قم بتكوين مومل 802.1X لنقاط الوصول باستخدام وحدة التحكم 9800

المحتويات

قمدقملا

يصف هذا المستند كيفية تكوين نقطة وصول (AP) من Cisco على أنها طلب 802.1x ليتم تخويلها على منفذ switchport مقابل خادم RADIUS.

ةيسايسألا تابلطتملا

تابلطتملا

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدة التحكم في شبكة LAN اللاسلكية (WLC) ونقطة الوصول في الوضع Lightweight (LAP).
- 802.1x على مجموعات Cisco و ISE
- بروتوكول المصادقة الموسع (EAP)
- خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS)

المكونات المستخدمة

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

- WS-C3560CX، Cisco IOS® XE، 15.2(3r)E2
- C9800-CL-K9، Cisco IOS® XE، 17.6.5
- ISE 3.0
- إير-CAP3702
- Air-AP3802

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

في هذا الإعداد، تعمل نقطة الوصول (AP) كملقم 802.1x وتتم مصادقتها بواسطة المحول مقابل ISE باستخدام أسلوب EAP-FAST.

ما إن تكون الميناء شكلت لمصادقة 802.1X، المفتاح لا يسمح أي حركة مرور غير 802.1X حركة مرور أن يمر عبر الميناء إلى أن الأداة يربط إلى الميناء يصادق بنجاح.

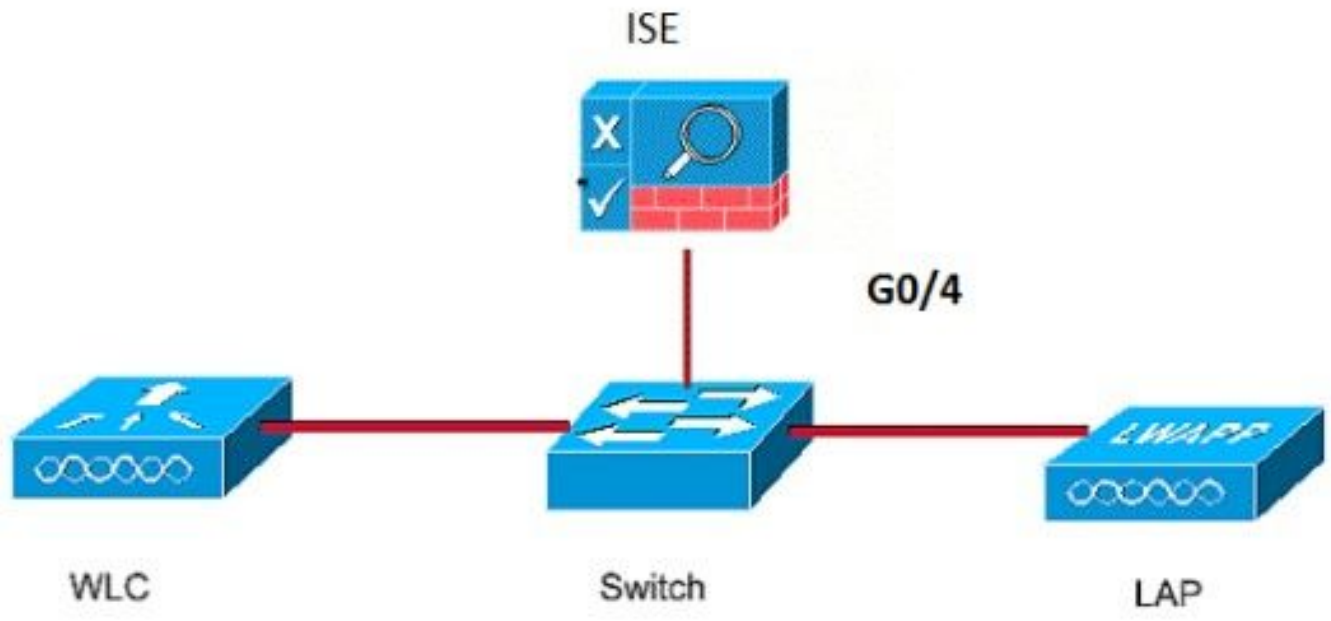
يمكن مصادقة نقطة الوصول إما قبل انضمامها إلى وحدة تحكم في الشبكة المحلية اللاسلكية (WLC) أو بعد انضمامها إلى وحدة تحكم في الشبكة المحلية اللاسلكية (WLC)، في هذه الحالة، قم بتكوين 802.1X على المحول بعد انضمام نقطة الوصول (LAP) إلى وحدة التحكم في الشبكة المحلية اللاسلكية (WLC).

