802.1x WLAN + زواج VLAN مع Mobility Express (ME) 8.2 و ISE 2.1

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

الرسم التخطيطي للشبكة

التكوينات

التكوين على

أعلني على ISE

إنشاء مستخدم جديد على ISE

إنشاء قاعدة المصادقة

إنشاء قاعدة التخويل

تكوين الجدار الطرفي

التحقق من الصحة

عملية المصادقة في ME

عملية المصادقة على ISE

المقدمة

يوضح هذا المستند كيفية إعداد شبكة WLAN (شبكة محلية السلكية) باستخدام أمان Wi-Fi Protected Access 2 (WPA2) على مستوى المؤسسة باستخدام وحدة تحكم Mobility Express وخادم خارجي لخدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS). يتم إستخدام محرك خدمة الهوية (ISE) كمثال على خوادم RADIUS الخارجية.

بروتوكول المصادقة المتوسع (EAP) المستخدم في هذا الدليل هو بروتوكول المصادقة المتوسع المحمي (PEAP). بالإضافة إلى أنه يتم تعيين العميل لشبكة VLAN معينة (بخلاف تلك المعينة للشبكة المحلية اللاسلكية (WLAN) بشكل افتراضي).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- 802,1x
- خوخ
- هيئة الشهادات (CA)
- الشهادات

المكونات المستخدمة

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

ME الإصدار 8.2

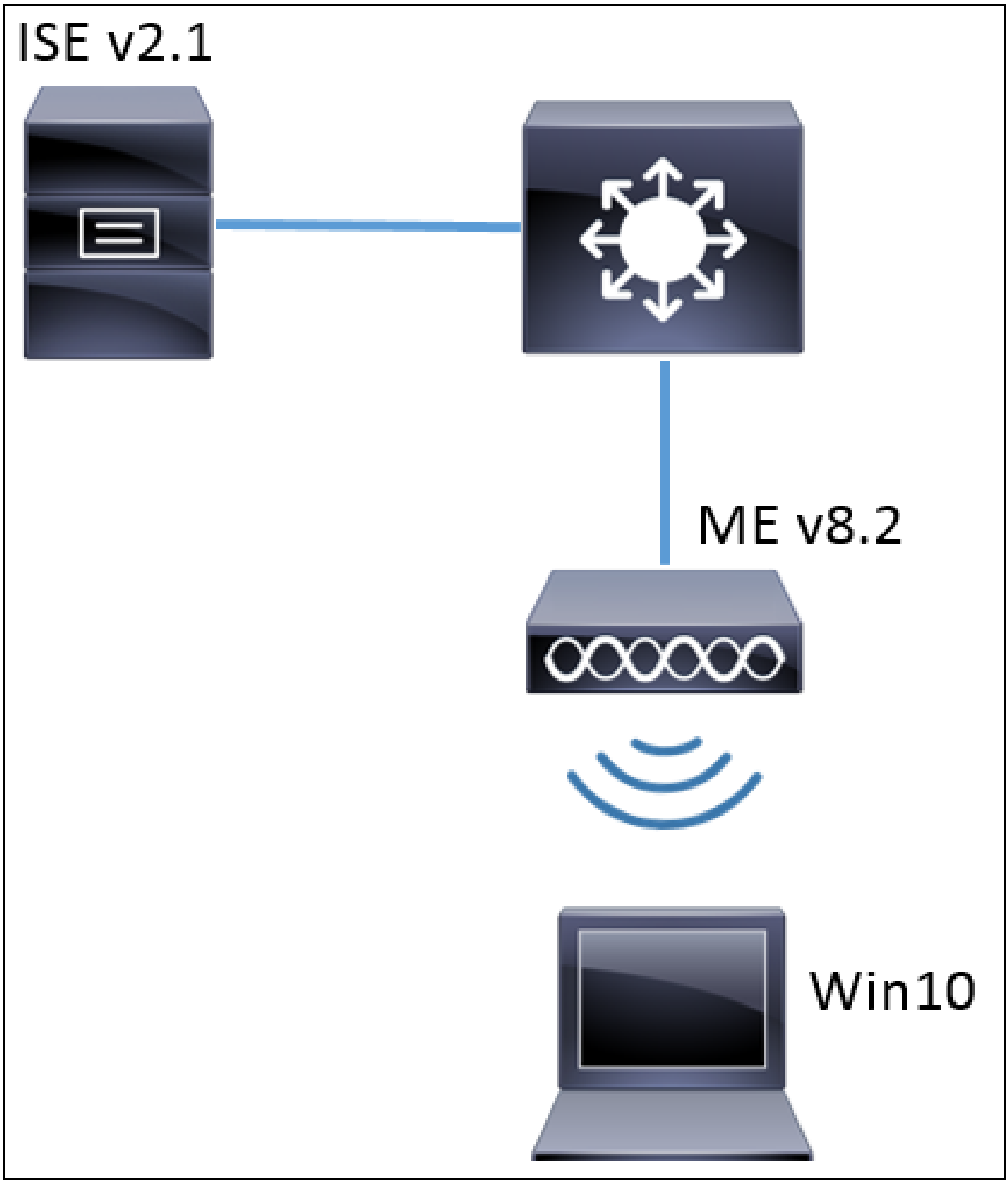
ISE الإصدار 2.1

الكمبيوتر المحمول طراز Windows 10

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

التكوين

الرسم التخطيطي للشبكة



التكوينات

والخطوات العامة هي:

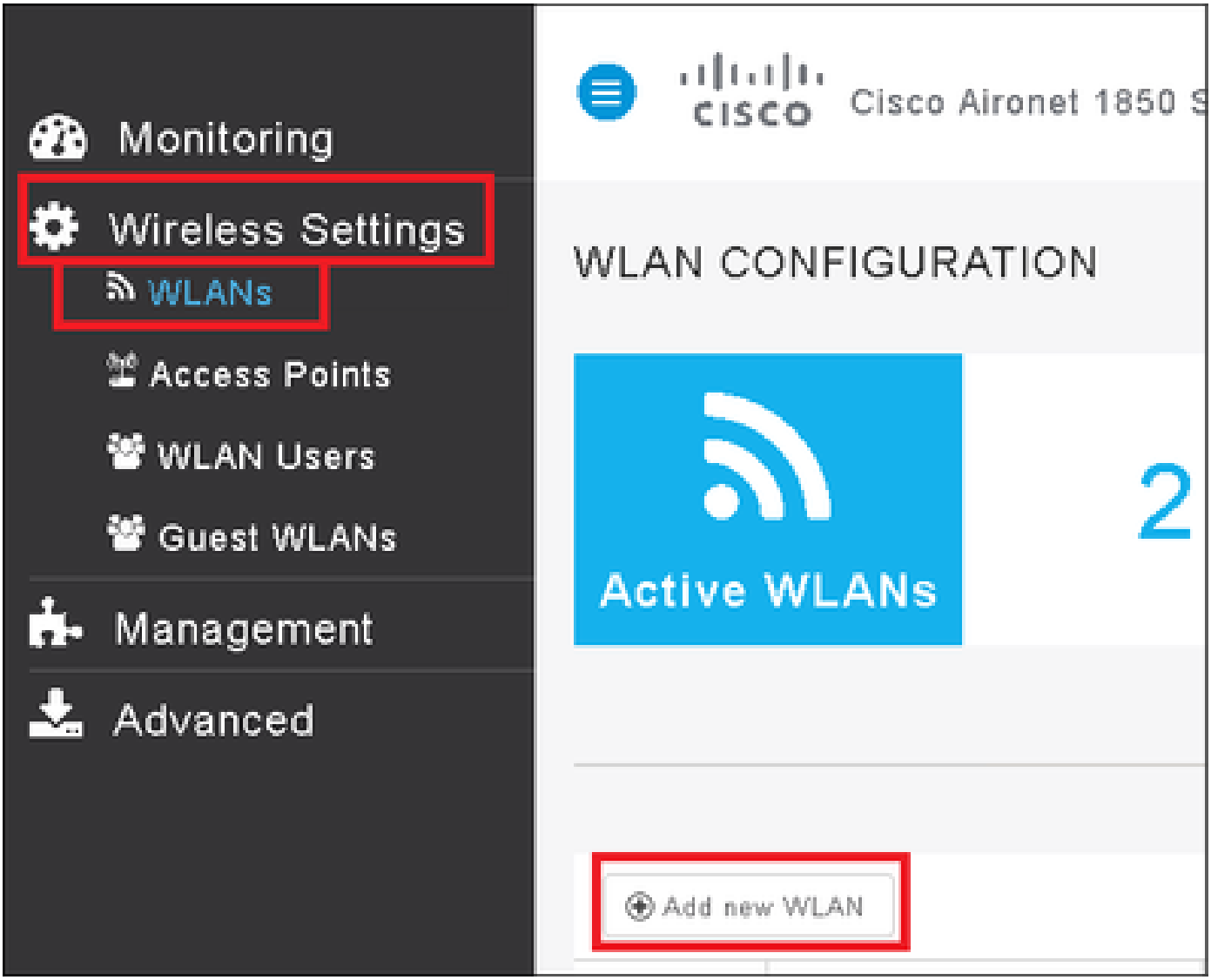
1. إنشاء معرف مجموعة الخدمة (SSID) في ME وإعلان خادم RADIUS (ISE في هذا المثال) على
2. الإعلان عن وجودي على خادم RADIUS (ISE)
3. إنشاء قاعدة المصادقة على ISE

4. إنشاء قاعدة التخويل على ISE
5. تكوين نقطة النهاية

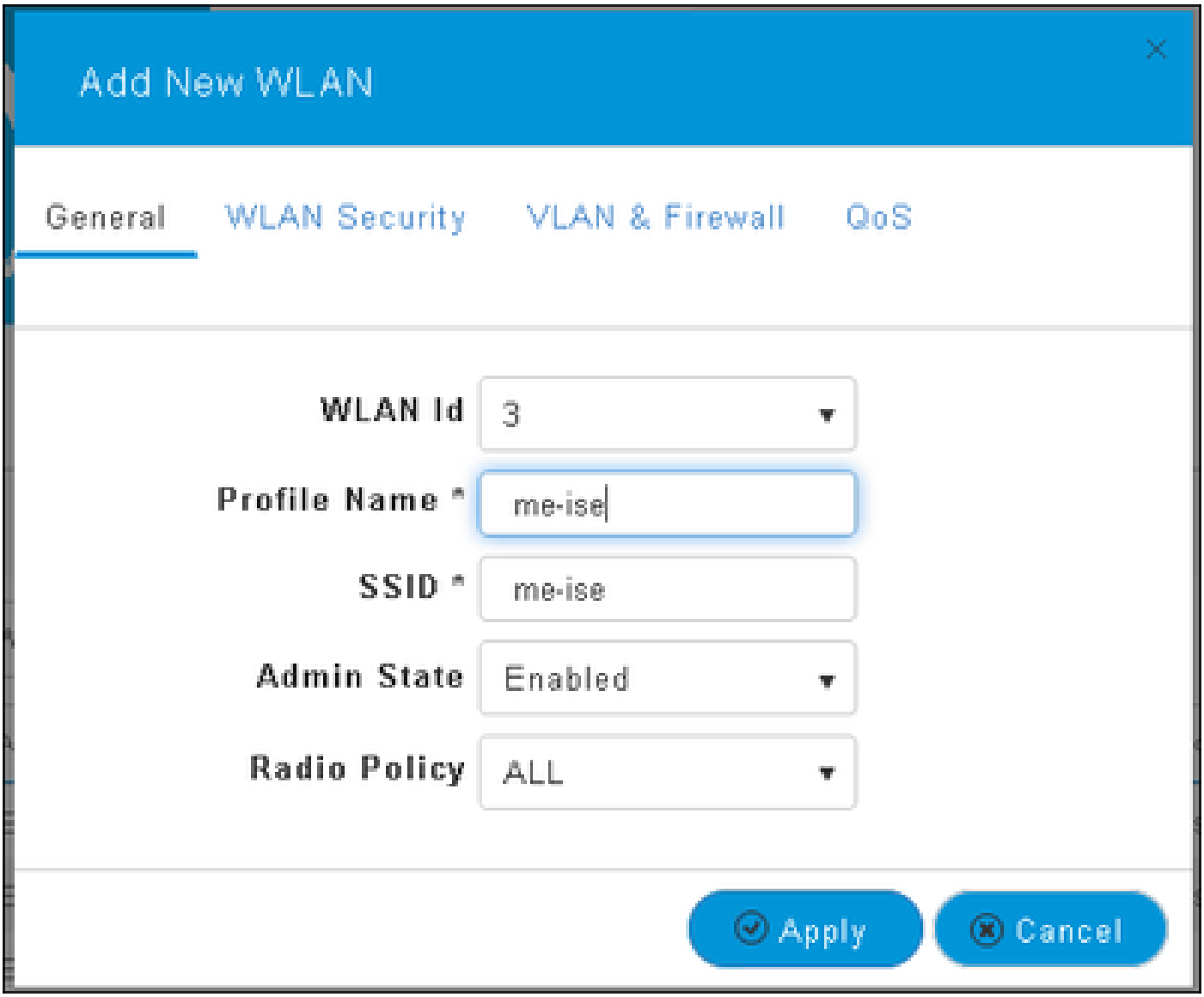
التكوين على

للسماح بالاتصال بين خادم RADIUS و ME، يلزم تسجيل خادم RADIUS على والعكس. توضح هذه الخطوة كيفية تسجيل خادم RADIUS على.

الخطوة 1. افتح واجهة المستخدم الرسومية الخاصة ب ME وانتقل إلى إعدادات لاسلكية > شبكات WLAN > إضافة شبكة WLAN جديدة.

