

使用ISE內部CA在9800 WLC上配置EAP-TLS

目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[背景資訊](#)

[EAP-TLS身份驗證流程](#)

[EAP-TLS流程中的步驟](#)

[設定](#)

[網路圖表](#)

[組態](#)

[ISE 組態](#)

[新增網路裝置](#)

[驗證內部CA](#)

[新增身份驗證方法](#)

[指定證書模板](#)

[建立證書門戶](#)

[新增內部使用者](#)

[ISE證書調配門戶和RADIUS策略配置](#)

[9800 WLC組態](#)

[將ISE伺服器新增到9800 WLC](#)

[在9800 WLC上新增伺服器組](#)

[在9800 WLC上設定AAA方法清單](#)

[在9800 WLC上設定授權方法清單](#)

[在9800 WLC上建立原則設定檔](#)

[在9800 WLC上建立WLAN](#)

[在9800 WLC上使用原則設定檔對應WLAN](#)

[將策略標籤對映到9800 WLC上的接入點](#)

[安裝完成後運行WLC的配置](#)

[為使用者建立和下載證書](#)

[Windows 10電腦上的證書安裝](#)

[驗證](#)

[疑難排解](#)

[參考資料](#)

簡介

本文檔介紹使用身份服務引擎的證書頒發機構對使用者進行身份驗證的EAP-TLS身份驗證。

必要條件

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 無線控制器：運行17.09.04a的C9800-40-K9
- Cisco ISE:運行版本3補丁4
- AP型號：C9130AXI-D
- 交換器:9200-L-24P

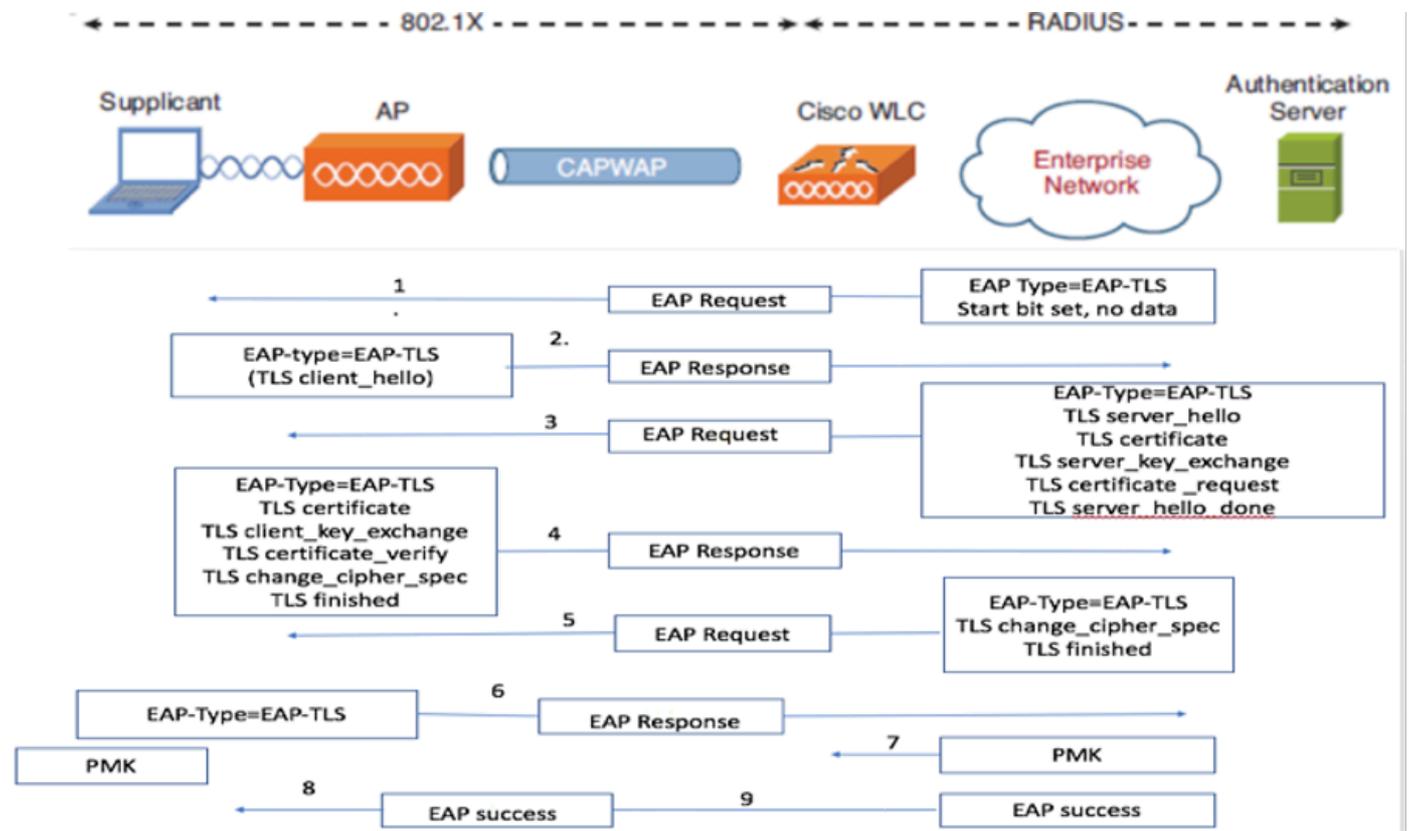
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

大多陣列織都有自己的CA向終端使用者頒發證書以進行EAP-TLS身份驗證。ISE包括一個內建證書頒發機構，可用於為在EAP-TLS身份驗證中使用的使用者生成證書。在無法使用完整CA的情況下，使用ISE CA進行使用者身份驗證是有利的。

本文檔概述了有效使用ISE CA對無線使用者進行身份驗證所需的配置步驟。EAP-TLS身份驗證流程

EAP-TLS身份驗證流程



EAP-TLS身份驗證流程

EAP-TLS流程中的步驟

1. 無線客戶端與接入點(AP)關聯。
2. 在此階段，AP不允許資料傳輸並傳送身份驗證請求。
3. 客戶端作為請求方，使用EAP-Response Identity響應。
4. 無線LAN控制器(WLC)將使用者ID資訊轉送到驗證伺服器。
5. RADIUS伺服器使用EAP-TLS啟動資料包回覆客戶端。
6. EAP-TLS對話從此點開始。
7. 客戶端將EAP-Response傳送回身份驗證伺服器，包括密碼設定為NULL的client_hello握手消息。
8. 身份驗證伺服器使用訪問質詢資料包進行響應，該資料包包含：

```
TLS_server_hello  
Handshake_message  
Certificate  
Server_key_exchange  
Certificate_request  
Server_hello_done
```

9. 客戶端使用EAP-Response消息進行回覆，該消息包括：

```
Certificate (for server validation)  
Client_key_exchange  
Certificate_verify (to verify server trust)  
Change_cipher_spec  
TLS_finished
```

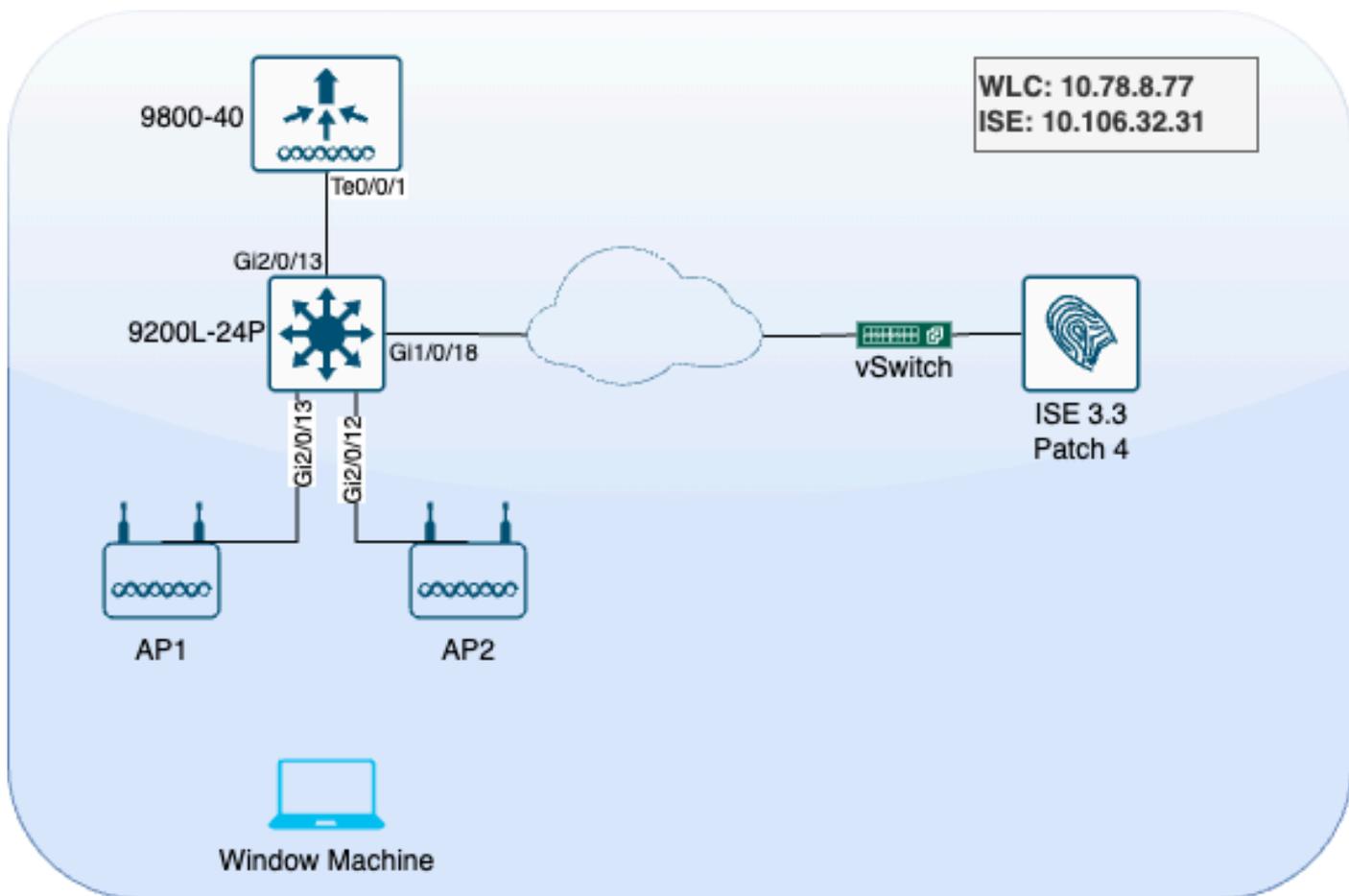
10. 成功進行客戶端身份驗證後，RADIUS伺服器會傳送訪問質詢，內容包括：

```
Change_cipher_spec  
Handshake_finished_message
```

11. 使用者端驗證雜湊以驗證RADIUS伺服器。
12. 在TLS握手期間，從金鑰動態地派生出新的加密金鑰。
13. 從伺服器向驗證者傳送EAP-Success消息，然後向請求者傳送。
14. 啟用了EAP-TLS的無線客戶端現在可以訪問無線網路。

