使用安全客戶端5配置MKA並對其進行故障排除

目錄

簡介

本文檔介紹如何使用Secure Client 5作為請求方在終端中配置MACsec加密。

必要條件

思科建議瞭解以下主題：

- 身分識別服務引擎
- 802.1x和Radius

- MACsec MKA加密
- 安全客戶端版本5（以前稱為Anyconnect）

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎 (ISE) 3.3 版
- Catalyst 9300版本17.06.05
- 思科安全使用者端5.0.4032

背景資訊

MACSec（媒體存取控制安全）是一種網路安全標準，為OSI模型（資料連結）第2層的乙太網路訊框提供加密和保護（由802.1AE IEEE標準定義）。

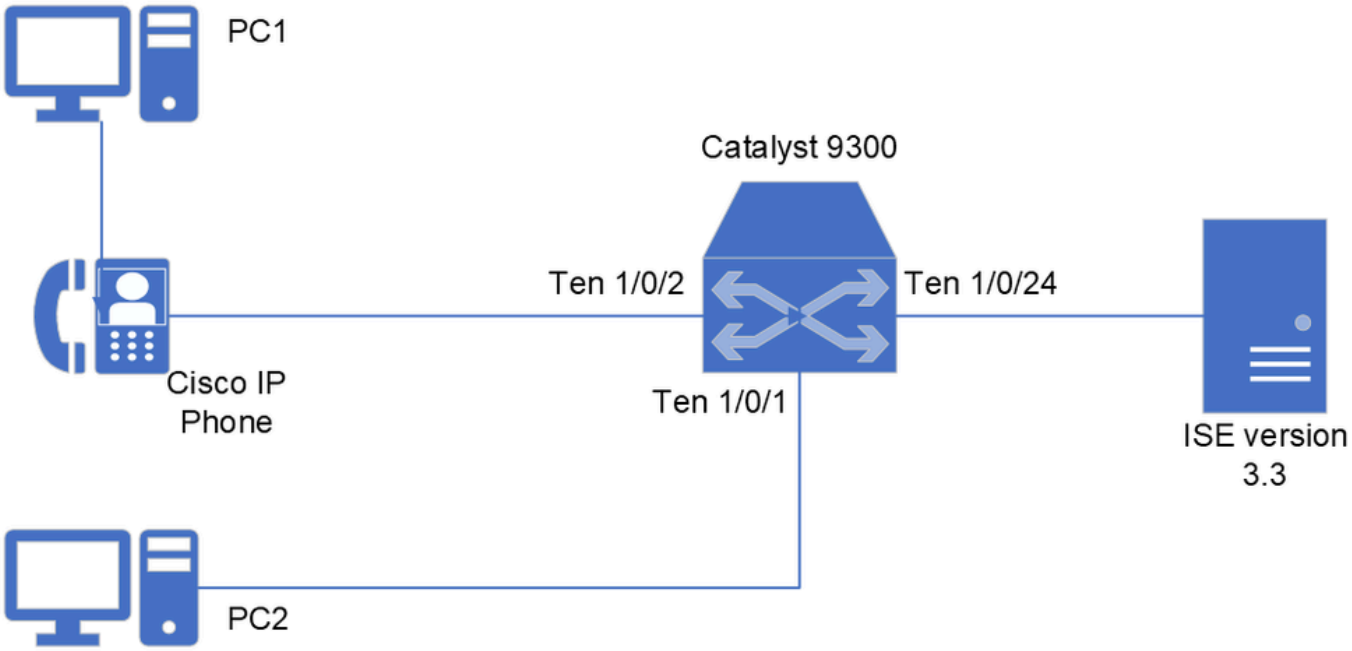
MACSec在點對點連線中提供這種加密，這種連線可以是交換機到交換機或交換機到主機的連線，因此該標準的覆蓋範圍僅限於有線連線。

此標準加密第2層連線中傳輸的幀的源MAC地址和目的MAC地址以外的整個資料。

MACsec金鑰協定(MKA)協定是MACsec對等體用來協商安全鏈路所需的安全金鑰的機制。

設定

網路圖表



附註：本文檔認為您已為PC裝置和Cisco IP電話配置並使用Radius身份驗證的規則。要從頭開始設定配置，請參閱ISE安全有線訪問規範部署指南，檢視身份服務引擎和交換機中的配置以進行基於身份的網路訪問。

在ISE上設定策略

第一個任務是配置應用於上述圖中所示的兩台PC（以及Cisco IP電話）的相應授權配置檔案。

在此假設方案中，PC將使用802.1X協定作為身份驗證方法，而Cisco IP電話使用Mac地址旁路(MAB)。

ISE通過RADIUS協定與交換機通訊，瞭解交換機在終端通過RADIUS會話連線的介面中需要強制執行的屬性。

對於主機中的MACsec加密，所需的屬性為cisco-av-pair = linksec-policy，它具有以下3個可能的值：

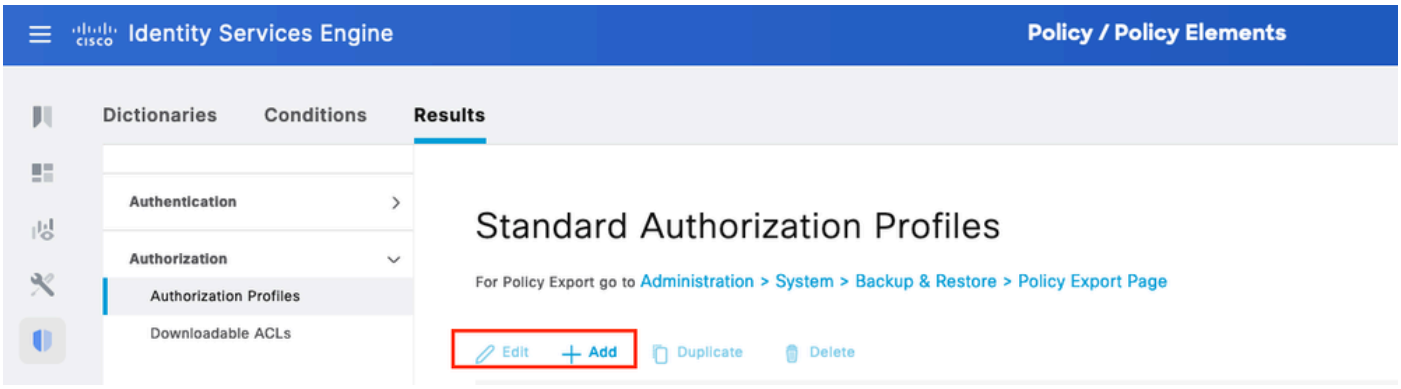
- Should-not-Secure:交換器在發生Radius作業階段的介面中不執行MKA加密。
- Must-Secure:交換器必須在與Radius作業階段連結的流量中強制執行加密。如果MKA會話失敗（或超時），則連線被視為授權失敗，並再次嘗試建立MKA會話。

- Should-Secure:交換機嘗試執行MKA加密。如果連結到Radius作業階段的MKA作業階段成功，則流量會加密。如果MKA失敗或超時，交換機將允許該未加密流量連結到該Radius會話。

