瞭解和配置WLC和ISE的EAP-TLS

目錄

簡介

本文說明如何使用802.1X和可擴展身份驗證協定EAP-TLS設定無線區域網(WLAN)

必要條件

需求

思科建議您瞭解以下主題：

- 802.1X身份驗證過程
- 憑證

採用元件

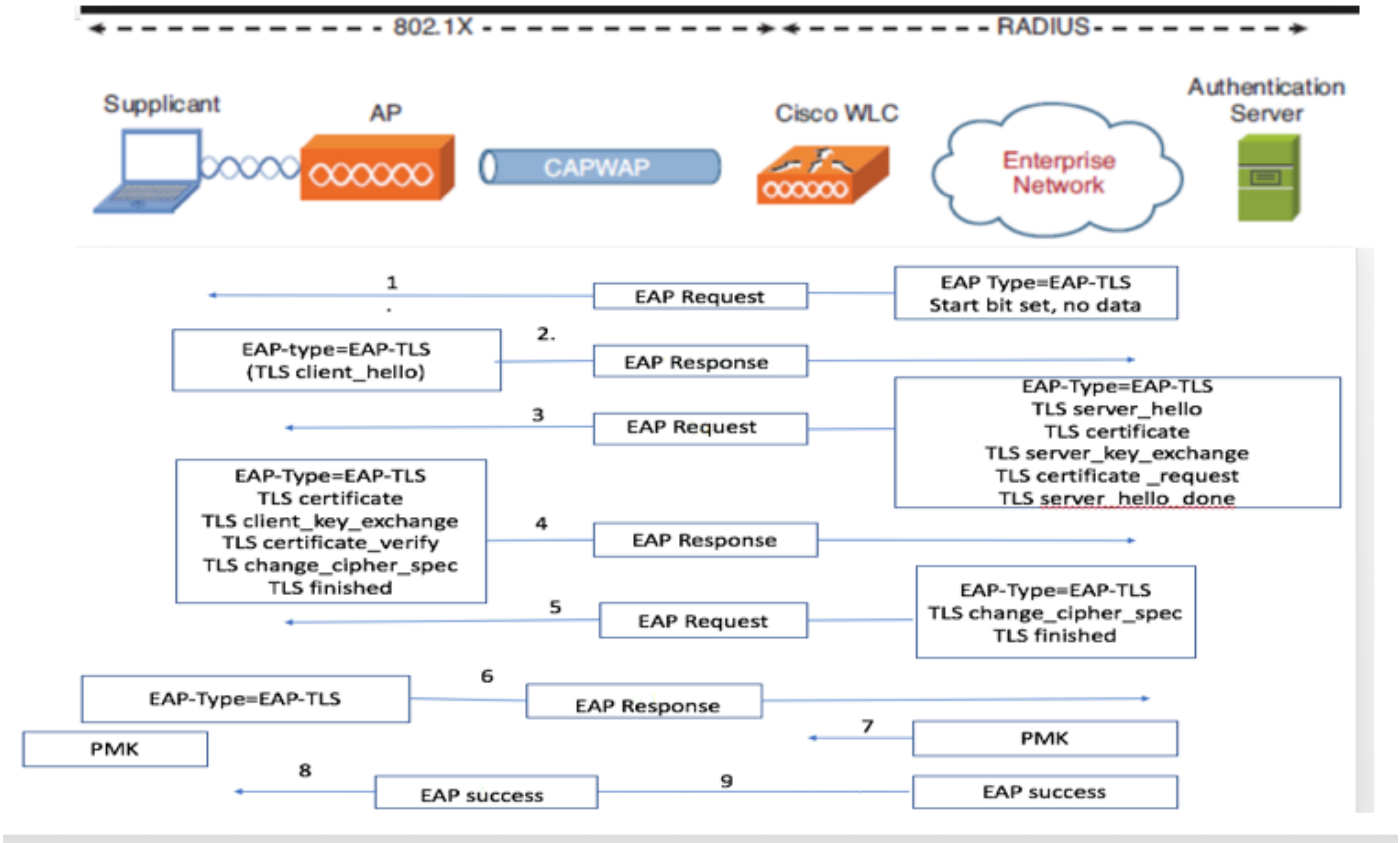
本文中的資訊係根據以下軟體和硬體版本：

- WLC 3504 8.10 版
- 身分識別服務引擎 (ISE) 2.7 版

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

EAP-TLS 流程



EAP-TLS 流程中的步驟

1. 無線用戶端與存取點 (AP) 建立關聯。AP不允許客戶端此時傳送任何資料並傳送身份驗證請求。請求方隨後使用EAP-Response Identity進行響應。WLC 接著會將使用者 ID 資訊傳播至驗證伺服器。RADIUS 伺服器會以 EAP-TLS 起始封包回應用戶端。EAP-TLS 對話會在此時開始。
2. 對等體將EAP-Response傳送回包含「client_hello」握手消息的身份驗證伺服器，該握手消息是設定為NULL的密碼
3. 驗證伺服器會以 Access-challenge 封包回應，其中包含：

```
TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.
```

4.客戶端使用EAP-Response消息進行響應，該消息包含：

```
Certificate ¬ Server can validate to verify that it is trusted.
```

```
client_key_exchange

certificate_verify ¬ Verifies the server is trusted

change_cipher_spec

TLS finished
```

5.客戶端成功進行身份驗證後，RADIUS伺服器會使用訪問質詢進行響應，其中包含「change_cipher_spec」和握手完成消息。

6.收到此資訊時，使用者端會驗證雜湊以進行驗證radius伺服器。

7.在TLS握手過程中，動態地從金鑰派生出新的加密金鑰

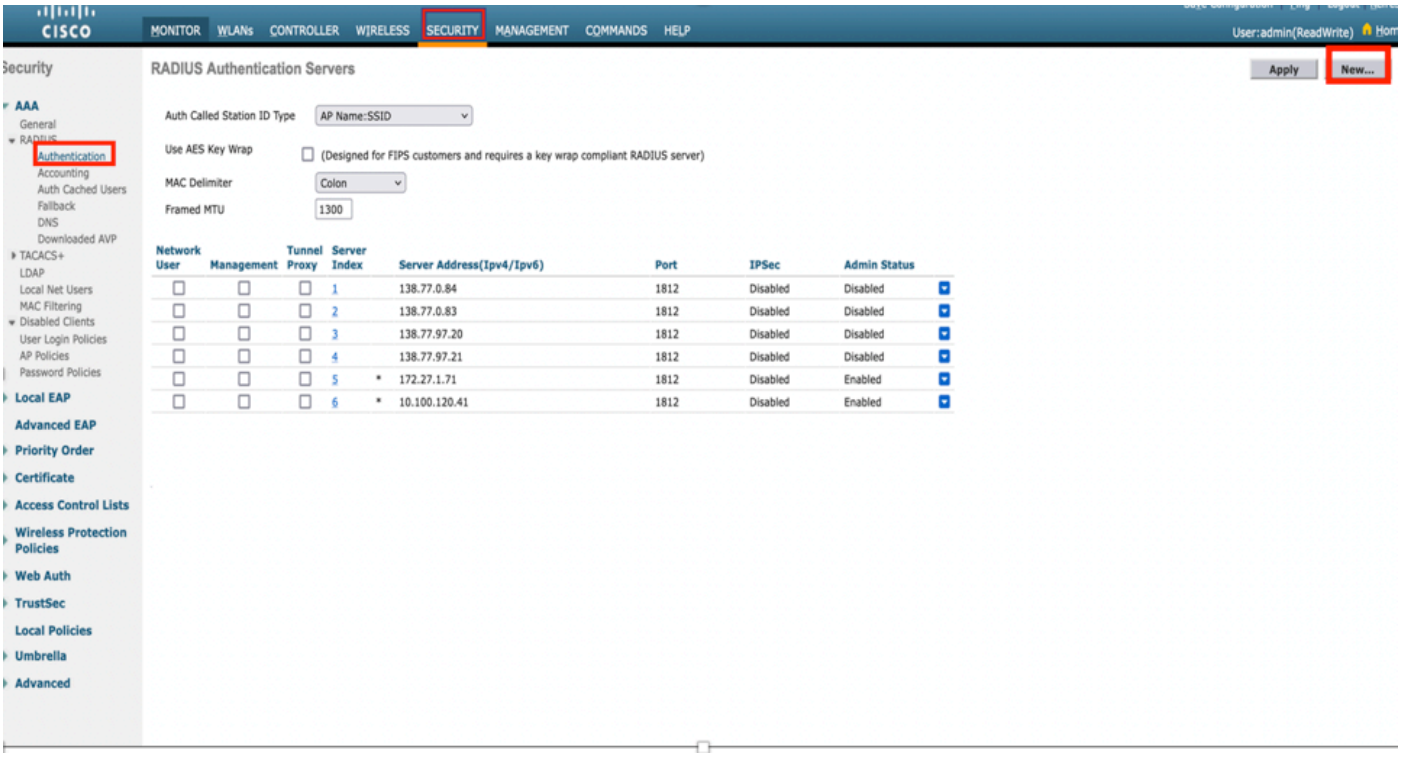
8/9.EAP-Success最終從伺服器傳送到身份驗證器，然後傳遞給請求方。

此時，支援 EAP-TLS 的無線用戶端可存取無線網路。

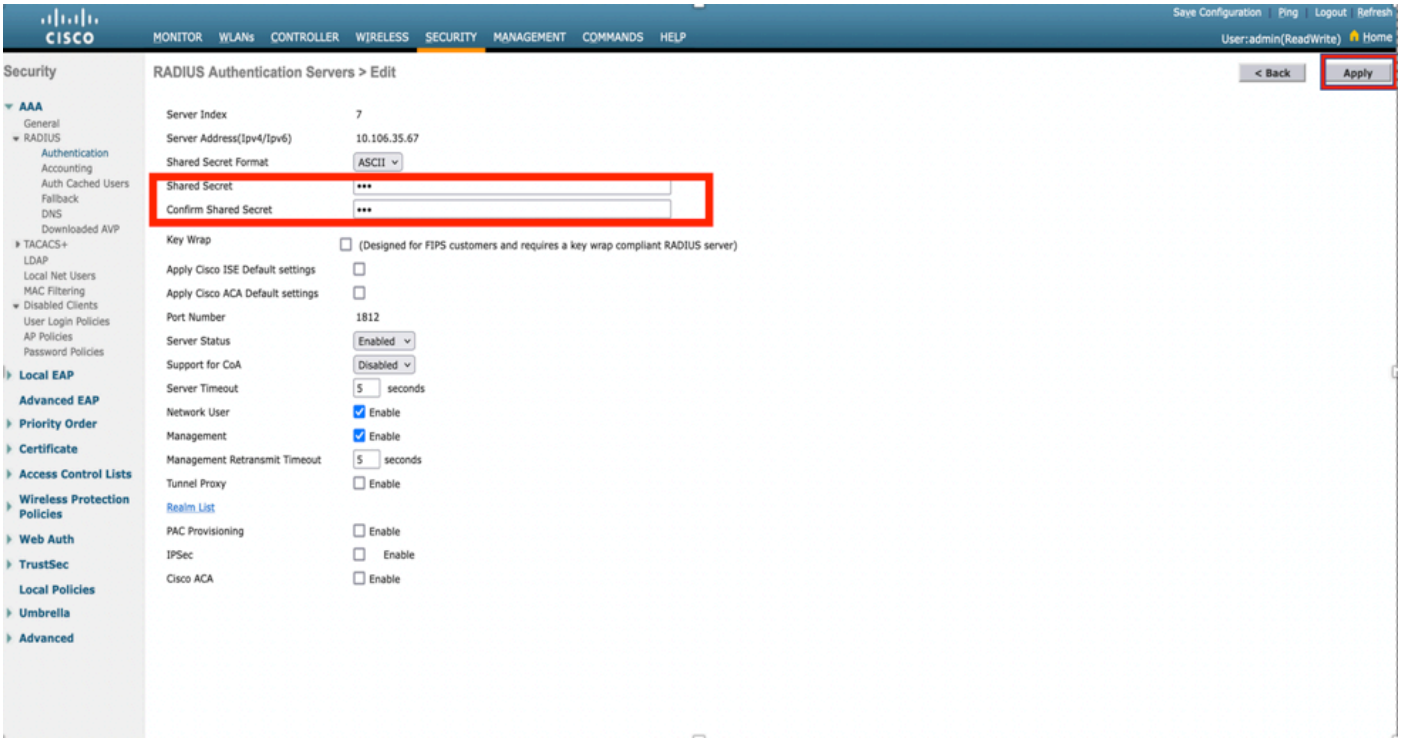
設定

Cisco無線LAN控制器

步驟 1. 第一步為設定 Cisco WLC 的 RADIUS 伺服器。若要新增 RADIUS 伺服器，請導覽至**「安全性」>「RADIUS」>「驗證」**。按一下**「新增」**（如影像所示）。