設定

網路圖表



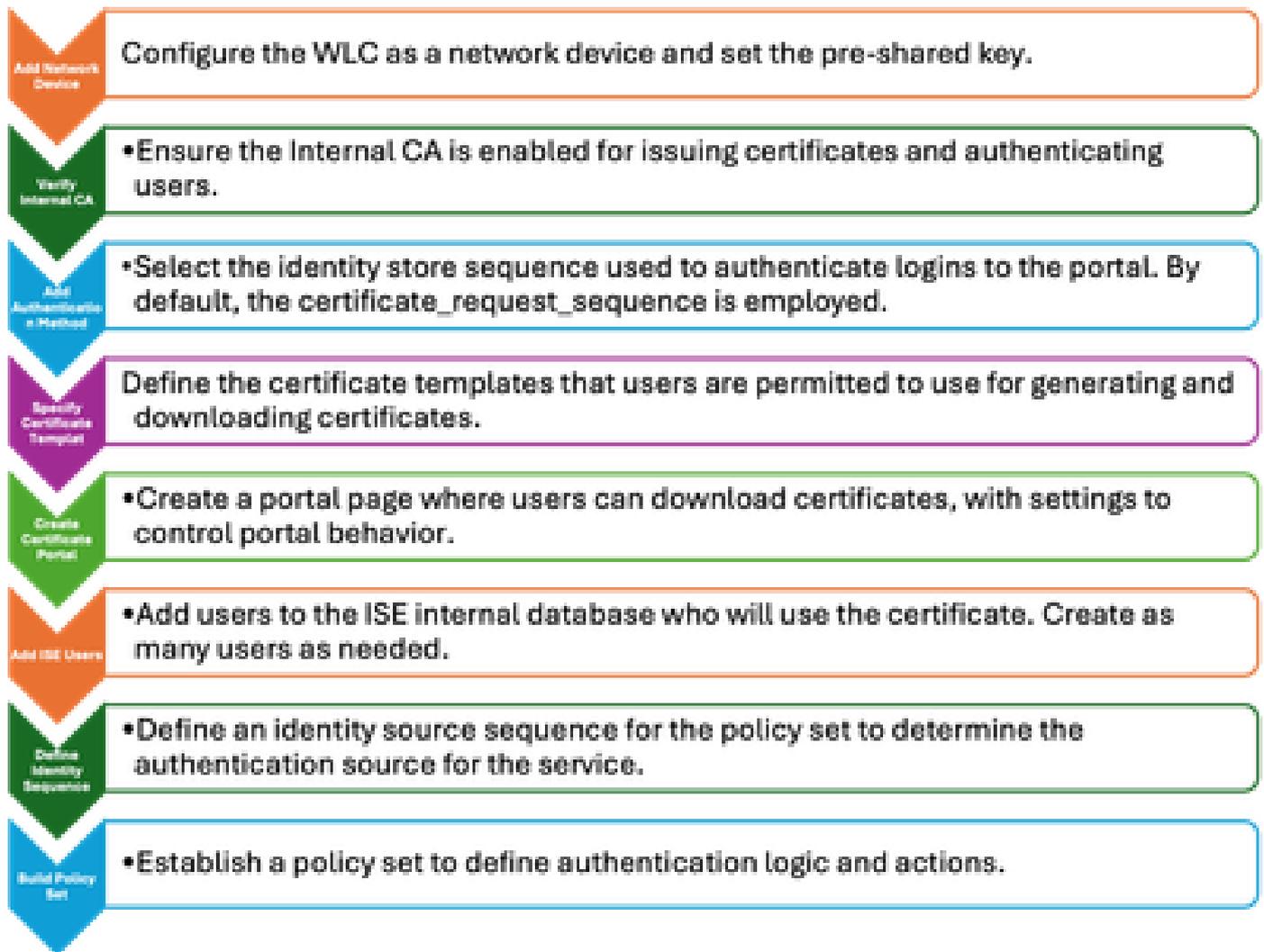
實驗拓撲

組態

在本節中，我們將配置兩個元件：ISE和9800 WLC。

ISE 組態

以下是ISE伺服器的配置步驟。每個步驟都附帶此部分中的螢幕截圖以提供可視指導。

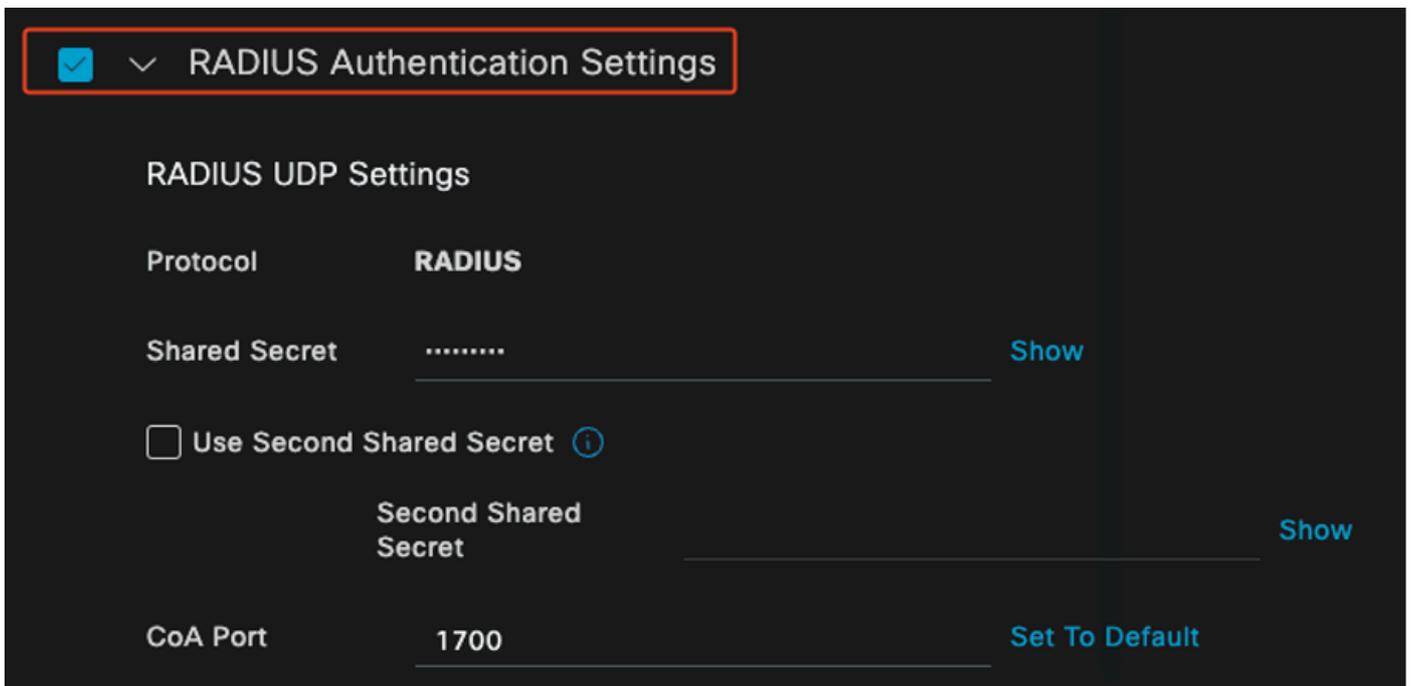


ISE伺服器配置步驟

新增網路裝置

若要將無線LAN控制器(WLC)新增為網路裝置，請使用以下說明：

1. 導覽至Administration > Network Resources > Network Devices。
2. 按一下+Add圖示以啟動新增WLC的過程。
3. 確保預共用金鑰與WLC和ISE伺服器匹配，以啟用正確的通訊。
4. 正確輸入所有詳細資訊後，按一下左下角的Submit儲存配置

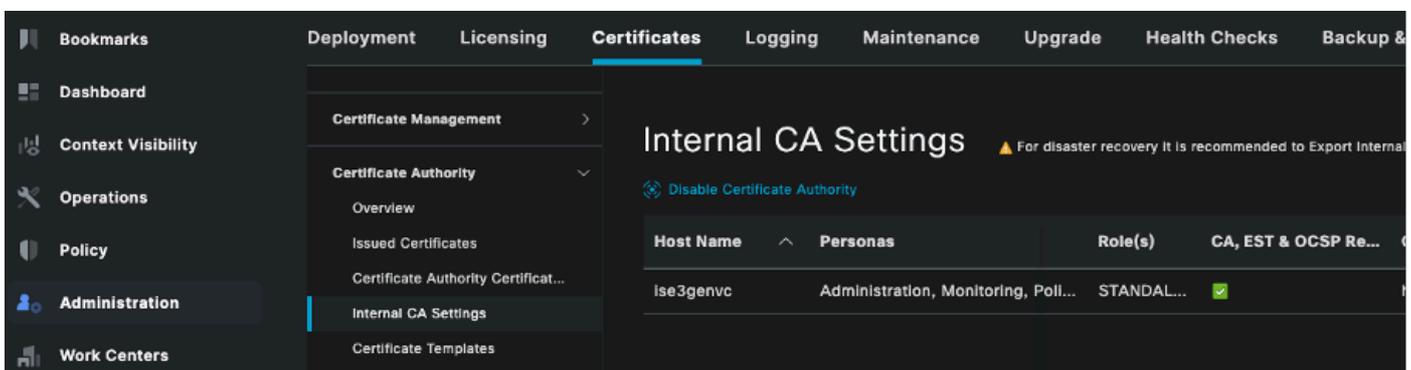


新增網路裝置

驗證內部CA

要驗證內部證書頒發機構(CA)設定，請執行以下步驟：

1. 轉至Administration > System > Certificates > Certificate Authority > Internal CA Settings。
2. 確保CA列已啟用，以確認內部CA處於活動狀態。



驗證內部CA

新增身份驗證方法

導航到管理>身份管理>身份源序列。新增自定義身份序列以控制門戶登入源。

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > Allow_EMP_Cert

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile Preloaded_Certific

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	<input checked="" type="checkbox"/> Internal Users
Guest Users	
All_AD_Join_Points	

> < < >

驗證方法

指定證書模板

要指定證書模板，請執行以下步驟：

步驟1. 導覽至Administration > System > Certificates > Certificate Authority > Certificate Templates。

步驟2. 按一下+Add圖示建立新的證書模板：

2.1 為模板提供ISE伺服器的本地唯一名稱。

2.2確保公用名(CN)設定為\$UserName\$。

2.3驗證主體備用名稱(SAN)是否已對映到MAC地址。

2.4 將SCEP RA配置檔案設定為ISE內部CA。

2.5在「擴展金鑰用法」部分，啟用客戶端身份驗證。

Field	Value
* Name	EAP_Authentication_Certificate_Template
Description	This template will be used to issue certificates for EAP Authentication
Subject	\$UserName\$
Common Name (CN)	\$UserName\$
Organizational Unit (OU)	Example unit
Organization (O)	Company name
City (L)	City
State (ST)	State
Country (C)	US
Subject Alternative Name (SAN)	MAC Address
Key Type	RSA
Key Size	2048
* SCEP RA Profile	ISE Internal CA
Valid Period	730 Day(s) (Valid Range 1 - 3652)
Extended Key Usage	<input checked="" type="checkbox"/> Client Authentication <input type="checkbox"/> Server Authentication

證書模板

建立證書門戶

要建立用於生成客戶端證書的證書門戶，請執行以下步驟：

步驟1. 導覽至Administration > Device Portal Management > Certificate Provisioning。

步驟2. 單擊Create以設定新的門戶頁面。

步驟3. 為入口提供唯一名稱，以便輕鬆識別它。

3.1. 選擇入口的埠號；將此設定為8443。

3.2.指定ISE偵聽此門戶的介面。

3.3.選擇Certificate Group Tag作為預設門戶證書組。

3.4.選擇身份驗證方法，它指示用於驗證登入到此門戶的身份儲存序列。

3.5.包括其成員可以訪問門戶的授權組。例如，如果您的使用者屬於此組，請選擇Employee使用者組。

3.6.定義Certificate Provisioning設定下允許的證書模板。

The screenshot displays the Cisco ISE Administration console interface. The top navigation bar includes 'Bookmarks', 'Blocked List', 'BYOD', 'Certificate Provisioning' (which is the active tab), and 'Client Provisioning'. The left sidebar contains a menu with 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted), and 'Work Centers'. The main content area is titled 'Portals Settings and Customization'. It features a form with the following fields: 'Portal Name' (set to 'EMP CERTIFICATE PORTAL'), 'Description', and 'Language File' (with a dropdown arrow). Below these fields is a link for 'Portal test URL'. At the bottom of the main area, there are two sub-sections: 'Portal Behavior and Flow Settings' (underlined) and 'Portal Page Customization'.