步驟1。在兩台PC中，強制實施should-secure MKA策略，以便在沒有MKA功能的電腦連線到介面Ten 1/0/1時具有靈活性。

作為一個選項，您可以為PC2配置實施必須安全的策略的策略。

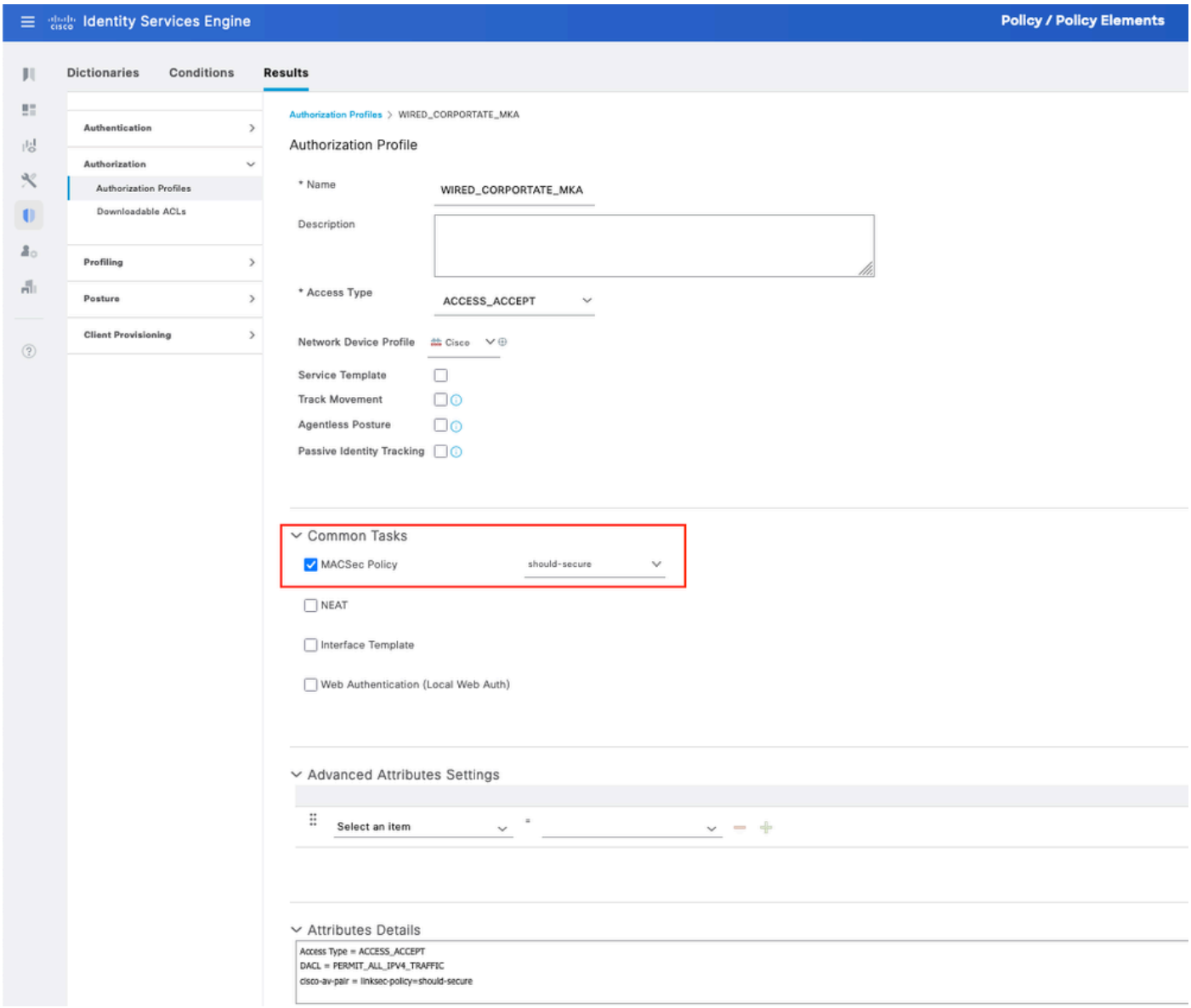
在本示例中，按照Policy > Policy Elements > Results > Authorization Profiles和+Add或Edit中的說明配置電腦的策略



步驟2。完成或自訂設定檔所需的欄位。

確保在常見任務中選擇了MACSec策略和要應用的相應策略。

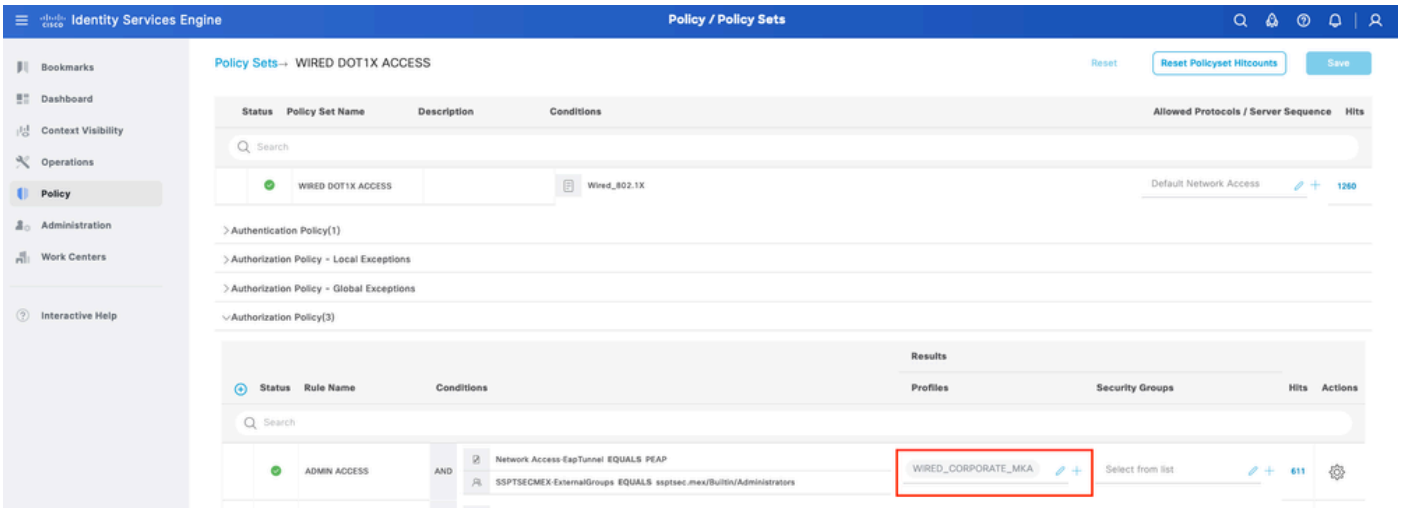
向下滾動並儲存組態。



步驟3.將對應的授權配置檔案分配到裝置所命中的授權規則。

導航到Policy > Policy Sets >(Select Policy Set assigned)> Authorization Policy。

將授權規則與具有MACsec設定的授權配置檔案相關聯。向下滾動並儲存您的組態。



在Catalyst 9300中設定MKA

步驟1.設定新的MKA原則，如以下範例所示：

```
!
  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
!
```

步驟2.在連線PC的介面中啟用MACsec加密。

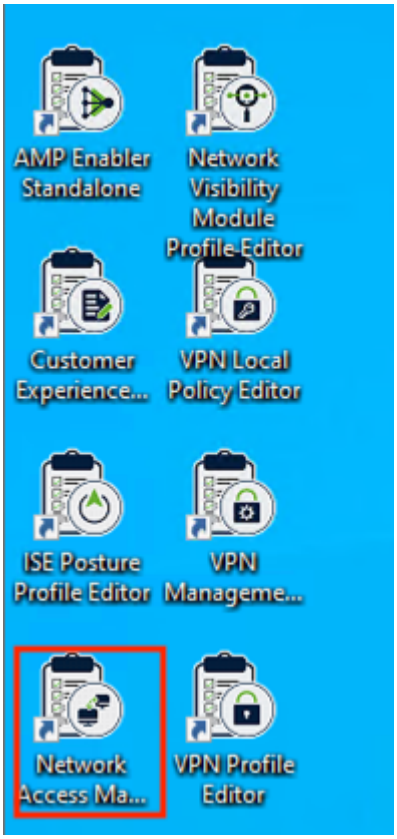
```
!
interface TenGigabitEthernet1/0/1
 macsec
 mka policy MKA_PC
!
```

附註：有關MKA配置中的命令和選項的更多資訊，請參閱與您使用的交換機版本對應的安全配置指南。在此案例中，[安全組態設定指南Cisco IOS XE Bengaluru 17.6.x（Catalyst 9300交換器）]

