802.1x WLAN + VLAN覆蓋，帶Mobility Express(ME)8.2和ISE 2.1

目錄

簡介

本檔案介紹如何使用Wi-Fi Protected Access 2(WPA2)Enterprise security(含Mobility Express控制器和外部遠端驗證撥入使用者服務(RADIUS)伺服器)設定WLAN（無線區域網路）。身份服務引擎(ISE)用作外部RADIUS伺服器的示例。

本指南中使用的可擴展身份驗證協定(EAP)是受保護的可擴展身份驗證協定(PEAP)。 此外，使用者端會指派給特定的VLAN（除了指派給WLAN的任何預設值這個VLAN）。

必要條件

需求

思科建議您瞭解以下主題：

- 802.1x
- PEAP
- 證書頒發機構(CA)
- 憑證

採用元件

本文中的資訊係根據以下軟體和硬體版本：

ME v8.2

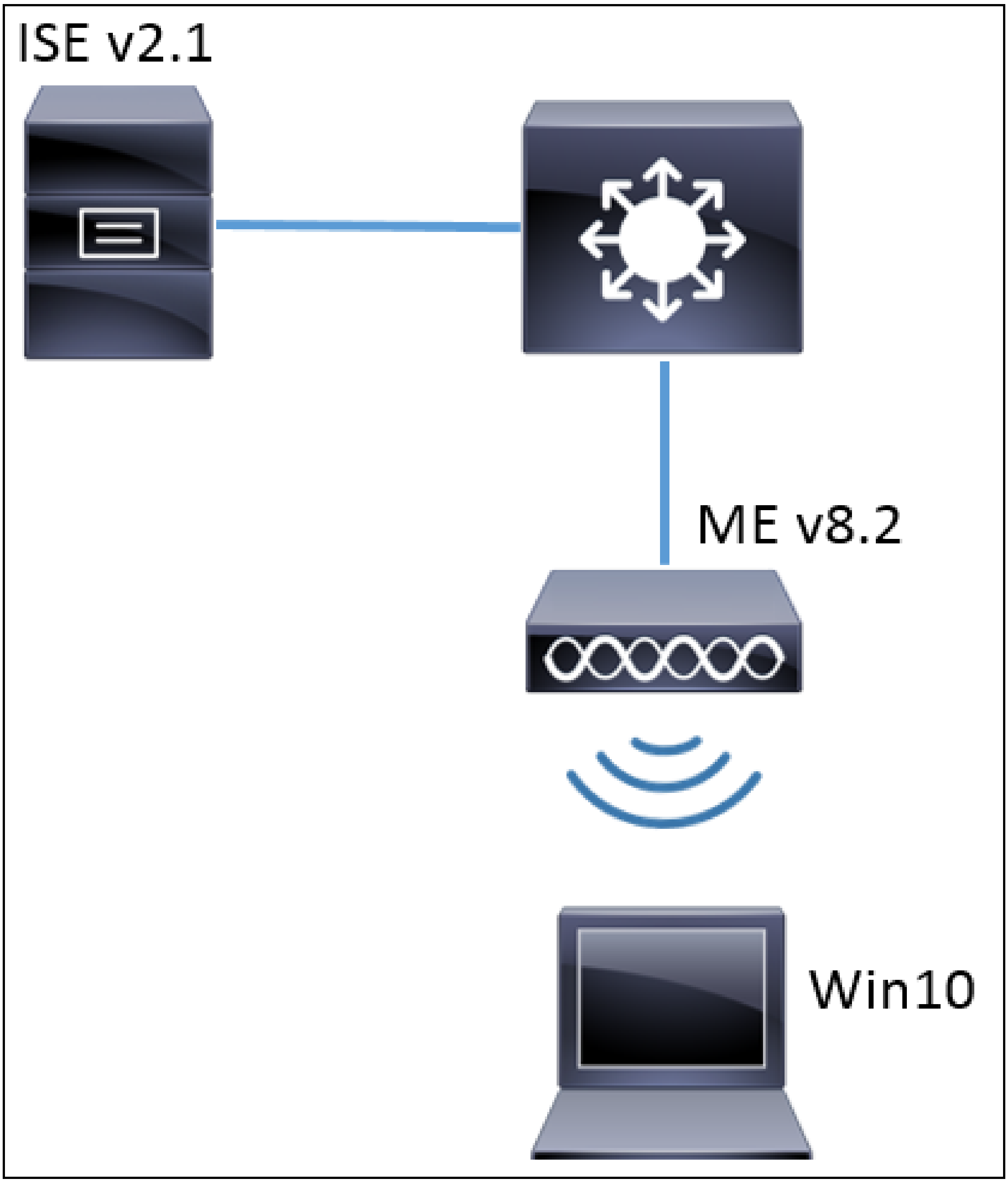
ISE v2.1

Windows 10筆記型電腦

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

網路圖表



組態

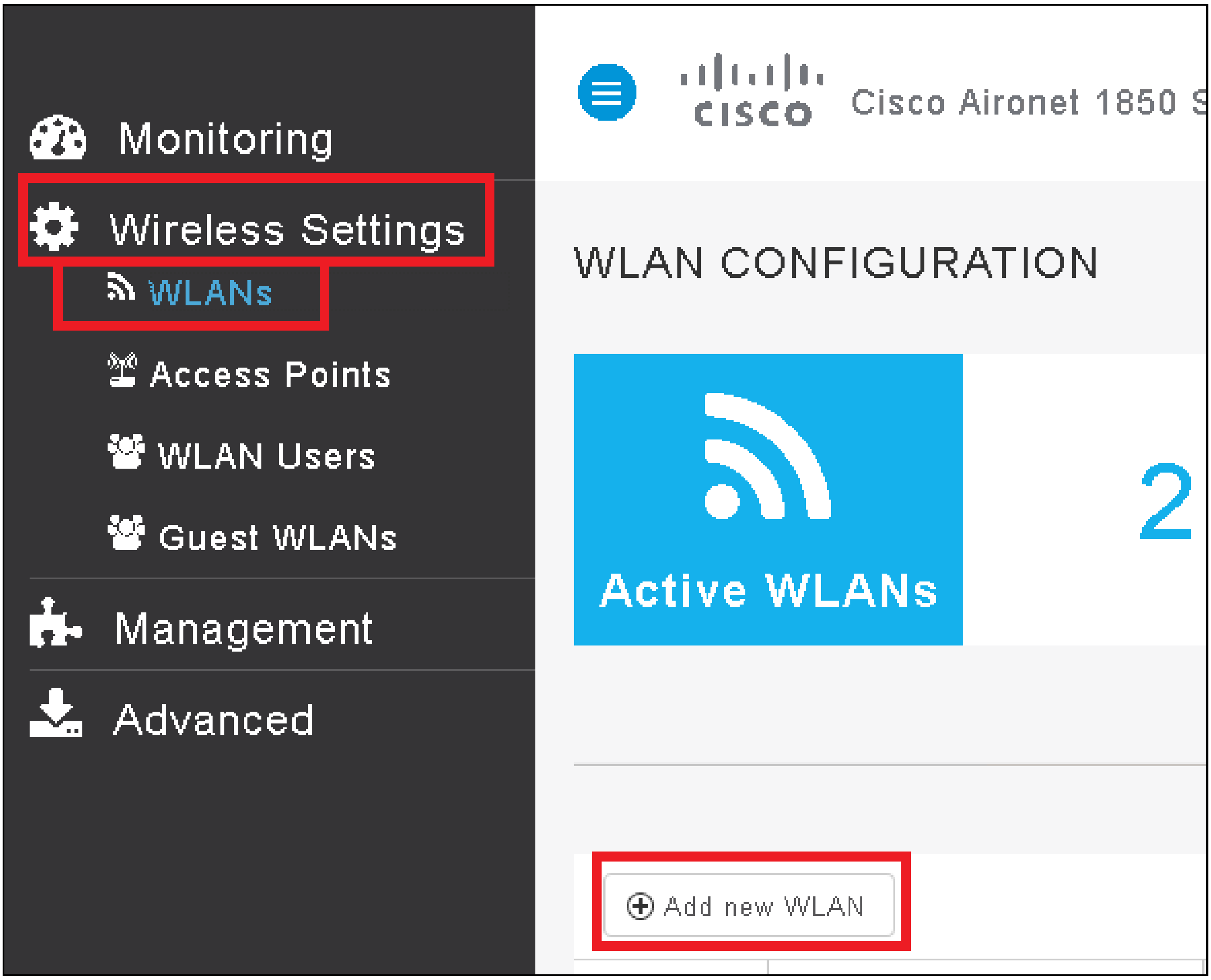
一般步驟如下：

1. 在ME中建立服務集識別符號(SSID)，並在ME上宣告RADIUS伺服器（本示例中的ISE）
2. 在RADIUS伺服器(ISE)上宣告ME
3. 在ISE上建立身份驗證規則
4. 在ISE上建立授權規則
5. 配置終端

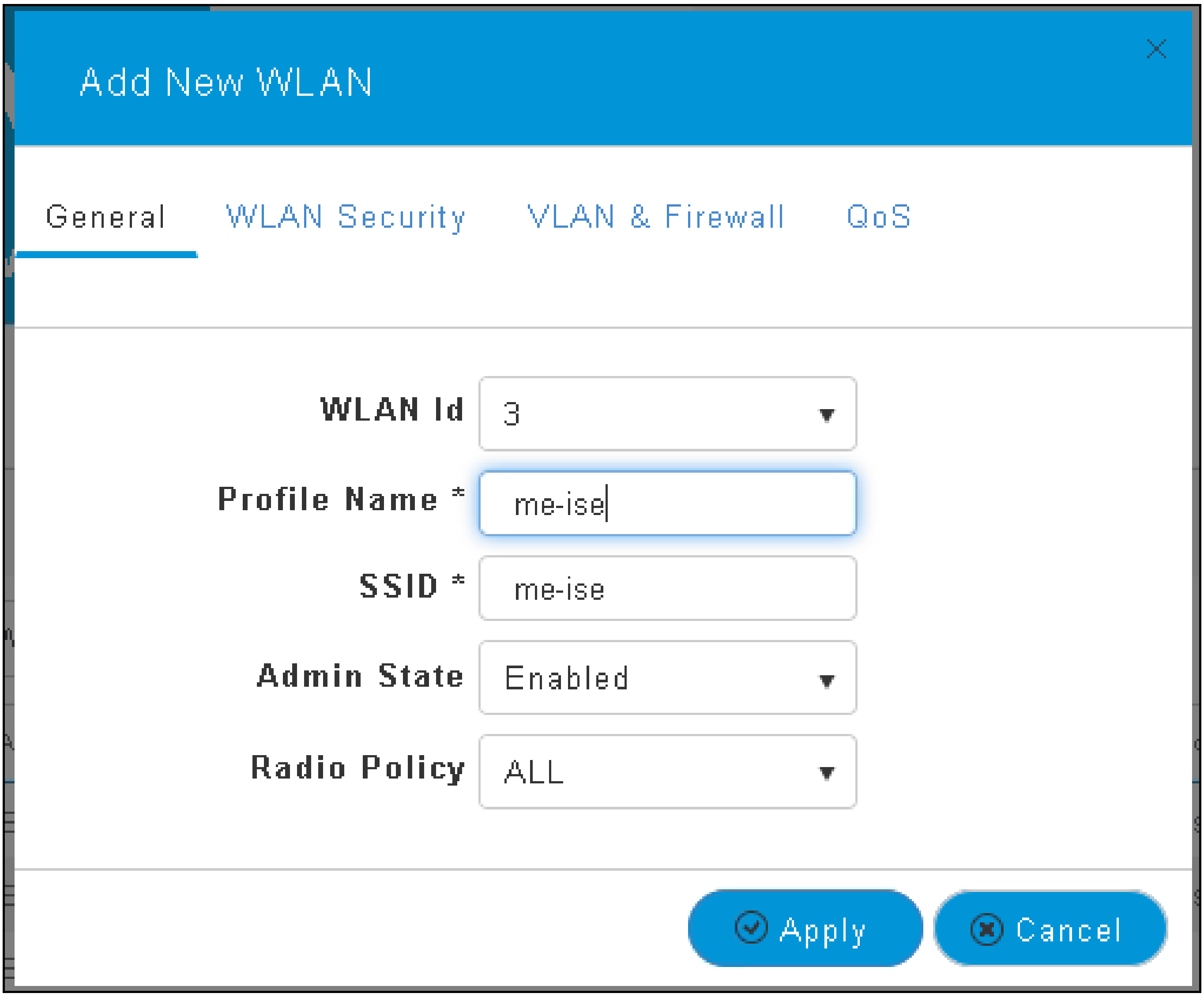
ME上的配置

若要允許RADIUS伺服器和ME之間的通訊，需要在ME上註冊RADIUS伺服器，反之亦然。此步驟顯示如何在ME上註冊RADIUS伺服器。

步驟1.開啟ME的GUI並導航至 **Wireless Settings > WLANs > Add new WLAN。**



步驟2.選擇WLAN的名稱。



Add New WLAN

WLAN Id: 3

Profile Name *: me-ise

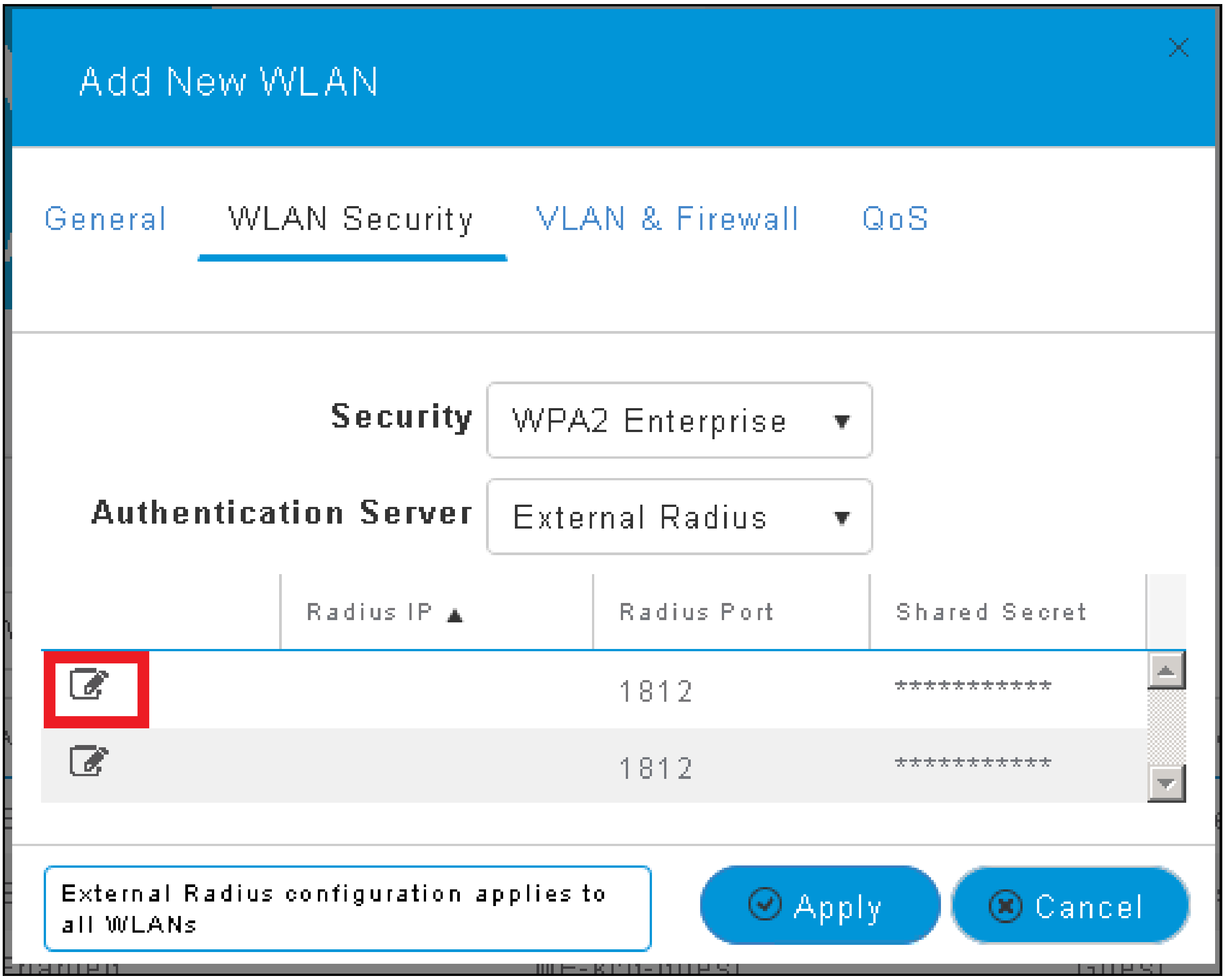
SSID *: me-ise

Admin State: Enabled

Radio Policy: ALL

步驟3.在**WLAN Security**頁籤下指定**安全配置**。

選擇**WPA2 Enterprise**，對於Authentication server選擇**External RADIUS**。按一下編輯選項以新增RADIUS的IP地址並選擇共**享密鑰**。

