

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Secure Client 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. 一般預設組態](#)
- [4. 方案1：配置PEAP \(MS-CHAPv2\)使用者身份驗證的安全客戶端NAM請求方](#)
- [5. 方案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. 方案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. 根據方案1 PEAP MSCHAPv2配置ISR 1100和ISE以允許身份驗證](#)

[驗證](#)

[疑難排解](#)

[問題1：安全客戶端未使用NAM配置檔案。](#)

[問題2：需要收集日誌以供進一步分析。](#)

- [1. 啟用NAM擴展日誌記錄](#)
- [2. 重現問題。](#)
- [3. 收集安全客戶端DART捆綁包。](#)

[相關資訊](#)

簡介

本檔案介紹如何在Windows上設定Secure Client Network Analysis Module (NAM)。

必要條件

需求

思科建議您瞭解以下主題：

- 對RADIUS請求方的基本瞭解
- 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Secure Client 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，還提供了如何實現這一目標的一些示例。

在網路中，請求方是位於點對點LAN網段一端的實體，它尋求透過連線到該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」來表示硬體或軟體。實際上，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據以將電腦連線到安全網路。如果驗證成功，驗證者通常會允許電腦連線到網路。

關於網路存取管理員

Network Access Manager是客戶端軟體，根據策略提供安全的第2層網路。它檢測和選擇最佳的第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，防止終端使用者建立違反管理員定義策略的連線。

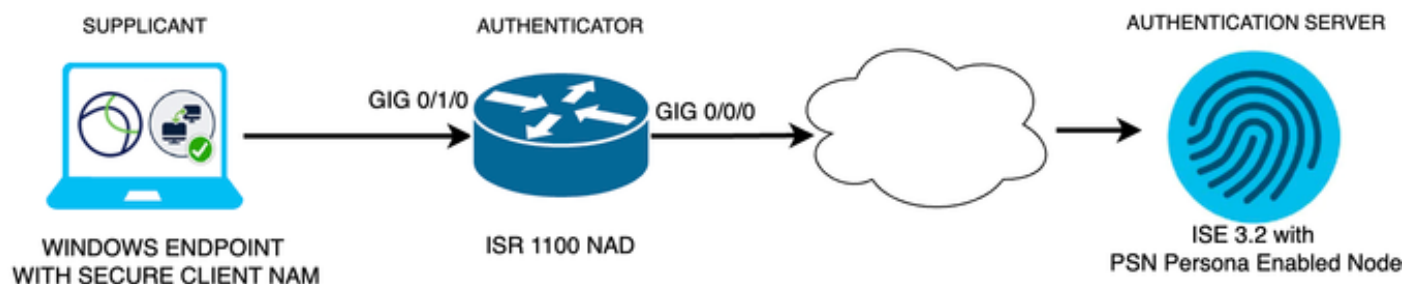
Network Access Manager設計為單宿主，一次只允許一個網路連線。此外，有線連線的優先順序高於無線，因此如果您使用有線連線插入網路，無線介面卡會停用，而且沒有IP位址。

設定

網路圖表

需要瞭解的是，對於dot1x身份驗證，需要3個部分；可以執行dot1x的請求方、用作封裝RADIUS內dot1x流量的代理的身份驗證器（也稱為NAS/NAD）以及身份驗證伺服器。

在本示例中，請求方的安裝和配置方式有所不同。稍後，會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Secure Client 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. 一般預設組態
4. 方案1：配置PEAP (MS-CHAPv2)使用者身份驗證的安全客戶端NAM請求方。
5. 方案2：在配置了使用者和電腦身份驗證的同時為EAP-FAST配置安全客戶端NAM請求方。
6. 方案3第1部分：為EAP-TLS配置安全客戶端NAM請求方。
7. 場景3第2部分：配置NAD和ISE演示。

1. 下載並安裝Secure Client NAM（網路訪問管理器）

[思科軟體下載](#)

在產品名稱搜尋欄中，鍵入Secure Client 5。

Downloads Home > Security > VPN and Endpoint Security Clients > Secure Client (including AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software。

在此組態範例中，使用的版本是5.1.2.42版。

有多種方法可將安全客戶端部署到Windows裝置；從SCCM、從身份服務引擎和VPN前端。但是，在本文中，使用的安裝方法是預部署方法。

在頁面上，搜尋檔案Cisco Secure Client Headend Deployment Package (Windows)。















Cisco Secure Client Pre-Deployment
Package (Windows) - includes individual MSI
files
cisco-secure-client-win-5.1.2.42-predeploy-k9.zip
Advisories

06-Feb-2024 108.30 MB



Msi zip檔案

下載並解壓後，按一下Setup。

 Profiles	4/4/2024 7:16 PM
 Setup	4/4/2024 7:16 PM
 cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-dart-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-nam-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-posture-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9	4/4/2024 7:16 PM
 Setup	4/4/2024 7:16 PM
 setup	4/4/2024 7:16 PM

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嚮導，VPN模組將自動安裝並在GUI中隱藏。如果未安裝VPN模組，則NAM不起作用。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。

Select the Cisco Secure Client 5.1.2.42 modules you wish to install:

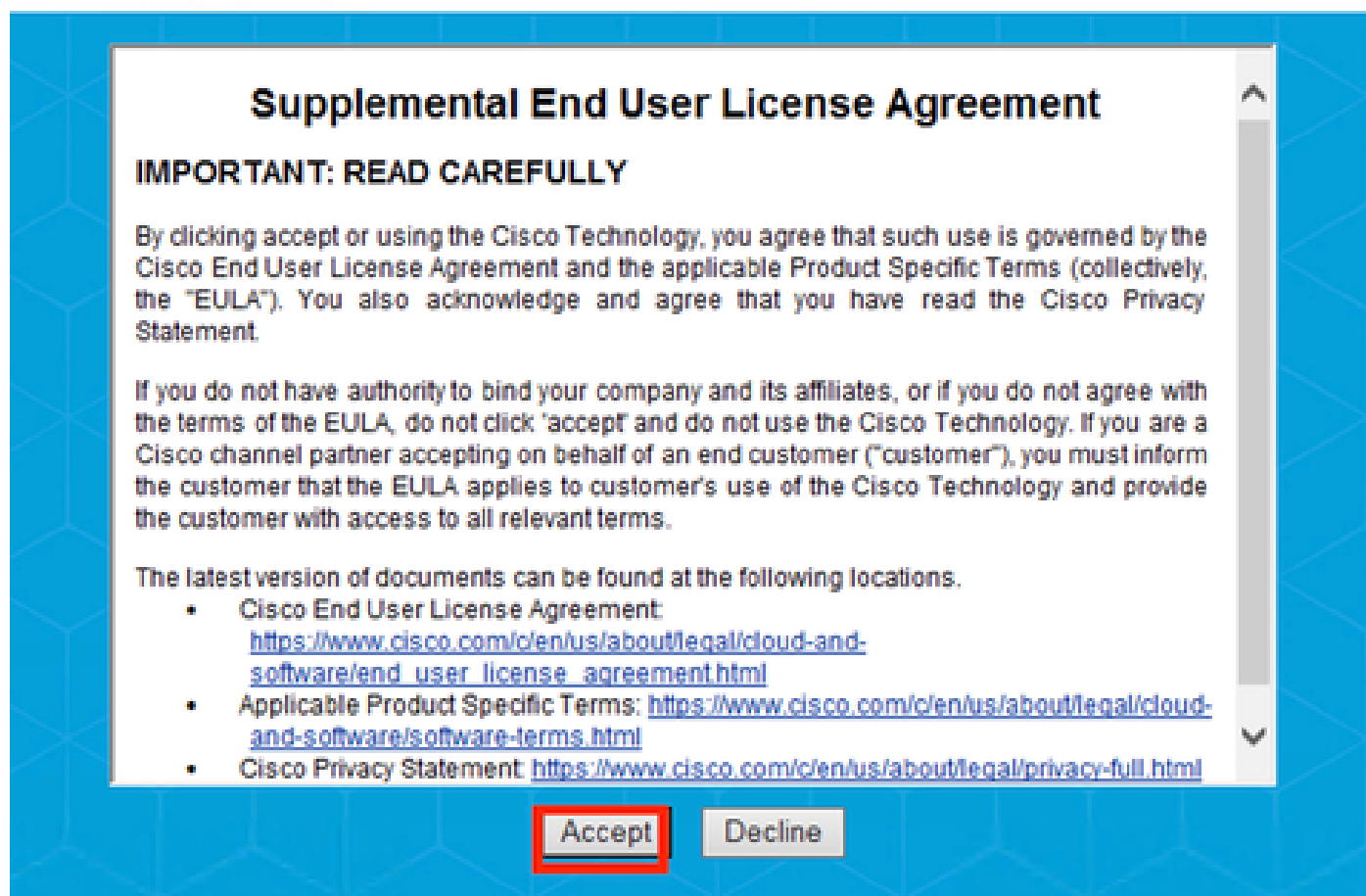
- ☐ Core & AnyConnect VPN
- ☐ Start Before Login
- ☒ Network Access Manager
- ☐ Secure Firewall Posture
- ☐ Network Visibility Module
- ☐ Umbrella
- ☐ ISE Posture
- ☐ ThousandEyes
- ☐ Zero Trust Access
- ☐ Select All
- ☒ Diagnostic And Reporting Tool
- ☐ Lock Down Component Services

Install Selected

安裝選取器

按一下「安裝所選內容」。

接受EULA。



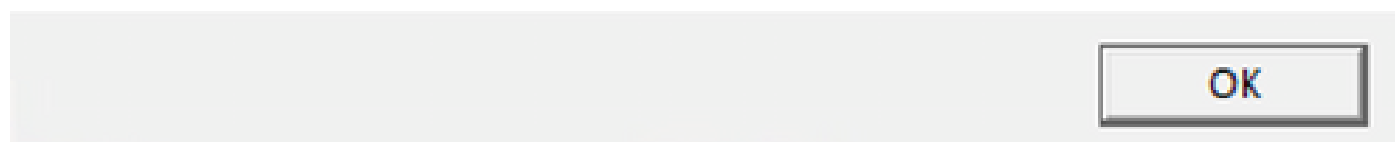
EULA視窗

安裝NAM後需要重新啟動。

Cisco Secure Client Install Selector

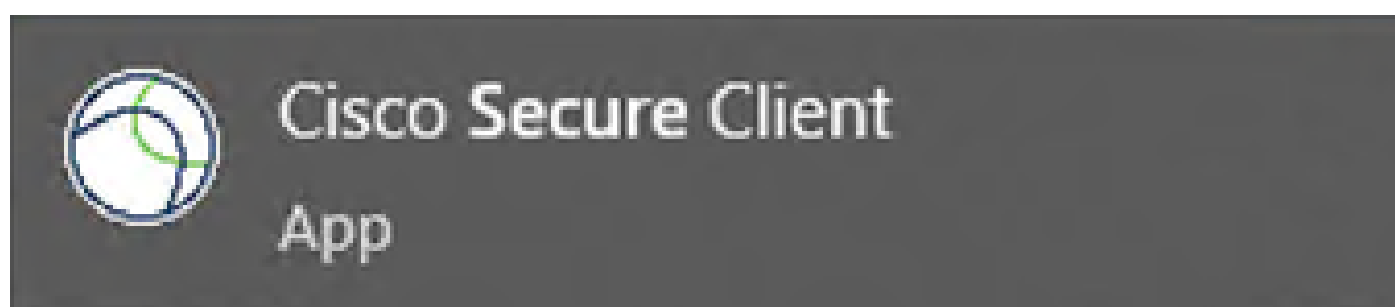


You must reboot your system for the installed changes to take effect.



