# MKA mit Secure Client konfigurieren und Fehlerbehebung durchführen 5

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie die MACsec-Verschlüsselung auf einem Endgerät konfiguriert wird, wobei Secure Client 5 als Komponente verwendet wird.

### Voraussetzungen

Cisco empfiehlt Fachwissen in folgenden Bereichen:

- Identity Services Engine
- 802.1x und Radius
- MACsec-MKA-Verschlüsselung
- Secure Client Version 5 (ehemals AnyConnect)

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

### Hintergrundinformationen

MACSec (Media Access Control Security) ist ein Netzwerksicherheitsstandard, der Verschlüsselung und Schutz für Ethernet-Frames auf Layer 2 des OSI-Modells (Data Link) bietet, das durch den 802.1AE IEEE-Standard definiert ist.

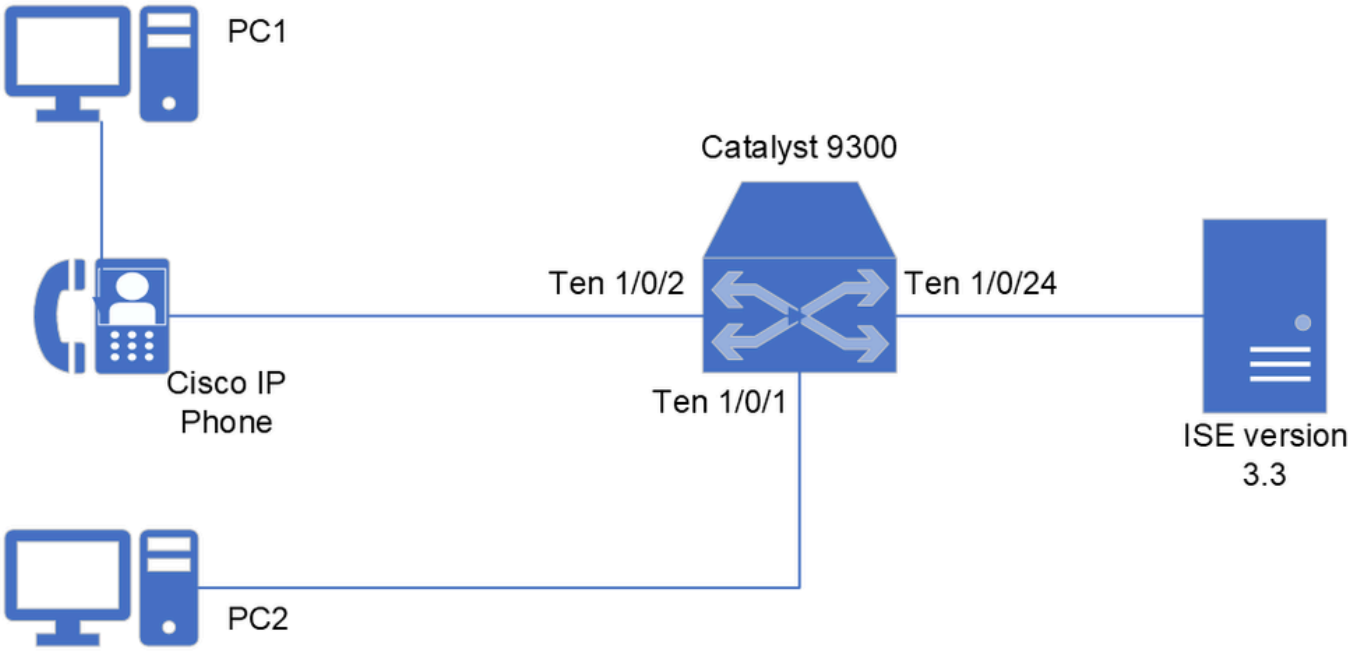
MACSec liefert diese Verschlüsselung in einer Punkt-zu-Punkt-Verbindung, die Switch-zu-Switch- oder Switch-zu-Host-Verbindungen sein kann, daher ist die Abdeckung dieses Standards auf kabelgebundene Verbindungen beschränkt.

Dieser Standard verschlüsselt die gesamten Daten mit Ausnahme der Quell- und Ziel-MAC-Adresse von Frames, die in einer Layer-2-Verbindung übertragen werden.

Das MACsec Key Agreement (MKA)-Protokoll ist der Mechanismus, über den MACsec-Peers die Sicherheitsschlüssel aushandeln, die zum Sichern der Verbindung erforderlich sind.

## Konfigurieren

### Netzwerkdiagramm




Anmerkung: In dieser Dokumentation wird berücksichtigt, dass Sie Regeln für die Radius-Authentifizierung für die PC-Geräte und das Cisco IP-Telefon konfiguriert haben. Informationen zum Einrichten einer neuen Konfiguration finden Sie im ISE Secure Wired Access Prescriptive Deployment Guide, um die Konfiguration in Identity Services Engine and Switch for Identity-Based Network Access zu überprüfen.

## Einrichtung von Richtlinien auf der ISE

Die erste Aufgabe besteht darin, die entsprechenden Autorisierungsprofile zu konfigurieren, die für beide PCs (sowie das Cisco IP-Telefon) angewendet werden, die im vorherigen Diagramm angezeigt werden.

In diesem hypothetischen Szenario verwenden die PCs das 802.1X-Protokoll als Authentifizierungsmethode, und das Cisco IP-Telefon verwendet MAB (Mac Address Bypass).

Die ISE kommuniziert mit dem Switch über das Radius-Protokoll über die Attribute, die der Switch in der Schnittstelle durchsetzen muss, von der aus der Endpunkt über eine Radius-Sitzung verbunden ist.

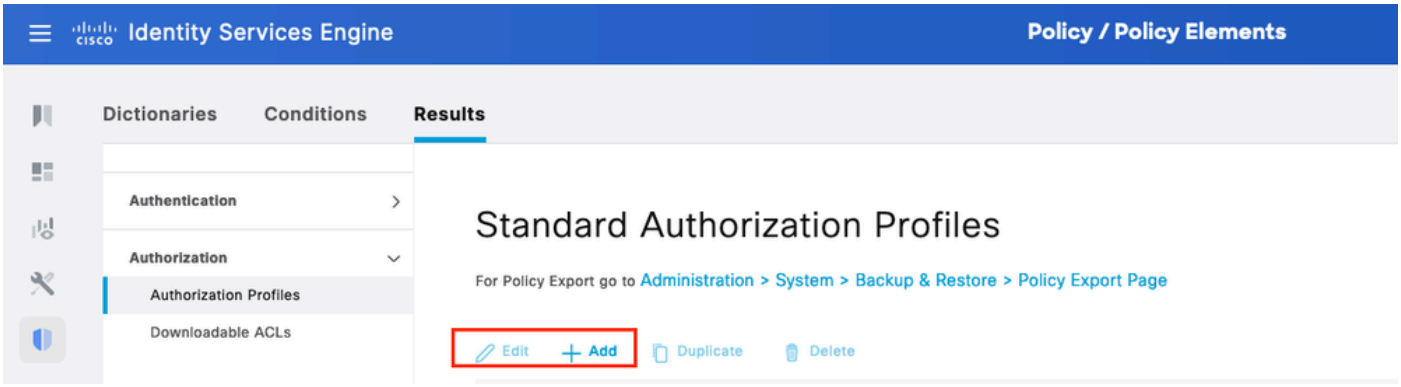
Für die MACsec-Verschlüsselung in Hosts ist das erforderliche Attribut cisco-av-pair = linksec-policy, das über die folgenden drei möglichen Werte verfügt:

- Sollte-nicht-sicher: Der Switch führt in der Schnittstelle, in der die Radius-Sitzung stattfindet, keine MKA-Verschlüsselung durch.
- Sicherheit ist unverzichtbar: Der Switch muss die Verschlüsselung für den Datenverkehr durchsetzen, der mit der Radius-Sitzung verknüpft ist. Wenn die MKA-Sitzung fehlschlägt (oder eine Zeitüberschreitung aufweist), wird die Verbindung als Autorisierungsfehler betrachtet, und es wird erneut versucht, die MKA-Sitzung herzustellen.
- Soll-sicher: Der Switch versucht, eine MKA-Verschlüsselung durchzuführen. Wenn die mit der Radius-Sitzung verknüpfte MKA-Sitzung erfolgreich ist, wird der Datenverkehr verschlüsselt. Wenn der MKA ausfällt oder eine Zeitüberschreitung auftritt, lässt der Switch den unverschlüsselten Datenverkehr zu, der mit dieser Radius-Sitzung verknüpft ist.

Schritt 1. Setzen Sie auf beiden PCs eine sichere MKA-Richtlinie durch, um flexibel zu sein, falls ein Computer ohne MKA-Funktionen eine Verbindung mit der Schnittstelle Ten 1/0/1 herstellt.

Optional können Sie eine Richtlinie für PC2 konfigurieren, die eine Richtlinie erzwingt, die ein Muss enthält.