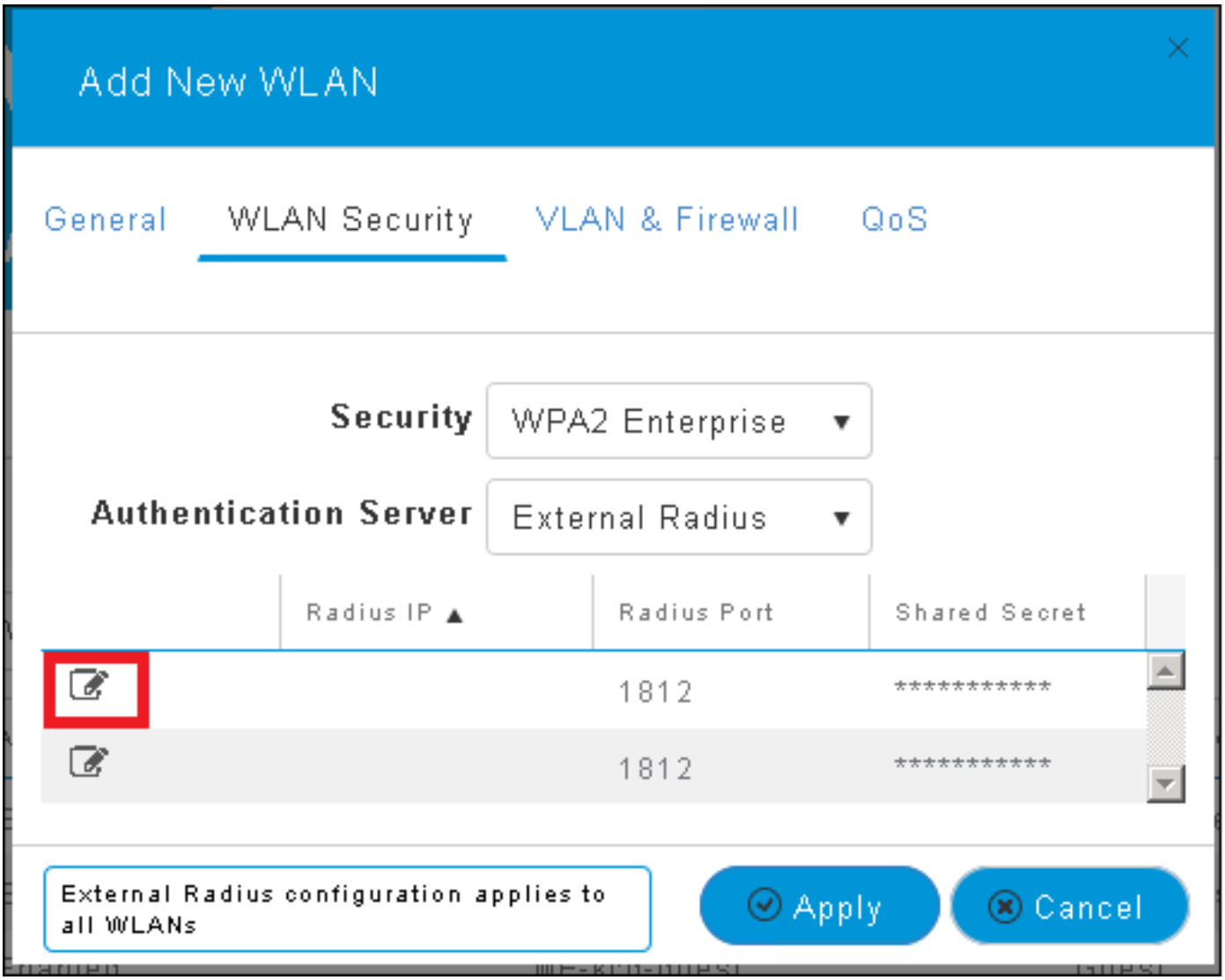


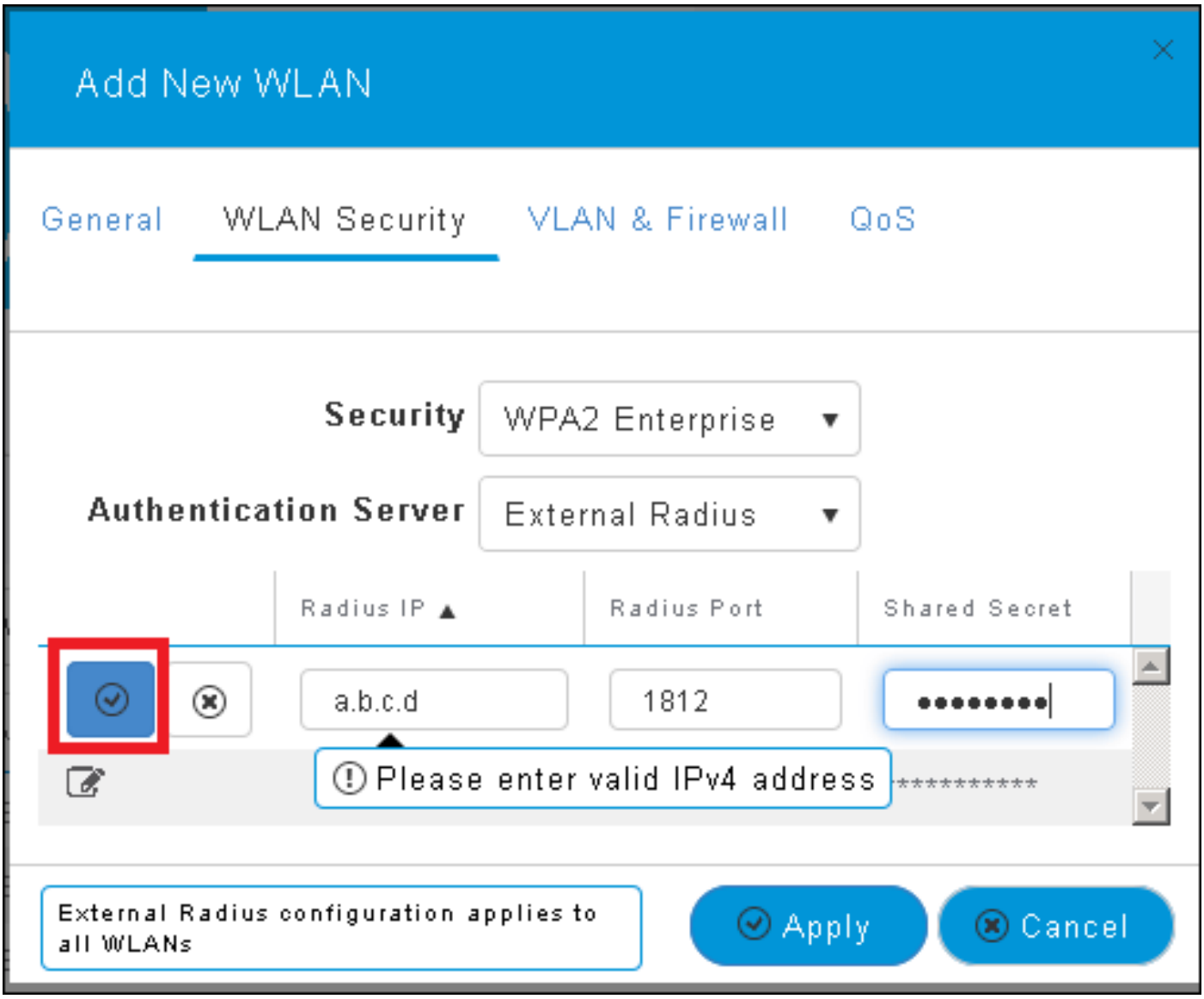
الخطوة 2. حدد اسما للشبكة المحلية اللاسلكية (WLAN).



الخطوة 3. حدد تكوين الأمان ضمن علامة تبويب أمان WLAN.

أختر WPA2 Enterprise، لاختيار خادم المصادقة RADIUS الخارجي. انقر فوق خيار التحرير لإضافة عنوان IP الخاص ب RADIUS وانتقاء مفتاح سري مشترك.


Add New WLAN
General
WLAN Security
VLAN & Firewall
QoS
Security
WPA2 Enterprise
Authentication Server
External Radius
Radius IP
Radius Port
Shared Secret
1812
****
1812
****
External Radius configuration applies to all WLANs
Apply
Cancel

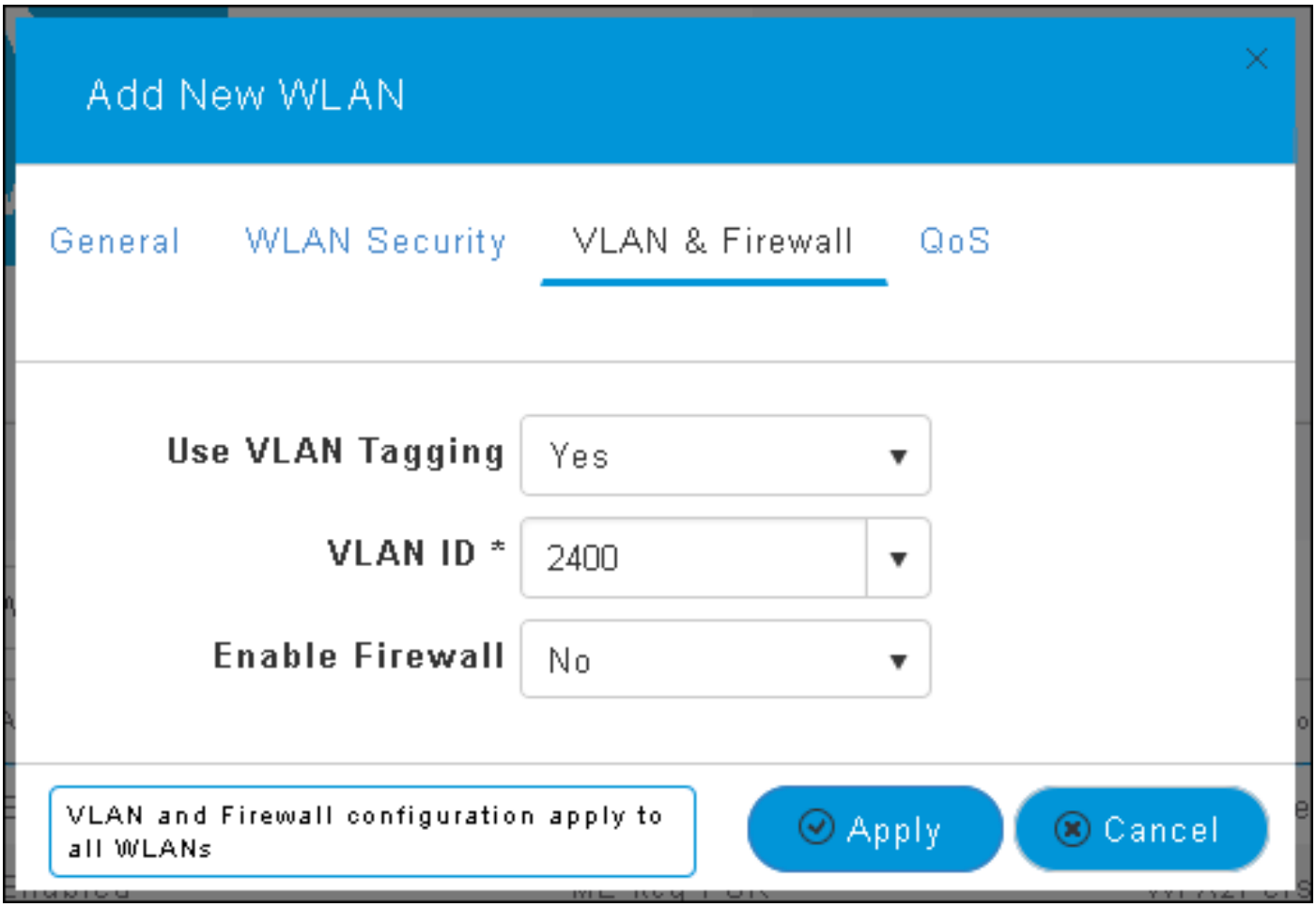


<a.b.c.d> يمثل خادم RADIUS.

الخطوة 4. قم بتخصيص شبكة VLAN لمعرف SSID.

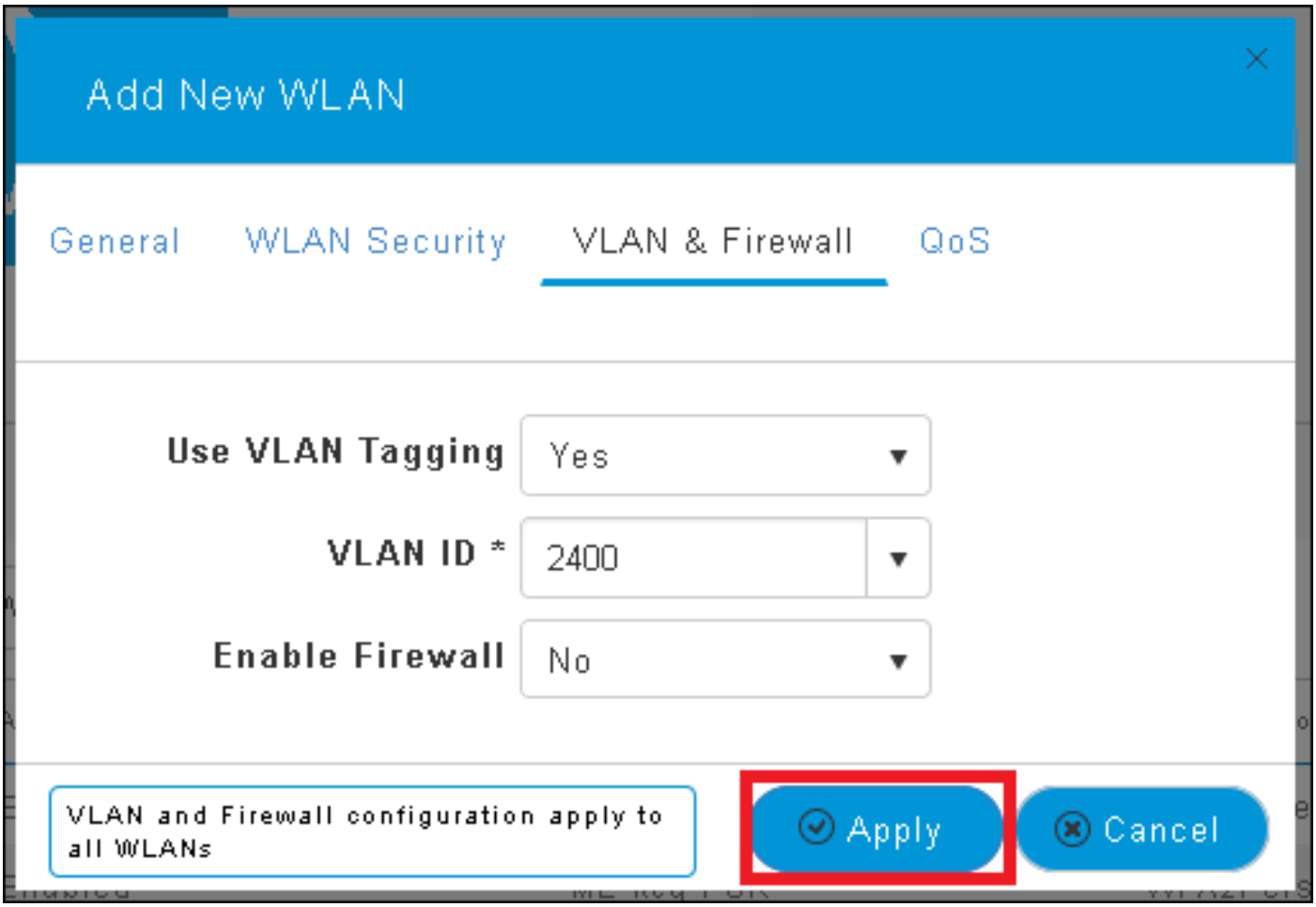
إذا كان يلزم تعيين SSID لشبكة VLAN الخاصة بنقطة الوصول، يمكن تجاوز هذه الخطوة.

لتخصيص المستخدمين لمعرف SSID هذا لشبكة VLAN معينة (بخلاف شبكة VLAN الخاصة بنقطة الوصول)، يمكنك إستخدام وضع علامات على شبكة VLAN وتخصيص معرف شبكة VLAN المرغوب.



ملاحظة: إذا تم إستخدام وضع علامات على الشبكة المحلية الظاهرية (VLAN)، فتأكد من تكوين switchport الذي يتم توصيل نقطة الوصول به كمنفذ خط اتصال ومن تكوين شبكة VLAN الخاصة بنقطة الوصول كشبكة أصلية.

الخطوة 5. انقر فوق تطبيق لإنهاء التكوين.



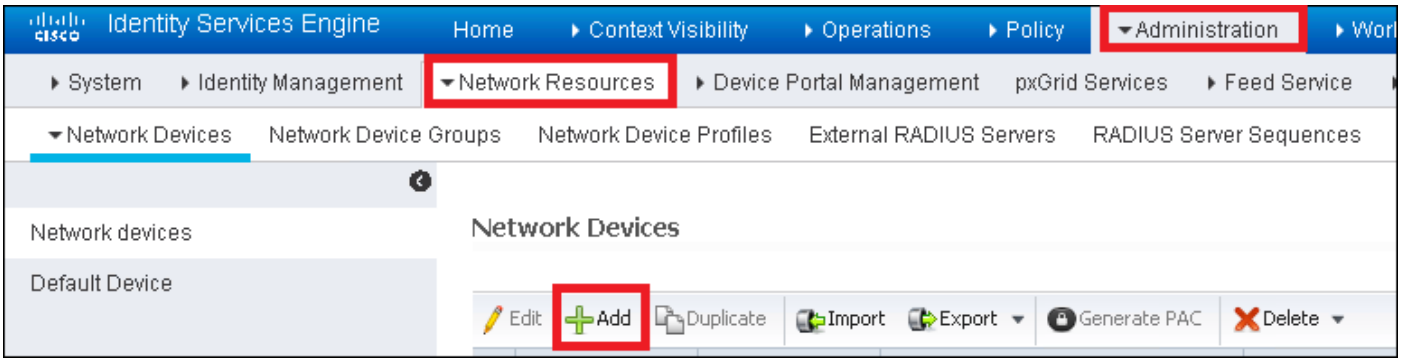
الخطوة 6. إختياري، قم بتكوين شبكة WLAN لقبول تجاوز شبكة VLAN.

قم بتمكين تجاوز AAA على شبكة WLAN وأضف شبكات VLAN المطلوبة. للقيام بذلك، سيتعين عليك فتح جلسة CLI إلى واجهة إدارة ME وإصدار الأوامر التالية:

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

أعلني على ISE

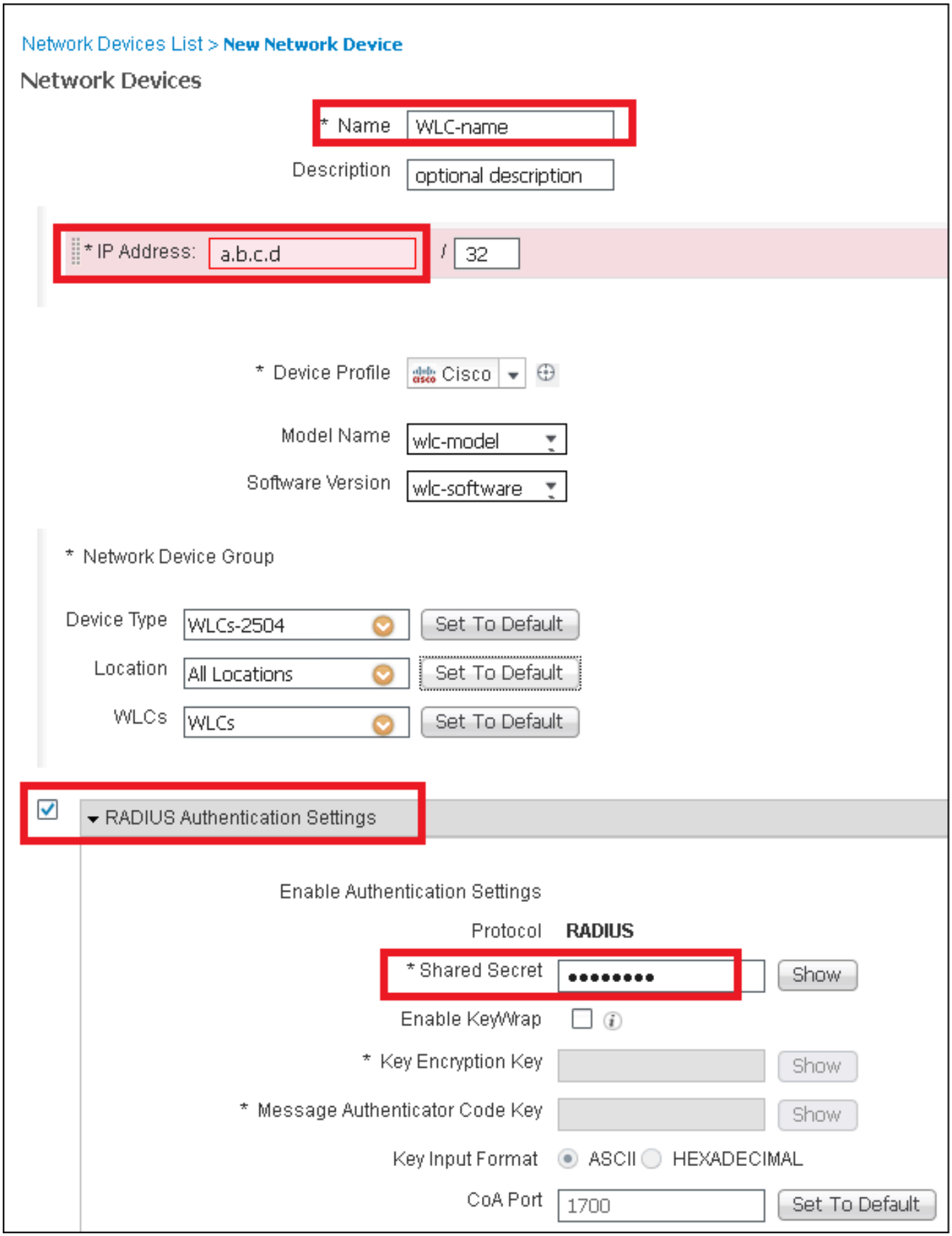
الخطوة 1. افتح وحدة تحكم ISE وانتقل إلى الإدارة > موارد الشبكة > أجهزة الشبكة > إضافة.



