تكوين المصادقة المحلية على وضع FlexConnect

المحتويات

المقدمة

معلومات أساسية

متطلبات وملاحظات عامة حول FlexConnect

التشعيب الأوضاع

السير الآلي للتوجيه

وضع FlexConnect على النطاق

دعم Wi-Fi 7 FlexConnect

سيناريوهات نشر FlexConnect

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

الرسم التخطيطي للشبكة

تكوين خوادم AAA

تكوين وضع FlexConnect على المواقع البعيدة

تكوين شبكة 802.1x WLAN باستخدام المصادقة المحلية باستخدام خادم RADIUS خارجي

تكوين ISE

تكوين PSK WLAN باستخدام المصادقة المحلية

التحقق من الصحة

استكشاف الأخطاء وإصلاحها

السيناريو المستقبلي

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية عمل المصادقة المحلية FlexConnect وكيفية تكوينها باستخدام وحدة التحكم اللاسلكية Cisco Catalyst 9800 Series (WLC)

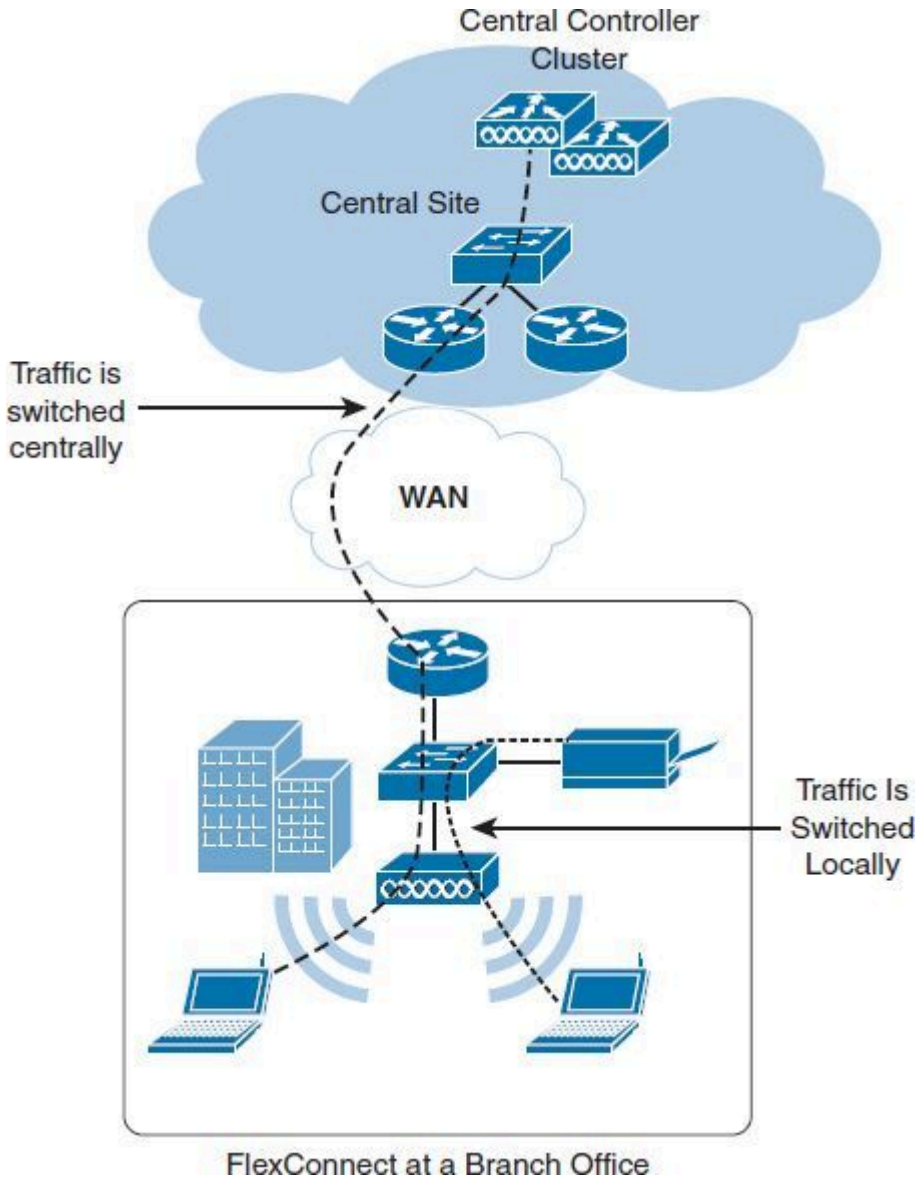
معلومات أساسية

متطلبات وملاحظات عامة حول FlexConnect

يمكن تقنية FlexConnect نقطة الوصول (AP) في المكاتب البعيدة أو الفرعية من

الاتصال بوحدة تحكم مركزية مع السماح في الوقت نفسه بالمعالجة المحلية لحركة مرور البيانات اللاسلكية. على عكس عمليات النشر اللاسلكية المركزية التقليدية حيث يتم إنشاء قنوات لجميع حركة مرور البيانات اللاسلكية إلى وحدة التحكم باستخدام FlexConnect تتيح تقنية CAPWAP (التحكم في نقاط الوصول اللاسلكية وإمدادها) — لنقطة الوصول مباشرة بواسطة معالجتها ومحليا حركة مرور البيانات تحويل إمكانية الفرعية. يوفر هذا التحويل المحلي لنقطة الوصول درجة من الاستقلالية، مما يمكن الخدمات الأساسية مثل الأمان والتجوال ووجودة الخدمة (QoS) من العمل بشكل مستقل عن وحدة التحكم.

على الرغم من أن FlexConnect مصمم بشكل أساسي لتحويل حركة مرور البيانات المحلية، إلا أنه يوفر أيضا المرونة لتبديل بعض SSIDs (معرف مجموعة الخدمات) مركزيا عند الحاجة. على سبيل المثال، إذا كان يجب أن تمر حركة مرور معينة عبر جدار حماية مركزي، يمكن إرسال SSIDs هذه مرة أخرى إلى وحدة التحكم من خلال CAPWAP للتحويل المركزي. وتتيح هذه القدرة المزدوجة لنقطة وصول واحدة بتقنية FlexConnect إمكانية دعم شبكات WLAN المحولة محليا ومركزيا (الشبكة المحلية اللاسلكية) في نفس الوقت.



واحد (SSID) هيئة تعريف مدعم تقنية FlexConnect في أحد الفروع محليا حيث تعمل على تبديل تعريف نقطة وصول تدعم يتم نشر

لي أوضاع التشغ

تعمل نقاط الوصول (AP) من FlexConnect في وضعين: الوضع المتصل والوضع المستقل.

- الوضع المتصل، تحتفظ نقطة الوصول باتصال نشط بوحدة التحكم عبر قناة تحكم CAPWAP.
- الوضع المستقل هو حالة إحتياطية تحدث عندما تفقد نقطة الوصول الاتصال بوحدة التحكم.

في الظروف العادية، تعمل نقاط الوصول (AP) طراز FlexConnect في الوضع المتصل، حيث تقوم وحدة التحكم بإدارة الخدمات الحيوية مثل المصادقة المركزية والتنميط للعملاء وإدارة الموارد اللاسلكية (RRM). بينما من المتوقع أن تظل نقطة الوصول في هذا الوضع في معظم الوقت، فإنها تتحول تلقائيا إلى الوضع المستقل إذا فقد الاتصال بوحدة التحكم. في الوضع المستقل، تستمر نقطة الوصول في العمل، حيث تعمل على تحويل حركة مرور البيانات محليا وتسمح للعملاء بالبقاء على اتصال دائم. تقوم نقاط الوصول بمصادقة العملاء بشكل مستقل دون إعادة توجيه طلبات المصادقة إلى وحدة تحكم مركزية. ومع ذلك، وظائف الإدارة الراديوية (RRM) - مثل إدارة الخدمات المعتمدة على وحدة التحكم لا تتوفر بشكل مؤقت بعض الخدمات المعتمدة على وحدة التحكم ومصادقة العميل المركزية.

على سبيل المثال، إذا أدى انقطاع شبكة واسعة النطاق (WAN) إلى قطع الاتصال بين نقطة الوصول ووحدة التحكم ولكن ظل الوصول إلى الإنترنت نشطا، فإن نقاط الوصول تنتقل إلى الوضع المستقل وتستمر في معالجة حركة مرور البيانات المحولة محليا دون انقطاع. ويظل العملاء الحاليون متصلين، ولكن العملاء الجدد الذين يحتاجون إلى مصادقة مركزية لا يستطيعون الانضمام إلى الشبكة - ما لم يتم تكوين المصادقة المحلية. يمكن إعداد نقاط الوصول FlexConnect APs لإجراء المصادقة المحلية أثناء حالات فشل شبكة الاتصال واسعة النطاق (WAN)، مما يضمن إستمرارية الخدمة حتى عندما تكون وحدة التحكم غير قابلة للوصول إليها.

في الوضع المستقل، لا تتوفر هذه المميزات لنقطة الوصول:

- مصادقة ويب العميل
- مصادقة الضيف (إعادة توجيه البوابة)
- أي SSIDs محولة مركزيا
- RRM
- IPv6 لوتوكول عبر برو الثالث المستوى من التنقل إمكانية

- تنميط أصلي
- تصنيف السياسة
- عبارة اكتشاف الخدمات
- تحديثات التكوين

للحصول على قائمة كاملة بالميزات وتكوينات شبكة WLAN المدعومة في الوضع المستقل (المصادقة المحلية)، راجع مصفوفة الميزات: مصفوفة ميزات نقاط الوصول اللاسلكية من Cisco

يتضمن سيناريو فشل FlexConnect الشائع فقدان كامل أو انخفاض كبير في شبكة الاتصال WAN، مما يعطل قناة التحكم في CAPWAP. عندما تفقد نقطة الوصول إمكانية الوصول إلى وحدة التحكم بسبب مشكل شبكة الاتصال واسعة النطاق (WAN)، فإنها تتحول على الفور إلى الوضع المستقل.

يتمثل الهدف الأساسي خلال عطل شبكة الاتصال واسعة النطاق (WAN) في إستعادة الاتصال بوحدة التحكم في أسرع وقت ممكن لاستئناف التشغيل الكامل.

عندما تدخل نقطة الوصول FlexConnect إلى الوضع المستقل بسبب فشل شبكة الاتصال واسعة النطاق (WAN)، يظل العملاء النشطون متصلين ويمكن أن يتجولوا بين نقاط الوصول ضمن عالمة المجال/الموقع لـ FlexConnect، ولكن التجوال بين عالمات المواقع المختلفة لـ FlexConnect قد يتطلب إعادة مصادقة كاملة. ومع ذلك، يتعذر على العملاء الجدد الذين يحاولون الانضمام إلى شبكة WLAN المحولة محليا المصادقة على خادم AAA (خادم المصادقة والتفويض والمحاسبة) في الموقع المركزي لأن يتعذر الوصول إليه.

التجوال الآمن السريع

توفر مصادقة EAP (بروتوكول المصادقة المتوسع) زمن وصول أعلى مقارنة بمصادقة PSK (مفتاح مشترك مسبقا) بسبب تبادل إطارات EAP مع خادم AAA. ومع ذلك، فإن مع التجوال الآمن السريع، يخضع العميل لمصادقة 802. 1X/EAP بالكامل أثناء اقترانه الأولي بالشبكة فقط. في الدرهات اللاحقة إلى نقاط الوصول المجاورة، يتم تجاوز تبادل EAP، تقريبا مصافحة الأطراف الأربعة فقط، والتي تكون أسرع بشكل ملحوظ لمنع أن تتضمن الميزة المدعومة من قبل عنصر خادم AAA. يوضح هذا الجدول مختلف طرق التجوال الآمن السريع المدعومة من قبل كل من عمليات النشر في التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 9800 وبرنامج FlexConnect.

الميزة	الوضع المحلي	تقنية FlexConnect (الوضع المتصل)	تقنية FlexConnect (الوضع المتصل)	تقنية FlexConnect (مستقل)

		المصادقة (المركزية)	المصادقة - المصادقة (المحلية)	
التخزين المؤقت للمفاتيح الخاص (SKC)	غير مدعوم	غير مدعوم	غير مدعوم	غير مدعوم
التخزين المؤقت للمفاتيح الانتهازي (OKC)	مدعوم	مدعوم	مدعوم	مدعوم (حتى تنتهي صلاحية جلسة عمل العميل)
إدارة المفاتيح المركزية من Cisco (CCKM)	مدعوم	مدعوم	مدعوم	غير مدعوم
FT-802. 11R/ Adaptive 11R (انتقال سريع) (عبر الهواء)	مدعوم	مدعوم	مدعوم	مدعوم (حتى تنتهي صلاحية جلسة عمل العميل)
FT-802. 11r/ Adaptive 11R (انتقال سريع) (عبر DS)	مدعوم	مدعوم	غير مدعوم	غير مدعوم

في الوضع المستقل، يعتمد التجوال السريع على بقاء مواد المفاتيح المخزنة مؤقتا، ال صالحة. عندما تنتهي صلاحية PMK (Pairwise Master Key)/جلسة العمل المخزنة مؤقتا، يمكن لنقطة الوصول الحصول على معلومات مفاتيح مستمدة من وحدة تحكم جديدة حتى تتم إستعادة اتصال وحدة التحكم.

وضع FlexConnect على النطاق

بدءا من برنامج Cisco IOS XE 17.8.1 وما بعده، تم زيادة سعة الموقع المزن لاستيعاب 300 عميل 802.1x و 3000 نقطة وصول.

يسمح نشر PMK لنقاط الوصول ضمن نفس موقع FlexConnect بمشاركة معلومات PMK، مما يقلل الحاجة إلى تبادل EAP كامل أثناء التجوال. لم يتم تمكين نشر PMK بشكل افتراضي.

أستخدم هذه الأوامر للتحقق من نشر PMK وتمكين PMK:

- إظهار الحالات اللاسلكية لنشر PMK
- نشر PMK

دعم Wi-Fi 7 FlexConnect

يلخص هذا الجدول ميزات FlexConnect المدعومة عبر عائلة نقطة الوصول CW917x Wi-Fi 7.

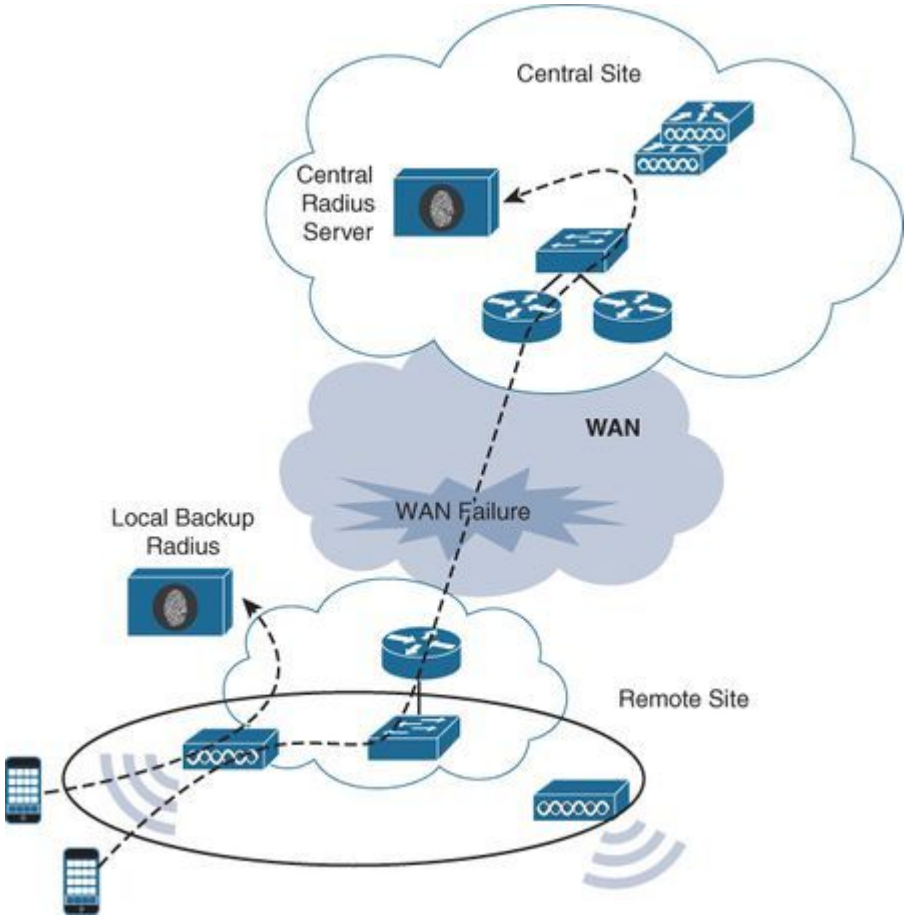
الميزة	الدعم
التحويل المحلي	مدعوم
تبديل مركزي	مدعوم
تخطيط WLAN-VLAN	مدعوم
المصادقة المحلية مع RADIUS الخارجي	مدعوم
WPA3-مؤسسي	مدعوم
التجوال السريع FT-802.11R	مدعوم
عملية الارتباط المتعدد (MLO)	مدعوم
المصادقة المحلية مع RADIUS الداخلي	غير مدعومة
WPA3-Enterprise-192	غير مدعومة

سيناريوهات مرونة FlexConnect

1. في إعداد مرونة N+1، تشترك وحدات التحكم النشطة المتعددة في وحدة تحكم مشتركة. عند اتصال وحدة تحكم أساسية دون اتصال، تتحول نقاط الوصول من FlexConnect APs على الفور إلى الوضع المستقل وتبدأ البحث عن وحدة التحكم في النسخ الاحتياطي. خلال فترة قطع الاتصال هذه، يتم قطع اتصال العملاء المحوليين مركزيا بنقاط الوصول. بمجرد أن تقوم نقاط الوصول بتحديد موقع وحدة التحكم في النسخ الاحتياطي ومزامنتها، يتم إعادة توصيل العملاء الذين يحتاجون إلى الوصول إلى SSIDs المحولة مركزيا. وفي الوقت نفسه، لا يزال العملاء الذين يتم تحويلهم محليا غير متأثرين ويواصلون العمل دون ملاحظة انقطاع الخدمة.
2. توفير خادم AAA إحتياطي في الموقع البعيد، والذي يمكن الوصول إليه بواسطة مجموعة FlexConnect. مع تمكين المصادقة المحلية، يتم إستخدام خادم RADIUS للنسخ الاحتياطي هذا فقط عندما تدخل نقاط الوصول في الوضع المستقل—حيث تظل غير نشطة بينما تكون نقاط الوصول في الوضع المتصل. عندما تستخدم نقاط الوصول FlexConnect خادم AAA للنسخ الاحتياطي المحلي للمصادقة، يتم توزيع مفاتيح المصادقة عبر جميع نقاط الوصول في مجموعة FlexConnect، تماما كما هي الحال

مع خادم AAA مركزي. وهذا يضمن إستمرارية تجول العملاء الجدد بسلاسة بين نقاط الوصول (AP) دون الحاجة إلى إعادة المصادقة، حتى عند إستخدام خادم RADIUS للنسخ الاحتياطي.