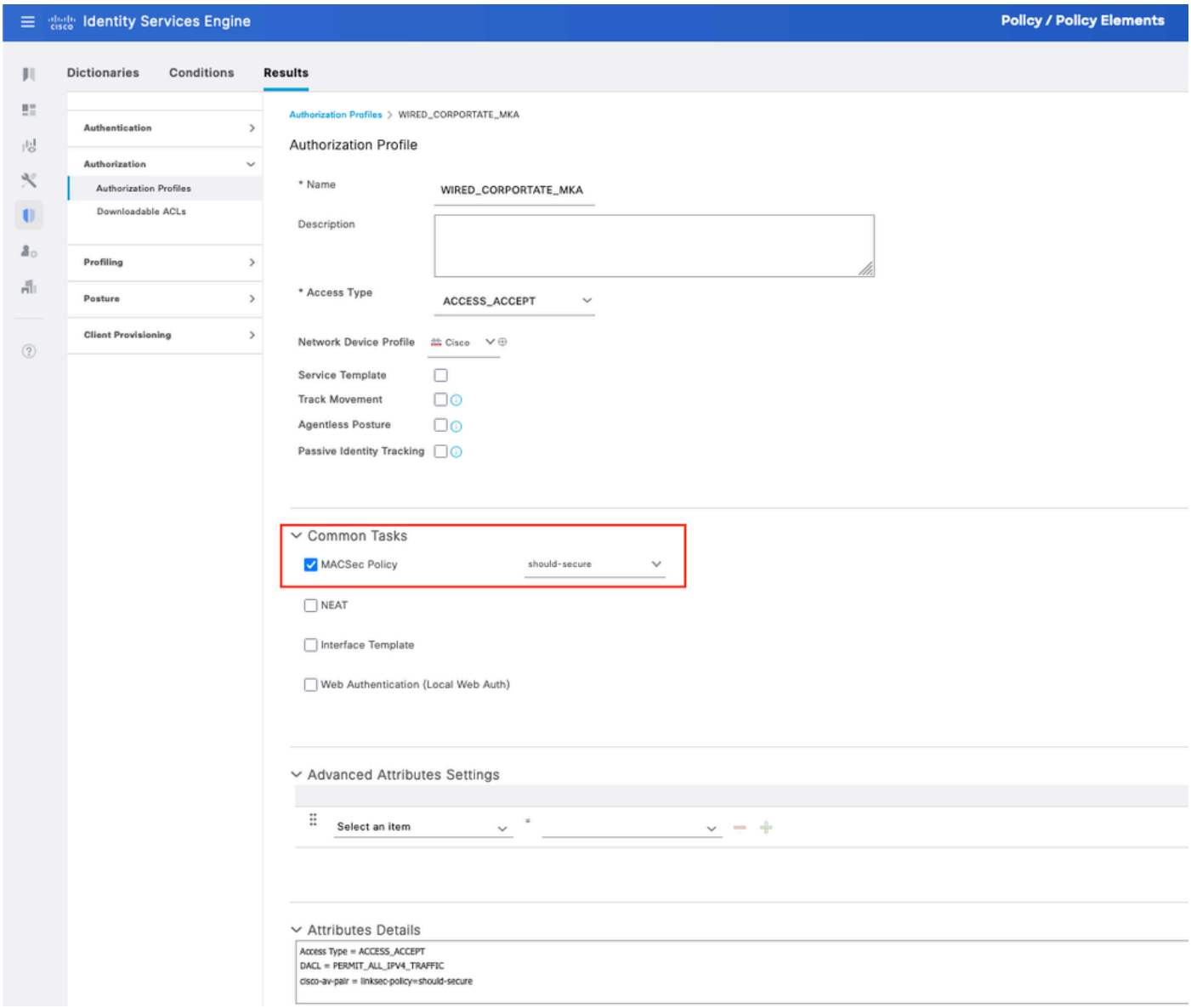
Konfigurieren Sie in diesem Beispiel die Richtlinie für die PCs wie unter Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierungsprofile, und klicken Sie dann auf +Vorhandenes Profil hinzufügen oder bearbeiten




Schritt 2. Füllen Sie die für das Profil erforderlichen Felder aus, oder passen Sie sie an.

Stellen Sie sicher, dass Sie in Allgemeine Aufgaben MACSec-Richtlinie und die entsprechende anzuwendende Richtlinie ausgewählt haben.

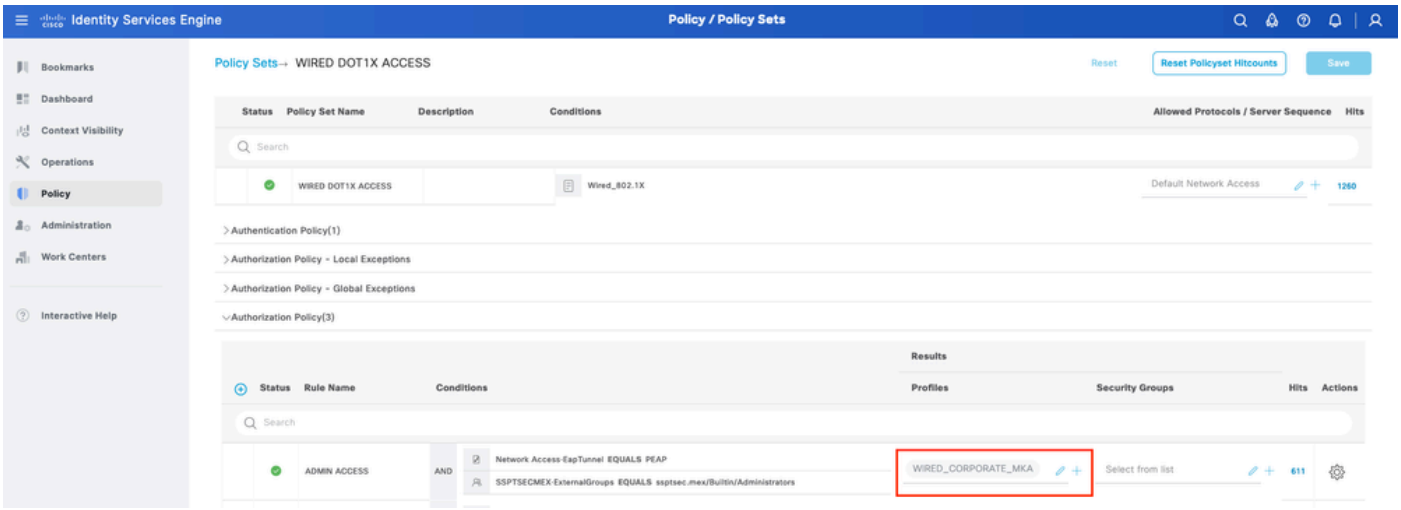
Blättern Sie nach unten, und speichern Sie die Konfiguration.




Schritt 3: Weisen Sie den Autorisierungsregeln, die von den Geräten betroffen sind, das entsprechende Autorisierungsprofil zu.

Navigieren Sie zu Policy > Policy Sets > (Select Policy Set assigned) > Authorization Policy.

Ordnen Sie die Autorisierungsregel dem Autorisierungsprofil MACsec-Einstellungen zu. Blättern Sie nach unten, und speichern Sie Ihre Konfiguration.




## Einrichtung von MKA in Catalyst 9300

Schritt 1. Konfigurieren Sie eine neue MKA-Richtlinie, wie in diesem Beispiel vorgeschlagen:

```
!
  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
!
```

Schritt 2: Aktivieren Sie die MACsec-Verschlüsselung an der Schnittstelle, an der die PCs angeschlossen sind.

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

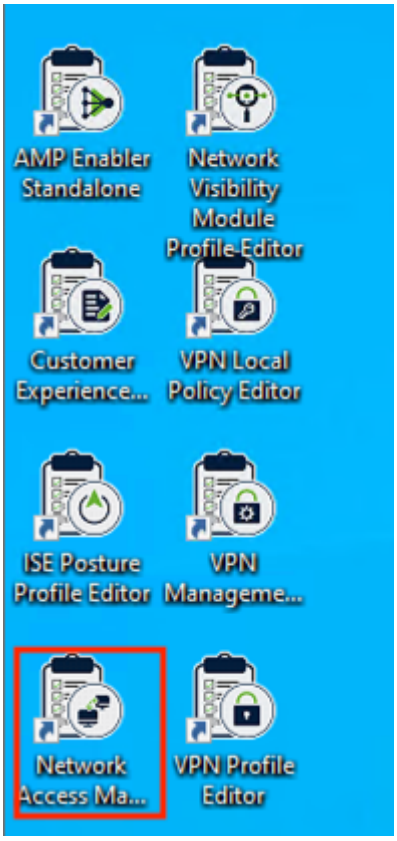
Anmerkung: Weitere Informationen zu den Befehlen und Optionen in der MKA-Konfiguration finden Sie im Security Configuration Guide

(Sicherheitskonfigurationshandbuch), das der verwendeten Switch-Version entspricht. In diesem Szenario für dieses Beispiel: Security Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches)