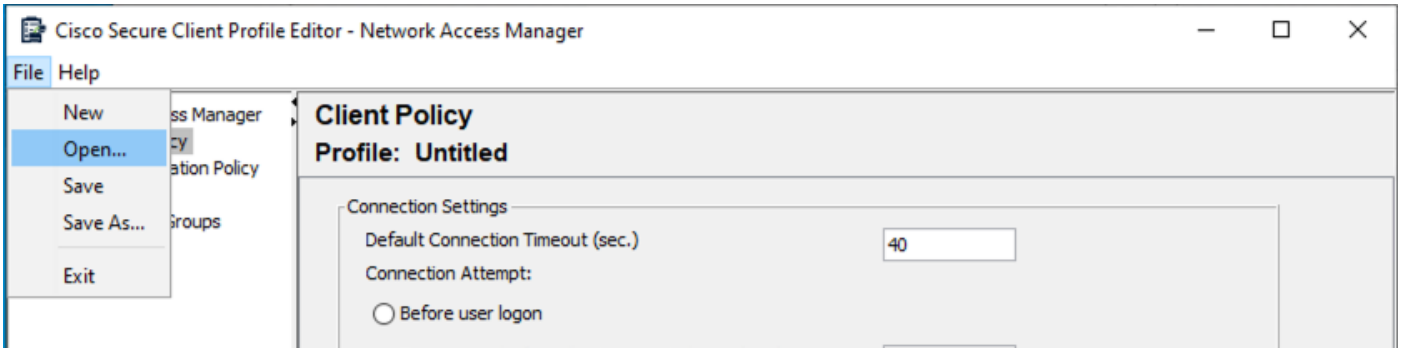
使用網路訪問管理器配置檔案編輯器設定MKA。

步驟1。下載（從思科的下載網站）並開啟與所用Secure Client版本相符的設定檔編輯器。

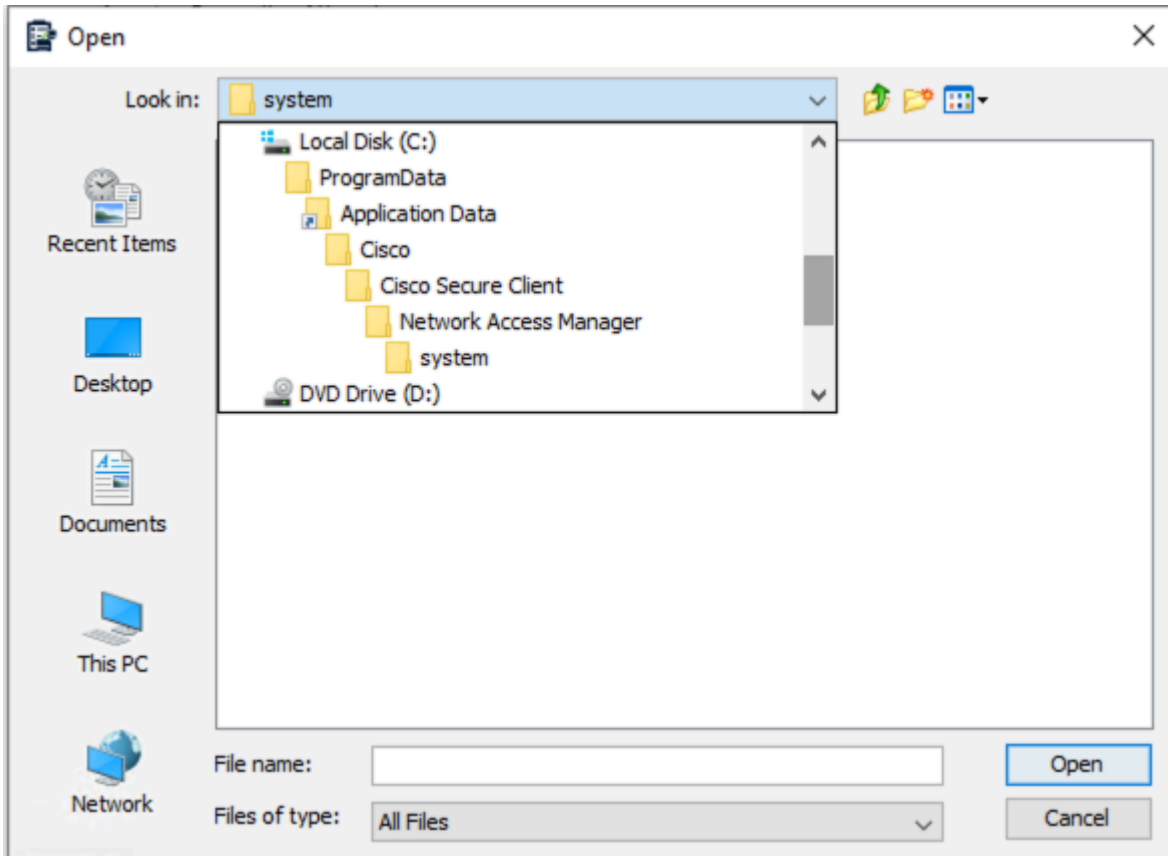
在電腦中安裝了此程式後，繼續開啟思科安全客戶端配置檔案編輯器 — 網路訪問管理器。