重新開機需求視窗

安裝後，可從Windows搜尋欄找到並打開它。

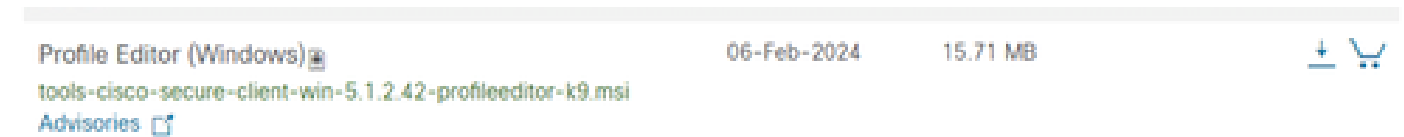


2. 下載並安裝安全客戶端NAM配置檔案編輯器。

需要思科網路訪問管理器配置檔案編輯器來配置Dot1x首選項。

在Secure Client下載所在的頁面上，可找到Profile Editor選項。

本示例使用版本5.1.2.42中的選項。



設定檔編輯器

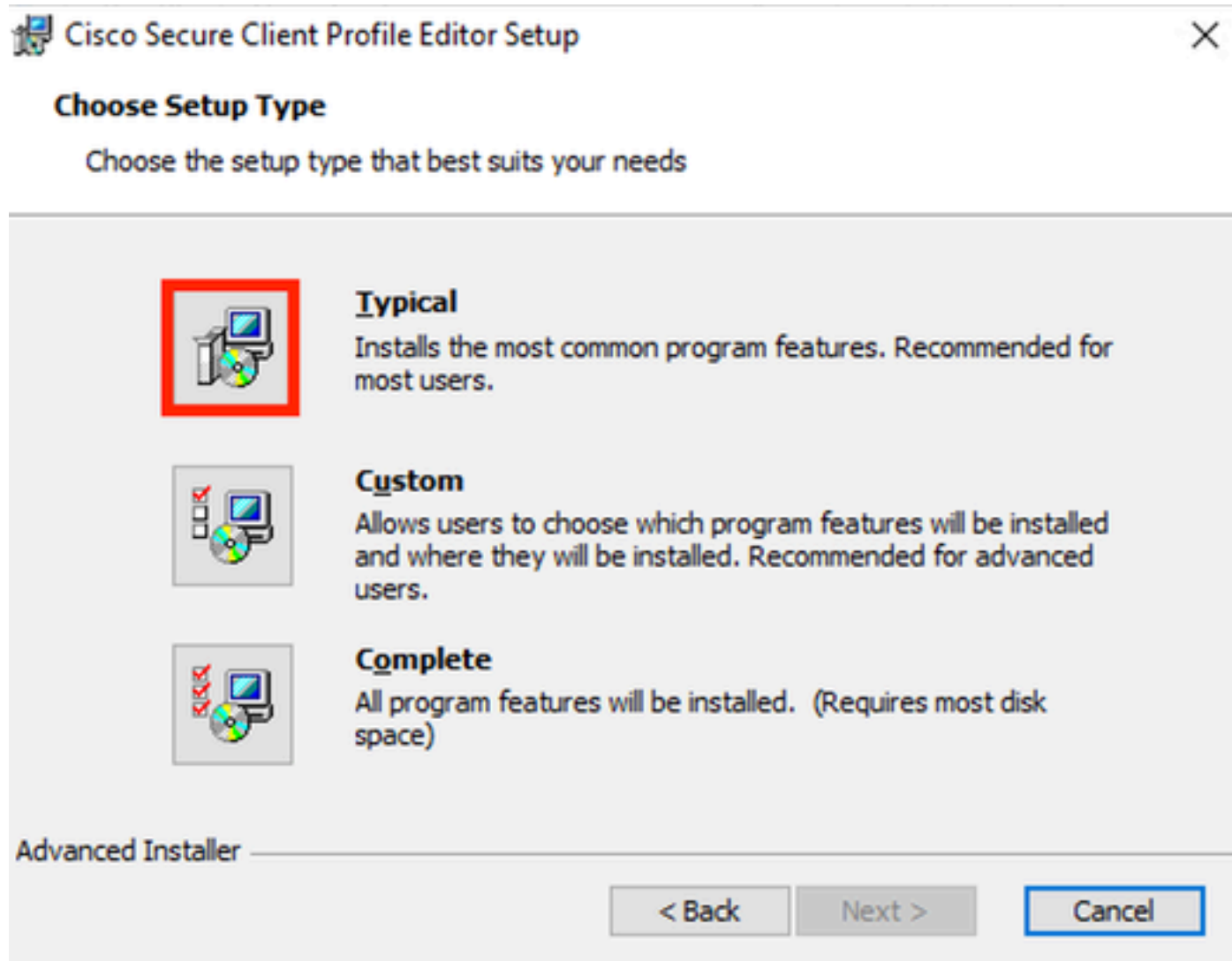
下載後，繼續進行安裝。

運行msi檔案。

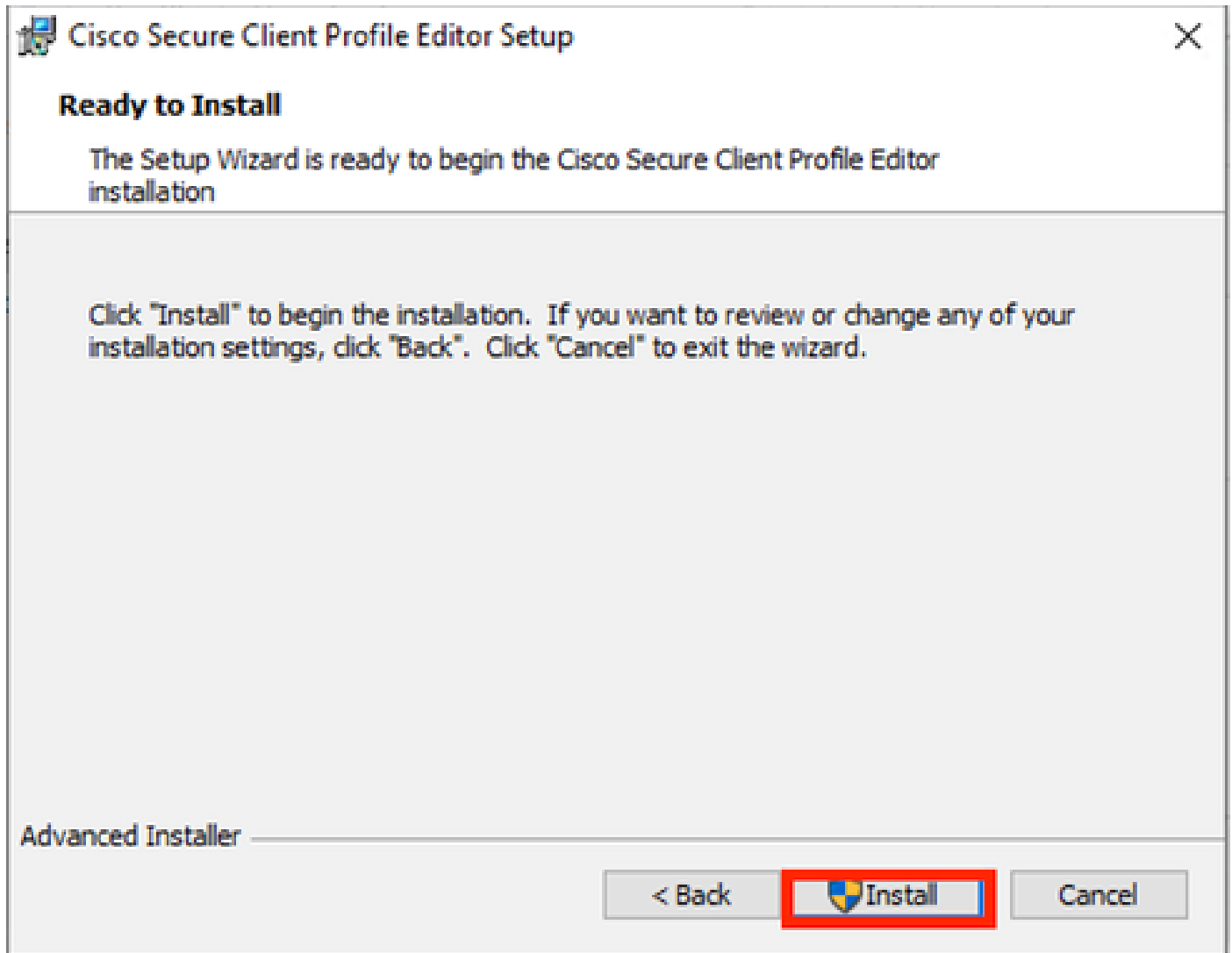


設定檔編輯器設定視窗

使用典型設定選項。

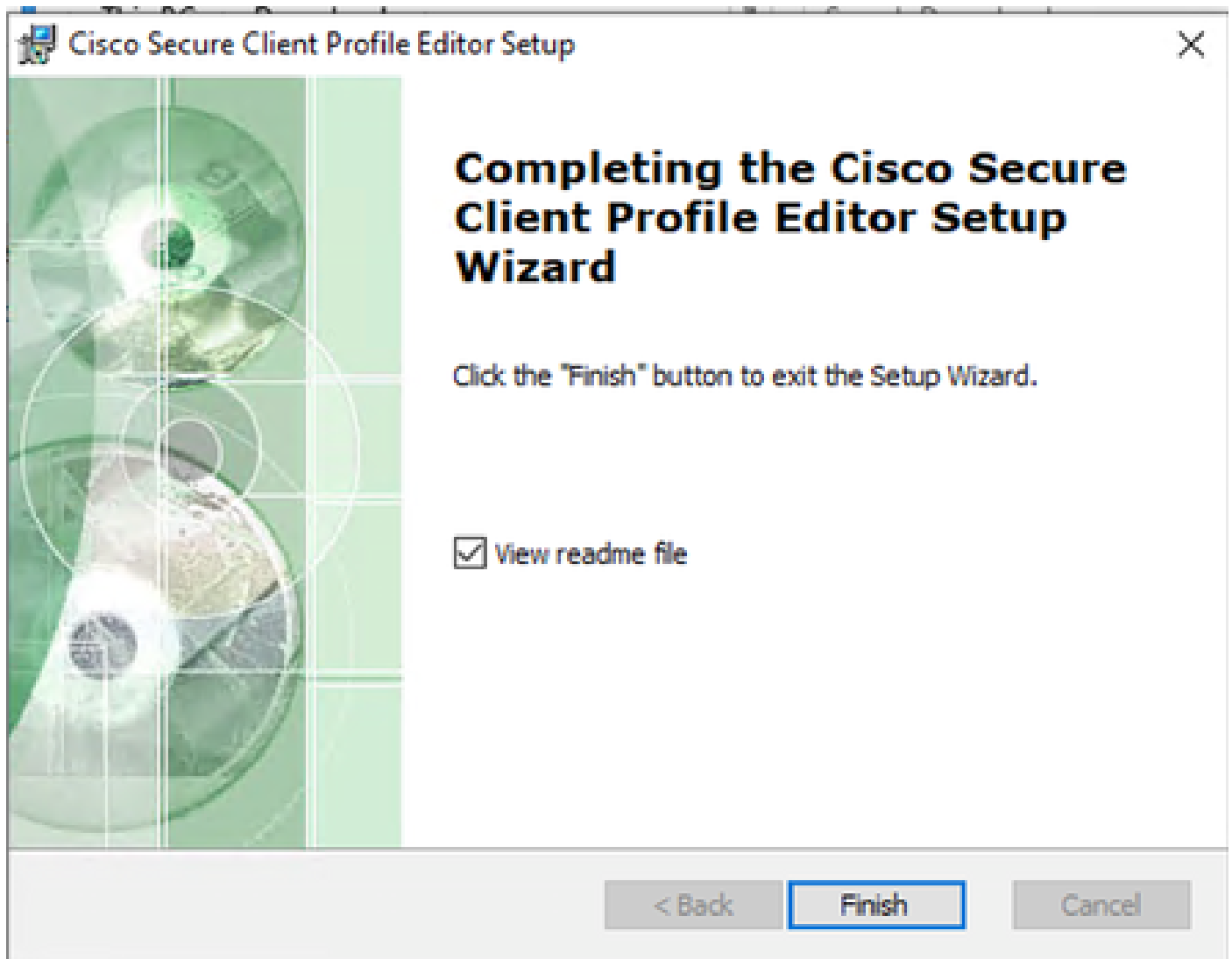


設定檔編輯器設定



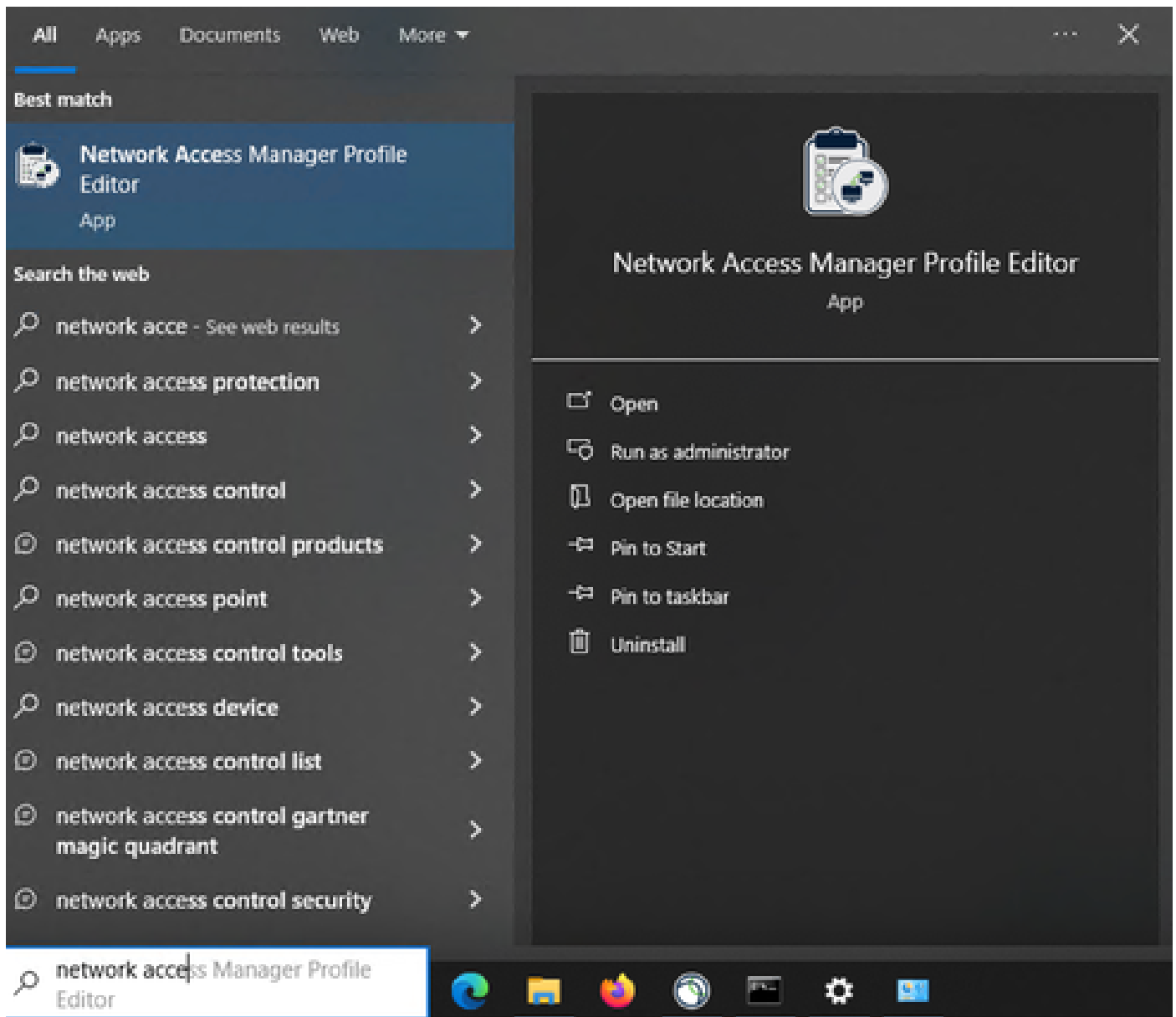
安裝視窗

按一下「Finish」（結束）。



設定檔編輯器安裝結束

安裝後，從搜尋欄打開網路訪問管理器配置檔案編輯器。



搜尋列上的NAM設定檔編輯器

網路存取管理員和設定檔編輯器的安裝完成。

3. 一般預設組態

本文中介紹的所有場景都包含以下配置：

- 客戶端策略
- 身份驗證策略
- 網路組

Network Access Manager

- Client Policy
- Authentication Policy
- Networks
- Network Groups

Client Policy

Profile: Untitled

Connection Settings

Default Connection Timeout (sec.)

Connection Attempt:

☐ Before user logon

Time to wait before allowing user to logon (sec.)

☒ After user logon

Media

☒ Manage Wi-Fi (wireless) Media

☒ Enable validation of WPA/WPA2/WPA3 handshake

☐ Enable Randomized MAC Address

Default Association Timeout (sec.)

☒ Manage Wired (802.3) Media

☐ Manage Mobile Broadband (3G) Media

☒ Enable Data Roaming

End-user Control

Allow end-user to:

☒ Disable Client

☒ Display user groups

☐ Specify a script or application to run when connected

☒ Auto-connect

☒ Select machine connection type

☒ Enable by default

Administrative Status

Service Operation: ☒ Enable ☐ Disable

FIPS Mode: ☐ Enable ☒ Disable

Captive Portal Detection: ☐ Enable ☒ Disable

File Help

Network Access Manager

- Client Policy
- Authentication Policy**
- Networks
- Network Groups

Authentication Policy

Profile: Untitled

Allow Association Modes

- ☒ Select All (Personal)
 - ☒ Open (no encryption)
 - ☒ Open (Static WEP)
 - ☒ Shared (WEP)
 - ☒ WPA Personal TKIP
 - ☒ WPA Personal AES
 - ☒ WPA2 Personal TKIP
 - ☒ WPA2 Personal AES
 - ☒ WPA3 Open (OWE)
 - ☒ WPA3 Personal AES (SAE)
- ☒ Select All (Enterprise)
 - ☒ Open (Dynamic (802.1X) WEP)
 - ☒ WPA Enterprise TKIP
 - ☒ WPA Enterprise AES
 - ☒ WPA2 Enterprise TKIP
 - ☒ WPA2 Enterprise AES
 - ☒ COCK Enterprise TKIP
 - ☒ COCK Enterprise AES
 - ☒ WPA3 Enterprise AES

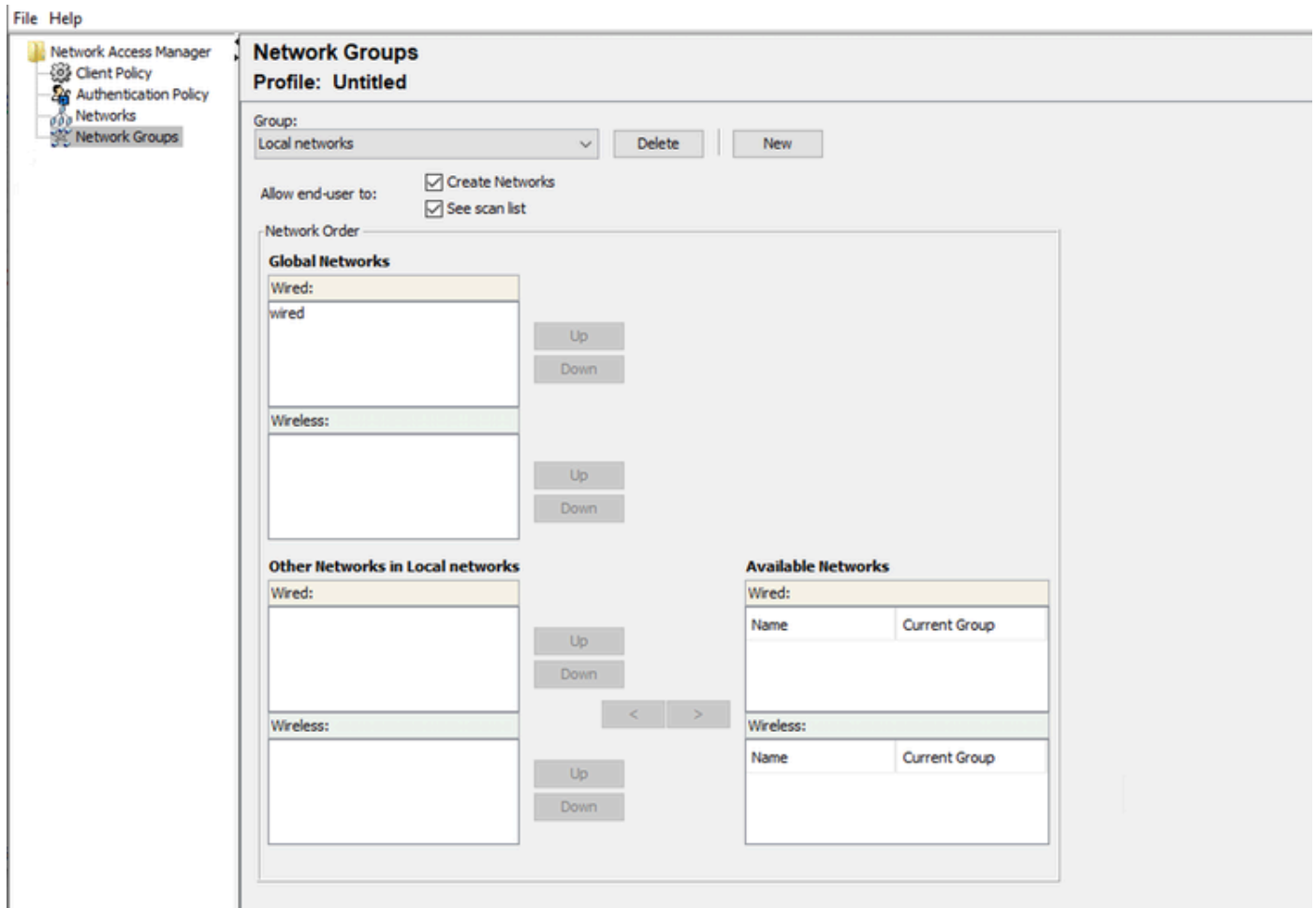
Allowed Authentication Modes

- ☒ Select All Outer
 - ☒ EAP-FAST
 - ☒ EAP-GTC
 - ☒ EAP-MSCHAPv2
 - ☒ EAP-TLS
 - ☒ EAP-TLS
 - ☒ EAP-TTLS
 - ☐ EAP-MD5
 - ☒ EAP-MSCHAPv2
 - ☒ PAP (legacy)
 - ☐ CHAP (legacy)
 - ☐ MSCHAP (legacy)
 - ☐ MSCHAPv2 (legacy)
 - ☒ LEAP
 - ☒ PEAP
 - ☒ EAP-GTC
 - ☒ EAP-MSCHAPv2
 - ☒ EAP-TLS

Allowed Wired Security

- ☒ Select All
 - ☒ Open (no encryption)
 - ☒ 802.1x only
 - ☒ 802.1x with MacSec
 - ☒ AES-GCM-128
 - ☒ AES-GCM-256

NAM配置檔案編輯器身份驗證策略



網路群組標籤

4. 方案1：配置PEAP (MS-CHAPv2)使用者身份驗證的安全客戶端NAM請求方

導航到網路部分。

可以刪除預設的網路配置檔案。

按一下Add。

Networks

Profile: Untitled

Network

Name	Media Type	Group*

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

網路設定檔建立

為網路配置檔案命名。

為Group Membership選擇Global。選擇有線網路介質。

Networks

Profile: Untitled

Name:	PEAP MSCHAPv2	Media Type
Group Membership		Security Level
<input type="radio"/> In group:	Local networks	
<input checked="" type="radio"/> In all groups (Global)		
Choose Your Network Media		
<input checked="" type="radio"/> Wired (802.3) Network		
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.		
<input type="radio"/> Wi-Fi (wireless) Network		
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.		
SSID (max 32 chars):		
<input type="checkbox"/> Hidden Network		
<input type="checkbox"/> Corporate Network		
Association Timeout	5	seconds
Common Settings		
Script or application on each user's machine to run when connected.		
		Browse Local Machine
Connection Timeout	40	seconds

Next Cancel

網路設定檔媒體型態段落

按「Next」(下一步)。

選擇Authenticating Network，並使用Security Level部分中其餘選項的預設值。

Networks
Profile: Untitled

Security Level

☐ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

☒ **Authenticating Network**
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

Media Type
Security Level
Connection Type

802.1X Settings

authPeriod (sec.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

Security

Key Management
None

Encryption

☐ AES GCM 128
☐ AES GCM 256

Port Authentication Exception Policy

☐ Enable port exceptions

☐ Allow data traffic before authentication

☒ Allow data traffic after authentication even if

☐ EAP fails
☐ EAP succeeds but key management fails

Next Cancel

網路設定檔安全等級

點選下一步以繼續進行連線型別部分。

Networks
Profile: Untitled

Network Connection Type

☐ Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

☒ **User Connection**

The user connection should be used when a machine connection is not needed.
A user connection will make the network available after the user has logged on.

☐ Machine and User Connection

This type of connection will be made automatically when the machine boots.
It will then be brought down, and back up again with different credentials when the user logs in.

Media Type
Security Level
Connection Type
User Auth
Credentials

Next Cancel

網路配置檔案連線型別

選擇User Connection連線型別。

點選下一步，繼續顯示當前可用的使用者身份驗證部分。

選擇PEAP作為常規EAP方法。

Networks
Profile: Untitled

EAP Methods

- ☐ EAP-MD5
- ☐ EAP-MSCHAPv2
- ☐ EAP-GTC
- ☐ EAP-TLS
- ☐ EAP-TTLS
- ☒ PEAP
- ☐ EAP-FAST

☐ Extend user connection beyond log off

EAP-PEAP Settings

- ☒ Validate Server Identity
- ☒ Enable Fast Reconnect
- ☐ Disable when using a Smart Card

Inner Methods based on Credentials Source

- ☒ Authenticate using a Password
 - ☒ EAP-MSCHAPv2
 - ☐ EAP-GTC
- ☐ EAP-TLS, using a Certificate
- ☐ Authenticate using a Token and EAP-GTC

Media Type
Security Level
Connection Type: **User Auth**
Certificates
Credentials