## Einrichtung von MKA mit dem Network Access Manager Profile Editor.

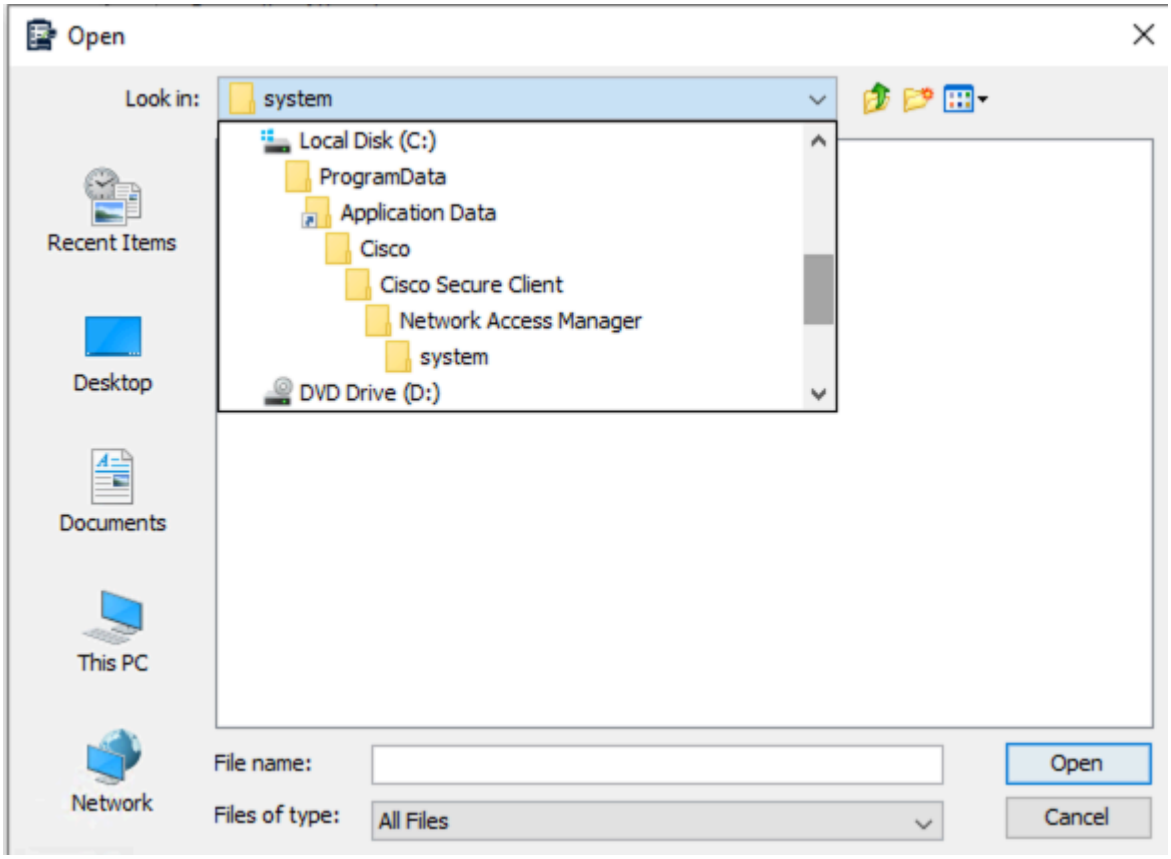
Schritt 1: Laden Sie den Editor herunter (von der Download-Website von Cisco), und öffnen Sie den Profil-Editor, der mit der verwendeten Version des sicheren Clients übereinstimmt.

Sobald Sie dieses Programm auf Ihrem Computer installiert haben, öffnen Sie den Cisco Secure Client Profile Editor - Network Access Manager.

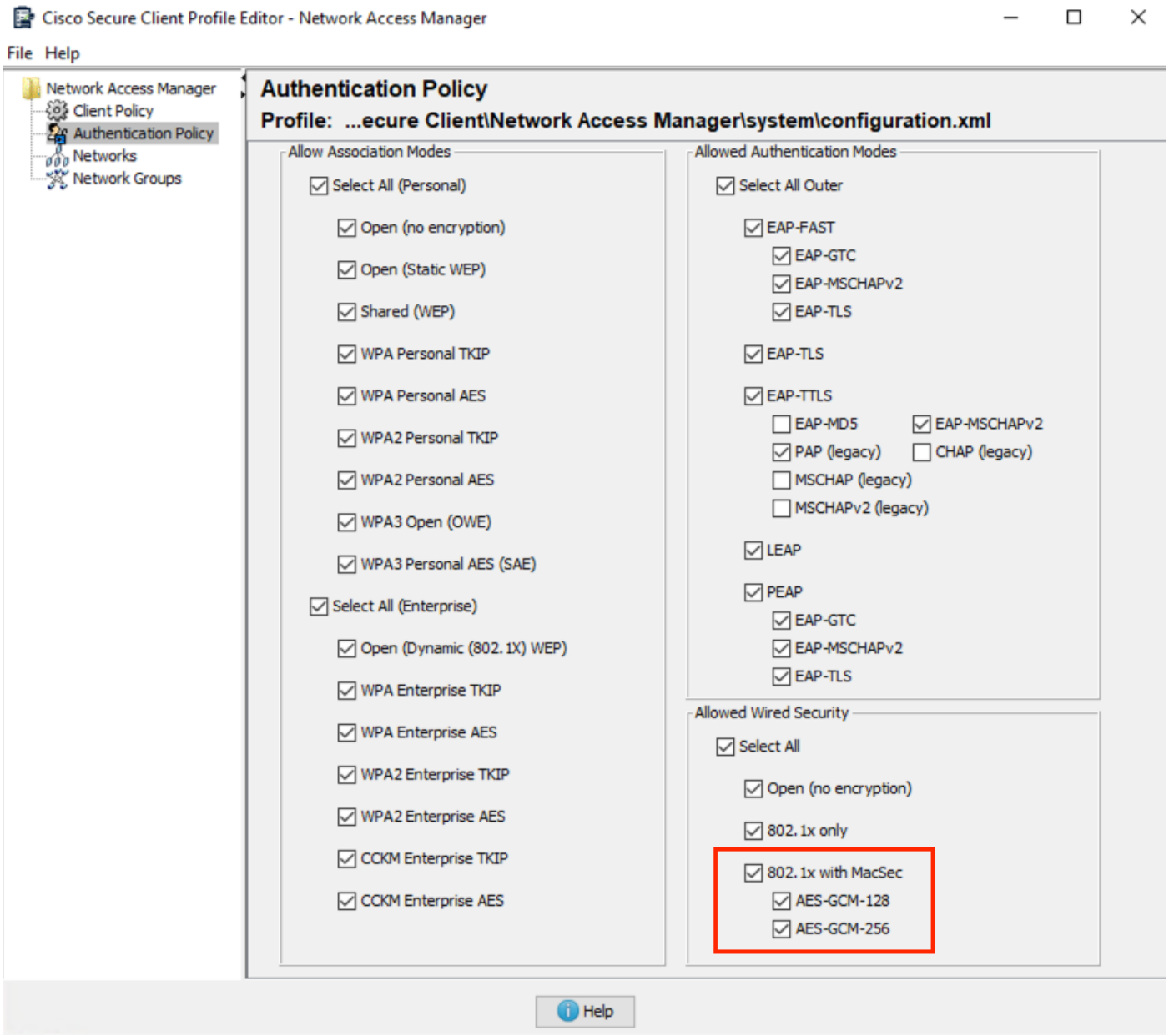



Schritt 2. Wählen Sie Datei > Öffnen aus.


Schritt 3. Wählen Sie das Ordnersystem, das in diesem Bild angezeigt wird. Öffnen Sie in diesem Ordner die Datei configuration.xml.

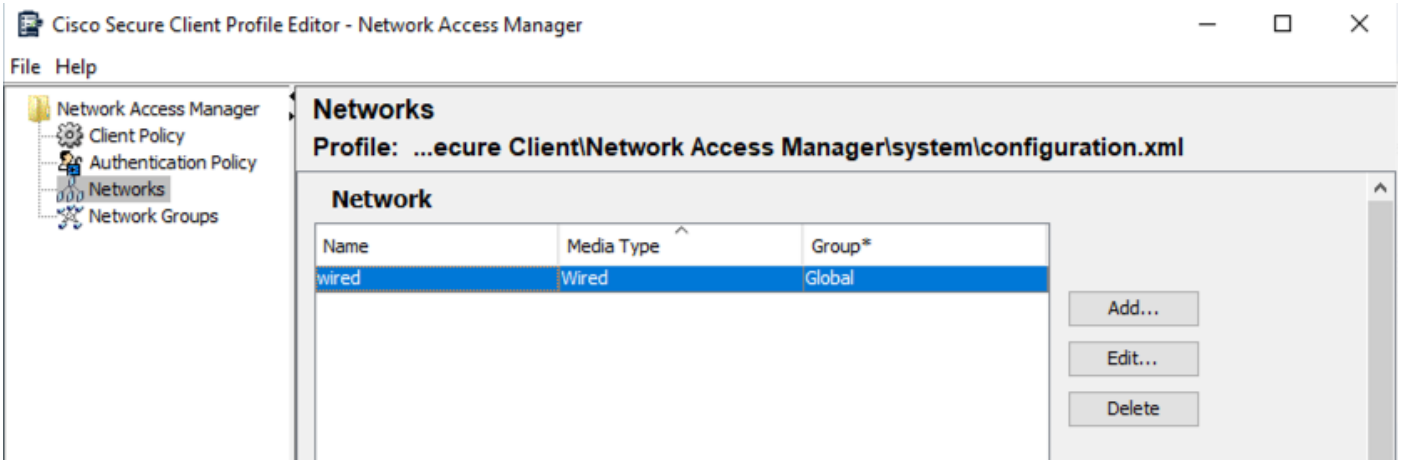



Schritt 4. Nachdem die Datei vom Profil-Editor geladen wurde, wählen Sie die Option "Authentifizierungsrichtlinie" aus, und stellen Sie sicher, dass die Option für 802.1x mit MACSec aktiviert ist.



