

瞭解並配置EAP-TLS with Mobility Express和ISE

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[EAP-TLS 流程](#)

[EAP-TLS 流程中的步驟](#)

[設定](#)

[Cisco Mobility Express](#)

[採用Cisco Mobility Express的ISE](#)

[EAP-TLS 設定](#)

[ISE上的移動性Express設定](#)

[ISE 的信任憑證](#)

[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](#)

[EAP-TLS 的無線設定檔](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹如何在行動化Express控制器中設定具有802.1x安全性的無線區域網路(WLAN)。本文檔還專門介紹可擴展身份驗證協定(EAP) — 傳輸層安全(TLS)的使用。

必要條件

需求

思科建議您瞭解以下主題：

- Mobility Express初始設定
- 802.1x 驗證程序
- 憑證

採用元件

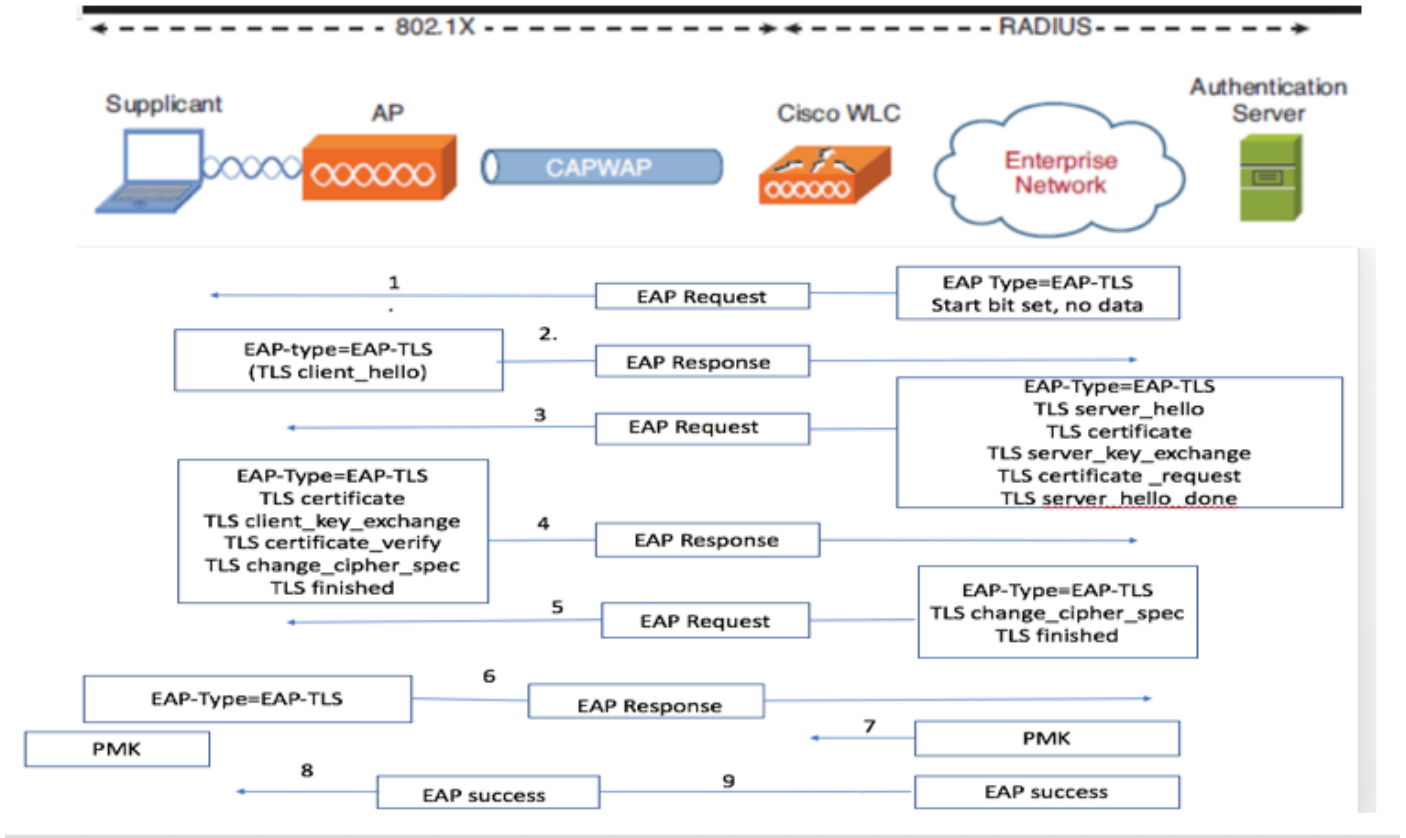
本文中的資訊係根據以下軟體和硬體版本：

- WLC 5508 8.5 版
- 身分識別服務引擎 (ISE) 2.1 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。
2. AP 此時不允許用戶端傳送任何資料與傳送驗證要求。
3. 要求者會以 EAP-Response Identity 回應。WLC 接著會將使用者 ID 資訊傳播至驗證伺服器。
4. 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。
5. 同儕節點會將 EAP-Response 傳送回驗證伺服器，其中包含「client_hello」交握訊息 (針對 NULL 設定的密碼) 。
6. 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.
```

7. 用戶端會以 EAP-Response 訊息回應，其中包含：

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

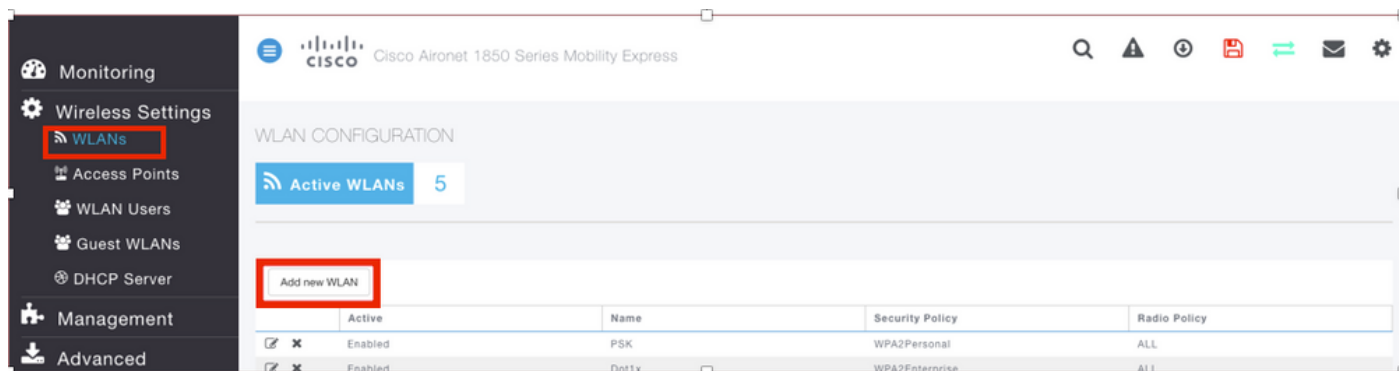
8. 用戶端成功驗證後，RADIUS 伺服器會以 Access-challenge 回應，其中包含「change_cipher_spec」和交握結束訊息。擷取此訊息時，用戶端會確認雜湊以驗證 RADIUS 伺服器。新的加密金鑰會在 TLS 交握期間透過密碼動態衍生。

9. 此時，支援 EAP-TLS 的無線用戶端可存取無線網路。

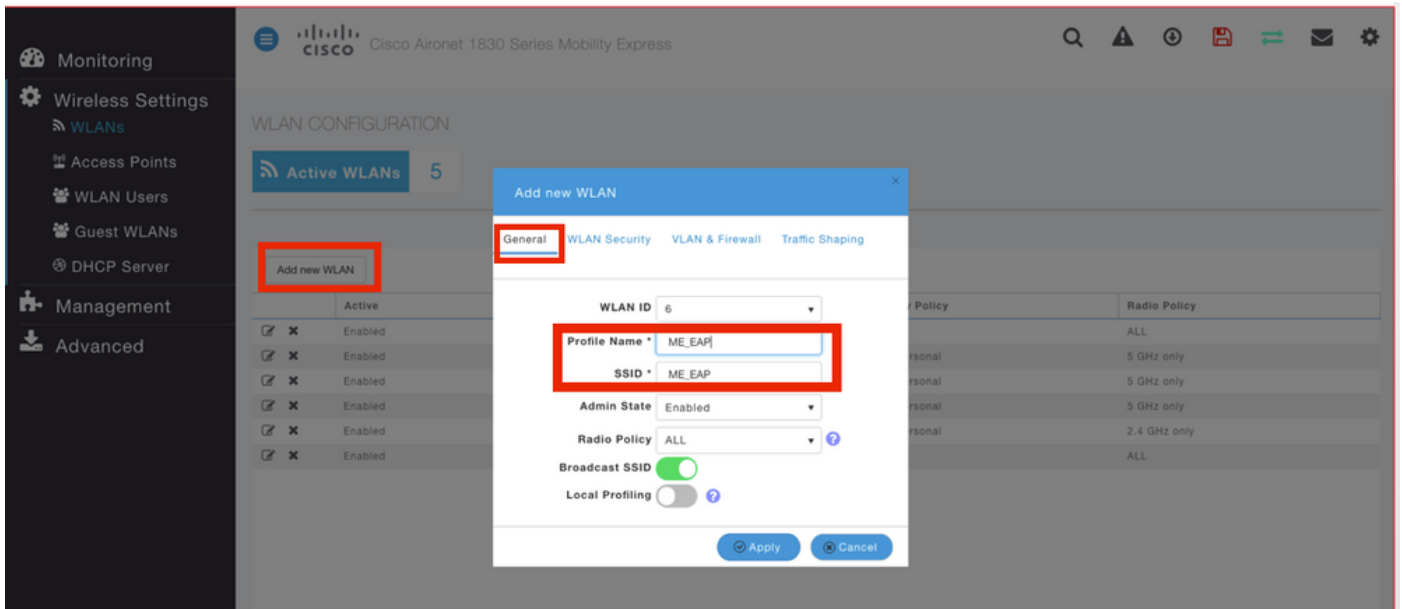
設定

Cisco Mobility Express

