使用EAP-TTLS配置電腦和使用者身份驗證

目錄

簡介

本文檔介紹如何在安全客戶端NAM和Cisco ISE上使用EAP-TTLS(EAP-MSCHAPv2)配置電腦和使用者身份驗證。

必要條件

需求

思科建議您在繼續此部署之前瞭解以下主題：

- 思科身分識別服務引擎(ISE)
- 安全使用者端網路分析模組(NAM)
- EAP協定

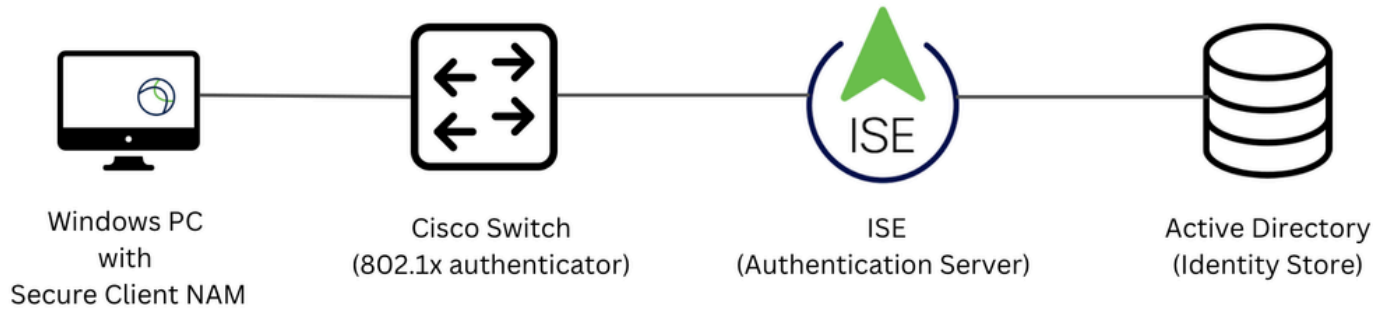
採用元件

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) 3.4 版
- 採用Cisco IOS® XE軟體版本16.12.01的C9300交換器
- Windows 10 Pro版本22H2，內建19045.3930

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路拓撲



網路拓撲

設定

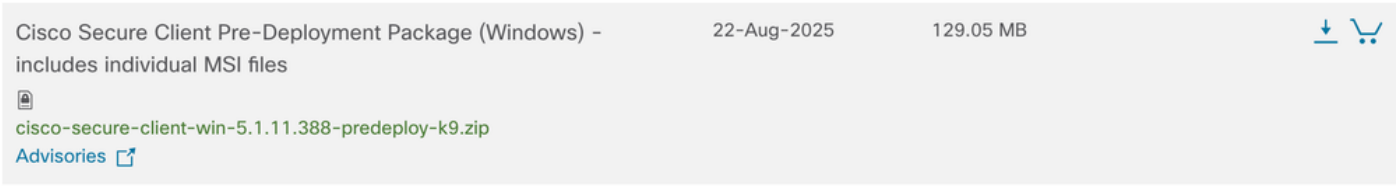
組態

第1部分： 下載和安裝Secure Client NAM（網路訪問管理器）

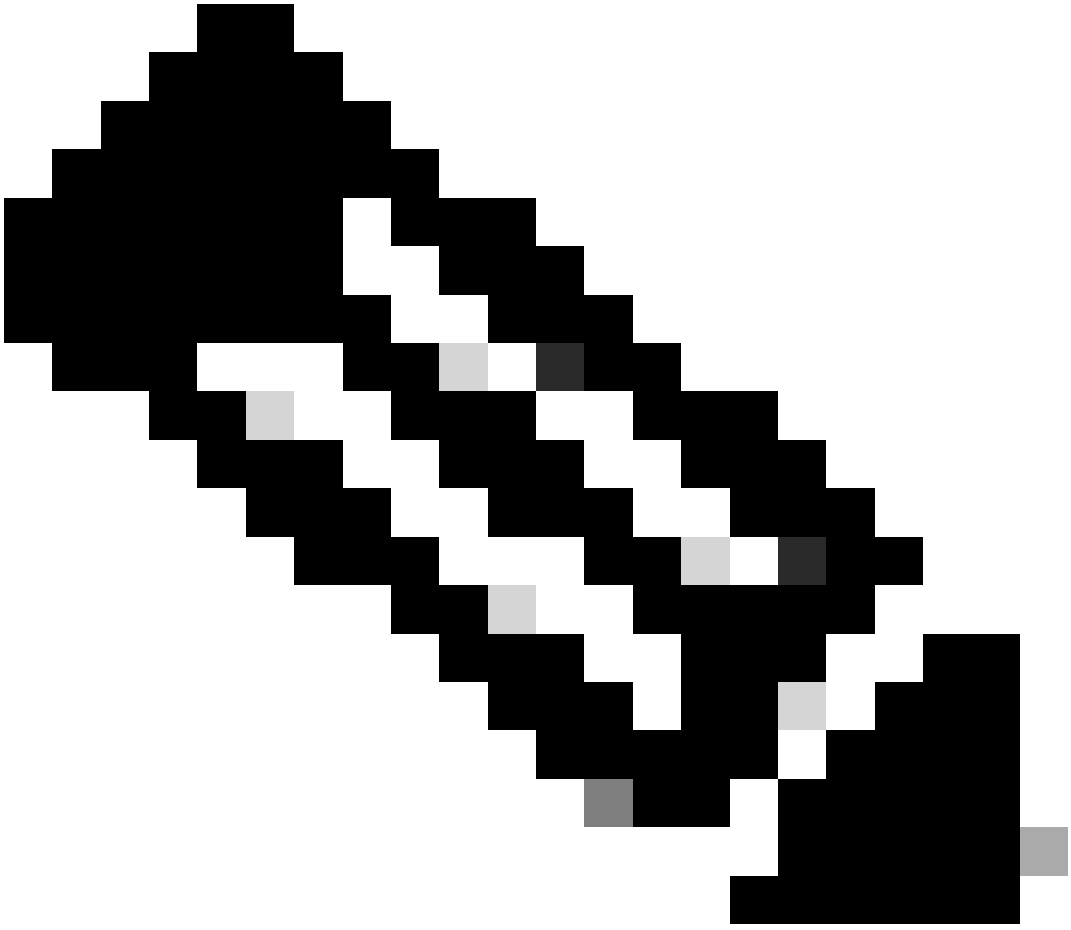
步驟1。前往Cisco Software Download。在產品搜尋欄中，輸入安全客戶端5。

此配置示例使用版本5.1.11.388。安裝是使用預部署方法執行的。

在下載頁面上，找到並下載思科安全客戶端預部署包(Windows)。

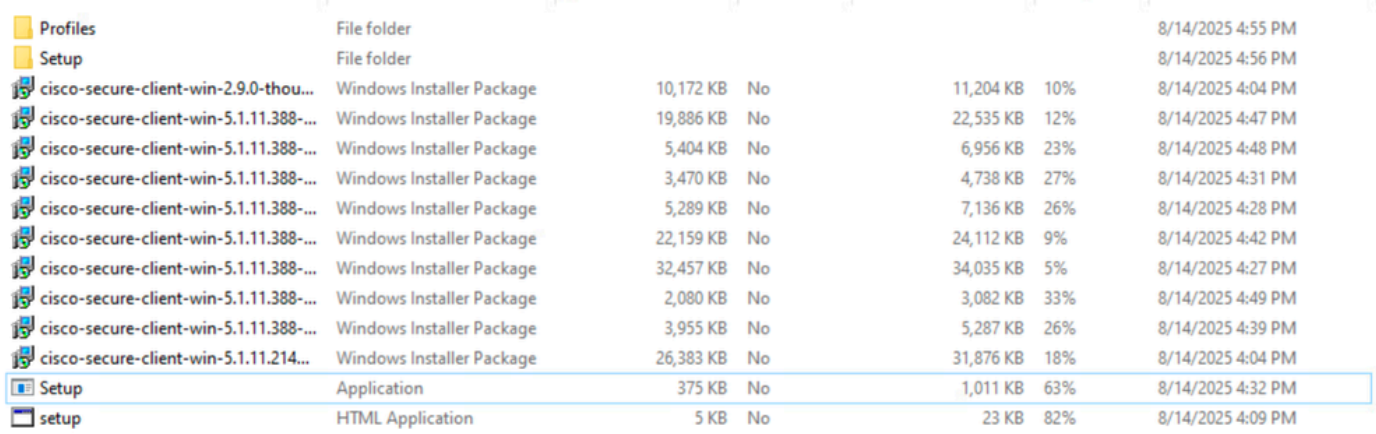


預部署zip檔案



附註：Cisco AnyConnect已被棄用，不再在思科軟體下載站點上可用。

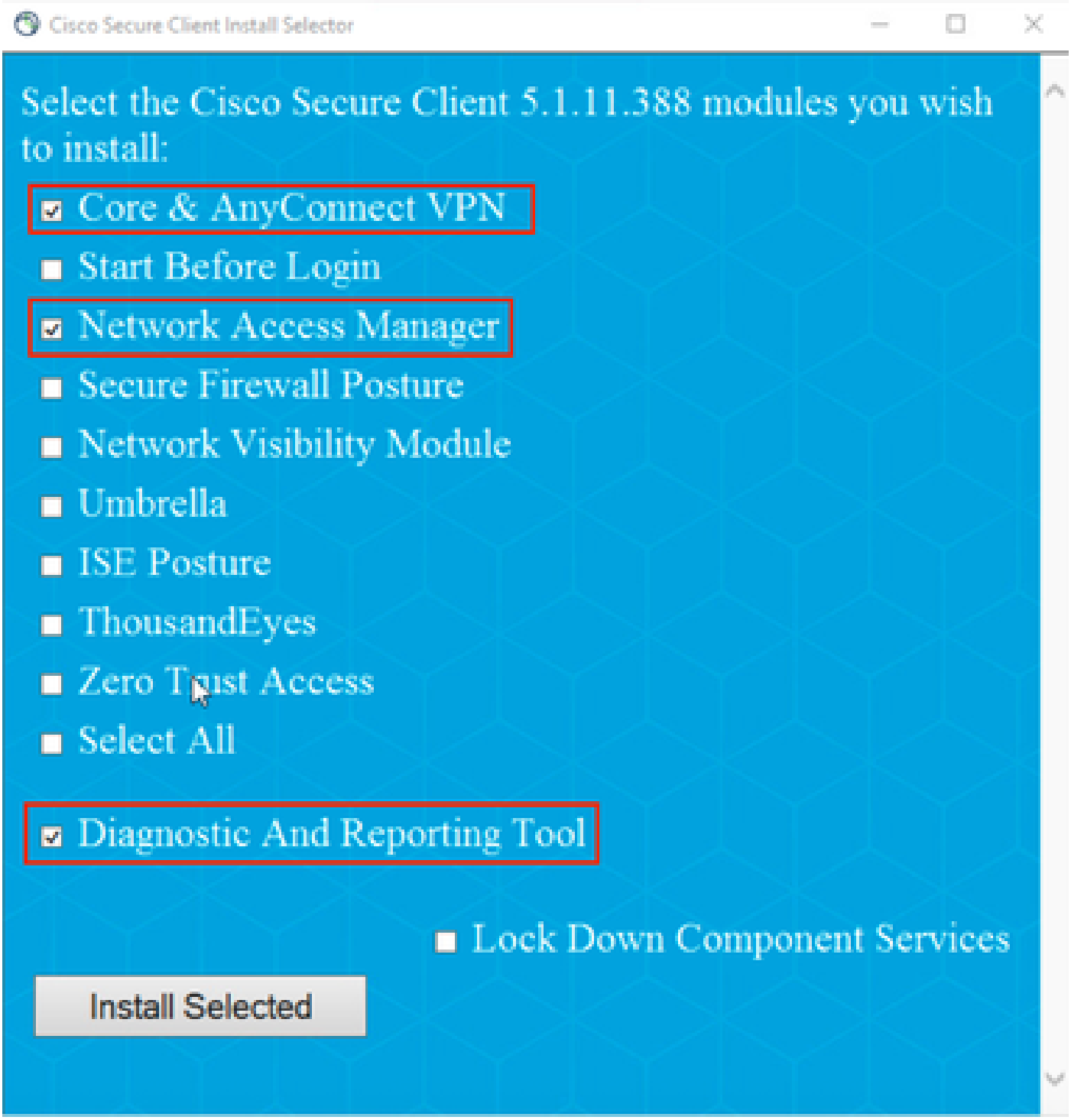
步驟2.下載並解壓後，按一下「Setup」。



Profiles	File folder					8/14/2025 4:55 PM
Setup	File folder					8/14/2025 4:56 PM
cisco-secure-client-win-2.9.0-thou...	Windows Installer Package	10,172 KB	No	11,204 KB	10%	8/14/2025 4:04 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	19,886 KB	No	22,535 KB	12%	8/14/2025 4:47 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,404 KB	No	6,956 KB	23%	8/14/2025 4:48 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,470 KB	No	4,738 KB	27%	8/14/2025 4:31 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,289 KB	No	7,136 KB	26%	8/14/2025 4:28 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	22,159 KB	No	24,112 KB	9%	8/14/2025 4:42 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	32,457 KB	No	34,035 KB	5%	8/14/2025 4:27 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	2,080 KB	No	3,082 KB	33%	8/14/2025 4:49 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,955 KB	No	5,287 KB	26%	8/14/2025 4:39 PM
cisco-secure-client-win-5.1.11.214...	Windows Installer Package	26,383 KB	No	31,876 KB	18%	8/14/2025 4:04 PM
Setup	Application	375 KB	No	1,011 KB	63%	8/14/2025 4:32 PM
setup	HTML Application	5 KB	No	23 KB	82%	8/14/2025 4:09 PM