3. أي طريقة موجودة في مصفوفة المميزات لنقاط الوصول اللاسلكية من Cisco التي تتيح المصادقة المحلية.



يقوم العملاء بالمصادقة مقابل خادم AAA محلي للنسخ الاحتياطي عندما يصبح خادم AAA المركزي غير متاح بسبب فشل WAN

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

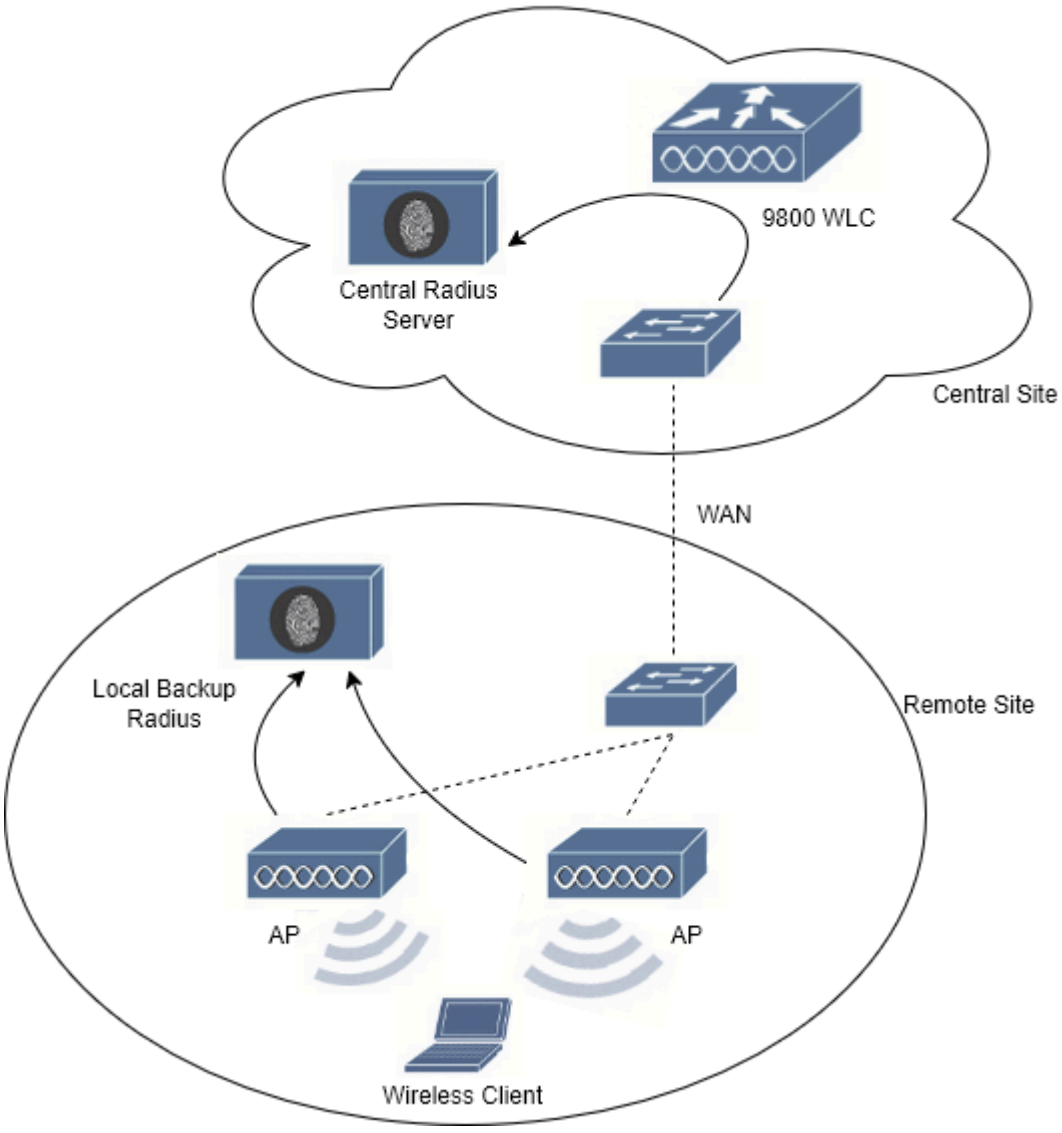
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم اللاسلكية Catalyst C9800-CL للسحابة مع برنامج Cisco IOS® XE Dublin، الإصدار 17.18.3
- نقطة وصول Catalyst CW9164I-ROW v17.18.3.18
- نقطة وصول Aironet® AIR-AP2802I-E-K9 v17.18.3.18
- 2 x Identity Services Engine v3.2.0.542

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.

التكوين

الرسم التخطيطي للشبكة



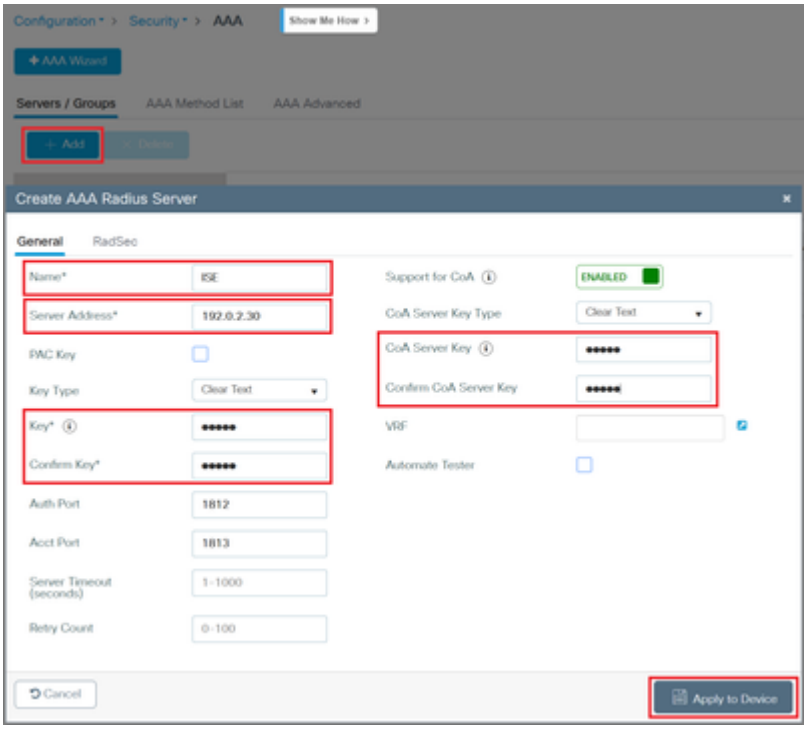
الرسم التخطيطي للشبكة

تكوين خوادم AAA

الخطوة 1. لتكوين شبكة محلية لاسلكية (WLAN) طراز 802.1x، يلزمك إنشاء مجموعة خوادم AAA على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 9800.

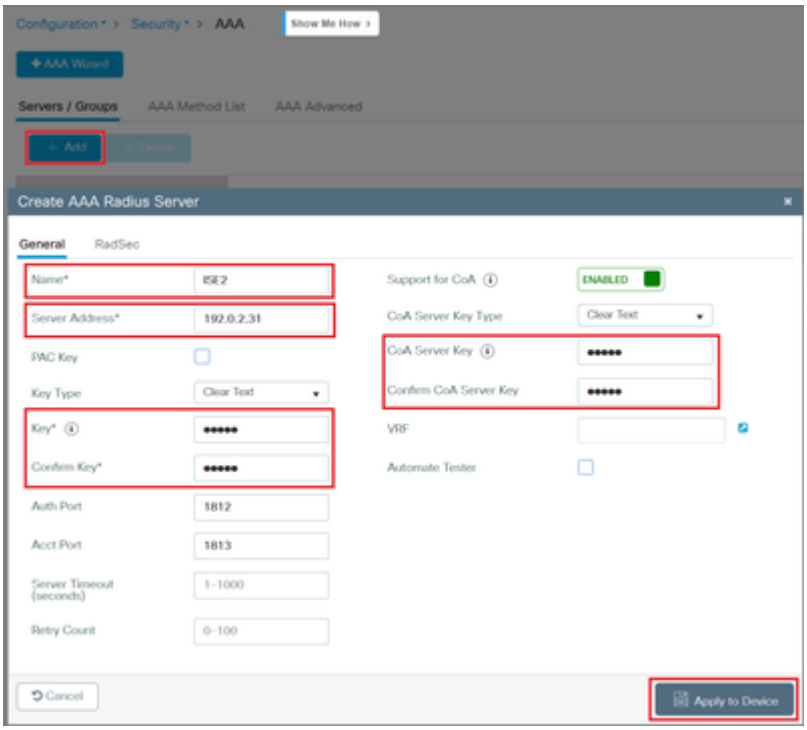
قم بإنشاء خادم AAA لكل موقع - واحد على الموقع المركزي والآخر على الموقع البعيد.

انتقل إلى التكوين > الأمان > AAA > الخادم/المجموعات > الخوادم وحدد +إضافة. قم بإعطاء تغيير CoA (تمكين دعم CoA) والمفاتيح (مفاتيح التأكيد) وعنوان IP الخاص به واسم للخادم وإدخال مفاتيح خادم CoA (وتأكيد مفاتيح خادم CoA). يجب أن تكون المفاتيح واحدة.



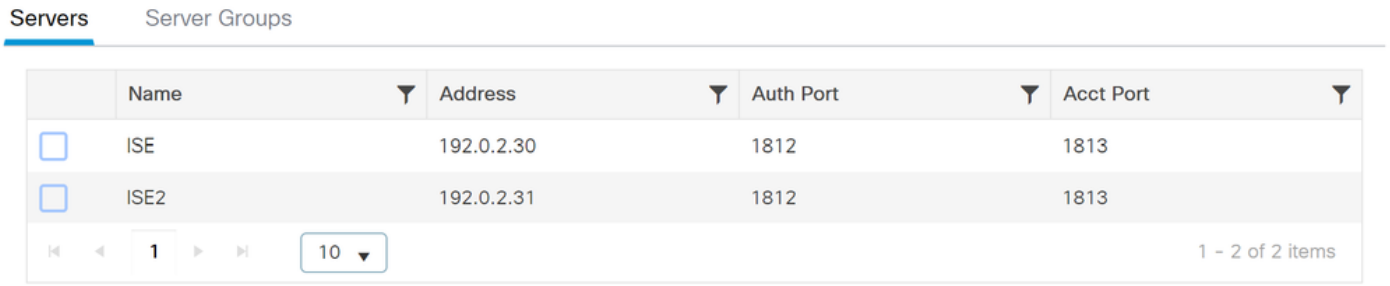
انقر فوق تطبيق على الجهاز.

الخطوة 2. قم بإنشاء خادم AAA الآخر:

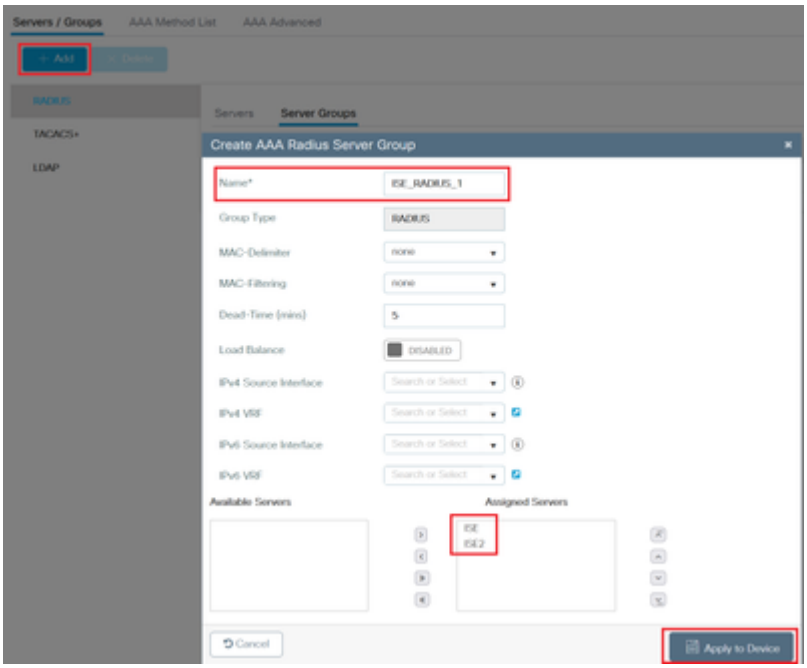


انقر فوق تطبيق على الجهاز.

يمكنك الآن عرض خوادم AAA التي تم تكوينها:

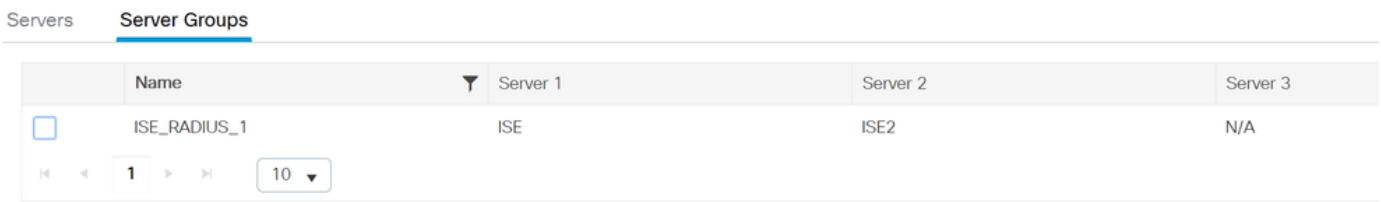


الخطوة 3. انتقل إلى التكوين > الأمان > AAA > الخادم/المجموعات > مجموعات الخوادم وحدد +إضافة. قم بإعطاء اسم لخادم المجموعة، وحدد خوادم AAA التي تم إنشاؤها مسبقا إلى العمود الخوادم المعينة:



انقر فوق تطبيق على الجهاز.