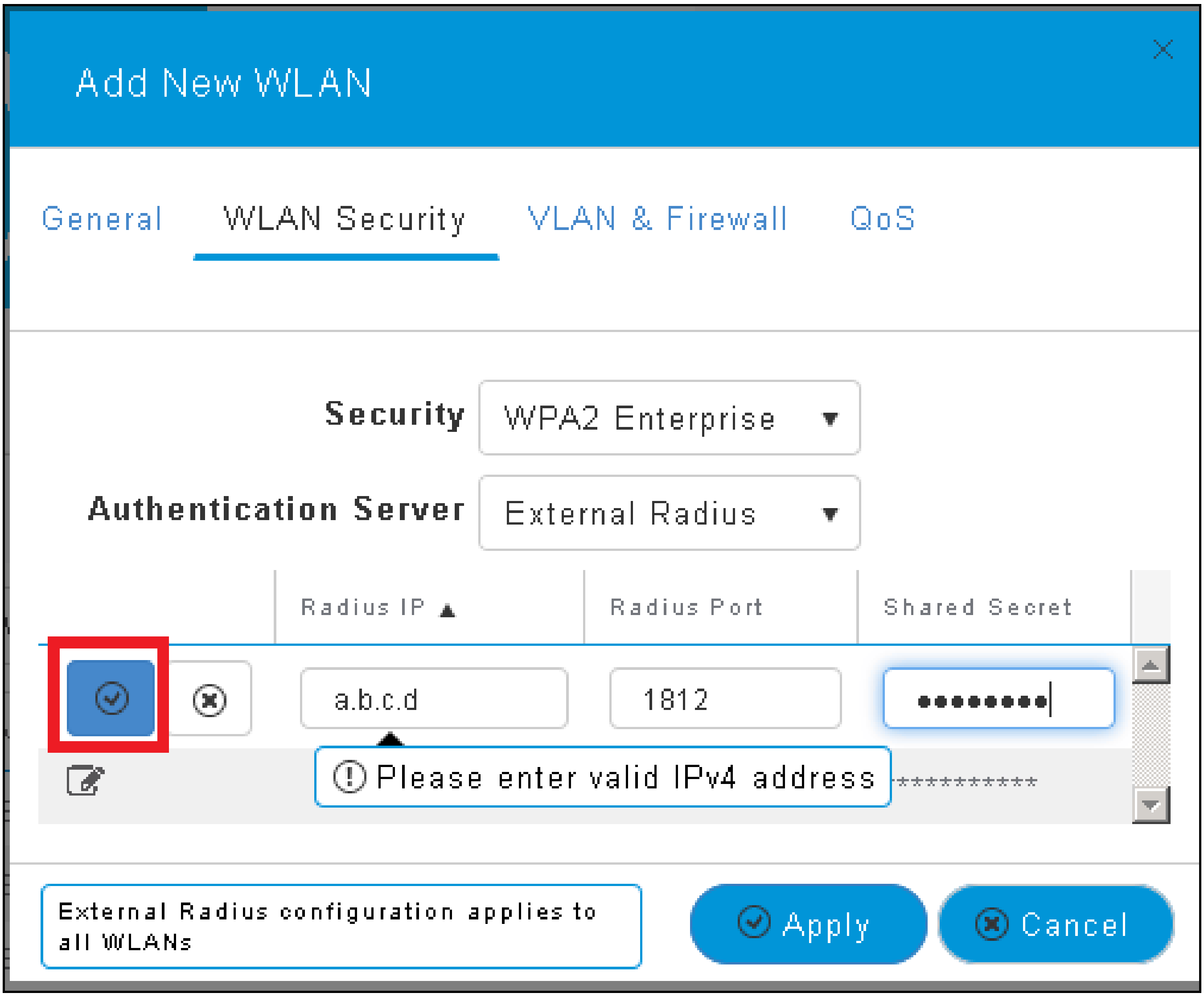


Security WPA2 Enterprise ▾

Authentication Server External Radius ▾

	Radius IP ▲	Radius Port	Shared Secret
✎		1812	************
✎		1812	************

External Radius configuration applies to all WLANs



Security: WPA2 Enterprise

Authentication Server: External Radius

	Radius IP ▲	Radius Port	Shared Secret
	a.b.c.d	1812	●●●●●●●●●
			***********

Please enter valid IPv4 address

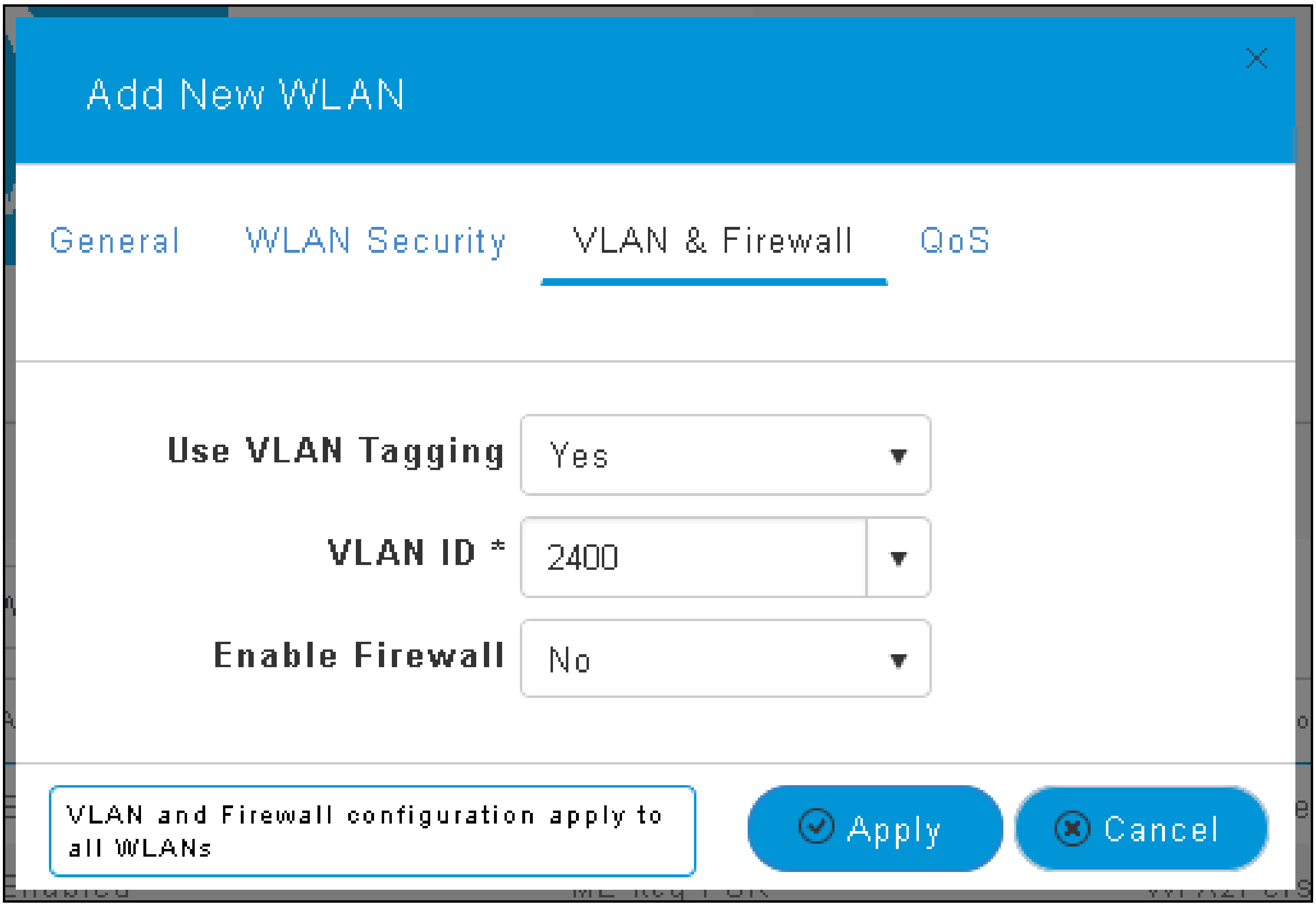
External Radius configuration applies to all WLANs