步驟 2. 此處，您需要輸入 IP 位址和共用密碼 <password>，用於驗證 ISE 的 WLC。按一下**「套用」**以繼續（如影像所示）。

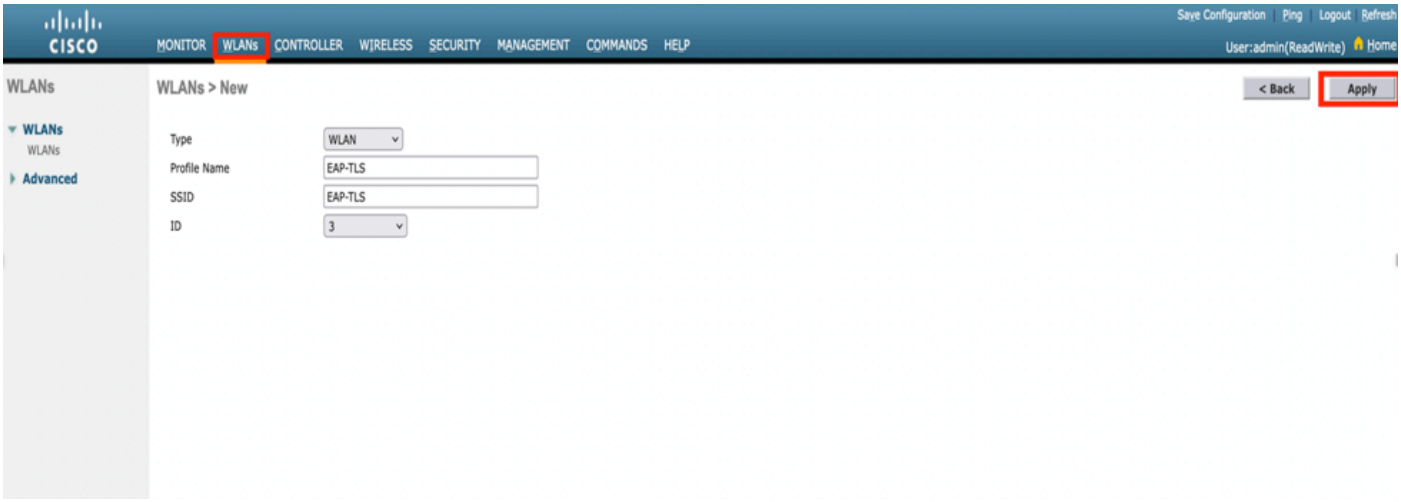


步驟 3. 建立 WLAN 以進行 RADIUS 驗證。

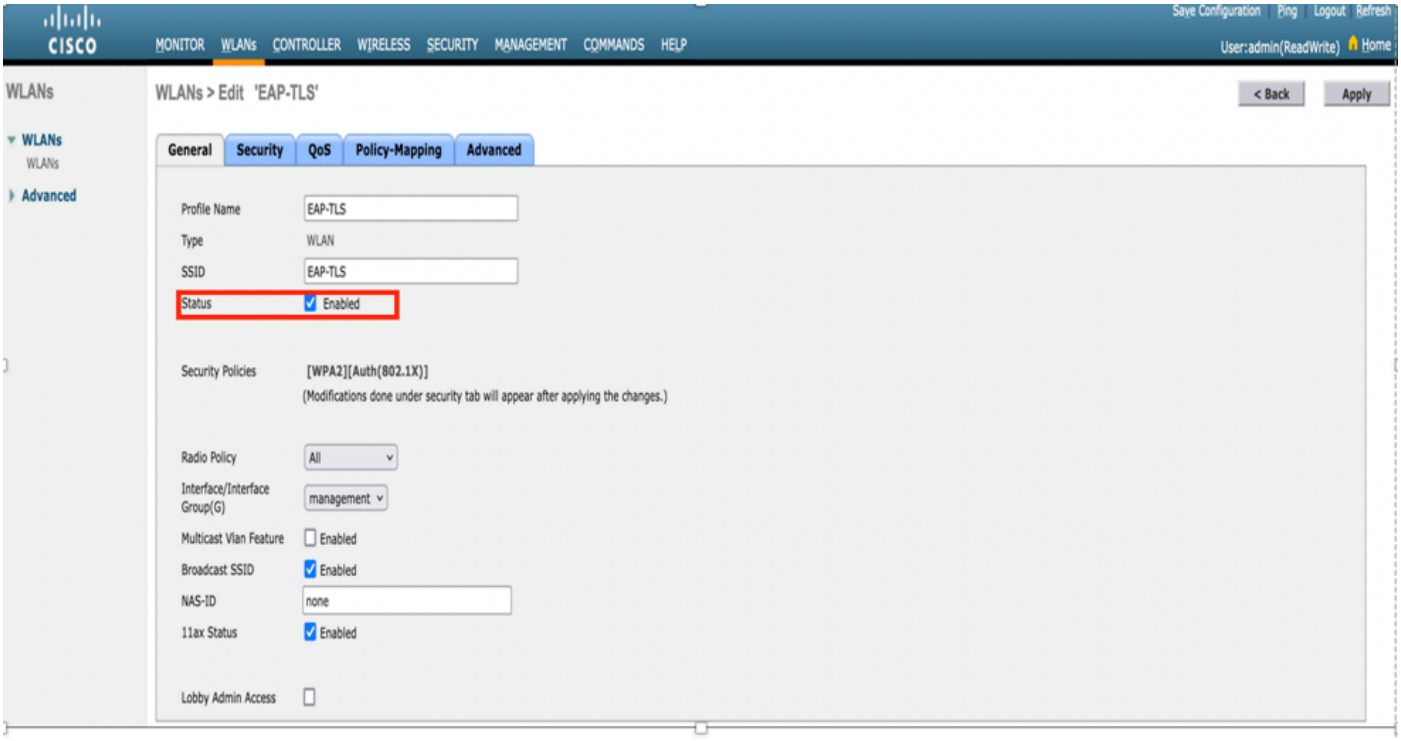
現在，您可以建立新的 WLAN，並將其設定為使用 WPA-Enterprise 模式，使其得以使用 RADIUS 進行驗證。

步驟 4. 從主功能表選取 **WLAN**，選擇**新建**，然後按一下**執行**（如影像所示）。

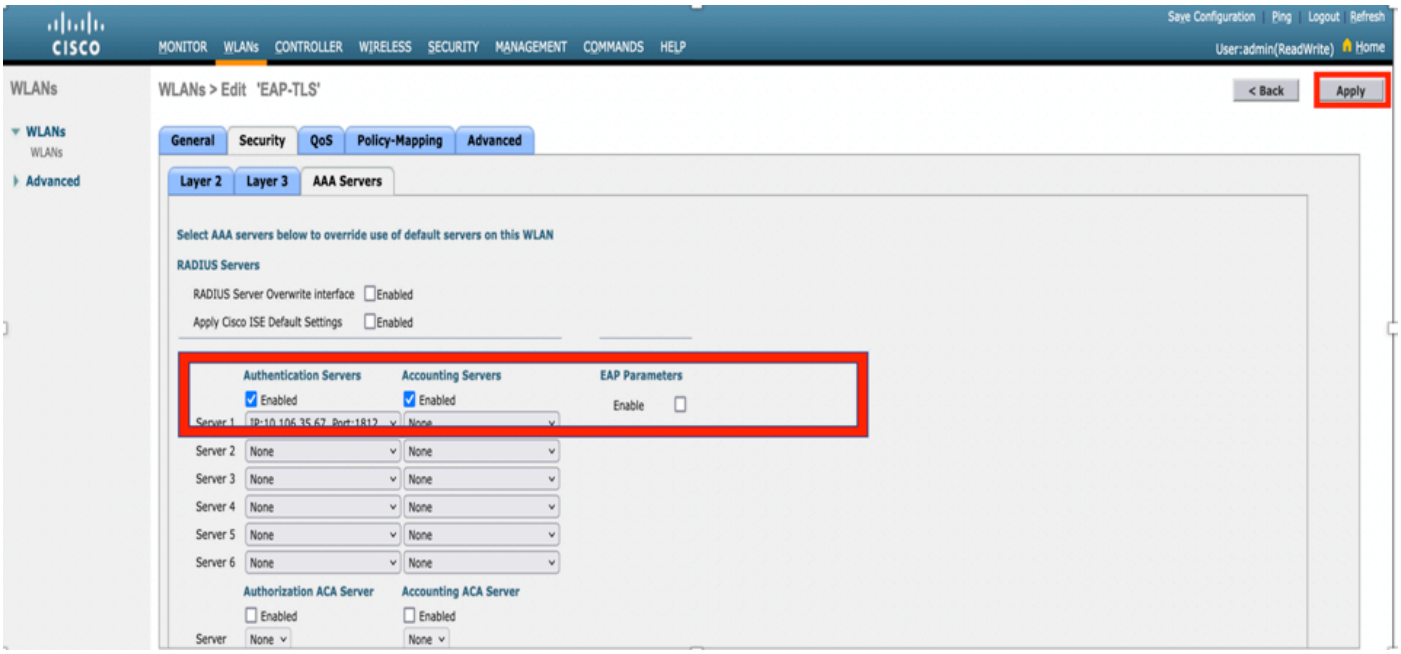
步驟5.將新的WLAN命**名為EAP-TLS**。按一下「套用」以繼續（如影像所示）。



步驟 6. 按一下「**一般**」，並確認狀態為「**啟用**」。預設安全性原則為 802.1X 驗證和 WPA2（如影像所示）。



步驟 7. 現在，導覽至「**安全性**」>「**AAA 伺服器**」索引標籤，選取您剛剛設定的 RADIUS 伺服器（如影像所示）。



附註：繼續執行之前，請務必確認您可從 WLC 連線至 RADIUS 伺服器。RADIUS 使用 UDP 連接埠 1812（用於驗證），因此您需要確認此流量不會在網路任何位置遭封鎖。