يمكنك حينئذ رؤية مجموعة خوادم AAA التي تم تكوينها:



CLI:

```
aaa new-model
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

تكوين وضع FlexConnect على الموقع البعيد

الخطوة 1. تتمثل الخطوة الأولى في تكوين FlexConnect على الموقع البعيد.

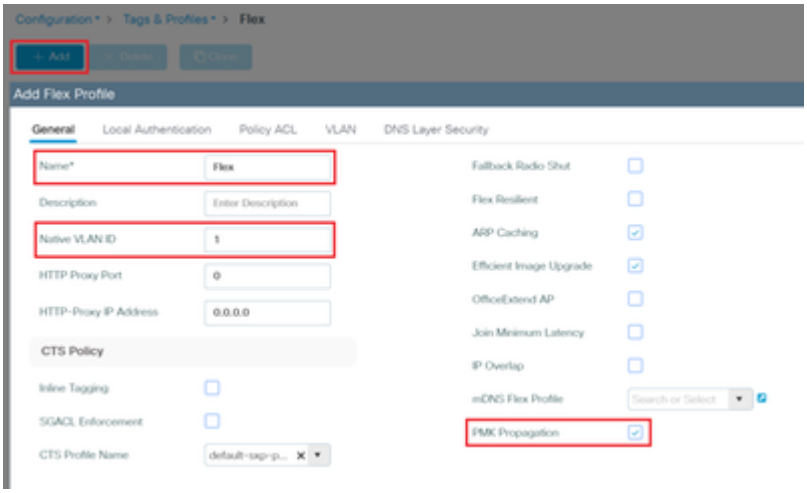
أستخدم هذا الدليل لتغيير وضع نقاط الوصول (APs) إلى Flex: فهم FlexConnect على وحدة التحكم اللاسلكية Catalyst 9800.

تستخدم نقاط الوصول في هذا الدليل/المختبر نفس ملف تخصيص Flex.

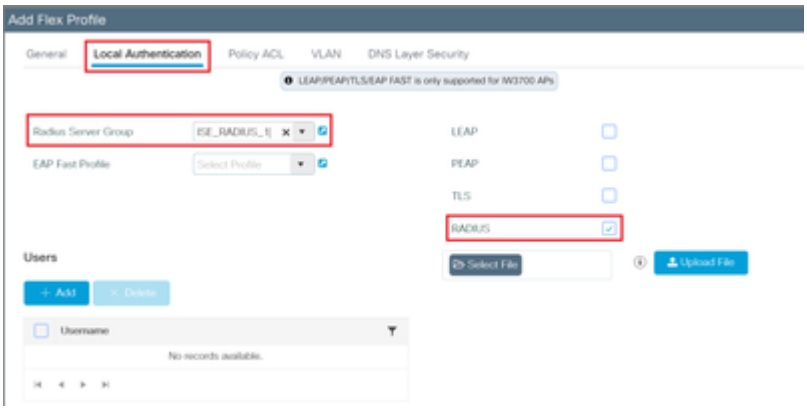
الخطوة 2. انتقل إلى التكوين > العلامات وملفات التعريف > Flex.

قم بإنشاء اسم ملف تعريف مرن جديد باستخدام +إضافة. على علامة التبويب عام أضف اسما على ملف التعريف، أدخل معرف شبكة VLAN الأصلية (شبكة المنطقة المحلية الظاهرية)، وقم بتمكين نشر PMK.

يمكنك نشر PMK لتسهيل التجوال السلس للعملاء اللاسلكيين من خلال مشاركة معلومات PMK بين AP داخل موقع واحد.

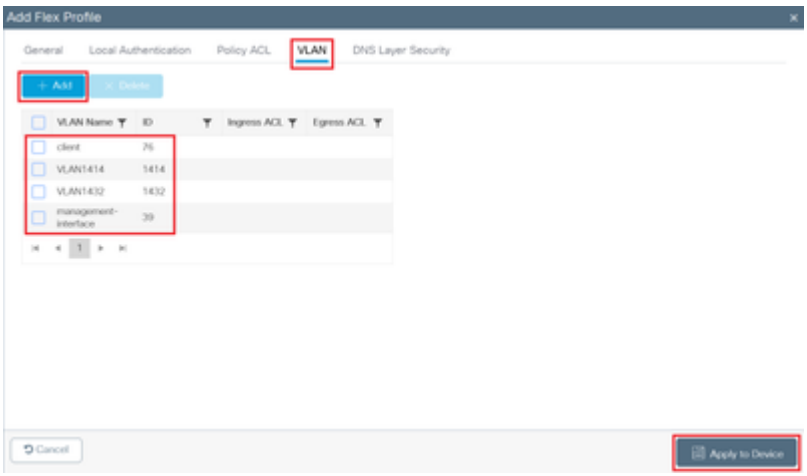


الخطوة 3. بالنسبة للشبكة المحلية اللاسلكية (WLAN) المتوافقة مع معيار 802. 1x، تكوين RADIUS: حدد على علامة التبويب المصادقة المحلية مجموعة خوادم RADIUS



تلميح: بالنسبة للشبكة المحلية اللاسلكية (WLAN) الخاصة بمنفذ PSK، لا تحتاج إلى إضافة أي شيء على علامة التبويب هذه.

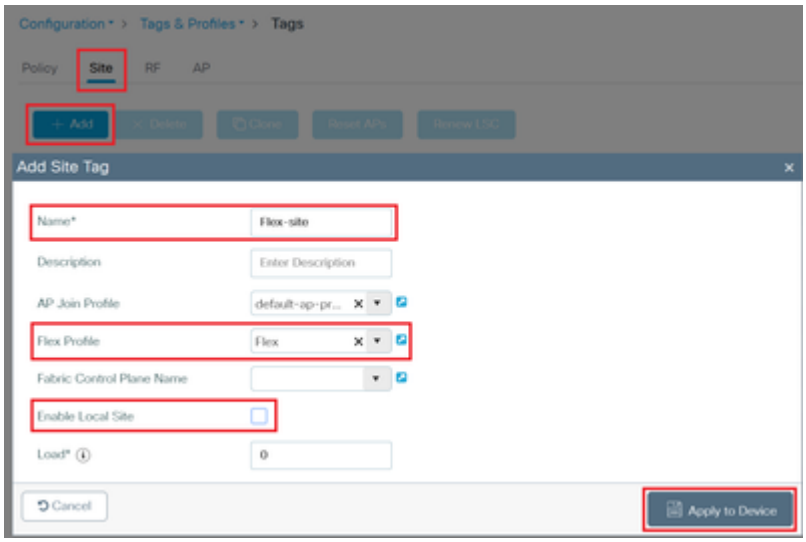
الخطوة 4. على علامة التبويب VLAN أضف جميع شبكات VLAN التي يتم إستخدامها من قبل العملاء، نقاط الوصول، وخادم RADIUS. تأكد من عمل المراسلات الصحيحة لكل اسم VLAN إلى معرف VLAN الصحيح:



في النهاية انقر فوق تحديث وتطبيق على الجهاز.

الخطوة 5. انتقل إلى التكوين > العلامات وملفات التعريف > علامات التمييز > الموقع وحدد +إضافة.

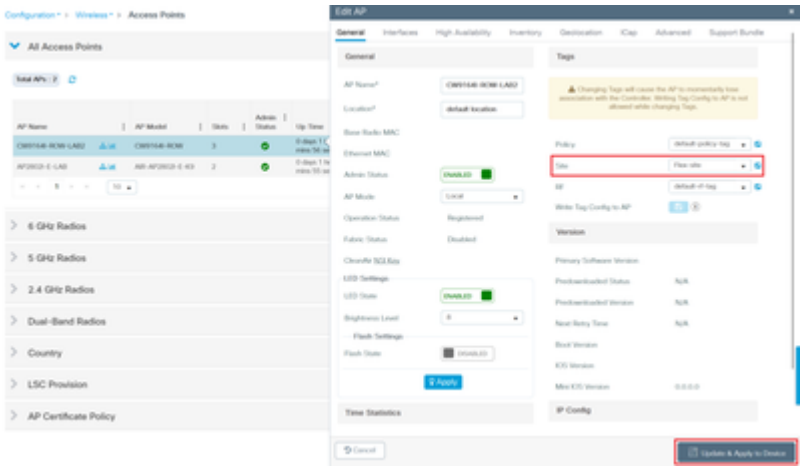
قم بإنشاء علامة الموقع باستخدام ملف تعريف Flex الذي تم إنشاؤه مسبقا. أعطه اسما، وحدد ملف تعريف Flex الأيمن، وقم بتعطيل تمكين الموقع المحلي. تأكد من أن ملف تعريف ربط نقطة الوصول هو الصحيح.



انقر فوق تطبيق على الجهاز.

الخطوة 6. انتقل إلى التكوين > لاسلكي > نقاط الوصول.

حدد نقطة الوصول الخاصة بك، في عام > علامات التمييز قم بتغيير علامة الموقع إلى العلامة التي تم تكوينها مسبقا:



انقر على تحديث وتطبيق على الجهاز.

تنفصل نقطة الوصول عن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وتعيد الانضمام باستخدام وضع نقطة الوصول (AP) المرنة.

على نفس الصفحة، عندما تعيد ربط نقطة الوصول، يمكنك التحقق من وضع نقطة الوصول في وضع نقطة الوصول للعمود.

إذا قمت بتحديد نقطة الوصول، فإنها تعرض علامة الموقع الجديدة:



CLI:

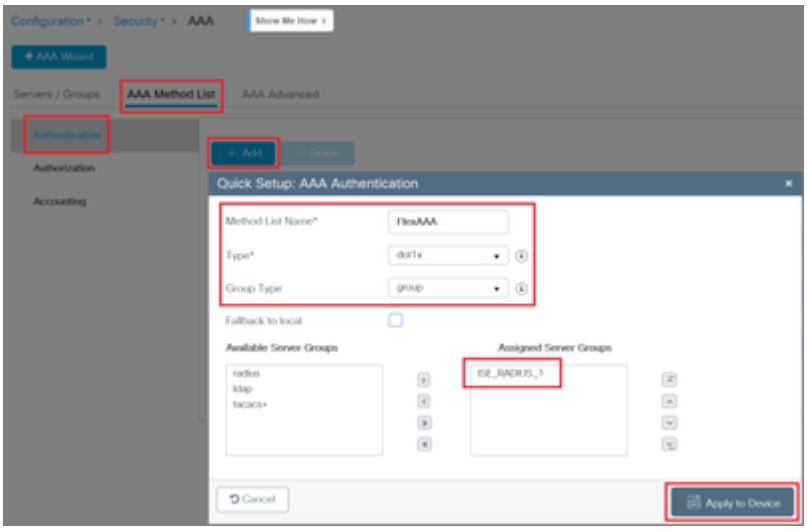
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

قم بتكوين شبكة 802.1x WLAN باستخدام المصادقة المحلية باستخدام RADIUS خارجي

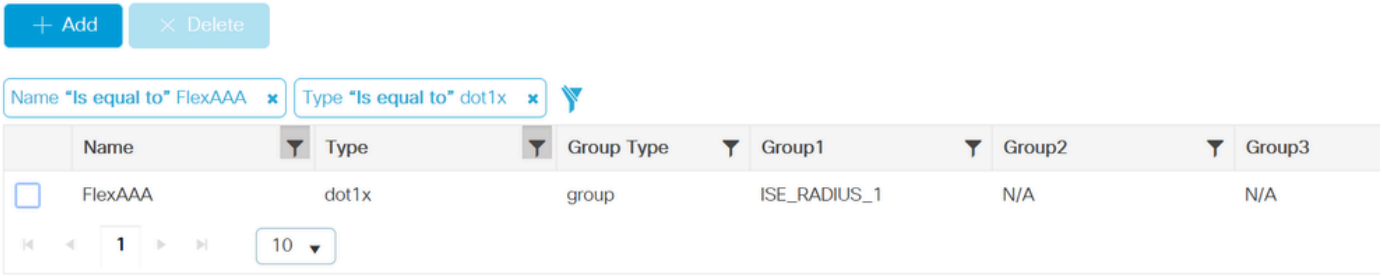
الخطوة 1. قم بإنشاء قائمة أساليب المصادقة.

انتقل إلى التكوين > الأمان > AAA، في قائمة طرق AAA > عامة تبويب المصادقة.

حدد +إضافة، وقم بتسمية اسم السرد قائمة الطرق، وحدد dot1x كنوع، وحدد مجموعة كنوع مجموعة، وقم بتعيين مجموعة خوادم AAA على عمود مجموعات الخوادم المعينة:



يمكنك الآن الاطلاع على قائمة أساليب AAA التي تم إنشاؤها:



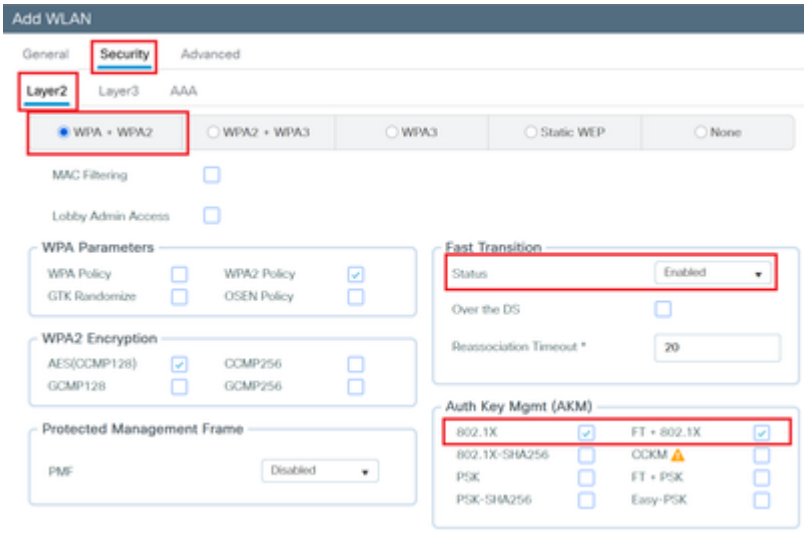
الخطوة 2. إنشاء شبكة WLAN.

انتقل إلى التكوين > العلامات وملفات التعريف > شبكات WLAN، حدد +إضافة.

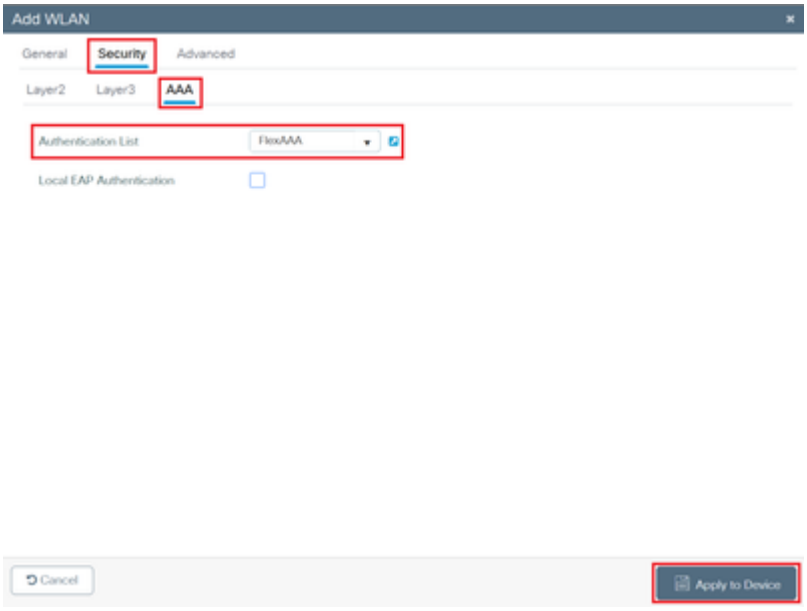
في علامة العلامة قم بإنشاء اسم على اسم التوصيف، SSID، وحالة التمكين:



الخطوة 3. انتقل إلى الأمان > علامة التبويب الطبقة 2، حدد WPA+WPA2 (وصول Wi-Fi المحمي)، انتقال سريع عند تمكينه، إدارة مفتاح المصادقة 802. 1X و FT+802. 1X:



الخطوة 4. انتقل إلى الأمان > علامة التبويب AAA، في قائمة قائمة المصادقة المنسدلة حدد القائمة التي تم إنشاؤها مسبقا:



انقر على تحديث وتطبيق على الجهاز.

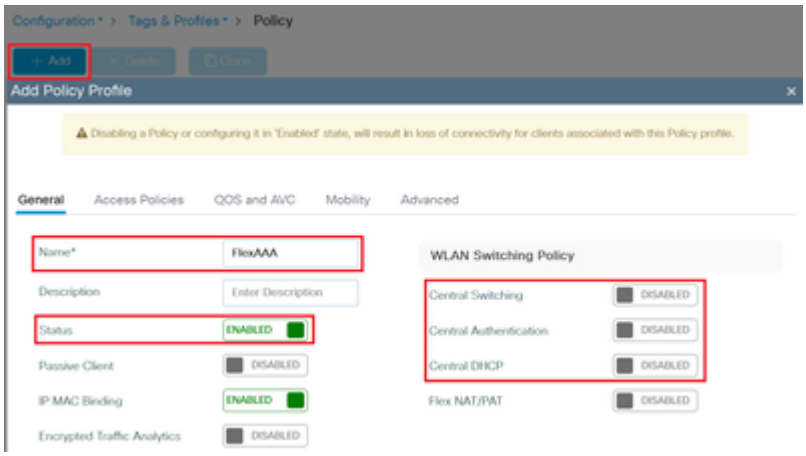
أنت بعد ذلك ترى ال WLAN يخلق:



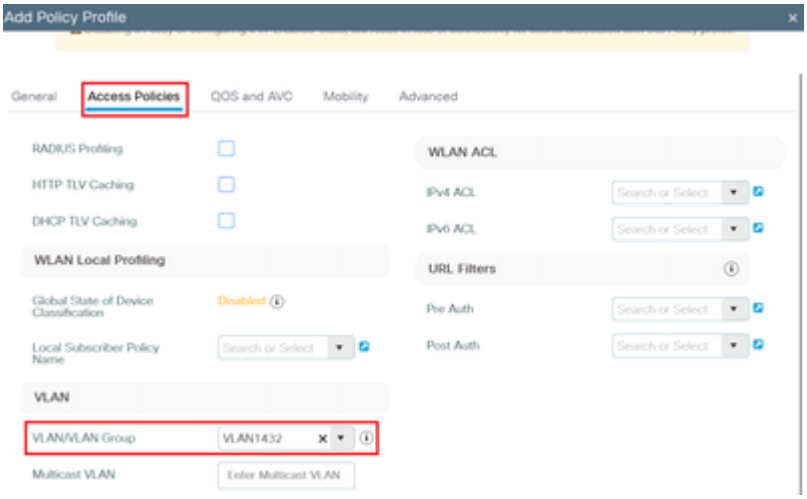
الخطوة 5. إنشاء ملف تعريف السياسة.

انتقل إلى التكوين > العلامات وملفات التعريف > السياسة.

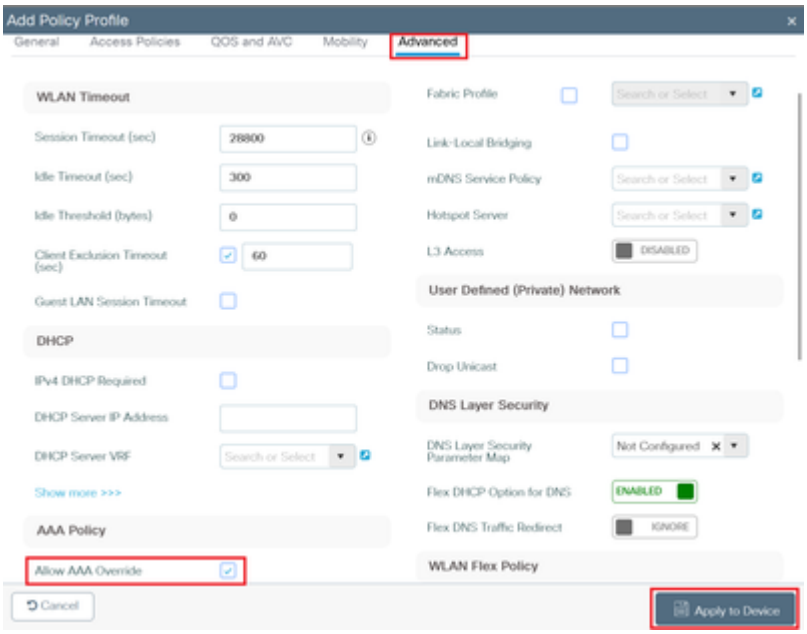
حدد +إضافة وفي علامة التبويب عام امنح اسم لملف تعريف السياسة، وقم بتمكين الحالة، وتعطيل التحويل المركزي والمصادقة المركزية و DHCP المركزي (بروتوكول تكوين المضيف الديناميكي):



الخطوة 6. انتقل إلى سياسات الوصول إلى علامة التبويب، حدد شبكة VLAN:

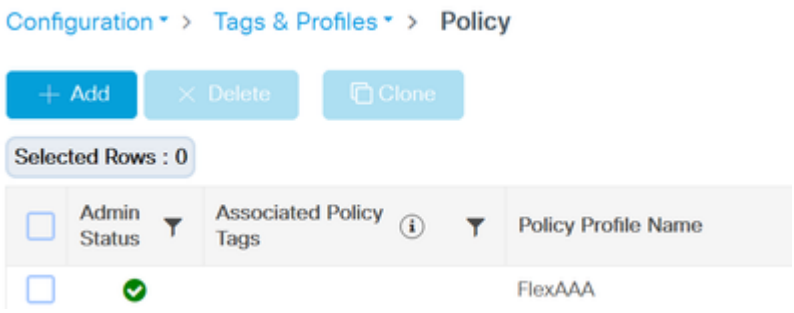


الخطوة 7. انتقل إلى علامة التبويب خيارات متقدمة، وقم بتمكين السماح بتجاوز AAA.:



انقر فوق تحديث وتطبيق على الجهاز.

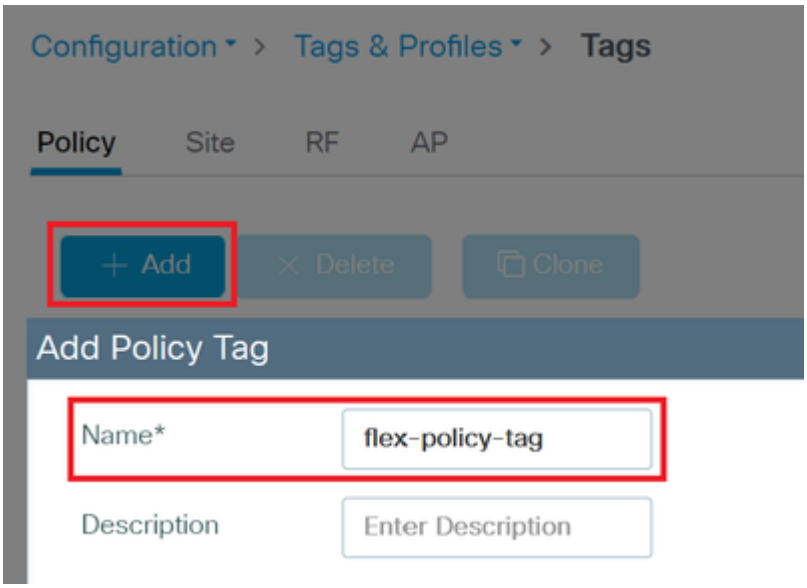
يمكنك رؤية ملف تعريف النهج في القائمة:



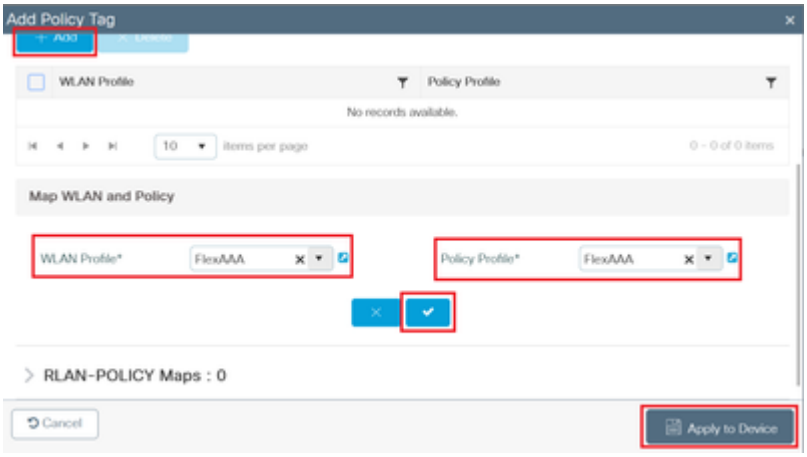
الخطوة 8. إنشاء علامة نهج.

انتقل إلى التكوين > علامات تمييز وتوصيفات > علامات تمييز

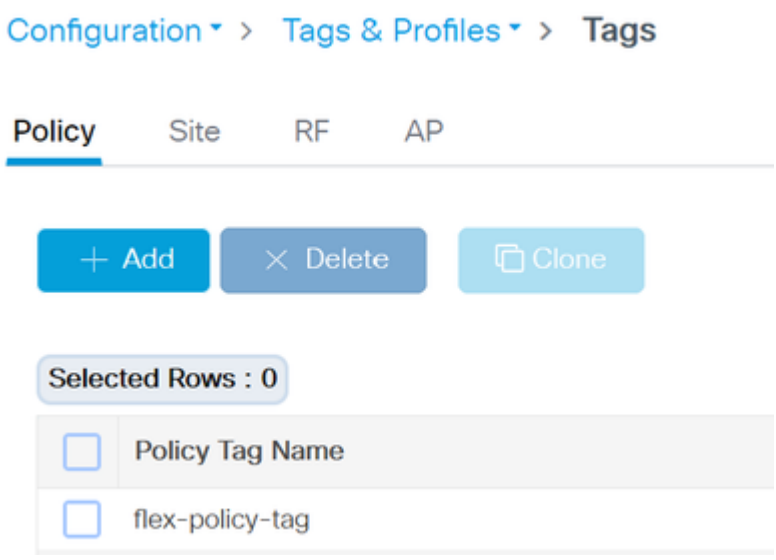
في علامة التبويب نهج، حدد +إضافة. إعطاء اسم لعلامة النهج:



قم بالتمرير لأسفل وحدد +إضافة ضمن خرائط نهج WLAN. في ملف تعريف WLAN، حدد شبكة WLAN التي تم إنشاؤها مسبقا من القائمة المنسدلة. في "ملف تعريف النهج" حدد "ملف تعريف النهج" الذي تم إنشاؤه مسبقا من القائمة المنسدلة. انقر فوق زر التحقق، ثم فوق تطبيق على الجهاز:

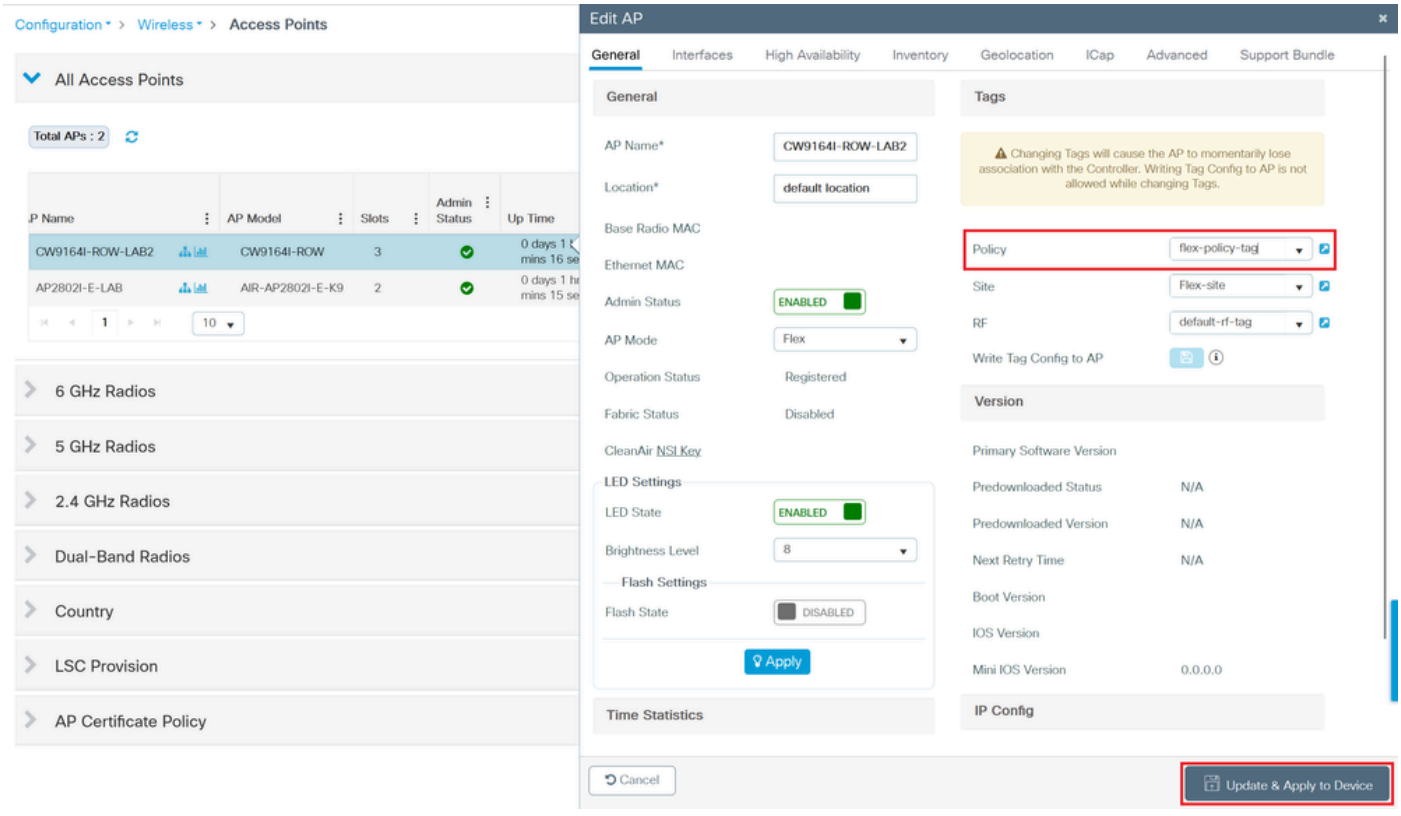


يمكنك رؤية علامة النهج في القائمة:



الخطوة 9. قم بتعيين علامة النهج على علامة APs.

انتقل إلى التكوين > لاسلكي > نقاط الوصول. حدد نقطة الوصول لتغيير العلامة.

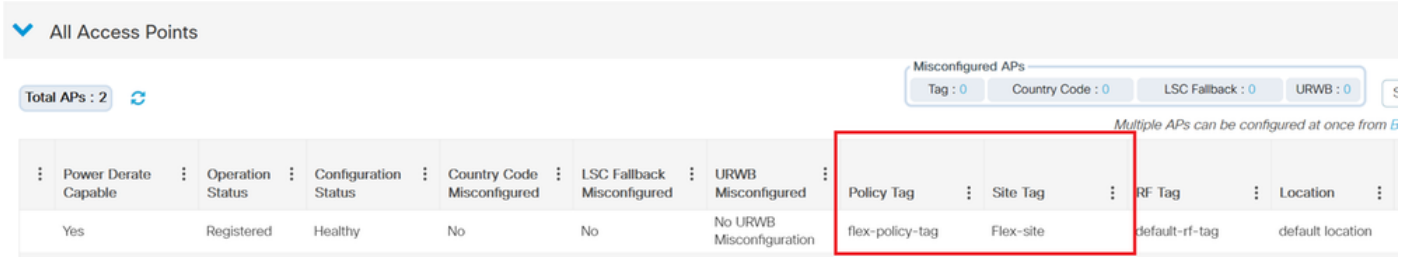


انقر على تحديث وتطبيق على الجهاز.

تنفصل نقطة الوصول وتتحد مرة أخرى بعلامة النهج الجديدة.

عندما تنضم نقطة الوصول للخلف، يمكنك التحقق من قائمة نقاط الوصول، والتأكيد

على أن نقطة الوصول في الوضع المرن، والعلامات المعينة:



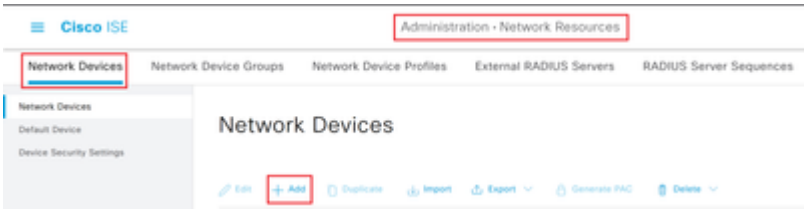
CLI:

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 security ft
 security wpa akm ft dot1x
 security dot1x authentication-list FlexAAA
 no shutdown
!
wireless profile policy FlexAAA
 aaa-override
 no central authentication
 no central dhcp
 no central switching
 vlan VLAN1432
 no shutdown
!
wireless tag policy flex-policy-tag
 wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
 policy-tag flex-policy-tag
 site-tag Flex-site
 rf-tag default-rf-tag
```

