فهم EAP-TLS وتكوينه باستخدام WLC و ISE

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد شبكة محلية السلكية (WLAN) باستخدام بروتوكول 802.1X و EAP-TLS المصادقة المتوسع

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- عملية مصادقة وقفا لمعيار 802.1X
- الشهادات

المكونات المستخدمة

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

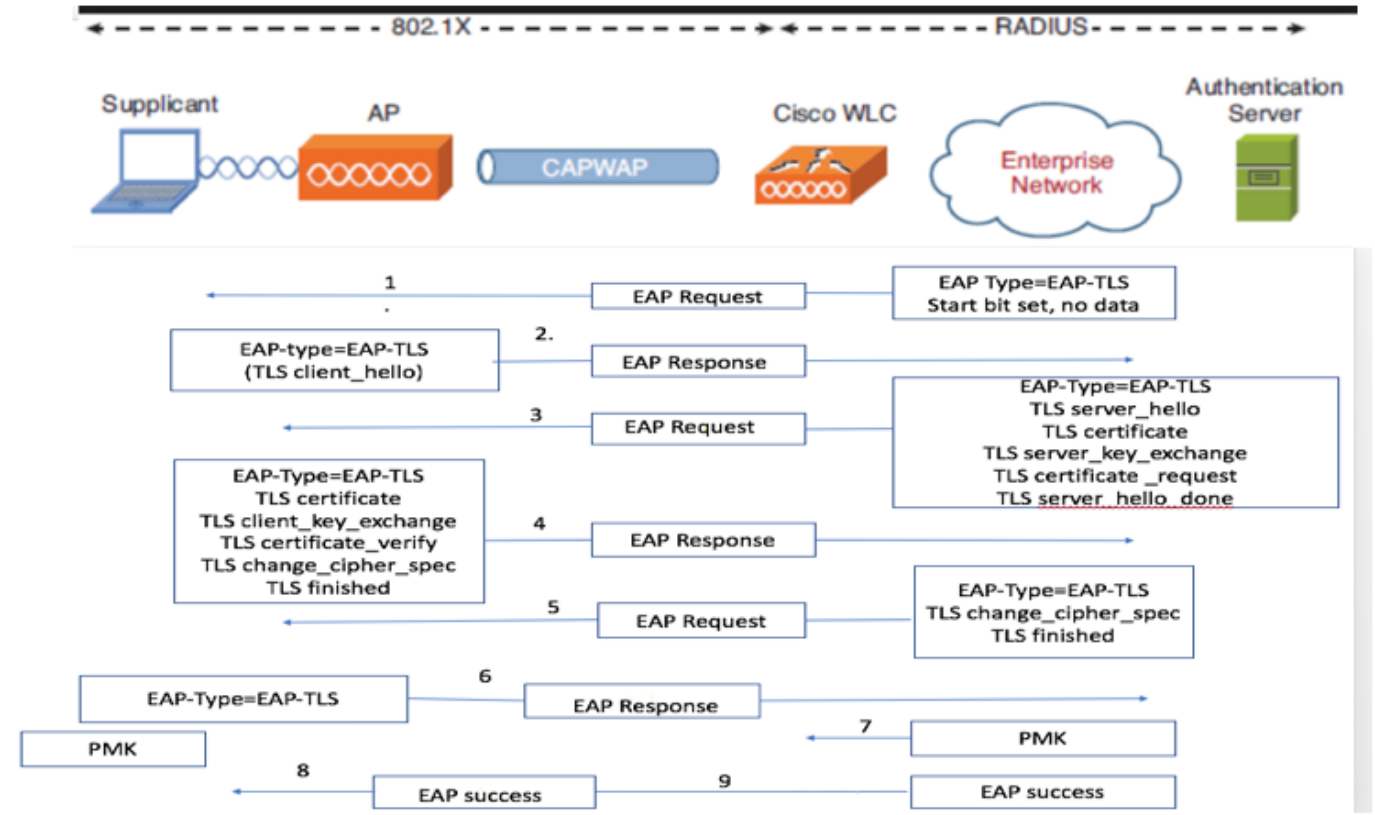
- WLC 3504، الإصدار 8.10

- Identity Services Engine (ISE)، الإصدار 2.7

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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). لا تسمح نقطة الوصول للعميل بإرسال أي بيانات عند هذه النقطة وترسل طلب مصادقة. ثم يستجيب مقدم الطلب بهوية EAP-Response. يقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بعد ذلك بتوصيل معلومات معرف المستخدم إلى خادم المصادقة. يستجيب خادم RADIUS للعميل مرة أخرى باستخدام حزمة بدء EAP-TLS. تبدأ محادثة EAP-TLS عند هذه النقطة.
2. يرسل النظير EAP-Response مرة أخرى إلى خادم المصادقة الذي يحتوي على رسالة مصافحة "client_hello"، وهي تشفير تم تعيينه إلى NULL
3. يستجيب خادم المصادقة باستخدام حزمة Access-challenge التي تحتوي على:

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

4. يستجيب العميل برسالة EAP-Response التي 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
```

5.بعد مصادقة العميل بنجاح، يستجيب خادم RADIUS لتحدي الوصول الذي يحتوي على الرسالة "change_cipher_spec" وانتهاء المصافحة.

6.عندما يستلم هذا، يتحقق العميل من التجزئة لمصادقة خادم RADIUS.

7.يتم اشتقاق مفتاح تشفير جديد ديناميكيا من السر أثناء مصافحة TLS

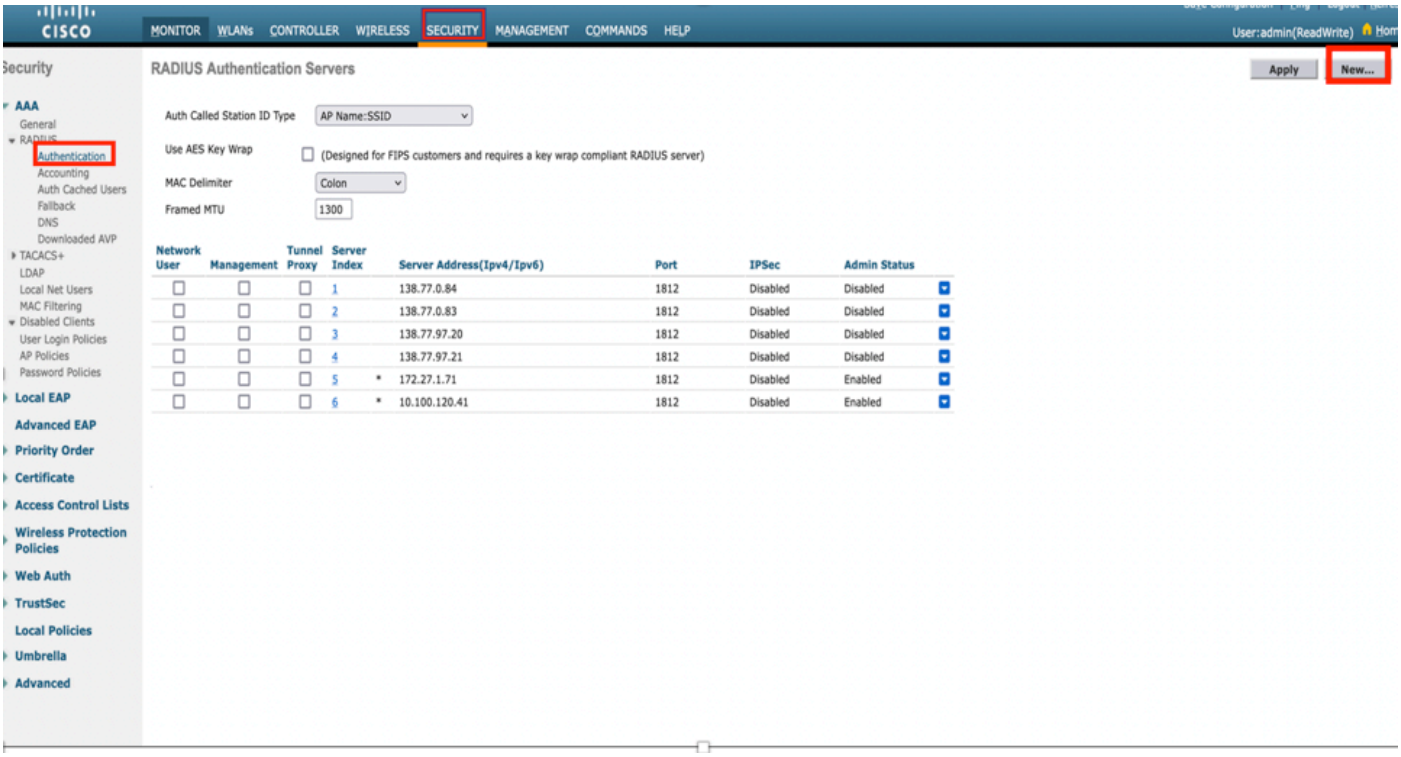
8/9.EAP-يتم إرسال Success أخيرا من الخادم إلى المصدق ثم يتم إلحاقه بالمطالب.

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

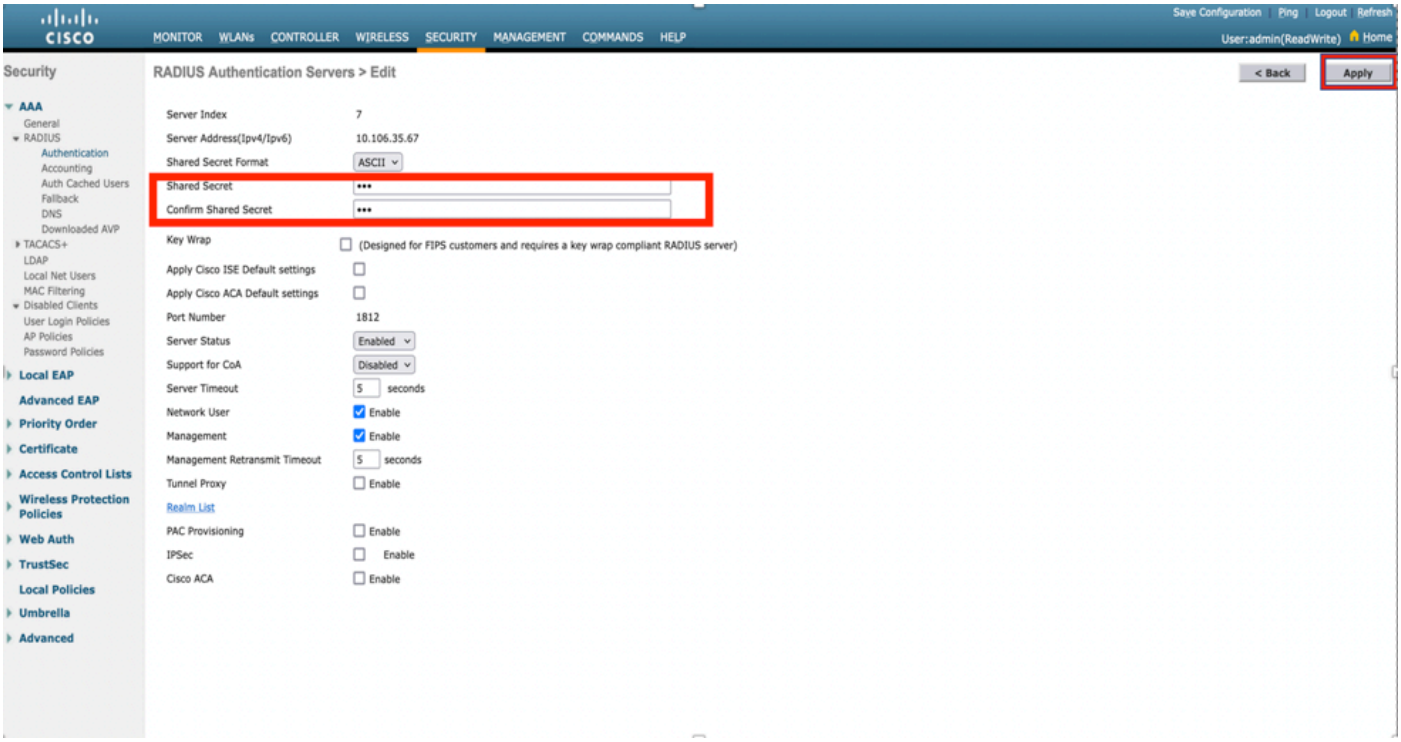
التكوين

وحدة التحكم في شبكة LAN اللاسلكية من Cisco

الخطوة 1. الخطوة الأولى هي تكوين خادم RADIUS على Cisco WLC. لإضافة خادم RADIUS، انتقل إلى **الأمان > RADIUS > المصادقة**. انقر **جديد** كما هو موضح في الصورة.