預部署Zip檔案

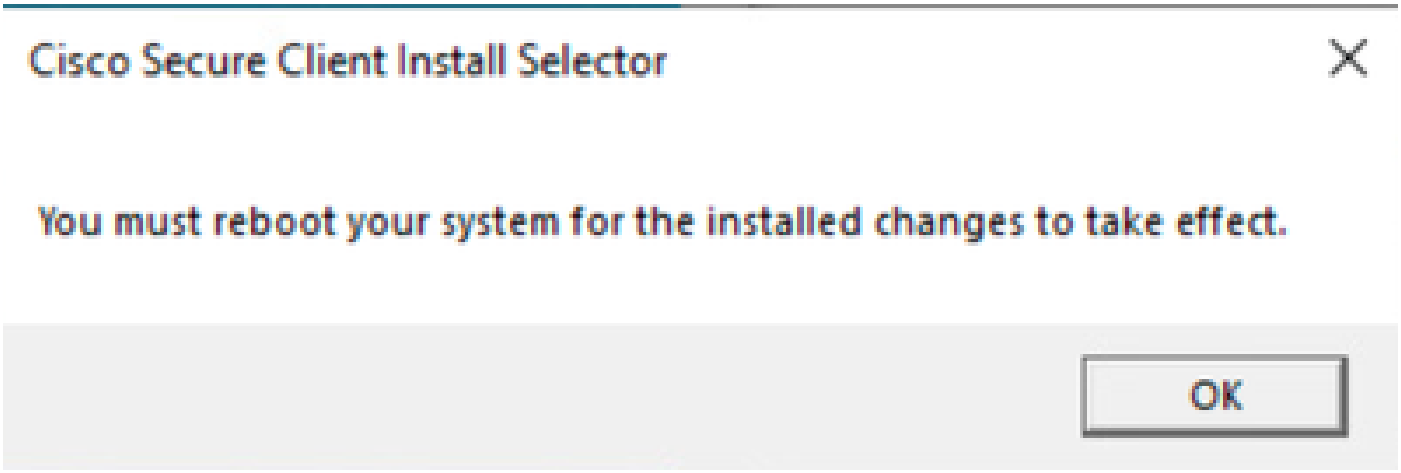
步驟3.安裝Core & AnyConnect VPN、Network Access Manager以及Diagnostics and Reporting 工具模組。



