تكوين CWA باستخدام نقاط الوصول FlexConnect في الشبكة التي تحكم فيها وحدة تحكم لاسلكية محلية (WLC) باستخدام تقنية ISE

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة الويب المركزية باستخدام نقاط الوصول (APs) إلى وحدة تحكم شبكة محلية لاسلكية (WLC) باستخدام محرك خدمات الهوية (ISE) في وضع التحويل المحلي.

ملاحظة هامة: في هذا الوقت، لا يتم دعم المصادقة المحلية على نقاط الوصول FlexAPs لهذا السيناريو.

مستندات أخرى في هذه السلسلة

- المصادقة المركزية للويب مع محول ومثال تكوين محرك خدمات الهوية
- مثال على تكوين مصادقة الويب المركزية على شبكة LAN اللاسلكية (WLC) ومحرك خدمات كشف الهوية (ISE)

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- Cisco Identity Services Engine (ISE)، الإصدار 1.2.1
- برنامج Wireless LAN Controller، إصدار - 7.4.100.0

التكوين

هناك طرق متعددة لتكوين مصادقة الويب المركزية على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC). الطريقة الأولى هي مصادقة الويب المحلية حيث يقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بإعادة توجيه حركة مرور بيانات HTTP إلى خادم داخلي أو خارجي حيث يتم مطالبة المستخدم بالمصادقة. تقوم WLC بعد ذلك بجلب بيانات الاعتماد (يتم إرسالها مرة أخرى عبر طلب HTTP GET في حالة وجود خادم خارجي) وإجراء مصادقة RADIUS. في حالة مستخدم ضيف، يلزم توفر خادم خارجي (مثل محرك خدمة الهوية (ISE) أو خادم ضيف NAC (NGS) حيث توفر البوابة ميزات مثل تسجيل الجهاز والإمداد الذاتي. تتضمن هذه العملية الخطوات التالية:

1. يتصل المستخدم ب SSID لمصادقة الويب.
2. يفتح المستخدم المستعرض.
3. تتم إعادة توجيه عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إلى مدخل الضيف (مثل ISE أو NGS) بمجرد إدخال عنوان URL.
4. يقوم المستخدم بالمصادقة على البوابة.
5. تقوم بوابة الضيف بإعادة التوجيه إلى WLC مع بيانات الاعتماد التي تم إدخالها.
6. يقوم WLC بمصادقة المستخدم الضيف عبر RADIUS.
7. يقوم WLC بإعادة التوجيه إلى عنوان URL الأصلي.

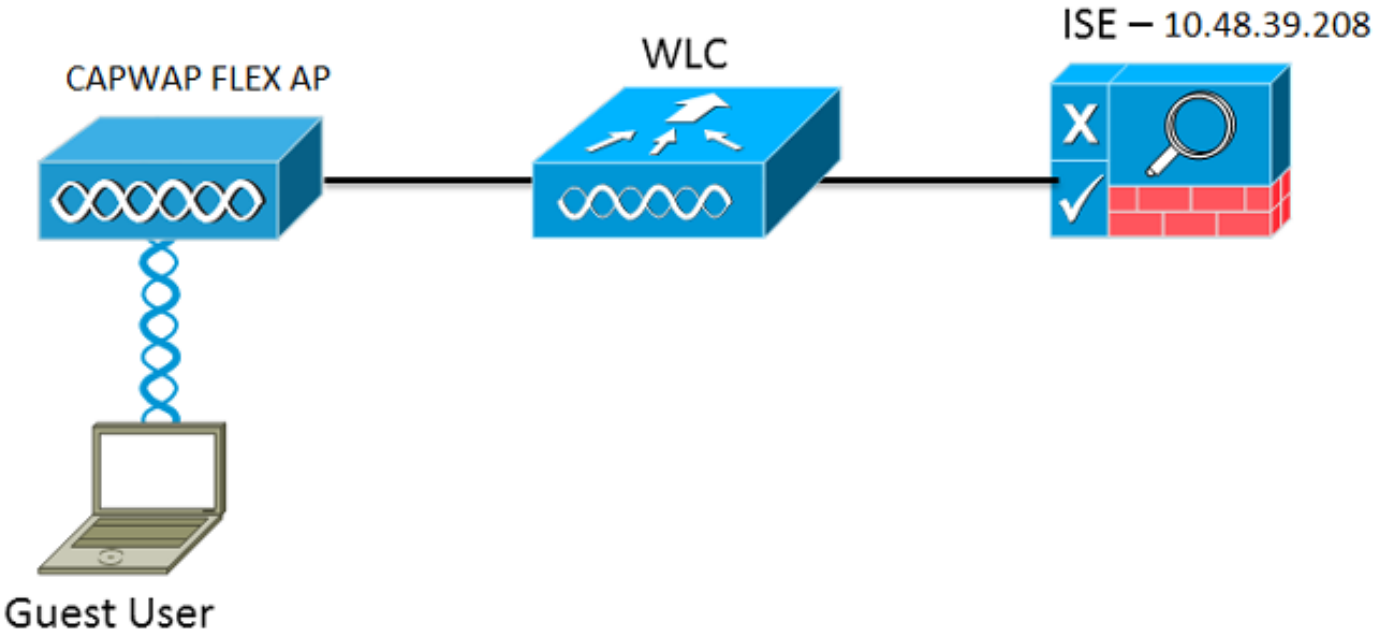
تتضمن هذه العملية الكثير من إعادة التوجيه. تتمثل الطريقة الجديدة في إستخدام مصادقة الويب المركزية التي تعمل مع ISE (الإصدارات الأحدث من 1.1) و WLC (الإصدارات الأحدث من 7.2). تتضمن هذه العملية الخطوات التالية:

1. يتصل المستخدم ب SSID لمصادقة الويب.
2. يفتح المستخدم المستعرض.
3. يقوم WLC بإعادة التوجيه إلى بوابة الضيف.
4. يقوم المستخدم بالمصادقة على البوابة.
5. يرسل ISE تغيير تفويض RADIUS (CoA - UDP port 1700) للإشارة إلى وحدة التحكم إلى أن المستخدم صالح ويدفع أخيرا سمات RADIUS مثل قائمة التحكم في الوصول (ACL).
6. تتم مطالبة المستخدم بإعادة محاولة عنوان URL الأصلي.

يصف هذا القسم الخطوات اللازمة لتكوين مصادقة الويب المركزية على WLC و ISE.

الرسم التخطيطي للشبكة

يستخدم هذا التكوين إعداد الشبكة التالي:

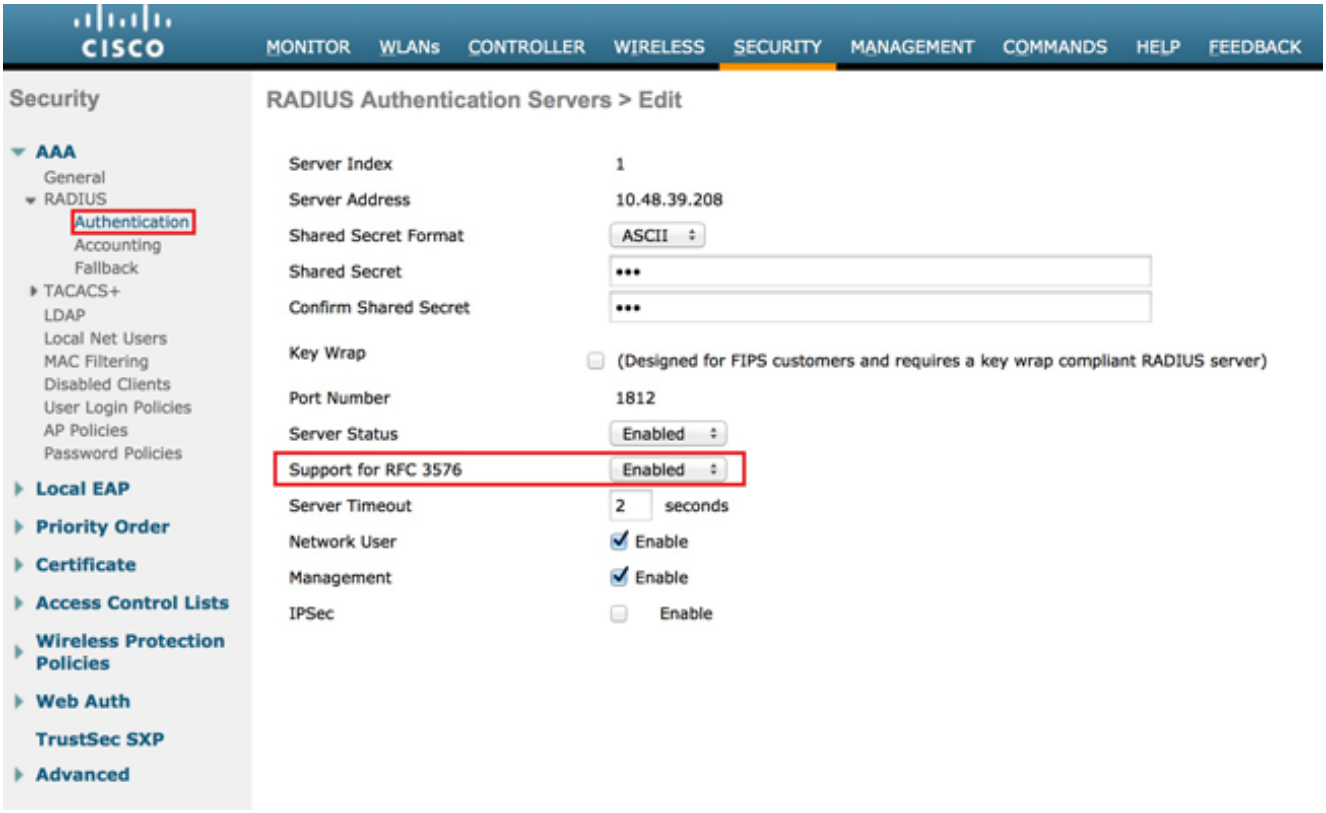


تكوين وحدة التحكّم في شبكة LAN اللاسلكية (WLC)