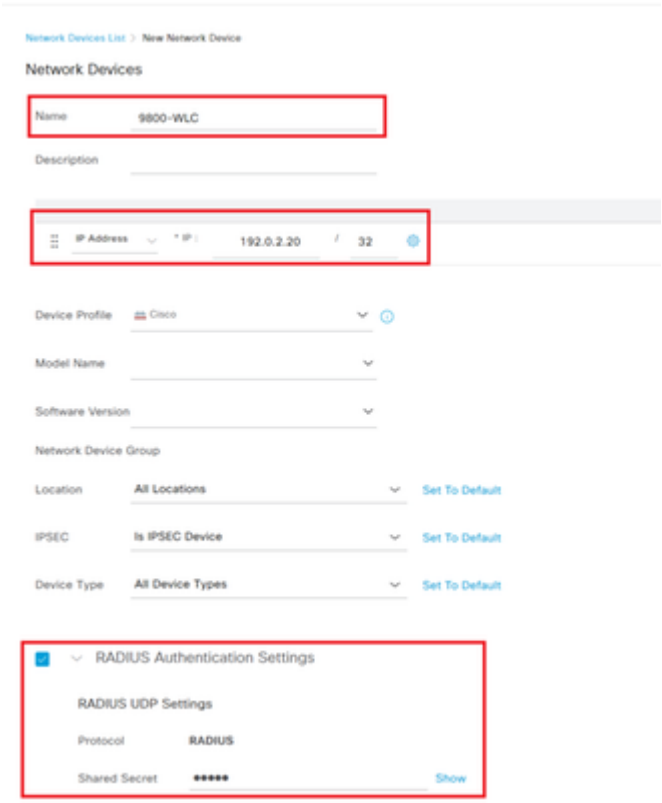
تكوين ISE

أنت تحتاج الآن إلى تكوين ISE ليكون قادرا على مصادقة العملاء عندما يكونون في المصادقة المحلية.