安全客戶端安裝程式

按一下「安裝所選內容」。

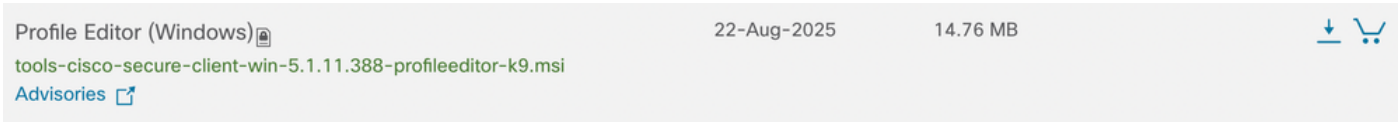
步驟4.安裝後需要重新啟動。按一下OK並重新啟動裝置。



需要重新啟動的彈出視窗

第2部分： 下載並安裝安全客戶端NAM配置檔案編輯器

步驟1。可以在與安全客戶端相同的下載頁上找到配置檔案編輯器。此配置示例使用5.1.11.388版本。



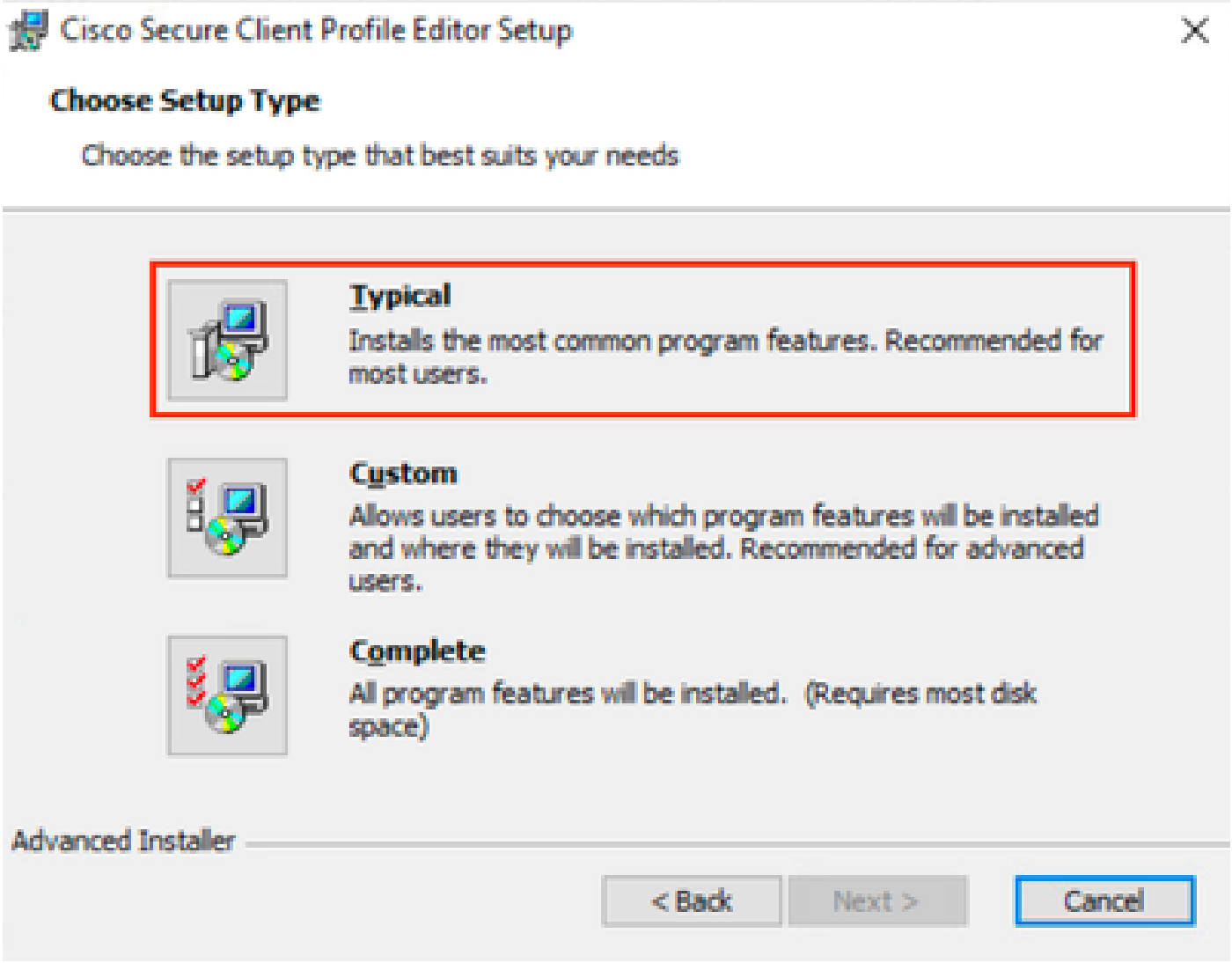
配置檔案編輯器

下載並安裝配置檔案編輯器。

步驟2.運行MSI檔案。

配置檔案編輯器安裝程式開始

步驟3.使用Typical setup選項並安裝NAM Profile Editor。

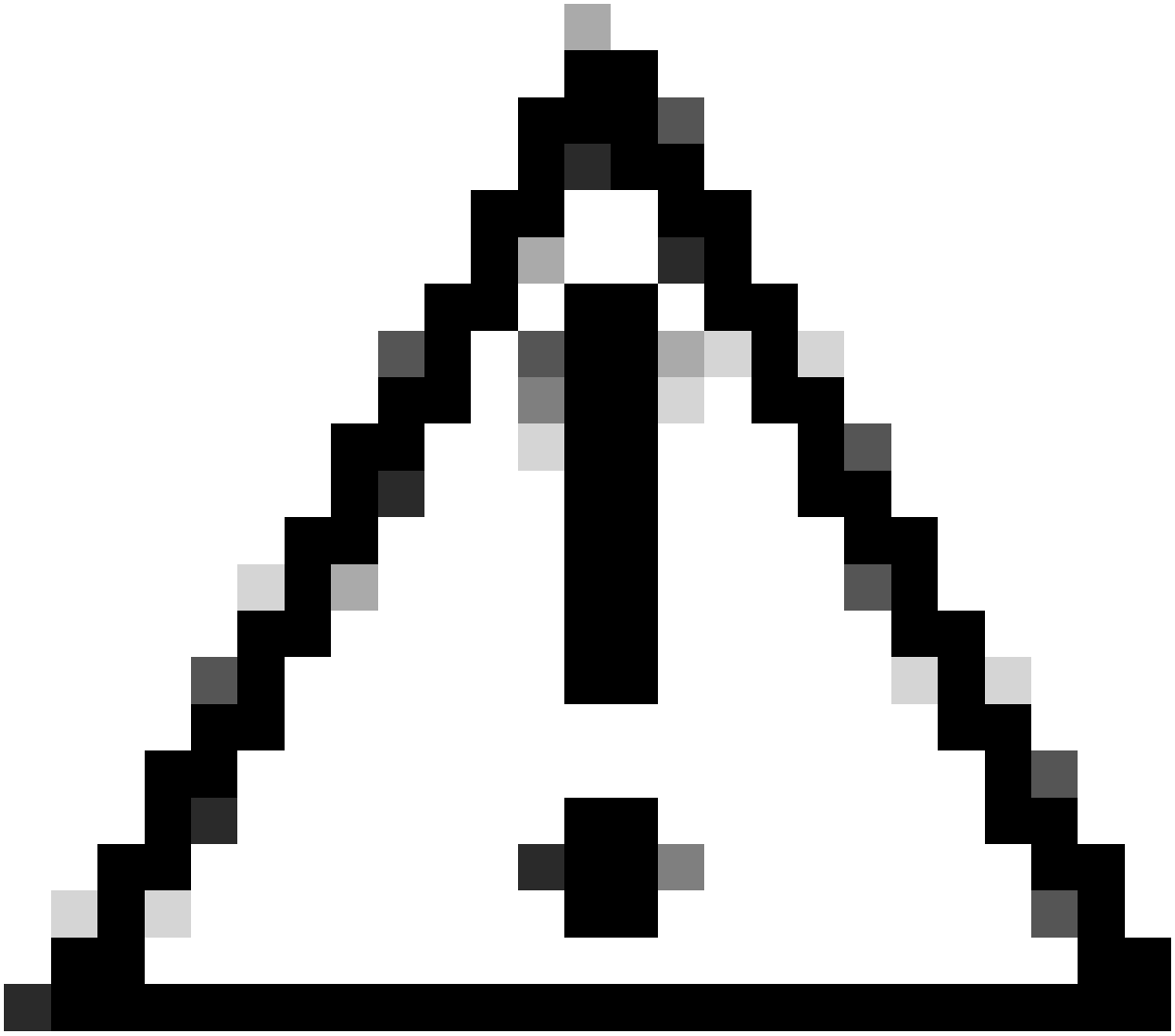


配置檔案編輯器安裝程式

第3部分：允許NAM訪問Windows快取憑據

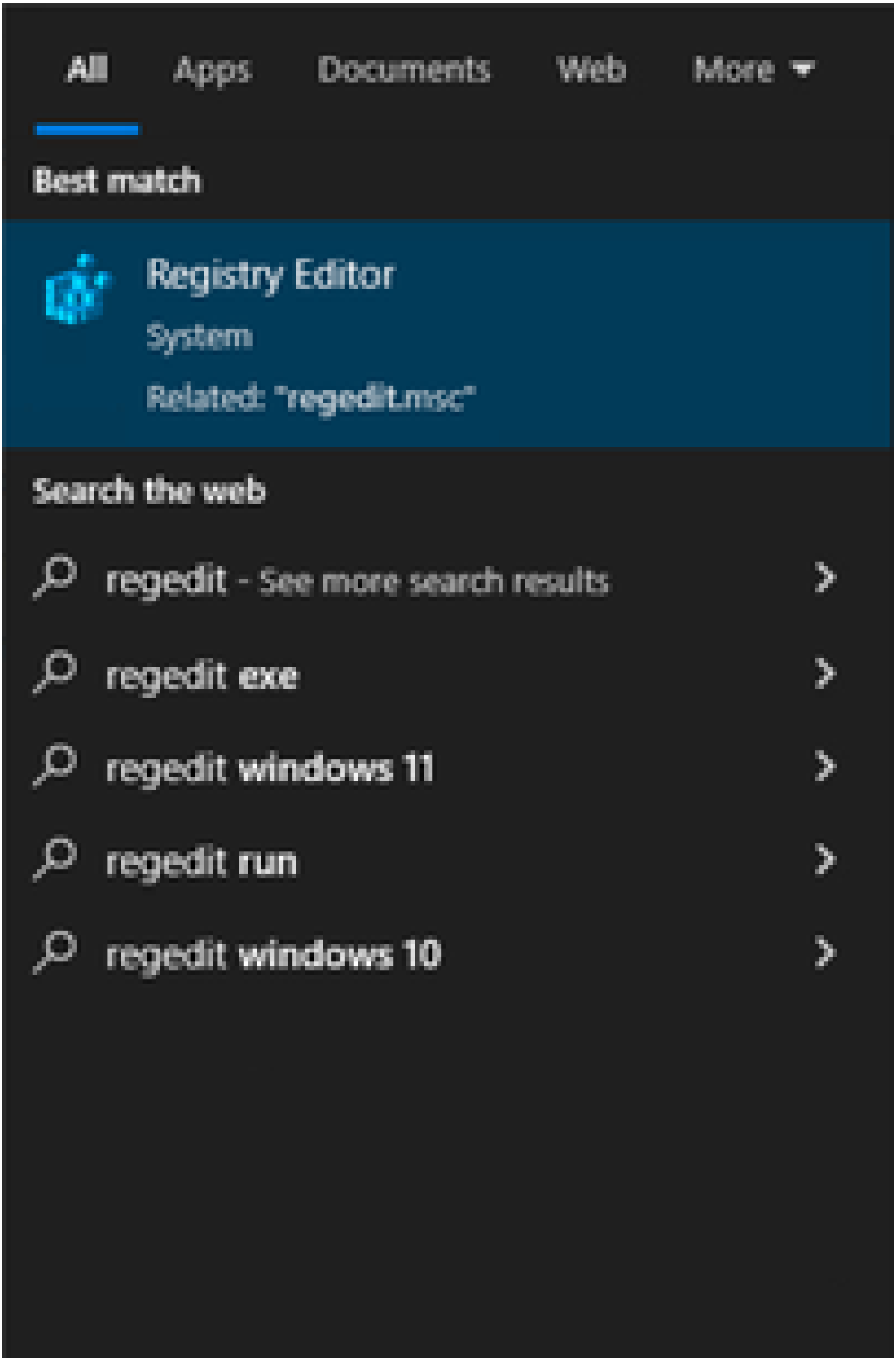
預設情況下，在Windows 10、Windows 11和Windows Server 2012上，作業系統阻止網路訪問管理器(NAM)檢索電腦身份驗證所需的電腦密碼。因此，除非應用登錄檔修復，否則使用電腦密碼的電腦身份驗證不起作用。

要啟用NAM以訪問電腦憑據，請在客戶端案頭上應用Microsoft KB 2743127修補程式。



注意：不正確地編輯Windows登錄檔可能導致嚴重的問題。在進行更改之前請務必備份登錄檔。

步驟1。在Windows搜尋欄中，輸入regedit，然後按一下Registry Editor。

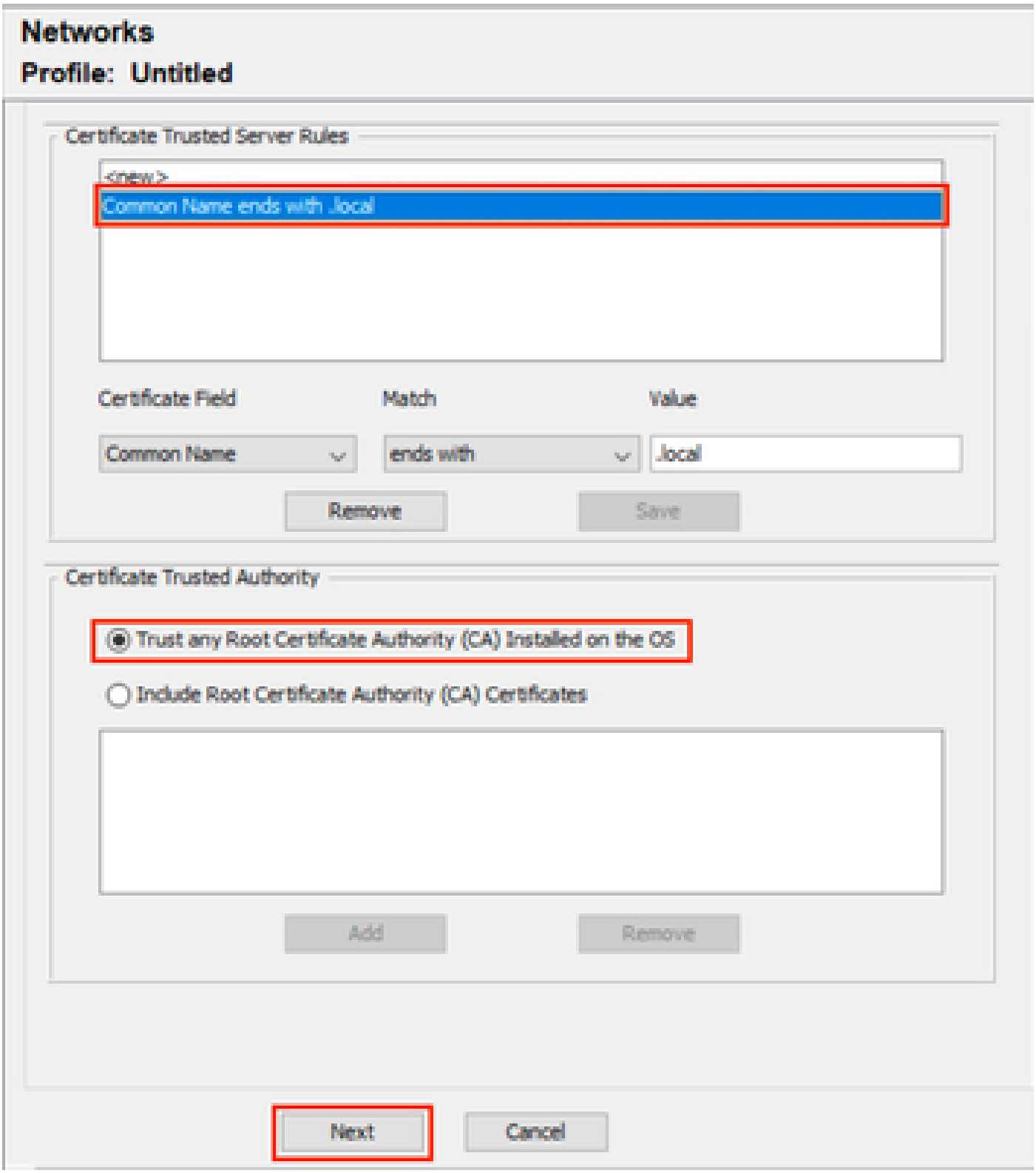

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

在本示例中，PSN節點證書由varshaah.varshaah.local頒發。因此，使用規則Common Name以.local結尾。此規則驗證伺服器在EAP-TTLS流期間顯示的證書。

您還可以指定策略服務節點(PSN)EAP身份驗證證書的公用名稱。

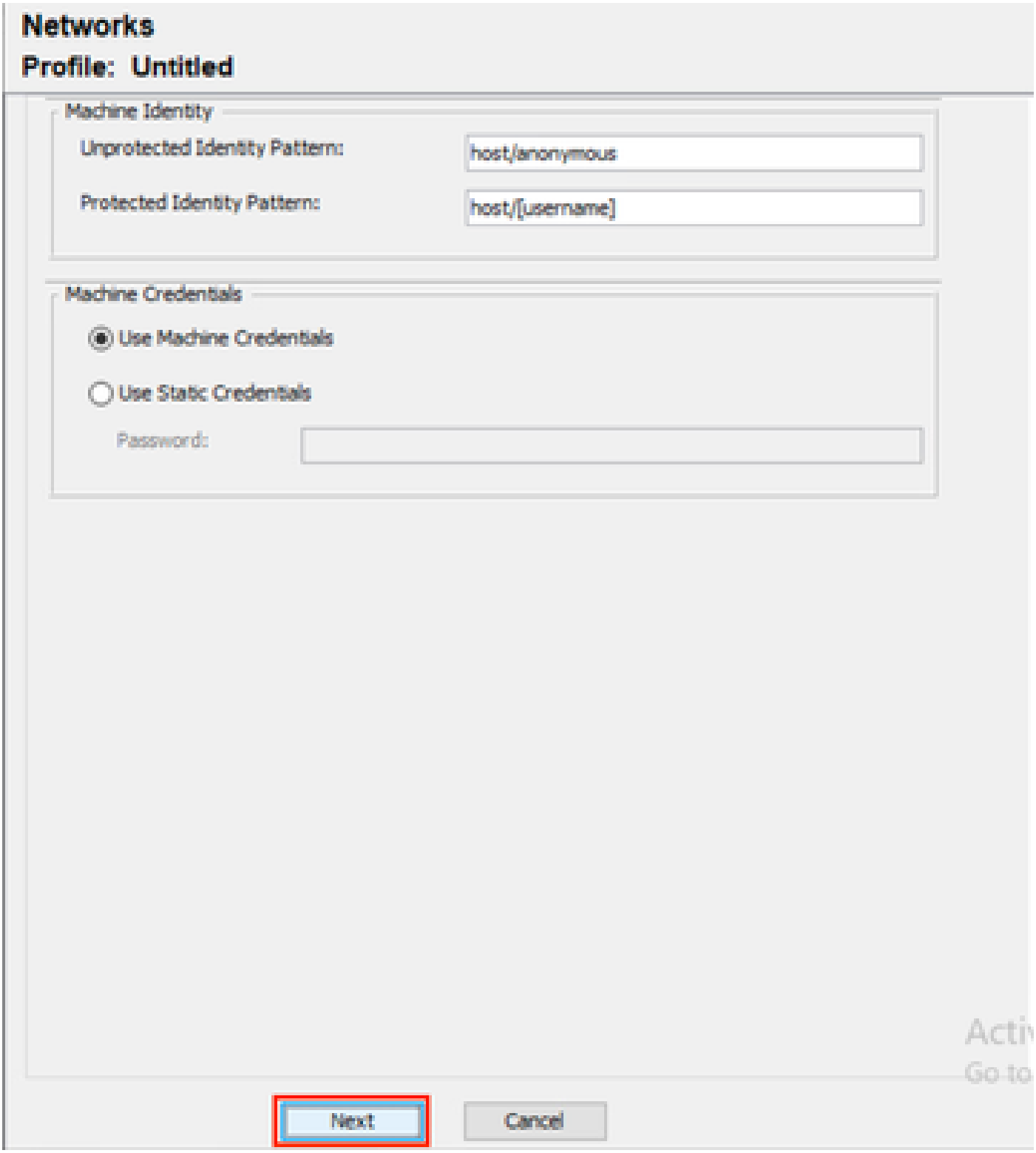
- 在Certificate Trusted Authority下，有兩個選項可用。
  在此案例中，會使用Trust any Root Certificate Authority(CA)選項（安裝在作業系統上），而不是新增特定CA證書。

  使用此選項，Windows裝置將信任由證書 — 當前使用者>受信任的根證書頒發機構>證書（由作業系統管理）中包含的證書簽名的任何EAP證書。
- 按一下下一步繼續。



