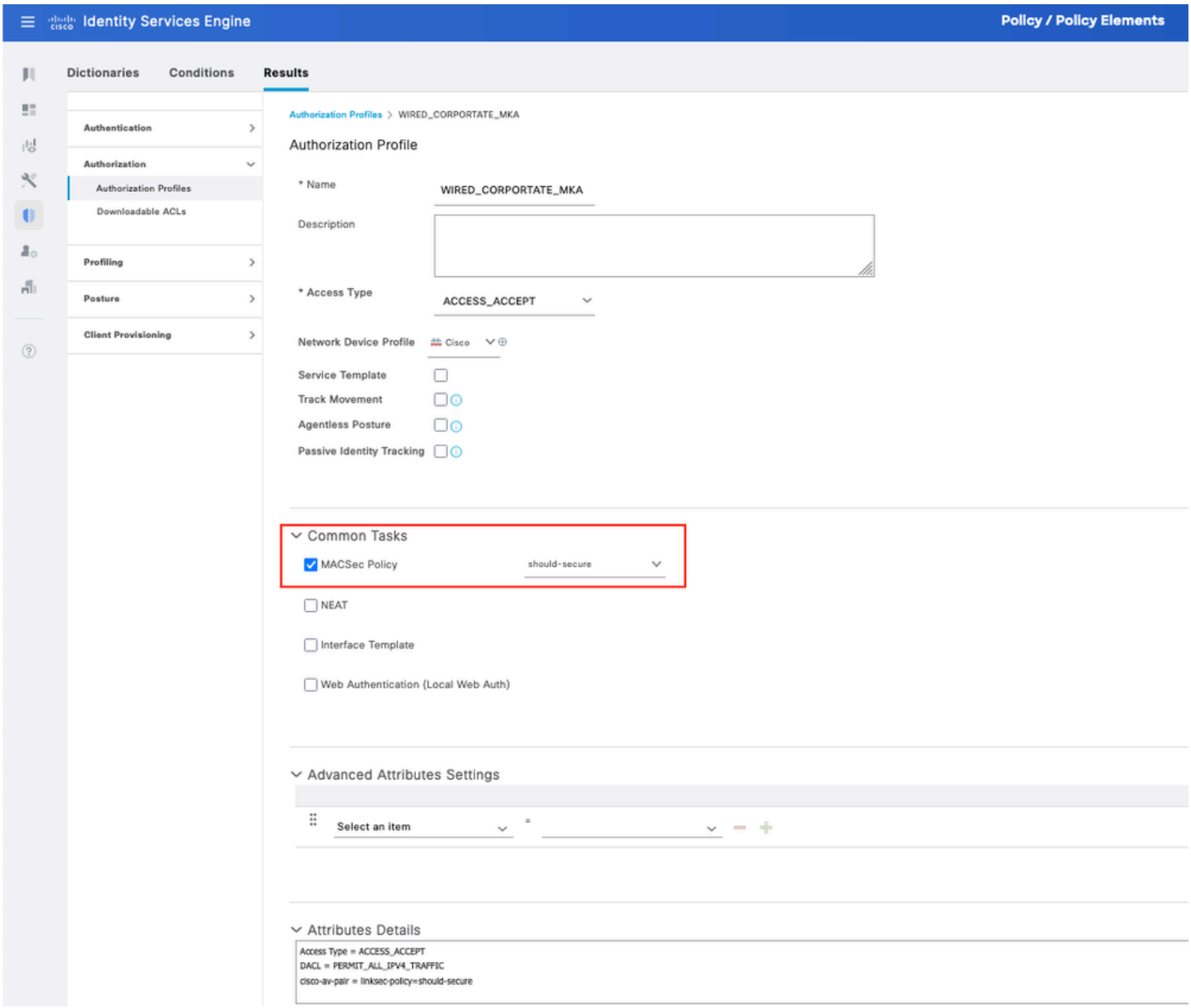
Configureer in dit voorbeeld het beleid voor de pc's zoals in Beleid > Beleidselementen > Resultaten > Autorisatieprofielen en +Voeg of Bewerk een bestaand profiel toe



Stap 2. Vul de voor het profiel vereiste velden in of pas deze aan.

Zorg ervoor dat u in Algemene taken MACSec-beleid hebt geselecteerd en het bijbehorende beleid dat moet worden toegepast.

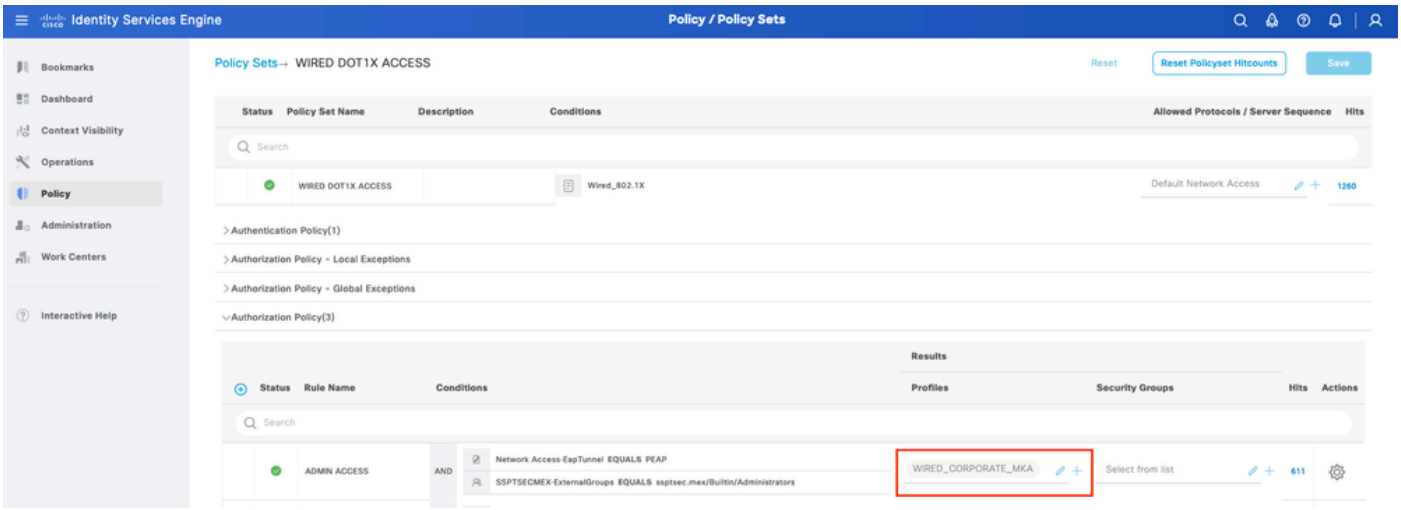
Scroll naar beneden en sla de configuratie op.



Stap 3. Wijs het bijbehorende autorisatieprofiel toe aan de autorisatieregels die door de apparaten worden getroffen.

Navigeer naar Beleid > Beleidsreeksen > (Beleidsreeks selecteren toegewezen) > Autorisatiebeleid.

Koppel de autorisatieregel aan het autorisatieprofiel met MACsec-instellingen. Scroll naar beneden en sla uw configuratie op.



Opstelling van MKA in Catalyst 9300

Stap 1. Configureer een nieuw MKA-beleid zoals dit voorbeeld doet vermoeden:

```
!
  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
  include-icv-indicator
  no send-secure-announcements
  no use-updated-eth-header
  no ssci-based-on-sci
!
```

Stap 2. Schakel MACsec-codering in op de interface waar de pc's zijn aangesloten.