الخطوة 1.انتقل إلى إدارة > موارد الشبكة > أجهزة الشبكة. تحديد +إضافة.



الخطوة 2. أضف عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 9800. منح اسما، وإضافة عنوان IP الخاص به، وتمكين إعدادات مصادقة RADIUS، وإضافة المفتاح السري المشترك. يجب أن يكون هذا المفتاح هو المفتاح نفسه الذي قمت بتكوينه مسبقا عند إنشاء خوادم AAA على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 9800.



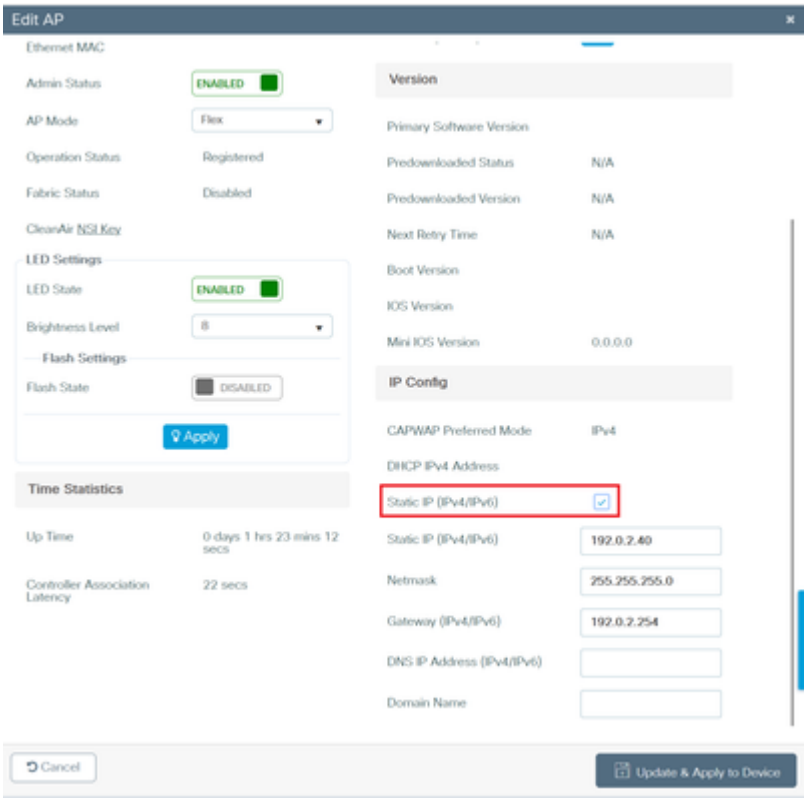
في أسفل الزاوية اليمنى، انقر على حفظ.

الخطوة 3. نحتاج إلى إضافة نقاط الوصول في قائمة أجهزة الشبكة، لكي تتمكن من العمل كموجهات/موجهات AAA عندما يقفد الموقع البعيد إرتباط شبكة WAN (وعندما تنتقل نقاط الوصول إلى الوضع المستقل).

انتقل إلى التكوين > السلكي > نقاط الوصول على واجهة المستخدم الرسومية (GUI) الخاصة بوحدة تحكم الشبكة المحلية اللاسلكية (WLC) طراز 9800 واحذف علما بكل عنوان من عناوين IP لنقطة الوصول.

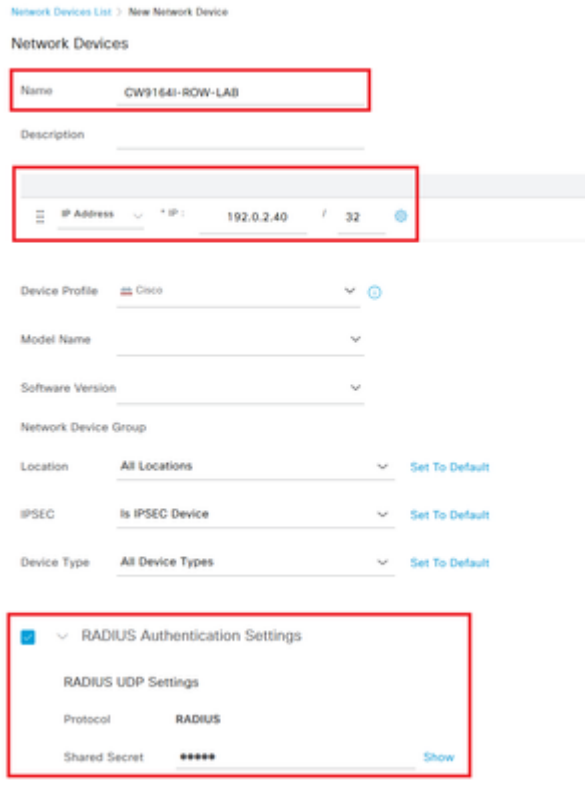
ملاحظة: قم بتكوين عنوان IP لكل نقطة وصول مرنة إلى وضع ثابت. عندما تفقد نقاط الوصول الاتصال وتستعيد الاتصال بـ 9800 WLC، فإنها يمكن أن تعود بعنوان IP مختلف من DHCP، وبالتالي تفقد الاتصال مع ISE.

تمكين IP الثابت (IPv4/IPv6). انقر فوق تحديث وتطبيق على الجهاز:



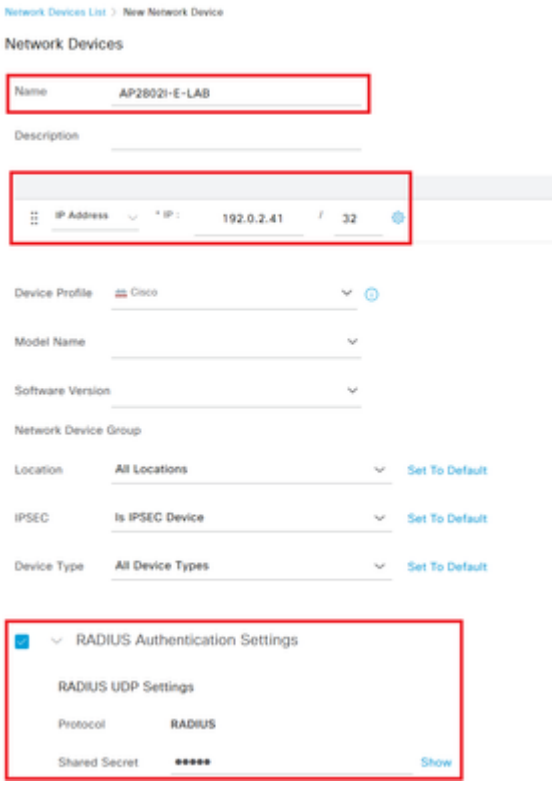
الخطوة 4. ارجع إلى ISE، انتقل إلى الإدارة > موارد الشبكة > أجهزة الشبكة. تحديد +إضافة.

قم بإضافة نقاط الوصول الخاصة بك كأجهزة شبكة، ذات التكوين نفسه الخاص ب 9800 WLC:



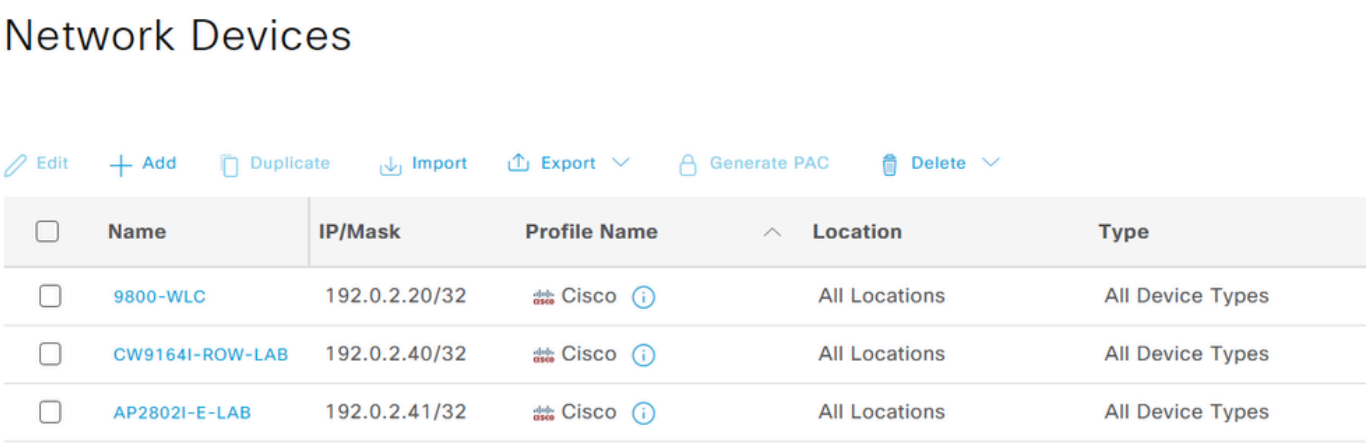
في أسفل الزاوية اليمنى، انقر على حفظ.

بالنسبة لنقطة الوصول الثانية:



في أسفل الزاوية اليمنى، انقر على حفظ.

يمكنك الاطلاع على قائمة أجهزة الشبكة التالية:



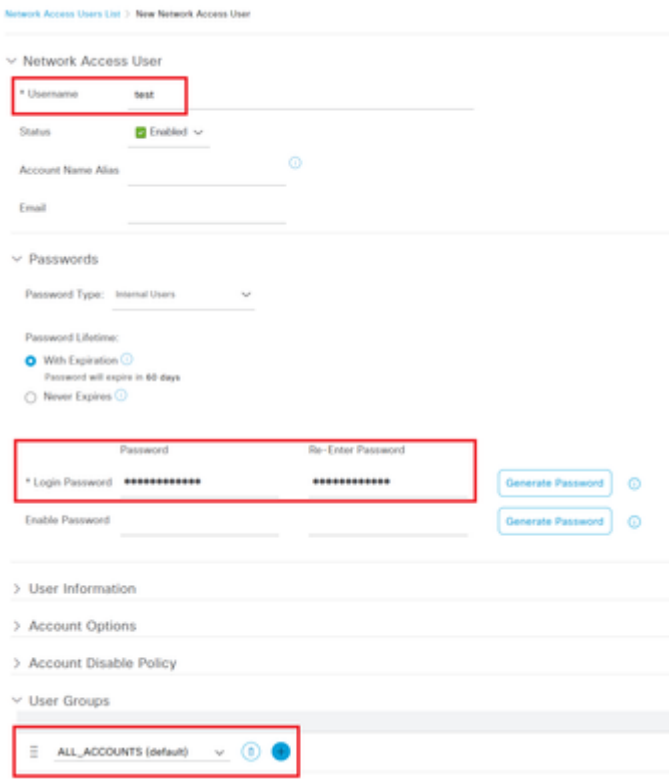
إذا كانت نقاط الوصول في نطاقات IP المتصلة، فيمكنك إستخدام ميزة القناع لتكوين إدخال واحد يحدد السر المشترك لمجموعة كاملة (إن لم يكن كلها) من نقاط الوصول. ال توجد

حاجة فعلية لتكوين جهاز شبكة واحد لكل نقطة وصول في ISE. لاحظ مع ذلك، أنه باستخدام أحرف البدل والأقنعة، تترك مساحة للجهاز المخادع لمحاولة العمل كموجه لـ ISE.

الخطوة 5. انتقل إلى إدارة > إدارة الهوية > الهويات، في علامة التبويب مستخدمون، وقم بإنشاء مستخدم لمصادقة 802.1x. تحديد +إضافة:

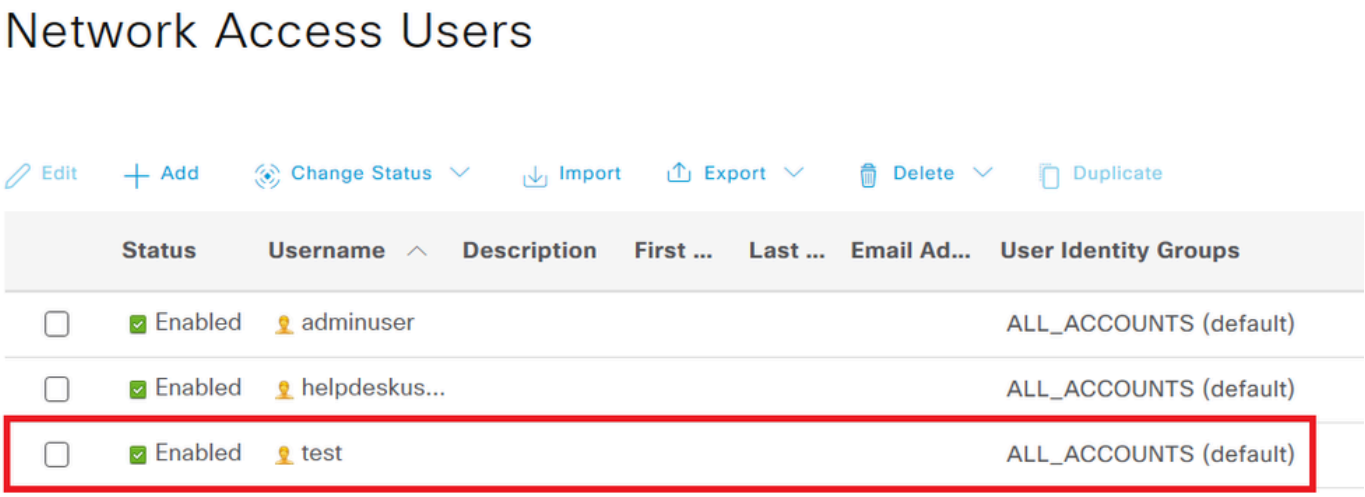


قم بإنشاء اسم مستخدم وكلمة مرور (واكتب نفس كلمة المرور على إعادة إدخال كلمة المرور) وحدد ALL_ACCOUNTS (الافتراضي) من القائمة المنسدلة لمجموعات المستخدمين:



في أسفل الزاوية اليمنى، انقر على إرسال.

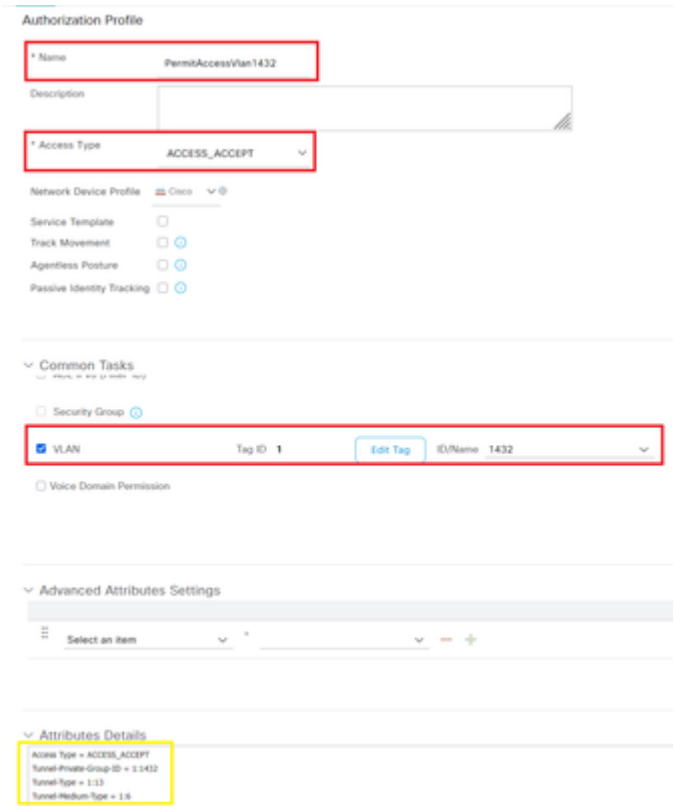
يمكنك الاطلاع على المستخدم في قائمة مستخدمي Network Access:



الخطوة 6. انتقل إلى السياسة > عناصر السياسة > النتائج. في التخويل > تويب توصيفات التخويل، حدد +إضافة.