NAM配置檔案編輯器證書

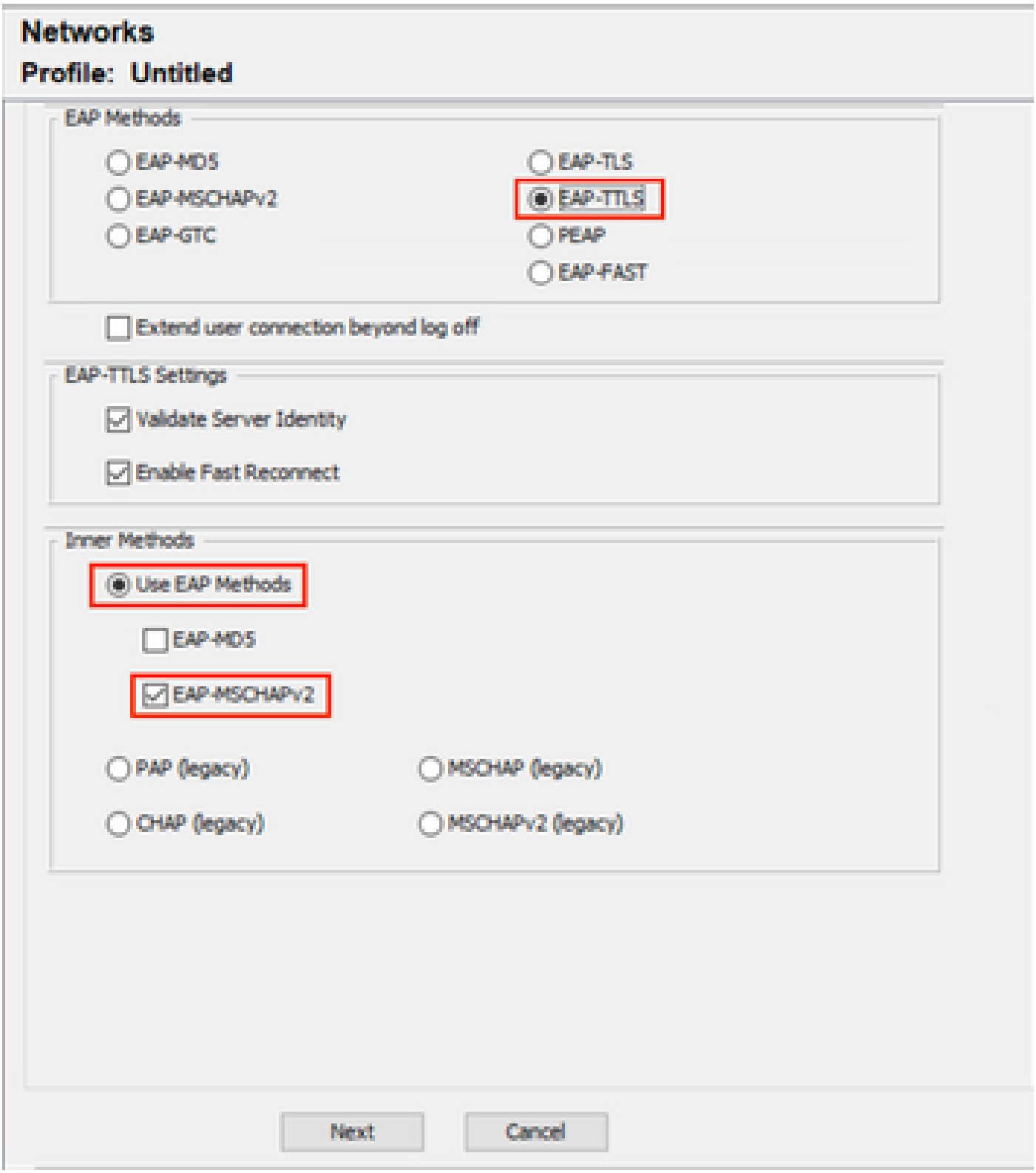
步驟6.在Machine Credentials部分，選擇Use Machine Credentials，然後按一下Next。



NAM配置檔案編輯器憑據

步驟7.配置用戶身份驗證部分。

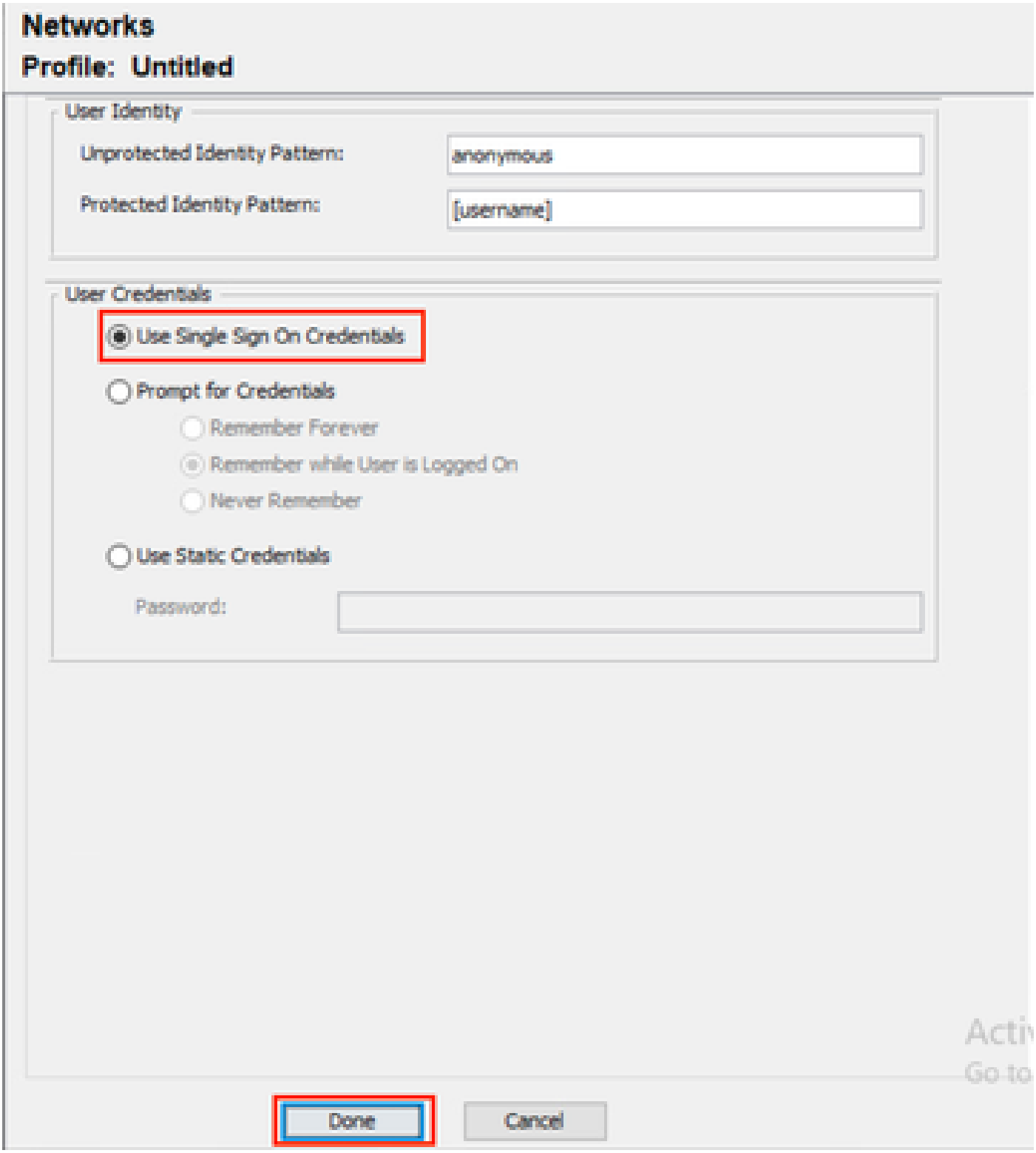
- 在EAP Methods下選擇EAP-TTLS。
- 在Inner Methods下，選擇Use EAP Methods，然後選擇EAP-MSCHAPv2。
- 按「Next」（下一步）。



NAM配置檔案編輯器使用者身份驗證

步驟8.在憑證中，設定步驟5所述的相同憑證驗證規則。

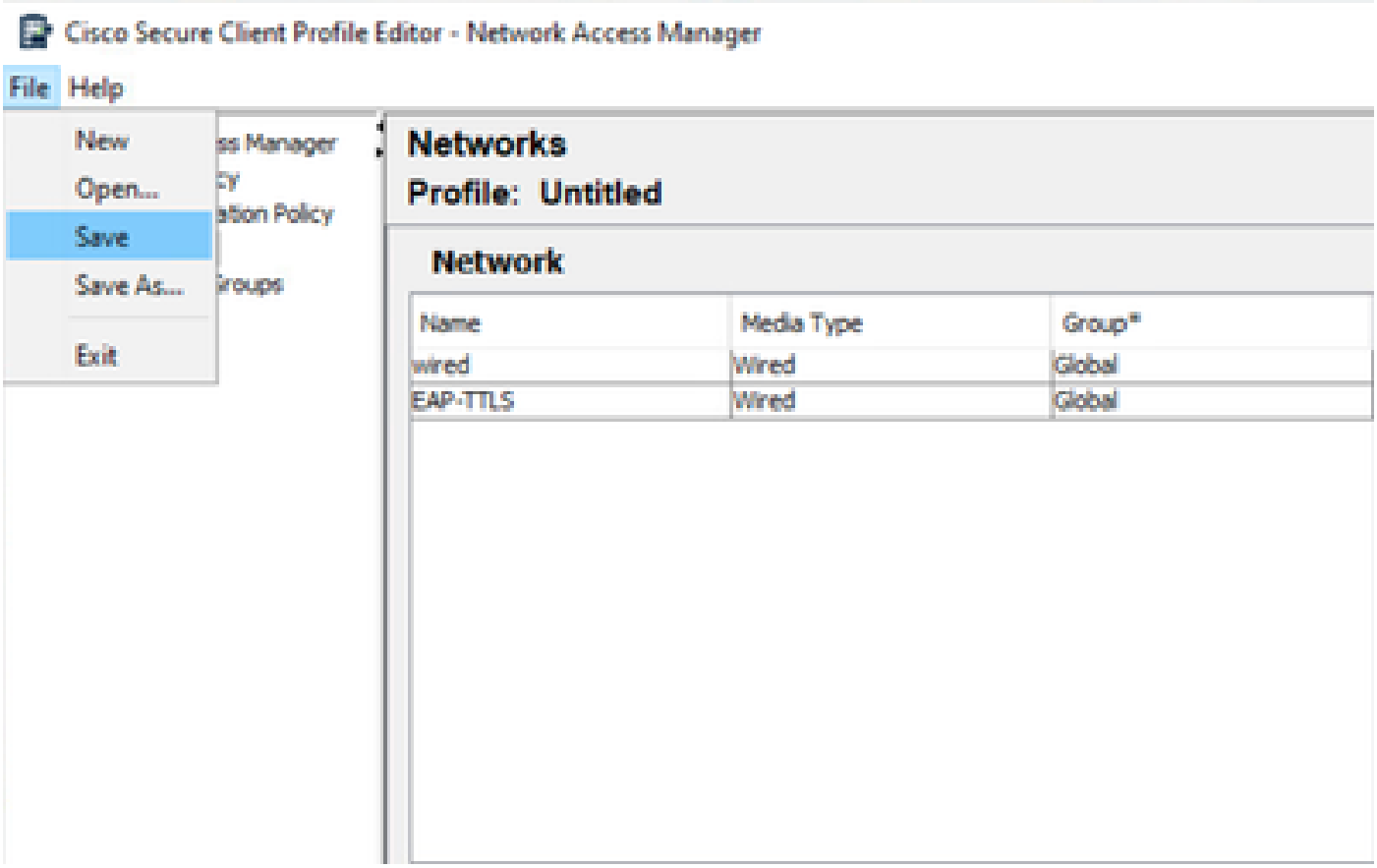
步驟9.在User Credentials中，選擇Use Single Sign-On Credentials，然後按一下Done。