Next Cancel

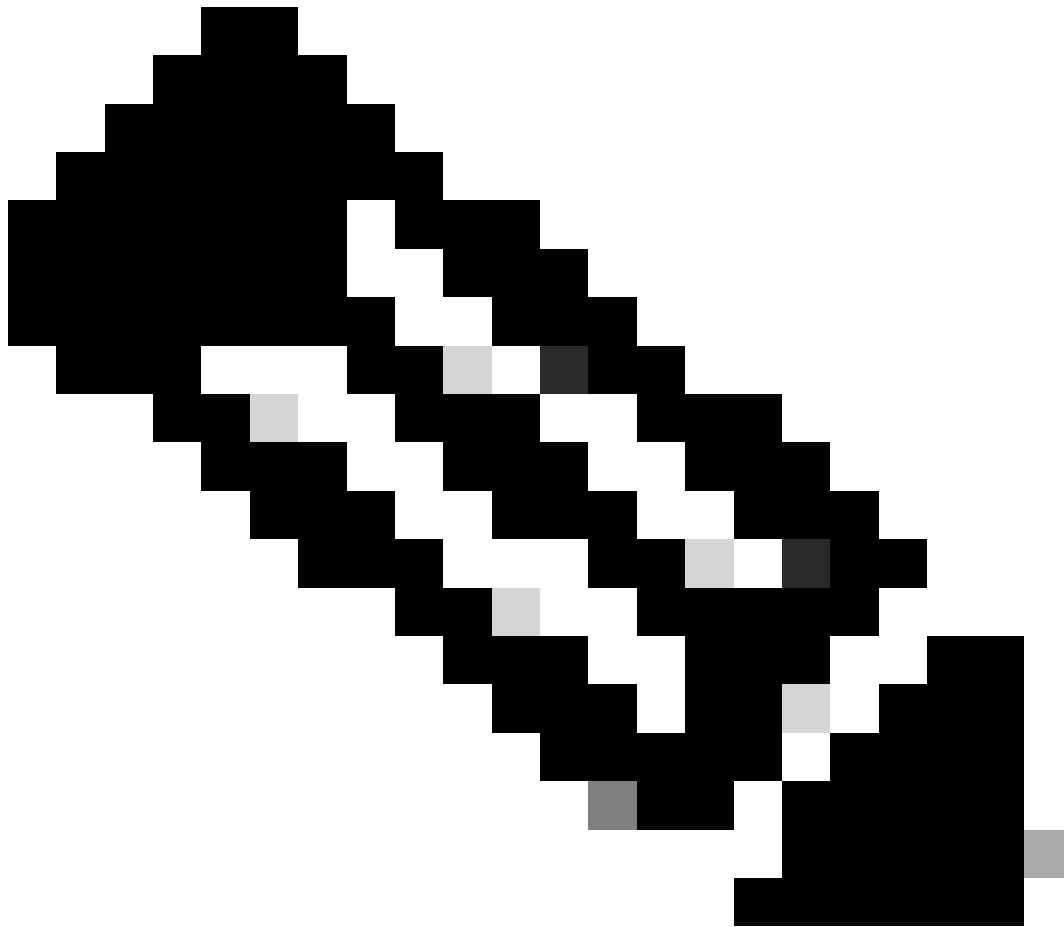
網路配置檔案使用者身份驗證

請勿更改EAP-PEAP Settings中的預設值。

繼續執行基於憑據源的內部方法部分。

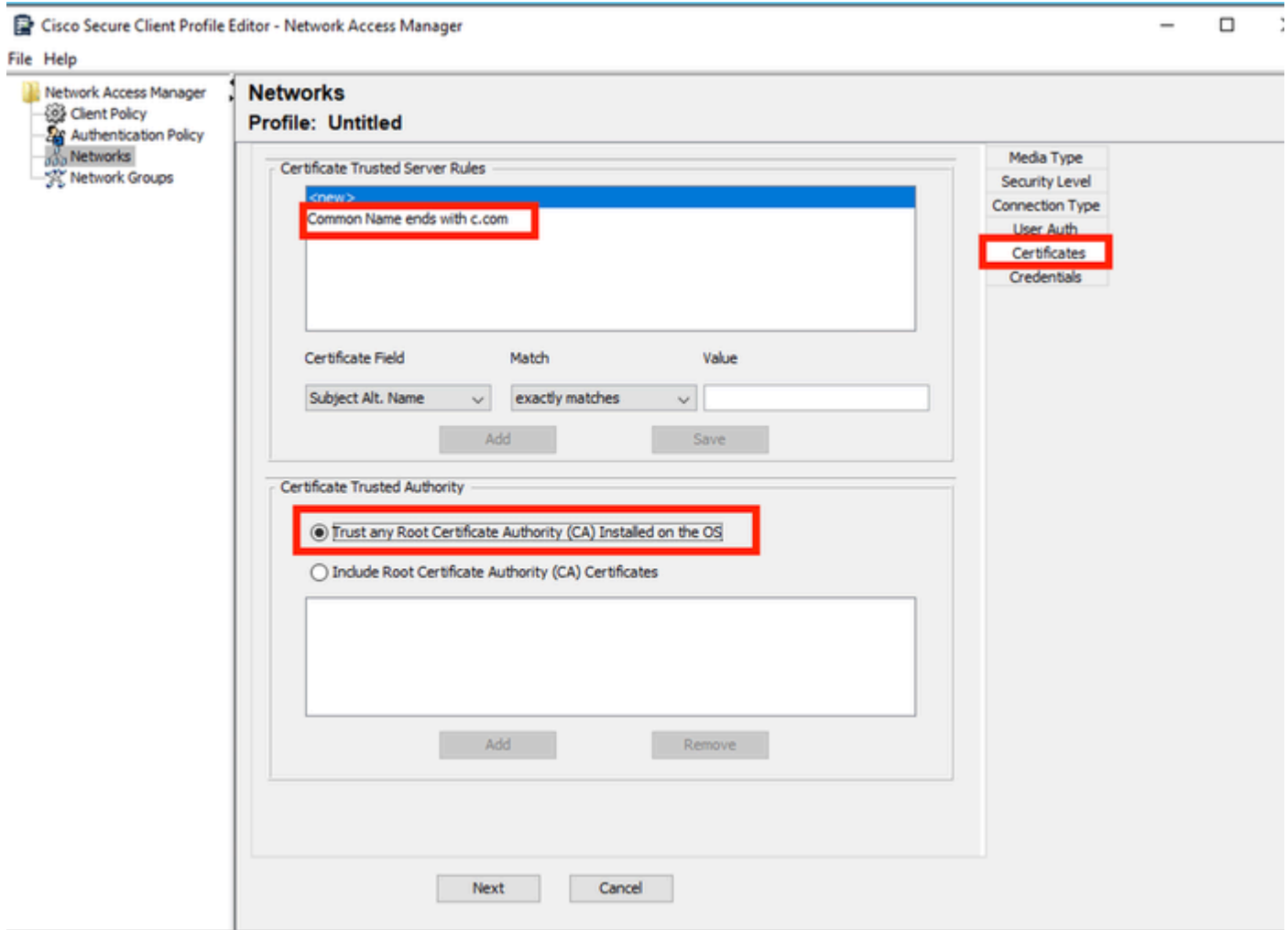
從EAP PEAP存在的多個內部方法中，選擇Authenticate using a Password，然後選擇EAP-MSCHAPv2。

按一下下一步以繼續轉至證書部分。



注意：顯示證書部分，因為選中了在EAP-PEAP設定中驗證伺服器身份選項。對於EAP PEAP，它使用伺服器證書執行封裝。

在證書部分中，在證書受信任的伺服器規則中使用規則公用名以c.com結尾。此組態的區段是指伺服器在EAP PEAP流程期間使用的憑證。如果在您的環境中使用了身份服務引擎(ISE)，則可以使用策略伺服器節點EAP證書的公用名稱。

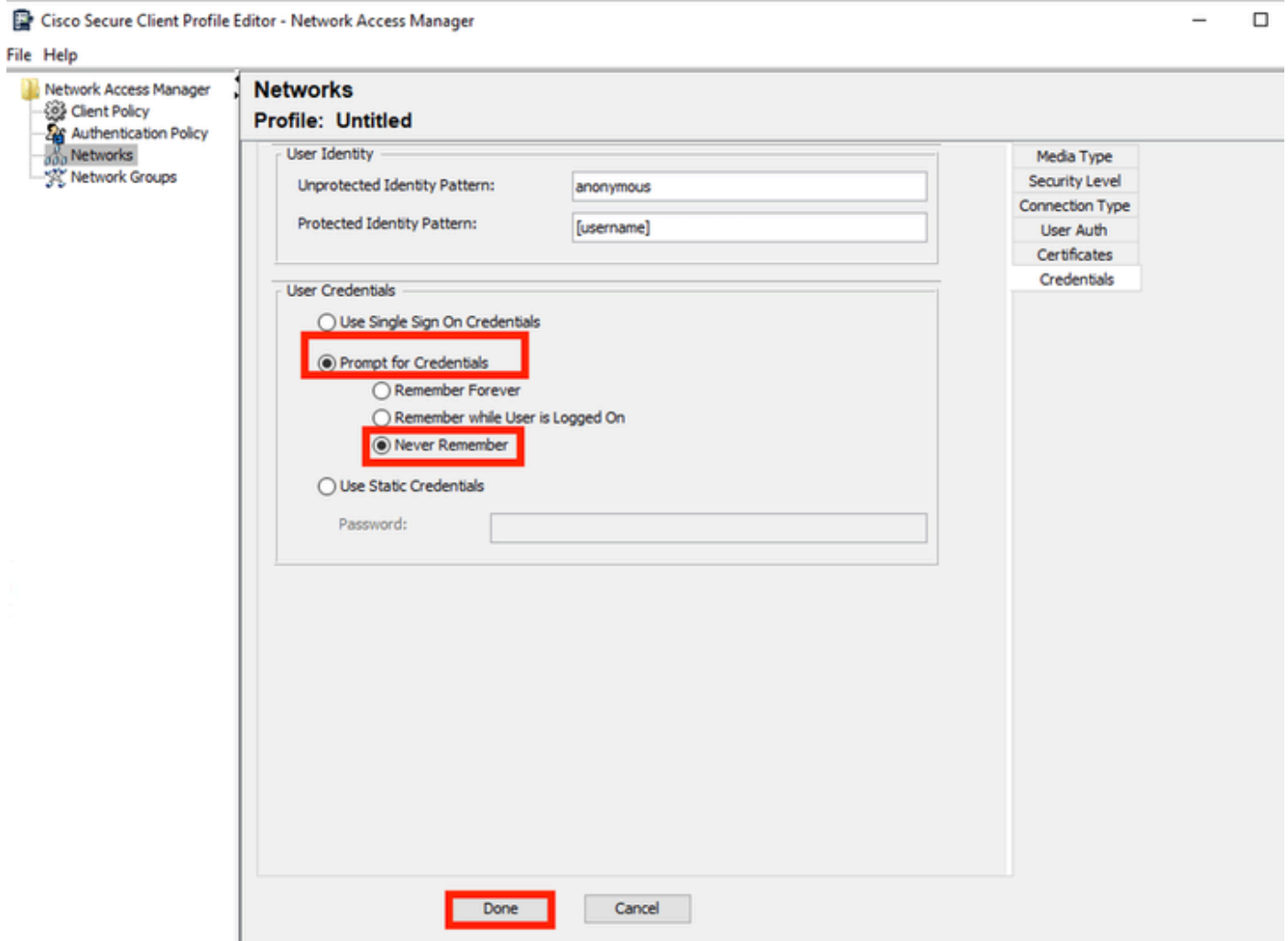


網路設定檔憑證段落

可以在證書受信任機構中選擇兩個選項。對於此情況，使用選項Trust any Root Certificate Authority (CA) Installed on the OS而不增加簽署RADIUS EAP證書的特定CA證書。

使用此選項，Windows裝置將信任由「Manage User Certs」程式證書— Current User > Trusted Root Certification Authorities > Certificates中包含的證書簽名的任何EAP證書。

按「Next」（下一步）。



網路設定檔證明資料段落

在憑據部分中，只有使用者憑據部分被更改。

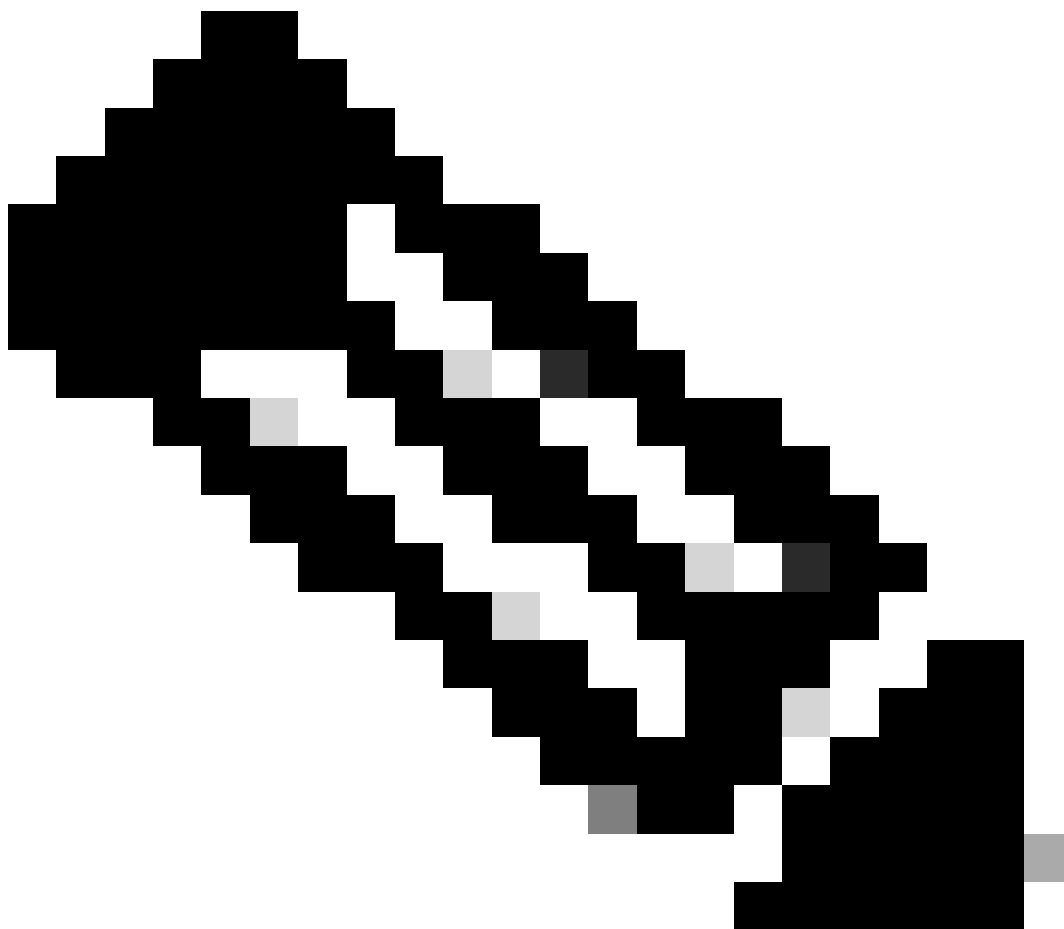
選中Prompt for Credentials > Never Remember選項，因此在每個身份驗證中，進行身份驗證的使用者必須輸入其憑據。

按一下「完成」。

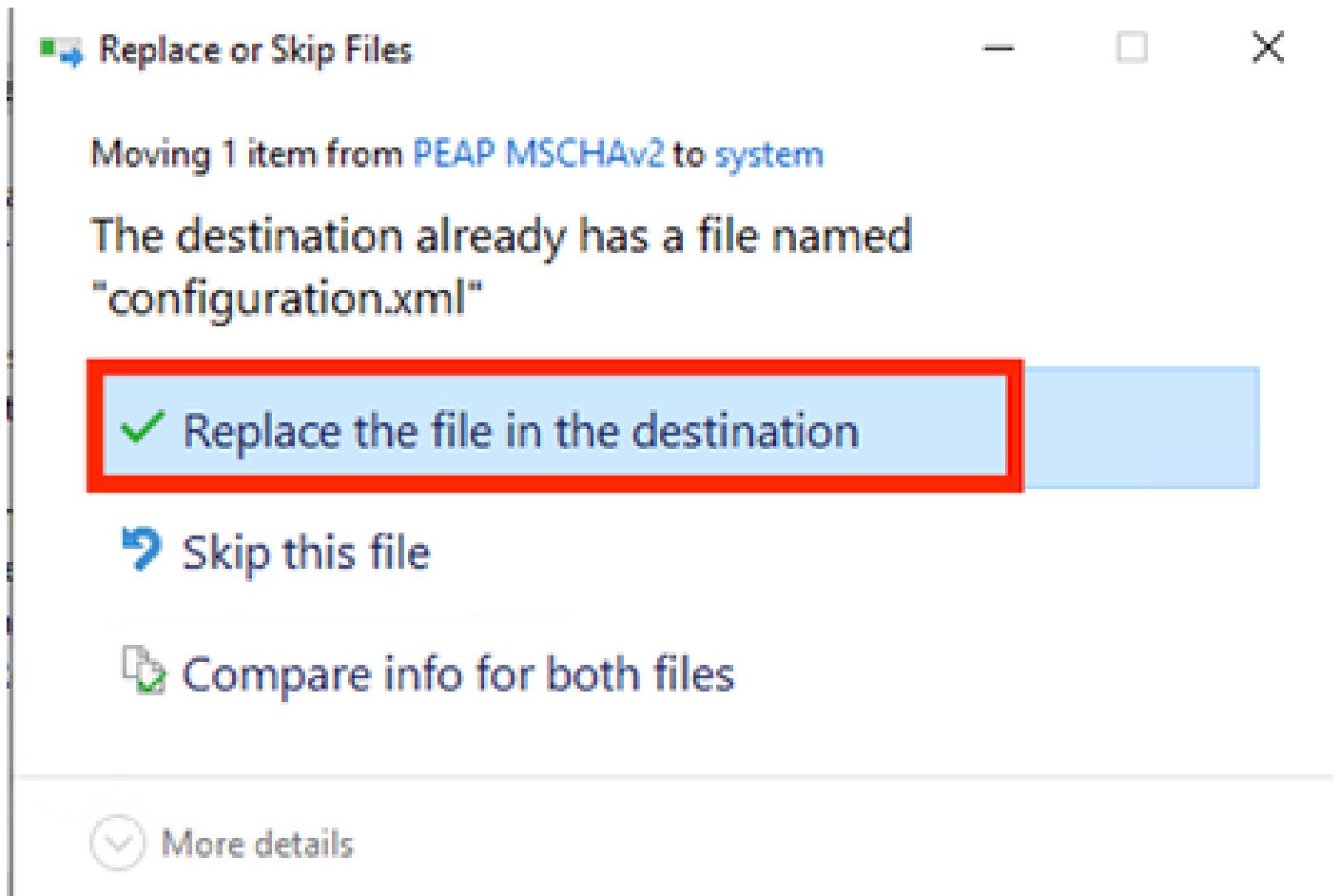
使用File > Save As選項將Secure Client Network Access Manager配置檔案另存為configuration.xml。

若要讓Secure Client Network Access Manager使用剛建立的設定檔，請將下一個目錄中的configuration.xml檔案取代為新的檔案：

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



注意：檔案必須命名為configuration.xml，否則將無法運作。



取代檔案區段

5. 方案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

打開NAM配置檔案編輯器，然後導航至網路部分。

按一下Add。

Networks

Profile: Untitled

Network

Name	Media Type	Group*

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

NAM配置檔案編輯器網路頁籤

在網路配置檔案中輸入名稱。

為Group Membership選擇Global。選擇WiredNetwork介質。

File Help

Networks
Profile: Untitled

Name: **EAP-FAST**

Group Membership

☐ In group: Local networks

☒ In all groups (Global)

Choose Your Network Media

☒ **Wired (802.3) Network**
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

☐ Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

☐ Hidden Network

☐ Corporate Network

Association Timeout: 5 seconds

Common Settings

Script or application on each user's machine to run when connected.

