فهم EAP-TLS وتكوينه باستخدام Mobility Express و ISE

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد شبكة محلية السلكية (WLAN) مع تأمين 802.1x في وحدة تحكم Mobility Express. يشرح هذا المستند أيضا إستخدام برنامج OpenSSL المصادقة الموسع (EAP) -أمان طبقة النقل (TLS) بشكل محدد.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إعداد Mobility Express الأولي
- عملية مصادقة وقفا لمعيار 802.1x
- الشهادات

المكونات المستخدمة

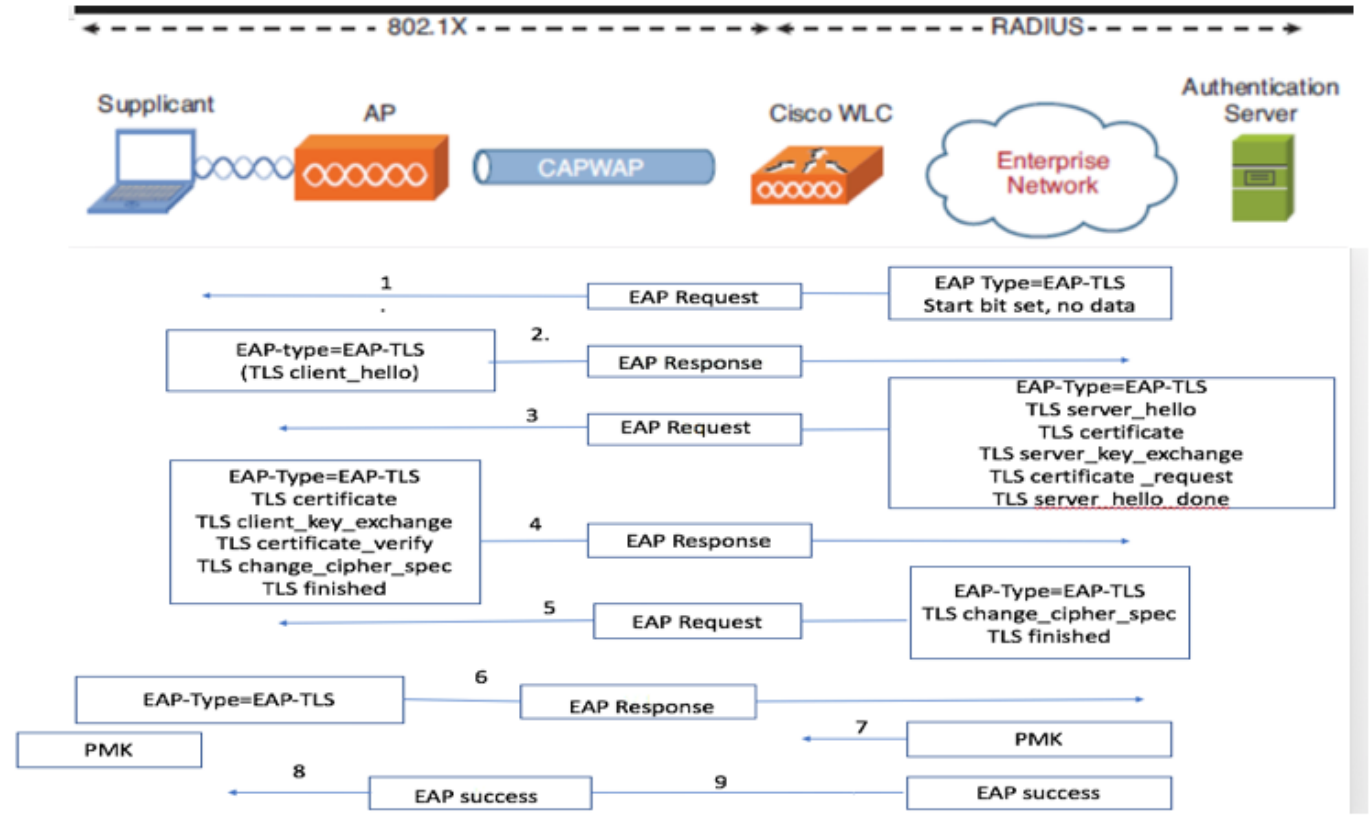
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- WLC 5508، الإصدار 8.5
- Identity Services Engine (ISE)، الإصدار 2.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تدفق EAP-TLS



خطوات في تدفق EAP-TLS

1. يرتبط العميل اللاسلكي بنقطة الوصول (AP).
2. لا تسمح نقطة الوصول للعميل بإرسال أي بيانات عند هذه النقطة وترسل طلب مصادقة.
3. ثم يستجيب المطالب بهوية EAP-Response. يقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بعد ذلك بتوصيل معلومات معرف المستخدم إلى خادم المصادقة.
4. يستجيب خادم RADIUS للعميل مرة أخرى باستخدام حزمة بدء EAP-TLS. تبدأ محادثة EAP-TLS عند هذه النقطة.
5. يرسل النظير EAP-Response مرة أخرى إلى خادم المصادقة الذي يحتوي على رسالة مصافحة "client_hello"، وهي تشفير تم تعيينه ل NULL.
6. يستجيب خادم المصادقة باستخدام حزمة Access-challenge التي تحتوي على:

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

7. يستجيب العميل برسالة إستجابة EAP تحتوي على:

```
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
```

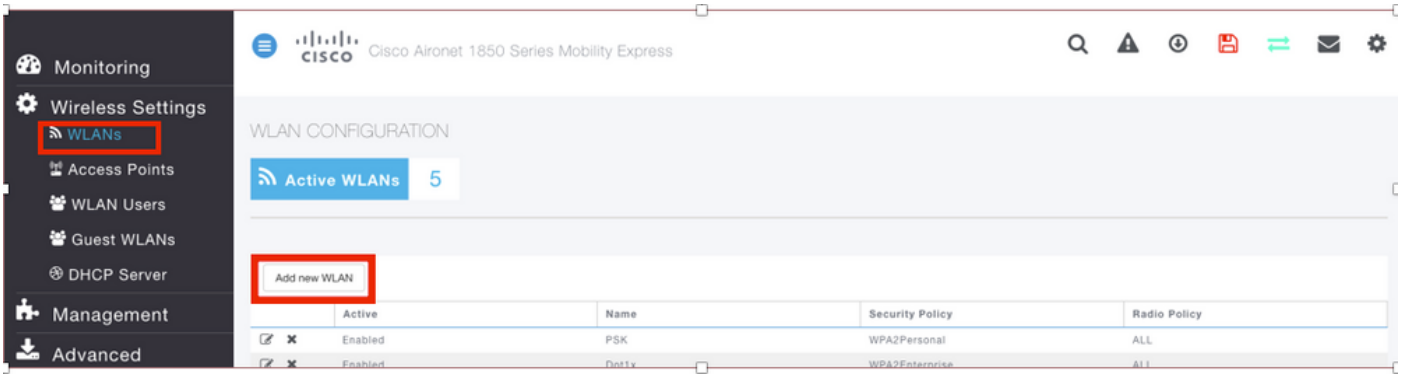
8. بعد مصادقة العميل بنجاح، يستجيب خادم RADIUS بتحدي الوصول الذي يحتوي على الرسالة "change_cipher_spec" وانتهاء المصافحة. وعند إستلام هذا الإجراء، يتحقق العميل من التجزئة لمصادقة خادم RADIUS. يتم اشتقاق مفتاح تشفير جديد ديناميكيا من السر أثناء مصافحة TLS.

9. في هذه المرحلة يستطيع العميل اللاسلكي الذي يدعم EAP-TLS الوصول إلى الشبكة اللاسلكية.