قم بإنشاء ملف تعريف التخويل لشبكة VLAN التي يتم تعيين عملاء المصادقة المحليين لها:

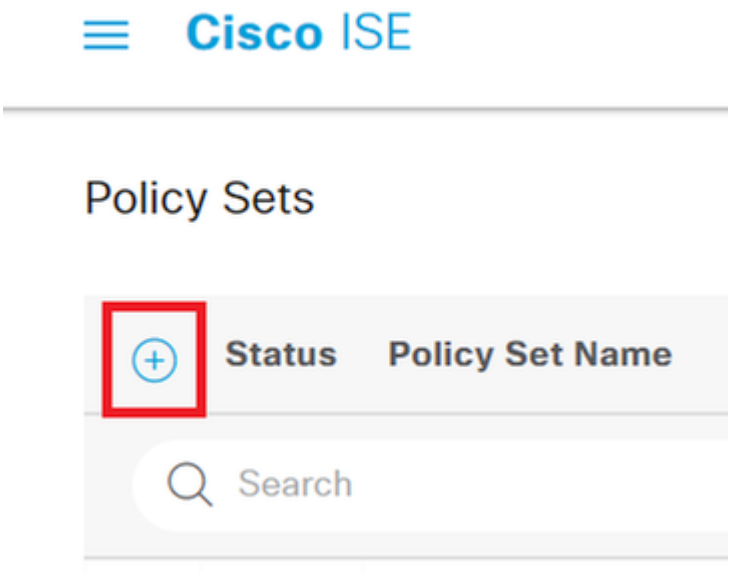


في أسفل الزاوية اليمنى، انقر على إرسال.

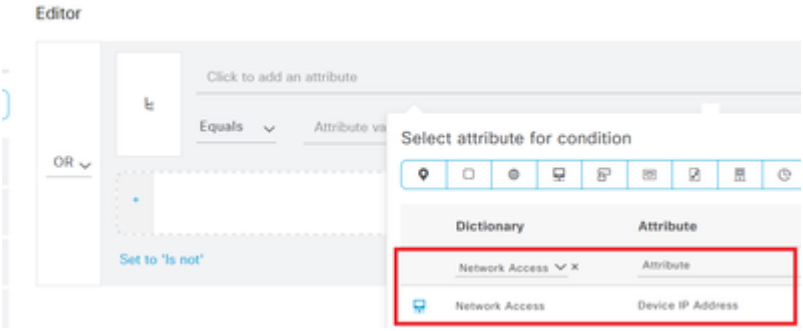
ترى تفاصيل السمات التي يرسلها ISE إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)/نقاط الوصول في سيناريو ناجح.

الخطوة 7. انتقل إلى السياسة > مجموعات السياسة. إنشاء مجموعة نهج جديدة.

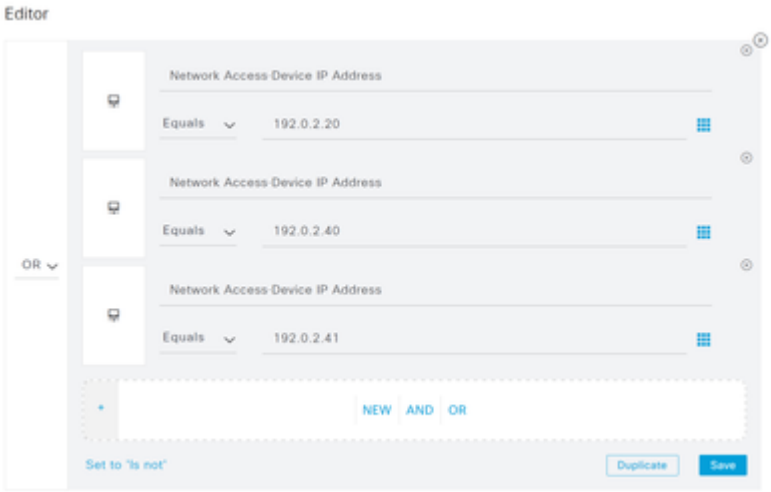
انقر فوق علامة +:



قم بتسمية مجموعة النهج. في شروط العمود، قم بإضافة القاعدة OR وأضف القاموس يساوي: Device IP Address، حدد السمة Network Access، باستخدام

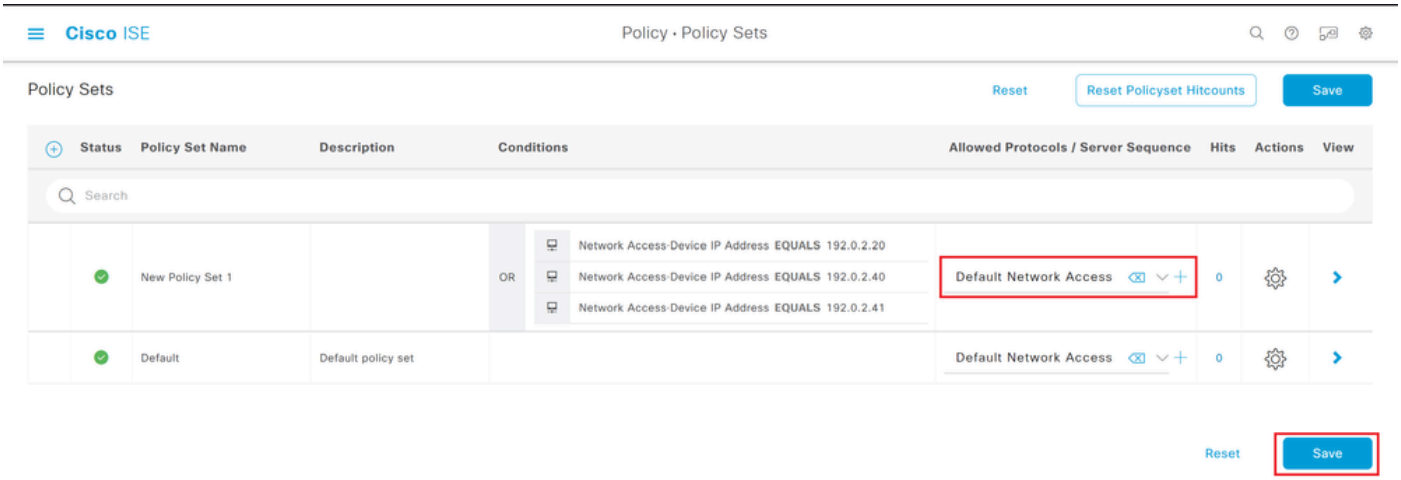


أضفت ال 9800 WLC وال APs عنوان:

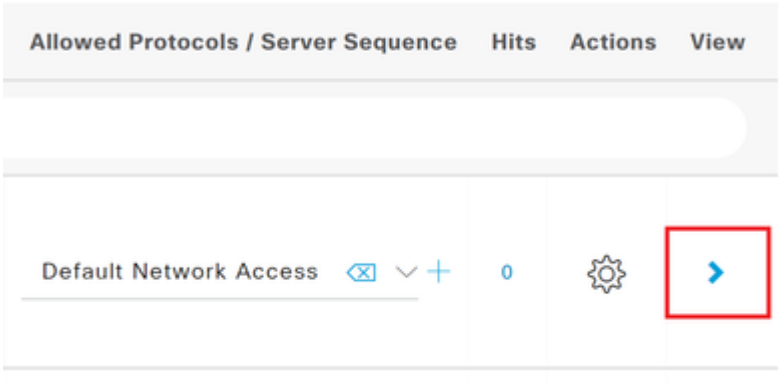


في أسفل الزاوية اليمنى، انقر على إستخدام.

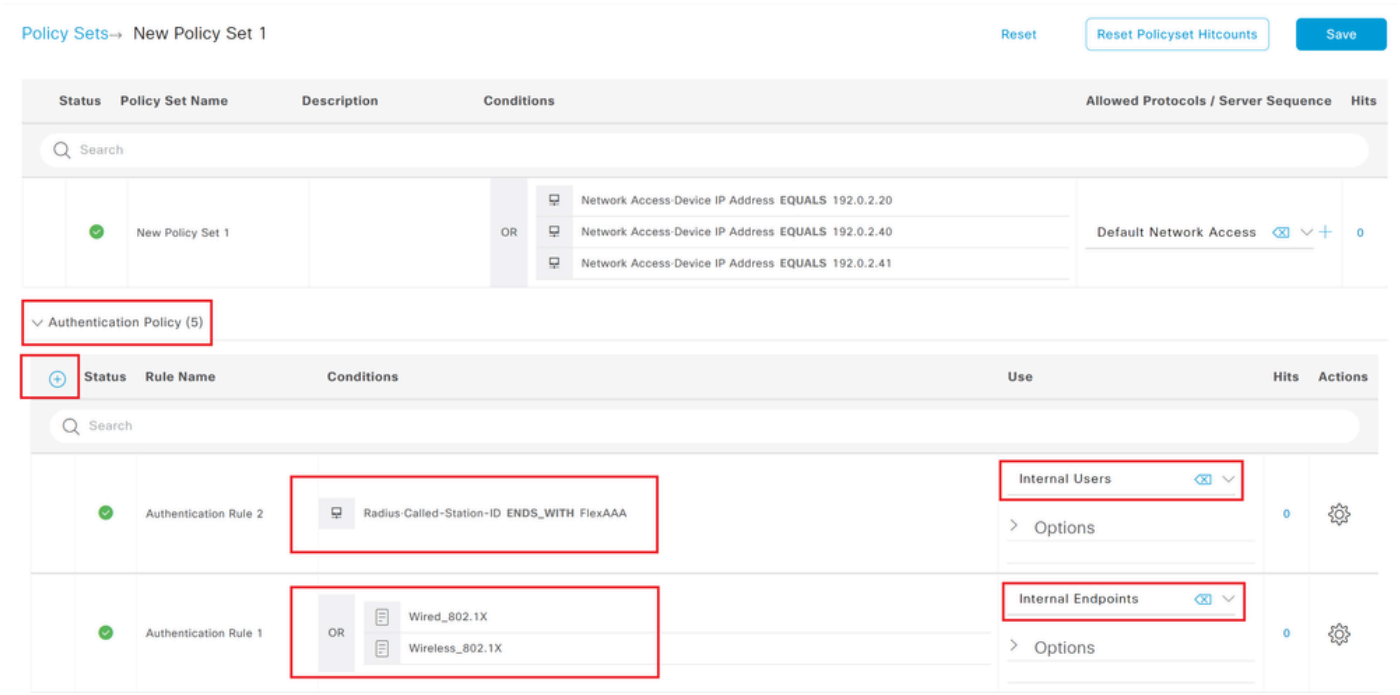
الخطوة 8. في العمود للبروتوكولات المسموح بها حدد الوصول الافتراضي إلى الشبكة. في النهاية، انقر على حفظ:



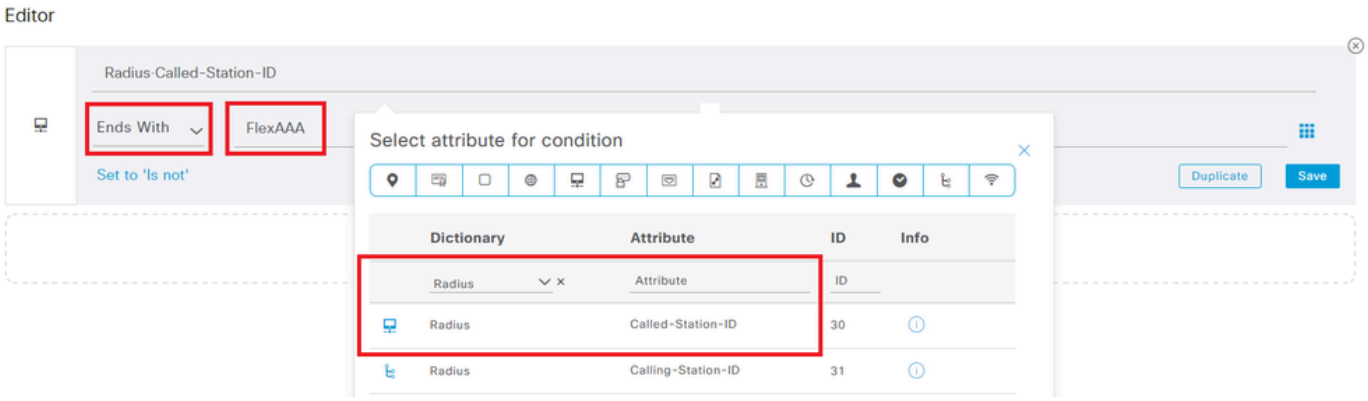
الخطوة 9. في عرض العمود، انقر فوق علامة السهم:



الخطوة 10. قم بتوسيع سياسة المصادقة، وإنشاء سياستين جديدتين: واحد لاسم WLAN، والآخر لتكوين 802.1X:

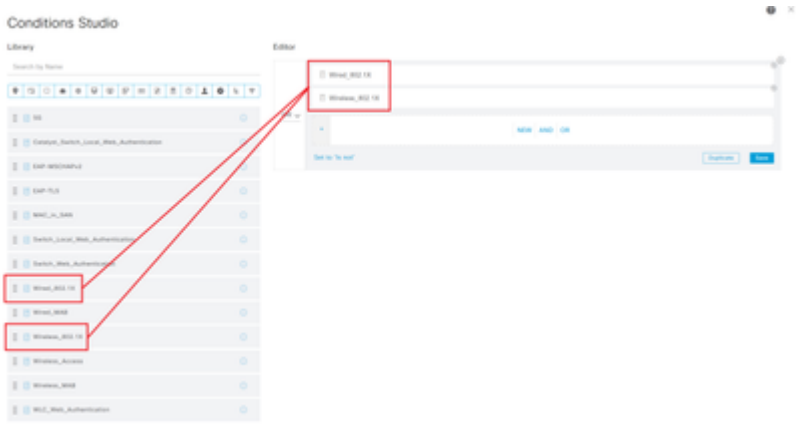


لاسم WLAN، قم بإنشاء الشرط باستخدام Radius الخاص بالقاموس والسمة تسمى-station-id. حدد نهايات باسم WLAN واكتب به:



في أسفل الزاوية اليمنى، انقر على إستخدام. بالنسبة لهذا النهج، في إستخدام العمود، حدد "المستخدمون الداخليون".

الخطوة 11. بالنسبة لسياسة 802.1X، قم بإنشاء الشرط باستخدام مكتبة Wired_802.1X و Wireless_802.1X المتوفرة على ISE. يمكنك سحب وإلقاء هذه العناصر، وحدد الشرط أو:



في أسفل الزاوية اليمنى، انقر على إستخدام. بالنسبة لهذا النهج، في إستخدام الأعمدة، حدد نقاط النهاية الداخلية.

الخطوة 12. قم بالتمرير لأسفل إلى نهج التخويل وإنشاء سياسة جديدة. اعطه اسما، وقم بإنشاء الشرط نفسه كالذي تم إنشاؤه لاسم WLAN في نهج المصادقة.

في توصيفات العمود حدد من القائمة المنسدلة ملف التعريف PermitAccessVlan1432:



في أسفل الزاوية اليمنى، انقر على حفظ.

تكوين PSK WLAN باستخدام المصادقة المحلية

الخطوة 1. قم أولا بتكوين نقاط الوصول في الوضع Flex كما هو موضح في القسم تكوين وضع FlexConnect على الموقع البعيد.

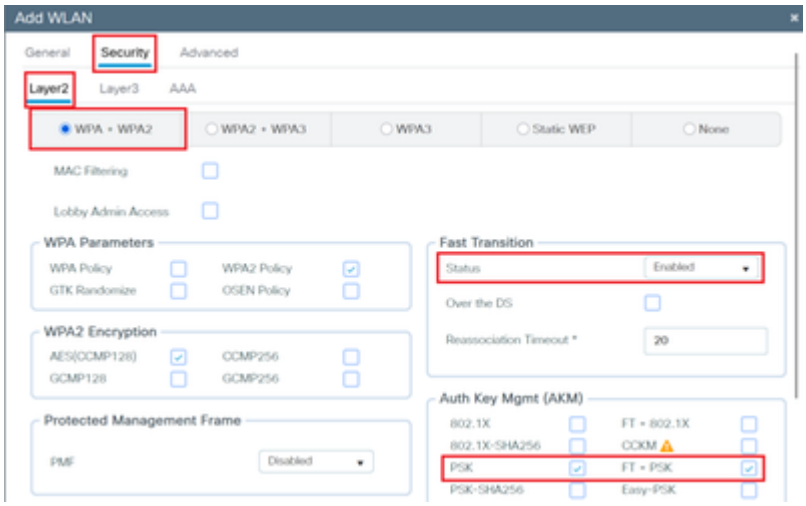
الخطوة 2. إنشاء شبكة WLAN.