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

Opmerking: voor meer informatie over de opdrachten en opties in MKA-configuratie raadpleegt u de configuratiehandleiding voor beveiliging die overeenkomt met de versie van de switch die u gebruikt. In dit scenario voor dit voorbeeld, Security Configuration

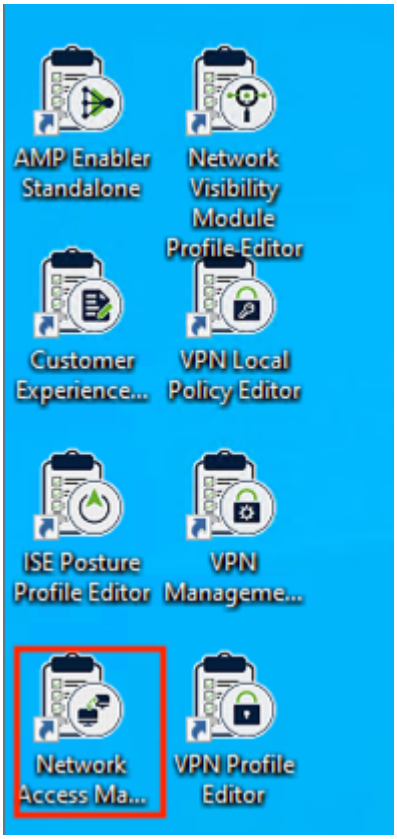
---

Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches)

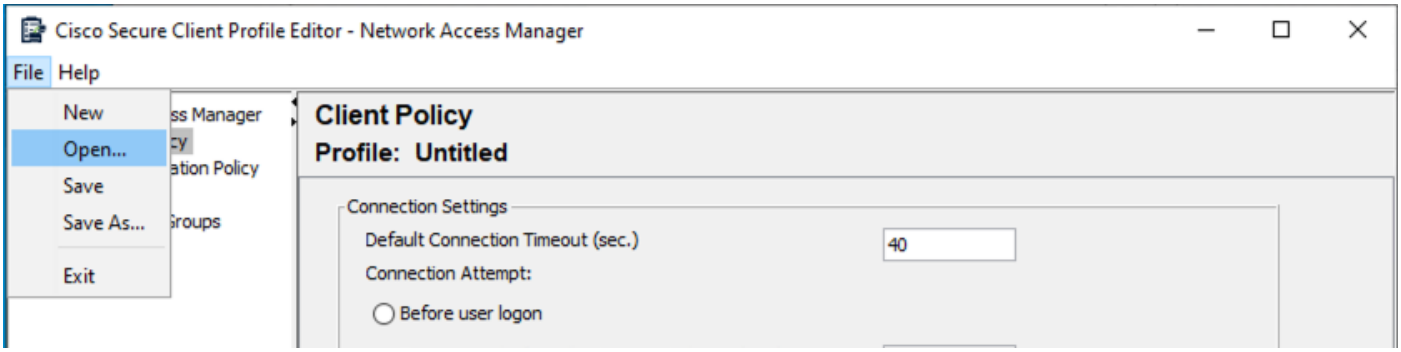
MKA instellen met de profieleditor van Network Access Manager.

Stap 1. Download (van de downloadwebsite van Cisco) en open de profieleditor die overeenkomt met de versie van Secure Client die wordt gebruikt.

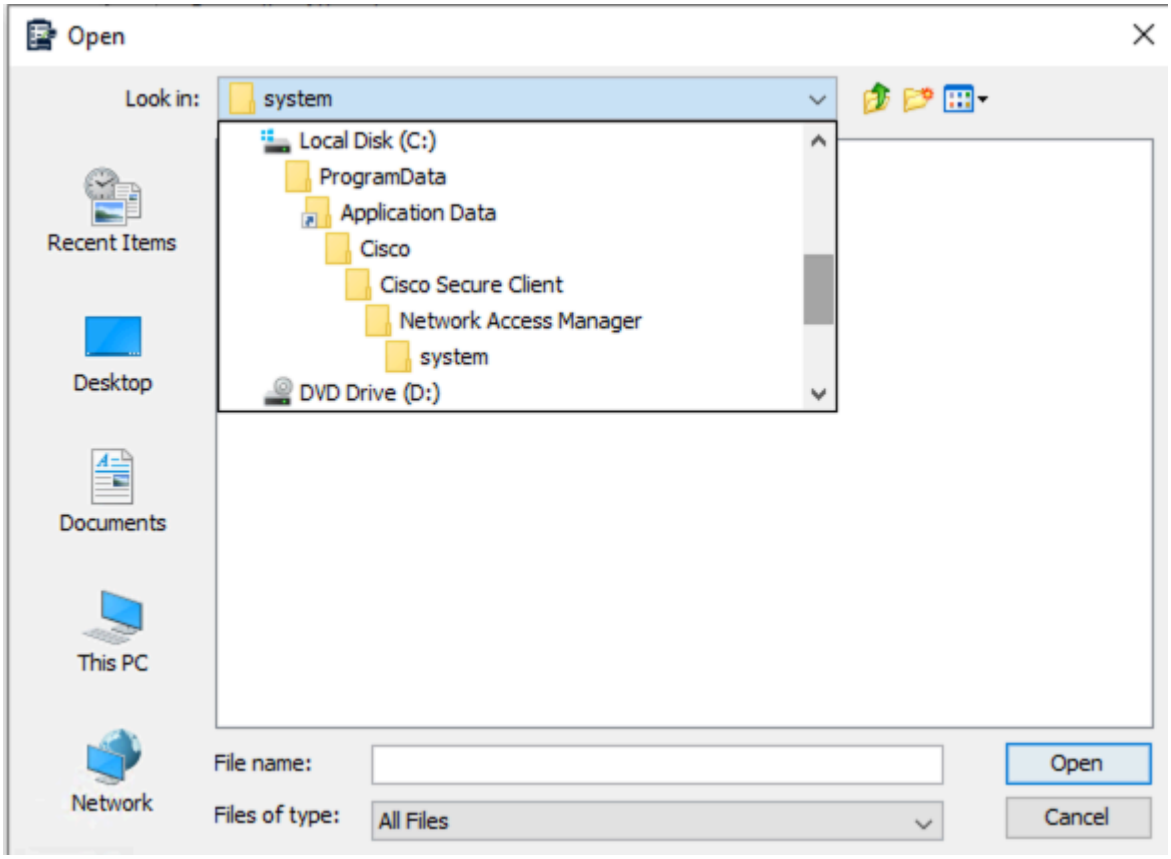
Nadat u dit programma op uw computer hebt geïnstalleerd, gaat u verder met het openen van de Cisco Secure Client Profile Editor – Network Access Manager.



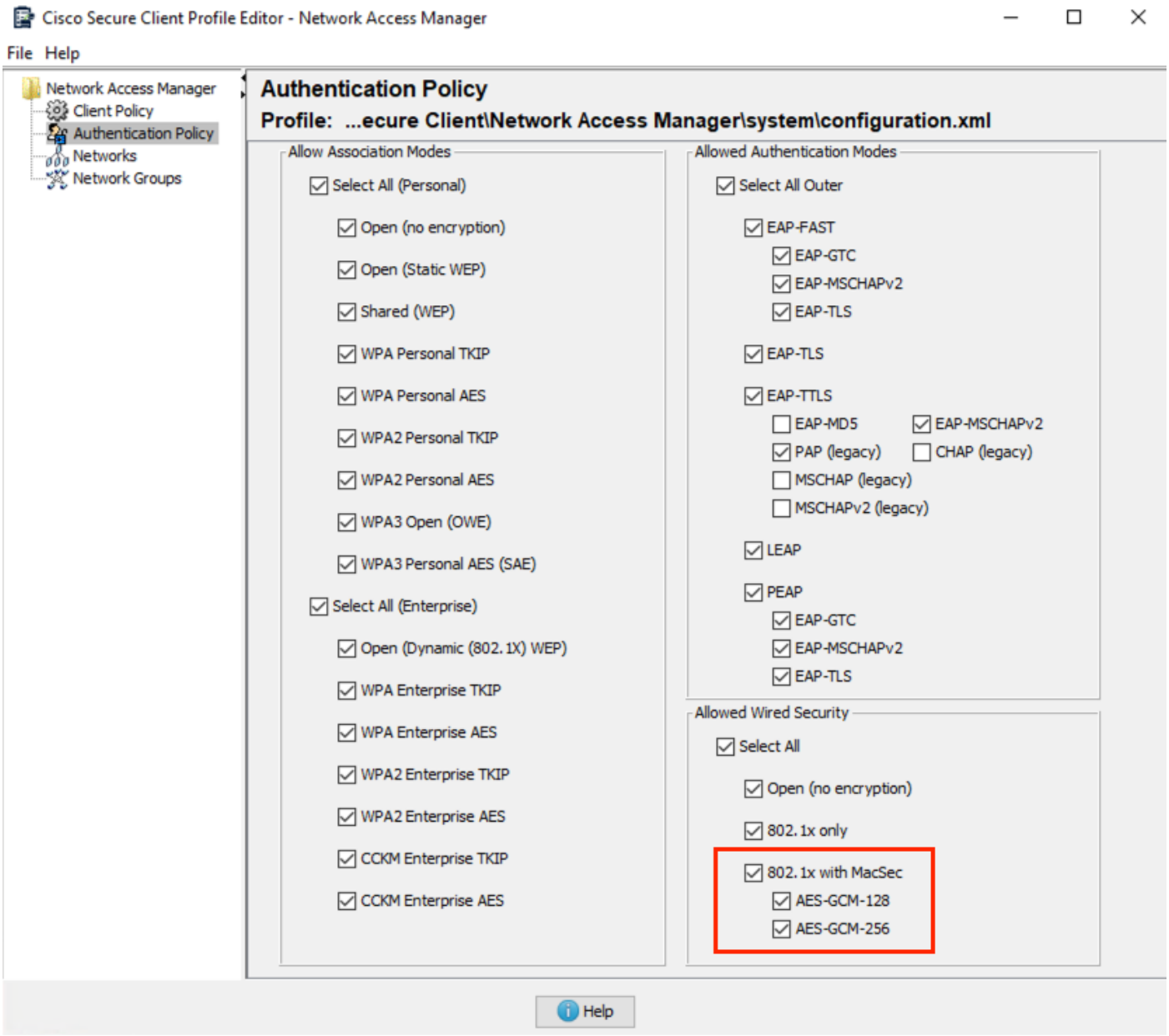
Stap 2. Selecteer Bestand > Openen.