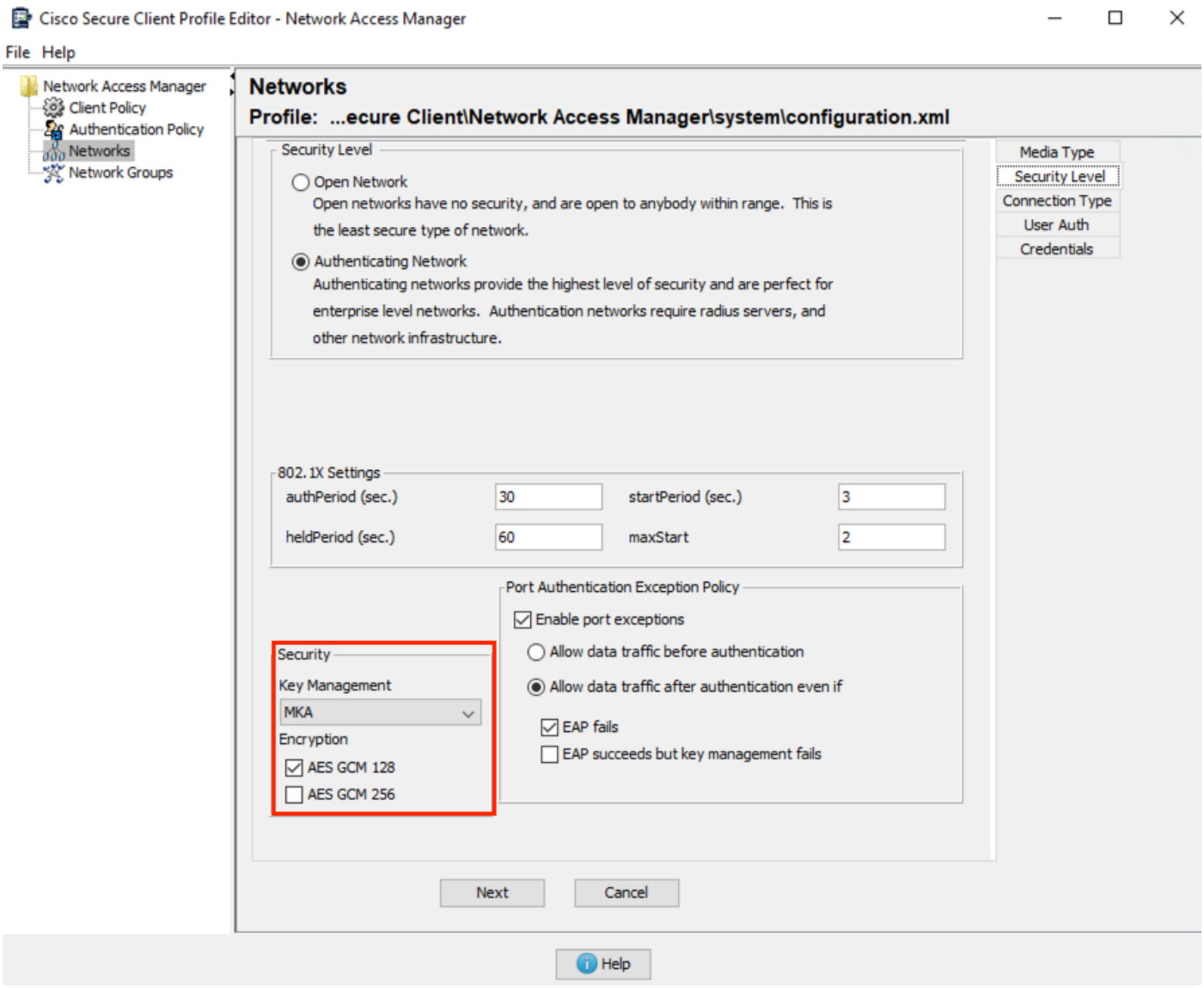

Schritt 5. Fahren Sie mit dem Abschnitt Netzwerke fort. In diesem Teil können Sie ein neues Profil für eine Kabelverbindung hinzufügen oder das mit Secure Client 5.0 installierte Standardprofil bearbeiten.

In diesem Szenario bearbeiten Sie das vorhandene Kabelprofil.




Schritt 6: Konfigurieren des Profils Passen Sie im Abschnitt Sicherheitsstufe die Schlüsselverwaltung an, sodass MKA gefolgt von einer Verschlüsselung AES GCM 128 verwendet wird.

Passen Sie auch die anderen Parameter für die dot1x-Authentifizierung und die Richtlinien an.

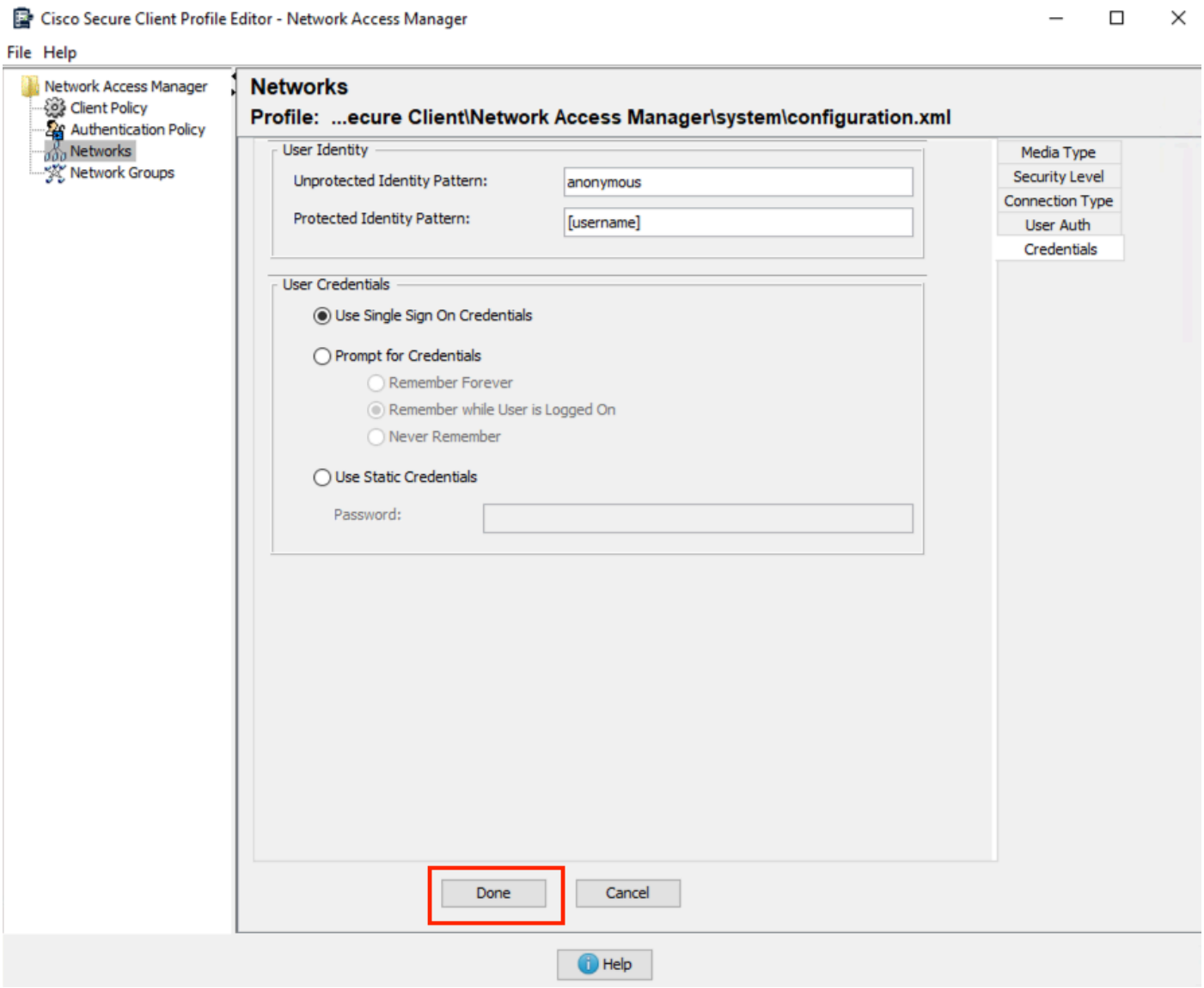


Schritt 7. Konfigurieren Sie die verbleibenden Abschnitte zu Verbindungstyp, Benutzerauthentifizierung und Anmeldeinformationen.