الخطوة 2. هنا، يحتاج أنت أن يدخل العنوان والسر المشترك <password> أن يكون استعملت in order to دقق ال WLC على ال ISE. انقر فوق **تطبيق** للمتابعة كما هو موضح في الصورة.

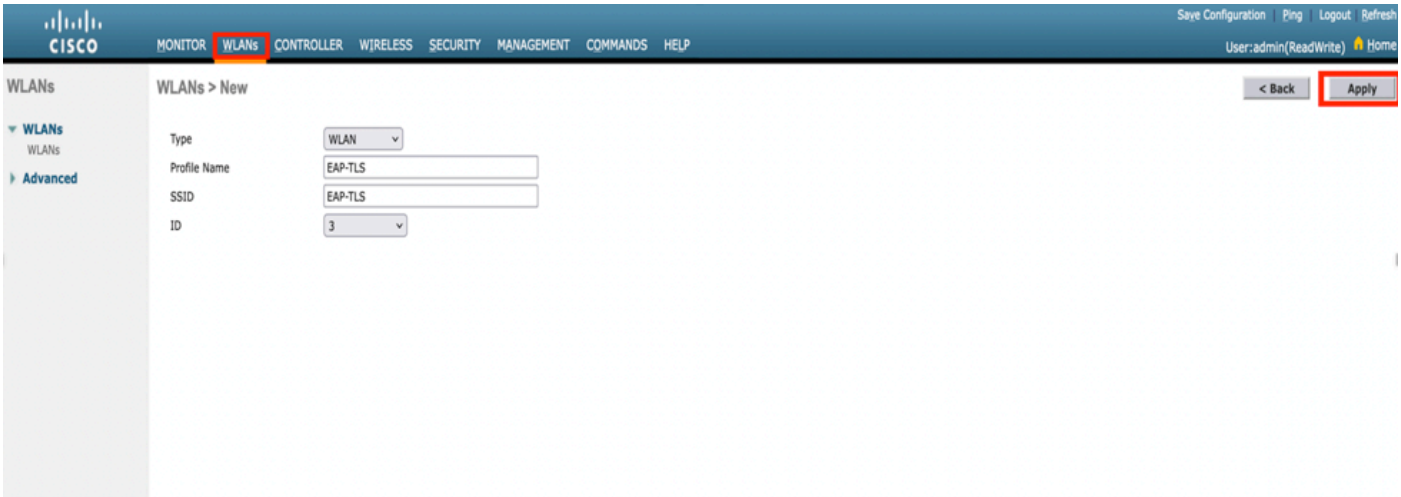


الخطوة 3. إنشاء شبكة WLAN لمصادقة RADIUS.

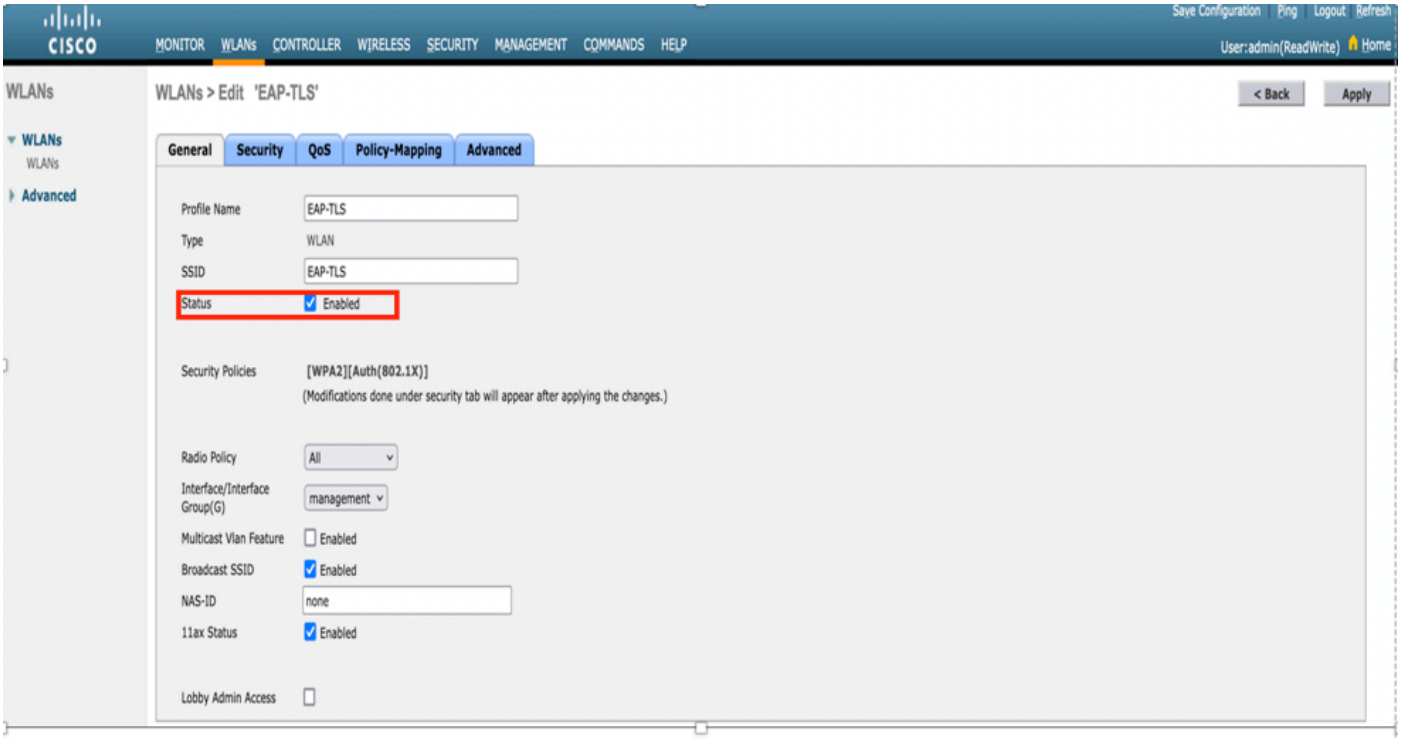
الآن، يمكنك إنشاء شبكة WLAN جديدة وتكوينها لاستخدام وضع WPA-مؤسسي، حتى يمكنها إستخدام RADIUS للمصادقة.

الخطوة 4. حدد **شبكات WLAN** من القائمة الرئيسية، أختر **إنشاء جديد** وانقر **انتقال** كما هو موضح في الصورة.

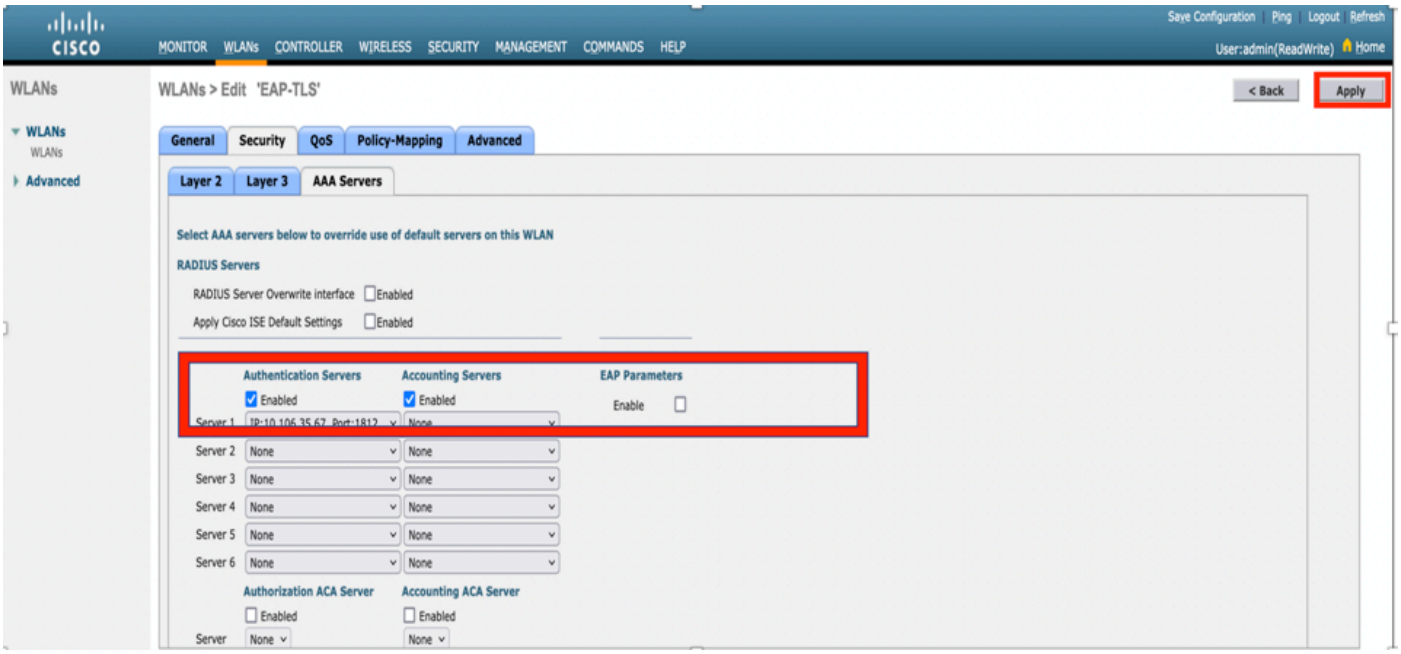
الخطوة 5. قم بتسمية **EAP-TLS** الجديد لشبكة WLAN. انقر فوق **تطبيق** للمتابعة كما هو موضح في الصورة.



الخطوة 6. انقر على **عام** وتأكد من أن الحالة **ممكنة**. سياسات التأمين الافتراضية هي مصادقة 802.1X و WPA2 كما هو موضح في الصورة.



الخطوة 7. الآن، انتقل إلى **التأمين > عامة التوبيب خوادم AAA**، حدد خادم RADIUS الذي قمت بتكوينه كما هو موضح في الصورة.



ملاحظة: من الأفضل التحقق من إمكانية الوصول إلى خادم RADIUS من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) قبل المتابعة. يستخدم RADIUS منفذ UDP 1812 (للمصادقة)، لذلك تحتاج إلى التأكد من عدم حظر حركة المرور هذه في أي مكان في الشبكة.