Browse Local Machine

Connection Timeout: 40 seconds

Next Cancel

Media Type
Security Level

媒體型別段落

按「Next」（下一步）。

選擇驗證網路，並且不要更改此部分中其餘選項的預設值。

File Help

Networks
Profile: Untitled

Security Level

☐ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

☒ Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

Security

Key Management
None

Encryption

☐ AES GCM 128
☐ AES GCM 256

Port Authentication Exception Policy

☐ Enable port exceptions

☐ Allow data traffic before authentication

☒ Allow data traffic after authentication even if

☐ EAP fails

☐ EAP succeeds but key management fails

Next Cancel

安全層次設定檔編輯器段落

點選下一步以繼續進行連線型別部分。

File Help

Networks
Profile: Untitled

Network Connection Type

☐ Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

☐ User Connection

The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

☒ Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

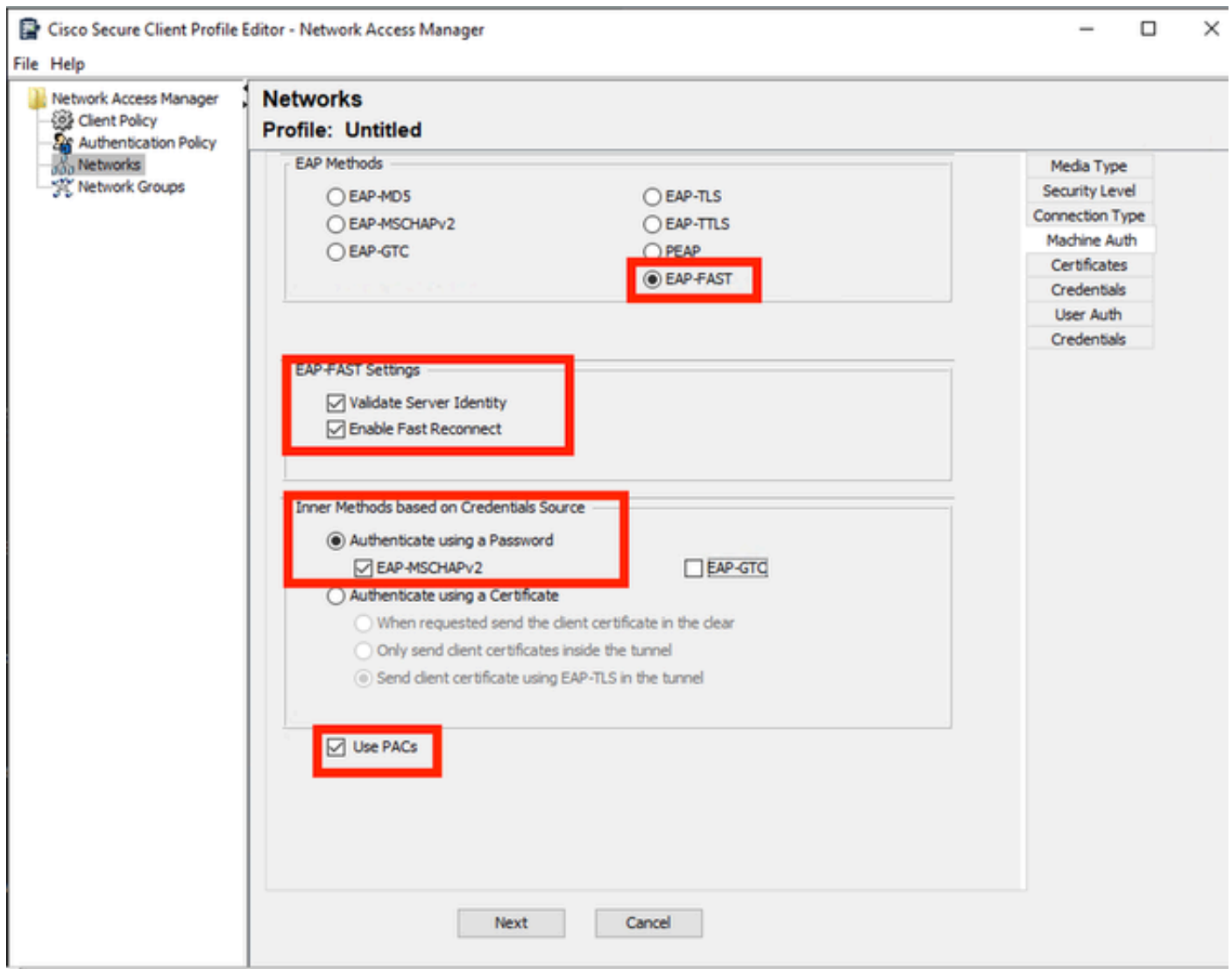
Media Type
Security Level
Connection Type
Machine Auth
Credentials
User Auth
Credentials

Next Cancel

連線型別段落

選取第三個選項，即可同時設定使用者和機器驗證。

按「Next」（下一步）。



電腦身份驗證部分

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和EAP-MSCHAPv2作為方法。然後選擇使用PAC選項。

按「Next」（下一步）。

在證書部分的證書受信任的伺服器規則中，規則公用名以c.com結尾。此區段是指伺服器在EAP PEAP流程期間使用的憑證。如果在您的環境中使用身份服務引擎(ISE)，可以使用策略伺服器節點EAP證書的公用名稱。

Networks

Profile: Untitled

Certificate Trusted Server Rules

<new>

Subject Alternative Name ends with c.com

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

AddSave

Certificate Trusted Authority

☒ Trust any Root Certificate Authority (CA) Installed on the OS

☐ Include Root Certificate Authority (CA) Certificates

AddRemove

Next

Cancel

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

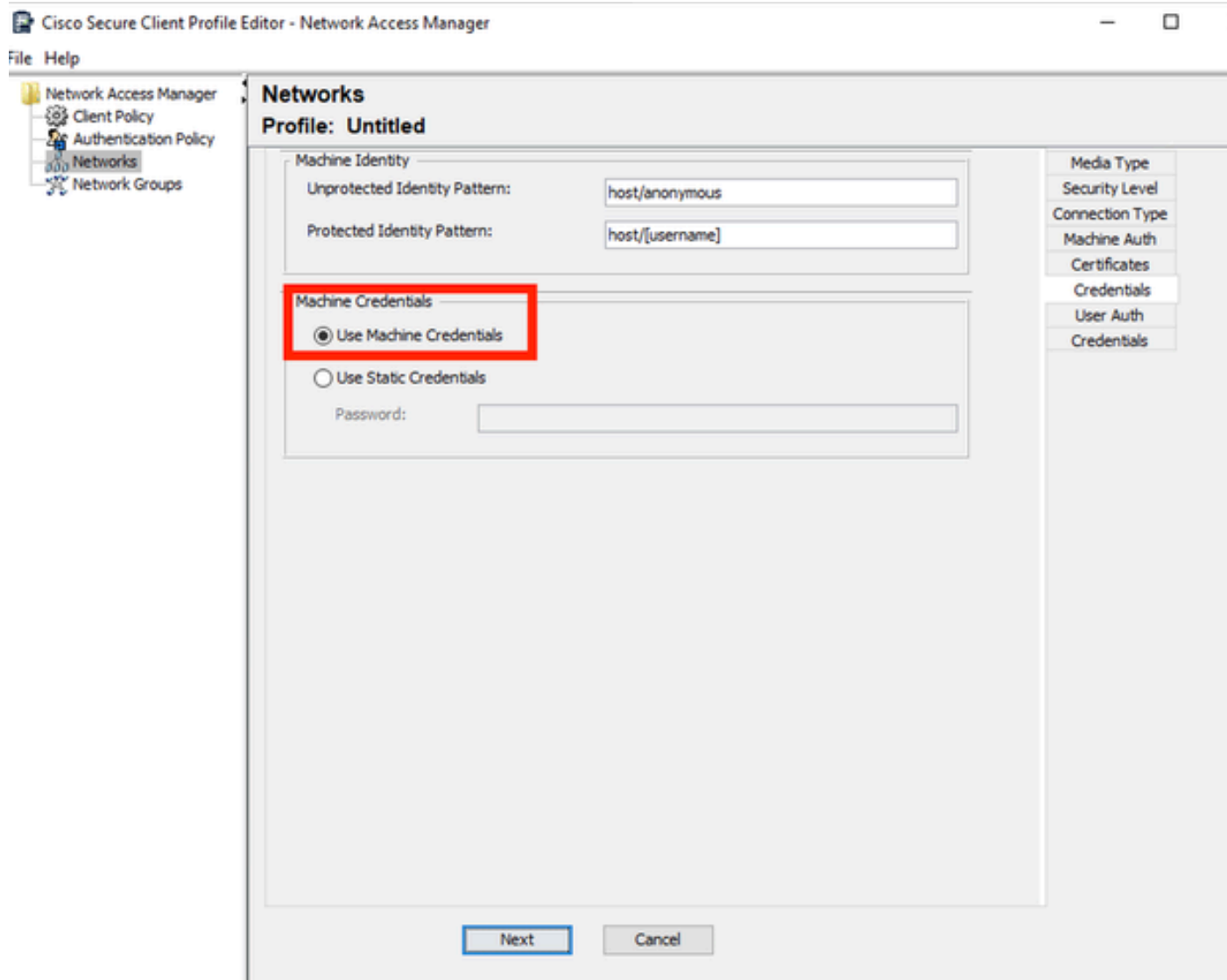
Credentials

電腦身份驗證伺服器證書信任部分

可以在證書受信任機構中選擇兩個選項。對於此情況，請使用Trust any Root Certificate Authority (CA) Installed on the OS選項，而不增加簽署RADIUS EAP證書的特定CA證書。

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

按「Next」(下一步)。



Machine Auth Credentials部分

在電腦憑據部分中選擇使用電腦憑據。

按「Next」(下一步)。

File Help

Networks
Profile: Untitled

EAP Methods

☐ EAP-MD5 ☐ EAP-TLS
☐ EAP-MSCHAPv2 ☐ EAP-TTLS
☐ EAP-GTC ☐ PEAP
☒ EAP-FAST

☐ Extend user connection beyond log off

EAP-FAST Settings

☒ Validate Server Identity
☒ Enable Fast Reconnect
☐ Disable when using a Smart Card

Inner Methods based on Credentials Source

☒ Authenticate using a Password
☒ EAP-MSCHAPv2 ☐ EAP-GTC
☐ Authenticate using a Certificate
☐ When requested send the client certificate in the clear
☐ Only send client certificates inside the tunnel
☒ Send client certificate using EAP-TLS in the tunnel
☐ Authenticate using a Token and EAP-GTC

☒ Use PACs

Next Cancel

Media Type
 Security Level
 Connection Type
 Machine Auth
 Certificates
 Credentials
 User Auth
 Certificates
 Credentials

使用者驗證段落

對於User Auth，請選擇EAP-FAST作為EAP方法。

請勿更改EAP-FAST設定部分中的預設值。

對於Inner Method based on credentials source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）。

在證書部分的證書受信任的伺服器規則中，規則為公用名以c.com結尾。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。

Networks

Profile: C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml

The screenshot shows a network configuration window with two main sections: 'Certificate Trusted Server Rules' and 'Certificate Trusted Authority'. In the 'Certificate Trusted Server Rules' section, a list contains one rule: 'Common Name ends with c.com', which is highlighted with a blue selection bar and a red rectangular border. Below this list is a table with three columns: 'Certificate Field', 'Match', and 'Value'. The first row shows 'Common Name' in the first column, 'ends with' in the second, and 'c.com' in the third. Below the table are 'Remove' and 'Save' buttons. The 'Certificate Trusted Authority' section below it has two radio button options: 'Trust any Root Certificate Authority (CA) Installed on the OS' (which is selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these options is an empty list box with 'Add' and 'Remove' buttons. On the right side of the window is a vertical pane with a list of tabs: 'Media Type', 'Security Level', 'Connection Type', 'Machine Auth', 'Certificates', 'Credentials', 'User Auth', and 'Certificates' (repeated). The 'Certificates' tab is highlighted with a red rectangular border. At the bottom of the window are 'Next' and 'Cancel' buttons.

Certificate Field	Match	Value
Common Name	ends with	c.com

Buttons: Remove, Save

Radio buttons:
☒ Trust any Root Certificate Authority (CA) Installed on the OS
☐ Include Root Certificate Authority (CA) Certificates

Buttons: Add, Remove

Bottom buttons: Next, Cancel

Right-hand pane tabs: Media Type, Security Level, Connection Type, Machine Auth, **Certificates**, Credentials, User Auth, Certificates

使用者身份驗證伺服器證書信任部分

可以在證書受信任機構中選擇兩個選項。對於此情況，使用選項Trust any Root Certificate Authority (CA) Installed on the OS而不增加簽署RADIUS EAP證書的特定CA證書。

按「Next」(下一步)。

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

anonymous

Protected Identity Pattern:

[username]

User Credentials

☐ Use Single Sign On Credentials

☒ Prompt for Credentials

☐ Remember Forever

☐ Remember while User is Logged On

☒ Never Remember

☐ Use Static Credentials

Password:

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

Credentials

Done

Cancel

使用者身份驗證憑據

在「身份證明」部分中，僅更改了使用者身份證明部分。

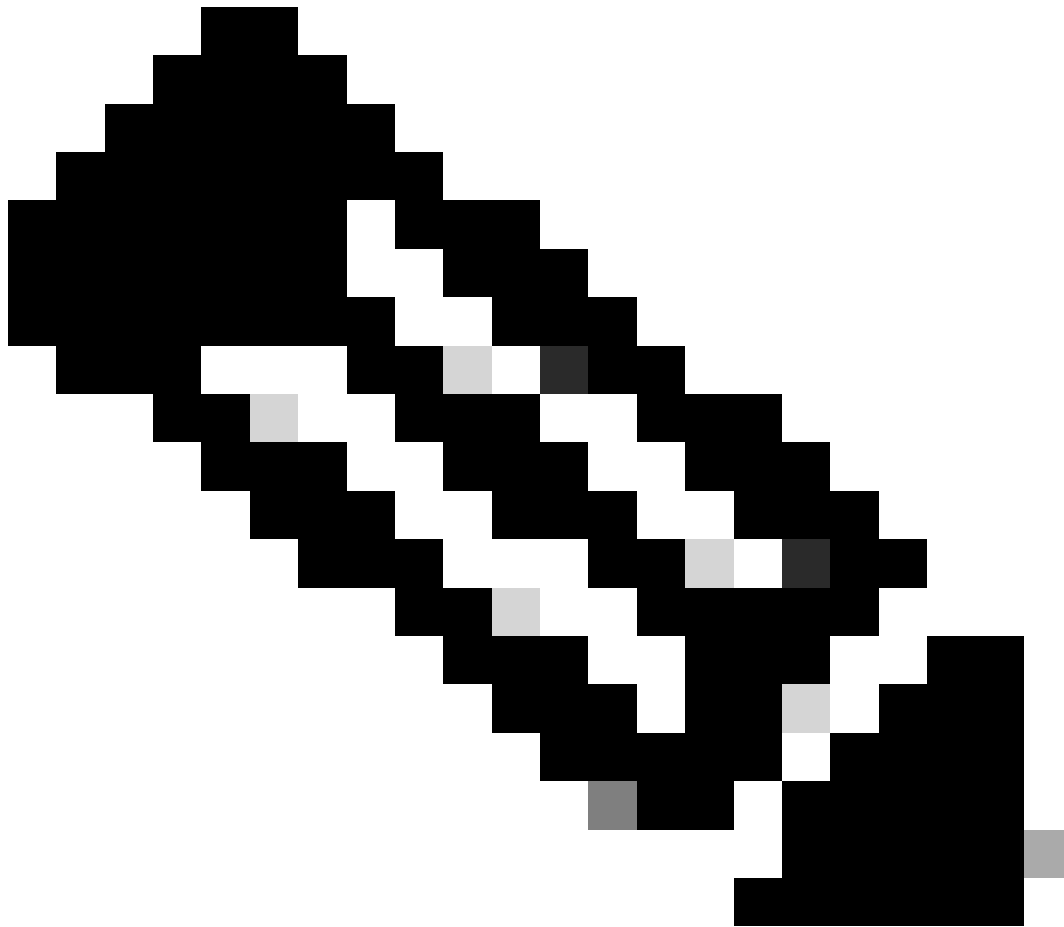
已選中提示輸入憑據>永不記憶選項。因此，在每次身份驗證中，使用者身份驗證必須輸入其憑據。

按一下Done按鈕。

選擇File > Save as，然後將Secure Client Network Access Manager配置檔案儲存為configuration.xml。

要使Secure Client Network Access Manager使用剛才建立的配置檔案，請用新目錄替換下一個目錄中的configuration.xml檔案：

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



注意：檔案必須命名為configuration.xml，否則將無法運作。

6. 方案3：為EAP TLS使用者證書身份驗證配置安全客戶端NAM請求方

打開NAM Profile Editor，然後導航到Networks部分。

按一下Add。

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

網路建立段落

命名網路設定檔，在此案例中，命名為用於此案例的EAP通訊協定。

為Group Membership選擇Global。和有線網路介質。

Networks
Profile: Untitled

Name: EAP-TLS

Group Membership

☐ In group: Local networks

☒ In all groups (Global)

Choose Your Network Media

☒ Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

☐ Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

☐ Hidden Network

☐ Corporate Network

Association Timeout: 5 seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: 40 seconds

Media Type

Security Level

媒體型別段落

按「Next」（下一步）。

選擇驗證網路，並且不要更改安全級別部分其他選項的預設值。

Cisco Secure Client Profile Editor - Network Access Manager

File Help

Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups

Networks

Profile: Untitled

Security Level

☐ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

☒ **Authenticating Network**
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) startPeriod (sec.)

heldPeriod (sec.) maxStart

Security

Key Management
None

Encryption

☐ AES GCM 128
☐ AES GCM 256

Port Authentication Exception Policy

☐ Enable port exceptions

☐ Allow data traffic before authentication

☒ Allow data traffic after authentication even if

☐ EAP fails
☐ EAP succeeds but key management fails

Media Type
Security Level
Connection Type

Next Cancel

安全性層級

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

Cisco Secure Client Profile Editor - Network Access Manager

File Help

Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups

Networks

Profile: Untitled

Network Connection Type

☐ Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

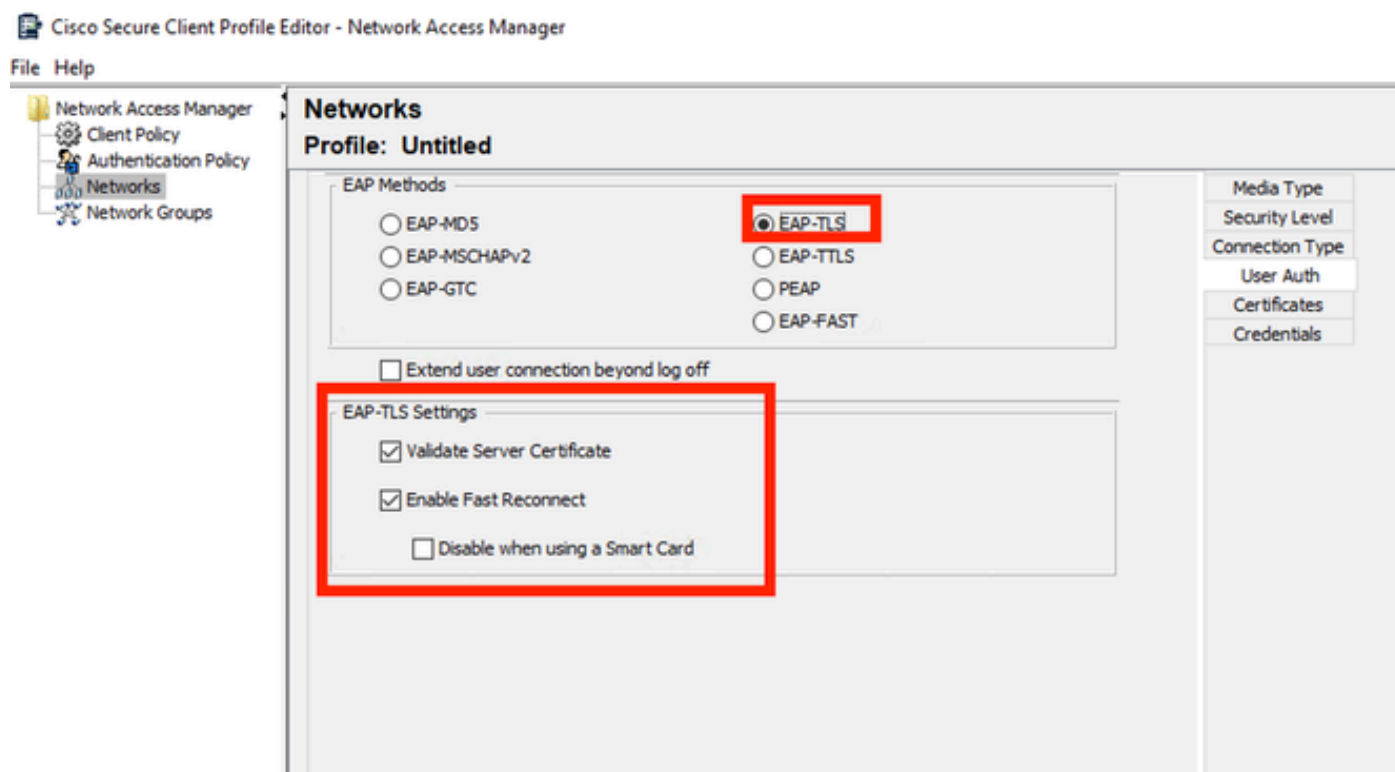
☒ **User Connection**
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

☐ Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Media Type
Security Level
Connection Type
User Auth
Credentials

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

在「憑證」段落中，建立與AAA EAP-TLS憑證相符的規則。如果您使用ISE，請在管理>系統>證書部分找到此規則。

對於證書受信任機構部分，選擇信任作業系統上安裝的任意根證書機構(CA)。

Networks
Profile: Untitled

Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups

Certificate Trusted Server Rules

Common Name ends with c.com

Certificate Field: Subject Alt. Name
Match: exactly matches
Value:

Add Save

Certificate Trusted Authority

☒ Trust any Root Certificate Authority (CA) Installed on the OS
☐ Include Root Certificate Authority (CA) Certificates

Add Remove

Media Type
Security Level
Connection Type
User Auth
Certificates
Credentials

Next Cancel

使用者身份驗證伺服器證書信任設定

按「Next」（下一步）。

對於User Credentials部分，請勿更改第一部分中的預設值。

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

User Credentials

☒ Use Single Sign On Credentials (Requires Smart Card)

☐ Prompt for Credentials

☐ Remember Forever

☒ Remember while User is Logged On

☐ Never Remember

Certificate Source

☒ Smart Card or OS certificates

☐ Smart Card certificates only

Remember Smart Card Pin

☐ Remember Forever

☐ Remember while User is Logged On

☒ Never Remember

Smart Card Removal Policy

☐ Disconnect from Network

☒ Use Certificate Matching Rule (Max 10)