Portal & Page Settings

Portal Settings

HTTPS port:*

1

8443

(8000 - 8999)

Allowed Interfaces:*

2

For PSNs Using Physical Interfaces

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3
- Gigabit Ethernet 4
- Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured

- Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
- Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
- Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: *

3

Default Portal Certificate Group

Configure certificates at:

[Administration > System > Certificates > System Certificates](#)

Authentication method: *

4

Certificate_Request_Sequence

Configure authentication methods at:

[Administration > Identity Management > Identity Source Sequences](#)

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available

Q

- ALL_ACCOUNTS (default)
- GROUP_ACCOUNTS (default)
- OWN_ACCOUNTS (default)

Chosen

Employee

Choose all

Clear all

Fully qualified domain name (FQDN):

> Login Page Settings

> Acceptable Use Policy (AUP) Page Settings

> Post-Login Banner Page Settings

> Change Password Settings

∨ Certificate Portal Settings

Certificate Templates: * EAP_Authentication_Certificate_Template × ∨

證書門戶配置

完成此設定後，您可以通過按一下門戶測試URL來測試門戶。此操作將開啟門戶頁面。

Portals Settings and Customization

Portal Name:

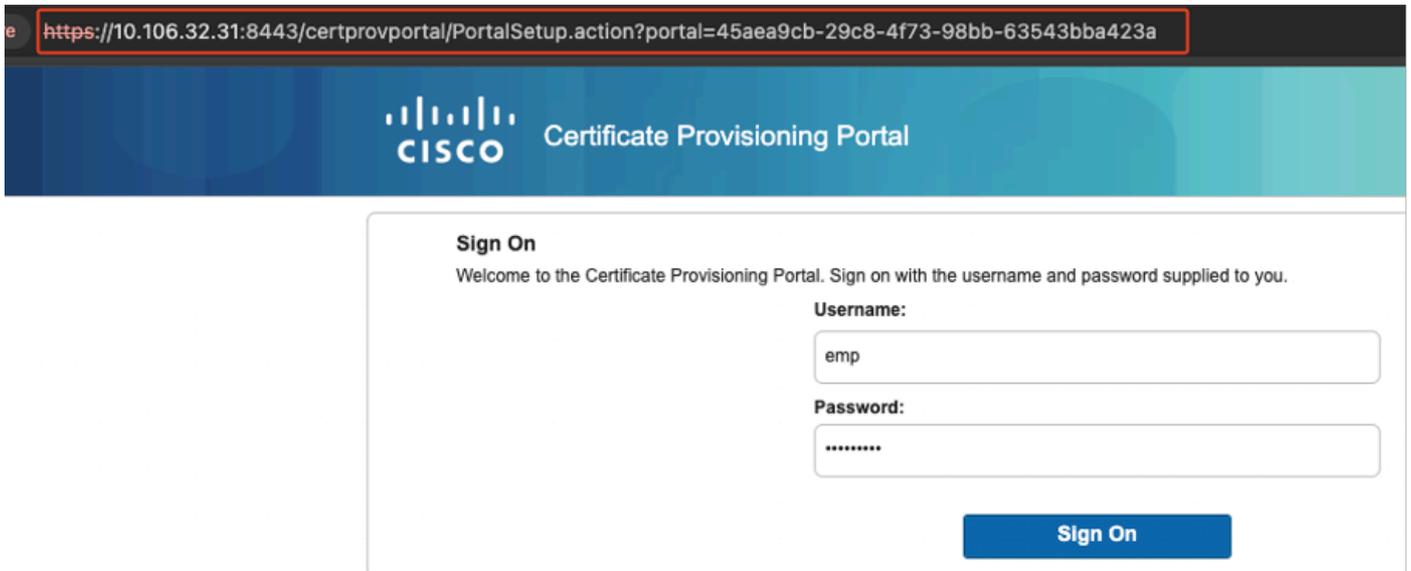
EMP CERTIFICATE PORTAL

Description:

Language File

Portal test URL

測試門戶頁面URL

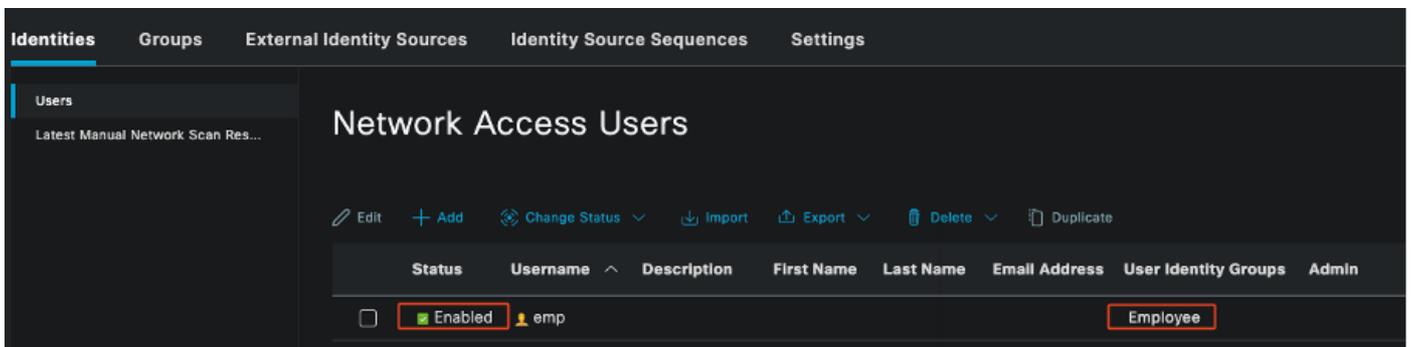


門戶頁面

新增內部使用者

要建立通過證書門戶進行身份驗證的使用者，請執行以下步驟：

1. 轉至Administration > Identity Management > Identities > Users。
2. 按一下該選項將使用者新增到系統。
3. 選擇使用者所屬的User Identity Groups。在本例中，將使用者分配給Employee組。



新增內部使用者

ISE證書調配門戶和RADIUS策略配置

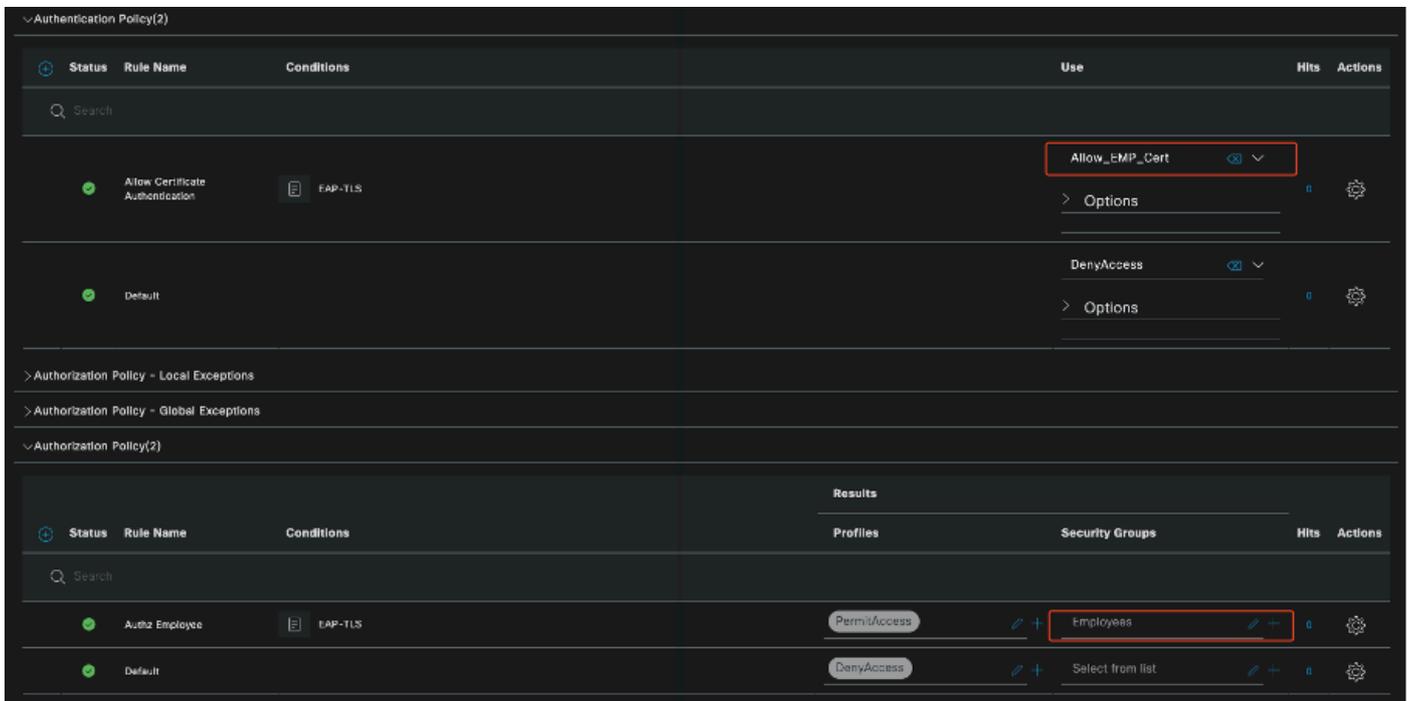
上一節介紹了ISE證書調配門戶的設定。現在，我們將ISE RADIUS策略集配置為允許使用者身份驗證。

1. 配置ISE RADIUS策略集
2. 導航到Policy > Policy Sets。
3. 按一下加號(+)建立新的策略集。

在此示例中，設定一個簡單的策略集，用於使用使用者證書對使用者進行身份驗證。



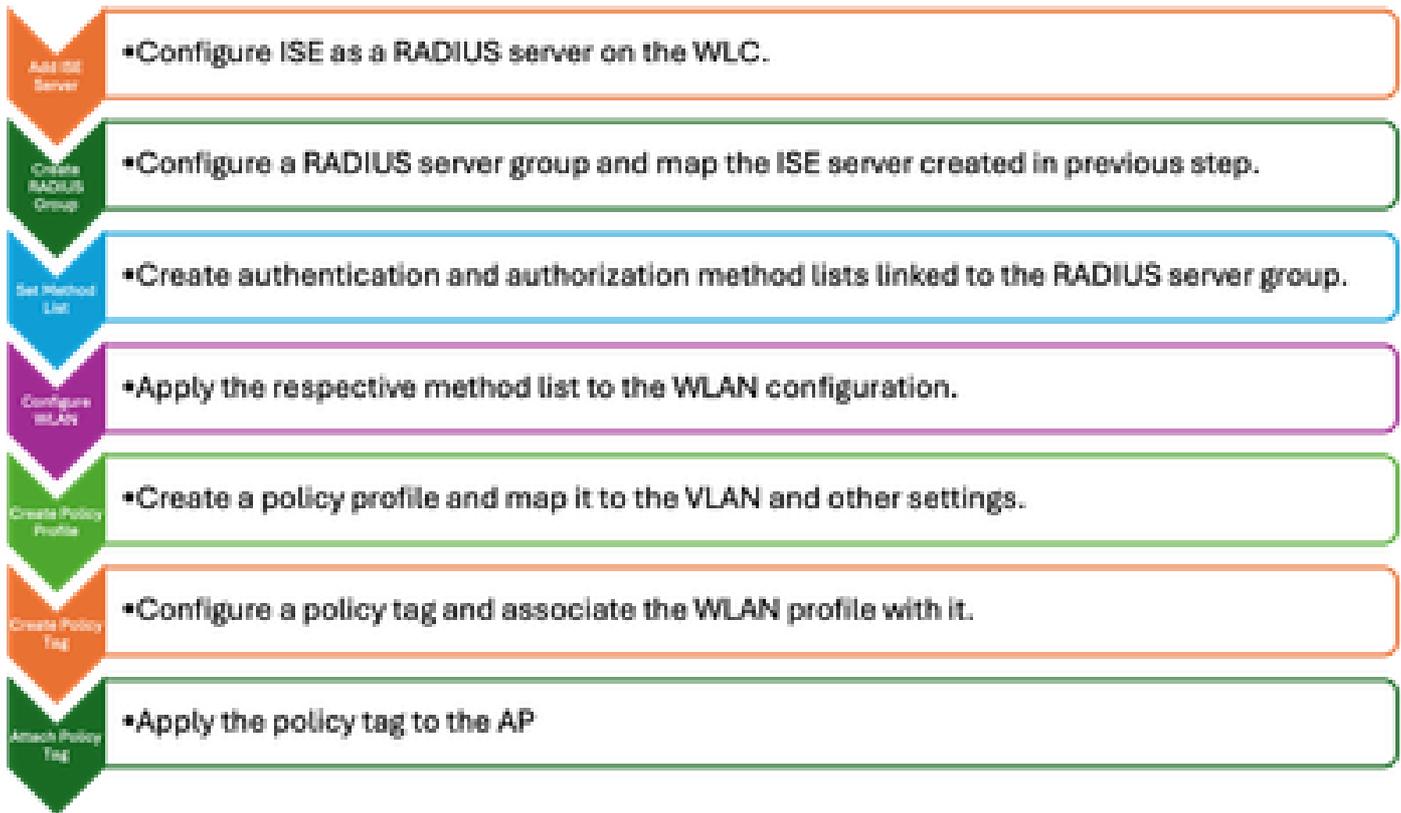
策略集



顯示身份驗證和授權策略的策略集

9800 WLC組態

以下是9800 WLC的設定步驟。每個步驟都伴有本節的截圖，以提供視覺指南。



WLC配置步驟

將ISE伺服器新增到9800 WLC

1. 要將ISE伺服器與9800無線LAN控制器(WLC)整合，請執行以下步驟：
2. 前往Configuration > Security > AAA。
3. 按一下Add按鈕將ISE伺服器包括在WLC配置中。