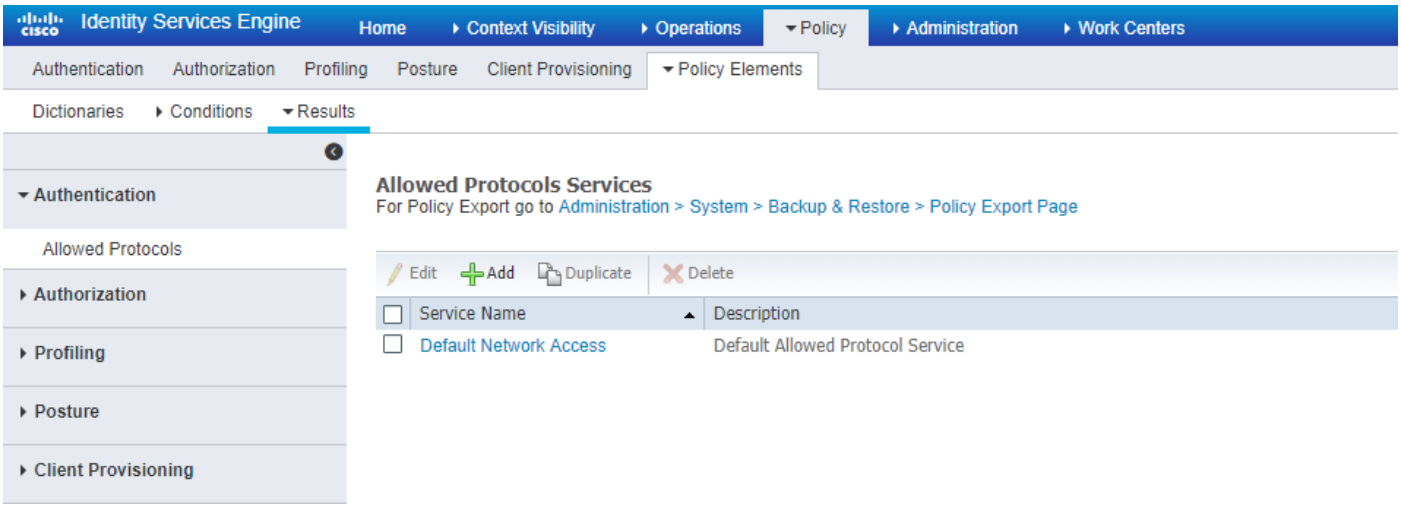
ISE مع Cisco WLC

إعدادات EAP-TLS

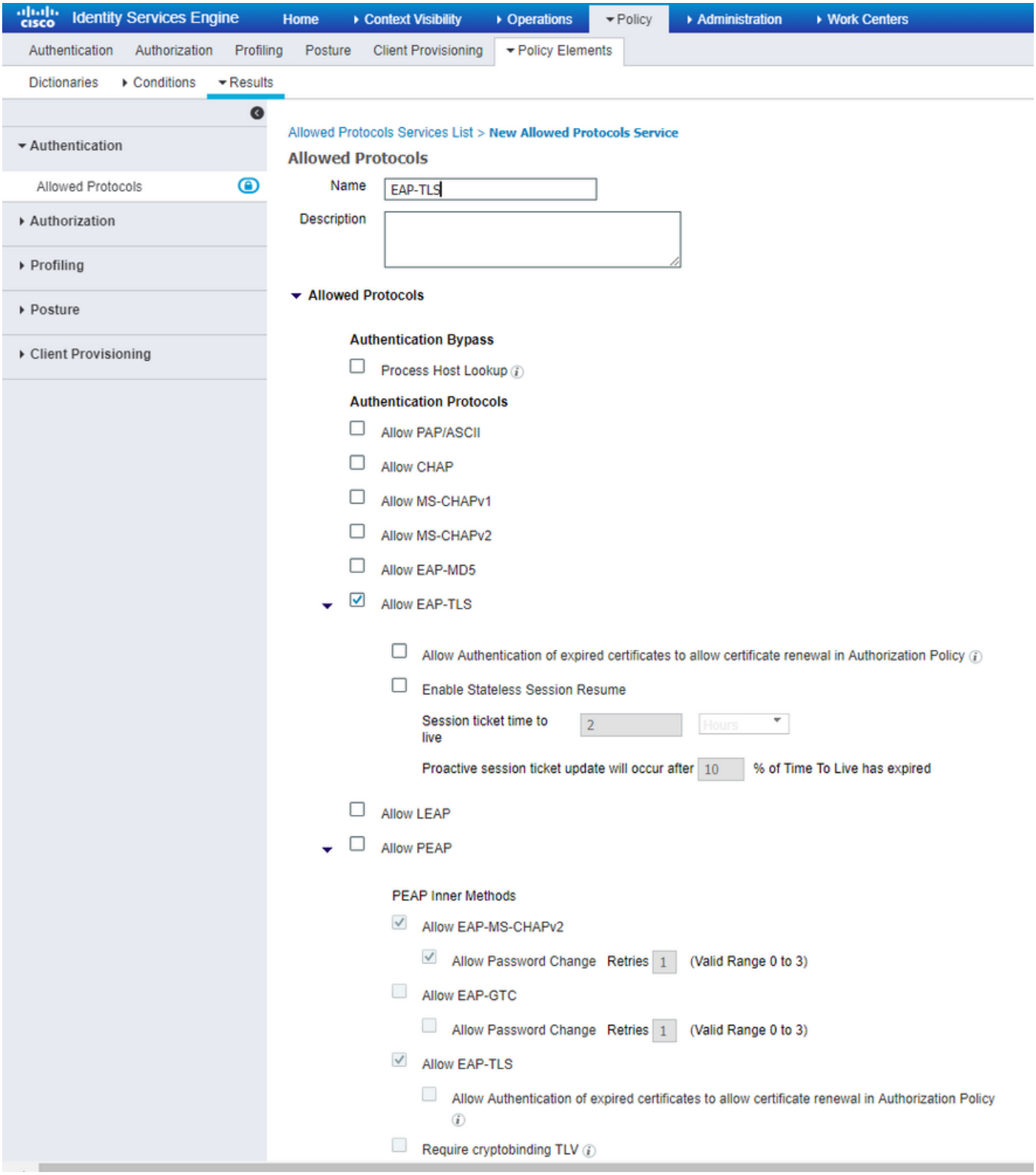
لإنشاء النهج، تحتاج إلى إنشاء قائمة البروتوكولات المسموح باستخدامها في سياستان. بما أن سياسة dot1x تمت كتابتها، حدد نوع EAP المسموح به بناء على كيفية تكوين السياسة.

إذا كنت تستخدم الإعداد الافتراضي، فإنك تسمح بمعظم أنواع EAP للمصادقة غير المفضلة إذا كنت بحاجة إلى تأمين الوصول إلى نوع EAP معين.

الخطوة 1. انتقل **إلى Policy > عناصر النهج > النتائج > المصادقة >** البروتوكولات **المسموح بها انقر** على **إضافة** كما هو موضح في الصورة.

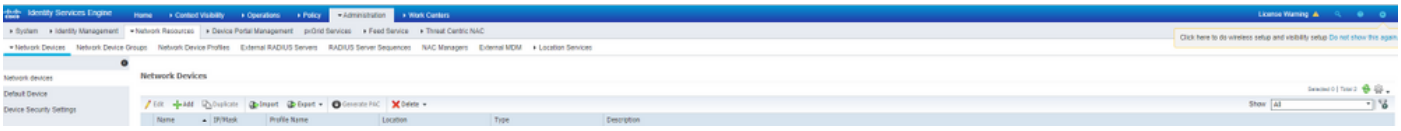


الخطوة 2. في قائمة البروتوكولات المسموح بها، يمكنك إدخال اسم القائمة. في هذه الحالة، يتم تحديد **السماح** لمربع **EAP-TLS** ويتم إلغاء تحديد مربعات أخرى كما هو موضح في الصورة.

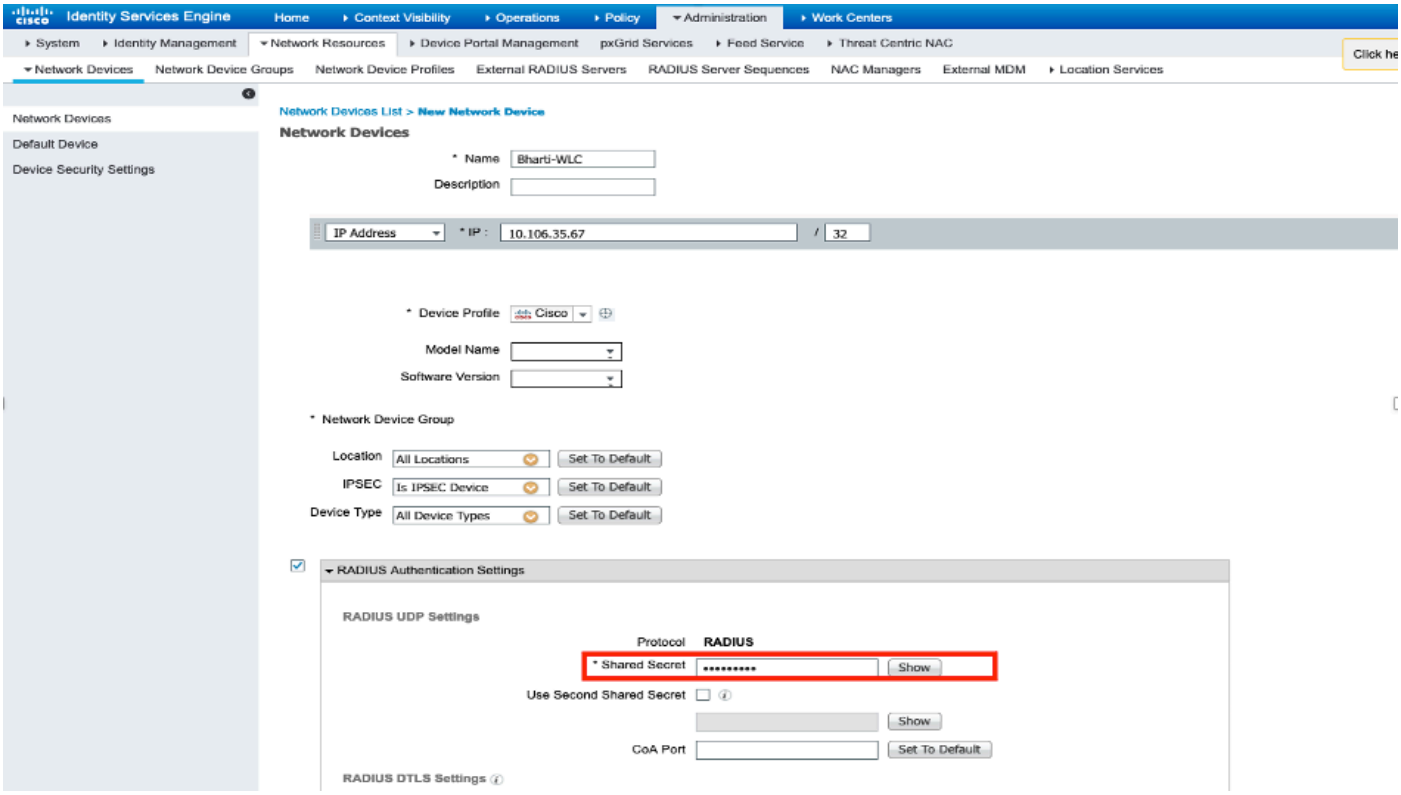


إعدادات WLC على ISE

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

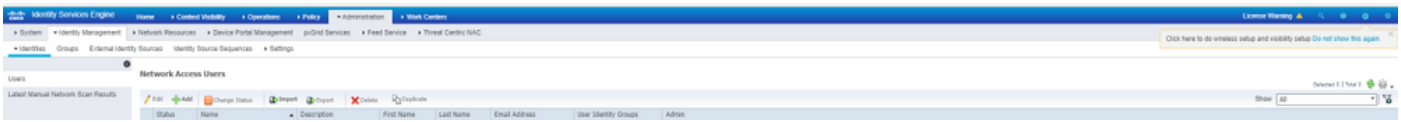


الخطوة 2. قم بإدخال القيم كما هو موضح في الصورة.

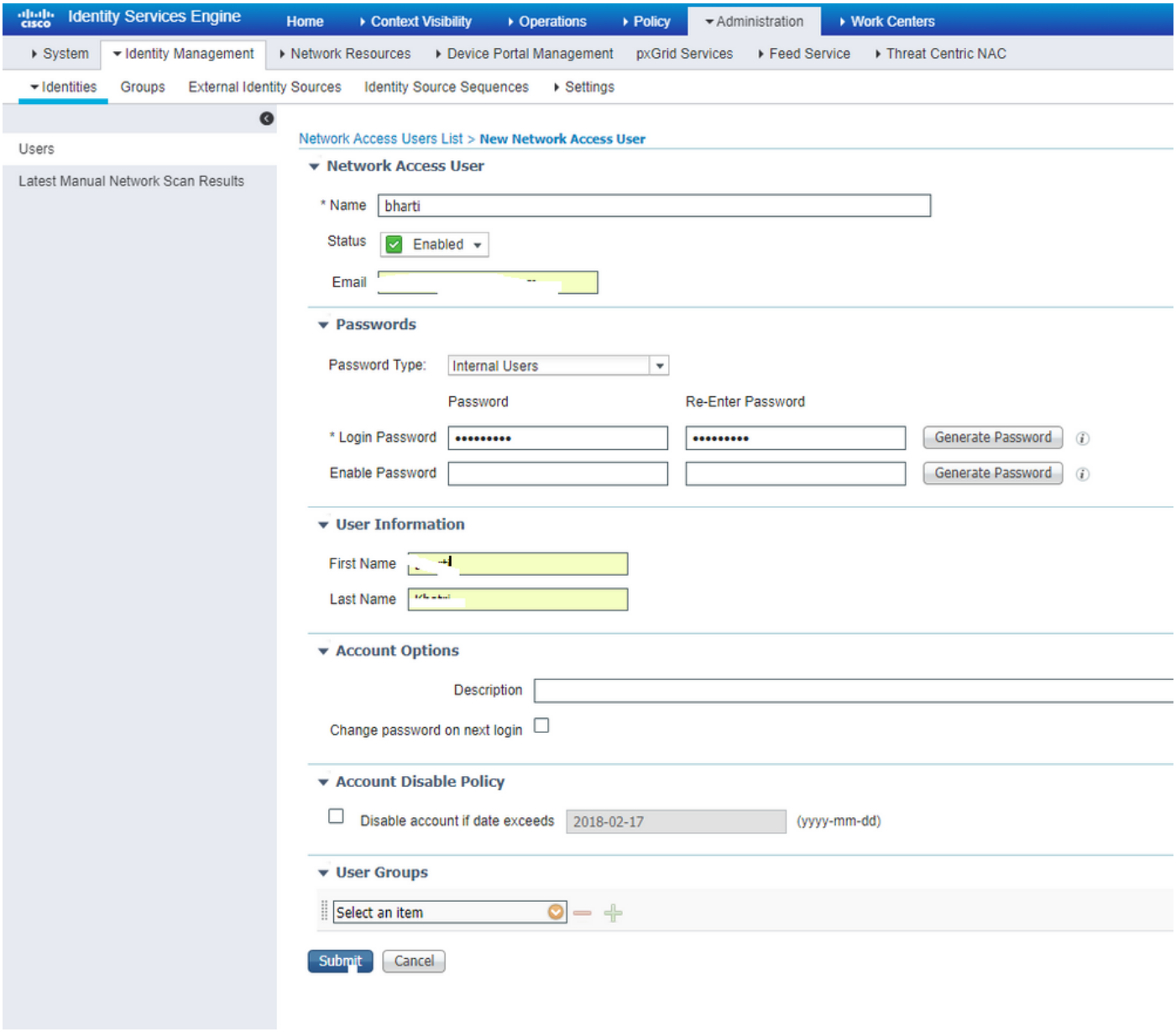


إنشاء مستخدم جديد على ISE

الخطوة 1. انتقل إلى **إدارة > إدارة الهوية > هويات > مستخدمين > إضافة** كما هو موضح في الصورة.