انتقل إلى التكوين > العلامات وملفات التعريف > شبكات WLAN، حدد +إضافة.

في علامة العلامة قم بإنشاء اسم على اسم التوصيف، SSID، وحالة التمكين:



الخطوة 3. انتقل إلى الأمان > علامة التبويب الطبقة 2 حدد WPA+WPA2، الانتقال السريع PSK الذي تريده، وتخزين PSK و FT+PSK، Auth Key Mgmt PSK عند تمكينه، واكتب المفتاح المشترك مسبقا الذي تريد أن يستخدمه عملاؤك:





انقر على تحديث وتطبيق على الجهاز.

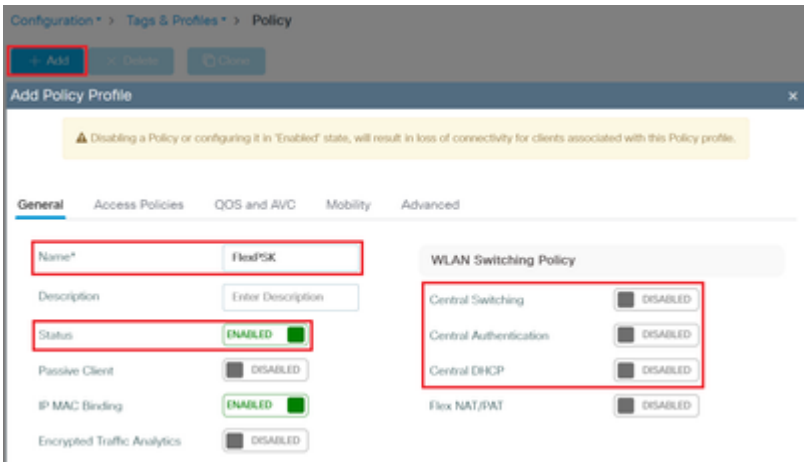
أنت يستطيع رأيت ال WLAN يخلق:



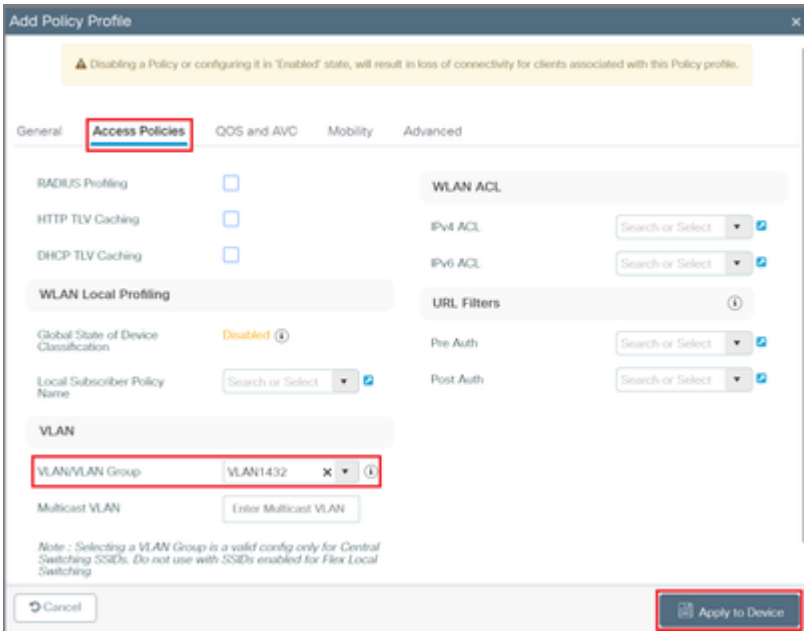
الخطوة 4. إنشاء ملف تعريف السياسة.

انتقل إلى التكوين > العلامات وملفات التعريف > السياسة.

حدد +إضافة وفي علامة التبويب عام امنح اسم لملف تعريف السياسة، وقم بتمكين الحالة، وتعطيل التحويل المركزي والمصادقة المركزية و DHCP المركزي:

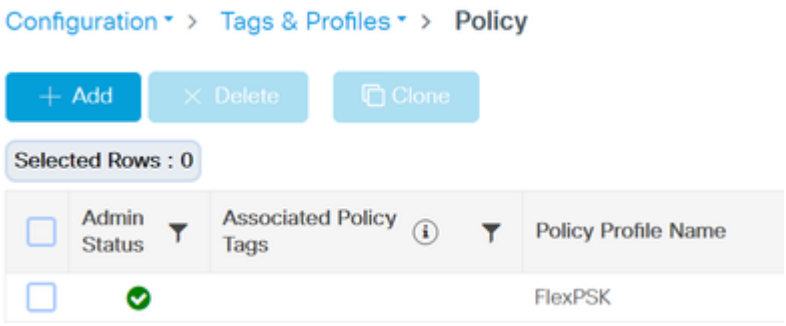


الخطوة 5. انتقل إلى سياسات الوصول إلى علامة التبويب، حدد شبكة VLAN:



انقر على تحديث وتطبيق على الجهاز.

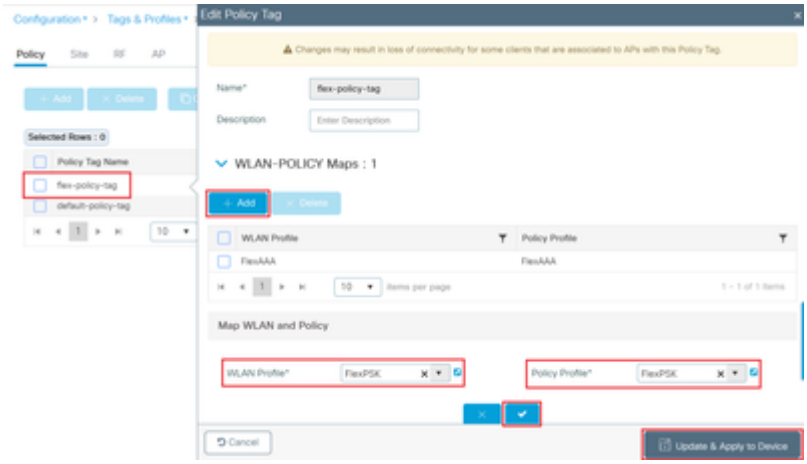
يمكنك رؤية ملف تعريف النهج في القائمة:



الخطوة 6. يمكنك إنشاء علامة نهج جديدة، أو تحرير علامة النهج المتبقية.

انتقل إلى التكوين > علامات تمييز وملفات تعريف > علامات تمييز لتحرير علامة السياسة الموجودة. حدد العلامة المراد تحريرها.

حدد +إضافة ضمن خرائط نهج WLAN. في ملف تعريف WLAN، حدد شبكة WLAN التي تم إنشاؤها مسبقا من القائمة المنسدلة. في "ملف تعريف النهج" حدد "ملف تعريف النهج" الذي تم إنشاؤه مسبقا من القائمة المنسدلة. انقر فوق زر التحقق، ثم فوق تطبيق على الجهاز:



إذا كانت علامة النهج معينة بالفعل على نقطة الوصول، فلن تحتاج إلى القيام بأي شيء آخر.

إذا لم تكن كذلك، قم بتعيين علامة النهج على علامة APs. انتقل إلى التكوين > السلكي > نقاط الوصول. حدد نقطة الوصول لتغيير علامة النهج، وانقر فوق "تحديث وتطبيق على الجهاز".

يفكك نقطة الوصول ويعيد الربط مع علامة النهج الجديدة.

عندما تتصل نقطة الوصول للخلف، يمكنك التحقق من قائمة نقاط الوصول، والتأكيد على أن نقطة الوصول في الوضع Flex، ولها العلامات المعينة الصحيحة.

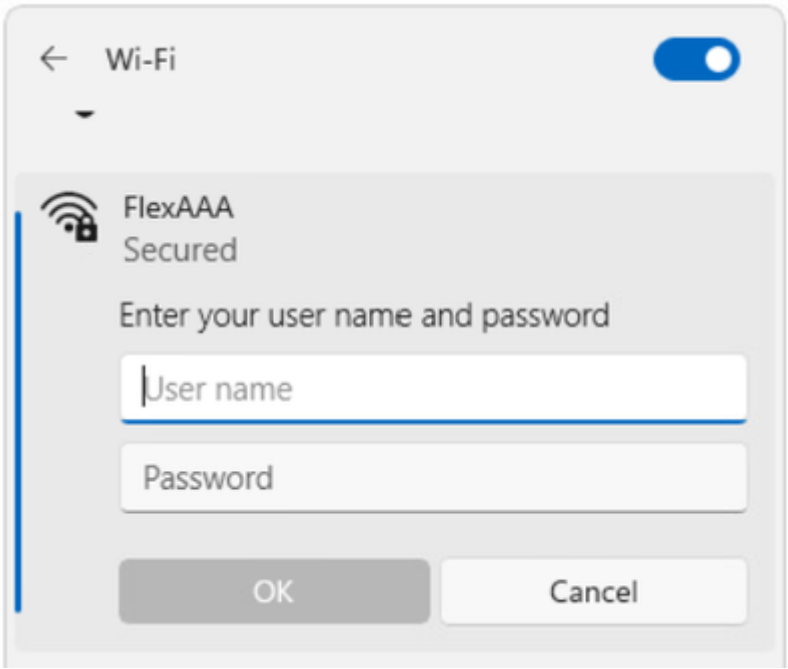
CLI:

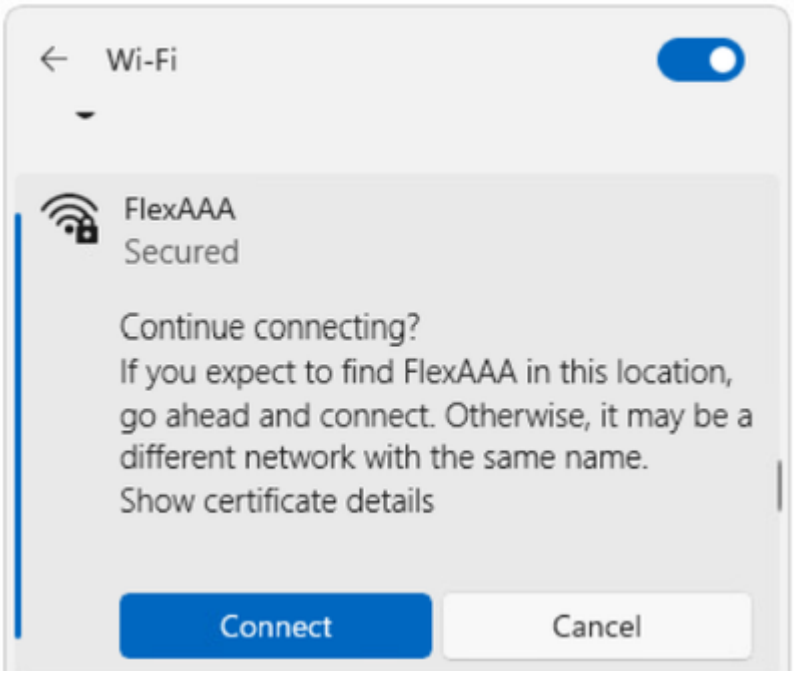
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
```

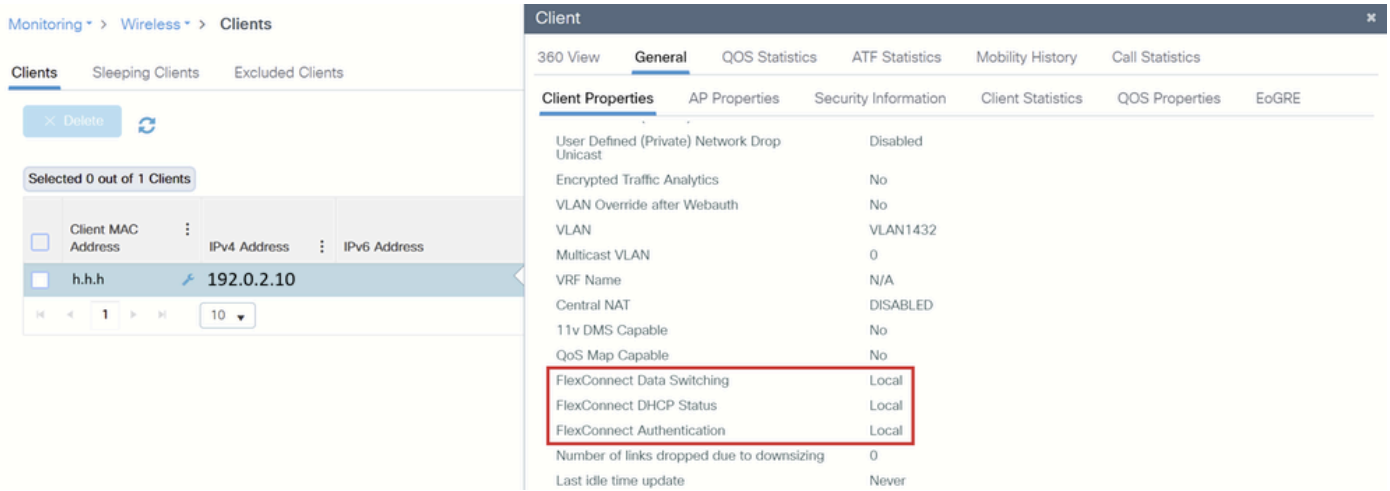
```
                                security wpa akm psk
                                no shutdown
                                !
                wireless profile policy FlexPSK
                      no central authentication
                                no central dhcp
                             no central switching
                                    vlan VLAN1432
                                no shutdown
                                !
            wireless tag policy flex-policy-tag
                    wlan FlexAAA policy FlexAAA
                    wlan FlexPSK policy FlexPSK
                                !
            ap h.h.h (AP Radio MAC address)
                 policy-tag flex-policy-tag
                         site-tag Flex-site
                     rf-tag default-rf-tag
```

التحقق من الصحة

بالنسبة للشبكة المحلية اللاسلكية (WLAN) وفقا لمعيار 802. 1x:







CLI:

```
C9800-1#show wireless client mac-address      h.h.h         detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

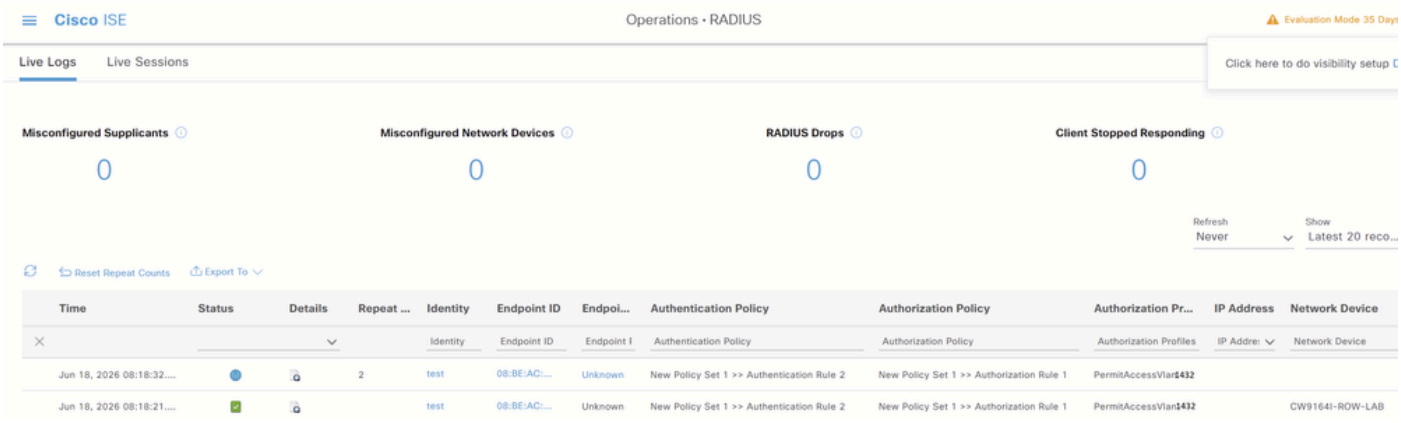
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

رمأوا رطس ةهجاو ىلع AP:

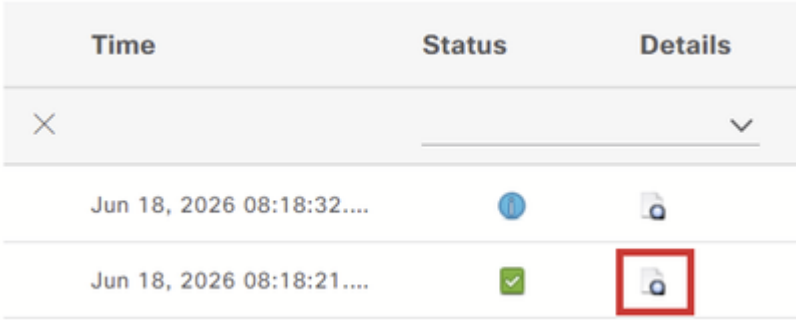
```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH          1       1  33   FlexAAA  -45 MCS9ISS           No         No
```