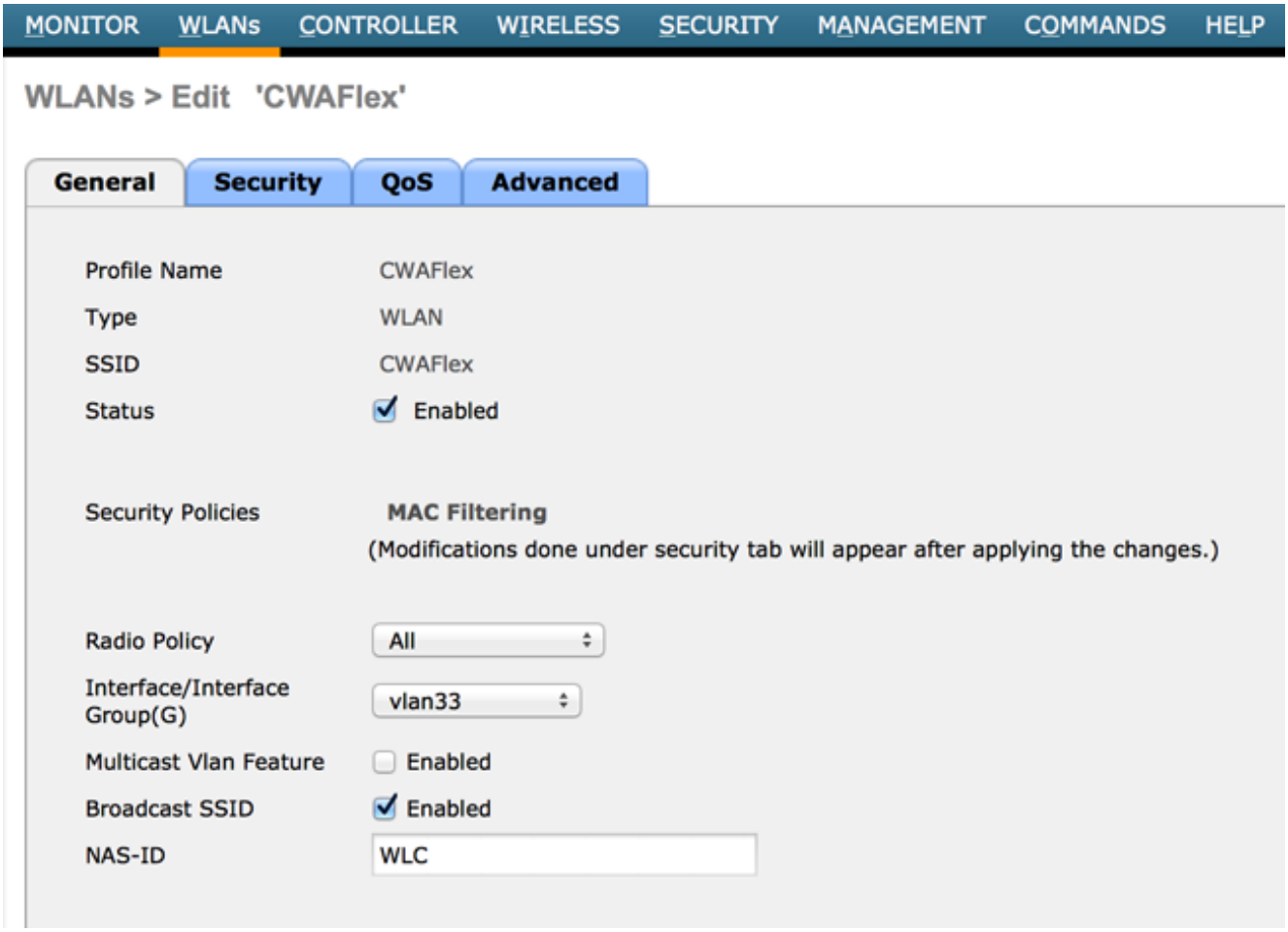
يكون تكوين WLC بسيطًا إلى حد ما. يتم إستخدام "خدعة؟" (مثل المحولات) للحصول على عنوان URL للمصادقة الديناميكية من ISE. (نظرا لأنه يستخدم CoA، يلزم إنشاء جلسة نظرا لأن معرف الجلسة هو جزء من عنوان URL.) يتم تكوين SSID لاستخدام تصفية MAC، ويتم تكوين ISE لإرجاع رسالة قبول الوصول حتى إذا لم يتم العثور على عنوان MAC بحيث يرسل عنوان URL لإعادة التوجيه لجميع المستخدمين.

وبالإضافة إلى ذلك، يجب تمكين التحكم في الدخول إلى شبكة (RADIUS (NAC) وتجاوز AAA. يسمح RADIUS NAC ل ISE بإرسال طلب CoA يشير إلى أن المستخدم قد تمت مصادقته الآن وقادر على الوصول إلى الشبكة. كما يتم إستخدامه لتقييم الوضع حيث يقوم ISE بتغيير ملف تعريف المستخدم استنادا إلى نتيجة الوضع.

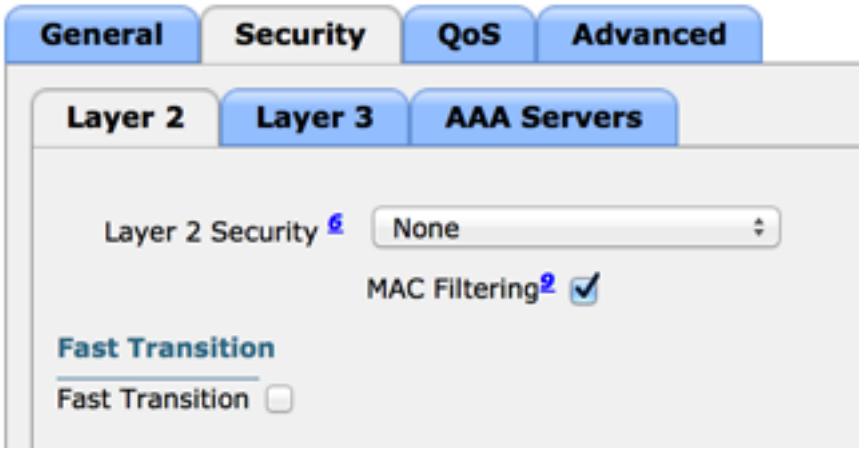
1. تأكد من أن خادم RADIUS به تمكين CoA) RFC3576)، وهو الإعداد الافتراضي.



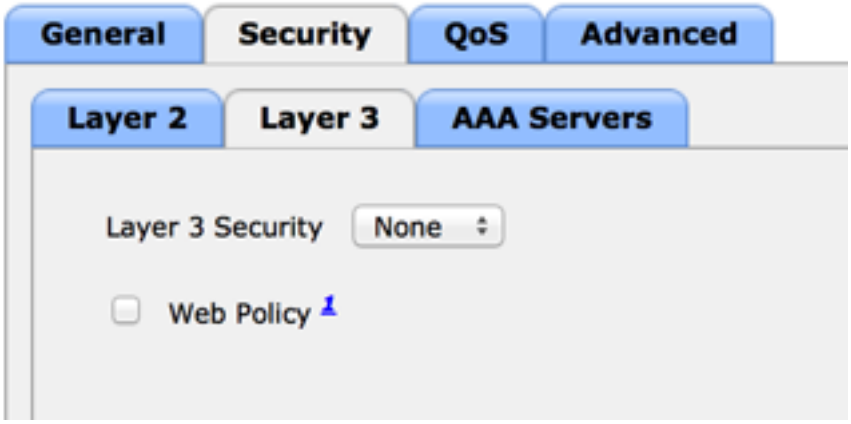
إنشاء شبكة WLAN جديدة. يخلق هذا مثال WLAN جديد يعين *CWAFlex* ويعين هو إلى VLAN33. (لاحظ أن هو لن يتلقى كثير تأثير بما أن نقطة الوصول في محلي تحويل أسلوب.)2.