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

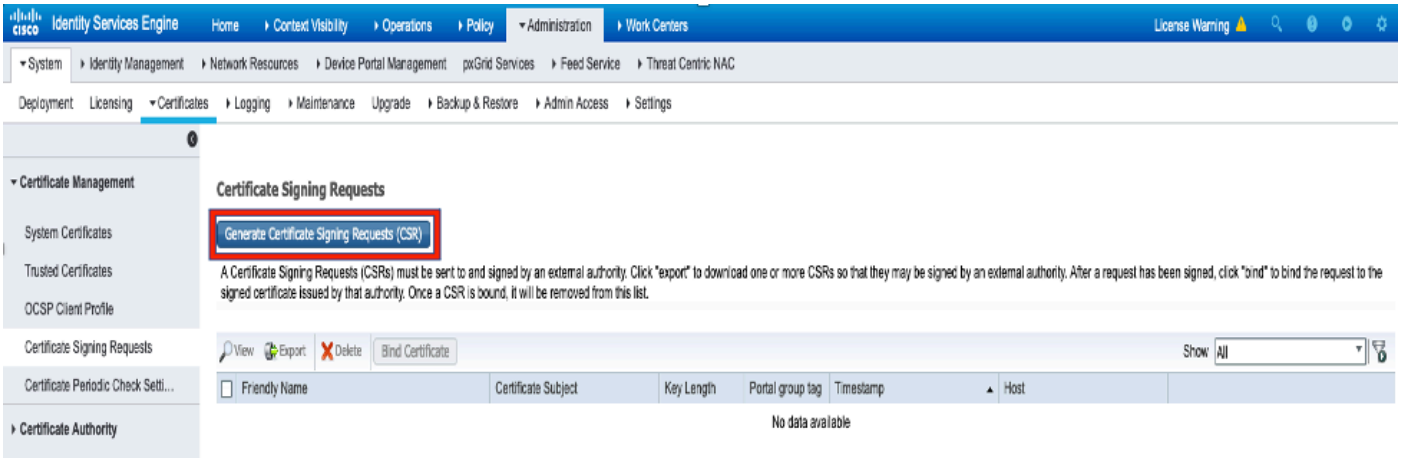


شهادة الثقة على ISE

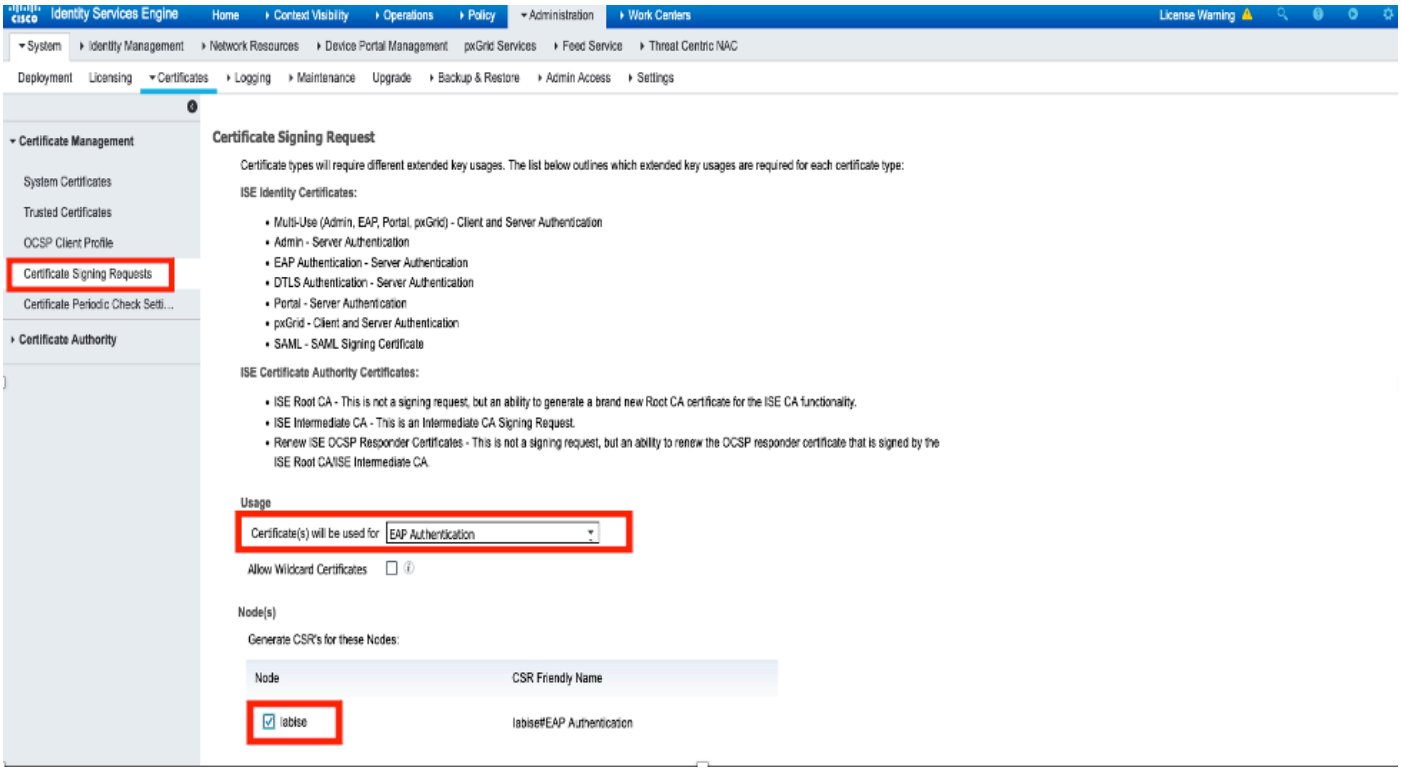
الخطوة 1. انتقل إلى **إدارة > نظام > شهادات > إدارة الشهادات > شهادات موثوق بها**.

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 نحن بحاجة إلى توليد CSR.

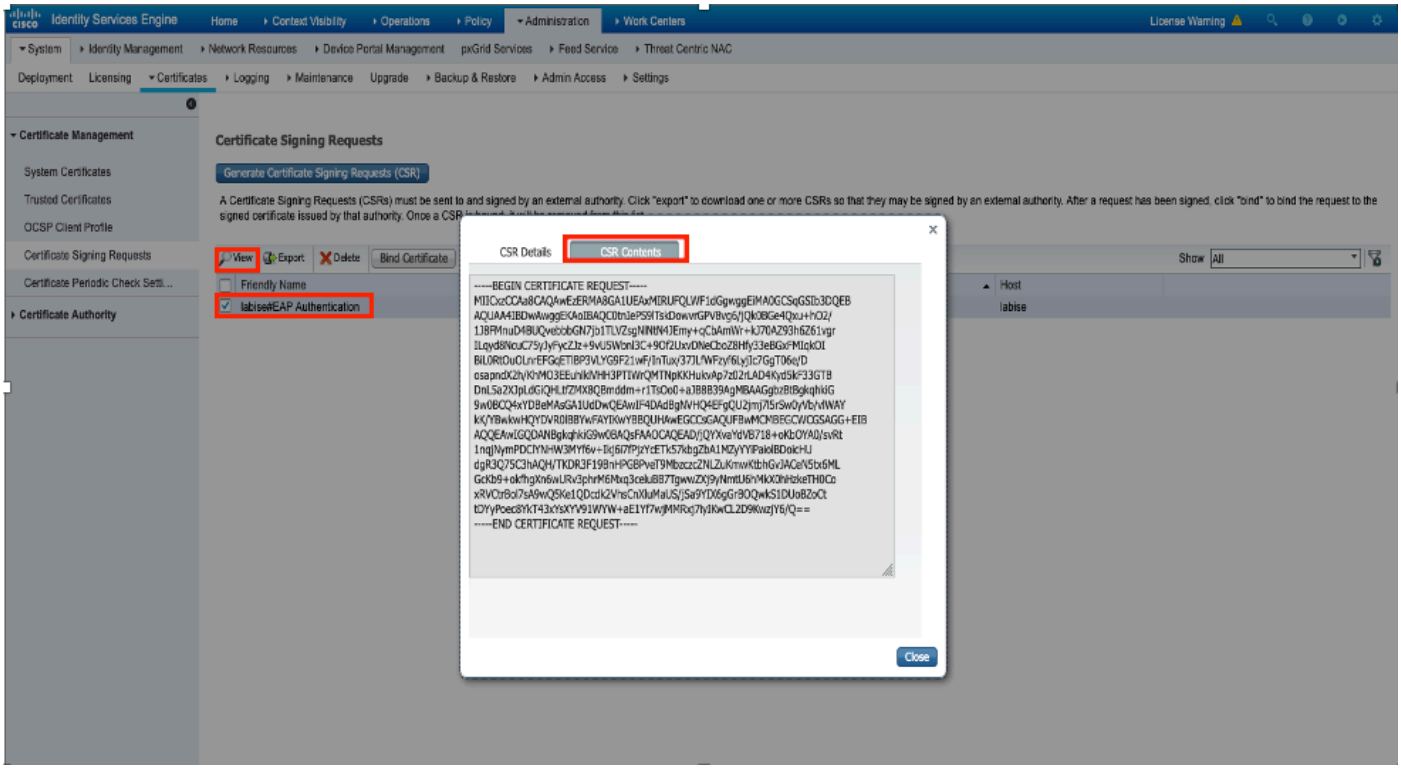
الخطوة 2. انتقل إلى **الإدارة > الشهادات > طلبات توقيع الشهادة > إنشاء طلبات توقيع الشهادة (CSR)** كما هو موضح في الصورة.



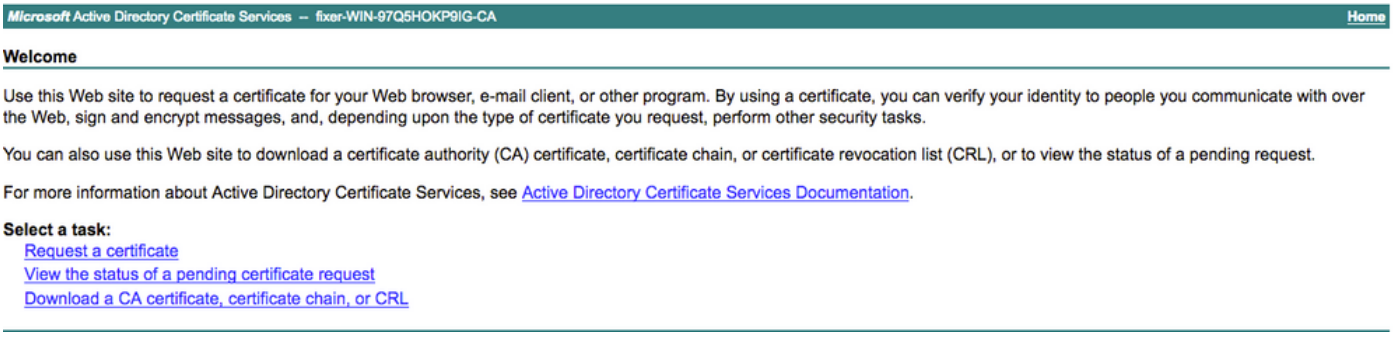
الخطوة 3. لإنشاء CSR، انتقل إلى **الاستخدام** ومن **الشهادة (الشهادات) يتم إستخدامها** للخيارات المنسدلة حدد **مصادقة EAP** كما هو موضح في الصورة.