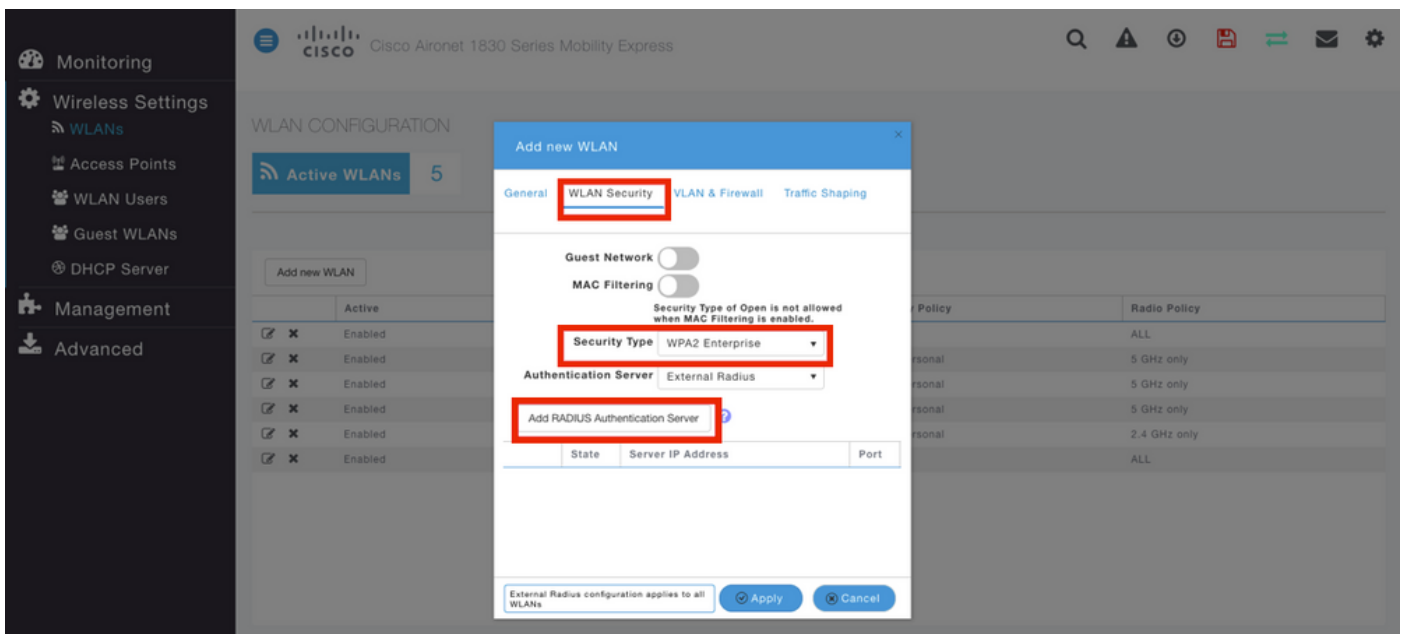
步驟1. 第一步是在Mobility Express上建立WLAN。若要建立WLAN，請導覽至WLAN > Add new WLAN，如下圖所示。



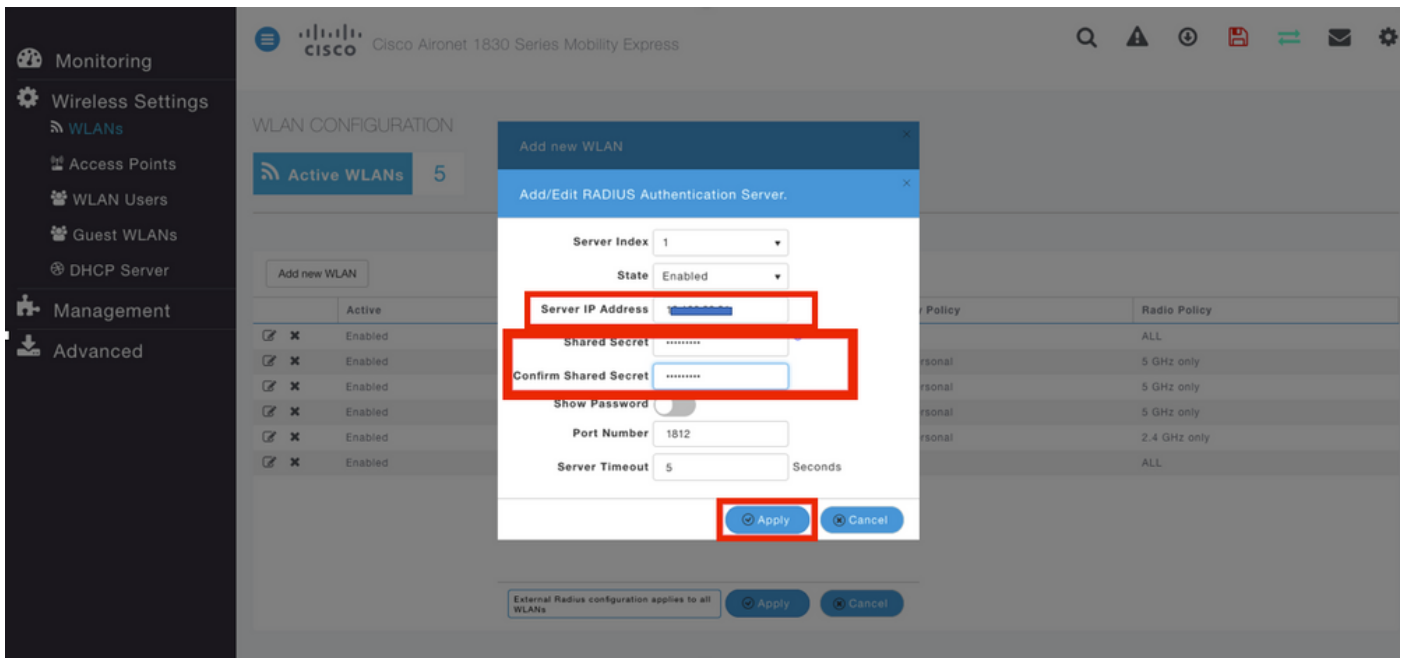
步驟2. 按一下Add new WLAN後，系統會顯示一個新的彈出視窗。若要建立設定檔名稱，請導覽至新增的WLAN > General，如下圖所示。



步驟3.將驗證型別配置為802.1x的WPA Enterprise，並在Add new WLAN > WLAN Security下配置RADIUS伺服器，如下圖所示。



步驟4.按一下「Add RADIUS Authentication Server」，並提供RADIUS伺服器的IP位址和共用密碼（必須與ISE上的設定完全相符），然後按一下「Apply」，如下圖所示。



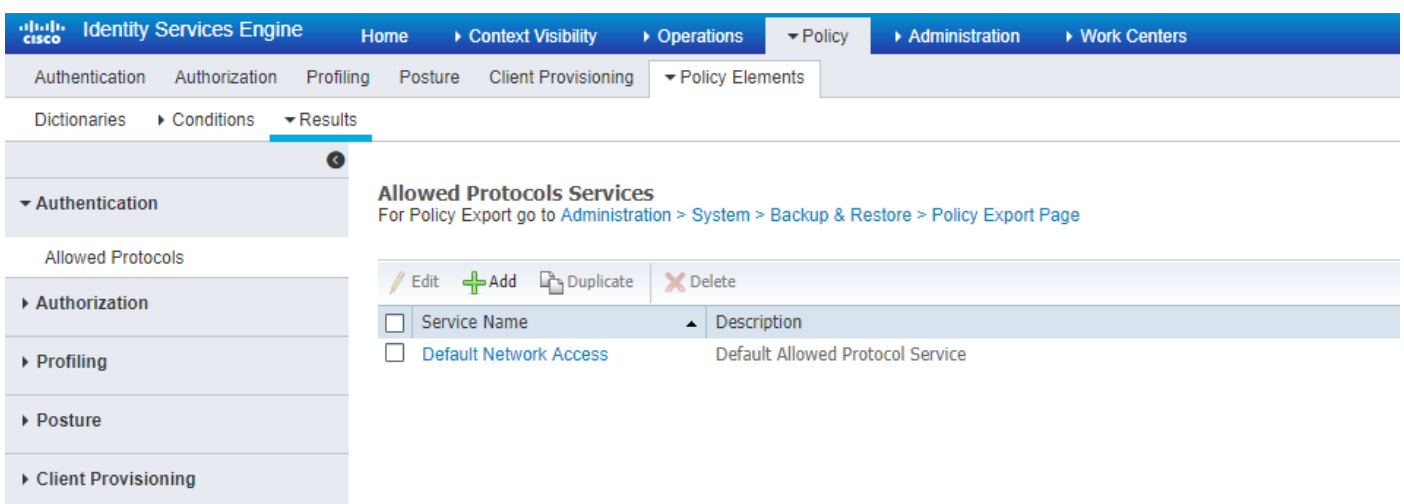
採用Cisco Mobility Express的ISE

EAP-TLS 設定

為了構建策略，您需要建立允許在策略中使用的協定清單。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。

如果使用預設，即表示您允許大多數用於驗證的 EAP 類型（如果您需要鎖定特定 EAP 類型的存取權，則預設設定可能不會是首選的類型）。

步驟1. 導覽至Policy > Policy Elements > Results > Authentication > Allowed Protocols，然後按一下Add，如下圖所示。



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）。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

Allowed Protocols Services List > New Allowed Protocols Service

Allowed Protocols

Name

Description

Allowed Protocols

- Authentication Bypass
 - Process Host Lookup (i)
- Authentication Protocols
 - Allow PAP/ASCII
 - Allow CHAP
 - Allow MS-CHAPv1
 - Allow MS-CHAPv2
 - Allow EAP-MD5
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)
 - Enable Stateless Session Resume
 - Session ticket time to live Hours
 - Proactive session ticket update will occur after % of Time To Live has expired