NAM配置檔案編輯器使用者憑據

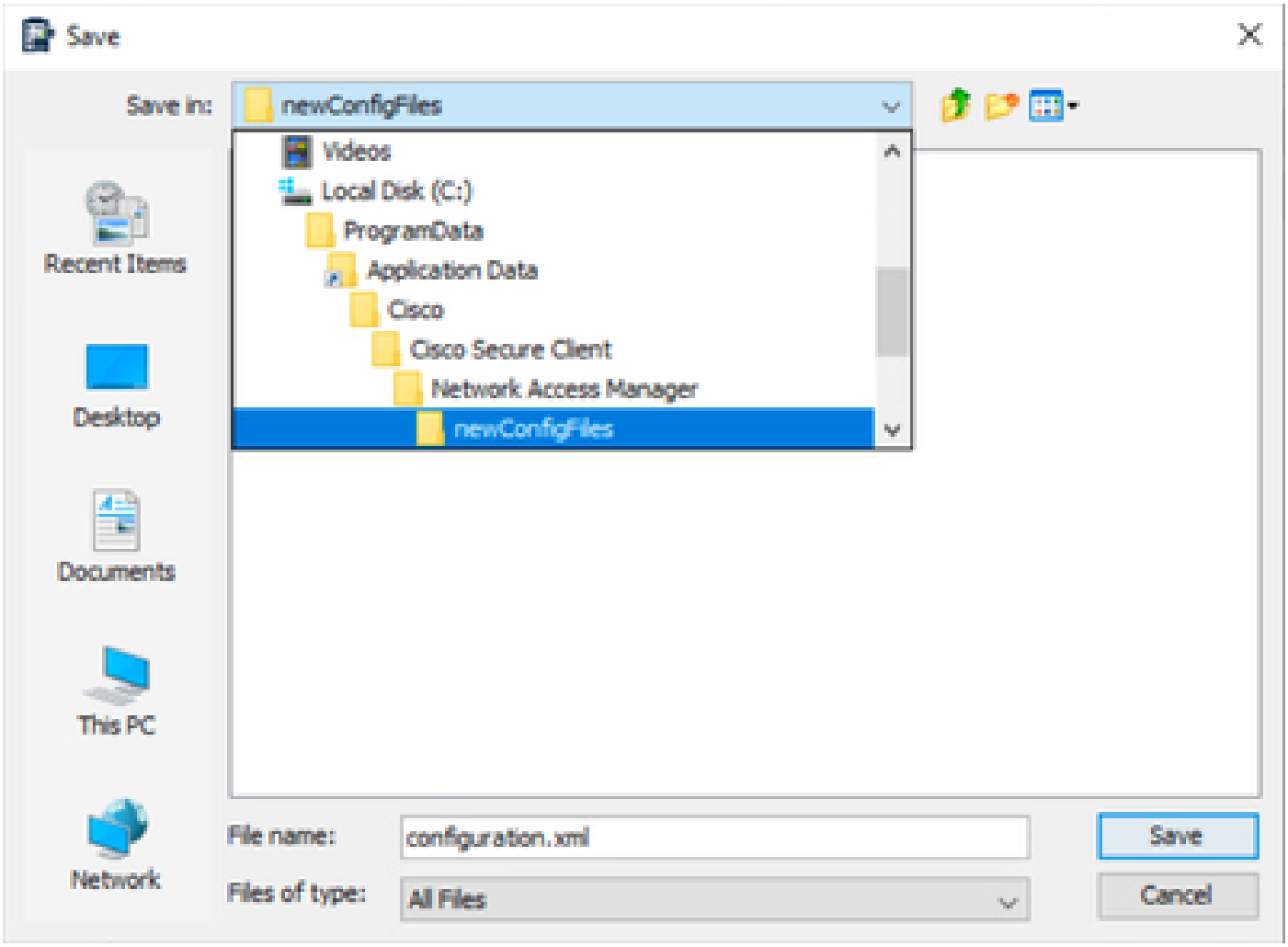
第6部分：儲存網路配置檔案

步驟1.按一下「File」>「Save」。



NAM配置檔案編輯器儲存網路配置

步驟2.在newConfigFiles資料夾中將檔案另存為configuration.xml。

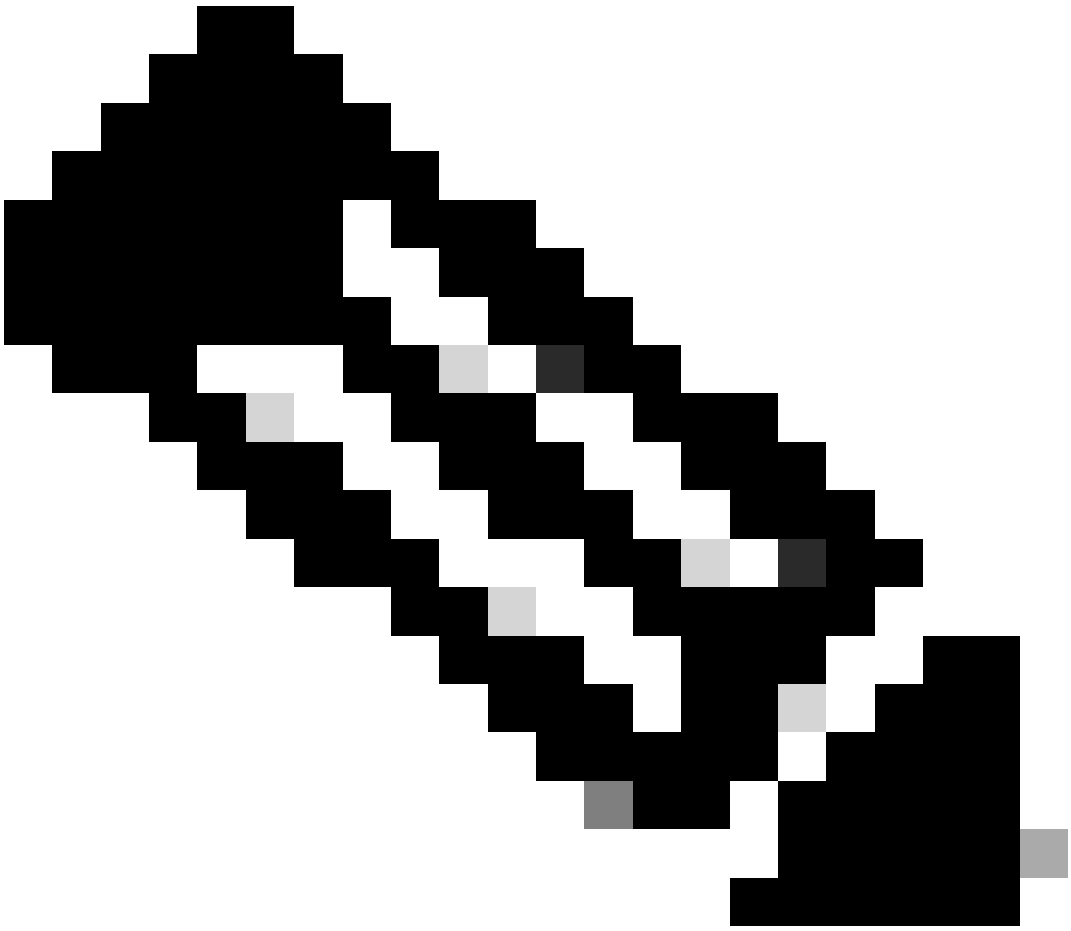


儲存網路配置

第7部分：在交換機上配置AAA

```
C9300-1#sh run aaa
!
aaa authentication dot1x default group labgroup
aaa authorization network default group labgroup
aaa accounting dot1x default start-stop group labgroup
aaa accounting update newinfo periodic 2880
!
!
!
!
aaa server radius dynamic-author
 client 10.76.112.135 server-key cisco
!
!
radius server labserver
 address ipv4 10.76.112.135 auth-port 1812 acct-port 1813
 key cisco
!
!
aaa group server radius labgroup
 server name labserver
!
```

```
!
!
!
aaa new-model
aaa session-id common
!
!



C9300-1(config)#dot1x system-auth-control
```



附註：dot1x system-auth-control命令不會顯示在show running-config輸出中，但需要該命令才能全域性啟用802.1X。

為802.1X配置交換機介面：

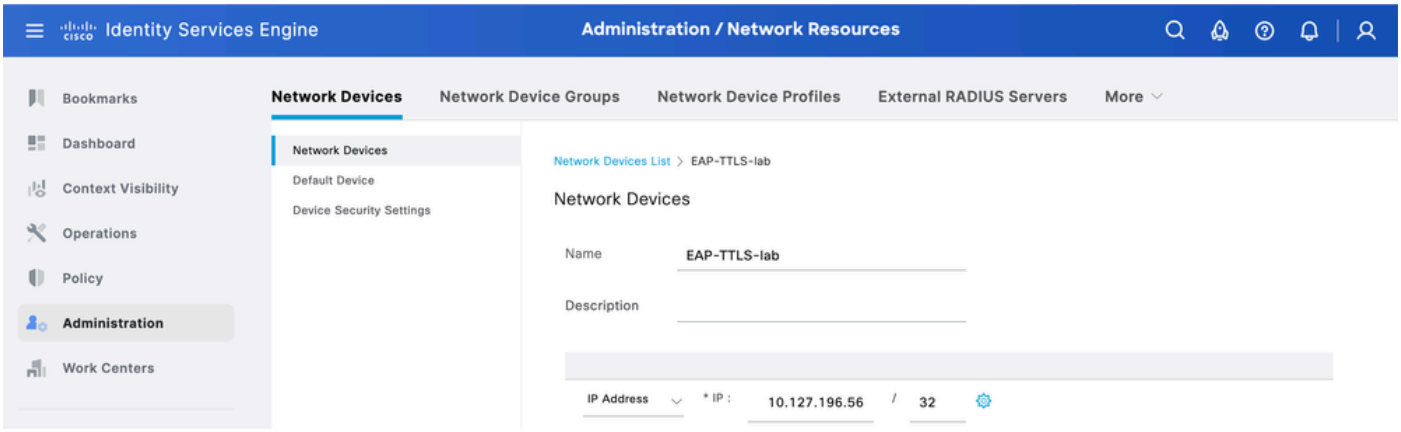
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

Current configuration : 242 bytes
!
interface GigabitEthernet1/0/44
 switchport access vlan 96
 switchport mode access
 device-tracking
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-auth
 authentication periodic