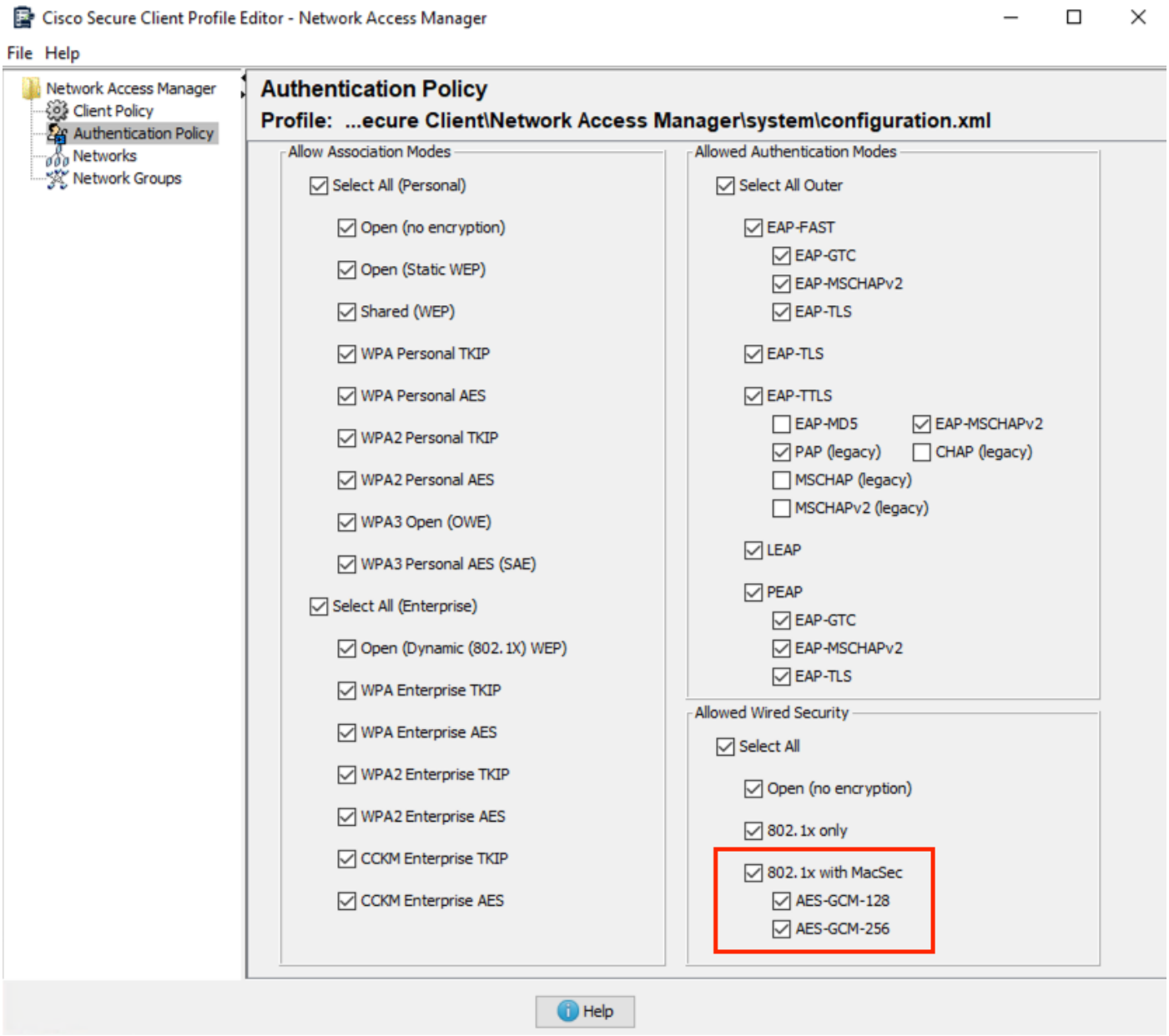
步驟2。選擇File > Open。



步驟3.選擇此影象中顯示的資料夾系統。在此資料夾中開啟名為configuration.xml的檔案。

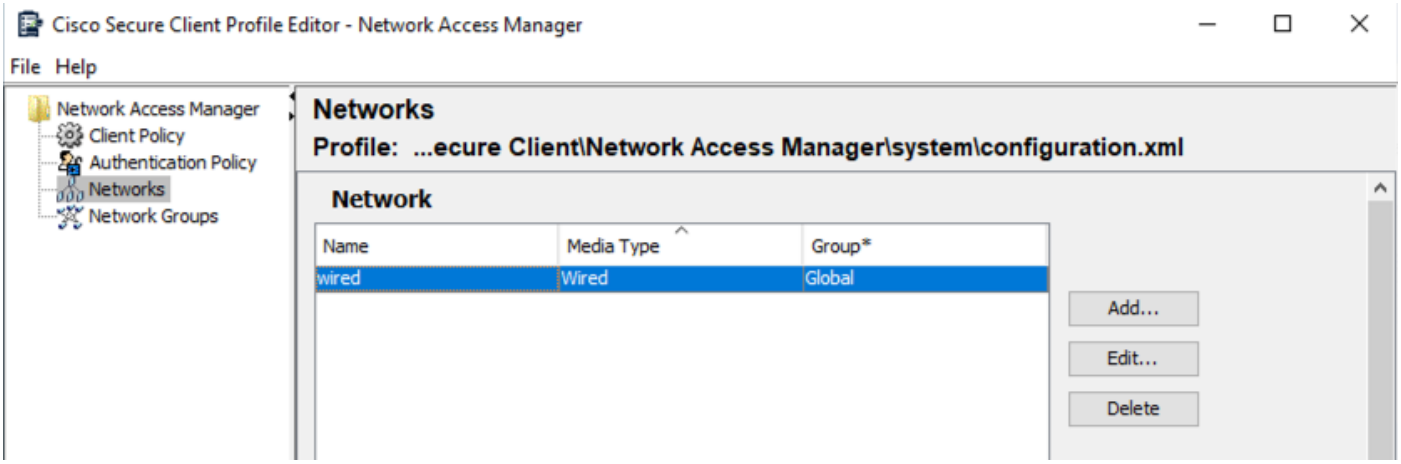


步驟4。一旦配置檔案編輯器載入了檔案，請選擇Authentication Policy選項，並確保啟用與802.1x with MACSec相關的選項。



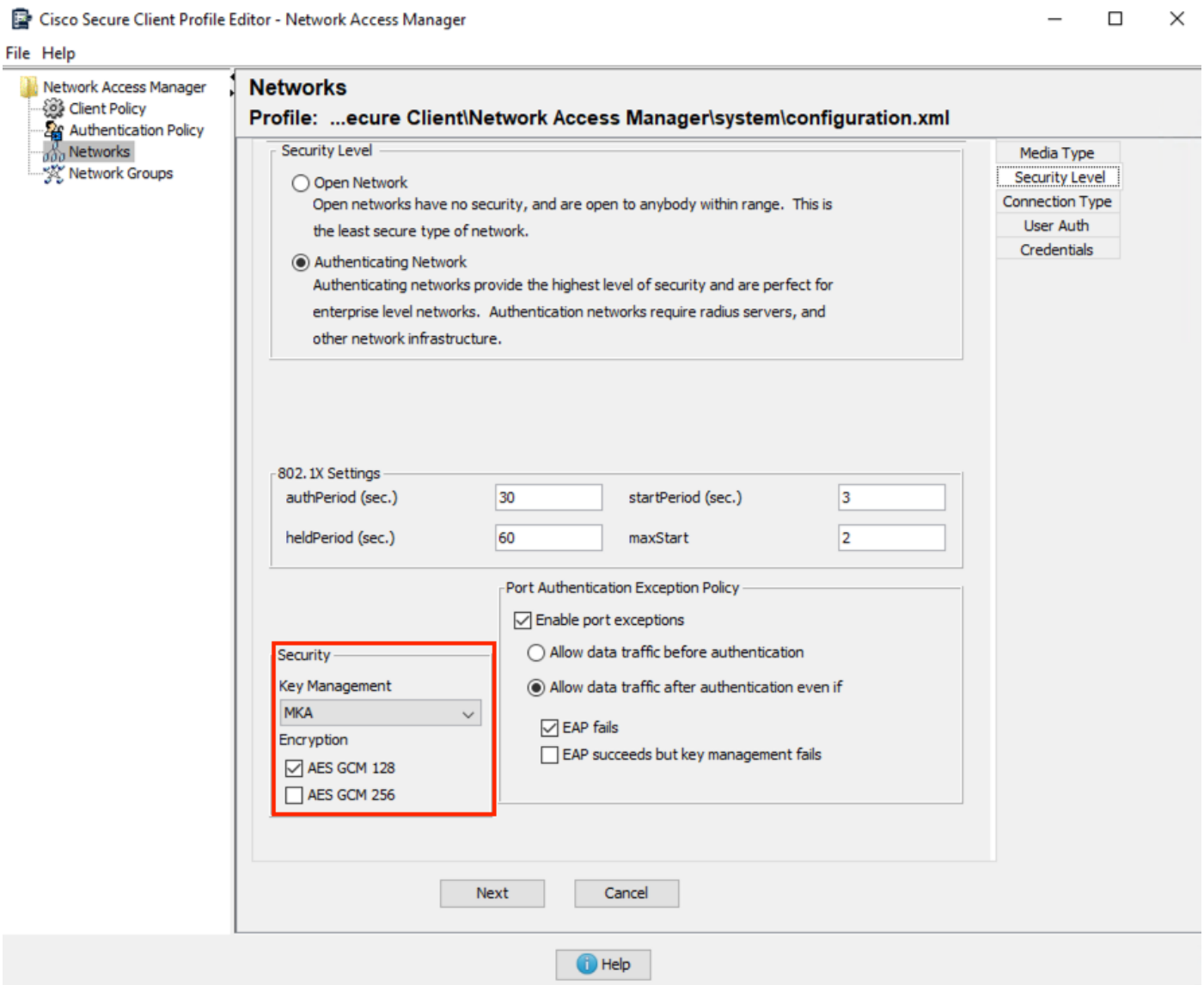
步驟5.繼續前往Networks一節。在此部分中，您可以為有線連線新增新配置檔案，或編輯隨Secure Client 5.0一起安裝的預設有線配置檔案。

