دليل نشر تقنية BYOD اللاسلكية لـ FlexConnect

المحتويات

المقدمة

أصبحت الأجهزة المحمولة أكثر قوة من الناحية الحسابية وأكثر شيوعا بين المستهلكين. ويتم بيع ملايين هذه الأجهزة للمستهلكين الذين يستخدمون تقنية Wi-Fi عالية السرعة حتى يتسنى للمستخدمين الاتصال والتعاون. وقد تعود المستهلكون الآن على تحسين الإنتاجية الذي تجلبه هذه الأجهزة النقالة في حياتهم، وهم يسعون إلى إدخال تجاربهم الشخصية إلى مساحة العمل. يؤدي هذا إلى إنشاء إحتياجات الوظائف الخاصة بحل "إحضار الجهاز الخاص بك (BYOD)" في مكان العمل.

يوفر هذا المستند نشر الفرع لحل BYOD. يتصل الموظف بمعرف مجموعة خدمات الشركة (SSID) باستخدام iPad الجديد الخاص به ويتم إعادة توجيهه إلى بوابة التسجيل الذاتي. يصادق محرك خدمات الهوية من Cisco (ISE)

المستخدم مقابل Active Directory (AD) للشركة وينزل شهادة بعنوان MAC مدمج لاسم مستخدم iPad إلى iPad، بالإضافة إلى ملف تعريف ملحق يفرض إستخدام بروتوكول المصادقة المتوسع - أمان طبقة النقل (EAP-TLS) كطريقة لاتصال dot1x. استنادا إلى سياسة التخويل في ISE، يمكن للمستخدم بعد ذلك الاتصال باستخدام dot1x والحصول على الوصول إلى الموارد المناسبة.

لم تكن وظائف برنامج ISE في إصدارات برنامج وحدة تحكم الشبكة المحلية (LAN) اللاسلكية من Cisco التي تسبق الإصدار 7.2.110.0 تدعم عملاء التحويل المحليين الذين يقترنون من خلال نقاط الوصول (APs) إلى FlexConnect. يدعم الإصدار 7.2.110.0 وظائف ISE هذه لنقاط الوصول FlexConnect APs للتحويل المحلي والعملاء المعتمدين مركزيا. علاوة على ذلك، يوفر الإصدار 7.2.110.0 المدمج مع ISE 1.1.1 ميزات حل BYOD هذه (ولكن لا يقتصر عليها) للشبكة اللاسلكية:

- تنميط الجهاز ووضعه
- تسجيل الجهاز وتوفير المتطلب
- توصيل أجهزة شخصية (توفير أجهزة iOS أو Android)

ملاحظة: على الرغم من دعم أجهزة أخرى مثل أجهزة الكمبيوتر الشخصي أو أجهزة Mac اللاسلكية ومحطات العمل، فهي غير مشمولة في هذا الدليل.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- المحولات Cisco Catalyst Switches
- وحدات التحكم في الشبكة المحلية اللاسلكية (WLAN) من Cisco
- برنامج Cisco WLAN Controller (WLC) الإصدار 7.2.110.0 والإصدارات الأحدث
- نقاط الوصول من شبكة 802.11n في وضع FlexConnect
- برنامج Cisco ISE الإصدار 1.1.1 والإصدارات الأحدث
- Windows 2008 AD مع جهة منح الشهادة (CA)
- خادم DHCP
- خادم نظام اسم المجال (DNS)
- بروتوكول وقت الشبكة (NTP)
- الكمبيوتر المحمول العميل اللاسلكي والهاتف الذكي وأجهزة الكمبيوتر اللوحية (نظام التشغيل iOS من Apple ونظام التشغيل Android و Windows و Mac)

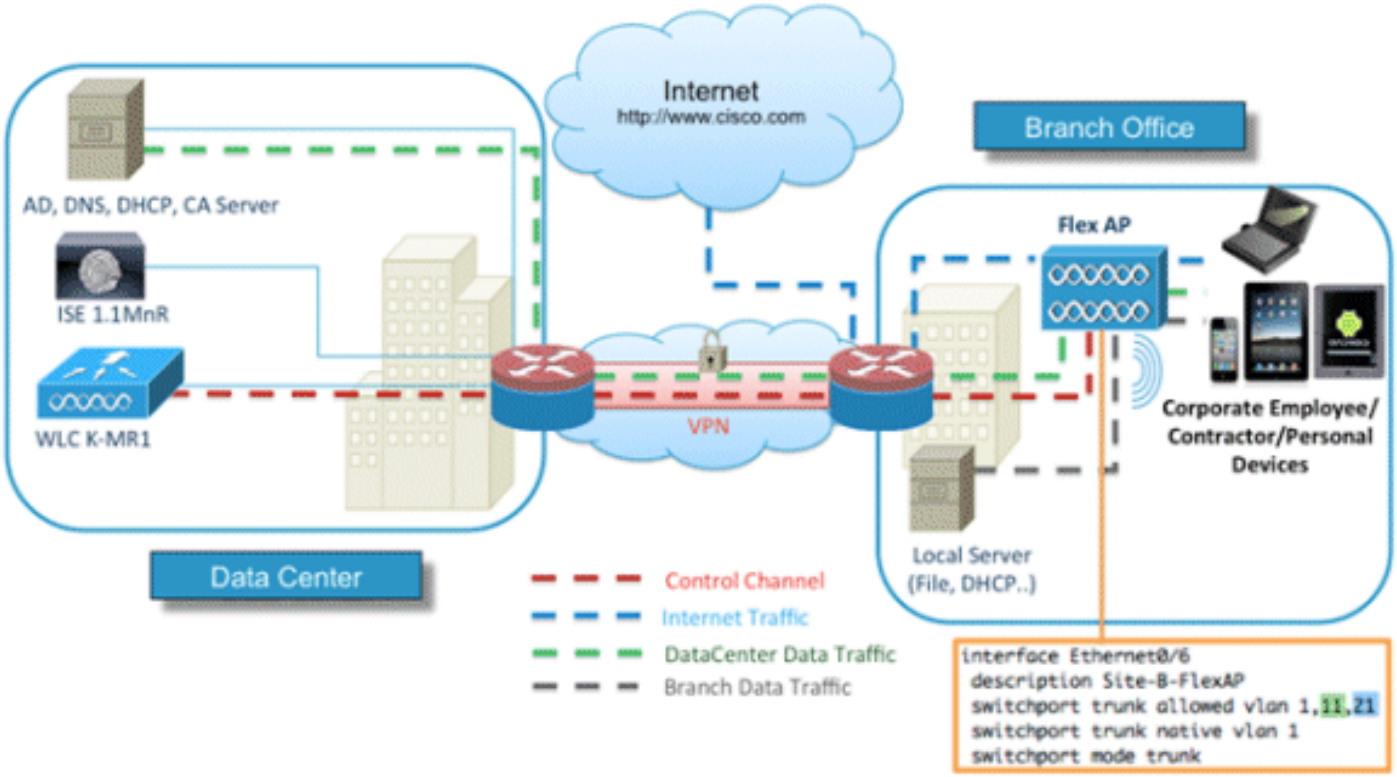
ملاحظة: راجع ملاحظات الإصدار الخاصة بوحدات تحكم الشبكة المحلية اللاسلكية من Cisco ونقاط الوصول في الوضع Lightweight للإصدار 7.2.110.0 للحصول على معلومات مهمة حول إصدار هذا البرنامج. قم بتسجيل الدخول إلى موقع Cisco.com للحصول على أحدث ملاحظات الإصدار قبل تحميل البرنامج واختباره.

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

أمر.

طوبولوجيا

يلزم وجود إعداد شبكة أدنى، كما هو موضح في هذا المخطط لتنفيذ هذه الميزات واختبارها بشكل صحيح:



لهذه المحاكاة، تحتاج إلى شبكة مع نقطة وصول FlexConnect، وموقع محلي/بعيد مع DHCP المحلي و DNS و WLC و ISE. يتم توصيل نقطة الوصول FlexConnect بشنطة لاختبار التحويل المحلي باستخدام شبكات VLAN متعددة.

تسجيل الجهاز وتوفير ملتمس

يجب تسجيل الجهاز بحيث يمكن للمطالب الأصلي الخاص به توفير مصادقة dot1x. استنادا إلى نهج المصادقة الصحيح، تتم إعادة توجيه المستخدم إلى صفحة الضيف وتتم مصادقته بواسطة بيانات اعتماد الموظف. يرى المستخدم صفحة تسجيل الجهاز، والتي تطلب معلومات الجهاز الخاصة به. تبدأ عملية توفير الجهاز بعد ذلك. إذا لم يكن نظام التشغيل (OS) مدعوما للتوفير، تتم إعادة توجيه المستخدم إلى مدخل تسجيل الأصول لوضع علامة على ذلك الجهاز للوصول إلى مجرى مصادقة MAB) MAC). إذا كان نظام التشغيل مدعوما، تبدأ عملية التسجيل وتقوم بتكوين المطلوب الأصلي للجهاز لمصادقة dot1x.

بوابة تسجيل الأصول

بوابة تسجيل الأصول هي عنصر النظام الأساسي ISE الذي يسمح للموظفين ببدء تشغيل نقاط النهاية من خلال عملية المصادقة والتسجيل.

يمكن للمسؤولين حذف الأصول من صفحة هويات نقاط النهاية. يمكن لكل موظف تحرير الأصول التي قام بتسجيلها وحذفها ووضعها في قائمة سوداء. يتم تعيين نقاط النهاية المدرجة على القائمة السوداء إلى مجموعة هوية قائمة سوداء، ويتم إنشاء سياسة تخويل لمنع الوصول إلى الشبكة بواسطة نقاط النهاية المدرجة على القائمة السوداء.

بوابة التسجيل الذاتي

في تدفق مصادقة الويب المركزية (CWA)، تتم إعادة توجيه الموظفين إلى بوابة تتيح لهم إدخال بيانات الاعتماد الخاصة بهم والمصادقة عليها وإدخال مواصفات الأصل المعين الذي يرغبون في تسجيله. يسمى هذا المدخل مدخل الإمداد الذاتي وهو مماثل لبوابة تسجيل الأجهزة. وهو يسمح للموظفين بإدخال عنوان MAC وكذلك وصف ذي مغزى لنقطة النهاية.

المصادقة والإمداد

بمجرد أن يقوم الموظفون بتحديد مدخل التسجيل الذاتي، يتم تحديهم لتوفير مجموعة من بيانات اعتماد الموظفين الصالحة للمتابعة إلى مرحلة التوفير. بعد المصادقة الناجحة، يمكن توفير نقطة النهاية في قاعدة بيانات نقاط النهاية، ويتم إنشاء شهادة لنقطة النهاية. يسمح إرتباط موجود على الصفحة للموظف بتنزيل معالج SPW) Client Pilot).

ملاحظة: ارجع إلى مقالة FlexConnect Feature Matrix Cisco لعرض أحدث مصفوفة ميزة FlexConnect ل BYOD.

الإمداد بنظام التشغيل iOS (iPhone/iPad/iPod)

بالنسبة لتكوين EAP-TLS، يتبع ISE عملية التسجيل في OTA) Apple over-Air):

- بعد المصادقة الناجحة، يقوم محرك التقييم بتقييم سياسات إمداد العميل، والتي ينتج عنها ملف تعريف مسبب.
- إذا كان ملف تخصيص المتطلب خاص بإعداد EAP-TLS، فإن عملية OTA تحدد ما إذا كان ISE يستخدم التوقيع الذاتي أو الموقع من قبل مرجع مصدق غير معروف. إذا كان أحد الشروط صحيحا، فيطلب من المستخدم تنزيل شهادة ISE أو CA قبل بدء عملية التسجيل.
- بالنسبة لطرق EAP الأخرى، يدفع ISE التوصيف النهائي عند المصادقة الناجحة.

توفير ل Android

نظرا لاعتبارات الأمان، يجب تنزيل عامل Android من موقع سوق Android ولا يمكن توفيره من ISE. تقوم Cisco بتحميل إصدار مرشح إصدار من المعالج في سوق Android من خلال حساب ناشر سوق Cisco Android.

هذه هي عملية توفير Android:

1. تستخدم Cisco مجموعة أدوات تطوير البرامج (SDK) لإنشاء حزمة Android مع امتداد .apk.
2. تقوم Cisco بتحميل حزمة إلى سوق Android.
3. يقوم المستخدم بتكوين النهج في توفير العميل باستخدام المعلمات المناسبة.
4. بعد تسجيل الجهاز، تتم إعادة توجيه المستخدم النهائي إلى خدمة إمداد العميل عند فشل مصادقة dot1x.
5. توفر صفحة مدخل التوفير زر يقوم بإعادة توجيه المستخدم إلى مدخل سوق Android حيث يمكنهم تنزيل SPW.
6. يتم تشغيل SPW من Cisco ويتم توفير المطالب: يقوم SPW باكتشاف ISE وتنزيل ملف التعريف من ISE.يقوم SPW بإنشاء زوج مفاتيح/فرق EAP-TLS.يقوم SPW بإجراء إستدعاء طلب وكيل بروتوكول تسجيل الشهادة البسيط (SCEP) ل ISE ويحصل على الشهادة.يطبق SPW توصيفات اللاسلكي.يؤدي SPW إلى إعادة المصادقة إذا تم تطبيق التوصيفات بنجاح.مخرج SPW.

التسجيل الذاتي لبطاقة BYOD اللاسلكية المزدوجة لشبكة SSID

هذه هي عملية التسجيل الذاتي لمعرف SSID اللاسلكي المزدوج BYOD:

1. يرتبط المستخدم ب SSID Guest.
2. يقوم المستخدم بفتح مستعرض ويعاد توجيهه إلى بوابة ضيف ISE CWA.
3. يدخل المستخدم اسم مستخدم وكلمة مرور للموظف في مدخل الضيف.
4. يقوم ISE بمصادقة المستخدم، وبناء على حقيقة أنه موظف وليس ضيفا، فإنه يعيد توجيه المستخدم إلى صفحة ضيف تسجيل جهاز الموظف.
5. يتم ملء عنوان MAC مسبقا في صفحة ضيف تسجيل الأجهزة لمعرف الجهاز. يدخل المستخدم وصفا ويقبل سياسة الاستخدام المقبول (AUP) إذا لزم الأمر.
6. يحدد المستخدم **قبول** ويبدأ في تنزيل SPW وتثبيته.
7. يتم توفير مقدم الطلب لجهاز ذلك المستخدم مع أي شهادات.
8. يحدث CoA، ويعيد الجهاز تعيين SSID للشركة (CORP) ويصادق مع EAP-TLS (أو طريقة تخويل أخرى مستخدمة لذلك الطالب).

التسجيل الذاتي لبطاقة BYOD اللاسلكية أحادية SSID

في هذا السيناريو، يوجد معرف SSID واحد للوصول إلى الشركة (CORP) يدعم كلا من بروتوكول المصادقة الموسع المحمي (PEAP) و EAP-TLS. لا يوجد SSID للضيف.