 mab
 dot1x pae authenticator
end
```

第8部分：ISE配置

步驟1.在ISE上配置交換機。

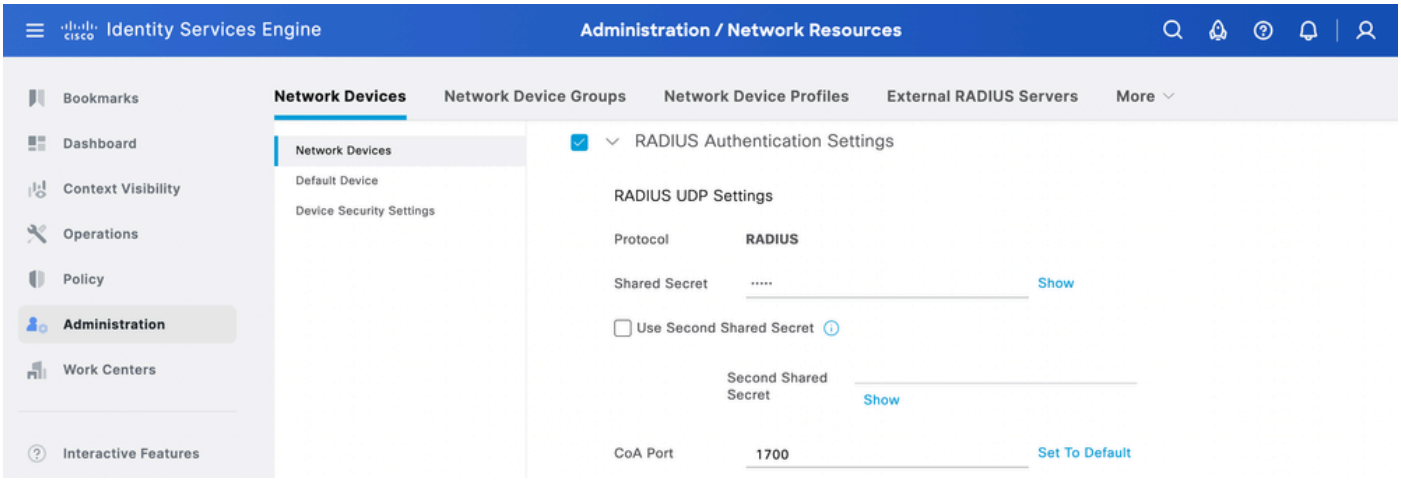
導覽至Administration > Network Resources > Network Devices，然後按一下Add。

在此處輸入交換機名稱和IP地址。



新增網路裝置ISE

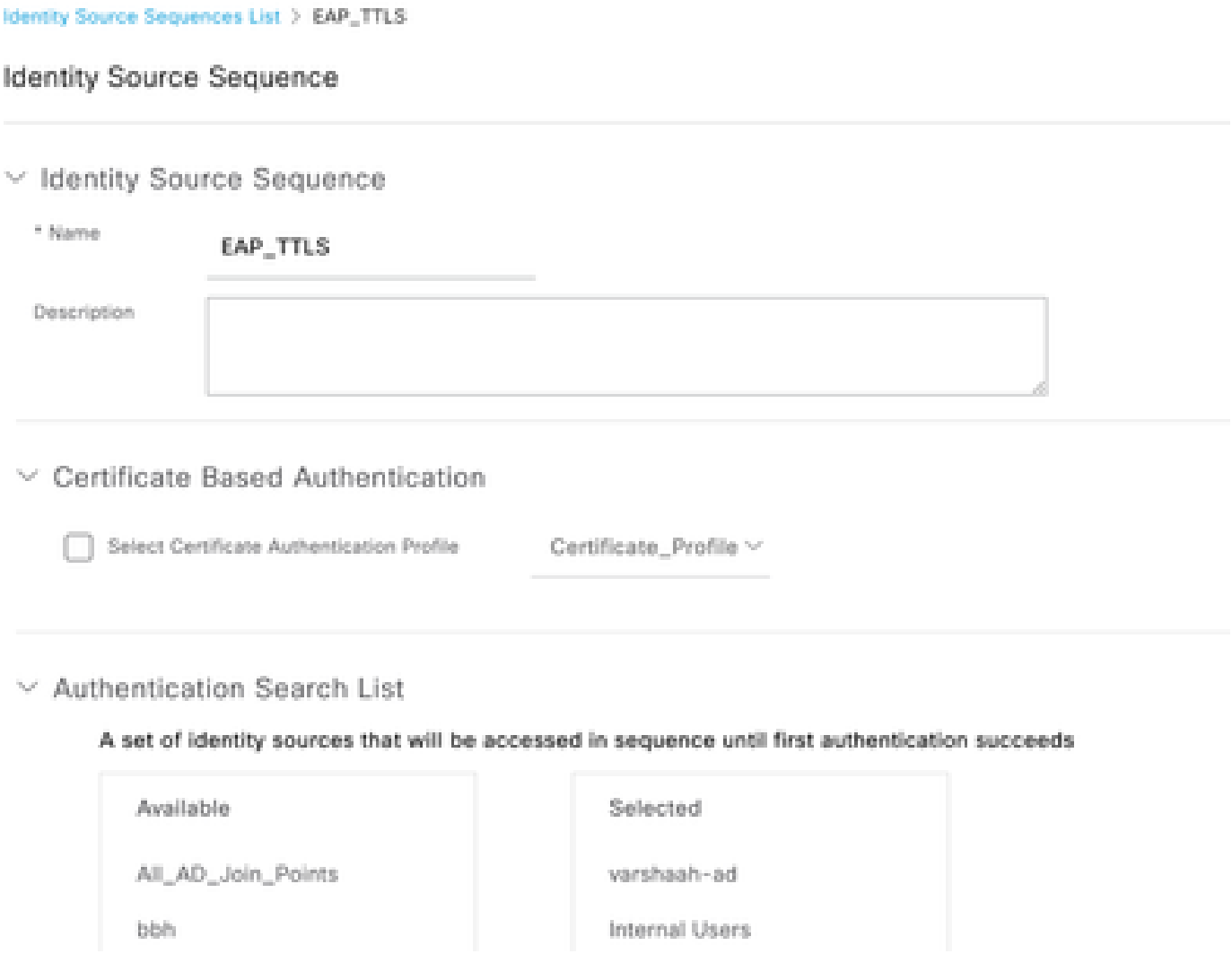
輸入RADIUS共用金鑰，與之前在交換機上配置的共用金鑰相同。



RADIUS共用密碼ISE

步驟2.配置身份源序列。

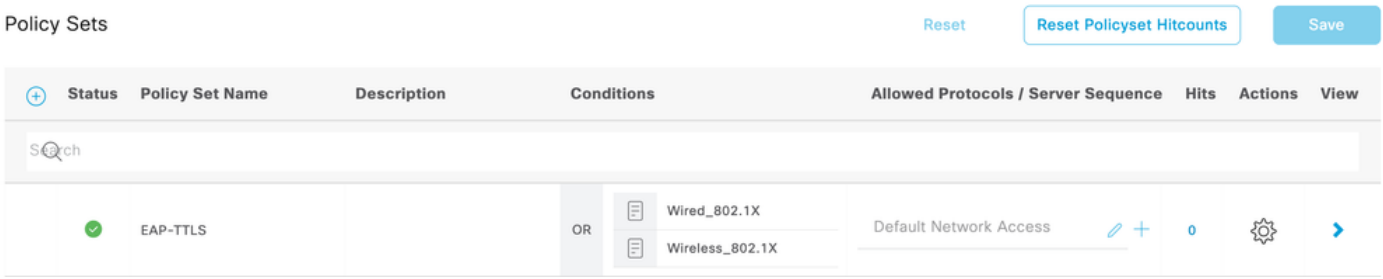
- 導航到管理>身份管理>身份源序列。
- 按一下Add以建立新的身份源序列。
- 在Authentication Search List下配置身份源。



ISE身份源序列

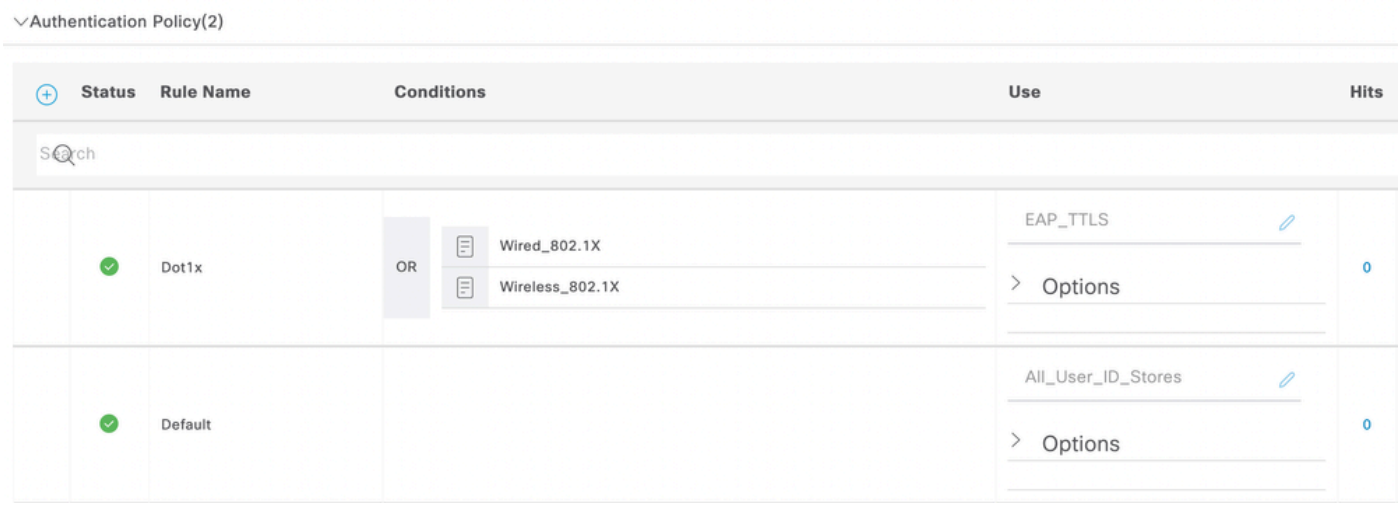
步驟3.配置策略集。

導航到Policy > Policy Sets，然後建立新的策略集。將條件配置為Wired_802.1x或Wireless_802.1x。對於Allowed Protocols，選擇Default Network Access:



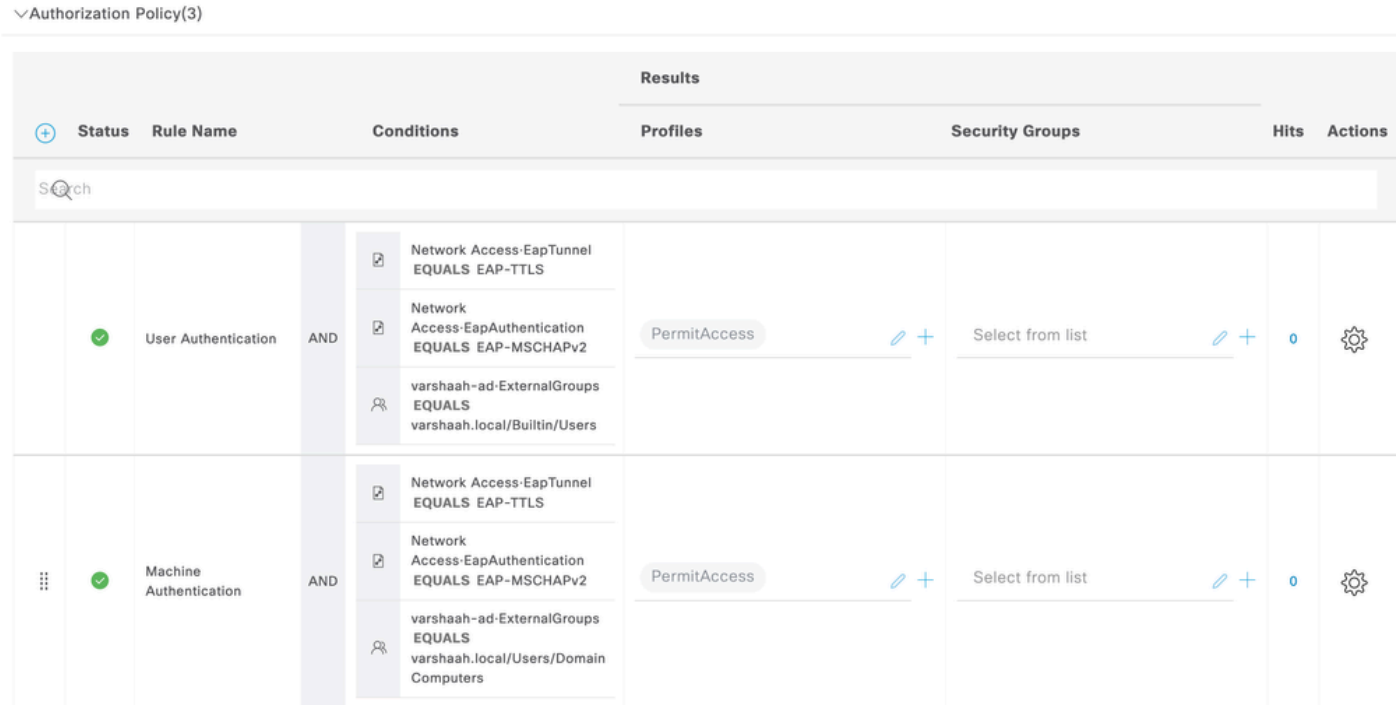
EAP-TTLS策略設定

為dot1x建立身份驗證策略，並選擇步驟4中建立的身份源序列。



EAP-TTLS身份驗證策略

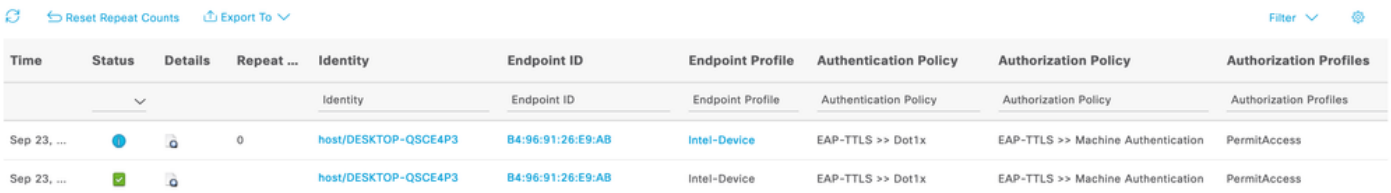
對於授權策略，請建立包含三個條件的規則。第一個條件檢查使用EAP-TTLS隧道的條件。第二個條件檢查EAP-MSCHAPv2是否用作內部EAP方法。第三個條件檢查各自AD組。



Dot1x授權策略

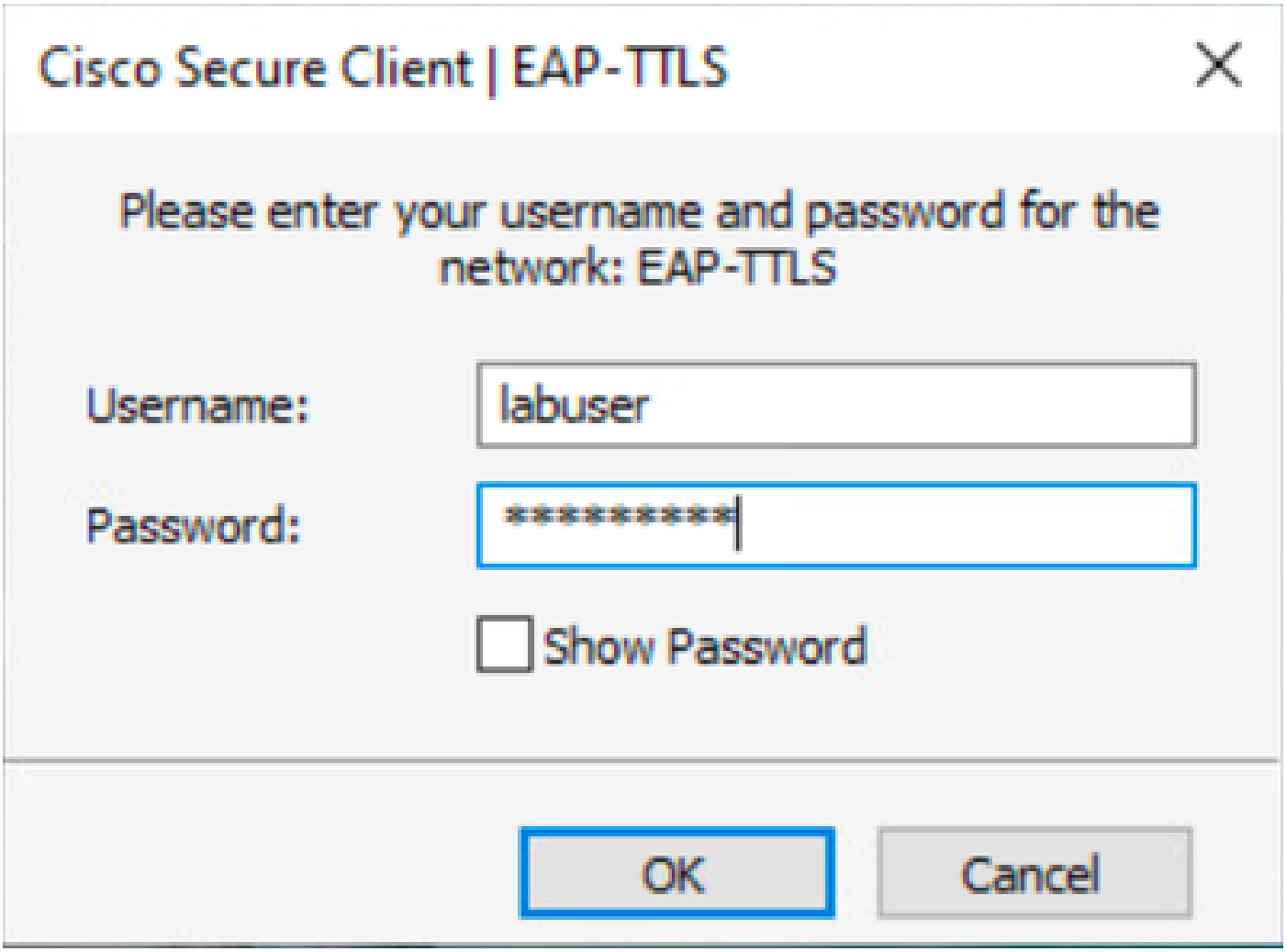
驗證

您可以重新啟動Windows 10電腦，也可以註銷然後登入。只要顯示windows登入螢幕，就會觸發電腦身份驗證。

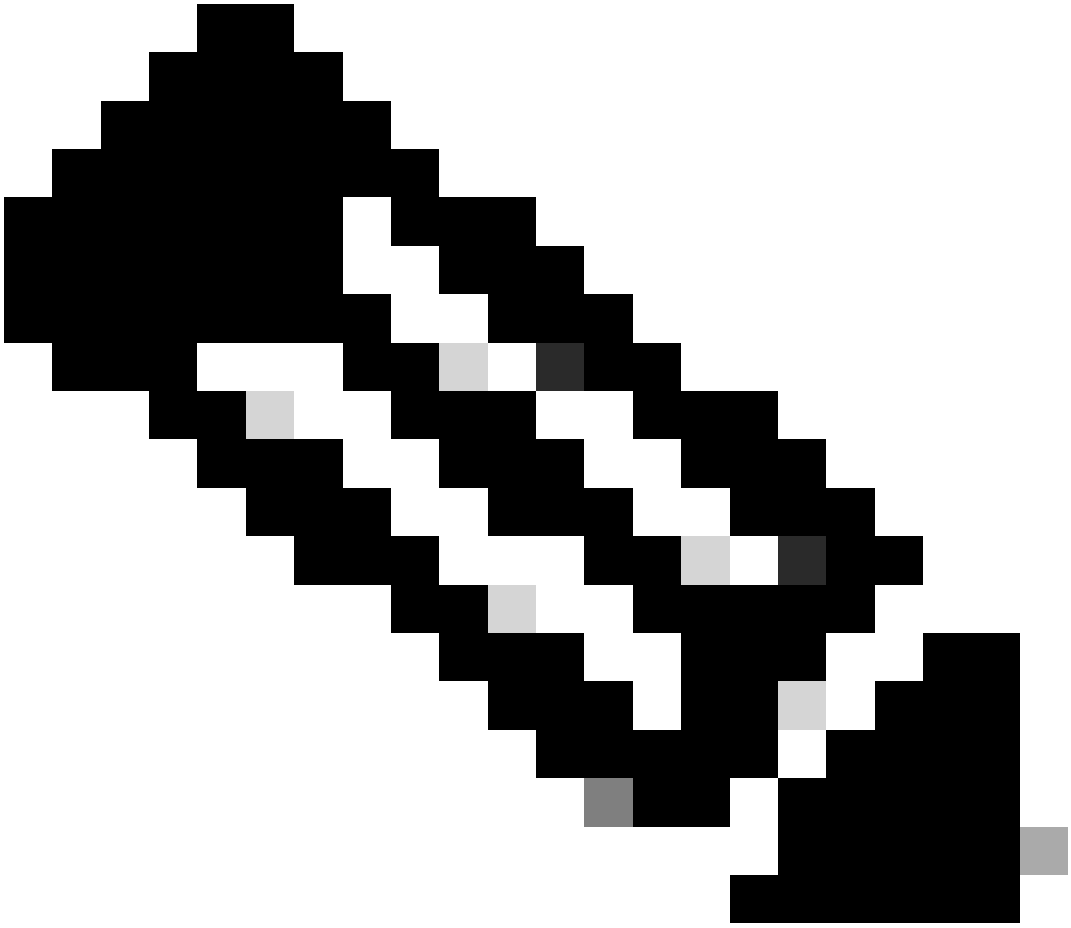


即時日誌電腦身份驗證

當您使用憑證登入到PC時，會觸發使用者身份驗證。

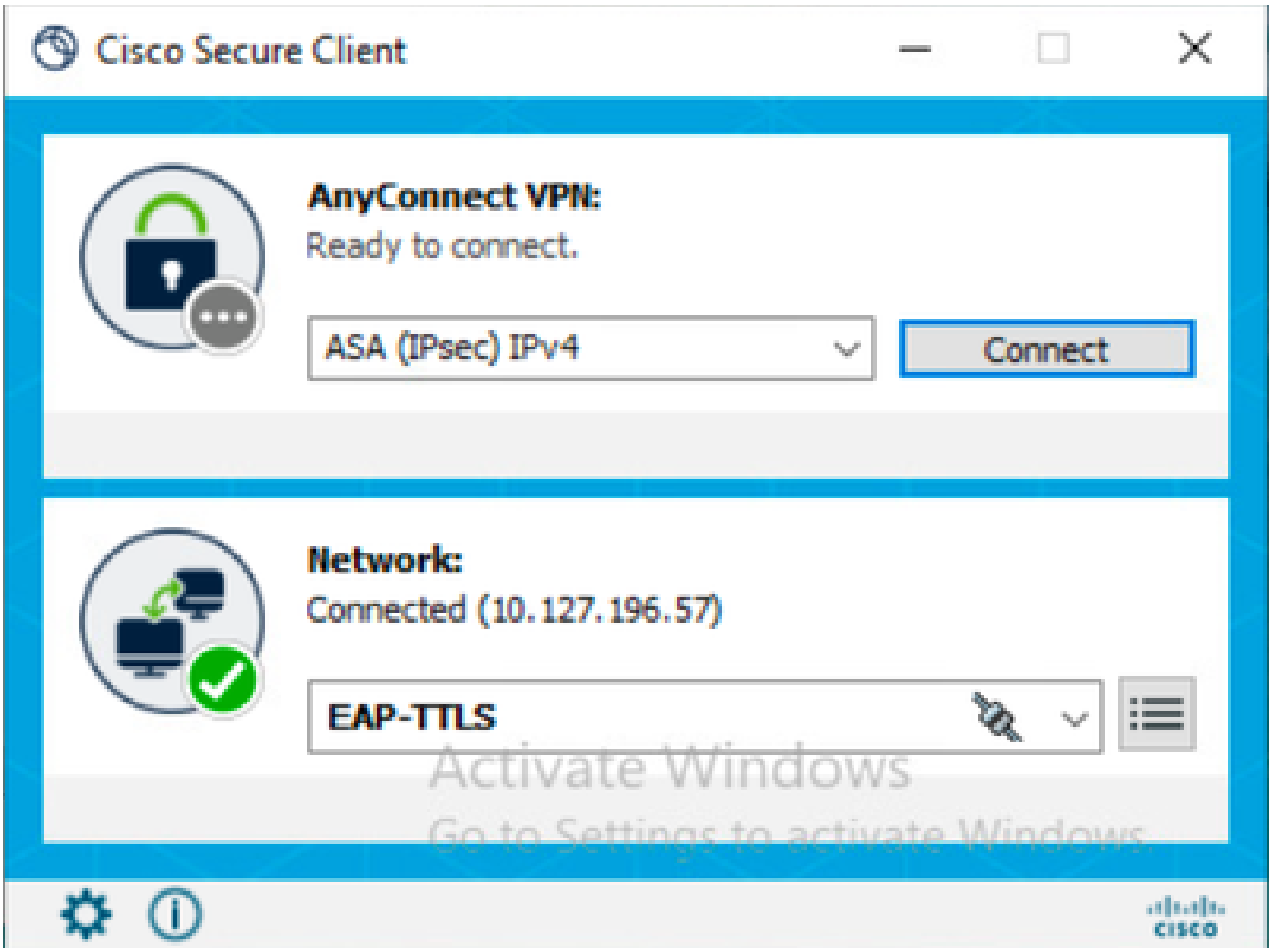

Cisco Secure Client | EAP-TTLS
Please enter your username and password for the network: EAP-TTLS
Username:
labuser
Password:
****
Show Password
OK
Cancel

使用者身份驗證憑據

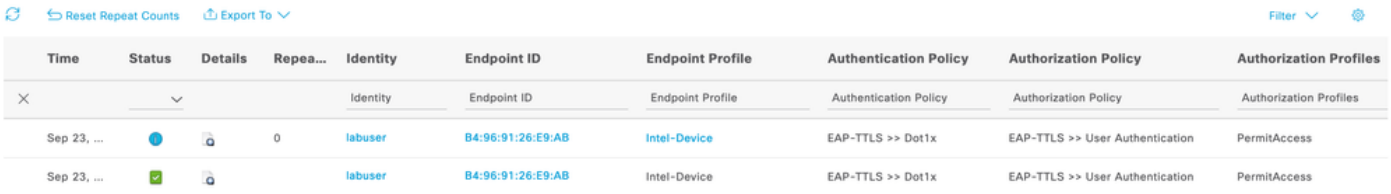


附註：此示例使用Active Directory使用者憑據進行身份驗證。或者，您也可以在思科ISE中建立內部使用者並使用這些憑證登入。