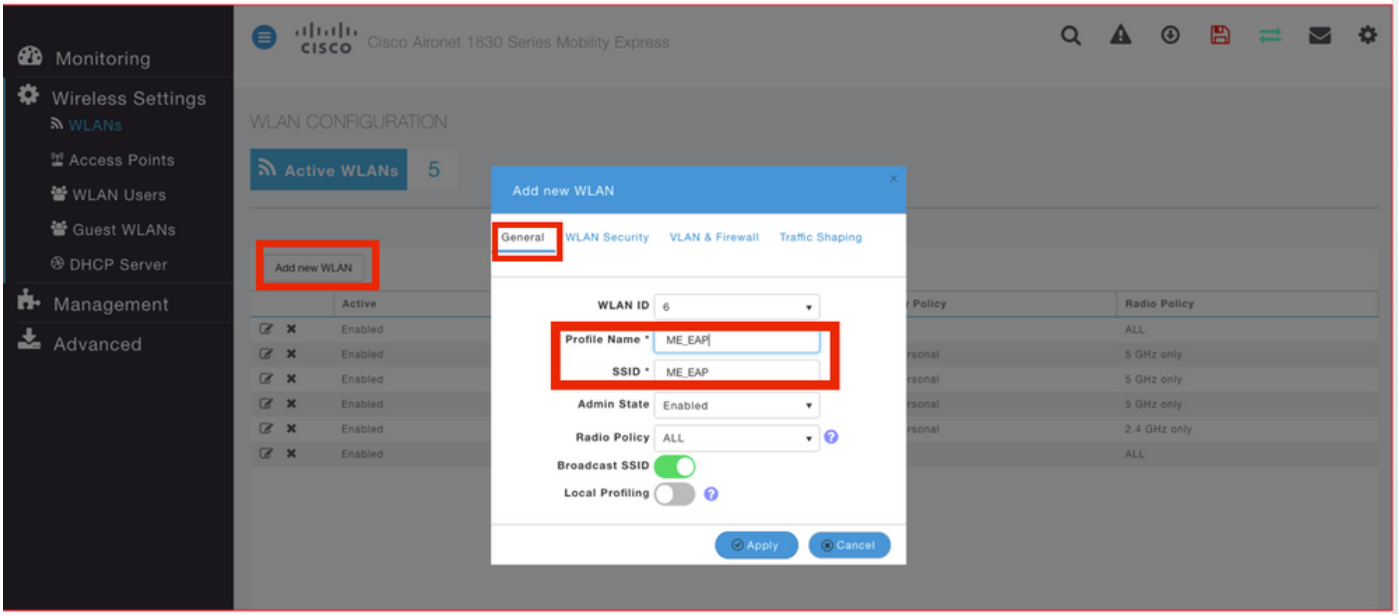
التكوين

Cisco Mobility Express

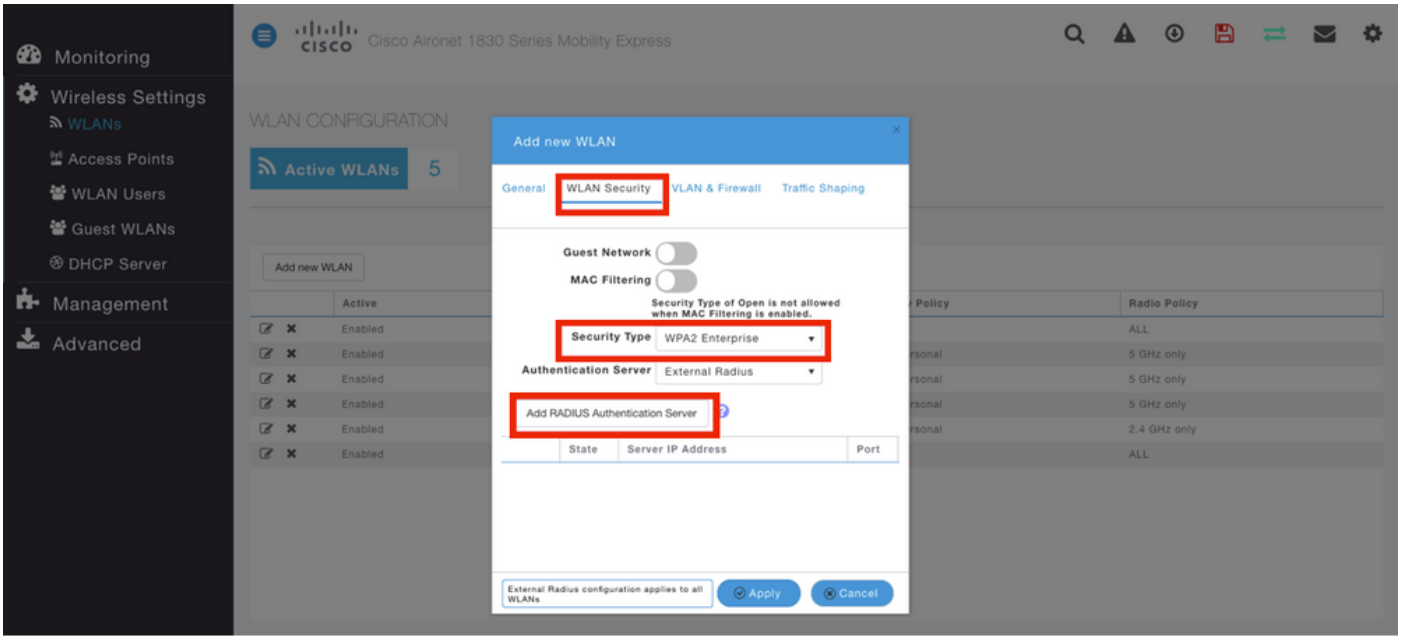
الخطوة 1. الخطوة الأولى هي إنشاء شبكة WLAN على Mobility Express. لإنشاء شبكة WLAN، انتقل إلى **WLAN > إضافة شبكة WLAN جديدة** كما هو موضح في الصورة.



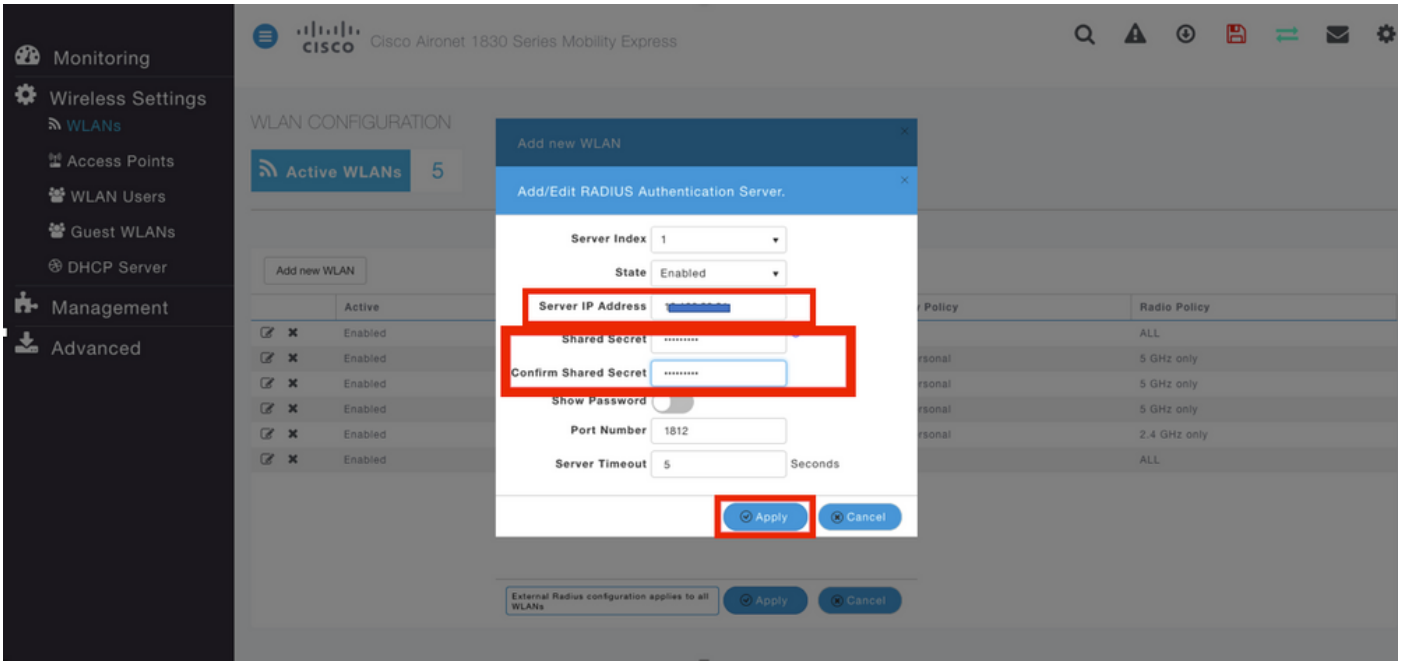
الخطوة 2. ستظهر نافذة منبثقة جديدة بمجرد النقر فوق **إضافة شبكة WLAN جديدة**. لإنشاء اسم ملف تخصيص، انتقل إلى **إضافة شبكة محلية لاسلكية (WLAN) جديدة > عامة** كما هو موضح في الصورة.



الخطوة 3. قم بتكوين نوع المصادقة مثل WPA Enterprise لـ 802.1x وشكلت RADIUS Server تحت **إضافة WLAN جديد > تأمين WLAN** كما هو موضح في الصورة.



الخطوة 4. انقر فوق **إضافة خادم مصادقة RADIUS** ووفر عنوان IP الخاص بخادم RADIUS والسر المشترك الذي يجب أن يطابق تمامًا ما تم تكوينه على ISE ثم انقر على **تطبيق** كما هو موضح في الصورة.



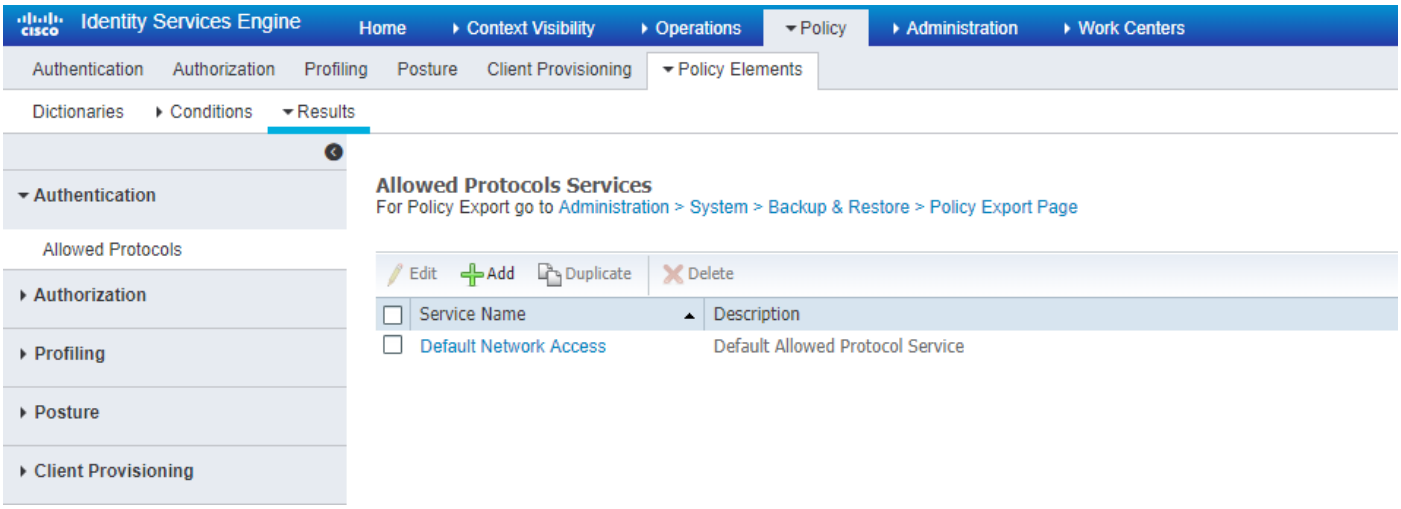
ISE مع Cisco Mobility Express

إعدادات EAP-TLS

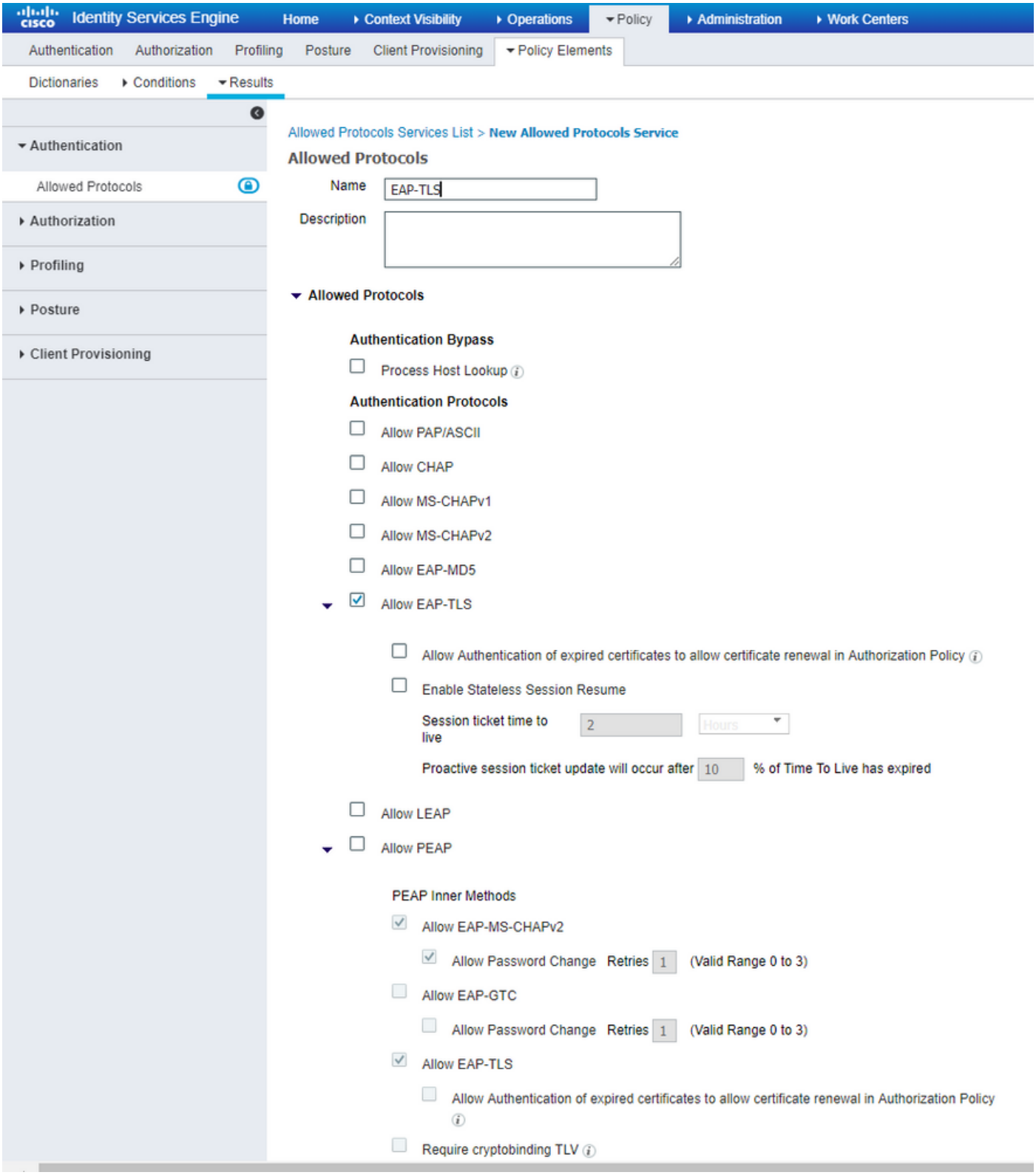
لإنشاء النهج، تحتاج إلى إنشاء قائمة البروتوكولات المسموح باستخدامها في النهج الخاص بك. بما أن سياسة dot1x تمت كتابتها، حدد نوع EAP المسموح به بناء على كيفية تكوين السياسة.

