使用Windows和ISE 3.2為Dot1x配置安全客戶端NAM

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

設定

- 網路圖表
- 組態
  - 1.下載並安裝安全客戶端NAM（網路訪問管理器）
  - 2.下載並安裝安全客戶端NAM配置檔案編輯器。
  - 3.常規預設配置
  - 4.案例1:為PEAP(MS-CHAPv2)使用者身份驗證配置安全客戶端NAM請求方
  - 5.案例2:為EAP-FAST同步使用者和電腦身份驗證配置安全客戶端NAM請求方
  - 6.案例3:為EAP TLS使用者證書身份驗證配置安全客戶端NAM請求方
  - 7.配置ISR 1100和ISE以允許基於方案1 PEAP MSCHAPv2的身份驗證

驗證

疑難排解

- 問題:安全客戶端未使用NAM配置檔案。
- 問題2:需要收集日誌以進行進一步分析。
  - 1.啟用NAM擴展日誌
  - 2.重現問題。
  - 3.收集安全客戶端DART捆綁包。

相關資訊

簡介

本文描述如何在Windows上配置安全客戶端網路分析模組(NAM)。

必要條件

需求

思科建議您瞭解以下主題：

- 對RADIUS請求者的基本瞭解
- Dot1x
- PEAP
- PKI

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Windows 10 Pro版本22H2，內建19045.3930
- ISE 3.2
- 思科C1117 Cisco IOS® XE軟體版本17.12.02
- Active Directory 2016

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。

背景資訊

本文檔介紹如何在Windows上配置安全客戶端NAM。使用預部署選項和配置檔案編輯器執行dot1x身份驗證。此外，還提供了如何實現此目標的一些示例。

在網路中，請求方是點對點LAN網段一端的實體，該網段尋求由連線到鏈路另一端的身份驗證器進行身份驗證。

IEEE 802.1X標準使用術語「請求方」來指代硬體或軟體。在實踐中，請求方是安裝在終端使用者電腦上的軟體應用程式。

使用者呼叫請求方並提交憑證以將電腦連線到安全網路。如果驗證成功，驗證器通常允許電腦連線到網路。

關於網路訪問管理器

Network Access Manager是一種客戶端軟體，根據策略提供安全的第2層網路。

它檢測並選擇最佳第2層接入網路，並對有線和無線網路的訪問執行裝置身份驗證。

Network Access Manager管理使用者和裝置身份以及安全訪問所需的網路訪問協定。

它可以智慧地工作，防止終端使用者進行違反管理員定義的策略的連線。

網路訪問管理器設計為單宿主，一次只允許一個網路連線。

此外，有線連線的優先順序高於無線，因此，如果您通過有線連線插入網路，無線介面卡會變為禁用狀態，且沒有IP地址。

設定

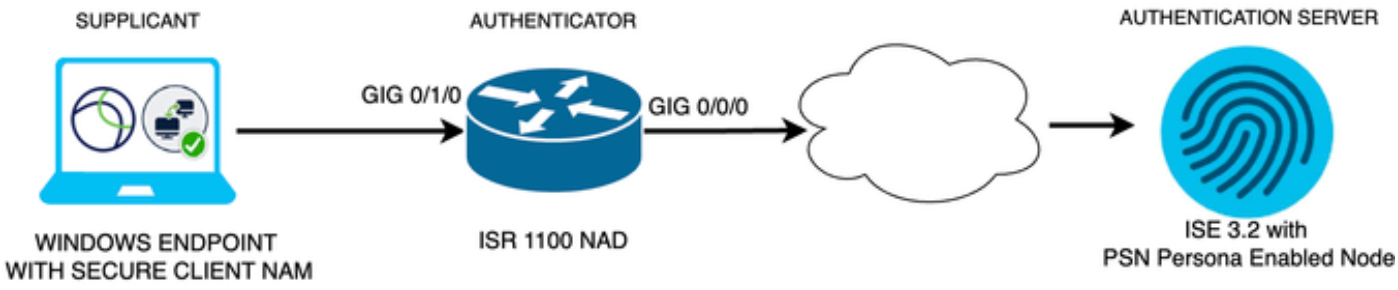
網路圖表

對於dot1x身份驗證，需要3個部分；

1. 能夠執行dot1x的請求方，

2. 身份驗證器也稱為NAS/NAD，用作封裝RADIUS內dot1x流量的代理，
3. 和身份驗證伺服器。

在本示例中，以不同方式安裝和配置請求方。稍後，顯示一個包含網路裝置配置和身份驗證伺服器的場景。



網路圖表

組態

1. 下載並安裝安全客戶端NAM（網路訪問管理器）。

2. 下載並安裝安全客戶端NAM配置檔案編輯器。
3. 常規預設配置
4. 案例 1:配置用於PEAP(MS-CHAPv2)使用者身份驗證的安全客戶端NAM請求方。
5. 案例 2:配置使用者和電腦身份驗證時，同時為EAP-FAST配置安全客戶端NAM請求方。
6. 案例3第1部分：為EAP-TLS配置安全客戶端NAM請求方。
7. 案例3第2部分：配置NAD和ISE演示。

1.下載並安裝安全客戶端NAM（網路訪問管理器）

[思科軟體下載]

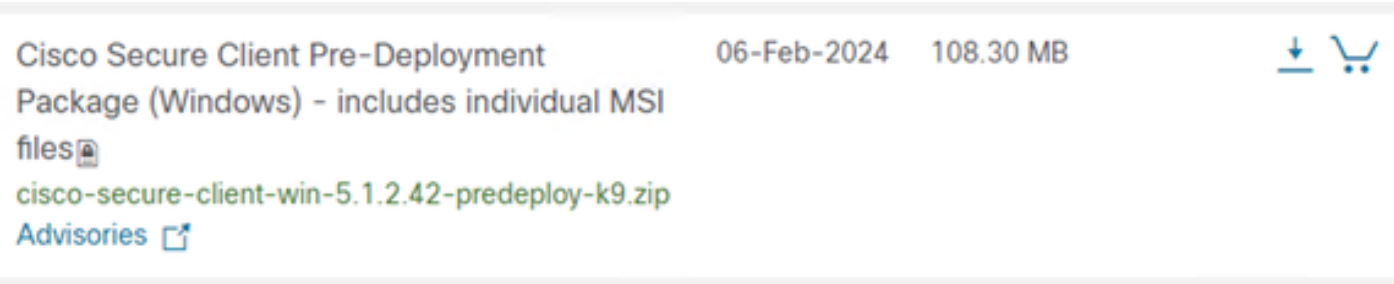
在產品名稱搜尋欄上鍵入Secure Client 5。

下載Home > Security > VPN and Endpoint Security Clients > Secure Client（包括AnyConnect）> Secure Client 5 > AnyConnect VPN Client Software。

在此配置示例中，使用的是5.1.2.42版。

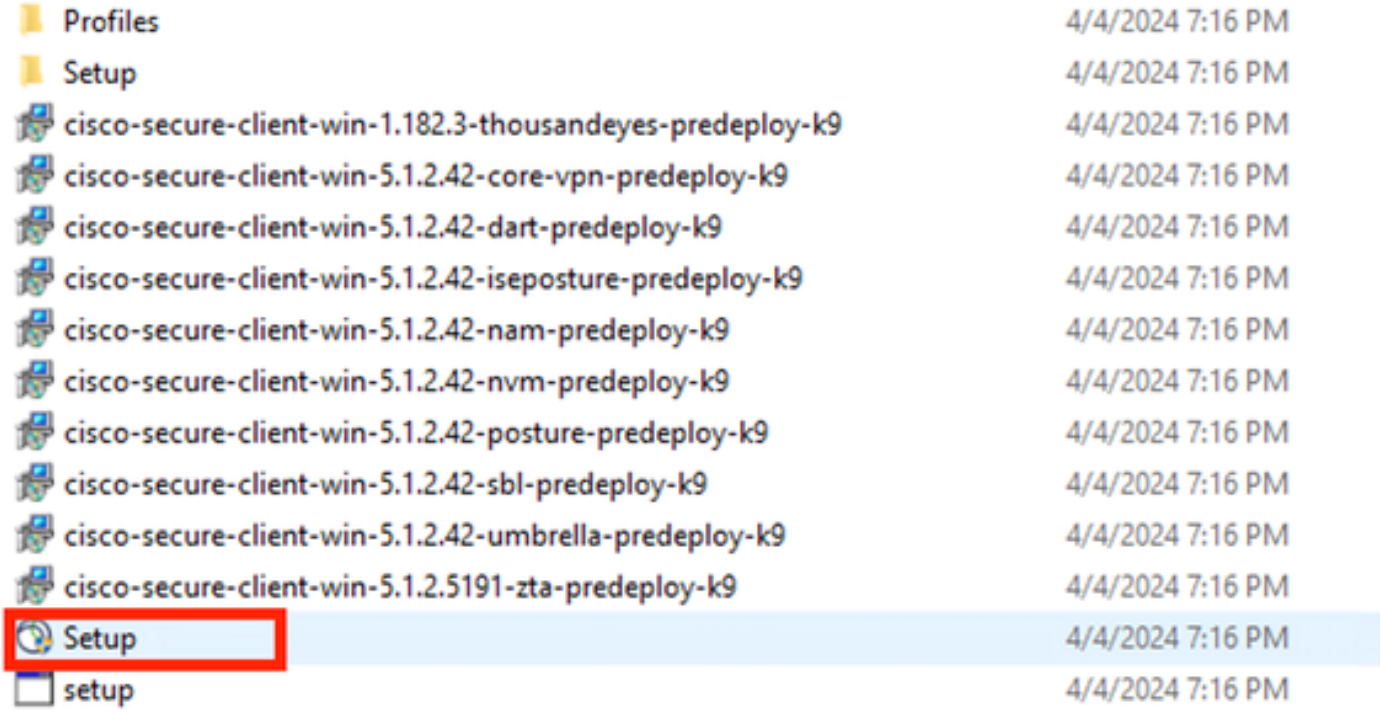
將Secure Client部署到Windows裝置的方法有多種；從SCCM、從身份服務引擎和VPN頭端。但是，在本文中，使用的安裝方法是預部署方法。

在該頁面上，搜尋思科安全客戶端頭端部署包(Windows)檔案。



Msi zip檔案

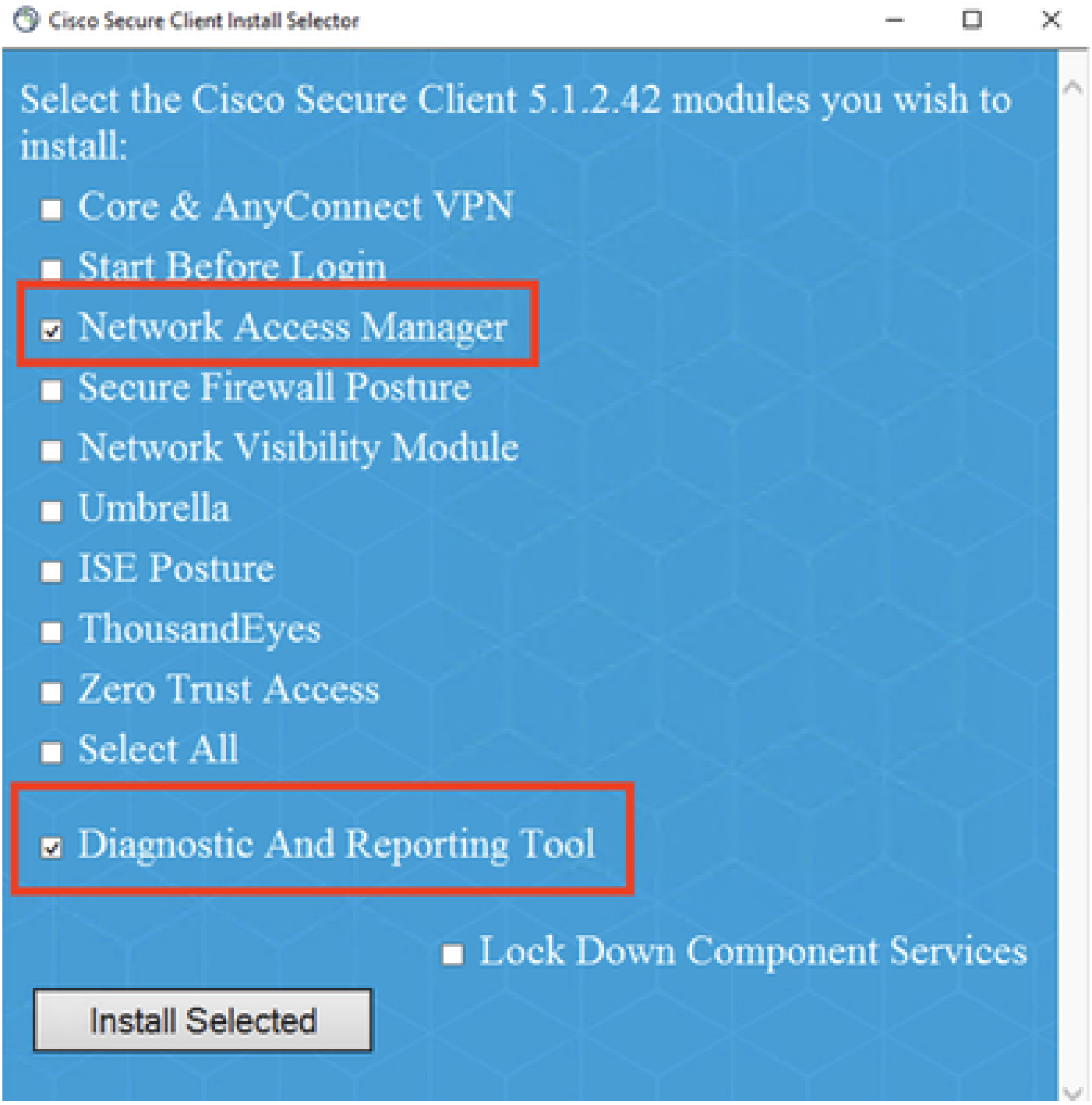
下載並解壓後，按一下「Setup」。



安全客戶端檔案

安裝網路訪問管理器和診斷和報告工具模組。

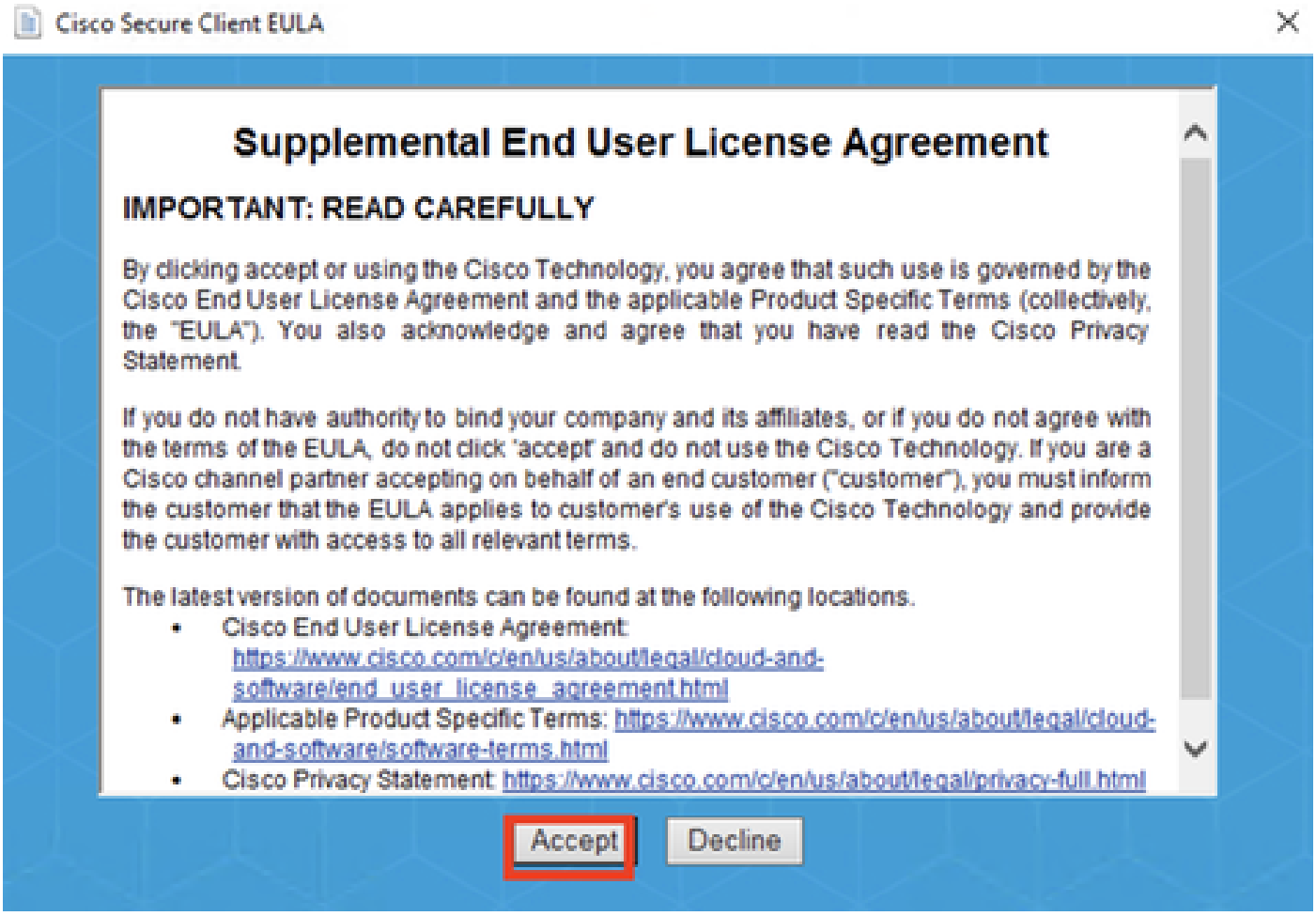
警告：如果使用Cisco Secure Client Wizard，則會自動安裝VPN模組並將其隱藏在GUI中。如果未安裝VPN模組，則NAM無法正常工作。如果使用單個MSI檔案或不同的安裝方法，請確保安裝VPN模組。