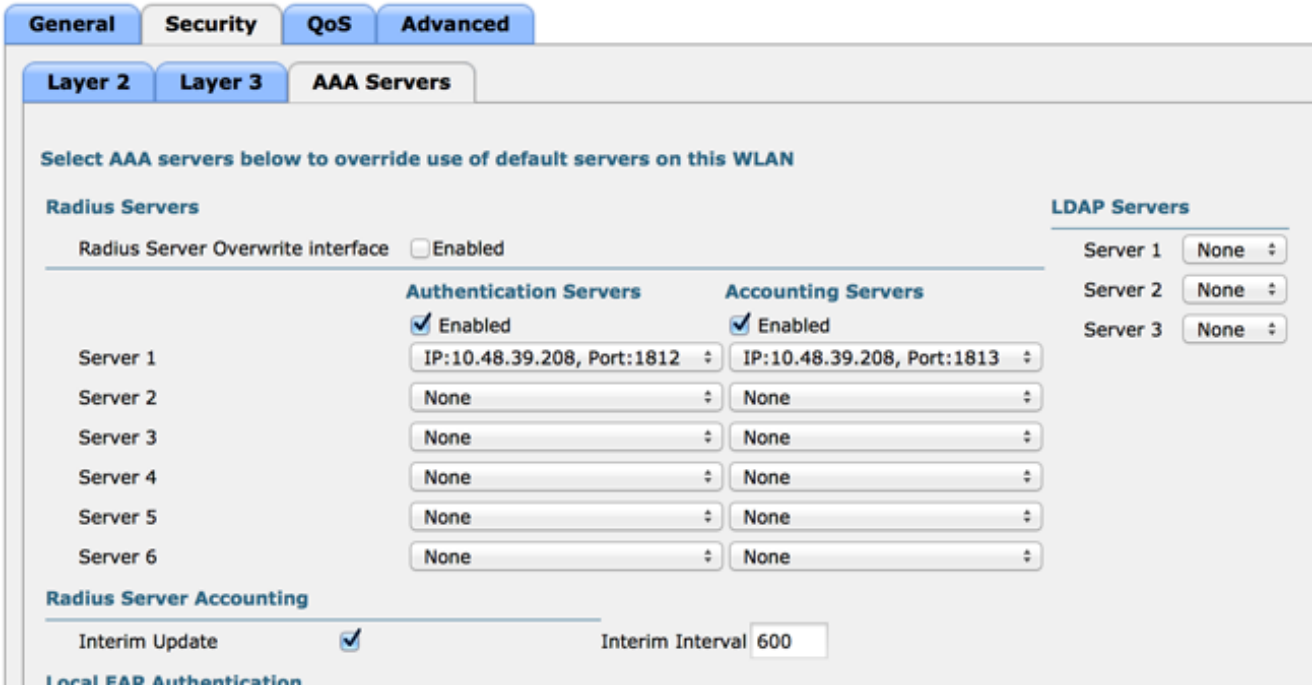
3. في صفحة التأمين، قم بتمكين تصفية MAC كطبقة 2 تأمين.



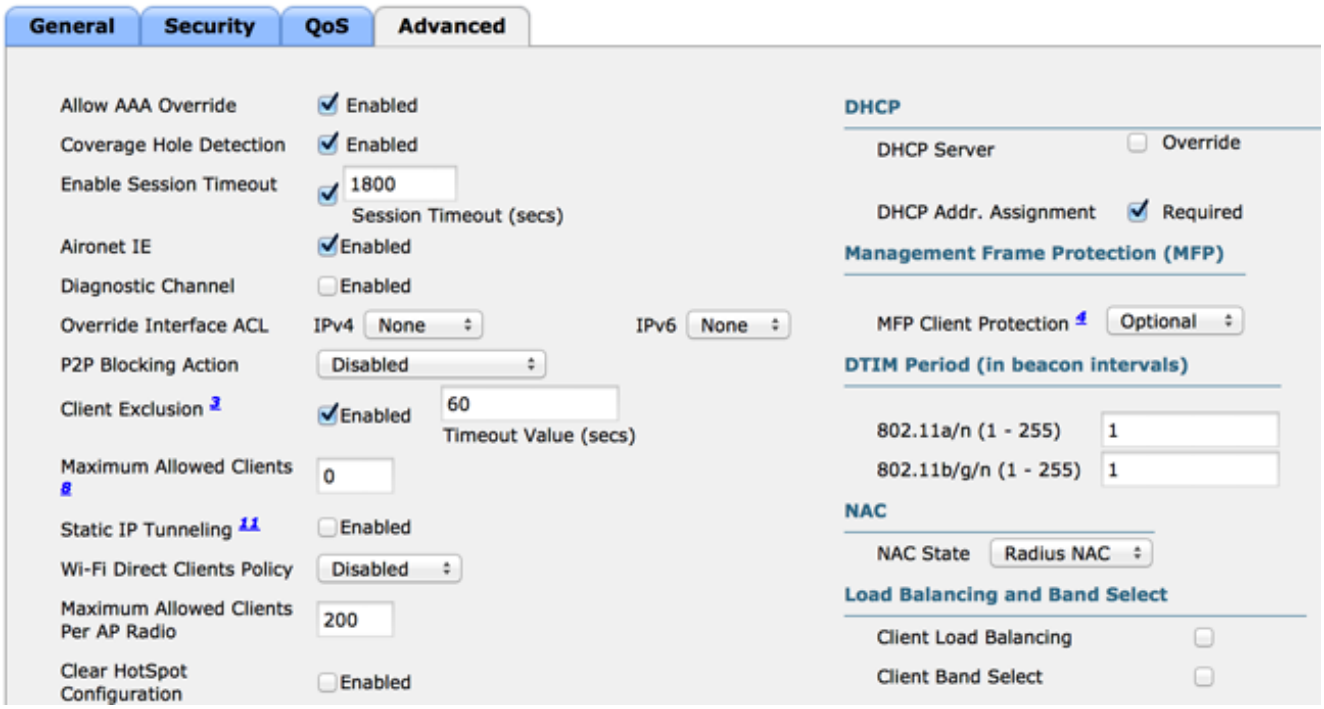
على علامة تبويب الطبقة 3، تأكد من تعطيل التأمين. (في حالة تمكين مصادقة الويب على الطبقة 3، يتم تمكين مصادقة الويب المحلية، وليس مصادقة الويب المركزية.)



على علامة التبويب خوادم AAA، حدد خادم ISE كخادم RADIUS للشبكة المحلية اللاسلكية (WLAN). وبشكل إختياري، يمكنك تحديده للمحاسبة للحصول على معلومات أكثر تفصيلا حول ISE.