<a.b.c.d>對應於RADIUS伺服器。

步驟4.為SSID分配VLAN。

如果需要將SSID分配給AP的VLAN，則可以跳過此步驟。

要將此SSID的使用者分配給特定VLAN（AP的VLAN除外），請啟用**Use VLAN Tagging**並分配所需的**VLAN ID**。



Use VLAN Tagging: Yes

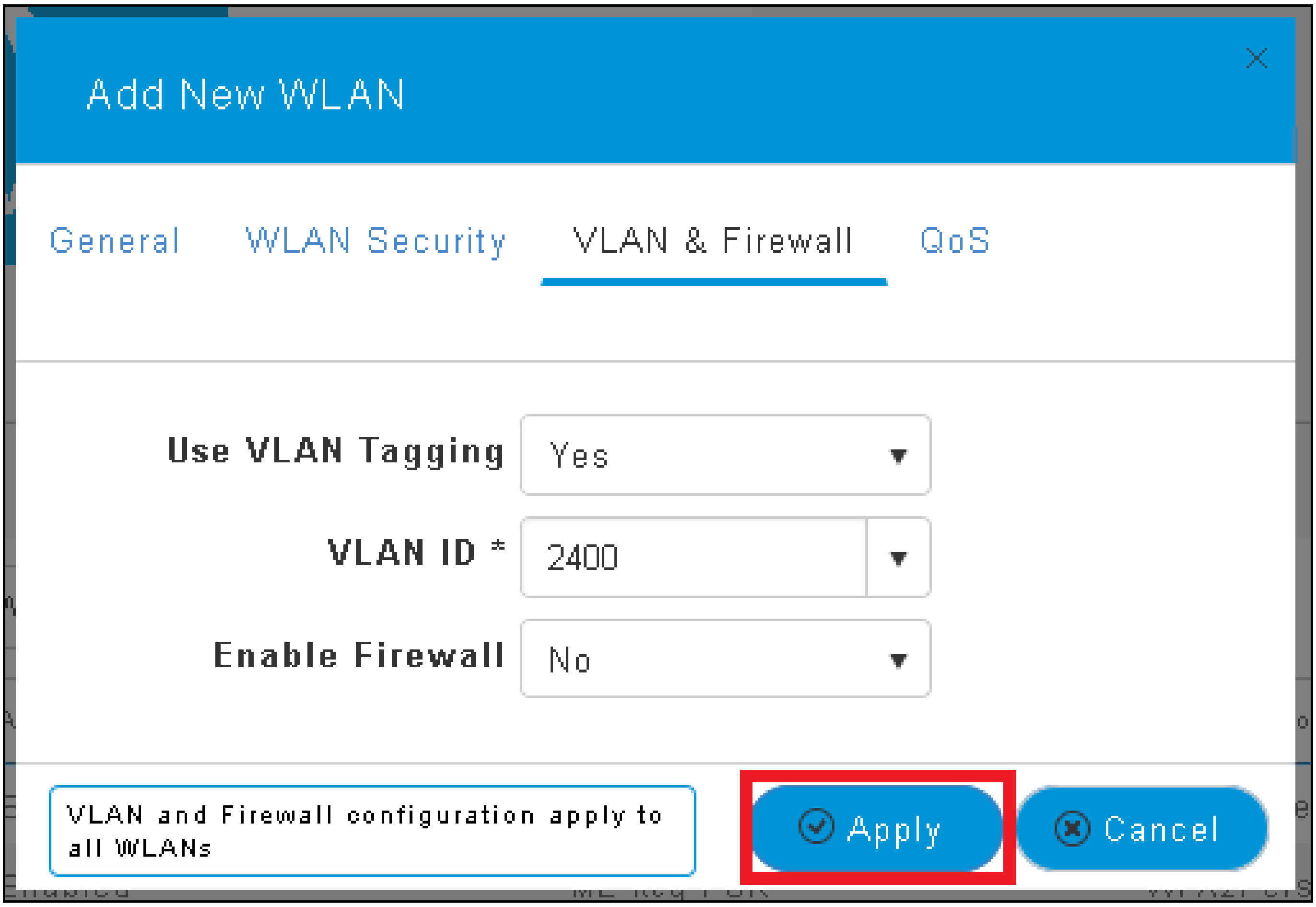
VLAN ID *: 2400

Enable Firewall: No

VLAN and Firewall configuration apply to all WLANs

附註：如果使用VLAN標籤，請確保將接入點所連線的switchport配置為中繼埠，並將AP VLAN配置為本徵。

步驟5.按一下**Apply** 以完成設定。



Add New WLAN

Use VLAN Tagging: Yes

VLAN ID *: 2400

Enable Firewall: No

VLAN and Firewall configuration apply to all WLANs

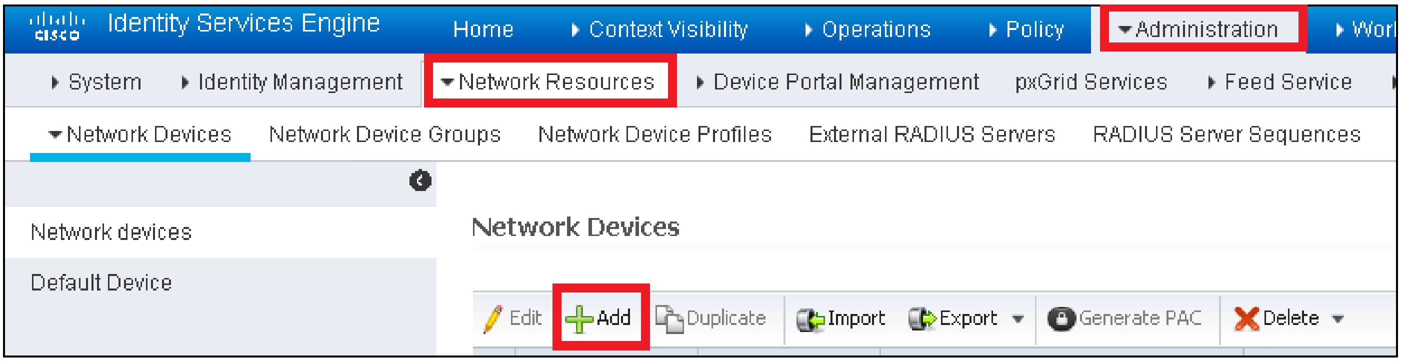
步驟6.可選，將WLAN配置為接受VLAN覆蓋。

在WLAN上啟用AAA覆寫，並新增所需的VLAN。為此，您需要開啟ME管理介面的CLI會話並發出以下命令：

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

在ISE上宣告我

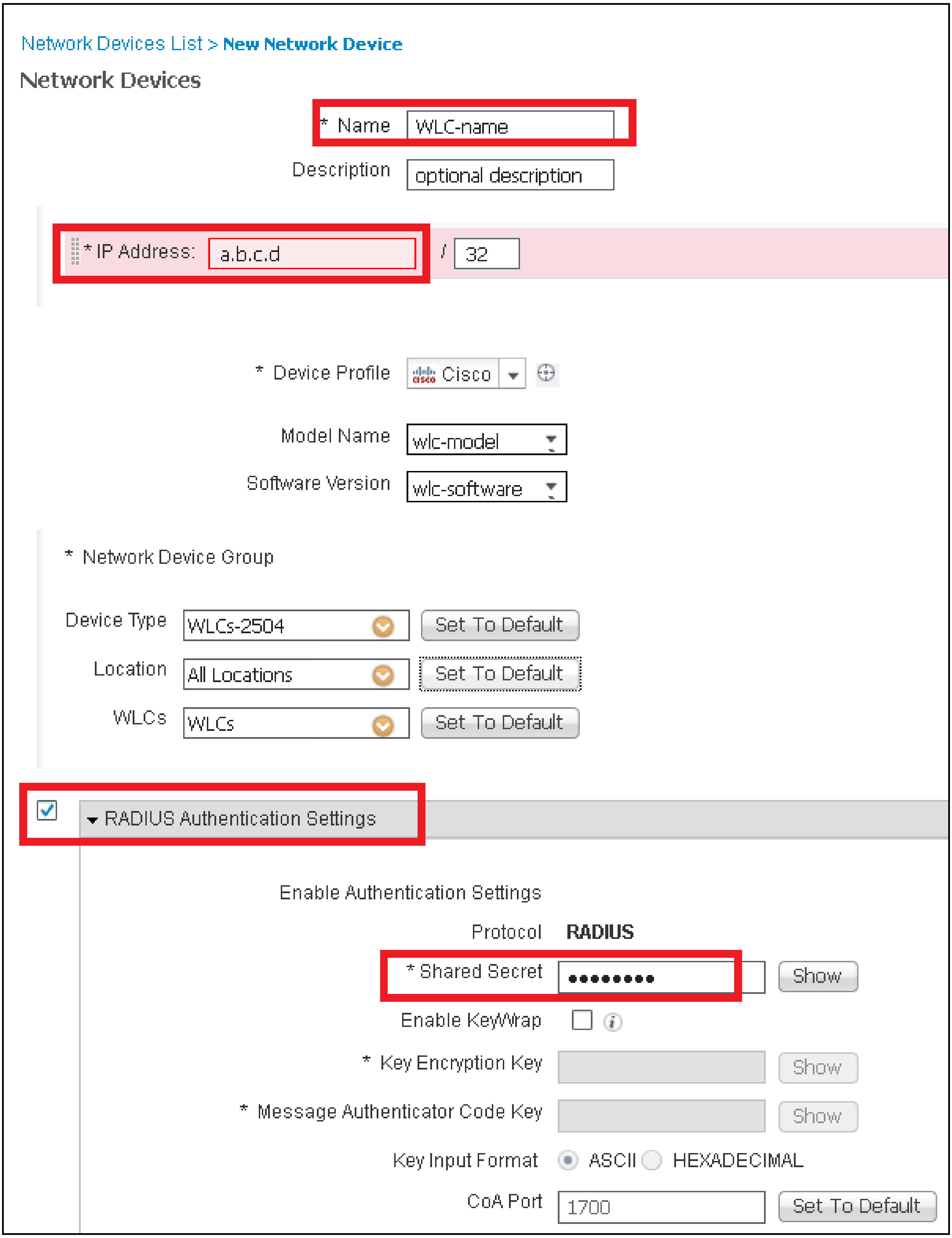
步驟1.開啟ISE控制檯並導航到**管理>網路資源>網路裝置>新增。**



步驟2.輸入資訊。

或者，可以指定型號名稱、軟體版本、說明並根據裝置型別、位置或WLC分配網路裝置組。

a.b.c.d對應於ME的IP地址。



Network Devices List > **New Network Device**

Network Devices

* Name: WLC-name

Description: optional description

* IP Address: a.b.c.d / 32

* Device Profile: Cisco

Model Name: wlc-model

Software Version: wlc-software

* Network Device Group

Device Type: WLCs-2504 — Set To Default

Location: All Locations — Set To Default

WLCs: WLCs — Set To Default

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ●●●●●●●●● Show

Enable KeyWrap: □

* Key Encryption Key: Show

* Message Authenticator Code Key: Show

Key Input Format: ● ASCII ○ HEXADECIMAL

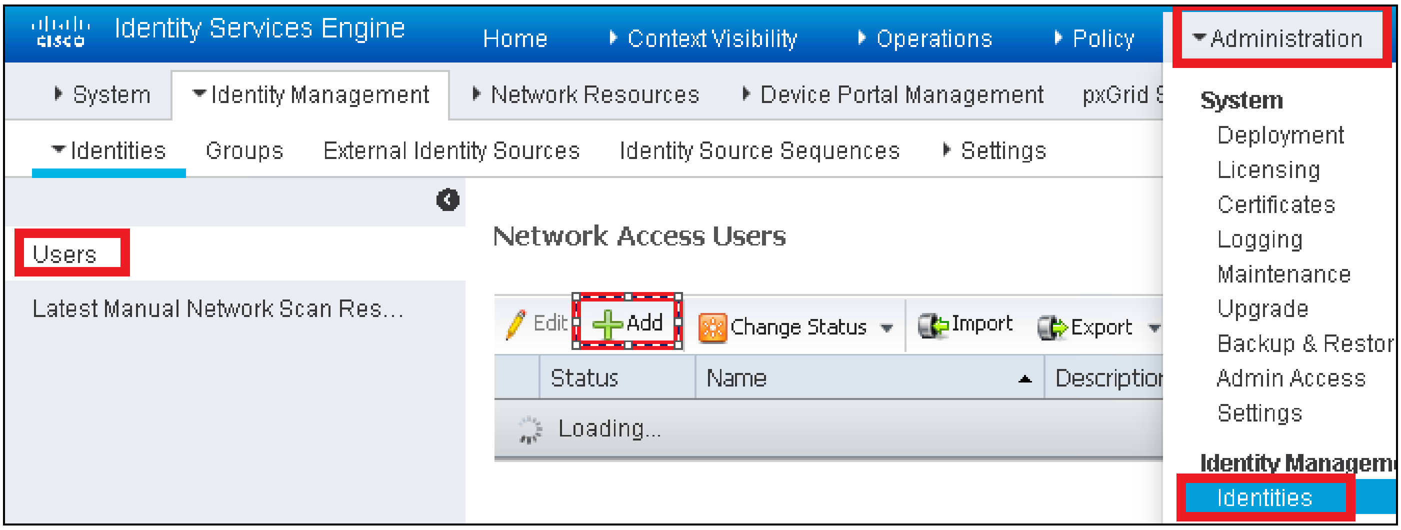
CoA Port: 1700 — Set To Default

有關網路裝置組的詳細資訊，請檢視此連結：

ISE – 網路裝置群組

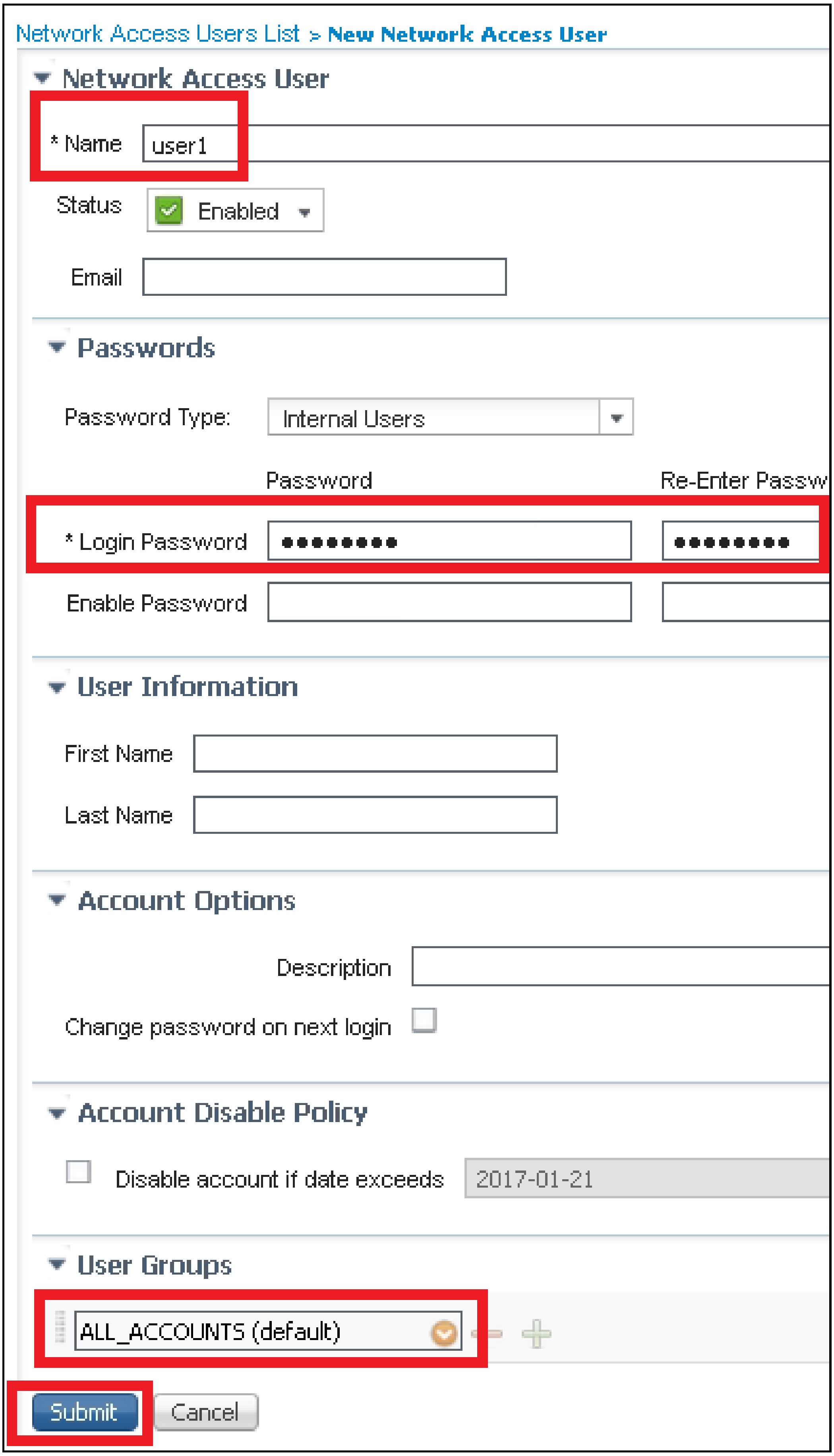
在ISE上建立新使用者

步驟1.導航至 **管理>身份管理>身份>使用者>新增。**



步驟2.輸入資訊。

在此示例中，此使用者屬於名為ALL_ACCOUNTS的組，但可以根據需要對其進行調整。



Network Access Users List > **New Network Access User**

Network Access User

* Name: user1

Status: ✓ Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Passw
* Login Password	●●●●●●●●●	●●●●●●●●●
Enable Password		

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

Account Disable Policy

□ Disable account if date exceeds 2017-01-21

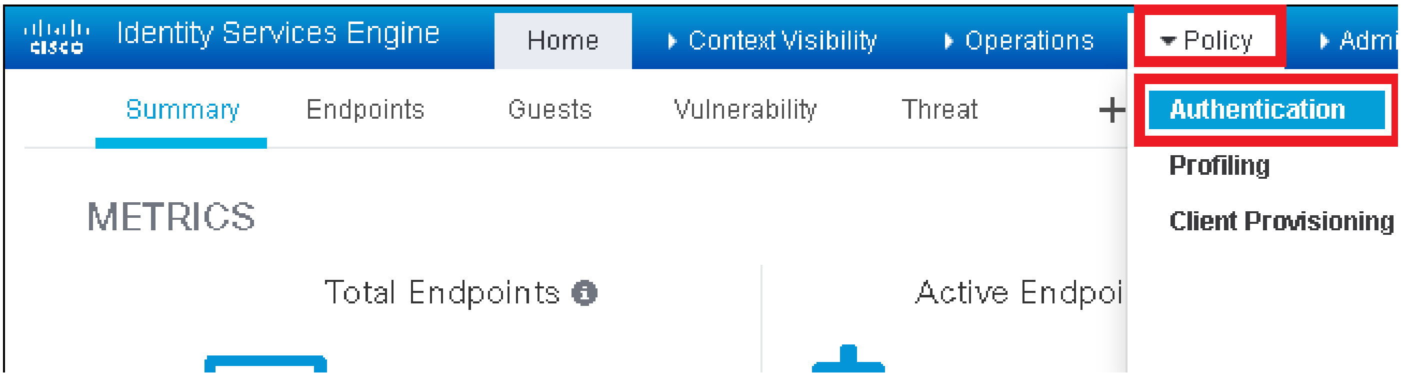
User Groups

ALL_ACCOUNTS (default)

建立身份驗證規則

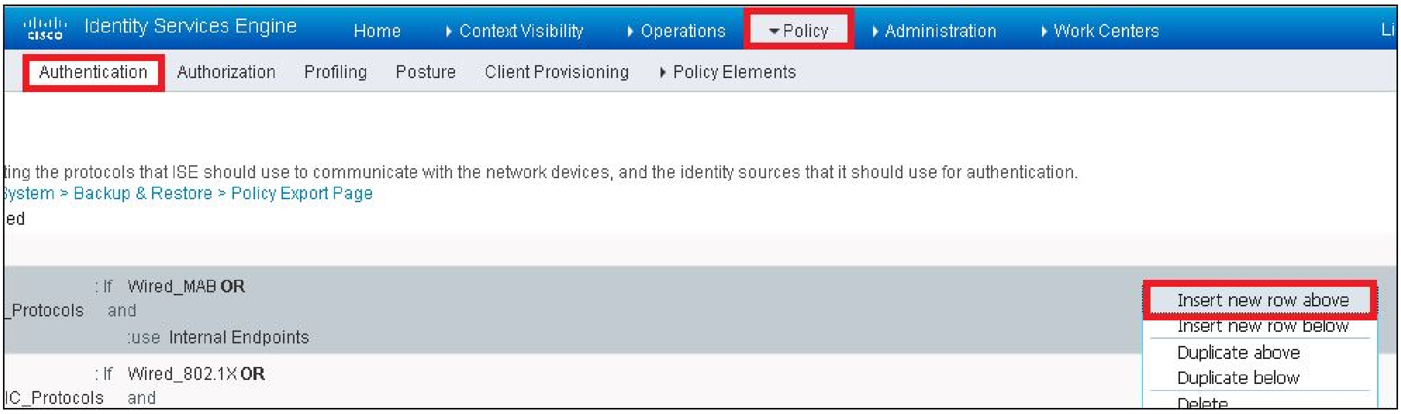
驗證規則用於驗證使用者的憑證是否正確（驗證使用者是否真正是其所言者）並限制允許其使用的驗證方法。

步驟1. 導覽 到**Policy > Authentication**。



步驟2.插入新的身份驗證規則。

為此，請導航至**Policy > Authentication > Insert new row above/below**。



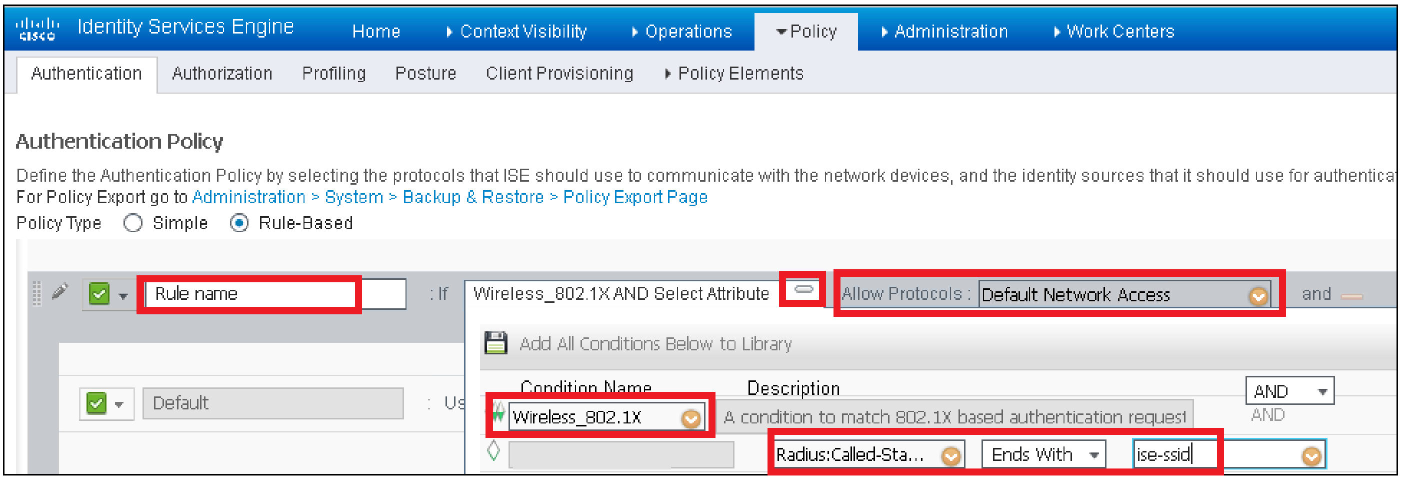
ing the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
ystem > Backup & Restore > Policy Export Page
ed

: If Wired_MAB **OR**
_Protocols and
:use Internal Endpoints

: If Wired_802.1X **OR**
IC_Protocols and

步驟3.輸入所需資訊

此身份驗證規則示例允許在**Default Network Access**清單中列出的所有協定，這適用於無線802.1x客戶端的身份驗證請求（使用Called-Station-ID），並以*ise-ssid*結尾。



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentica
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page
Policy Type ○ Simple ● Rule-Based

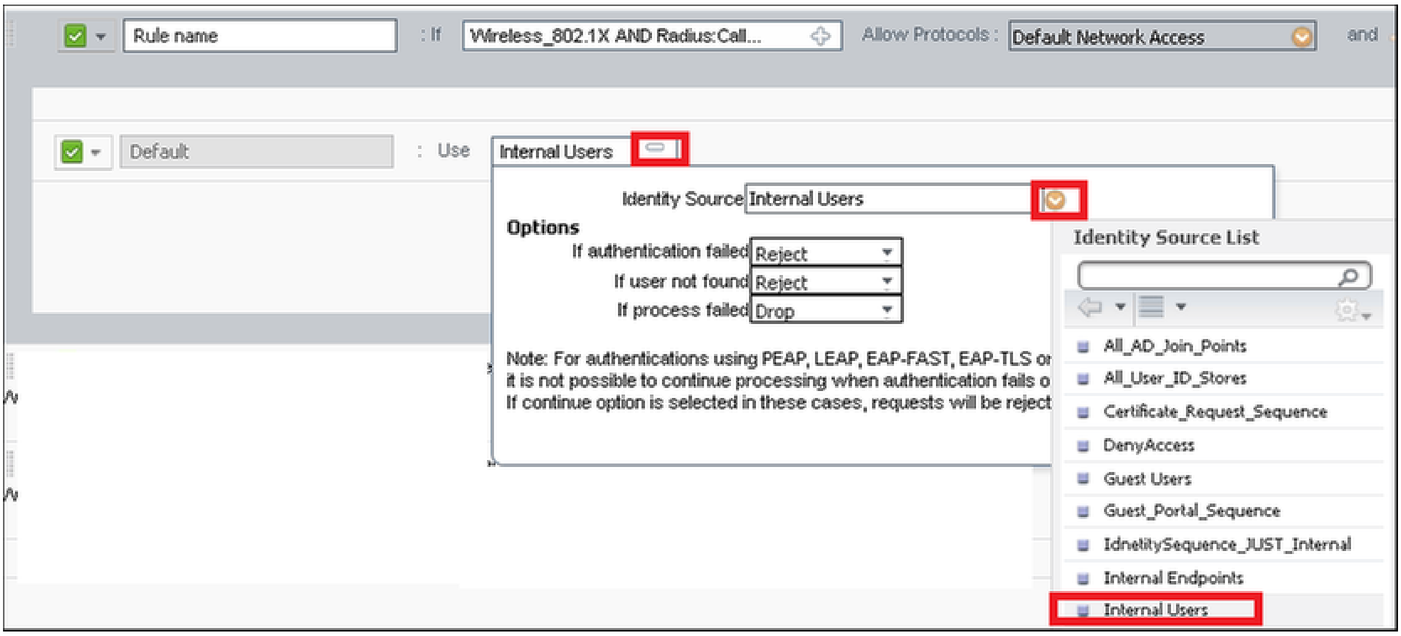
☑ Rule name : If Wireless_802.1X AND Select Attribute Allow Protocols : Default Network Access and

Wireless_802.1X A condition to match 802.1X based authentication request AND

Radius:Called-Sta... Ends With ise-ssid AND

☑ Default : Us

此外，為與此身份驗證規則匹配的客戶端選擇身份源，在本例中將該身份源用於*內部使用者*



Rule name : If Wireless_802.1X AND Radius:Call... Allow Protocols : Default Network Access and