安裝選擇器

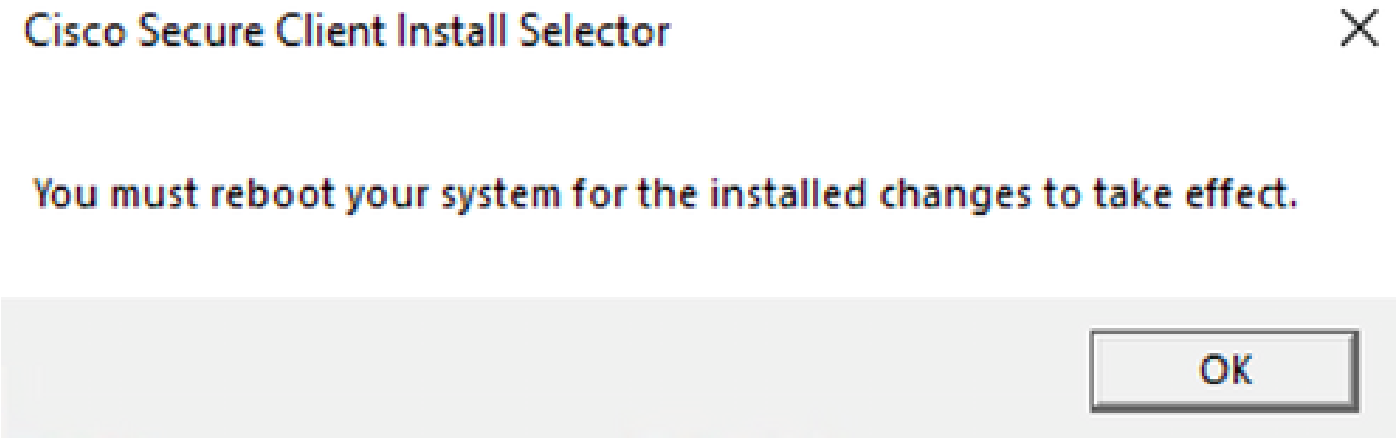
按一下「安裝所選內容」。

接受EULA。



EULA視窗

安裝NAM後需要重新啟動。



Reboot Requirement視窗

安裝後，可從Windows搜尋欄找到並開啟它。

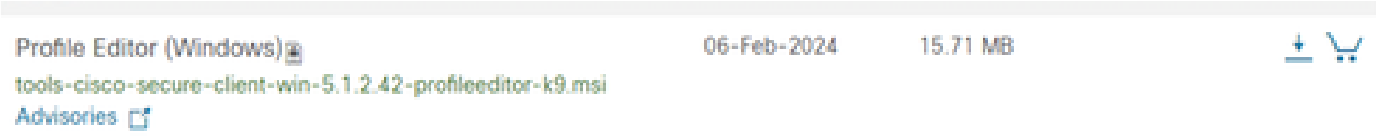
安全客戶端程式

2.下載並安裝安全客戶端NAM配置檔案編輯器。

配置Dot1x首選項需要思科網路訪問管理器配置檔案編輯器。

在下載Secure Client的同一頁面上，找到Profile Editor選項。

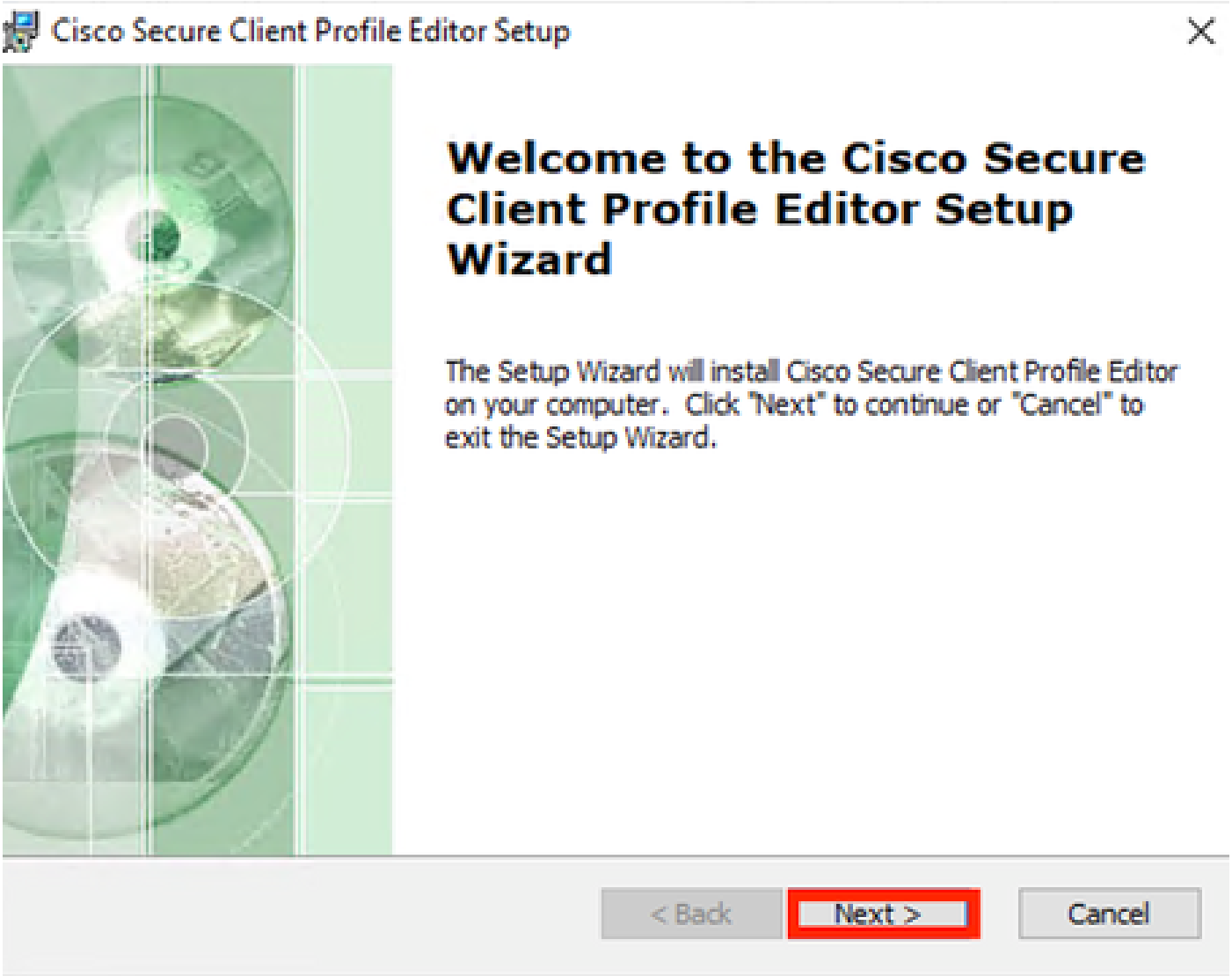
本示例使用5.1.2.42版中的選項。



配置檔案編輯器

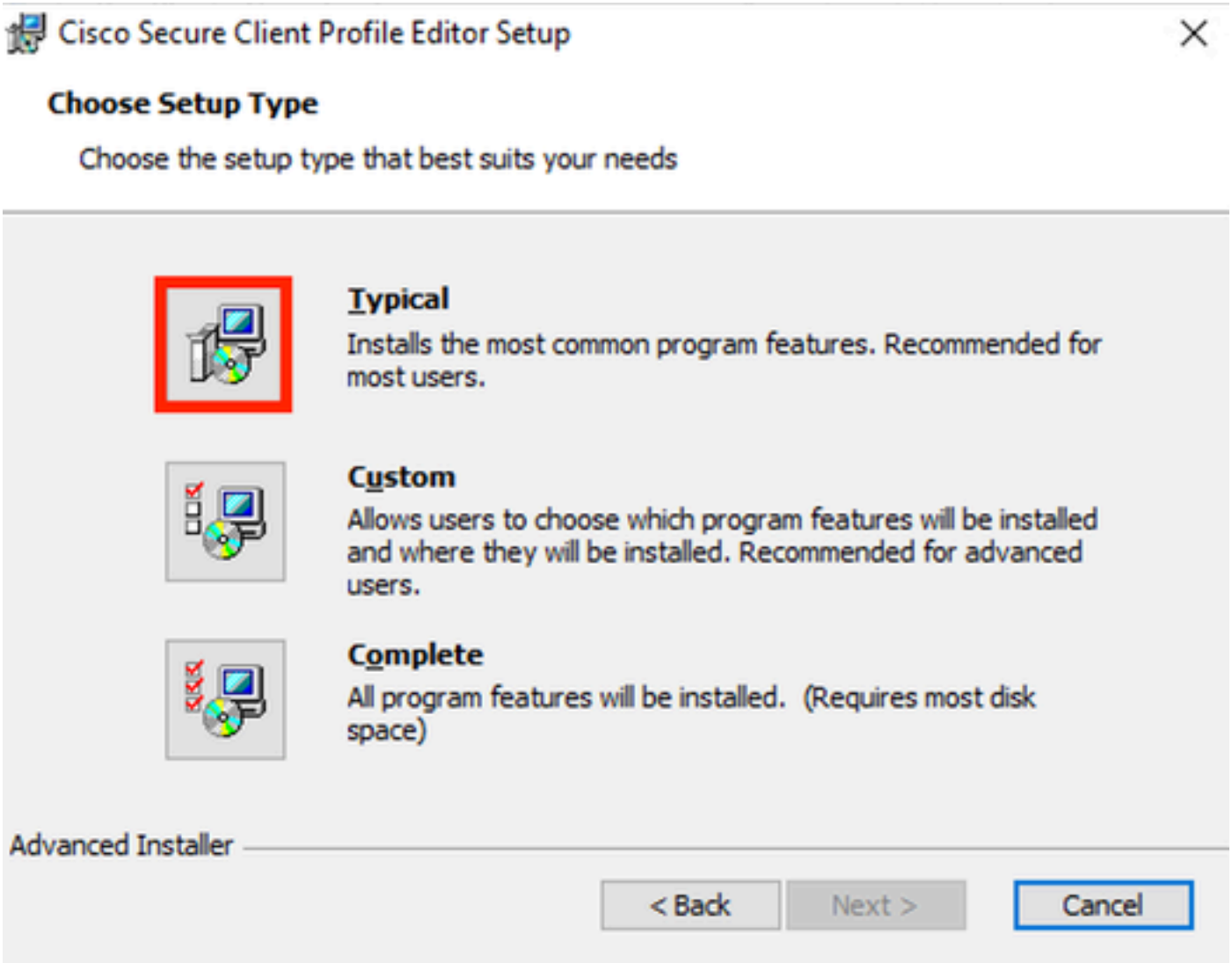
下載後，繼續安裝。

運行msi檔案。

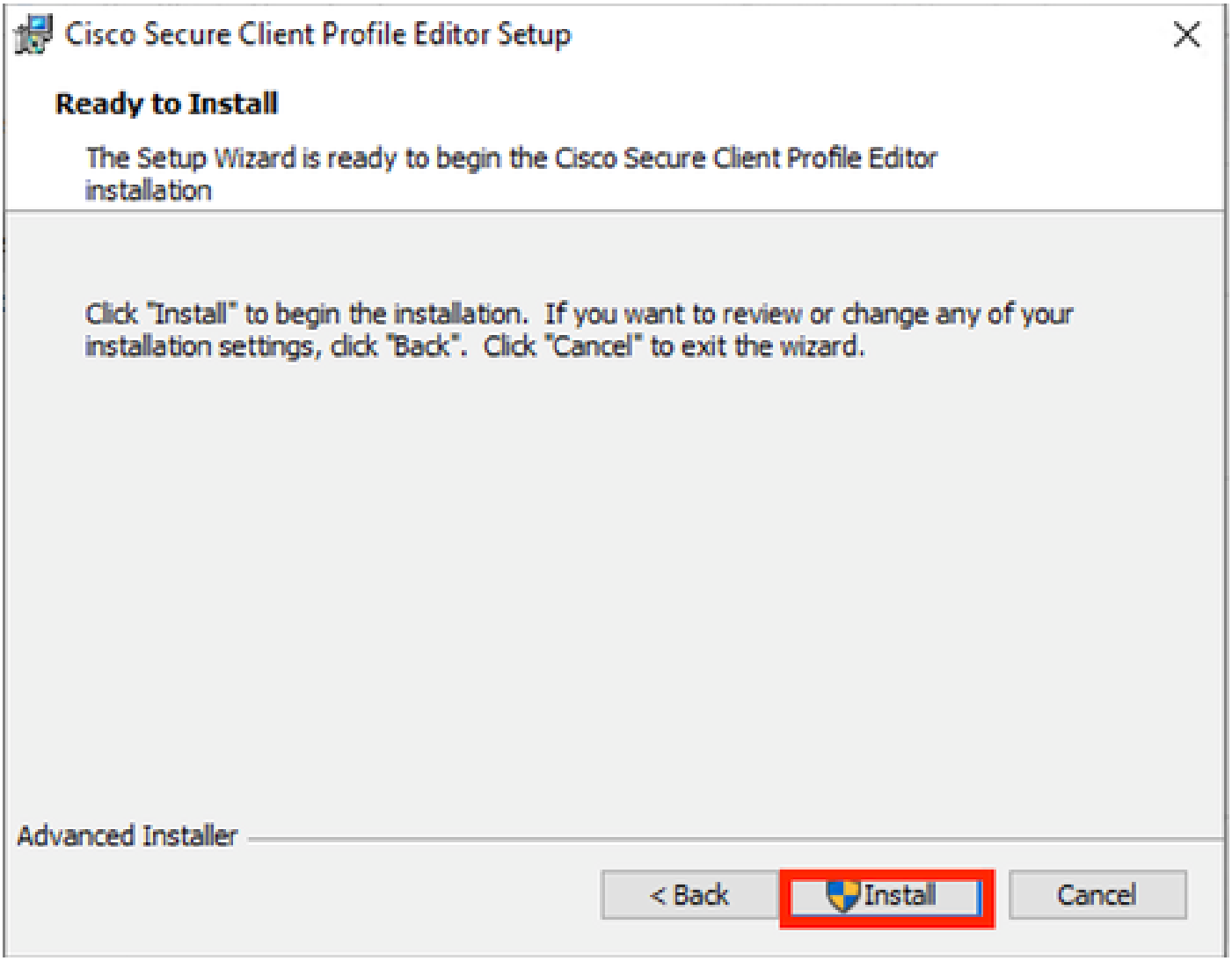


配置檔案編輯器設定視窗

使用Typical設定選項。

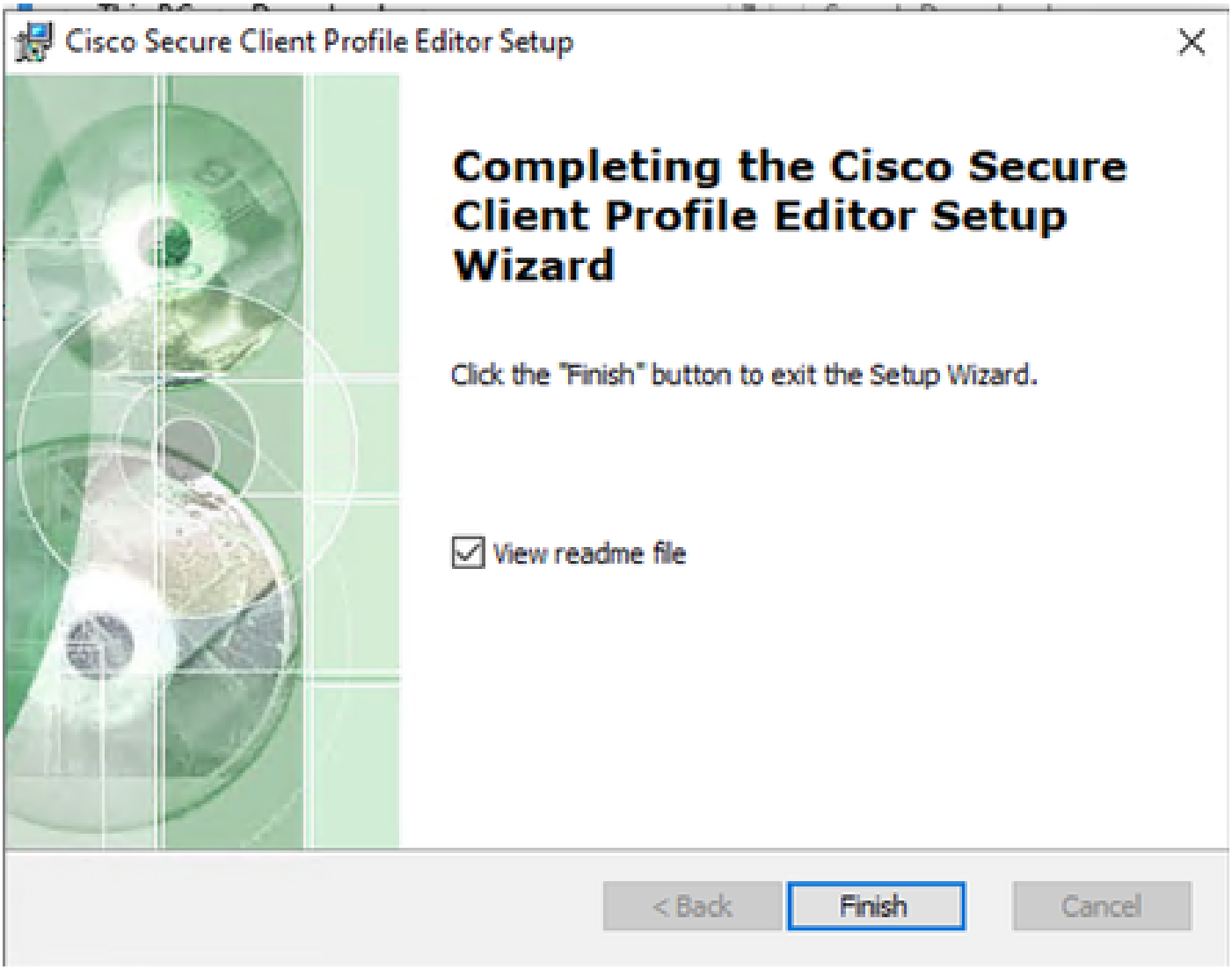


配置檔案編輯器安裝程式



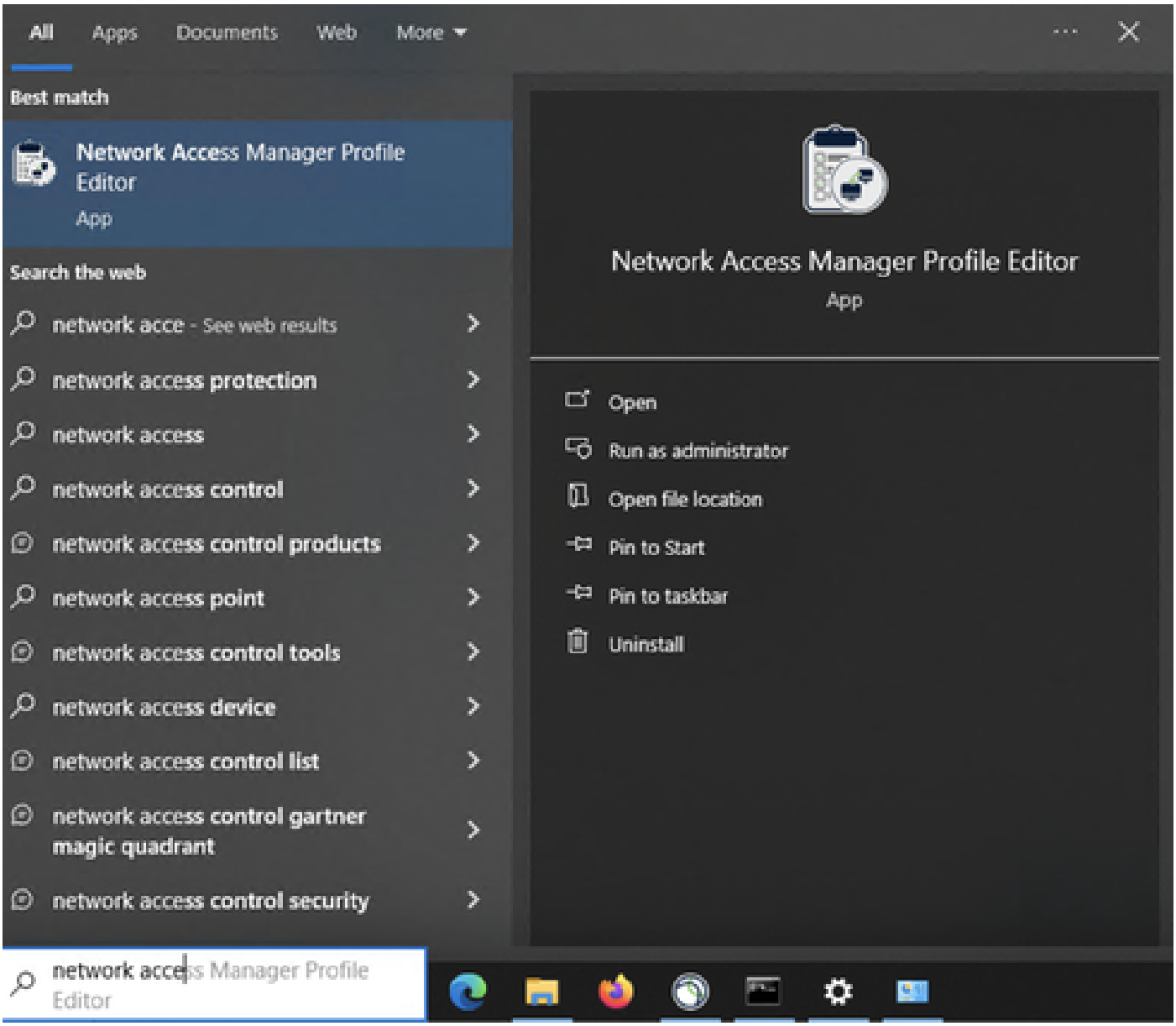
安裝視窗

按一下「Finish」（結束）。



配置檔案編輯器安裝結束

安裝後，從搜尋欄開啟Network Access Manager Profile Editor。



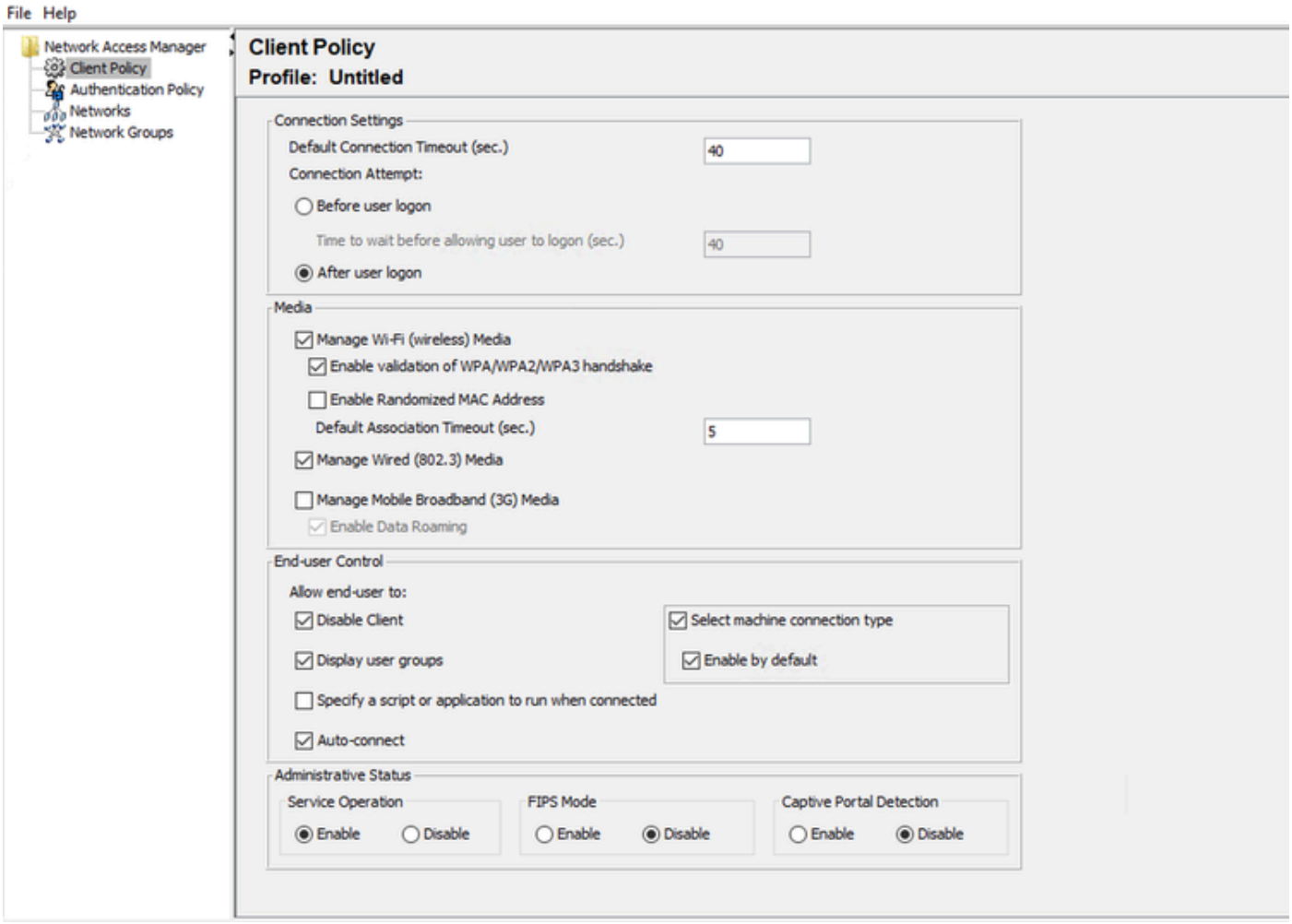
搜尋欄上的NAM配置檔案編輯器

網路訪問管理器和配置檔案編輯器的安裝已完成。

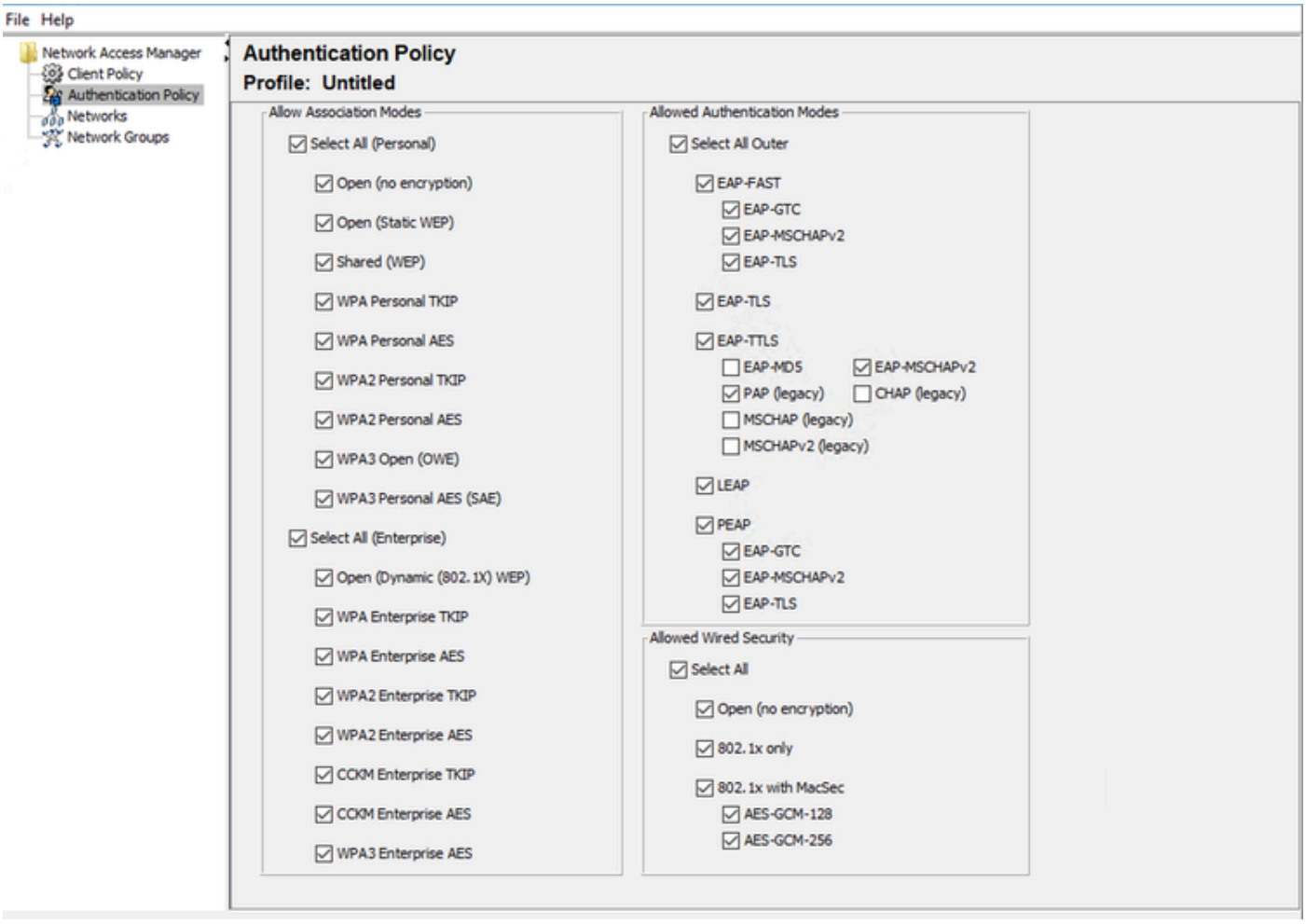
3.常規預設配置

本文中顯示的所有方案都包含下列配置：

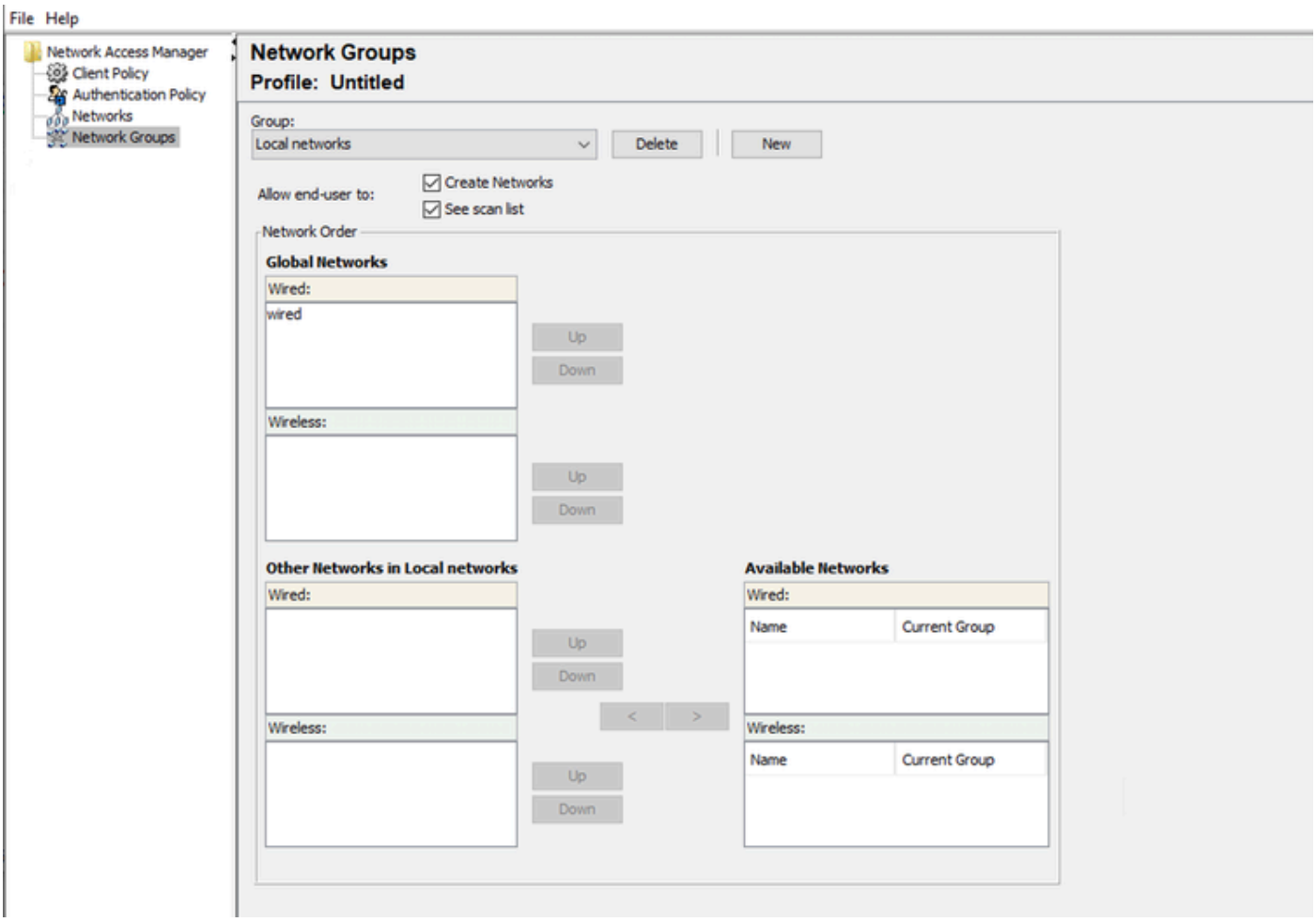
- 客戶端策略
- 身份驗證策略
- 網路組



*NAM*配置檔案編輯器客戶端策略



*NAM*配置檔案編輯器身份驗證策略



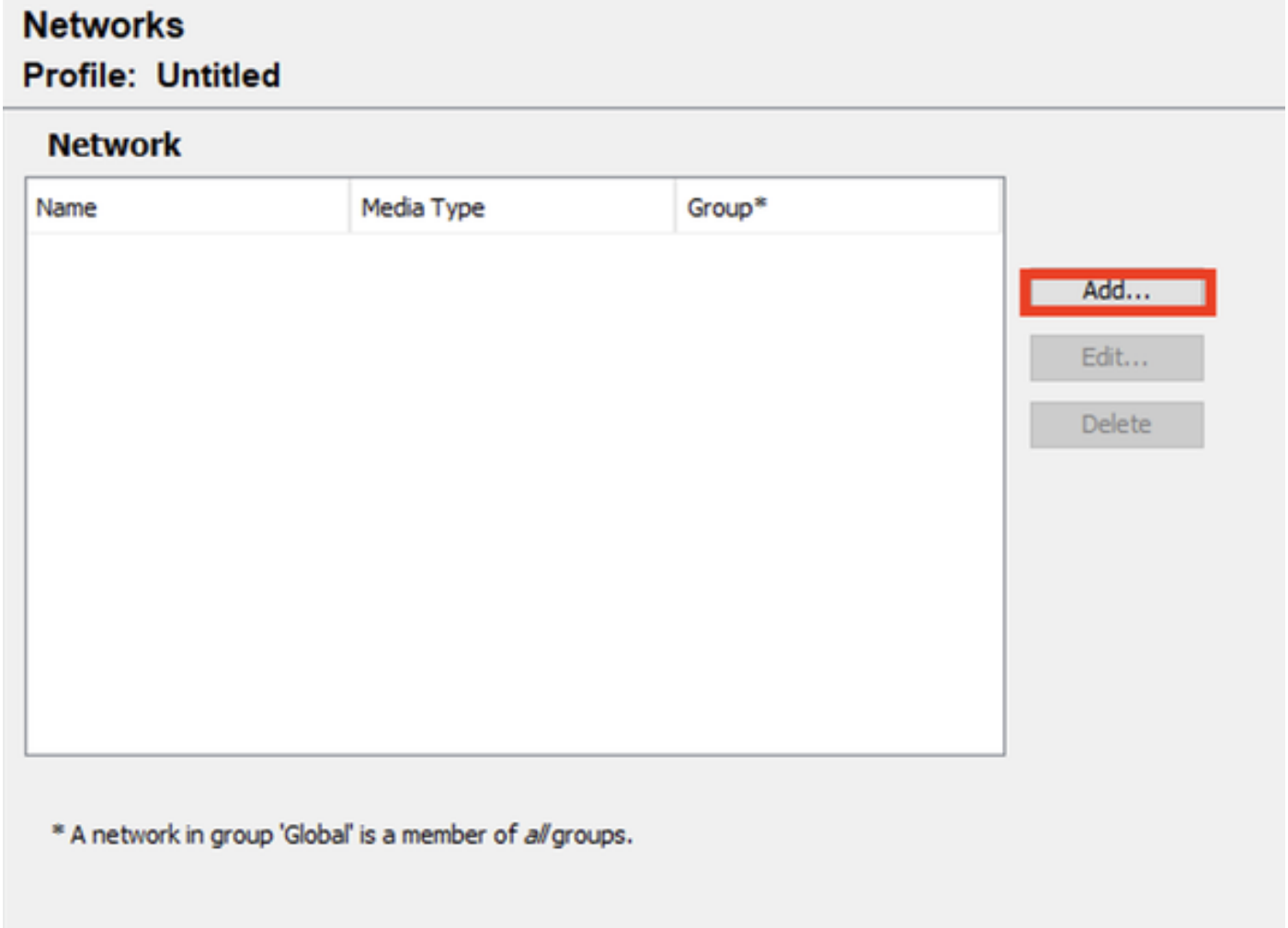
「網路組」頁籤

4.案例1:為PEAP(MS-CHAPv2)使用者身份驗證配置安全客戶端NAM請求方

導覽至Networks部分。

可以刪除預設的Network配置檔案。

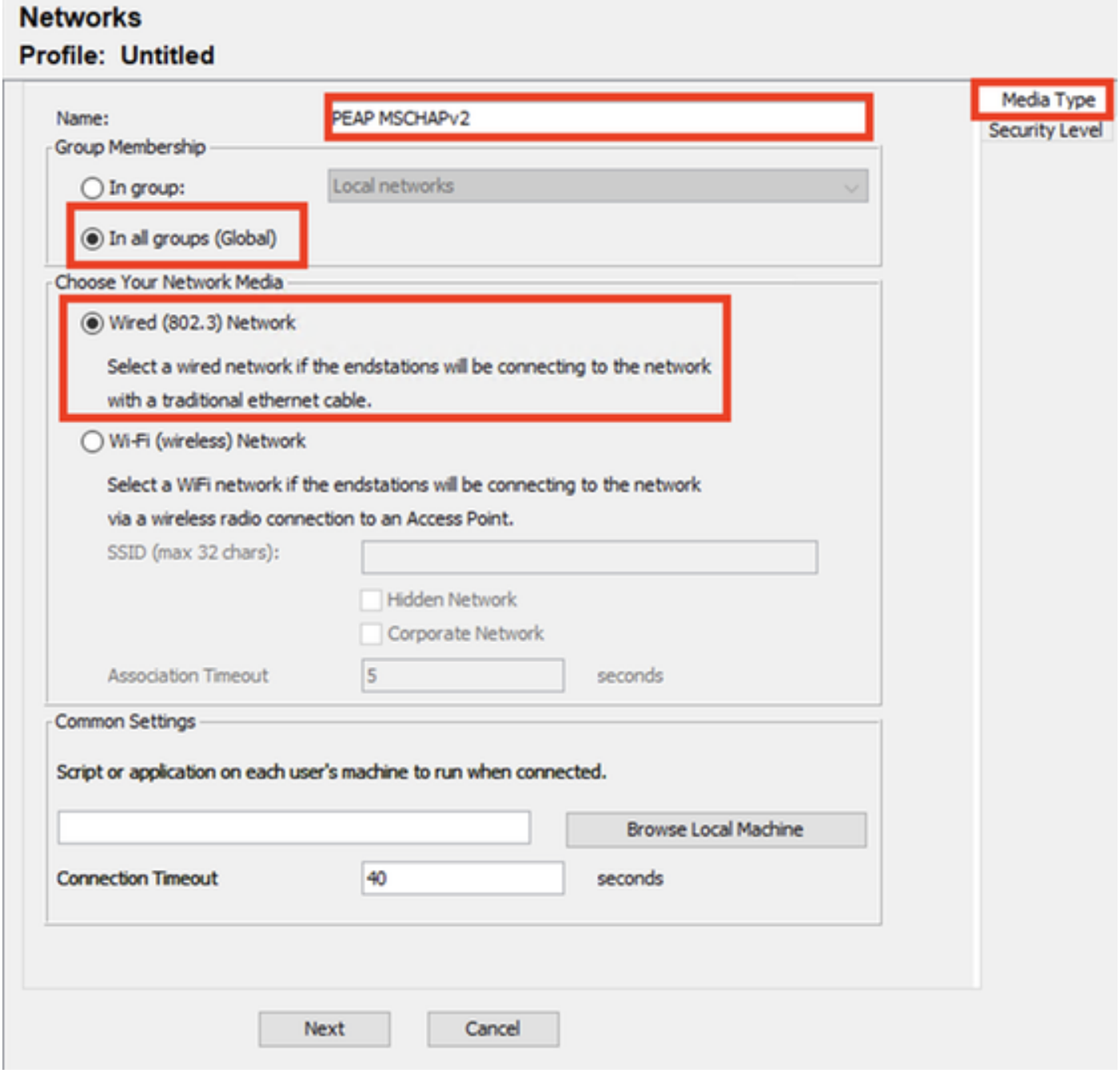
按一下「新增」。



網路設定檔建立

為網路配置檔案命名。

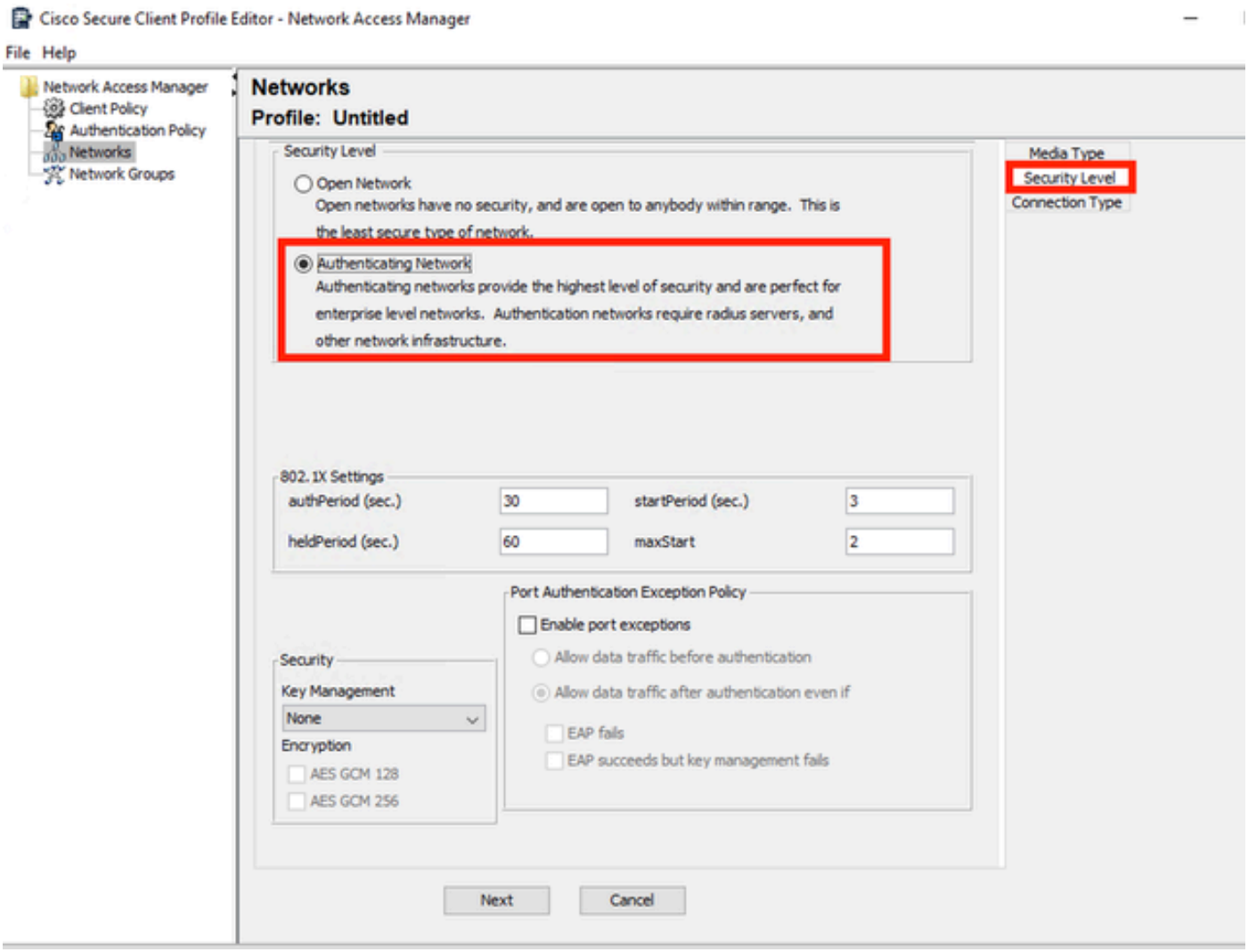
選擇Global作為Group Membership。選擇Wired Network介質。