Rule Logic ☒ OR ☐ AND

Field	Operator	Value

Add

Edit

Delete

Media Type

Security Level

Connection Type

User Auth

Certificates

Credentials

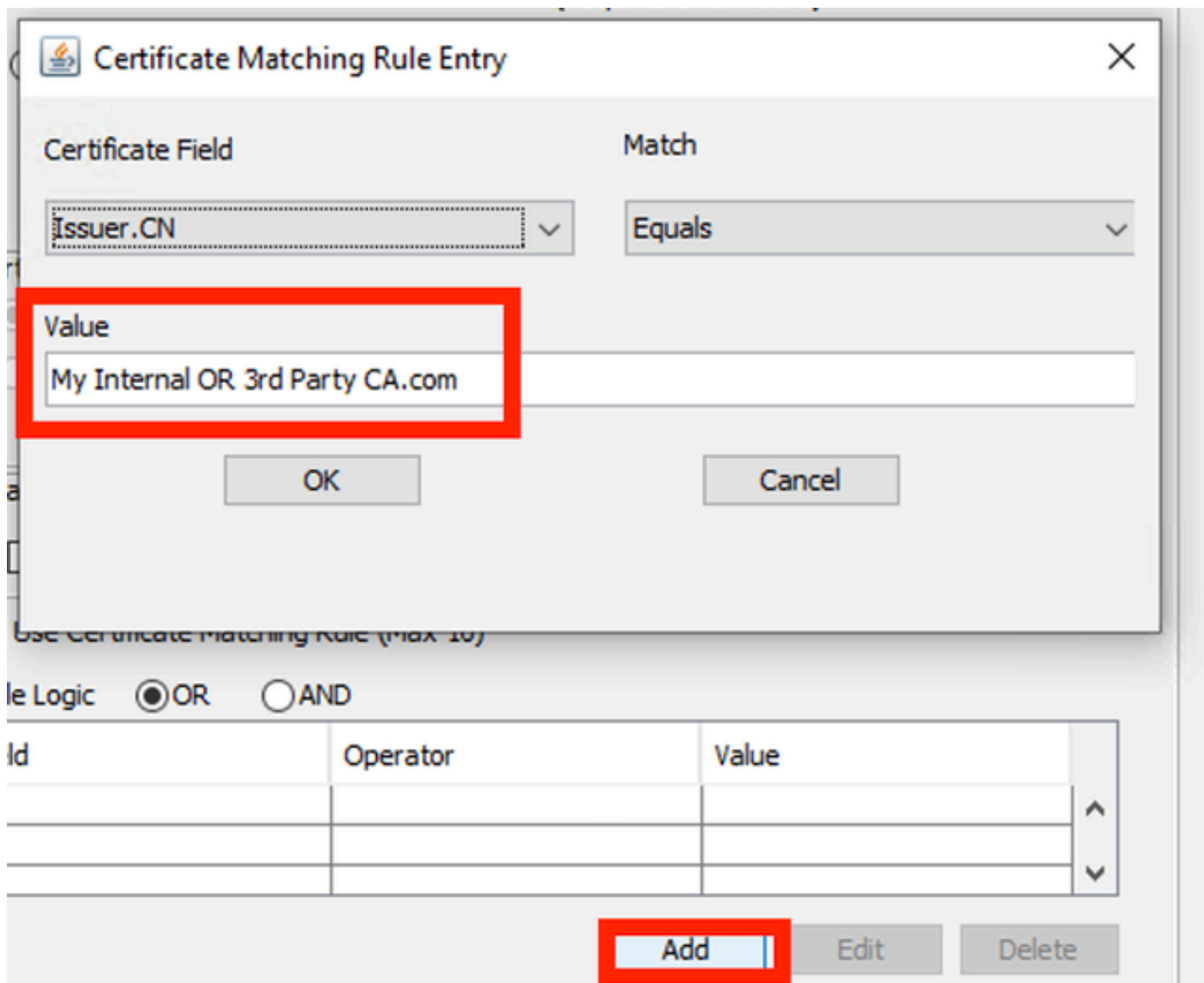
Done

Cancel

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，請按一下Use Certificate Matching Rule (Max 10)旁邊的覈取方塊。

按一下Add。

The image shows a 'Certificate Matching Rule Entry' dialog box. It has a title bar with a close button. Inside, there are two dropdown menus: 'Certificate Field' and 'Match'. The 'Certificate Field' dropdown is set to 'Issuer.CN'. The 'Match' dropdown is set to 'Equals'. Below these is a 'Value' text box containing the text 'My Internal OR 3rd Party CA.com'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. Below the dialog, there is a section for 'Use Certificate Matching Rule (Max 10)' with a radio button for 'OR' selected and 'AND' unselected. Below this is a table with three columns: 'Id', 'Operator', and 'Value'. The table is currently empty. At the bottom right of the table are three buttons: 'Add', 'Edit', and 'Delete'. The 'Add' button is highlighted with a red box.

Certificate Matching Rule Entry

Certificate Field: Issuer.CN

Match: Equals

Value: My Internal OR 3rd Party CA.com

OK Cancel

Use Certificate Matching Rule (Max 10)

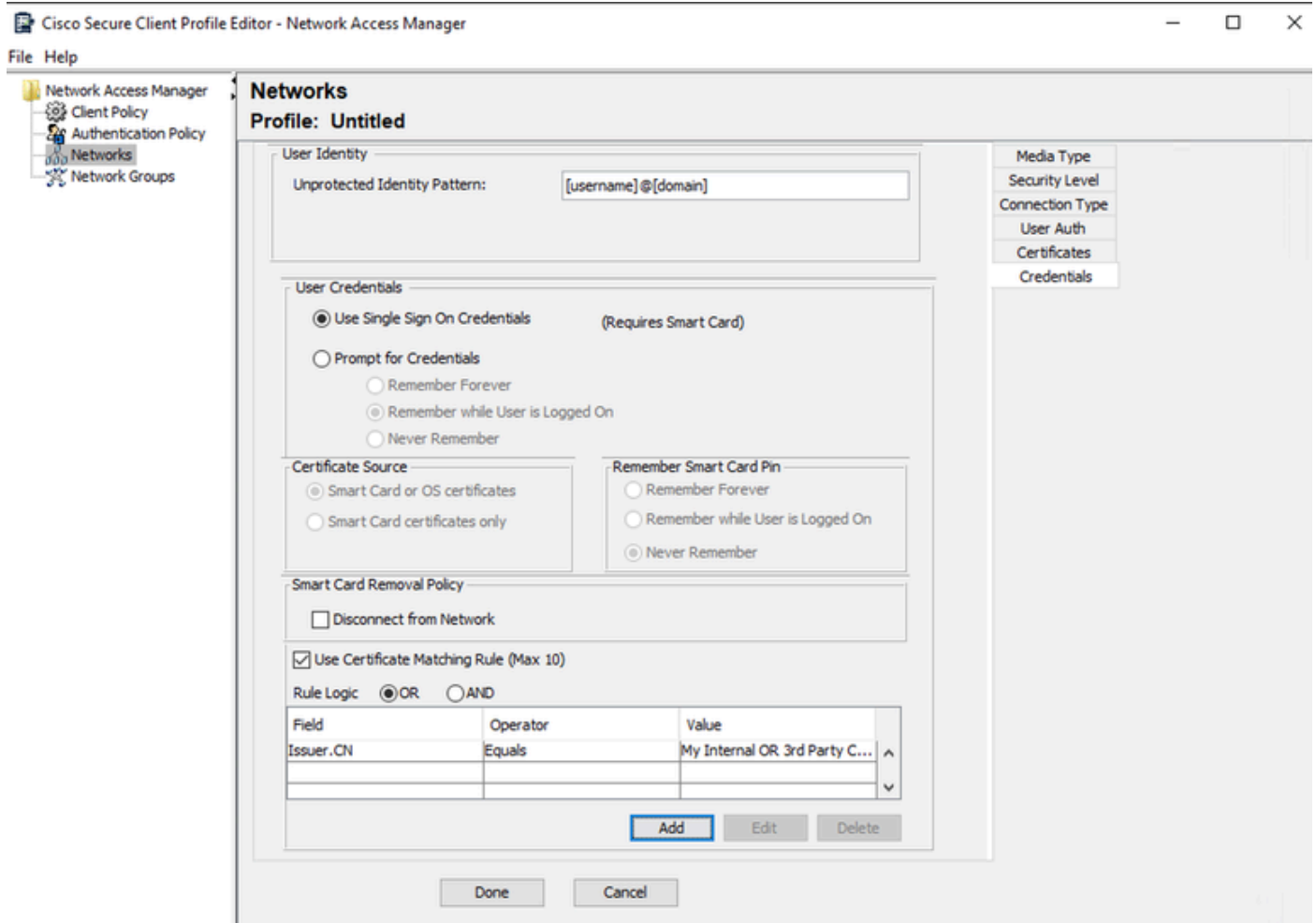
le Logic: ☒ OR ☐ AND

Id	Operator	Value

Add Edit Delete

憑證比對規則視窗

用使用者證書的CN替換值My Internal或第三方CA.com。



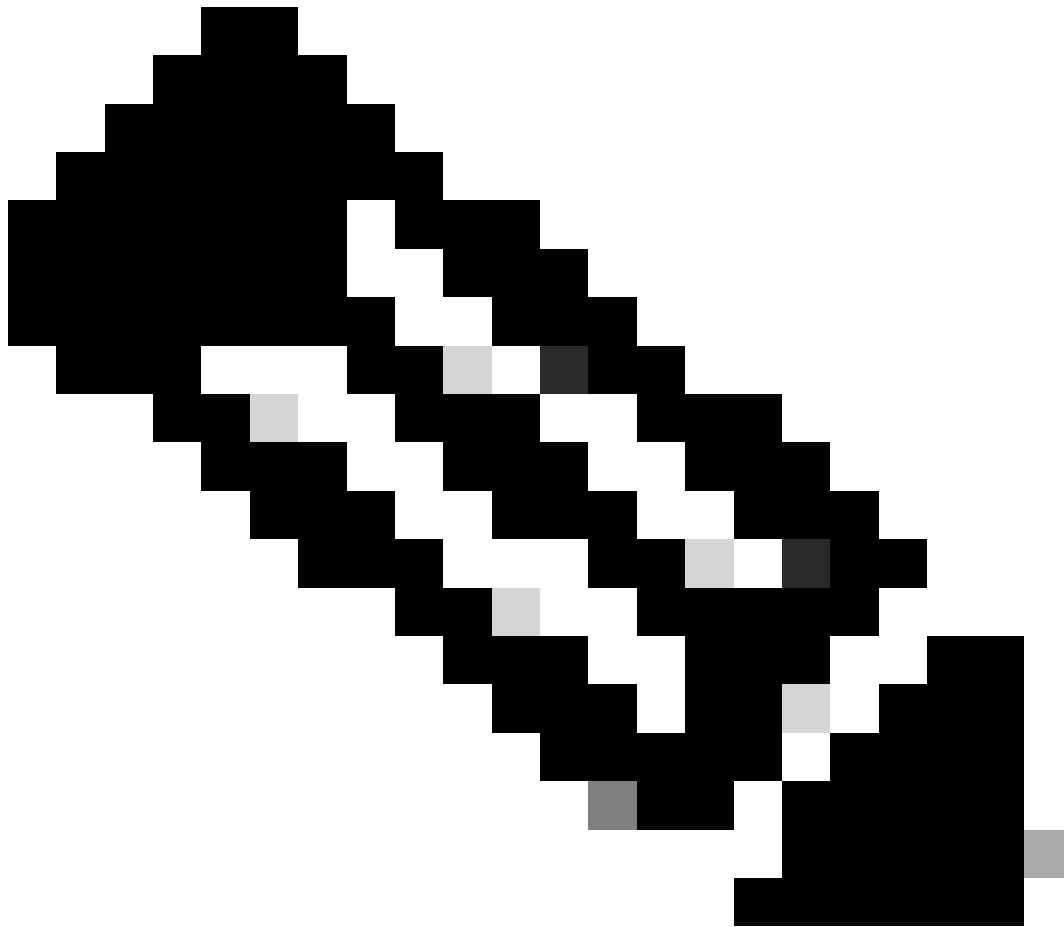
使用者驗證憑證段落

按一下Done完成配置。

選擇File > Save as將Secure Client Network Access Manager配置檔案儲存為configuration.xml。

要使Secure Client Network Access Manager使用剛才建立的配置檔案，請用新目錄替換下一個目錄中的configuration.xml檔案：

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

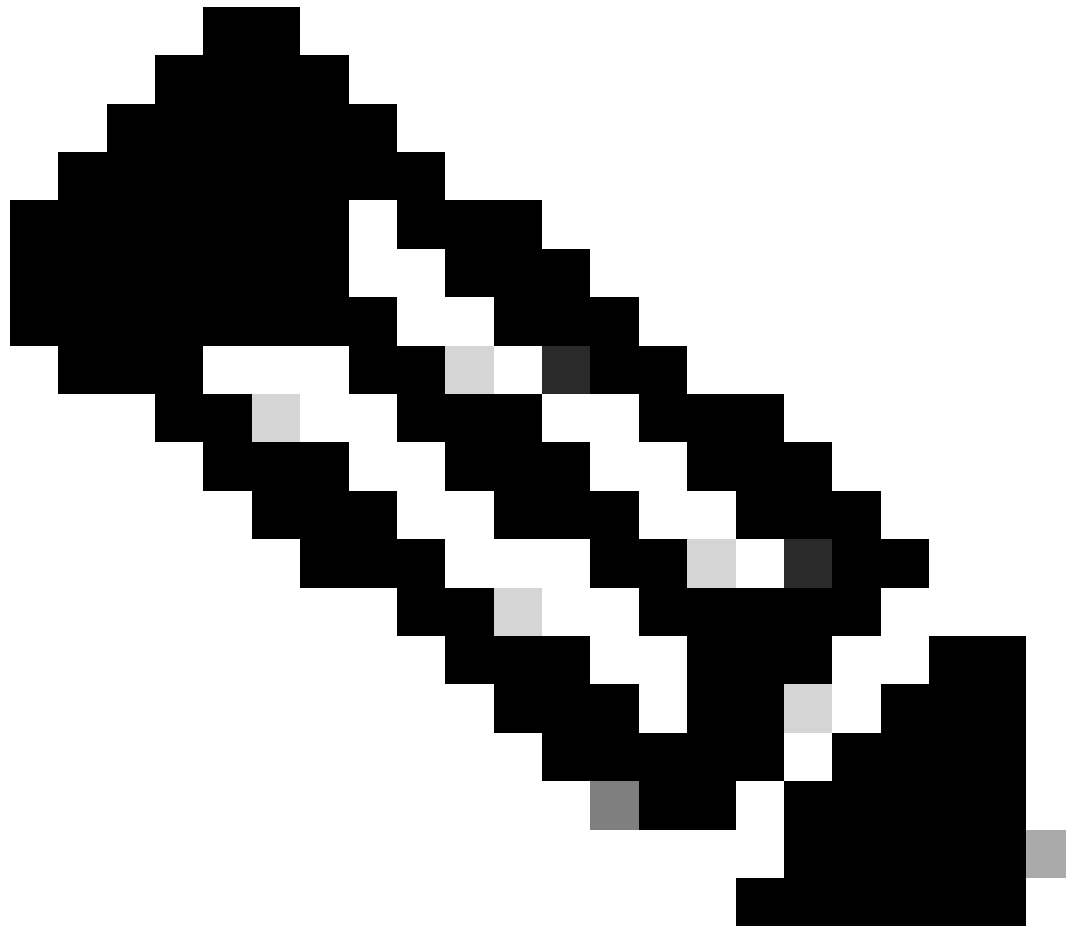


注意：檔案必須命名為configuration.xml，否則將無法運作。

7. 根據方案1 PEAP MSCHAPv2配置ISR 1100和ISE以允許身份驗證

配置ISR 1100路由器。

本節介紹NAD必須具備的基本配置，才能使dot1x正常工作。



注意：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。可透過導航到管理>系統>部署頁籤中的ISE進行檢查。

```
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>
!
!
```