Stap 3. Selecteer de systeemmap die in deze afbeelding wordt weergegeven. Open in deze map het bestand met de naam configuration.xml.

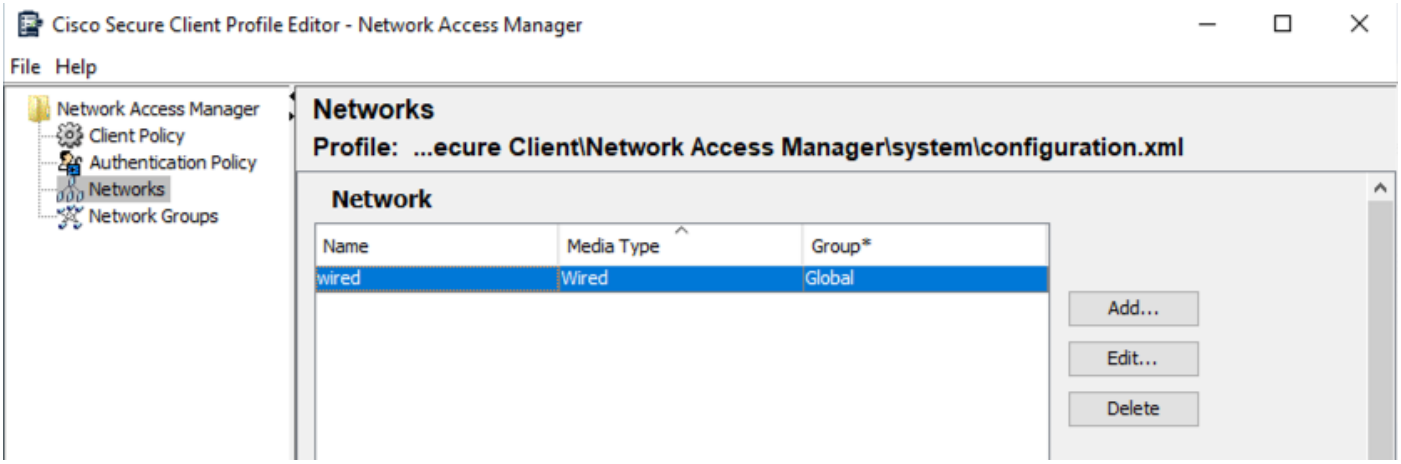


Stap 4. Nadat het bestand door de profieleditor is geladen, selecteert u de optie Verificatiebeleid en zorgt u ervoor dat de optie met betrekking tot 802.1x met MACSec is ingeschakeld.



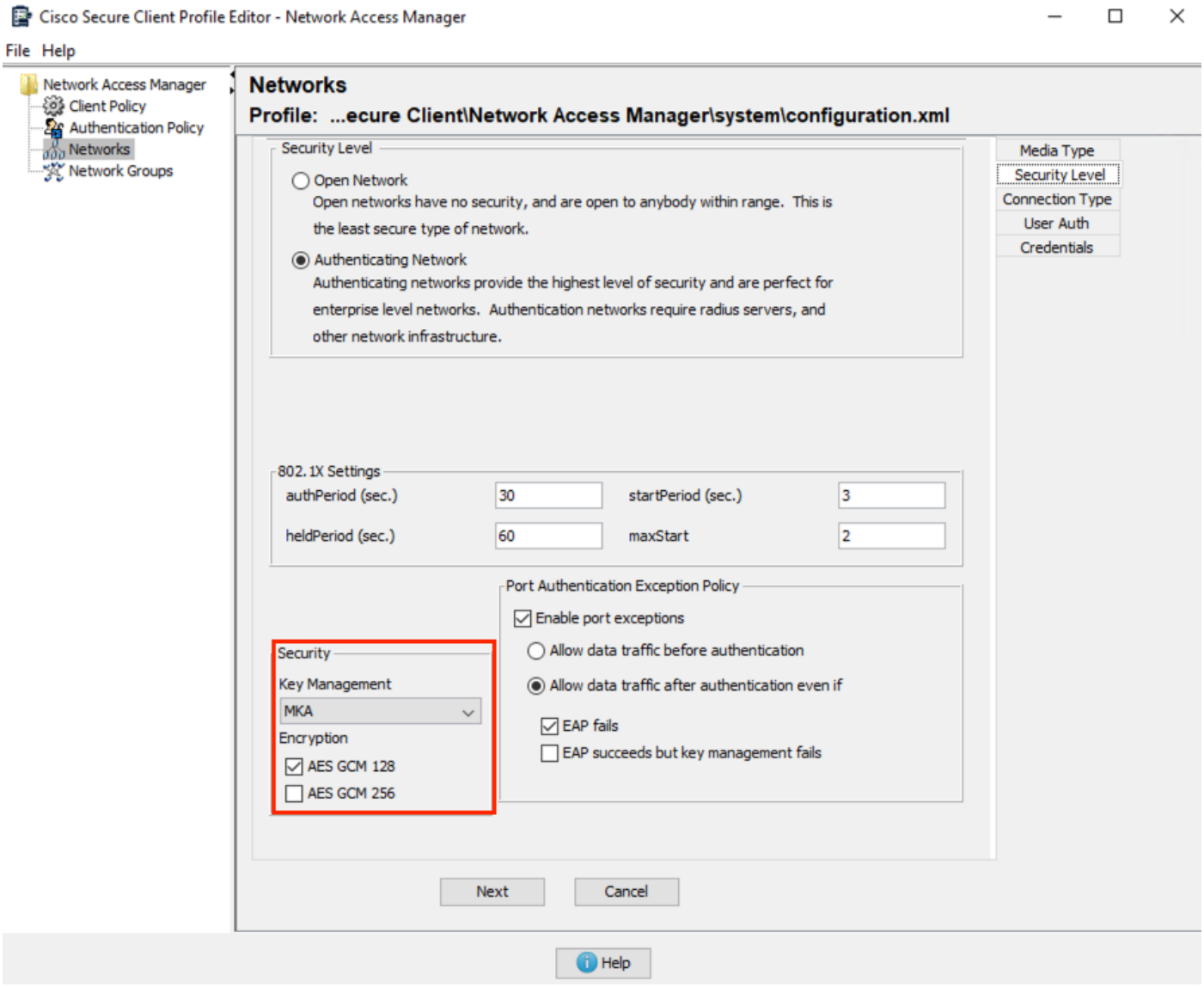
Stap 5. Ga naar de sectie Netwerken. In dit deel kunt u een nieuw profiel toevoegen voor een bekabelde verbinding of het standaard bekabelde profiel bewerken dat is geïnstalleerd met Secure Client 5.0.