هذه هي عملية التسجيل الذاتي لمعرف SSID اللاسلكي الفردي لترتيب BYOD:

1. يرتبط المستخدم ب CORP.
2. يدخل المستخدم اسم مستخدم وكلمة مرور للموظف في طلب مصادقة PEAP.
3. يصادق ISE المستخدم، واستنادا إلى أسلوب PEAP، يوفر سياسة تخويل للقبول مع إعادة التوجيه إلى صفحة ضيف تسجيل جهاز الموظف.
4. يقوم المستخدم بفتح مستعرض ويعاد توجيهه إلى صفحة ضيف تسجيل جهاز الموظف.
5. يتم ملء عنوان MAC مسبقا في صفحة ضيف تسجيل الأجهزة لمعرف الجهاز. يقوم المستخدم بإدخال وصف ويقبل بروتوكول AUP.
6. يحدد المستخدم **قبول** ويبدأ في تنزيل SPW وتثبيته.
7. يتم توفير مقدم الطلب لجهاز ذلك المستخدم مع أي شهادات.
8. يحدث CoA، ويعيد الجهاز تعيين SSID الخاص ب CORP ويصادق مع EAP-TLS.

تكوين الميزة

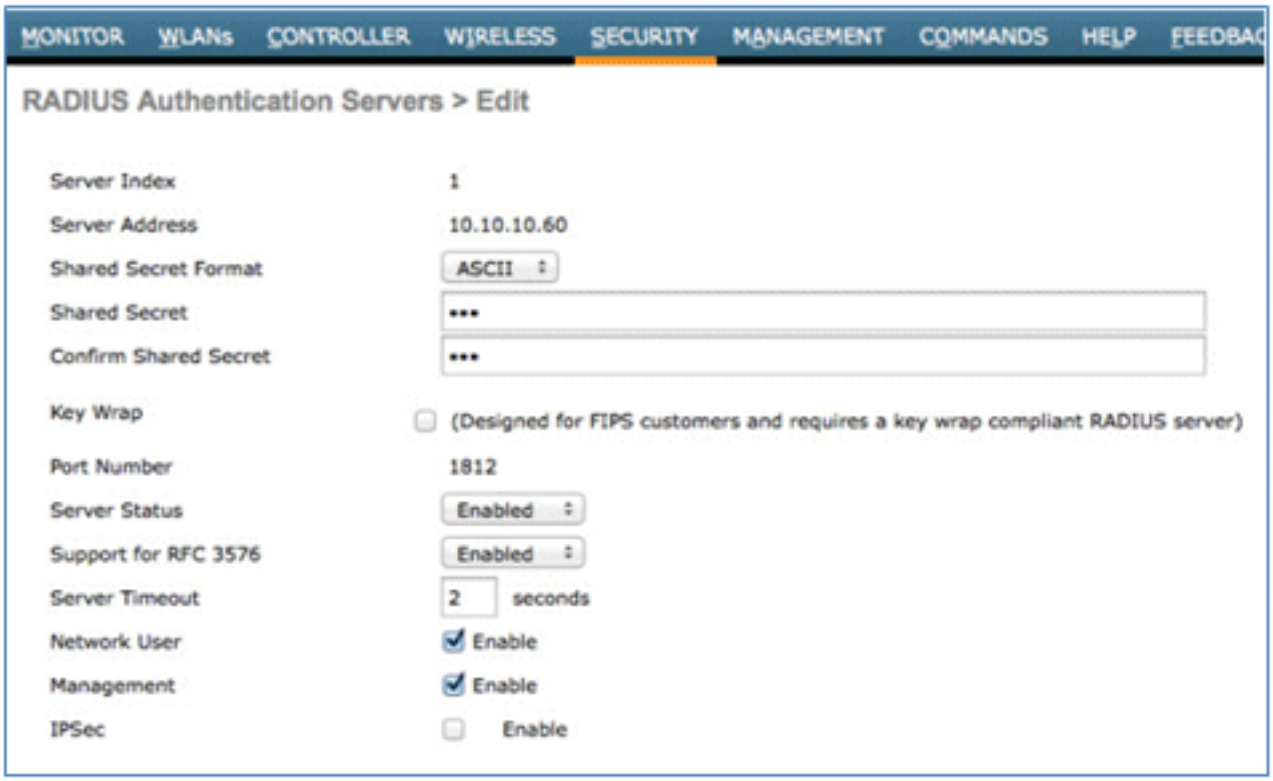
أتمت هذا steps in order to بدأت تشكيل:

1. لهذا الدليل، تأكد من أن إصدار WLC هو 7.2.110.0 أو إصدار أحدث.

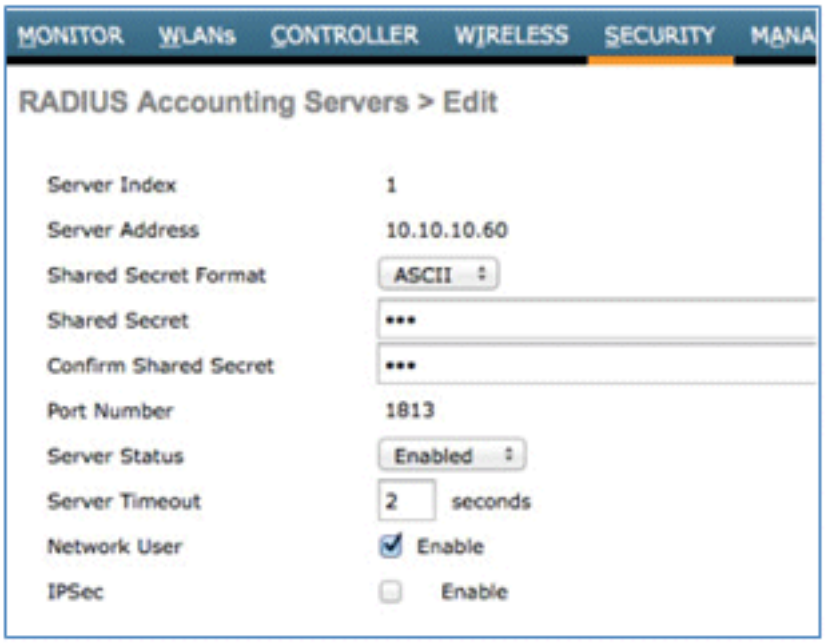
2. انتقل إلى **الأمان** > **RADIUS** > **المصادقة**، وأضف خادم RADIUS إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

3. إضافة ISE 1.1.1 إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC):

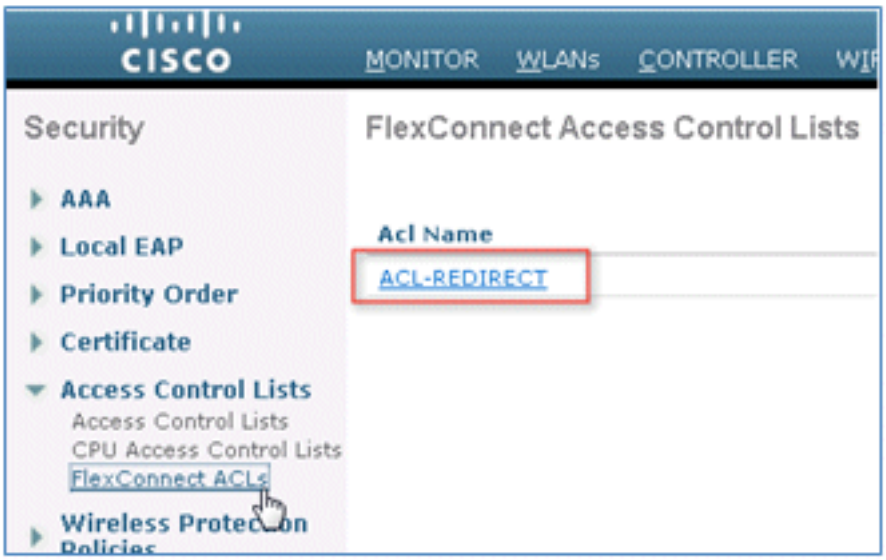
أدخل سر مشترك.قم بتعيين دعم RFC 3576 إلى **ممكن**.



4. قم بإضافة خادم ISE نفسه كخادم محاسبة RADIUS.



3. قم بإنشاء قائمة تحكم في الوصول (ACL) سابقة للمصادقة ل WLC لاستخدامها في سياسة ISE لاحقا. انتقل إلى WLC > **الأمان > قوائم التحكم في الوصول > قوائم التحكم في الوصول (ACL) لنظام FlexConnect**، وقم بإنشاء قائمة تحكم في الوصول (ACL) جديدة لنظام FlexConnect باسم ACL-REDIRECT (في هذا المثال).

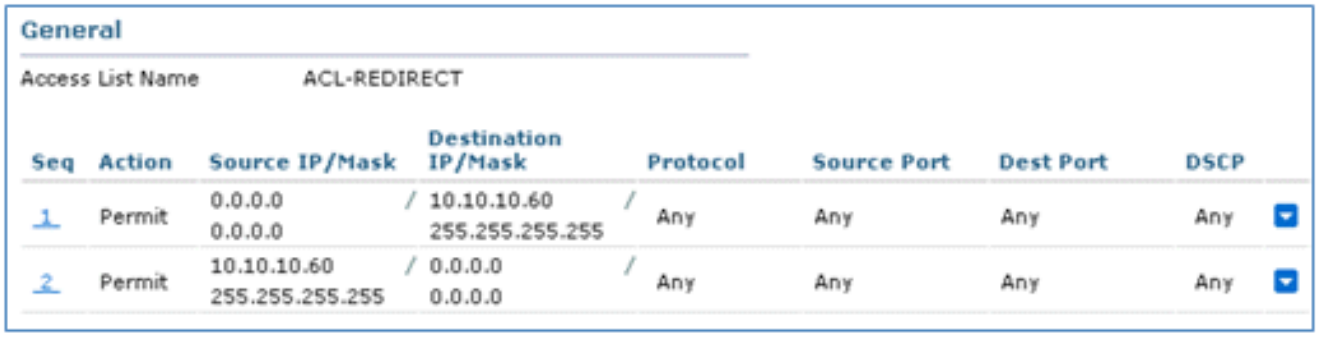


6. في قواعد قائمة التحكم في الوصول (ACL)، يمكنك السماح لجميع حركة المرور من/إلى محرك خدمات الهوية (ISE)، والسماح لحركة مرور العميل أثناء تزويد العميل.

للقاعدة الأولى (التسلسل 1):

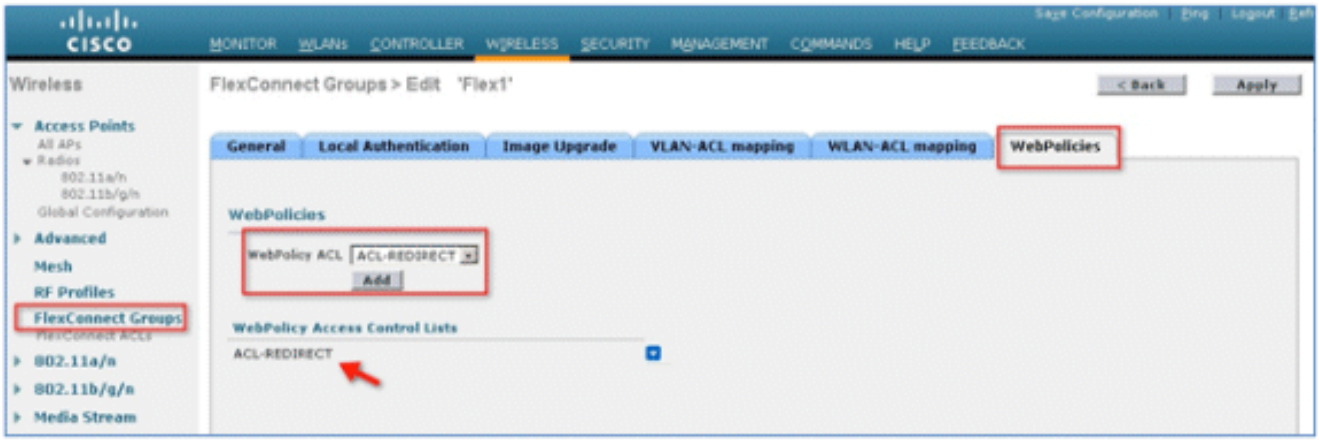
قم بتعيين المصدر إلى **أي**.ip set (عنوان **255.255.255.255** NetMask /(ISE.تعيين إجراء **للسماح**.

بالنسبة للقاعدة الثانية (التسلسل 2)، قم بتعيين مصدر IP (عنوان ISE)/ قناع 255.255.255.255 على **أي** إجراء **للسماح**.



7. إنشاء مجموعة FlexConnect جديدة باسم Flex1 (في هذا المثال):

انتقل إلى **مجموعة FlexConnect** > علامة التبويب **سياسات الويب**.ضمن حقل قائمة التحكم في الوصول (ACL) ل WebPolicy، انقر فوق **إضافة**، وحدد **ACL-REDIRECT** أو قائمة التحكم في الوصول (ACL) ل FlexConnect التي تم إنشاؤها مسبقا.تأكد من أنه يقوم بملء حقل **قوائم التحكم في الوصول إلى WebPolicy**.



8. طقطقة **يطبق ويحفظ تشكيل**.

تكوين شبكة WLAN

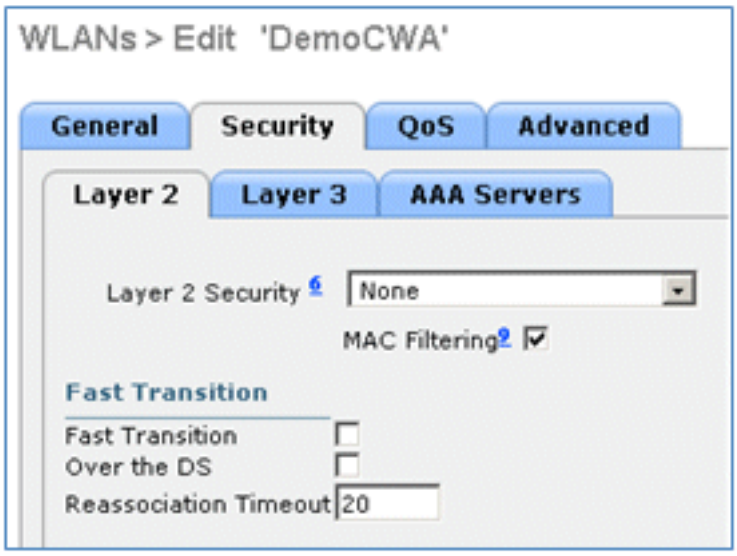
أتمت هذا steps in order to شكلت ال WLAN:

1. إنشاء WLAN SSID مفتوح لمثال SSID المزدوج:

أدخل اسم شبكة WLAN: **DemoCWA** (في هذا المثال).حدد خيار **التمكين** للحالة.