在輸入憑證並成功驗證後，終端通過使用者身份驗證連線到網路。



已連線EAP-TTLS



Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
Sep 23, ...			0	labuser	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> User Authentication	PermitAccess
Sep 23, ...				labuser	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> User Authentication	PermitAccess

即時日誌使用者身份驗證

分析ISE RADIUS即時日誌

本節說明了用於成功進行電腦身份驗證和使用者身份驗證的RADIUS即時日誌條目。

機器驗證

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** **11806**

Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24431 Authenticating machine against Active Directory - varshaah-ad 24325 Resolving identity - host/DESKTOP-QSCE4P3 ... ... 24343 RPC Logon request succeeded - DESKTOP-QSCE4P3$@varshaah.local **24470 Machine authentication against Active Directory is successful - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - host/DESKTOP-QSCE4P3 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

使用者驗證

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - labuser@varshaah.local ... ... 24343 RPC Logon request succeeded - labuser@varshaah.local **24402 User authentication against Active Directory succeeded - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - labuser 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

分析NAM日誌

NAM日誌（尤其是在啟用擴展日誌記錄之後）包含大量資料，其中大部分資料是無關的，可以忽略。本部分列出調試行，以演示NAM建立網路連線的每個步驟。當您處理日誌時，這些關鍵短語有助於查詢日誌中與問題相關的部分。

機器驗證