 - Allow LEAP
 - Allow PEAP
 - PEAP Inner Methods
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-GTC
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)
 - Require cryptobinding TLV (i)

ISE上的移動性Express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）。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Selected 0 | Total 1

Name	IP/Mask	Profile Name	Location	Type	Description

步驟 2. 輸入資訊 (如影像所示) 。

The screenshot shows the 'New Network Device' configuration page in Cisco ISE. The 'RADIUS Authentication Settings' section is expanded, showing the following fields and options:

- RADIUS Authentication Settings
- Enable Authentication Settings
- Protocol: RADIUS
- * Shared Secret: [Text Field] [Show]
- Enable KeyWrap: [i]
- * Key Encryption Key: [Text Field] [Show]
- * Message Authenticator Code Key: [Text Field] [Show]
- Key Input Format: ASCII HEXADECIMAL
- CoA Port: 1700 [Set To Default]

Below the RADIUS settings, there are three collapsed sections:

- TACACS Authentication Settings
- SNMP Settings
- Advanced TrustSec Settings

At the bottom, there are two buttons: **Submit** (highlighted with a red box) and **Cancel**.

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」。

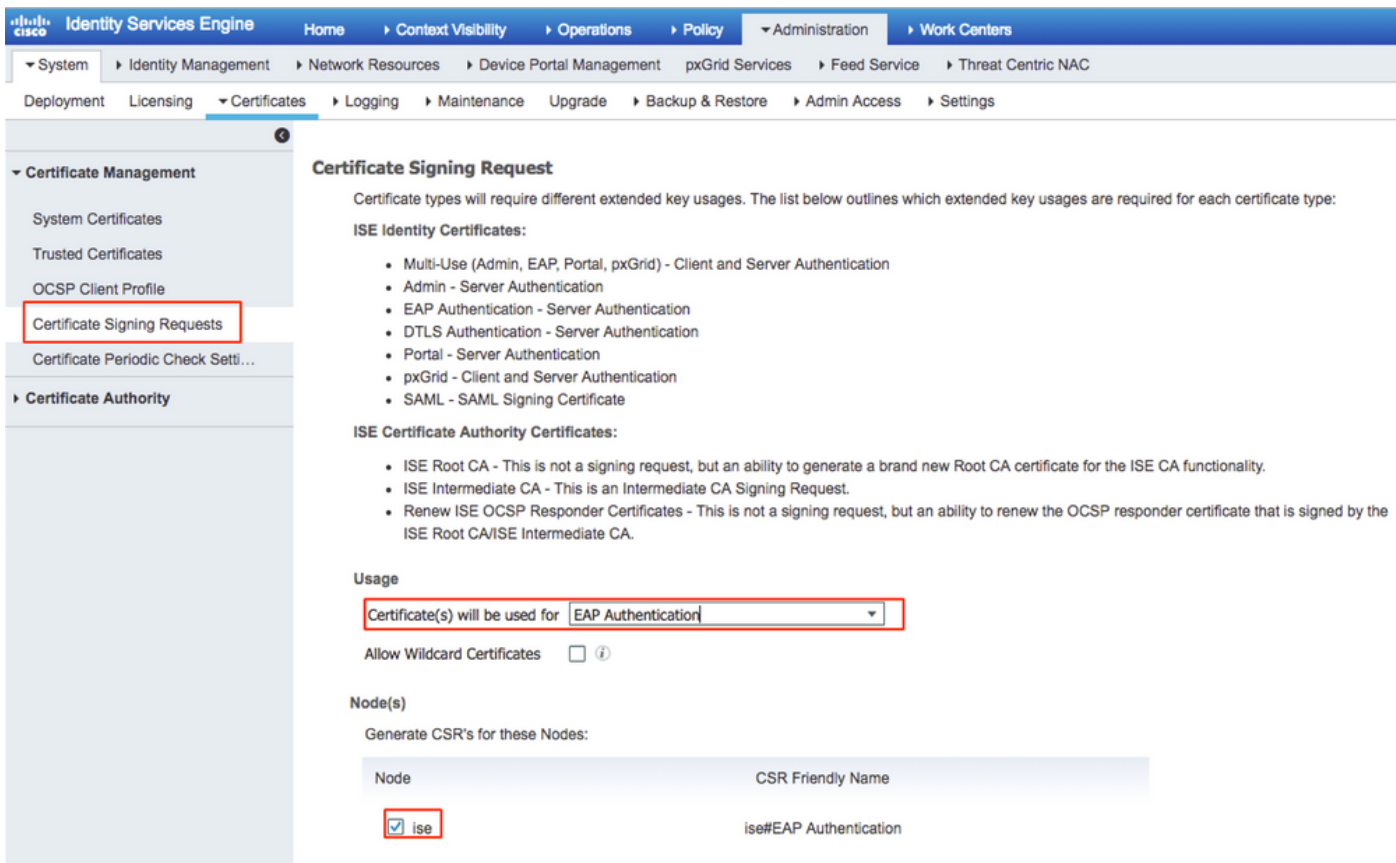
按一下「匯入」以將憑證匯入至 ISE。在 ISE 新增 WLC 並建立使用者後，您需要執行 EAP-TLS 最重要的作業：信任 ISE 的憑證。為此，您需要產生 CSR。