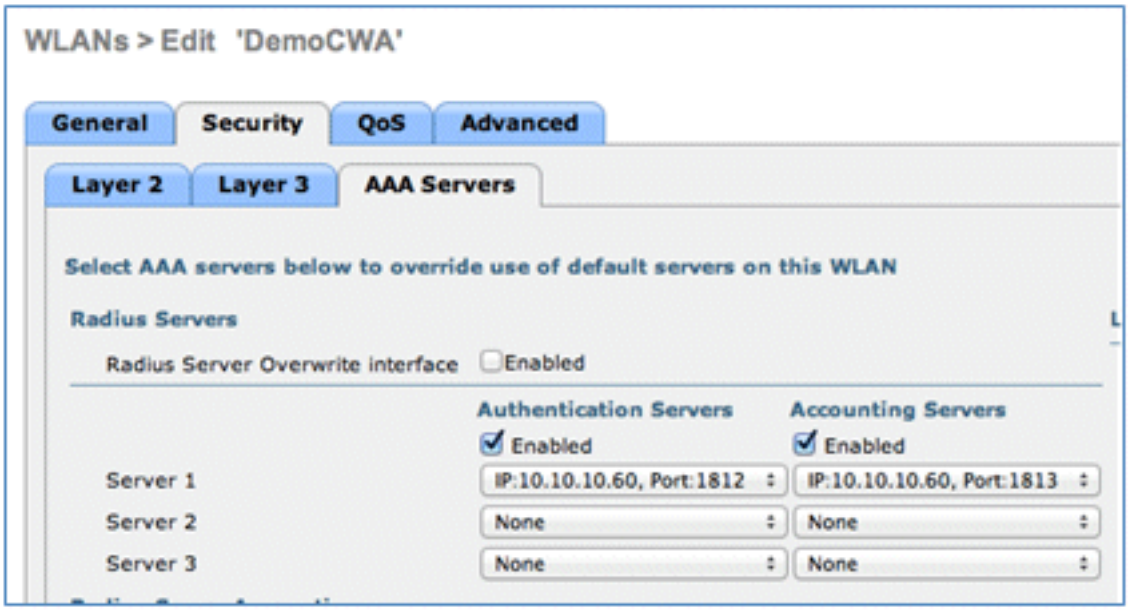
2. انتقل إلى صفحة **التأمين** > صفحة **الطبقة 2**، واضبط الخصائص التالية:

أمان الطبقة 2: **لا يوجد**تصفية MAC: **ممكن** (المربع محدد)انتقال سريع: **معطل** (لم يتم تحديد المربع)



3. انتقل إلى علامة التبويب **خوادم AAA**، وقم بضبط السمات التالية:

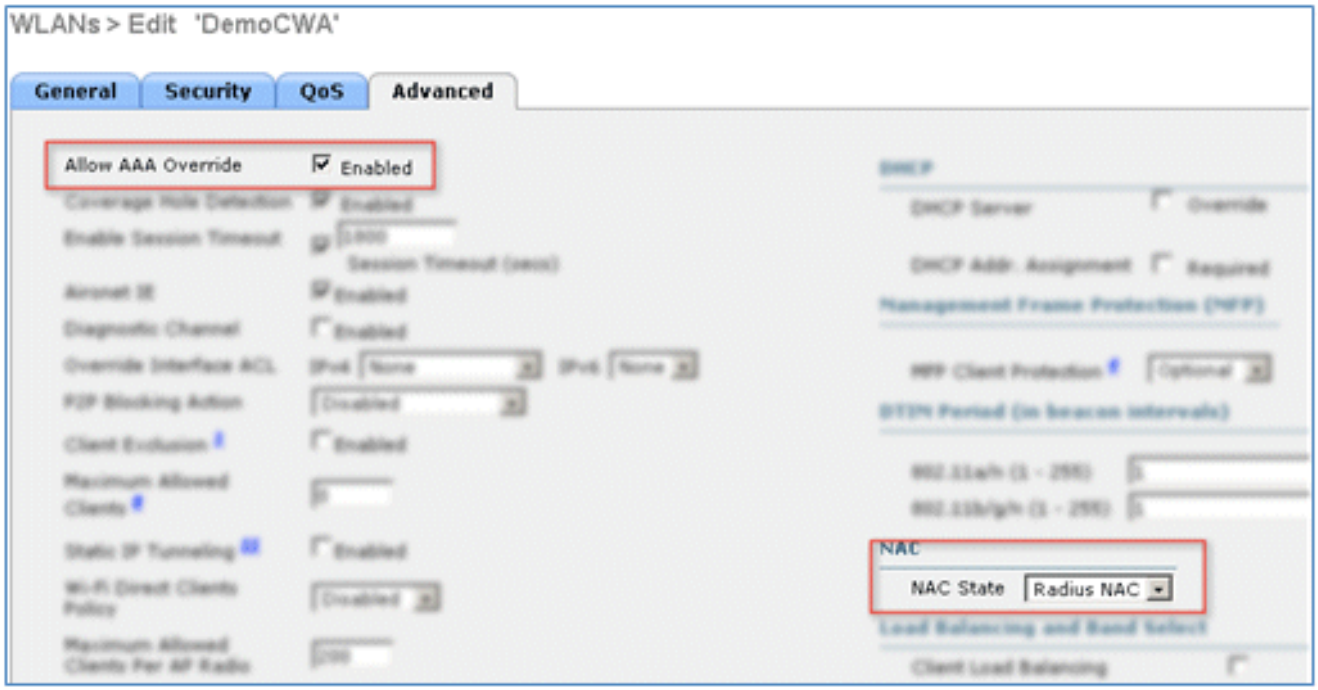
خوادم المصادقة والحساب: **ممكن**الخادم 1: *<عنوان ISE IP>*



4. قم بالتمرير لأسفل من علامة التبويب **خوادم AAA**. تحت ترتيب أولوية المصادقة لمستخدم مصادقة الويب، تأكد من إستخدام **RADIUS** للمصادقة وعدم إستخدام الآخرين.

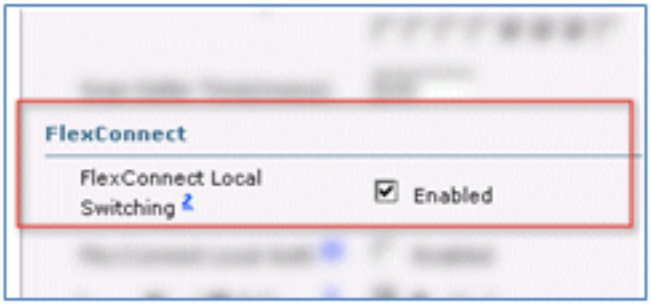
5. انتقل إلى علامة التبويب **خيارات متقدمة**، وقم بضبط السمات التالية:

السماح بتجاوز AAA: **ممكن**حالة NAC: **RADIUS NAC**

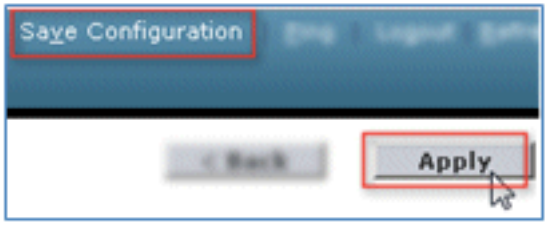


ملاحظة: لا يكون التحكم في الدخول إلى شبكة NAC) RADIUS) مدعوما عندما تكون نقطة الوصول FlexConnect في وضع غير متصل. وبالتالي، إذا كانت نقطة الوصول من FlexConnect في الوضع المستقل وفقدت الاتصال بعنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فسيتم قطع اتصال جميع العملاء، ولم يعد يتم الإعلان عن SSID.

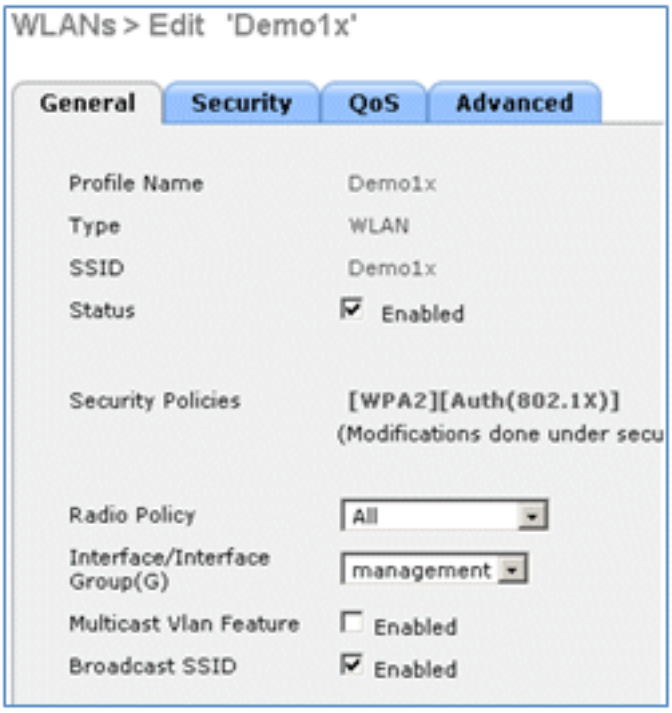
6. قم بالتمرير لأسفل في علامة التبويب خيارات متقدمة واضبط التحويل المحلي ل FlexConnect إلى **ممكن**.



7. طقطقة **يطبق ويحفظ تشكيل**.

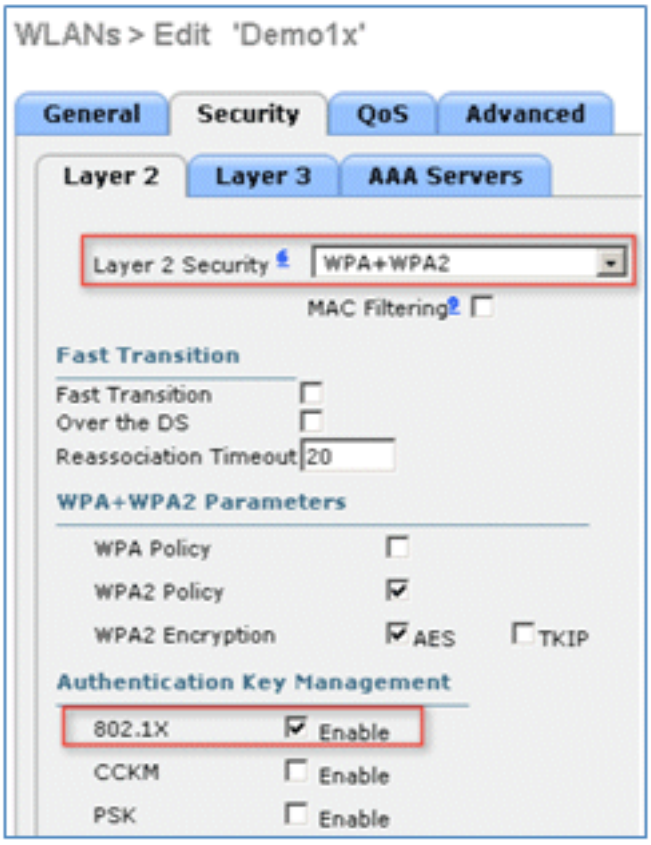


8. قم بإنشاء WLAN SSID باسم **Demo1x** (في هذا المثال) ل 802.1X لسيناريوهات SSID أحادية ومزدوجة.



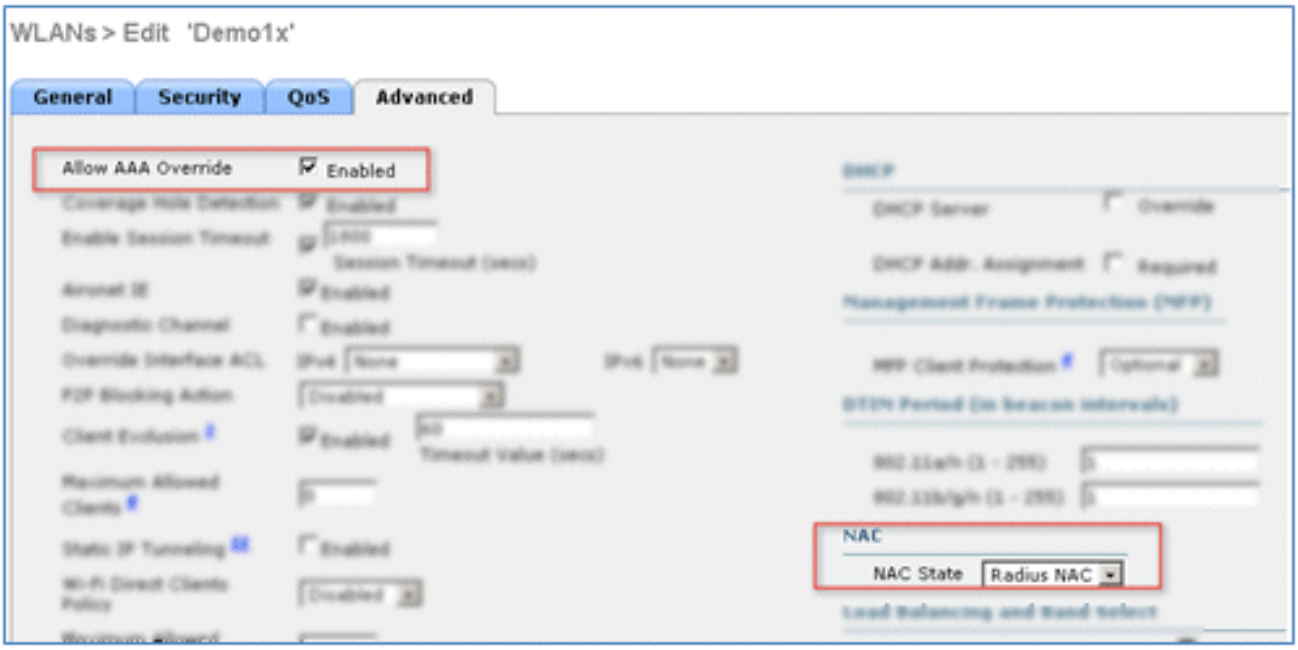
9. انتقل إلى صفحة **التأمين** > صفحة **الطبقة 2**، واضبط الخصائص التالية:

أمان الطبقة 2: **WPA+WPA2**انتقال سريع: **معطل** (لم يتم تحديد المربع)إدارة مفاتيح المصادقة: IX.802: **تمكين**

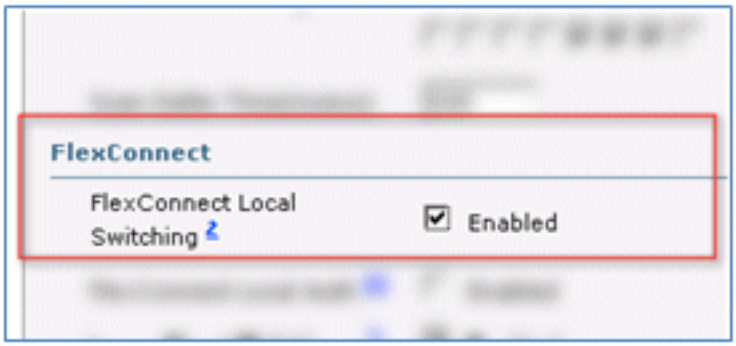


10. انتقل إلى علامة التبويب **خيارات متقدمة**، وقم بضبط السمات التالية:

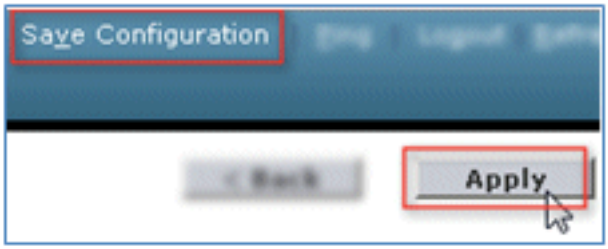
السماح بتجاوز AAA: **ممكن**حالة NAC: **RADIUS NAC**



قم بالتمرير لأسفل في علامة التبويب **خيارات متقدمة**، واضبط التحويل المحلي ل FlexConnect إلى **ممكن**.1



12. طقطقة **يطبق ويحفظ تشكيل**.