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

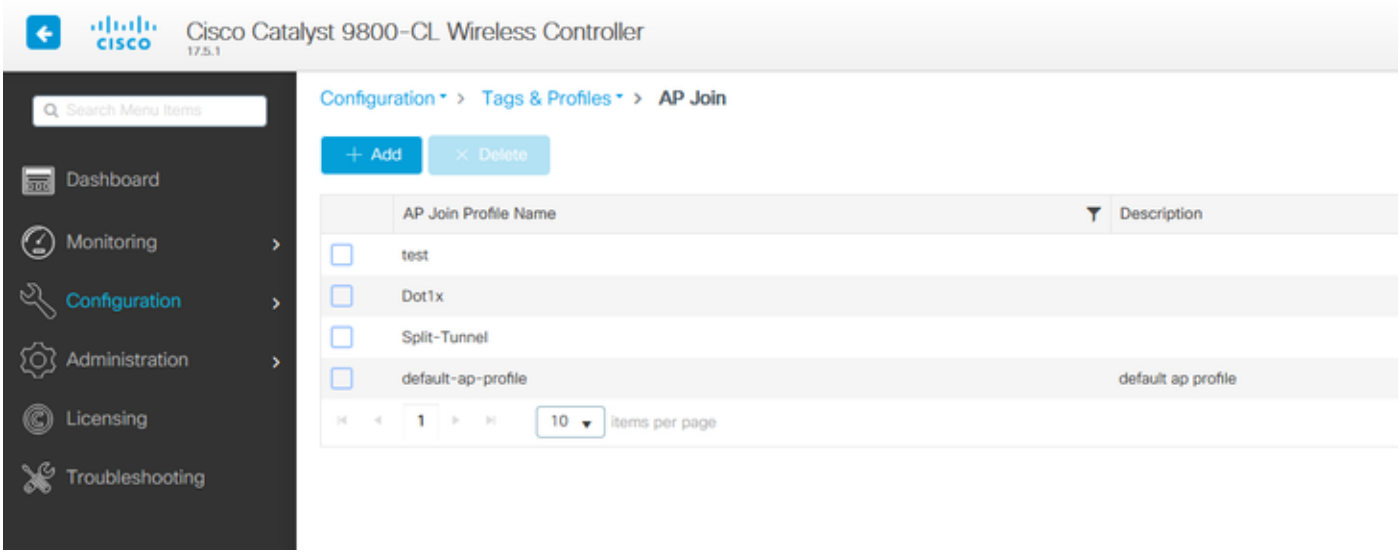


تكوين نقاط الوصول في الوضع Lightweight كمتمس 802.1x

إذا كانت نقطة الوصول متصلة بالفعل بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC):

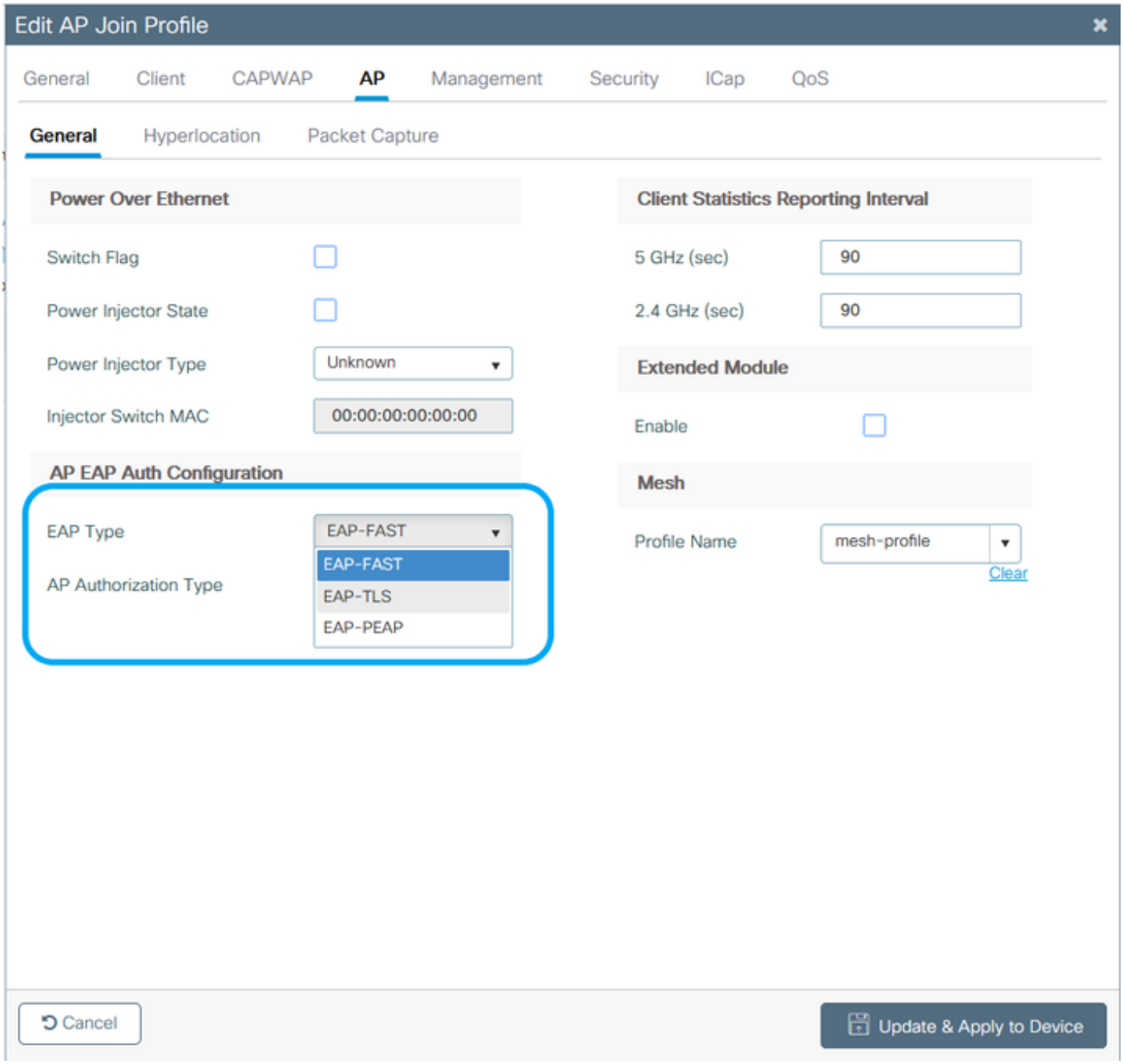
قم بتكوين نوع مصادقة 802.1x ونوع مصادقة AP للشهادة ذات الأهمية المحلية (LSC):

الخطوة 1. انتقل إلى تكوين >علامات وتوصيفاتربط AP>في صفحة ملف تعريف الانضمام إلى نقطة الوصولAP، انقر على إضافة لإضافة ملف تعريف ربط جديد أو تحرير ملف تعريف إرتباط نقطة وصول عندما تنقر فوق اسمه.