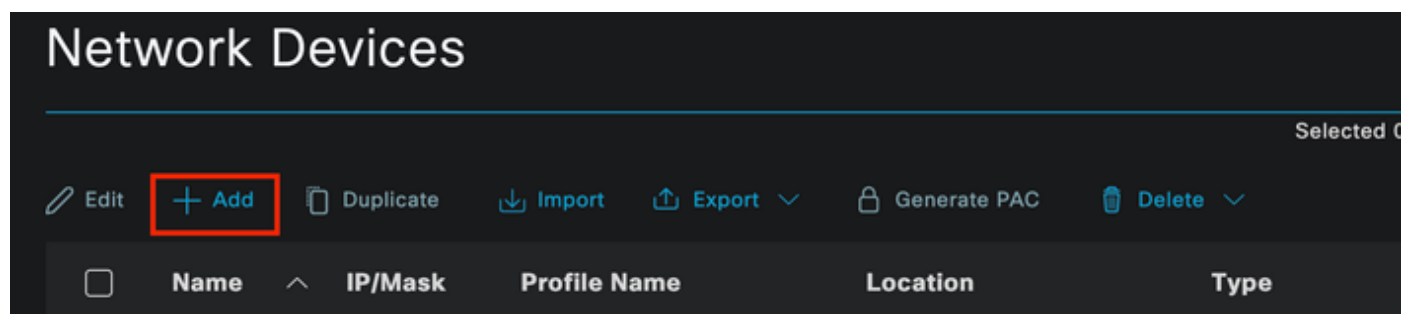
```
aaa group server radius ISE-CLUSTER
server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
description "Endpoint that supports dot1x"
switchport access vlan 15
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication 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。

增加ISR NAD到ISE Administration > Network Resources > Network Devices。

按一下Add。



網路裝置部分

為正在建立的NAD指定名稱。增加網路裝置IP。

Cisco ISE Administration · Network Resources Evaluation Mode 29 Days

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | More

Network Devices

Network Devices List > ISR1100

Network Devices

Name

Description

IP Address * IP: /

Device Profile

Model Name

Software Version

Network Device Group

網路裝置建立

在同一頁的底部，增加與網路裝置配置中使用的共用金鑰相同。

☒ **RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

☐ Use Second Shared Secret [i](#)

Second Shared Secret [Show](#)

CoA Port [Set To Default](#)

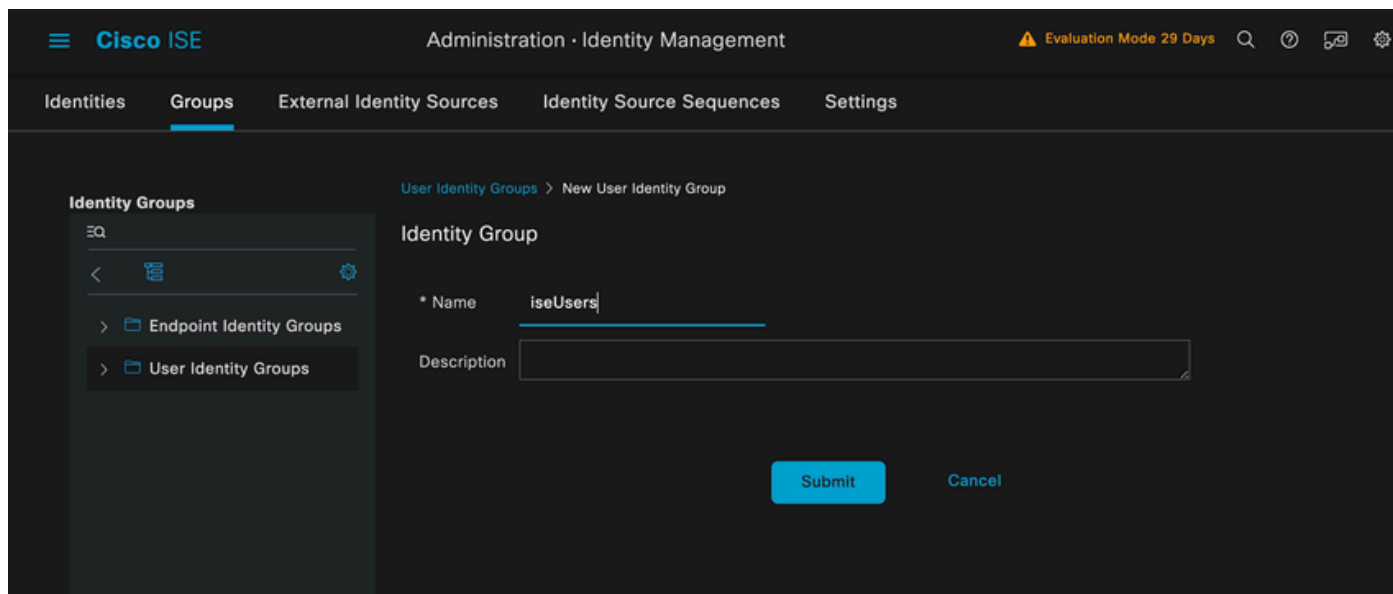
網路裝置Radius設定

儲存變更。

配置用於驗證終端的身份。

使用ISE本地身份驗證。本文未對外部ISE身份驗證進行說明。

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。



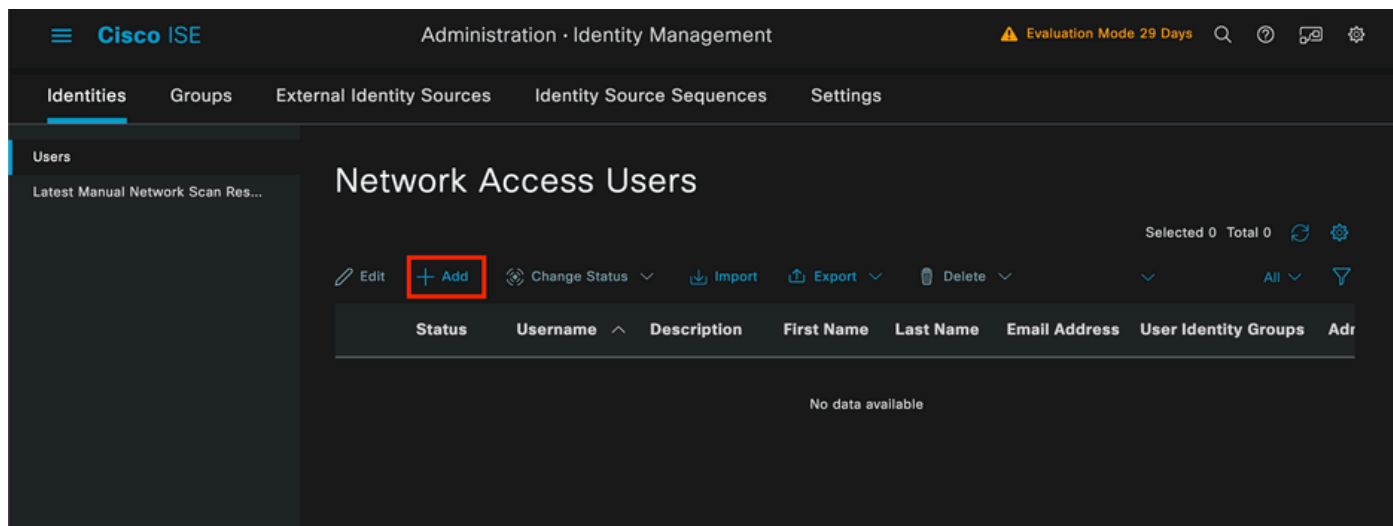
The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and a status indicator 'Evaluation Mode 29 Days'. The main navigation tabs are 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' tab is selected. On the left, the 'Identity Groups' sidebar shows a tree structure with 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups > New User Identity Group'. It contains a form with the following fields: 'Name' (required, filled with 'iseUsers') and 'Description' (empty). At the bottom right of the form are 'Submit' and 'Cancel' buttons.

身份組建立

按一下Submit。

導航到管理>身份管理>身份頁籤。

按一下Add。



The screenshot shows the Cisco ISE Administration console. The top navigation bar is the same as the previous image. The main navigation tabs are 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Identities' tab is selected. On the left, the 'Users' sidebar shows a tree structure with 'Latest Manual Network Scan Res...'. The main content area is titled 'Network Access Users'. It contains a toolbar with buttons: 'Edit', '+ Add' (highlighted with a red box), 'Change Status', 'Import', 'Export', and 'Delete'. Below the toolbar is a table with the following columns: 'Status', 'Username', 'Description', 'First Name', 'Last Name', 'Email Address', 'User Identity Groups', and 'Address'. The table is currently empty, with the text 'No data available' at the bottom.