الخطوة 2. أدخل المعلومات.

وبشكل إختياري، يمكن تحديد اسم طراز أو إصدار برنامج أو وصف وتعيين مجموعات أجهزة شبكة الاتصال استنادا إلى أنواع الأجهزة أو الموقع أو أدوات التحكم في الشبكة المحلية اللاسلكية (WLC).

يتوافق a.b.c.d مع عنوان IP الخاص ب ME.

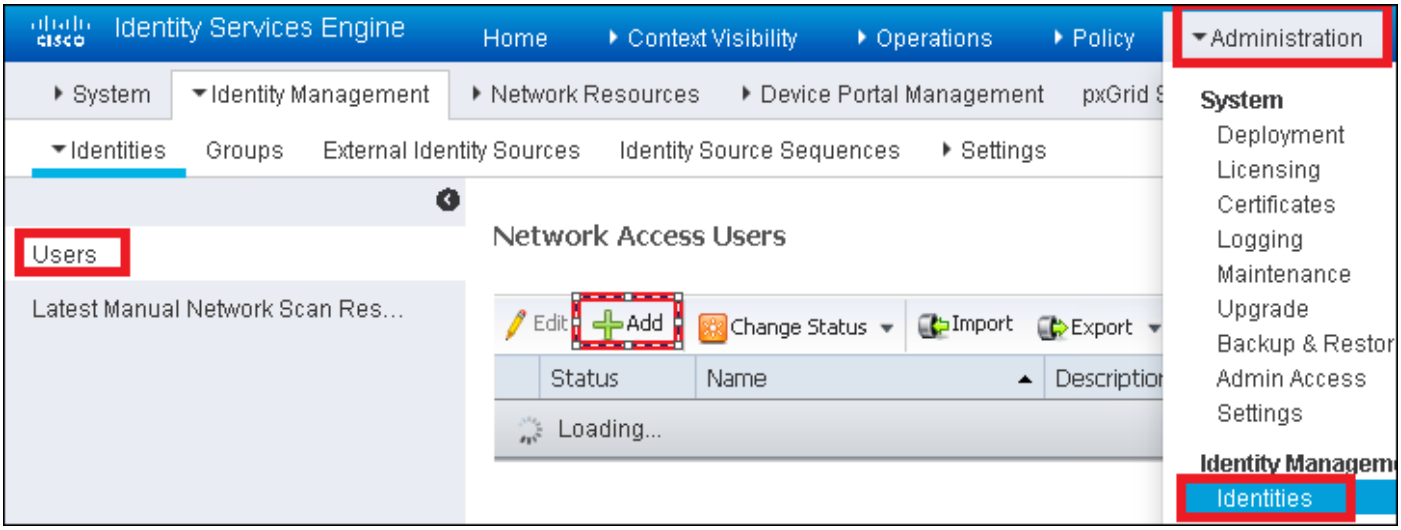


لمزيد من المعلومات حول مجموعات أجهزة الشبكة راجع هذا الارتباط:

[ISE - مجموعات أجهزة الشبكة]

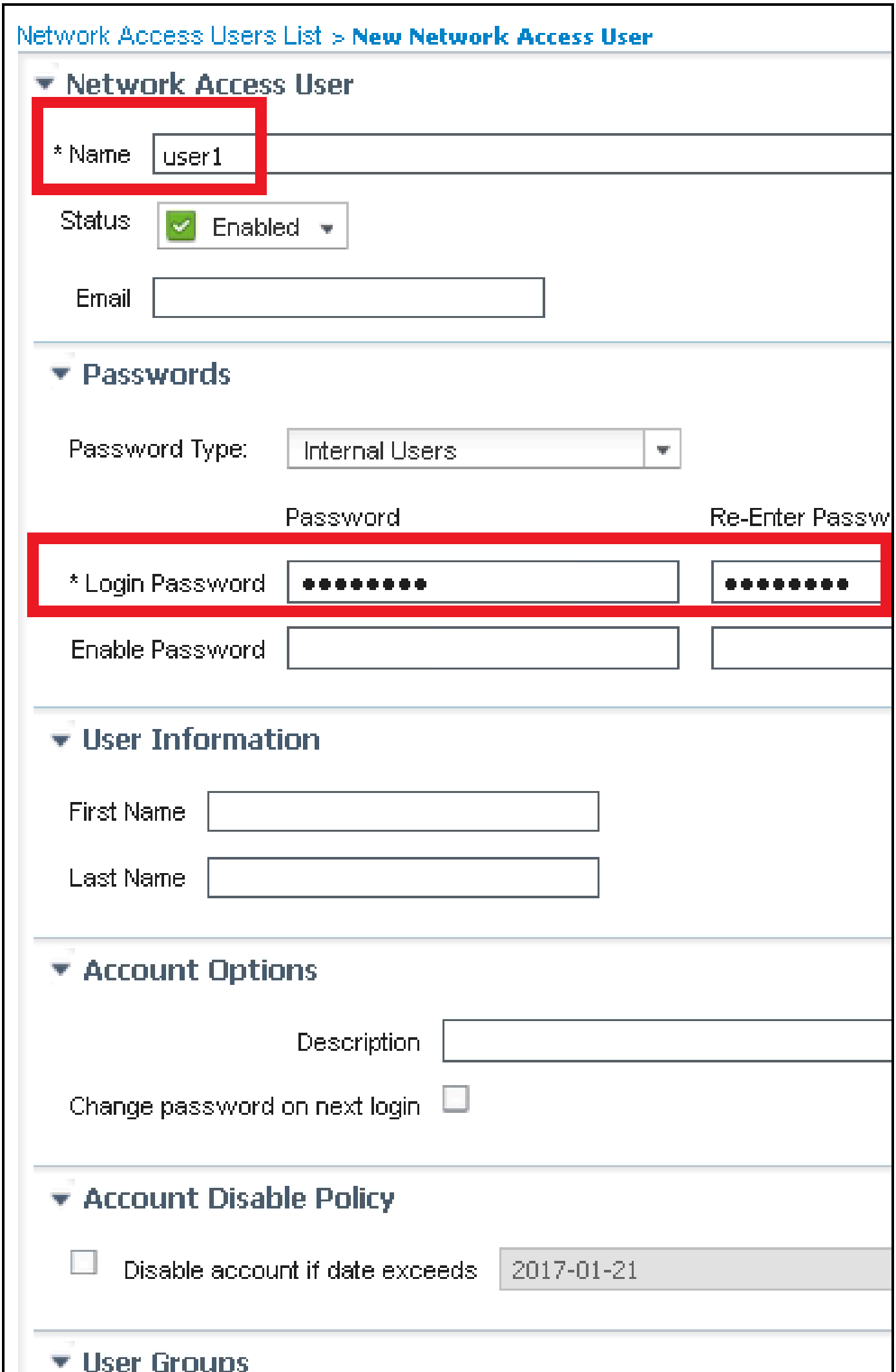
إنشاء مستخدم جديد على ISE

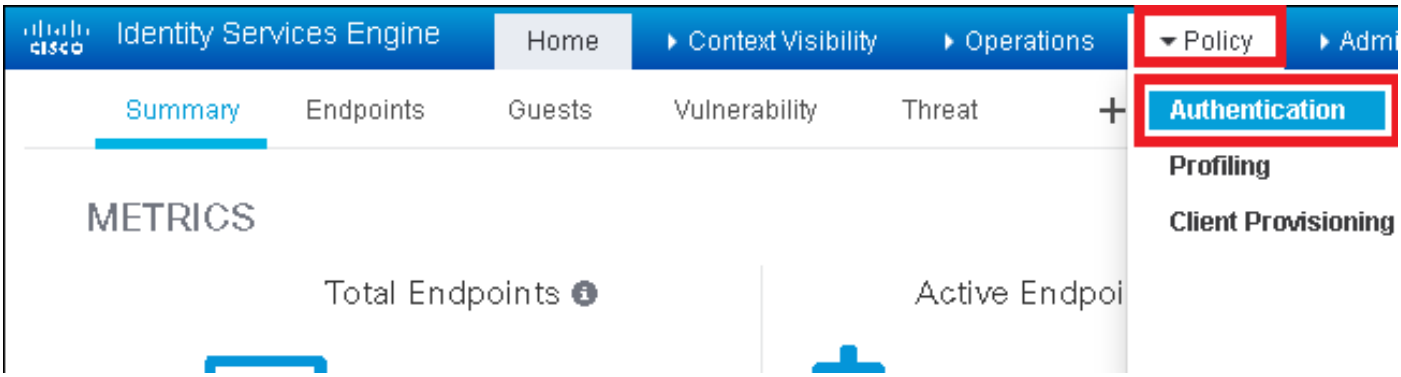
الخطوة 1. انتقل إلى الإدارة > إدارة الهوية > الهويات > المستخدمين > إضافة.



الخطوة 2. أدخل المعلومات.

في هذا المثال، ينتمي هذا المستخدم إلى مجموعة تسمى all_accounts ولكن يمكن تعديلها حسب الحاجة.


Network Access Users List > New Network Access User
Network Access User
* Name
user1
Status
Enabled
Email
Passwords
Password Type:
Internal Users
Password
Re-Enter Passw
* Login Password
Enable Password
User Information
First Name
Last Name
Account Options
Description
Change password on next login
Account Disable Policy
Disable account if date exceeds
2017-01-21
User Groups

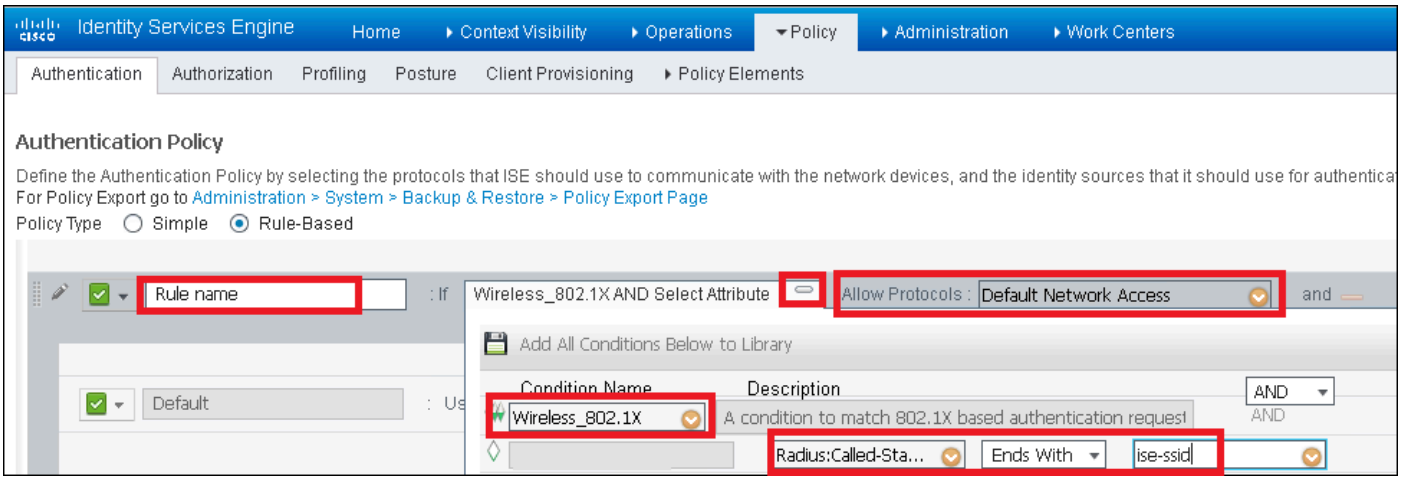


الخطوة 2. إدراج قاعدة مصادقة جديدة.

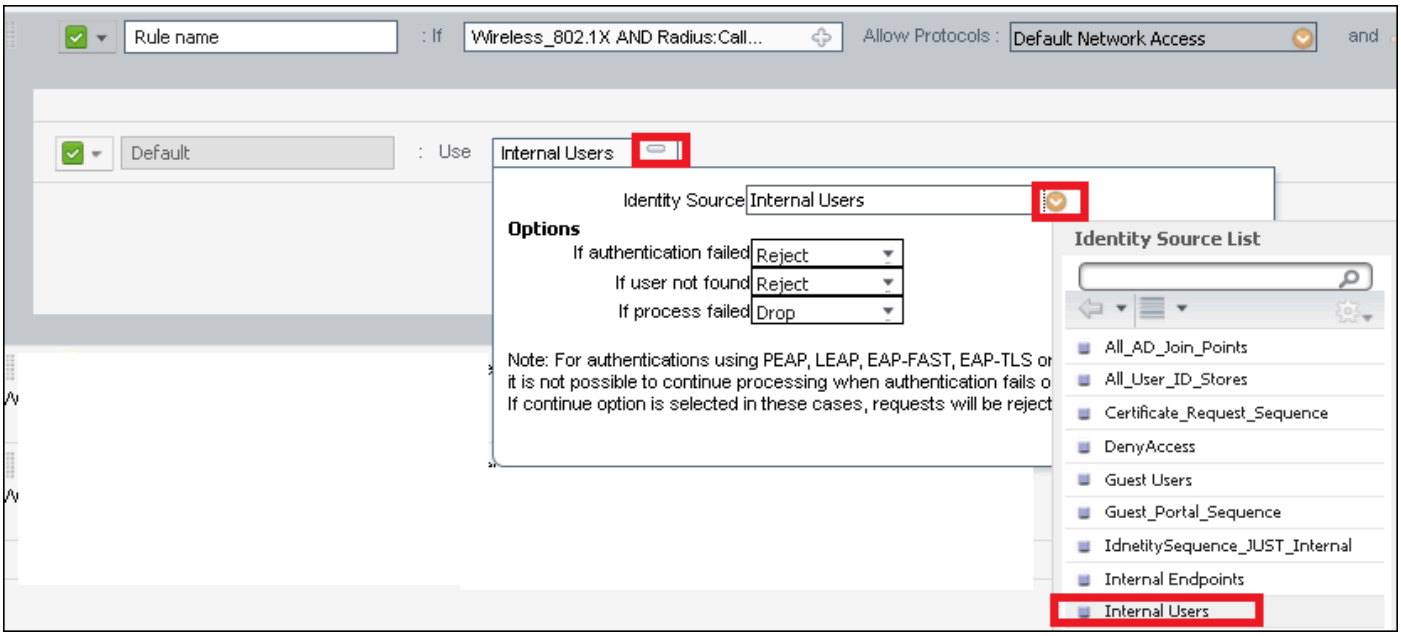
للقيام بذلك، انتقل إلى نهج > مصادقة > إدراج صف جديد أعلى/أسفل.

الخطوة 3. أدخل المعلومات المطلوبة

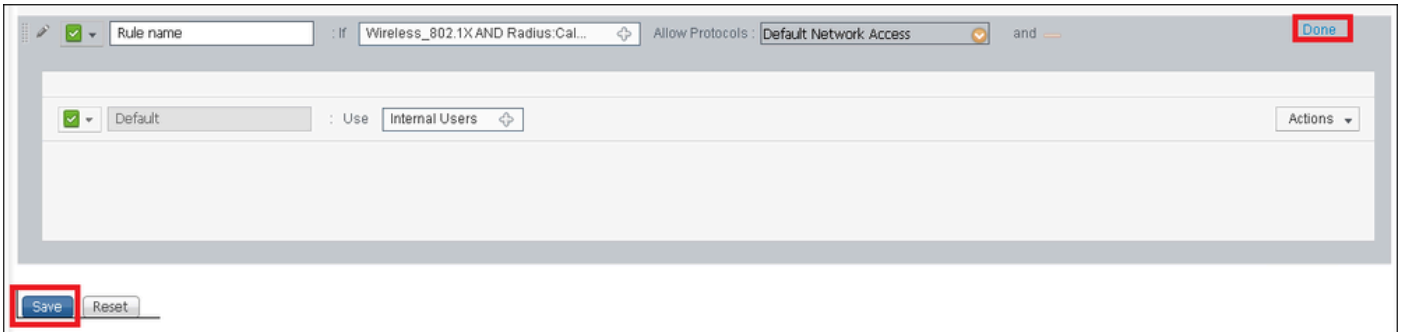
يسمح مثال قاعدة المصادقة هذا لجميع البروتوكولات المدرجة تحت قائمة الوصول إلى الشبكة الافتراضية، وينطبق هذا على طلب المصادقة لعملاء Wireless 802.1x وباستخدام معرف المحطة الاستدعاء وينتهي ب ISE-SSID.