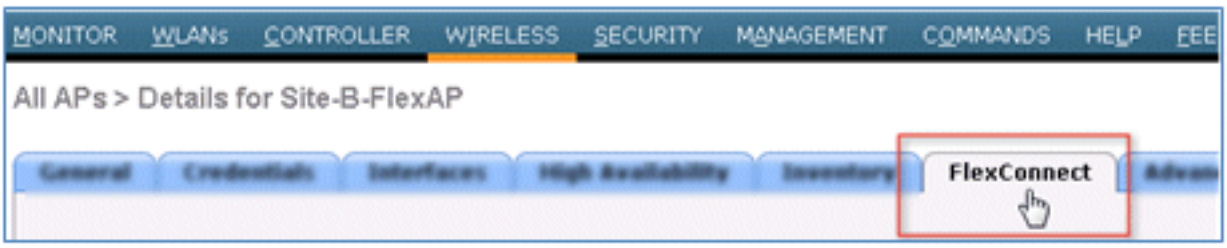
13. تأكد من إنشاء كل من شبكات WLAN الجديدة.

تكوين نقطة الوصول عبر الإنترنت FlexConnect

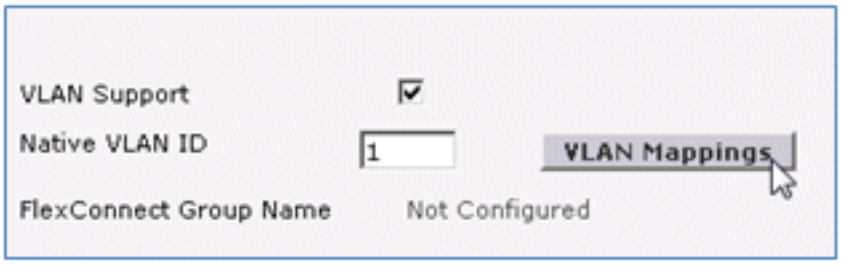
أتمت هذا steps in order to شكلت FlexConnect AP:

1. انتقل إلى **WLC > لاسلكي**، وانقر فوق نقطة الوصول FlexConnect AP الهدف.

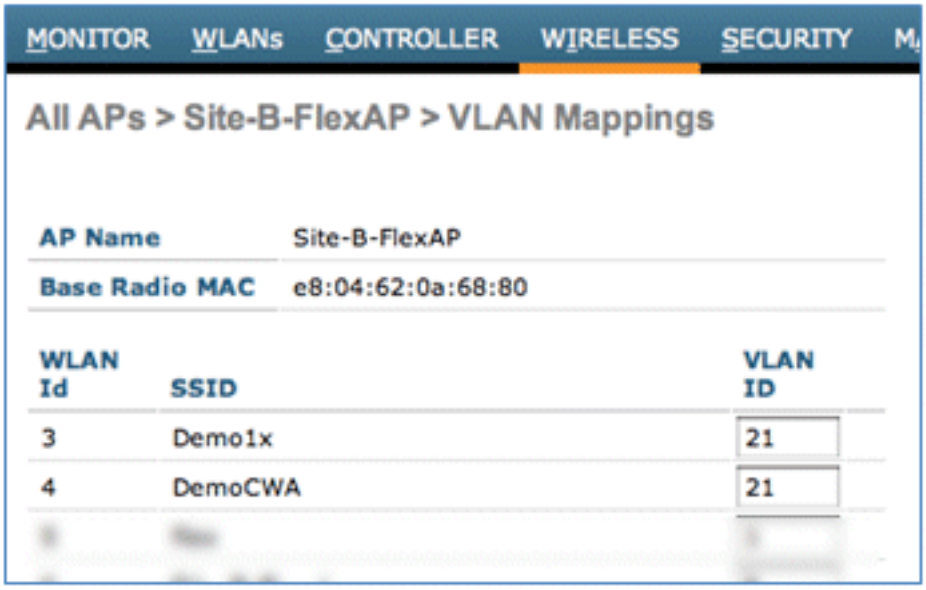
2. انقر فوق علامة التبويب **FlexConnect**.



3. مكنت دعم VLAN (صندوق يكون محددا)، ثبتت ال VLAN id أهلي طبيعي، وطقطقة **VLAN يخطط**.



4. ثبت ال VLAN id إلى **21** (في هذا مثال) ل ال SSID للتحويل المحلي.



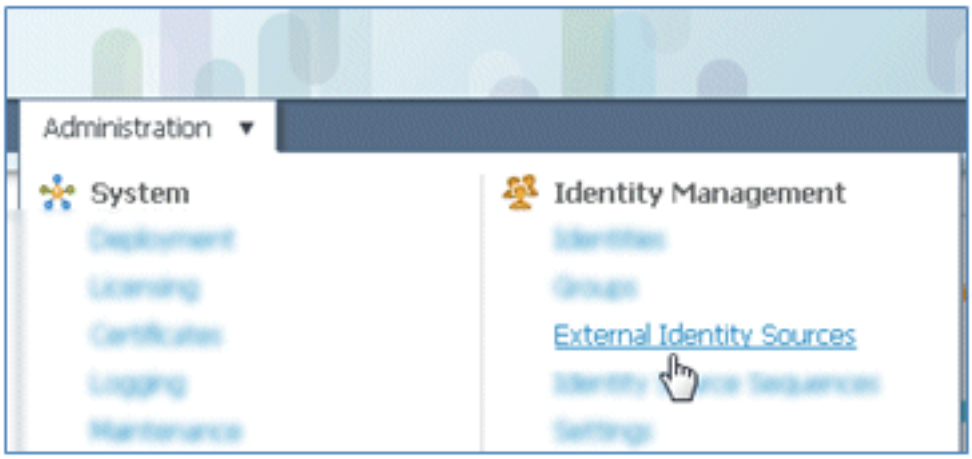
5. طقطقة **يطبق ويحفظ تشكيل**.

تكوين ISE

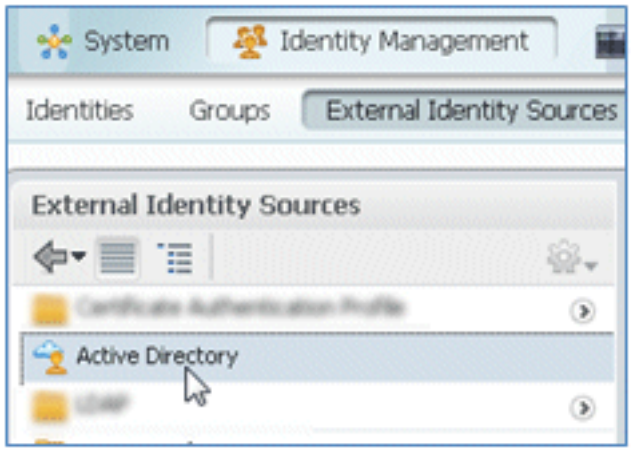
أتمت هذا steps in order to شكلت ال ISE:

1. سجل الدخول إلى خادم *https://ise*> :ISE<.

2. انتقل إلى **إدارة** > **إدارة الهوية** > **مصادر الهوية الخارجية**.

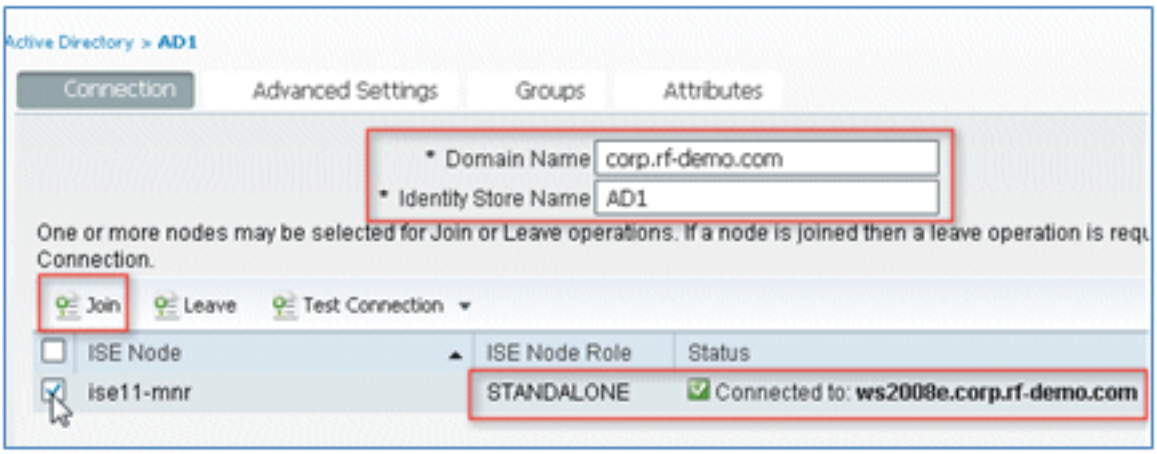


3. انقر فوق **Active Directory**.

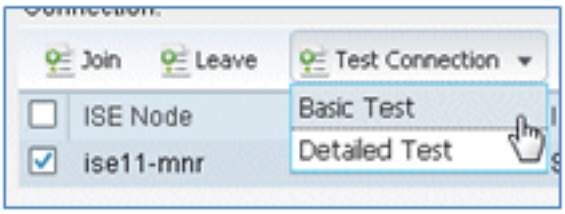


4. في علامة تبويب التوصيل:

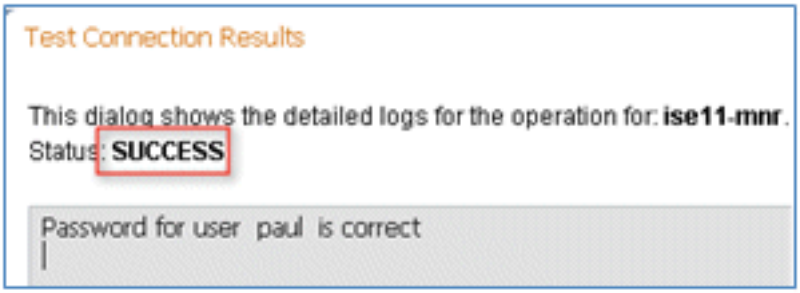
قم بإضافة اسم المجال ل **corp.rf-demo.com** (في هذا المثال)، وقم بتغيير إعداد اسم مخزن الهوية الافتراضي إلى **AD1**.انقر على **حفظ التكوين**.انقر فوق **انضمام**، وقم بتوفير اسم مستخدم حساب مسؤول AD وكلمة المرور المطلوبة للانضمام.يجب أن تكون الحالة خضراء. تمكين **الاتصال ب:** (تم تحديد المربع).



5. قم بإجراء إختبار اتصال أساسي ب AD مع مستخدم المجال الحالي.

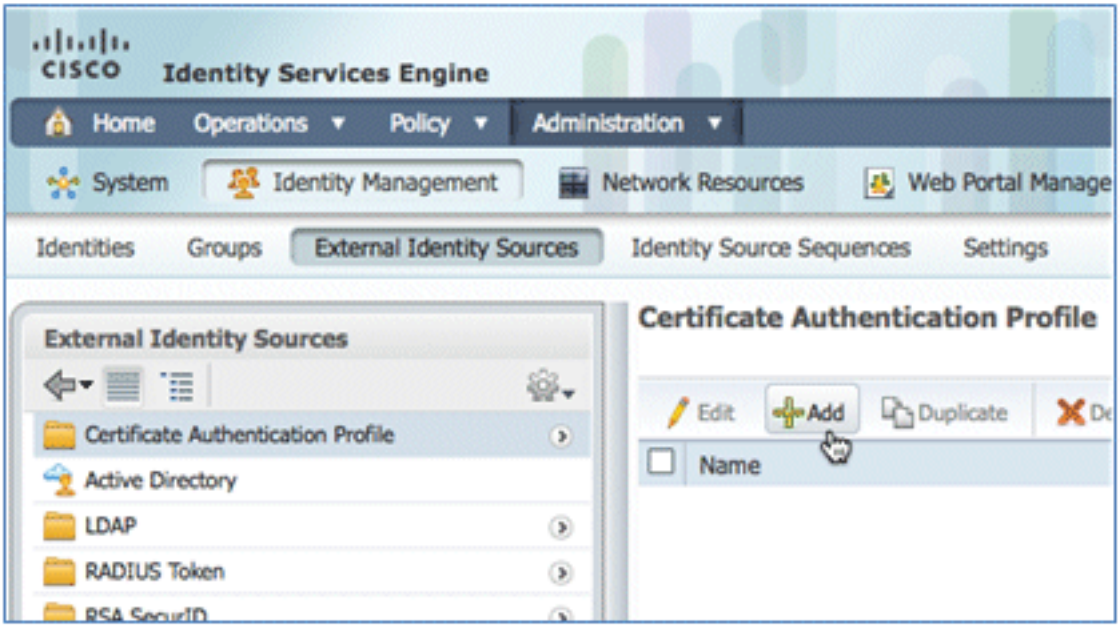


6. إذا نجح التوصيل ب AD، سيؤكد حوار أن كلمة المرور صحيحة.