網路存取使用者段落

作為必填欄位的一部分，以使用者名稱開頭。本示例中使用使用者名稱iseischool。

Network Access User

* Username iseiscool

Status ☒ Enabled

Account Name Alias

Email

網路存取使用者建立

為使用者指定密碼。 使用VainillaISE97。

Passwords

Password Type: Internal Users

Password Lifetime:

☒ With Expiration
Password will expire in 60 days

☐ Never Expires

Password

Re-Enter Password

* Login Password

Enable Password

Generate Password

Generate Password

使用者建立密碼段落

將使用者分配到組iseUsers。

User Groups



iseUsers

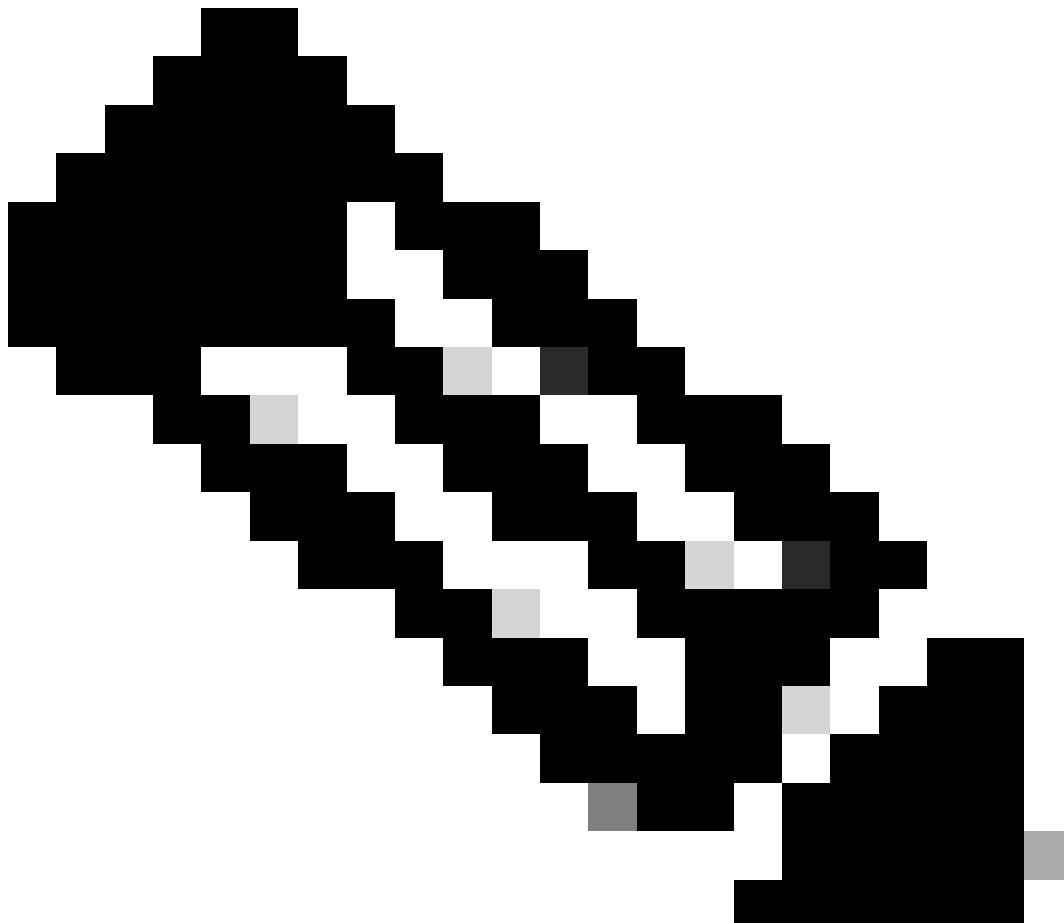


使用者組分配

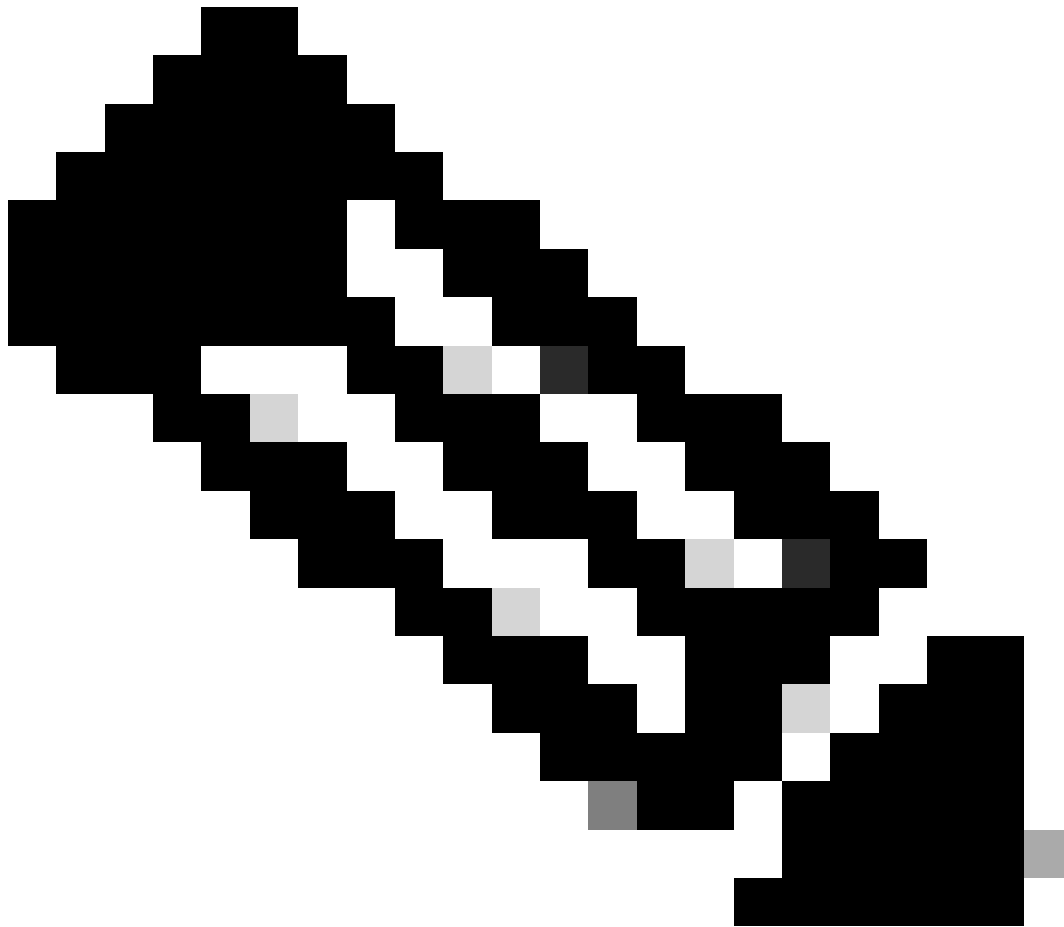
配置策略集。

導航到ISE選單>策略>策略集。

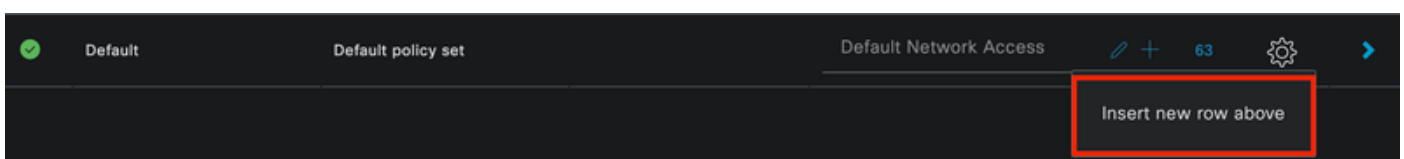
可以使用預設策略集。但是，本示例建立了一個名為Wired的示例。



註：對策略集進行分類和區分有助於排除故障，

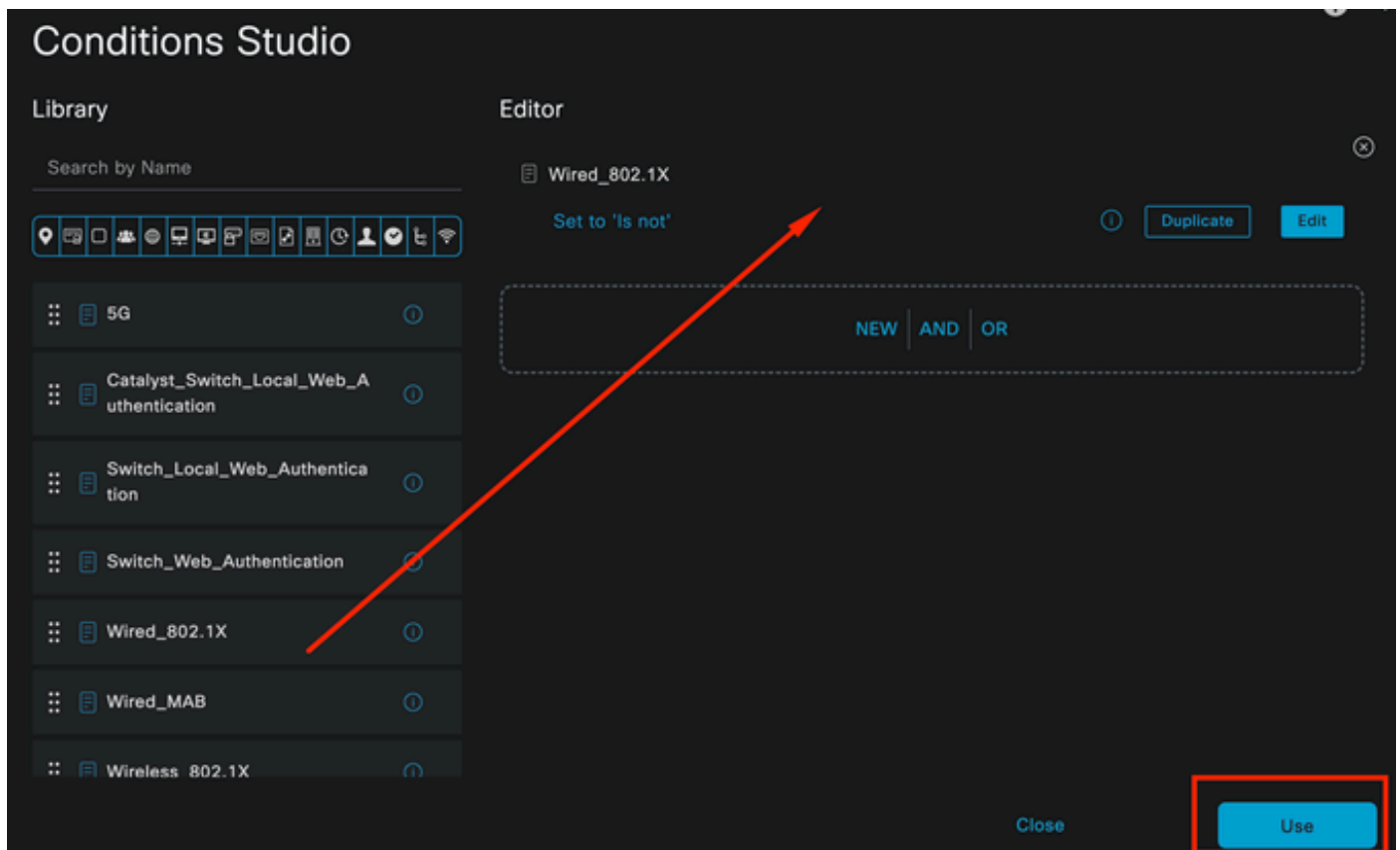


附註：如果看不到新增或加號圖示，可以按一下任何原則集的齒輪圖示，然後選取在上方插入新列。



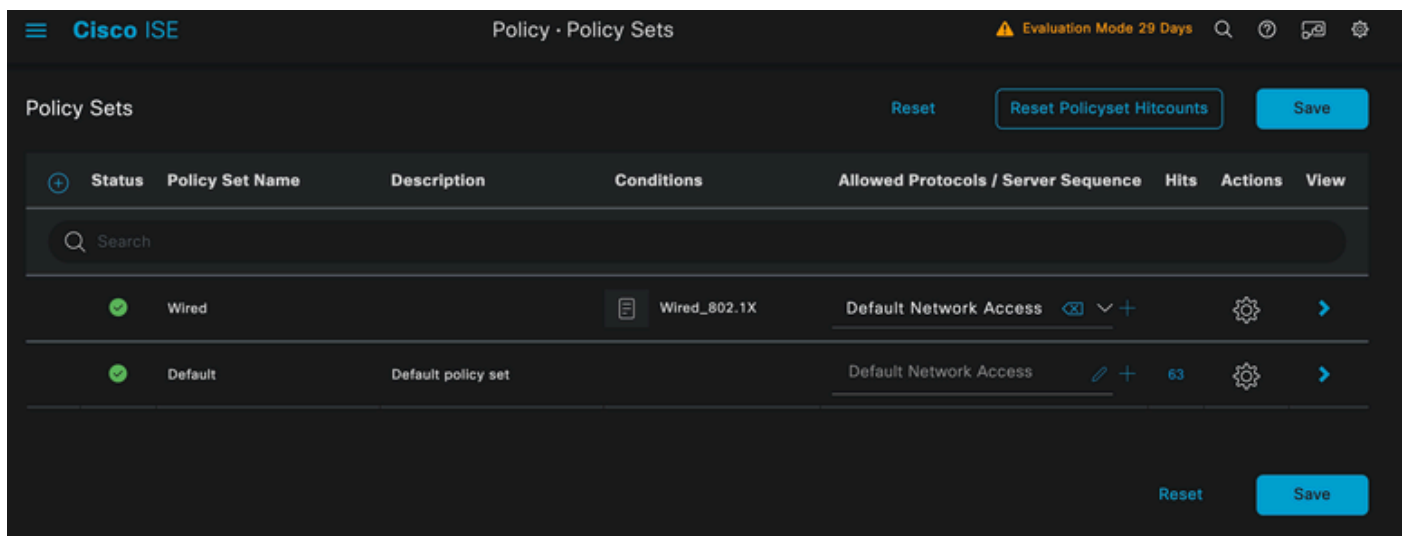
齒輪圖示選項

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。



原則集一般檢視

按一下Save。

2.d.配置身份驗證和授權策略。

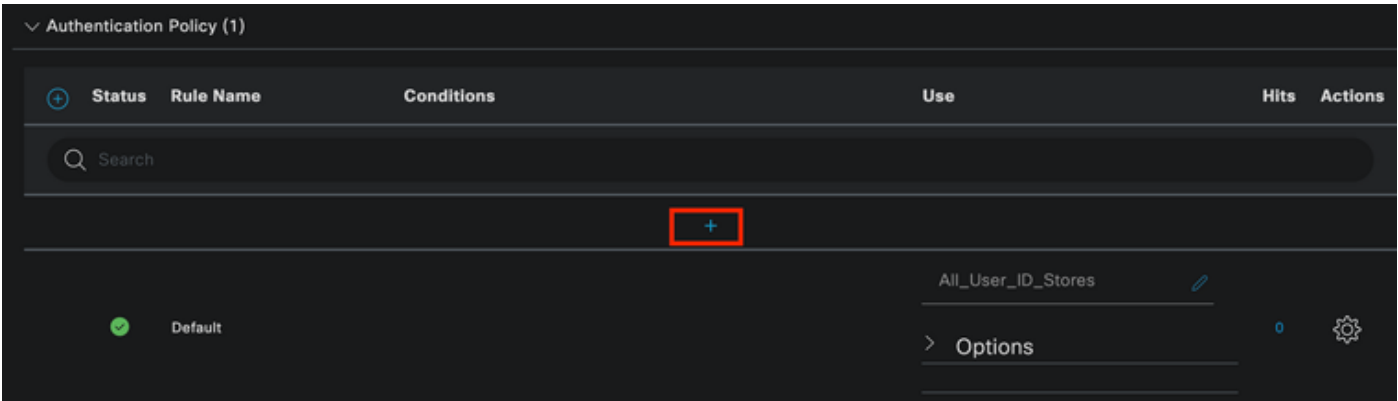
按一下>圖示。



有線策略集

展開Authentication Policy部分。

按一下+圖示。



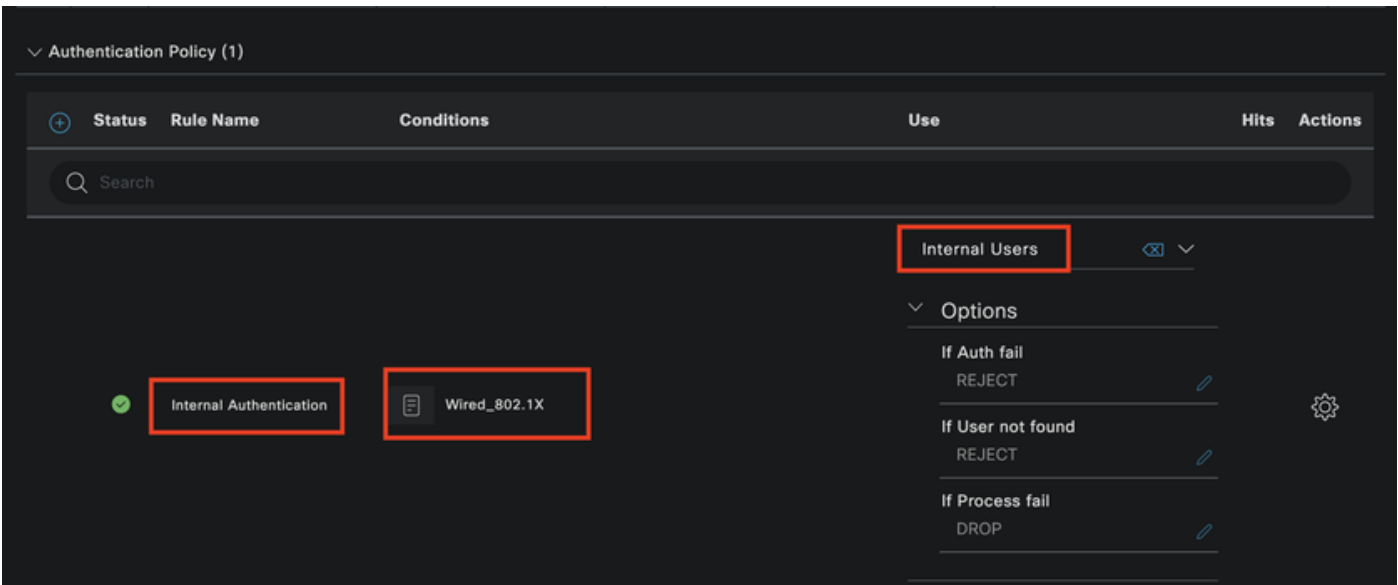
身份驗證策略

為Authentication Policy指定一個名稱。此示例中使用Internal Authentication。

按一下此新身份驗證策略的「條件」列上的+圖示。

使用的是預配置條件Wired Dot1x。

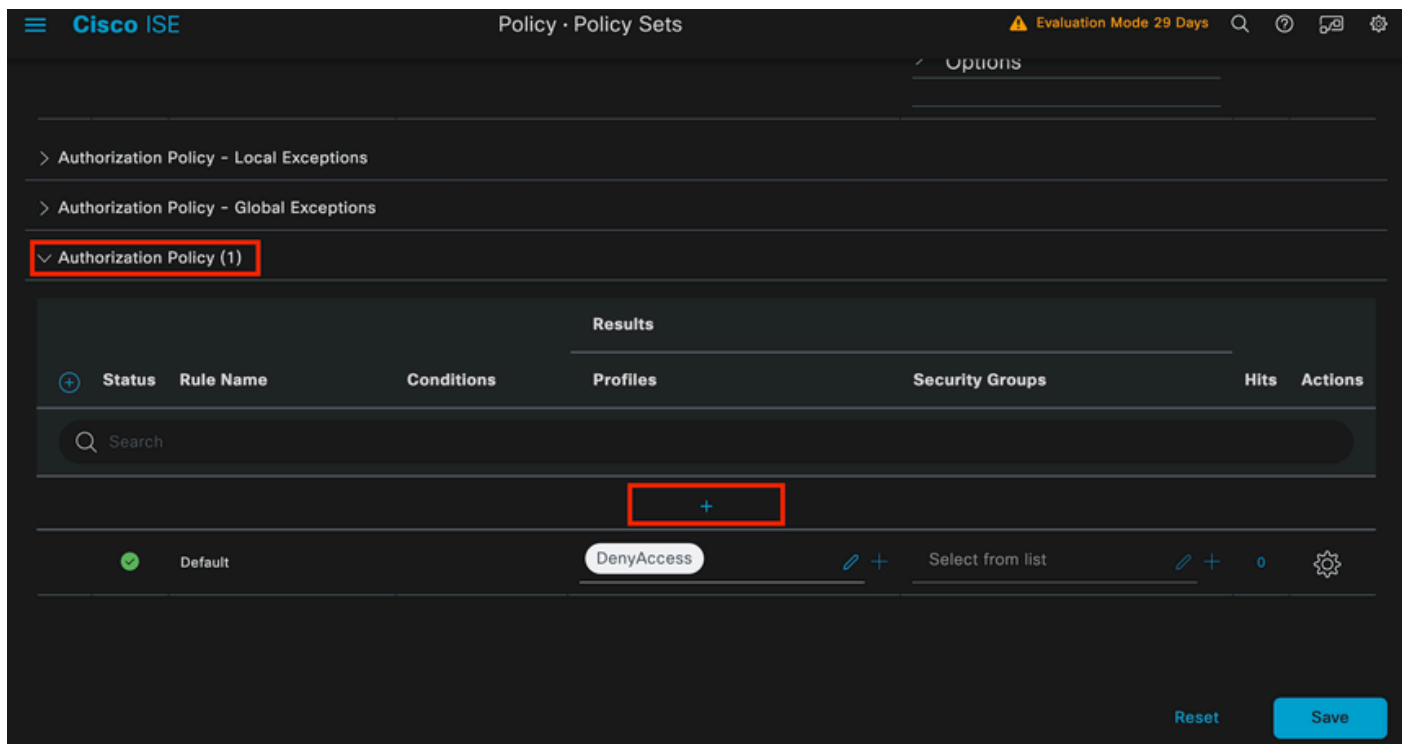
最後，在使用列中選擇內部使用者。



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+圖示。



授權策略

為最近建立的授權策略命名。在此配置示例中，使用名稱Internal ISE Users。

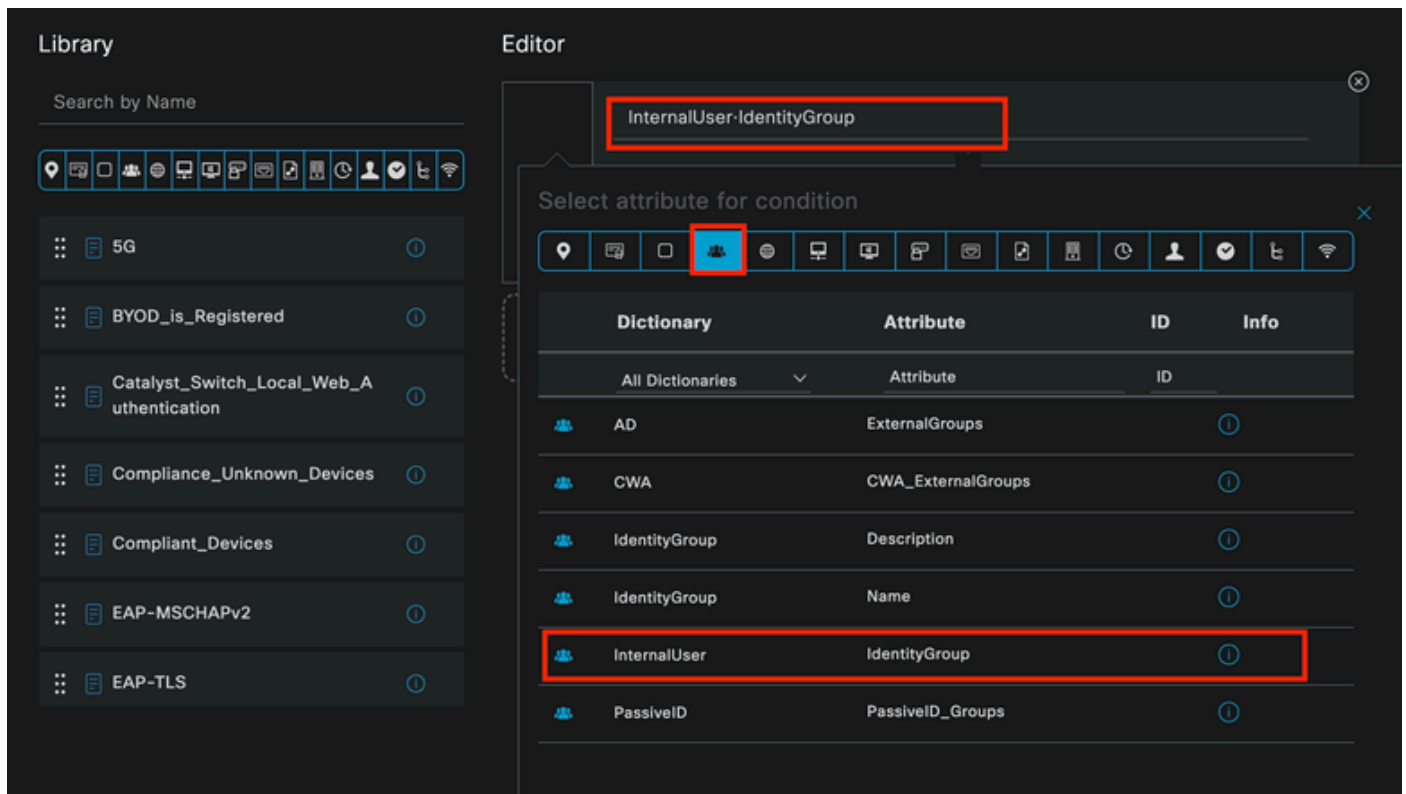
要為此授權策略建立條件，請在條件列中點選+圖示。

使用組IseUsers。

按一下Attribute部分。

選擇IdentityGroup圖示。

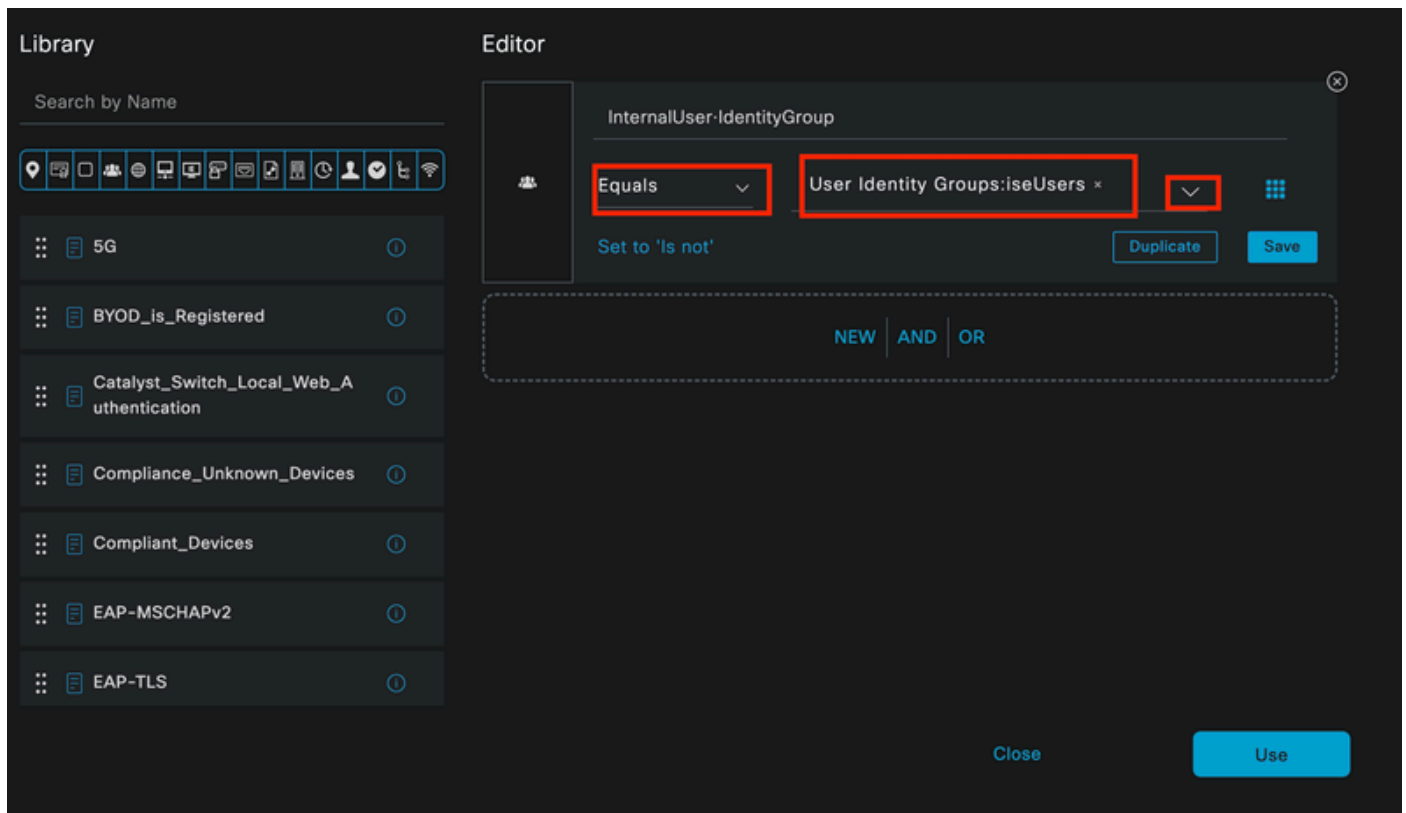
從詞典中，選擇帶有IdentityGroup屬性的InternalUser詞典。



條件建立

選取等於運算子。

從使用者身份組中，選擇組IseUsers。

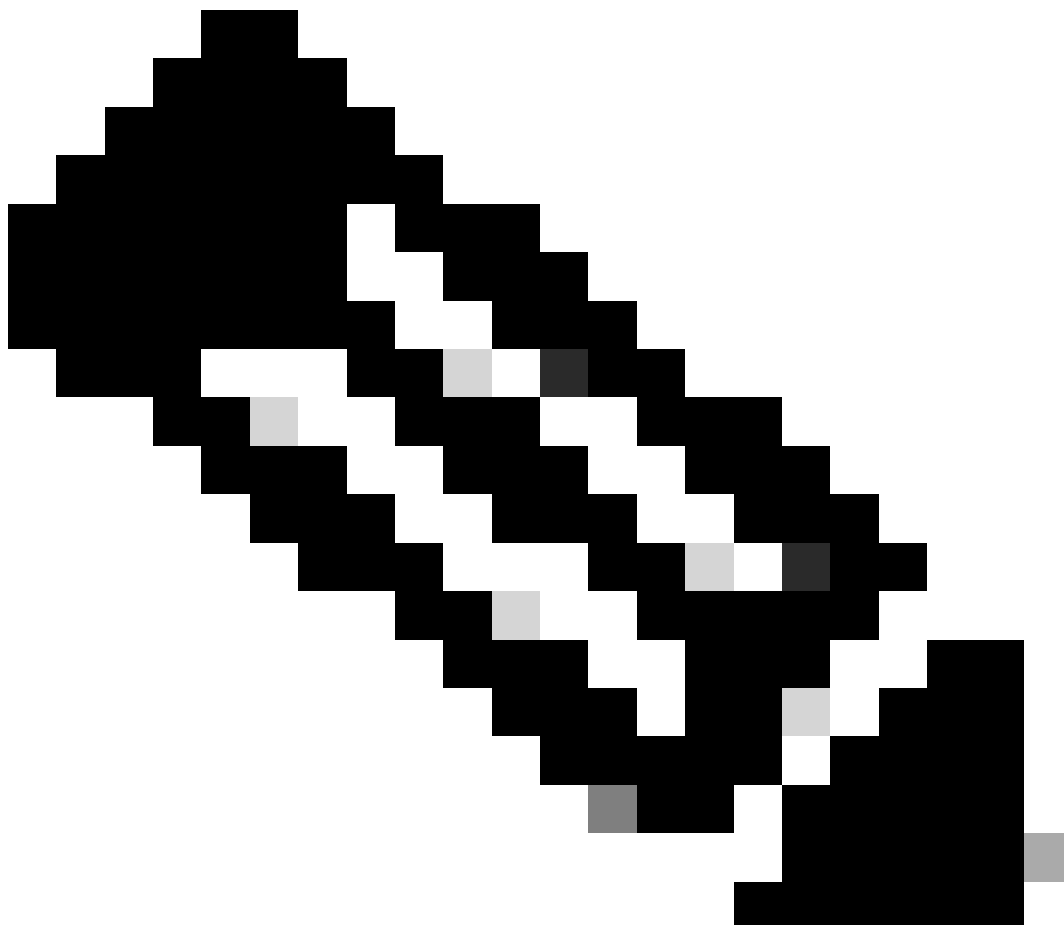


條件建立

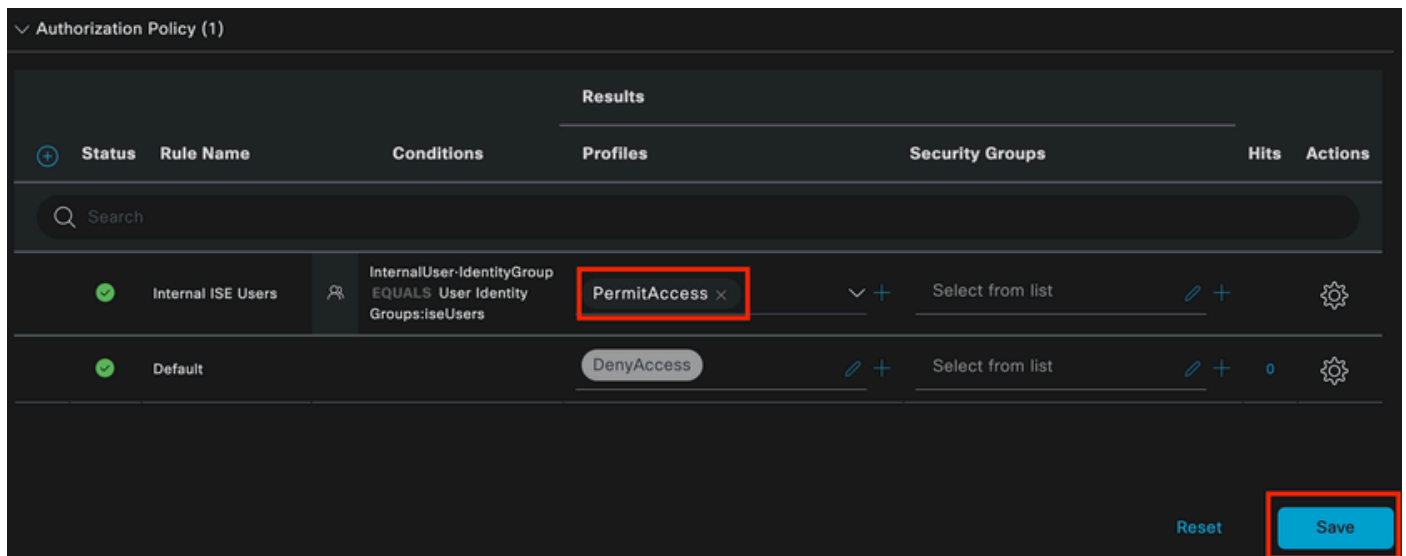
按一下Use。

增加結果授權配置檔案。

使用的是預配置的配置檔案Permit Access。



注意：請注意，傳送到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的一部分），點選預設授權策略，其結果為DenyAccess。



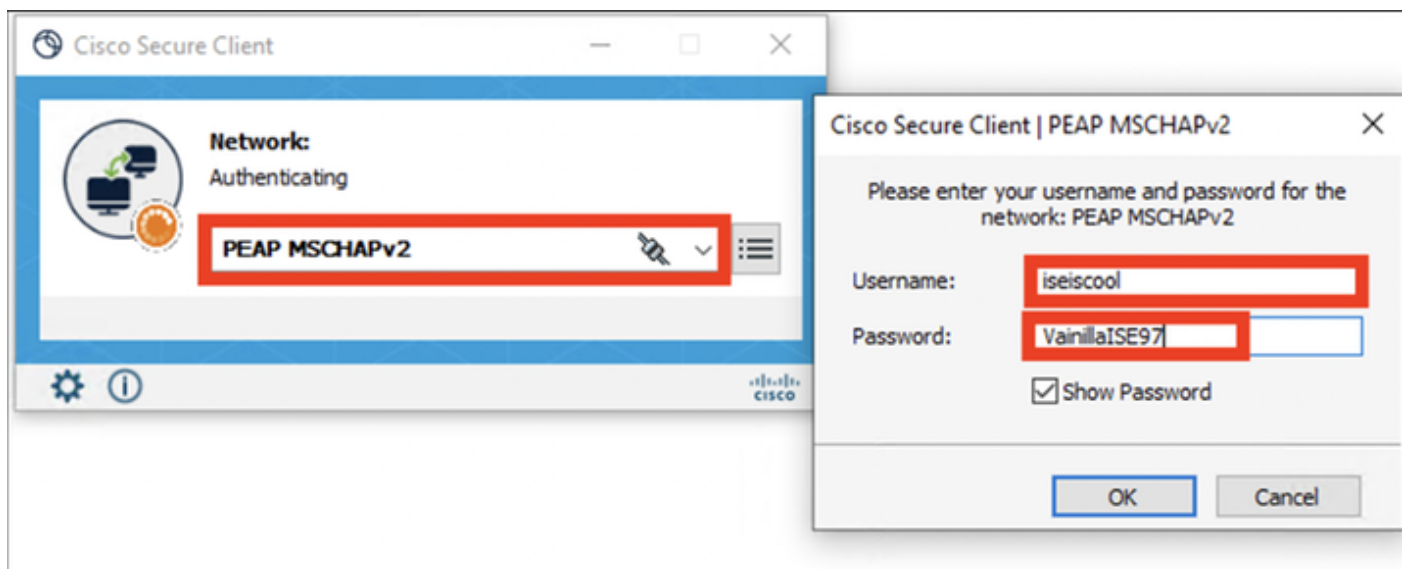
授權策略

按一下Save。

驗證

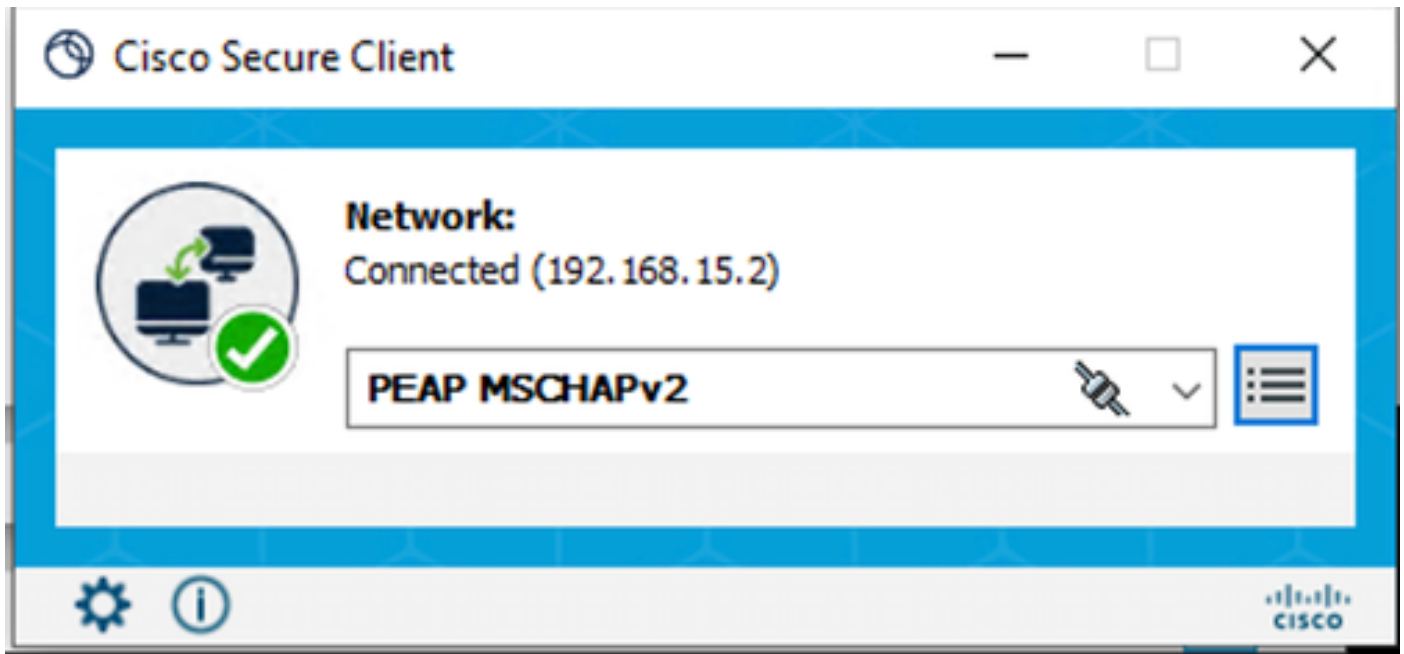
配置完成後，安全客戶端將提示輸入憑證，並指定PEAP MSCHAPv2配置檔案的使用。

輸入先前建立的身份證明。



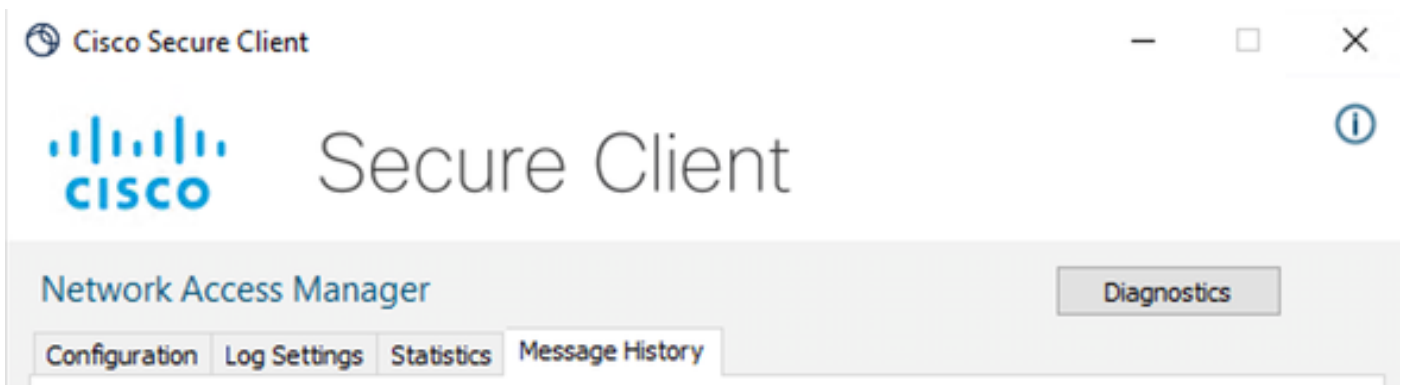
安全使用者端NAM

如果終端身份驗證正確，。NAM顯示已連線。



安全使用者端NAM

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



安全客戶端消息歷史記錄