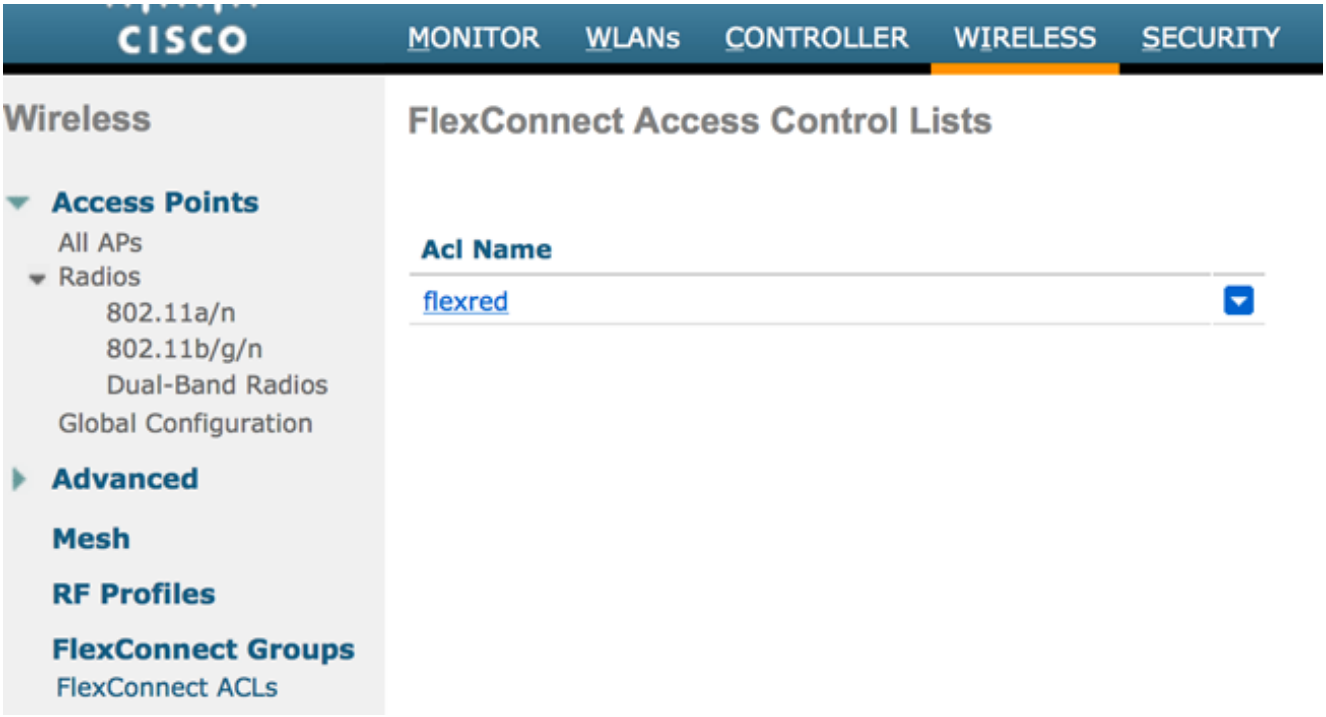


6. على علامة التبويب خيارات متقدمة، تأكد من تحديد السماح بتجاوز AAA وتحديد RADIUS NAC لحالة NAC.

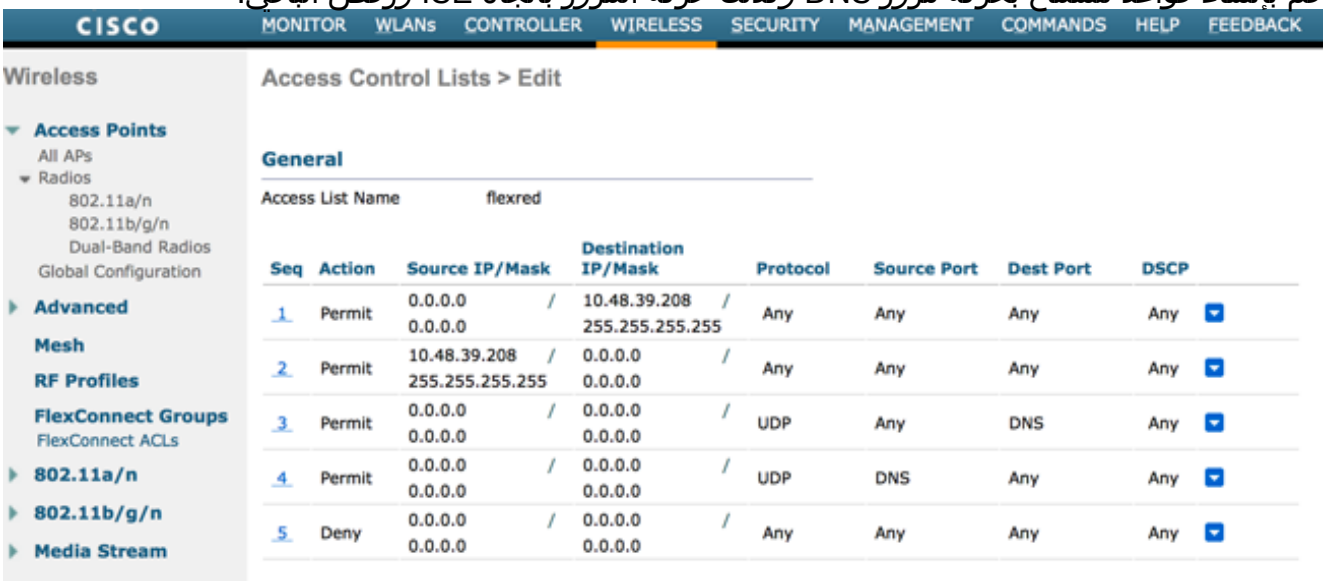


7. إنشاء قائمة تحكم في الوصول (ACL) لإعادة التوجيه.

تتم الإشارة إلى قائمة التحكم في الوصول هذه في رسالة قبول الوصول الخاصة ب ISE وتحدد حركة المرور التي يجب إعادة توجيهها (رفضها بواسطة قائمة التحكم في الوصول إلى النقل) وكذلك حركة المرور التي يجب عدم إعادة توجيهها (المسموح بها بواسطة قائمة التحكم في الوصول إلى النقل (ACL). وبشكل أساسي، يلزم السماح بحركة مرور البيانات DNS وحركة المرور من/إلى ISE. **ملاحظة**: توجد مشكلة في نقاط الوصول FlexConnect APs وهي أنه يجب عليك إنشاء قائمة تحكم في الوصول (ACL) ل FlexConnect منفصلة عن قائمة التحكم في الوصول (ACL) العادية لديك. وثقت هذا إصدار في cisco بق CSCue68065 وصلح في إطلاق 7.5. في WLC 7.5 وفيما بعد، تطلبت فقط FlexACL، ولا يحتاج إلى قائمة تحكم في الوصول قياسية. تتوقع وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) أن تكون قائمة التحكم في الوصول (ACL) المعاد توجيهها بواسطة ISE قائمة تحكم في الوصول (ACL) عادية. ومع ذلك، لضمان عمله، يلزمك تطبيق قائمة التحكم في الوصول (ACL) نفسها المطبقة على قائمة التحكم في الوصول (ACL) ل FlexConnect. يوضح هذا المثال كيفية إنشاء قائمة تحكم في الوصول (ACL) المسماة *FlexRed* FlexConnect:

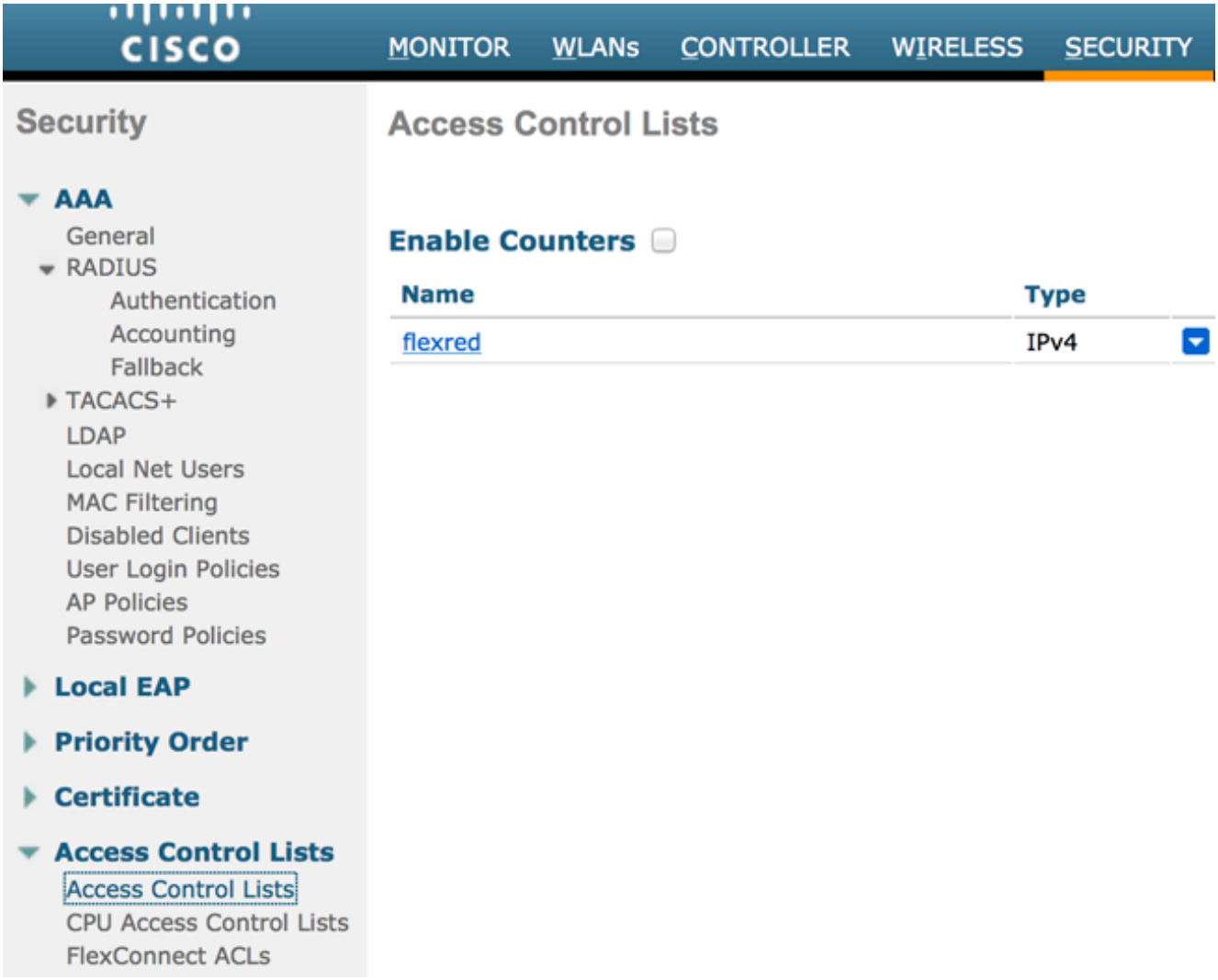


قم بإنشاء قواعد للسماح بحركة مرور DNS وكذلك حركة المرور باتجاه ISE ورفض الباقي.