使用 Cisco WLC 的 ISE

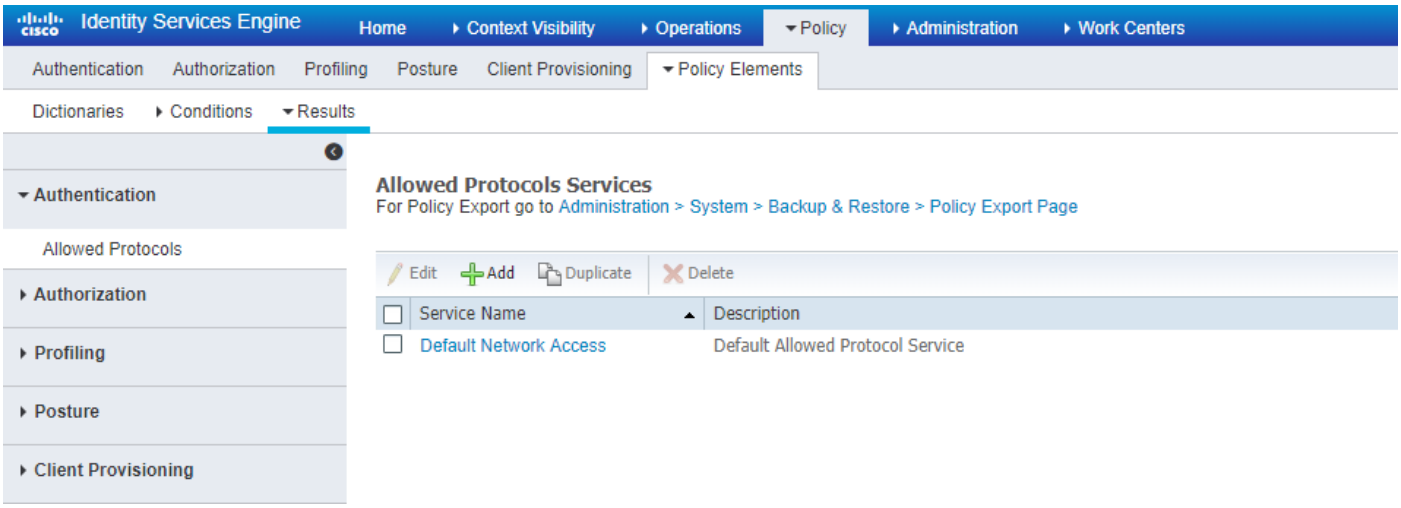
EAP-TLS 設定

若要建置原則，您需要建立允許的通訊協定清單，以用於我們的原則。 由於 dot1x 原則已寫入，因

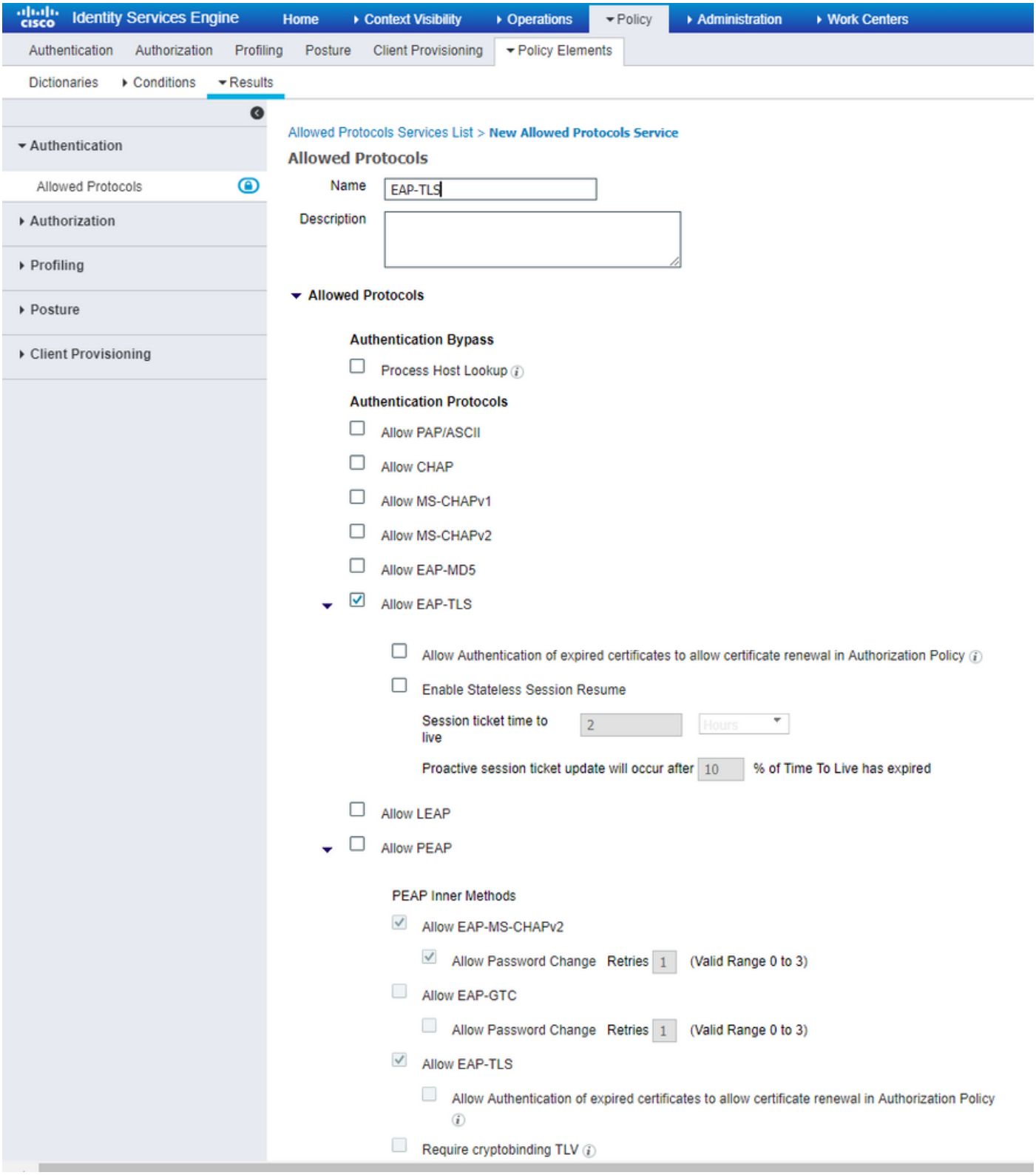
此請根據原則設定方式指定允許的 EAP 類型。

如果您使用預設值，則允許大多數EAP型別進行身份驗證，如果您需要鎖定對特定EAP型別的訪問，則這些型別不是首選的。

步驟 1. 導覽至**「原則」>「原則項目」>「結果」>「驗證」>「允許的通訊協定」**，然後按一下**「新增」**（如影像所示）。

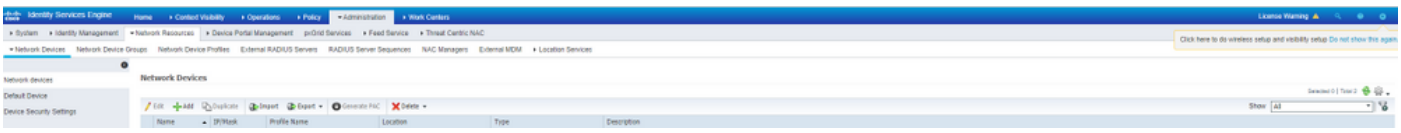


步驟 2. 在此「允許的通訊協定」清單中，可以輸入清單的名稱。在此案例中，**「允許 EAP-TLS」**方塊已核取，而其他方塊已取消核取（如影像所示）。

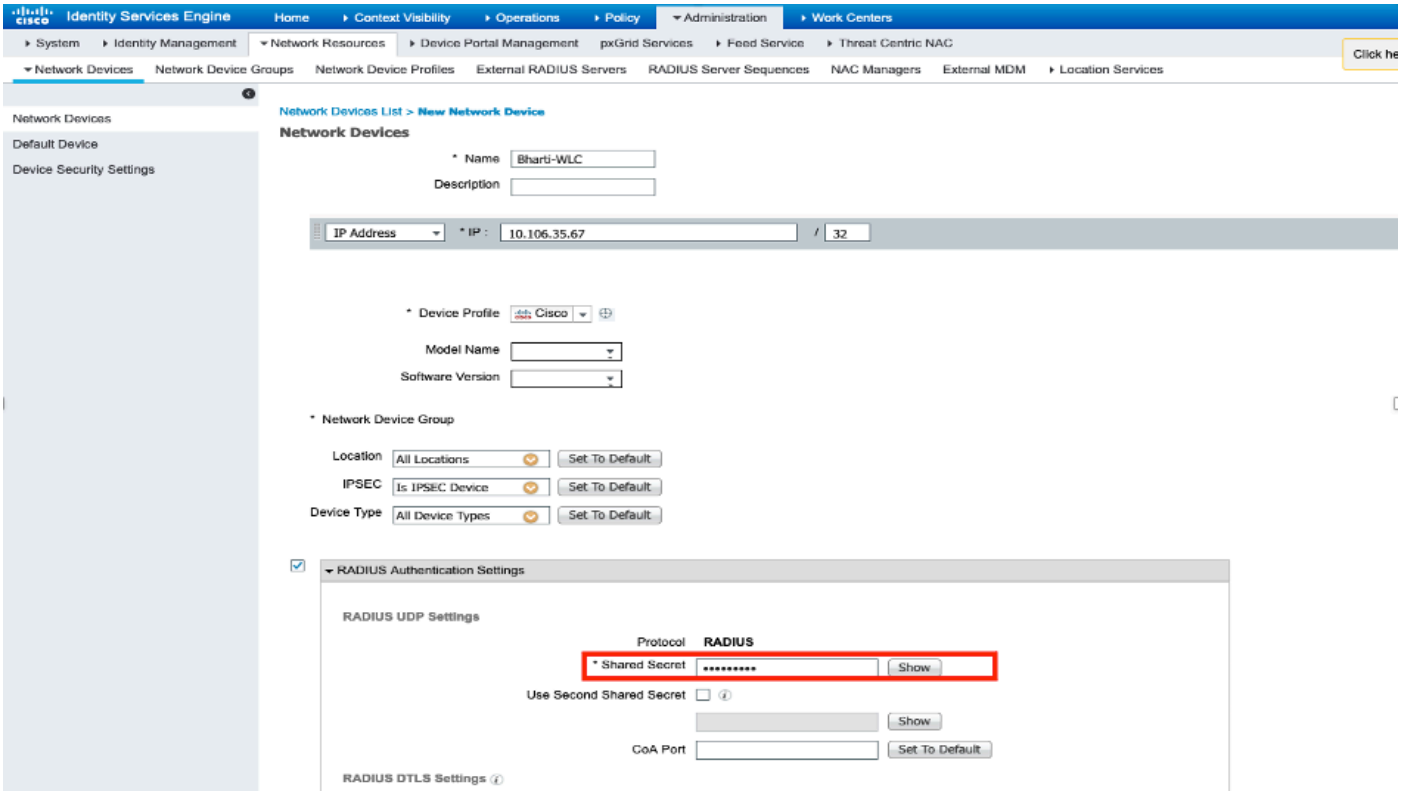


ISE 的 WLC 設定

步驟 1. 開啟 ISE 主控台，然後導覽至**「管理」>「網路資源」>「網路裝置」>「新增」**（如影像所示）。

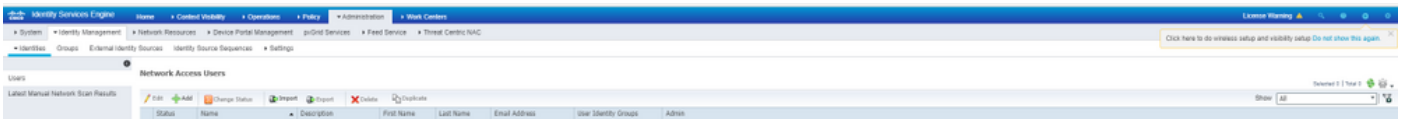


步驟 2. 輸入值（如影像所示）。