أختر أيضا مصدر الهوية للعملاء الذين تطابق قاعدة المصادقة هذه، وهو في هذا المثال مستخدم للمستخدمين الداخليين



بمجرد انتهائك، انقر فوق تم و احفظ



لمزيد من المعلومات حول السماح لنهج البروتوكولات راجع هذا الارتباط:

خدمة البروتوكولات المسموح بها

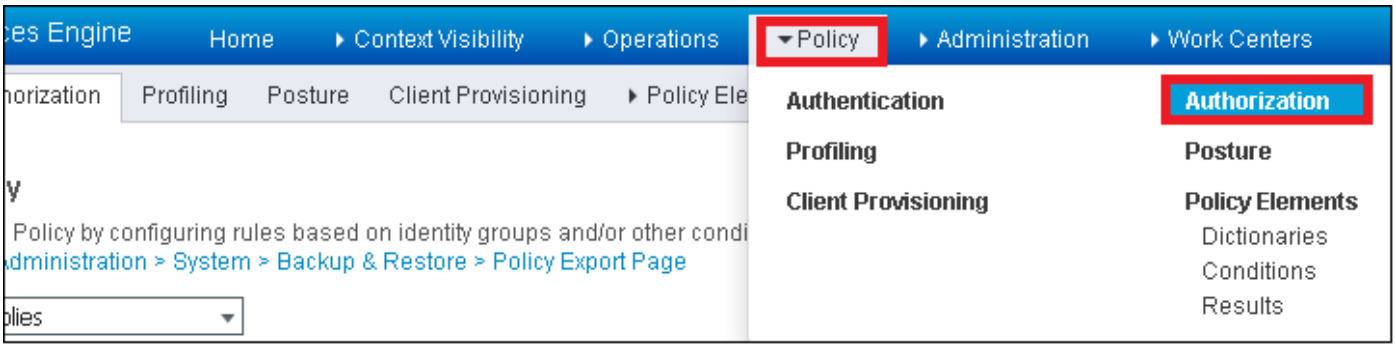
للحصول على مزيد من المعلومات حول مصادر الهوية راجع هذا الارتباط:

إنشاء مجموعة هوية مستخدم

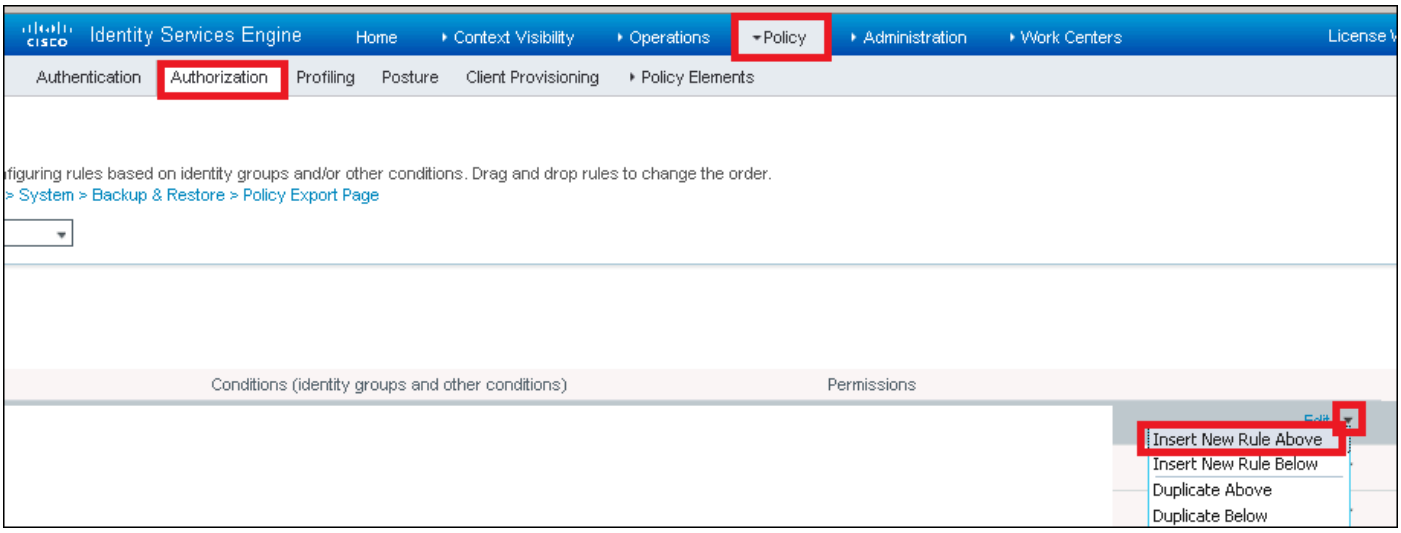
إنشاء قاعدة التخويل

قاعدة التخويل هي القاعدة المسؤولة لتحديد ما إذا كان يسمح للعميل بالانضمام إلى الشبكة أم لا

الخطوة 1. انتقل إلى السياسة > التفويض.

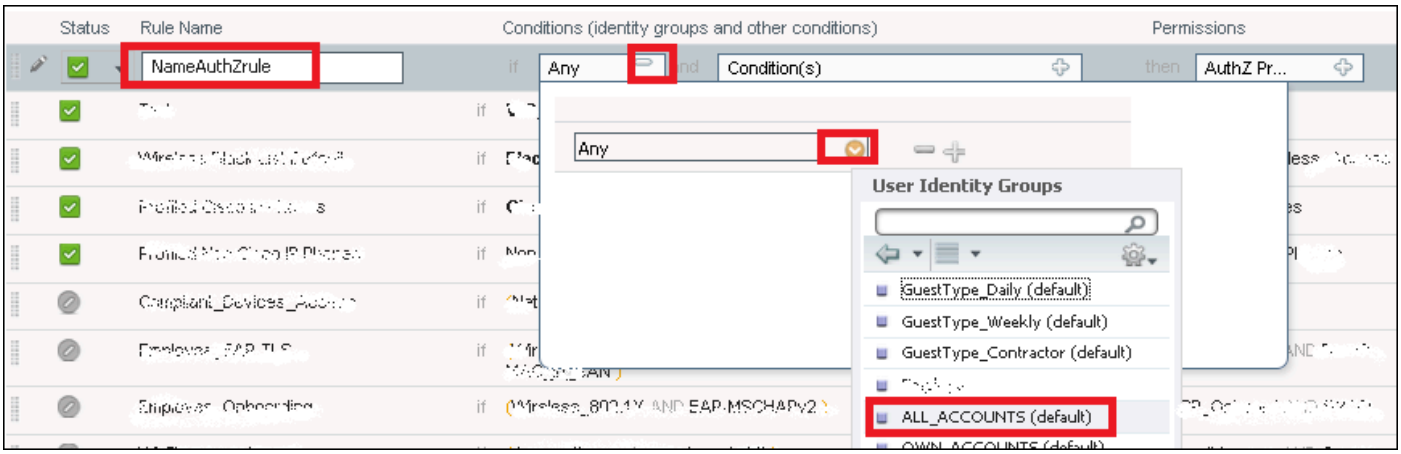


الخطوة 2. إدراج قاعدة جديدة. انتقل إلى النهج > التخويل > إدراج قاعدة جديدة أعلاه/أدناه.

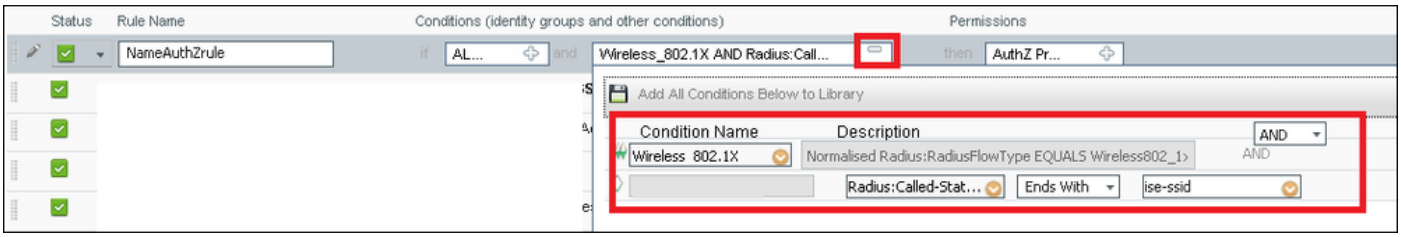


الخطوة 3. أدخل المعلومات.

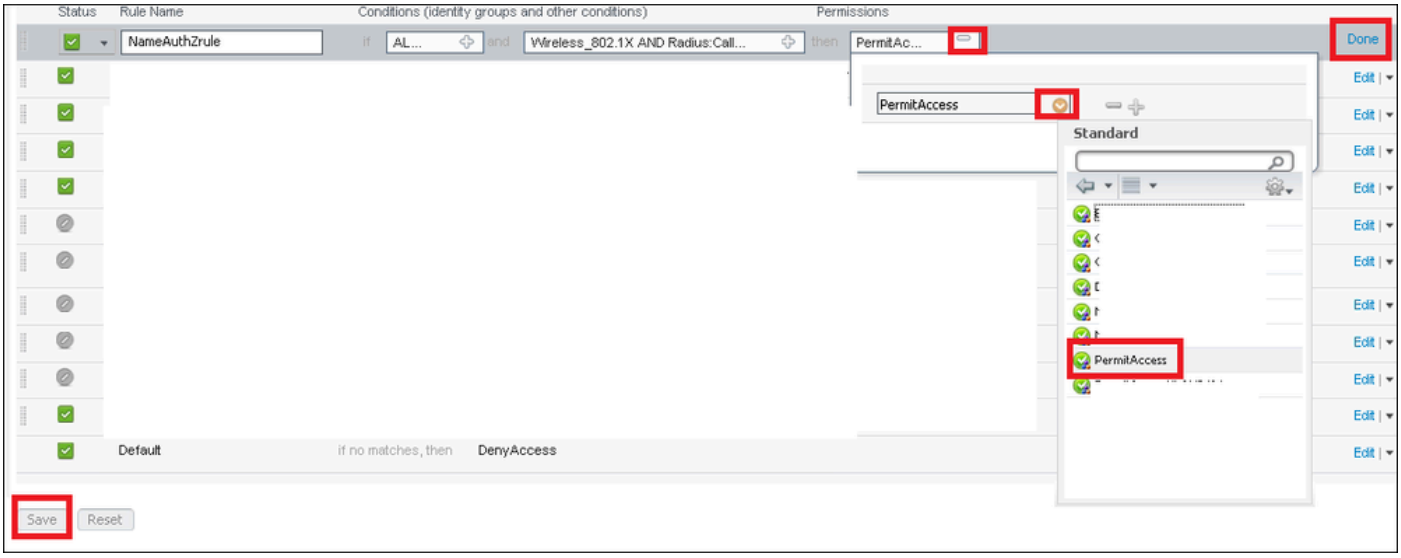
أختر أوال اسم للقاعدة ومجموعات الهوية حيث يتم تخزين المستخدم. في هذا المثال، يتم تخزين المستخدم في مجموعة ALL_ACCOUNTS.



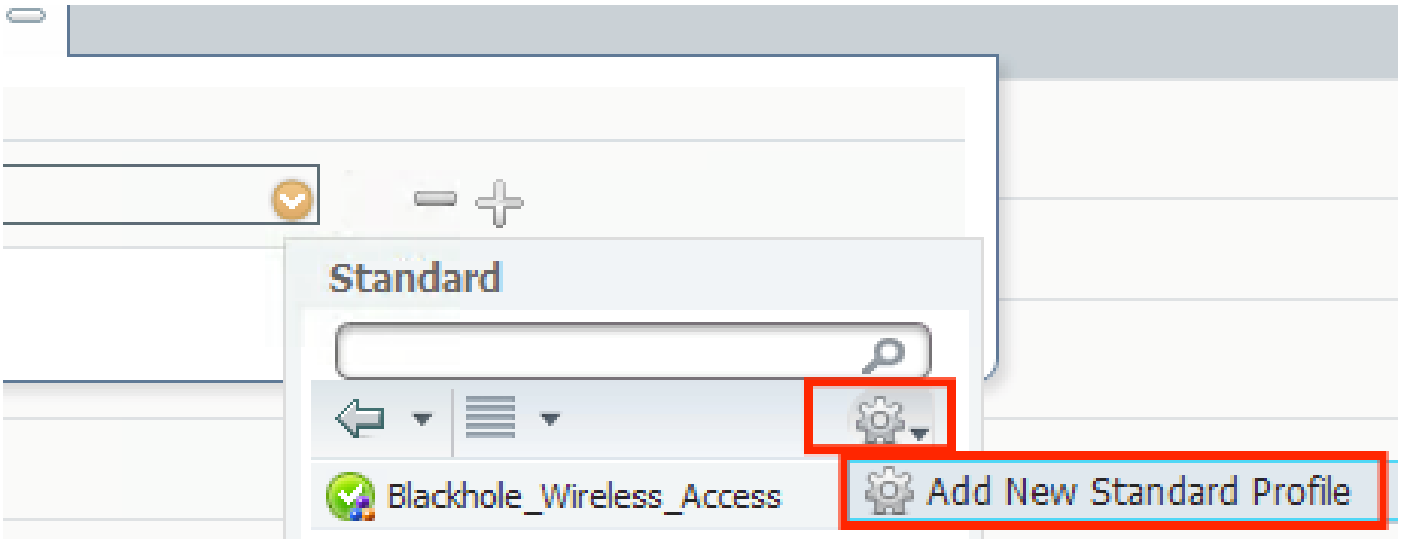
بعد ذلك أختر شروط أخرى تجعل عملية التخويل تقع في هذه القاعدة. في هذا المثال، تتجاوز عملية التخويل هذه القاعدة إذا كانت تستخدم شبكة 802.1x Wireless ويسمى ID Station Id (معرف المحطة) مع ISE-SSID.



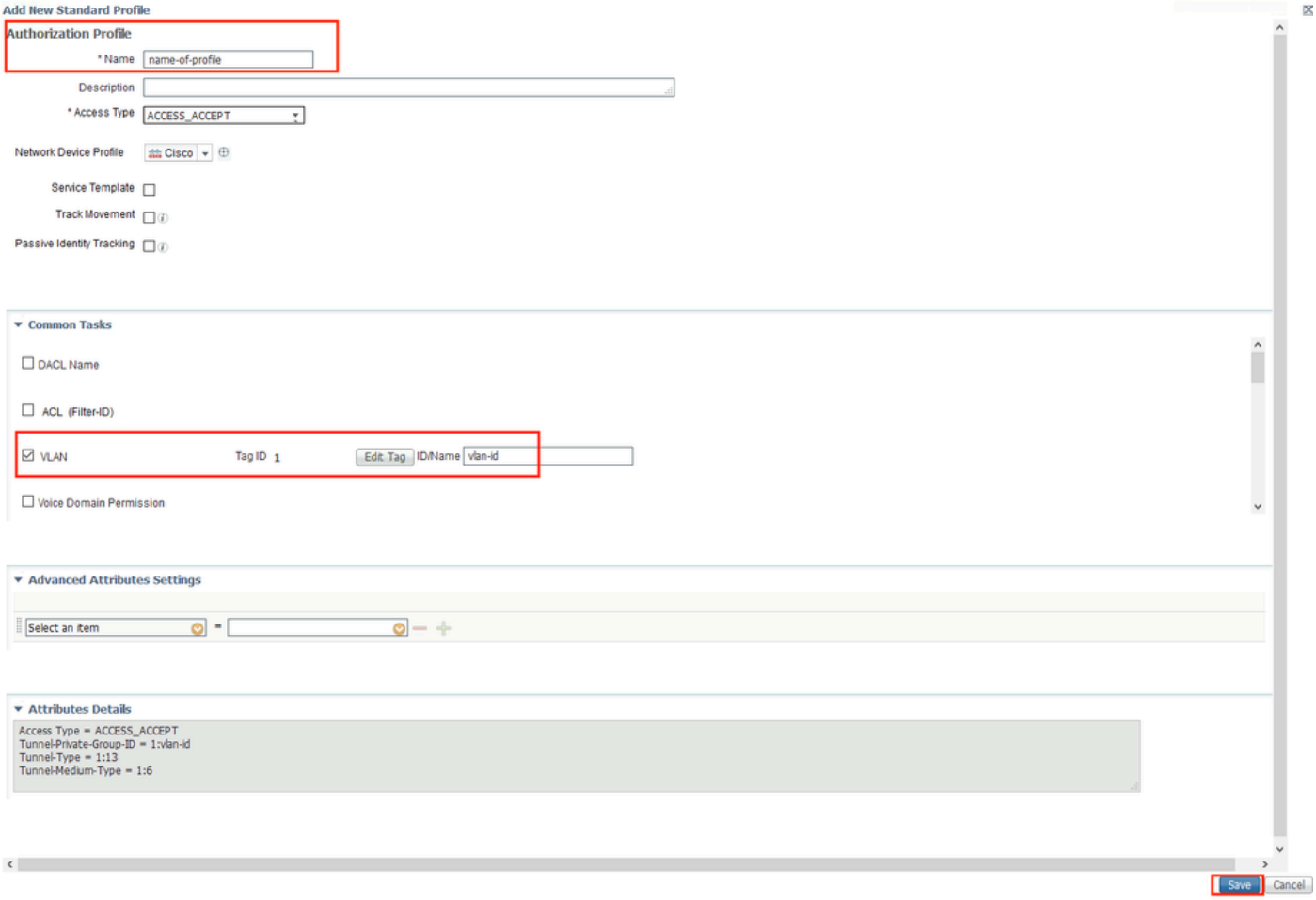
وأخيرا أختر ملف تعريف التخويل الذي يسمح للعملاء بالانضمام إلى الشبكة، انقر على تم وحفظ.