Network Profile Media Type部分

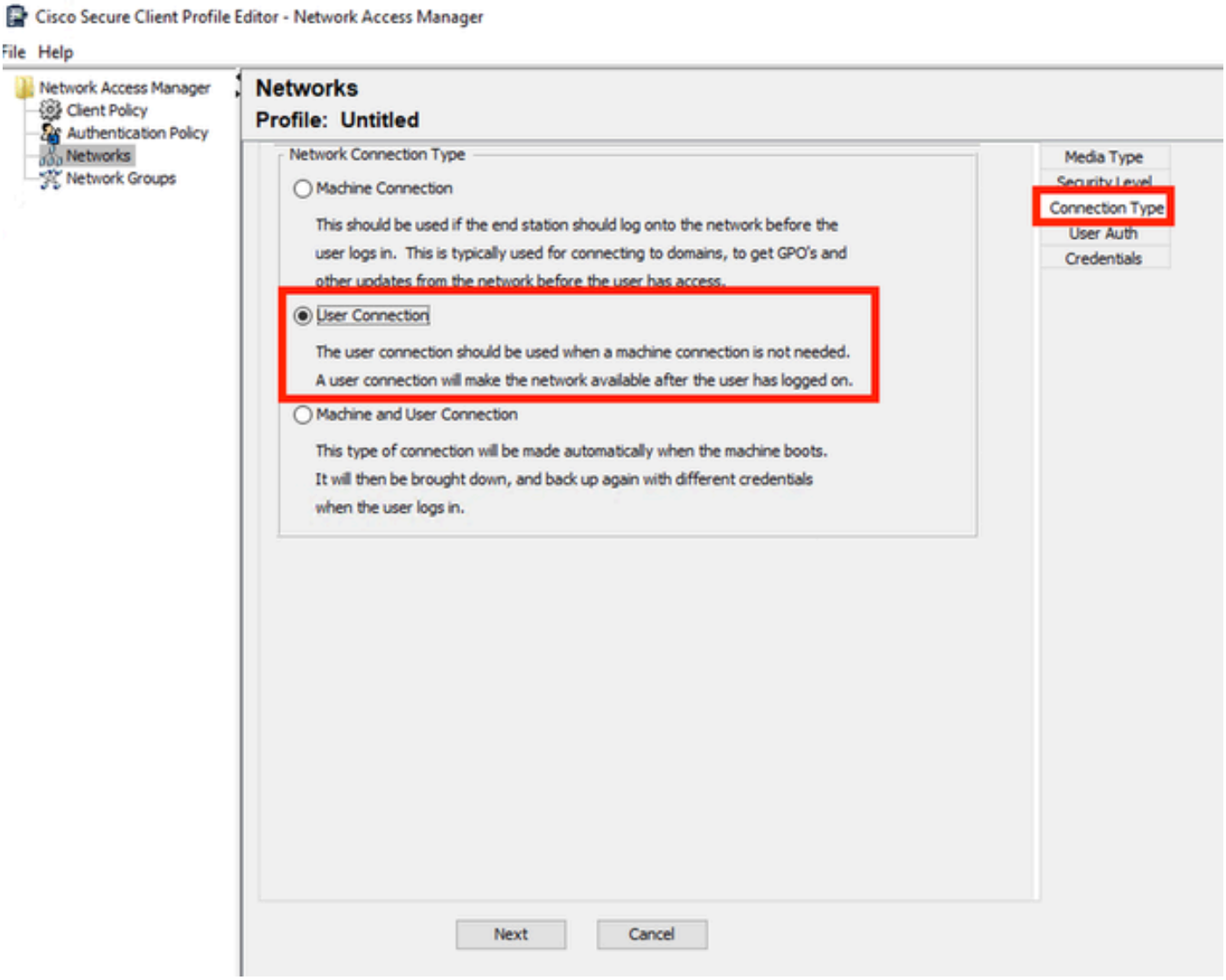
按「Next」（下一步）。

選擇Authenticating Network，並為Security Level部分中的其餘選項使用預設值。



網路配置檔案安全級別

按一下Next以繼續Connection Type部分。

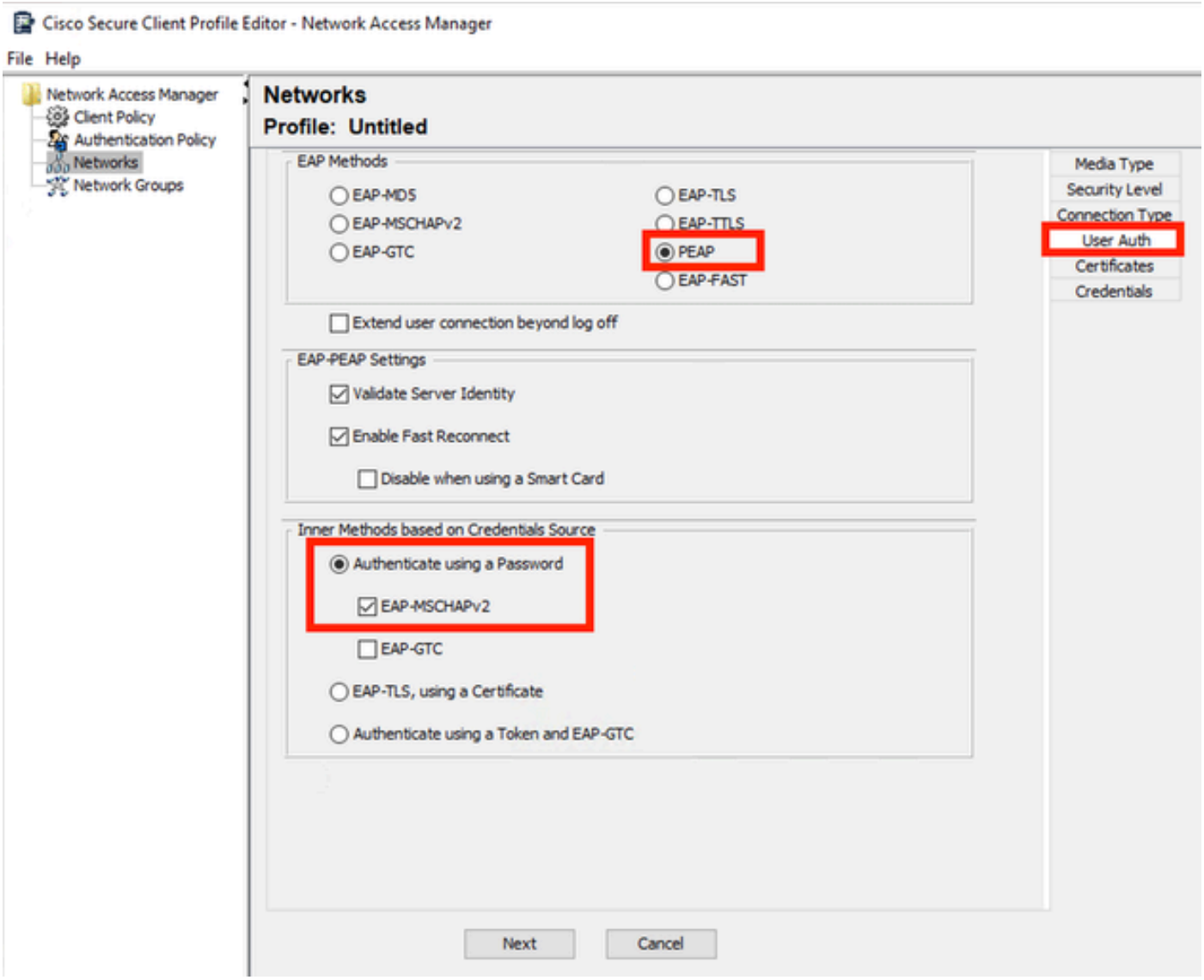


網路配置檔案連線型別

選擇User Connection連接型別。

按一下「Next」以繼續「User Auth」一節，該節目前可用。

選擇PEAP作為常規EAP方法。



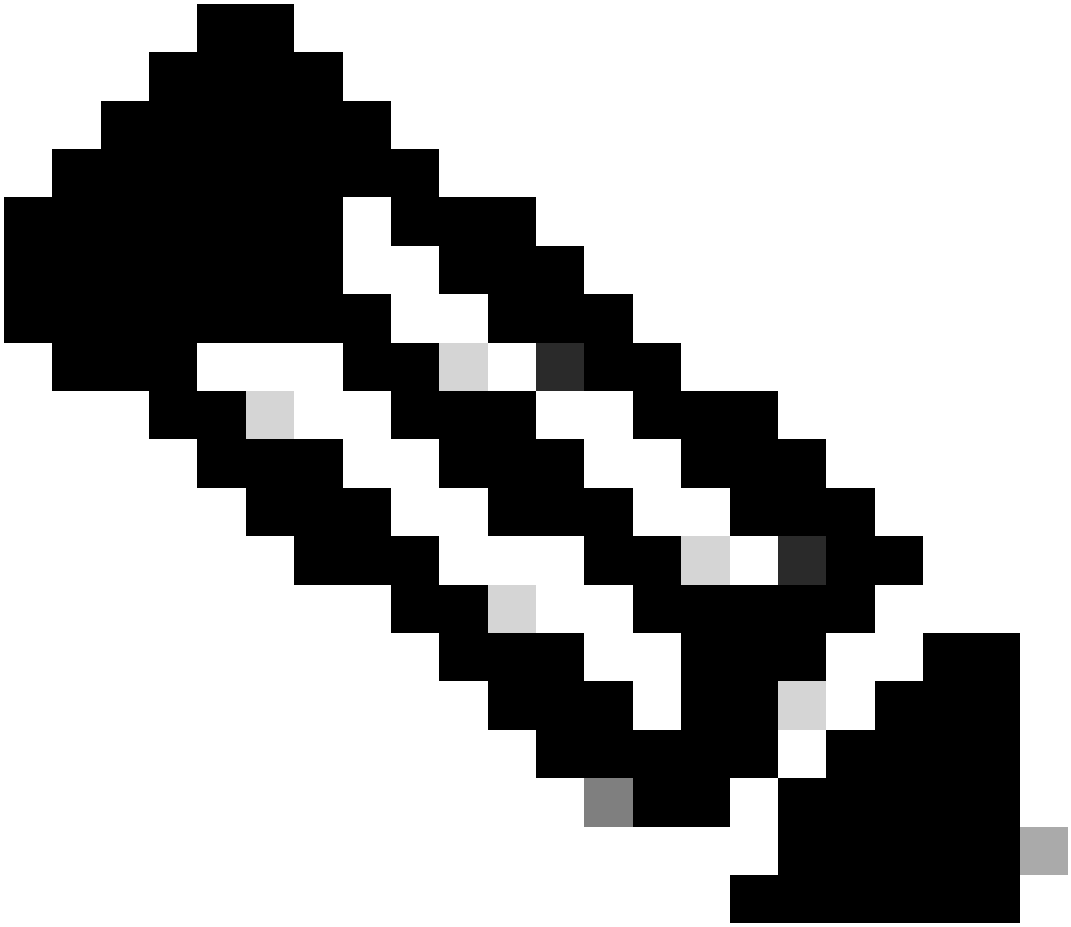
網路設定檔使用者驗證

請勿更改EAP-PEAP設定中的預設值。

繼續使用基於憑據源的內部方法部分。

從EAP PEAP存在的多個內部方法中，選擇Authenticate using a Password，然後選擇EAP-MSCHAPv2。

按一下「Next」以繼續前往「Certificate」部分。

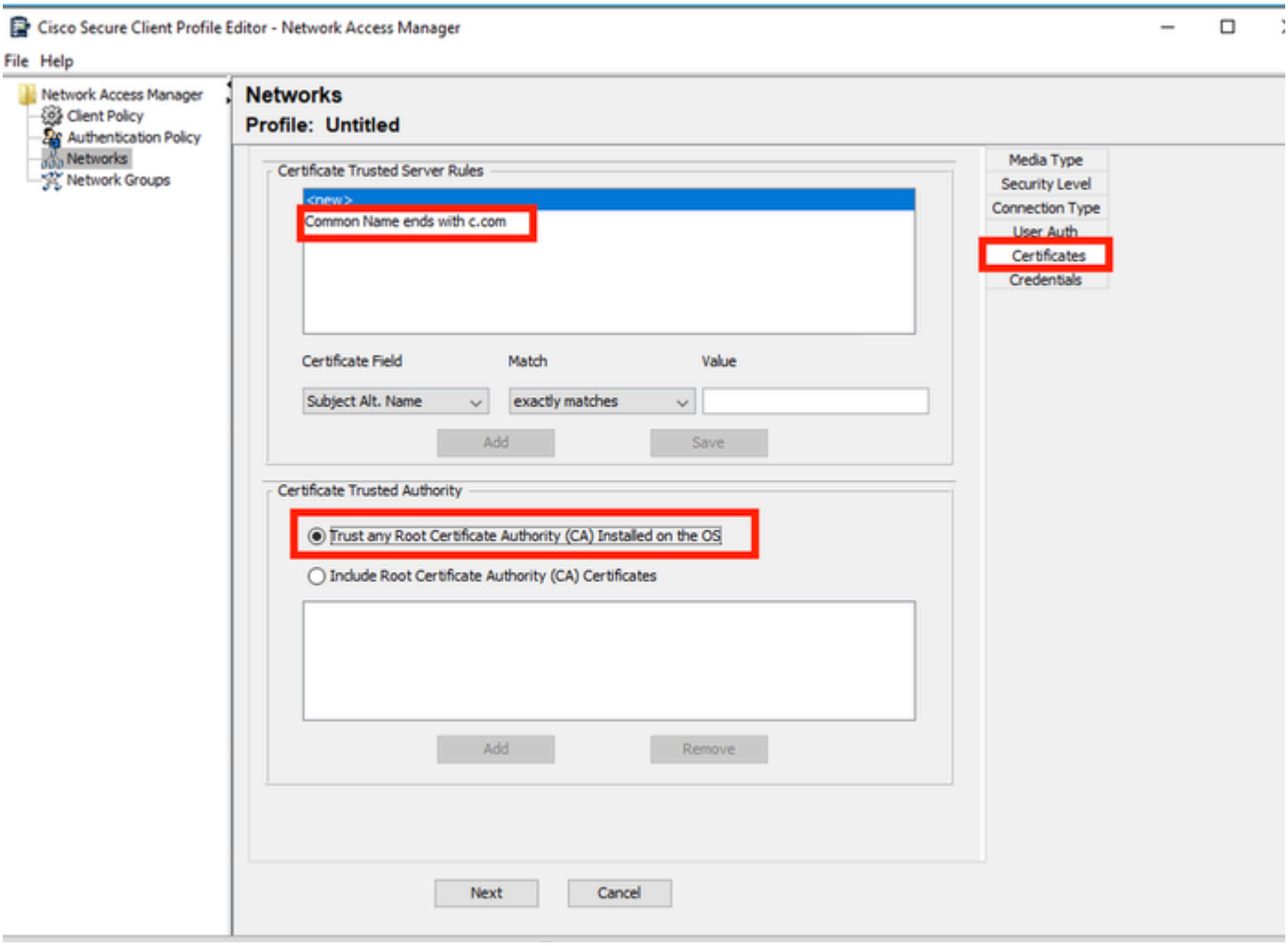


附註：將顯示Certificate部分，因為選中了Validate Server Identity in EAP-PEAP Settings選項。對於EAP PEAP，它使用伺服器證書進行封裝。

在Certificates部分，在Certificate Trusted Server Rules中，使用以c.com結尾的規則Common Name。

此部分配置是指伺服器在EAP PEAP流期間使用的證書。

如果在您的環境中使用身份服務引擎(ISE)，則可以使用策略伺服器節點EAP證書的公用名。

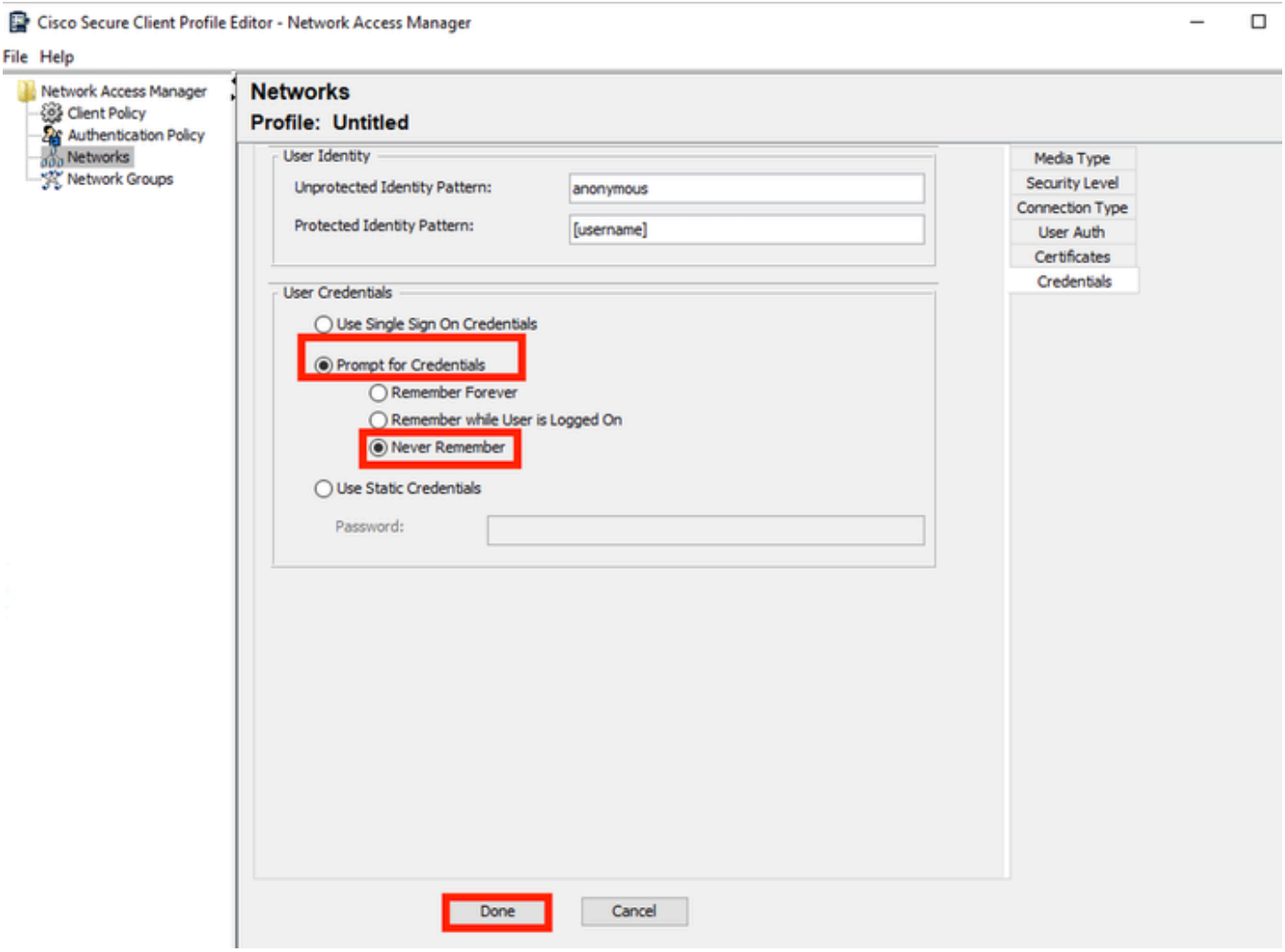


網路配置檔案證書部分

可在證書受信任頒發機構中選擇兩個選項。對於此方案，使用選項Trust any Root Certificate Authority(CA)，而不是新增簽署RADIUS EAP證書的特定CA證書。

使用此選項，Windows裝置信任由包含在Manage User Certs程式Certificates — Current User > Trusted Root Certification Authorities > Certificates中的證書簽名的任何EAP證書。

按「Next」（下一步）。



Network Profile Credentials部分

在Credentials部分中，僅更改User Credentials部分。

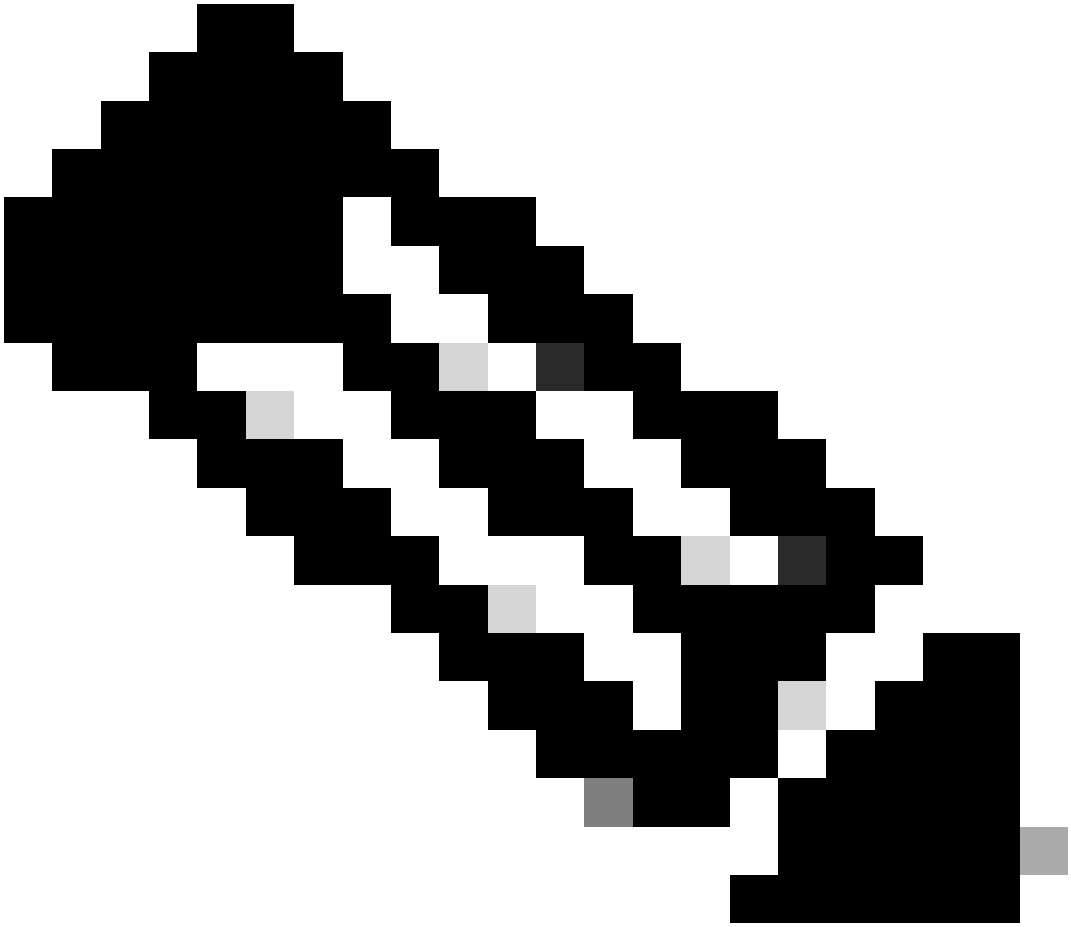
選擇了提示輸入憑據>從不記住選項，因此在每個身份驗證中，進行身份驗證的使用者必須輸入其憑據。

按一下「完成」。

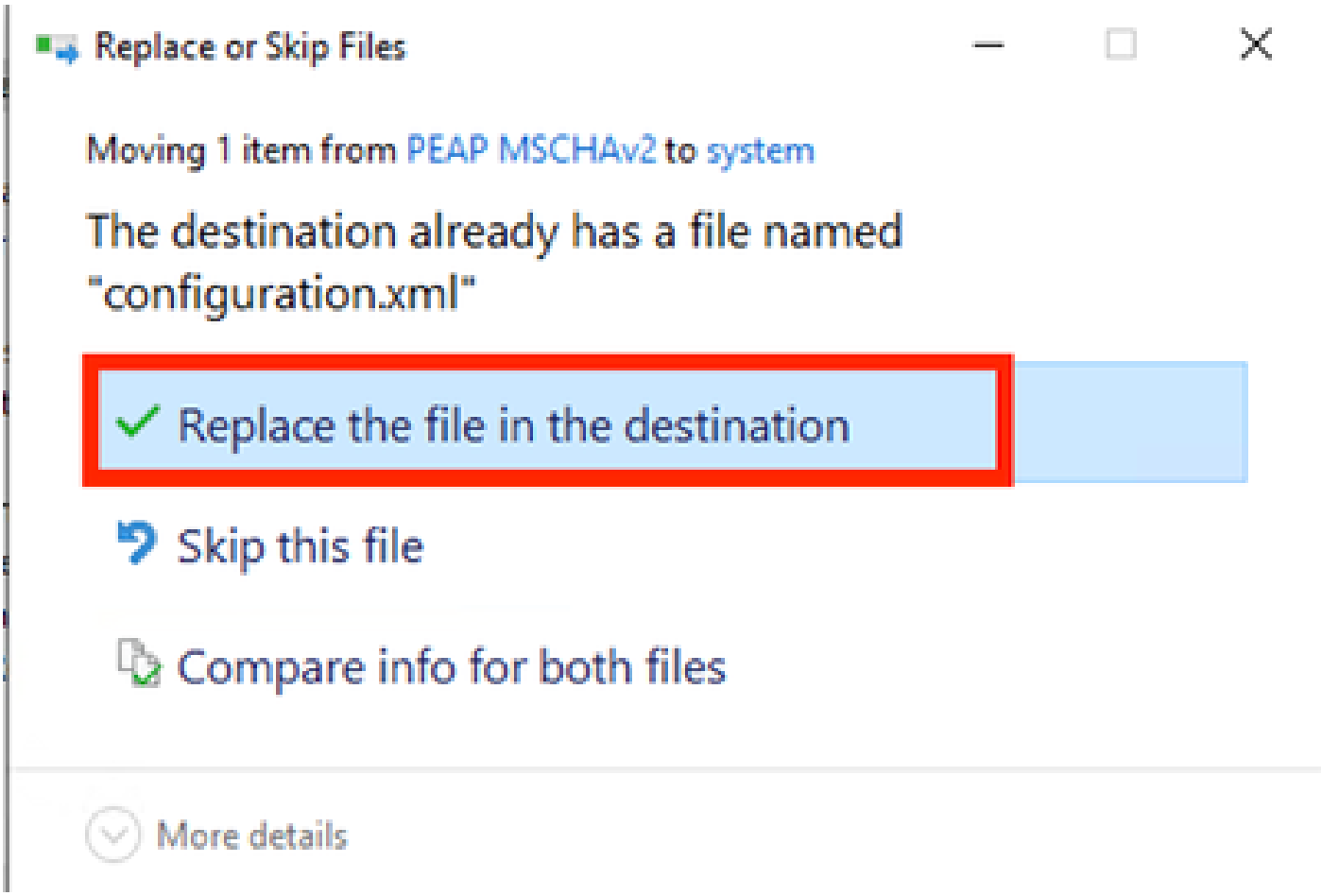
使用File > Save As 選項，將Secure Client Network Access Manager配置檔案另存為configuration.xml。

要使Secure Client Network Access Manage使用剛剛建立的配置檔案，請將下一個目錄中的configuration.xml檔案替換為新檔案：

C:\ProgramData\Cisco\Cisco安全客戶端\網路訪問管理器\系統



附註：檔案必須命名為configuration.xml，否則無法正常工作。

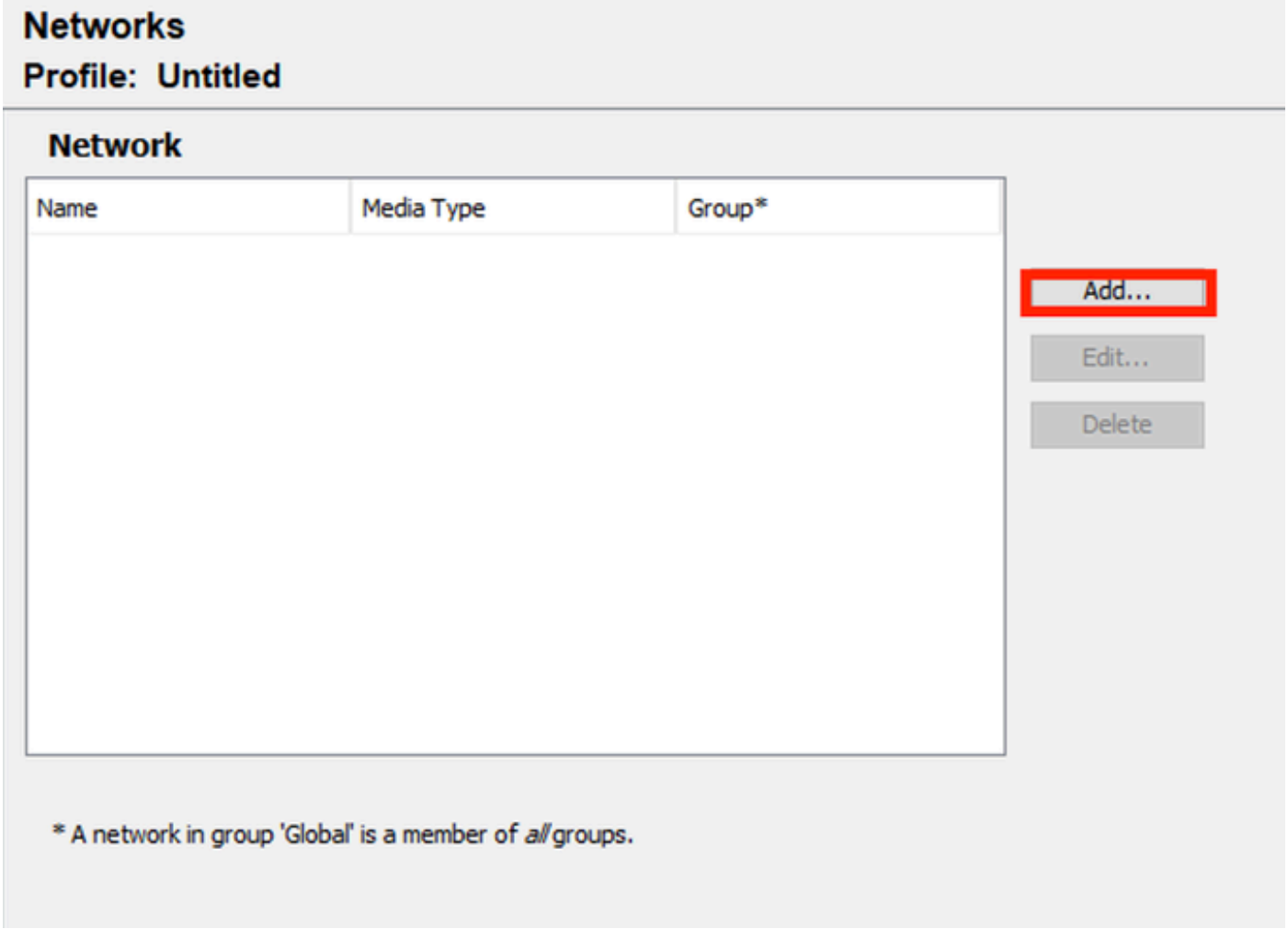


替換檔案節

5.案例2:為EAP-FAST同步使用者和電腦身份驗證配置安全客戶端NAM請求方

開啟NAM配置檔案編輯器並導航至Networks部分。

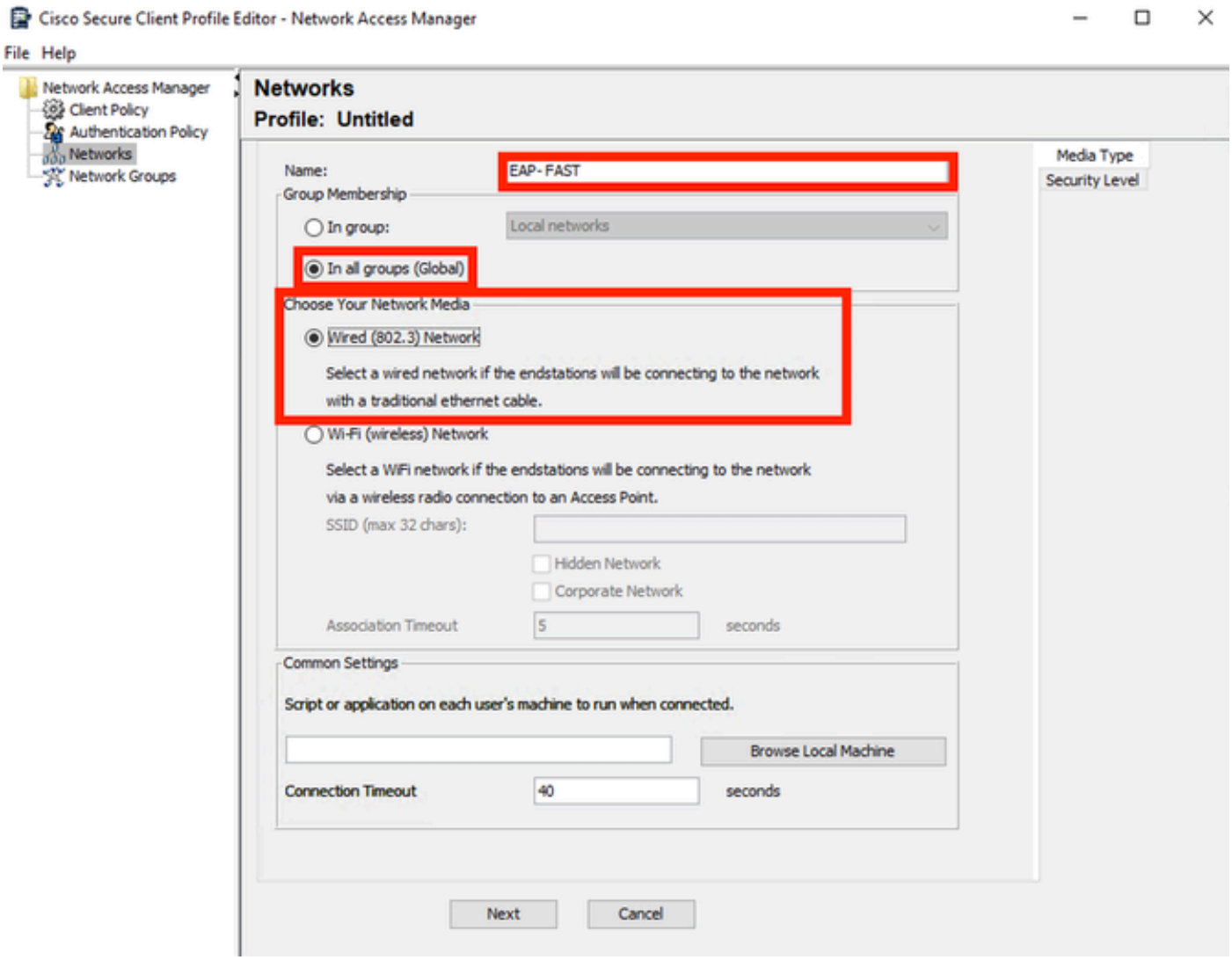
按一下「新增」。



NAM配置檔案編輯器「網路」頁籤

在網路配置檔案中輸入名稱。

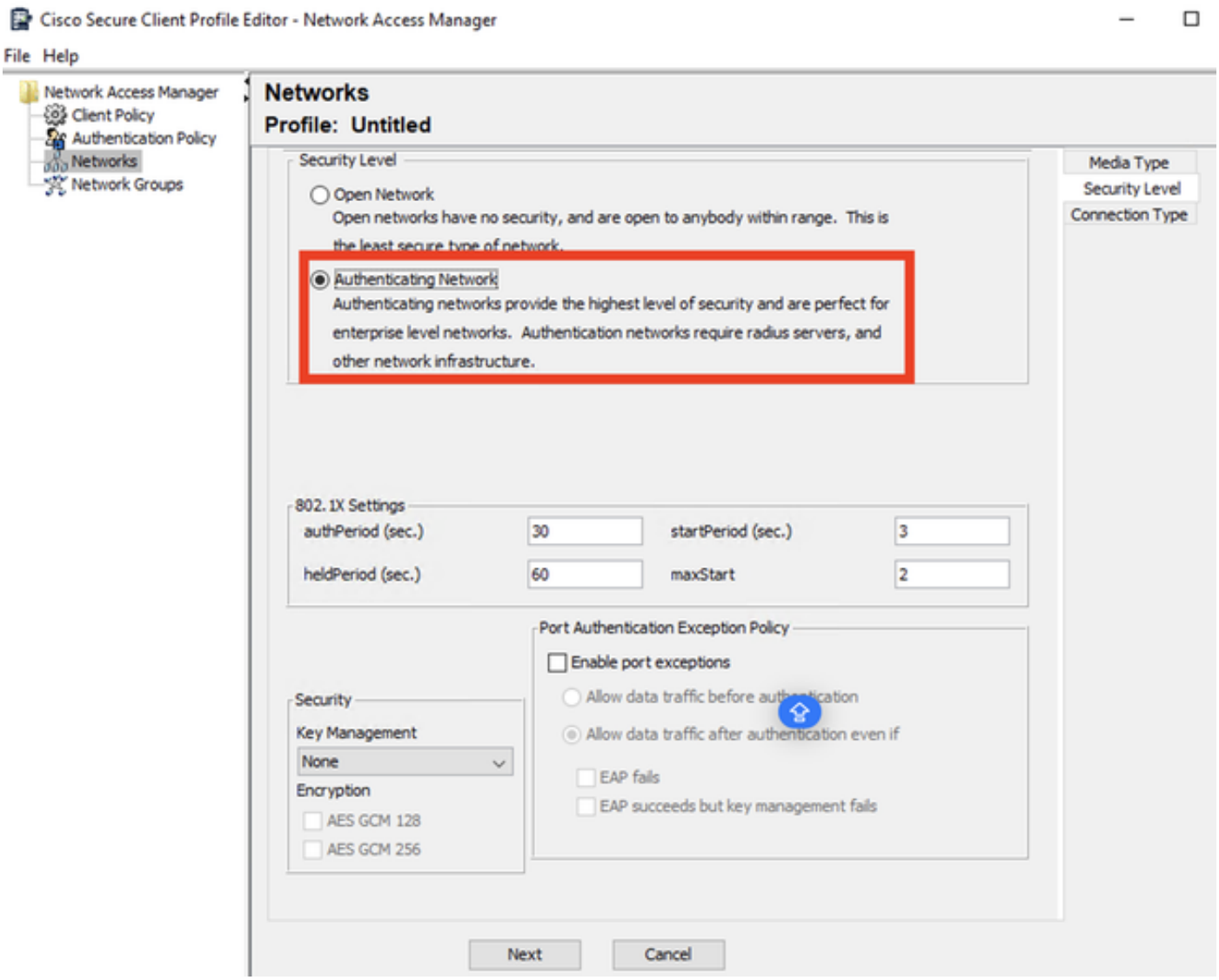
選擇Global作為Group Membership。選擇WiredNetwork Media。