In dit scenario gaan we het bestaande bekabelde profiel bewerken.



Stap 6. Configureer het profiel. Pas in het gedeelte Beveiligingsniveau het sleutelbeheer aan om MKA te gebruiken gevolgd door een codering AES GCM 128.

Pas ook de andere parameters voor de verificatie dot1x en het beleid aan.

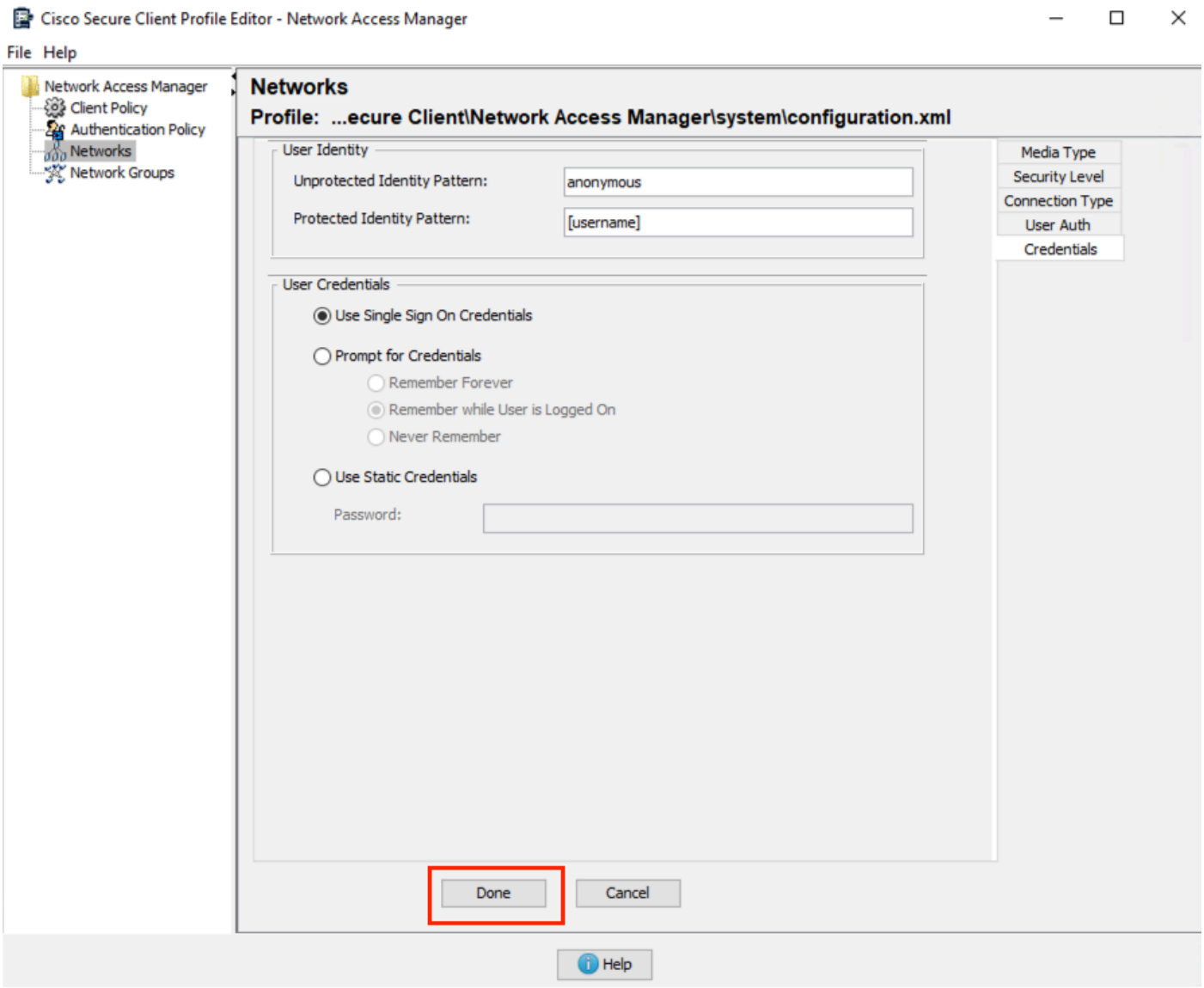


Stap 7. Configureer de overige secties met betrekking tot verbindingstype, gebruikersverificatie en referenties.

Deze secties zijn afhankelijk van de verificatie-instellingen die zijn geselecteerd in het gedeelte Beveiligingsniveau.

Wanneer u klaar bent met de configuraties, klikt u op Gereed.

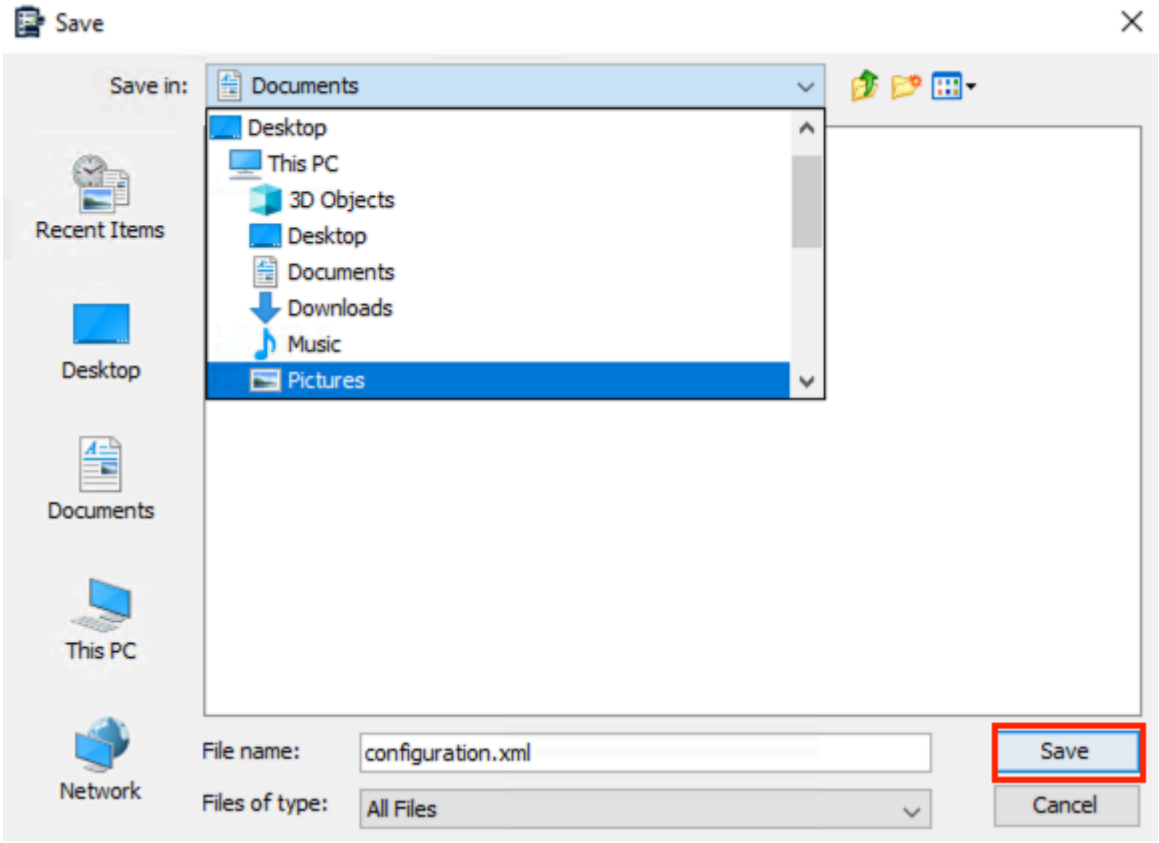
Voor dit scenario gebruiken we Protected Extensible Authentication Protocol (PEAP) met gebruikersreferenties.



Stap 8. Navigeer naar het menu Bestand. Ga verder met Opslaan als optie.