Diese Abschnitte unterscheiden sich je nach den im Abschnitt Sicherheitsstufe ausgewählten Authentifizierungseinstellungen.

Wenn Sie die Konfigurationen abgeschlossen haben, klicken Sie auf Fertig.

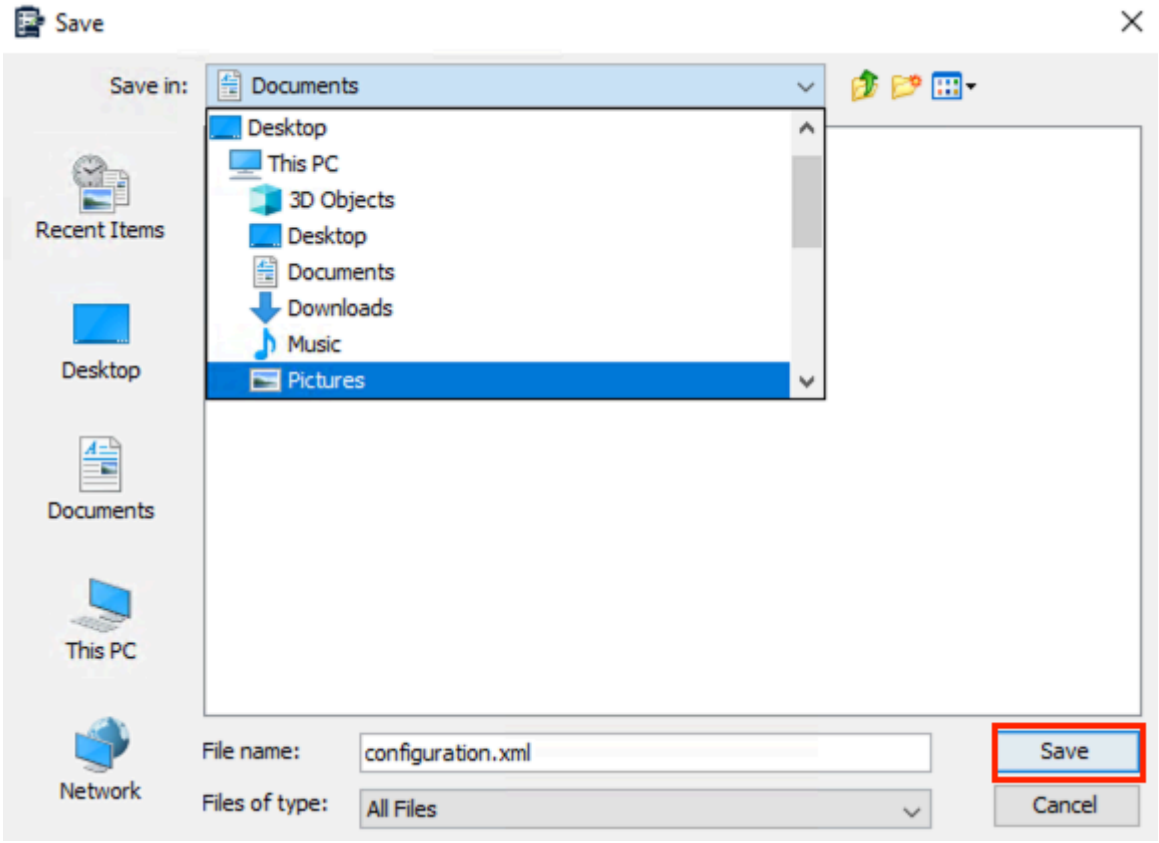
Für dieses Szenario wird das Protected Extensible Authentication Protocol (PEAP) mit Benutzeranmeldeinformationen verwendet.




Schritt 8. Navigieren Sie zum Menü Datei. Fahren Sie mit der Option Speichern unter fort.

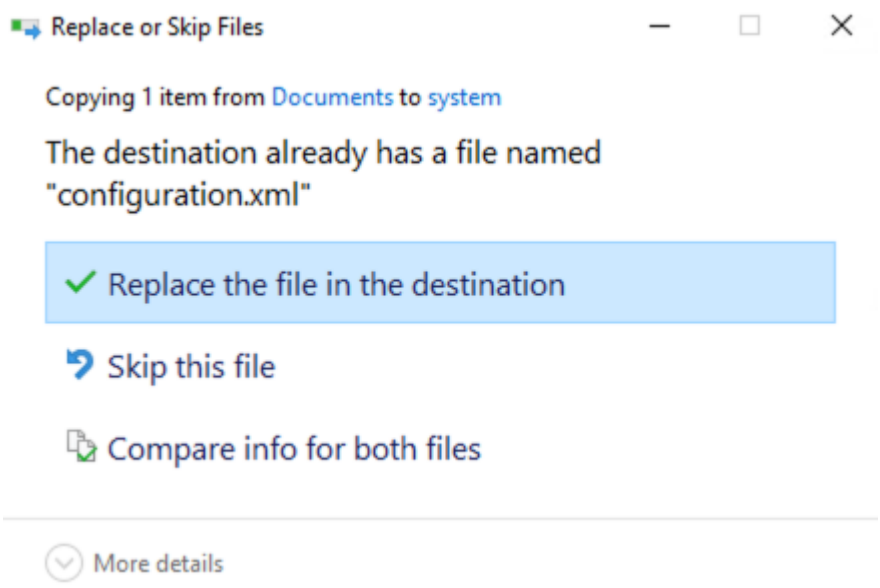
Geben Sie der Datei den Namen configuration.xml, und speichern Sie sie in einem anderen Ordner als ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system.

In diesem Beispiel wurde die Datei im Ordner Dokumente gespeichert. Speichern Sie das Profil.




Schritt 8. Fahren Sie mit dem Profilspeicherort fort, kopieren Sie die Datei, und ersetzen Sie die Datei im Ordner ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system.

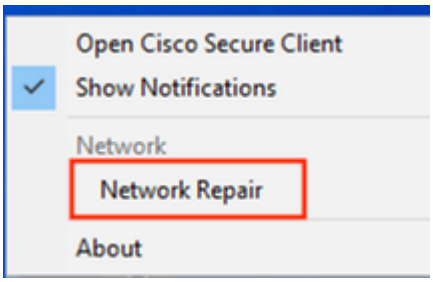
Wählen Sie die Option Datei im Ziel ersetzen aus.




Schritt 9. Klicken Sie mit der rechten Maustaste auf das Symbol Sicherer Client in der unteren

rechten Taskleiste Ihres Windows-Computers, um das in Security Client 5.0 geänderte Profil zu laden.

Führen Sie eine Netzwerkreparatur durch.

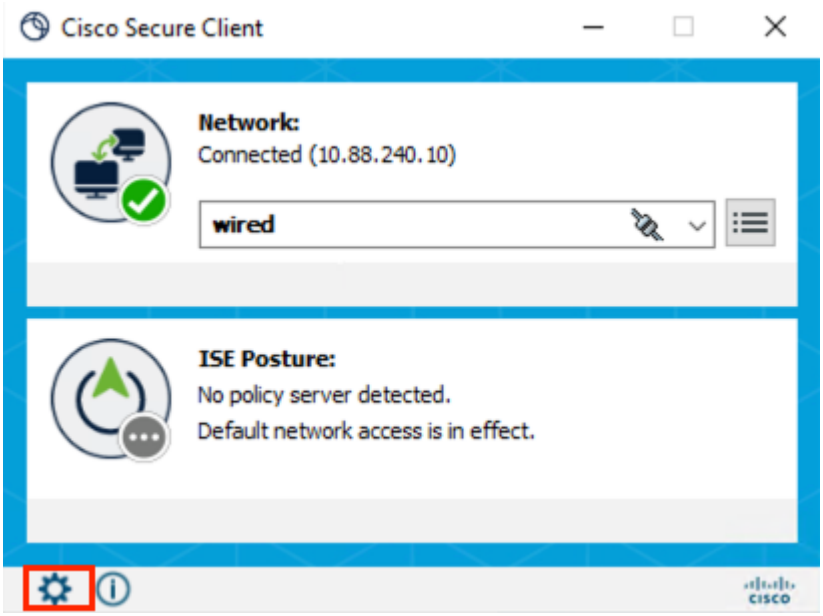



Anmerkung: Alle Netzwerke, die über den Profil-Editor konfiguriert wurden, haben die Berechtigungen "Administrator Network". Daher können die Benutzer den Inhalt, den Sie mit diesem Tool konfiguriert haben, nicht anpassen/ändern.