步驟2. 導覽至管理>憑證>憑證簽署請求>產生憑證簽署請求(CSR)，如下圖所示。

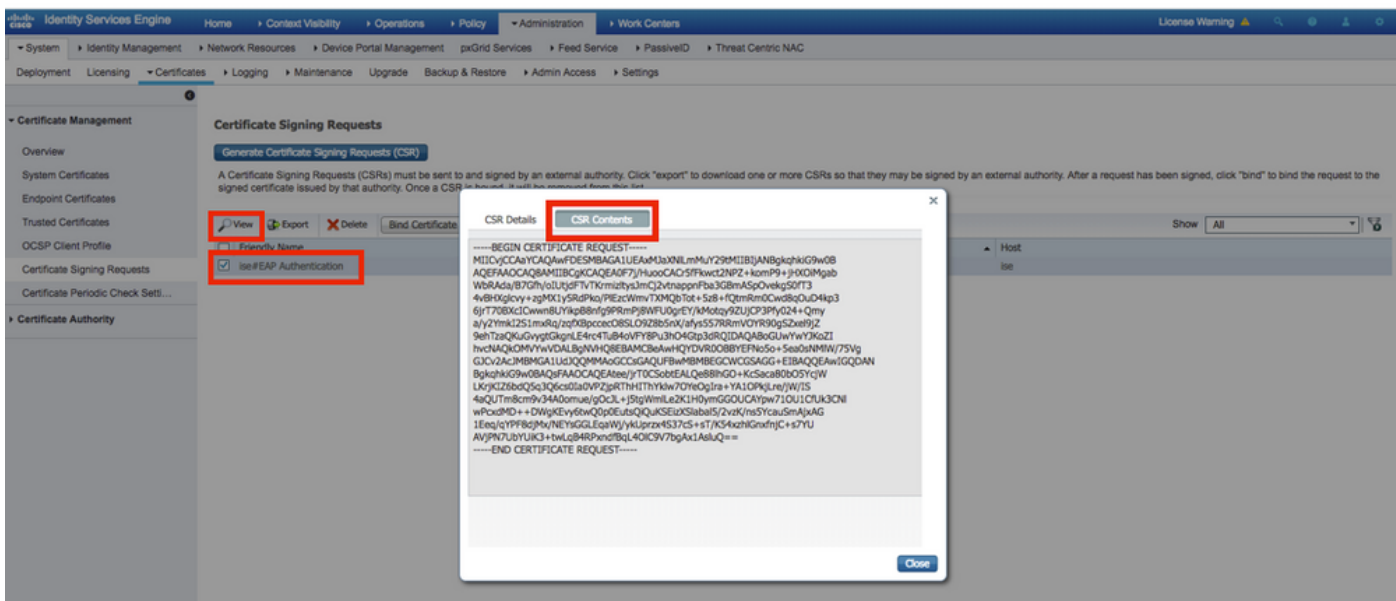
The screenshot shows the 'Certificate Signing Requests' page in Cisco ISE. The 'Generate Certificate Signing Requests (CSR)' button is highlighted. Below the button, there is a table with one row of data:

View	Export	Delete	Bind Certificate	Friendy Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ISE#EAP Authentication	CN=ise.c.com	2048		Wed, 11 Jul 2016	ise

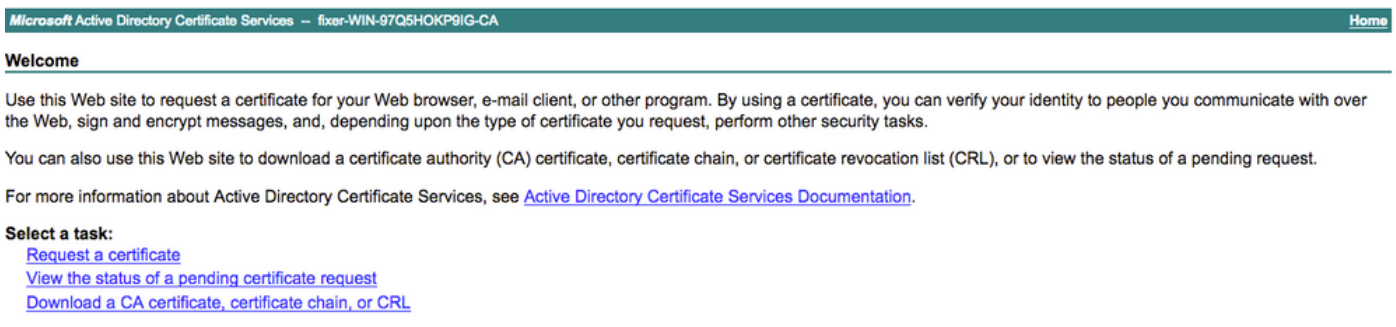
步驟3. 若要產生CSR，請導覽至Usage，然後從Certificate(s) will be used下拉選項中選擇EAP Authentication，如下圖所示。



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，瀏覽至CA伺服器，然後按一下Request a certificate，如下圖所示：



步驟6。申請憑證後，您會收到User Certificate和advanced certificate request的選項，請按一下advanced certificate request，如下圖所示。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#)

步驟 7. 在「Base-64 編碼的憑證要求」中貼上產生的 CSR。在「Certificate Template:」下拉選單中，選擇「Web Server」，然後按一下「Submit」，如下圖所示。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

Additional Attributes:
Attributes:

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）。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Certificate Issued

The certificate you requested was issued to you.

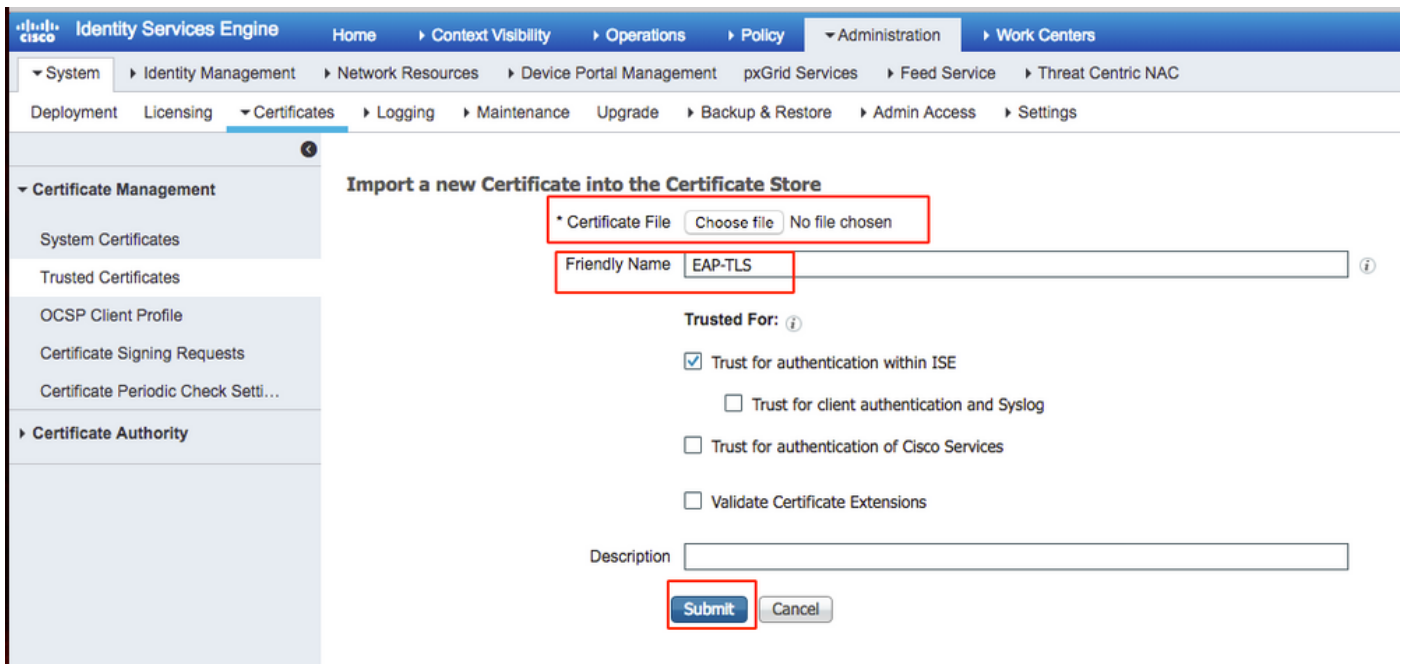
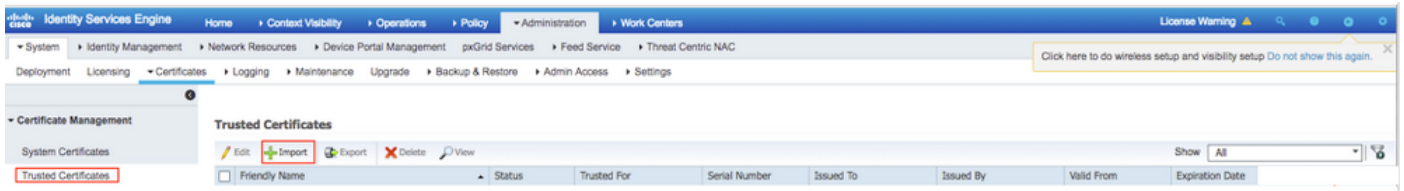
DER encoded or Base 64 encoded