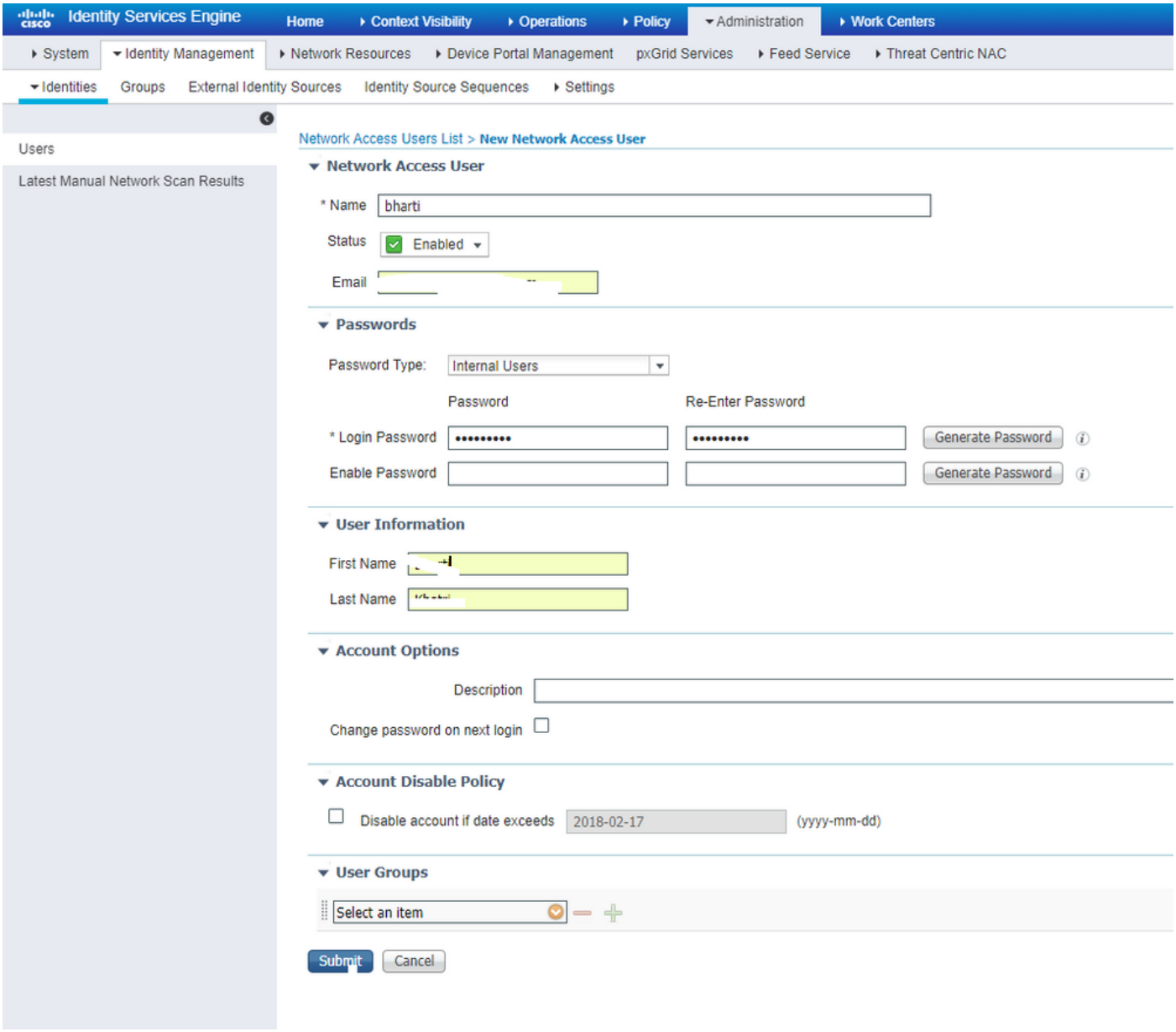


在 ISE 上建立新使用者

步驟 1. 導覽至**「管理」>「身分管理」>「身分」>「使用者」>「新增」**（如影像所示）。



步驟 2. 輸入資訊（如影像所示）。

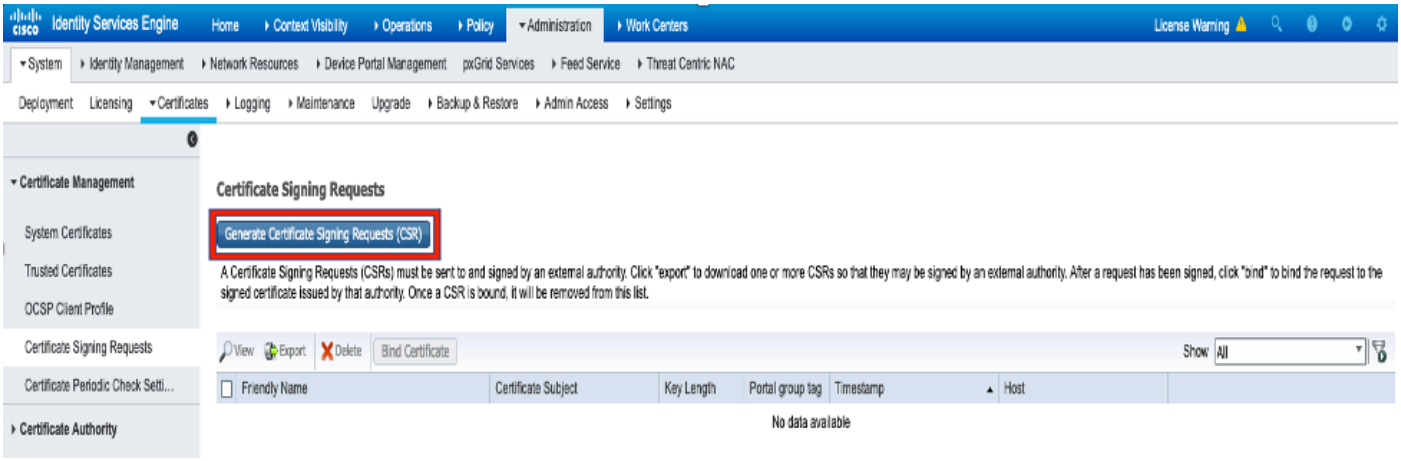


ISE 的信任憑證

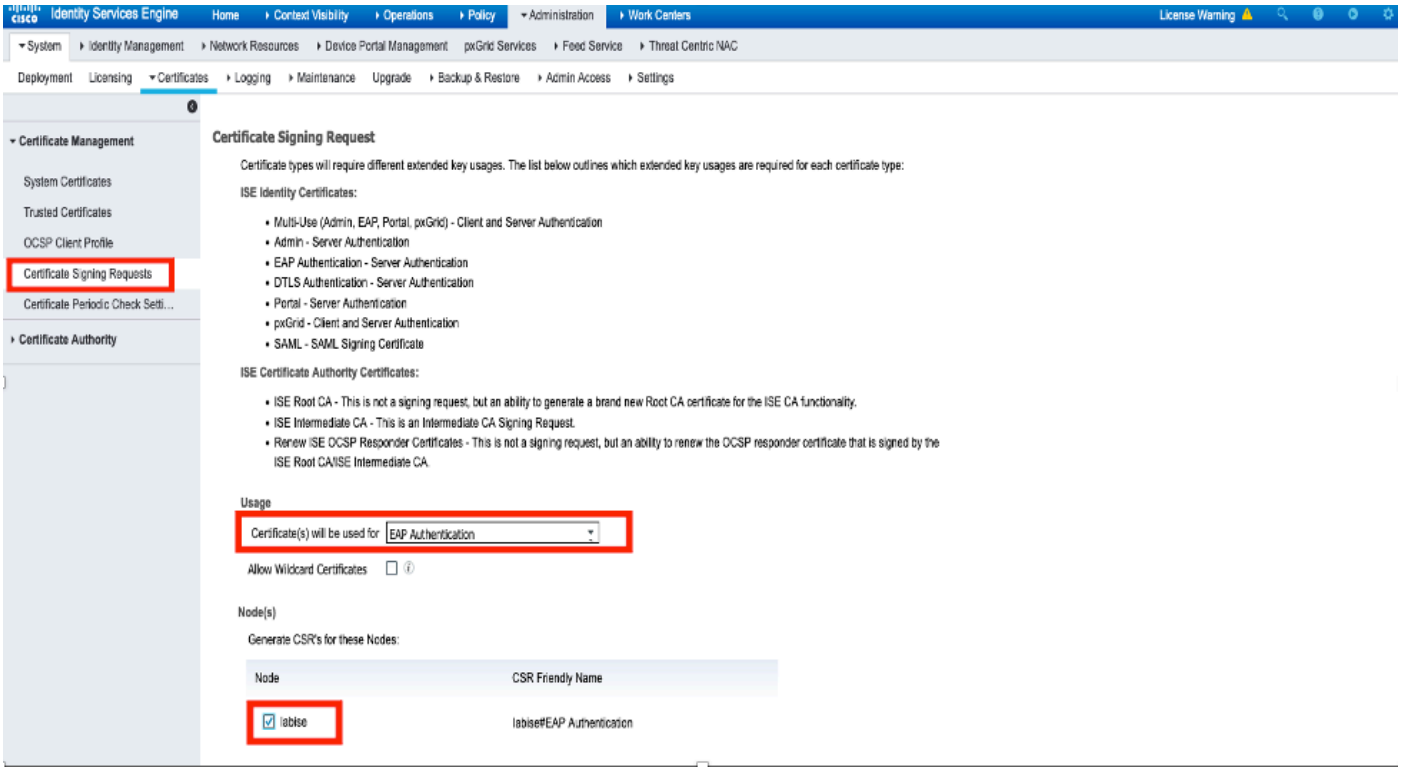
步驟 1. 導覽至**「管理」>「系統」>「憑證」>「憑證管理」>「受信任的憑證」**。

按一下**「匯入」**以將憑證匯入至 ISE。在 ISE 新增 WLC 並建立使用者後，您需要執行 EAP-TLS 最重要的作業：信任 ISE 的憑證。若要進行這項作業，我們需要產生 CSR。

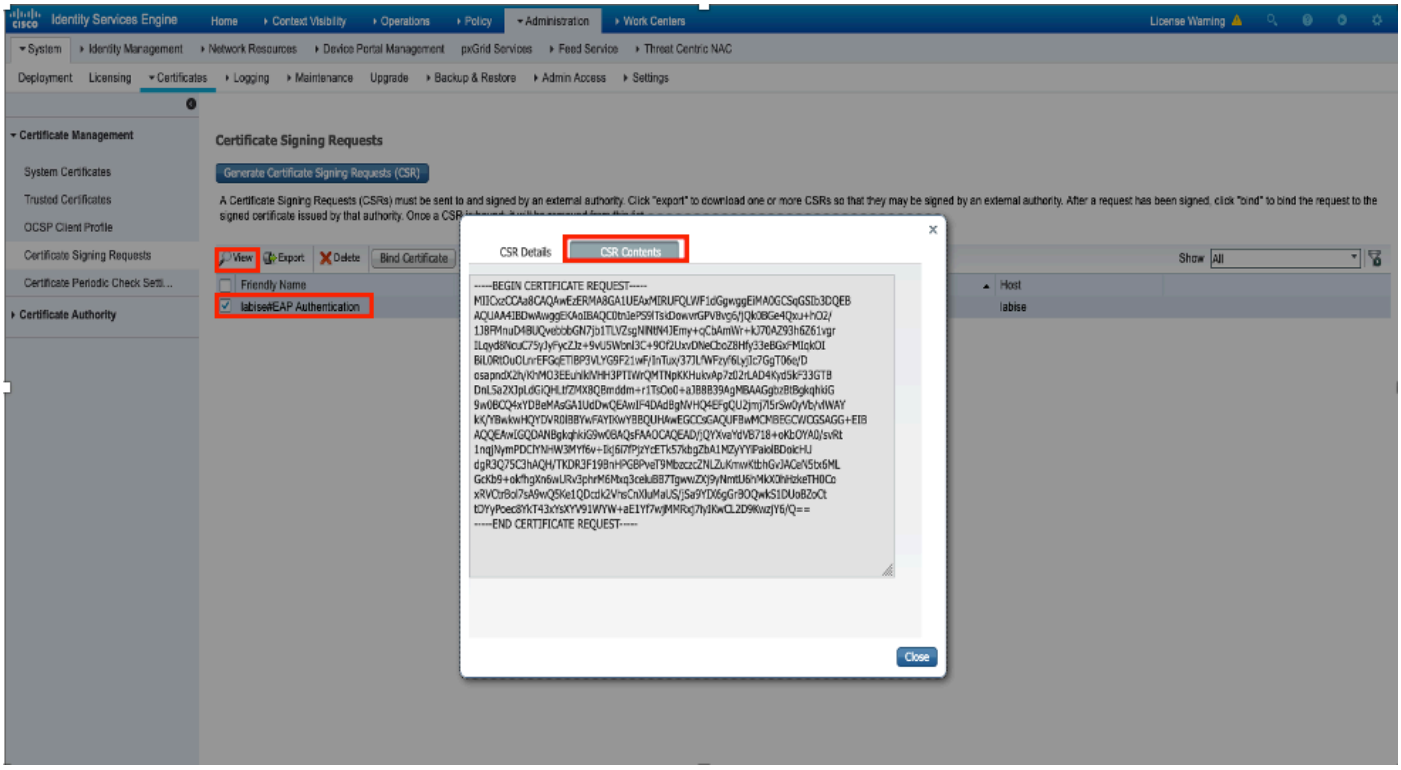
步驟 2. 導覽至**「管理」 >「憑證」>「憑證簽署要求」>「產生憑證簽署要求 (CSR)」**（如影像所示）。



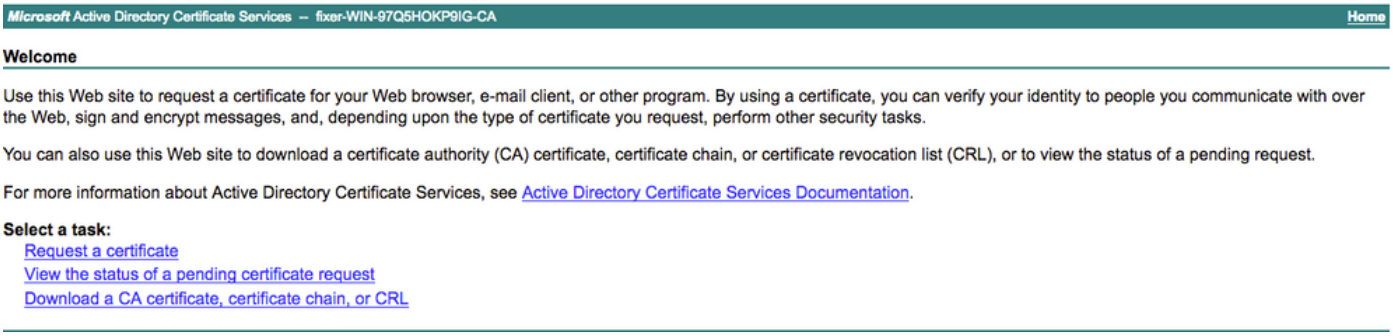
步驟3。若要產生CSR，請導覽至**Usage**，然後從**Certificate(s)as for**下拉選項中選擇**EAP Authentication**，如下圖所示。