إذا كنت تستخدم الافتراضي فإنك تسمح لمعظم أنواع EAP للمصادقة وهو ما قد لا يكون مفضلا إذا كنت بحاجة إلى تأمين الوصول إلى نوع EAP معين.

الخطوة 1. انتقل إلى **السياسة > عناصر السياسة > النتائج > المصادقة > البروتوكولات المسموح بها** وانقر **إضافة** كما هو موضح في الصورة.

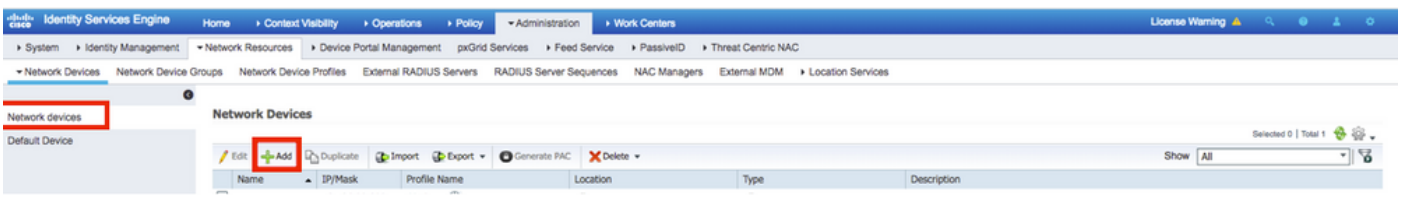


الخطوة 2. في قائمة البروتوكولات المسموح بها، يمكنك إدخال اسم القائمة. في هذه الحالة، يتم تحديد **السماح** لمربع **EAP-TLS** ويتم إلغاء تحديد مربعات أخرى كما هو موضح في الصورة.

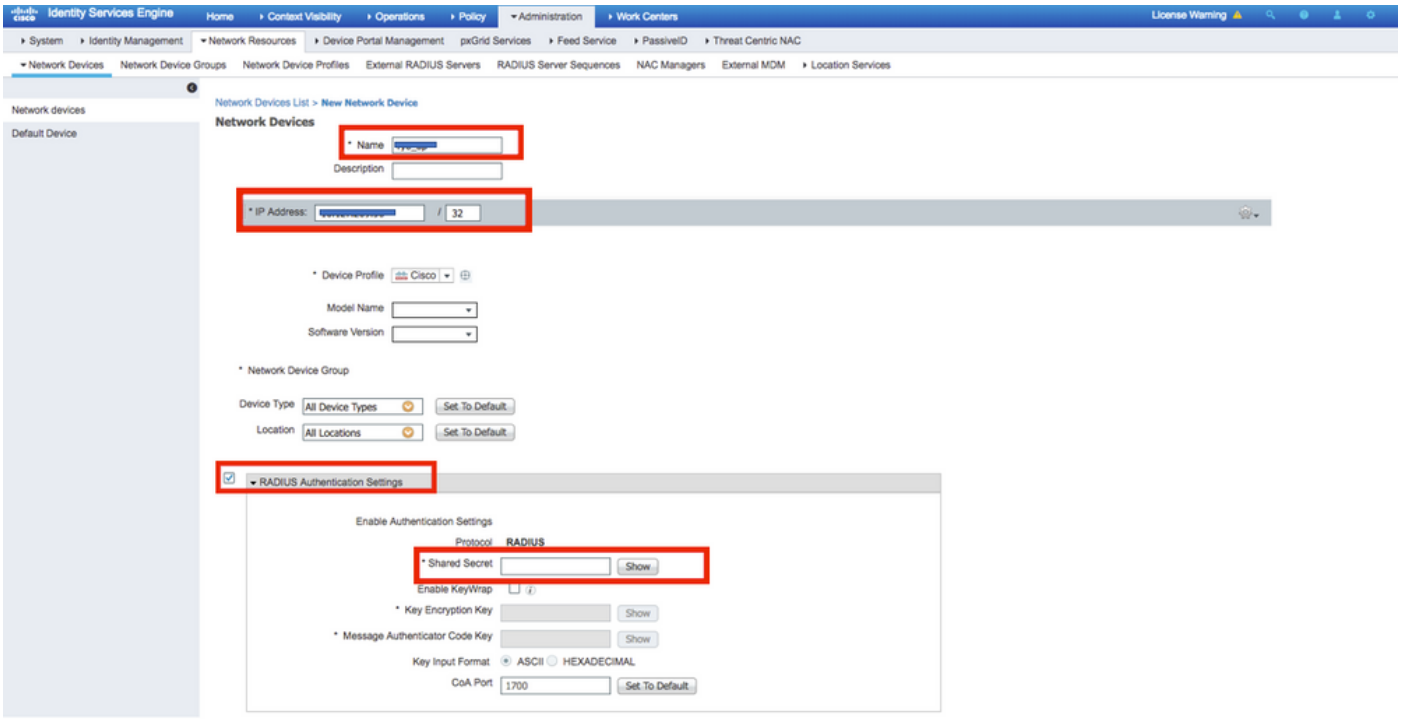


إعدادات Mobility Express على ISE

الخطوة 1. افتح وحدة تحكم ISE وانتقل إلى **الإدارة > موارد الشبكة > أجهزة الشبكة > إضافة** كما هو موضح في الصورة.



الخطوة 2. قم بإدخال المعلومات كما هو موضح في الصورة.

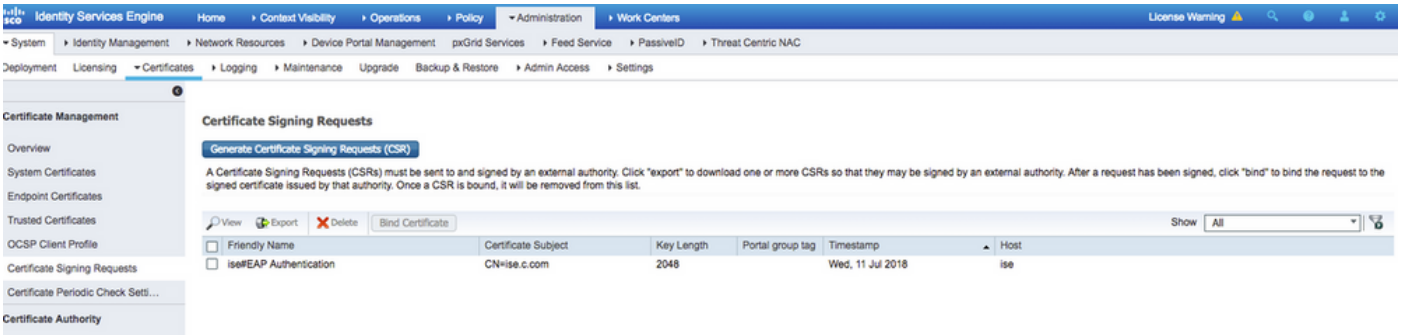


شهادة الثقة على ISE

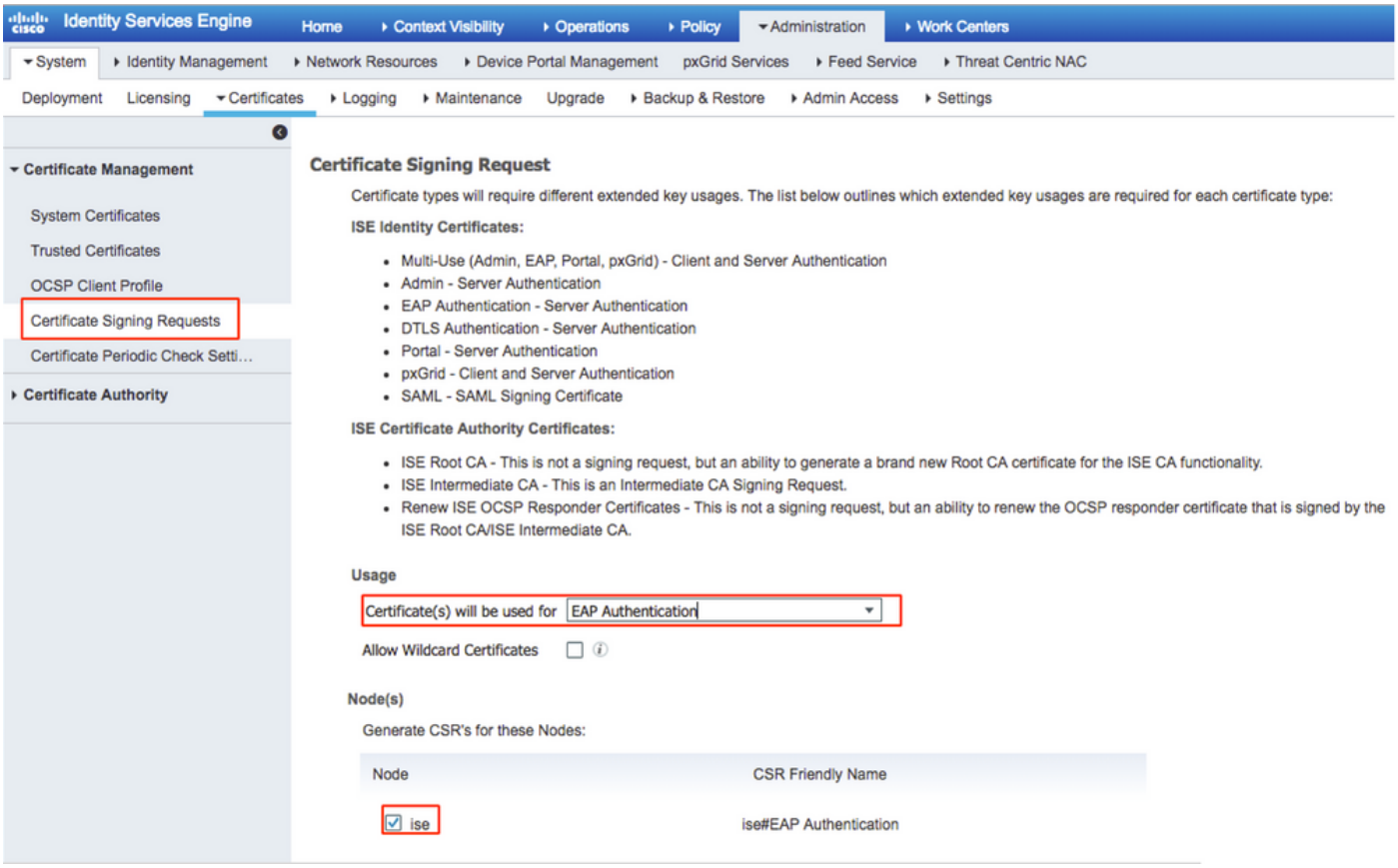
الخطوة 1. انتقل إلى **إدارة > نظام > شهادات > إدارة الشهادات > شهادات موثوق بها**.