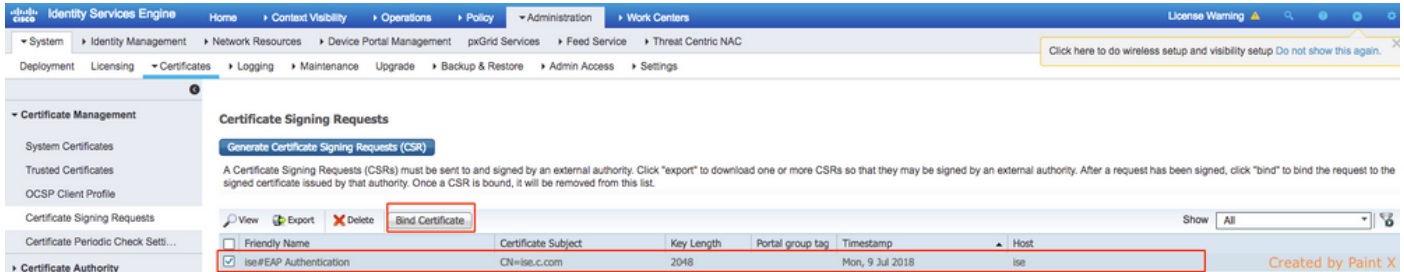
[Download certificate](#)

[Download certificate chain](#)

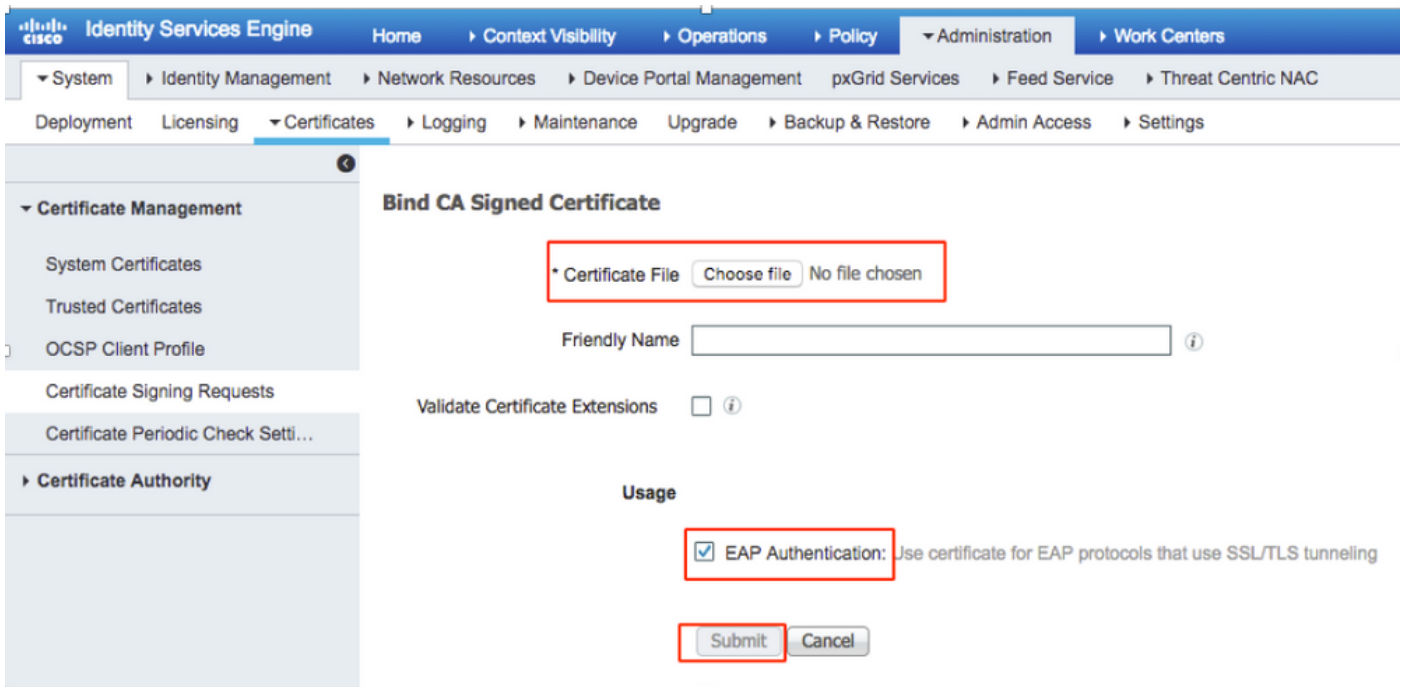
步驟 9. ISE 伺服器的憑證下載隨即完成。您可擷取憑證，該憑證將會包含兩個憑證，一個為根憑證，另一個為中繼憑證。根憑證可在「管理」>「憑證」>「受信任的憑證」>「匯入」下匯入（如影像所示）。



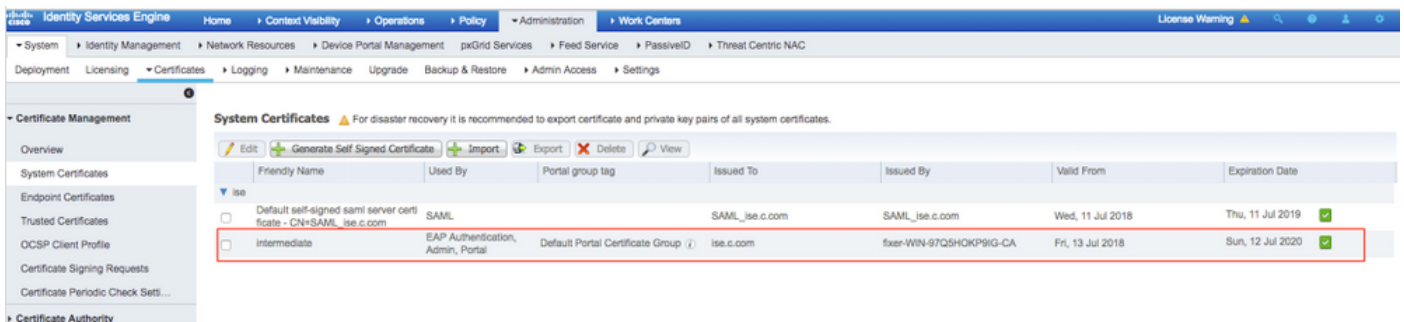
步驟 10. 按一下「提交」後，該憑證會新增至受信任的憑證清單。此外，需要使用中繼憑證才可與 CSR 繫結（如影像所示）。



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**，如下圖所示。



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://server ip addr/certsrv--->

步驟2.請注意，CA必須與為ISE下載證書的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）。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIspJry  
aF4l2aLpmDFp1PfVZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

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）。

獲得證書後，請按照以下步驟操作，以便在windows筆記型電腦上匯入證書。

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. 選擇**Computer Account**。
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**」。

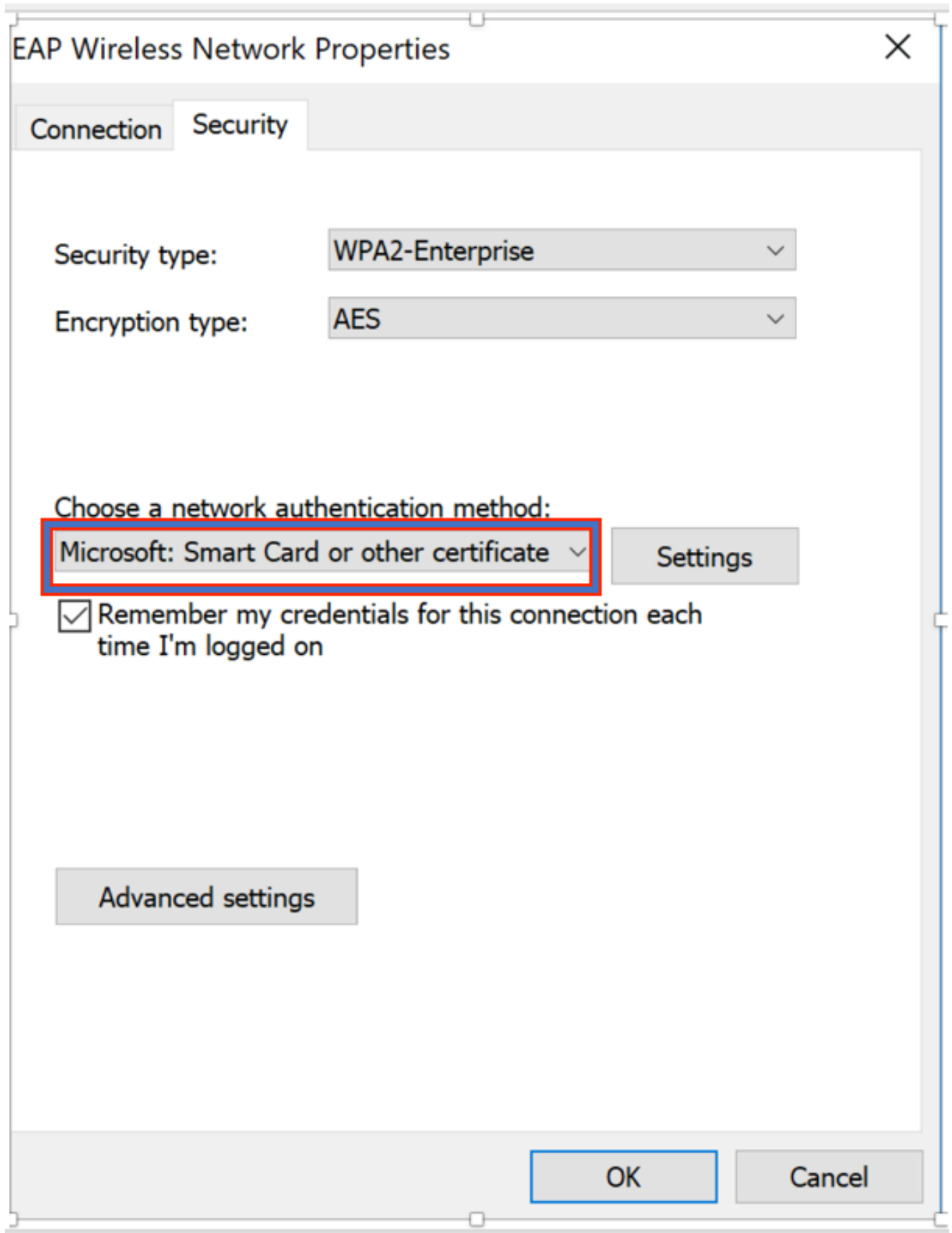
憑證匯入完成後，您需要將無線用戶端（此範例為 Windows 桌上型電腦）設定為 EAP-TLS。

EAP-TLS 的無線設定檔

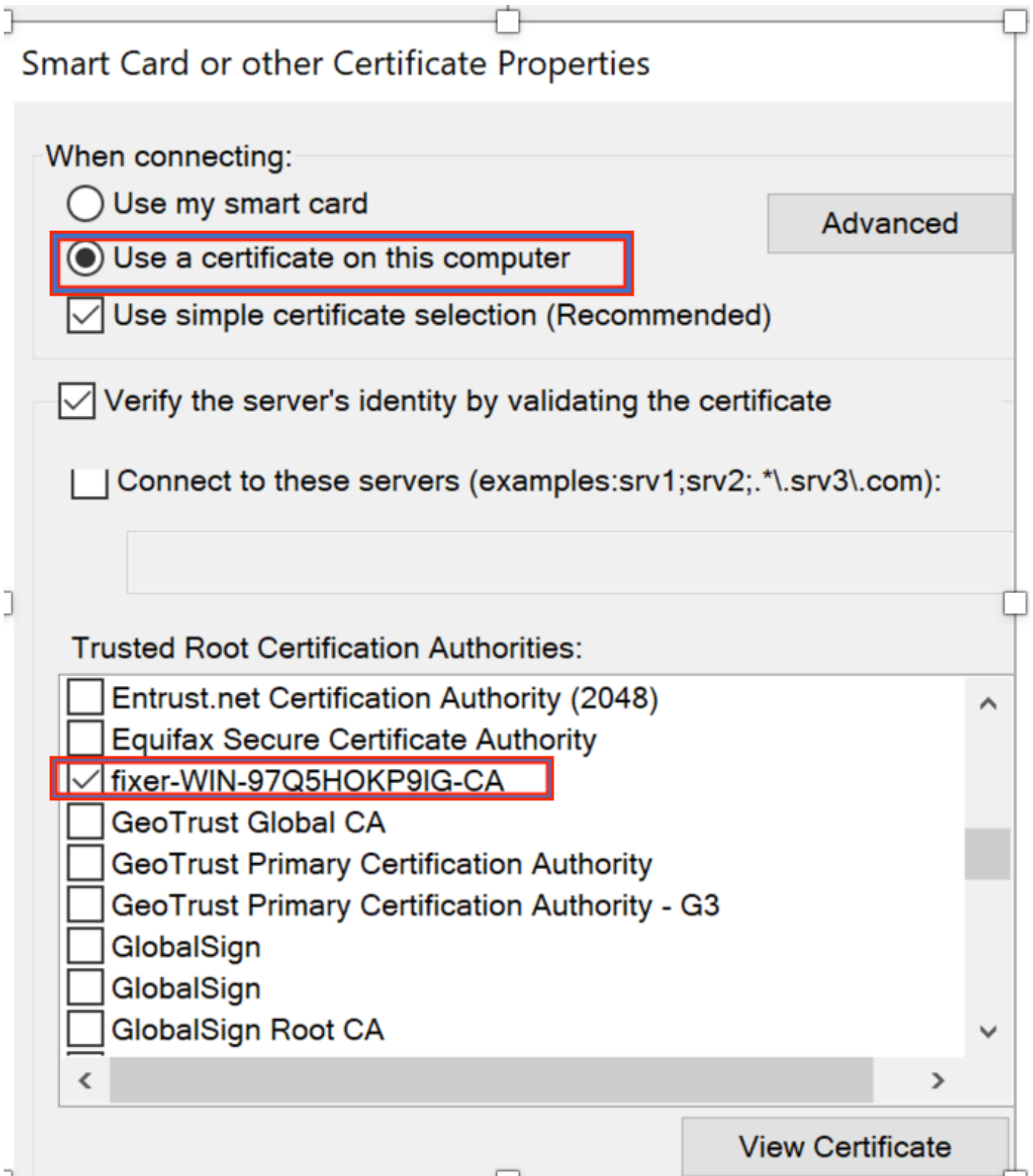
步驟1.更改之前為受保護的可擴展身份驗證協定(PEAP)建立的無線配置檔案，以便改用EAP-TLS。

按一下「**EAP 無線設定檔**」。

步驟 2. 選取「**Microsoft:智慧卡或其他證書**」，然後按一下**OK**，如下圖所示。



步驟3.按一下**Settings**，然後選擇從CA伺服器核發的根憑證，如下圖所示。



步驟4. 按一下 **Advanced Settings**，然後在 802.1x settings 索引標籤中選擇 **User or computer authentication**，如下圖所示。