## Einrichtung von MKA-Netzwerken mit Network Access Manager (optional).

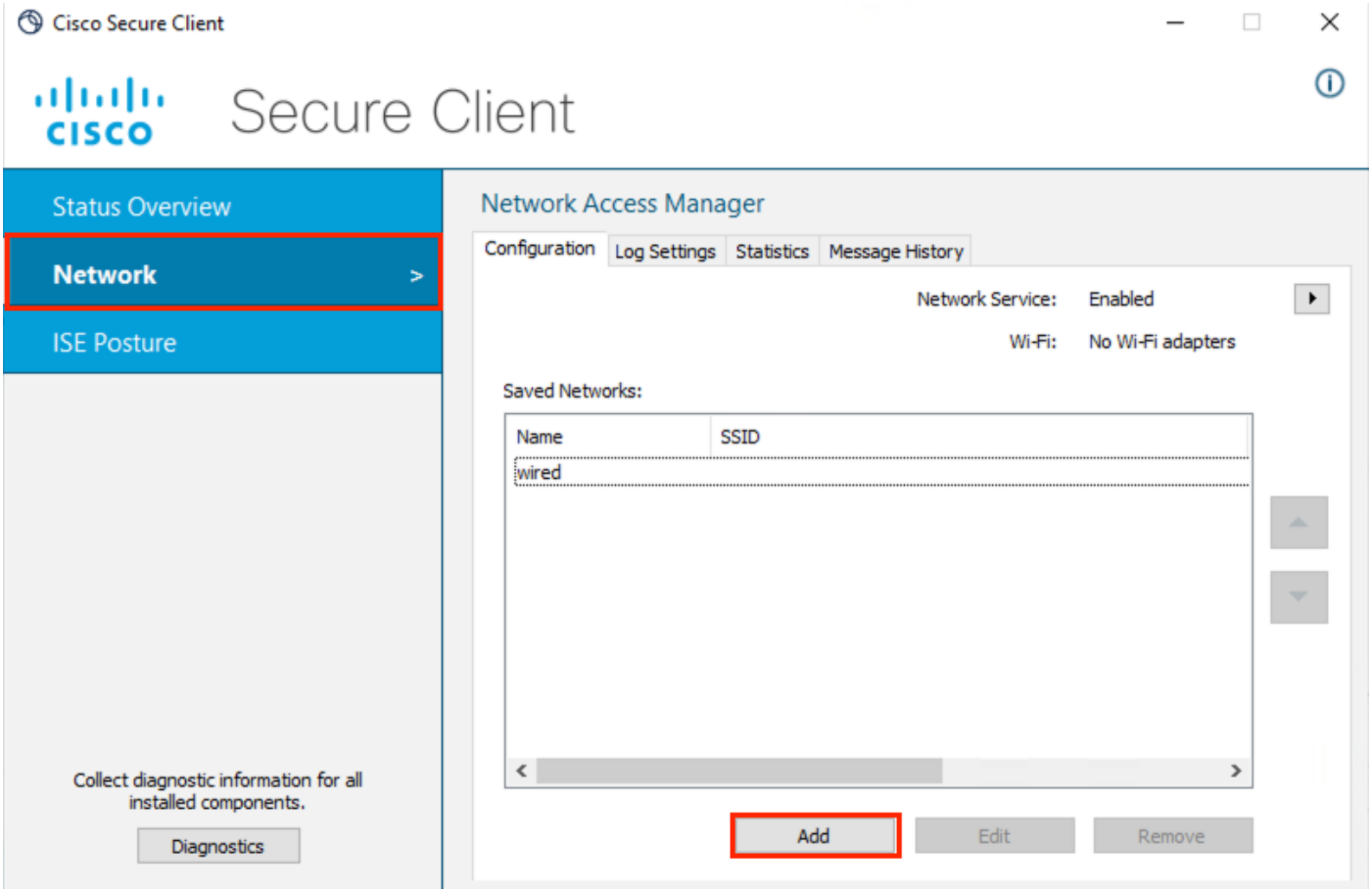
Schritt 1: Als Alternative zur MKA-Einrichtung mit dem Profil-Editor können Sie Netzwerke ohne Verwendung dieses Tools hinzufügen.

Wählen Sie in der Secure Client Suite das Zahnrad-Symbol aus.



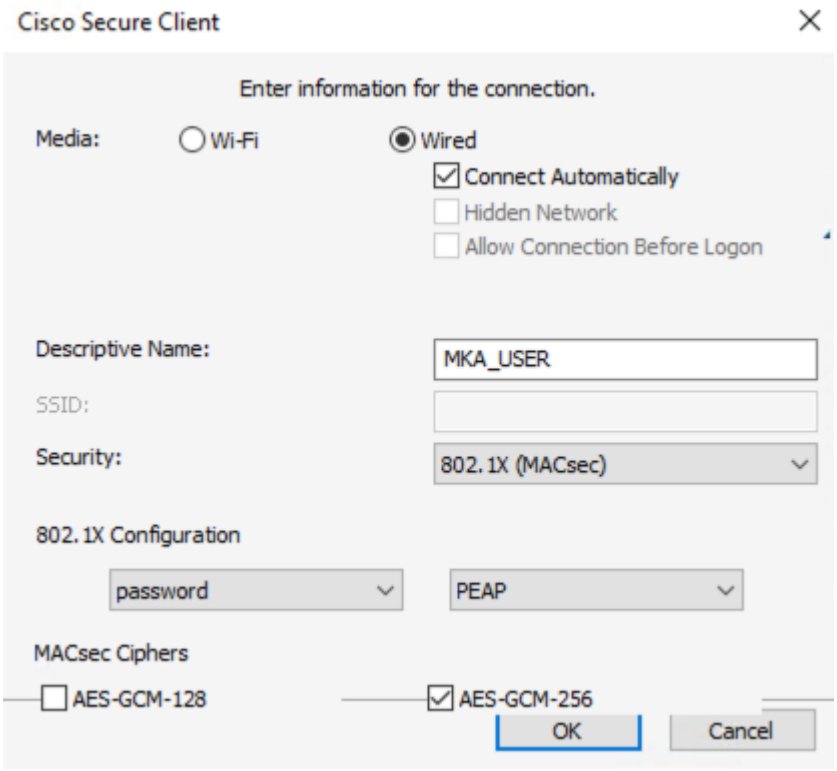

Schritt 2. Wählen Sie im neuen Fenster die Option Netzwerk.

Wählen Sie im Abschnitt "Konfiguration" die Option Hinzufügen aus, um einen Netzwerk-MKA einzugeben, der über die Berechtigungen User Network (Benutzernetzwerk) verfügt.




Schritt 3: Richten Sie im neuen Konfigurationsfenster die Merkmale der Verbindung ein, und geben Sie dem Netzwerk einen Namen.

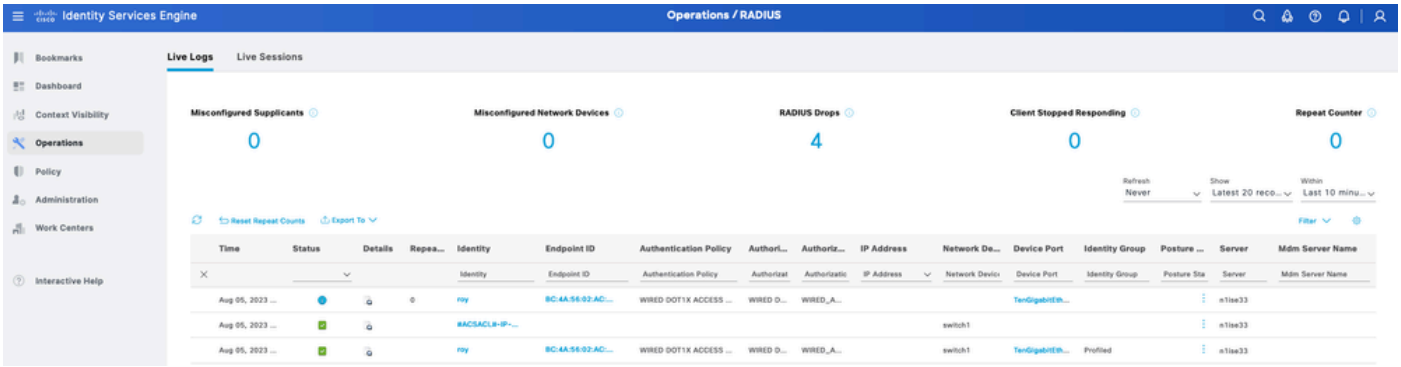
Wenn Sie fertig sind, wählen Sie die Schaltfläche OK.




# Überprüfung

## Validierung auf der ISE

Beachten Sie bei der ISE nach Abschluss der Konfiguration dieses Datenflusses, dass das Gerät authentifiziert und in Livelogs autorisiert wurde.




Navigieren Sie im Abschnitt Details der Authentifizierung und im Abschnitt Result (Ergebnis).