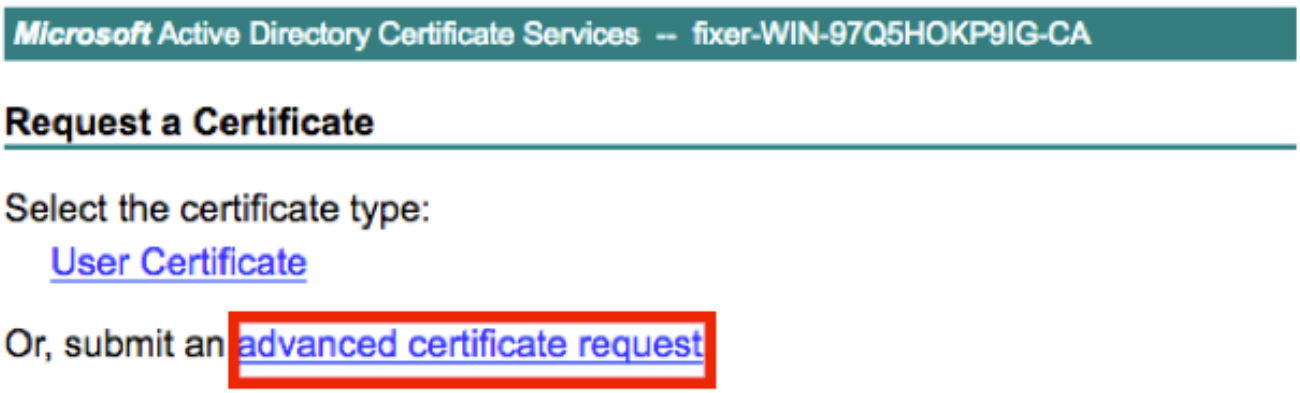
步驟 4. 在 ISE 產生的 CSR 可檢視。按一下「**檢視**」（如影像所示）。



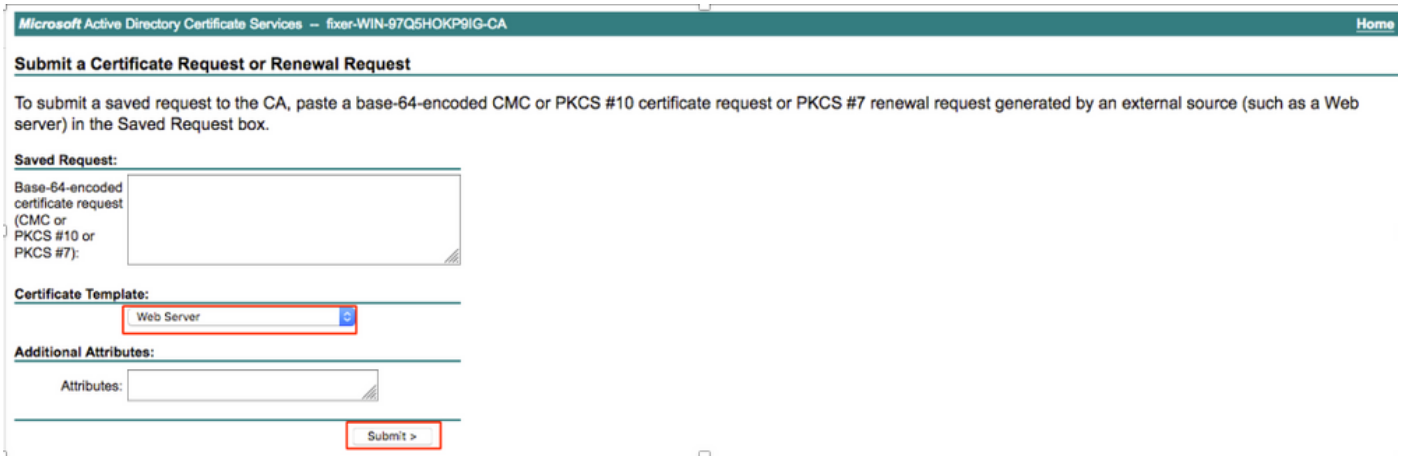
步驟 5. 產生 CSR 後，請瀏覽 CA 伺服器，然後按一下「**要求憑證**」（如影像所示）：



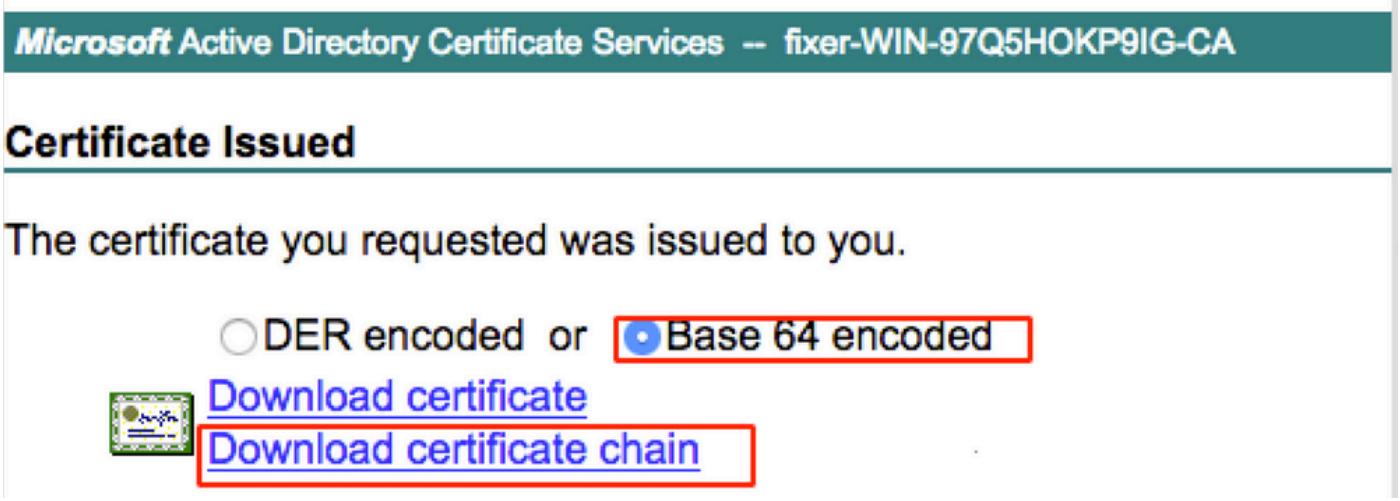
步驟 6. 要求憑證後，您會取得「**使用者憑證**」和「**進階憑證要求**」的選項，按一下**進階憑證要求**（如影像所示）。



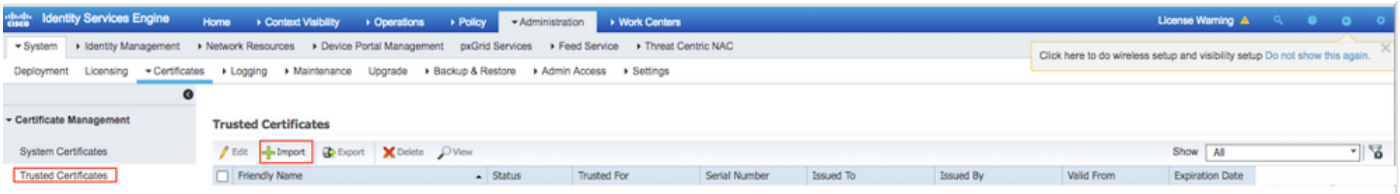
步驟 7. 在「**Base-64 編碼的憑證要求**」中貼上產生的 CSR。從「**憑證範本：**」下拉式選項，選擇「**Web 伺服器**」「，然後按一下**提交**」（如影像所示）。

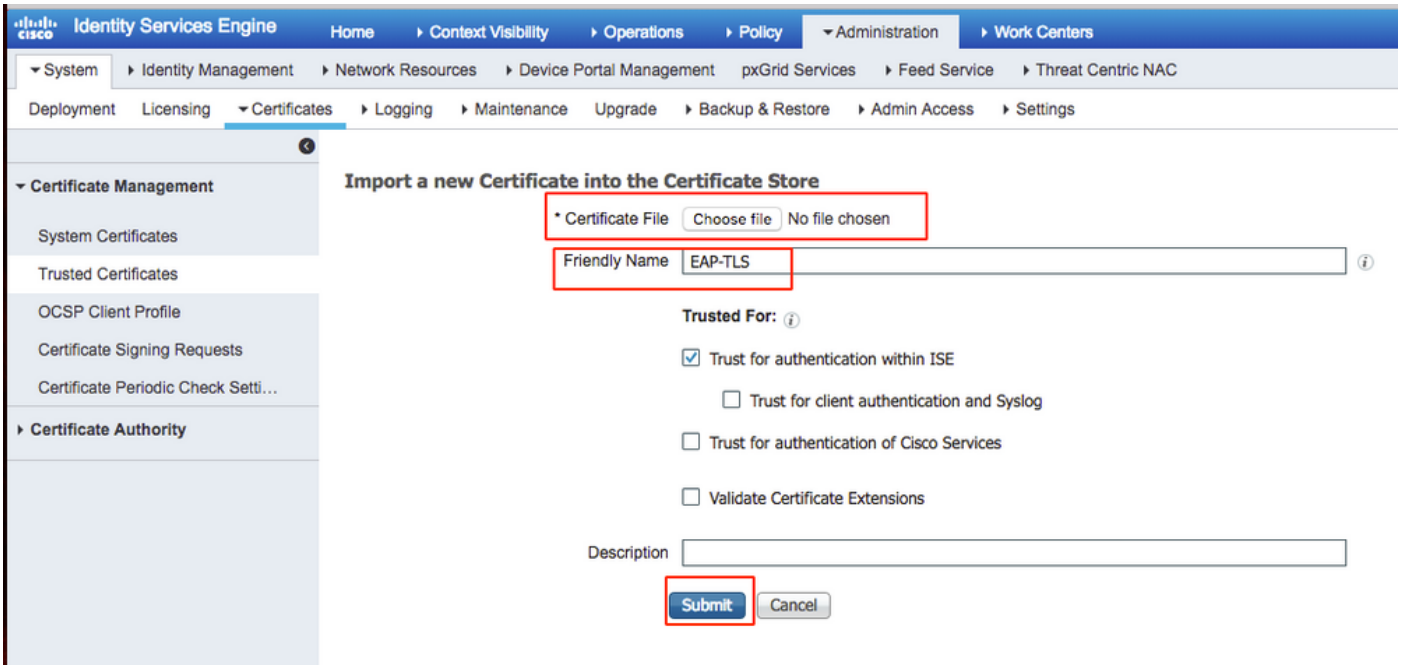


步驟 8. 按一下「**提交**」後，您會取得選取憑證類型的選項，選取「**Base-64 編碼**」，然後按「**下載憑證鏈結**」（如影像所示）。

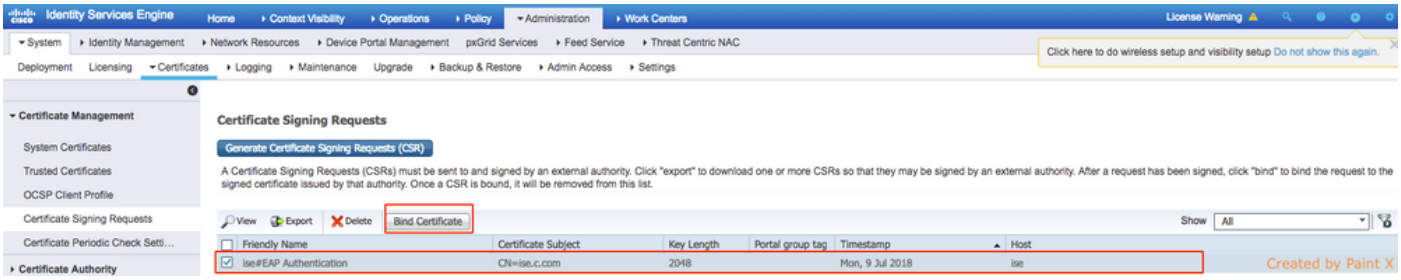


步驟 9. ISE 伺服器的憑證下載隨即完成。您可以提取證書，該證書包含兩個證書，一個根證書和其他中間證書。根憑證可在「**管理**」>「**憑證**」>「**受信任的憑證**」>「**匯入**」下匯入（如影像所示）。