Advanced settings

802.1X settings

802.11 settings

Specify authentication mode:

User or computer authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

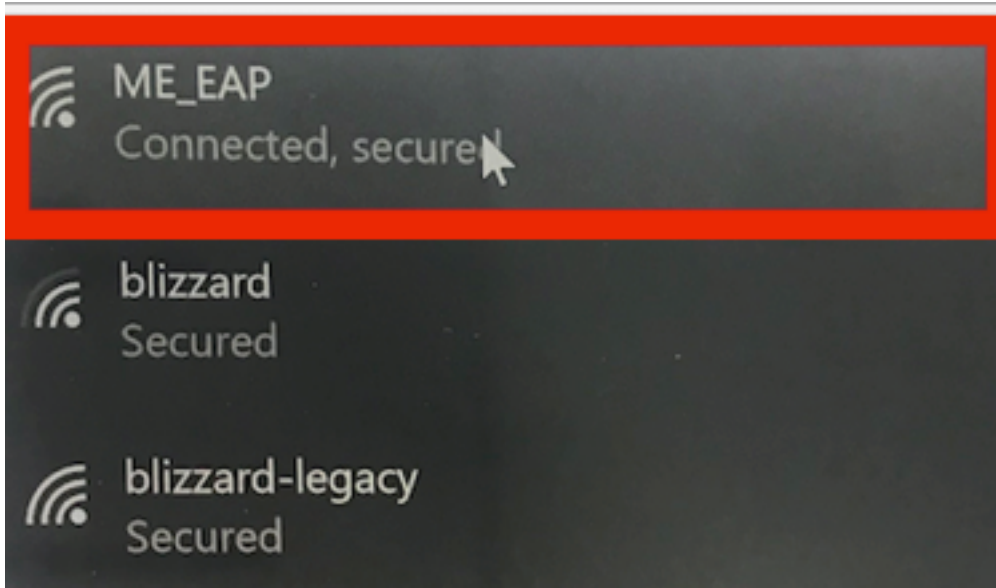
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

步驟5.現在，嘗試再次連線到無線網路，選擇正確的配置檔案（本示例中的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EAP型別必須為EAP-TLS。這表示客戶端已使用EAP-TLS完成身份驗證，獲取了IP地址並準備傳遞流量，如圖所示。

The screenshot displays the 'CLIENT VIEW' interface. On the left is a navigation sidebar with categories: Monitoring (Network Summary, Access Points, Clients), Applications, Rogues (Access Points, Clients), Interferers, Wireless Dashboard (AP Performance, Client Performance), Best Practices, Wireless Settings, Management, and Advanced.

The main content area is titled 'CLIENT VIEW' and contains several sections:

- GENERAL:** Includes a laptop icon, User Name 'Administrator', Host Name 'Unknown', MAC Address '34:02:86:96:2f:b7', Uptime 'Associated since 37 Seconds', and SSID 'ME_EAP' (highlighted with a red box). Other fields include AP Name 'AP442b.03a9.7f72 (Ch 56)', Nearest APs, Device Type, Performance (Signal Strength: 0 dBm, Signal Quality: 0 dB, Connection Speed: 0, Channel Width: 40 MHz), Capabilities '802.11n (5GHz) Spatial Stream: 0', Cisco Compatible 'Supported (CCX v 4)', and Connection Score '0%'.