「介質型別」部分

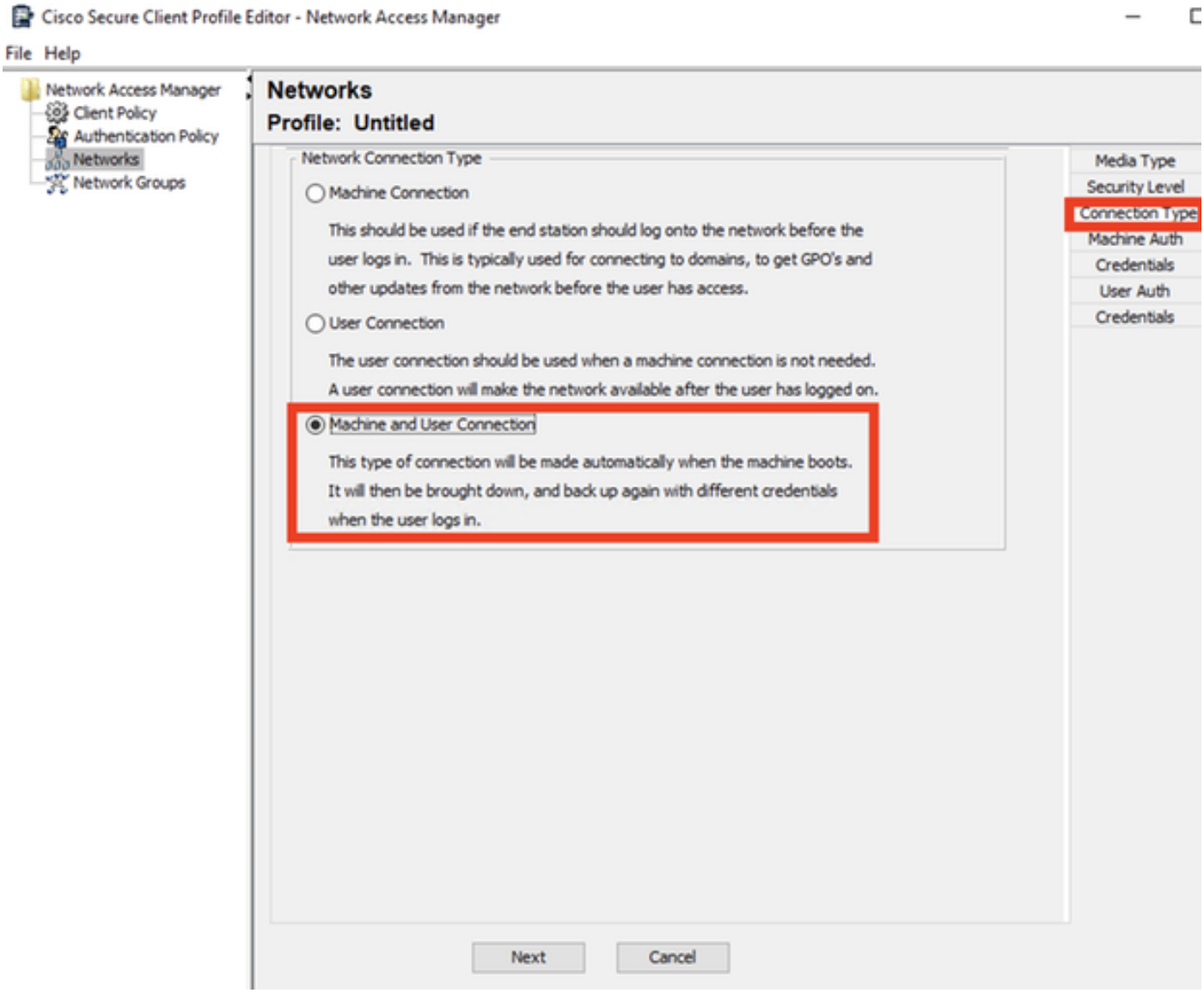
按「Next」（下一步）。

選擇Authenticating Network，不要更改本節中其餘選項的預設值。



安全級別配置檔案編輯器部分

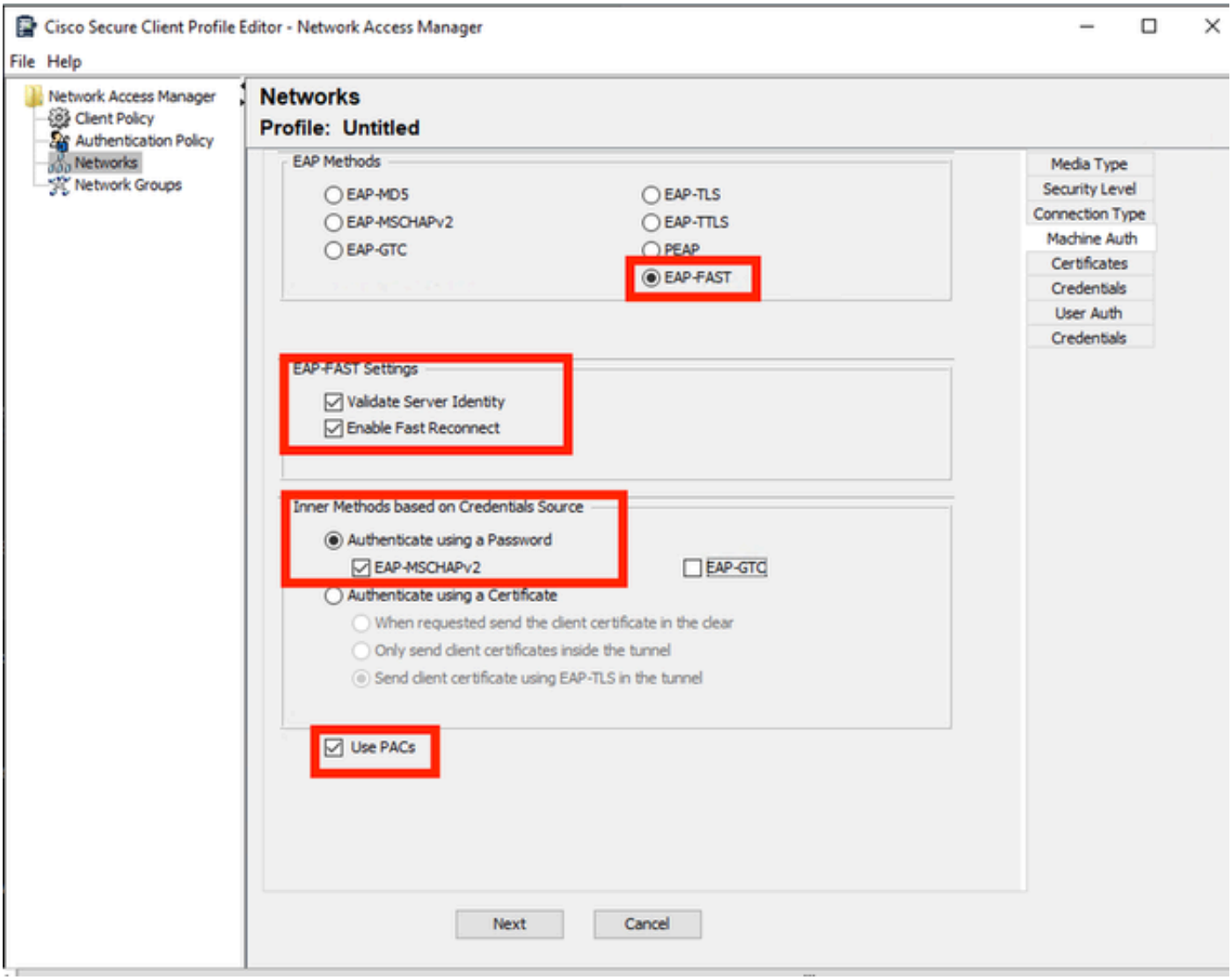
按一下Next以繼續Connection Type部分。



連線型別部分

通過選擇第三個選項同時配置使用者和電腦身份驗證。

按「Next」（下一步）。



機器身份驗證部分

在Machine Auth部分中，選擇EAP-FAST作為EAP方法。請勿更改EAP FAST設定預設值。

對於Inner methods based on Credentials Source部分，選擇Authenticate using a Password，然後選擇EAP-MSCHAPv2作為方法。

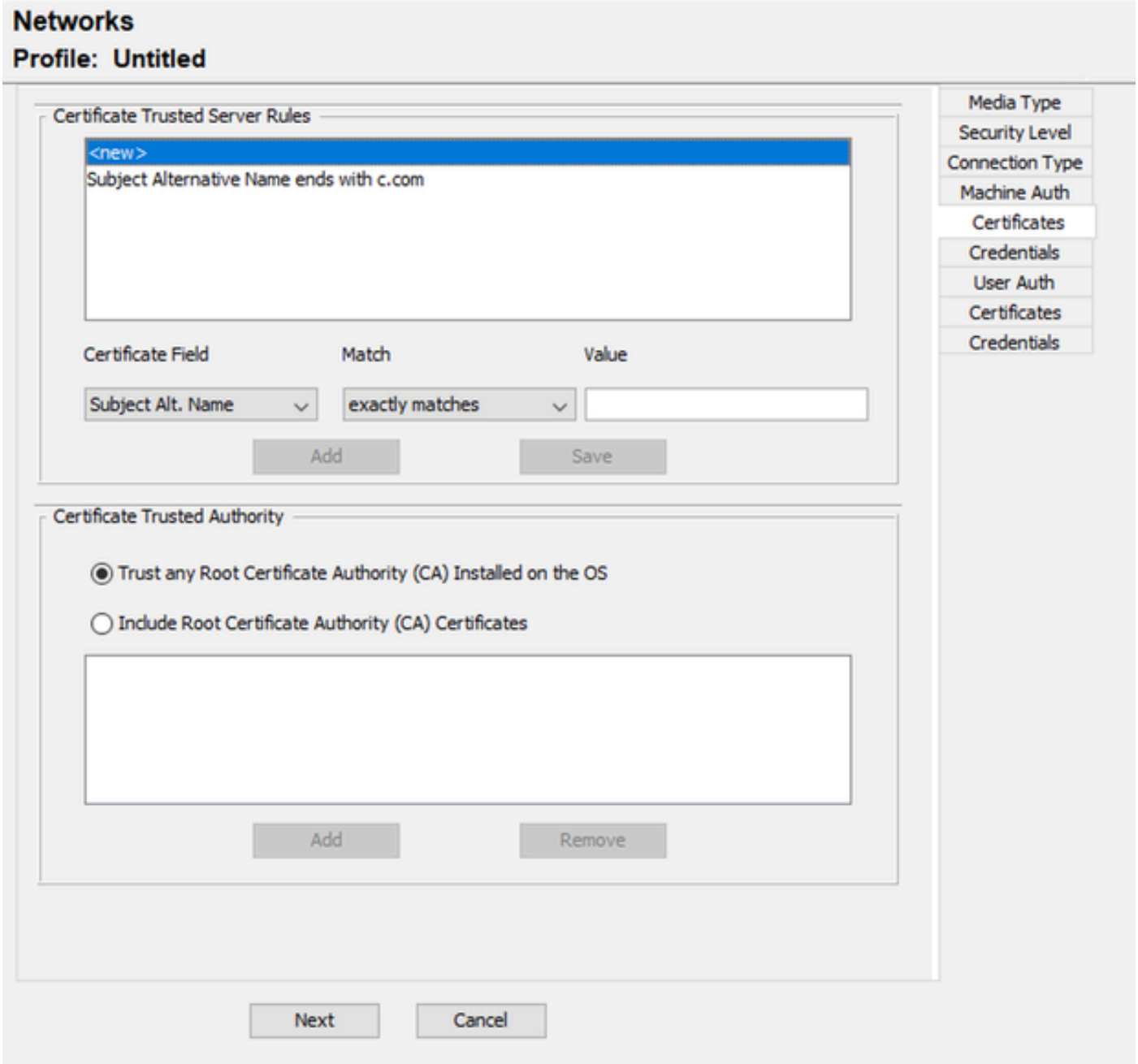
然後選擇使用PAC選項。

按「Next」（下一步）。

在Certificates部分的Certificate Trusted Server Rules中，規則公用名以c.com結尾。

此部分是指伺服器在EAP PEAP流期間使用的證書。

如果在您的環境中使用身份服務引擎(ISE)，則可以使用策略伺服器節點EAP證書的公用名稱。

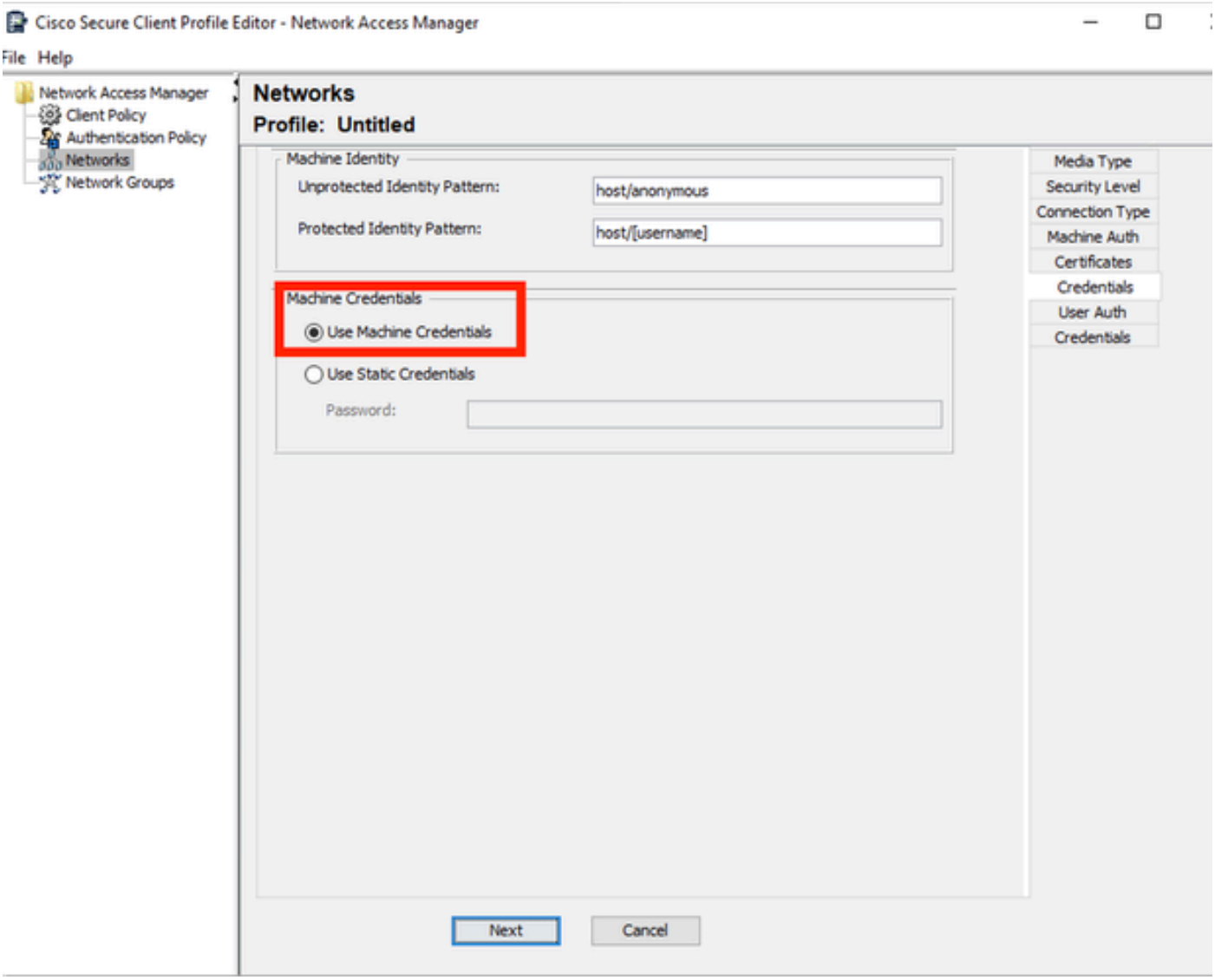


Machine Auth Server Certificate Trust部分

可在證書受信任頒發機構中選擇兩個選項。對於此方案，使用選項Trust any Root Certificate Authority(CA)Installed on the OS，而不是新增簽署RADIUS EAP證書的特定CA證書。

使用此選項，Windows信任由包含在Manage User Certs程式(Current User > Trusted Root Certification Authorities > Certificates)中的證書簽名的任何EAP證書。

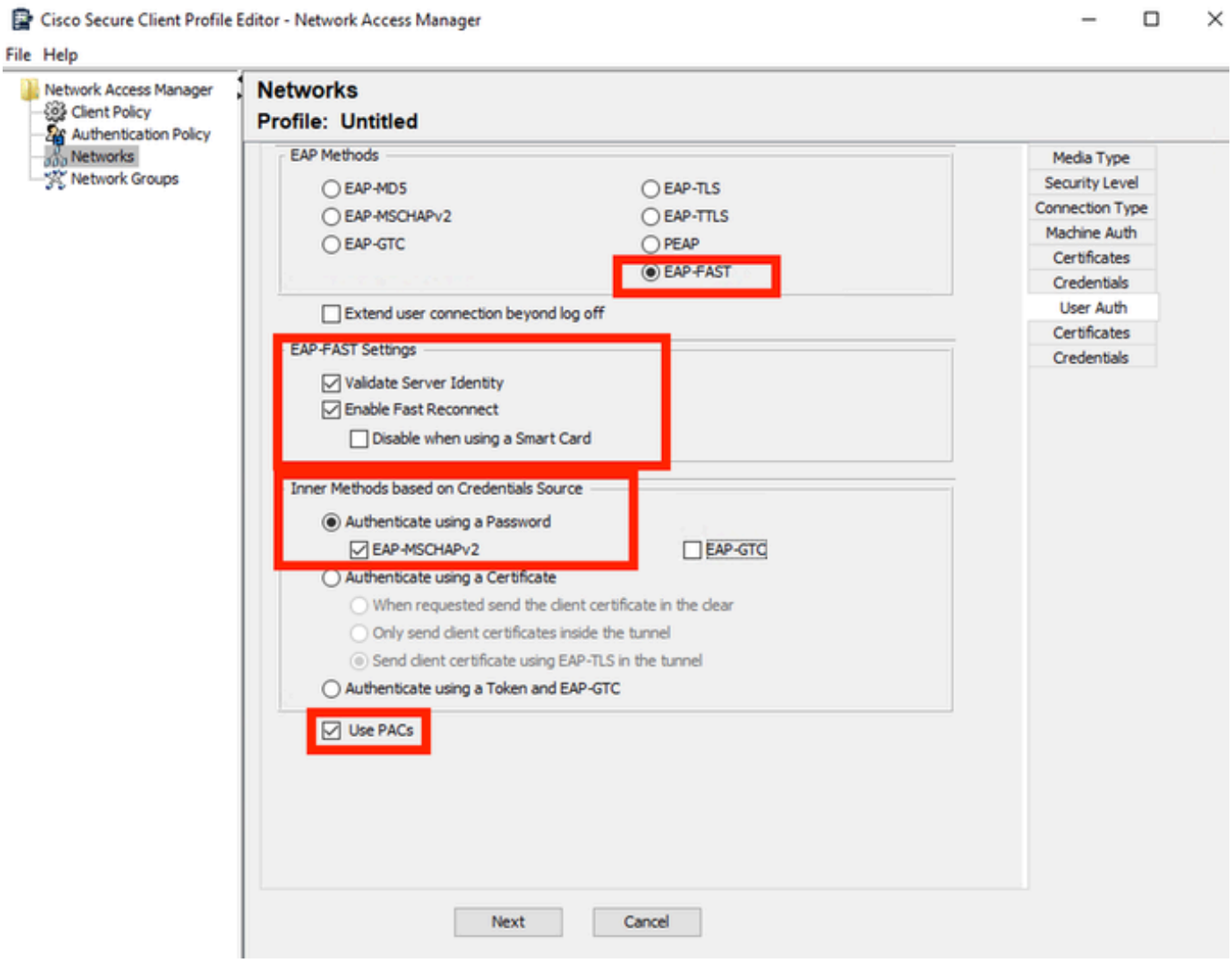
按「Next」（下一步）。



機器身份驗證憑證部分

在Machine Credentials部分中選擇Use Machine Credentials。

按「Next」（下一步）。



User Authentication部分

對於User Auth，選擇EAP-FAST作為EAP方法。

請勿更改EAP-FAST設定部分中的預設值。

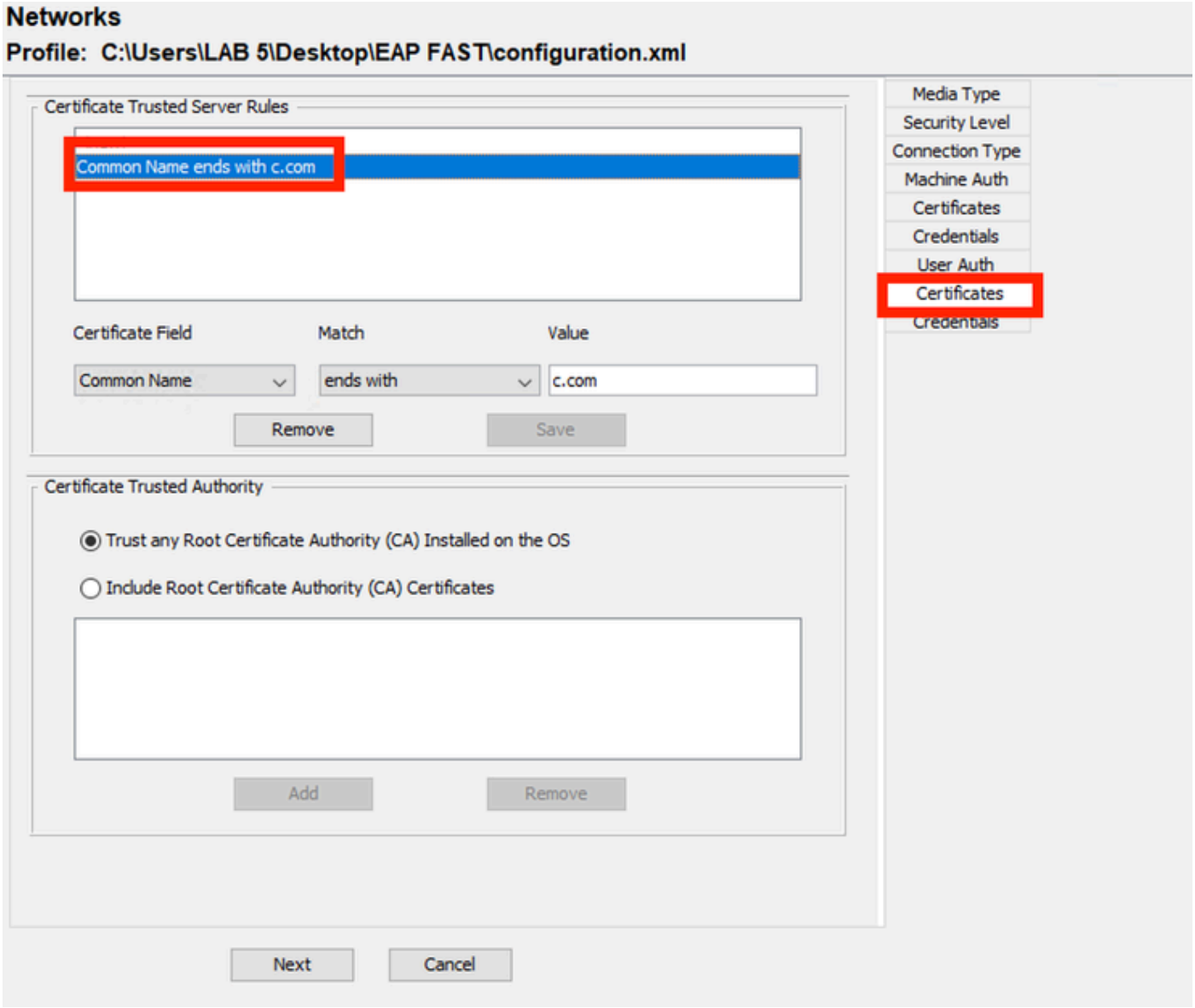
對於「基於憑據的內部方法」源部分，選擇Authenticate using a Password和EAP-MSCHAPv2作為方法。

選擇使用PAC。

按「Next」（下一步）。

在Certificates部分的Certificate Trusted Server Rules中，規則為Common Name ends with c.com。

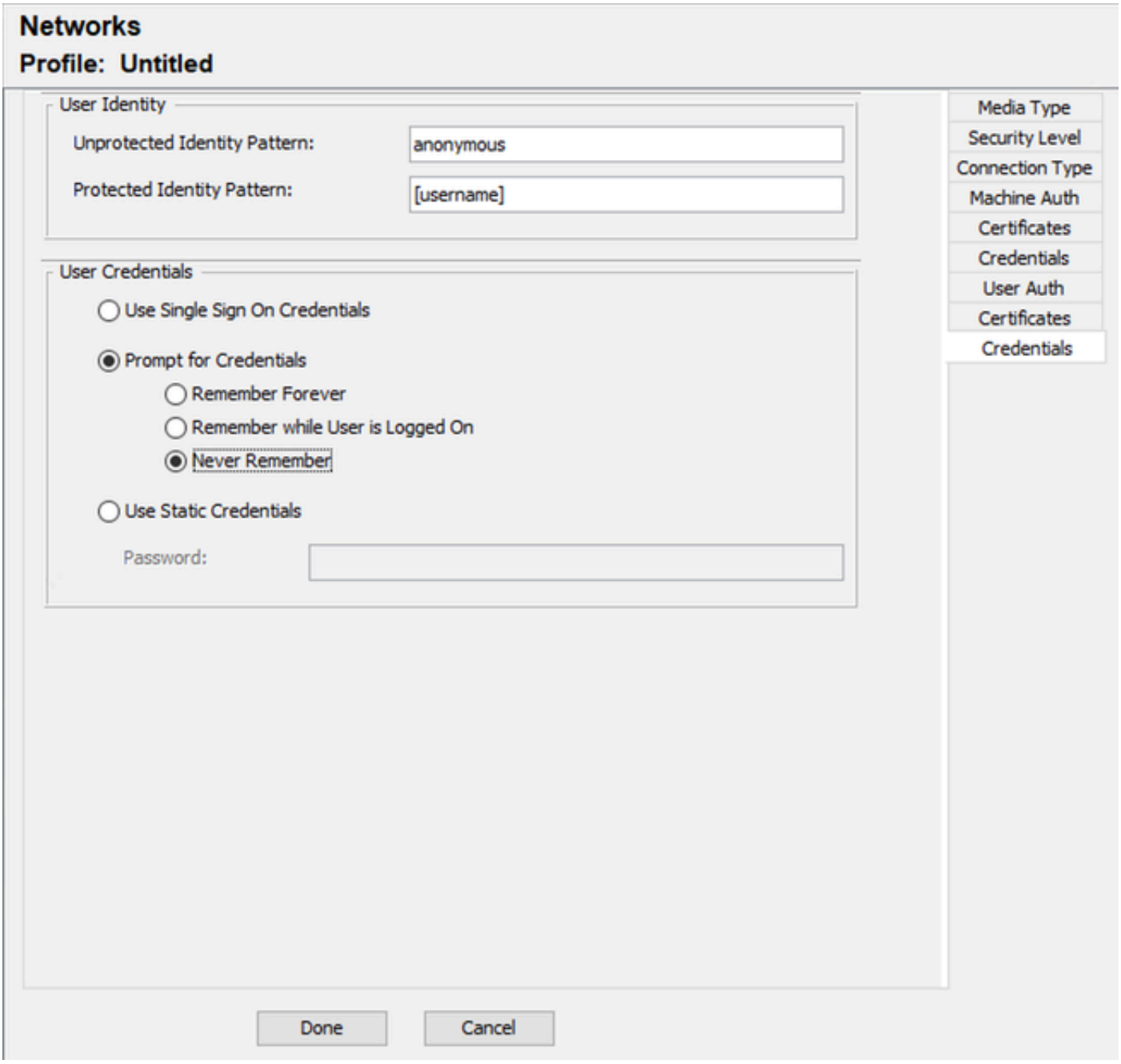
這些配置適用於伺服器在EAP PEAP流期間使用的證書。如果在您的環境中使用ISE，可以使用策略伺服器節點EAP證書的公用名稱。



使用者身份驗證伺服器證書信任部分

可在證書受信任頒發機構中選擇兩個選項。對於此方案，使用選項Trust any Root Certificate Authority(CA)，而不是新增簽署RADIUS EAP證書的特定CA證書。

按「Next」（下一步）。



使用者身份驗證憑據

在「身份證明」部分中，僅更改使用者身份證明部分。

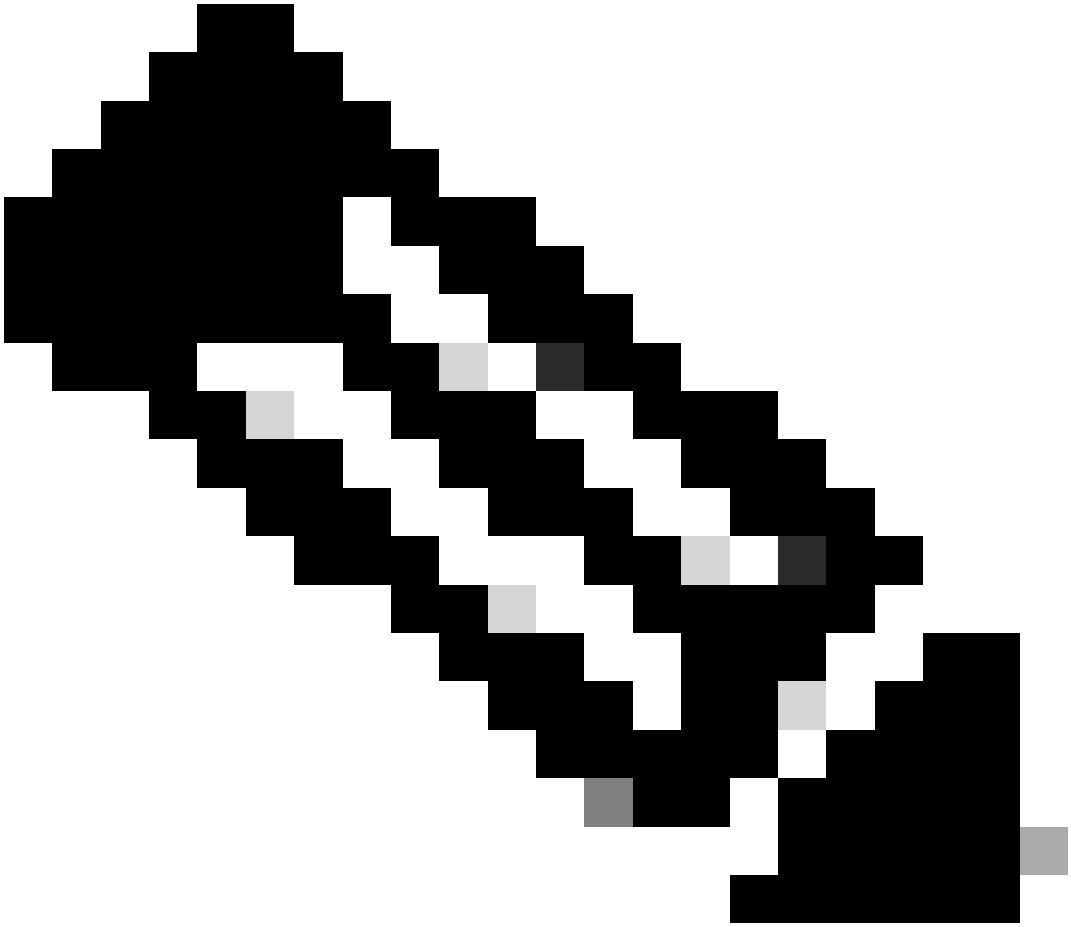
已選中提示輸入憑據>永不記憶選項。因此，在每個身份驗證中，使用者身份驗證必須輸入其憑據。

按一下Done按鈕。

選擇File > Save as，並將Secure Client Network Access Manager配置檔案另存為configuration.xml。

要使Secure Client Network Access Manager使用剛才建立的配置檔案，請將下一個目錄中的configuration.xml檔案替換為新檔案：