Die im Autorisierungsprofil festgelegten Attribute werden an das Netzwerkzugriffsgerät (Network Access Device, NAD) gesendet sowie die Nutzung einer Essential-Lizenz.

| | |
|---|---|
| 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. |

## Validierung auf dem Catalyst Switch

Diese Befehle können verwendet werden, um die ordnungsgemäße Funktion dieser Lösung zu überprüfen.

```
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
```

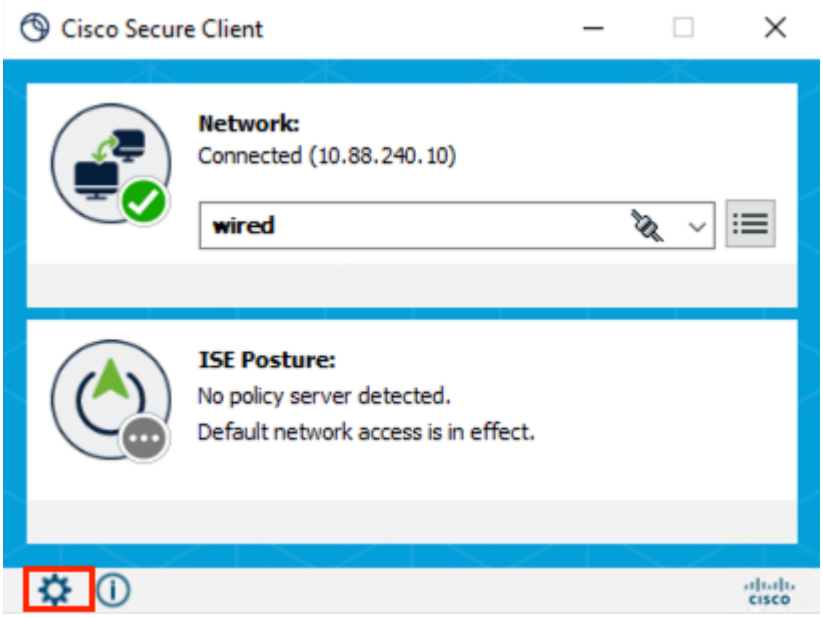
```
switch1#show mka session

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
```

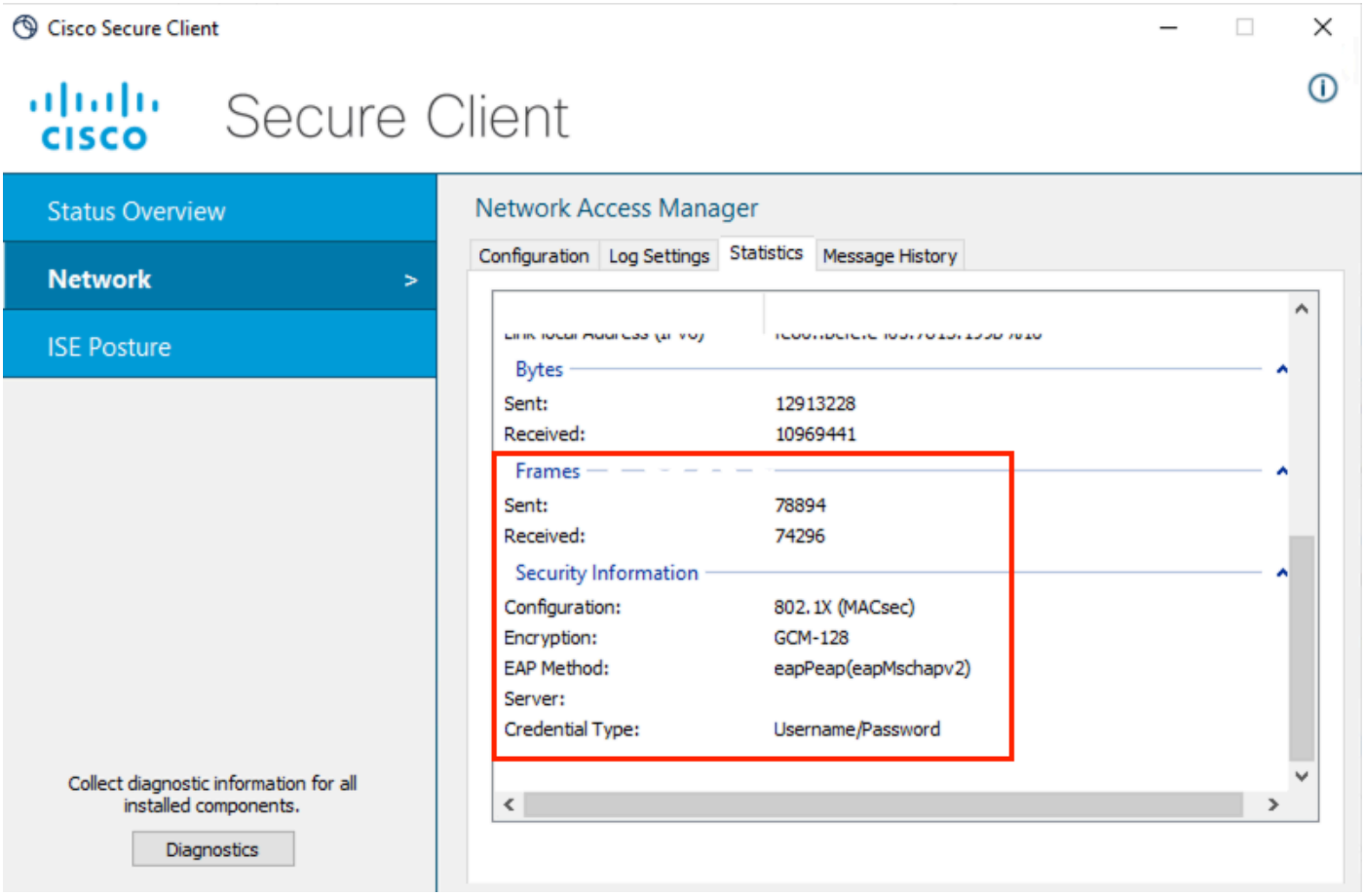
## Validierung auf sicherem Client

Die Authentifizierung ist mit dem Profil erfolgreich, das mit MACsec-Verschlüsselung erstellt wurde. Wenn Sie auf das Motorsymbol klicken, können weitere Informationen angezeigt werden.




Beachten Sie im hier angezeigten Menü für den sicheren Client im Abschnitt Netzwerkzugriffs-Manager > Statistiken die Verschlüsselung und die entsprechende MACsec-Konfiguration.

Die empfangenen und gesendeten Frames nehmen mit der Verschlüsselung auf Layer 2 zu.