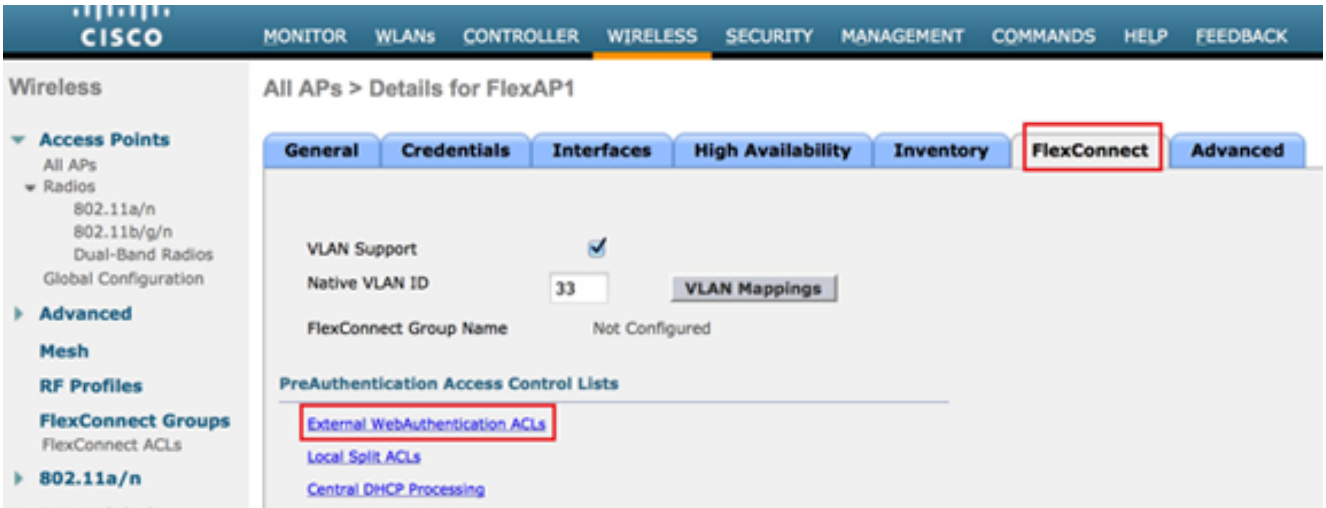
إن يريد أنت الحد الأقصى أمن، أنت يستطيع سمحت فقط ميناء 8443 باتجاه ISE. (إن posture، أنت ينبغي أضفت نموذجي وضعية ميناء، مثل 8905،8906،8909،8910.)

(فقط في الرمز قبل الإصدار 7.5 بسبب CSCue68065) أختر **أمان > قوائم التحكم في الوصول** لإنشاء قائمة تحكم في الوصول (ACL) متطابقة بنفس الاسم.



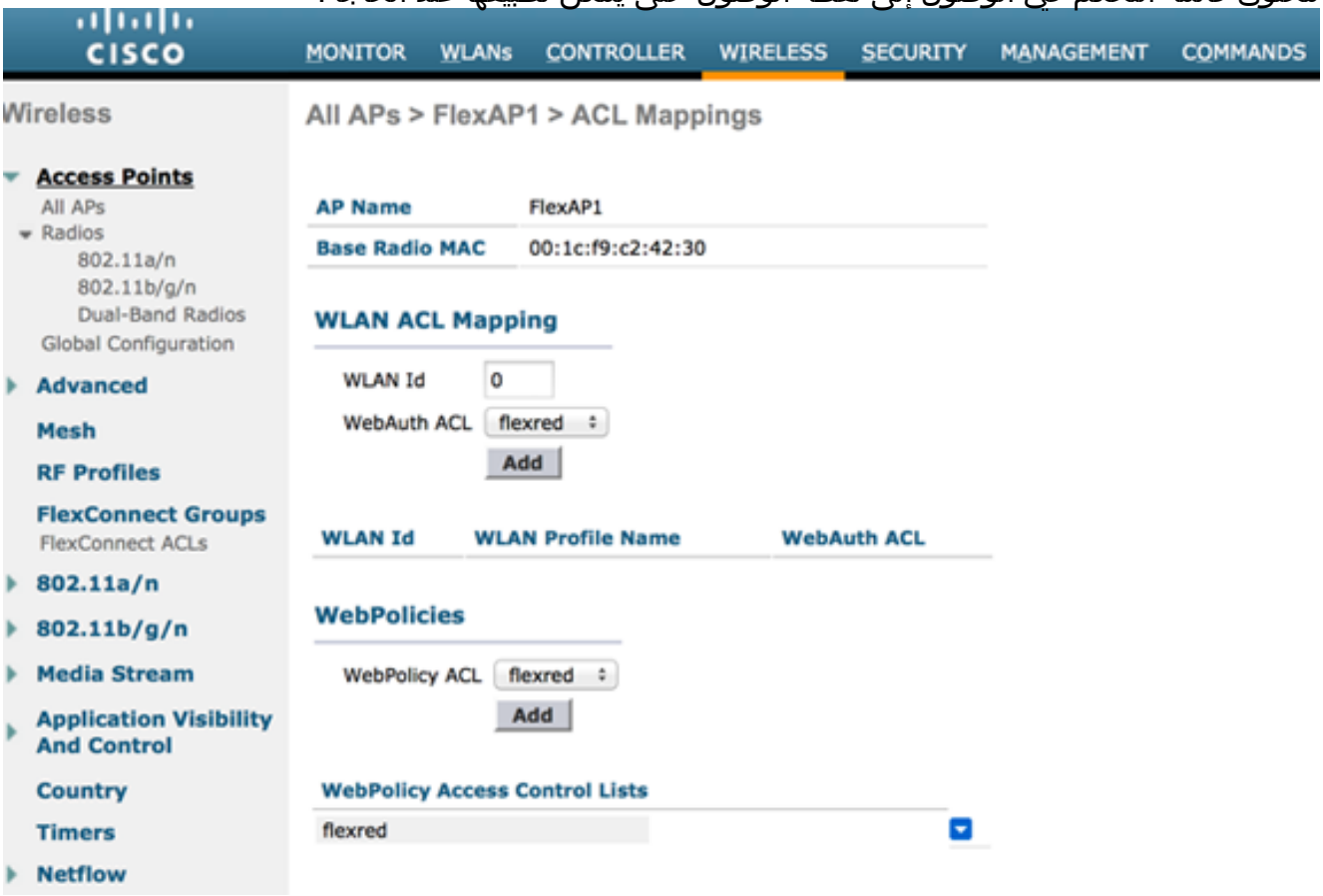
تجهيز نقطة الوصول FlexConnect AP المحددة. لاحظ أنه بالنسبة لعمليات نشر أكبر، فإنك تستخدم عادة مجموعات FlexConnect ولا تقوم بأداء هذه العناصر لكل نقطة وصول وذلك لأسباب تتعلق بقابلية التوسعة.

انقر على **لاسلكي**، وحدد نقطة الوصول المحددة.انقر فوق علامة التبويب **FlexConnect**، وانقر فوق **قوائم التحكم في الوصول (ACL) الخارجية لمصادقة الويب**. (قبل الإصدار 7.4، كان هذا الخيار يسمى *سياسات الويب*.)



إضافة قائمة التحكم في الوصول (ACL) (المسماة *flexRed* في هذا المثال) إلى منطقة سياسات الويب. يؤدي هذا إلى دفع قائمة التحكم في الوصول (ACL) مسبقا إلى نقطة الوصول. لا يتم تطبيقها بعد، ولكن يتم منح

محتوى قائمة التحكم في الوصول إلى نقطة الوصول حتى يمكن تطبيقها عند الحاجة.



اكتمل تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الآن.