C:\ProgramData\Cisco\Cisco安全客戶端\網路訪問管理器\系統

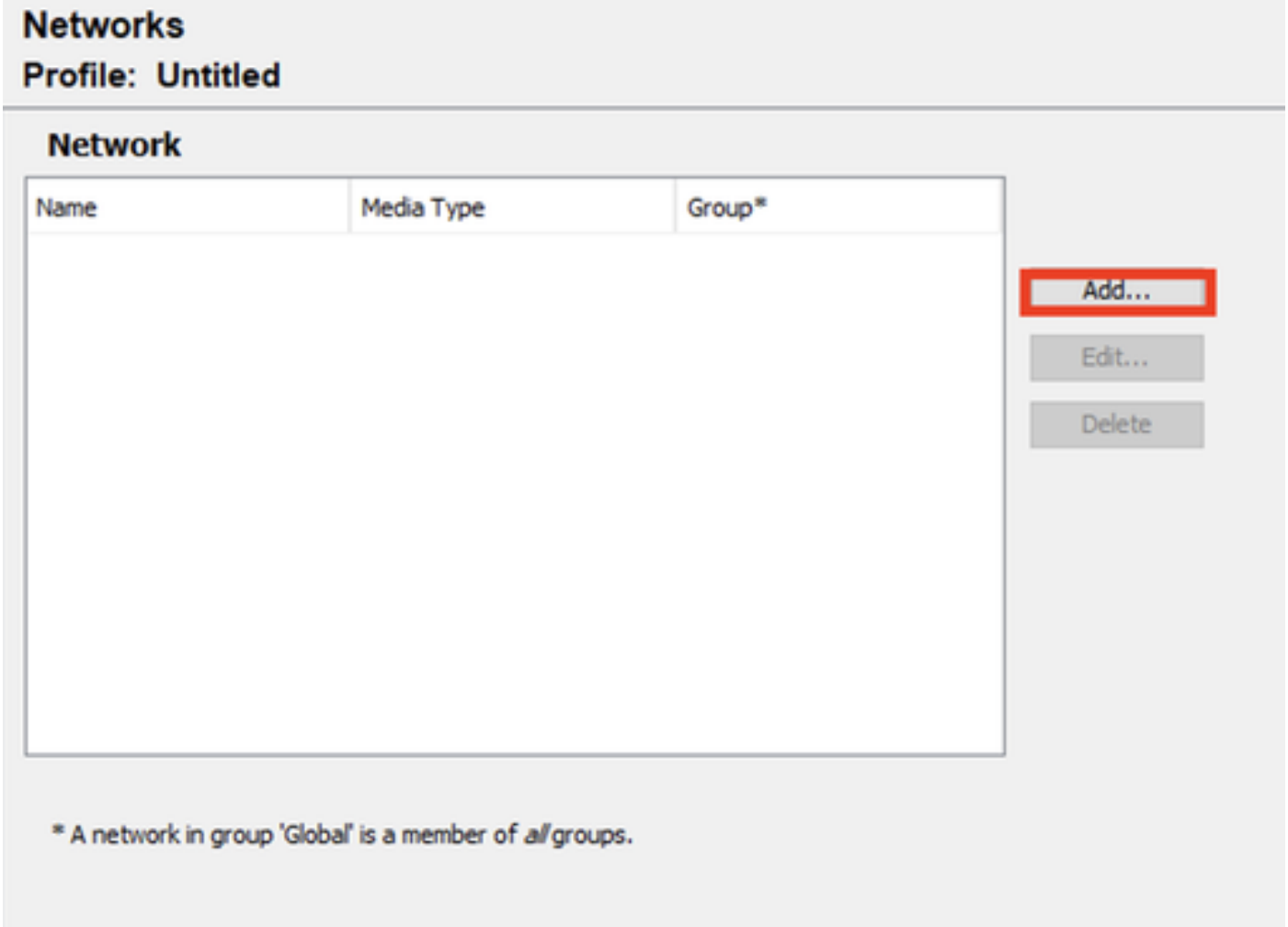


附註：檔案必須命名為configuration.xml，否則無法正常工作。

6.案例3:為EAP TLS使用者證書身份驗證配置安全客戶端NAM請求方

開啟NAM配置檔案編輯器，然後導航至Networks部分。

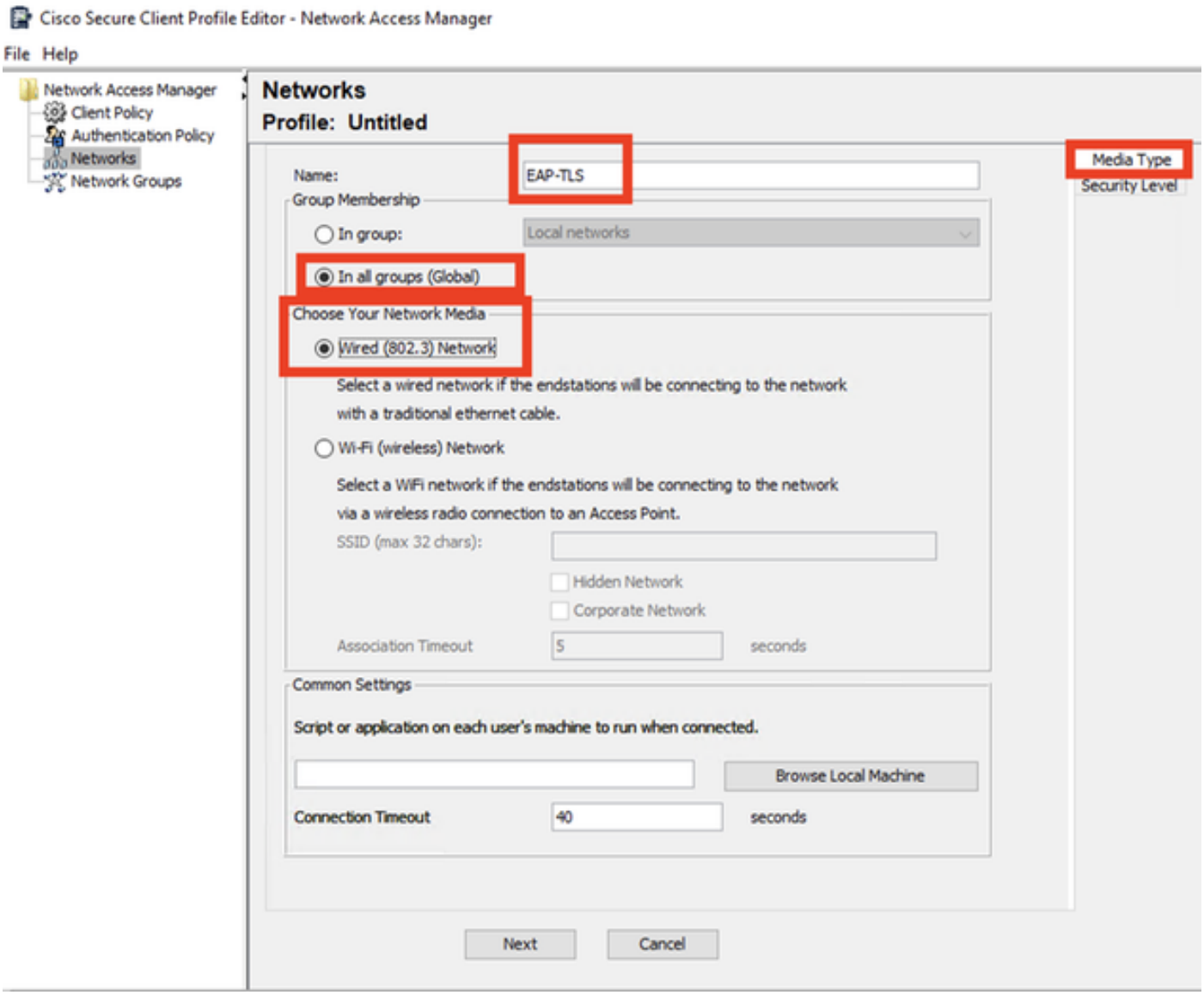
按一下「新增」。



網路建立部分

為網路配置檔案命名，在本例中，該名稱使用用於此方案的EAP協定。

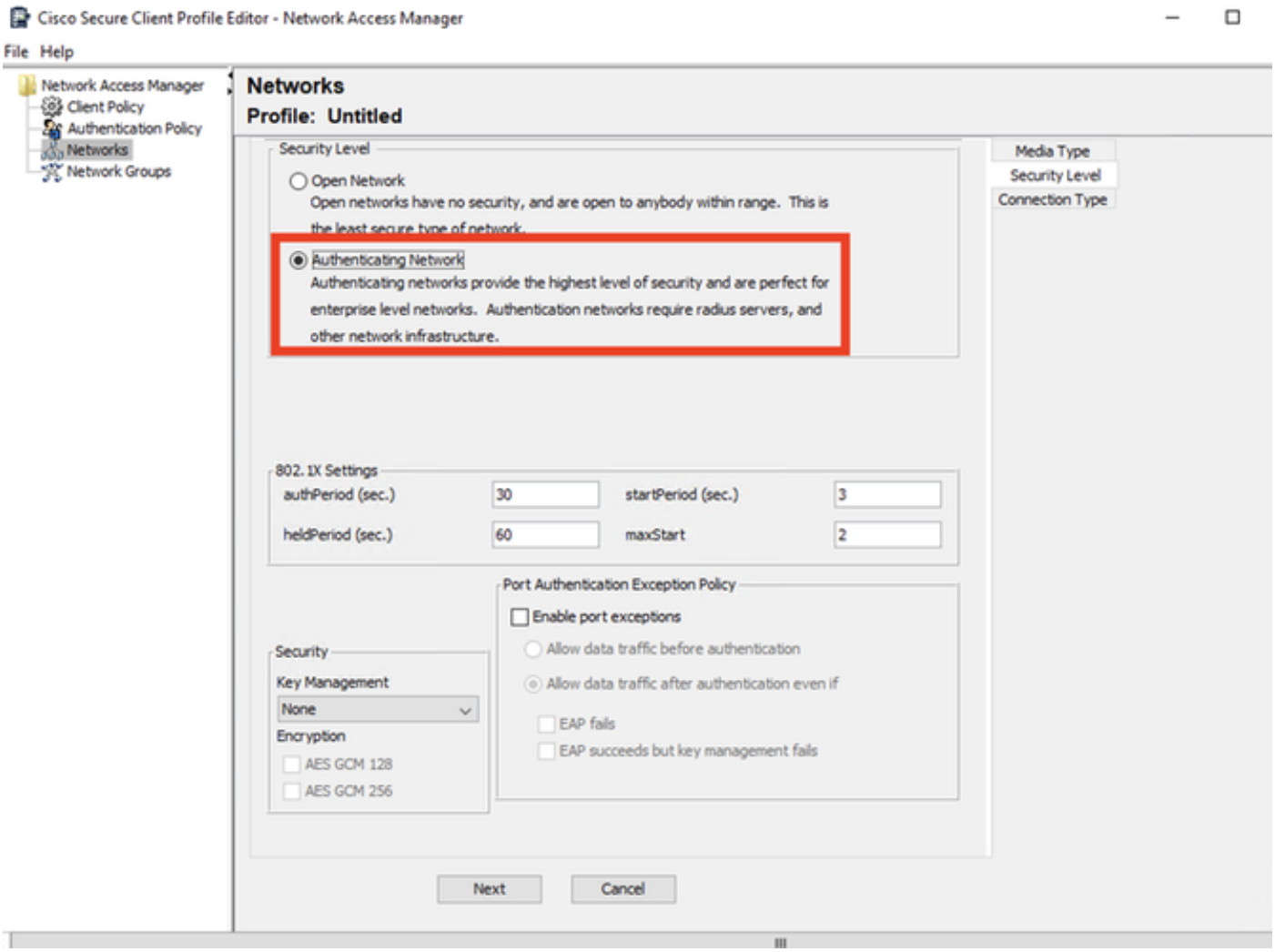
選擇Global作為Group Membership。和有線網路介質。



「介質型別」部分

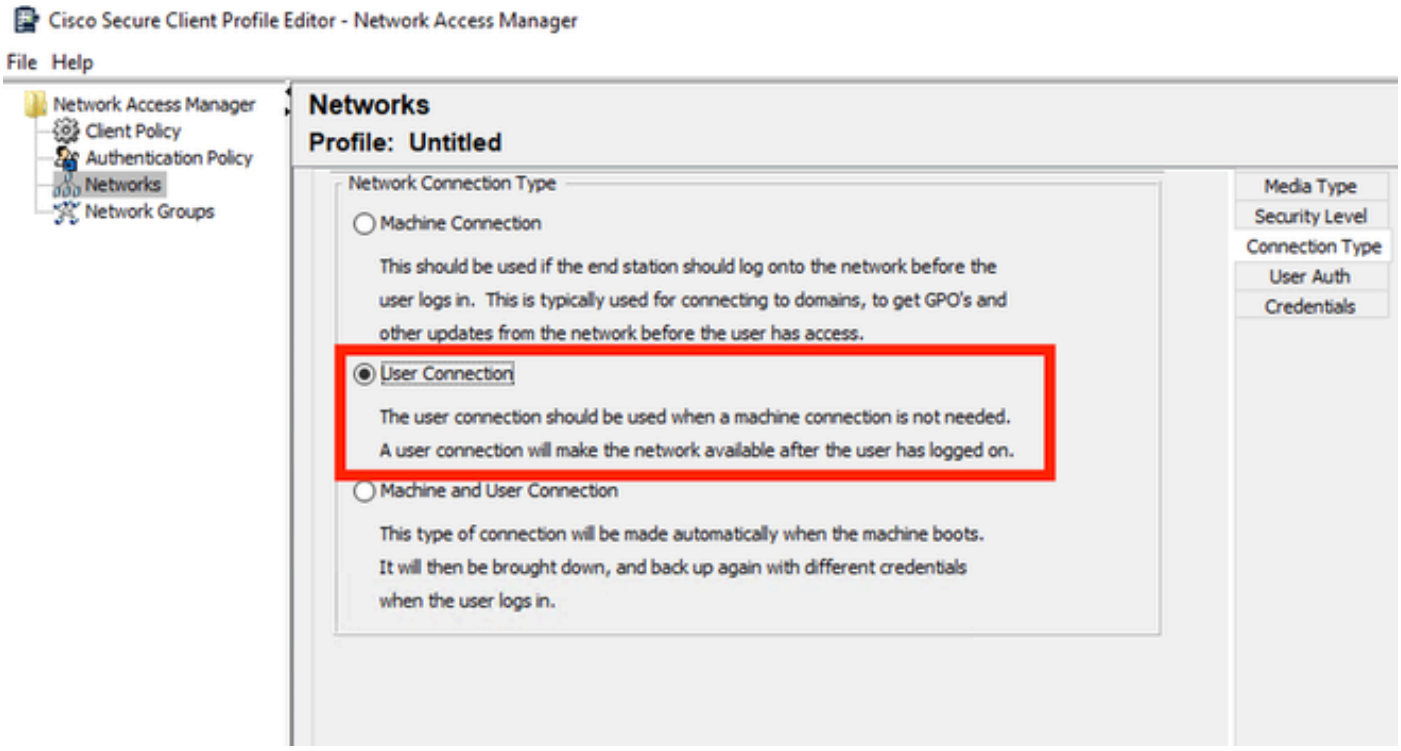
按「Next」（下一步）。

選擇Authenticating Network，不要更改Security Level部分中其餘選項的預設值。



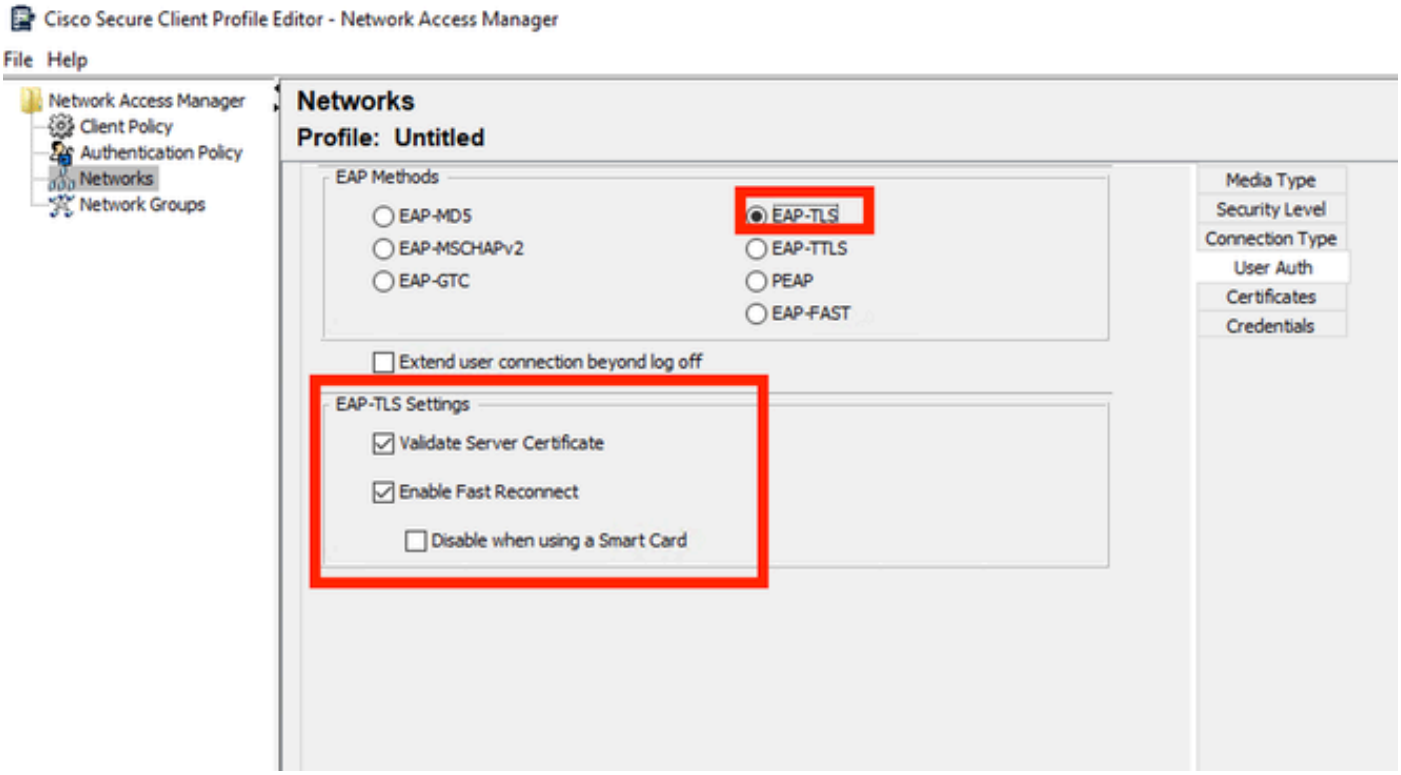
安全級別

此案例適用於使用憑證的使用者驗證。因此，使用User Connection選項。



連線型別

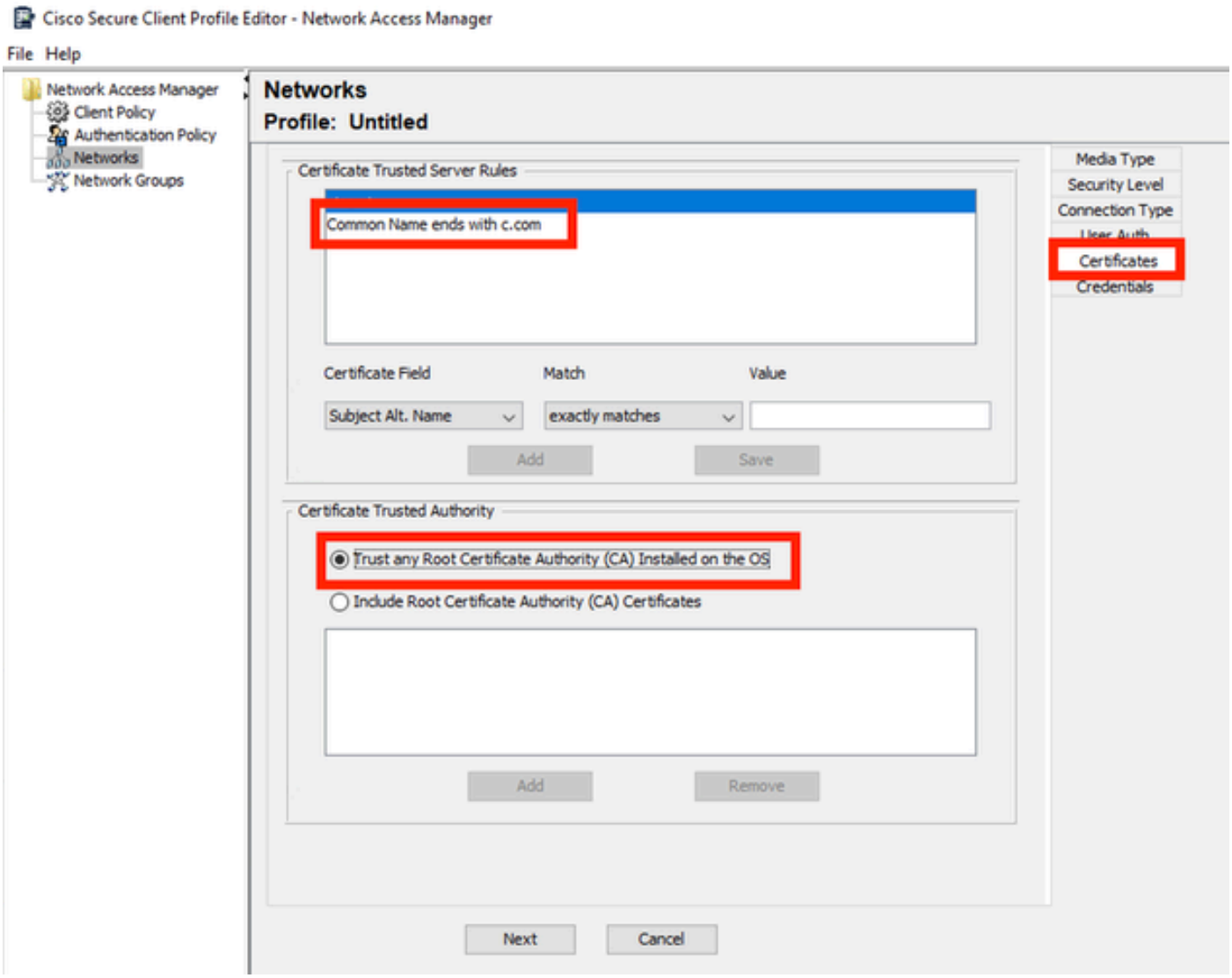
將EAP-TLS配置為EAP方法。請勿更改EAP-TLS設定部分中的預設值。



使用者身份驗證部分

對於「證書」部分，建立與AAA EAP-TLS證書匹配的規則。如果您使用的是ISE，請在Administration > System > Certificates部分中查詢此規則。

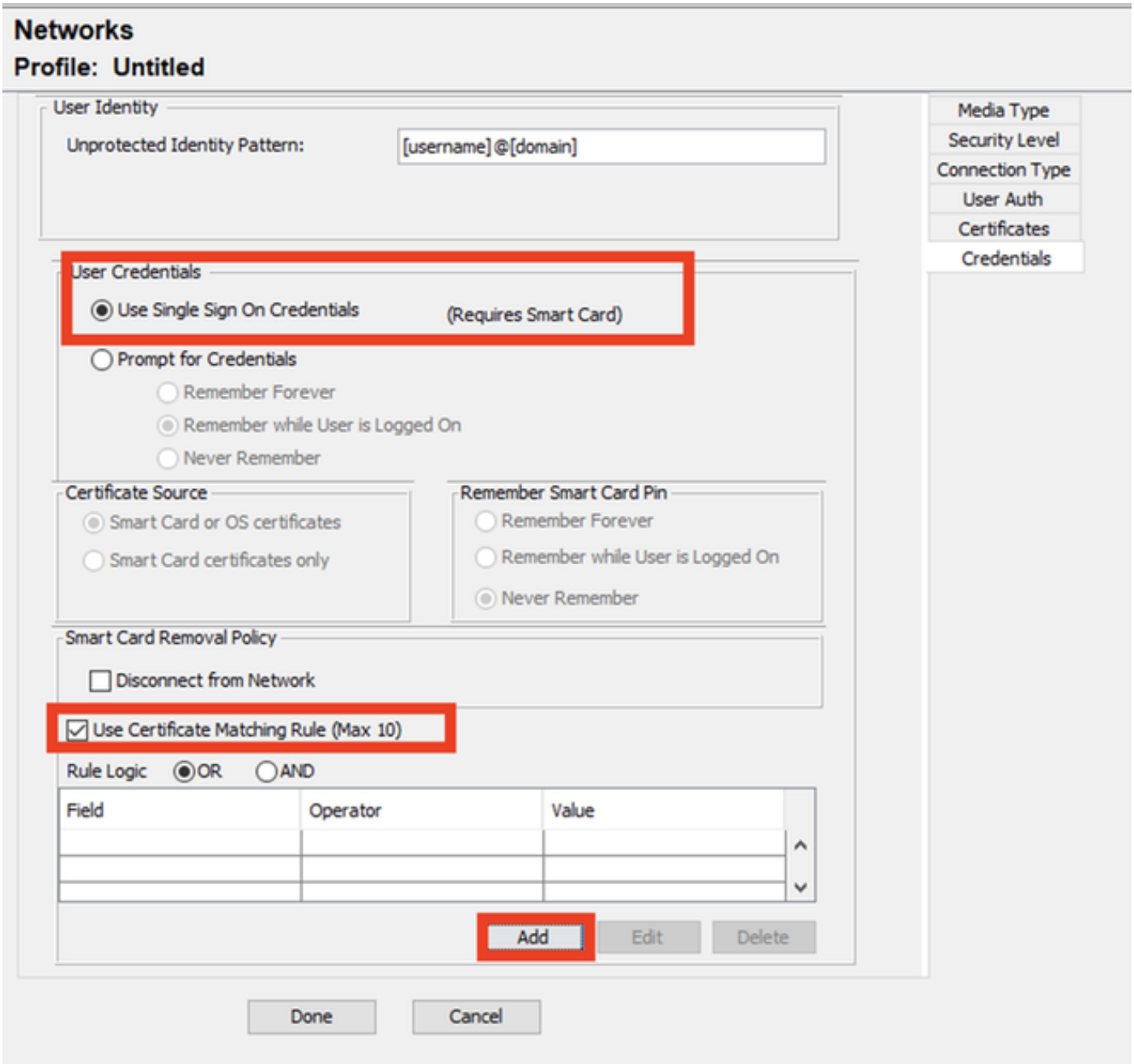
在Certificate Trusted Authority部分中，選擇Trust any Root Certificate Authority(CA)安裝在OS上。



使用者身份驗證伺服器證書信任設定

按「Next」（下一步）。

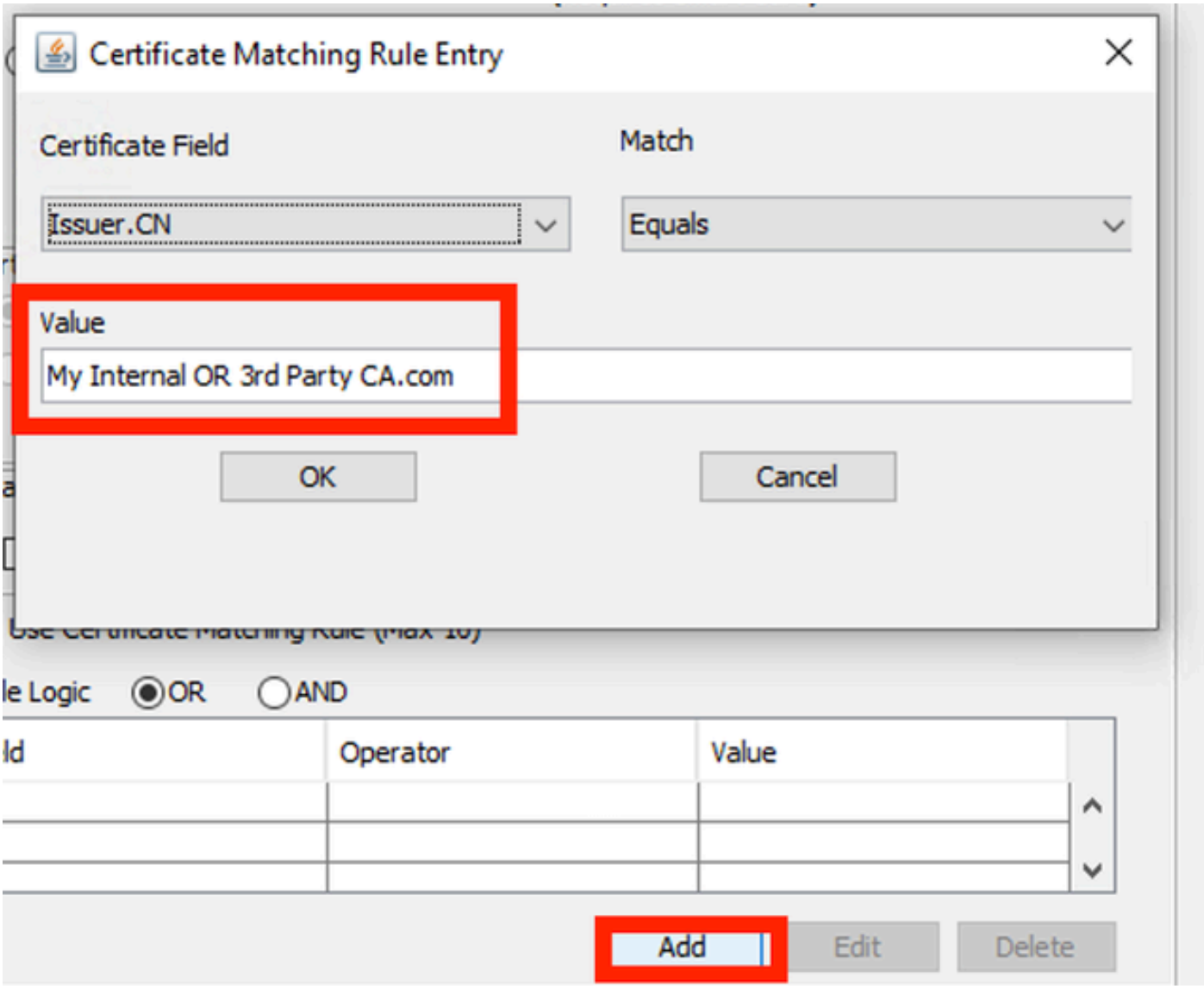
對於「使用者憑據」部分，請勿更改第一部分中的預設值。



User Auth Credentials部分

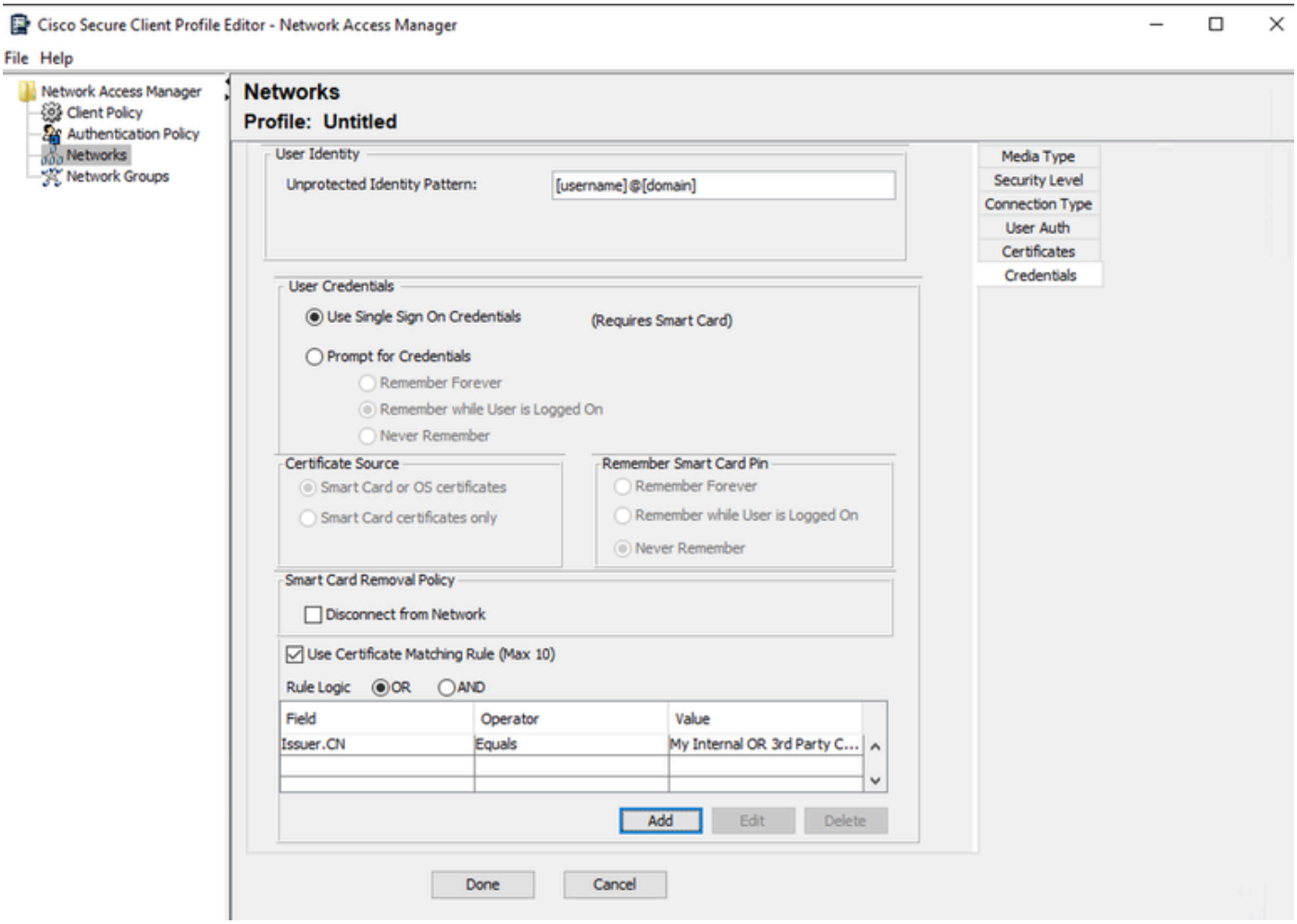
必須配置與使用者在EAP TLS過程中傳送的身份證書匹配的規則。要執行此操作，請點選Use Certificate Machining Rule(Max 10)旁邊的覈取方塊。

按一下「新增」。



證書匹配規則視窗

將值My Internal或第三方CA.com字串替換為使用者證書的CN。



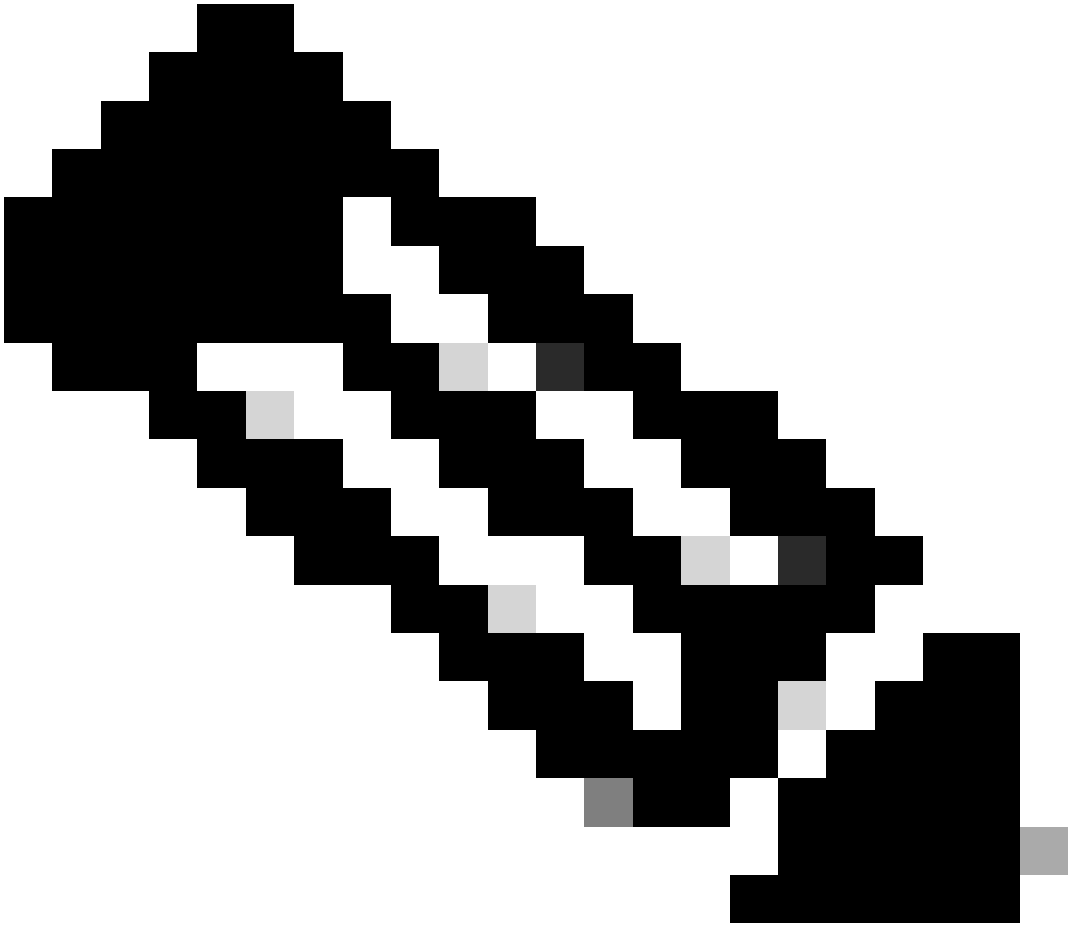
User Auth Certificate Credentials部分

按一下「Done」以完成設定。

選擇File > Save as，將Secure Client Network Access Manager配置檔案另存為configuration.xml。

要使Secure Client Network Access Manager使用剛才建立的配置檔案，請將下一個目錄中的configuration.xml檔案替換為新檔案：