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

RADIUS

TACACS+

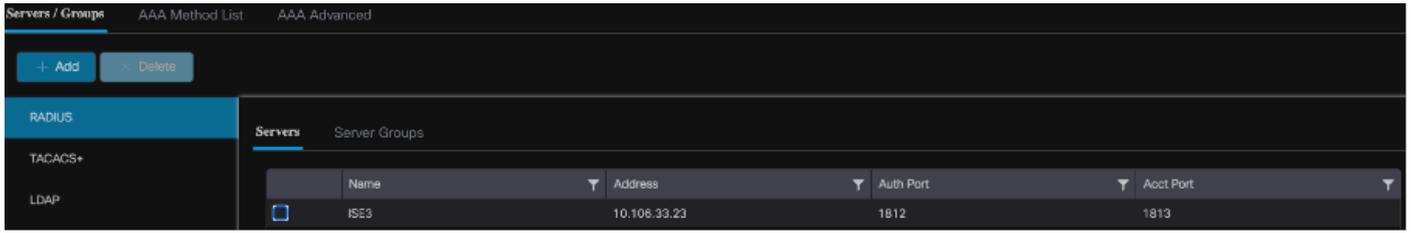
LDAP

Create AAA Radius Server

Name*	ISE3	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	10.106.32.31	CoA Server Key Type	Clear Text
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ
Key Type	Clear Text	Confirm CoA Server Key
Key* ⓘ	Automate Tester	<input type="checkbox"/>
Confirm Key*		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

在WLC中新增ISE伺服器

新增伺服器後，它將顯示在伺服器清單中。

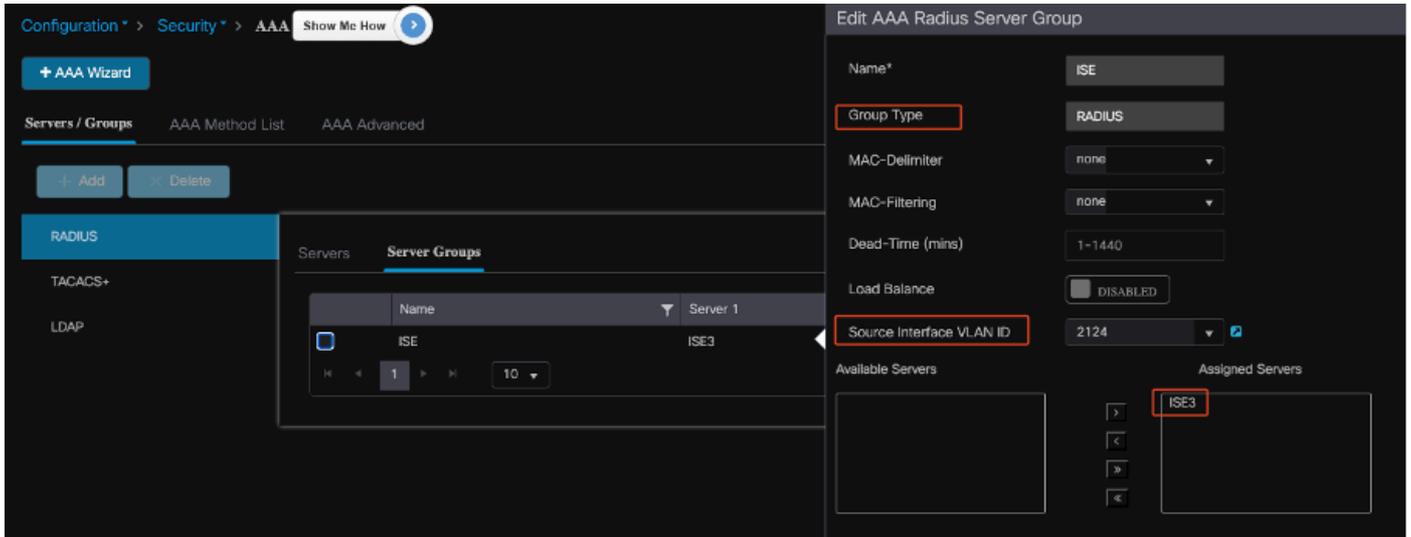


顯示Radius伺服器

在9800 WLC上新增伺服器組

要在9800無線LAN控制器上新增伺服器組，請完成以下步驟：

1. 導覽至Configuration > Security > AAA。
2. 按一下Server Group頁籤，然後按一下Add以建立新的伺服器組。

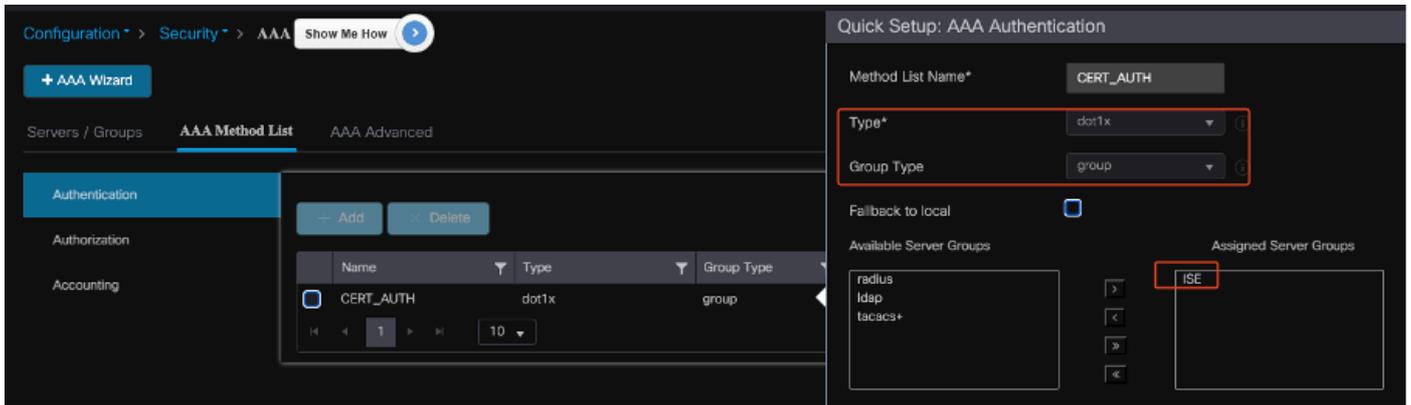


將ISE伺服器對映到Radius伺服器組

在9800 WLC上設定AAA方法清單

建立伺服器組後，使用以下步驟配置身份驗證方法清單：

1. 導覽至Configuration > Security > AAA > AAA Method List。
2. 在Authentication頁籤中，新增新的身份驗證方法清單。
3. 將型別設定為dot1x。
4. 選擇group作為組型別。
5. 包括您以前創建的ISE伺服器組作為伺服器組。

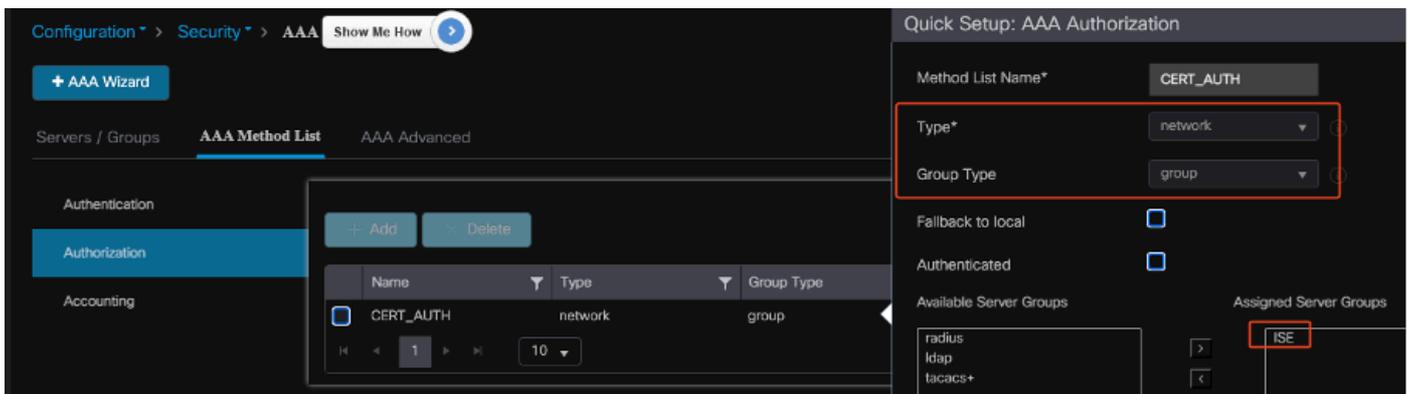


建立身份驗證方法清單

在9800 WLC上設定授權方法清單

要設定授權方法清單，請執行以下步驟：

1. 導航到AAA Method List部分中的Authorization頁籤。
2. 按一下Add建立新的授權方法清單。
3. 選擇network作為型別。
4. 選擇group作為組型別。
5. 包括ISE伺服器組作為伺服器組。