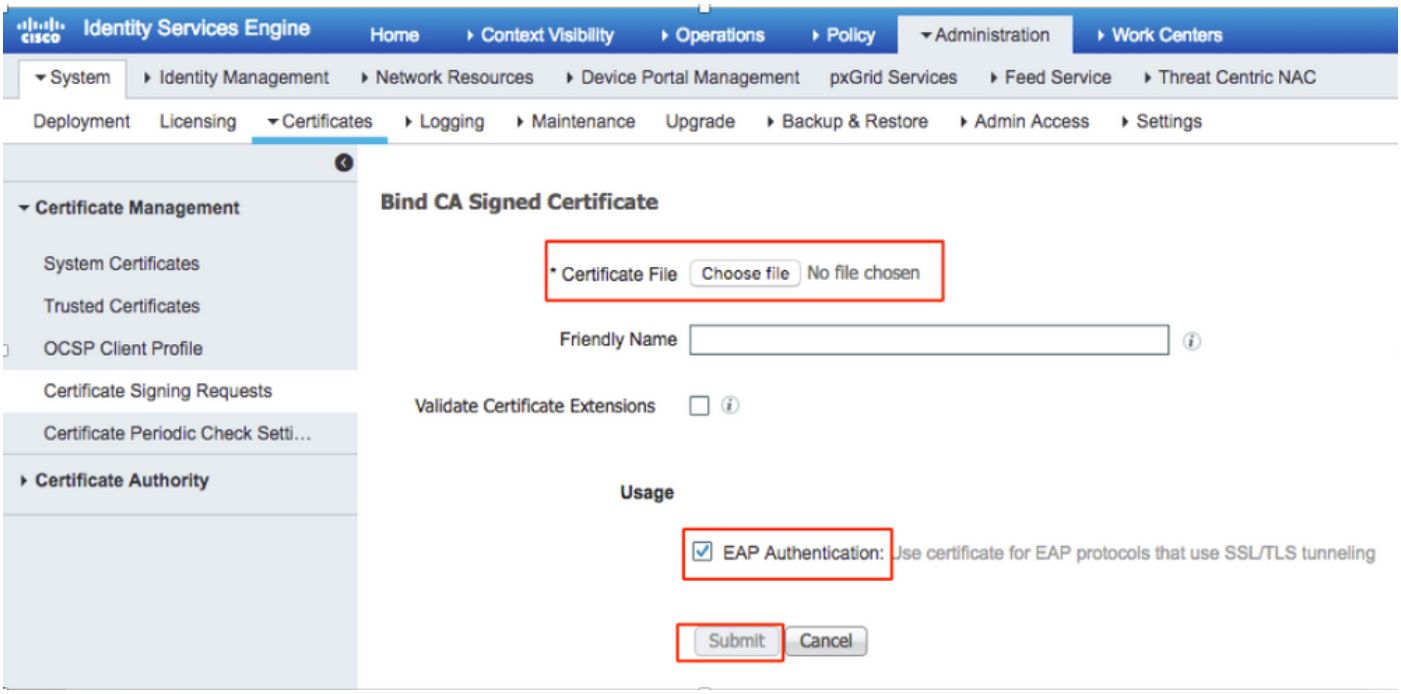




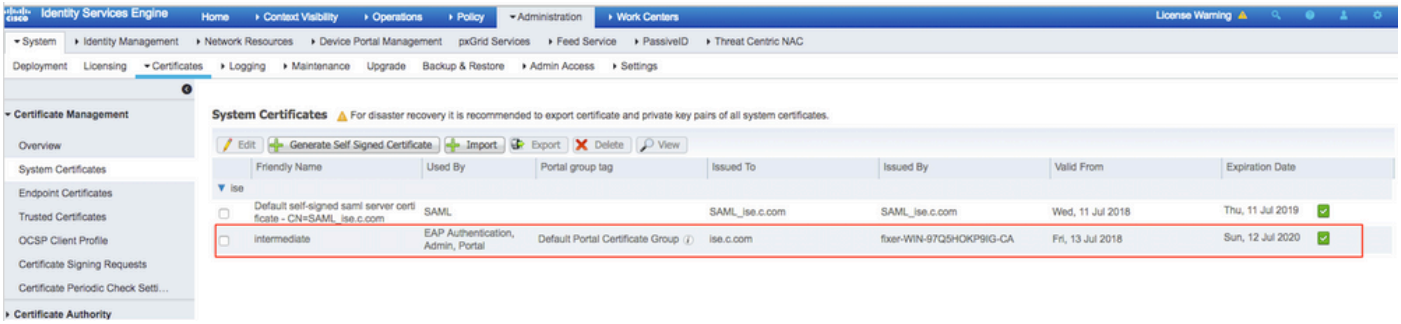
步驟 10. 按一下「**提交**」後，該憑證會新增至受信任的憑證清單。此外，需要使用中繼憑證才可與 CSR 繫結（如影像所示）。



步驟 11. 按一下「**繫結憑證**」後，其中具有選項可選擇儲存於桌上型電腦的憑證檔案。瀏覽至中繼憑證，然後按一下「**提交**」（如影像所示）。



步驟 12.若要檢視憑證，請導覽至「**管理**」>「**憑證**」>「**系統憑證**」（如影像所示）。



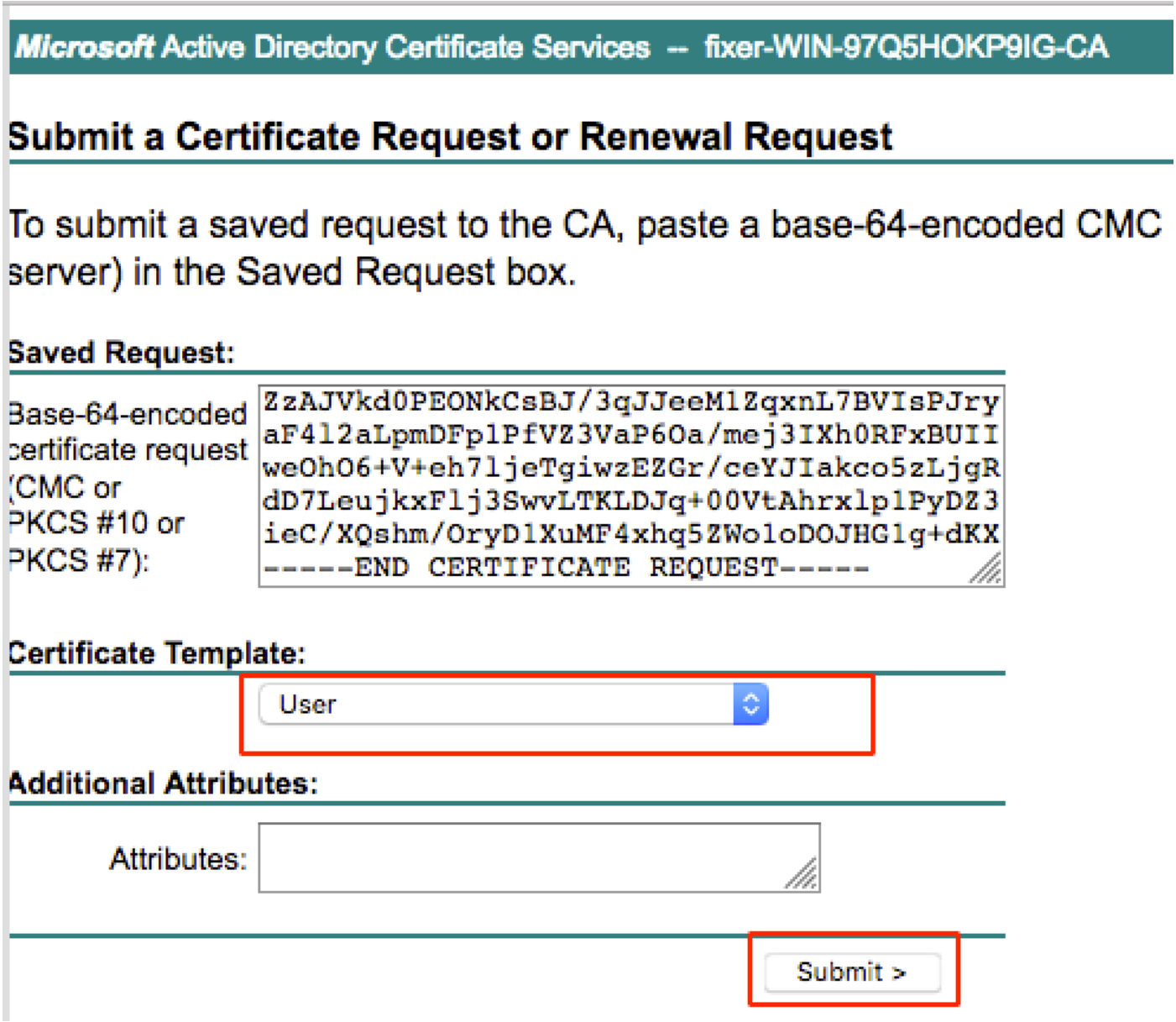
EAP-TLS 的用戶端

下載用戶端電腦（Windows 桌上型電腦）的使用者憑證

步驟 1. 若要透過 EAP-TLS 驗證無線使用者，您必須產生用戶端憑證。將您的 Windows 電腦連接至網路，即可存取伺服器。開啟 Web 瀏覽器，然後輸入此網址：https://sever ip addr/certsrv---

步驟 2. 請注意， CA 必須與為 ISE 下載憑證時使用的 CA 相同。

為此，您需要瀏覽用於下載伺服器憑證的相同 CA 伺服器。在相同 CA 上，按一下「**要求憑證**」（如同先前執行的動作），但此時您需要選取「**使用者**」做為憑證範本（如影像所示）。



步驟 3. 接著，按一下「**下載憑證鏈結**」（如同先前針對伺服器執行的動作）。

取得憑證後，請遵循以下步驟，以在 Windows 筆記型電腦上匯入憑證：

步驟 4. 若要匯入憑證，您需要透過 Microsoft Management Console (MMC) 存取。

1. 若要開啟 MMC，請導覽至**「開始」>「執行」>「MMC」**。
2. 導覽至**「檔案」>「新增/移除嵌入式管理單元」。**
3. 按兩下「**憑證**」。
4. 選取「**電腦帳戶**」。
5. 選取「**本機電腦**」>「**完成**」。
6. 按一下「**確定**」，以結束「嵌入式管理單元」視窗。
7. 按一下**「憑證」>「個人」>「憑證」**旁的 **[+]**。
8. 以滑鼠右鍵按一下「**憑證**」，然後選取「**所有工作**」>「**匯入**」。
9. 按「**Next**」（下一步）。
10. 按一下「**Browse**」。
11. 選取您想匯入的 **.cer, .crt, or .pfx**。
12. 按一下「**Open**」。
13. 按「**Next**」（下一步）。

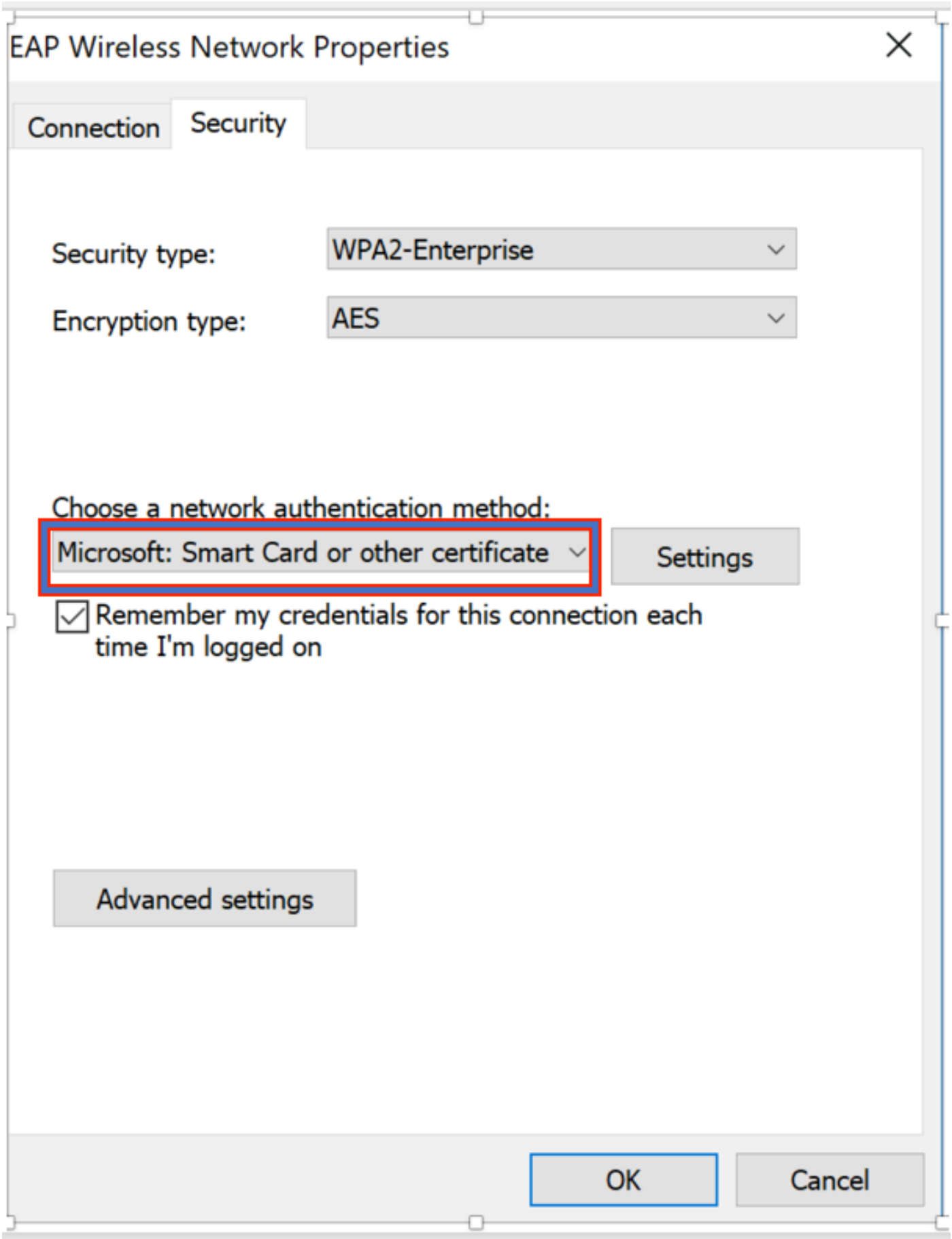
14. 選取「**自動根據憑證類型來選取憑證存放區**」。
15. 按一下「**完成並確定**」。