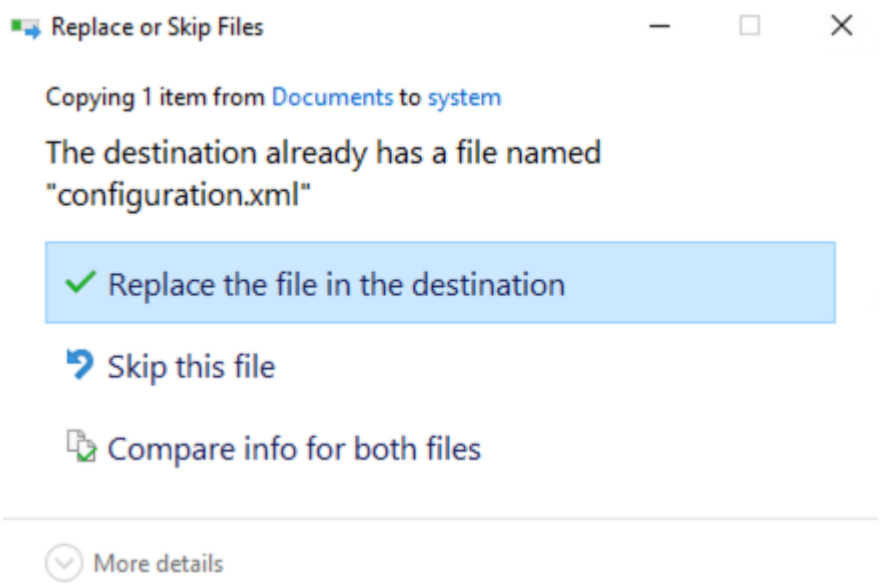
Noem het bestand als configuration.xml en sla het op in een andere map van ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system.

In dit voorbeeld is het bestand opgeslagen in de map Documenten. Sla het profiel op.



Stap 8. Ga naar de profiellocatie, kopieer het bestand en vervang het bestand in de map ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system.

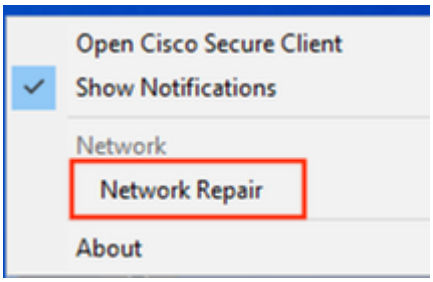
Selecteer de optie Bestand in bestemming vervangen.



Stap 9. Als u het aangepaste profiel in Beveiligingsclient 5.0 wilt laden, klikt u met de

rechtermuisknop op het pictogram Beveiligde client in de rechterbenedenbalk van uw Windows-systeem.

Voer een netwerkreparatie uit.

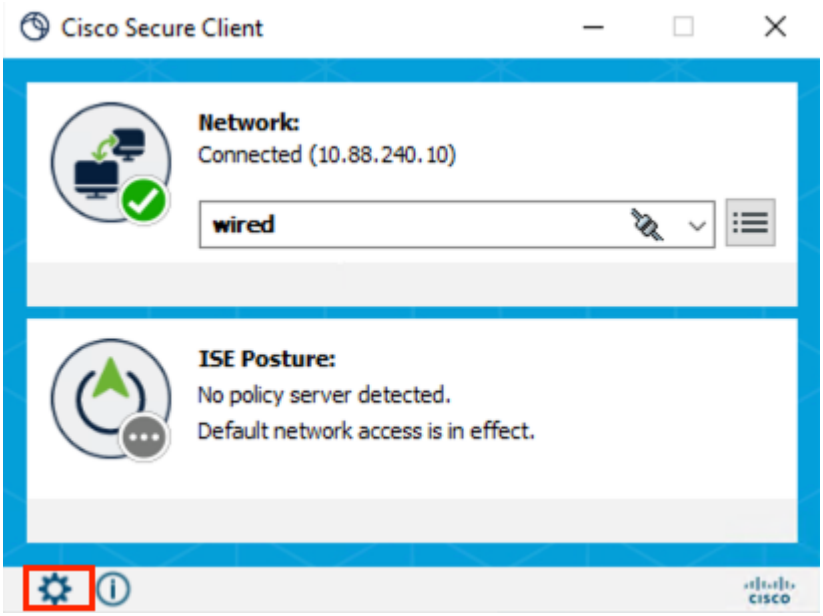


Opmerking: alle netwerken die via de profieleditor zijn geconfigureerd, hebben rechten van het beheerdersnetwerk. Daarom kunnen gebruikers de inhoud die u met dit hulpprogramma hebt geconfigureerd, niet aanpassen/wijzigen.

MKA-netwerken instellen met Network Access Manager (optioneel).

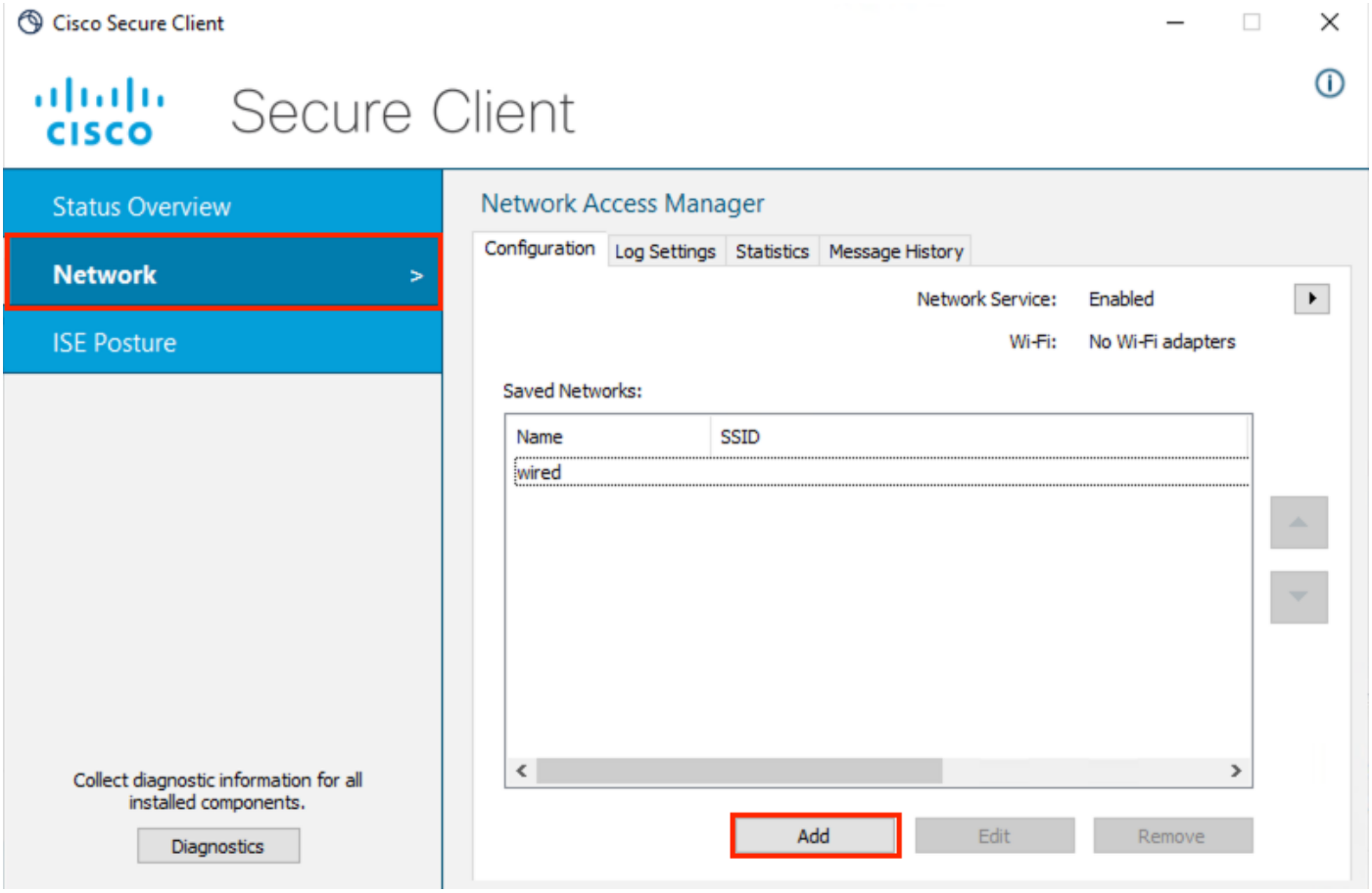
Stap 1. Als alternatief voor de MKA-installatie met behulp van de profieleditor, kunt u netwerken toevoegen zonder dit hulpprogramma te gebruiken.