C:\ProgramData\Cisco\Cisco安全客戶端\網路訪問管理器\系統

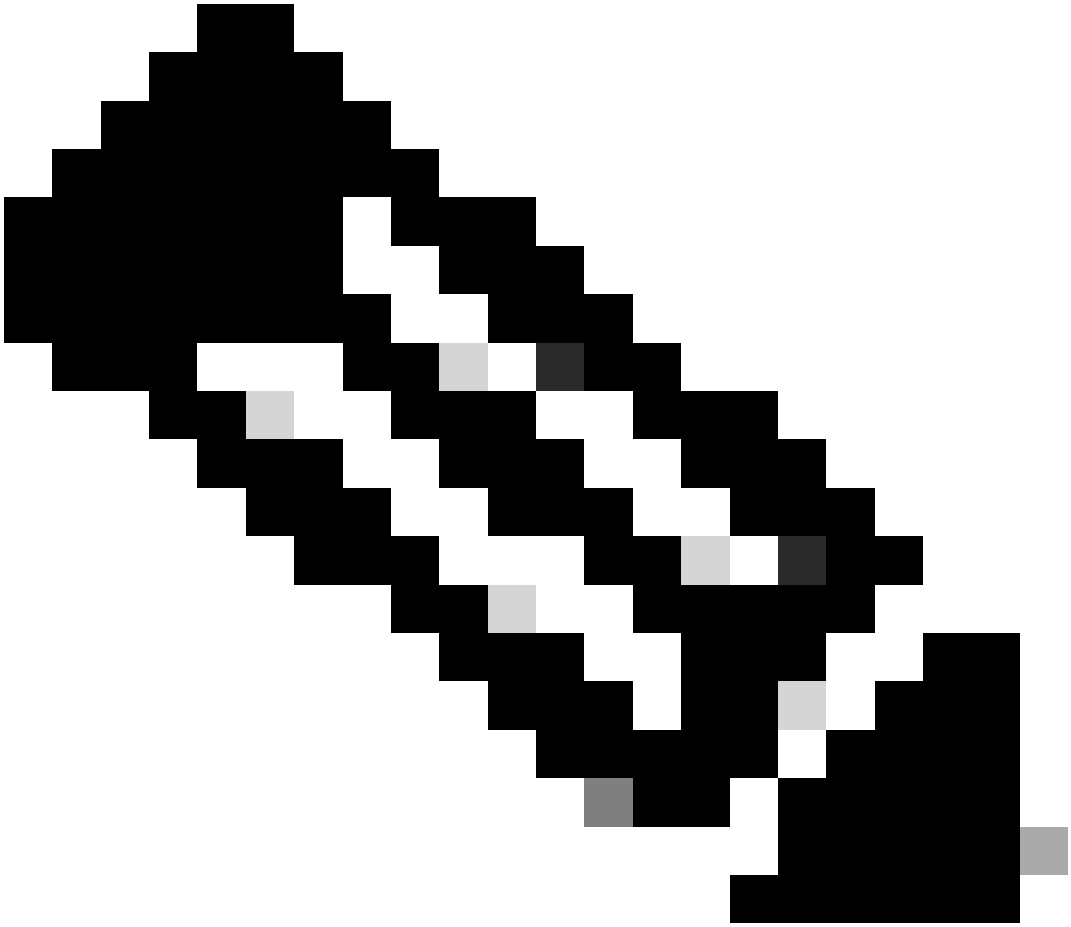


附註：檔案必須命名為configuration.xml，否則無法正常工作。

7.配置ISR 1100和ISE以允許基於方案1 PEAP MSCHAPv2的身份驗證

配置ISR 1100路由器。

本節介紹NAD使dot1x工作必須具備的基本配置。



附註：對於多節點ISE部署，指向啟用了策略伺服器節點角色的任何節點。可通過在Administration > System > Deployment頁籤中導航到ISE來檢查此問題。

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
 client A.B.C.D server-key  <Your shared secret>
!
!
radius server  ISE-PSN-1
 address ipv4 A.B.C.D auth-port 1645 acct-port 1646
 timeout 15
 key <Your shared secret>
!
!
```

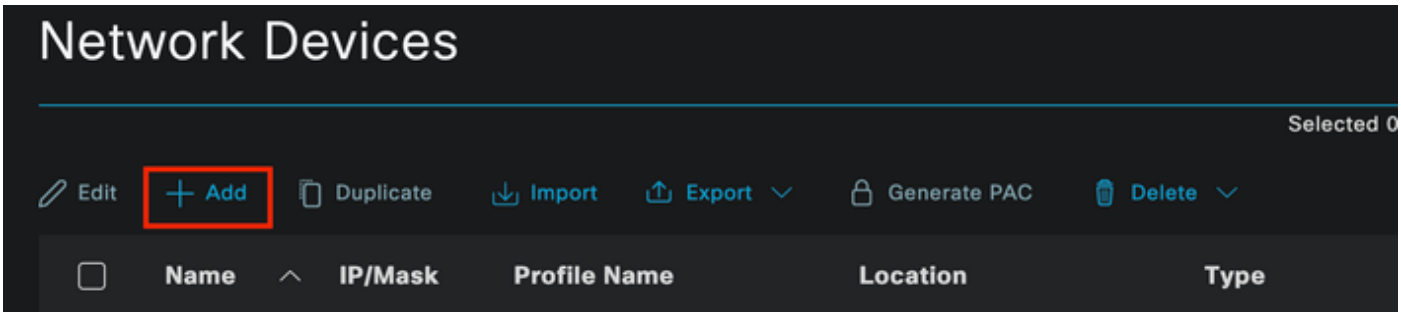
```
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

配置身份服務引擎3.2。

配置網路裝置。

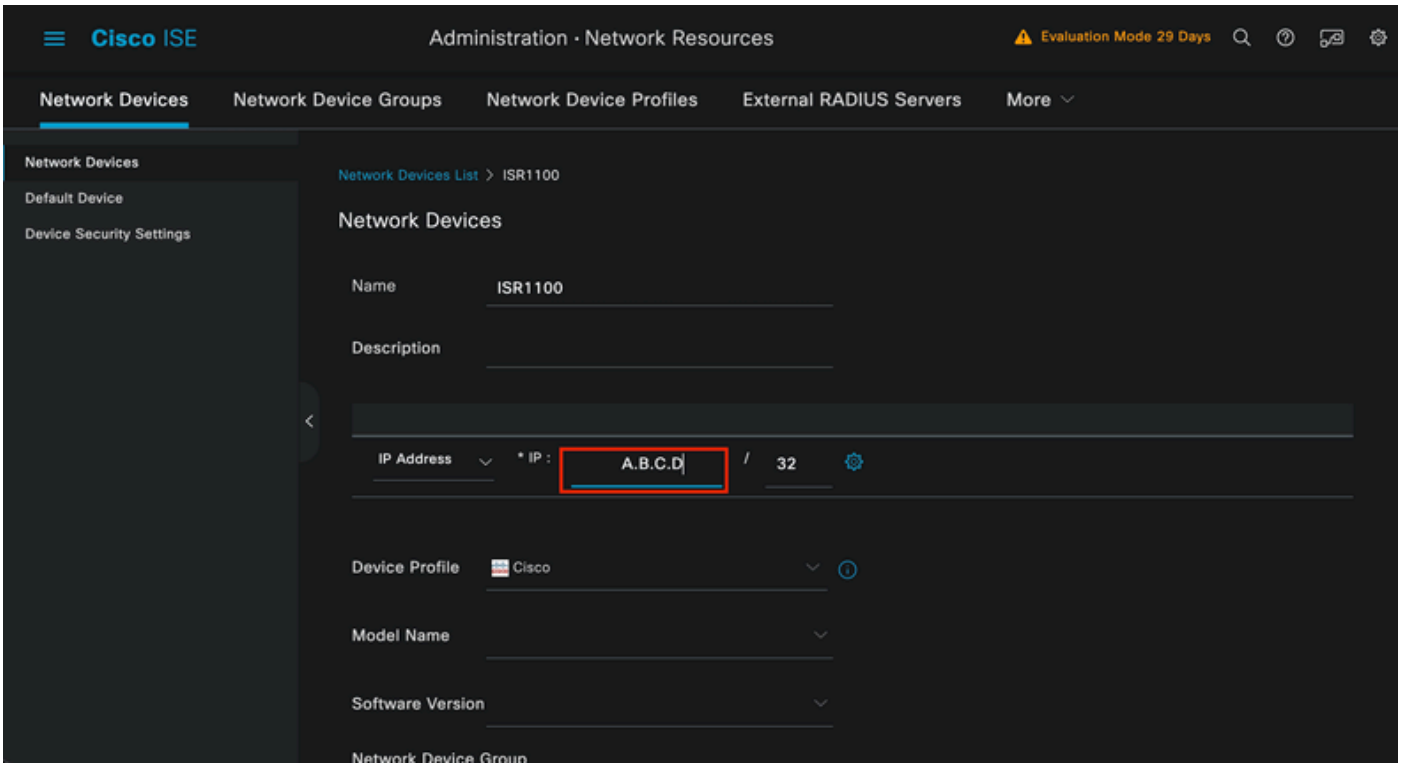
將ISR NAD新增到ISE管理>網路資源>網路裝置。

按一下「新增」。



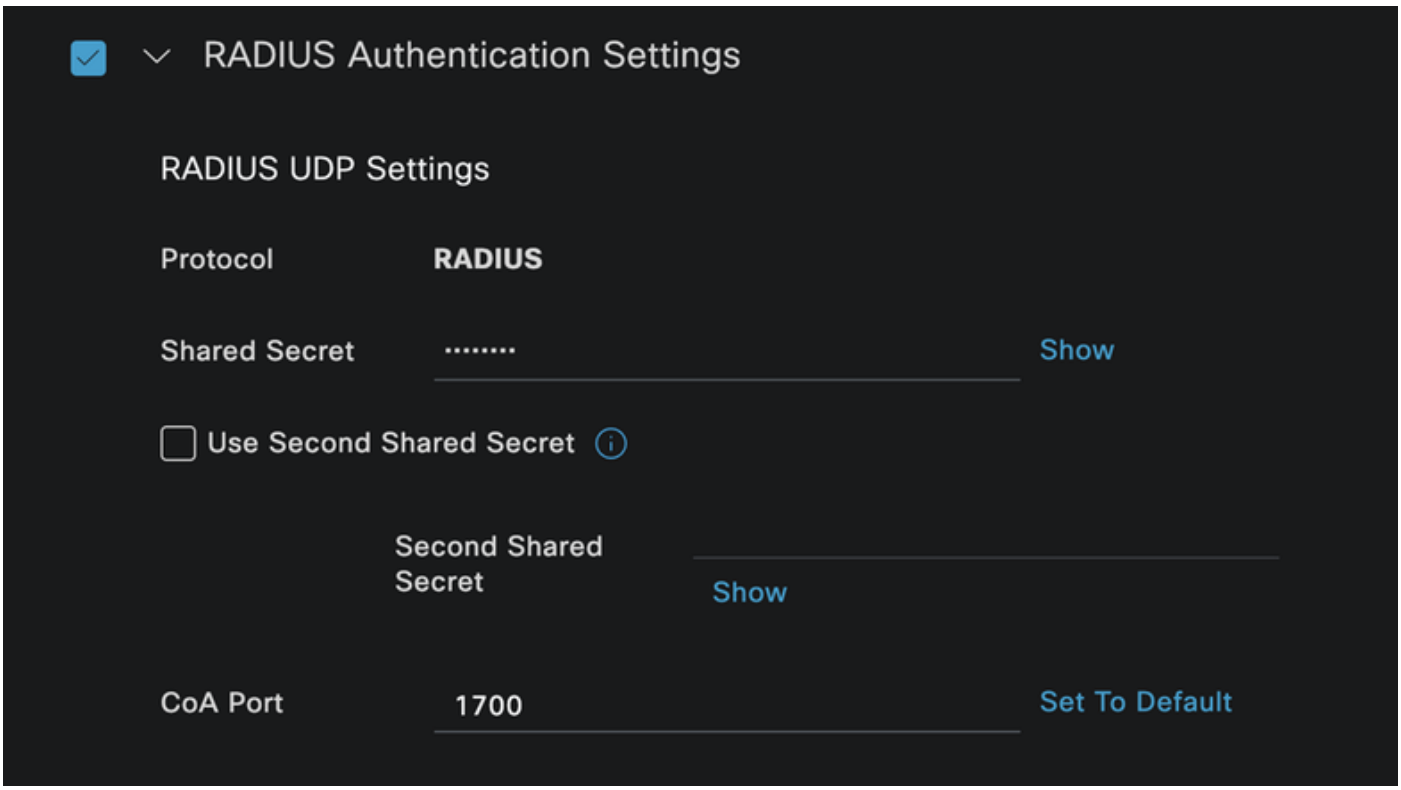
網路裝置部分

為正在建立的NAD指定名稱。新增網路裝置IP。



網路裝置建立

在同一頁的底部新增您在網路裝置配置中使用的共用金鑰。



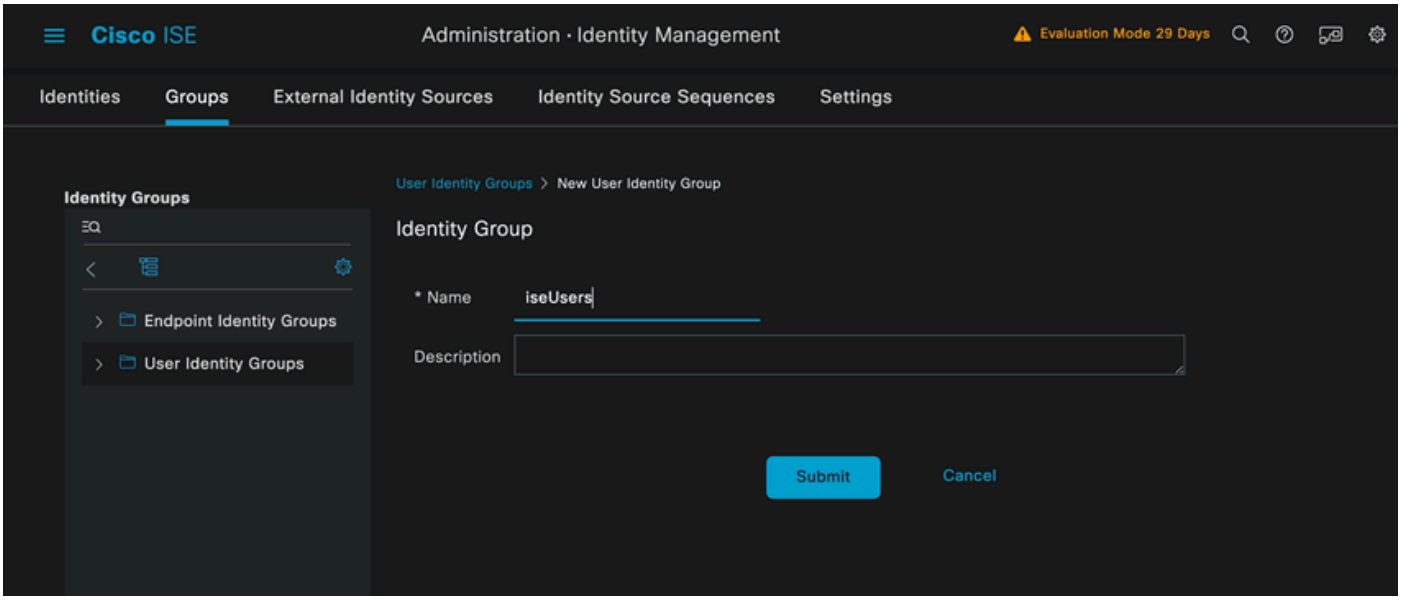
網路裝置*Radius*設定

儲存更改。

配置用於對端點進行身份驗證的標識。

使用ISE本地身份驗證。本文未解釋外部ISE身份驗證。

導航到Administration > Identity Management > Groups頁籤，然後建立使用者所屬的組。為此演示建立的身份組為iseUsers。