Default : Use Internal Users

Identity Source Internal Users

Options

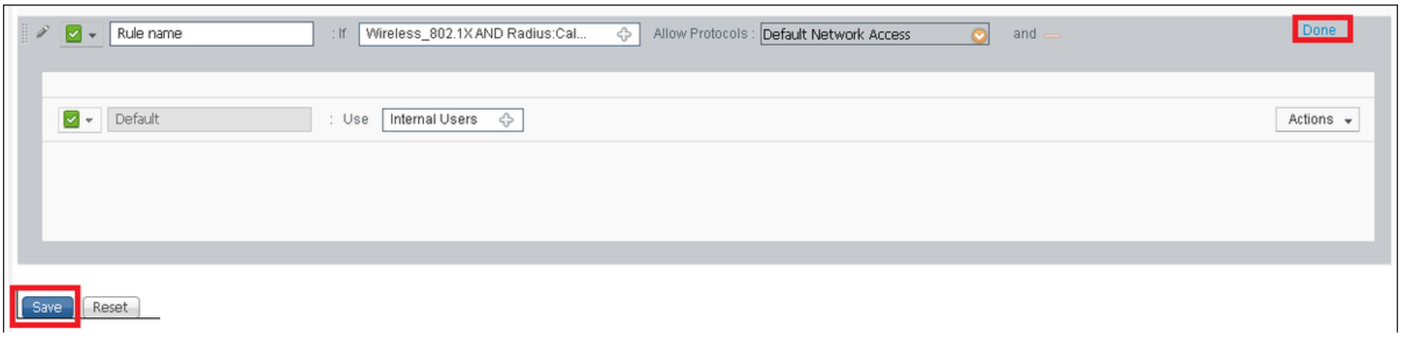
If authentication failed Reject

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or
it is not possible to continue processing when authentication fails o
If continue option is selected in these cases, requests will be reject

完成後，按一下Done和Save



Rule name : If Wireless_802.1X AND Radius:Cal... Allow Protocols : Default Network Access and

Default : Use Internal Users

有關「允許協定策略」的詳細資訊，請參閱以下連結：

[允許的協定服務]

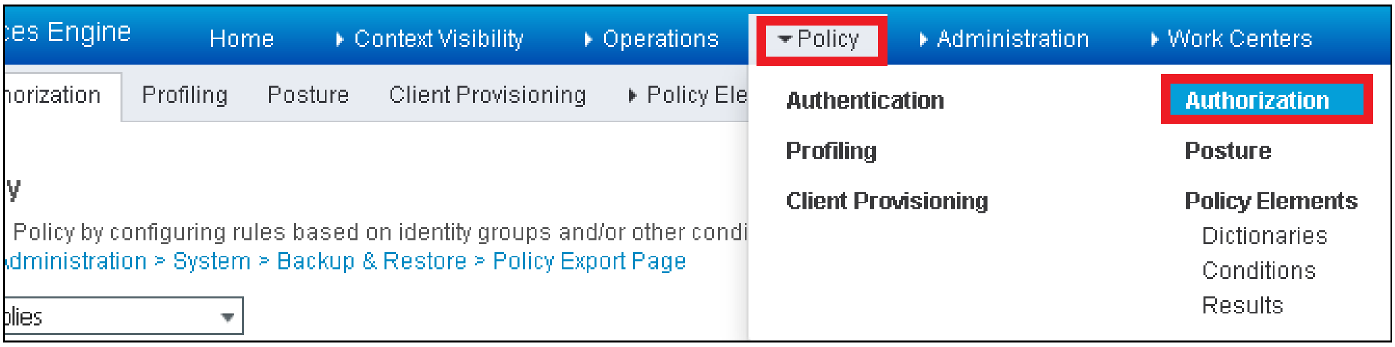
有關身份源的詳細資訊，請查閱以下連結：

[建立使用者身份組]

建立授權規則

授權規則是負責確定是否允許客戶端加入網路的規則

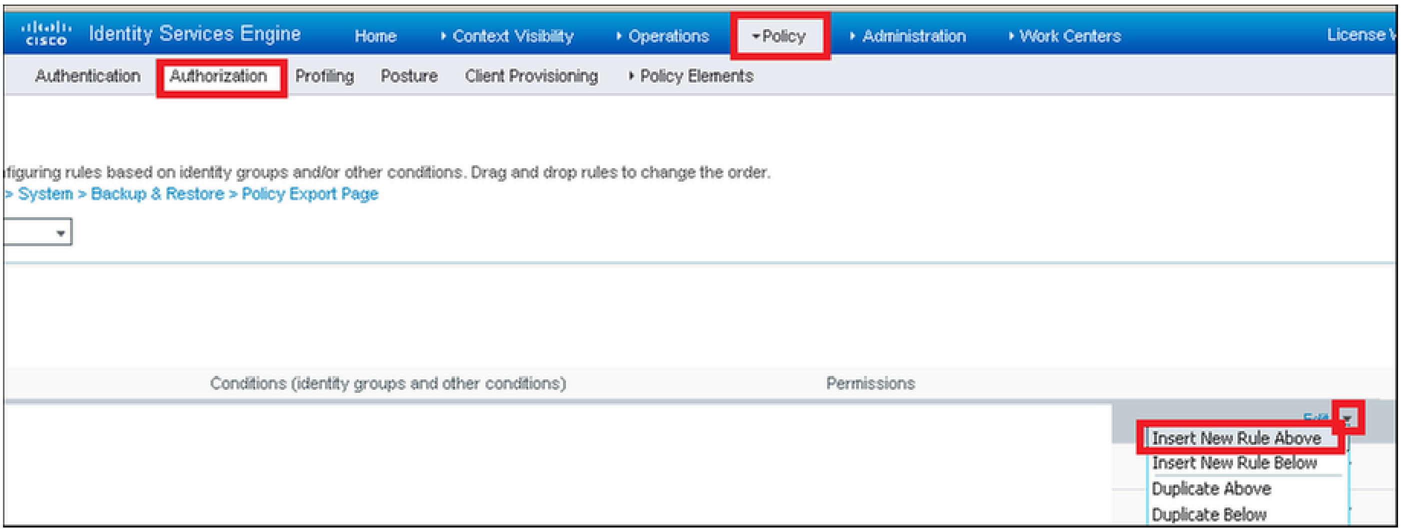
步驟1。導覽至Policy > Authorization。



y

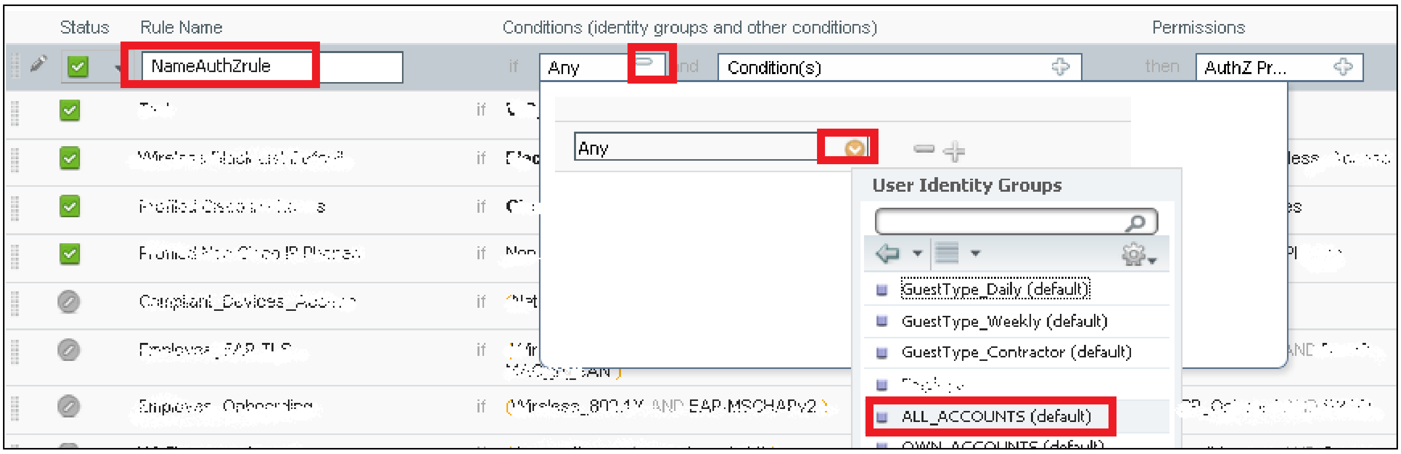
Policy by configuring rules based on identity groups and/or other condi
dministration > System > Backup & Restore > Policy Export Page

步驟2.插入新規則。導航到**Policy > Authorization > Insert New Rule Above/Below**。



步驟3.輸入資訊。

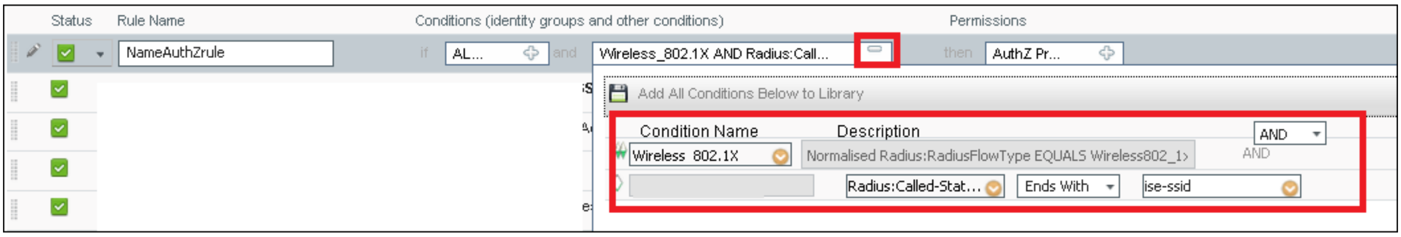
首先為規則以及儲存使用者的身份組選擇一個名稱。在本示例中，使用者儲存在*組 ALL_ACCOUNTS中*。



Rule Name: NameAuthZrule

Any

然後，選擇其他條件，使授權過程符合此規則。在本示例中，如果授權進程使用802.1x無線，並且稱為站ID以*ise-ssid結束，則授權進程會到達此規則。*

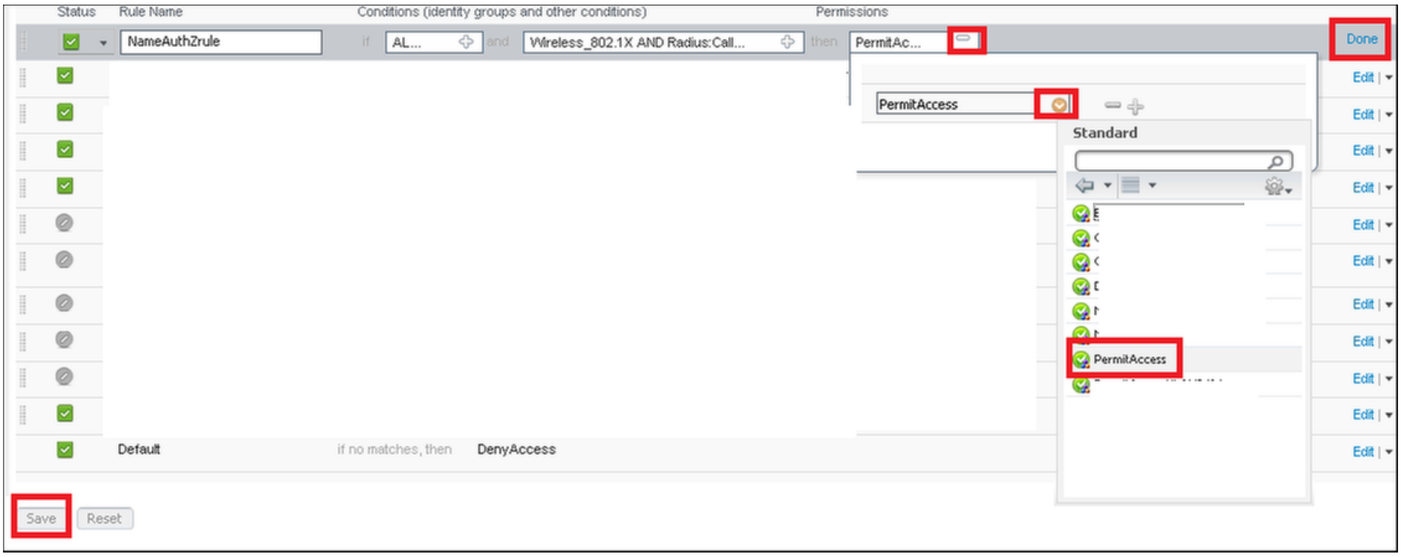

Status
Rule Name
Conditions (identity groups and other conditions)
Permissions
if
and
then
AL...
AuthZ Pr...
Add All Conditions Below to Library
Condition Name
Description
AND

NameAuthZrule

Wireless_802.1X AND Radius:Call...

Condition Name	Description	
Wireless_802.1X	Normalised Radius:RadiusFlowType EQUALS Wireless802_1x	AND
	Radius:Called-Stat... Ends With ise-ssid	

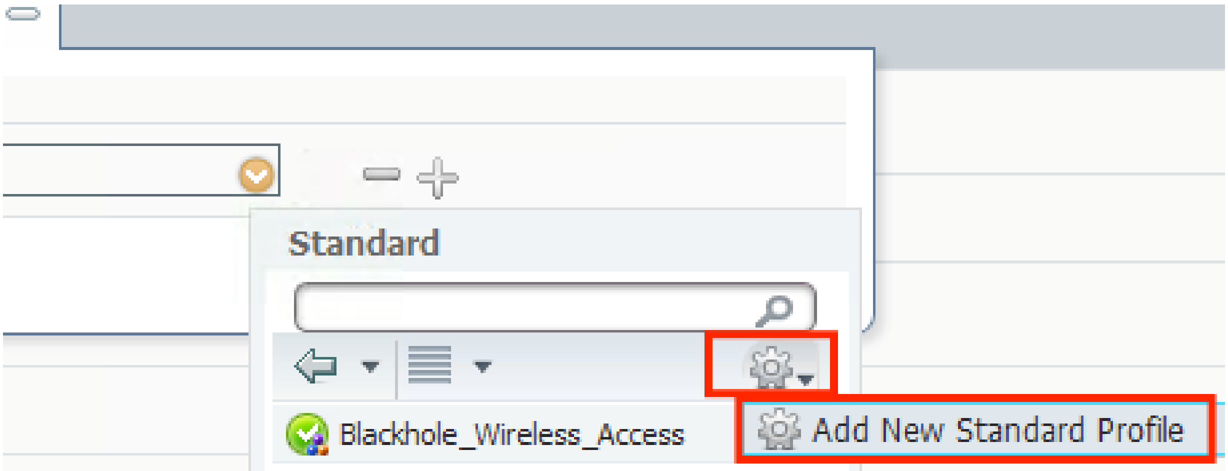
最後，選擇允許客戶端加入網路的授權配置檔案，按一下**完成**並儲存。



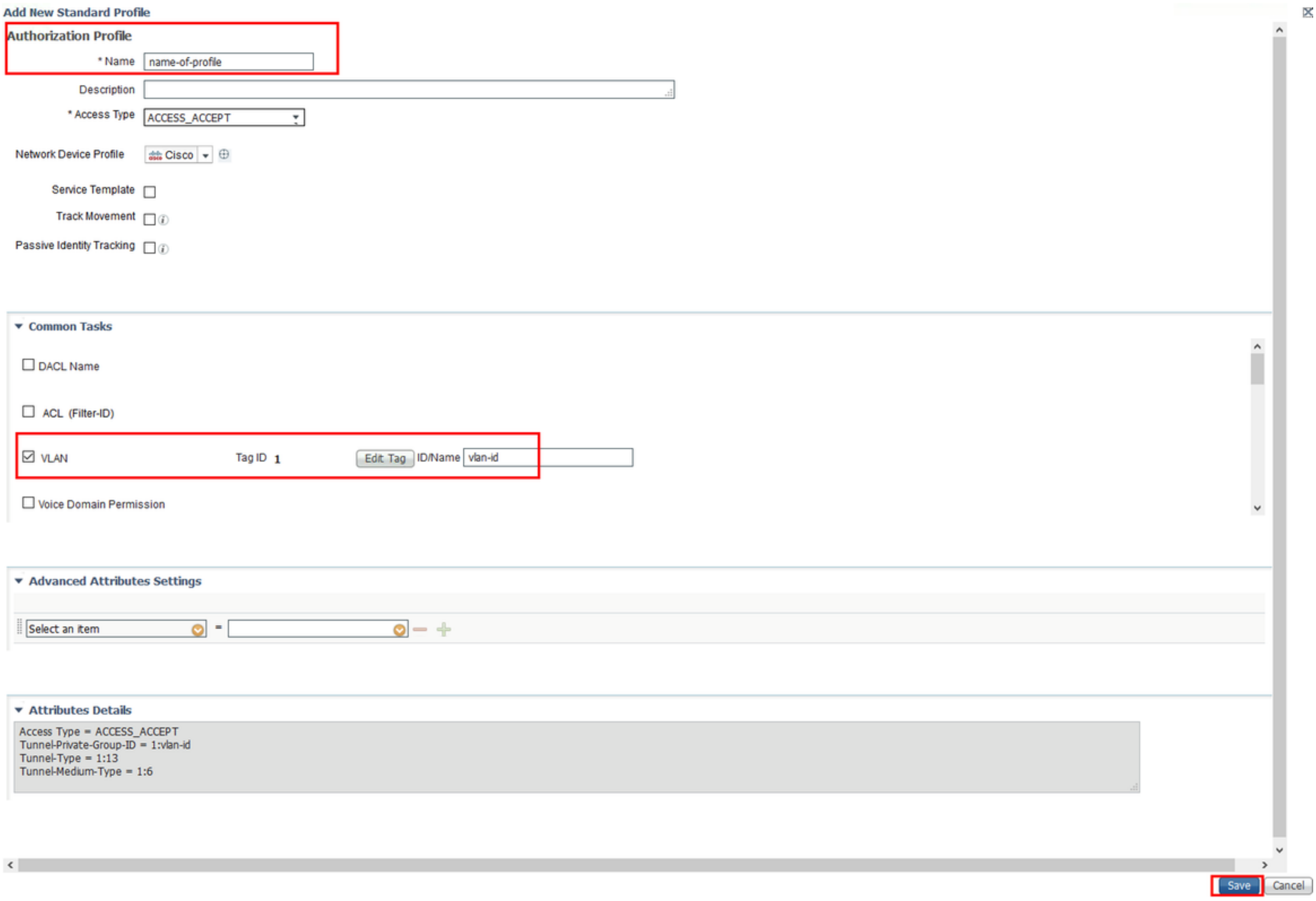
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
☑	NameAuthZrule	if AL... and Wireless_802.1X AND Radius:Call...	then PermitAc...
☑	Default	if no matches, then	DenyAccess