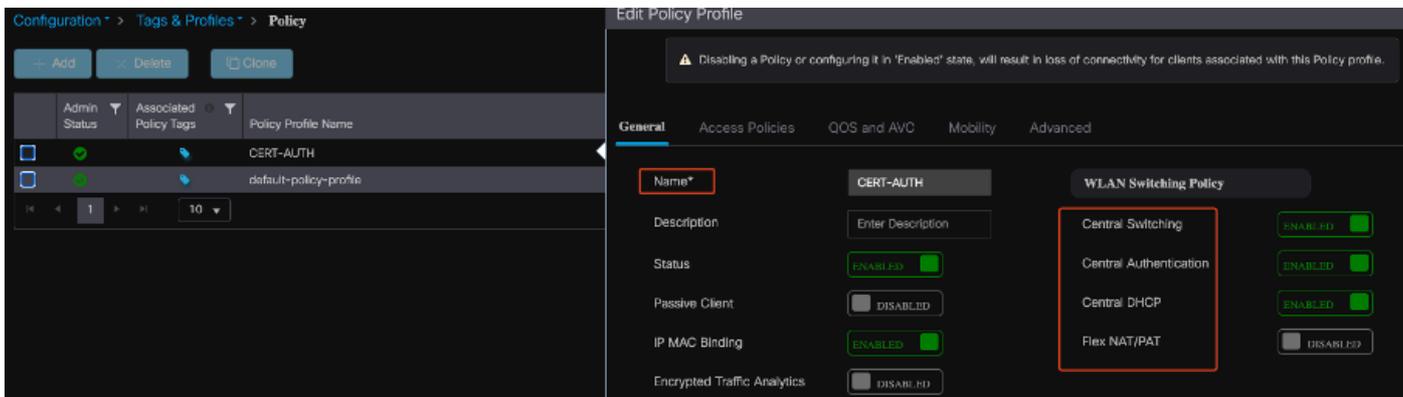


新增授權方法清單

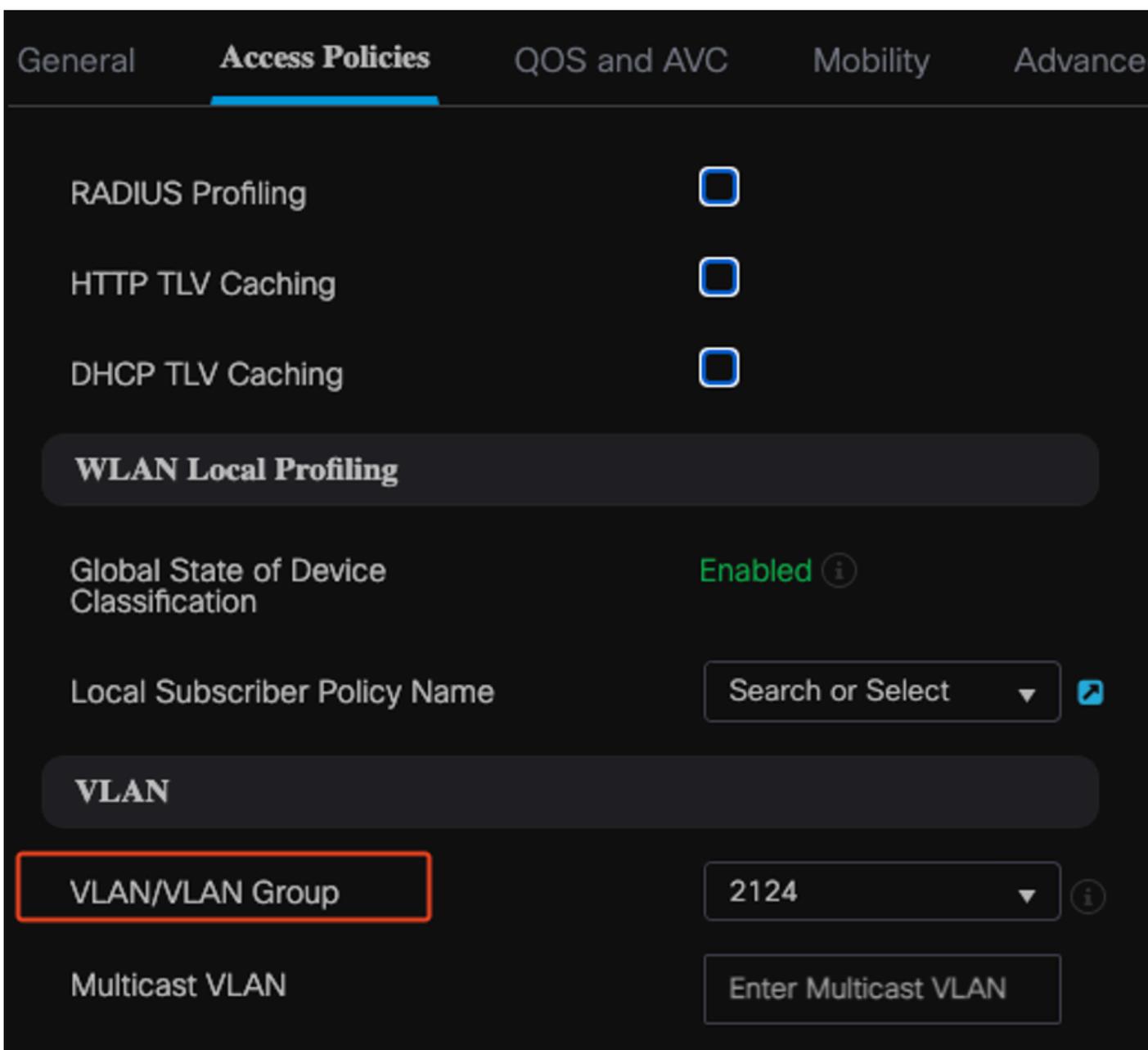
在9800 WLC上建立原則設定檔

完成RADIUS組配置後，繼續建立策略配置檔案：

1. 導航到Configuration > Tags & Profiles > Policy。
2. 按一下Add建立新的策略配置檔案。
3. 為您的策略配置檔案選擇適當的引數。在本例中，所有裝置都處於中心狀態，並且實驗VLAN用作客戶端VLAN。



配置策略配置檔案



VLAN到策略的對映

配置RADIUS授權時，確保在策略配置檔案設定的advanced頁籤中啟用AAA Override選項。此設定允許無線LAN控制器將基於RADIUS的授權策略應用於使用者和裝置。

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec) ⓘ

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

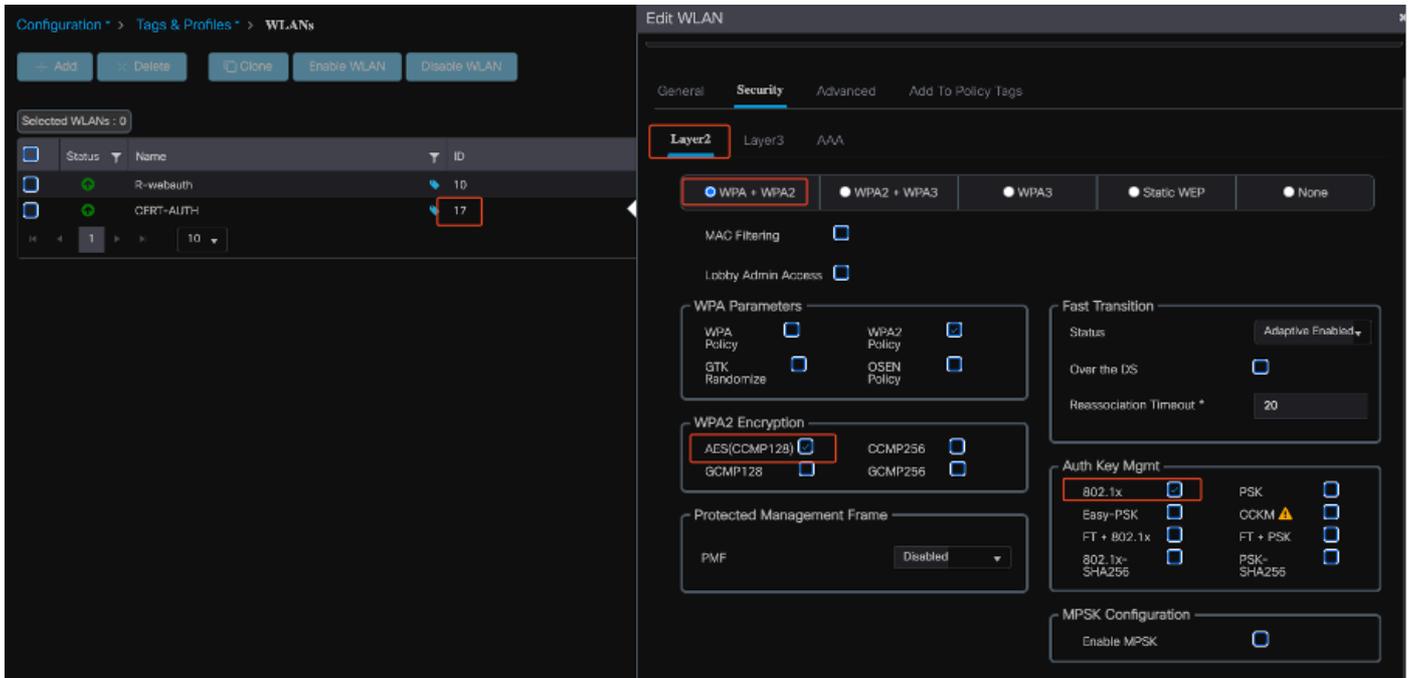
Allow AAA Override

AAA覆寫

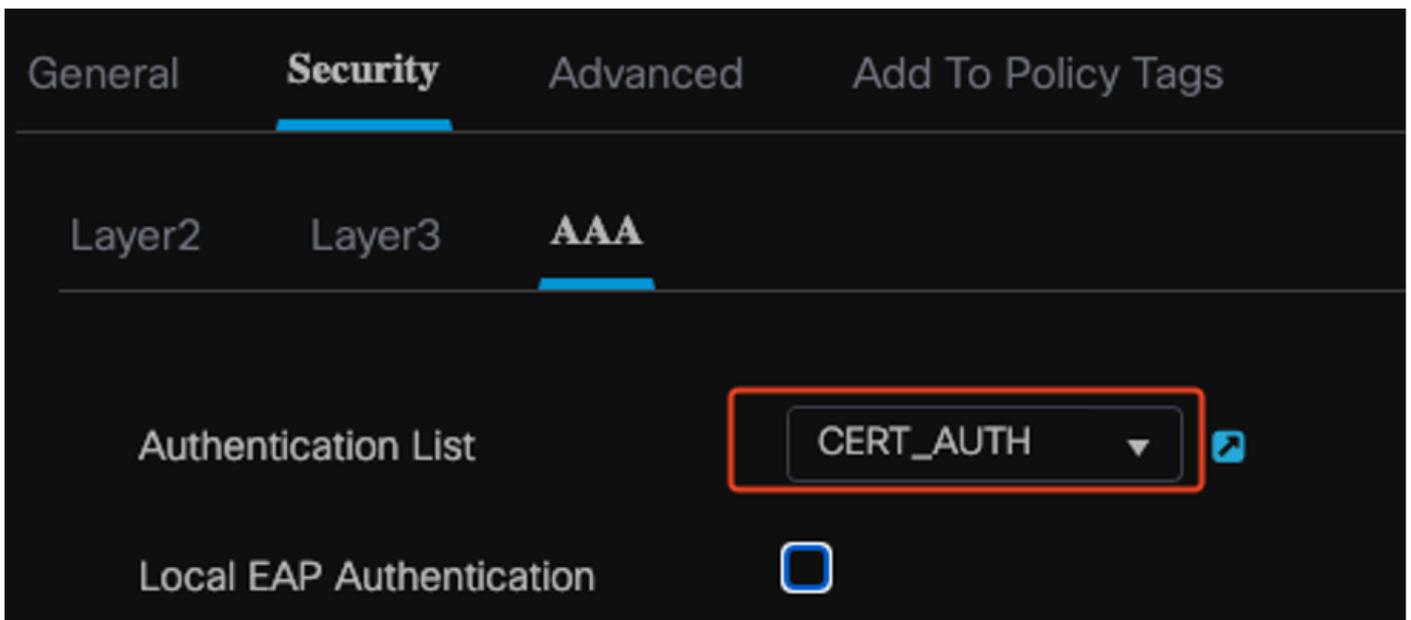
在9800 WLC上建立WLAN

要設定具有802.1x身份驗證的新WLAN，請執行以下步驟：

1. 導覽至Configuration > Tags & Profiles > WLANs。
2. 按一下「Add」以建立一個新的WLAN。
3. 選擇第2層身份驗證設定並啟用802.1x身份驗證。



WLAN配置檔案配置

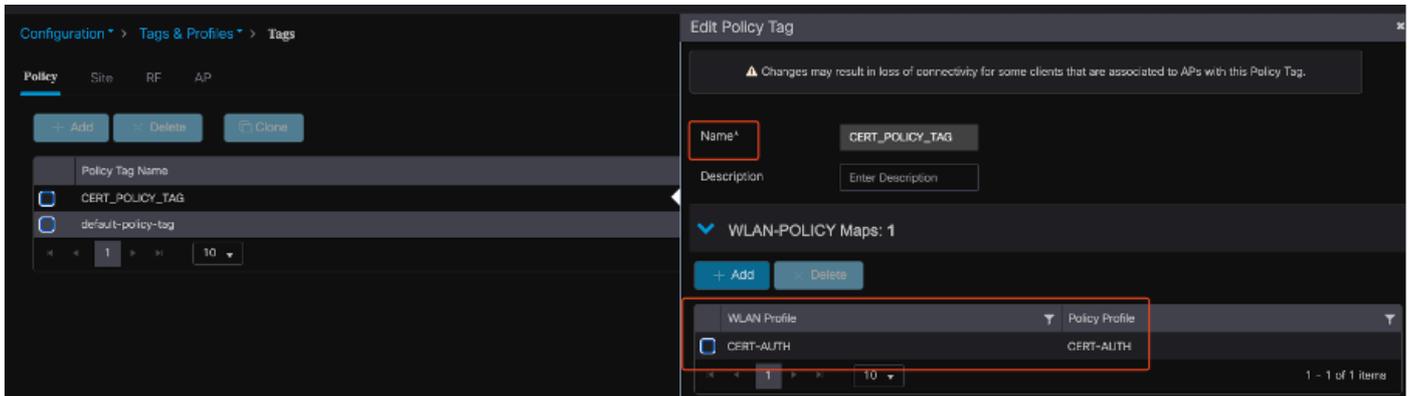


WLAN配置檔案到方法清單對映

在9800 WLC上使用原則設定檔對應WLAN

要將WLAN與策略配置檔案相關聯，請執行以下步驟：

1. 導航到Configuration > Tags & Profiles > Tags。
2. 按一下Add新增新標籤。
3. 在WLAN-POLICY部分，將新建立的WLAN對映到相應的策略配置檔案。