Selecteer in de Secure Client-suite het tandwielpictogram.



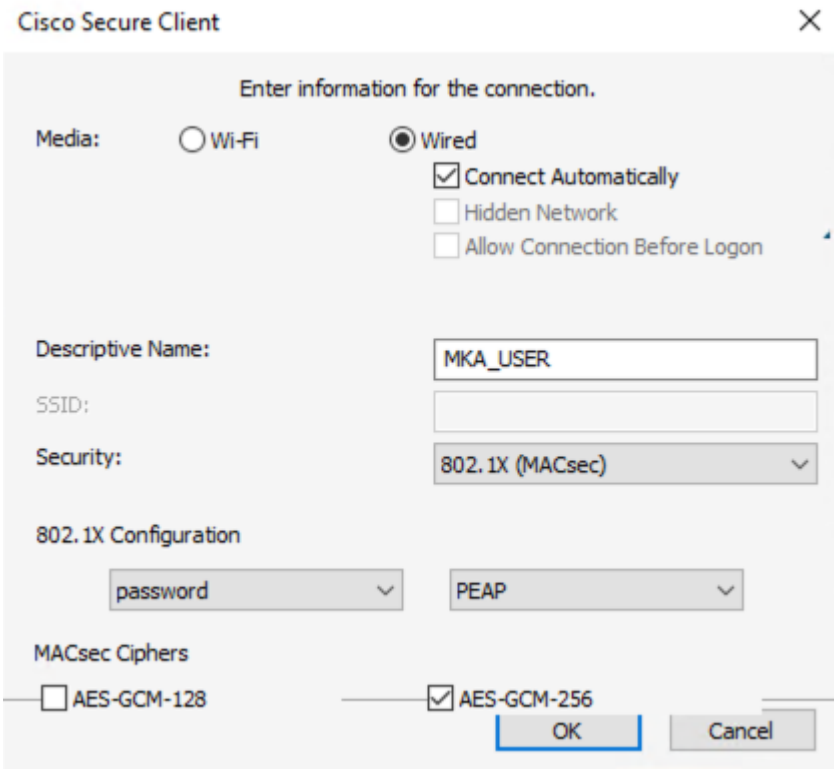
Stap 2. Selecteer in het nieuwe venster de optie Netwerk.

Selecteer in het gedeelte Configuratie de optie Toevoegen om toegang te krijgen tot een netwerk dat geschikt is voor MKA met rechten voor gebruikersnetwerk.



Stap 3. Stel in het nieuwe configuratievenster de kenmerken van uw verbinding in en geef het netwerk een naam.

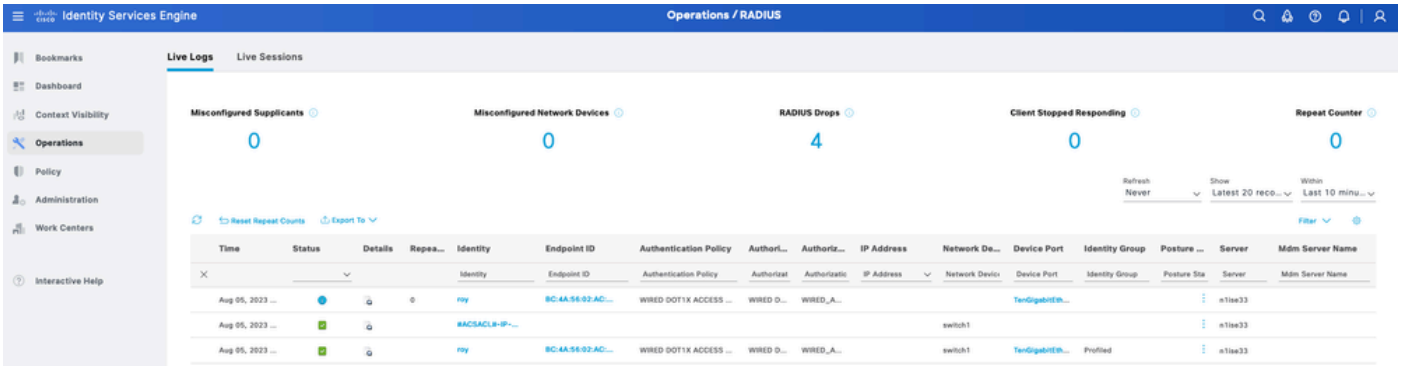
Wanneer u klaar bent, selecteert u de knop OK.



Verifiëren

Validatie op ISE

In ISE, na het voltooien van de configuratie van deze stroom, merkt u dat het apparaat wordt geverifieerd en geautoriseerd in Livelogs.



Navigeer in de sectie Details van de verificatie en het resultaat.

De attributen die zijn ingesteld in het autorisatieprofiel worden verzonden naar het Network Access Device (NAD) en het gebruik van één Essential-licentie.

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.

Validering op de Catalyst switch.

Deze opdrachten kunnen worden gebruikt om de juiste functionaliteit van deze oplossing te valideren.

```
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          Interfaces
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        Te1/0/2
```

```
switch1#show mka session
```

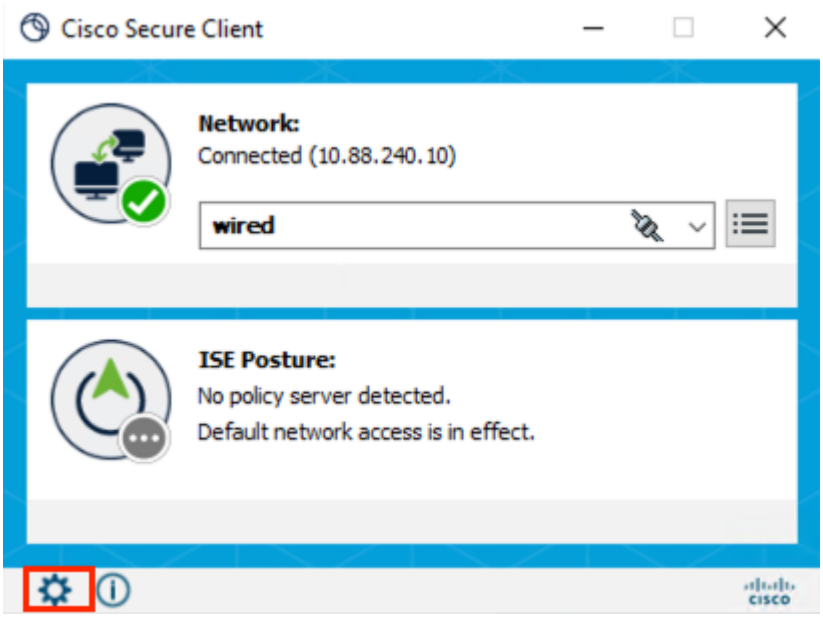
```
switch1#show mka session

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

===============================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited        Key-Server
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          60E8BC2A9EF5FE11532428862C747640

Te1/0/2        ac7a.5646.4d02/0002 MKA_PC           NO               YES
2              bc4a.5602.ac26/0000 1                Secured          C79300869F539BB534350133064744B6
```