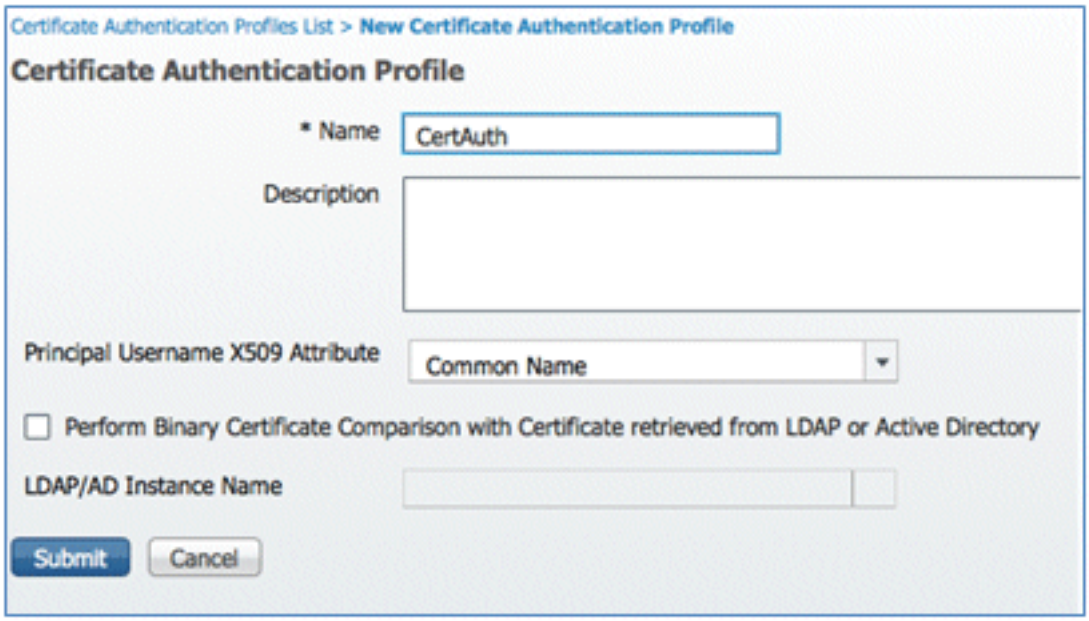


7. انتقل إلى **إدارة** > **إدارة الهوية** > **مصادر الهوية الخارجية**:

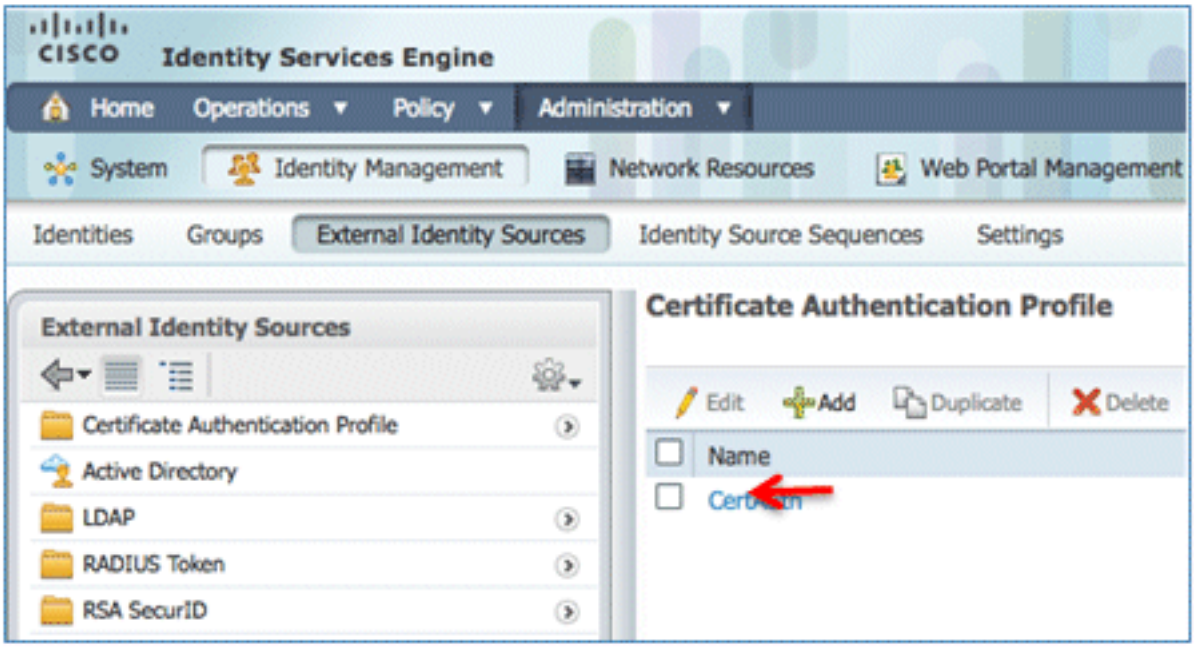
انقر على **ملف تعريف مصادقة الشهادة**.انقر على **إضافة** للحصول على توصيف مصادقة شهادة جديد (CAP).



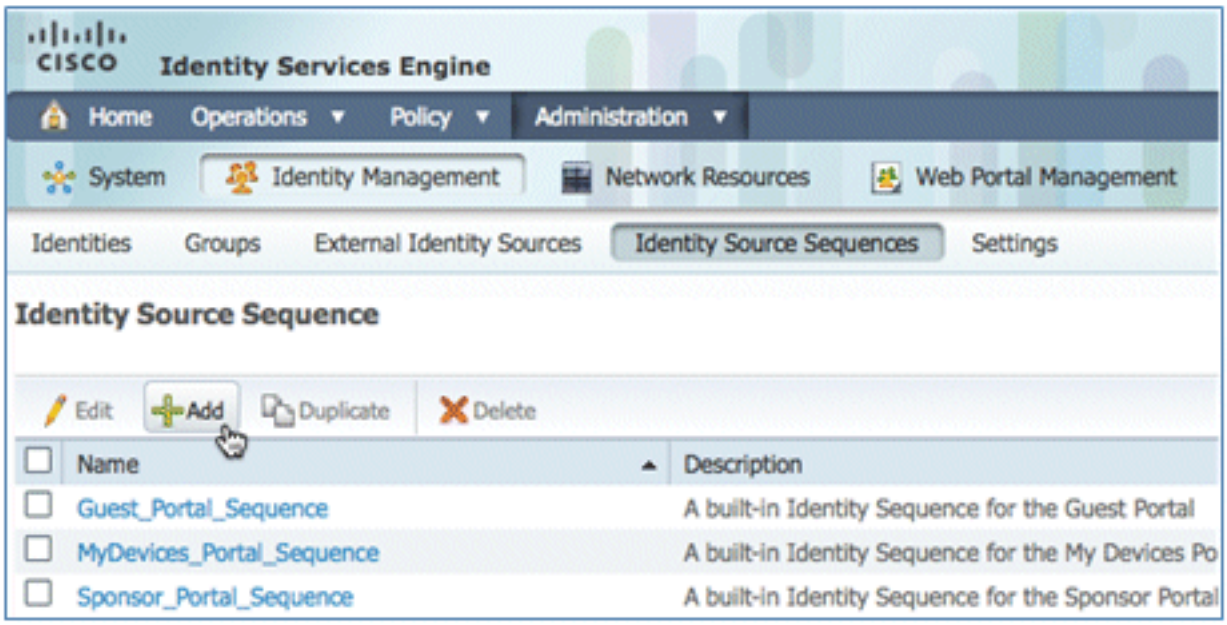
8. أدخل اسم **CertAuth** (في هذا المثال) ل CAP؛ بالنسبة للسمة X509 الخاصة باسم المستخدم الرئيسي، حدد **الاسم الشائع**؛ ثم انقر فوق **إرسال**.



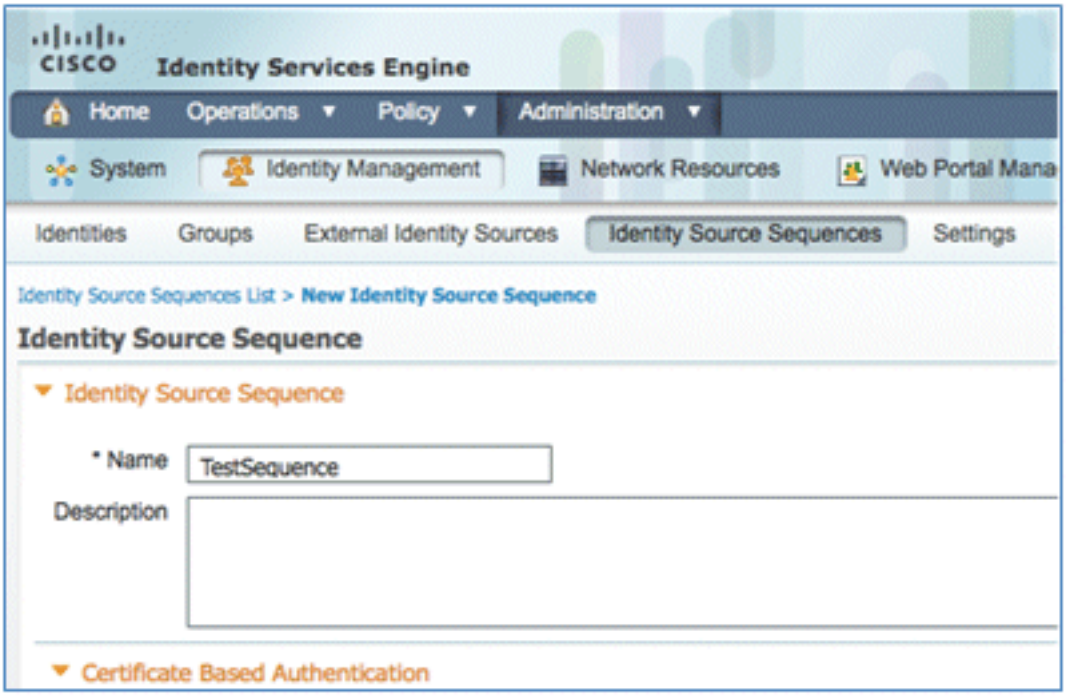
9. تأكد من إضافة CAP الجديد.



10. انتقل إلى **إدارة** > **إدارة الهوية** > **تسلسلات مصدر الهوية**، وانقر فوق **إضافة** .

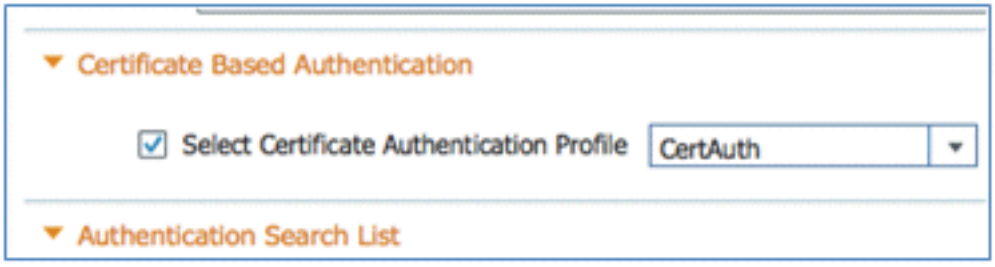


11. إعطاء التسلسل اسم **TestSequence** (في هذا المثال).



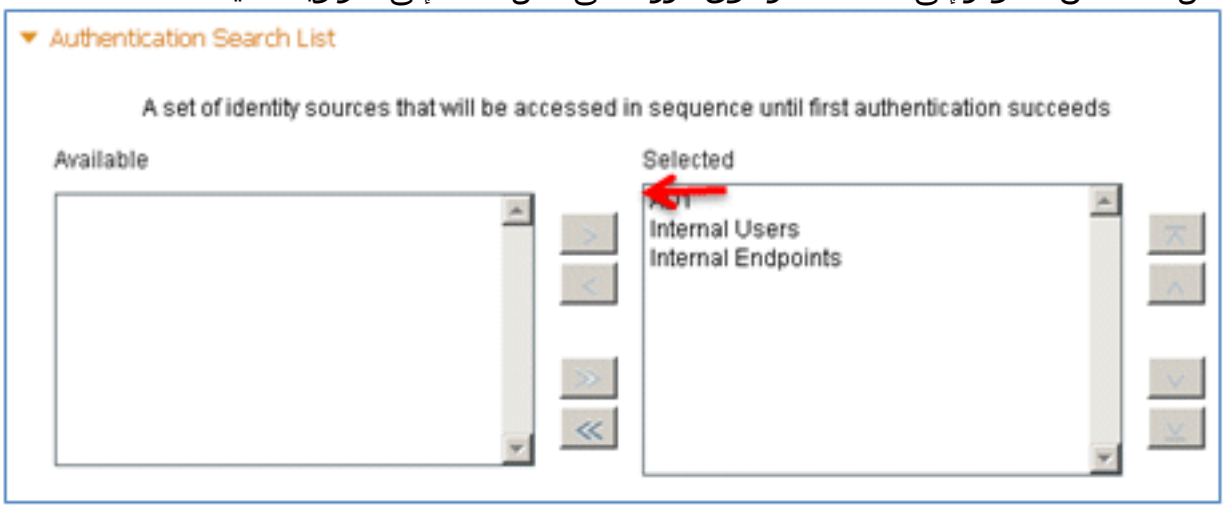
12. قم بالتمرير لأسفل إلى **المصادقة المستندة إلى الشهادة**:

مكن **تحديد توصيف مصادقة الشهادة** (خانة الاختيار).حدد **CertAuth** (أو ملف تعريف CAP آخر تم إنشاؤه مسبقا).

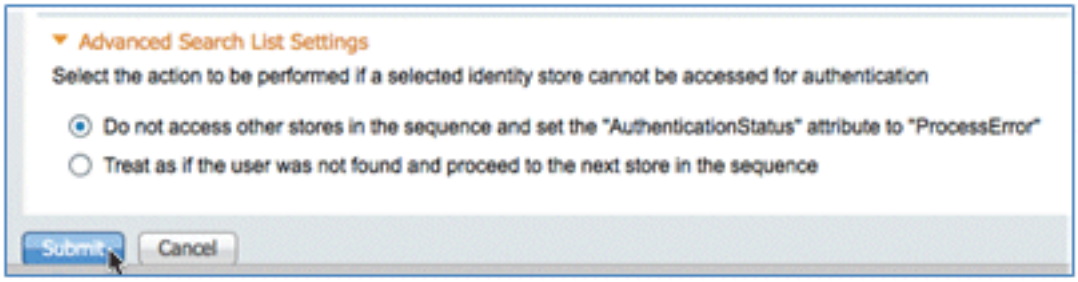


13. قم بالتمرير إلى **قائمة البحث عن المصادقة**:

نقل AD1 من المتوفر إلى المحدد.انقر فوق الزر لأعلى لنقل AD1 إلى الأولوية العليا.