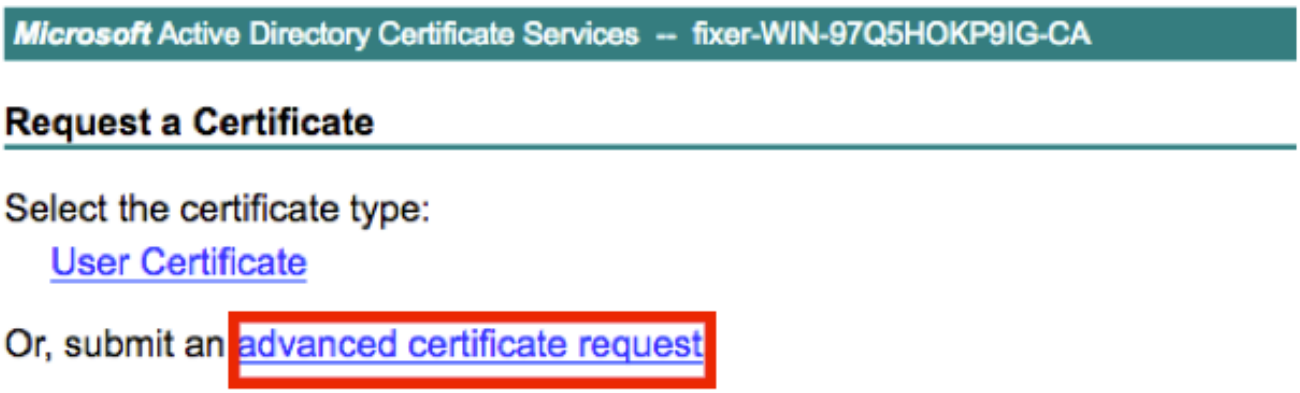
الخطوة 4. يمكن عرض CSR الذي تم إنشاؤه على ISE. انقر فوق **عرض** كما هو موضح في الصورة.



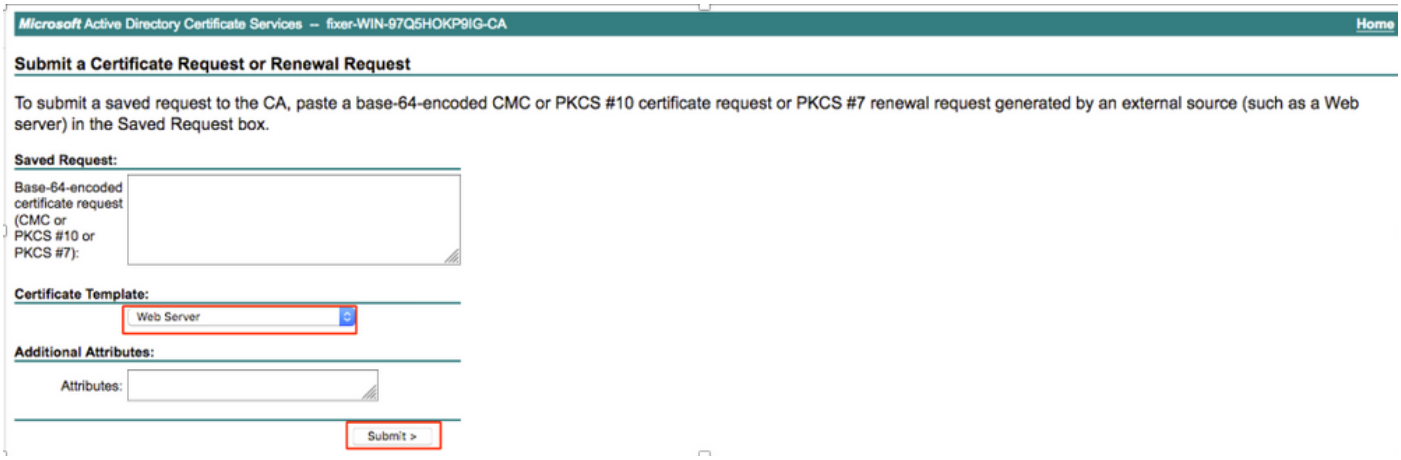
الخطوة 5. بمجرد إنشاء CSR، تصفح إلى خادم CA وانقر فوق **طلب شهادة** كما هو موضح في الصورة:



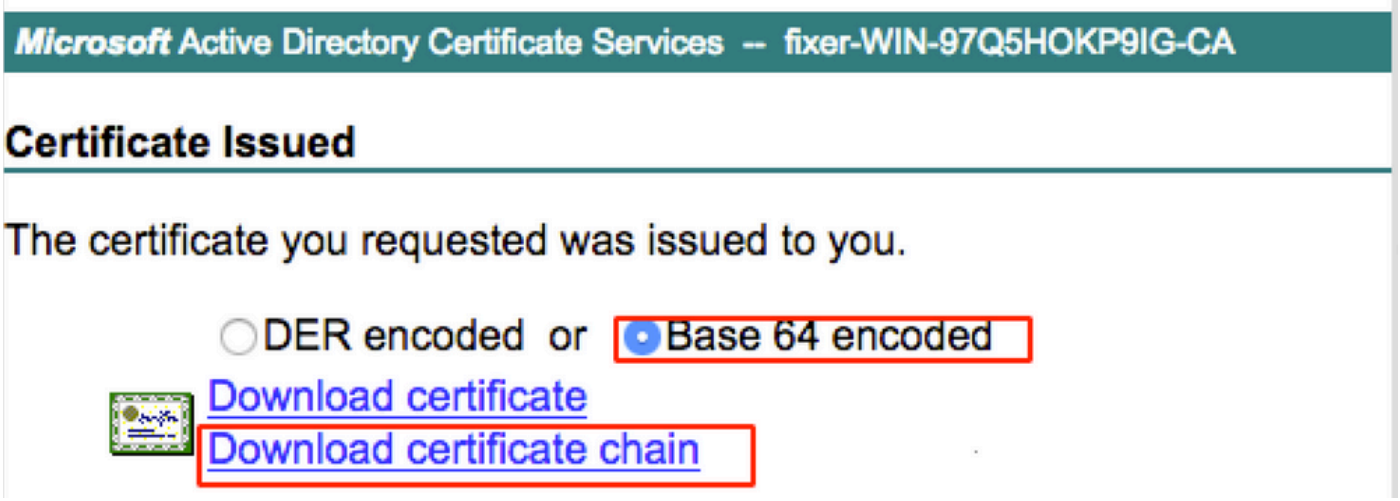
الخطوة 6. بمجرد أن تطلب شهادة، تحصل على خيارات **لشهادة المستخدم وطلب شهادة متقدم**، انقر على **طلب شهادة متقدم** كما هو موضح في الصورة.



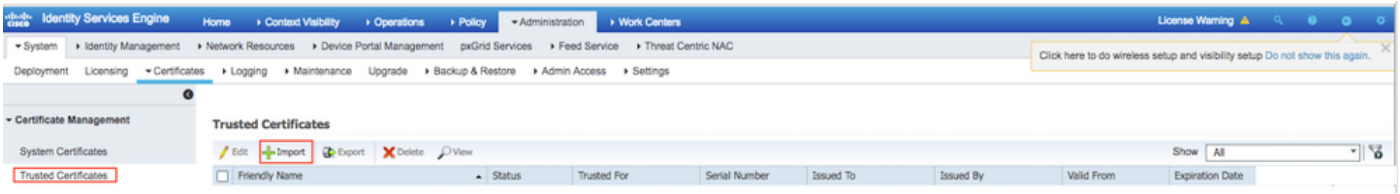
الخطوة 7. الصق CSR الذي تم إنشاؤه في **طلب الشهادة المرمزة ل Base-64**. من **قالب الشهادة:** خيار القائمة المنسدلة، أختر **خادم الويب** وانقر فوق **إرسال** كما هو موضح في الصورة.

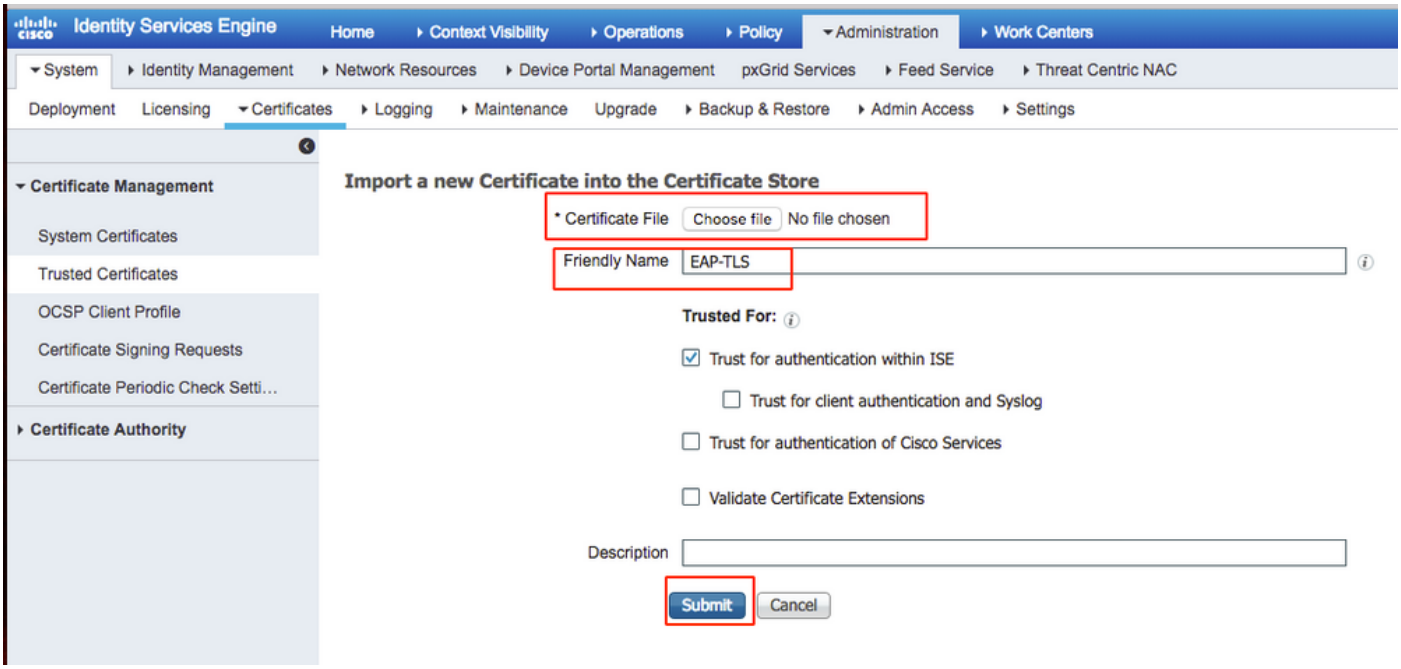


الخطوة 8. بمجرد النقر فوق **إرسال**، تحصل على الخيار لتحديد نوع الشهادة، حدد **Base-64 المشفر** وانقر فوق **سلسلة تنزيل الشهادة** كما هو موضح في الصورة.