憑證匯入完成後，您需要將無線用戶端（此範例為 Windows 桌上型電腦）設定為 EAP-TLS。

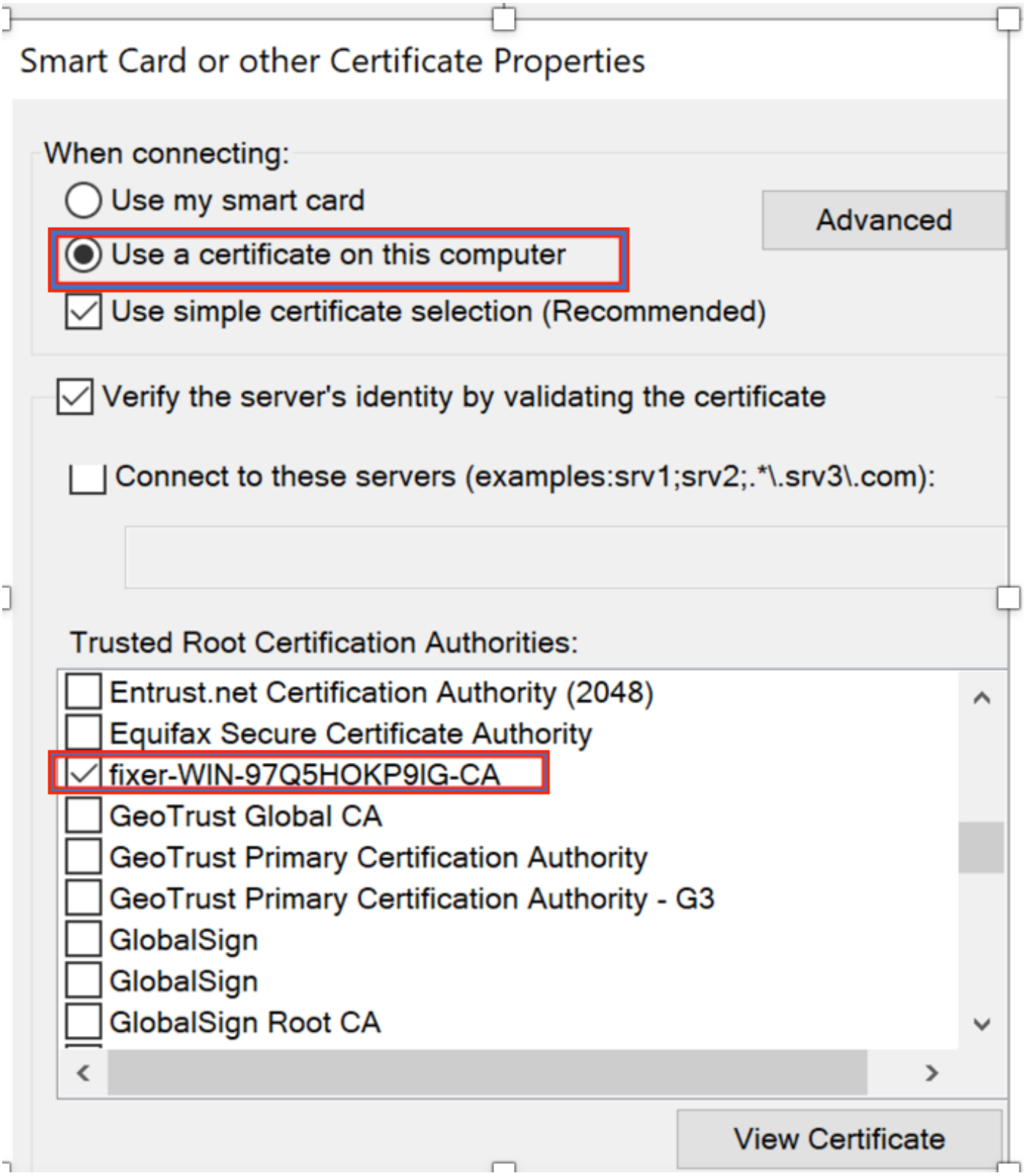
EAP-TLS 的無線設定檔

步驟 1. 變更先前為受保護的可延伸驗證通訊協定 (PEAP) 建立的無線設定檔，以改用 EAP-TLS。按一下「**EAP 無線設定檔**」。

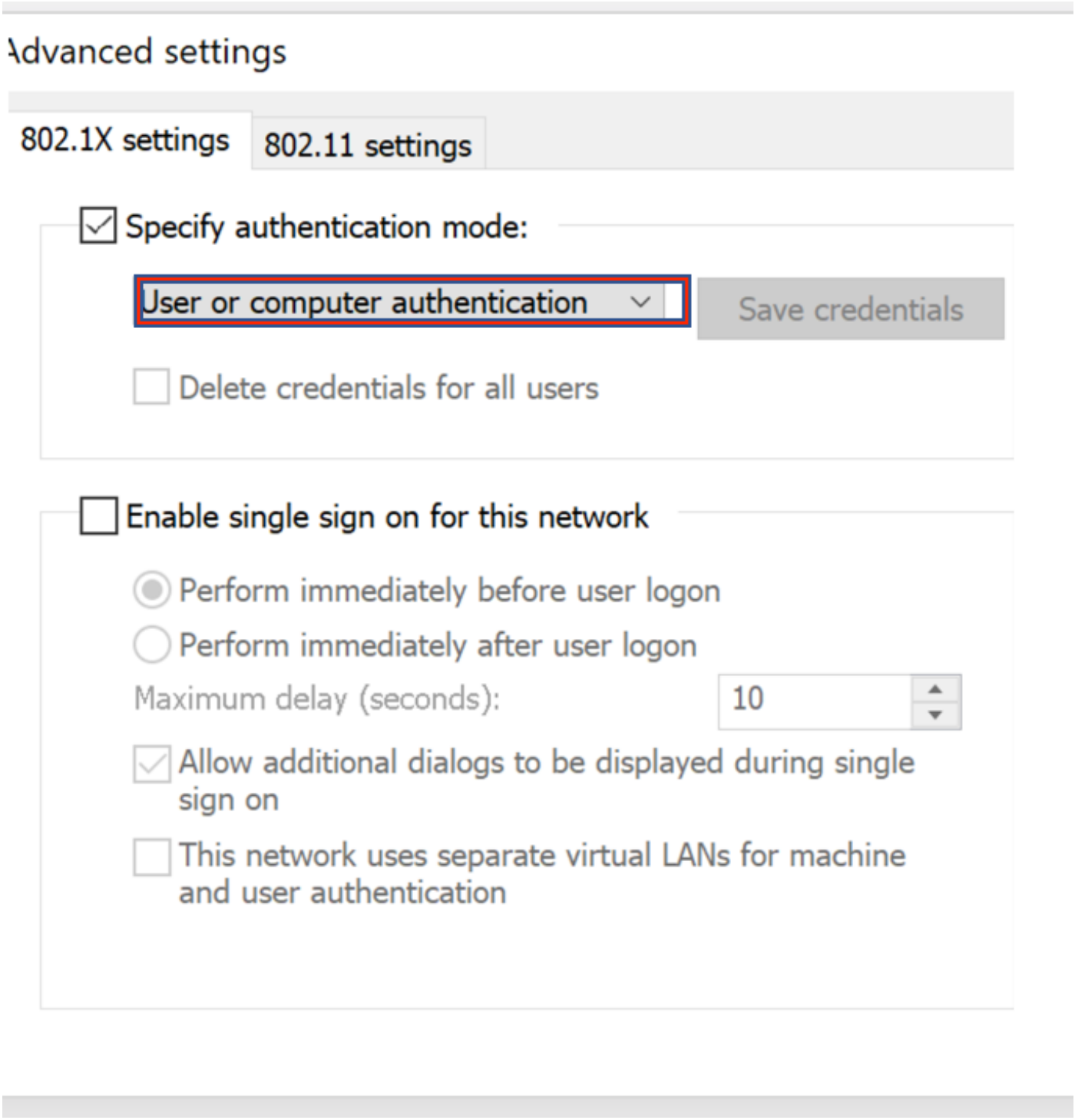
步驟 2. 選取「**Microsoft:智慧卡或其他憑證**」，然後按一下「**確定**」（如影像所示）。



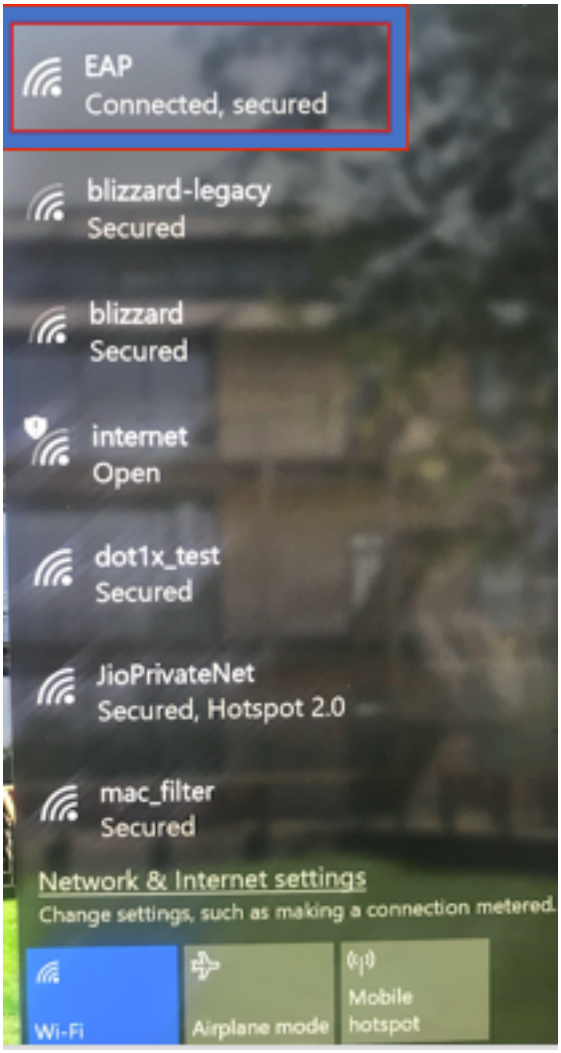
步驟 3. 按一下「**設定**」，然後選取從 CA 伺服器核發的根憑證（如影像所示）。