انقر على **استيراد** لاستيراد شهادة إلى ISE. بمجرد إضافة عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) وإنشاء مستخدم على ISE، يلزمك القيام بالجزء الأكثر أهمية من EAP-TLS وهو الثقة في الشهادة على ISE. لذلك، تحتاج إلى توليد CSR.

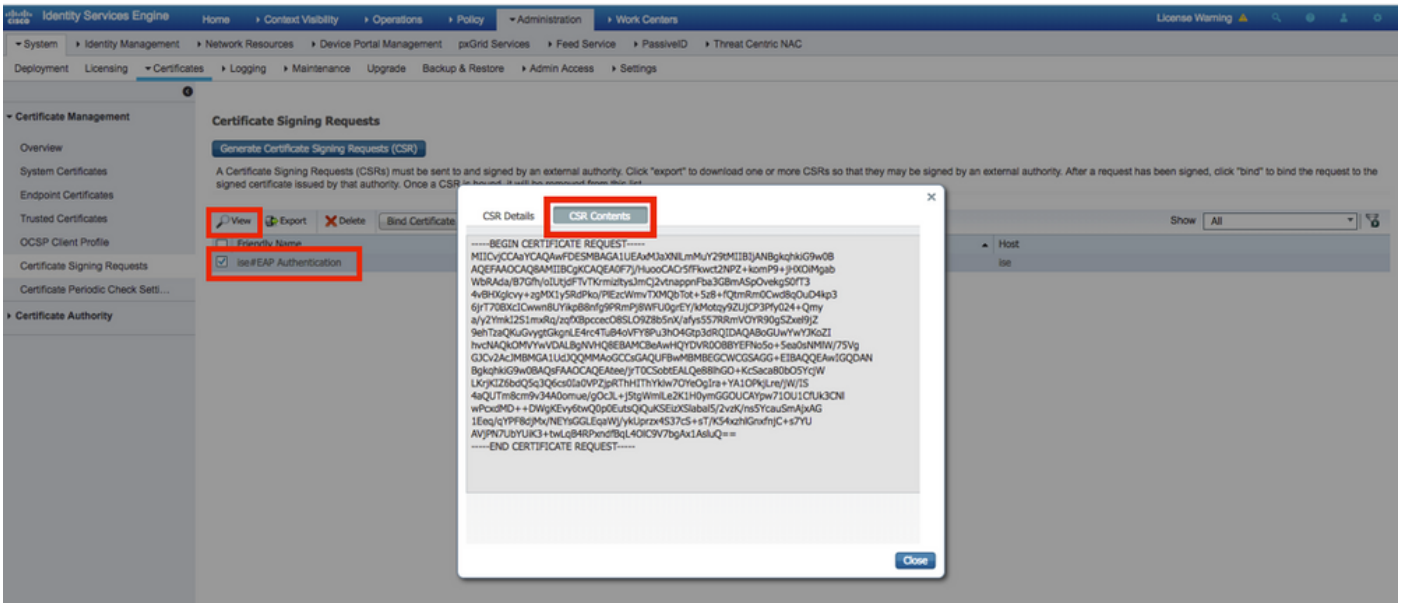
الخطوة 2. انتقل إلى **الإدارة > الشهادات > طلبات توقيع الشهادة > إنشاء طلبات توقيع الشهادة (CSR)** كما هو موضح في الصورة.



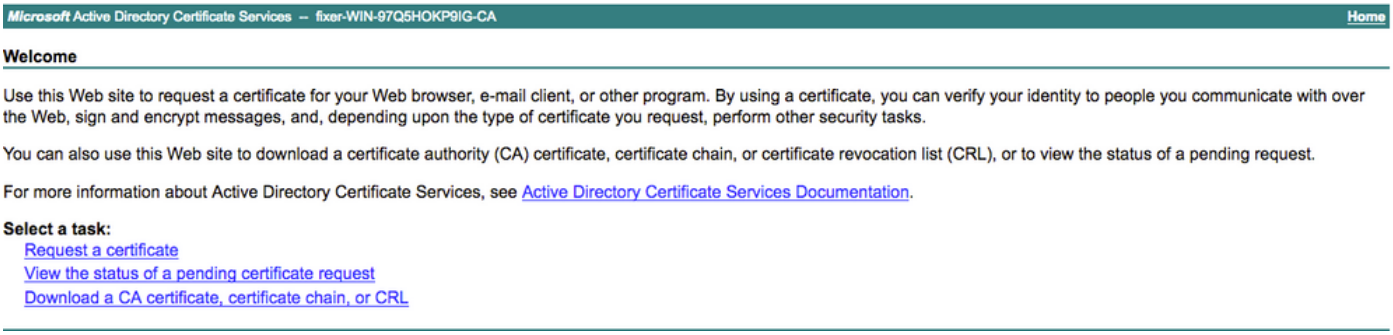
الخطوة 3. لإنشاء CSR، انتقل إلى **الاستخدام** ومن **الشهادة (الشهادات) سيتم استخدامها** للخيارات المنسدلة حدد **مصادقة EAP** كما هو موضح في الصورة.



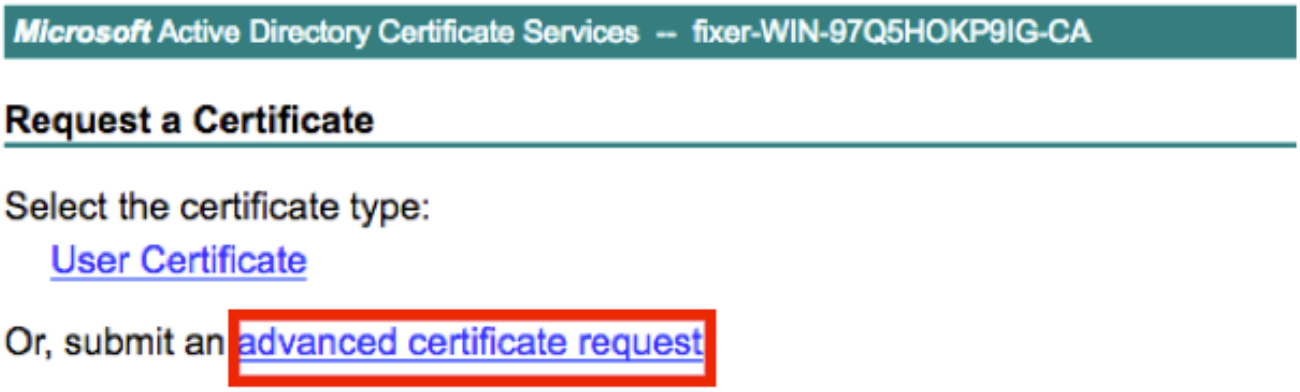
الخطوة 4. يمكن عرض CSR الذي تم إنشاؤه على ISE. انقر فوق **عرض** كما هو موضح في الصورة.



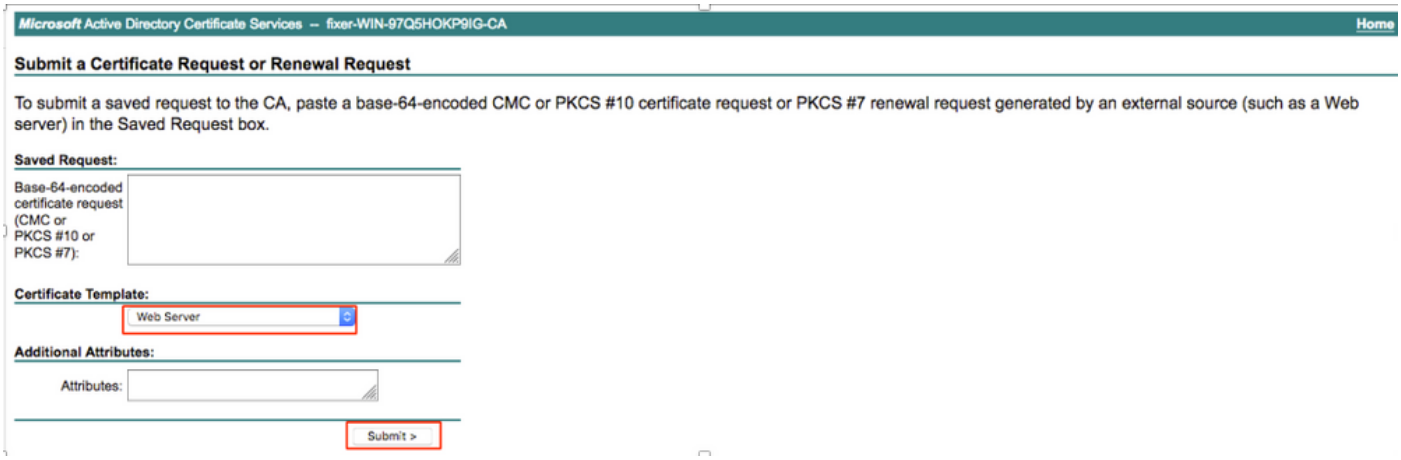
الخطوة 5. بمجرد إنشاء CSR، تصفح إلى خادم CA وانقر فوق **طلب شهادة** كما هو موضح في الصورة:



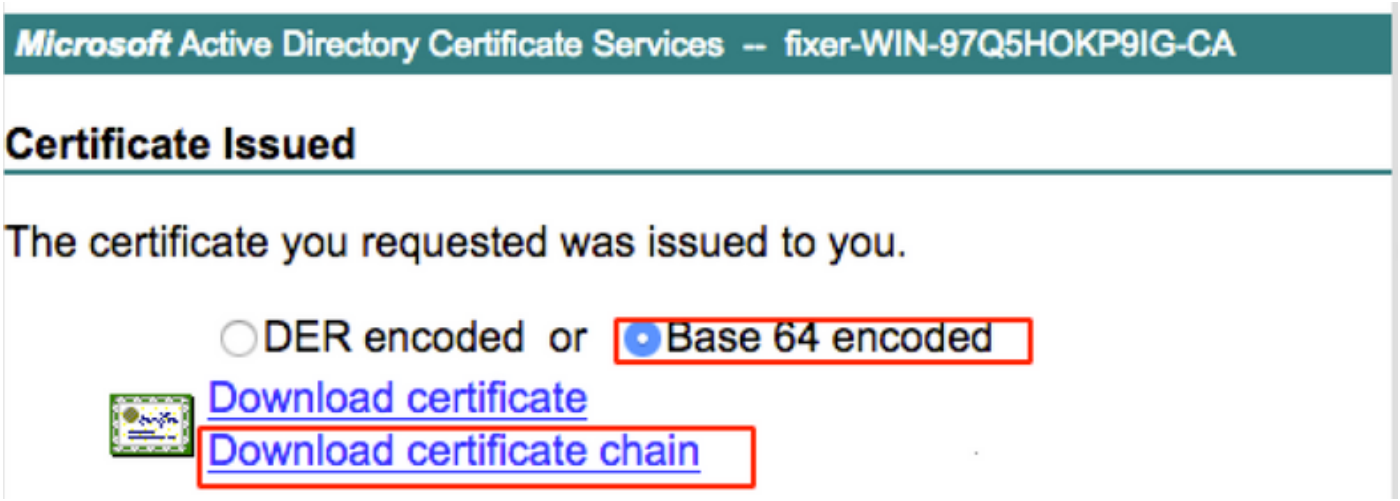
الخطوة 6. بمجرد أن تطلب شهادة، تحصل على خيارات **لشهادة المستخدم** و**طلب شهادة متقدم**، انقر على **طلب شهادة متقدم** كما هو موضح في الصورة.