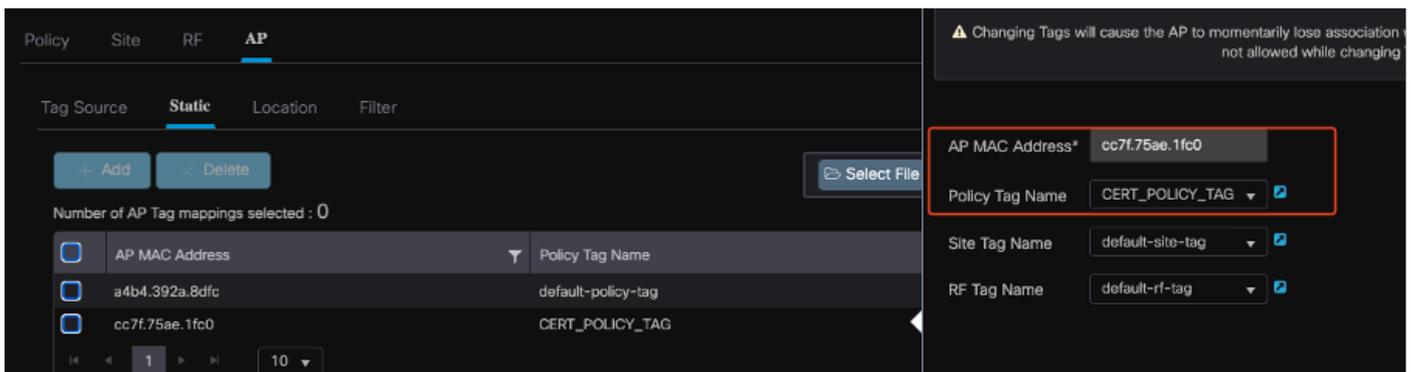


原則標籤組態

將策略標籤對映到9800 WLC上的接入點

要將策略標籤分配給接入點(AP)，請完成以下步驟：

1. 導航到 Configuration > Tags & Profiles > Tags > AP。
2. 轉到 AP 配置中的「靜態」部分。
3. 按一下要配置的特定 AP。
4. 將您建立的策略標籤分配給選定的 AP。



AP 標籤分配

安裝完成後運行WLC的配置

```

aaa group server radius ISE
  server name ISE3
  ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
  client 10.106.32.31 server-key Cisco!123
!
```

```

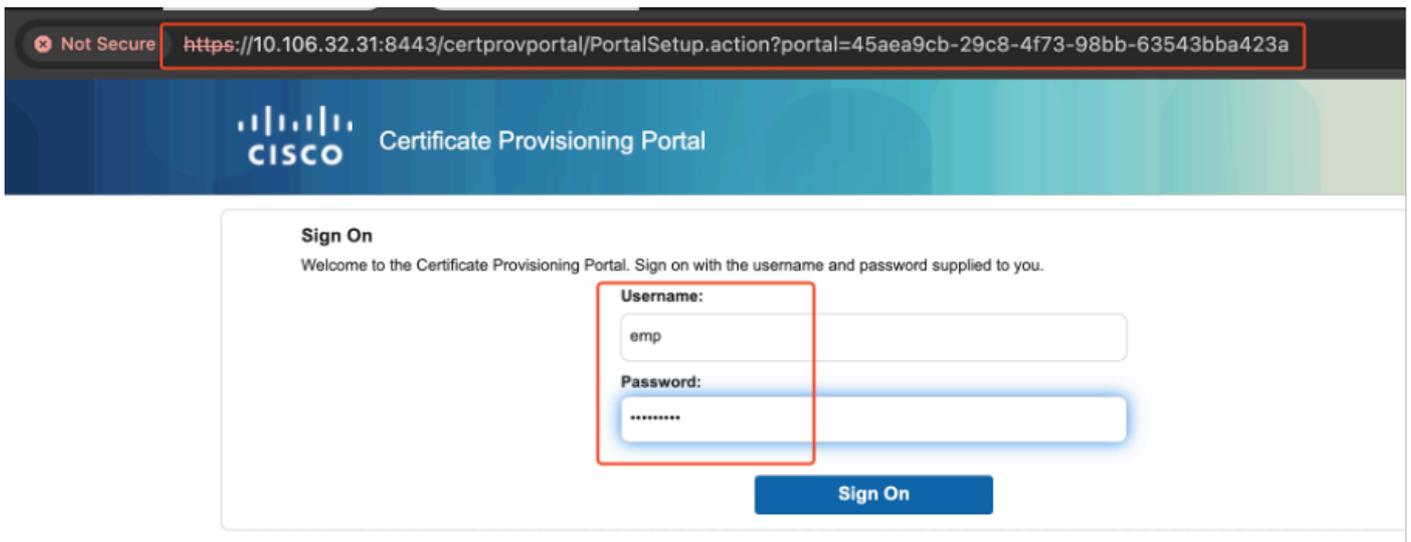
wireless profile policy CERT-AUTH
  aaa-override
  ipv4 dhcp required
  vlan 2124
  no shutdown
  wlan CERT-AUTH policy CERT-AUTH
  wlan CERT-AUTH 17 CERT-AUTH
```

```
security dot1x authentication-list CERT_AUTH
no shutdown
!
wireless tag policy CERT_POLICY_TAG
wlan CERT-AUTH policy CERT-AUTH
```

為使用者建立和下載證書

若要為使用者建立和下載證書，請完成以下步驟：

1.讓使用者登入到之前設定的證書門戶。



訪問證書門戶

2.接受「可接受的使用策略」(AUP)。然後ISE顯示用於生成證書的頁面。

3.選擇Generate a single certificate(無證書簽名請求)。

Certificate Provisioning

I want to: *

Generate a single certificate (without a certificate...) 1

Common Name (CN): *

emp 2

MAC Address: *

242f.d0da.a563 3

Choose Certificate Template: *

EAP_Authentication_Certificate_Template 4

Description:

Certificate Download Format: *

PKCS12 format, including certificate chain (...) 5

Certificate Password: *

Enter password to download and view/install the certificate

Confirm Password: *

Generate

Reset

正在生成證書

要通過證書調配門戶生成證書，請確保填寫以下必填欄位：

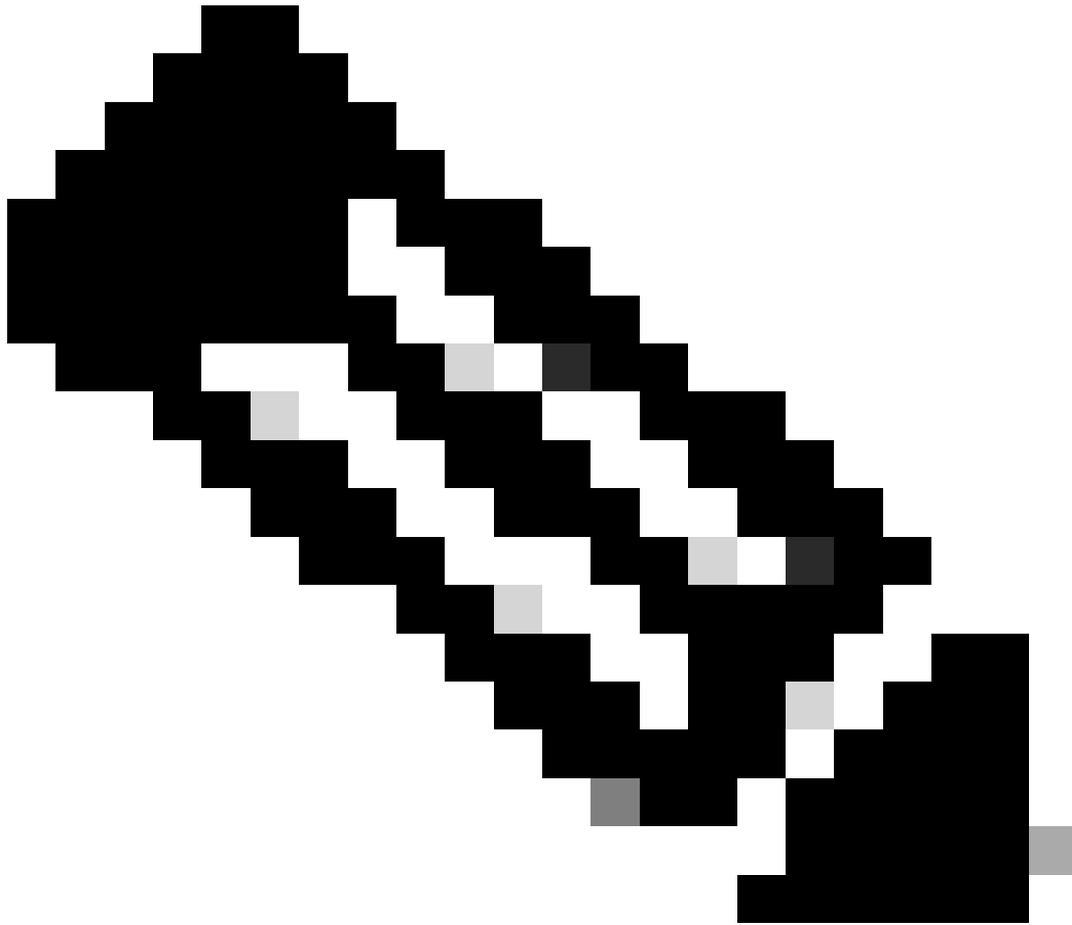
- CN:身份驗證伺服器使用客戶端證書中「公用名」欄位中顯示的值對使用者進行身份驗證。在 Common Name欄位中，輸入使用者名稱（用於登入證書調配門戶）。
- MAC 地址:使用者替代名稱(SAN)是一個X.509擴展，允許將各種值與安全證書關聯。Cisco ISE版本2.0僅支援MAC地址。因此，在SAN/MAC地址欄位中。
 - 證書模板：證書模板定義CA在驗證請求和頒發證書時使用的欄位集。公用名(CN)等欄位用於驗證請求（CN必須與使用者名稱匹配）。頒發證書時，CA會使用其他欄位。
- 證書密碼：您需要證書密碼來保護您的證書。必須提供證書密碼才能檢視證書的內容並在裝置上匯入證書。
- 您的密碼必須符合以下規則：
- 密碼必須至少包含1個大寫字母、1個小寫字母和1個數字

- 密碼的長度必須介於8到15個字元之間
- 允許的字元包括A-Z、a-z、0-9、_、#

填寫所有欄位後，選擇Generate以建立和下載證書。

Windows 10電腦上的證書安裝

要在Windows 10電腦上安裝證書，請按照以下步驟開啟Microsoft管理控制檯(MMC):

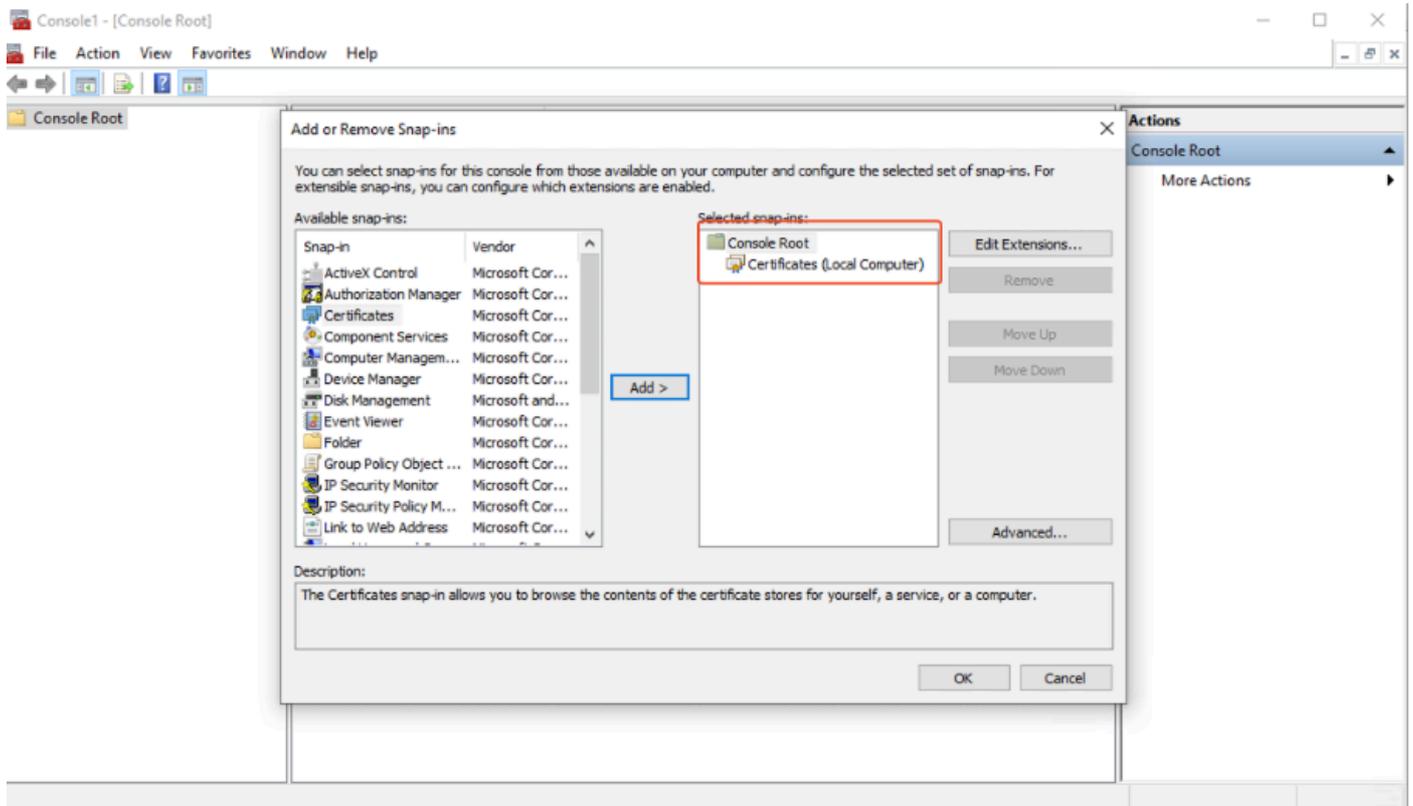


附註：這些說明可能會因您的Windows安裝程式而異，因此建議參閱Microsoft文檔以瞭解具體的詳細資訊。

1. 按一下「Start」，然後「Run」。
2. 在「Run (運行)」框中鍵入mmc，然後按Enter鍵。將開啟Microsoft管理控制檯。
3. 新增證書管理單元：
4. 轉到「檔案」>「新增/刪除管理單元」。
5. 選擇Add，然後選擇Certificates，然後按一下Add。