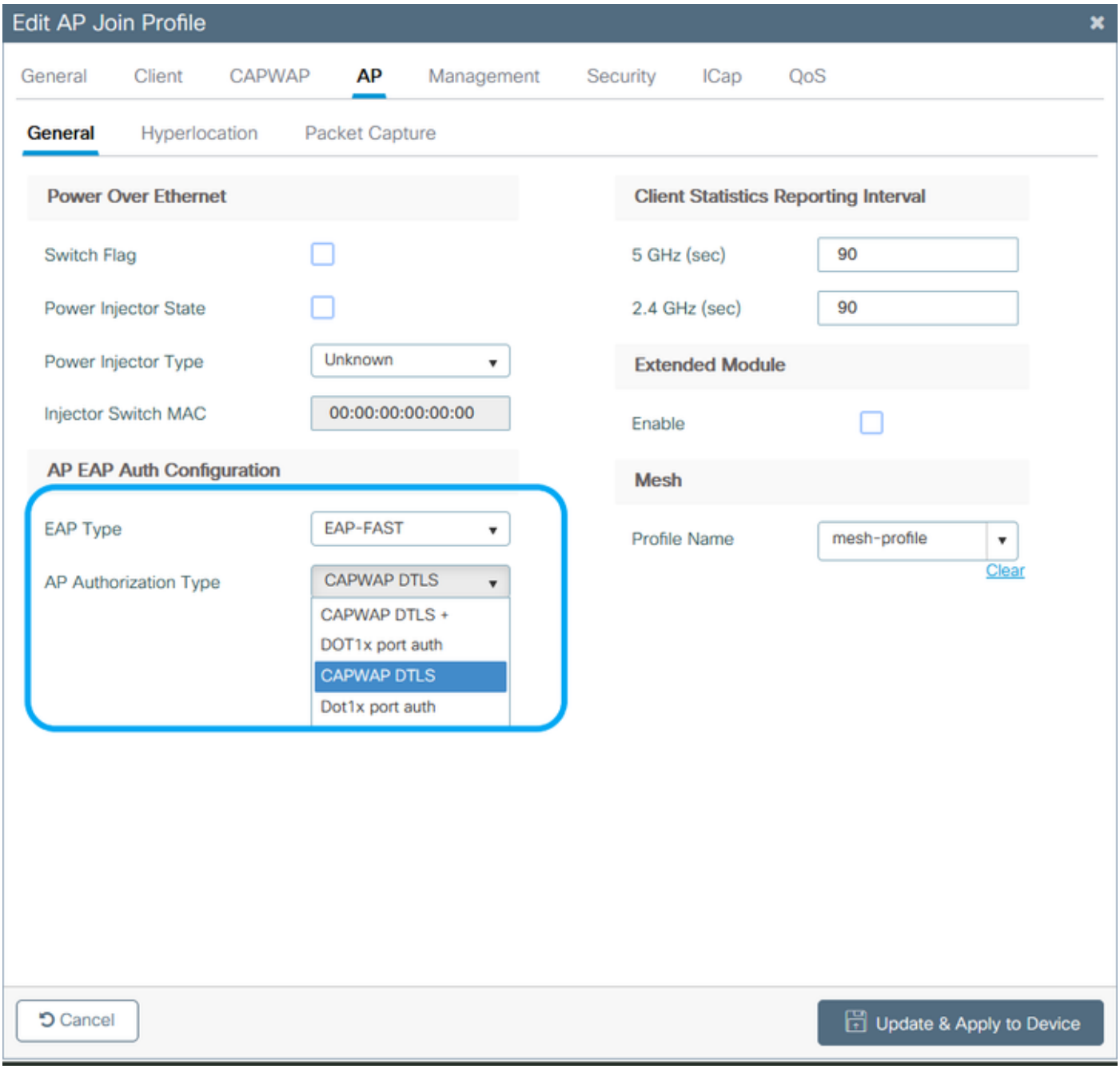


الخطوة 2. في صفحة ملف تعريف الانضمام إلى نقطة الوصول، من AP > عام، انتقل إلى قسم تكوين مصادقة AP EAP. من القائمة المنسدلة نوع EAP أختر نوع EAP مثل EAP-FAST أو EAP-TLS أو EAP-PEAP لتكوين نوع مصادقة dot1x. EAP-FAST هو نوع المصادقة

الوحيد الذي يستخدم اسم المستخدم وكلمات المرور فقط وهو الأسهل للإعداد. يتطلب LSC (راجع قسم المراجع) مما يوفر شهادات على نقاط الوصول من خلال سير عمل PEAP و EAP-TLS.