تكوين ISE

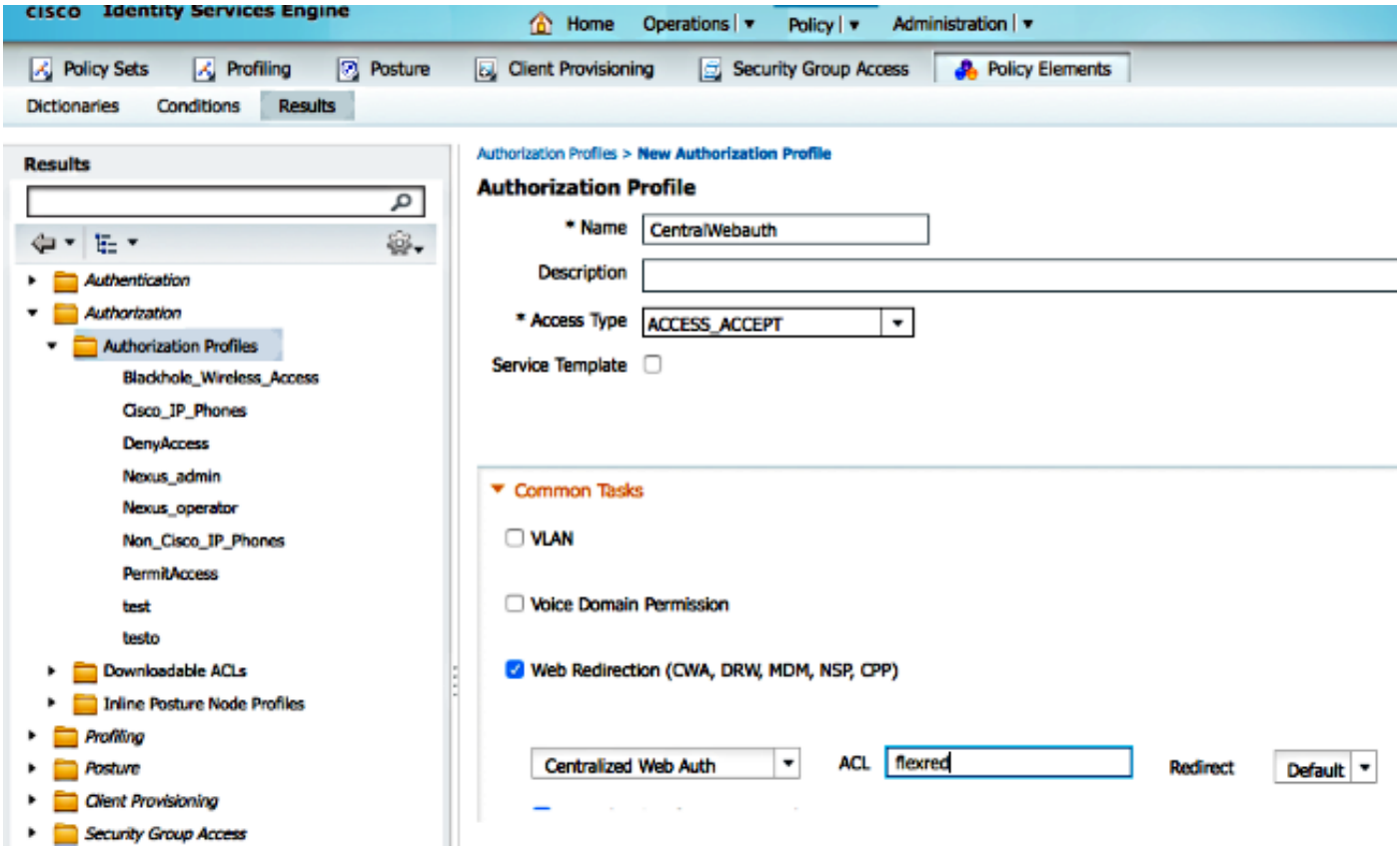
إنشاء ملف تعريف التفويض

أكمل الخطوات التالية لإنشاء ملف تعريف التخويل:

1. انقر فوق **السياسة**، ثم انقر فوق **عناصر السياسة**.
2. انقر فوق **النتائج**.
3. قم بتوسيع **التخويل**، ثم انقر فوق **ملف تعريف التخويل**.
4. انقر فوق الزر **إضافة** لإنشاء ملف تعريف تخويل جديد لـ webauth المركزي.
5. في حقل **الاسم**، أدخِل اسمًا لملف التعريف. يستخدم هذا المثال *CentralWebauth*.
6. اختر ACCESS_ACCEPT من القائمة المنسدلة نوع الوصول.
7. حدد خانة الاختيار **مصادقة الويب**، واختر **مصادقة الويب المركزية** من القائمة المنسدلة.
8. في حقل قائمة التحكم في الوصول (ACL)، أدخل اسم قائمة التحكم في الوصول (ACL) على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الذي يحدد حركة المرور التي سيتم إعادة توجيهها. تستخدم هذه الأمثلة *flexRed*.
9. أختر **الافتراضي** من القائمة المنسدلة إعادة التوجيه.

تحدد سمة إعادة التوجيه ما إذا كان ISE يرى مدخل ويب الافتراضي أو مدخل ويب مخصص أنشأه مسؤول ISE. على سبيل المثال، تقوم قائمة التحكم في الوصول (ACL) *المرنة* في هذا المثال بتشغيل إعادة توجيه على حركة مرور

HTTP من العميل إلى أي مكان.

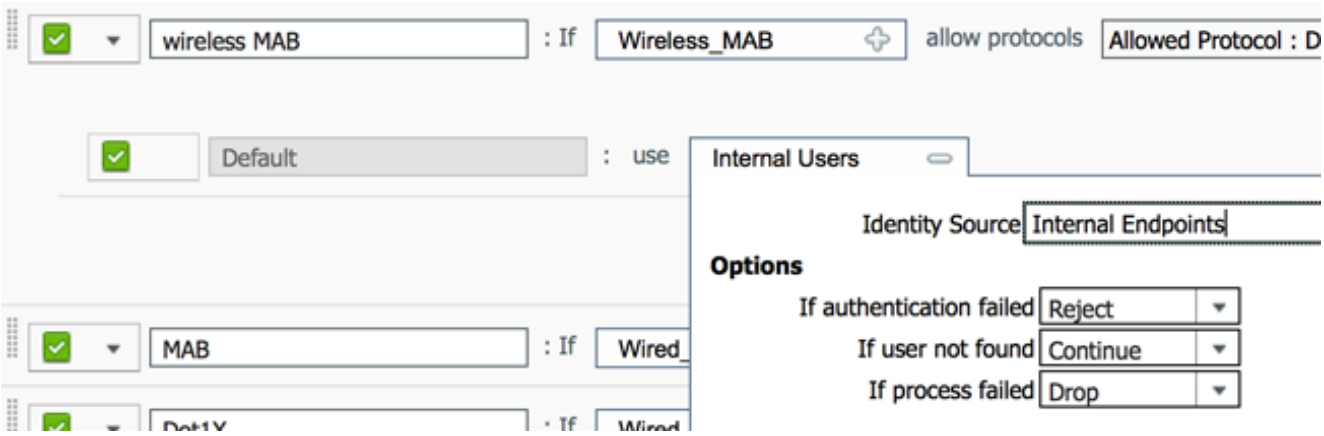


إنشاء قاعدة مصادقة

أكمل هذه الخطوات لاستخدام ملف تعريف المصادقة لإنشاء قاعدة المصادقة:

1. تحت قائمة "نهج"، انقر فوق **المصادقة**. توضح هذه الصورة مثالا لكيفية تكوين قاعدة سياسة المصادقة. في هذا المثال، يتم تكوين قاعدة سيتم تشغيلها عند اكتشاف تصفية MAC.

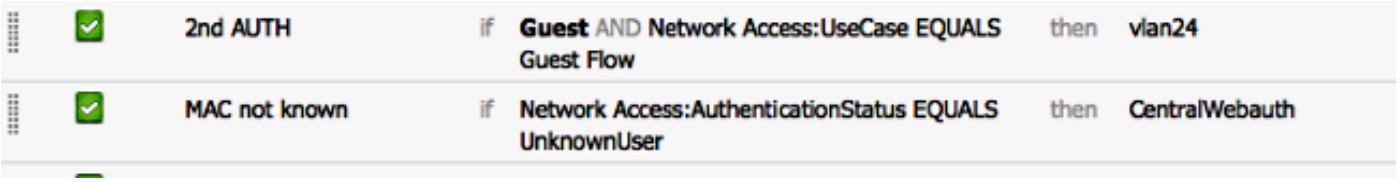
2. أدخل اسمًا لقاعدة المصادقة الخاصة بك. يستخدم هذا المثال *MAB اللاسلكي*.
3. حدد أيقونة زائد (+) في حقل شرط If.
4. أختر **حالة مركبة**، ثم أختر **Wireless_MAB**.
5. أختر "الوصول الافتراضي إلى الشبكة" كبروتوكول مسموح به.
6. انقر فوق السهم الموجود بجوار **و**... لتوسيع القاعدة بشكل أكبر.
7. انقر أيقونة **+** في حقل مصدر الهوية، واختر **نقاط النهاية الداخلية**.
8. أختر **متابعة** من القائمة المنسدلة إذا لم يتم العثور على المستخدم.