```
2160: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: 80
```

客戶端收到來自網路交換機的EAP-TTLS資料包，並啟動EAP-TTLS會話。這是電腦身份驗證隧道的

起點。

```
2171: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: EA
2172: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
2173: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
```

客戶端從ISE接收Server Hello，並開始驗證伺服器證書(CN=varshaah.varshaah.local)。 在客戶端的信任儲存中找到證書並新增以進行驗證。

```
2222: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Validating th
2223: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Server certif
```

已成功驗證伺服器證書，從而完成了TLS隧道的建立。

```
2563: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2564: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: NE
2565: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

客戶端發出已通過身份驗證的訊號。介面被解除阻止，並且內部狀態電腦將轉換為USER_T_NOT_DISCONNECTED，表示電腦現在可以傳遞流量。

```
2609: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2610: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2611: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2612: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2613: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2614: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2615: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

介面卡報告authenticated,NAM AccessStateMachine將轉換為ACCESS_AUTHENTICATED。這確認電腦已成功完成身份驗證並具有完全網路訪問許可權。

使用者驗證

```
100: DESKTOP-QSCE4P3: Sep 25 2025 14:01:26.669 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Network EAP-TT
```

NAM客戶端開始EAP-TTLS連線過程。

```
195: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Binding adapte
198: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
```

NAM將物理介面卡繫結到EAP-TTLS網路並進入ACCESS_ATTACHED狀態，確認介面卡已準備好進行身份驗證。

```
204: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
247: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3680][comp=SAE]: STAT
```

從802.1X交換開始，客戶端從ATTACHED轉換到CONNECTING。

```
291: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.388 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
```

客戶端傳送EAPOL-Start以觸發身份驗證過程。

```
331: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: PORT
332: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
340: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: EAP
```

交換機請求身份，客戶端準備使用外部身份進行響應。

```
402: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9580]: EAP-CB: creden
422: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: processin
460: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

NAM傳送外部標識。預設情況下，此值為anonymous，表示交換用於使用者身份驗證（而不是電腦）。

```
488: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP sugges
489: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP reques
490: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: EAP metho
491: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

客戶端和伺服器都同意使用EAP-TTLS作為外部方法。

```
660: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
661: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
```

客戶端傳送Client Hello並接收Server Hello，其中包括ISE證書。

```
706: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: 802
717: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
718: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
719: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
726: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
```

將顯示伺服器證書。客戶端查詢CN varshaah.varshaah.local，找到匹配項並驗證證書。握手在檢查X.509證書時暫停。

```
729: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
730: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EAP
1110: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1111: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

隧道已建立。NAM現在請求並準備受保護的身份和憑據以進行內部身份驗證。

```
1527: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1528: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1573: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1574: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1575: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
```

TLS握手完成。現在已建立用於內部驗證的安全隧道。

```
1616: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-6-INFO_MSG: %[tid=9664]: Protected iden
1620: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
1689: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
```

受保護身份（使用者名稱）由ISE傳送和接受。

```
1708: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9456][comp=SAE]: EAP
1738: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.758 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Protected pas
1741: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.200 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

ISE請求密碼。NAM在TLS隧道內傳送受保護的密碼。

```
1851: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1852: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: ST
1853: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1854: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: ST
1855: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: ST
```

ISE驗證密碼、傳送EAP-Success和NAM轉換為AUTHENTICATED。此時，使用者身份驗證已完成，並且允許客戶端訪問網路。

疑難排解

在排除與思科ISE和交換機整合有關的網路訪問管理器(NAM)問題時，必須從所有三個元件收集日誌：安全客戶端(NAM)、思科ISE和交換器。

安全使用者端(NAM)日誌

1. 按照以下步驟啟用NAM擴展日誌記錄。
2. 重現問題。如果網路配置檔案不適用，請在安全客戶端中運行Network Repair。
3. 使用診斷和報告工具(DART)收集DART捆綁包。

思科ISE日誌

在ISE上啟用這些調試以捕獲身份驗證和目錄互動：

- 運行時AAA
- nsf
- nsf-session

交換機日誌

基本調試

```
request platform software trace rotate all
set platform software trace smd switch active R0 radius debug
set platform software trace smd switch active R0 aaa debug
set platform software trace smd switch active R0 dot1x-all debug
set platform software trace smd switch active R0 eap-all debug
debug radius all
```

高級調試（如果需要）

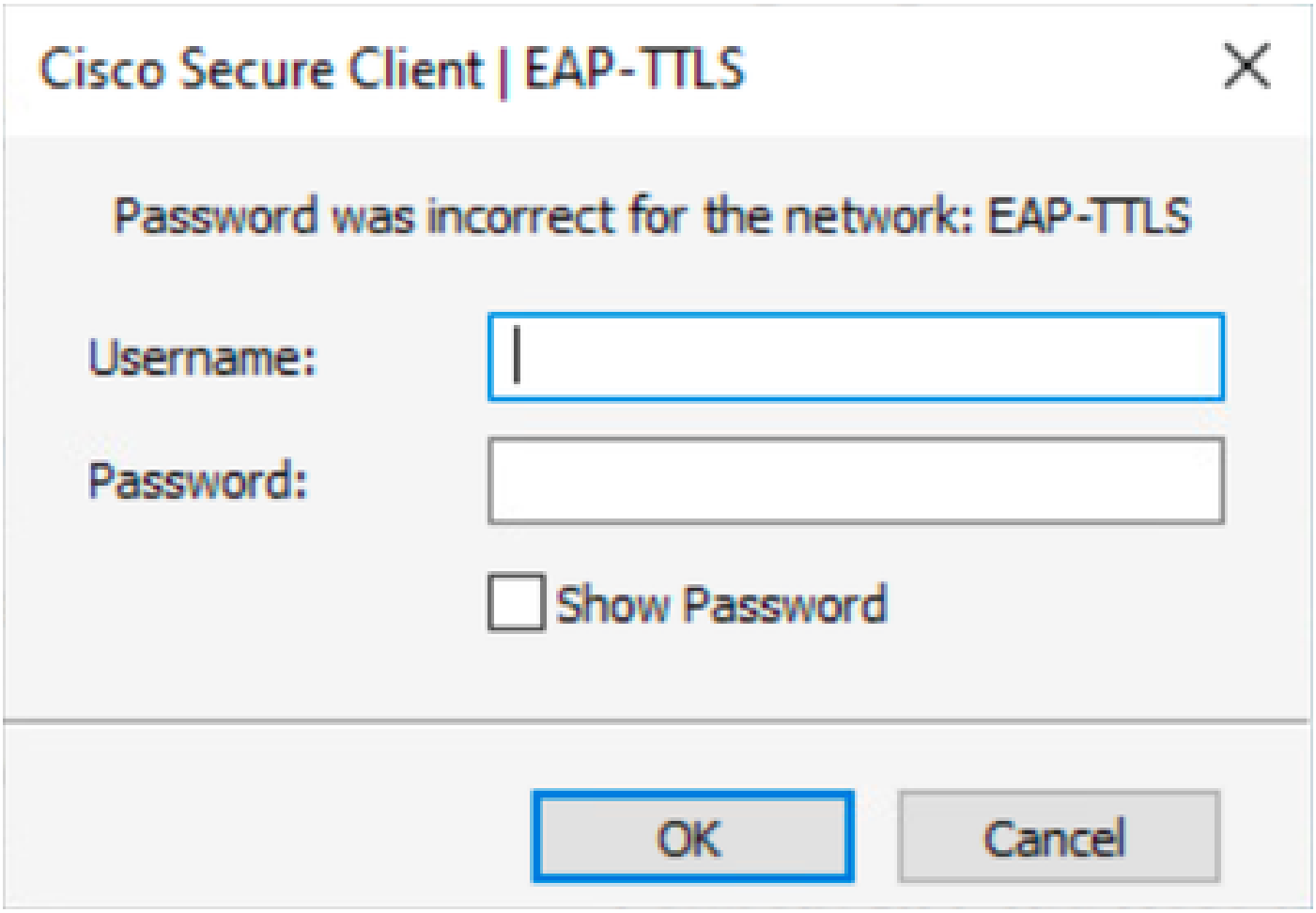
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

顯示命令

```
show version
show debugging
show running-config aaa
show authentication session interface gix/x details
show dot1x interface gix/x
show aaa servers
show platform software trace message smd switch active R0
```

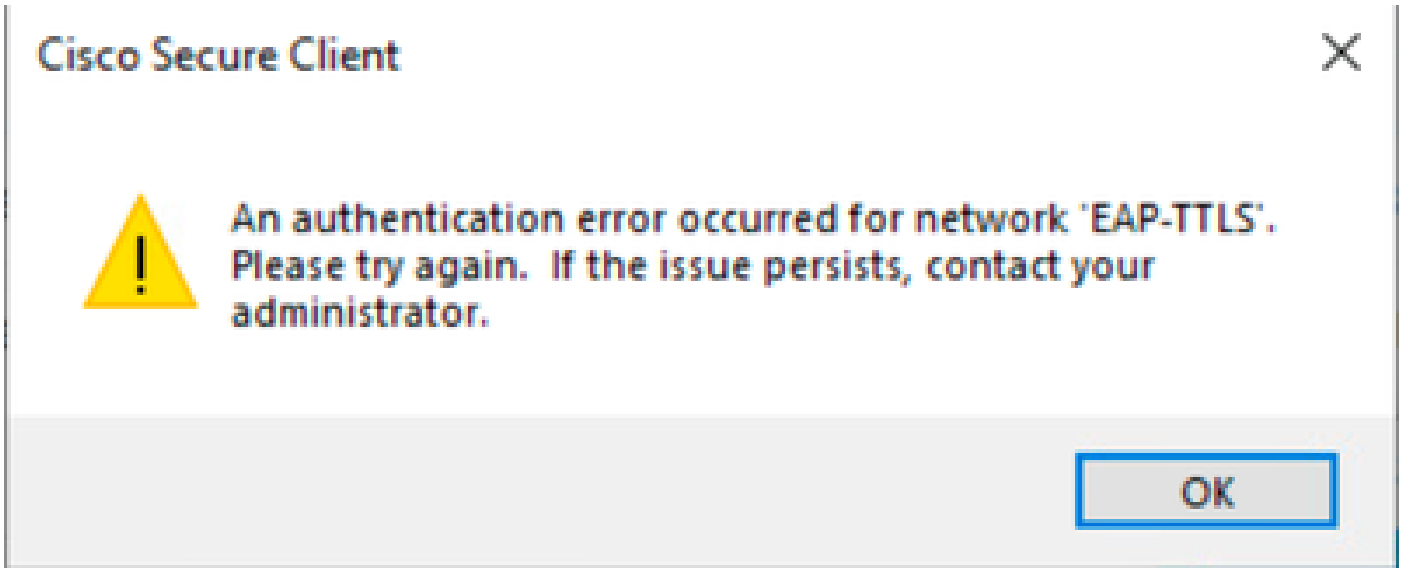
由於憑據無效，使用者身份驗證失敗

當使用者輸入不正確的憑證時，安全客戶端會顯示網路的通用密碼不正確：「EAP-TTLS」消息。螢幕上的錯誤沒有指定問題是由無效的使用者名稱還是密碼造成的。



錯誤密碼錯誤

如果身份驗證連續兩次失敗，安全客戶端將顯示以下消息：網路「EAP-TTLS」出現身份驗證錯誤。 請重試。如果問題仍然存在，請與管理員聯絡。



使用者身份驗證問題

要確定原因，請檢視NAM日誌。

1.密碼不正確：

當使用者輸入不正確的密碼時，NAM日誌會顯示類似於以下輸出的條目：

```
3775: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3776: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3777: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.922 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
```

在Cisco ISE即時日誌中，相應的事件顯示為：

Event	5400 Authentication failed
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Root cause	User authentication against Active Directory failed since user has entered the wrong password

密碼不正確

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity 10 **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge 0** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 0 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 0 **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - varshaah-ad 0 24430 Authenticating user against Active Directory - varshaah-ad 0 24325 Resolving identity - labuser@varshaah.local 4 24313 Search for matching accounts at join point - varshaah.local 0 24319 Single matching account found in forest - varshaah.local 0 24323 Identity resolution detected single matching account 0 **24344 RPC Logon request failed - STATUS_WRONG_PASSWORD, ERROR_INVALID_PASSWORD, labuser@varshaah.local 20 24408 User authentication against Active Directory failed since user has entered the wrong password - varshaah-ad 1** ... ... 11823 EAP-MSCHAP authentication attempt failed ... ... 11815 Inner EAP-MSCHAP authentication failed 0 ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11003 Returned RADIUS Access-Reject

2.使用者名稱不正確：

當使用者輸入不正確的使用者名稱時，NAM日誌會顯示類似以下輸出的條目：

```
3788: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3789: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300]: EAP-CB: EAP
```

在Cisco ISE即時日誌中，相應的事件顯示為：

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resoultion settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).

使用者名稱不正確

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-**

MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated ... ... 15013 Selected Identity Source - All_AD_Join_Points 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - user@varshaah.local 24313 Search for matching accounts at join point - varshaah.local ... ... 24352 Identity resolution failed - ERROR_NO_SUCH_USER **24412 User not found in Active Directory - varshaah-ad** ... ... 15013 Selected Identity Source - Internal Users 24210 Looking up User in Internal Users IDStore - user **24216 The user is not found in the internal users identity store** ... ... 22056 Subject not found in the applicable identity store(s) 22058 The advanced option that is configured for an unknown user is used 22061 The 'Reject' advanced option is configured in case of a failed authentication request **11823 EAP-MSCHAP authentication attempt failed** ... ... **11815 Inner EAP-MSCHAP authentication failed** ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11504 Prepared EAP-Failure 1 **11003 Returned RADIUS Access-Reject**

已知瑕疵

錯誤ID	說明
思科錯誤ID 63395	ISE 3.0在服務重新啟動後找不到REST ID儲存

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）。