在此案例中，我們將編輯現有的有線配置檔案。



步驟6.設定設定檔。在安全級別部分，調整金鑰管理以使用MKA，然後使用加密AES GCM 128。

調整身份驗證dot1x和策略的其他引數。

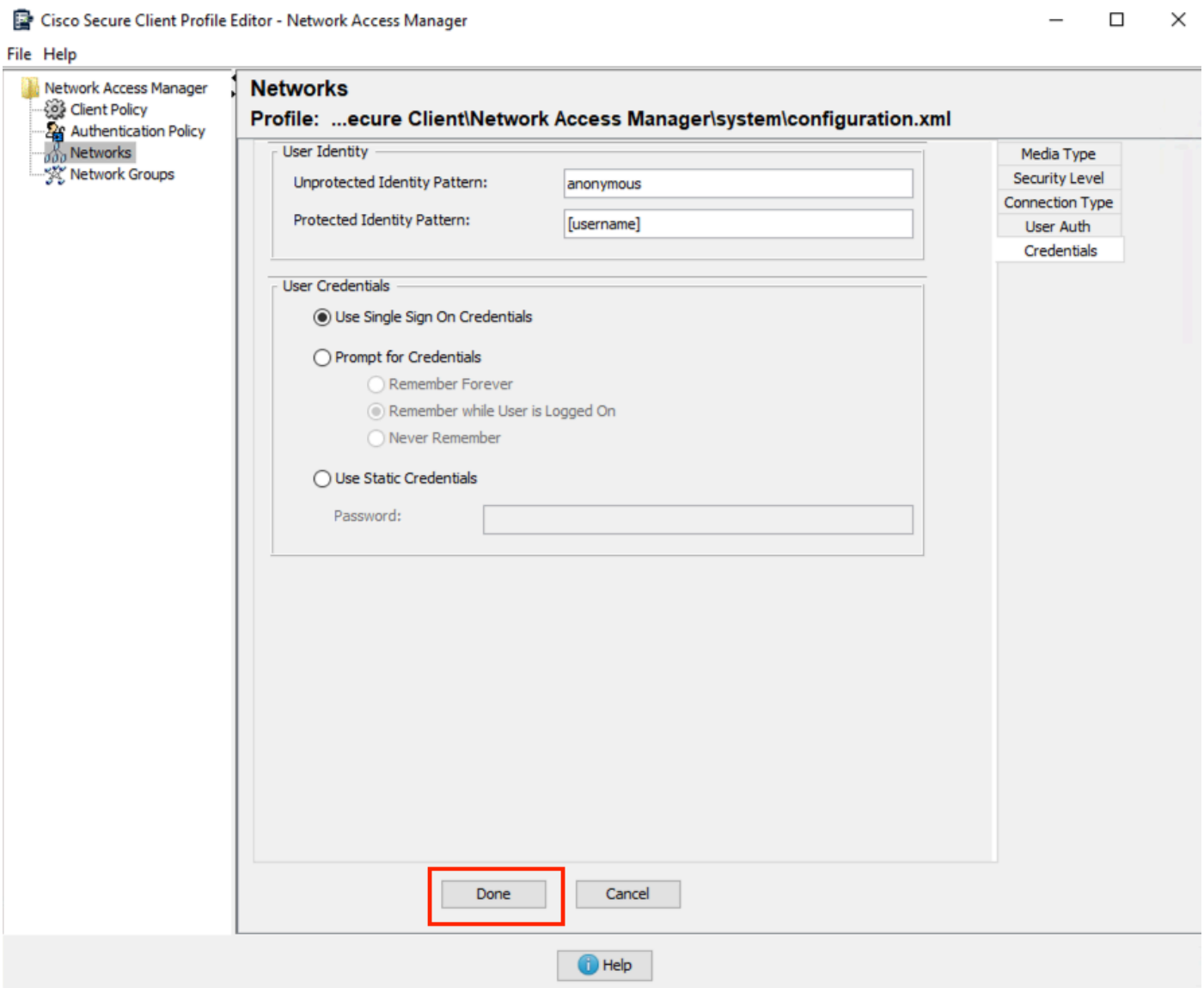


步驟7.設定其餘有關連線型別、User Auth和Credentials的部分。

這些部分因Security Level（安全級別）部分中選擇的身份驗證設定而異。

完成配置後，按一下完成。

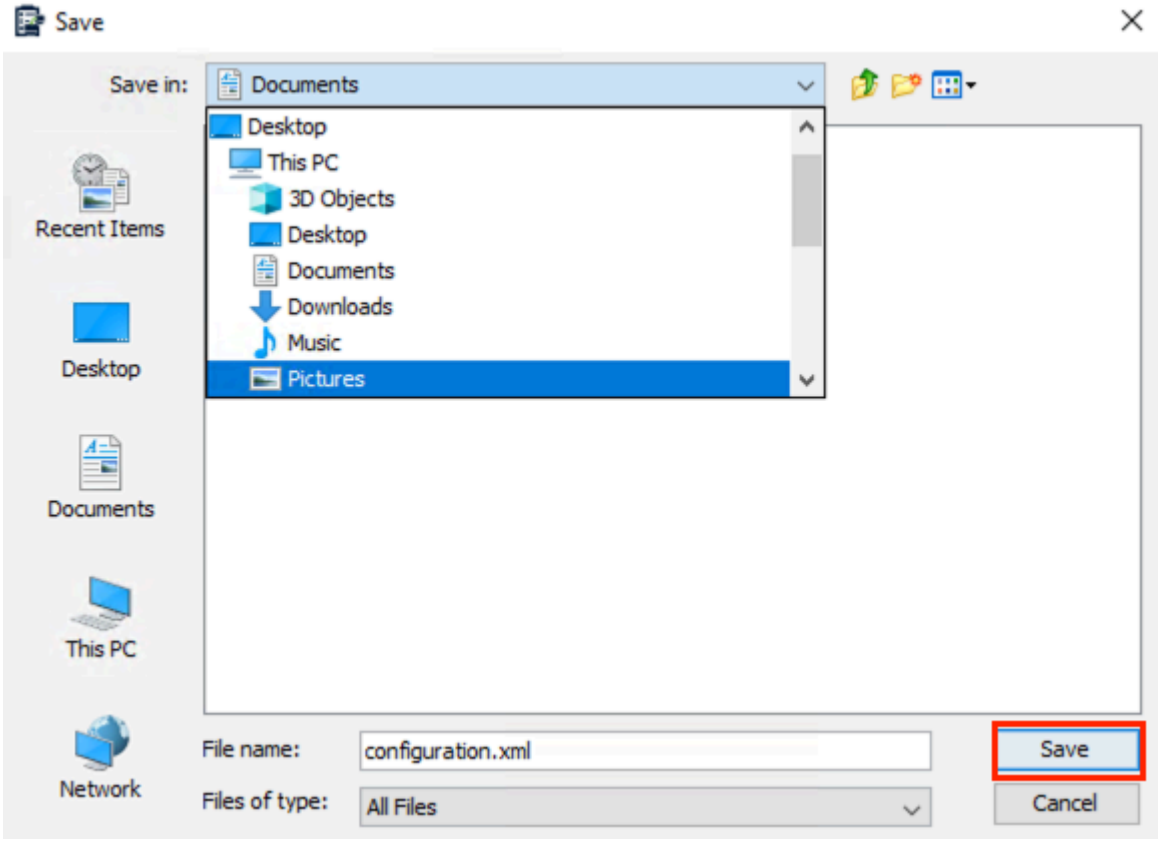
在此場景中，我們將受保護的可擴展身份驗證協定(PEAP)與用戶憑證配合使用。



步驟8。導航至功能表File。繼續執行Save as選項。

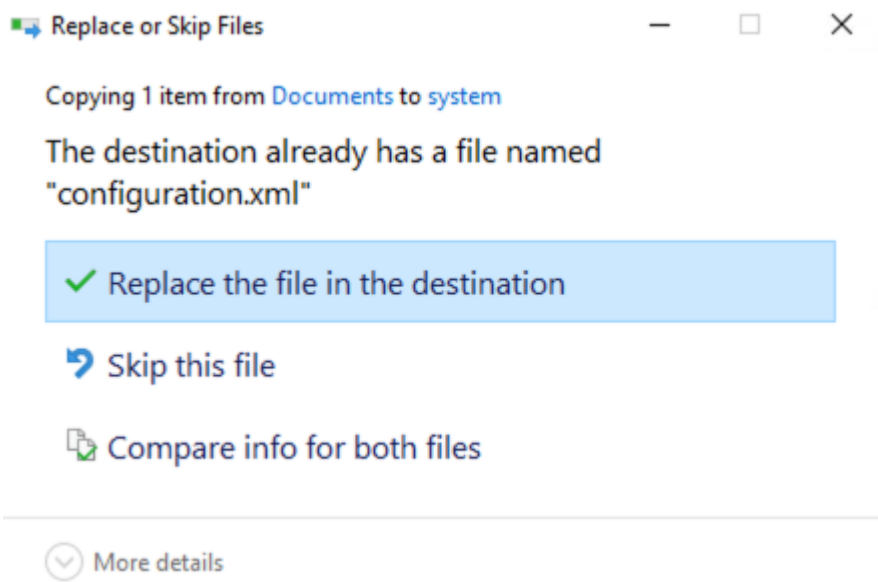
將檔案命名為configuration.xml，然後將其儲存在ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system以外的資料夾中。

在本示例中，檔案儲存在Documents資料夾中。儲存配置檔案。



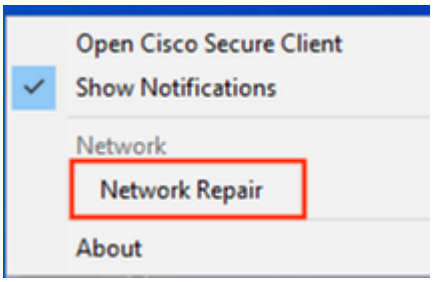
步驟8。繼續訪問配置檔案位置，複製檔案，並替換資料夾ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system中包含的檔案。