وبشكل إختياري، قم بإنشاء ملف تعريف تخويل جديد سيقوم بتعيين العميل اللاسلكي إلى شبكة VLAN مختلفة:



أدخل المعلومات:



تكوين الجهاز الطرفي

قم بتكوين كمبيوتر محمول يعمل بنظام التشغيل Windows 10 للاتصال بمعرف SSID بمصادقة 802. 1x باستخدام PEAP/MS-CHAPv2 (إصدار Microsoft من بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي الإصدار 2).

في مثال التكوين هذا، يستخدم ISE شهادته الموقعة ذاتيا لتنفيذ المصادقة.

لإنشاء ملف تعريف WLAN على جهاز Windows، هناك خياران:

1. قم بتثبيت الشهادة الموقعة ذاتيا على الجهاز للتحقق من صحة خادم ISE والثقة فيه لاستكمال المصادقة
2. تجاوز التحقق من خادم RADIUS والثقة في أي خادم RADIUS يستخدم لإجراء المصادقة (غير مستحسن، كما يمكن أن يصبح مشكلة تأمين)

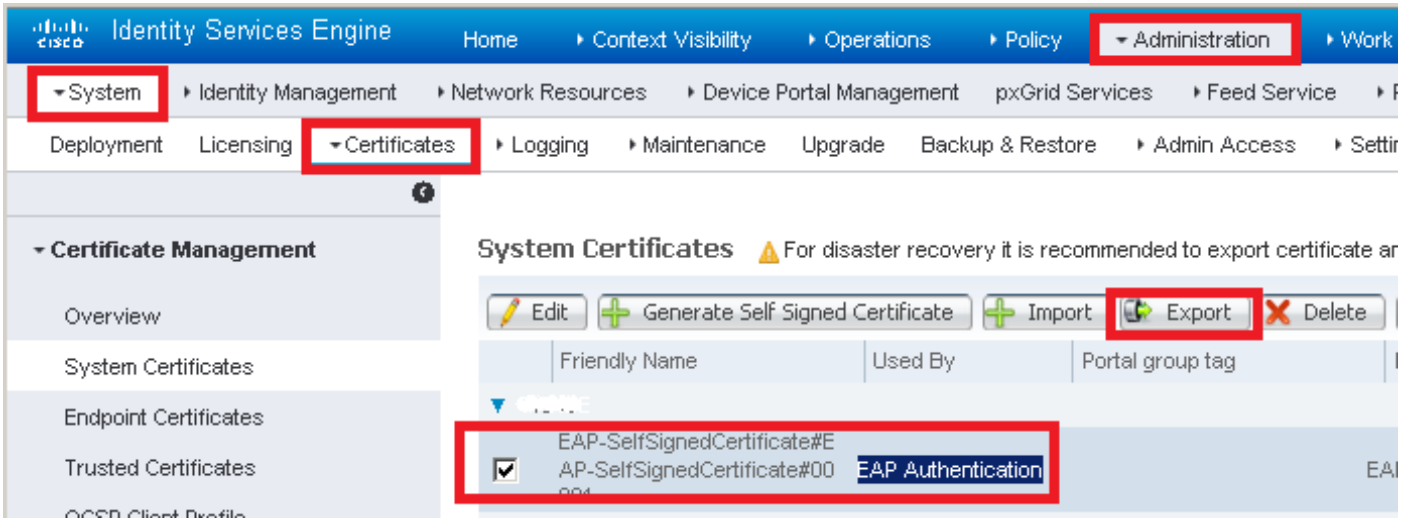
يتم شرح التكوين لهذه الخيارات في [تكوين الجهاز الطرفي - إنشاء ملف تعريف WLAN - الخطوة 7](#).

إنهاء تكوين الجهاز - تثبيت شهادة ISE ذاتية التوقيع

الخطوة 1. تصدير شهادة موقعة ذاتيا من ISE.

سجل الدخول إلى ISE وانتقل إلى إدارة > نظام > شهادات > شهادات النظام.

ثم حدد الشهادة المستخدمة لمصادقة EAP وانقر تصدير.

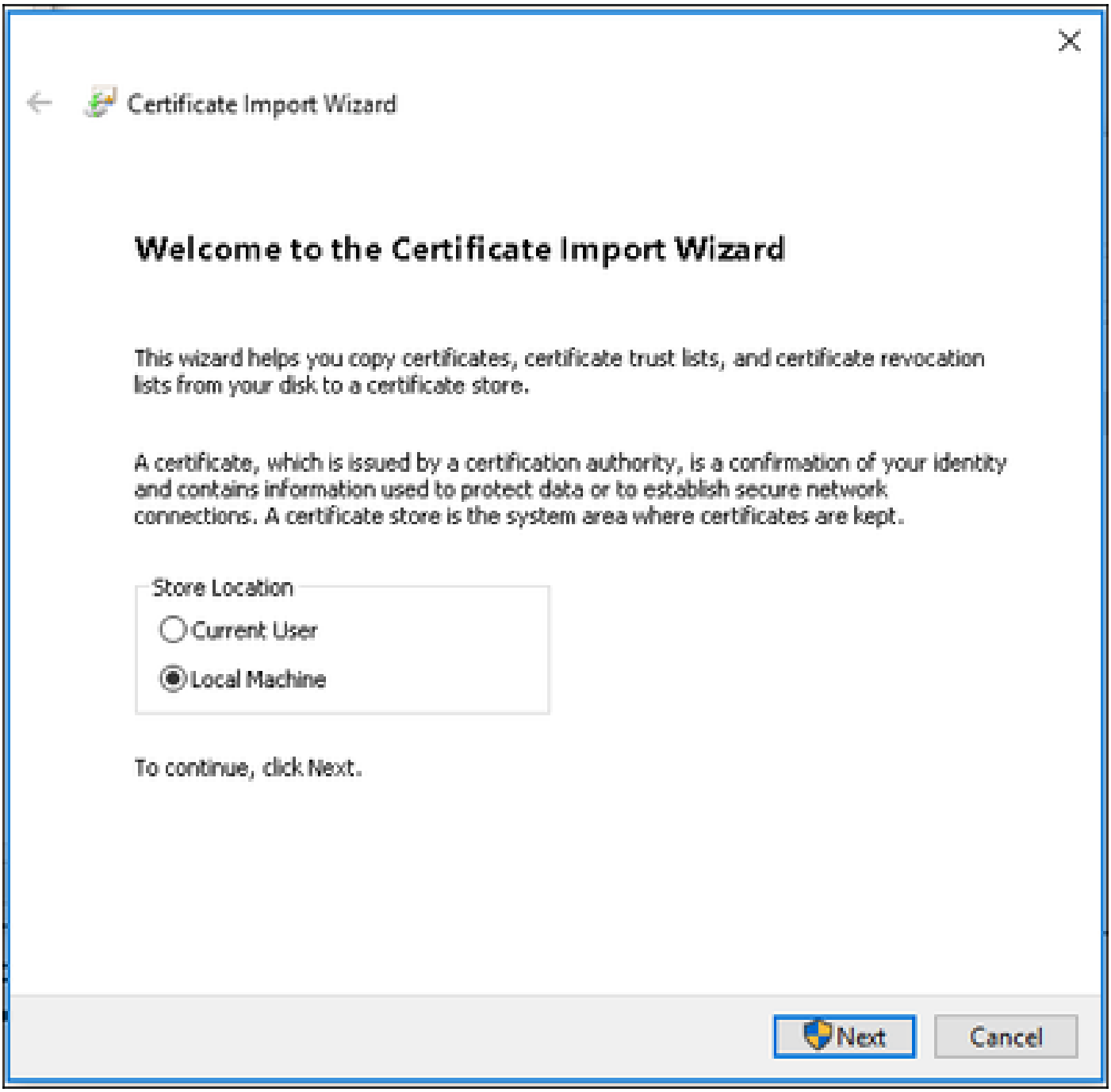


قم بحفظ الشهادة في الموقع المطلوب. هذه الشهادة مثبتة على جهاز Windows.

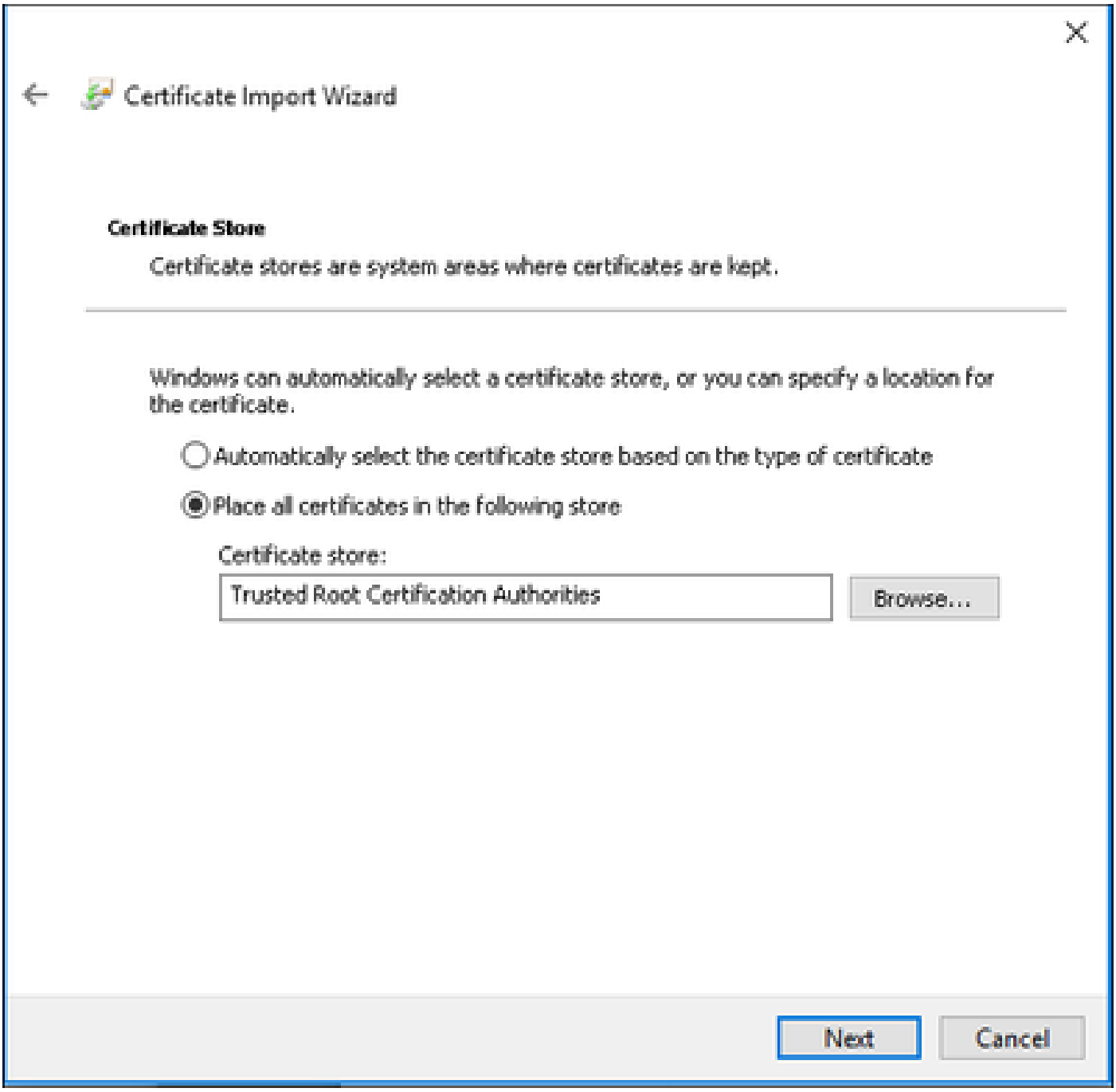
الخطوة 2. قم بتثبيت الشهادة في جهاز Windows.

انسخ الشهادة التي تم تصديرها قبل ذلك إلى جهاز Windows، وقم بتغيير امتداد الملف من .pem إلى .crt، بعد النقر المزدوج عليه وتحديد تثبيت الشهادة...

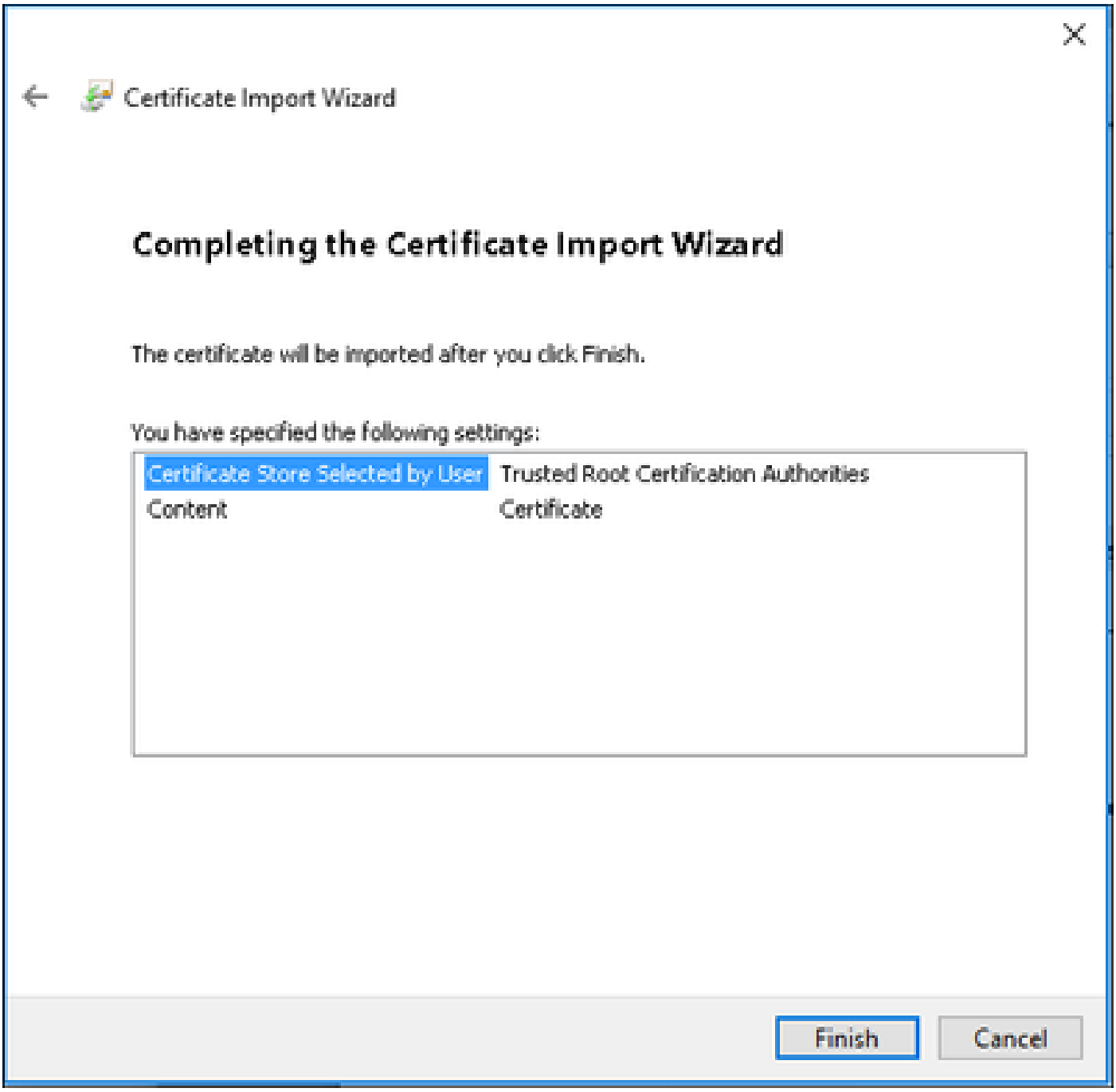
أختر تثبيته في الجهاز المحلي، ثم انقر فوق التالي.