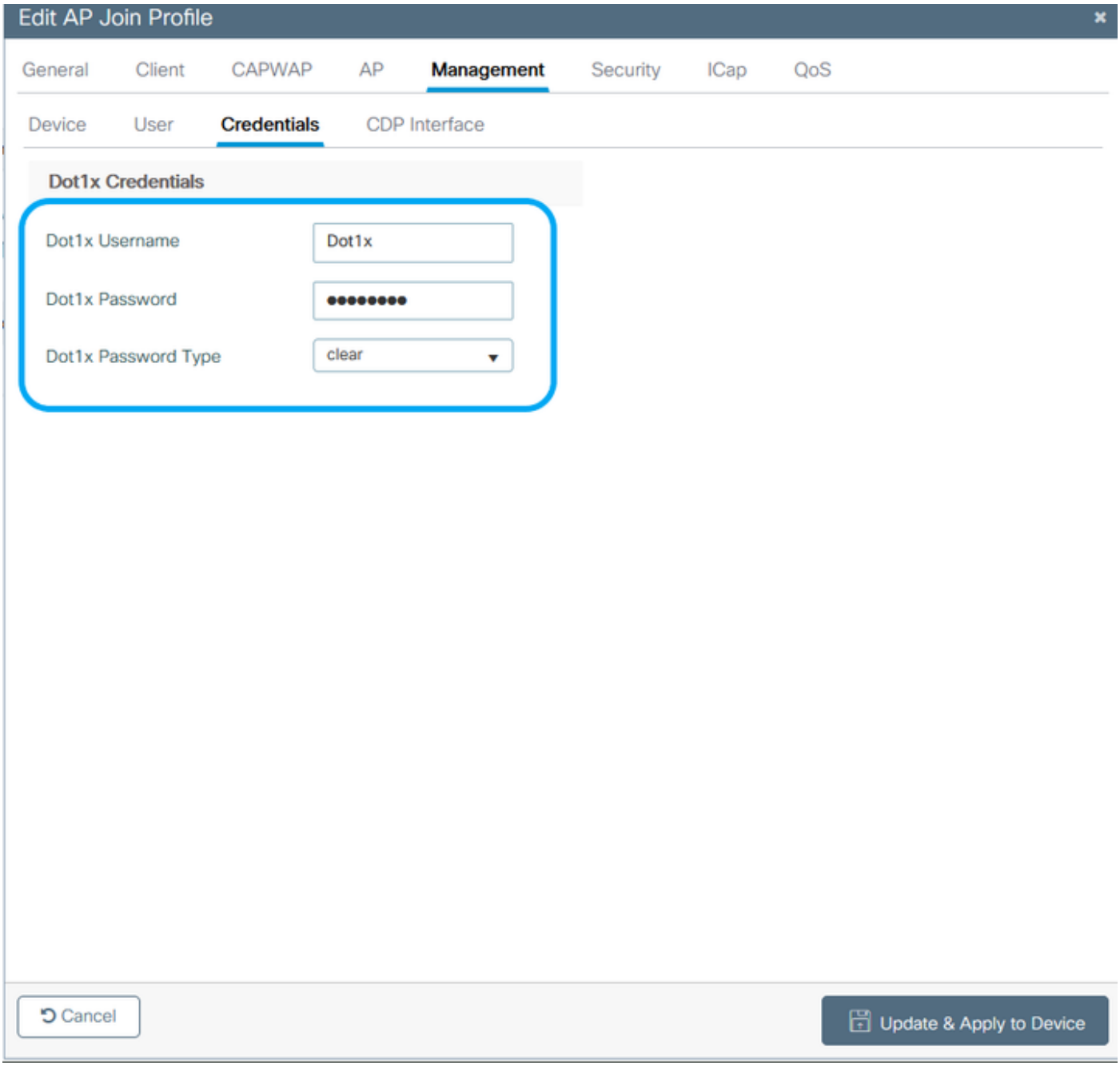


الخطوة 3. من القائمة المنسدلة نوع تفويض نقطة الوصول، أختر النوع إما CAPWAP DTLS أو CAPWAP DTLS+ > انقر فوق تحديث وتطبيق على الجهاز.



شكلت ال 802.1x username وكلمة:

الخطوة 1. من إدارة>بيانات الاعتماد>أدخل Dot1x اسم المستخدم وتفاصيل كلمة المرور > أختر نوع كلمة المرور 802.1x المناسب > انقر فوق تحديث وتطبيق على الجهاز



إذا لم تنضم نقطة الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بعد:

وحدة تحكم في نقطة الوصول (LAP) لتعيين بيانات الاعتماد واستخدام أوامر واجهة سطر الأوامر (CLI) التالية: (لنظام التشغيل Cisco IOS® APs و Cheetah)

CLI:

<#root>

LAP#

debug capwap console cli

LAP#

```
capwap ap dot1x username <username> password <password>
```

لمسح بيانات اعتماد dot1x على نقطة الوصول (إذا لزم الأمر)

لنقاط الوصول Cisco IOS® APs، بعد ذلك، قم بإعادة تحميل نقطة الوصول:

CLI:

```
<#root>

LAP#

clear capwap ap dot1x
```

لنقاط الوصول من Cisco CoS، بعد ذلك، قم بإعادة تحميل نقطة الوصول:

CLI:

```
<#root>

LAP#

capwap ap dot1x disable
```

تكوين المحول

قم بتمكين dot1x على المحول بشكل عام وأضف خادم ISE إلى المحول.

CLI:

```
<#root>

Enable


Configure terminal


aaa new-model
aaa authentication dot1x default group radius


aaa authorization network default group radius


dot1x system-auth-control
Radius-server host <ISE IP address> auth-port <port> acct-port <port>
```

```
key 7 <server key>
```

قم بتكوين منفذ محول AP.

CLI:

<#root>

```
configure terminal


interface GigabitEthernet</>
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge


end
```

إن يكون ال ap في Flex توصيل أسلوب، تحويل محلي، بعد ذلك تشكيل إضافي أن يكون جعلت على المفتاح قارن أن يسمح يتعدد {upper}mac address على الميناء، امب أن الزبون حركة مرور يكون أطلقت على ال ap مستوى :