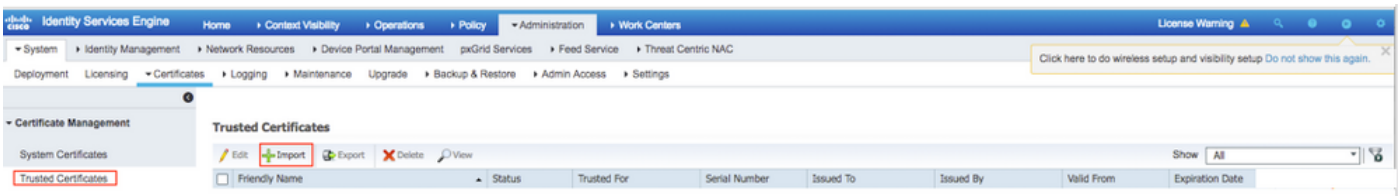
الخطوة 7. الصق CSR الذي تم إنشاؤه في **طلب الشهادة المرمزة ل Base-64**. من **قالب الشهادة:** خيار القائمة المنسدلة، أختر **خادم الويب** وانقر فوق **إرسال** كما هو موضح في الصورة.

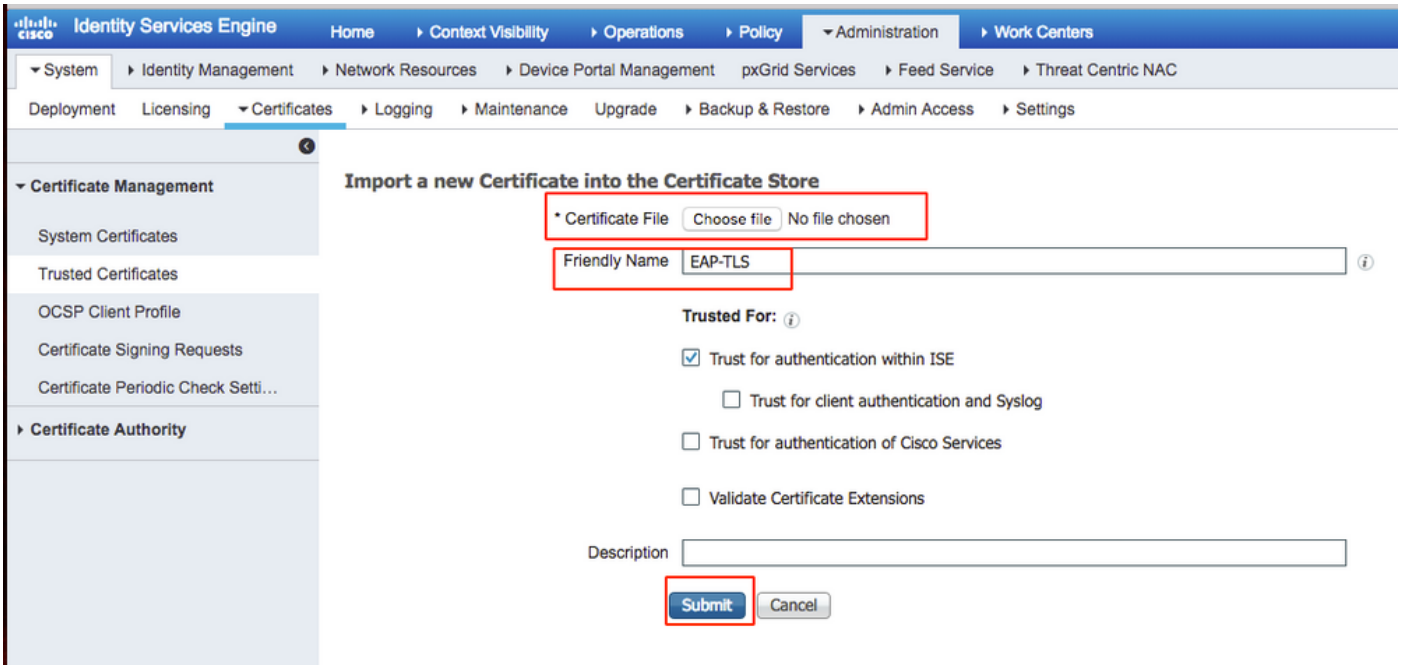


الخطوة 8. بمجرد النقر فوق **إرسال**، تحصل على الخيار لتحديد نوع الشهادة، حدد **Base-64 المشفر** وانقر فوق **سلسلة تنزيل الشهادة** كما هو موضح في الصورة.

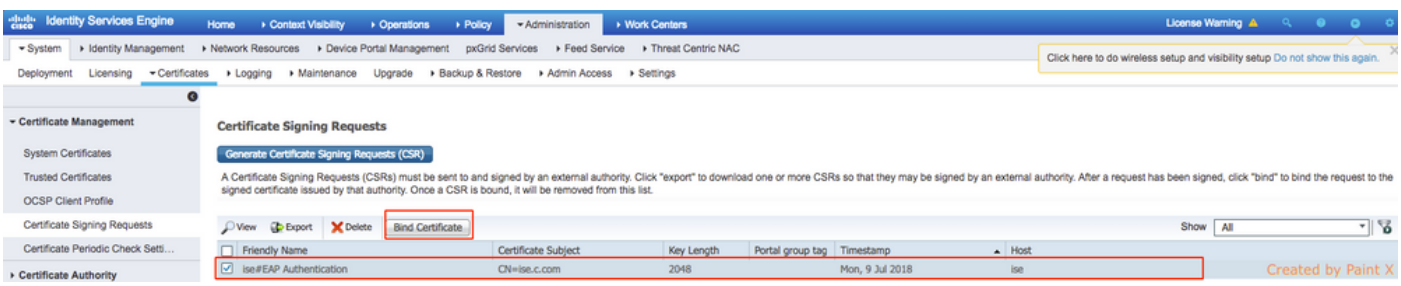


الخطوة 9. اكتمل تنزيل الشهادة لخادم ISE. يمكنك إستخراج الشهادة، وستحتوي الشهادة على شهادتين، شهادة جذر وشهادة وسيطة أخرى. يمكن إستيراد الشهادة الجذر تحت **إدارة > شهادات > شهادات موثوق بها > إستيراد** كما هو موضح في الصور.

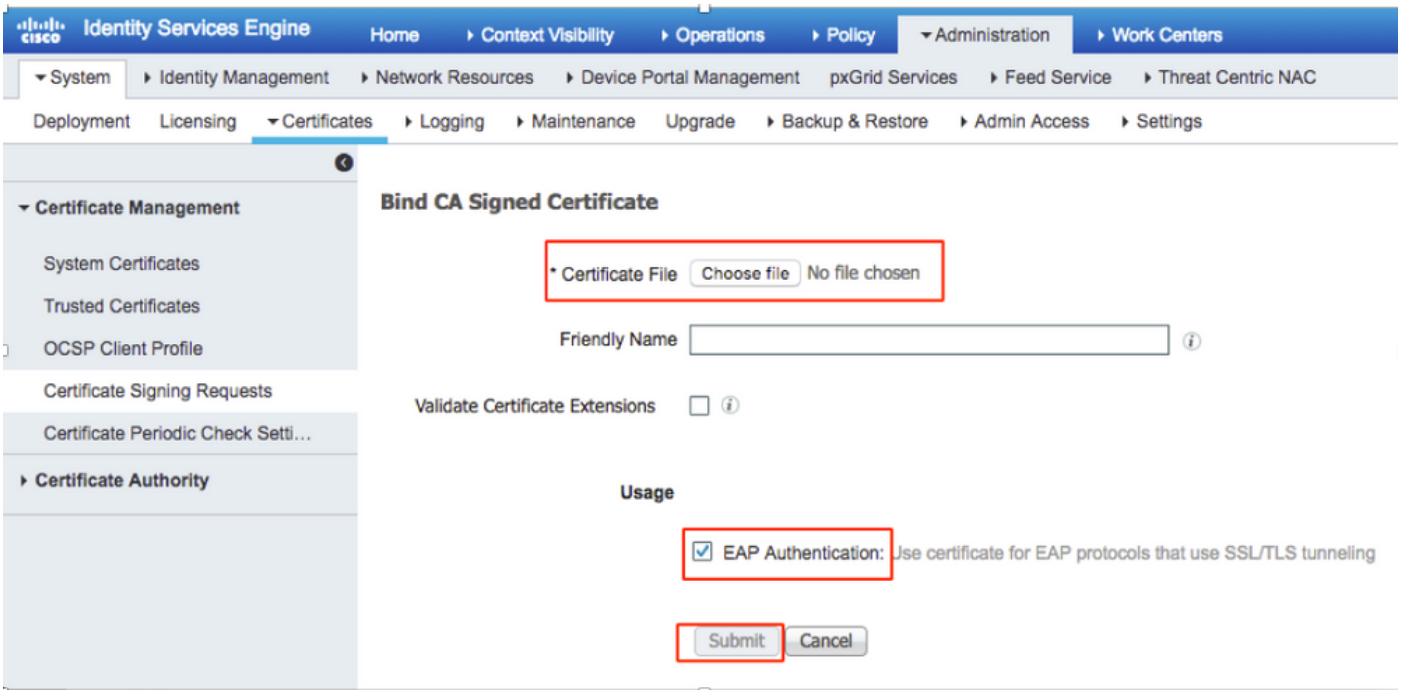




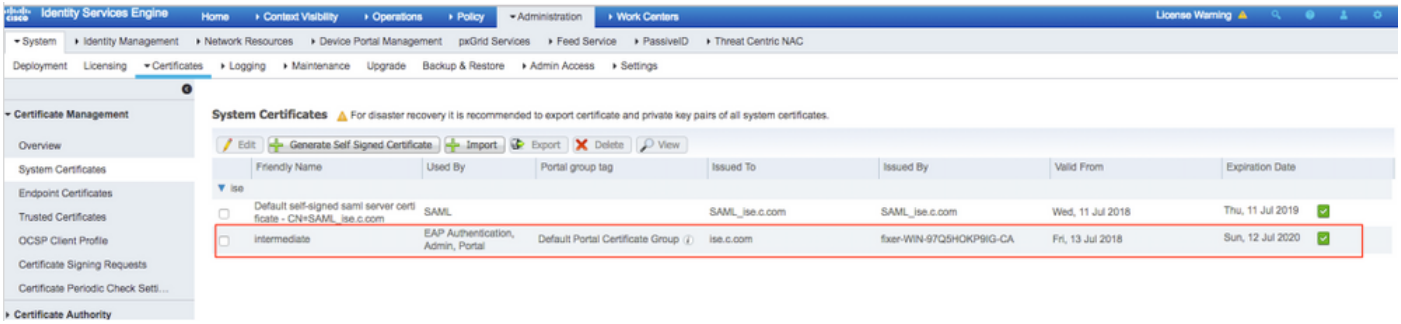
الخطوة 10. بمجرد النقر فوق **إرسال**، تتم إضافة الشهادة إلى قائمة الشهادات الموثوق بها. أيضا، يلزم الشهادة الوسيطة للربط مع CSR كما هو موضح في الصورة.