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
```

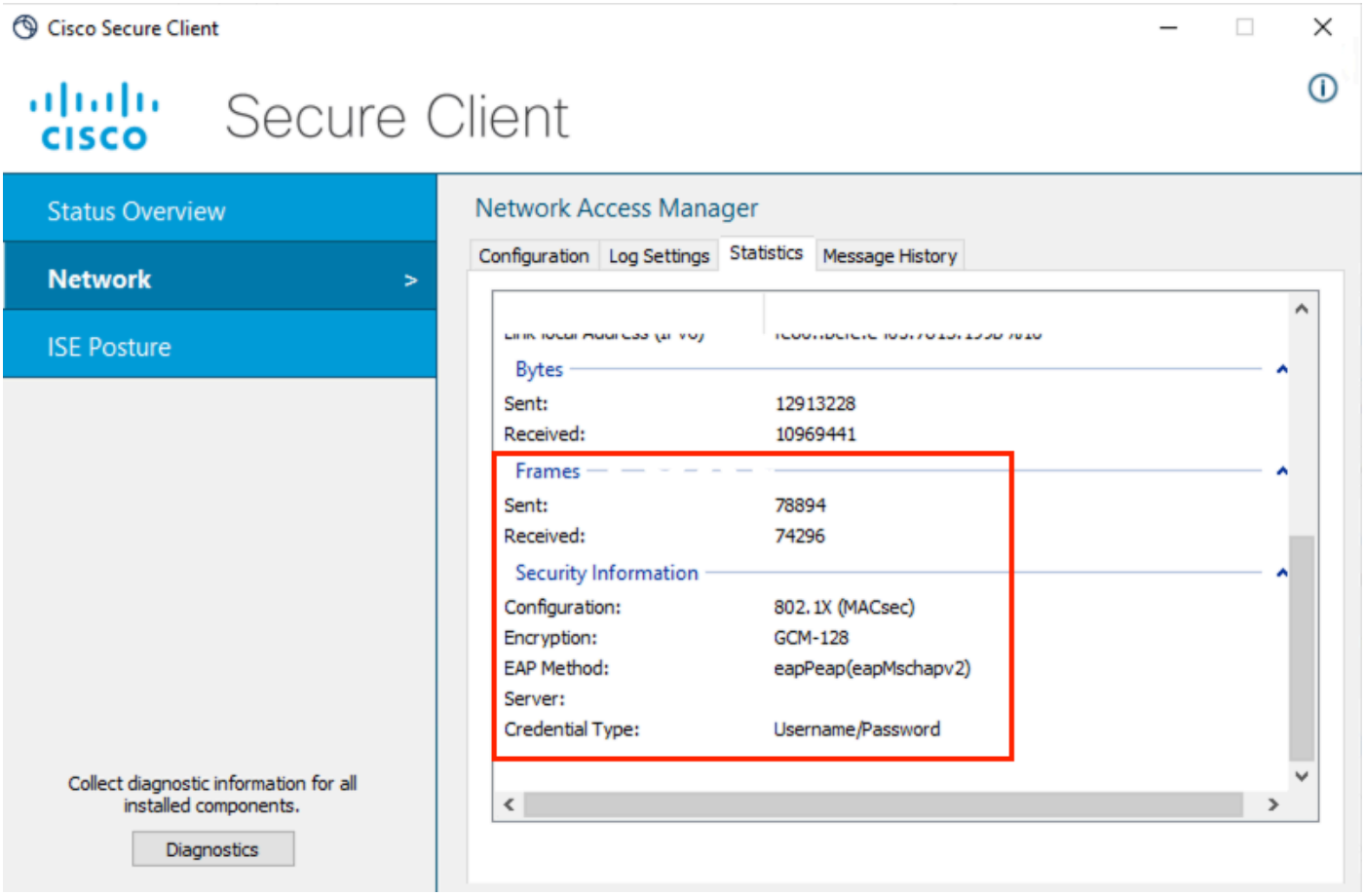
Validatie op een beveiligde client.

De verificatie is succesvol met het profiel dat is gemaakt met MACsec-codering. Als u op het motorpictogram klikt, kan meer informatie worden weergegeven.



In het menu dat hier wordt weergegeven voor de beveiligde client, in de sectie Network Access Manager > Statistics, ziet u de codering en de bijbehorende MACsec-configuratie.

De ontvangen en verzonden frames nemen toe naarmate de codering wordt uitgevoerd op laag 2.

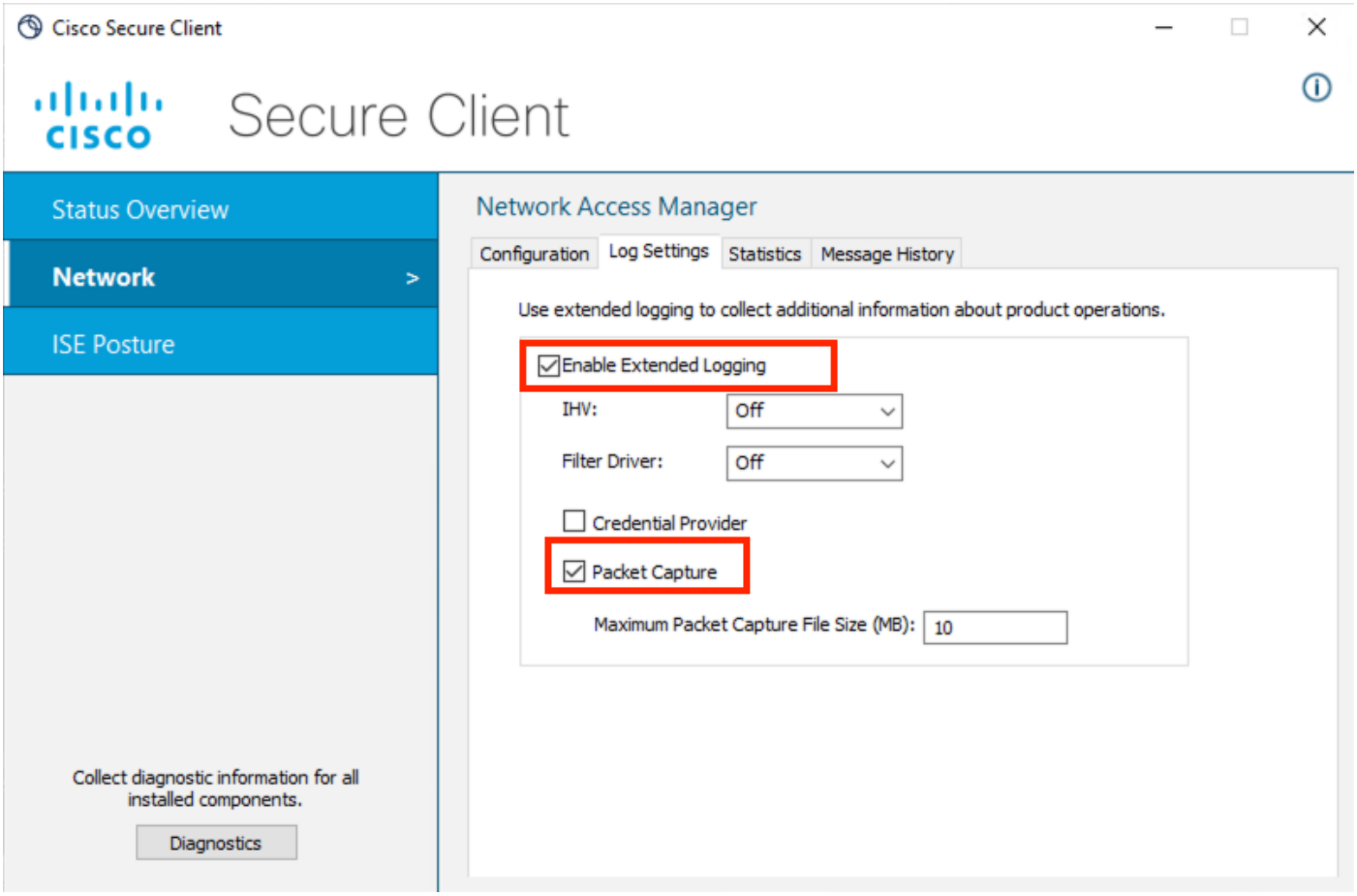


Problemen oplossen

Opmerking: Dit gedeelte behandelt het onderdeel voor probleemoplossing dat verband houdt met MKA-problemen die kunnen optreden. Als u te maken krijgt met een verificatie- of autorisatiefout, raadpleegt u de ISE Secure Wired Access Prescriptive Deployment Guide - Troubleshooting om dit te onderzoeken. In deze handleiding wordt ervan uitgegaan dat de verificaties goed werken zonder MACsec-codering.

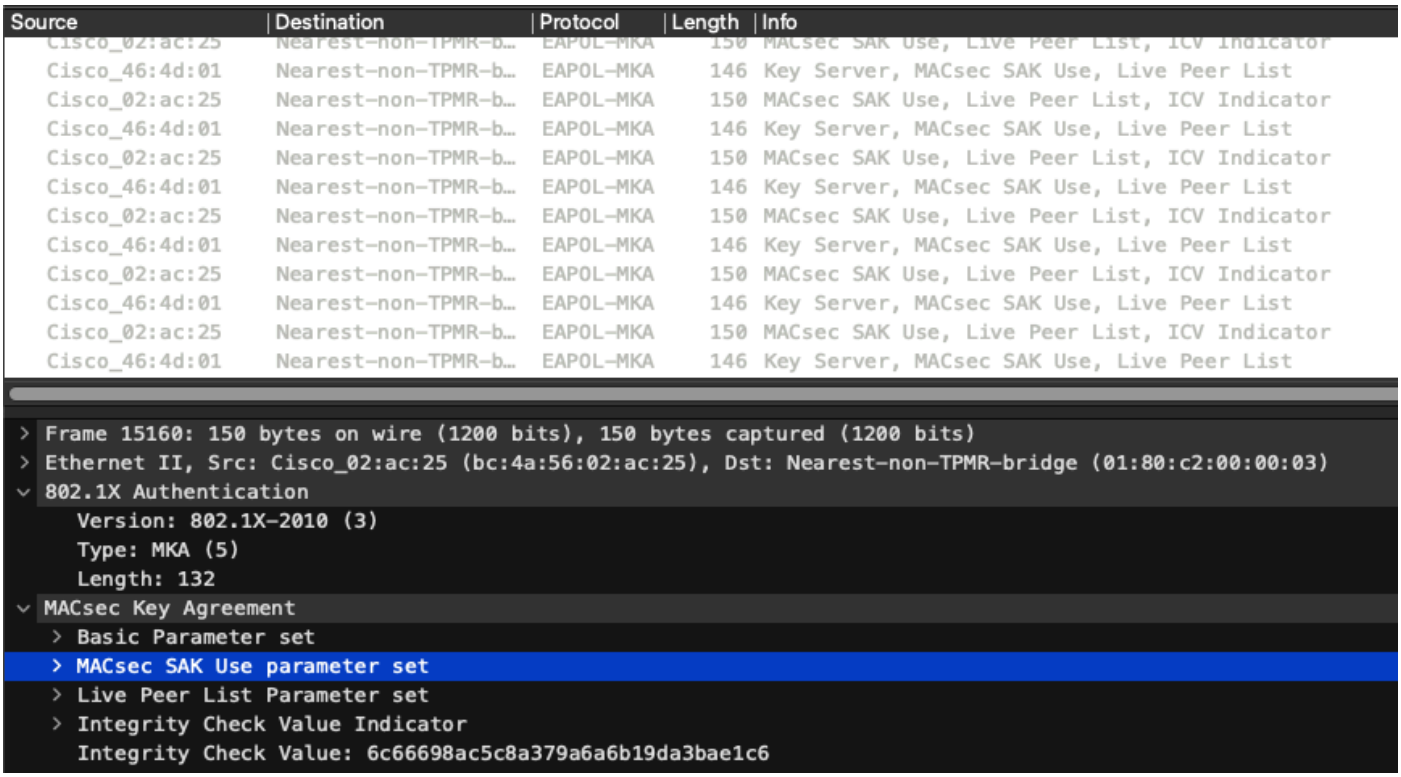
Cisco Secure Endpoint

- Schakel de DART-module in de Secure Endpoint-suite in.
- Schakel in dit menu Uitgebreide logboekregistratie in om meer gegevens over de MKA-verbinding van de gebruiker te verzamelen. U kunt ook een pakketopname inschakelen die deel uitmaakt van de DART-bundel.



- Verzamel DART-bundel om verder te gaan met de analyse van configuratie.xml en Network Access Manager. Raadpleeg de documentatie DART uitvoeren om gegevens te verzamelen voor probleemoplossing

In dit voorbeeld wordt weergegeven hoe de pakketten worden gezien als de informatie tussen de host en de switch wordt gecodeerd:



Vanuit de DART-bundel kunnen we nuttige informatie vinden voor de verificatie 802.1X en de MKA-sessie in het log met de naam NetworkAccessManager.txt.

Deze informatie wordt weergegeven in een geslaagde verificatie met MKA-codering.