<#root>

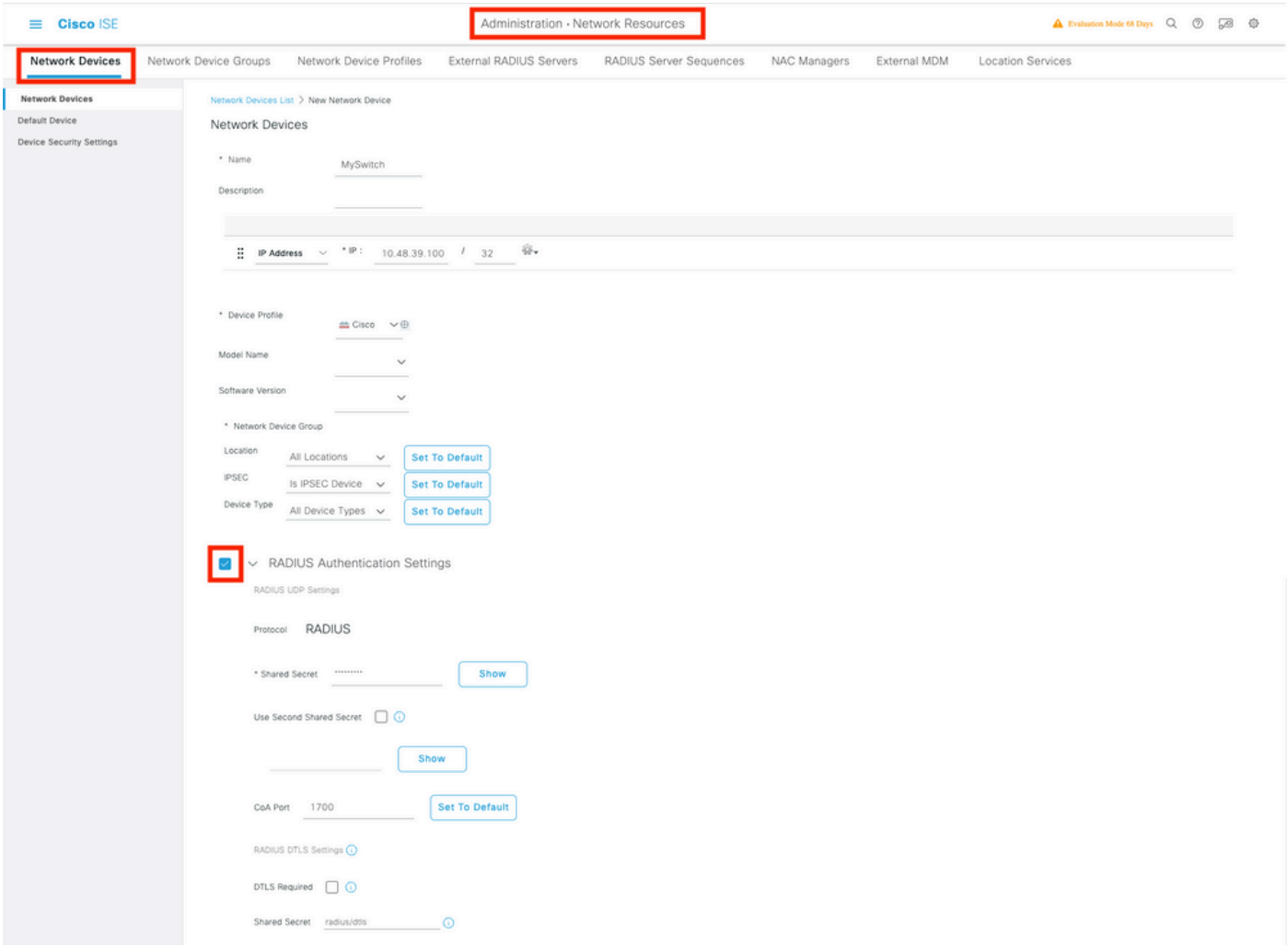
```
authentication host-mode multi-host
```

ملاحظة: تعني أن القارئ يلاحظ. تحتوي الملاحظات على اقتراحات مفيدة أو مراجع للمواد التي ال يغطيها المستند.

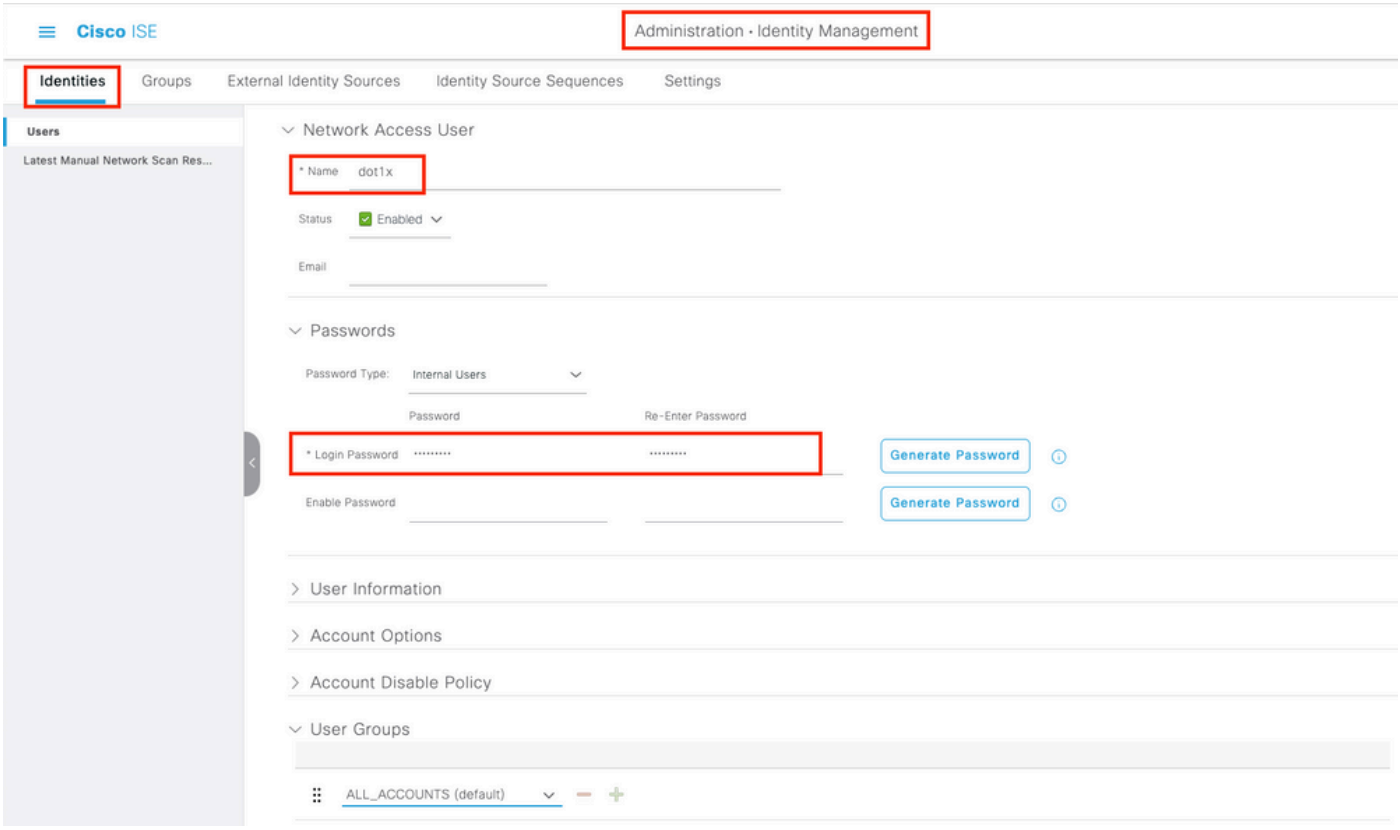
ملاحظة: يقوم وضع الأجهزة المضيفة المتعددة بمصادقة عنوان MAC الأول ثم يسمح بعدد غير محدود من عناوين MAC الأخرى. قم بتمكين وضع المضيف على منافذ المحول إذا تم تكوين نقطة الوصول المتصلة باستخدام وضع التحويل المحلي. هو يسمح الزبون حركة مرور رمي المفتاح ميناء. إذا كنت تريد مسار حركة مرور آمن، فقم بتمكين dot1x على الشبكة المحلية اللاسلكية (WLAN) لحماية بيانات العميل