7:06:01 PM	PEAP MSCHAPv2 : Authenticating
7:06:21 PM	PEAP MSCHAPv2 : Acquiring IP Address
7:06:21 PM	PEAP MSCHAPv2 : Connected

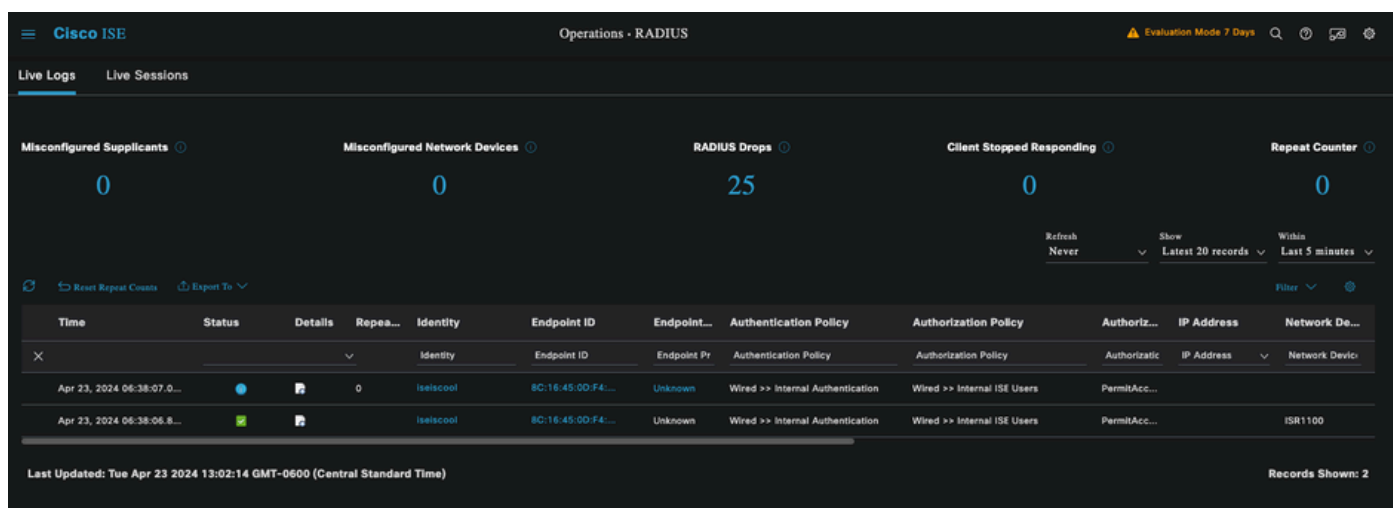
安全客戶端消息歷史記錄

從ISE導航到操作> Radius LiveLogs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：

- 時間戳記。
- MAC 地址。
- 使用的策略集。
- 身份驗證策略。
- 授權策略。

- 其他相關資訊。



ISE RADIUS即時日誌

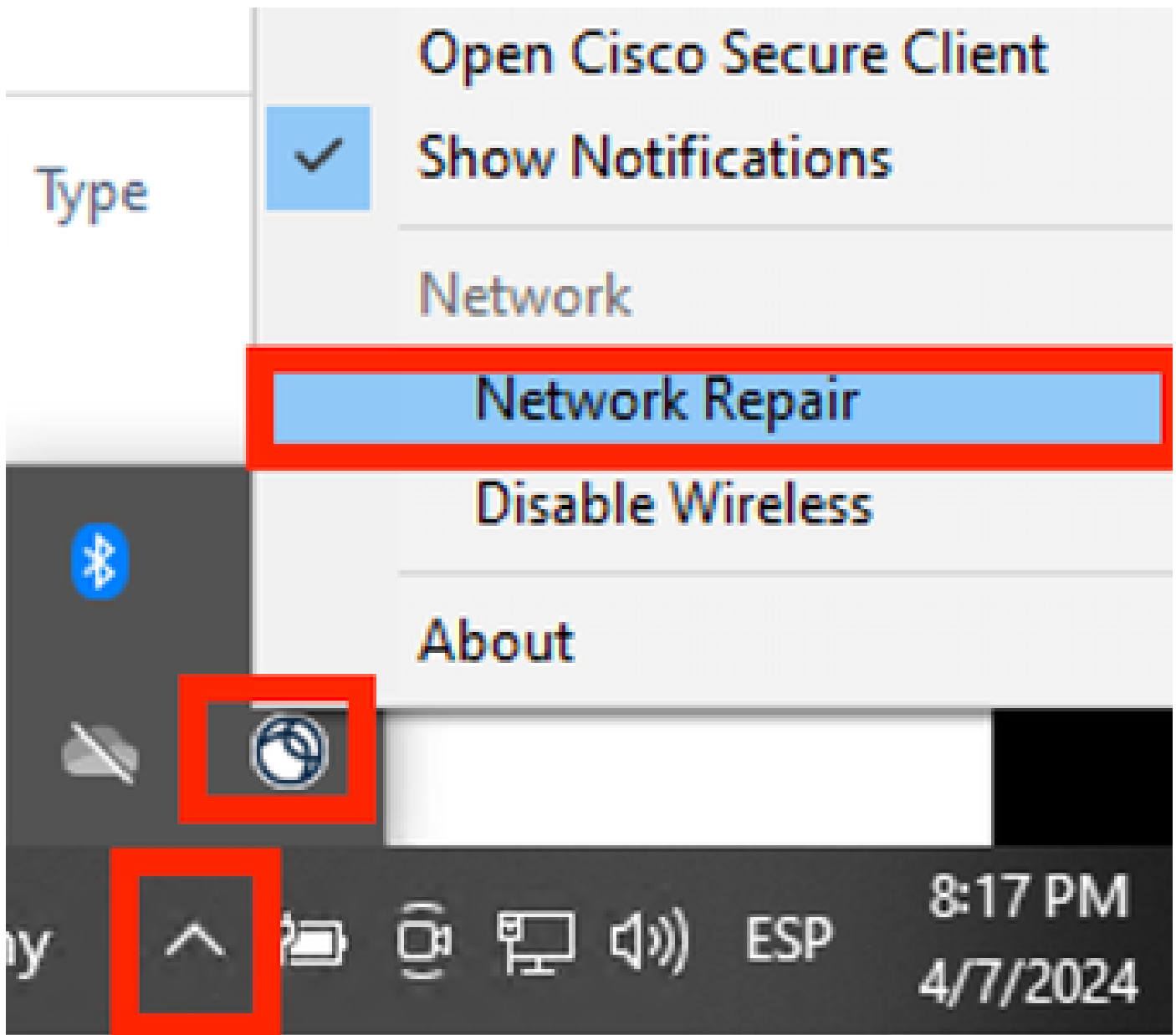
由於您會看到它符合正確的策略，並且結果是身份驗證狀態成功，因此可以斷定配置正確。

疑難排解

問題：安全客戶端未使用NAM配置檔案。

如果NAM未使用在配置檔案編輯器中建立的新配置檔案，請使用Secure Client的Network Repair選項。

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

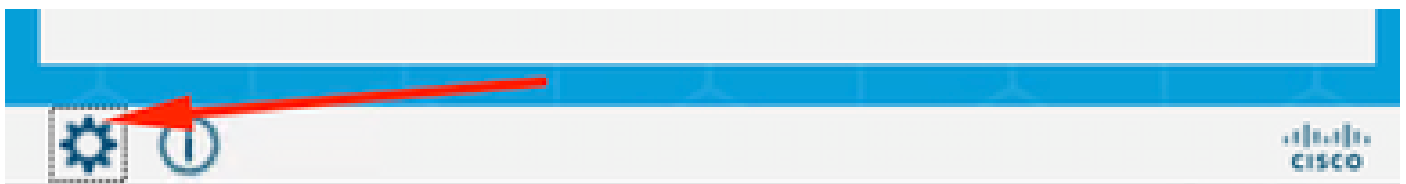


網路修復段落

問題2：需要收集日誌以供進一步分析。

1. 啟用NAM擴展日誌記錄

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釐取方塊。

將資料包捕獲檔案大小設定為100 MB。



Secure Client



Network Access Manager

Diagnostics

Configuration

Log Settings

Statistics

Message History

Use extended logging to collect additional information about product operations.

☒ Enable Extended Logging

IHV: Off

Filter Driver: Off

☐ Credential Provider☒ Packet Capture

Maximum Packet Capture File Size (MB): 100

安全客戶端NAM日誌設定

2. 重現問題。

啟用擴展日誌記錄後，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。



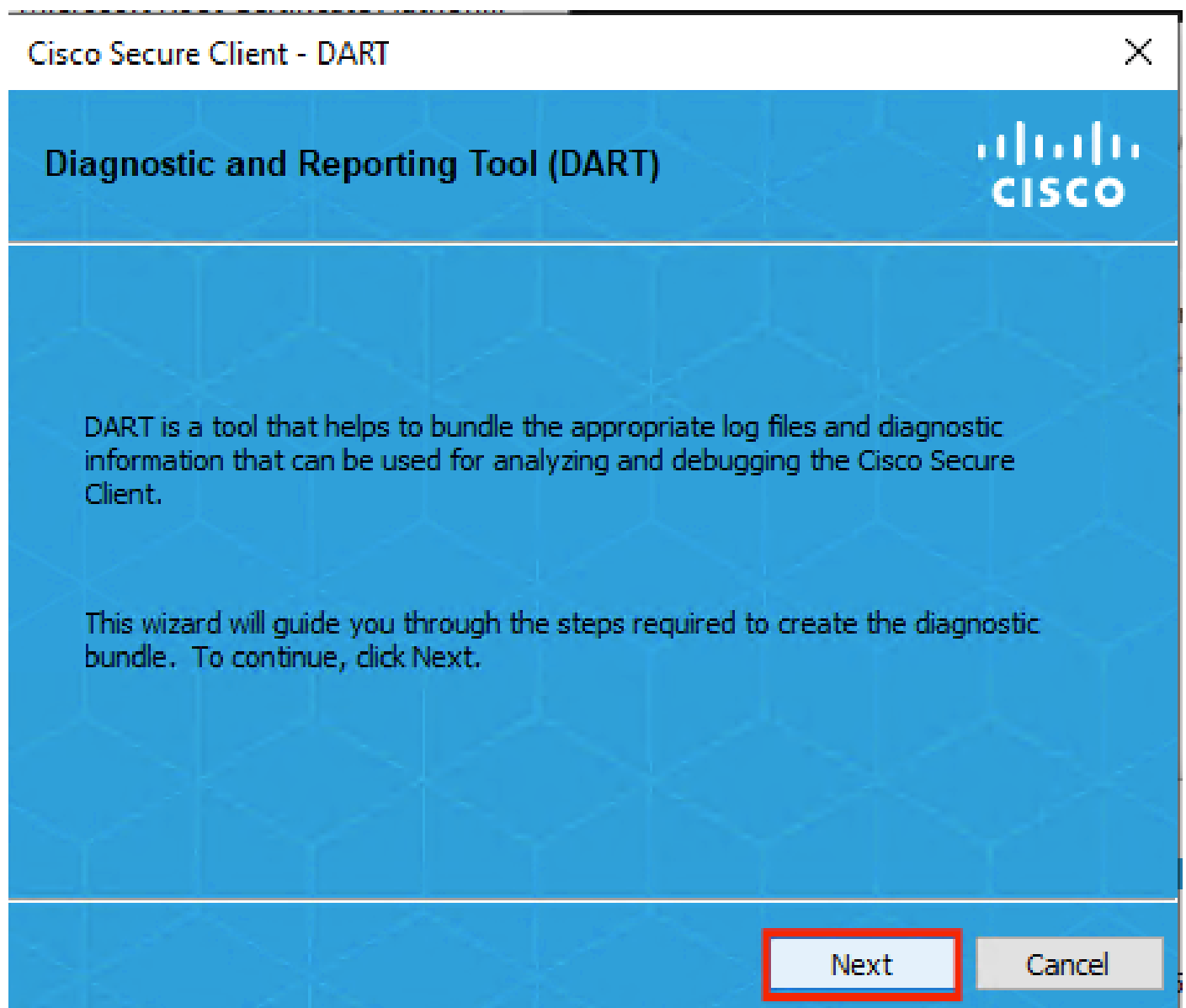
Cisco Secure Client Diagnostics and Reporting Tool

App

DART模組

在安裝過程中，您還安裝了此模組。它是在故障排除過程中透過收集日誌和相關dot1x會話資訊提供幫助的工具。

在第一個窗口中按一下Next。



DART模組

再次按一下Next，這樣日誌捆綁包才能儲存在案頭上。

Cisco Secure Client - DART



Bundle Creation Option



Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

☒ Default - Bundle will be saved to Desktop

☐ Custom



DART requires administrative privileges to clear Cisco Secure Client logs.

Clear All Logs

Back

Next

Cancel

DART模組

如有必要，請選中Enable Bundle Encryption覆取方塊。

Bundle Encryption Option



☐ Enable Bundle Encryption

☒ Mask Password

Encryption Password

Confirm Password

Back

Next

Cancel

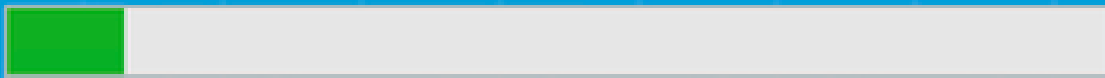
DART模組

DART日誌收集開始。

Bundle Creation Progress



Processing Application logs...




Finish

Cancel

DART日誌集合

此過程可能需要10分鐘或更長時間才能完成。

Bundle Creation Result




The bundle was created successfully in C:\Users\LAB5\Desktop\ DartBundle_0423_1538.zip.

Email Bundle

Finish

DART捆綁包建立結果

在案頭目錄中可找到DART結果檔案。

Name	Date modified	Type
 DartBundle_0423_1538	4/24/2024 1:14 PM	Compressed (zipped) Folder

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）。