PermitAccess

或者，建立新的授權配置檔案，將無線客戶端分配到不同的VLAN:



輸入以下資訊：



Authorization Profile

* Name: name-of-profile

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

□ DACL Name

□ ACL (Filter-ID)

☑ VLAN Tag ID 1 ID/Name vlan-id

□ Voice Domain Permission

Select an item =

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:vlan-id
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

終端裝置的配置

將Windows 10筆記型電腦配置為使用PEAP/MS-CHAPv2(Microsoft版本的質詢 — 握手身份驗證協定第2版)通過802.1x身份驗證連接到SSID。

在此配置示例中，ISE使用其自簽名證書執行身份驗證。

要在Windows電腦上建立WLAN配置檔案，有兩個選項：

1. 在電腦上安裝自簽名證書以驗證並信任ISE伺服器完成身份驗證
2. 繞過RADIUS伺服器的驗證，並信任任何用於執行驗證的RADIUS伺服器（不建議，因為這可能成為安全問題）

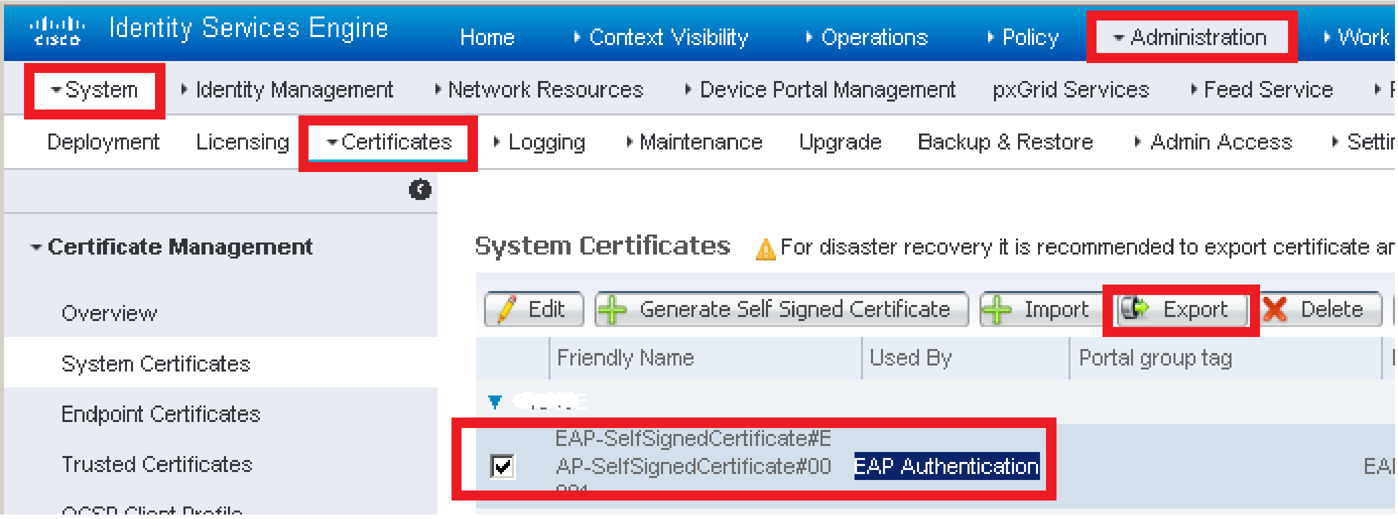
有關這些選項的配置，請參閱終端裝置配置 — 建立WLAN配置檔案 — 步驟7。

終端裝置配置 — 安裝ISE自簽名證書

步驟1.從ISE匯出自簽名證書。

登入到ISE並導航到**管理>系統>證書>系統證書**。

然後選擇用於**EAP身份驗證**的證書，然後按一下**匯出。**

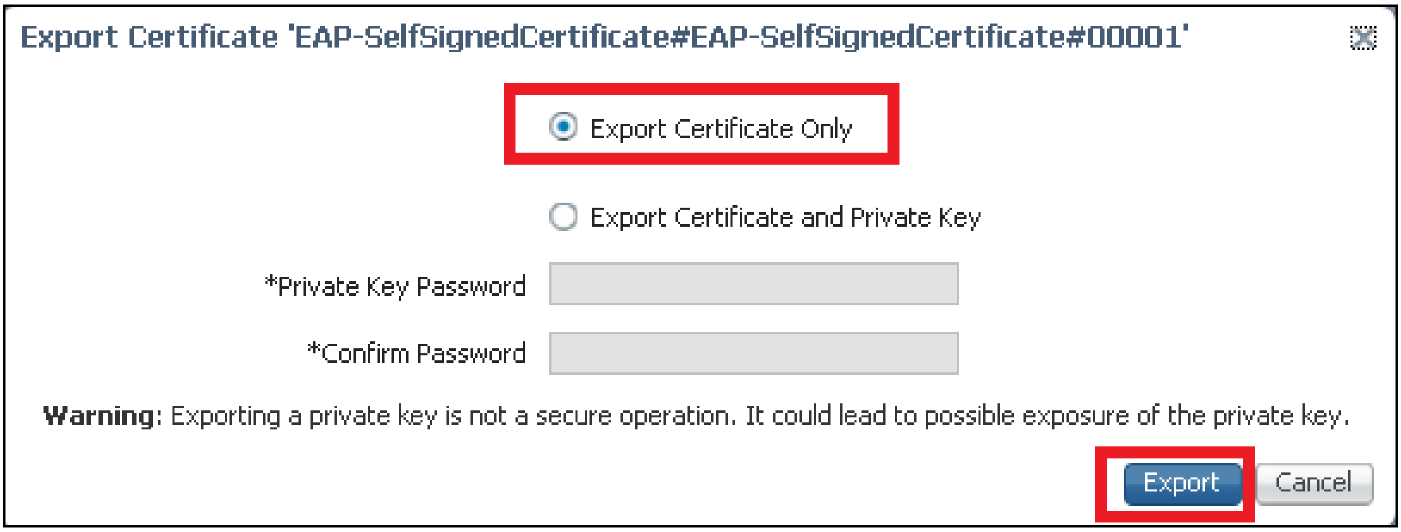


System Certificates

⚠ For disaster recovery it is recommended to export certificate ar

	Friendly Name	Used By	Portal group tag	
▼ [redacted]				
☑	EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001	EAP Authentication		EAI

將證書儲存到所需位置。此證書安裝在Windows電腦上。



Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'

● Export Certificate Only

○ Export Certificate and Private Key

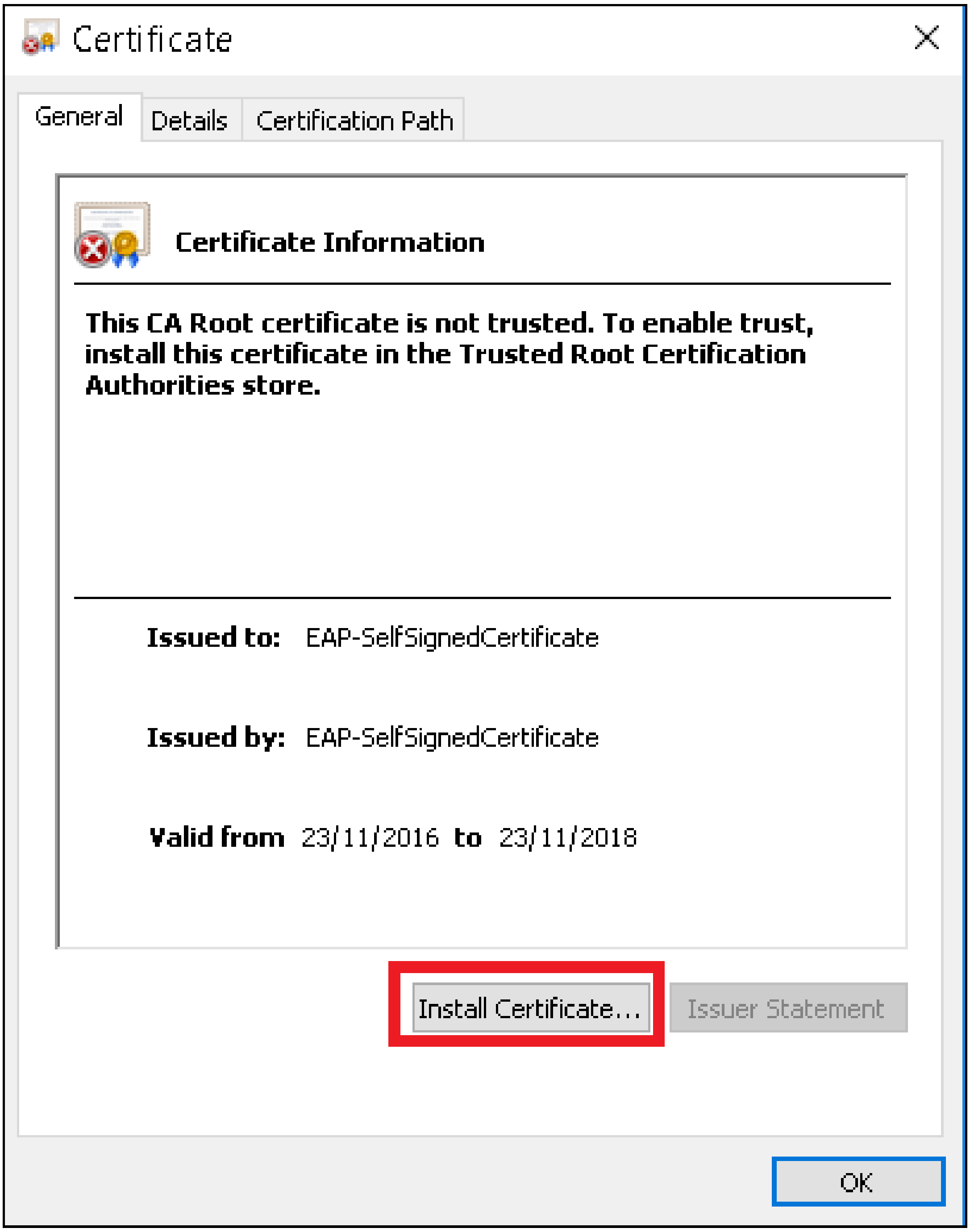
*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

步驟2.在Windows電腦上安裝證書。

將之前匯出的證書複製到Windows電腦，將檔案的副檔名從.pem更改為.crt，然後按兩下該檔案並選擇**安裝證書**.......



Certificate Information

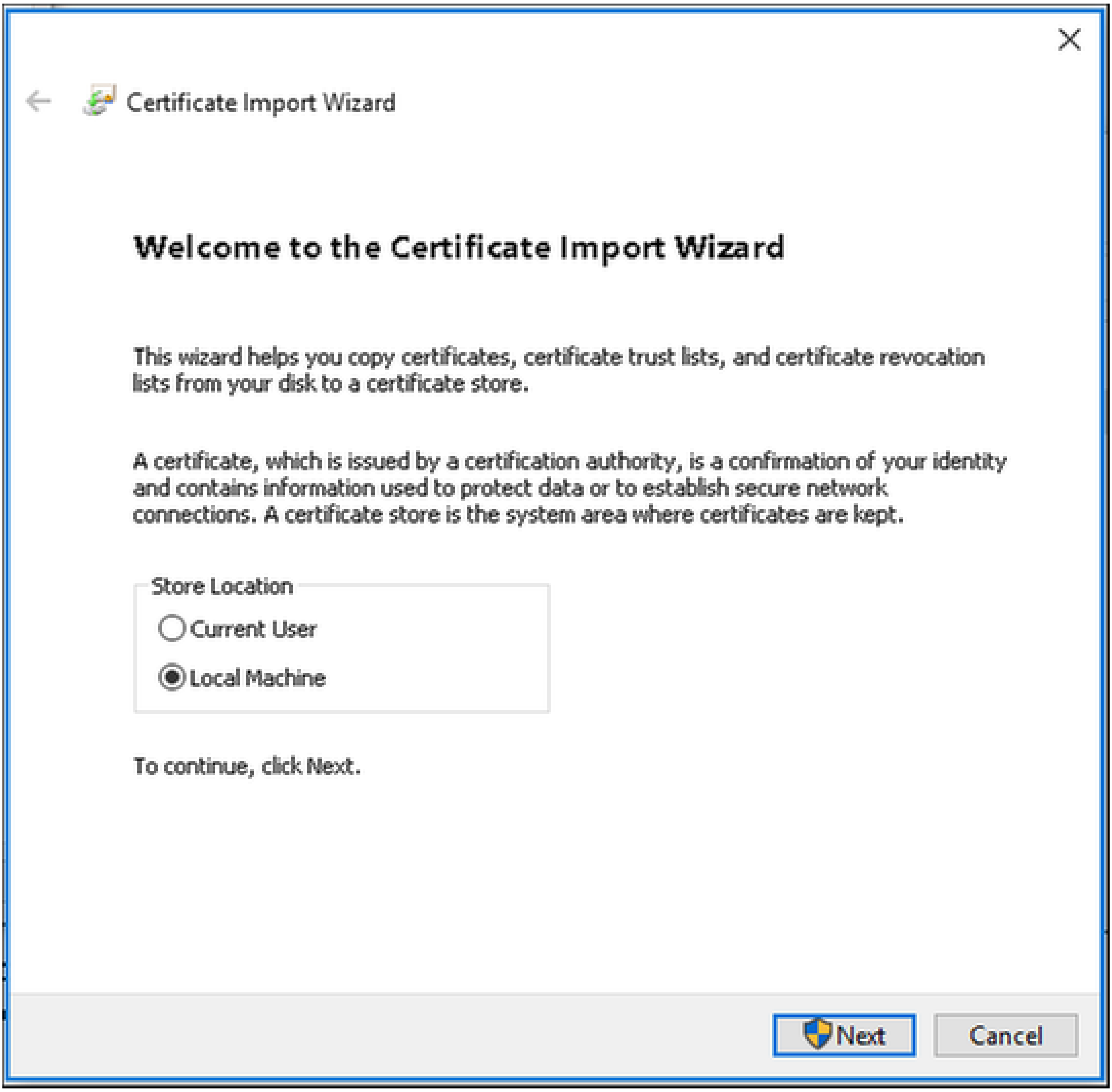
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: EAP-SelfSignedCertificate

Issued by: EAP-SelfSignedCertificate

Valid from 23/11/2016 to 23/11/2018

選擇將其安裝在Local Machine中，然後按一下Next(下一步)。



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

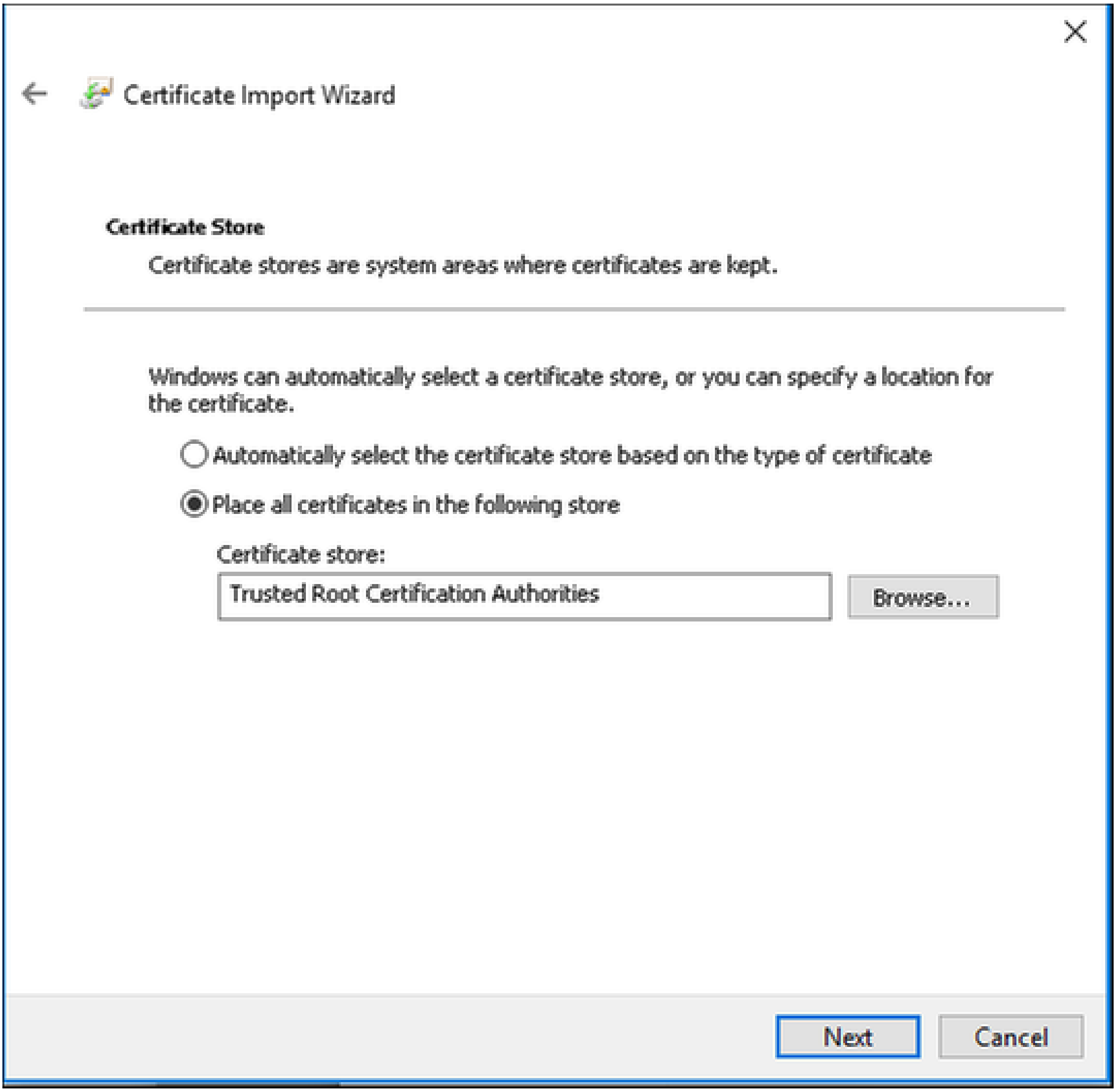
Store Location

○ Current User

● Local Machine

To continue, click Next.