6. 選擇Computer Account，然後選擇Local Computer，然後按一下Finish。

這些步驟允許您管理本地電腦上的證書。



Windows MMC控制檯

步驟1.匯入證書：

- 1.1.按一下選單中的Action。
- 1.2.轉到所有任務，然後選擇匯入。
- 1.3.按照提示查詢並選擇電腦上儲存的證書檔案。



←  Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\admin\Desktop\emp-2025-01-06_08-30-59\emp_C4-E9-0

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX, .P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

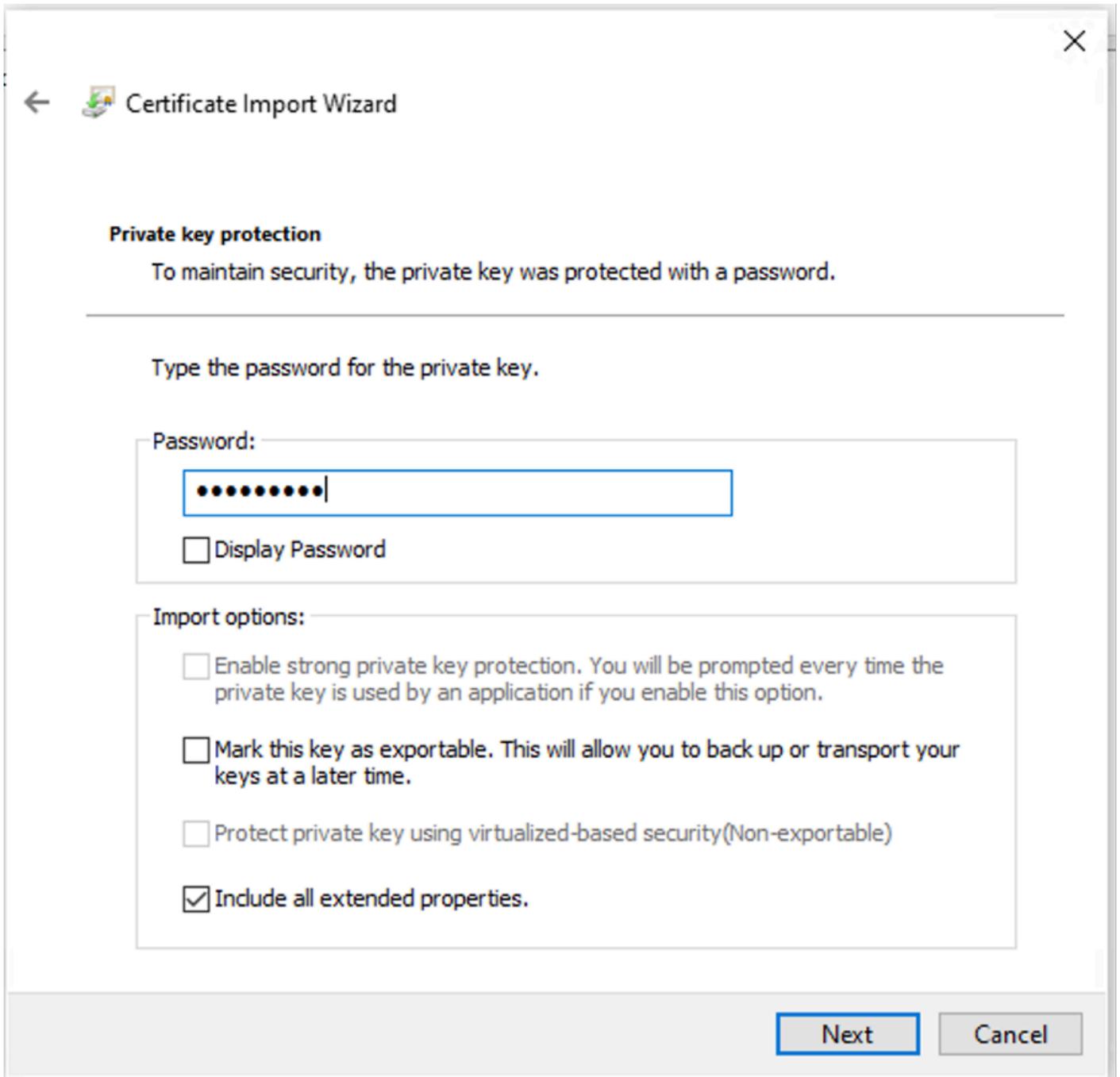
Microsoft Serialized Certificate Store (.SST)

Next

Cancel

正在匯入證書

在證書匯入過程中，系統將提示您輸入在門戶上生成證書時建立的密碼。請確保準確地輸入此密碼，以便成功匯入證書並在電腦上安裝。

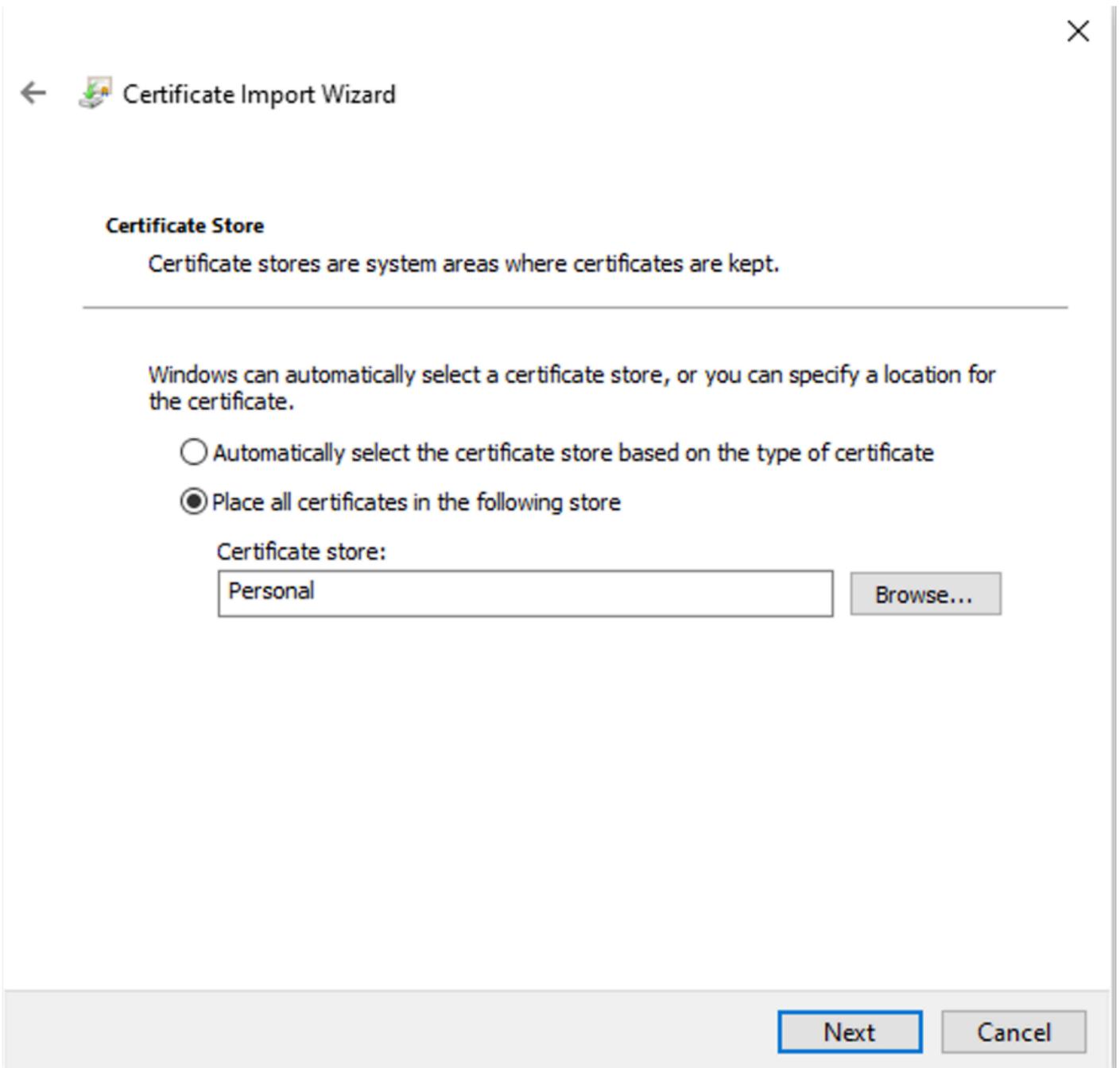


輸入證書密碼

步驟2.將證書移動到適當的資料夾：

- 2.1.開啟Microsoft Management Console(MMC)，然後導覽至Certificates(Local Computer)> Personal資料夾。
- 2.2.檢查證書並確定其型別（例如，根CA、中間CA或個人）。
- 2.3.將每個憑證移動到適當的儲存區：
- 2.4.根CA證書：移至受信任的根憑證授權單位。
- 2.5.中間CA證書：轉到中級證書頒發機構。

2.6.個人證明：留在Personal資料夾中。



在個人資料夾中儲存證書

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
Certificate Services Endpoint Sub CA - ise3genvc	Certificate Services Node CA - ise3genvc	1/3/2035	<All>	EndpointSubCA	
Certificate Services Node CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate_nodeCA	
Certificate Services Root CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate	
emp	Certificate Services Endpoint Sub CA - ise3genvc	1/6/2027	Client Authentication	emp_C4-E9-0A-00-...	
ise3genvc.lab.local	ise3genvc.lab.local	1/3/2027	Server Authentication, Client Authentication	Self-Signed	