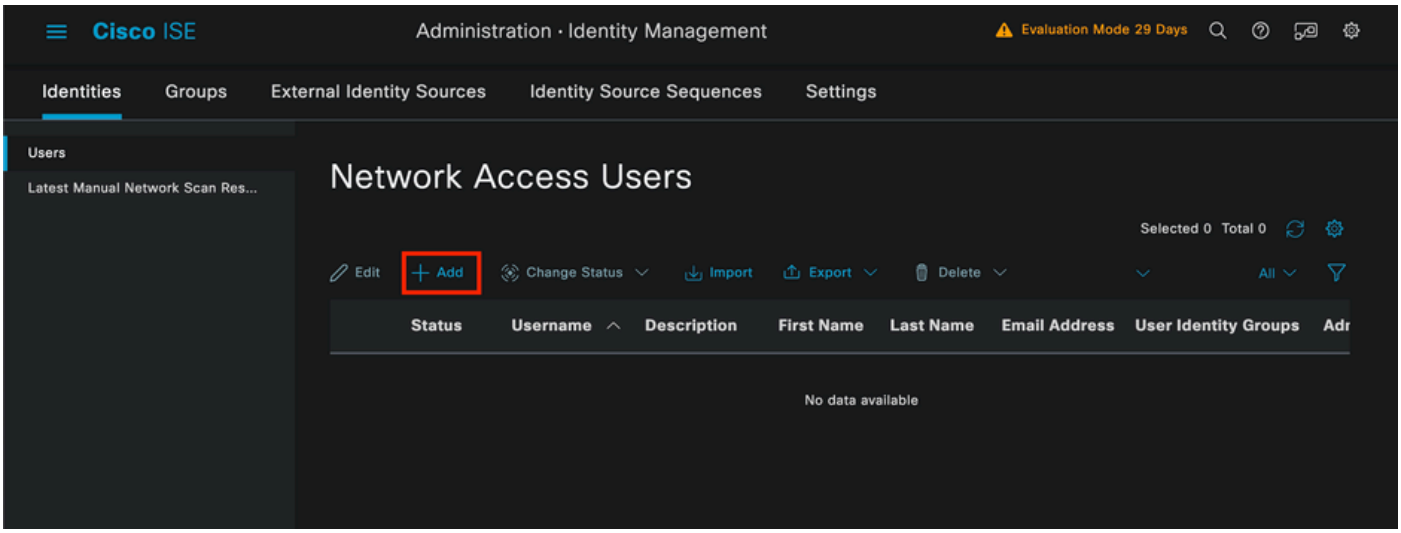


身份組建立

按一下「Submit」。

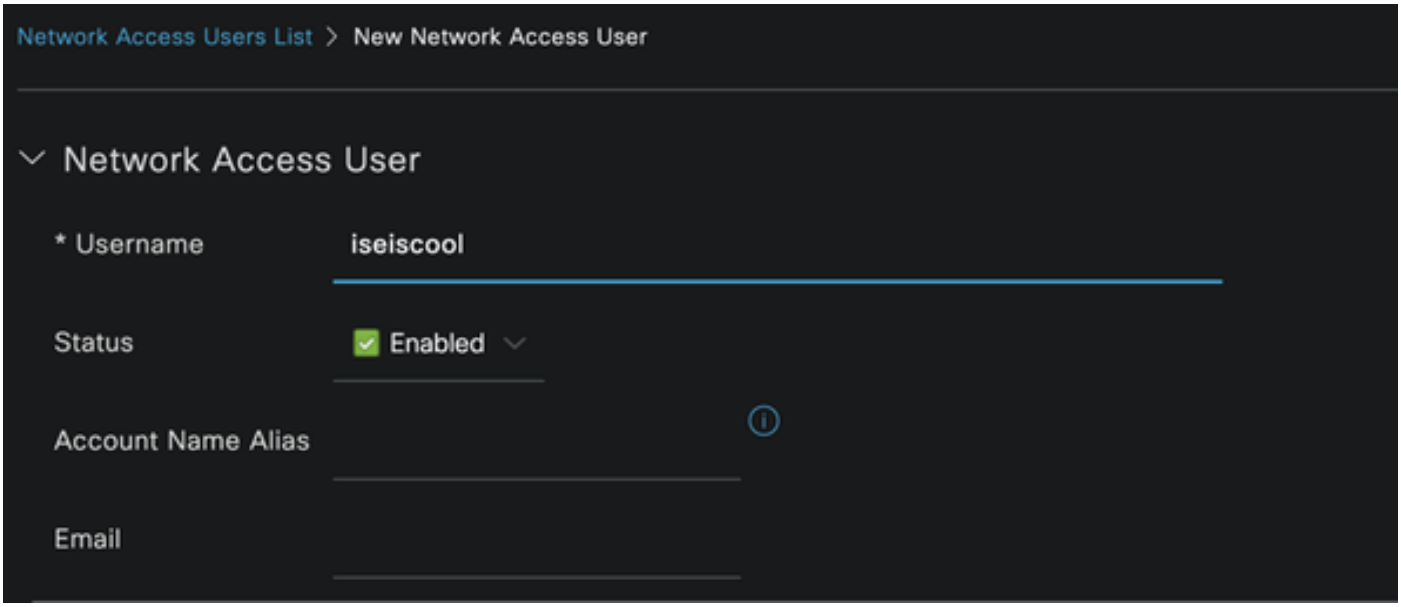
導航到管理>身份管理>身份選項卡。

按一下「新增」。



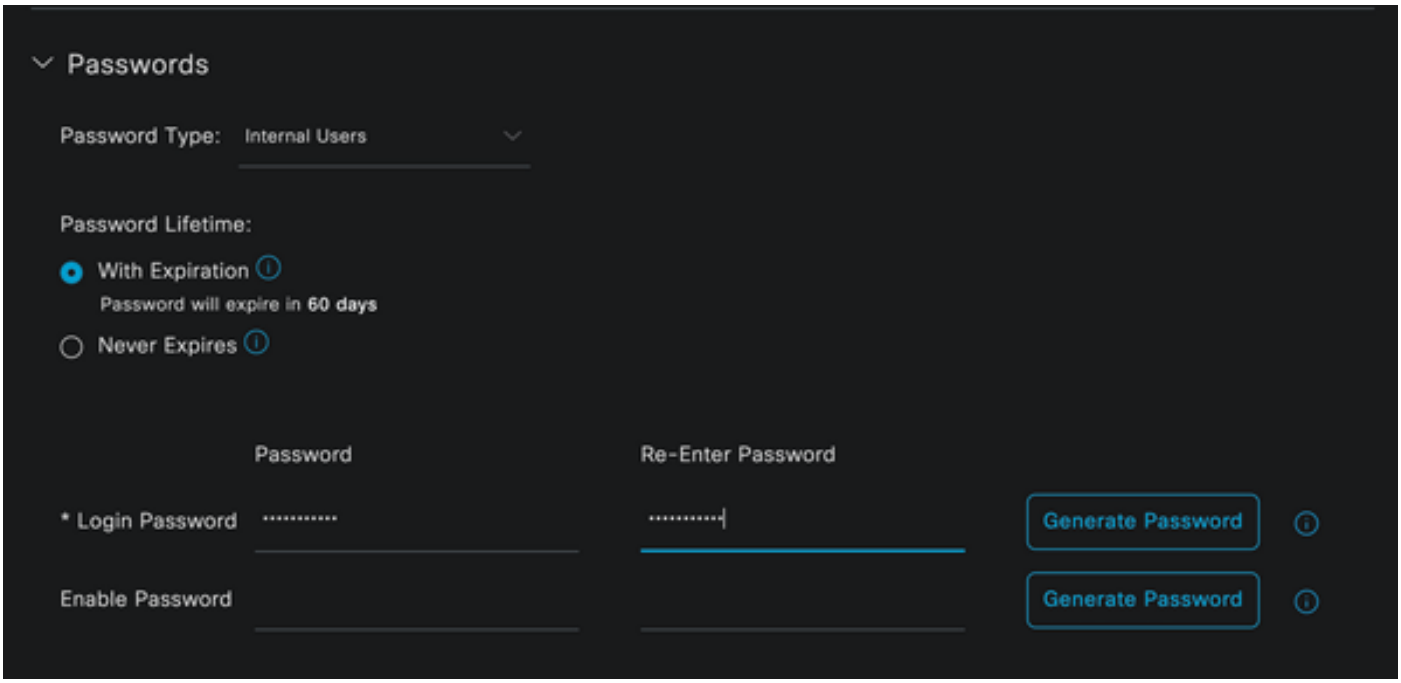
「網路訪問使用者」部分

作為必填欄位的一部分，以使用者的名稱開頭。本範例中使用的是使用者名稱iseiscool。



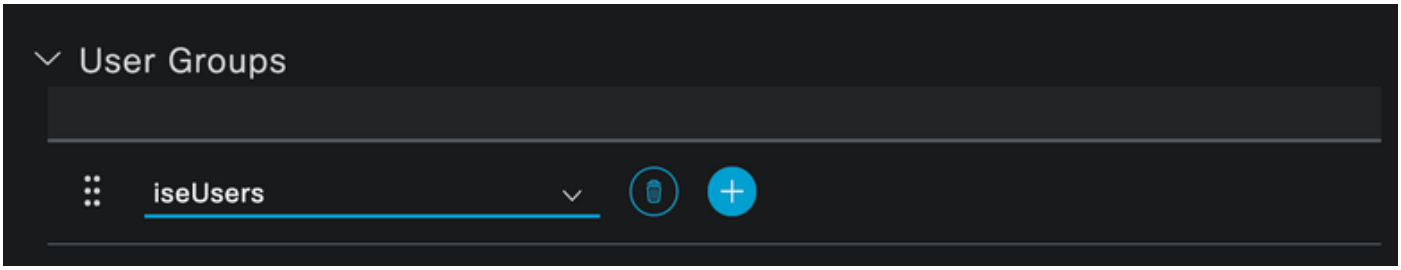
網路訪問使用者建立

為使用者分配密碼。使用VainillaISE97。



User Creation Password部分

將使用者分配到iseUsers組。

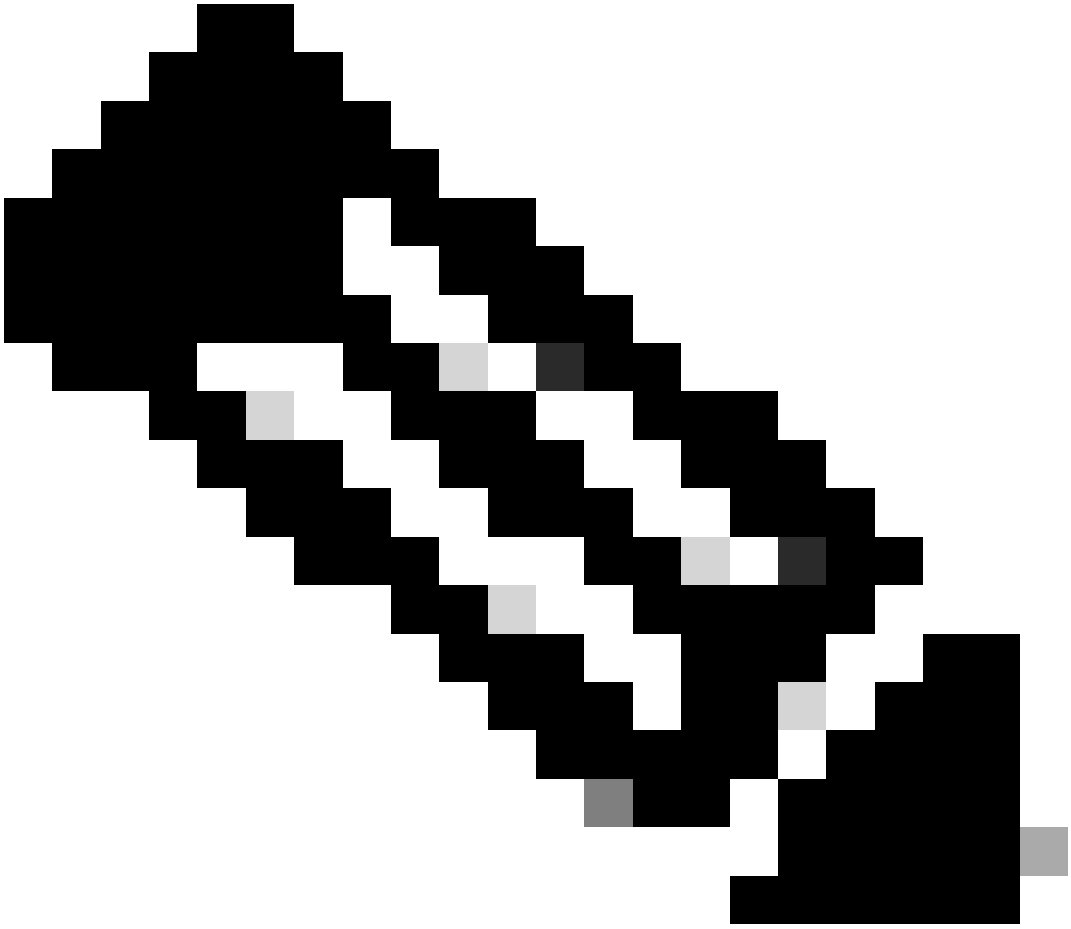


使用者組分配

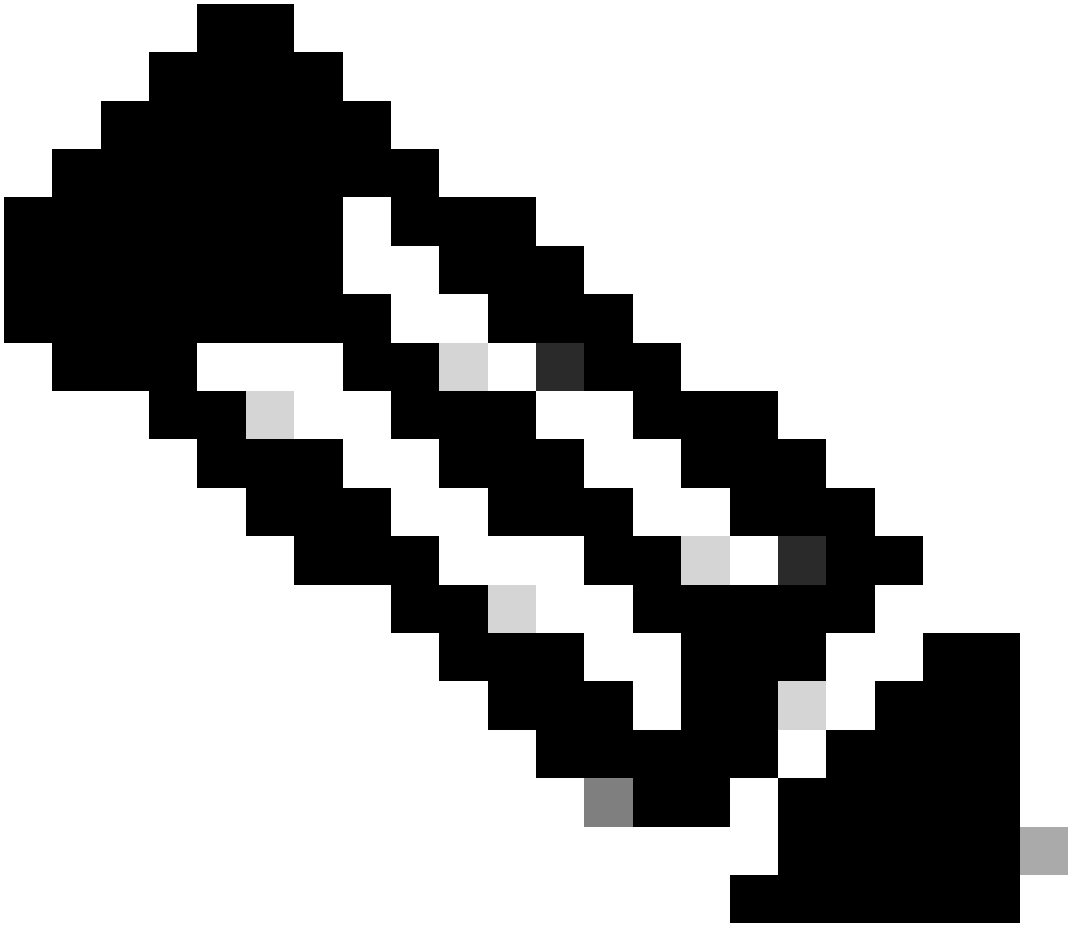
配置策略集。

導航到ISE選單>策略>策略集。

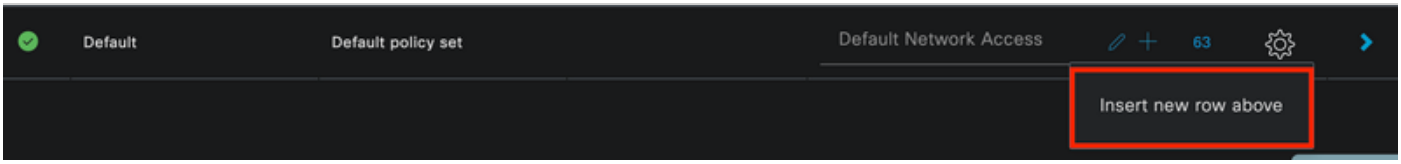
可以使用預設策略集。但是本範例建立了名為「有線」的網路。



附註：對策略集進行分類和區分有助於進行故障排除，

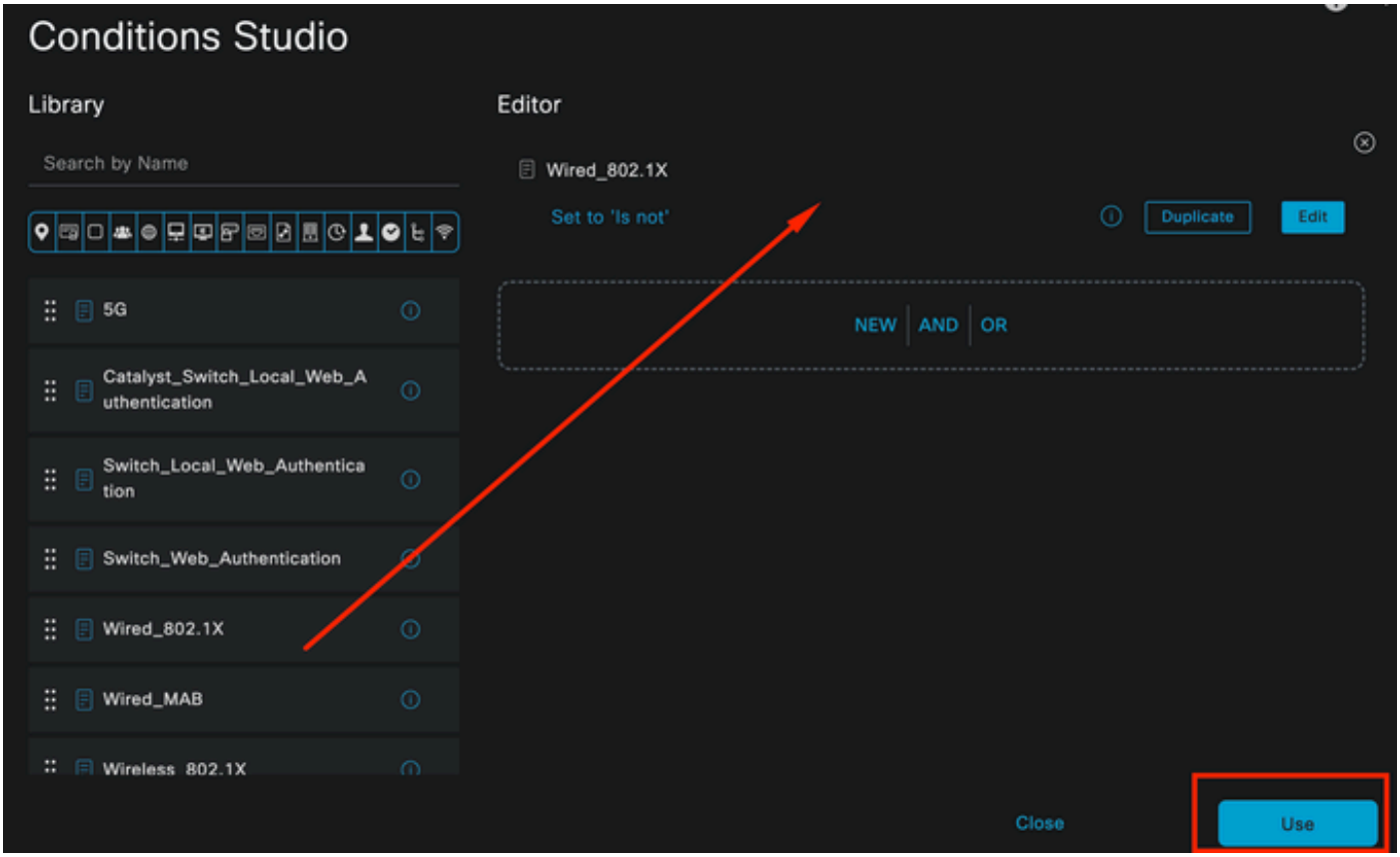


附註：如果看不到新增或加號圖示，則可以按一下任何策略集的齒輪圖示，然後選擇在上面插入新行。



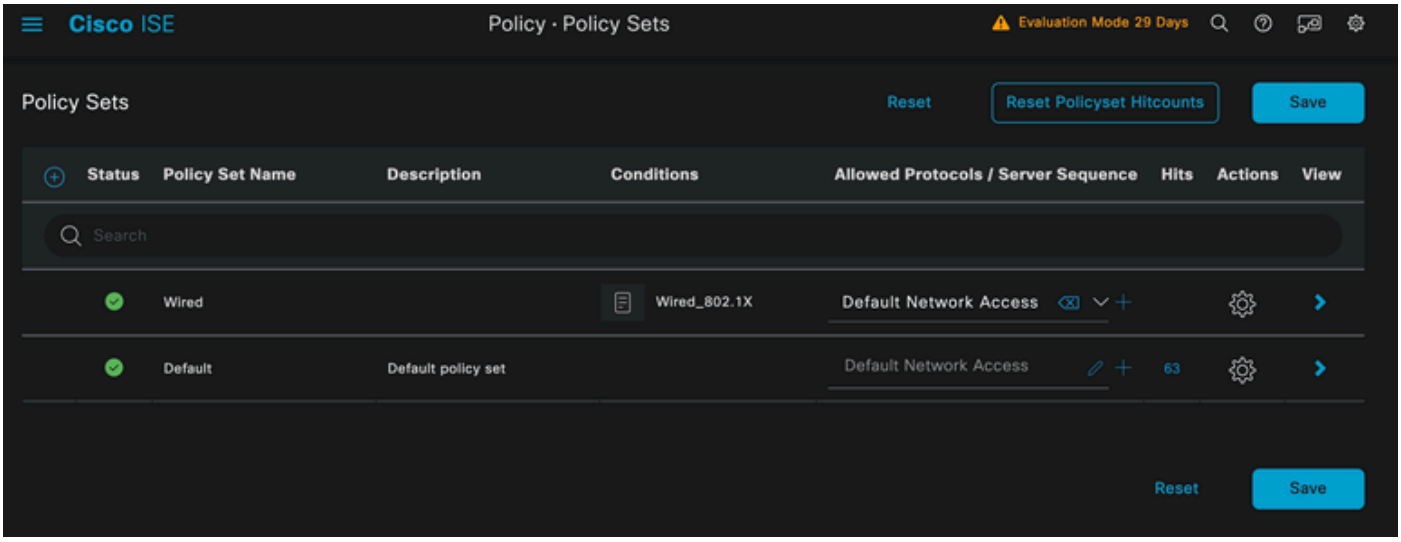
齒輪圖示選項

使用的條件是有線8021x。拖動它，然後按一下Use。



驗證原則條件工作室

在Allowed Protocols部分中選擇Default Network Access。

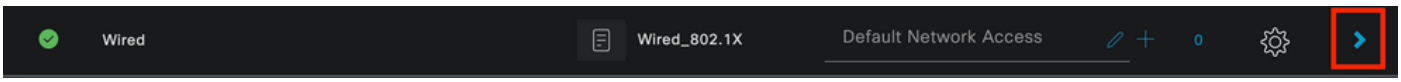


策略集常規檢視

按一下「Save」。

2.d.配置身份驗證和授權策略。

按一下>圖標。



有線策略集

展開Authentication Policy部分。

按一下+圖標。

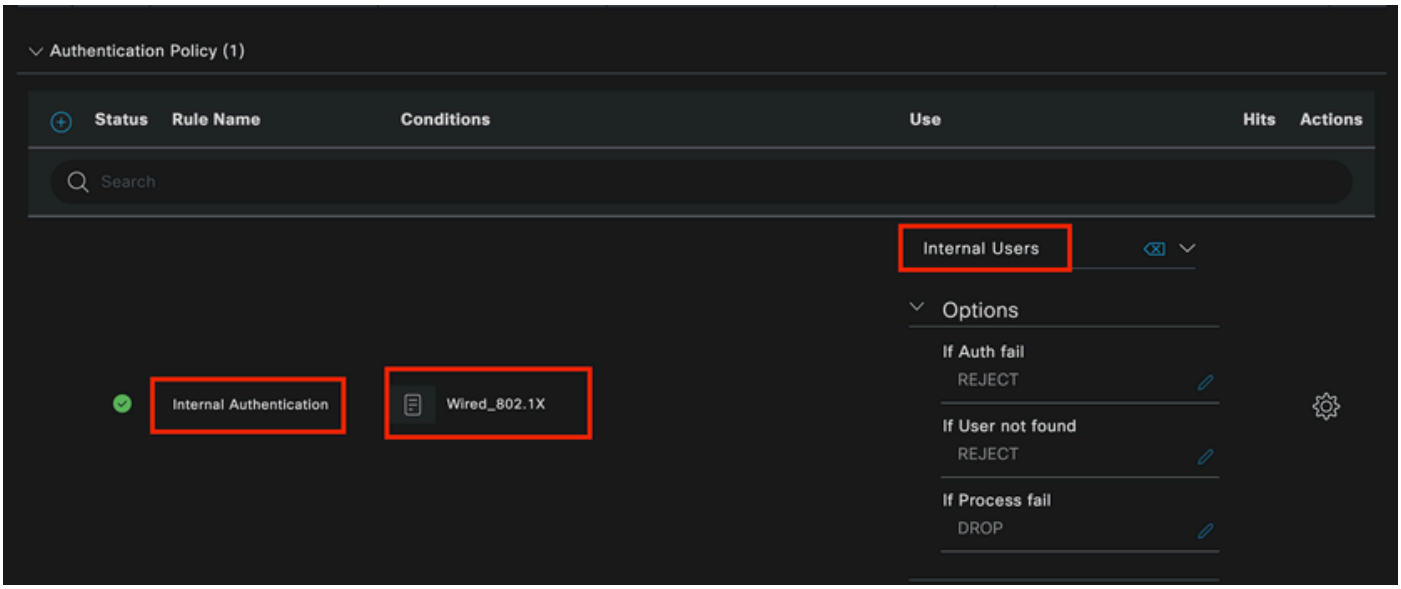
身份驗證策略

為身份驗證策略分配名稱。此示例使用內部身份驗證。

點選此新身份驗證策略的條件列上的+圖示。

使用預先設定的Wired Dot1x條件。

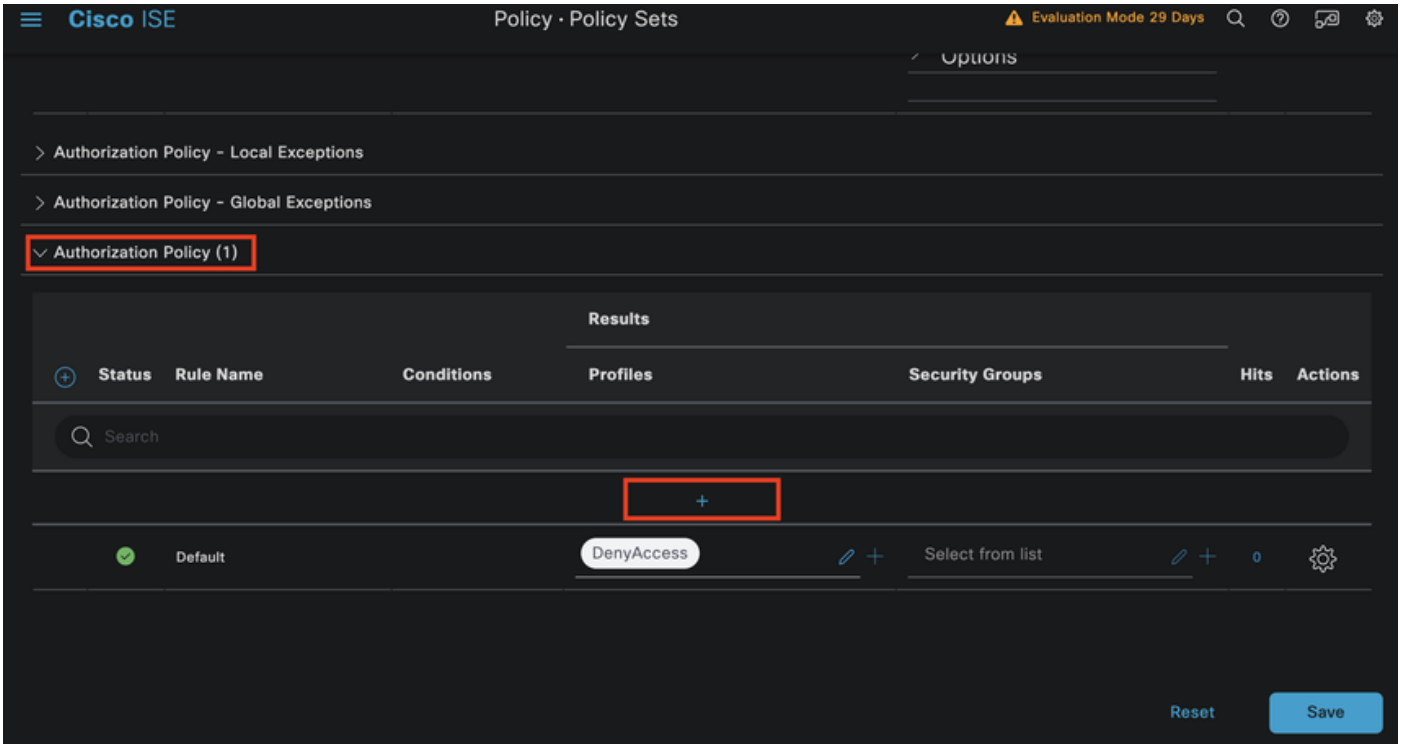
最後，在使用列中選擇內部使用者。



身份驗證策略

授權策略。

Authorization Policy部分位於頁面底部。展開它並按一下+圖標。



授權策略

為最近建立的授權策略命名。在此配置示例中，使用內部ISE使用者名稱。

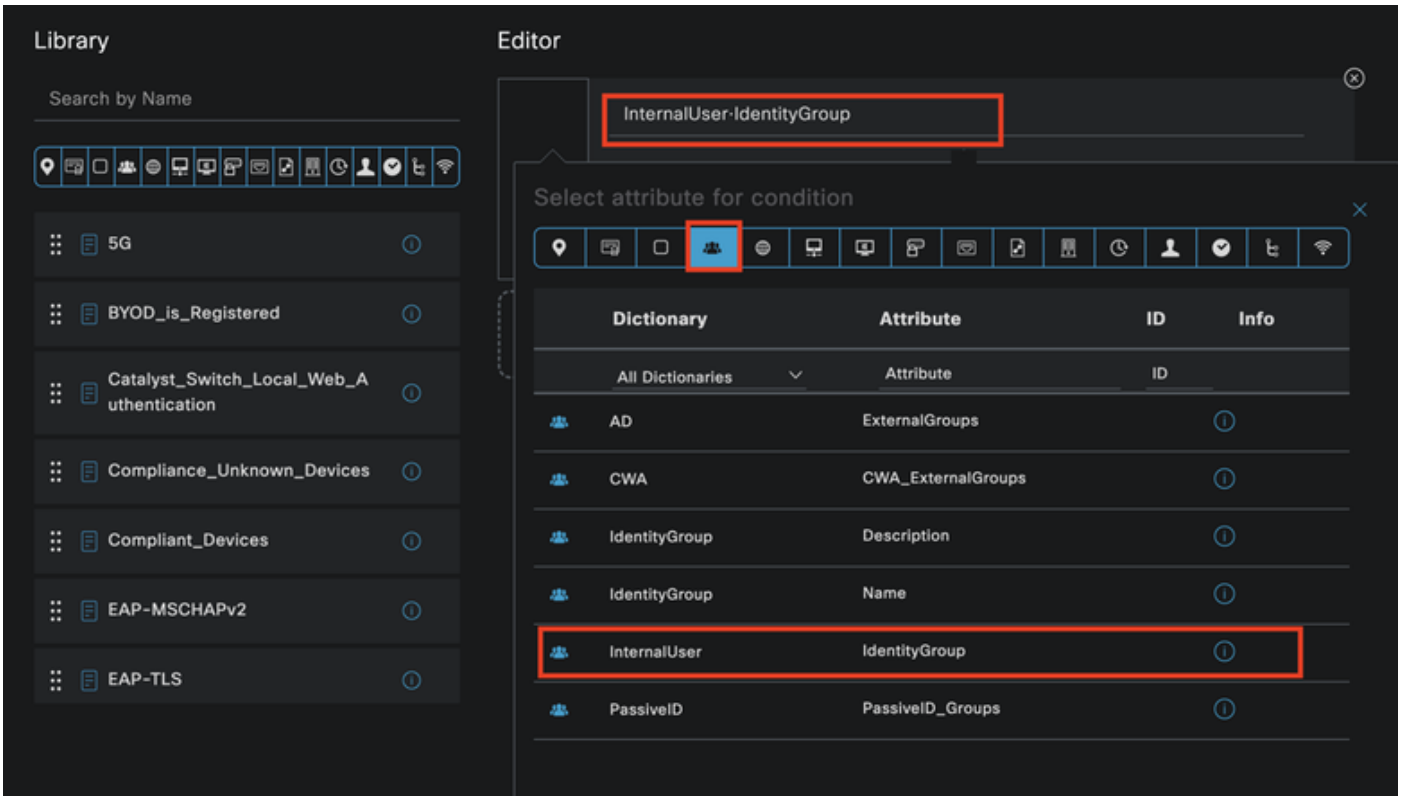
要為此授權策略建立條件，請按一下條件列中的+圖示。

使用IseUsers組。

按一下Attribute部分。

選擇IdentityGroup圖標。

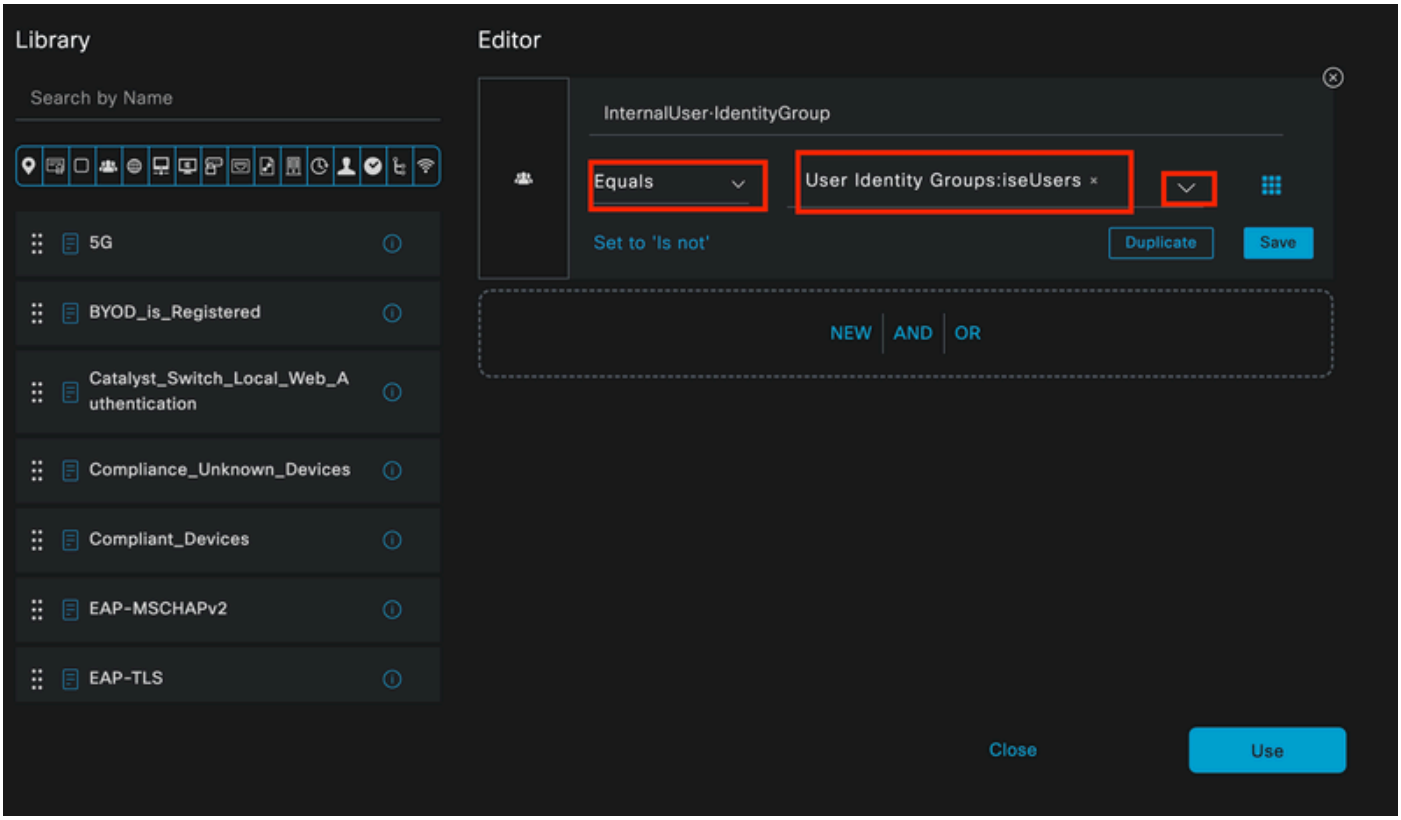
從字典中選擇隨IdentityGroup屬性提供的InternalUser字典。



條件建立

選擇Equals運算符。

在使用者身份組中，選擇組IseUsers。

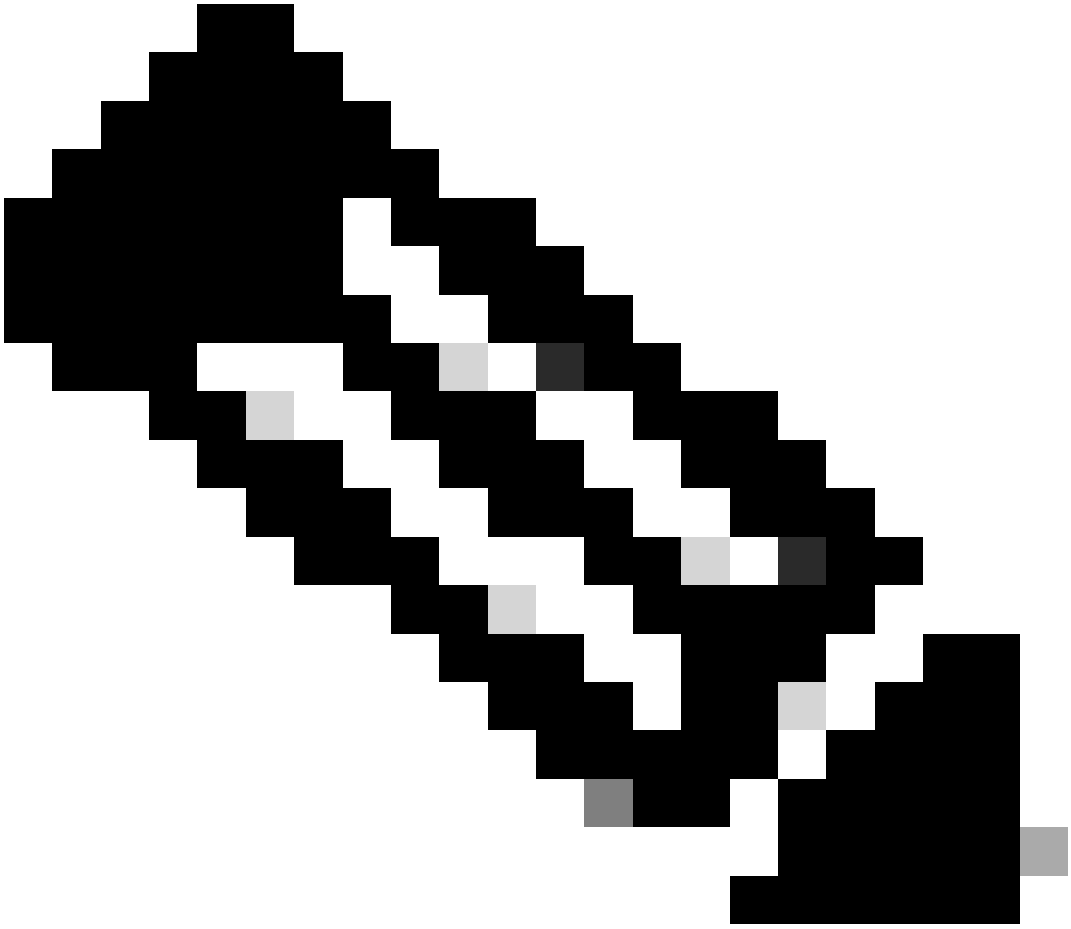


條件建立

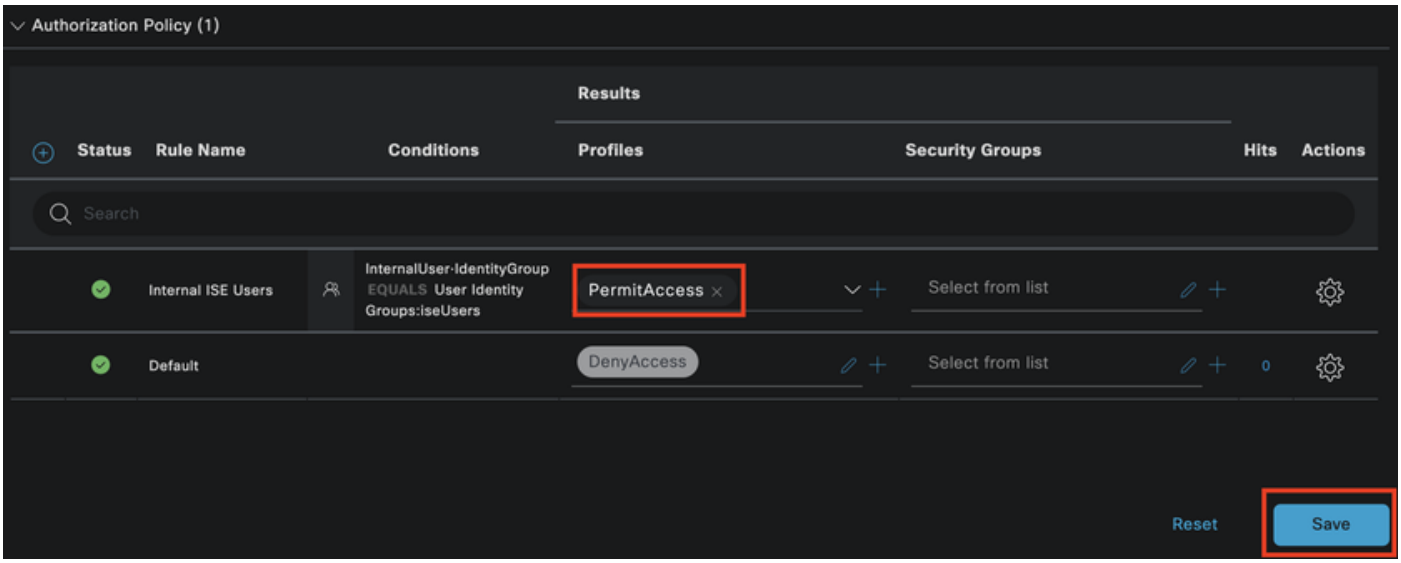
按一下「Use」。

新增結果授權配置檔案。

使用預配置的配置檔案Permit Access。



附註：請注意，進入到ISE的身份驗證點選此有線Dot1x策略集（不屬於使用者身份組ISEUsers），點選預設授權策略(其結果為DenyAccess)。



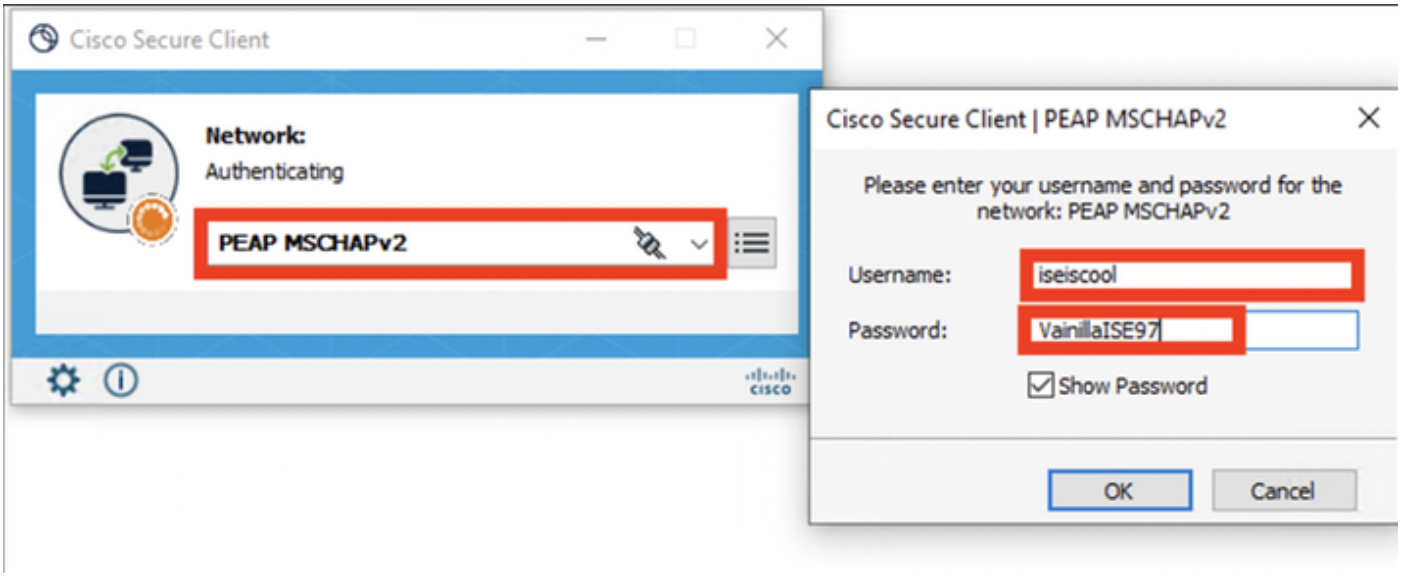
授權策略

按一下「Save」。

驗證

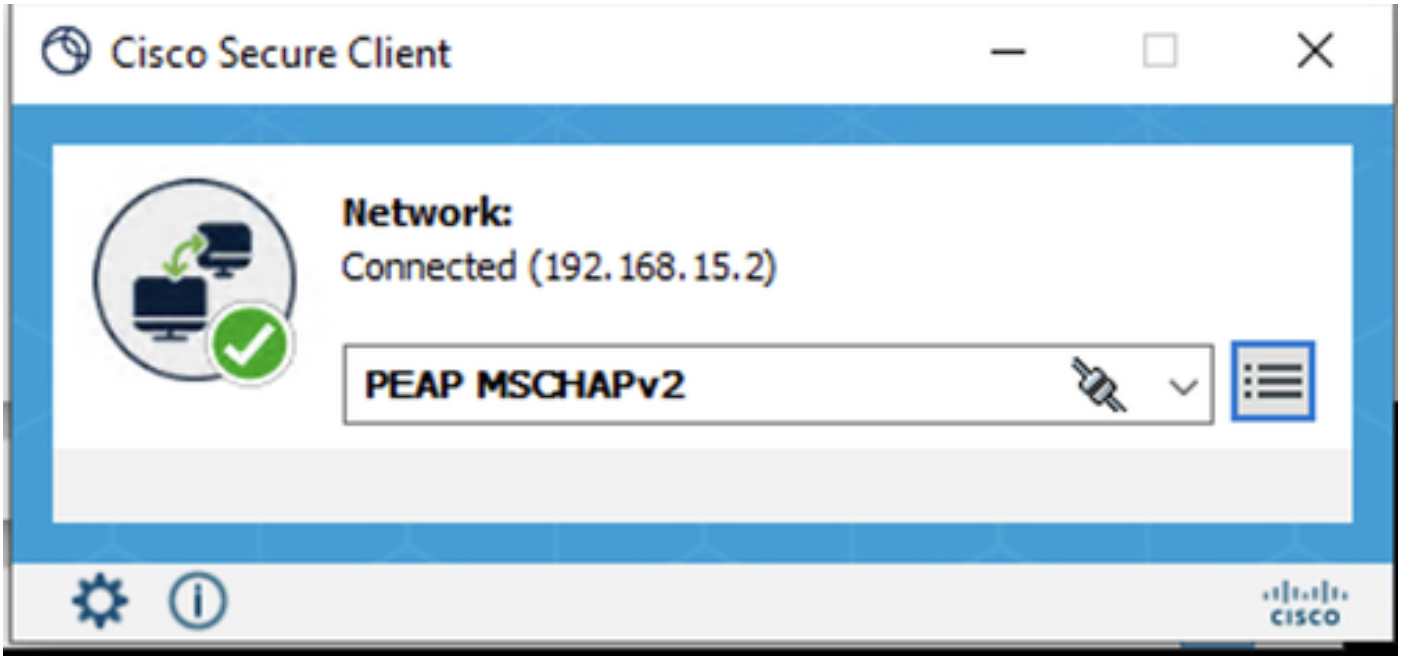
配置完成後，安全客戶端將提示輸入憑據，並指定PEAP MSCHAPv2配置檔案的用法。