- CONNECTIVITY:** A progress bar with five steps: Start, Association, Authentication, DHCP, and Online, all of which are completed.
- TOP APPLICATIONS:** A table with columns 'Name', 'Usage', and '% Usage'. It currently shows 'No Data Available!'.
- MOBILITY STATE:** A diagram showing the network path from 'WLC (LOCAL)' to 'Wired (CAPWAP)', then to 'AP (FlexConnect)', then to 'Wireless (802.11n (5GHz))', and finally to the 'Client (VLAN1)'.

The screenshot displays the Cisco ISE GUI for a specific client. The left sidebar contains navigation menus for Monitoring, Wireless Settings, and Management. The main content area is divided into several sections:



- MOBILITY STATE:** A diagram showing the client's connection path from a WLC (LOCAL) through a Wireless (CAPWAP) to an AP (FlexConnect), then to a Wireless (802.11n (5GHz)) and finally to the Client (VLAN1).
- NETWORK & QOS:** A table listing network parameters such as IP Address (10.127.209.55), IPv6 Address (fe80::2818:15a4:65f9:842), VLAN (1), and QoS Level (Silver).
- SECURITY & POLICY:** A table showing security settings. Two rows are highlighted with red boxes: 'Key Management' with a status of '802.1x' and 'EAP Type' with a status of 'EAP-TLS'.
- CLIENT TEST:** A section with tabs for PING TEST, CONNECTION, EVENT LOG, and PACKET CAPTURE.

步驟2. 以下是控制器CLI中的使用者端詳細資訊 (剪下的輸出) :