تكوين خادم ISE

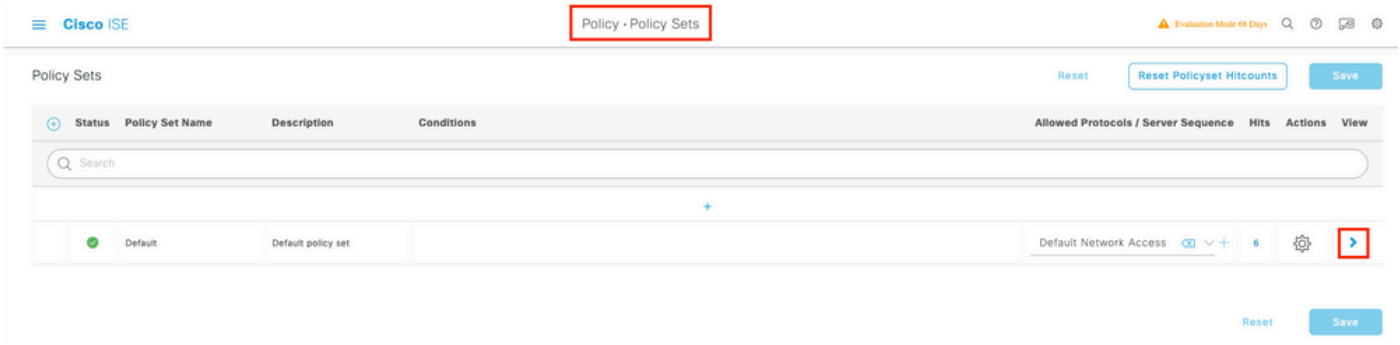
الخطوة 1. قم بإضافة المحول كجهاز شبكة على خادم ISE. انتقل إلى إدارة > موارد الشبكة > أجهزة الشبكة > انقر فوق إضافة > إدخال اسم الجهاز، عنوان IP، تمكين إعدادات مصادقة RADIUS، حدد قيمة سرية مشتركة، منفذ COA (أو تركه كقيمة افتراضية) > إرسال.