```
%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 = AUTHENTICATI
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) staying in 802.1x state: AUTHENTICATING (dot1x_s
%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_
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: EAP (0) tlsAuthOnAuthEnd: successful authentication, save
%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.
%csc_nam-7-DEBUG_MSG: %[tid=9028]: EAP-CB: EAP status notification: session-id=1, handle=04B2DD44, stat
%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_p
%csc_nam-7-DEBUG_MSG: %[tid=2716]: EAP: ...received EapStatusEvent: session-id=1, EAP handle=04B2DD44,
%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 = AUTHENTICATE
%csc_nam-7-DEBUG_MSG: %[tid=9028][comp=SAE]: STATE (2) S_enterStateAux calling sm8Event8021x due to aut
%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 authenticati
%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 (portWo
%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 (po
%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 (po
%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_PACKE
%csc_nam-7-DEBUG_MSG: %[tid=8140][comp=SAE]: NET (0) CIMD Event: evtSeq#=0 msg=4 ifIndex=1 len=36 (cimd
%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-probleemoplossing

Deze commando's kunnen worden geïmplementeerd in het Network Access Device (NAD) om de MKA-codering tussen het platform en de aanvrager te bekijken.

Voor meer informatie over de opdrachten raadpleegt u de bijbehorende configuratiehandleiding van het platform dat als NAD wordt gebruikt.

```
#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
```

Dit zijn debugs van één succesvolle MKA-verbinding met een host. Je kunt dit gebruiken als referentie:

```
%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 th
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
%MKA-5-SESSION_START: (Te1/0/1 : 2) MKA Session started for RxSCI bc4a.5602.ac25/0000, AuditSessionID C
MKA-EVENT: Started a new MKA Session on interface TenGigabitEthernet1/0/1 for Peer MAC bc4a.5602.ac25 w
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 i
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, Ol
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 A
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 S
%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 indic
MKA-EVENT: Reqd to Install TX SA for CA 0x80007F30A6B46F20 AN 0 CKN 9F0DC198 - on int(TenGigabitEtherne
MKA-EVENT bc4a.5602.ac25/0000 EC000025: >> FSM - Install TxSA for CA with CKN 9F0DC198 on VP with SCI A
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, PREVIOUS
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, AuditSessi
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
```

Problemen oplossen met Identity Services Engine (ISE)

De probleemoplossing met betrekking tot deze functie is beperkt tot de levering van het cisco-av-pair attribuut linksec-policy=should-secure.

Zorg ervoor dat het autorisatieresultaat die informatie verzendt naar de Radius-sessie die is gekoppeld aan de switchpoorten waarop de apparaten worden aangesloten.

Voor verdere authenticatie-analyse van ISE raadpleegt u Problemen oplossen en Foutopsporingen inschakelen op ISE

Gemeenschappelijke problemen

Mismatch van versleuteling

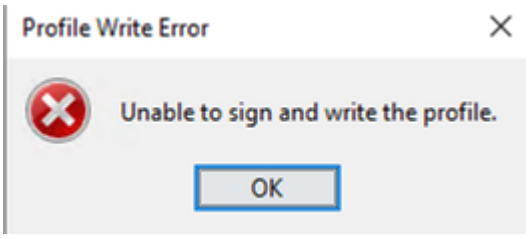
Deze log is te zien in de MKA debugs in de NAD.

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

Het eerste wat u in dit scenario moet controleren, is of de cijfers die zijn geconfigureerd in het MKA-beleid in de switch en in het profiel voor een beveiligd clientprofiel overeenkomen.

In het geval van AES-GCM-256-codering moet aan deze vereisten worden voldaan (per documentatie) Beheerdershandleiding voor Cisco Secure Client (inclusief AnyConnect), versie 5

Kan configuratie.xml niet opslaan.



Dit probleem met betrekking tot de schrijffout voor profielen wordt opgelost door de configuratie.xml (zoals eerder beschreven) met de naam Setup of MKA op te slaan met behulp van de profieleditor van Network Access Manager.

De fout is gerelateerd aan het feit dat het bestand configuratie.xml in gebruikt kan niet worden gewijzigd, Daarom, sla het bestand op een andere locatie om verder te gaan met de vervanging van de profielen.

Gerelateerde informatie

- MACsec-codering configureren
- MACsec-Switch configureren voor host met Cat9k & ISE

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.