```
(Cisco Controller) > show client detail 34:02:86:96:2f:b7
Client MAC Address..... 34:02:86:96:2f:b7
Client Username ..... Administrator
AP MAC Address..... c8:f9:f9:83:47:b0
AP Name..... AP442b.03a9.7f72
AP radio slot Id..... 1
Client State..... Associated
Client User Group..... Administrator
Client NAC OOB State..... Access
Wireless LAN Id..... 6
Wireless LAN Network Name (SSID)..... ME_EAP
Wireless LAN Profile Name..... ME_EAP
Hotspot (802.11u)..... Not Supported
BSSID..... c8:f9:f9:83:47:ba
Connected For ..... 18 secs
Channel..... 56
IP Address..... 10.127.209.55
Gateway Address..... 10.127.209.49
Netmask..... 255.255.255.240
IPv6 Address..... fe80::2818:15a4:65f9:842
--More-- or (q)uit
Security Policy Completed..... Yes
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3. 在ISE上，導航到Context Visibility > End Points > Attributes，如下圖所示。

Endpoints > 34:02:86:96:2F:B7

34:02:86:96:2F:B7   



MAC Address: 34:02:86:96:2F:B7
 Username: Administrator@fixer.com
 Endpoint Profile: Intel-Device
 Current IP Address:
 Location:

Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

Custom Attributes

Filter 

Attribute Name	Attribute Value
<input type="text" value="Attribute Name"/>	<input type="text" value="Attribute Value"/>

No data found. Add custom attributes here.

Other Attributes

AAA-Server	ise
AKI	88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id	6
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509_PKI
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access

BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
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, 1.3.6.1.4.1.311.11
FailureReason	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA,DC=fixer,DC=cc
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com
Key Usage	0, 2
Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7

MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
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"
OpenSSLStack	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	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。