選擇「替換目標中的文件」選項。



步驟9。要載入在安全客戶端5.0中修改的配置檔案，請按一下右鍵Windows電腦右下工作列中的安全客戶端圖示。

執行網路修復。

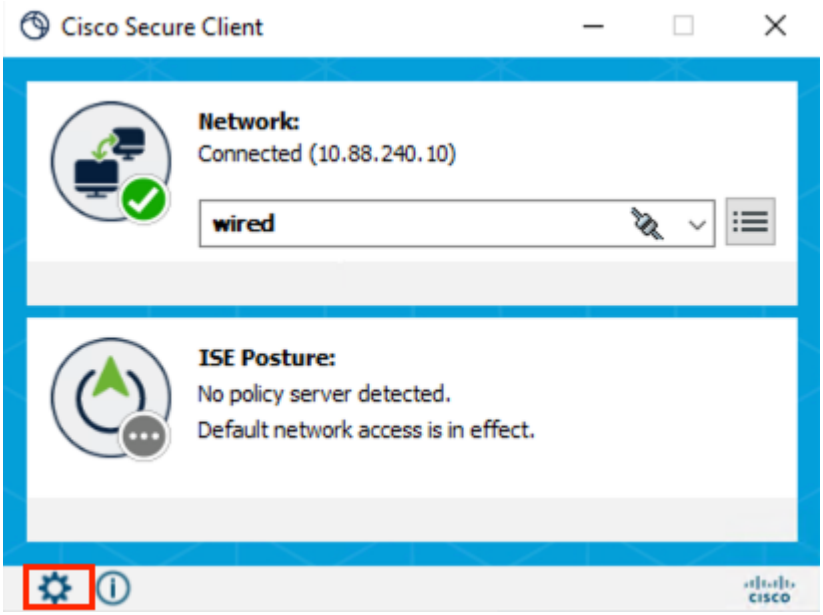


附註：通過配置檔案編輯器配置的所有網路都具有管理員網路的許可權，因此使用者無法定製/更改使用此工具配置的內容。

使用網路訪問管理器設定MKA網路（可選）。

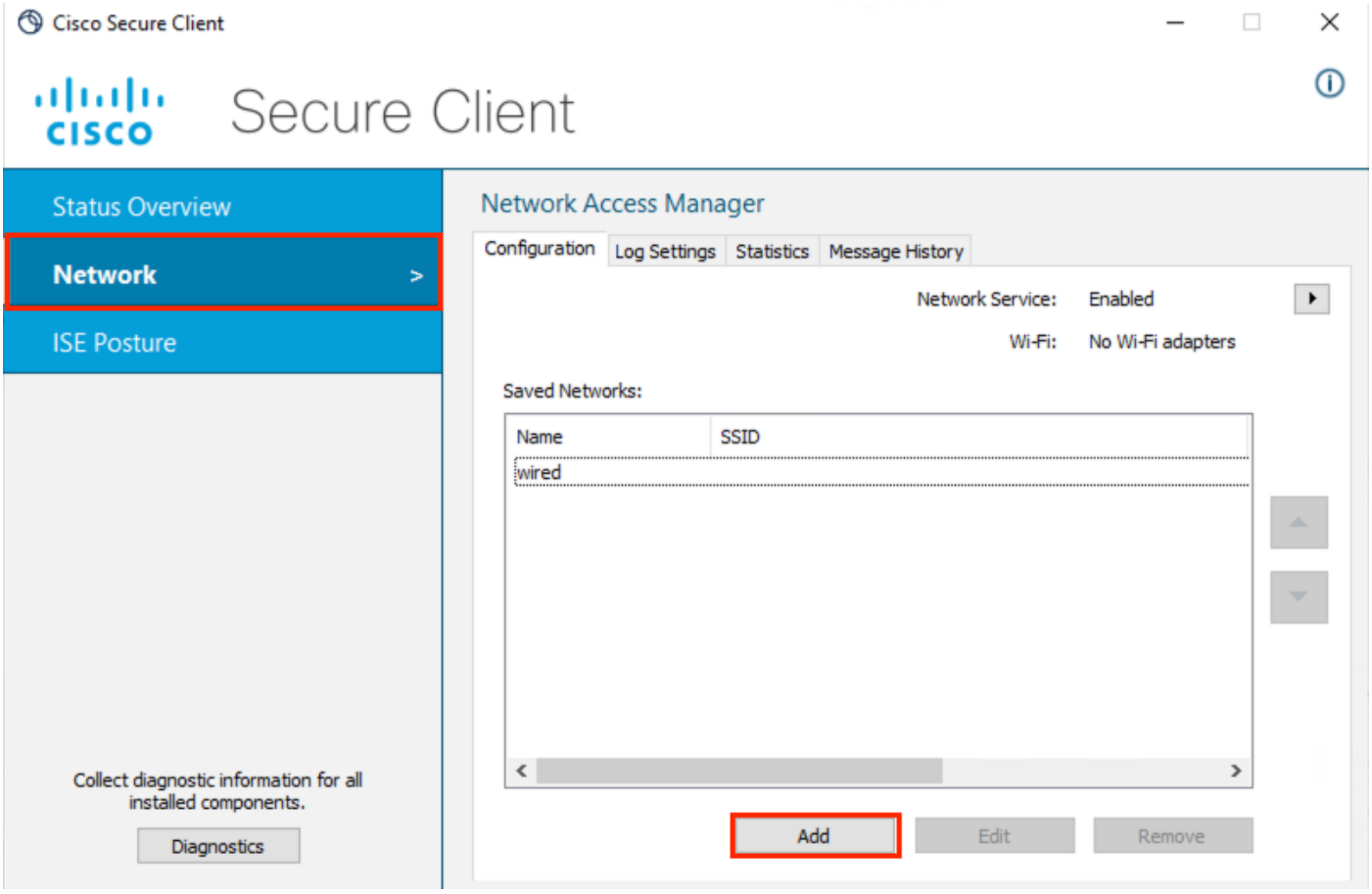
步驟1.作為使用配置檔案編輯器進行MKA設定的替代方法，您可以新增網路，而無需使用此工具。

從Secure Client套件中選擇齒輪圖示。



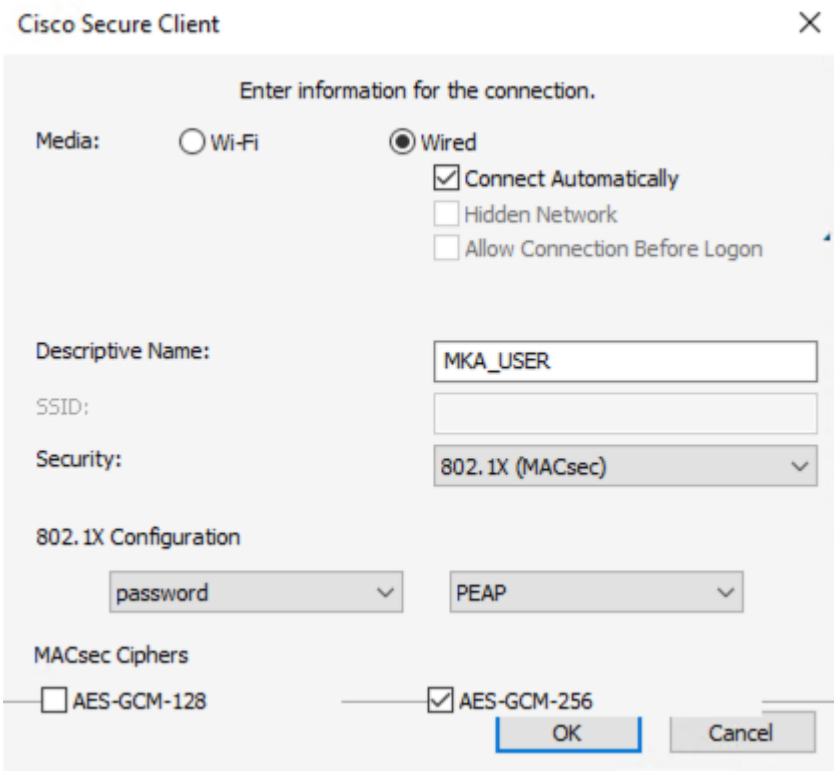
步驟2。在顯示的新視窗中，選擇選項Network。

在Configuration部分中，選擇Add選項，以入口具有使用者網路許可權的網路MKA。



步驟3.在新配置視窗中，設定連線特徵並命名網路。

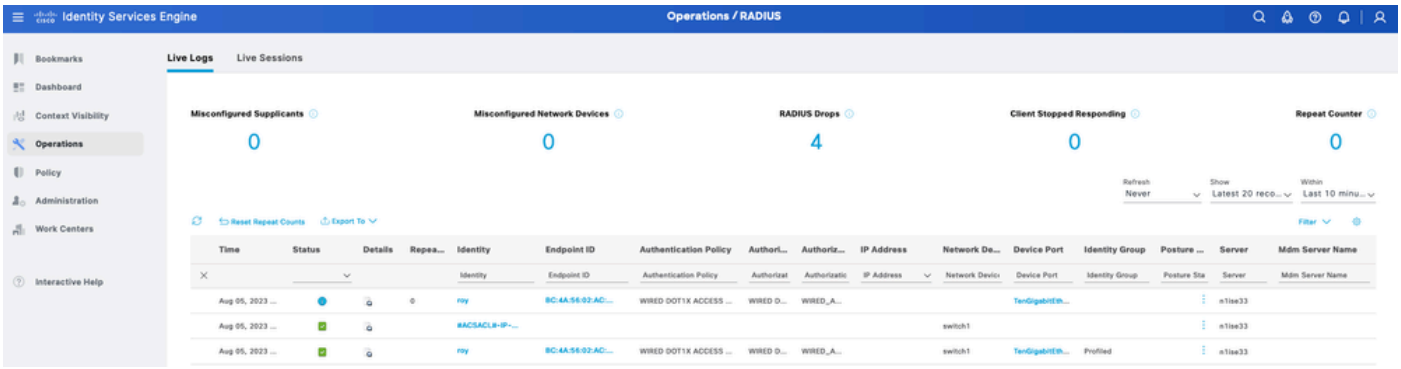
完成後，選擇OK按鈕。



驗證

ISE驗證

在ISE中，完成此流的配置後，請注意裝置在Livelogs中經過身份驗證和授權。



在Details of the authentication和Result部分中導航。

在授權配置檔案中設定的屬性將傳送到網路接入裝置(NAD)並消耗一個基本許可證。

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.