ISE ىلع



IP Address	Network Device	Device Port	Identity Group	Posture ...	Server
IP Addre:	Network Device	Device Port	Identity Group	Posture Sta	Server
		Radio:1Wlan:1			ISE1
	CW9164I-ROW-LAB	Radio:1Wlan:1	User Identity Groups:ALL_ACCOUNTS (default),Unknown		ISE1



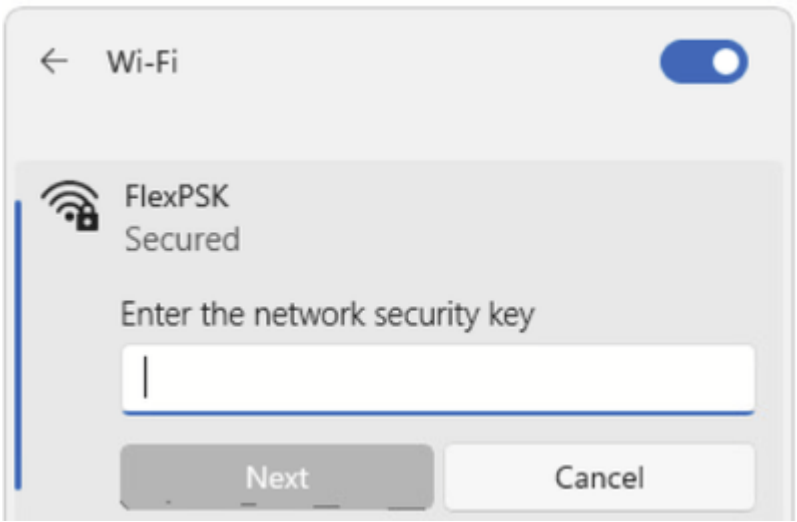
Cisco ISE

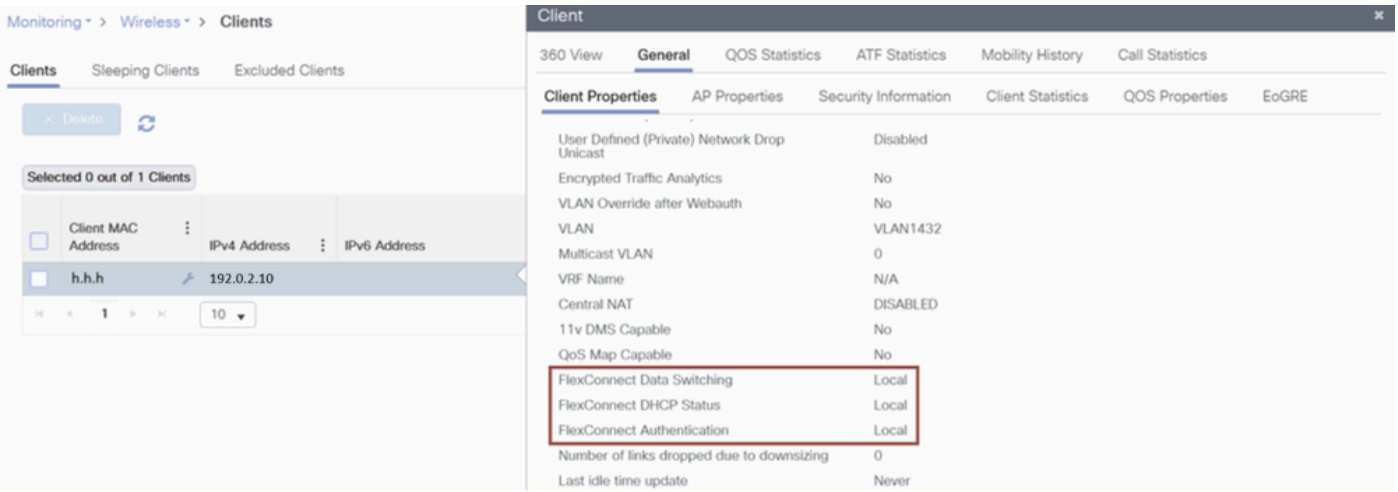
Overview

Event	5200 Authentication succeeded
Username	test
Endpoint Id	HH:HH:HH:HH:HH:HH
Endpoint Profile	Unknown
Authentication Policy	New Policy Set 1 >> Authentication Rule 2
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Authorization Result	PermitAccessVlan1432

Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

J PSK WLAN:





CLI:

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

في واجهة سطر الأوامر (CLI) لنقطة الوصول AP:

```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
  xxxx.xxxx.xxxx      1       2  33   FlexPSK  -45 MCS9_1SS          No          No
```

استكشاف الأخطاء وإصلاحها

قم بتمكين تصحيح أخطاء نقطة الوصول وتتبع RA باستخدام عنوان التحكم في الوصول للوسائط الخاص بالعميل، بشكل متزامن.

في نقطة الوصول قم بتمكين عمليات تصحيح الأخطاء التالية:

debug flexConnect حدث
debug flexconnect pmk
debug flexconnect dot11r
debug dot11 لعميل إدارة معلومات
debug dot11 لعميل إدارة حزمة
debug dot11 لعميل إدارة أخطاء
debug dot11 لعميل إدارة أحداث

بالنسبة للشبكة المحلية اللاسلكية (WLAN) وفقا لمعيار 802. 1x:

سجلات تصحيح أخطاء نقطة الوصول مع المصادقة الناجحة:

تتعامل نقطة الوصول مع إدارة جهاز الحالة 802.11 والمفاتيح المحلي.
تقوم نقطة الوصول بمعالجة الاقتران وإعداد العميل للمصادقة.

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

تقوم نقطة الوصول بمعالجة التخويل وتطبيق تجاوز شبكة VLAN ونقل العميل إلى حالة FWD. (إعادة توجيه)

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

سجلات تتبع RA لنفس المصادقة الناجحة:

ةكبشلا يف مكحتلا رصنع قيقحتي .ةسلجلل WLC مهيظنت ةيملعم RA عبتت لجسي
.ةمجنو ليمعلا هوية صحف نم (WLC) ةيكلساللا ةيلحملا
ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا رصنع ىلع (WLC) ةيقنت طابترإ فرعتي
FlexConnect.

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

.لوصو ةطقن ىلإ ةسايسلا WLC عفدت

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

.ضيوفتلا حاجن

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

.ليمعلا تامولعم
2026/06/19 06:49:20.939394217 {wncd_x_r0-1}{1}: [dot11] [18318]: (ةظحالم): مك:
hhhhh.hhhh.hhh ءازجإ لخاد ليمعلا تانايب - ssid:FlexAAA،slot_id:1 bssid ifid: 0x0، radio_ifid:
0x9040008، wlan_ifid: 0xf040004

.DHCP/ARP ىلحملا ربع تنرتنإلا لوكوتورب WLC مدختسم ملعتي
2026/06/19 06:49:21.00100218 {wncd_x_r0-1}{1}: [client-iplearn] [18318]: (ةظحالم): مك:
192.0.2.10 :لفطتلا IP :ةقيرطلا. حاجنب IP ليمعل IP فرعت hhhh.hhh.hhh

.ماكلاب لصتم ليمعلا
2026/06/19 06:49:21.002363496 {wncd_x_r0-1}{1}: [errmsg] [18318]: (عمولوتام):
٪CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/1: wncd: مدختسملا مسا لخاد

"(48 ة القناة ع ٥٥٥ ٥٥٥ ٥٥٥ ٥٥٥ ٥٥٥ ٥٥٥ :MAC ب دوزملا زاهجلل (FlexAAA) SSID ب طبترم (راباخإ)
:مكا :(ةظحالم) :[client-orch-state] [18318]: {wncd_x_r0-1}{1}: 2026/06/19 06:49:21.002795009
hhhh.hhhh.hhh ا تاقالا ةلاح ليمعلا: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

لسيناريو المستقل

.لسلوك أثناء فقدان اتصال AP-WLC والاسترداد اللاحق

.(WLC) يتم انضمام نقطة الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية
يقوم العميل بتنفيذ مصادقة 802.1X ناجحة، وتقوم نقطة الوصول بنقل العميل إلى حالة
.FWD (إعادة توجيه)

.على سجلات ISE RADIUS Live، نرى جلسة عمل العميل

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
   [*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
   [*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

تفشل نقطة الوصول في الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية
لا يزال .وتتوحل إلى الوضع المستقل، وتستنفد عدد مرات إعادة الإرسال الخاصة بها، و(WLC)
.العملاء الحاليون متصلين محليا

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
   [*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
                        [*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
                                    [*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

:ولكن العميل لا يزال متصلا

CW9164I-Row-Lab2#show dot11 عملاء

إجمالي عملاء نقطة 11: 1
مساعد معرف WLAN الخاص بمعرف MAC Slot للعميل اسم RSSI Maxrate is_wgb_wired
is_mld_sta
HH:HH:HH:HH:HH:0 1 FlexAAA -40 M7 ال

عندما يجول العميل إلى نقطة وصول أخرى في الوضع المستقل، يفشل تأكيد EAP بسبب عدم القدرة على الوصول إلى خادم RADIUS. يتم إلغاء تخويل العميل وإزالته من نقطة الوصول.

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUES
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

ترسل نقطة الوصول جلسة عمل العميل إلى خادم RADIUS للنسخ الاحتياطي.

تستعيد نقطة الوصول الاتصال ب WLC. تعود نقطة الوصول إلى الوضع المتصل وتزامن معلومات جلسة عمل العميل المحلي مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

عمليات انتقال جلسة عمل العميل بين عقد ISE الأساسية والنسخ الاحتياطي استنادا إلى حالة اتصال نقطة الوصول.

تظهر نقطة الوصول والعميل كمتصلين على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، ولم يلاحظ العميل أي قطع اتصال أو رفرفة عند تجوال بين نقطة الوصول و WLC.

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0
```

```
Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
```

```
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
          [*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
                      [*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, ma
             [*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
            [*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
            [*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
                          [*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc 4
           [*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
           [*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc 4
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASSO
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 fo
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
                          [*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
             [*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
  [*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
      [*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
    [*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
    [*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


                                                    CW9164I-ROW-LAB2#show dot11 clients

                                                                  Total dot11 clients: 1
                                  Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
                                                    HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No

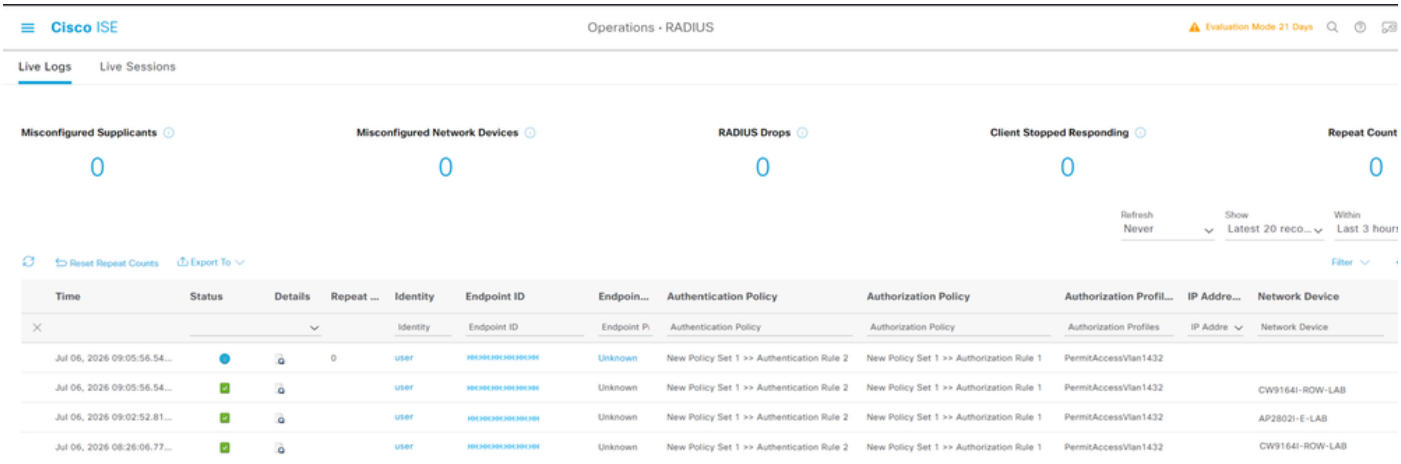



                                        *07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
                                                [*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
                                                      [*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
                          [*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
                                                [*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
                                                 [*07/06/2026 21:00:09.5020] CAPWAP State: Configure
                                                       [*07/06/2026 21:00:12.5510] CAPWAP State: Run
                                      [*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
                                   [*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
                             [*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
```

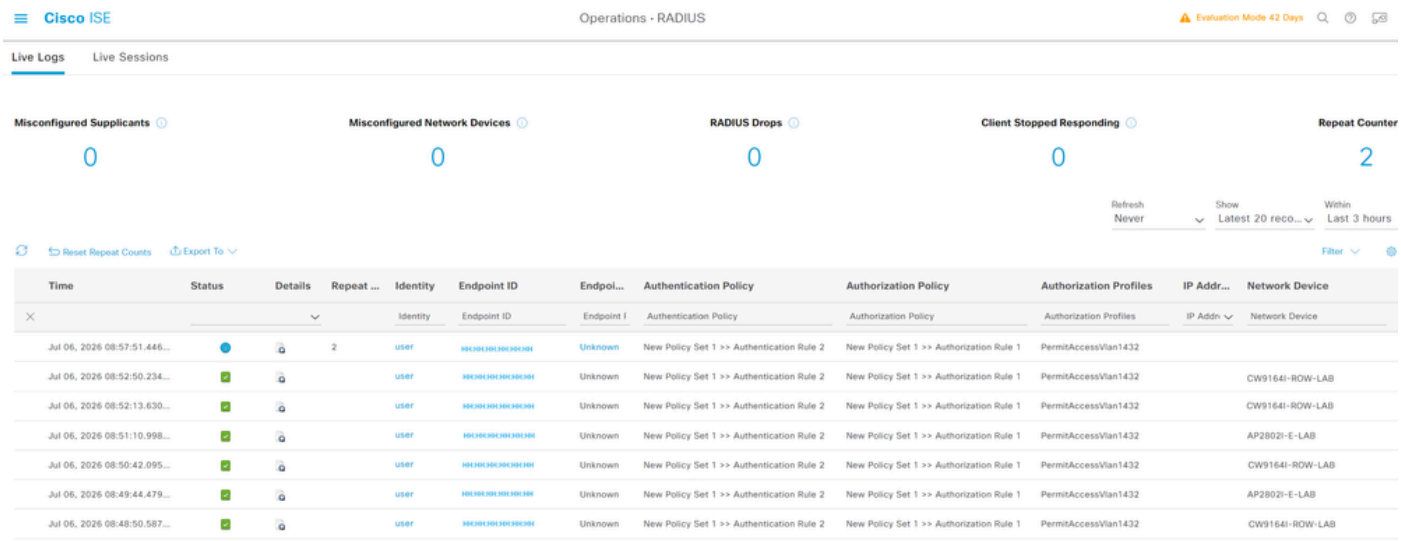
```
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716

CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



ISE الأساسي: تسجيل الجلسة الأولية (08:26:06) والجلسة المستأنفة بعد إستعادة اتصال WLC (09:02:52).



النسخ الاحتياطي ل ISE: يلتقط نشاط الجلسة (08:48:50 - 08:57:51) عندما كانت نقطة الوصول تعمل في الوضع المستقل.

كانت الجلسة الأولى في 08:26:06، بعد ذلك فقدت نقطة الوصول الاتصال ب WLC وانتقلت إلى الوضع المستقل.

الجلسة 09:02:52 هي الجلسة الأولى بعد أن أعاد AP الاتصال باستخدام WLC.

معلومات ذات صلة

- CCNP Enterprise Wireless Design ENWLSD 300-425 والتنفيذ WANlsi 300-430 المعياري الإصدار الثاني، Official Cert Guide
- دليل تكوين برنامج وحدة التحكم اللاسلكية من Cisco Catalyst 9800 Series، Cisco IOS XE 17.8.x - الفصل: تقنية FlexConnect
- ملاحظات الإصدار الخاصة بوحدة التحكم اللاسلكية من السلسلة Cisco Catalyst 9800 الإصدار 17.8.x، Cisco IOS XE Curelated Series
- مصفوفة ميزات نطاق الوصول اللاسلكية من Cisco
- الدعم الفني والتنزيلات من Cisco

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).