الخطوة 11. بمجرد النقر على **ترخيص الربط**، هناك خيار لاختيار ملف الترخيص المحفوظ على سطح مكتبك. تصفح إلى الشهادة الوسيطة وانقر **تسليم** كما هو موضح في الصورة.



الخطوة 12. لعرض الشهادة، انتقل إلى **إدارة > شهادات > شهادات النظام** كما هو موضح في الصورة.



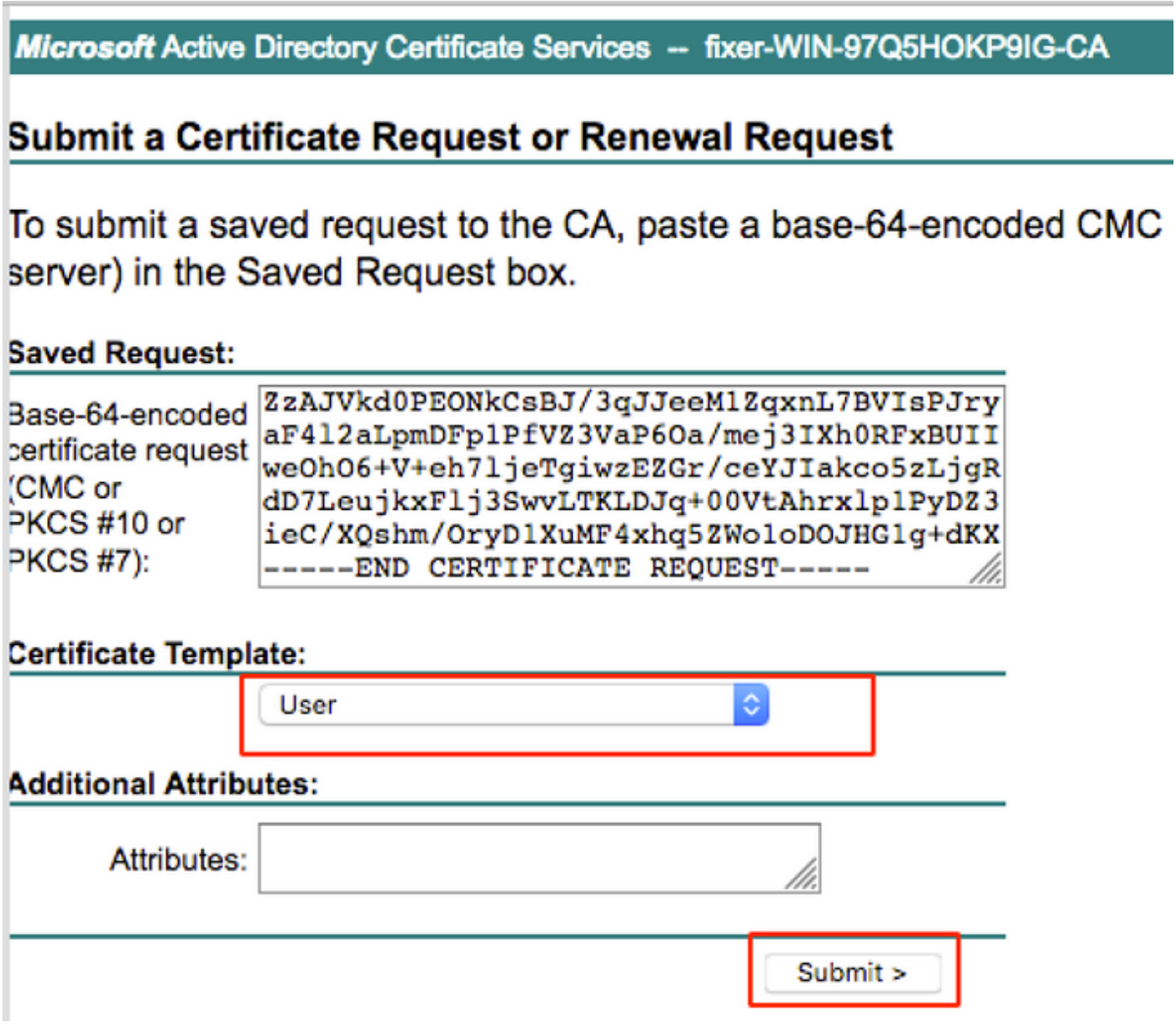
عميل EAP-TLS

تنزيل شهادة المستخدم على جهاز العميل (سطح مكتب Windows)

الخطوة 1. لمصادقة مستخدم السلكي من خلال EAP-TLS، يجب عليك إنشاء شهادة عميل. قم بتوصيل كمبيوتر Windows بالشبكة حتى تتمكن من الوصول إلى الخادم. افتح مستعرض ويب وأدخل هذا العنوان: https://sever ip addr/certsrv—

الخطوة 2. لاحظ أنه يجب أن يكون المرجع المصدق هو نفسه الذي تم به تنزيل الشهادة لـ ISE.

لهذا السبب تحتاج الاستعراض نفس خادم CA الذي أستخدمته لتنزيل الشهادة للخادم. في المرجع المصدق نفسه، انقر فوق **طلب شهادة** كما تم مسبقا، ومع ذلك هذه المرة تحتاج إلى تحديد **مستخدم** كقالب شهادة كما هو موضح في الصورة.



الخطوة 3. بعد ذلك، انقر فوق **تنزيل سلسلة الشهادات** كما تم سابقا للخادم.

بمجرد الحصول على الشهادات، اتبع هذه الخطوات لاستيراد الشهادة من كمبيوتر محمول يعمل بنظام التشغيل Windows.

الخطوة 4. لاستيراد الشهادة، تحتاج إلى الوصول إليها من وحدة تحكم الإدارة (MMC) ل Microsoft.

1. لفتح حركة MMC إلى **ابدأ > تشغيل > MMC**.
2. انتقل إلى **ملف > إضافة / إزالة الإنذار**
3. انقر نقرا مزدوجا على **شهادات**.
4. حدد **حساب الكمبيوتر**.
5. حدد **الكمبيوتر المحلي > إنهاء**
6. طقطقة **ok** in order to خرجت الأداة الإضافية نافذة.
7. انقر فوق **[+]** بجوار **الشهادات > شخصي > الشهادات**.
8. انقر بزر الماوس الأيمن على **التراخيص** وحدد **كل المهام > إستيراد**.
9. انقر فوق **Next (التالي)**.
10. انقر على **إستعراض**.
11. حدد **.cer** أو **.crt** أو **.pfx** الذي تريد إستيراده.

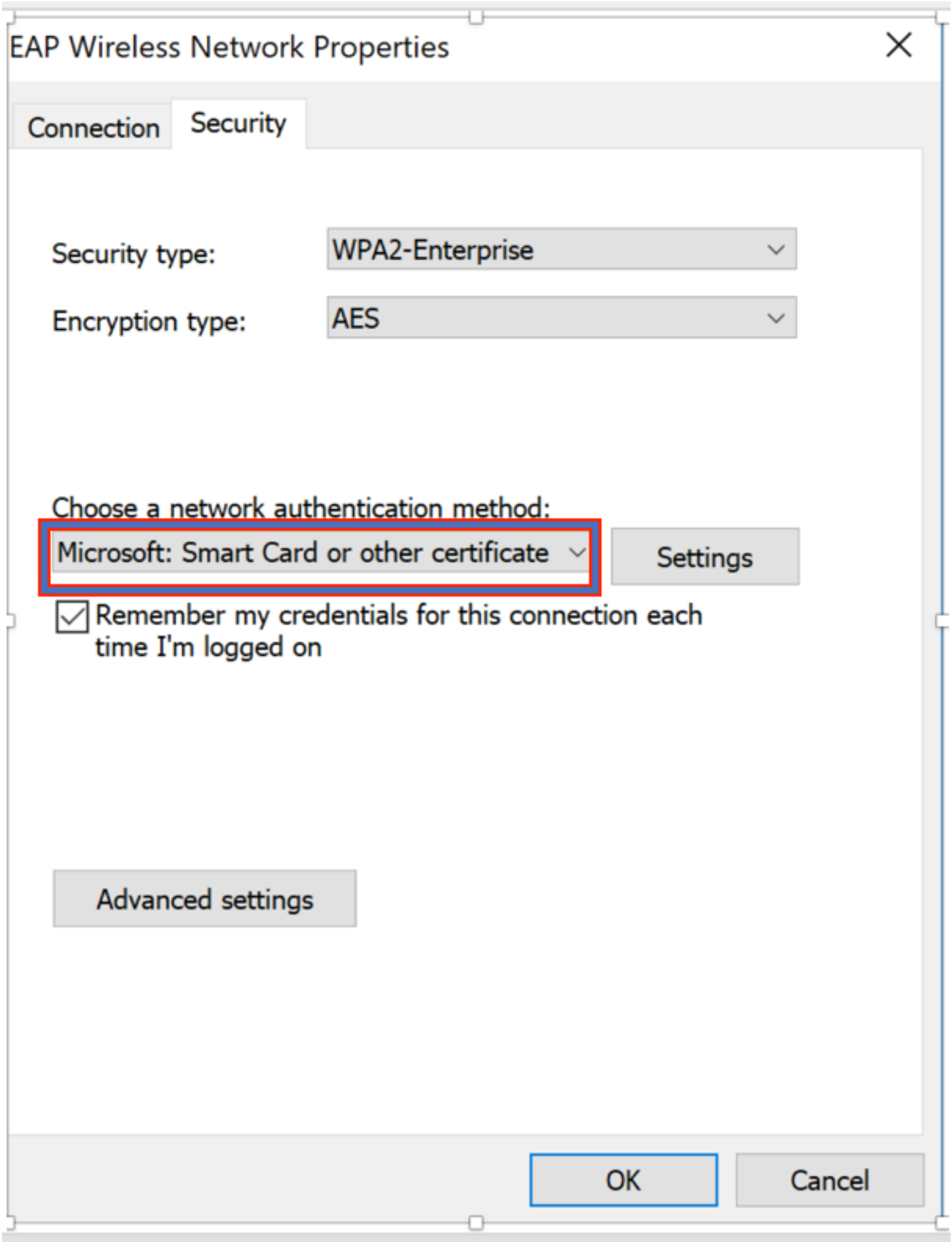
12. انقر فوق **فتح**.
13. انقر فوق **Next (التالي)**.
14. حدد **تحديد مخزن الشهادات تلقائيا بناء على نوع الشهادة**.
15. طقطقة **إنجاز و ok**

اذه في Windows (سطح مكتب) يلزمك تكوين عميلك السلكي، إذا تم إستيراد الشهادة من أجل EAP-TLS.