在Catalyst交換器上驗證。

這些命令可用於驗證此解決方案的正確功能。

```
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

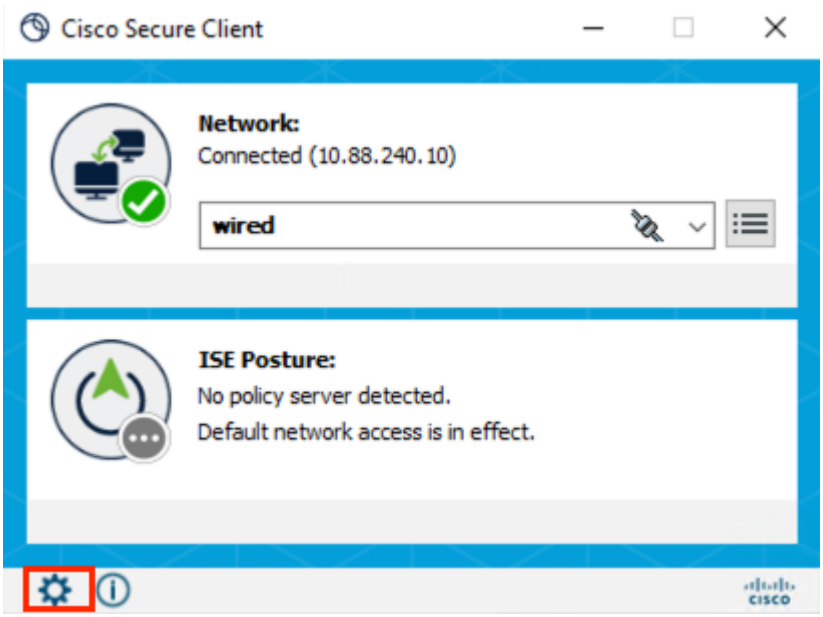
```
switch1#show mka session