選擇**將所有證書放入以下儲存**，然後瀏覽並選擇**受信任的根證書頒發機構**。完成之後，按一下「下一步」。



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

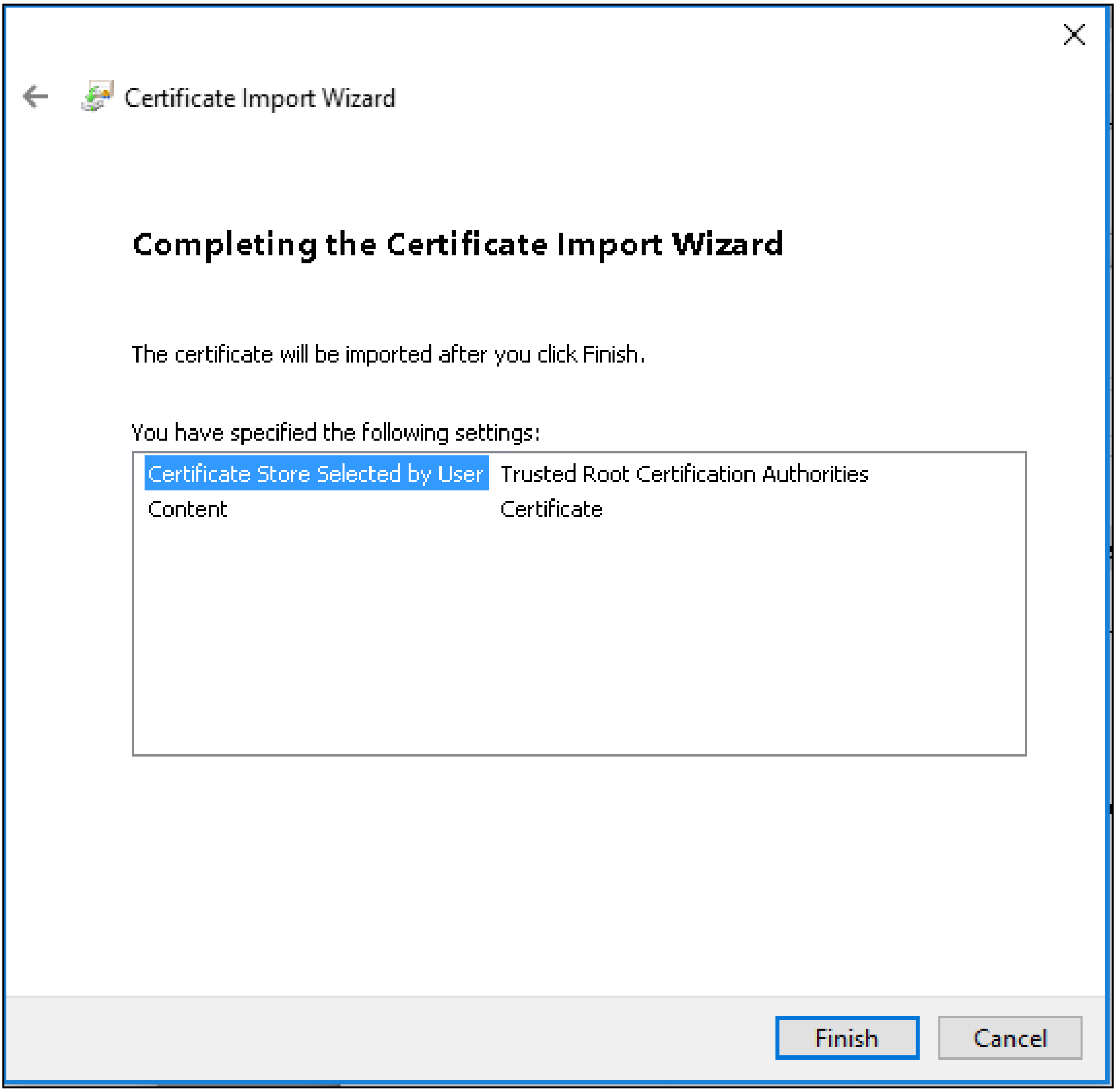
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

然後按一下**完成。**



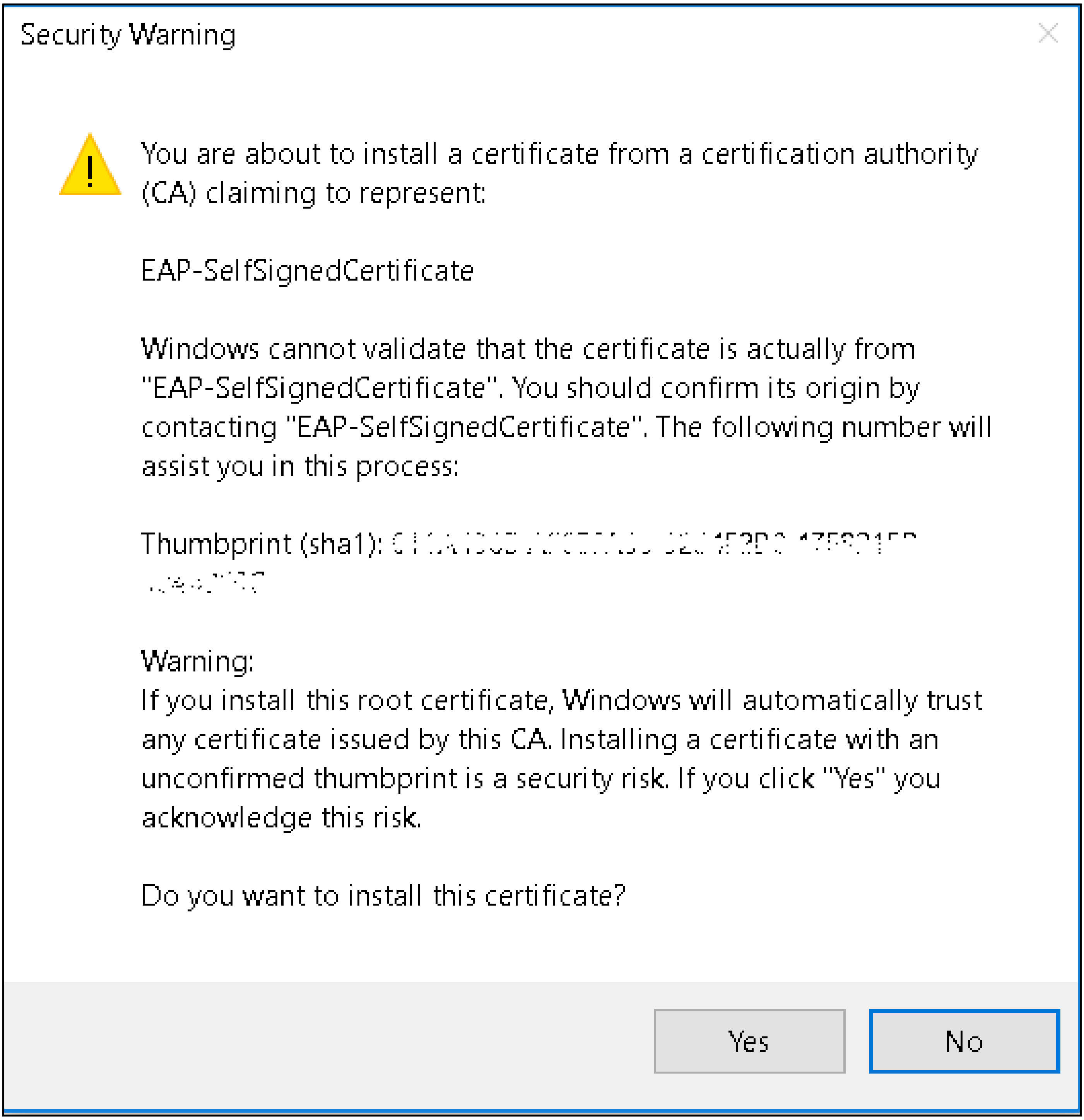
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

最後按一下Yes確認證書安裝。



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

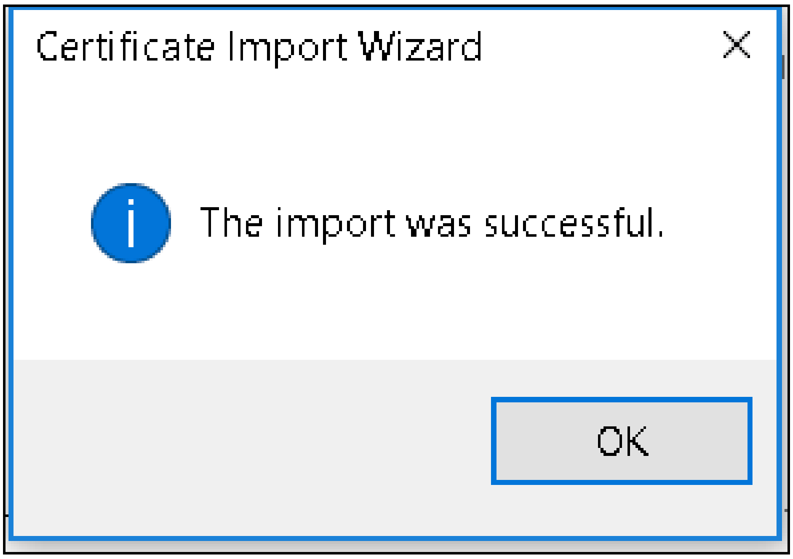
Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): [redacted]

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

最後按一下**確定。**

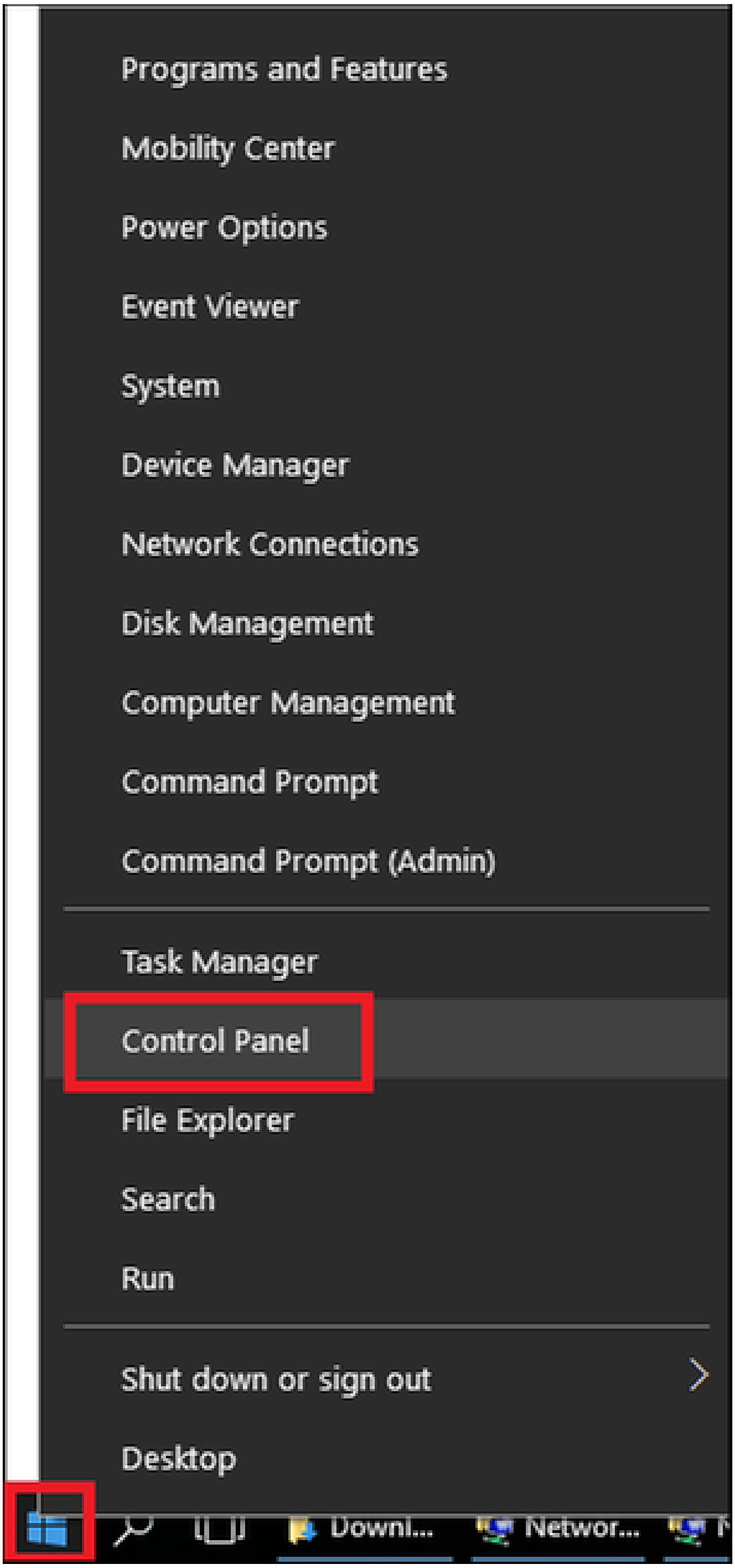


Certificate Import Wizard

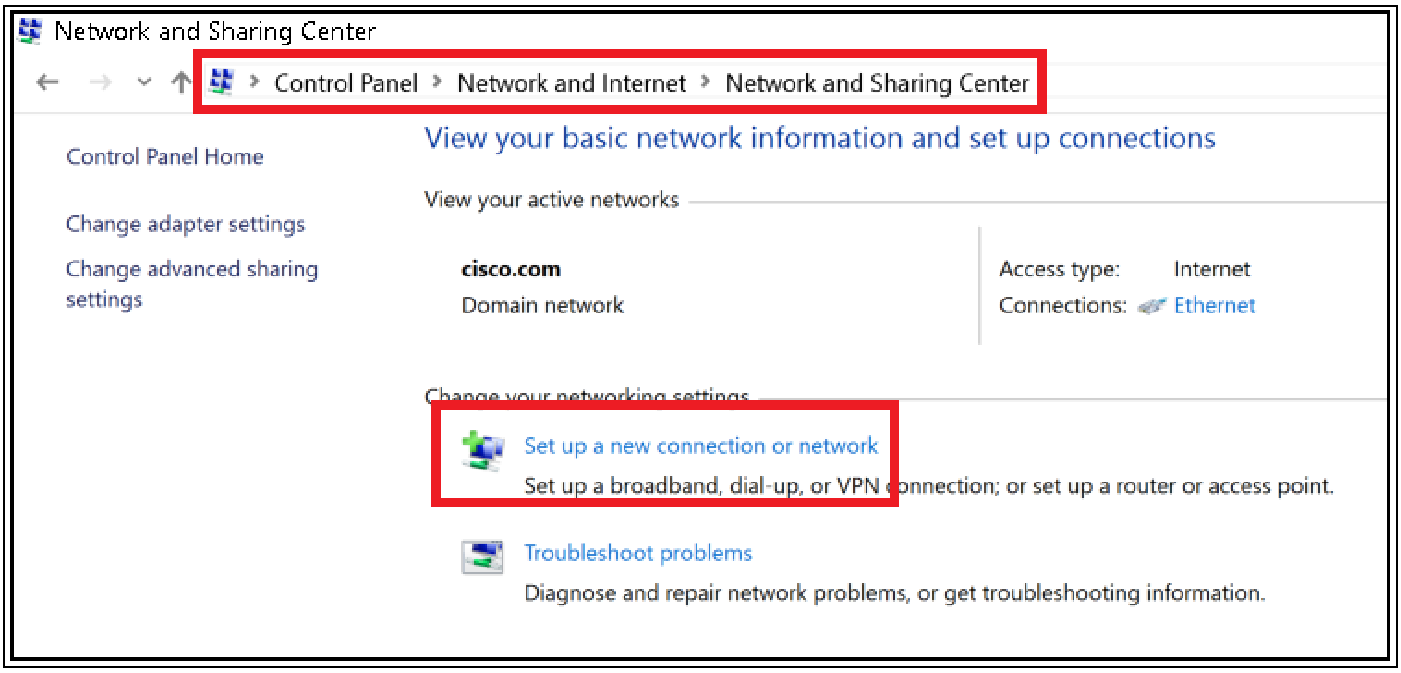
The import was successful.