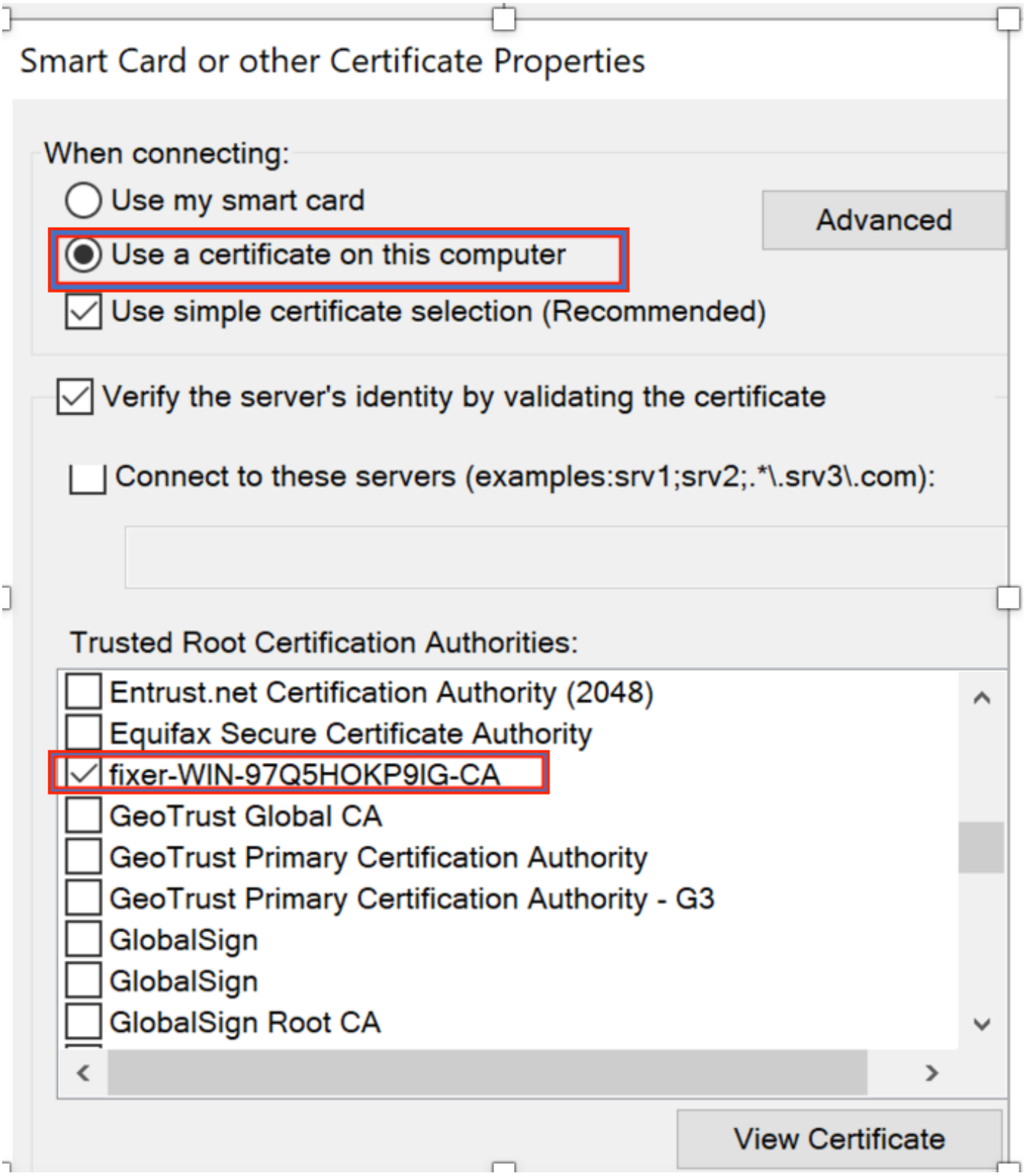
تكوين السلكي ل EAP-TLS

الخطوة 1. قم بتغيير التكوين السلكي الذي تم إنشاؤه سابقا لبروتوكول المصادقة المتوسع المحمي (PEAP) لاستخدام EAP-TLS بدلا من ذلك. انقر على **تكوين EAP السلكي**.

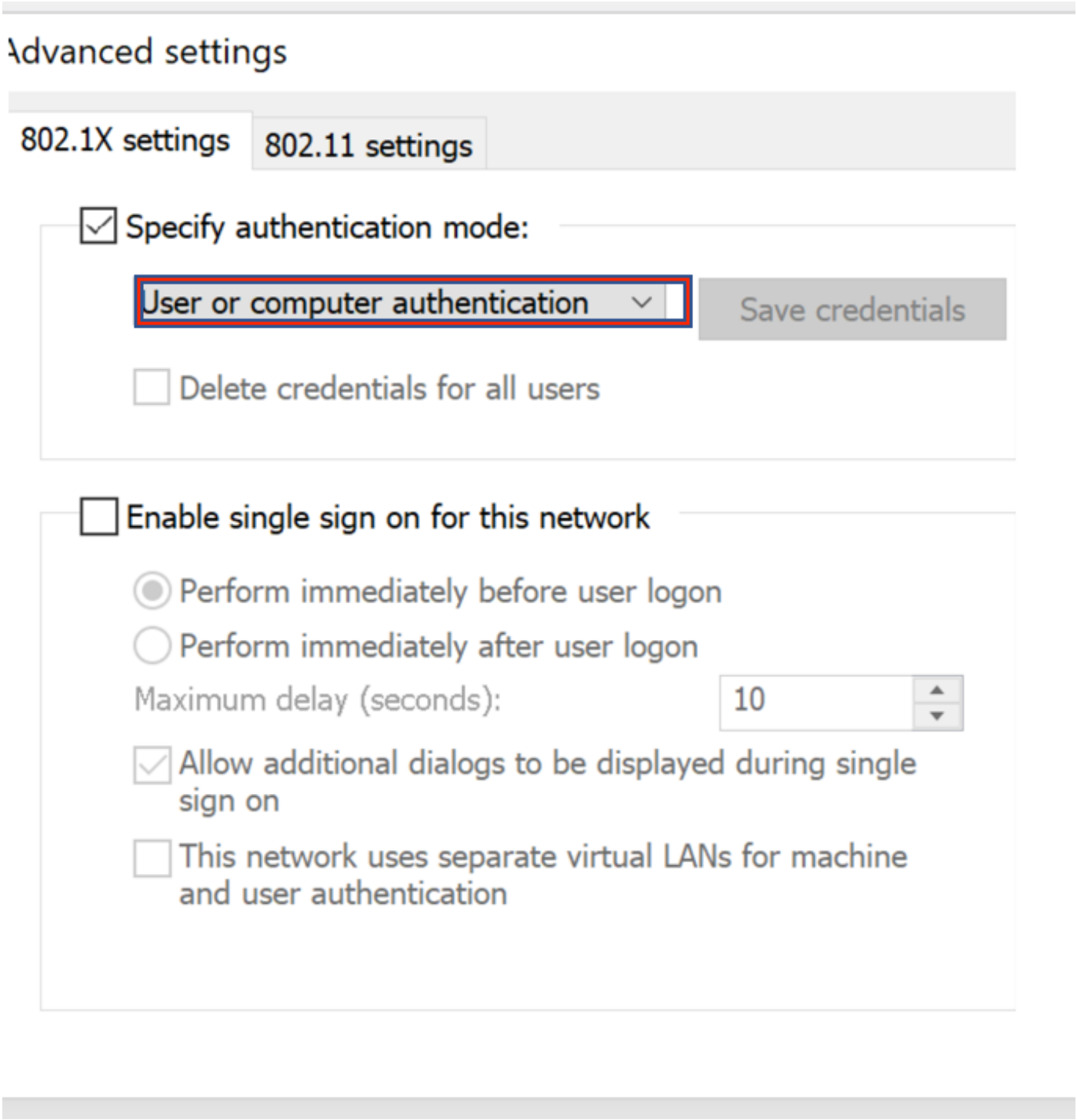
الخطوة 2. حدد **Microsoft: البطاقة الذكية أو أي شهادة أخرى** وانقر على **موافق** كما هو موضح في الصورة.



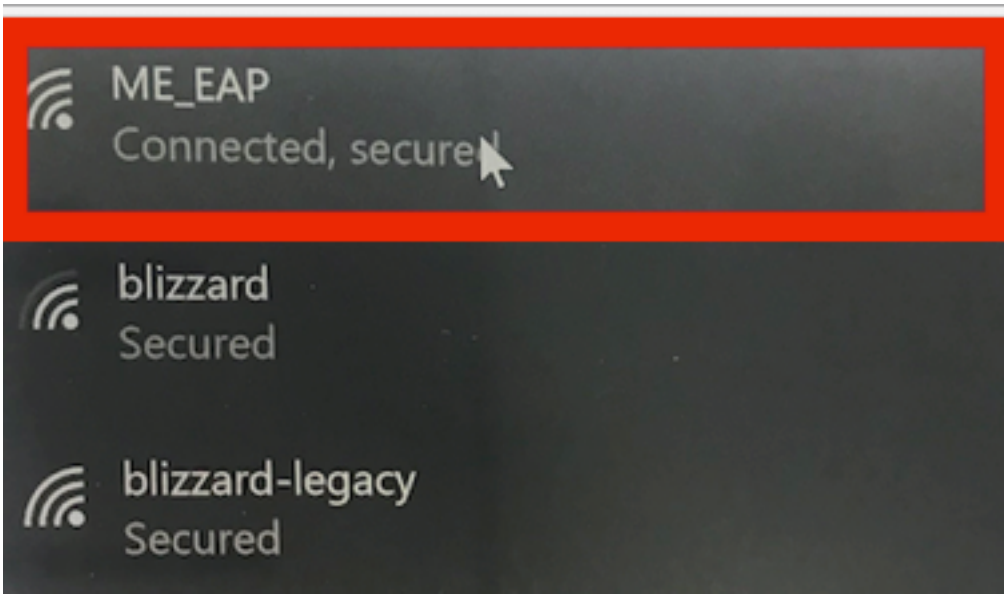
الخطوة 3. انقر على **الإعدادات** وحدد الشهادة الجذر الصادرة من خادم المرجع المصدق كما هو موضح في الصورة.