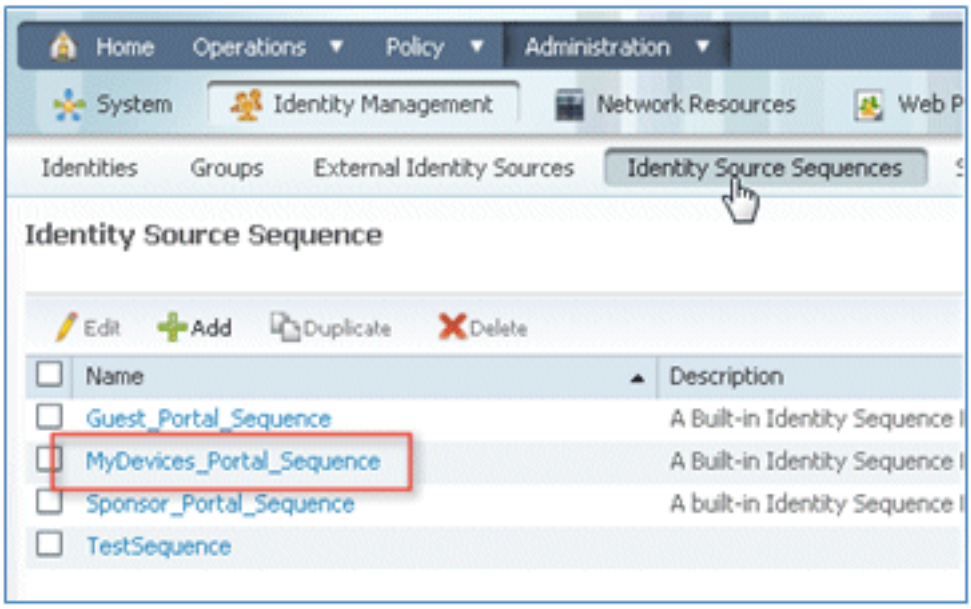


14. طقطقة **يسلم** in order to أنقذت.

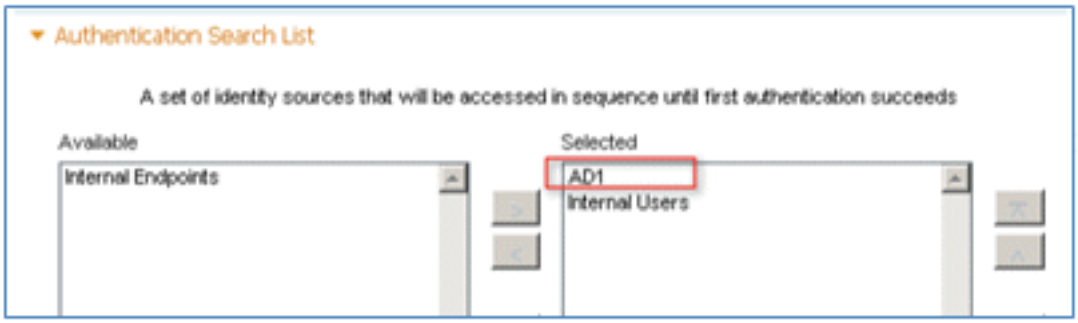


15. تأكد من إضافة تسلسل مصدر الهوية الجديد.

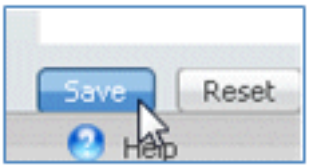
16. أستخدم الإعلان لمصادقة بوابة الأجهزة الخاصة بي. انتقل إلى ISE > **الإدارة** > **إدارة الهوية** > **Identity Source Sequence**، وقم بتحرير MyDevices_Portal_Sequence.



17. إضافة **AD1** إلى القائمة المحددة، وانقر فوق الزر لأعلى لنقل AD1 إلى الأولوية العليا.



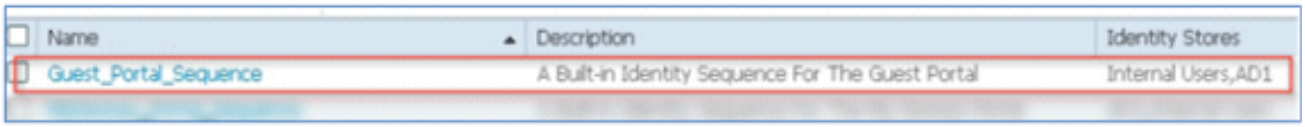
18. طقطقة **حفظ**.



19. تأكد من أن تسلسل مخزن الهويات الخاص ب MyDevices_Portal_Sequence يحتوي على **AD1**.

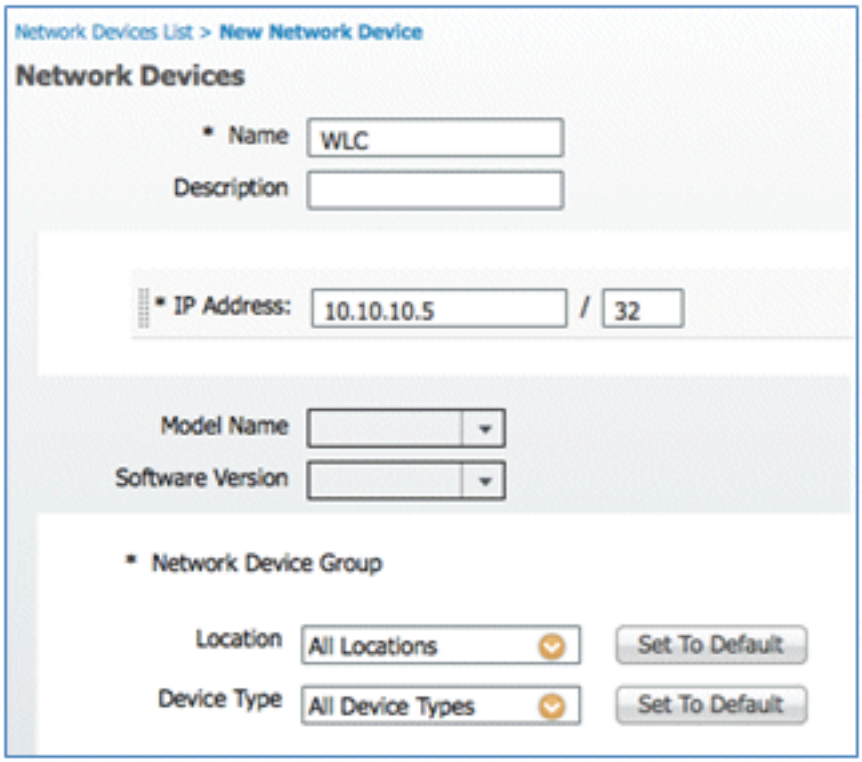
20. كرر الخطوات من 16 إلى 19 لإضافة AD1 ل Guest_Portal_Sequence، وانقر فوق **حفظ**.

21. تأكد من أن Guest_Portal_Sequence يحتوي على **AD1**.

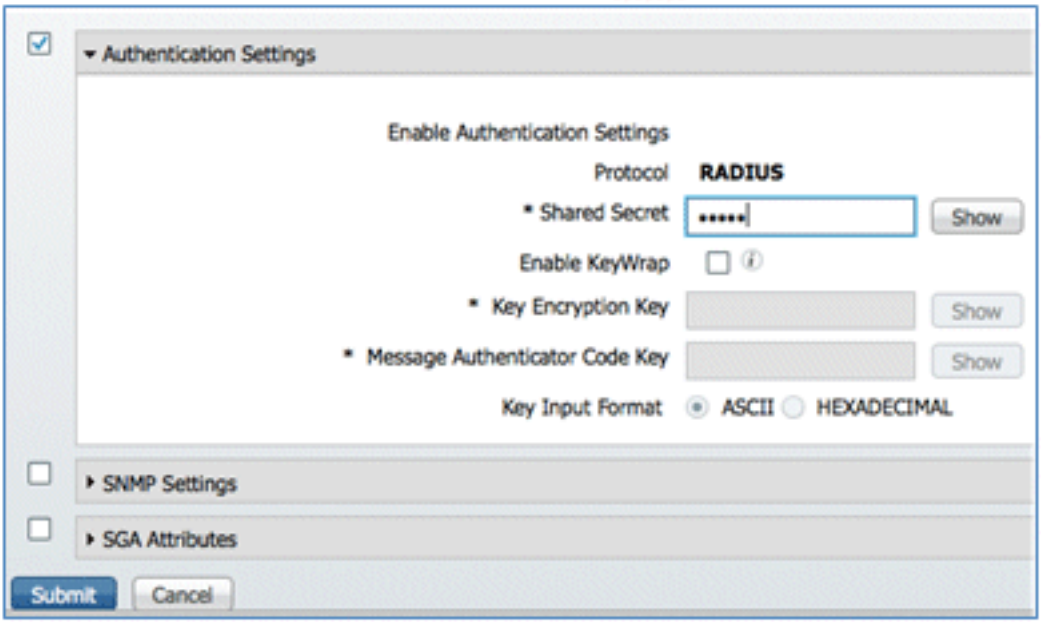


22. in order to أضفت ال WLC إلى شبكة منفذ أداة (WLC)، انتقل إلى **إدارة>شبكة مورد>شبكة أداة**، وطقطقة **يضيف**.

23. إضافة اسم WLC وعنوان IP وقناع الشبكة الفرعية وما إلى ذلك.

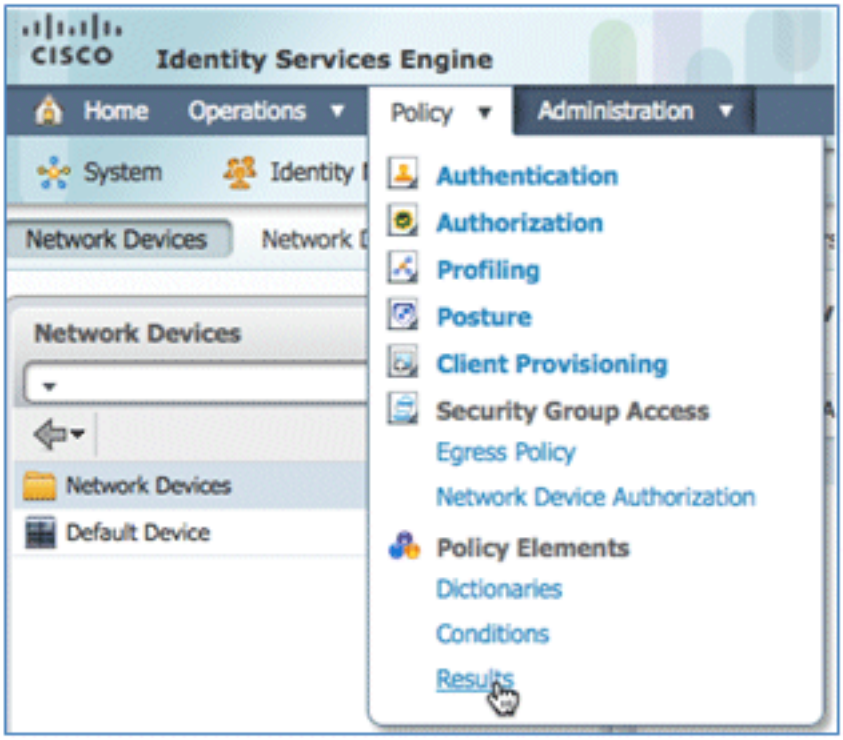


قم بالتمرير لأسفل إلى إعدادات المصادقة، وأدخل "السر المشترك". يجب أن يطابق هذا السر المشترك من24.
ال WLC RADIUS.

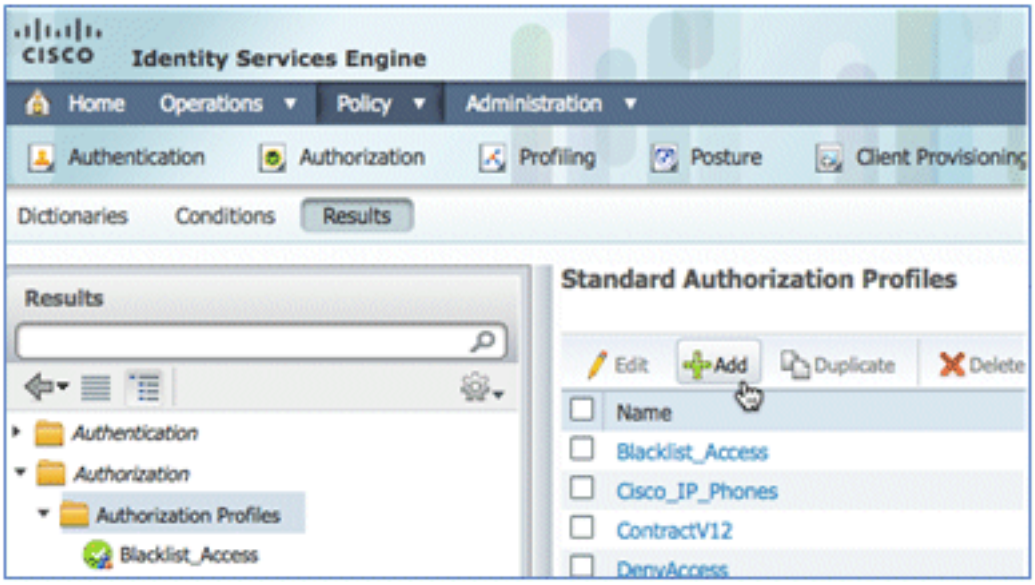


25. انقر على **إرسال**.

26. انتقل إلى **ISE > السياسة > عناصر السياسة > النتائج**.

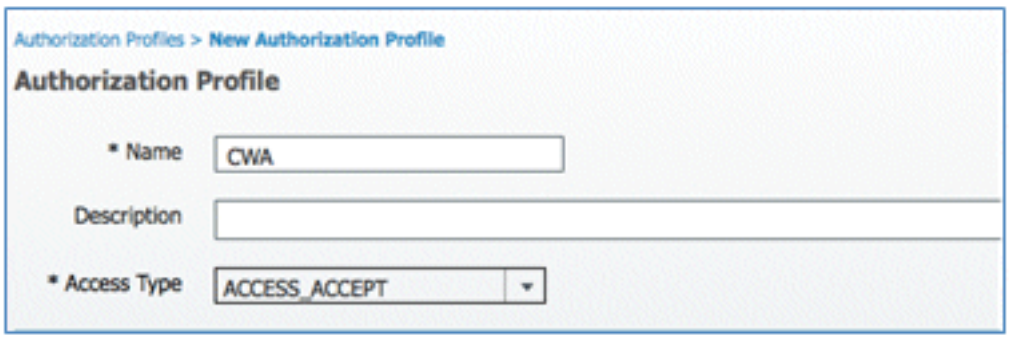


27. قم بتوسيع **النتائج** و**التفويض**، وانقر **توصيفات التفويض**، وانقر **إضافة** لتوصيف جديد.