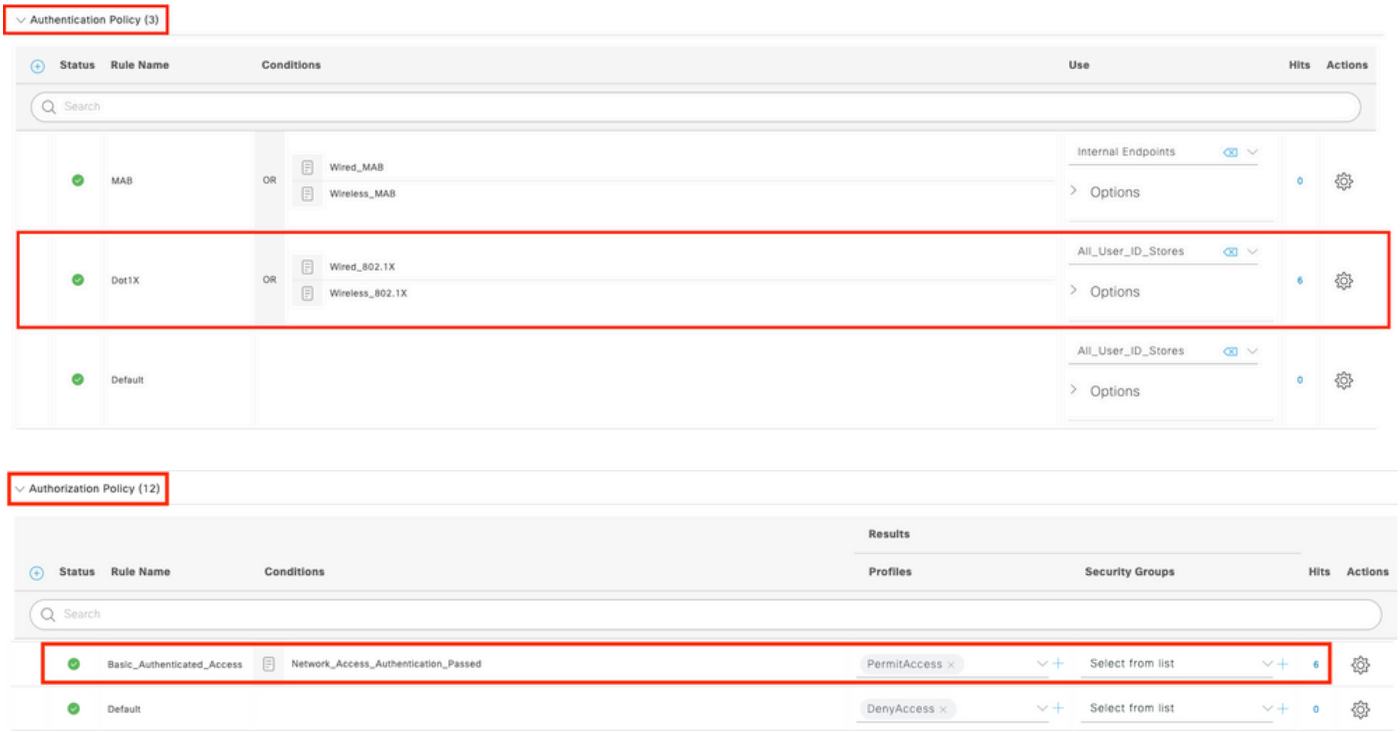
الخطوة 2. إضافة بيانات اعتماد نقطة الوصول إلى ISE. انتقل إلى إدارة > إدارة الهوية > هويات > مستخدمين وانقر فوق الزر إضافة لإضافة مستخدم. أدخل بيانات الاعتماد التي قمت بتكوينها على ملف تعريف انضمام نقطة الوصول على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). لاحظ أنه يتم وضع المستخدم في المجموعة الافتراضية هنا، ولكن يمكن ضبط هذا وفقا لمتطلباتك.



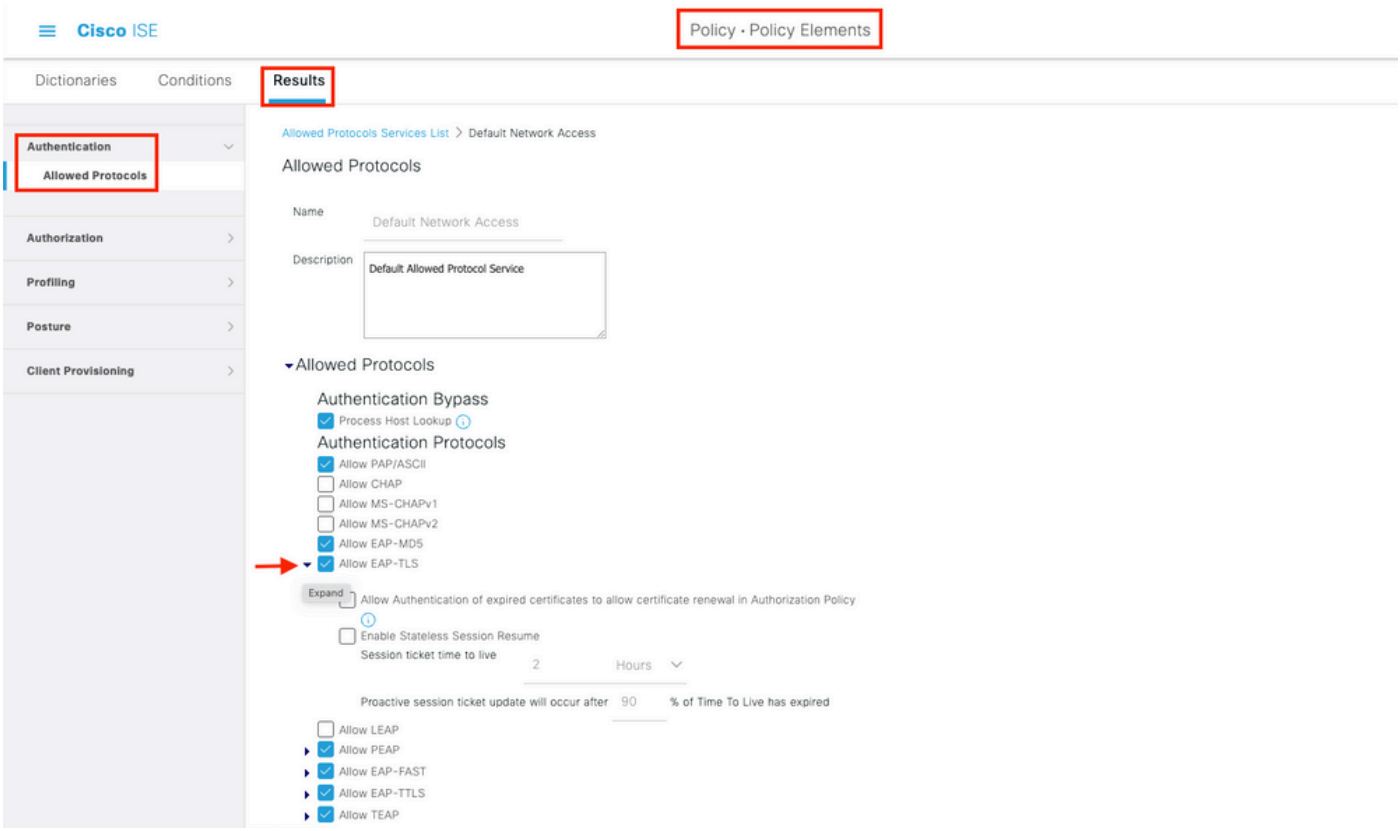
الخطوة 3. في ISE، قم بتكوين سياسة المصادقة ونهج التخويل. انتقل إلى النهج > مجموعات النهج وحدد مجموعة النهج للتكوين والسهم الأزرق الموجود على اليمين. في هذه الحالة، يتم إستخدام مجموعة النهج الافتراضية ولكن يمكن تخصيصها وفقا للمتطلبات.