الخطوة 4. انقر فوق **إعدادات متقدمة** وحدد **مصادقة المستخدم أو الكمبيوتر** من علامة التبويب إعدادات 802.1x كما هو موضح في الصورة.



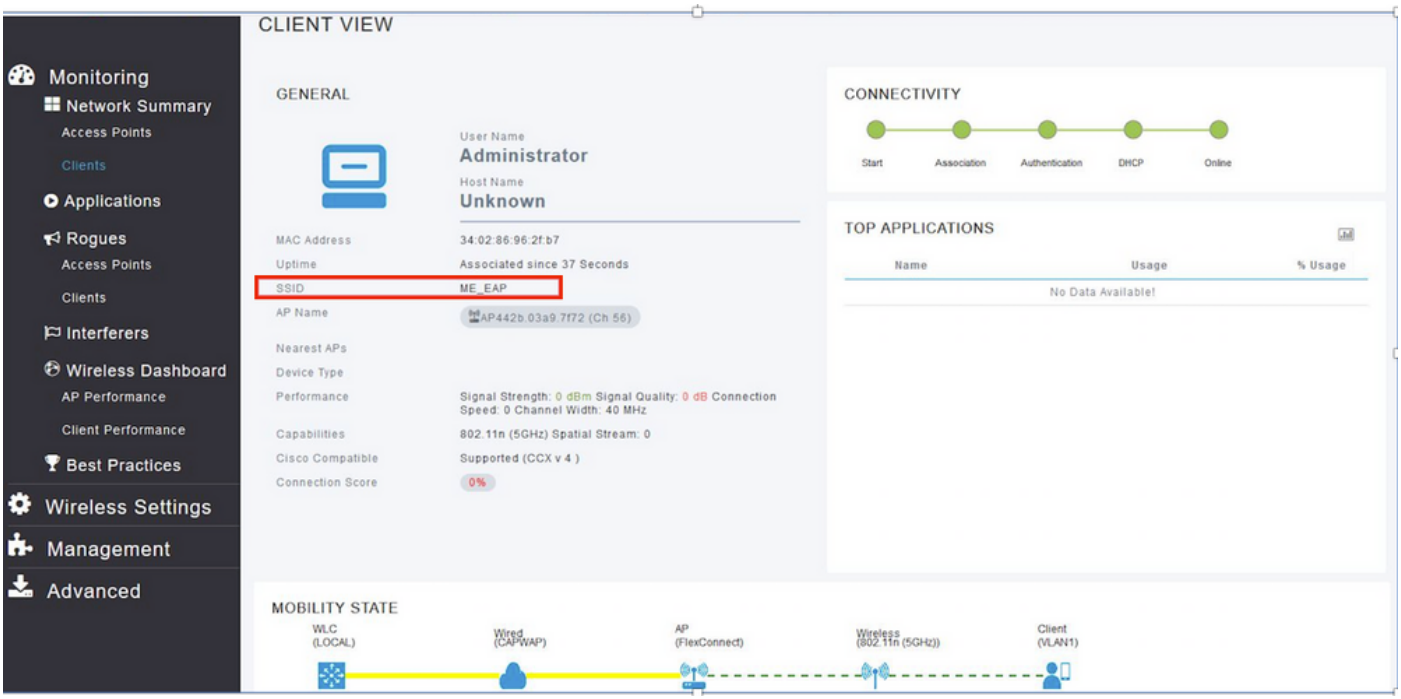
الخطوة 5. الآن حاول التوصيل مرة أخرى باللشبكة اللاسلكية ثم حدد التوصيف الصحيح (EAP في هذا المثال) ثم **توصيل**. أنت موصل باللشبكة اللاسلكية كما هو موضح في الصورة.

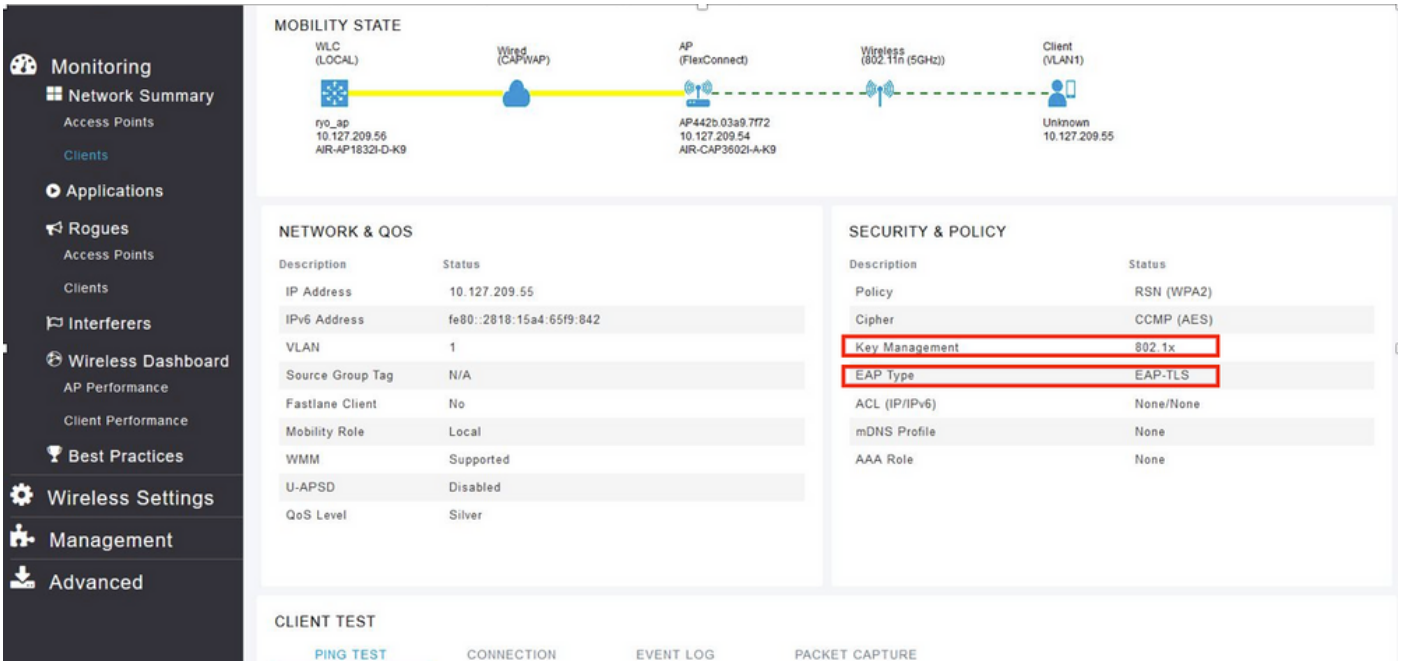


التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الخطوة 1. يجب أن يكون نوع EAP للعميل EAP-TLS. وهذا يعني أن العميل قد أكمل المصادقة باستخدام EAP-TLS وحصل على عنوان IP وهو جاهز لتمرير حركة المرور كما هو موضح في الصور.

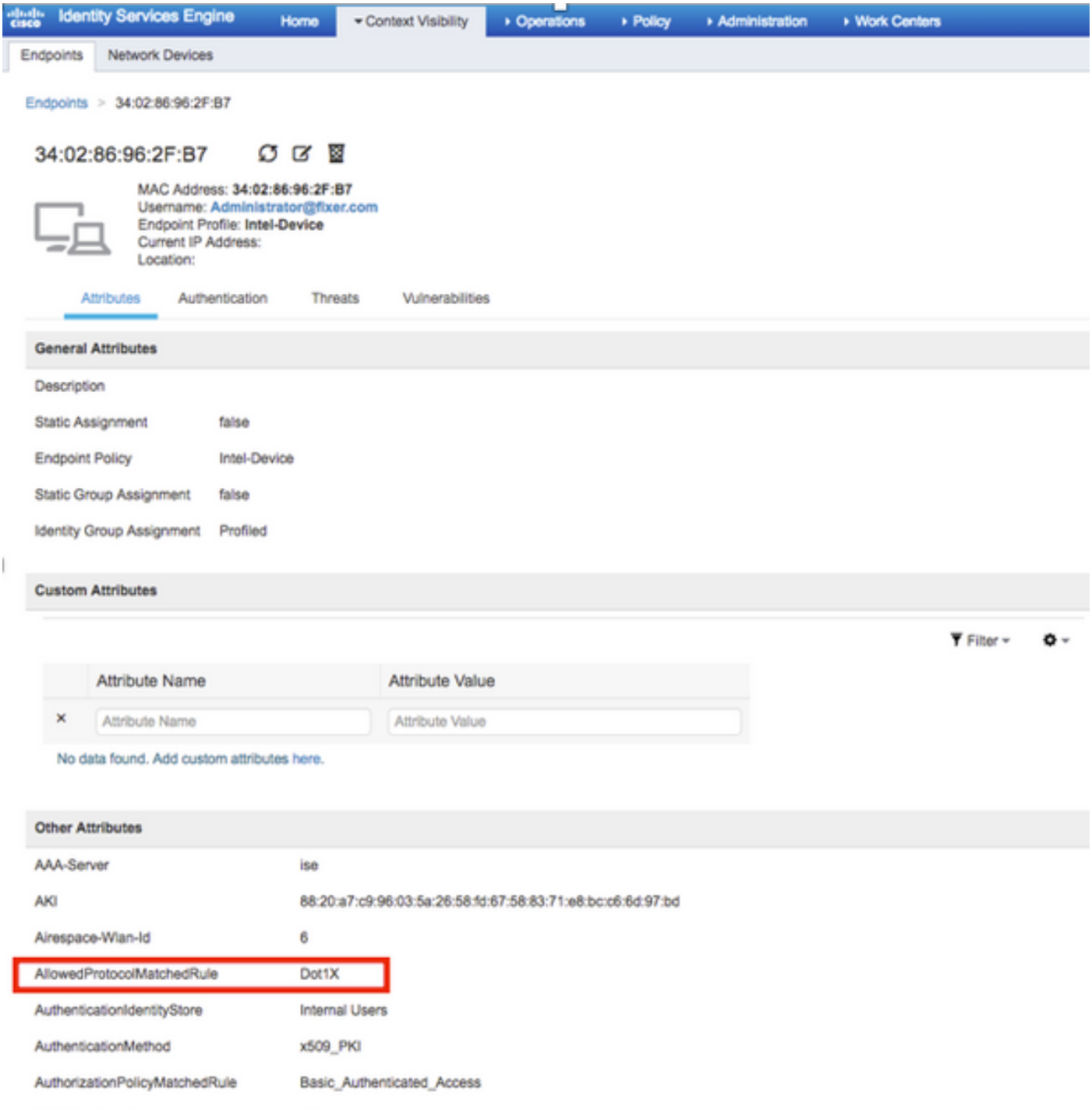




الخطوة 2. فيما يلي تفاصيل العميل من واجهة سطر الأوامر (CLI) لوحدة التحكم (تم قص الإخراج):

```
(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
```

الخطوة 3. على ISE، انتقل إلى **العمليات > المصادقات** كما هو موضح في الصور.


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Endpoints
Network Devices
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
Attribute Name
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, 1.3.6.1.4.1.311.1
FailureReason	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=co
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"
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	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 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).