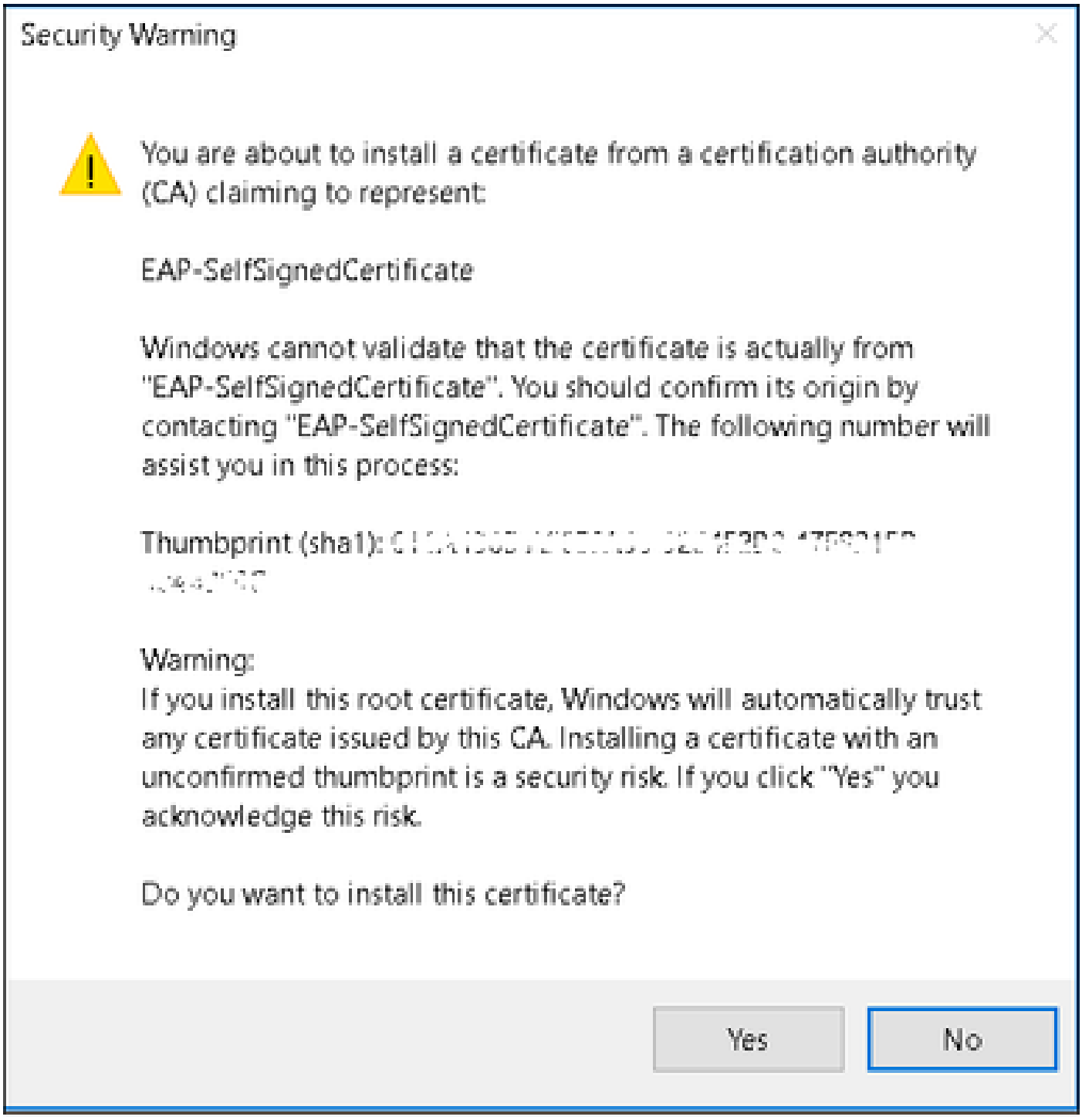
حدد وضع كل الشهادات في المتجر التالي، ثم استعرض واختر مراجع مصادقة الجذر الموثوق بها. بعد ذلك، انقر فوق التالي.



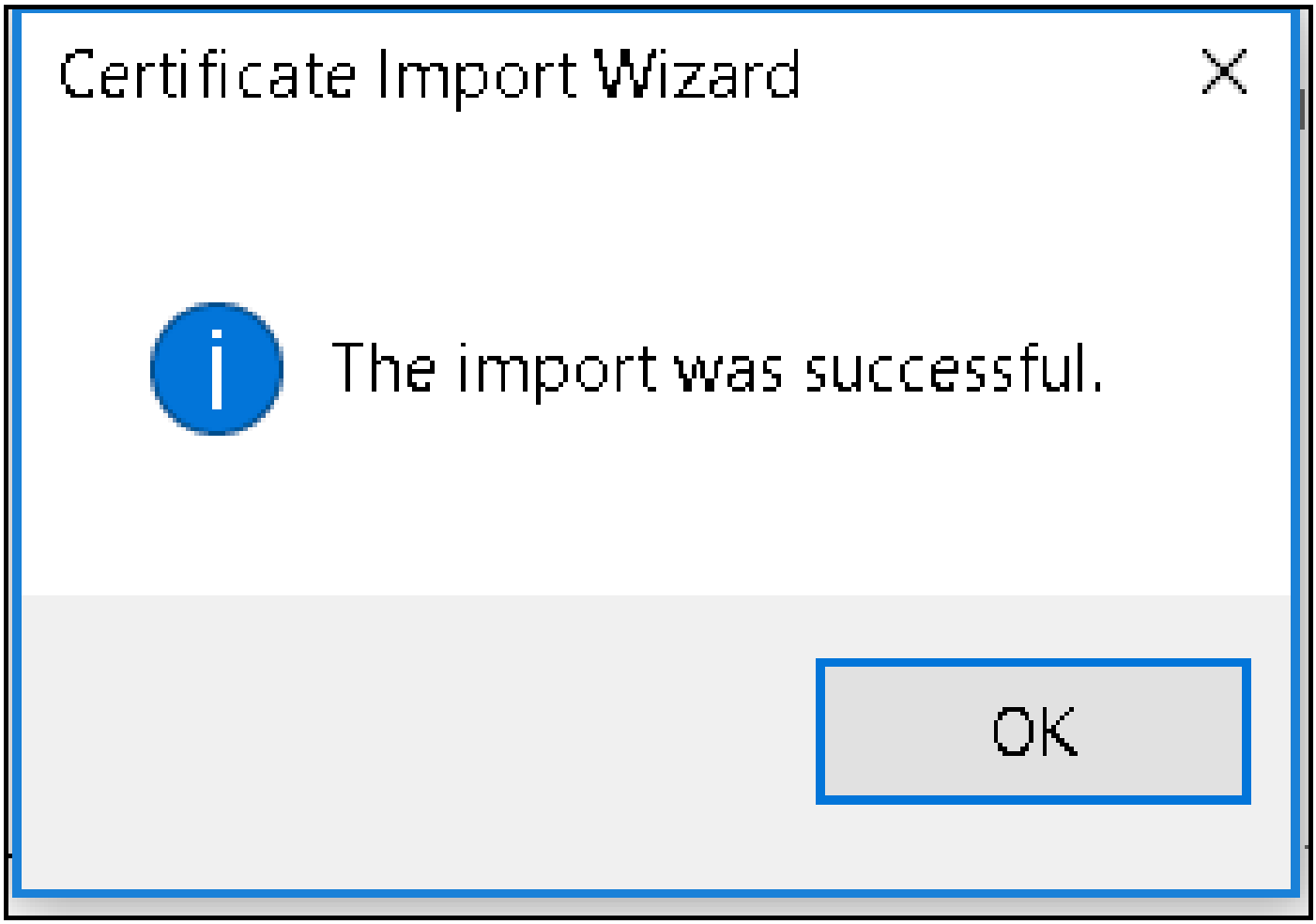
ثم انقر فوق إنهاء.



في النهاية انقر على نعم لتأكيد تثبيت الشهادة.

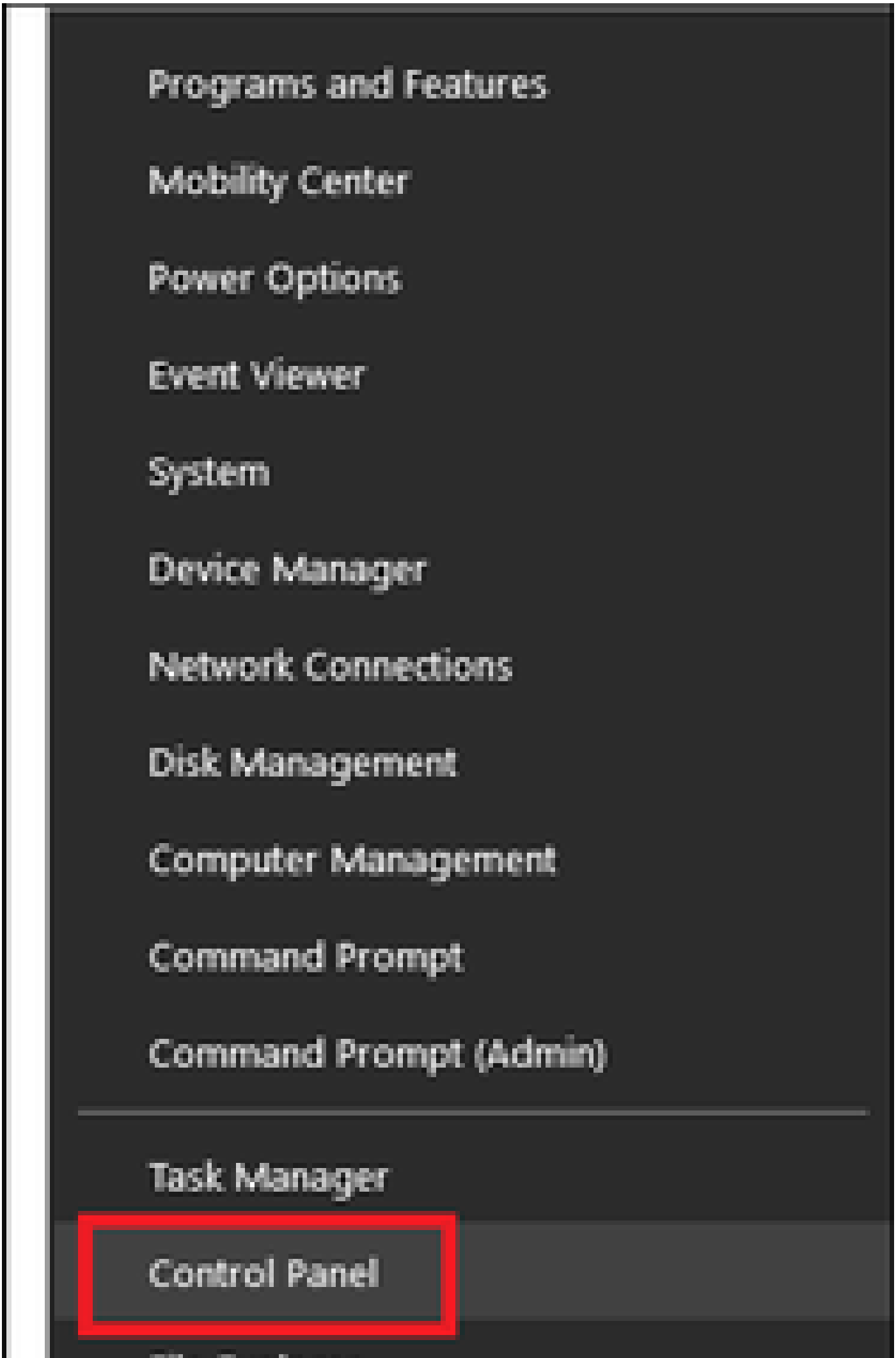


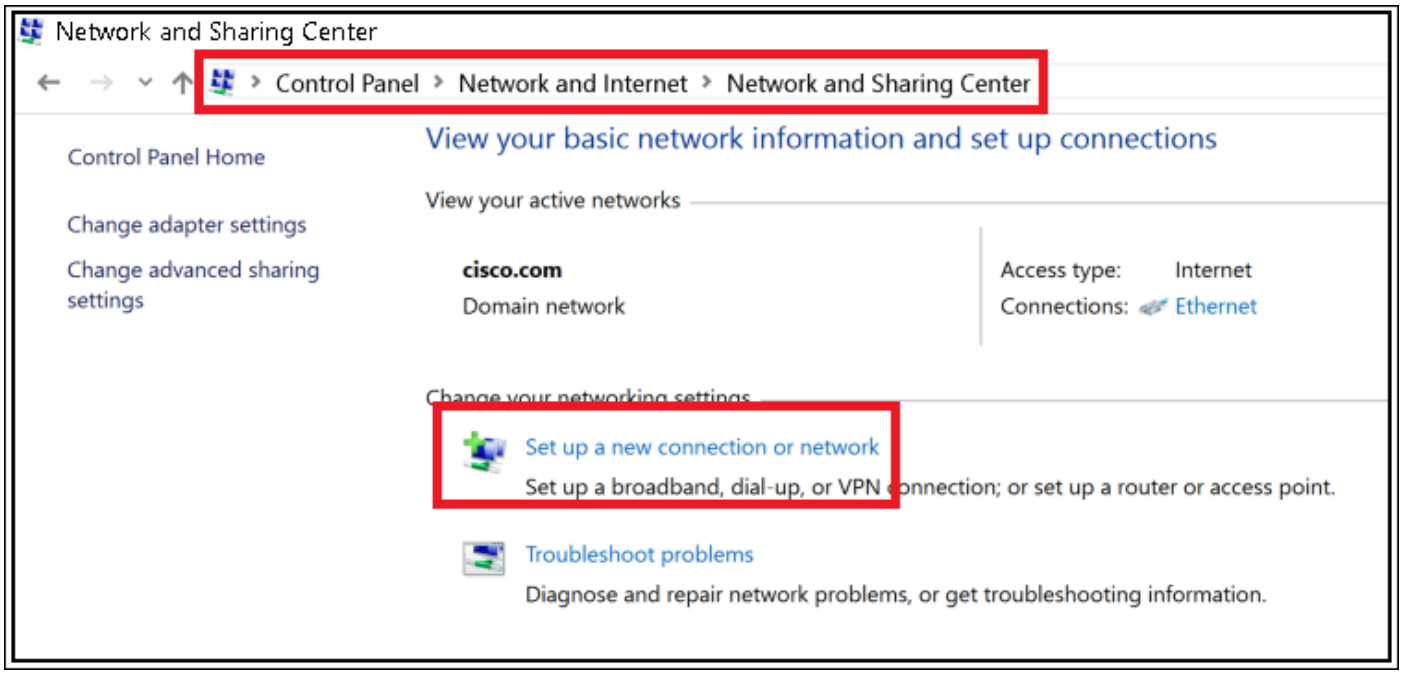
وانقر أخيرا فوق OK.



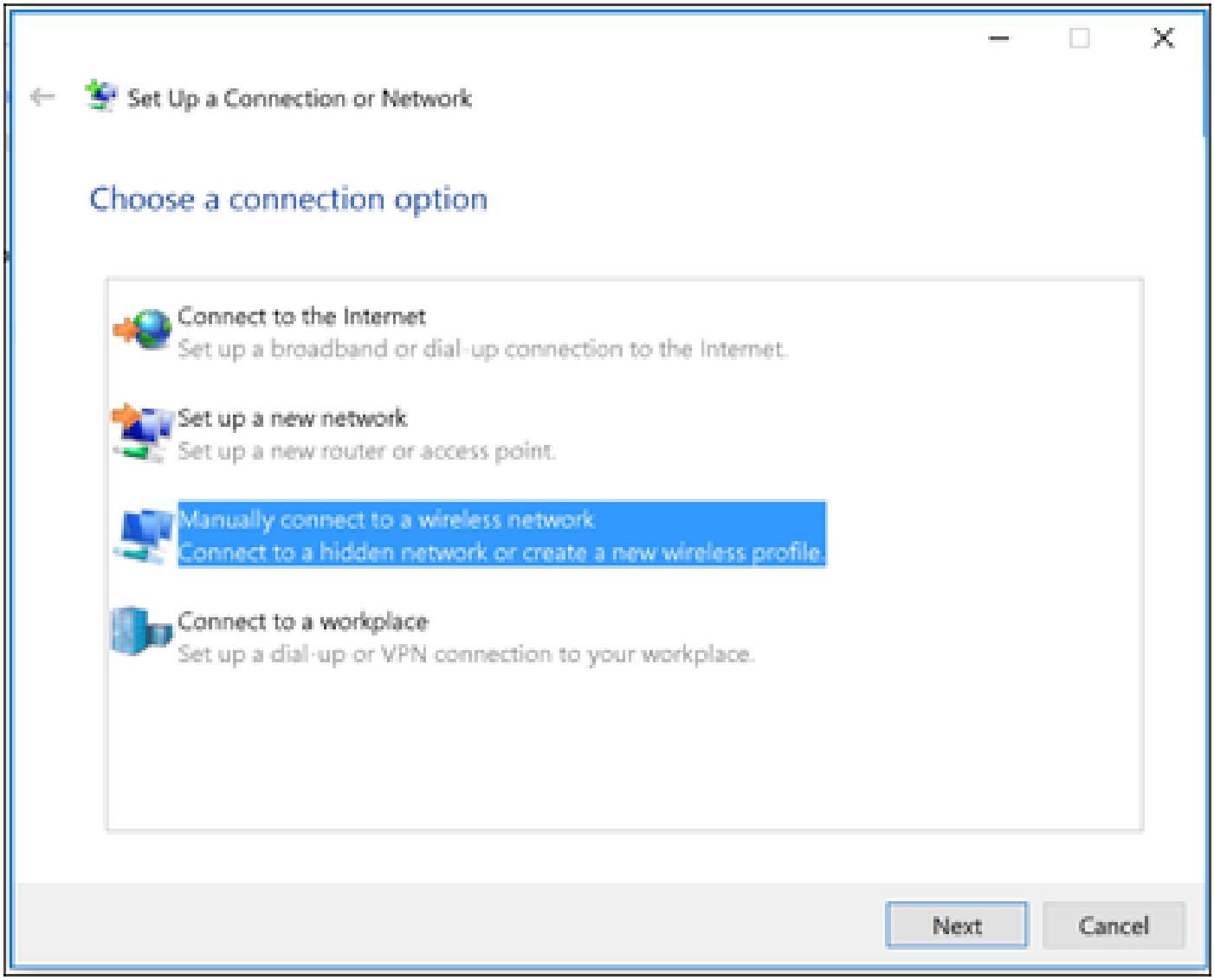
إنهاء تكوين الجهاز - إنشاء ملف تعريف WLAN

الخطوة 1. انقر بزر الماوس الأيمن على أيقونة البدء وحدد لوحة التحكم.