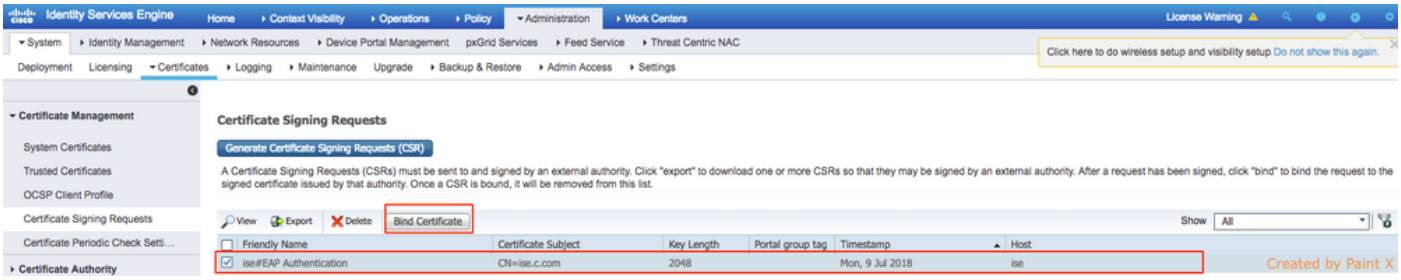


الخطوة 9. اكتمل تنزيل الشهادة لخادم ISE. يمكنك إستخراج الشهادة، وتحتوي الشهادة على شهادتين، شهادة جذر واحدة وأخرى وسيطة. يمكن إستيراد الشهادة الجذر تحت **إدارة > شهادات > شهادات موثوق بها > إستيراد** كما هو موضح في الصور.

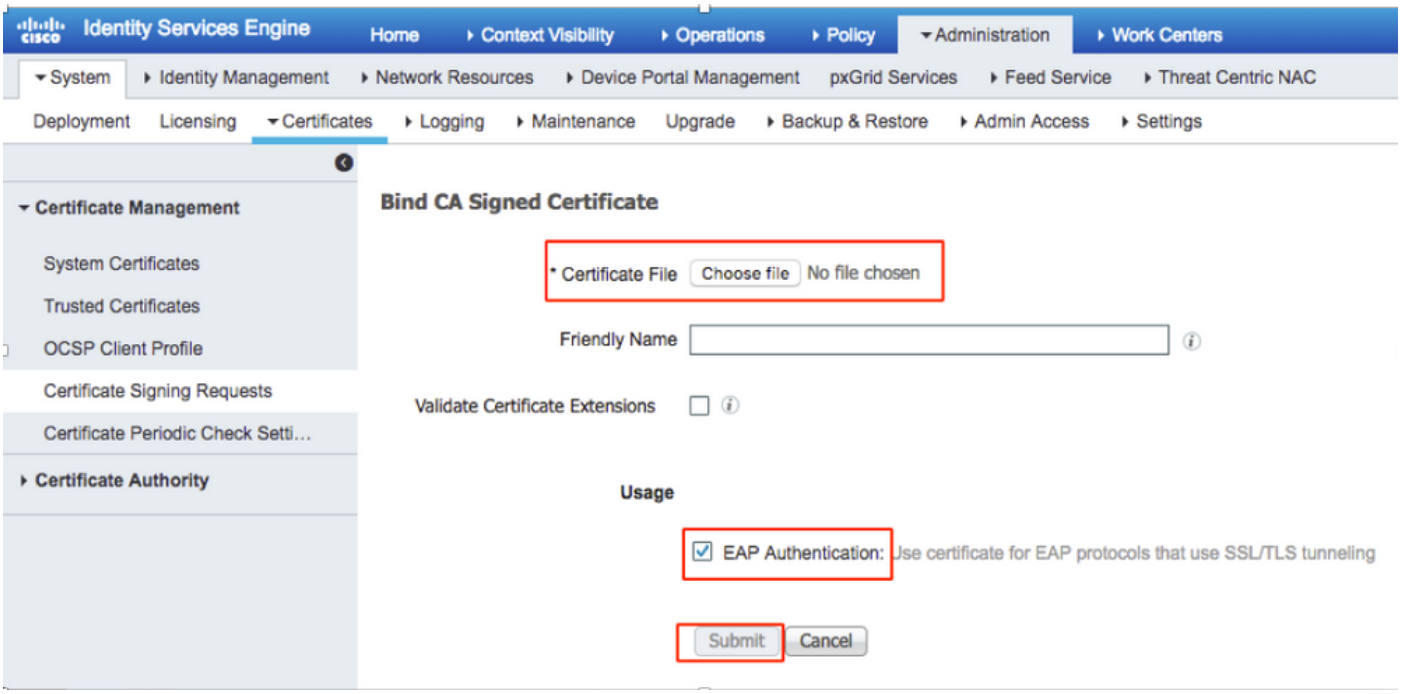




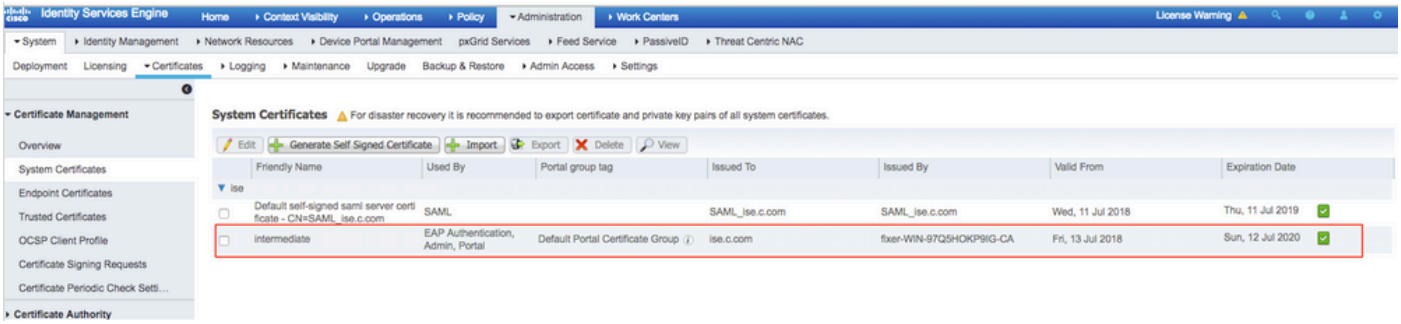
الخطوة 10. بمجرد النقر فوق **إرسال**، تتم إضافة الشهادة إلى قائمة الشهادات الموثوق بها. أيضا، يلزم الشهادة الوسيطة للربط مع CSR كما هو موضح في الصورة.



الخطوة 11. بمجرد النقر على **تربط الربط**، هناك خيار لاختيار ملف التربط 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.



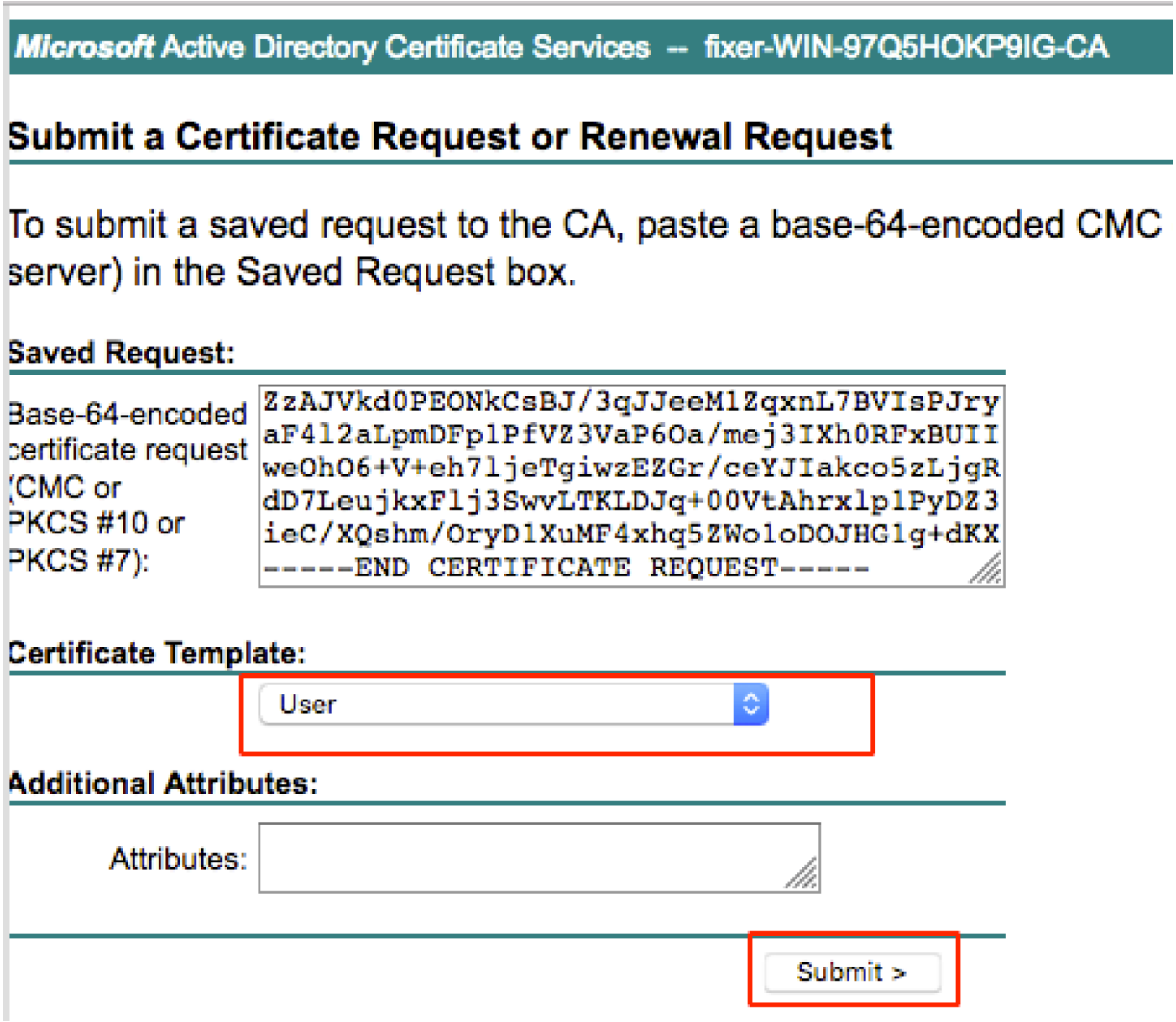
عميل EAP-TLS

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 الخطوات التالية 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. **حساب SelectComputer**.
5. تحديد **كمبيوتر محلي>إنهاء**
6. طقطقة **ok** in order to خرجت الأداة الإضافية نافذة.
7. انقر فوق **[+]** بجوار **الشهادات > شخصي > الشهادات**.
8. انقر بزر الماوس الأيمن على **الشهادات** وحدد **كل المهام > إستيراد**.
9. انقر فوق **Next (التالي)**.
10. انقر على **إستعراض**.
11. حدد **.cer** أو **.crt** أو **.pfx** الذي تريد إستيراده.

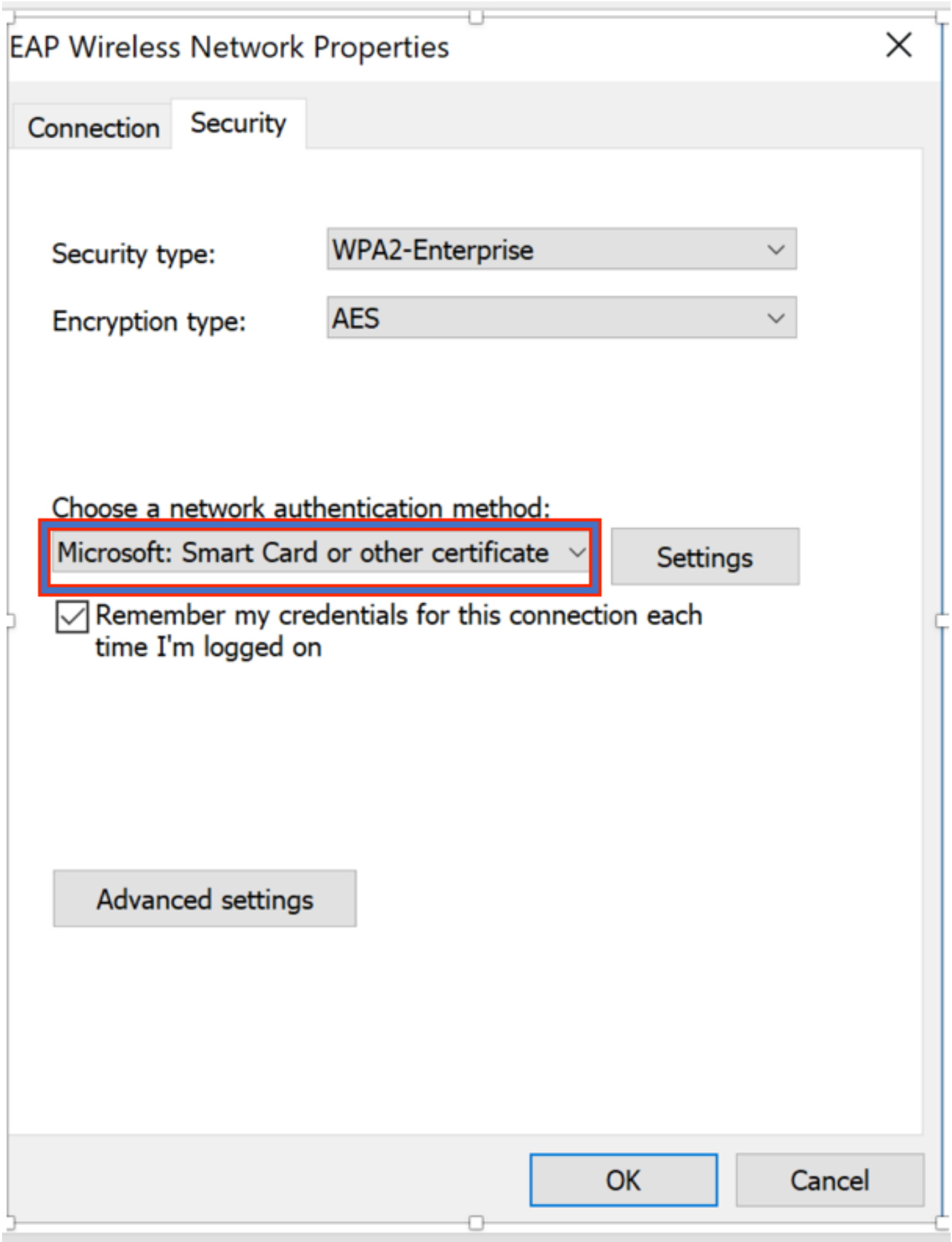
12. انقر فوق **فتح**.