輸入先前建立的憑據。



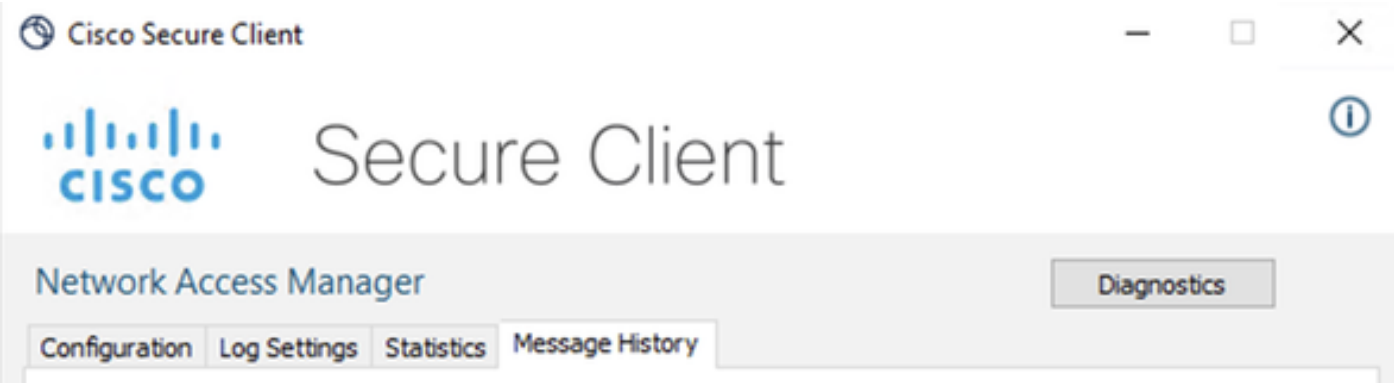
安全客戶端*NAM*

如果終端驗證正確，則NAM顯示其已連線。

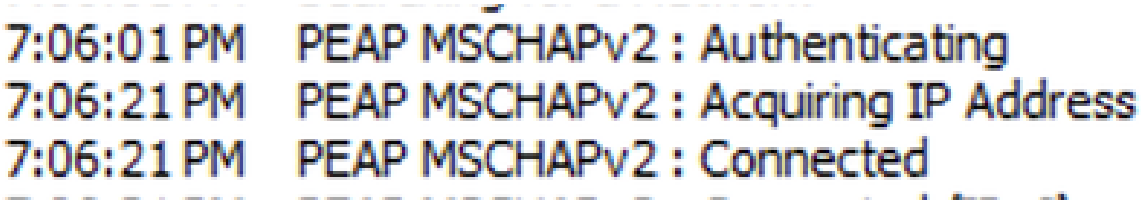


安全客戶端NAM

通過按一下資訊圖示並導航到消息歷史記錄部分，將顯示NAM執行的每個步驟的詳細資訊。



安全客戶端消息歷史記錄



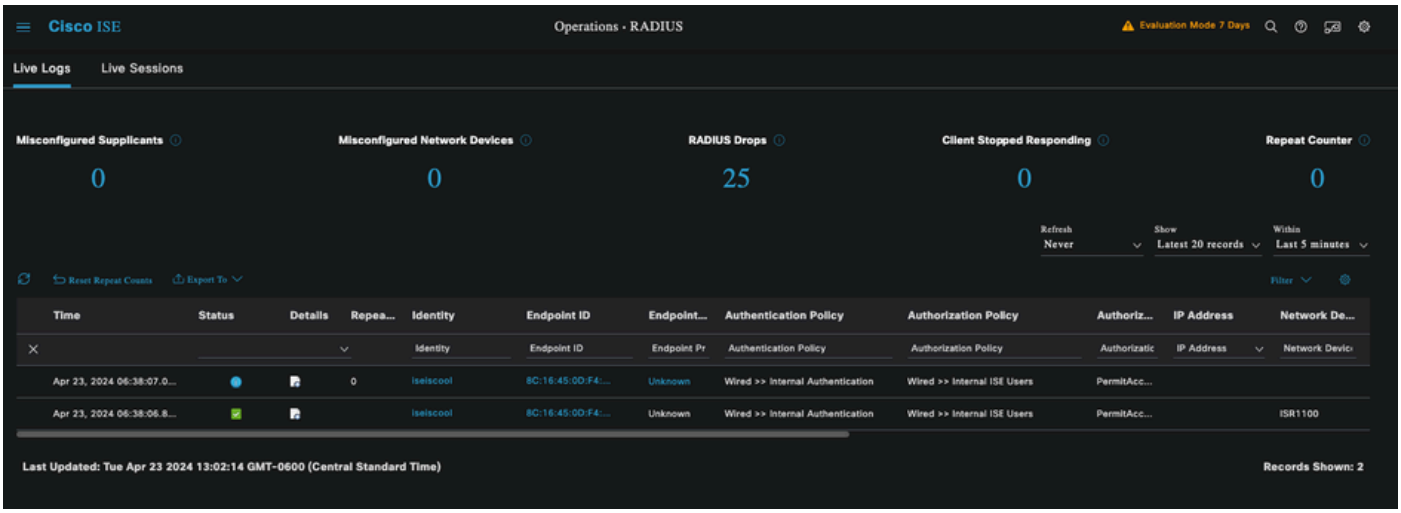
安全客戶端消息歷史記錄

從ISE導航到操作> Radius LiveLogs以檢視身份驗證的詳細資訊。如下圖所示，將顯示所使用的使用者名稱。

其他詳細資訊如：

- 時間戳。
- MAC 地址.
- 已使用策略集。
- 身份驗證策略。
- 授權策略。

- 其他有關資料。



ISE RADIUS即時日誌

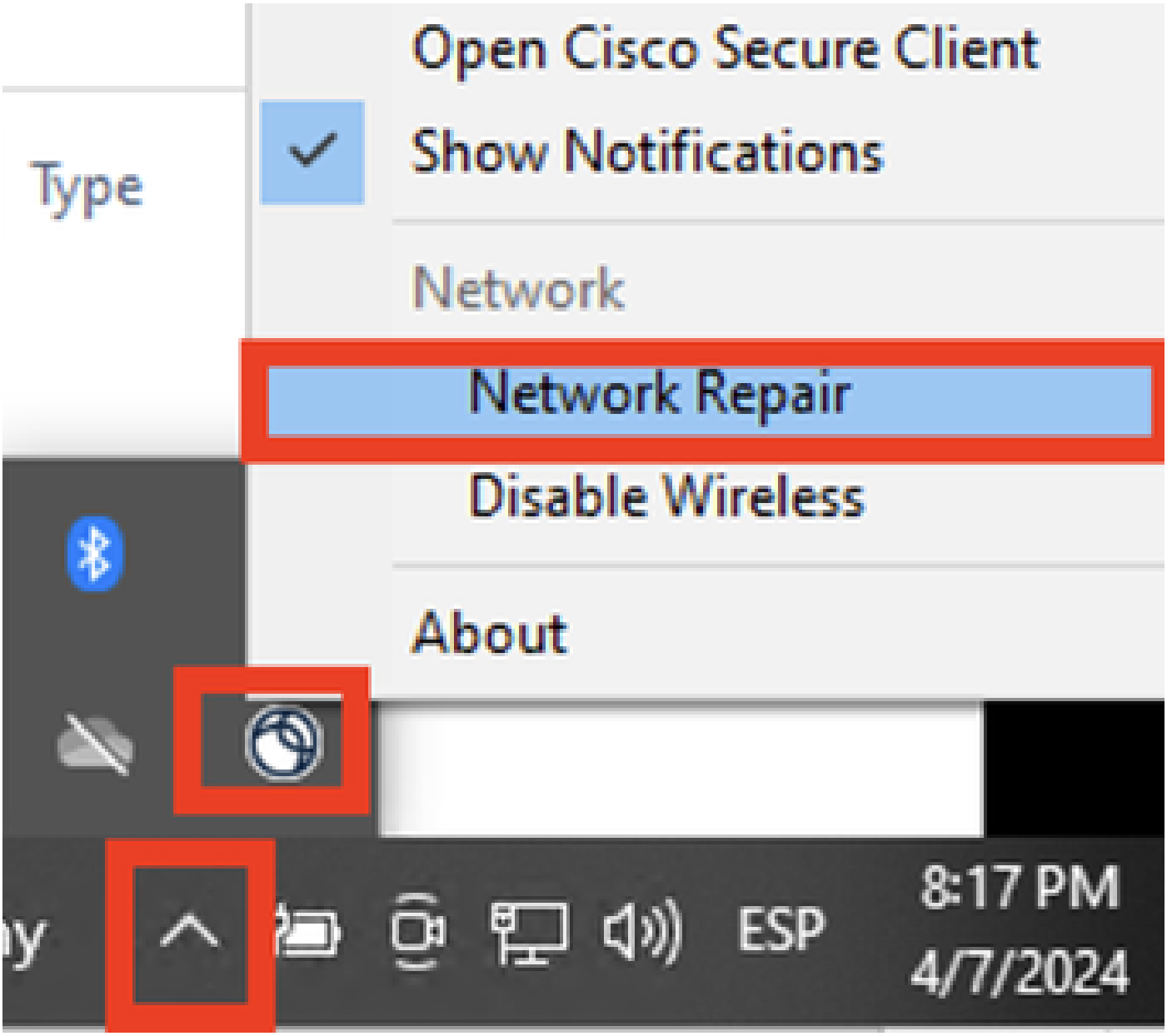
因為您可以看到它達到了正確的策略，並且結果是成功的身份驗證狀態，因此可以斷定配置是正確的。

疑難排解

問題:安全客戶端未使用NAM配置檔案。

如果配置檔案編輯器中建立的新配置檔案未被NAM使用，請對安全客戶端使用Network Repair選項。

通過導航到Windows欄>按一下揚抑符圖示>按一下右鍵安全客戶端圖示>按一下網路修復，可以找到此選項。



網路修復部分

問題2:需要收集日誌以進行進一步分析。

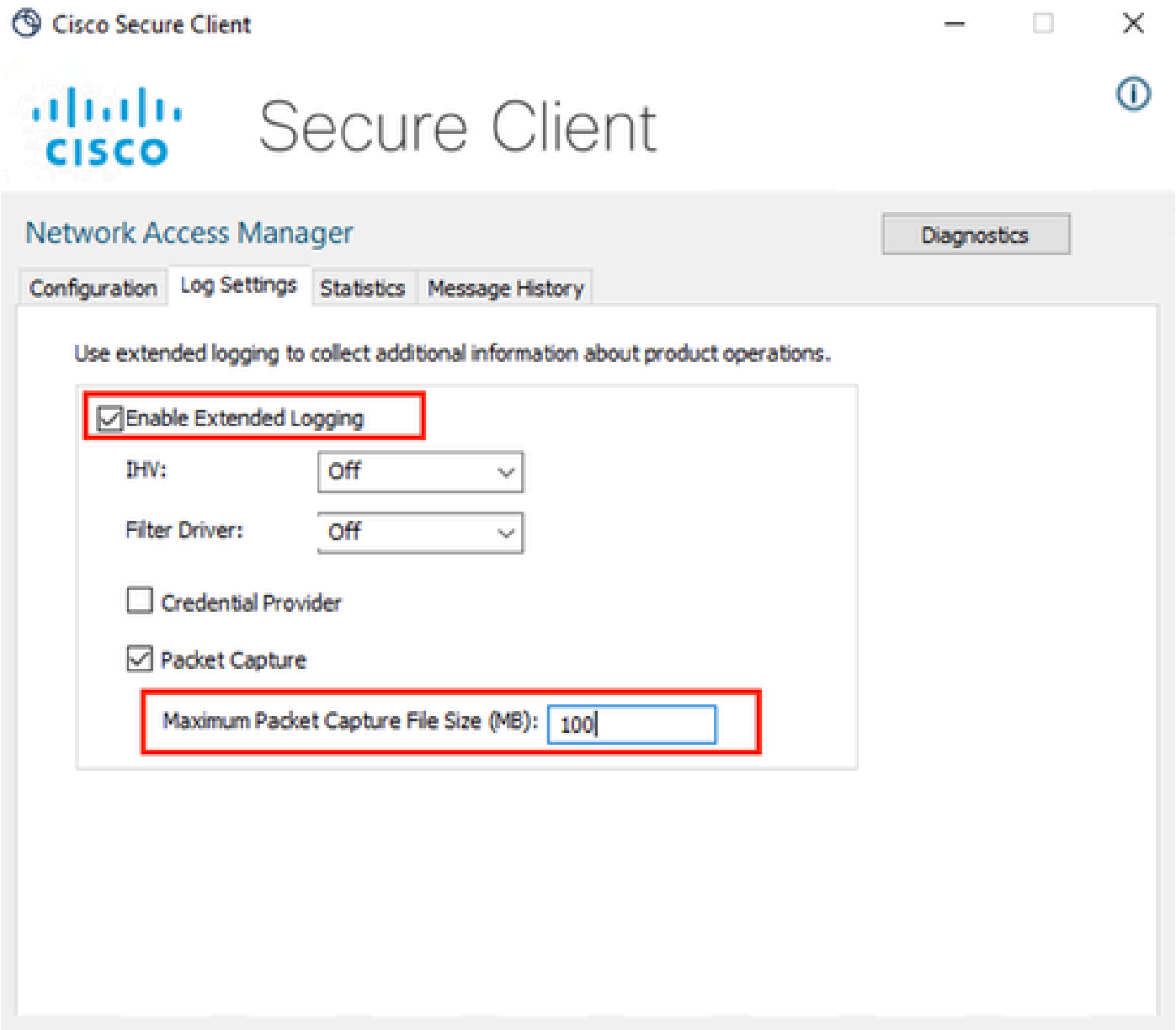
1.啟用NAM擴展日誌

開啟NAM，然後按一下齒輪圖示。

NAM介面

導航到日誌設定頁籤。選中Enable Extended Logging覈取方塊。

將Packet Capture File Size 設定為100 MB。



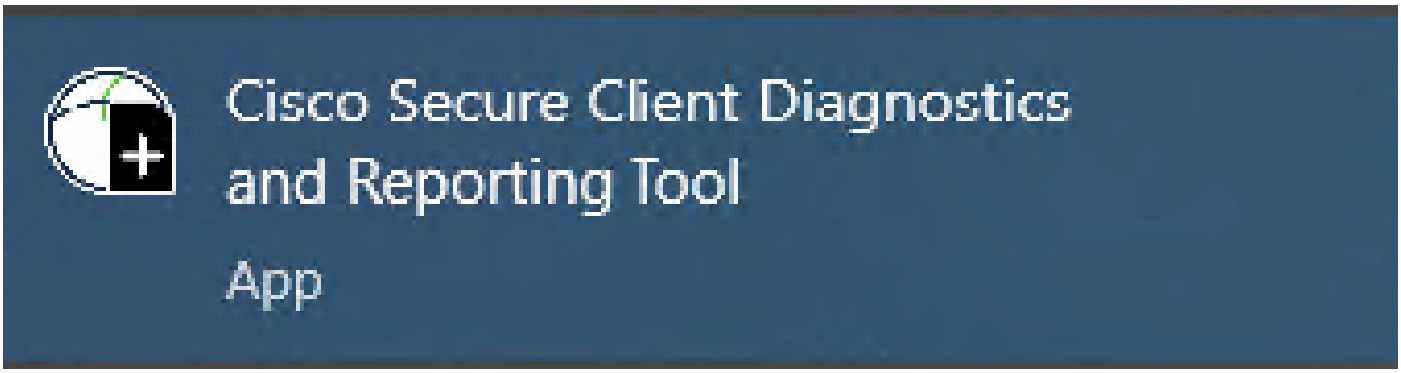
安全客戶端NAM日誌設定

2.重現問題。

啟用擴展日誌記錄後，會多次重現該問題，以確保生成日誌並捕獲流量。

3.收集安全客戶端DART捆綁包。

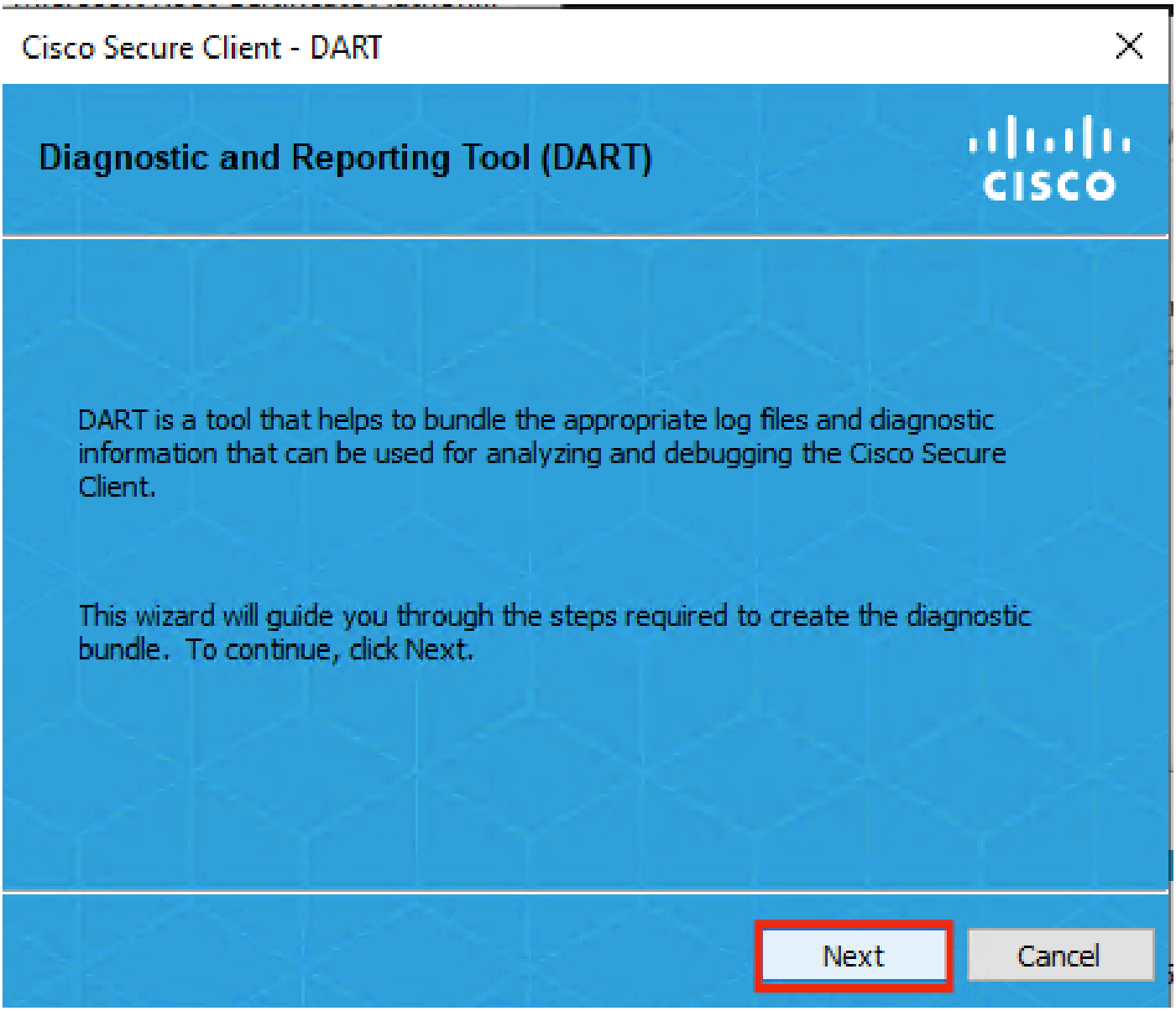
在Windows中，導航到搜尋欄並鍵入Cisco Secure Client Diagnostics and Reporting Tool。



DART模組

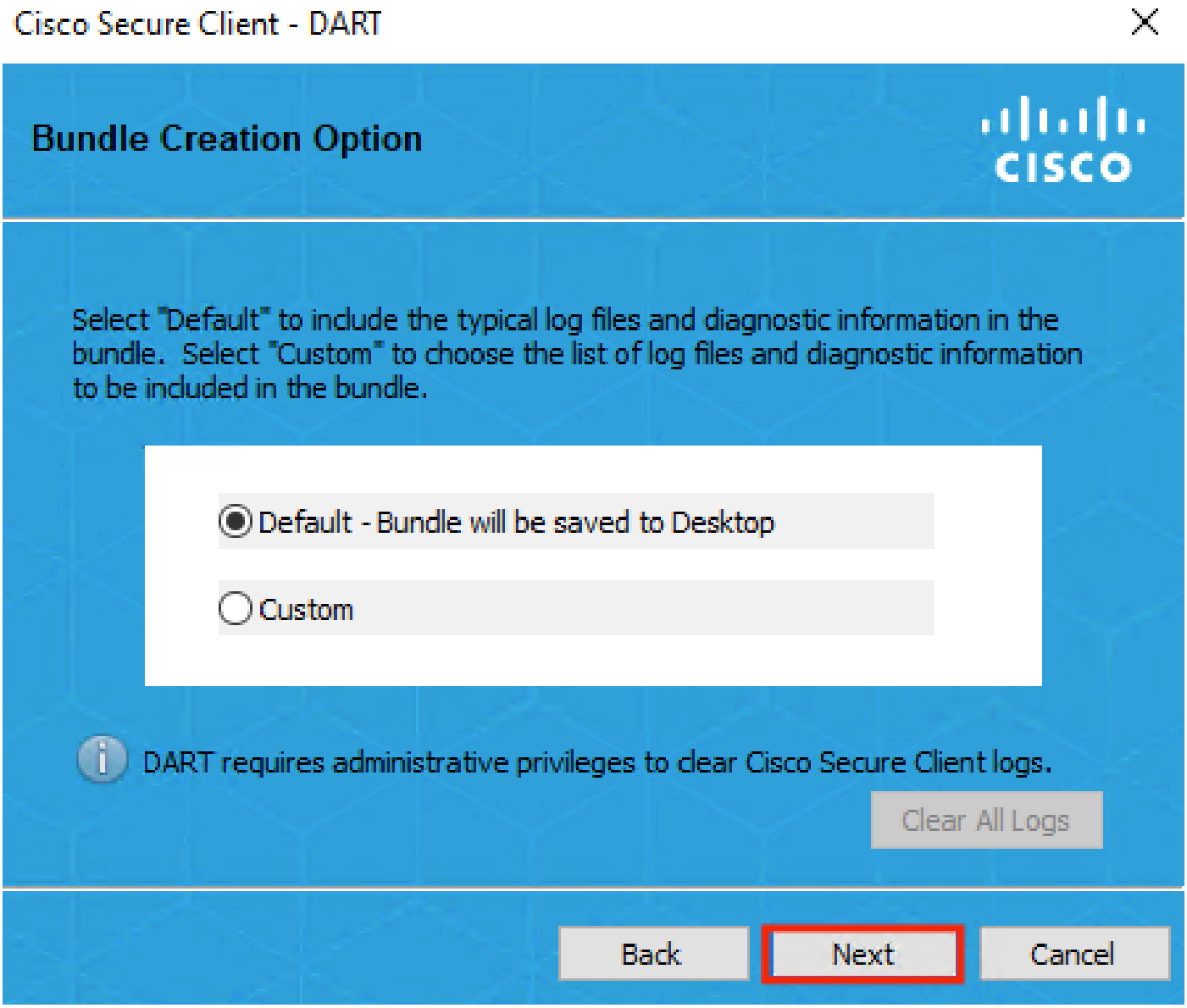
在安裝過程中，您還安裝了此模組。該工具通過收集日誌和相關dot1x會話資訊在故障排除過程中提供幫助。

在第一個視窗中按一下Next。



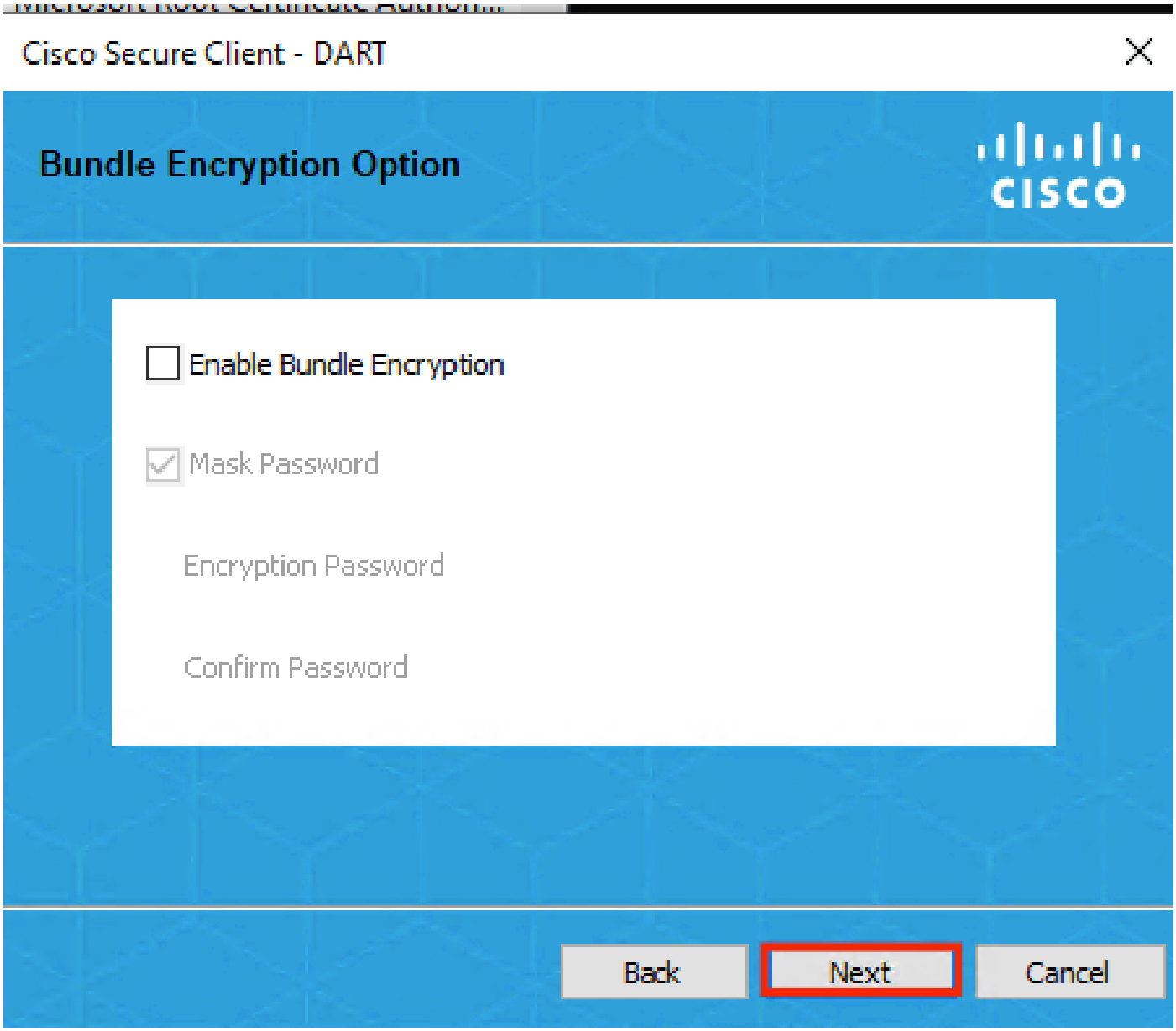
DART模組

再次按一下Next，這樣日誌捆綁包可以儲存在案頭上。



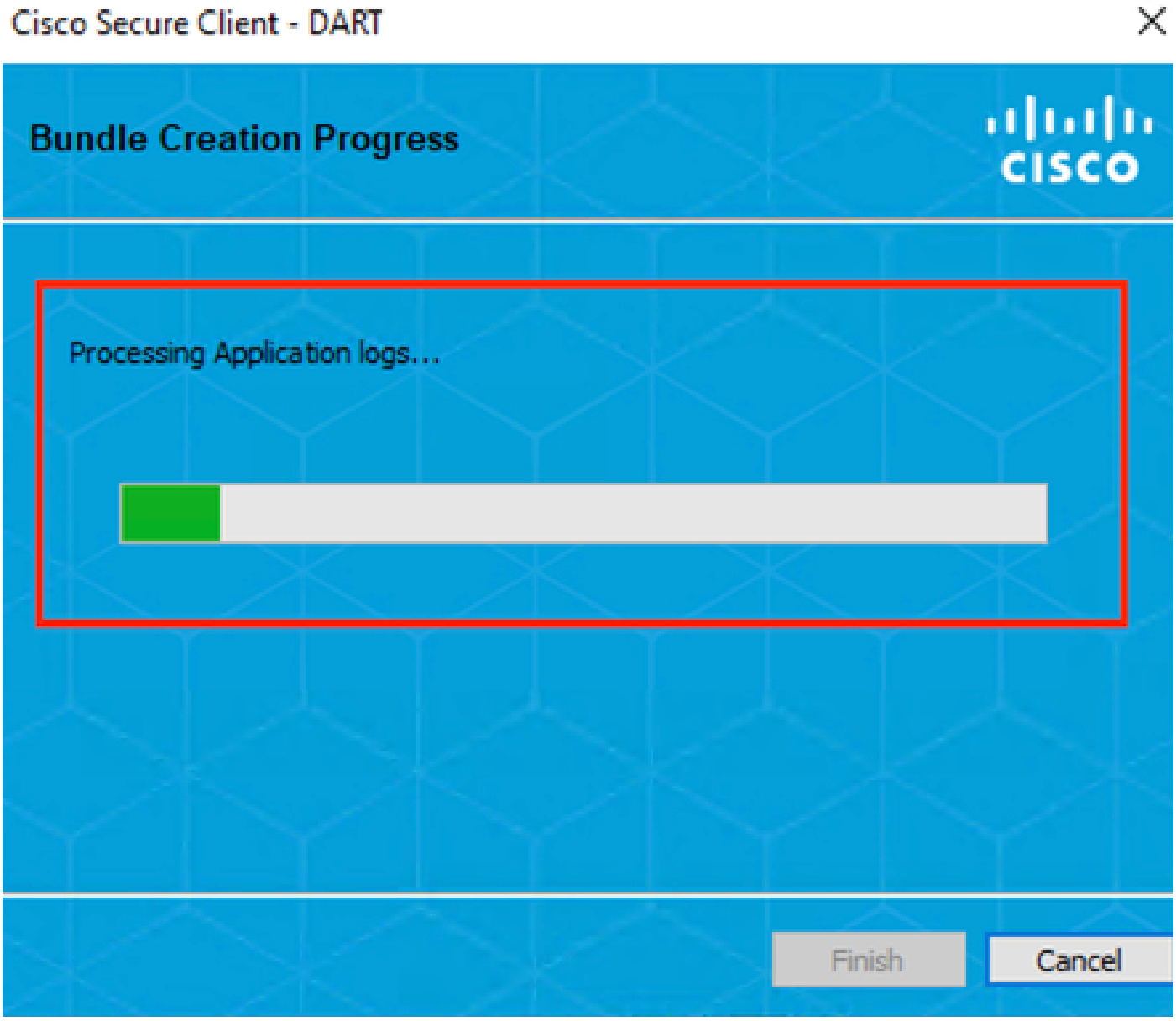
DART模組

如有必要，請勾選啟用捆綁包加密覈取方塊。



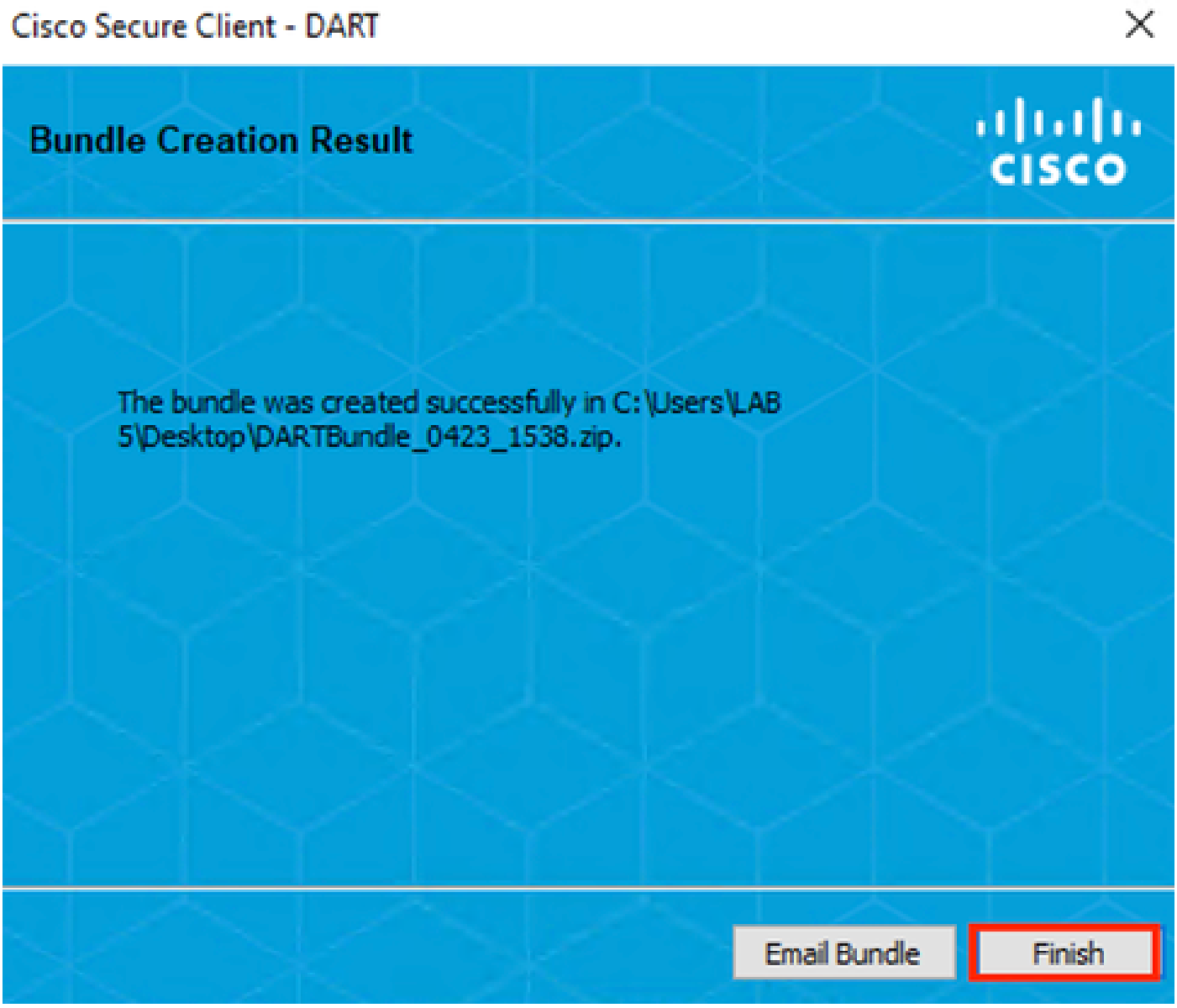
DART模組

DART日志收集啟動。



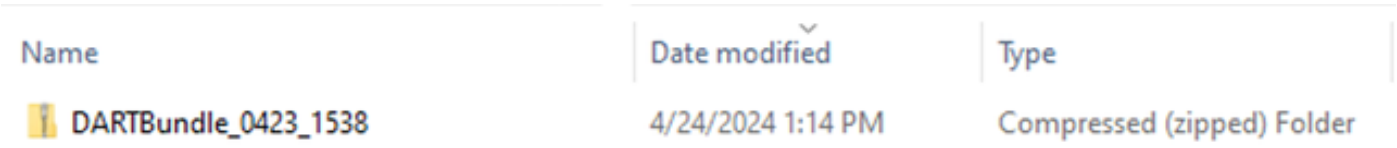
DART日誌集合

完成該過程可能需要10分鐘或更長時間。



DART捆綁包建立結果

DART結果檔案可以在案頭目錄中找到。



DART結果檔案

相關資訊

- 思科技術支援與下載

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）。