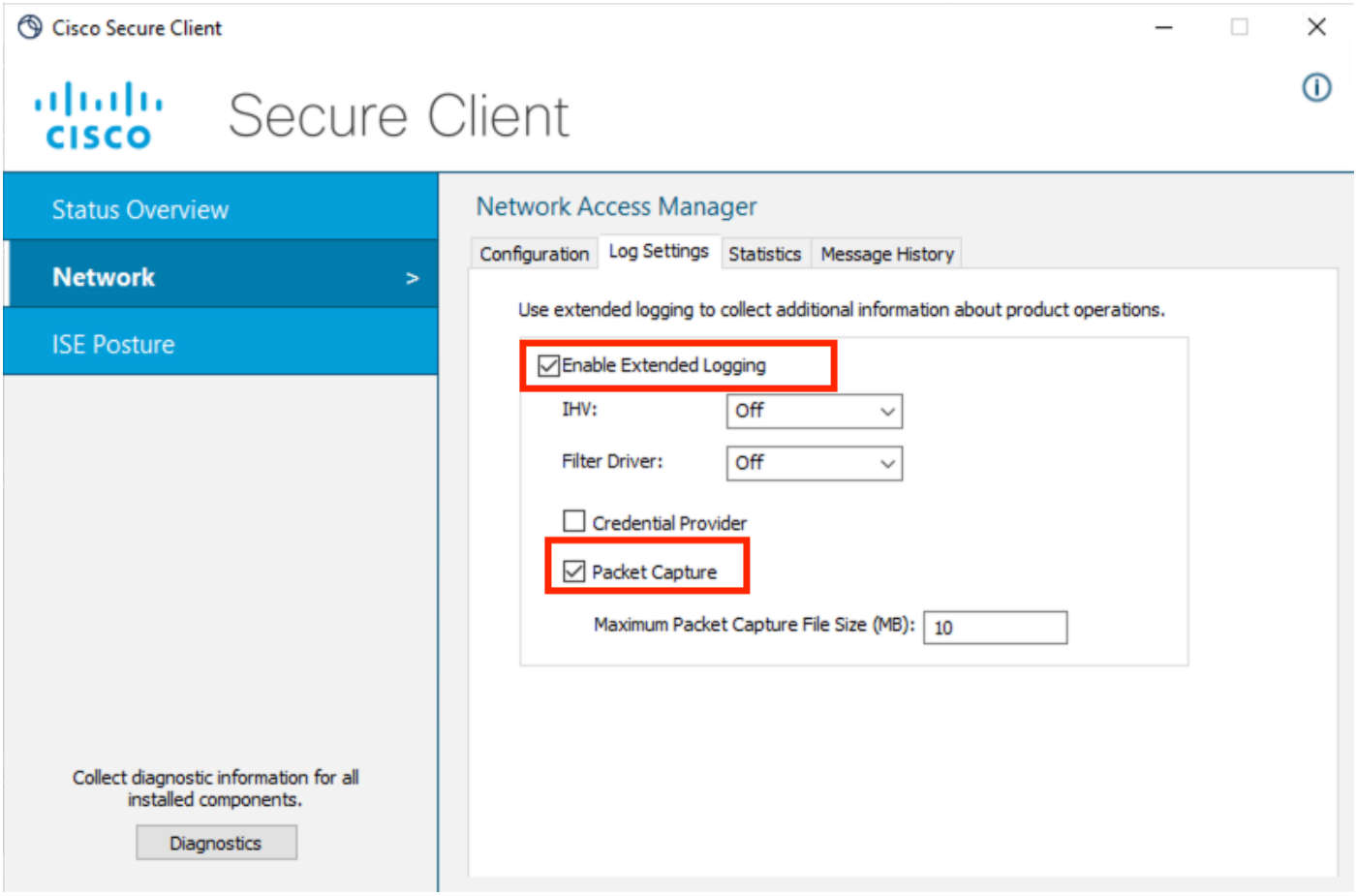



# Fehlerbehebung

Anmerkung: Dieser Abschnitt behandelt den Teil der Fehlerbehebung, der sich auf MKA-Probleme bezieht, die auftreten können. Wenn bei der Authentifizierung oder Autorisierung ein Fehler auftritt, finden Sie weitere Informationen im ISE Secure Wired Access Prescriptive Deployment Guide - Troubleshooting (ISE-Leitfaden für sichere kabelgebundene Zugriffsberechtigungen - Fehlerbehebung). In diesem Leitfaden wird davon ausgegangen, dass die Authentifizierungen ohne MACsec-Verschlüsselung einwandfrei funktionieren.

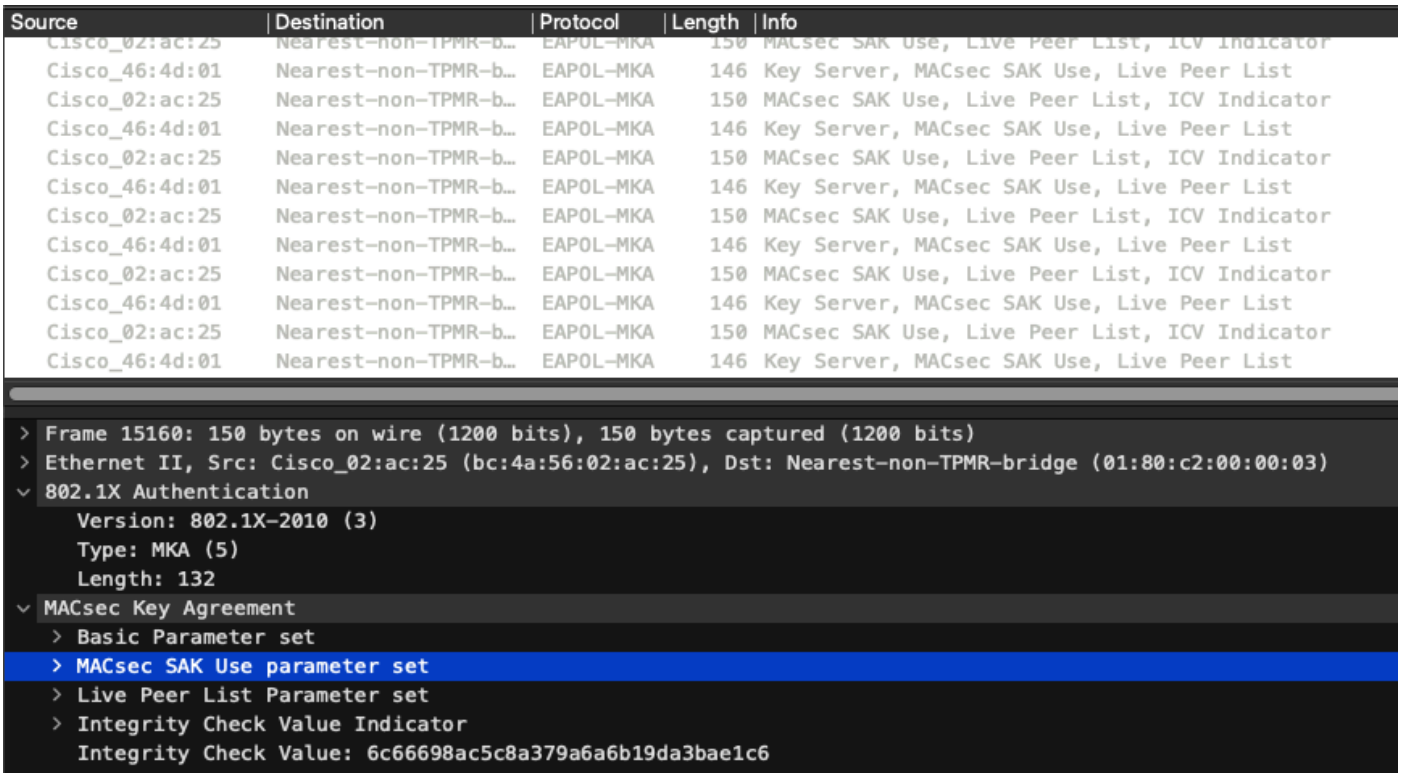
## Sichere Endgeräte von Cisco

- Aktivieren Sie das DART-Modul in der Secure Endpoint Suite.
- Aktivieren Sie in diesem Menü die erweiterte Protokollierung, um weitere Daten über die MKA-Benutzerverbindung zu sammeln. Sie können auch eine Paketerfassung aktivieren, die im DART-Paket enthalten ist.




- Sammeln Sie das DART-Paket, um mit der Analyse von configuration.xml und Network Access Manager fortzufahren. Informationen zur Fehlerbehebung finden Sie in der Dokumentation Ausführen von DART

Dieses Beispiel zeigt, wie die Pakete als Informationen zwischen dem Host und dem Switch angesehen werden:




Im DART-Paket finden wir nützliche Informationen für die 802.1X-Authentifizierung und die MKA-Sitzung im Protokoll NetworkAccessManager.txt.

Diese Informationen werden in einer erfolgreichen Authentifizierung mit MKA-Verschlüsselung angezeigt.

```
%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 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 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-Fehlerbehebung

Diese Befehle können im Network Access Device (NAD) implementiert werden, um die MKA-Verschlüsselung zwischen der Plattform und dem Supplicant zu überprüfen.

Weitere Informationen zu den Befehlen finden Sie im entsprechenden Konfigurationsleitfaden für die als NAD verwendete Plattform.

```
#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
```

Dies sind Debugs einer erfolgreichen MKA-Verbindung zu einem Host. Sie können dies als Referenz verwenden:

```
%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 A
%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
```

### Identity Services Engine (ISE) - Fehlerbehebung

Die Fehlerbehebung im Zusammenhang mit dieser Funktion ist auf die Bereitstellung des cisco-av-pair-Attributs linksec-policy=should-secure beschränkt.

Stellen Sie sicher, dass das Autorisierungsergebnis diese Informationen an die Radius-Sitzung sendet, die mit den Switch-Ports verbunden ist, an die die Geräte angeschlossen werden.

Weitere Informationen zur Authentifizierungsanalyse für ISE finden Sie unter Problembehandlung und Aktivieren von Debugs für ISE.

## Häufige Probleme

### Cipher Mismatch

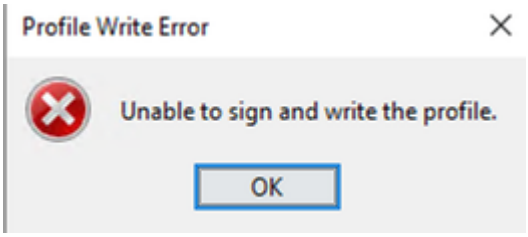
Dieses Protokoll ist in den MKA-Debugs im NAD zu sehen.

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

In diesem Szenario müssen Sie zunächst überprüfen, ob die in der MKA-Richtlinie im Switch und im Secure Client-Profil konfigurierten Chiffren übereinstimmen.

Für die AES-GCM-256-Verschlüsselung müssen diese Anforderungen (gemäß Dokumentation) erfüllt werden. Cisco Secure Client (einschließlich AnyConnect) Administratorhandbuch, Version 5

### Die Datei configuration.xml kann nicht gespeichert werden.



Dieses Problem im Zusammenhang mit Profile Write Error wird durch das Speichern der Datei configuration.xml (wie zuvor beschrieben) Setup von MKA mit Network Access Manager Profile Editor gelöst.

Der Fehler ist darauf zurückzuführen, dass die Datei configuration.xml in verwendet nicht geändert werden kann. Speichern Sie die Datei daher an einem anderen Speicherort, um mit dem Ersetzen der Profile fortzufahren.

## Zugehörige Informationen

- Konfigurieren der MACsec-Verschlüsselung
- Konfigurieren des MACsec-Switches für den Host mit Cat9k und ISE

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.