13. انقر فوق **Next (التالي)**.
14. حدد **تحديد مخزن الشهادات تلقائيا بناء على نوع الشهادة**.
15. طقطقة **إنجاز و ok**

ام إن يتم إستيراد الشهادة، يلزمك تكوين عميل السلكي (سطح مكتب Windows في هذا المثال) من أجل EAP-TLS.

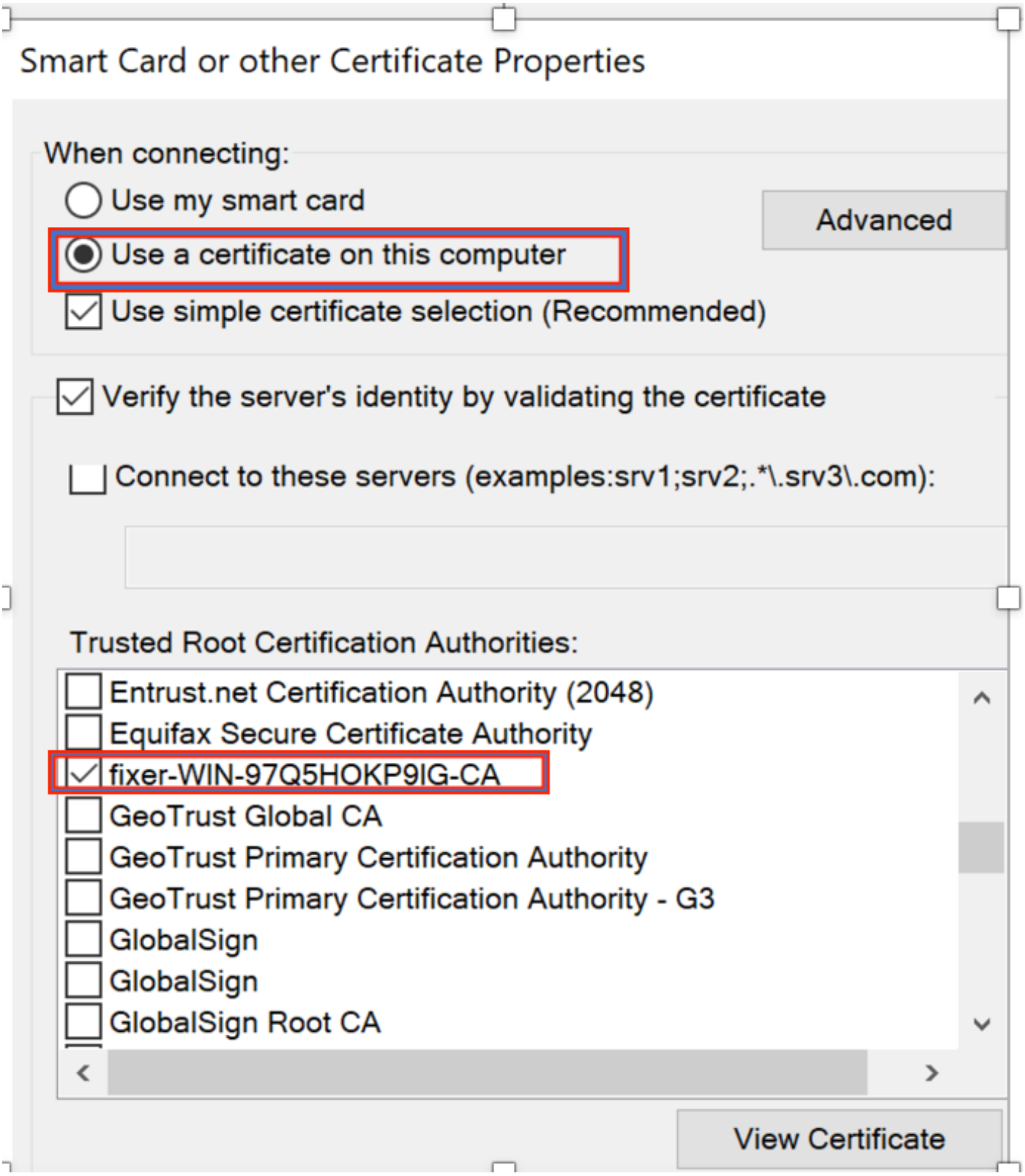
توصيف السلكي ل EAP-TLS

الخطوة 1. قم بتغيير التوصيف السلكي الذي تم إنشاؤه سابقا لبروتوكول المصادقة المتوسع المحمي (PEAP) استخدام EAP-TLS بدل من ذلك. انقر على **توصيف EAP السلكي**.

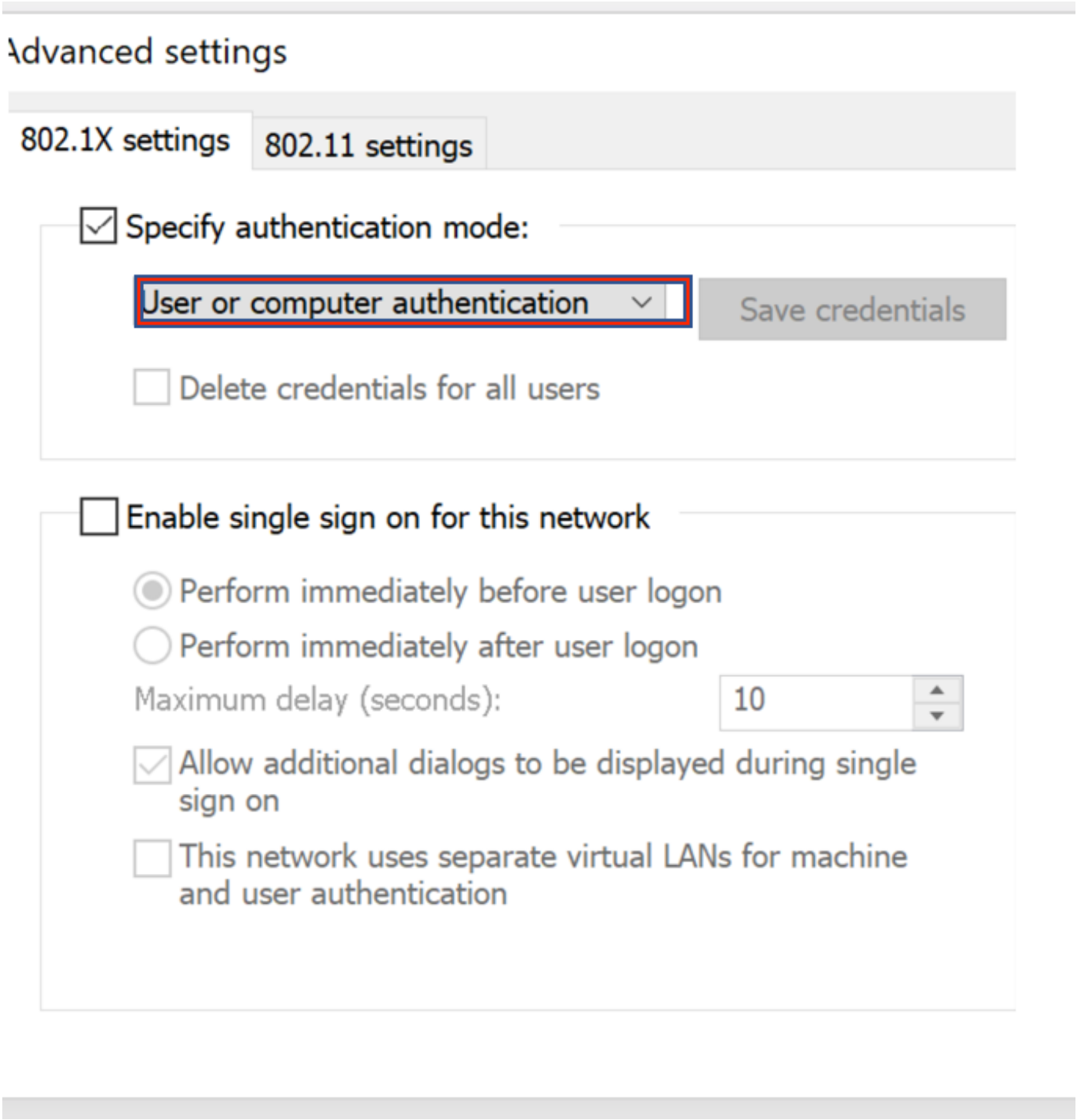
الخطوة 2. حدد **Microsoft: البطاقة الذكية أو أي شهادة أخرى** وانقر على **موافق** من عرض في الصورة.



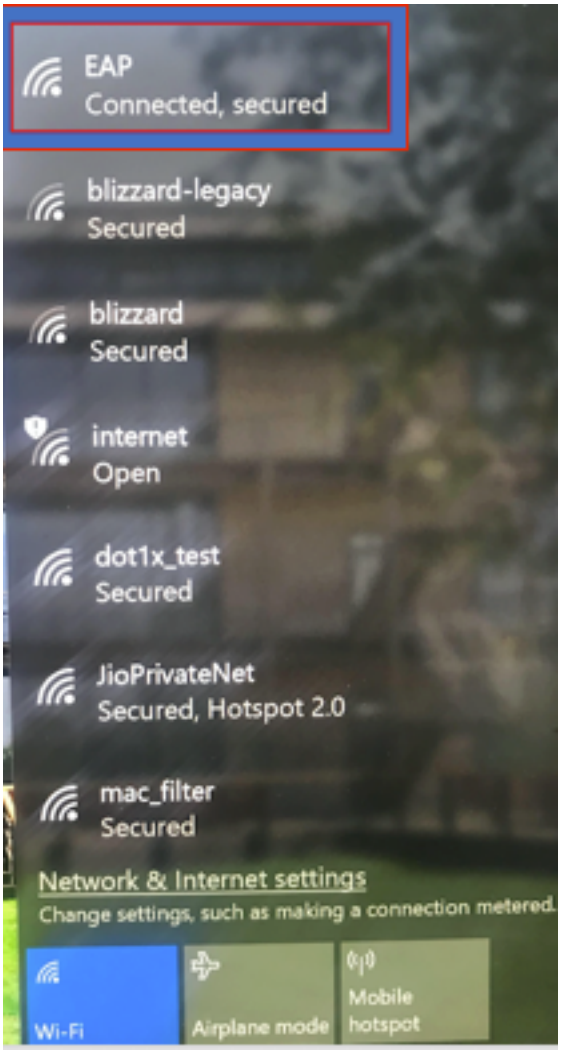
الخطوة 3. انقر على **الإعدادات** وحدد الشهادة الجذر الصادرة من خادم المرجع المصدق كما هو موضح في الصورة.