終端裝置組態 — 建立WLAN設定檔

步驟1.按一下右鍵**開始**圖示並選擇**控制面板。**



步驟2.導覽至Network and Internet，然後導覽至Network and Sharing Center，然後按一下Set up a new connection or network。


Network and Sharing Center
Control Panel > Network and Internet > Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings

View your basic network information and set up connections

View your active networks

cisco.com
Domain network

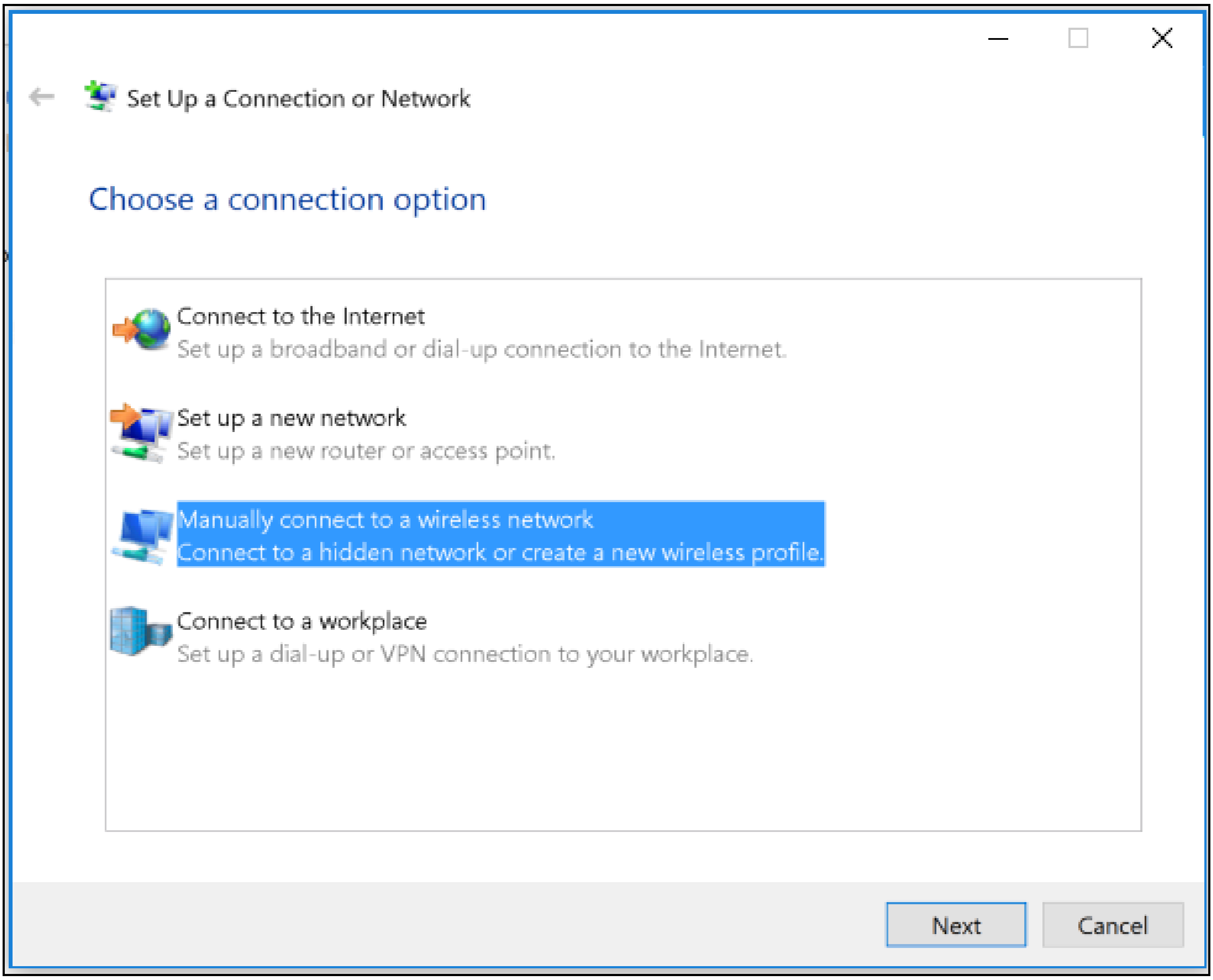
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

步驟3.選擇**Manually connect to a wireless network（手動連線到無線網路）**，然後單**擊Next(下一步)**。



Choose a connection option

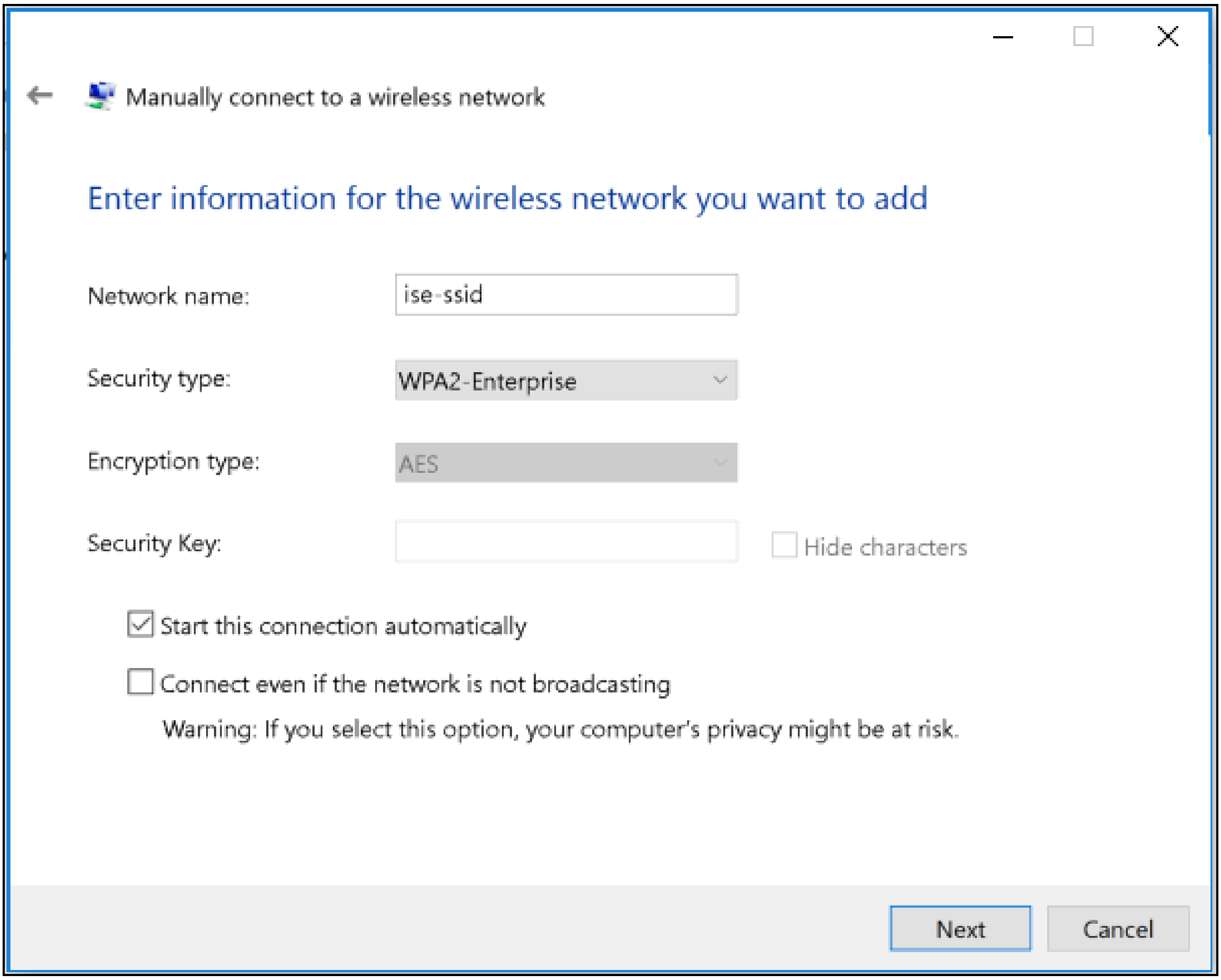
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

步驟4.輸入SSID名稱和安全型別WPA2-Enterprise的資訊，然後按一下**下一步**。



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: ise-ssid

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

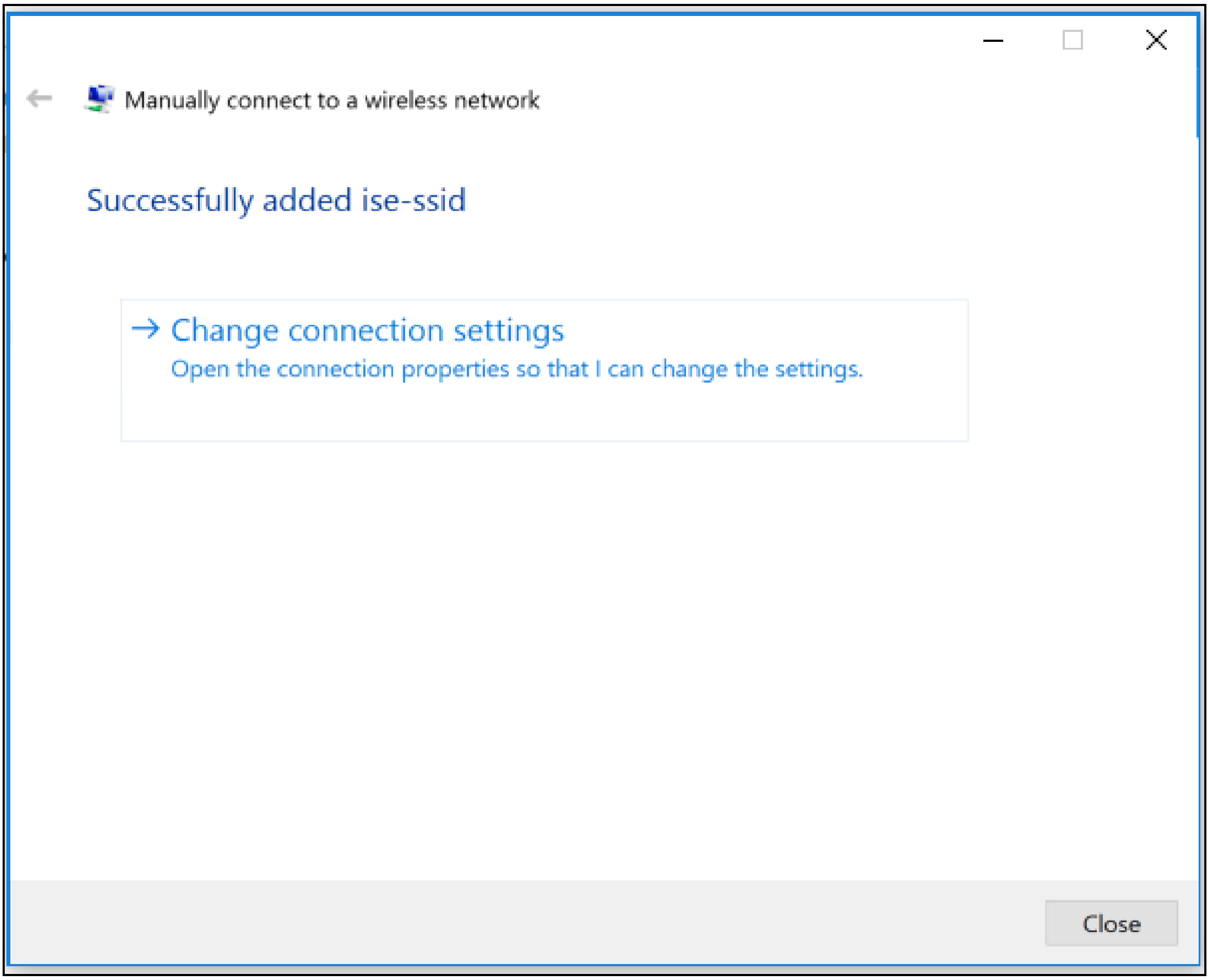
□ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

步驟5.選擇**更改連線設定**以自定義WLAN配置檔案的配置。



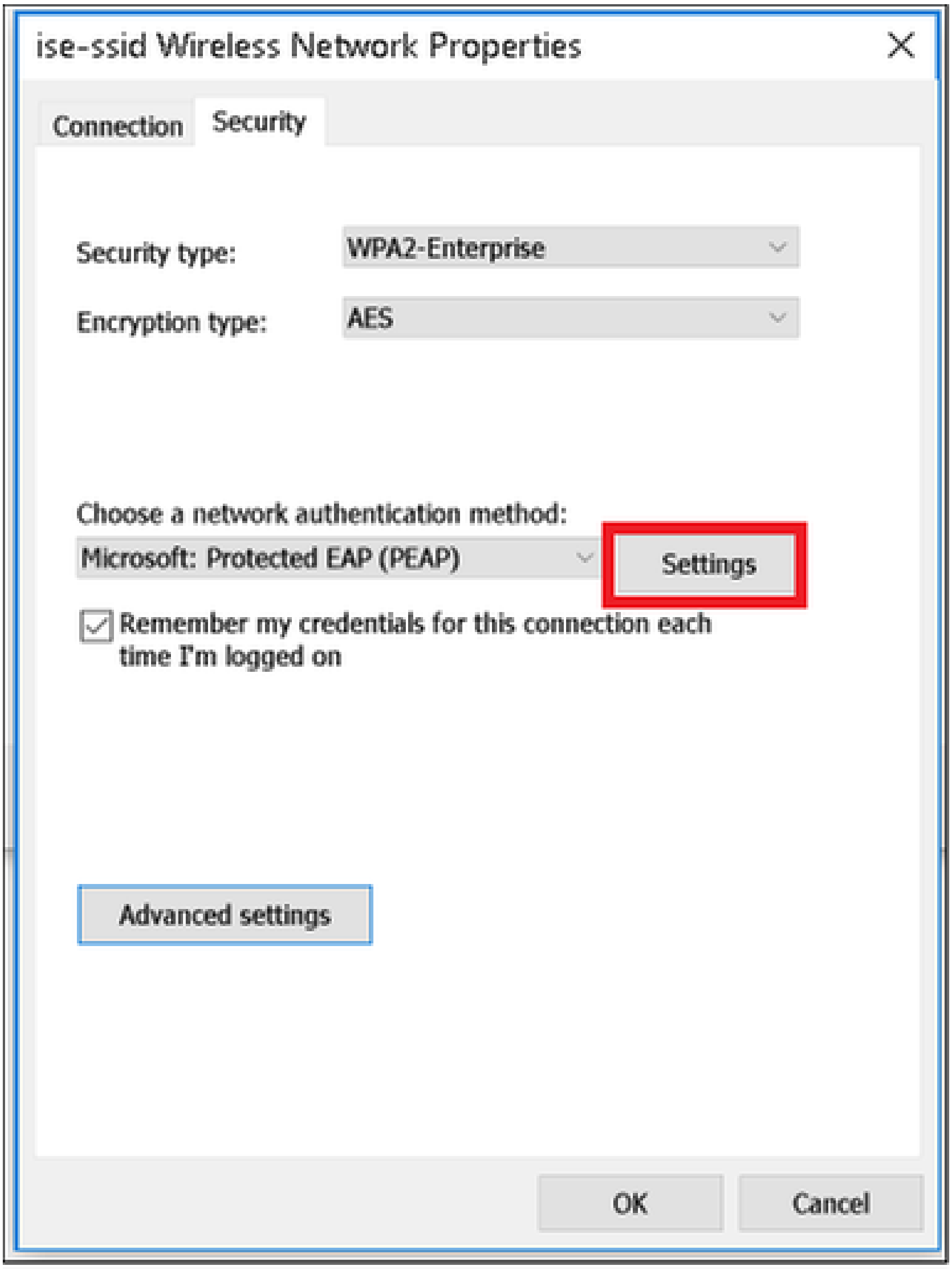
Manually connect to a wireless network

Successfully added ise-ssid

→ Change connection settings

Open the connection properties so that I can change the settings.

步驟6.導覽至Security索引標籤，然後按一下Settings。



ise-ssid Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

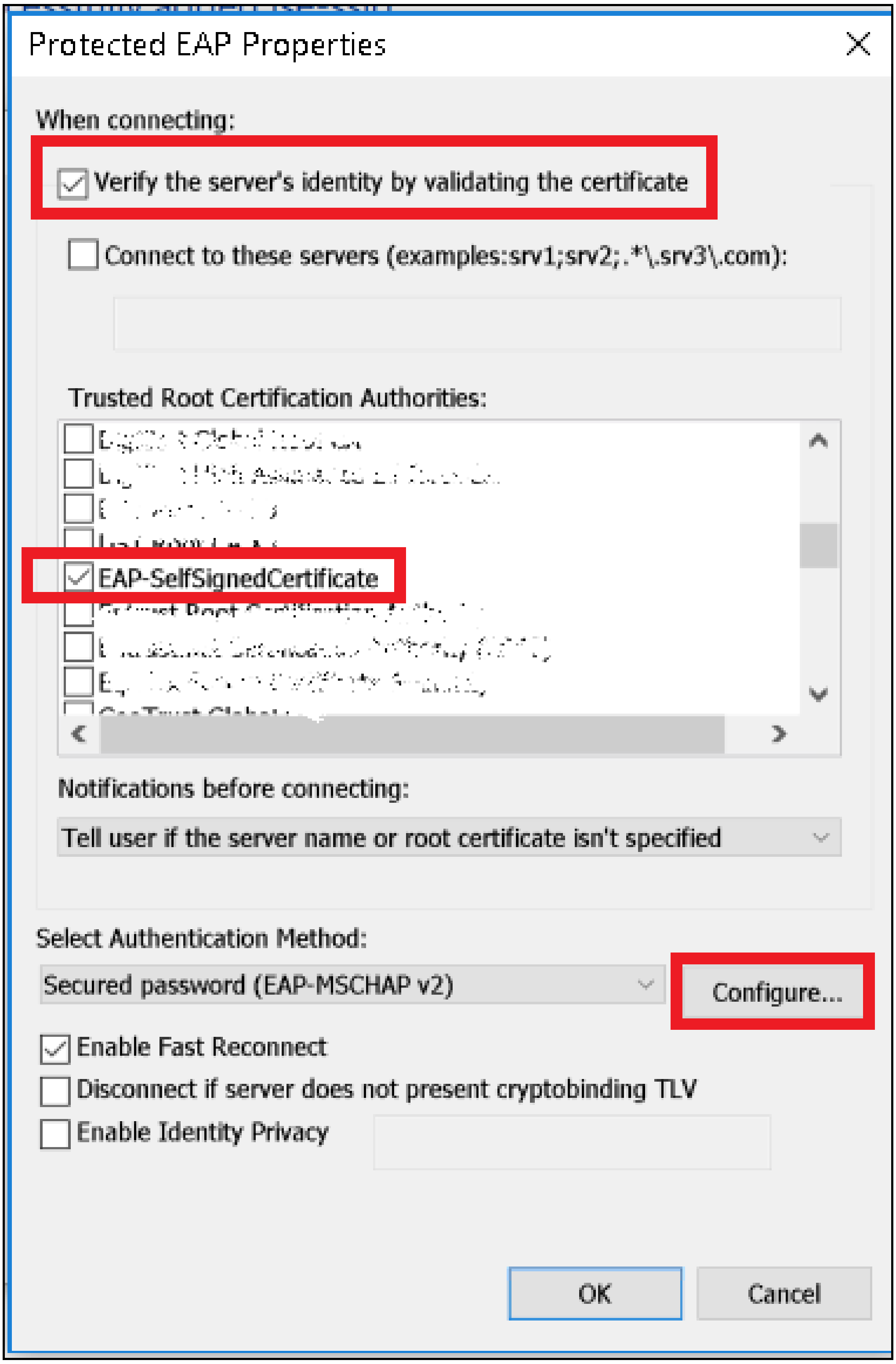
Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