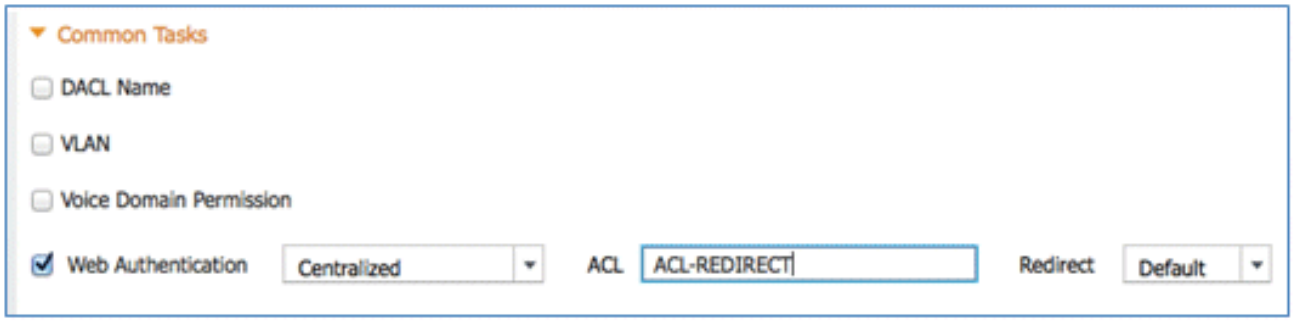
28. امنح ملف التخصيص هذا القيم:

الاسم: **CWA**

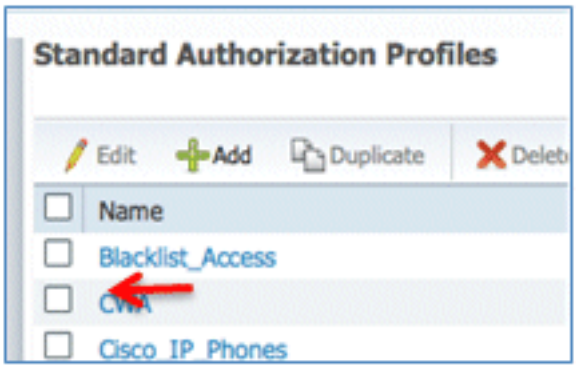


تمكين مصادقة الويب (تم تحديد المربع):

مصادقة الويب: **مركزي**قائمة التحكم في الوصول (ACL): **ACL-Redirect** (يجب أن يتطابق هذا مع اسم قائمة التحكم في الوصول (ACL) للمصادقة المسبقة ل WLC.)إعادة التوجيه: **الافتراضي**



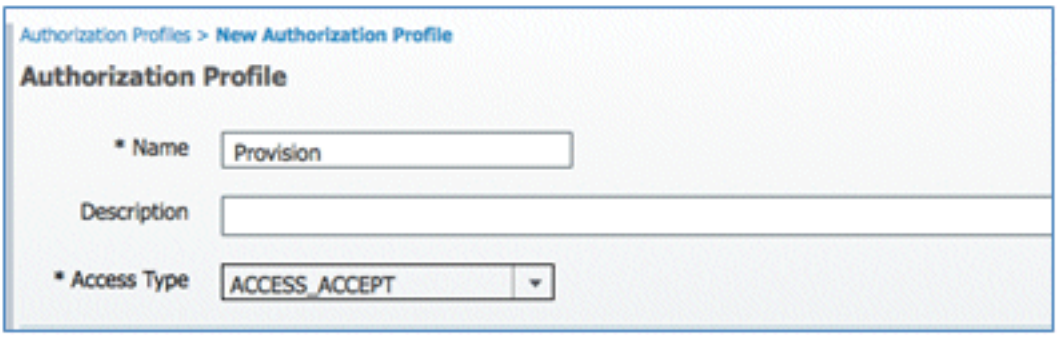
29. انقر على **إرسال**، وتأكد من إضافة ملف تعريف تخويل CWA.



30. انقر على **إضافة** لإنشاء ملف تعريف تخويل جديد.

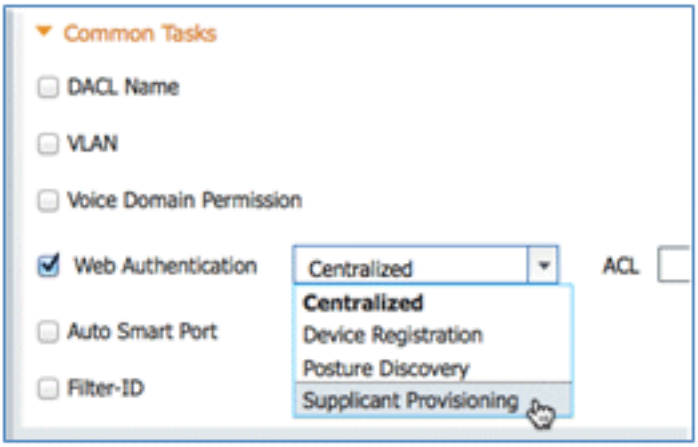
31. امنح ملف التخصيص هذا القيم:

الاسم: **الاعتماد**

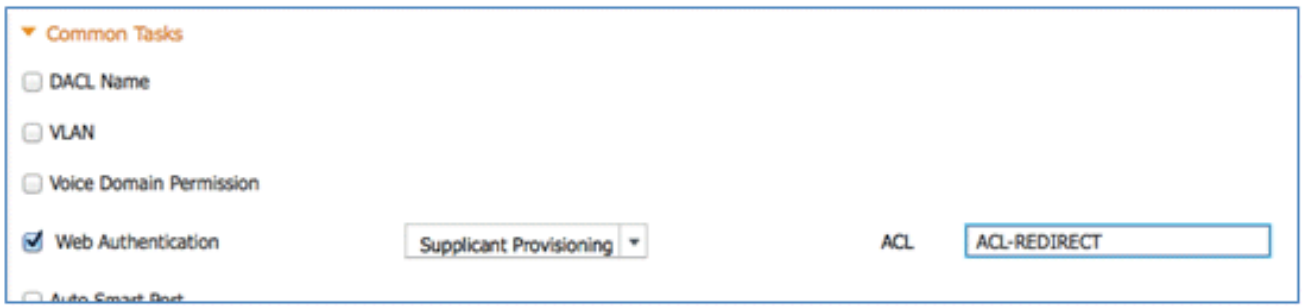


تمكين مصادقة الويب (تم تحديد المربع):

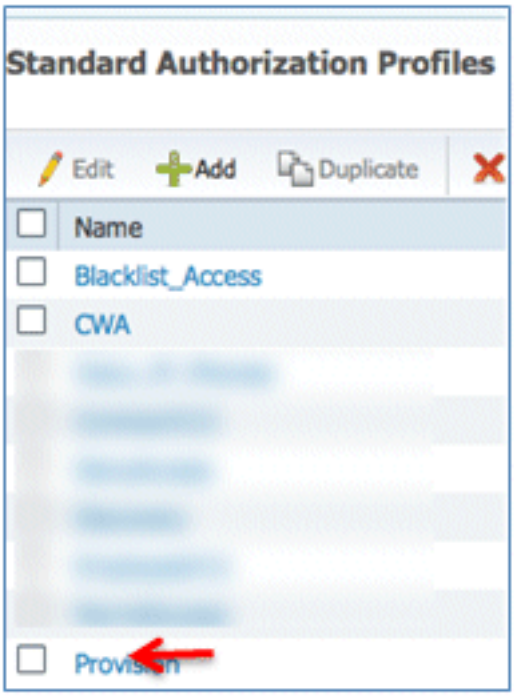
قيمة مصادقة الويب: **توفير الطالب**



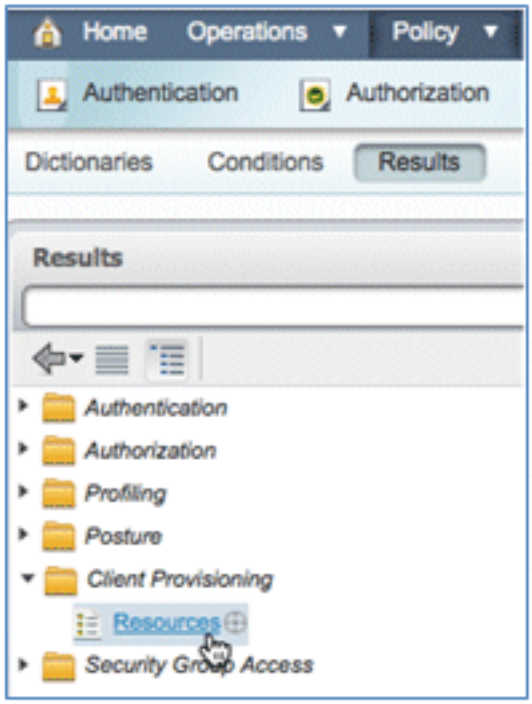
قائمة التحكم في الوصول (**ACL-Redirect**: ACL) (يجب أن يتطابق هذا مع اسم قائمة التحكم في الوصول (ACL) للمصادقة المسبقة ل WLC.)



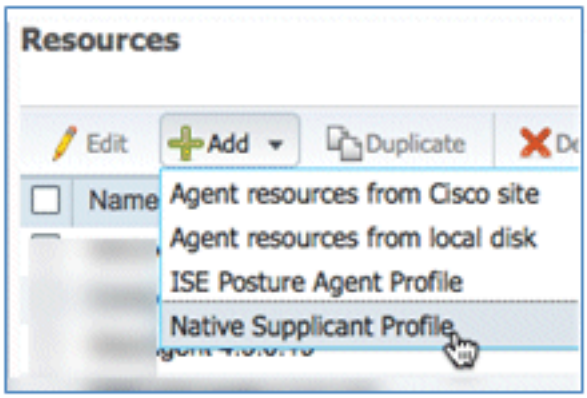
32. انقر فوق **إرسال**، وتأكد من إضافة ملف تعريف تفويض التوفير.



33. قم بالتمرير لأسفل في النتائج، وقم بتوسيع **إمداد العميل**، وانقر فوق **الموارد**.



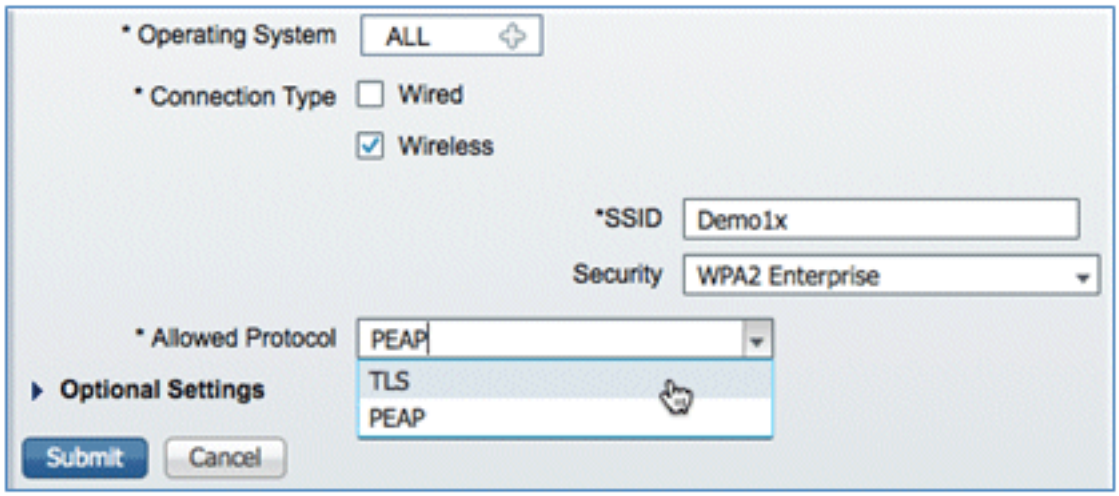
34. حدد **ملف تخصيص الطالب الأصلي**.



35. امنح التوصيف اسم **WirelessSP** (في هذا المثال).

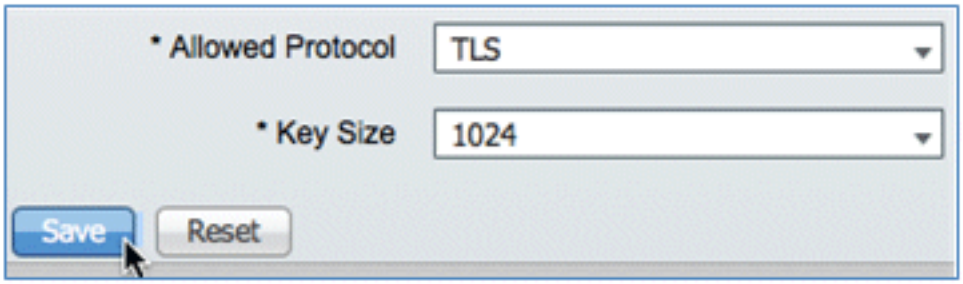
36. قم بإدخال القيم التالية:

نوع الاتصال: **لاسلكي**SSID: **العرض التوضيحي1x** (هذه القيمة من تكوين شبكة WLAN 802.1x WLC)البروتوكول المسموح به: **TLS**حجم المفتاح: **1024**

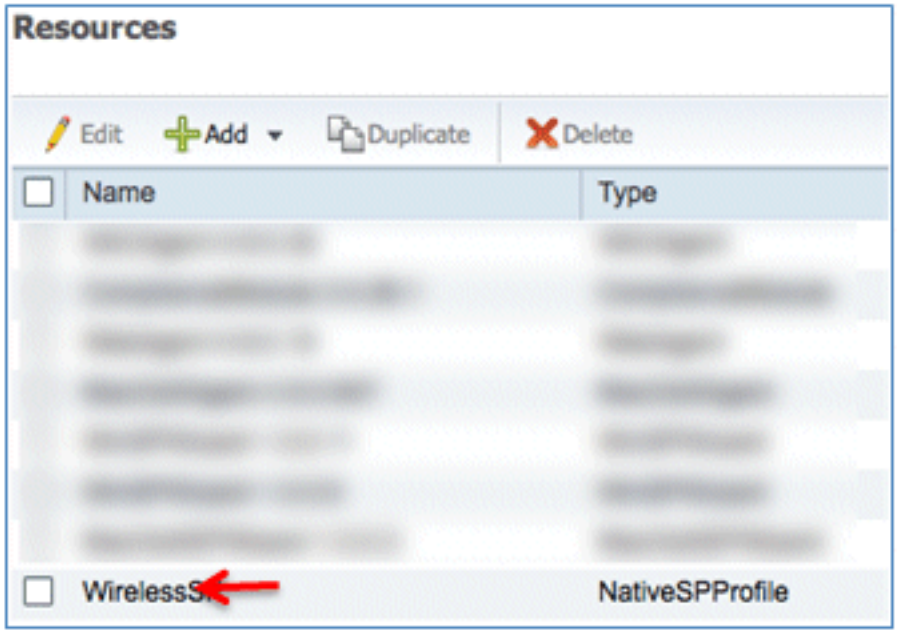


37. انقر على **إرسال**.