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



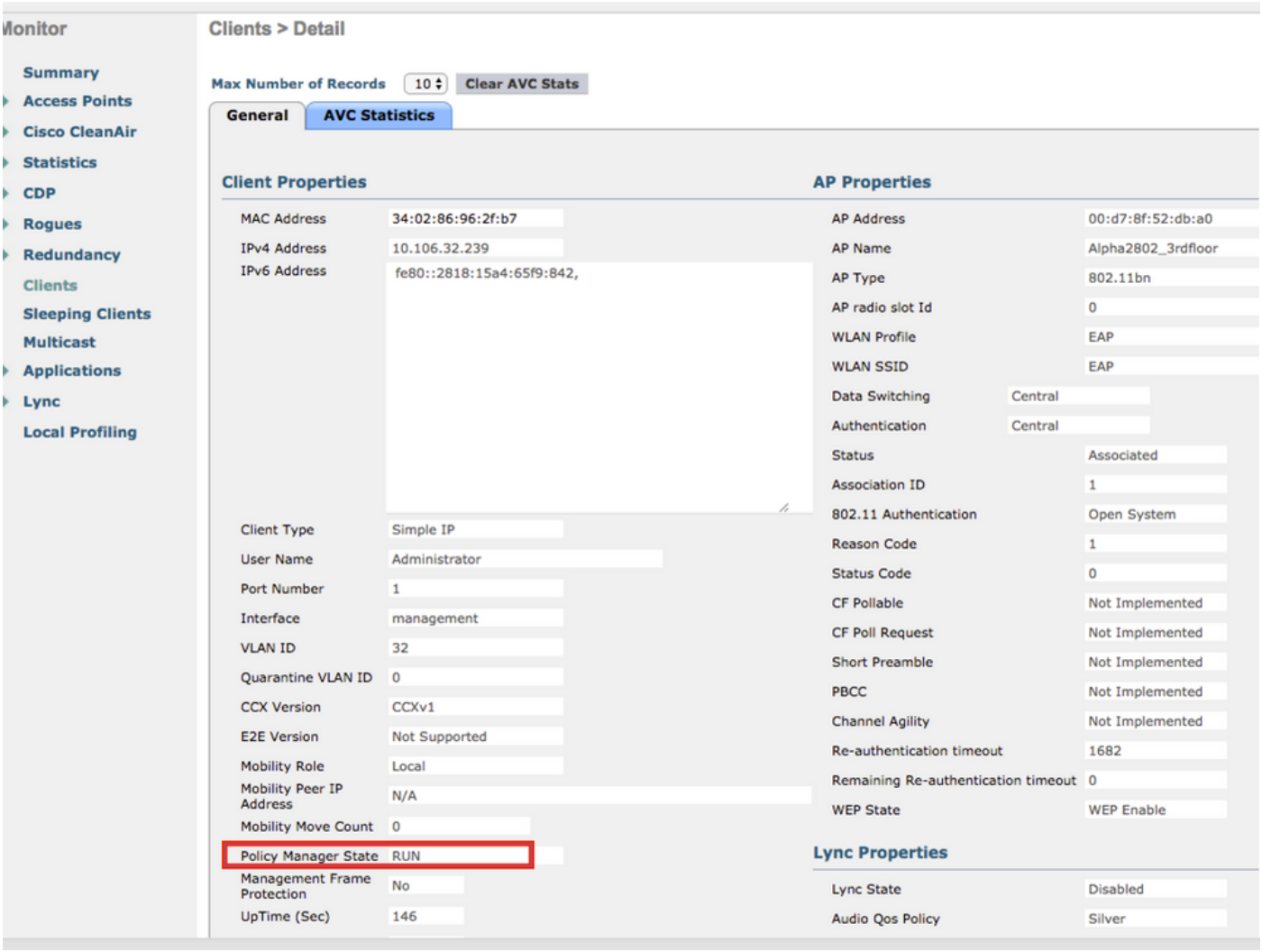
الخطوة 5. الآن حاول التوصيل مرة أخرى باللشبكة اللاسلكية ثم حدد التوصيف الصحيح (EAP في هذا المثال) ثم **توصيل**. أنت موصل باللشبكة اللاسلكية كما هو موضح في الصورة.



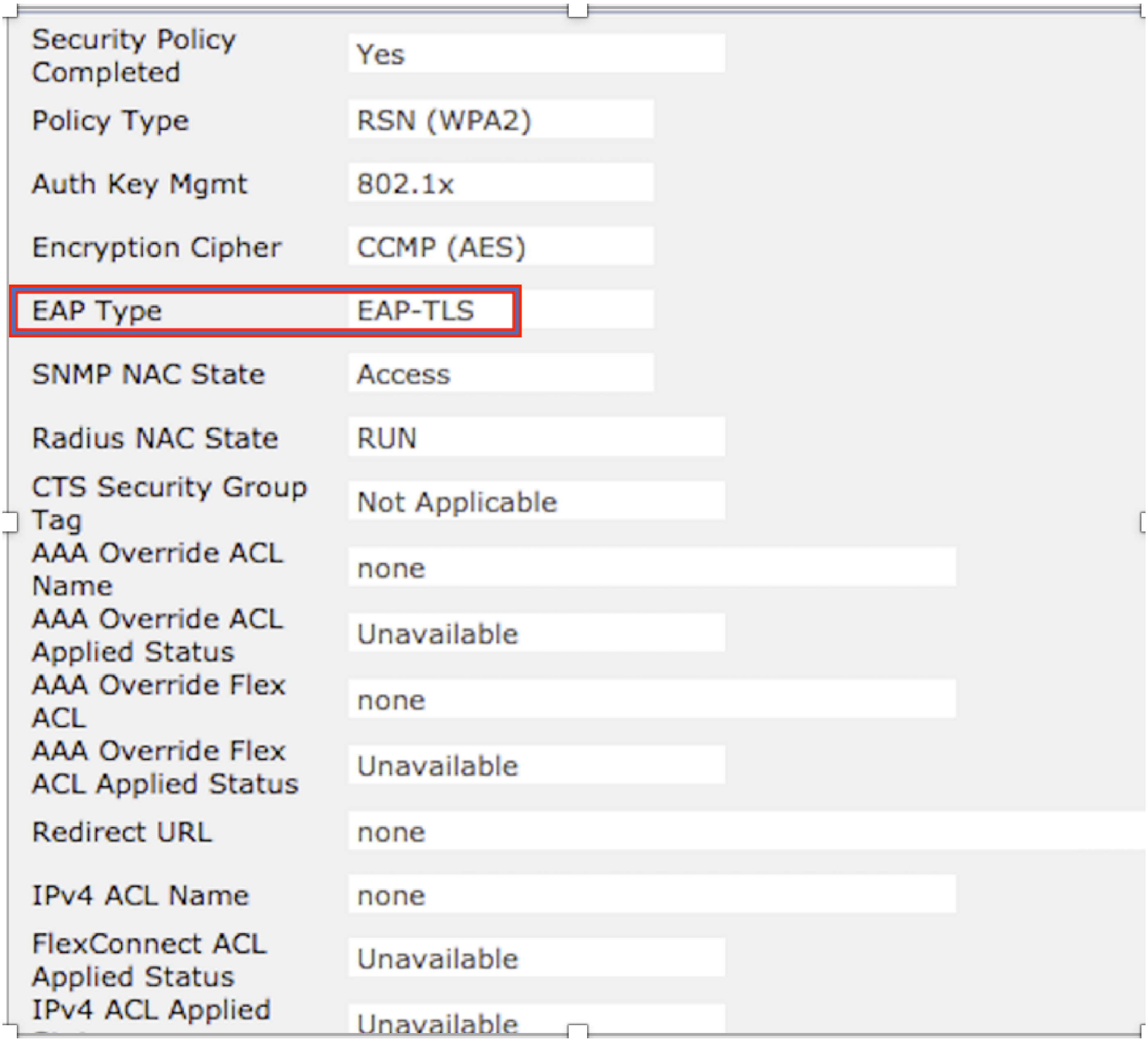
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الخطوة 1. يجب أن تظهر حالة مدير نهج العميل على أنها **RUN**. هذا يعني أن العميل قد أكمل المصادقة وحصل على عنوان IP وهو جاهز لتمرير حركة المرور الموضحة في الصورة.



الخطوة 2. تحقق أيضا من صحة أسلوب EAP على WLC في صفحة تفاصيل العميل كما هو موضح في الصورة.

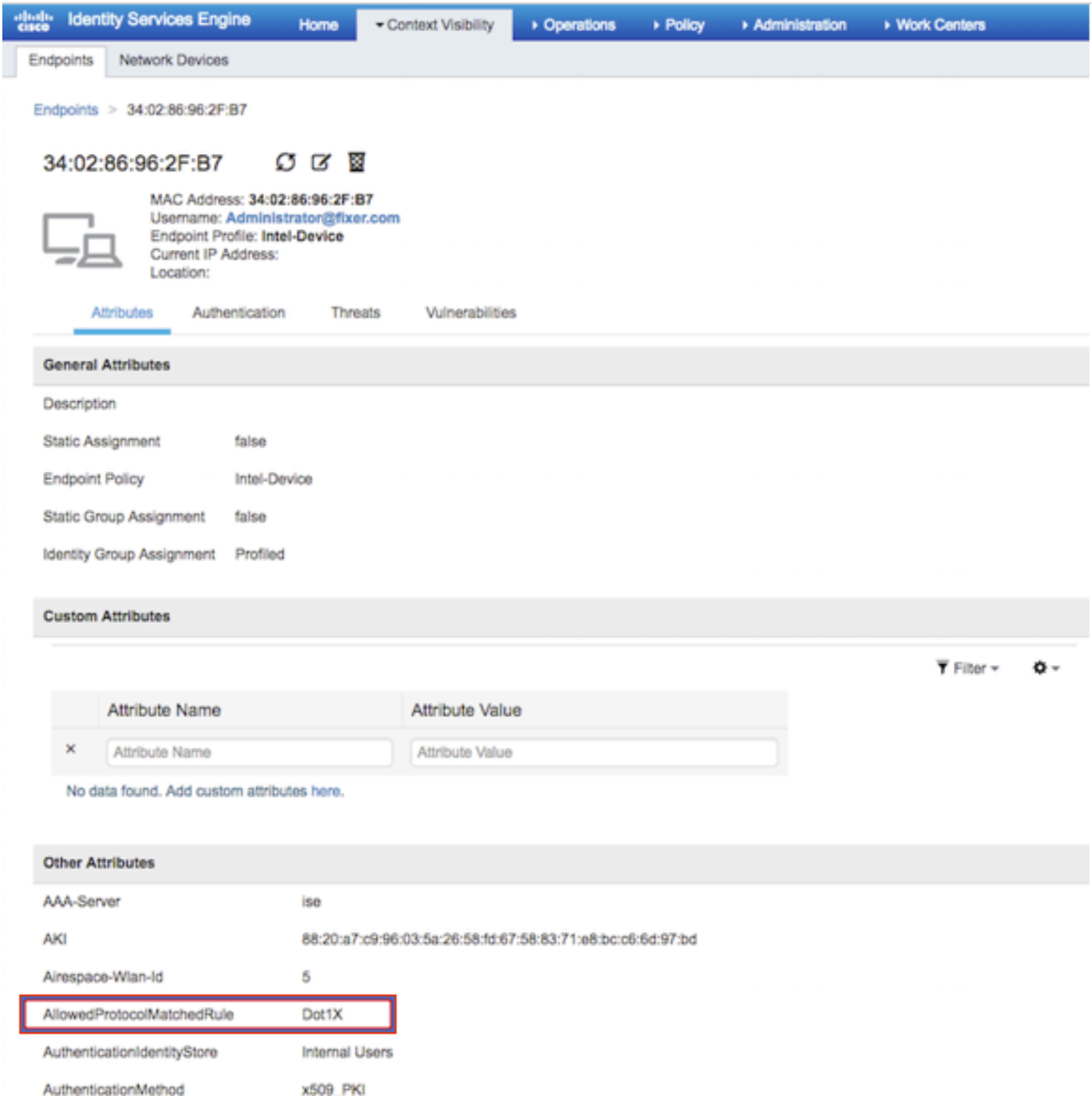


الخطوة 3. فيما يلي تفاصيل العميل من واجهة سطر الأوامر (CLI) لوحدة التحكم (تم قص الإخراج):

```
(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
```

الخطوة 4. على ISE، انتقل إلى **إمكانية رؤية السياق > نقاط النهاية > السمات** كما هو موضح في الصور.



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

استكشاف الأخطاء وإصلاحها

هناك حاليا ما من معلومة محددة يتوفر أن يتحرى ل هذا تشكيل.

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).