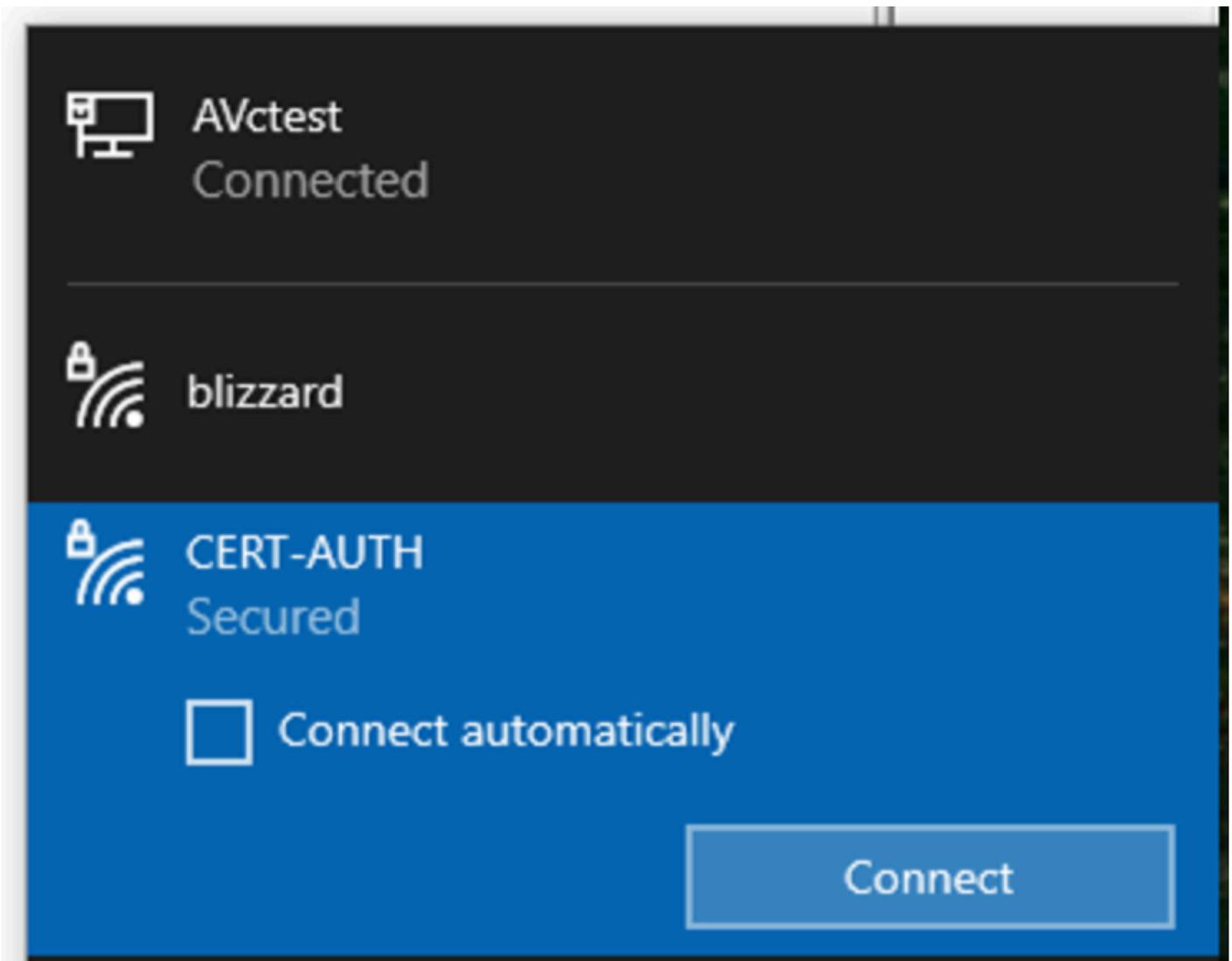
在其儲存區中移動證書

連線Windows電腦

將憑證移動到正確的儲存區後，請使用以下步驟連線到WLAN:

1. 按一下系統托盤中的network圖示可檢視可用的無線網路。

2. 找到並單擊您要連線的WLAN的名稱。
3. 按一下「Connect」，然後繼續任何其他提示，使用您的憑證進行驗證以完成連線過程。



連線到無線網路

在與WLAN的連線過程中出現提示時，選擇Connect using a certificate(使用證書連線)選項。



CERT-AUTH
Secured

Enter your user name and password

Connect using a certificate

OK

Cancel

使用證書作為憑據

這樣，您就可以使用證書成功連線到無線網路。

```
C:\>netsh wlan show interface
```

```
There is 1 interface on the system:
```

```
Name : Wi-Fi 3
Description : TP-Link Wireless USB Adapter
GUID : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
Physical address : 24:2f:d0:da:a5:63
State : connected
SSID : CERT-AUTH
BSSID : a4:88:73:9e:8d:af
Network type : Infrastructure
Radio type : 802.11ac
Authentication : WPA2-Enterprise
Cipher : CCMP
Connection mode : Profile
Channel : 36
Receive rate (Mbps) : 360
Transmit rate (Mbps) : 360
Signal : 100%
Profile : CERT-AUTH
```

```
Hosted network status : Not available
```

```
C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
```

```
EAP type : Microsoft: Smart Card or other certificate
```

驗證無線配置檔案

驗證

確認WLC正在廣播WLAN:

```
<#root>
```

```
POD6_9800#show wlan summ
```

```
Number of WLANs: 2
```

```
ID Profile Name SSID Status Security
```

```
-----
```

```
17
```

```
CERT-AUTH
```

```
CERT-AUTH
```

```
UP [WPA2][802.1x][AES]
```

確認WLC上的AP已啟動：

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-----
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

確保AP正在廣播WLAN:

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
-----
17 a488.739e.8da0
```

```
POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
-----
17
a488.739e.8daf
```

使用EAP-TLS連線的客戶端 :

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----
242f.d0da.a563 AP1 WLAN
```

```
17
IP Learn 11ac
```

Dot1x

Local

```
POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
Wireless LAN Network Name (SSID): CERT-AUTH
```

BSSID : a488.739e.8daf

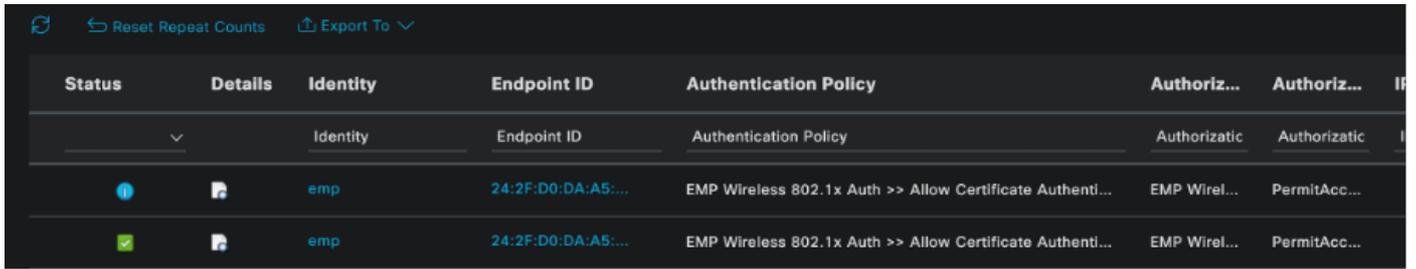
EAP Type : EAP-TLS

VLAN : 2124

Multicast VLAN : 0

VLAN : 2124

Cisco Radius ISE即時日誌 :



The screenshot shows a table of Cisco ISE logs. The table has columns for Status, Details, Identity, Endpoint ID, Authentication Policy, and Authoriz... (Authorization). The first row shows a failed authentication attempt with a status icon of a blue circle with an exclamation mark. The second row shows a successful authentication attempt with a status icon of a green checkmark.

Status	Details	Identity	Endpoint ID	Authentication Policy	Authoriz...	Authoriz...
		emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wirel...	PermitAcc...
		emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wirel...	PermitAcc...

ISE Radius即時日誌

詳細身份驗證型別 :

Authentication Details

Source Timestamp	2025-01-08 11:58:21.055
Received Timestamp	2025-01-08 11:58:21.055
Policy Server	ise3genvc
Event	5200 Authentication succeeded
Username	emp
Endpoint Id	24:2F:D0:DA:A5:63
Calling Station Id	24-2f-d0-da-a5-63
Endpoint Profile	TP-LINK-Device
Identity Group	User Identity Groups:Employee,Profiled
Audit Session Id	4D084E0A0000007E46F0C6F7
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	lab-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.78.8.77
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccess
Security Group	Employees

ISE詳細日誌

顯示EAP-TLS資料包的WLC EPC捕獲：

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

顯示EAP事務的WLC捕獲

- 資料包編號87對應於文檔開頭所述的EAP-TLS流中的步驟8。
- 資料包編號115對應於文檔開頭所述的EAP-TLS流中的步驟9。
- 資料包編號118對應於文檔開頭所述的EAP-TLS流中的步驟10。

顯示客戶端連線的無線活動(RA)跟蹤：此RA跟蹤經過過濾，以顯示身份驗證事務的一些相關行。

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (調試) 傳送加密的DTLS消息。目的IP 10.78.8.78[5256]，長499

2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求到10.106.33.23 1812 id 0/25,len 390

2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (資訊) 從id 1812/25 10.106.33.23 0、Access-Challenge、len 123接收的RADIUS

2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]傳送的EAPOL資料包 — 版本3,EAPOL型別EAP，負載長度6,EAP型別= EAP-TLS

2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]收到的EAPOL資料包 — 版本1,EAPOL型別EAP，負載長度204,EAP型別= EAP-TLS

2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求到10.106.33.23 1812 id 0/26,len 663

2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (資訊) 從id 1812/26 10.106.33.23 0、Access-Challenge、len 1135接收的RADIUS

2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]傳送的EAPOL資料包 — 版本3,EAPOL型別EAP，負載長度1012,EAP型別= EAP-TLS

2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]收到的EAPOL資料包 — 版本1,EAPOL型別EAP，負載長度6,EAP型別= EAP-TLS

2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求到10.106.33.23 1812 id 0/27,len 465

2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (資訊) 從id 1812/27 10.106.33.23 0、Access-Challenge、len 1131接收的RADIUS

2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]傳送的EAPOL資料包 — 版本3,EAPOL型別EAP，負載長度1008,EAP型別= EAP-TLS

2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]收到的EAPOL資料包 — 版本1,EAPOL型別EAP , 負載長度6,EAP型別= EAP-TLS

2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求到10.106.33.23 1812 id 0/28,len 465

2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS從id 1812/28 10.106.33.23 0、Access-Challenge、len 275接收

2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]傳送的EAPOL資料包 — 版本3,EAPOL型別EAP , 負載長度158,EAP型別= EAP-TLS

2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]收到的EAPOL資料包 — 版本1,EAPOL型別EAP , 負載長度1492,EAP型別= EAP-TLS

2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求到10.106.33.23 1812 id 0/29,len 1961

2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS從id 1812/29 10.106.33.23 0、Access-Challenge、len 123接收

2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]傳送的EAPOL資料包 — 版本3,EAPOL型別EAP , 負載長度6,EAP型別= EAP-TLS

2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]收到的EAPOL資料包 — 版本1,EAPOL型別EAP , 負載長度1492,EAP型別= EAP-TLS

2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求到10.106.33.23 1812 id 0/30,len 1961

2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (資訊) 從id 1812/30 10.106.33.23 0、Access-Challenge、len 123接收的RADIUS

2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]傳送的EAPOL資料包 — 版本3,EAPOL型別EAP , 負載長度6,EAP型別= EAP-TLS

2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]收到的EAPOL資料包 — 版本1,EAPOL型別EAP , 負載長度1492,EAP型別= EAP-TLS

2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求到10.106.33.23 1812 id 0/31,len 1961

2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (資訊) 從id 1812/31 10.106.33.23 0、Access-Challenge、len 123接收的RADIUS

2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]傳送的EAPOL資料包 — 版本3,EAPOL型別EAP , 負載長度6,EAP型別= EAP-TLS

2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563 capwap_90800005]收到的EAPOL資料包 — 版本1,EAPOL型別EAP , 負載長度247,EAP型別= EAP-TLS

2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求到10.106.33.23 1812 id 0/32,len 706

2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (資訊) 從id 1812/32

10.106.33.23 0、Access-Challenge、len 174接收的RADIUS
2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563
capwap_90800005]傳送的EAPOL資料包 — 版本3,EAPOL型別EAP , 負載長度57,EAP型別= EAP-
TLS
2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563
capwap_90800005]收到的EAPOL資料包 — 版本1,EAPOL型別EAP , 負載長度6,EAP型別= EAP-
TLS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (資訊) RADIUS傳送訪問請求
到10.106.33.23 1812 id 0/33,len 465
2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (資訊) 從id 1812/33
10.106.33.23 0、Access-Accept、len 324接收的RADIUS
2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (資訊) [242f.d0da.a563
capwap_90800005] Raised eap方法EAP-TLS的身份更新事件

疑難排解

除典型無線802.1x故障排除步驟外，沒有針對此問題的特定故障排除步驟：

1. 執行客戶端RA跟蹤調試以檢查身份驗證過程。
2. 執行WLC EPC擷取，檢查使用者端、WLC和RADIUS伺服器之間的封包。
3. 檢查ISE即時日誌以驗證請求是否與正確的策略匹配。
4. 在Windows終結點上驗證證書是否正確安裝，以及整個信任鏈是否存在。

參考資料

- [證書調配門戶常見問題解答，版本3.2](#)
- [瞭解ISE內部證書頒發機構服務](#)
- [瞭解和配置WLC和ISE的EAP-TLS](#)

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）。