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
```

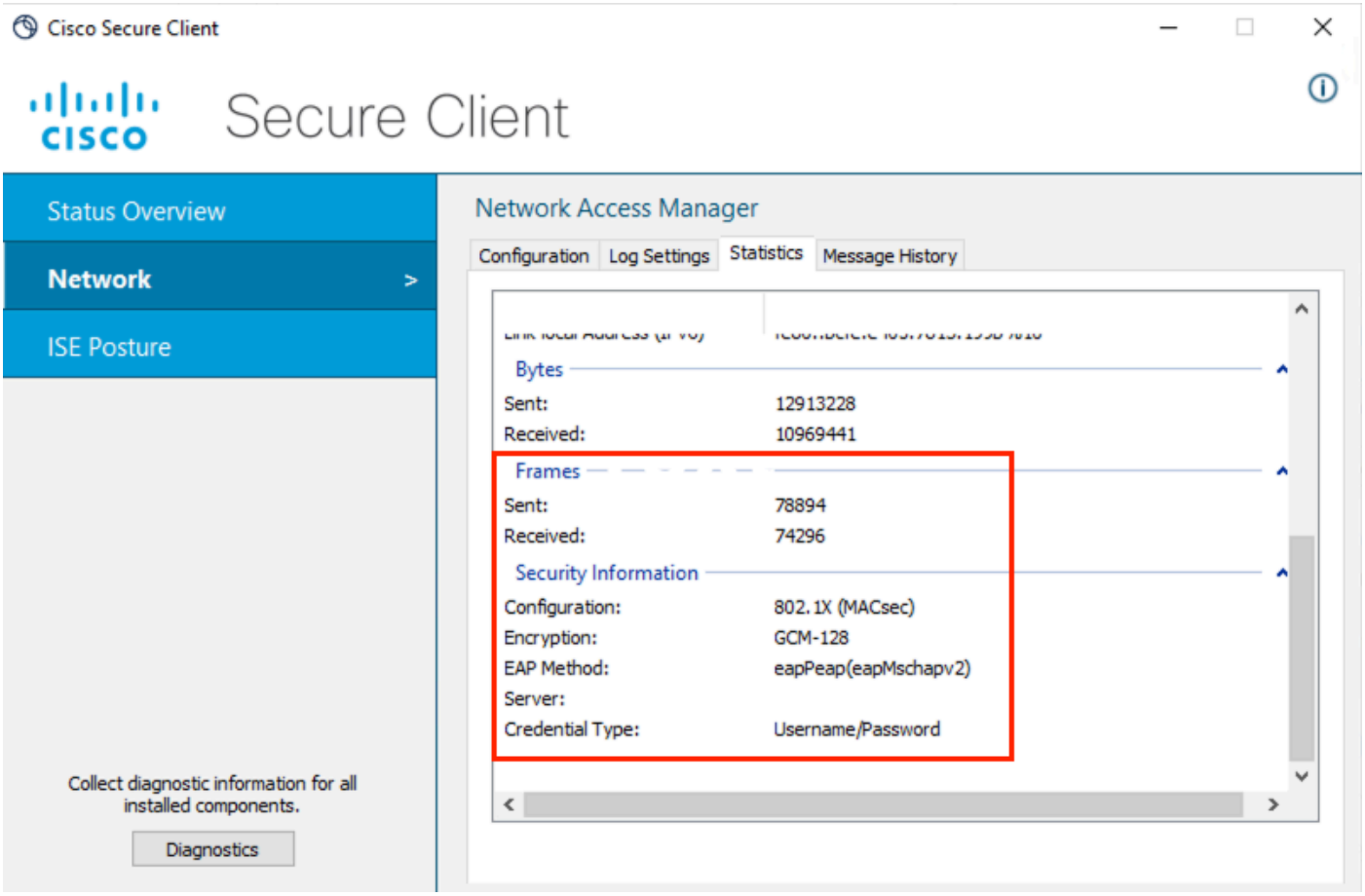
在安全客戶端上進行驗證。

使用使用MACsec加密建立的配置檔案成功進行身份驗證。如果按一下引擎圖示，則可以顯示更多資訊。



在此顯示的安全客戶端選單的網路訪問管理器>統計資訊部分中，注意加密和相應的MACsec配置。

在第2層執行加密時，接收和傳送的幀會增加。

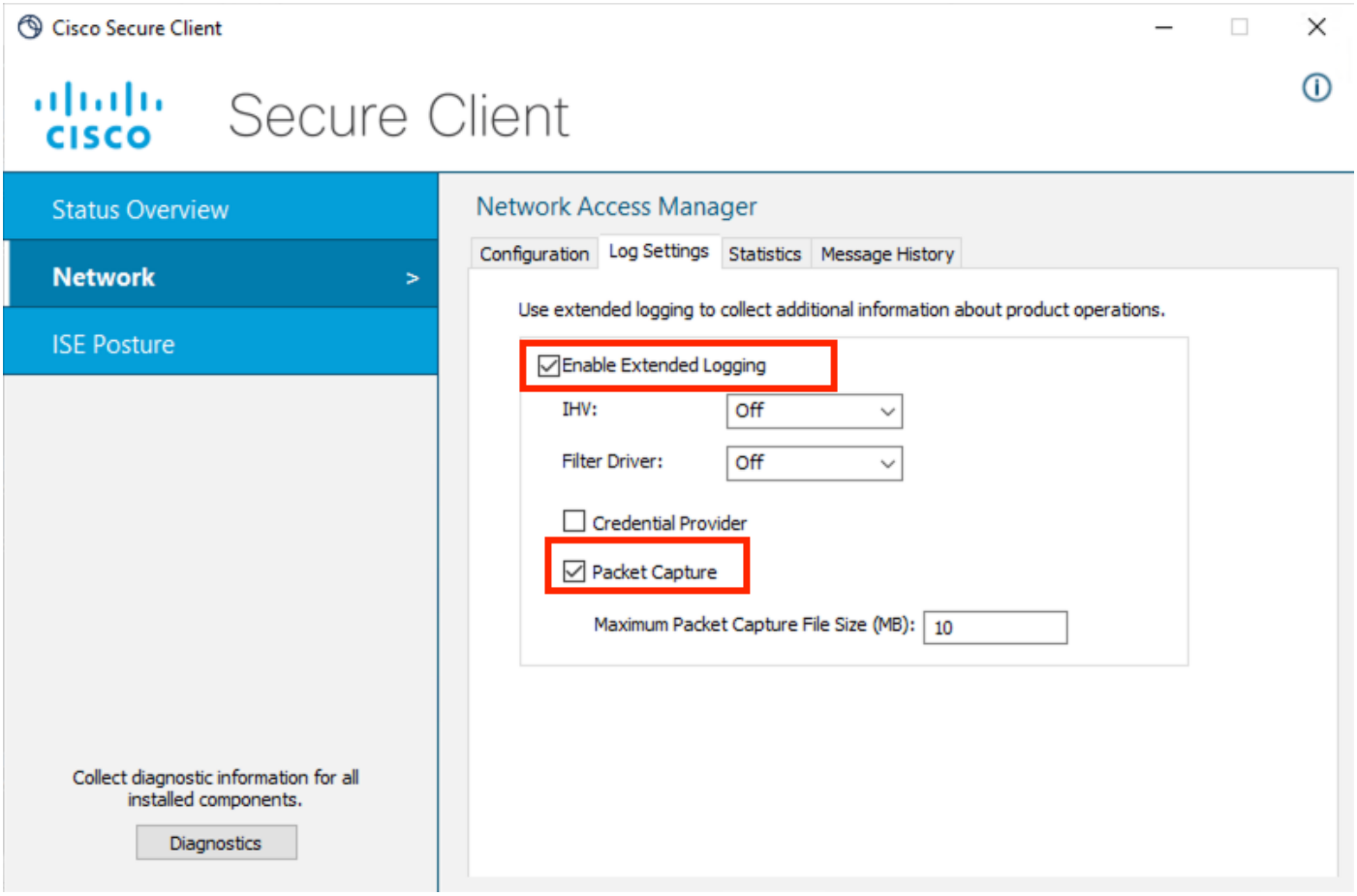


疑難排解

附註：本節介紹與可能出現的MKA問題相關的故障排除部分。如果遇到身份驗證或授權失敗，請參閱ISE安全有線訪問規範部署指南 — 故障排除以進行調查。本指南假設身份驗證在沒有MACsec加密的情況下工作正常。

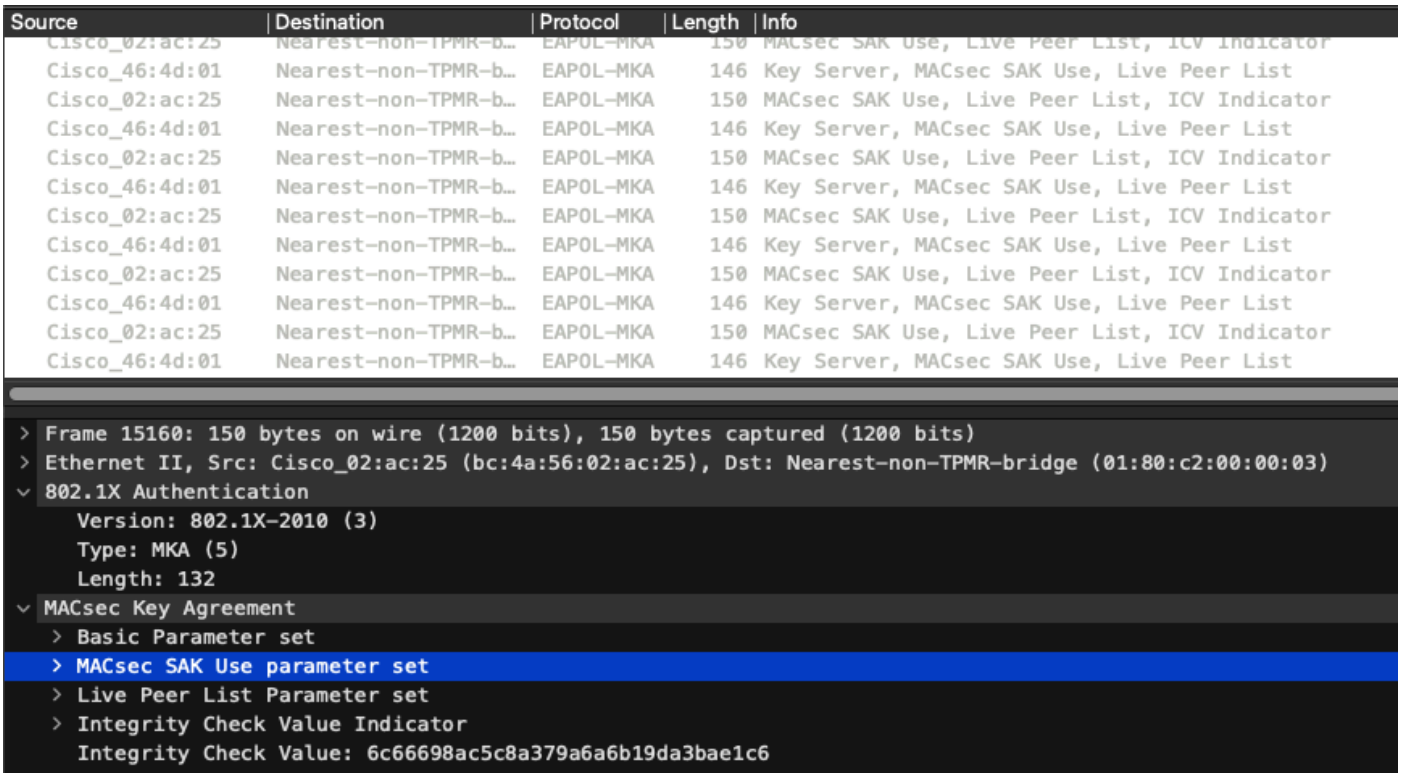
思科安全端點

- 在安全終端套件中啟用DART模組。
- 在此選單中，啟用擴展日誌記錄以收集有關使用者MKA連線的更多資料。您還可以啟用DART捆綁包中包含的資料包捕獲。



- 收集DART捆綁包，以繼續分析configuration.xml和網路訪問管理器。請參閱文檔運行DART以收集資料以進行故障排除

此範例顯示如何將封包視為主機和交換器之間的資訊加密：



從DART捆綁包中，我們可以在名為NetworkAccessManager.txt的日誌中找到有關身份驗證802.1X和MKA會話的有用資訊。

此資訊顯示在使用MKA加密的身份驗證成功中。

```
%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疑難排解

這些命令可在網路存取裝置(NAD)中實作，以檢查平台和請求方之間的MKA加密。

有關命令的更多資訊，請檢視用作NAD的平台的相應配置指南。

```
#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
```

以下是到主機的一個成功MKA連線的調試。您可以將此作為引用出現：

```
%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
```

身份服務引擎(ISE)故障排除

與此功能相關的疑難排解僅限於cisco-av-pair屬性linksec-policy=should-secure的傳送。

請確保授權結果正在將該資訊傳送到連結到裝置所連線的交換機埠的Radius會話。

有關ISE身份驗證分析的詳細資訊，請參閱ISE上的故障排除和啟用調試

常見問題

密碼不匹配

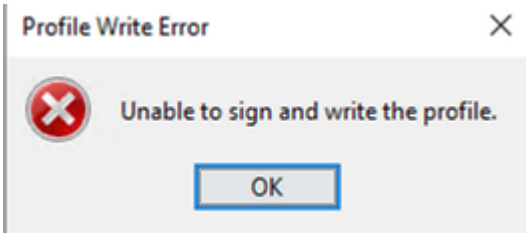
此日誌可在NAD的MKA調試中看到。

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

在此案例中，首先要驗證的是在交換機的MKA策略和安全客戶端配置檔案中配置的密碼是否匹配。

對於AES-GCM-256加密，需要滿足這些要求（根據文檔）Cisco Secure Client（包括AnyConnect）管理員指南，版本5

無法儲存configuration.xml。



通過使用網路訪問管理器配置檔案編輯器，儲存名為MKA的設定的configuration.xml（如前所述），解決了與配置檔案寫入錯誤相關的問題。

該錯誤與無法修改正在使用的檔案configuration.xml有關。因此，請將檔案儲存到另一個位置以繼續替換配置檔案。

相關資訊

- 配置MACsec加密
- 使用Cat9k和ISE配置MACsec交換機到主機

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。