步驟7.選擇是否已驗證RADIUS伺服器。

如果是，啟用**驗證證書並從受信任的根證書頒發機構**(Trusted Root Certification Authorities)中驗證伺服器的身份：清單選擇ISE的自簽名證書。

選擇**Configure**並禁用**Automatically use my Windows logon name and password..**後，按一下**OK**



Protected EAP Properties

When connecting:

☑ Verify the server's identity by validating the certificate

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

□ [illegible]
□ [illegible]
□ [illegible]
□ [illegible]
☑ EAP-SelfSignedCertificate
□ [illegible]
□ [illegible]
□ [illegible]
□ [illegible]

Notifications before connecting:

Tell user if the server name or root certificate isn't specified

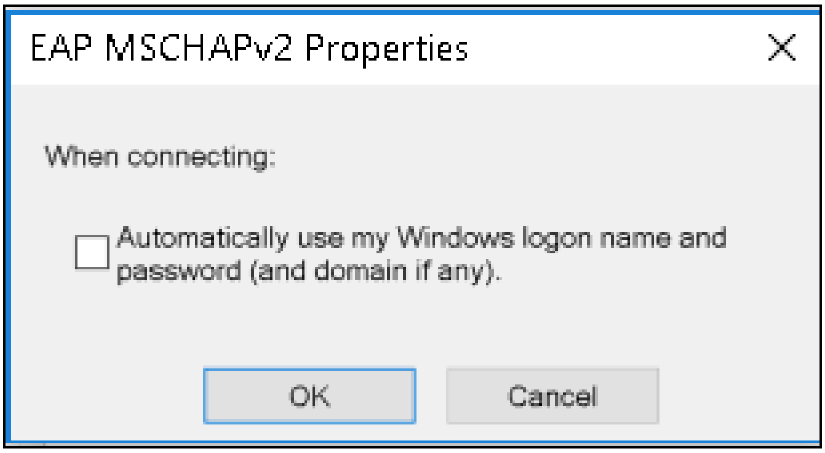
Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy



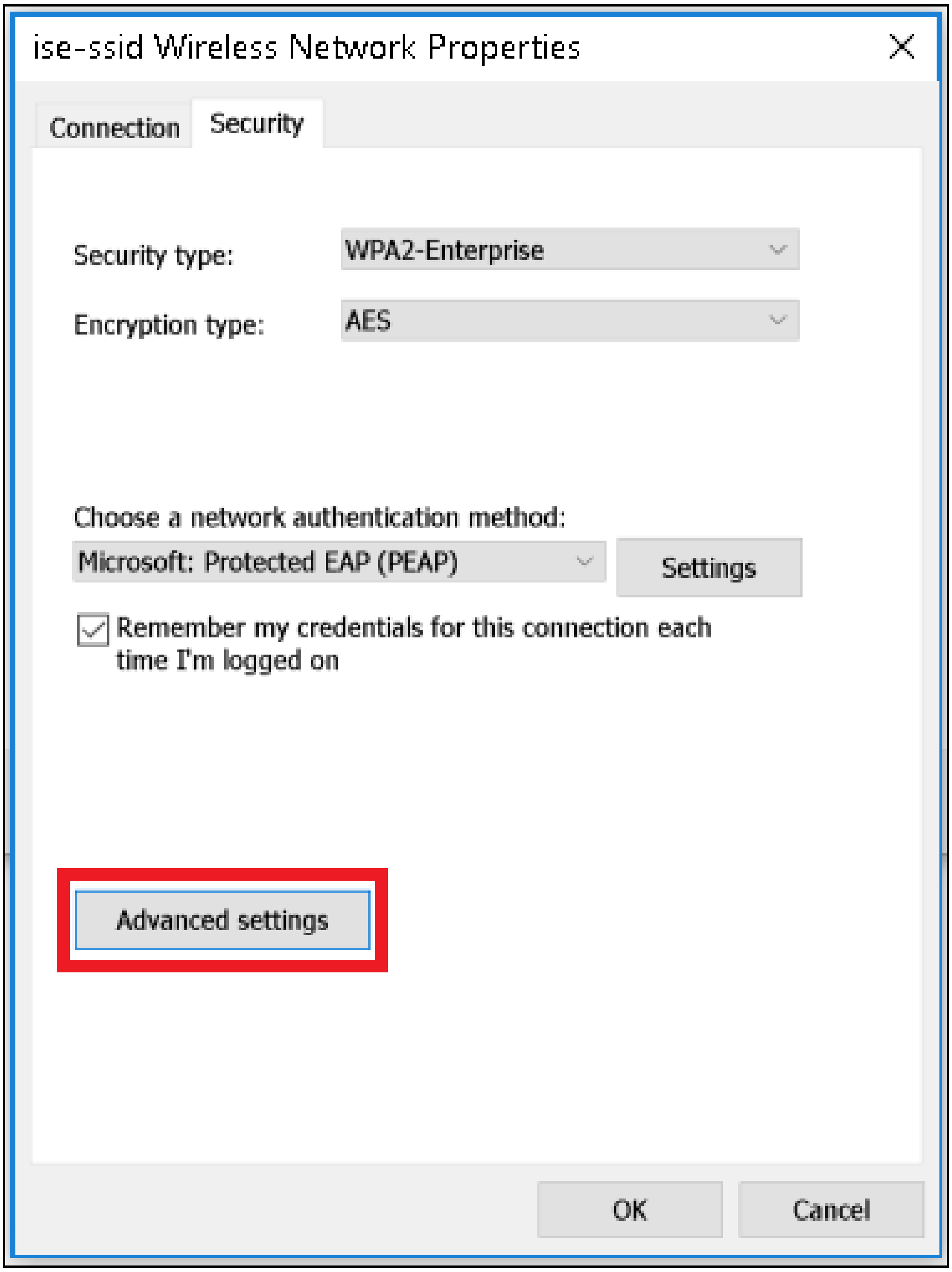
EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

步驟8.配置使用者憑據

返回**Security**頁籤後，選擇**Advanced settings**，將身份驗證模式指定為**User authentication**，並儲存在ISE上配置的用於驗證使用者的憑據。



ise-ssid Wireless Network Properties

Connection | Security

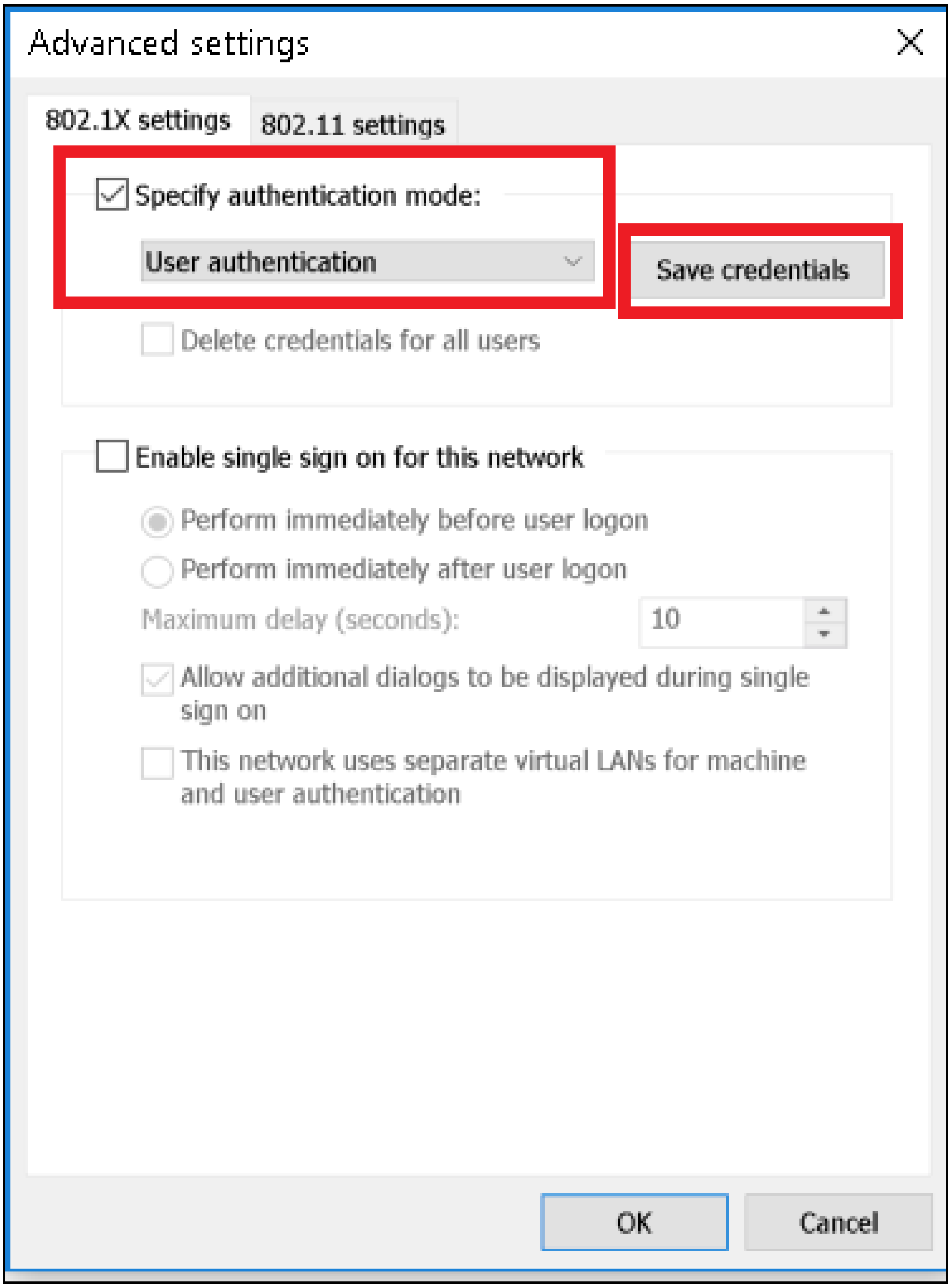
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on



Advanced settings

☑ Specify authentication mode:

User authentication

☐ Delete credentials for all users

☐ Enable single sign on for this network

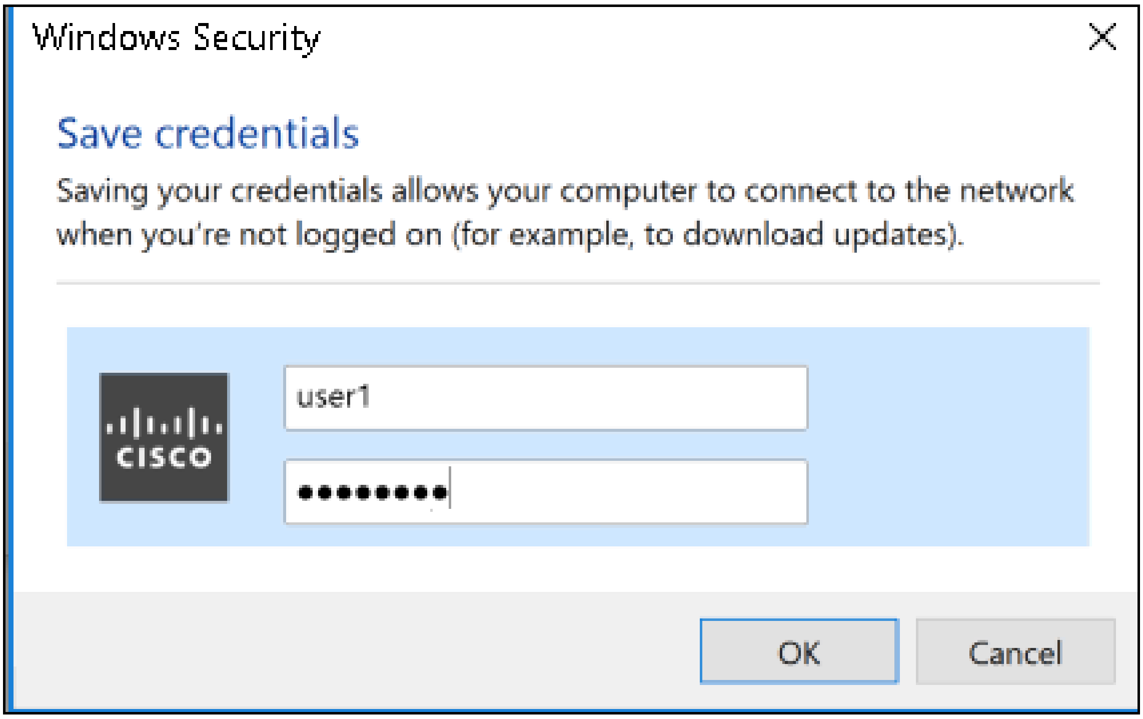
● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

☐ This network uses separate virtual LANs for machine and user authentication


Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

驗證

驗證流程可以從WLC或ISE角度驗證。

ME上的身份驗證過程

運行此命令可監控特定使用者的身份驗證過程：

```
> debug client <mac-add-client>
```

身份驗證成功的示例（某些輸出被省略）：

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```

```
AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout
forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is
0
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station:
(callerId: 48)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0,
Session Timeout = 0
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending assoc-resp with status 0
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending Assoc Response to station on
BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1
*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile
08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1
for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for
Wlan-Id :3 is disabled - applying Global eap timers and retries
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting
dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile
08:74:02:77:13:45 into Connecting state
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Sending EAP-Request/Identity to
mobile 08:74:02:77:13:45 (EAP Id 1)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received EAPOL EAPPKT from mobile
08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received Identity Response (count=1)
from mobile 08:74:02:77:13:45
.
.
.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Processing Access-Accept for mobile
08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Username entry (user1) created in
mscb for mobile, length = 253
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting
dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for
station 08:74:02:77:13:45 (RSN 2)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to
PMKID cache at index 0 for station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in
Mobility handoff
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime
can take care of same.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile
08:74:02:77:13:45 (EAP Id 70)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA
auth is done for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID
38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID
38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Starting key exchange to mobile
```

```
08:74:02:77:13:45, data packets will be dropped
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile
08:74:02:77:13:45
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt
for retransmission to mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state
(id=70) for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in
Authenticating state for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile
08:74:02:77:13:45 into Authenticated state
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile
08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK_START
state (message 2) from mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from
PMK!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key
Message M2!!!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01
00 0..............
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 ......
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00
0f ...............
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for
mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile
08:74:02:77:13:45
 state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt
for retransmission to mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in
PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for
mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state
to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State:
L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan
mask : 255.255.255.224
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP
required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap
00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed
mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change
state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7)
pemAdvanceState2 6623, Adding TMP rule
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast
Path rule
type = Airespace AP - Learn IP address
```

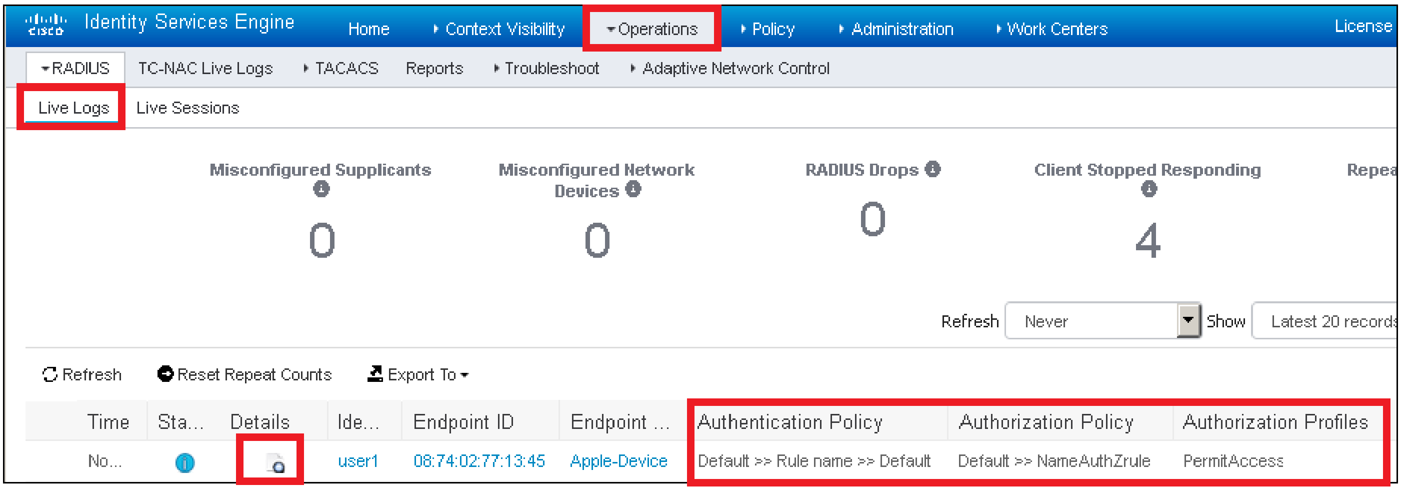
```
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state
to RUN (20) last state DHCP_REQD (7)
```

若要輕鬆讀取偵錯使用者端輸出，請使用*無線偵錯分析器*工具：

無線偵錯分析器

ISE上的身份驗證過程

導覽至Operations > RADIUS > Live Logs，以檢視分配給使用者的身份驗證策略、授權策略和授權配置檔案。



Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...	●		user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccess

有關詳細資訊，請按一下Details檢視更詳細的身份驗證過程。