يتيح هذا الخيار مصادقة الجهاز (من خلال مصادقة الويب) حتى إذا كان عنوان MAC الخاص به غير معروف. لا يزال بإمكان عملاء dot1x المصادقة باستخدام بيانات الاعتماد الخاصة بهم ولا يجب أن يكونوا مهتمين بهذا التكوين.

إنشاء قاعدة تخويل

هناك الآن عدة قواعد للتكوين في نهج التخويل. عند اقتران الكمبيوتر الشخصي، سيتم إجراء تصفية MAC، ومن المفترض أن عنوان MAC غير معروف، لذلك يتم إرجاع مصادقة الويب وقائمة التحكم في الوصول (ACL). تظهر قاعدة *MAC غير المعروفة هذه* في الصورة أدناه ويتم تكوينها في هذا القسم.



أكمل الخطوات التالية لإنشاء قاعدة التخويل:

1. أنشئ قاعدة جديدة وأدخِل اسمًا. يستخدم هذا المثال *MAC غير المعروف*.
2. انقر أيقونة زائد (+) في حقل الشرط، واختر إنشاء شرط جديد.
3. قم بتوسيع القائمة المنسدلة **بالتعبير**.
4. أختر **الوصول إلى الشبكة**، وقم بتمديده.
5. انقر فوق **AuthenticationStatus**، واختر المشغل **Equals**.
6. أختر **UnknownUser** في الحقل الأيمن.
7. في صفحة التخويل العام، أختر **CentralWebauth** (ملف تعريف التخويل) في الحقل إلى يمين الكلمة **بعد ذلك**.وهذه الخطوة تسمح باستمرار ISE حتى وإن كان المستخدم (أو MAC) غير معروف.يتم الآن تقديم مستخدمين غير معروفين بصفحة تسجيل الدخول. ومع ذلك، بمجرد إدخال بيانات الاعتماد الخاصة بهم، يتم تقديمها مرة أخرى مع طلب مصادقة على ISE، لذلك، يجب تكوين قاعدة أخرى مع شرط يتم تلبيته إذا كان المستخدم *ضيفا*. في هذا المثال، *إذا كان UserIdentityGroup يساوي Guest* يتم إستخدامه، ومن المفترض أن جميع الضيوف ينتمون إلى هذه المجموعة.
8. انقر زر الإجراءات الموجود في نهاية قاعدة *MAC غير المعروفة*، واختر إدراج قاعدة جديدة أعلاه.**ملاحظة:** من المهم جدا أن تأتي هذه القاعدة الجديدة قبل قاعدة *ماك غير المعروفة*.
9. أدخل **المصادقة الثانية** في حقل الاسم.
10. حدد مجموعة هوية كشرط. هذا المثال يختار **ضيف**.
11. في حقل الشرط، انقر أيقونة زائد (+)، واختر أن يخلق شرط جديد.

12. اختر **الوصول إلى الشبكة**، وانقر فوق **حالة الاستخدام**.

13. اختر **يساوي** كمشغل.

14. اختر **GuestFlow** كمعامل صحيح. وهذا يعني أنك ستقبض على المستخدمين الذين قاموا بتسجيل الدخول للتو على صفحة الويب ثم يعودون بعد تغيير التفويض (جزء تدفق الضيف من القاعدة) وفقط إذا كانوا ينتمون إلى مجموعة هوية الضيف.

15. في صفحة التخويل، انقر فوق أيقونة زائد (+) (الموجودة بجوار *ذلك*) لاختيار نتيجة للقاعدة الخاصة بك.

في هذا المثال، يتم تعيين ملف تعريف تم تكوينه مسبقا (VLAN34)، ولا يتم عرض هذا التكوين في هذا المستند.

يمكنك إختيار خيار **السماح بالوصول** أو إنشاء ملف تعريف مخصص لإرجاع شبكة VLAN أو السمات التي تعجبك.

ملاحظة هامة: في الإصدار 1.3 من ISE، اعتمادا على نوع مصادقة الويب، قد لا تتم مصادفة حالة إستخدام "تدفق الضيف" بعد الآن. يجب بعد ذلك أن تحتوي قاعدة التخويل على مجموعة المستخدمين الضيف كشرط ممكن فقط.

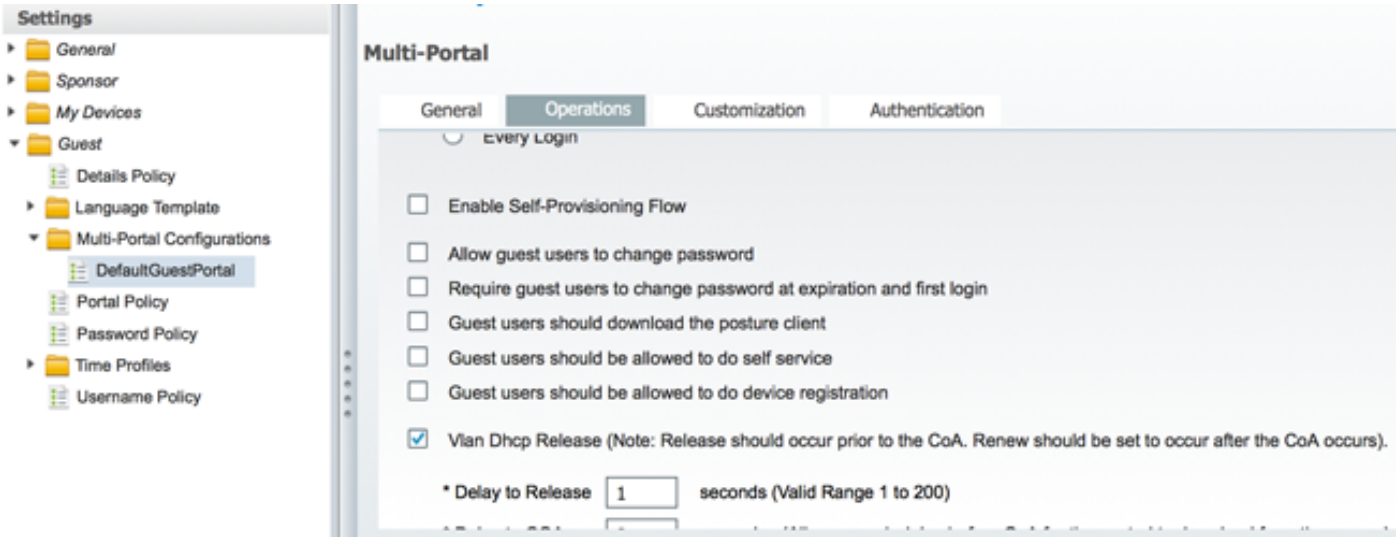
تمكين تجديد IP (إختياري)

إذا قمت بتعيين شبكة VLAN، فإن الخطوة الأخيرة هي أن يقوم جهاز الكمبيوتر الخاص بالعميل بتجديد عنوان IP الخاص به. يتم تنفيذ هذه الخطوة من خلال بوابة الضيف لعملاء Windows. إذا لم تقم بتعيين شبكة VLAN لقاعدة *AUTH الثانية* مسبقًا، فيمكنك تخطي هذه الخطوة.

لاحظ أنه في نقاط الوصول FlexConnect APs، يلزم وجود شبكة VLAN مسبقا على نقطة الوصول نفسها. لذلك، إن لا، أنت يستطيع خلقت VLAN-ACL يخطط على ال AP نفسه أو على المجموعة flex حيث أنت لا يطبق أي ACL ل ال VLAN جديد أنت تريد أن يخلق. في الواقع، يؤدي ذلك إلى إنشاء شبكة VLAN (بدون قائمة تحكم في الوصول عليها).

إذا قمت بتعيين VLAN، أكمل هذه الخطوات لتمكين تجديد IP:

1. انقر فوق **إدارة**، ثم انقر فوق **إدارة الضيوف**.
2. طقطقة **عملية إعداد**.
3. قم بتوسيع **Guest**، ثم قم بتوسيع **تكوين المنافذ المتعددة**.
4. انقر فوق **DefaultGuestPortal** أو اسم مدخل مخصص قد قمت بإنشائه.
5. انقر فوق مربع الاختيار **إصدار DHCP VLAN.ملاحظة:** يعمل هذا الخيار لعملاء Windows فقط.