步驟 4. 按一下「**進階設定**」，然後從 802.1x 設定索引標籤選取「**使用者或電腦驗證**」（如影像所示）。



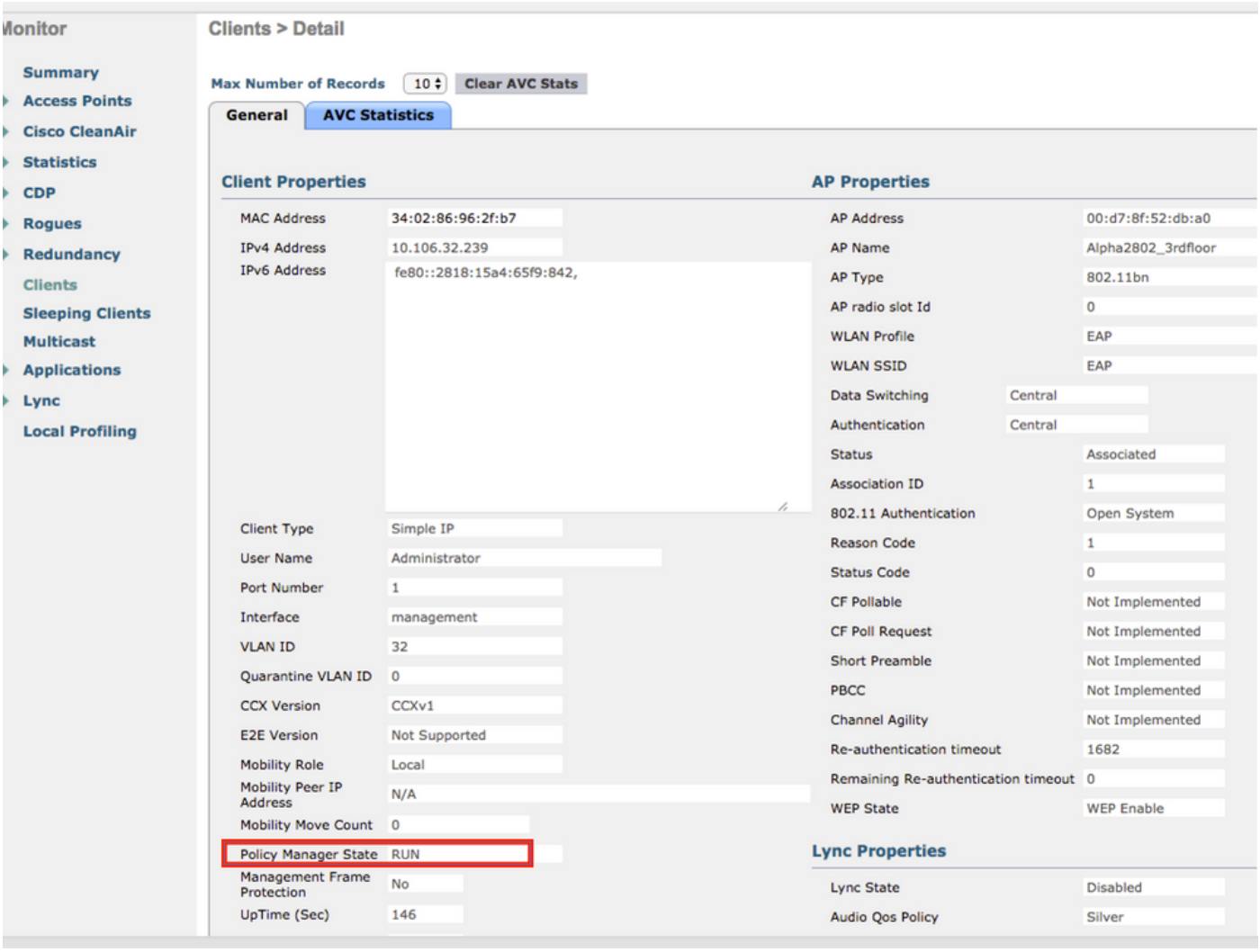
步驟 5. 現在，嘗試再次連線至無線網路，選取正確的設定檔（此範例為 EAP）和「**連線**」。您已連線至無線網路（如影像所示）。



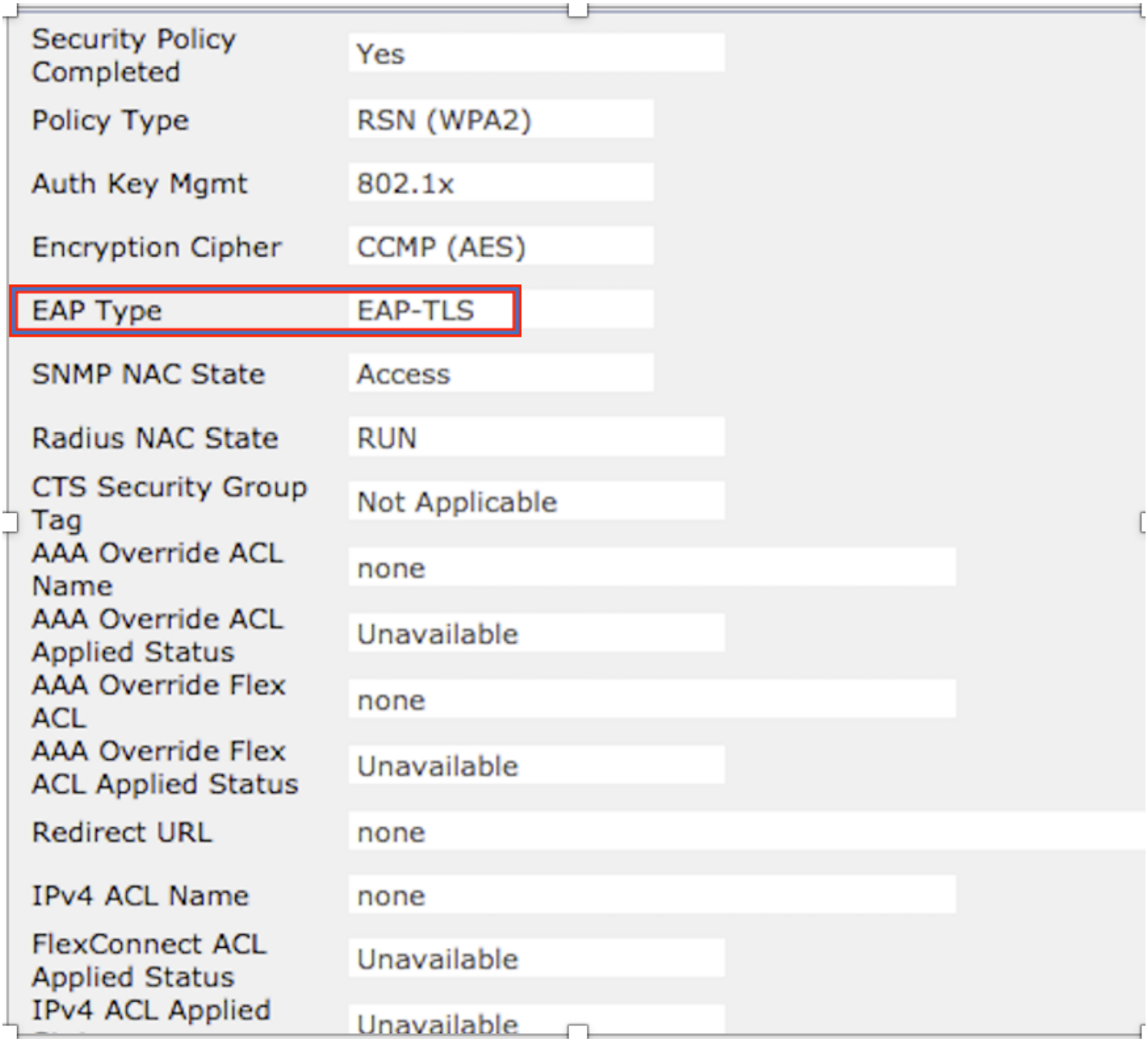
驗證

使用本節內容，確認您的組態是否正常運作。

步驟1.客戶端策略管理器狀態必須顯示為**RUN**。如此表示用戶端已完成驗證、取得 IP 位址，且可傳遞流量（如影像所示）。



步驟 2. 此外，請確認用戶端詳細資料頁面上 WLC 的正確 EAP 方法（如影像所示）。

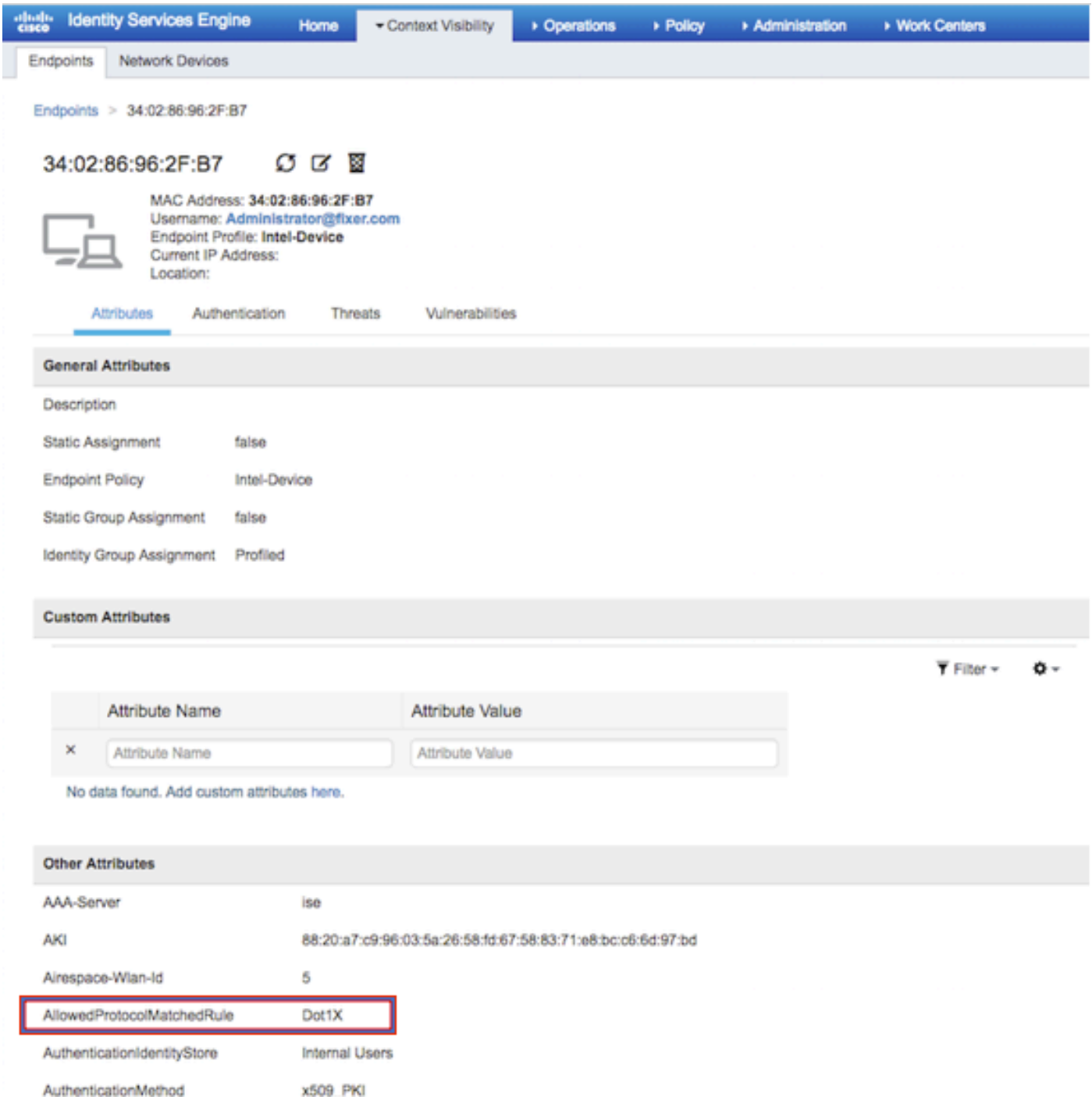


步驟 3. 以下為控制器之 CLI 的用戶端詳細資料（輸出已裁剪）：

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address.............................. 34:02:86:96:2f:b7
Client Username ................................ Administrator
AP MAC Address.................................. 00:d7:8f:52:db:a0
AP Name.......................................... Alpha2802_3rdfloor
AP radio slot Id................................ 0
Client State.................................... Associated
Wireless LAN Id................................. 5
Wireless LAN Network Name (SSID)................ EAP
Wireless LAN Profile Name....................... EAP
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:d7:8f:52:db:a4
Connected For .................................. 48 secs
Channel......................................... 1
IP Address...................................... 10.106.32.239
Gateway Address................................. 10.106.32.1
Netmask......................................... 255.255.255.0
Policy Manager State............................ RUN
Policy Type..................................... WPA2
Authentication Key Management................... 802.1x
```

```
Encryption Cipher.............................. CCMP-128 (AES)
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type....................................... EAP-TLS
```

步驟 4. 在 ISE 上，導覽至**「內容可見度」>「端點」>「屬性」**（如影像所示）。



BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11

疑難排解

目前尚無適用於此組態疑難排解的特定資訊。

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）。