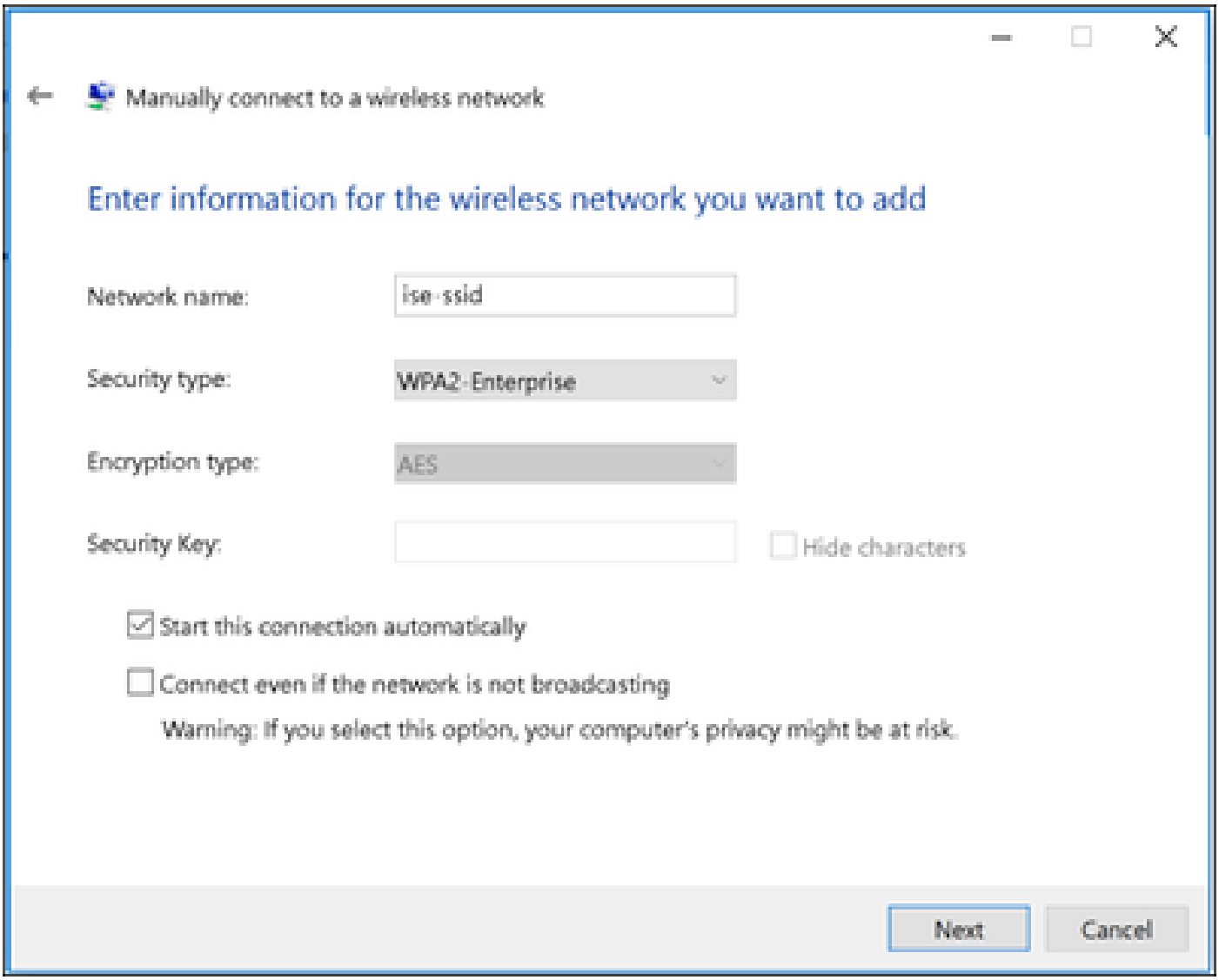

Programs and Features
Mobility Center
Power Options
Event Viewer
System
Device Manager
Network Connections
Disk Management
Computer Management
Command Prompt
Command Prompt (Admin)
Task Manager
Control Panel



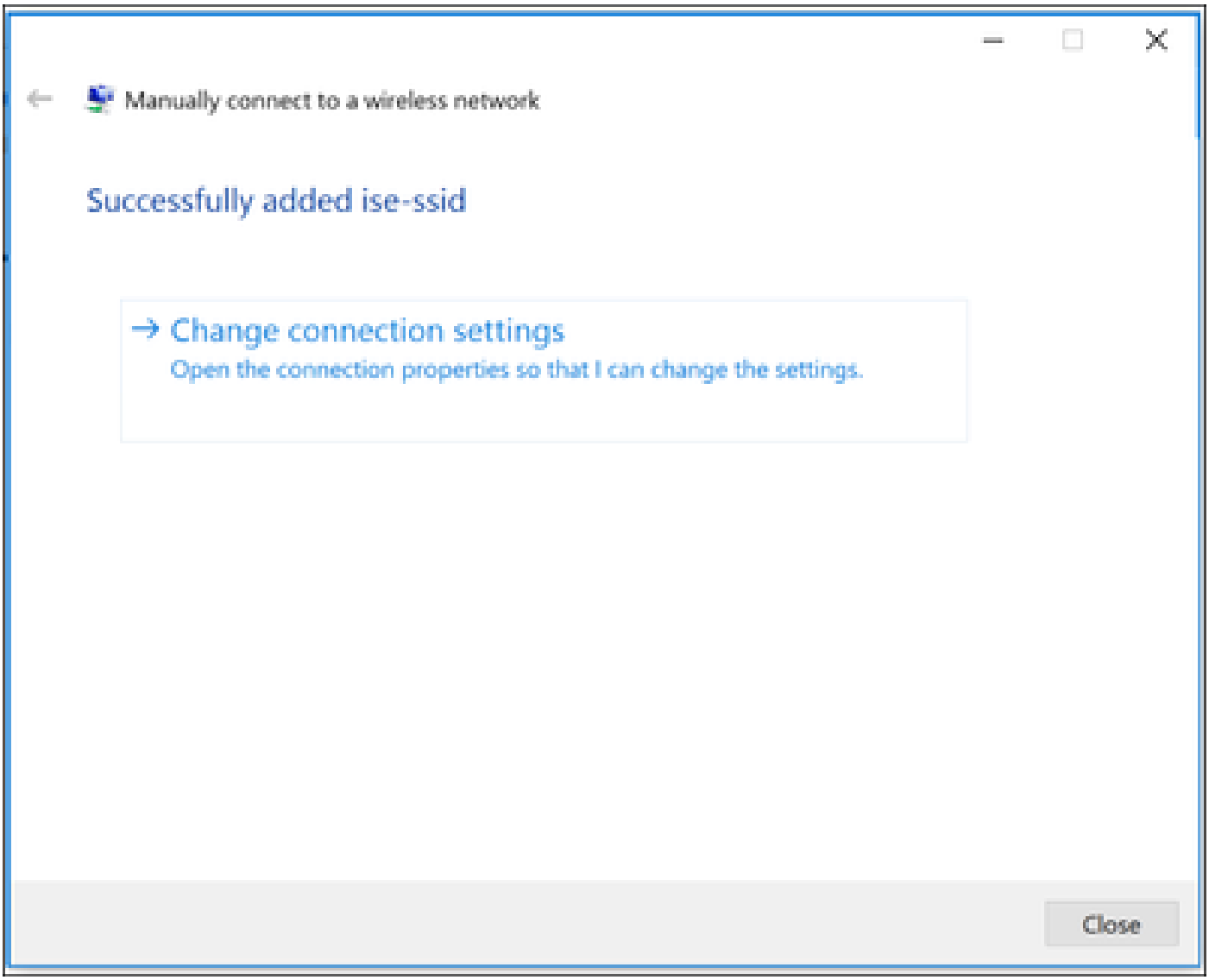
الخطوة 3. حدد التوصيل يدويا بشبكة لاسلكية ثم انقر على التالي.



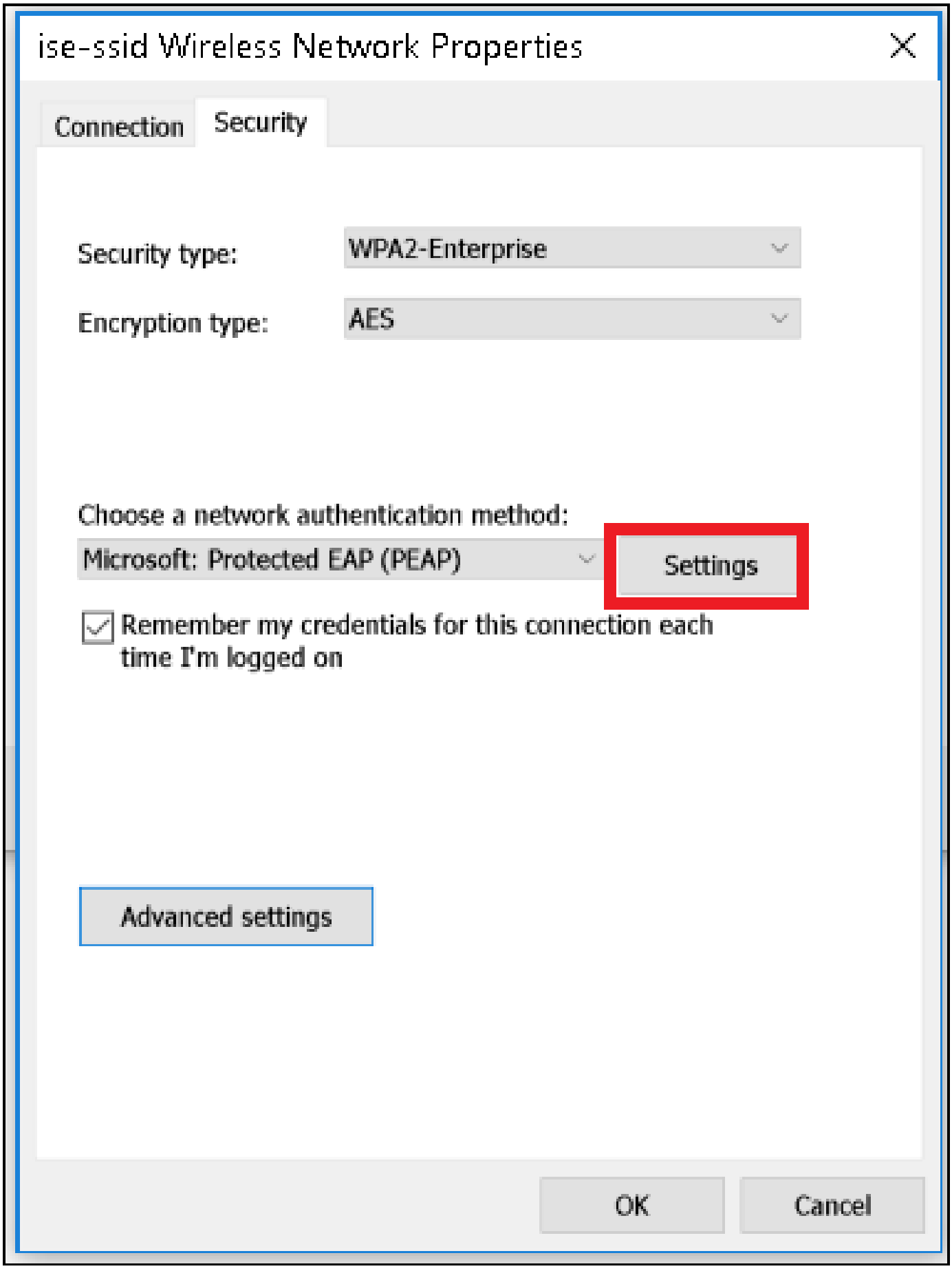
الخطوة 4. أدخل المعلومات باسم SSID ونوع التأمين WPA2-Enterprise ثم انقر على التالي.



الخطوة 5. حدد تغيير إعدادات الاتصال لتخصيص تكوين ملف تعريف WLAN.



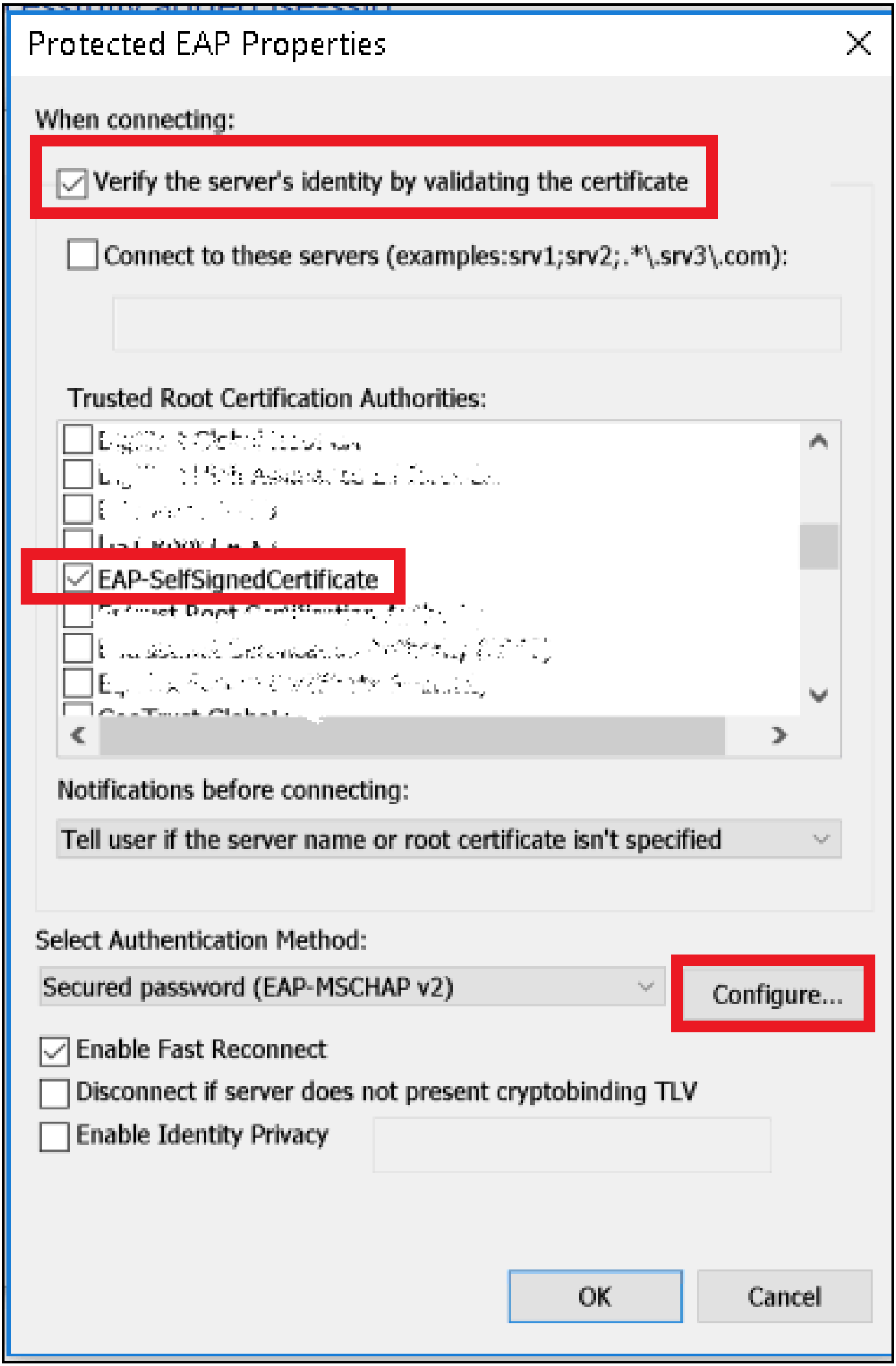
الخطوة 6. انتقل إلى علامة التبويب أمان وانقر فوق إعدادات.