تدفق حركة المرور

قد يبدو من الصعب فهم حركة المرور التي يتم إرسالها إلى أين في هذا السيناريو. فيما يلي مراجعة سريعة:

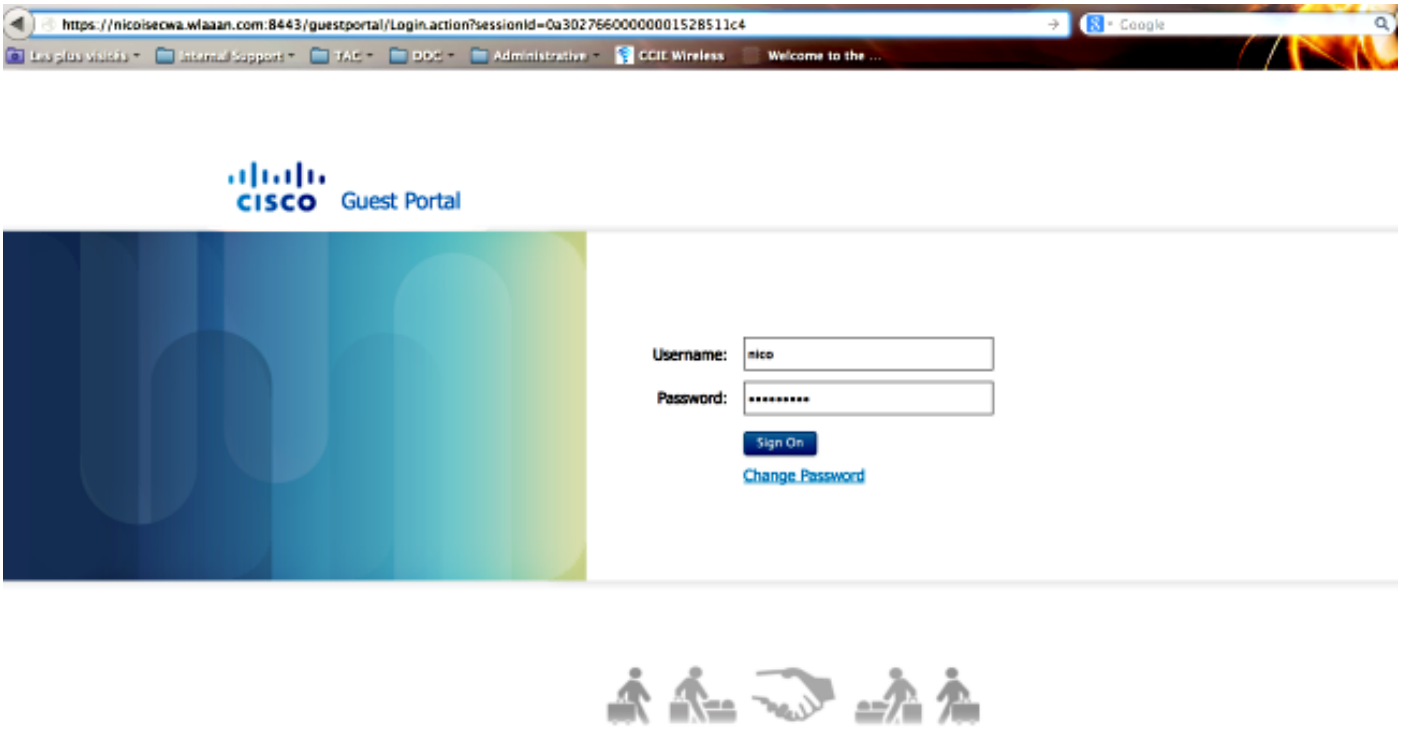
- يرسل العميل طلب اقتران عبر الهواء ل SSID.
- تعالج عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مصادقة تصفية MAC باستخدام ISE (حيث يستلم سمات إعادة التوجيه).
- يتلقى العميل إستجابة ASSOC فقط بعد اكتمال تصفية MAC.
- يقدم العميل طلب DHCP وهو **محليا** يتم تحويلها بواسطة نقطة الوصول للحصول على عنوان IP للموقع البعيد.
- في حالة central_webauth، تكون حركة المرور التي تم وضع علامة لرفضها على قائمة التحكم في الوصول (ACL) المعاد توجيهها (حتى HTTP عادة) **مركزيا** محول. إذا ليست نقطة الوصول هي التي تقوم بإعادة التوجيه ولكن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)؛ على سبيل المثال، عندما يطلب العميل أي موقع ويب، ترسل نقطة الوصول هذا إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) المضمن في CAPWAP ومزائف عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) التي تقوم بعنوان IP على موقع الويب وإعادة توجيهه نحو ISE.
- تتم إعادة توجيه العميل إلى URL لإعادة توجيه ISE. هذا هو **محليا** تم التبديل مرة أخرى (نظرا لأنه يعمل على الحصول على إذن على قائمة التحكم في الوصول (ACL) المرنة المعاد توجيهها).
- وبمجرد تشغيلها في حالة التشغيل، يتم تحويل حركة المرور محليا.

التحقق من الصحة

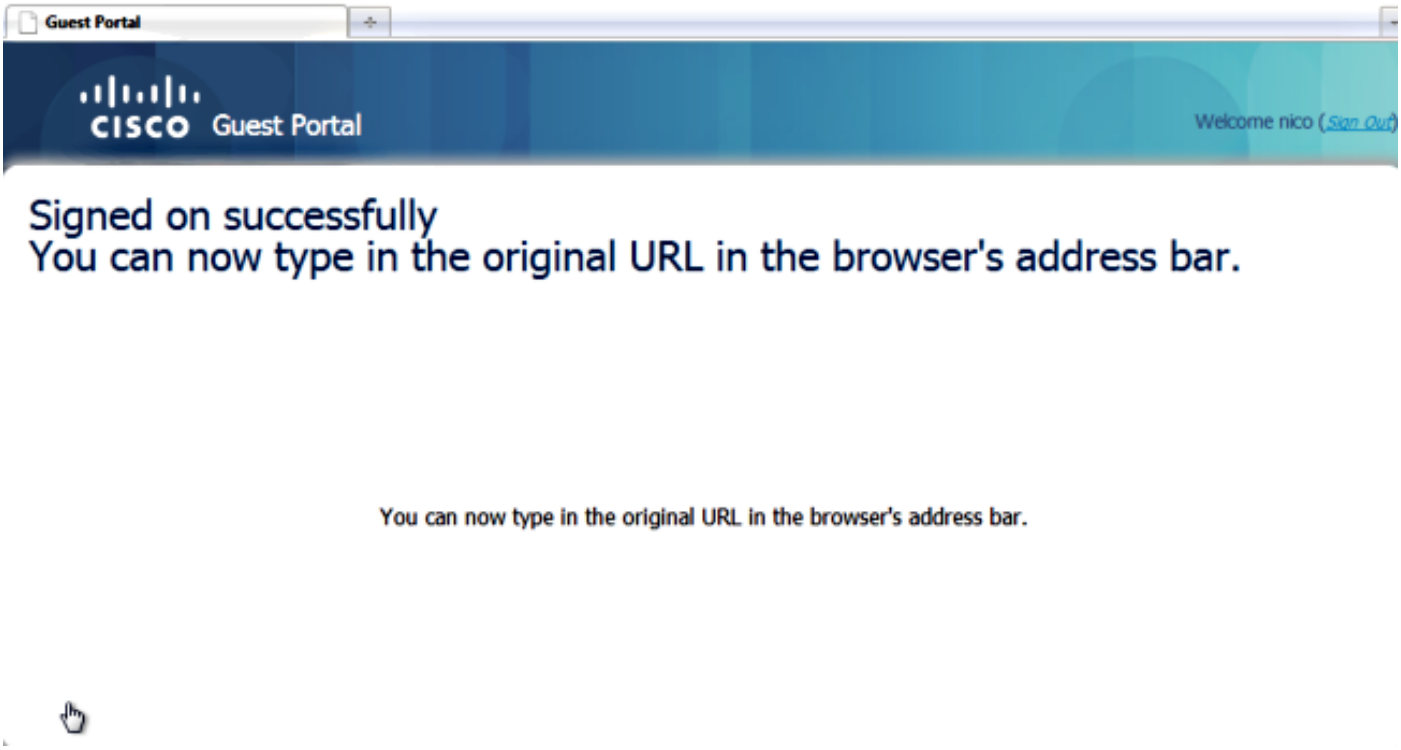
وبمجرد اقتران المستخدم ب SSID، يتم عرض التخويل في صفحة ISE.

من الأسفل إلى الأعلى، يمكنك أن ترى مصادقة تصفية عنوان MAC التي ترجع خصائص CWA. فيما يلي تسجيل دخول البوابة باسم المستخدم. بعد ذلك يرسل ISE CoA إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) والمصادقة الأخيرة هي مصادقة mac layer 2 على جانب عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، ولكن ISE يتذكر العميل واسم المستخدم ويطبق شبكة VLAN الضرورية التي قمنا بتكوينها في هذا المثال.

عند فتح أي عنوان على العميل، تتم إعادة توجيه المستعرض إلى ISE. تأكد من تكوين نظام اسم المجال (DNS) بشكل صحيح.



يتم منح الوصول إلى الشبكة بعد قبول المستخدم للنهج.



في وحدة التحكم، تتغير حالة مدير السياسة وحالة RADIUS NAC من *Posture_REQD* إلى *RUN*.

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).