ثم قم بتكوين نهج المصادقة ونهج التخويل. السياسات الموضحة هنا هي السياسات الافتراضية التي تم إنشاؤها على خادم ISE ولكن يمكن تكييفها وتخصيصها وفقا لمتطلباتك.
في هذا المثال، يمكن ترجمة التكوين إلى: "إذا تم إستخدام 802.1X سلكية وكان المستخدم معروفا على خادم ISE، فإننا نسمح بالوصول إلى المستخدمين الذين نجحت المصادقة بالنسبة لهم". يتم بعد ذلك تخويل نقطة الوصول مقابل خادم ISE.



الخطوة 4. تأكد من السماح ب EAP-FAST في البروتوكولات المسموح بها التي تقصير الوصول إلى الشبكة. انتقل إلى السياسة > عناصر السياسة > المصادقة > النتائج > البروتوكولات المسموح بها > الوصول الافتراضي إلى الشبكة> تمكين السماح ب EAP-TLS > حفظ.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

التحقق من نوع المصادقة

يعرض الأمر show معلومات المصادقة لتوصيف AP:

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

مثال:

```
9800WLC#show ap profile name default-ap-profile detailed
  AP Profile Name        : Dot1x
  …
  Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
  LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

دقق 802.1x على المفاتيح ميناء

يعرض الأمر show حالة المصادقة 802.1x على منفذ المحول:

CLI:

```
Switch# show dot1x all
```

مثال على الإخراج:

```
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for GigabitEthernet0/8
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

التحقق من مصادقة المنفذ أو عدم مصادقته

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

مثال على الإخراج:

```
Dot1x Info for GigabitEthernet0/8
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
EAP Method                = FAST
Supplicant                = f4db.e67e.dd16
Session ID                = 0A30279E00000BB7411A6BC4
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
ED
Auth BEND SM State = IDLE
```

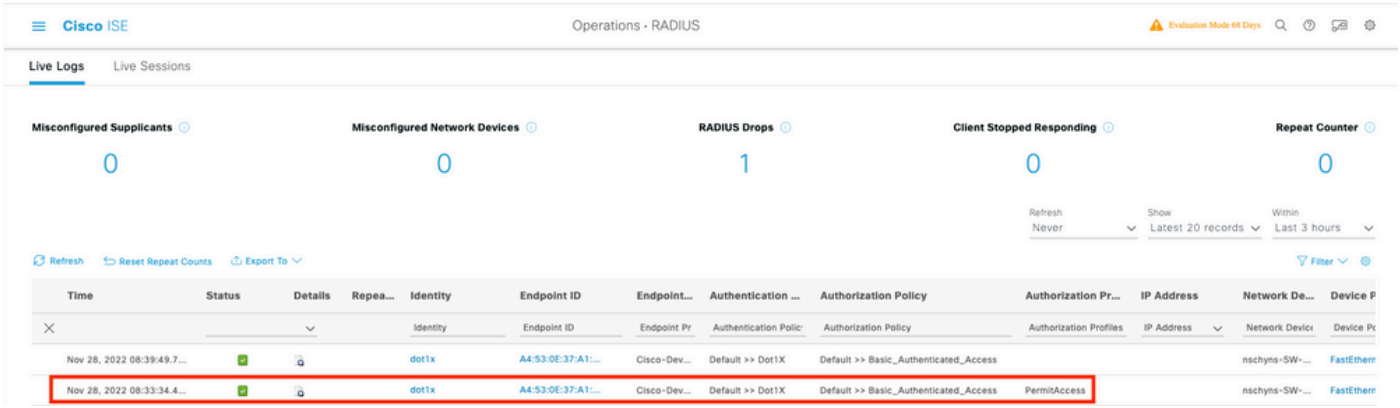
من واجهة سطر الأوامر:

```
Switch#show authentication sessions
```

مثال على الإخراج:

```
Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi0/8        f4db.e67e.dd16 dot1x   DATA    Auth      0A30279E00000BB7411A6BC4
```

في ISE، أختر عمليات > حوافز RADIUS وتأكد من نجاح المصادقة ودفع تصريف التخويل الصحيح.



استكشاف الأخطاء وإصلاحها

يوفر هذه القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. أدخل الأمر ping للتحقق من إمكانية الوصول إلى خادم ISE من المحول.
2. تأكد من تكوين المحول كعميل AAA على خادم ISE.
3. ضمنت أن ال يشارك سر ال نفس بين المفاتح و ال ISE نادل.
4. تحقق من تمكين EAP-FAST على خادم ISE.
5. تحقق مما إذا تم تكوين بيانات اعتماد 802.1x لنقطة الوصول في الوضع Lightweight (LAP) وما إذا كانت هي نفسها على خادم ISE.
   ملاحظة: اسم المستخدم وكلمة المرور متحساسان لحالة الأحرف.
6. إن يفشل صحة هويه، دخلت هذا أمر على المفاتح: debug dot1x وdebug صحة هويه.

لاحظ أن نقاط الوصول المستندة إلى Cisco IOS (802.11ac wave 1) ال تدعم TLS الإصدار 1.1 و 1.2. قد يتسبب ذلك في حدوث مشكلة إذا تم تكوين خادم ISE أو RADIUS للسماح فقط ل TLS 1.2 داخل مصادقة 802.1X.

المراجع

تكوين 802.1X على نقاط الوصول باستخدام PEAP و EAP-TLS

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).