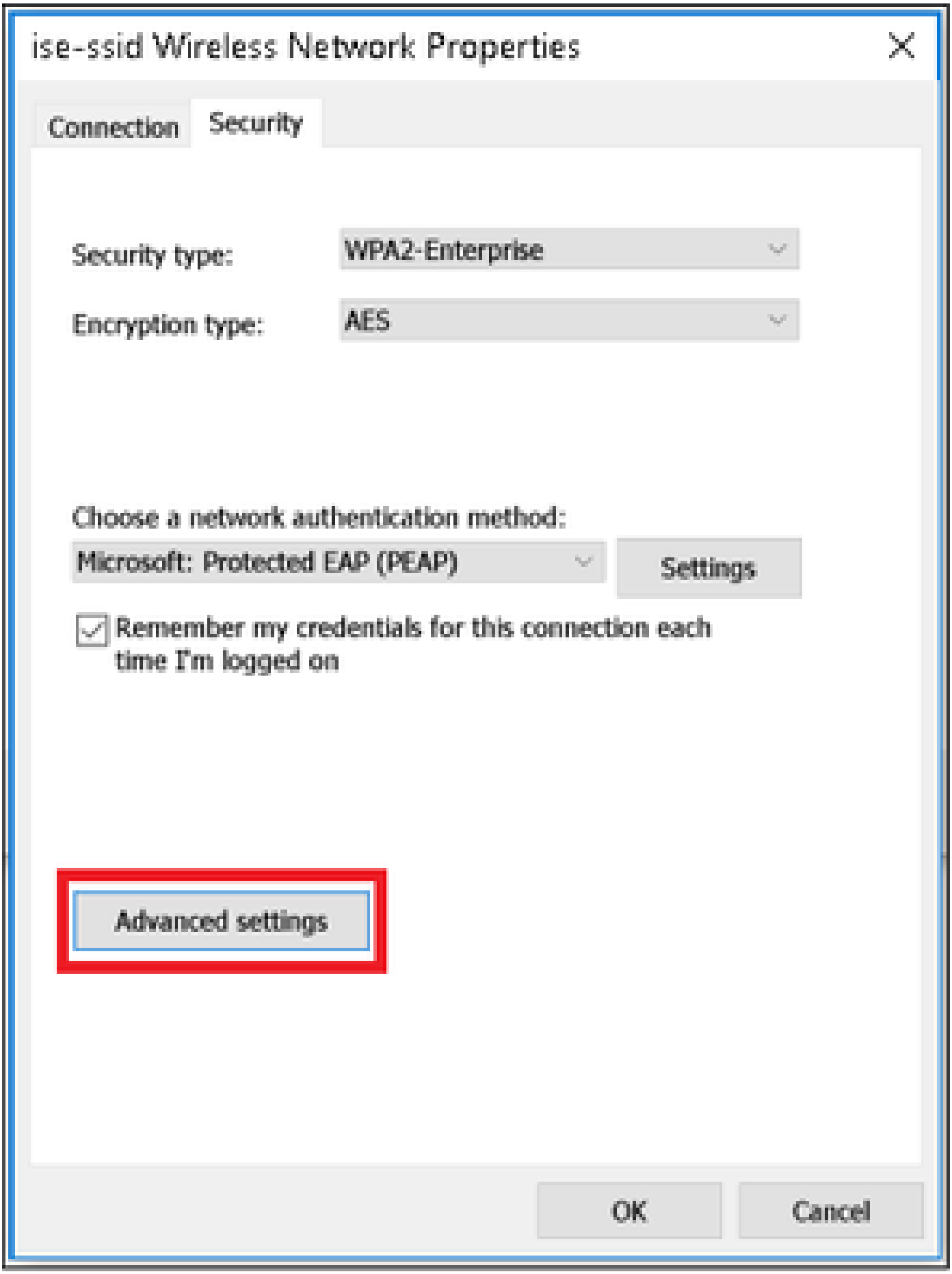
الخطوة 7. أختر ما إذا تم التحقق من صحة خادم RADIUS أم لا.

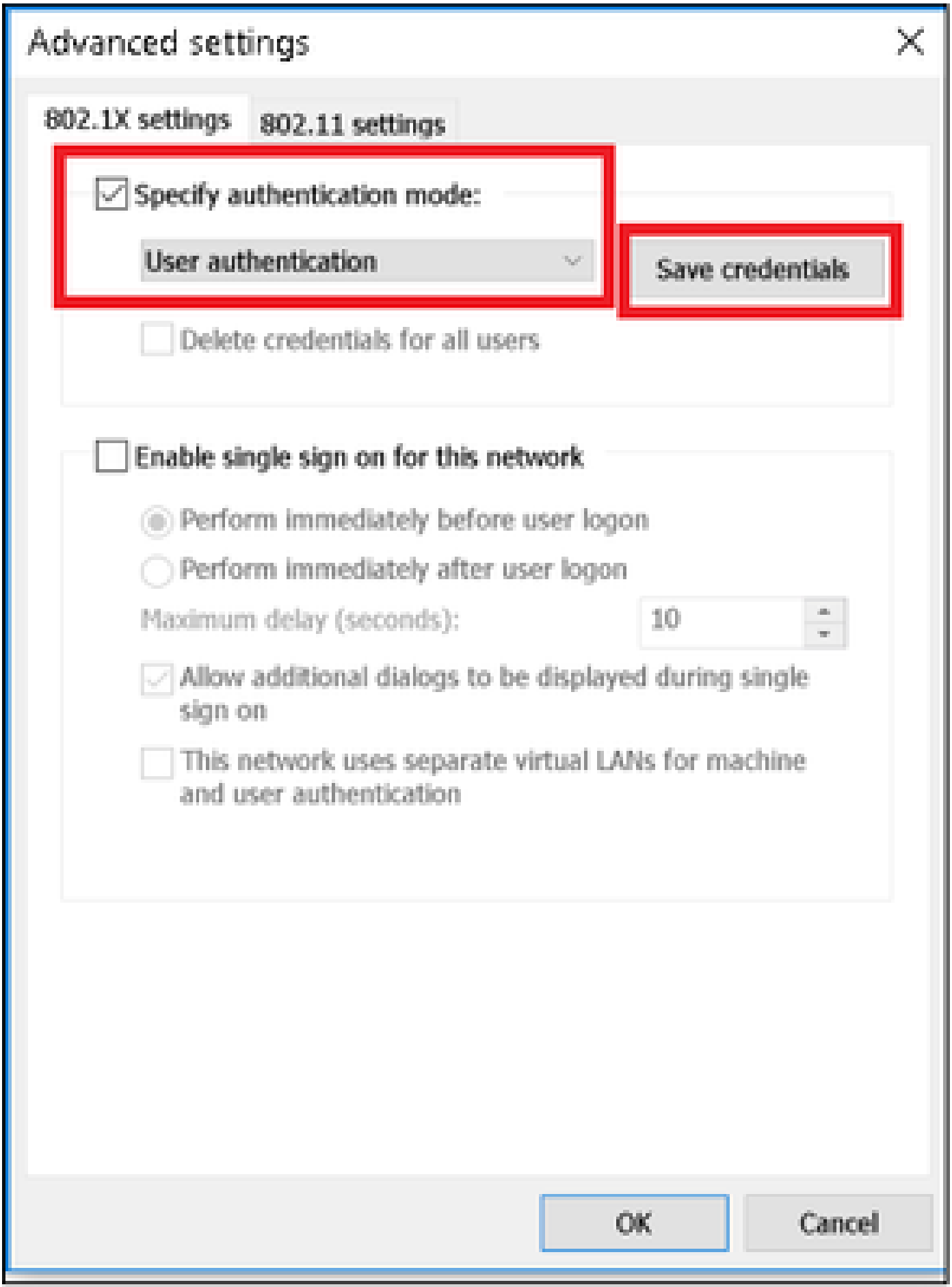
إذا كانت الإجابة بنعم، فقم بتمكين التحقق من هوية الخادم من خلال التحقق من صحة الشهادة ومن المراجع المصدقة الجذر الموثوق بها: تحدد القائمة شهادة ISE الموقعة ذاتيا.

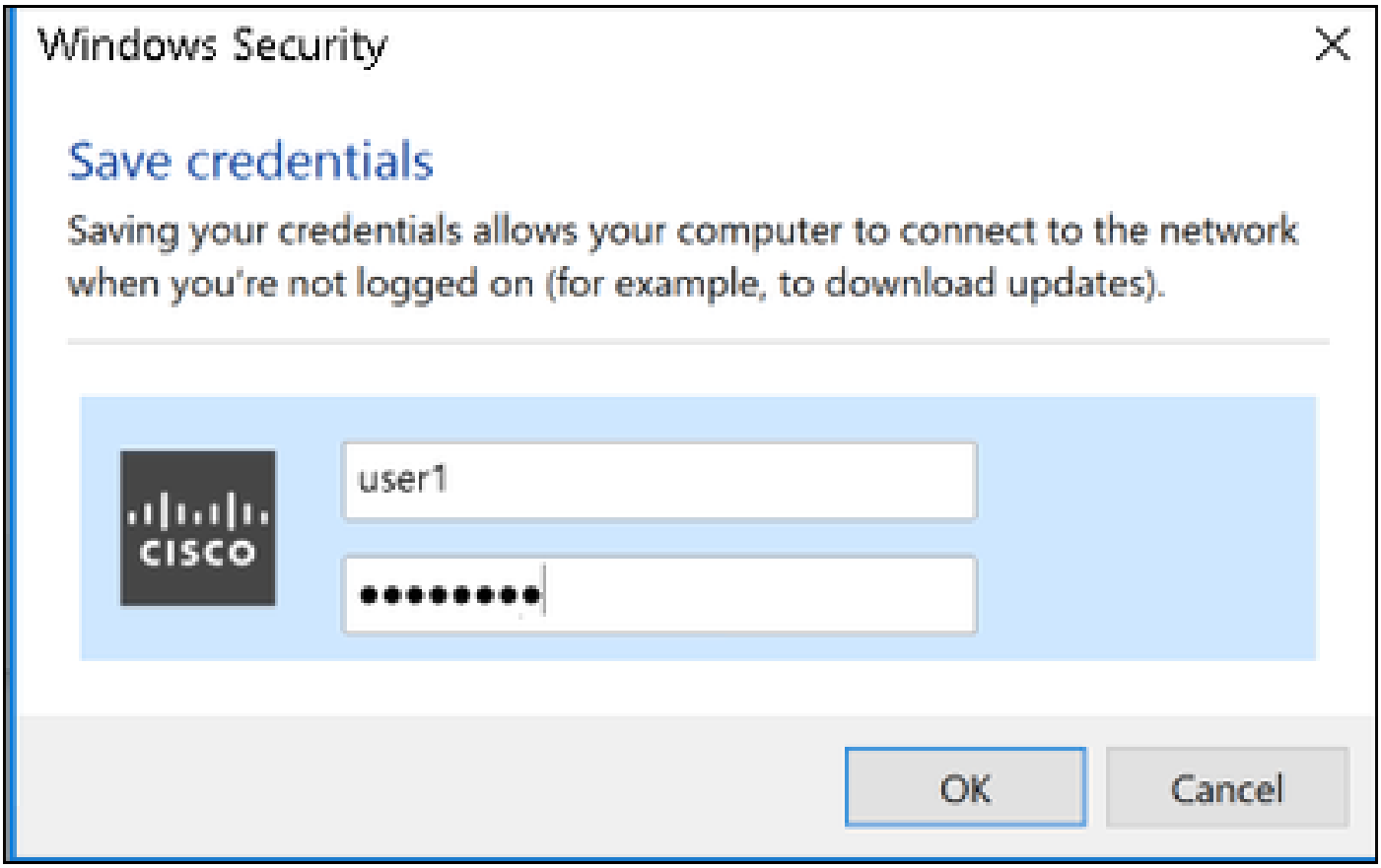
بعد ذلك، حدد تكوين وتعطيل إستخدام اسم وكلمة مرور تسجيل الدخول إلى Windows تلقائيا...، ثم انقر على موافق


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
EAP-SelfSignedCertificate
Notifications before connecting:
Tell user if the server name or root certificate isn't specified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

بمجرد الرجوع إلى علامة التبويب الأمان، حدد الإعدادات المتقدمة، حدد وضع المصادقة كمصادقة المستخدم وقم بحفظ بيانات الاعتماد التي تم تكوينها على ISE لمصادقة المستخدم.


ise-ssid Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User 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
OK
Cancel



التحقق من الصحة

يمكن التحقق من تدفق المصادقة من WLC أو من منظور ISE.

عملية المصادقة في ME

قم بتشغيل هذا الأمر لمراقبة عملية المصادقة لمستخدم معين:

```
> debug client <mac-add-client>
```

مثال للمصادقة الناجحة (تم حذف بعض المخرجات):

```
<#root>

*apfMsConnTask_0: Nov 25 16:36:24.333:

08:74:02:77:13:45 Processing assoc-req station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80

*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on BSSID 38:e
```

*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging override
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface Policy for s
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific apfMsAccessVlan = 2
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed later from
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management suite,
*apfMsConnTask_0: Nov 25 16:36:24.335:

08:74:02:77:13:45 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_0: Nov 25 16:36:24.335: 0

8:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_0: Nov 25 16:36:24.335:

08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:7
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session
*apfMsConnTask_0: Nov 25 16:36:24.335: 0

8:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on a

*apfMsConnTask_0: Nov 25 16:36:24.335:

08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot

*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mob
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 int
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342:

08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401:

08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401:

08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45

.
.
.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978:

08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978:

08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for statio
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cac
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can ta
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:1
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is d
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979:
```

08:74:02:77:13:45 Starting key exchange to mobile 08:74:02:77:13:45, data packets will be dropped

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980:
```

08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state INITPMK (message 1)

```
, replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticati
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 int
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983:
```

08:74:02:77:13:45 Received EAPOL-key in PTK_START state (message 2) from mobile 08:74:02:77:13:45

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0..
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 ......
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ...
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984:
```

08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state PTKINITNEGOTIATING (message 3),

```
replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988:
```

08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988:
```

08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 2
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LW
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988:
```

08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

```
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6623
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role update requ
 Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from Mobility
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6261, Ad
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
 IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobi
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB ip_learn
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug: regType=1 Inva
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB ip_learn
*apfReceiveTask: Nov 25 16:36:27.841:
```

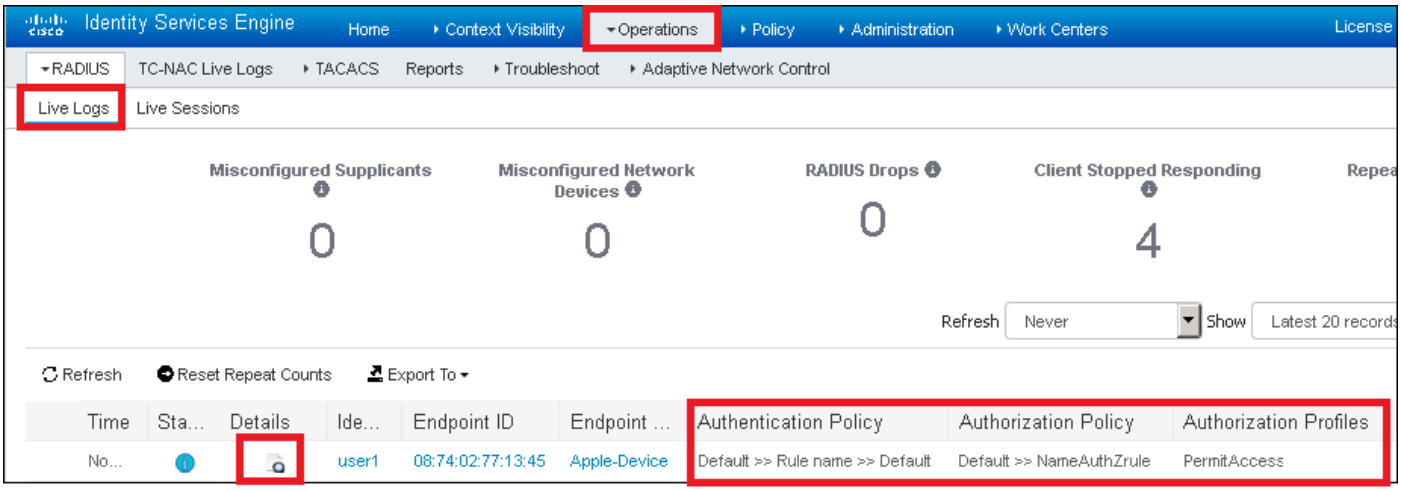
08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state to RUN (20) last state DHCP_REQD (7)

لقراءة مخرجات عميل تصحيح الأخطاء بطريقة سهلة، أستخدم أداة محلل تصحيح الأخطاء اللاسلكية:

Wireless Debug Analyzer (محلل التصحيح اللاسلكي)

عملية المصادقة على ISE

انتقل إلى العمليات > RADIUS > السجلات الحية للاطلاع على سياسة المصادقة ونهج التخويل وملف تعريف التخويل الذي تم تعيينه للمستخدم.



لمزيد من المعلومات، انقر فوق التفاصيل للاطلاع على عملية مصادقة أكثر تفصيلا.

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).