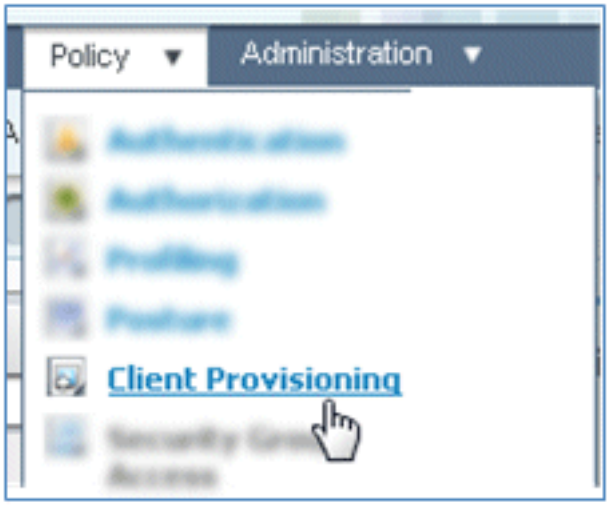
38. طقطقة **حفظ**.



39. تأكد من إضافة ملف التعريف الجديد.

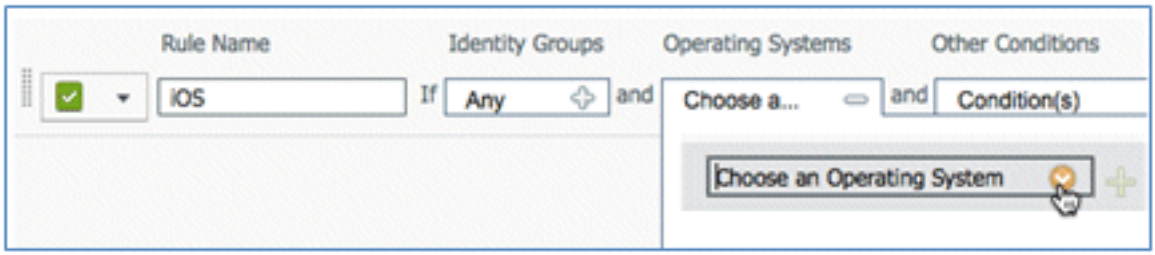


40. انتقل إلى **السياسة > إمداد العميل**.

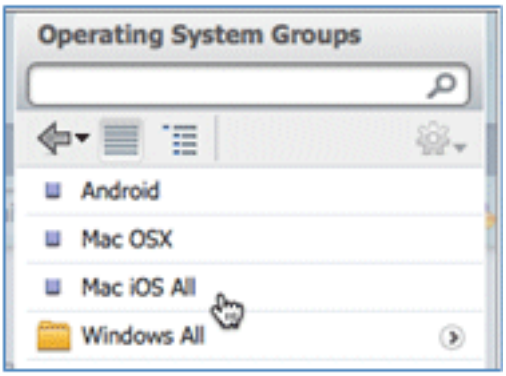


41. أدخل هذه القيم لقاعدة توفير أجهزة iOS:

اسم القاعدة: **iOS**مجموعات الهوية: **أي**

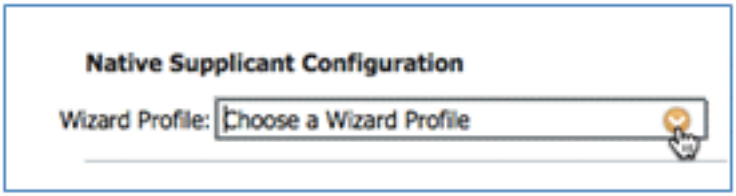


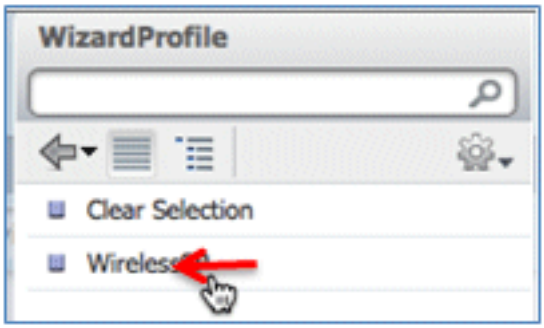
أنظمة التشغيل: **نظام التشغيل Mac iOS All**



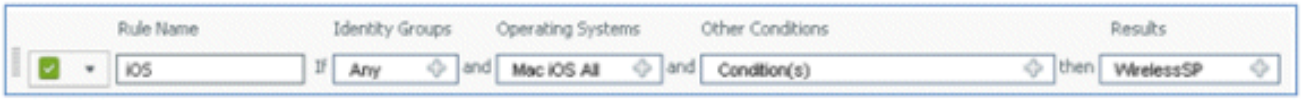
النتائج: **WirelessSP** (هذا هو ملف تعريف الطالب الأصلي الذي تم إنشاؤه سابقا)

انتقل إلى **النتائج** > **ملف تعريف المعالج** (القائمة المنسدلة) > **WirelessSP**.

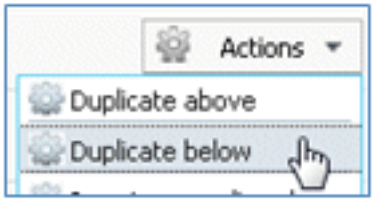




تأكد من إضافة ملف تعريف إعداد iOS.

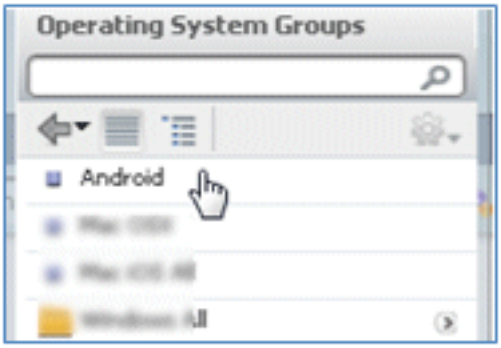


43. على الجانب الأيمن من القاعدة الأولى، حدد قائمة الإجراءات المنسدلة، وحدد **تكرار أدناه** (أو أعلى).



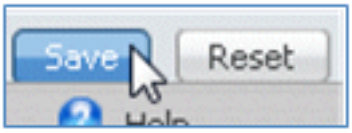
44. قم بتغيير اسم القاعدة الجديدة إلى **Android**.

45. قم بتغيير أنظمة التشغيل إلى **Android**.

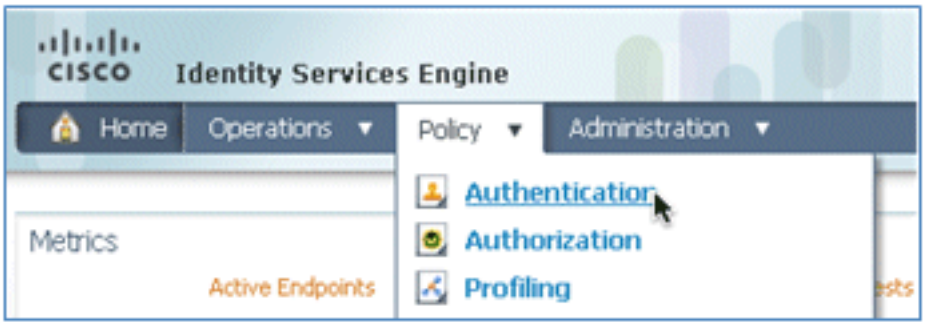


46. أترك القيم الأخرى بدون تغيير.

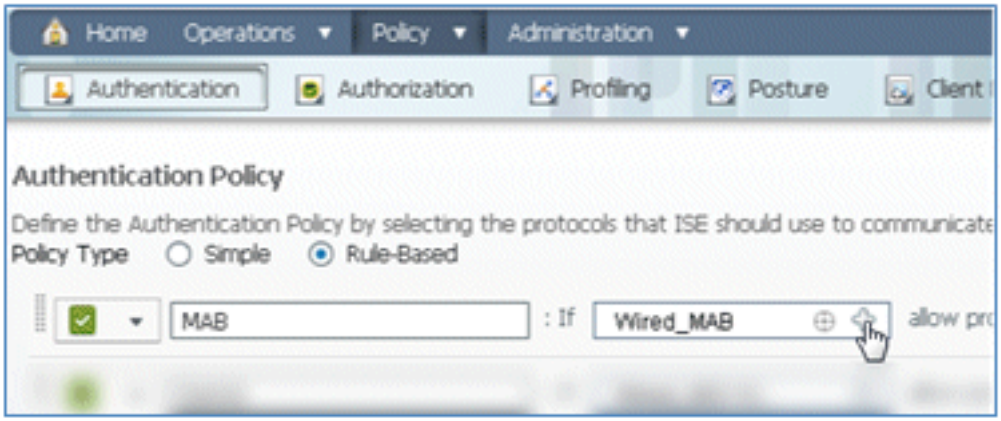
47. انقر فوق **حفظ** (الشاشة اليسرى السفلى).



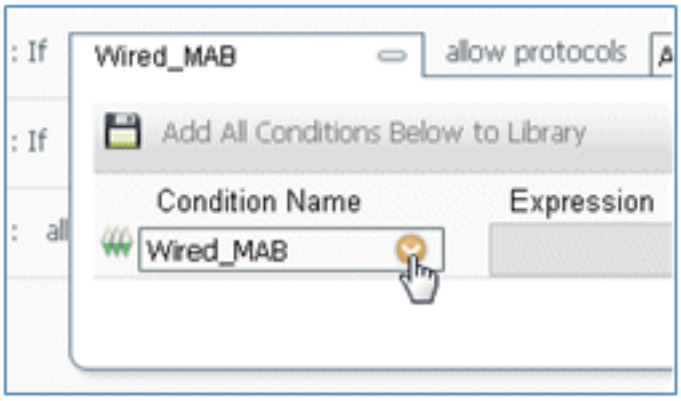
48. انتقل إلى **ISE > السياسة > المصادقة**.



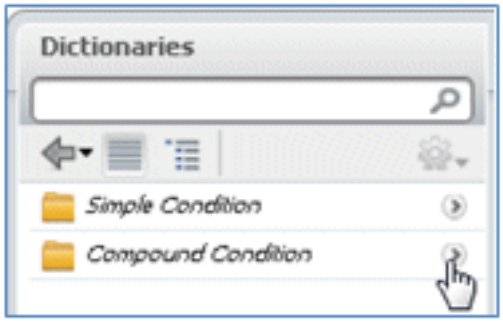
49. قم بتعديل الشرط ليشمل wireless_mab، ثم قم بتوسيع **wired_mab**.



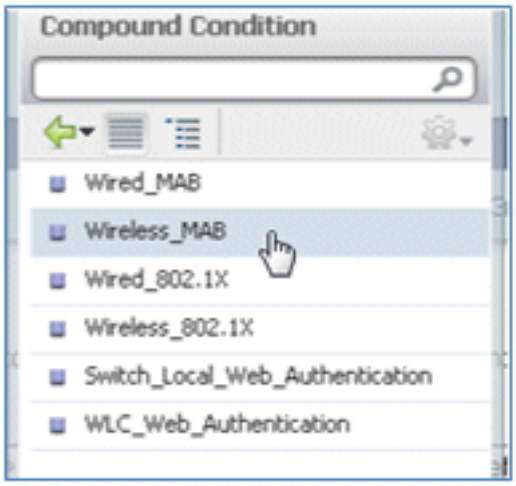
50. انقر فوق القائمة المنسدلة **اسم الشرط**.



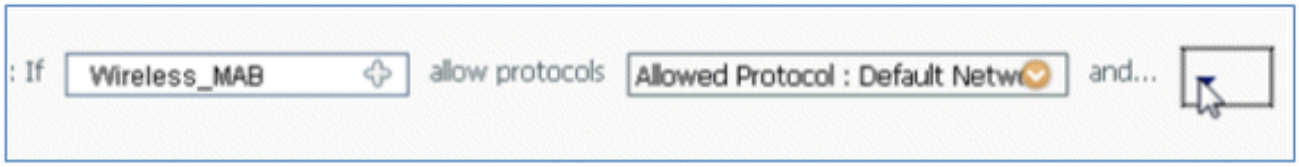
51. حدد **القواميس** > **شرط مركب**.



52. حدد **Wireless_MAB**.

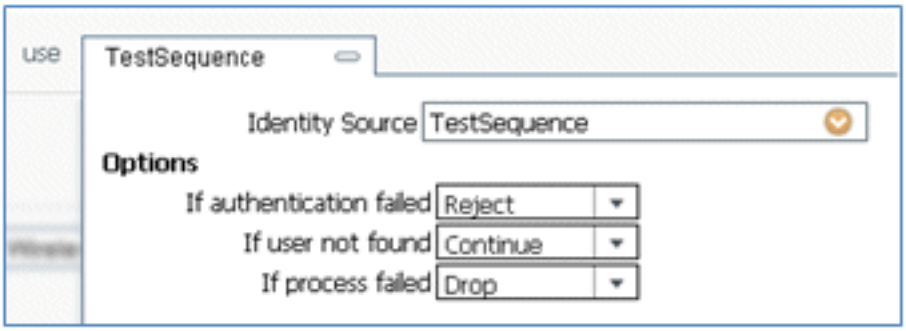


53. إلى يمين القاعدة، حدد السهم للتوسيع.

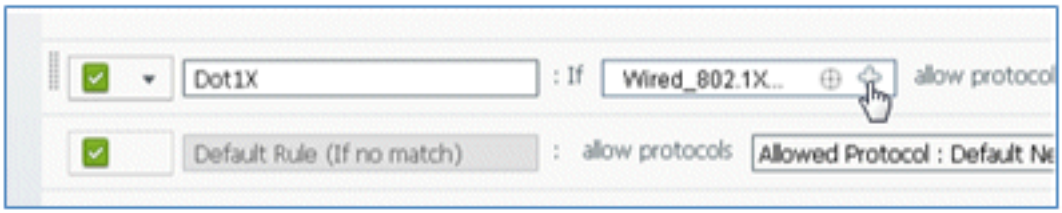


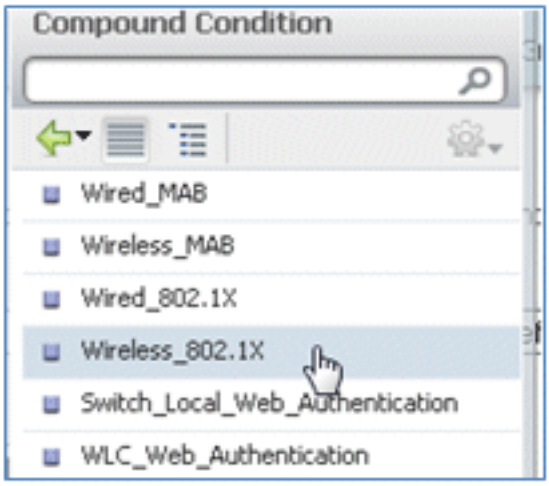
54. حدد هذه القيم من القائمة المنسدلة:

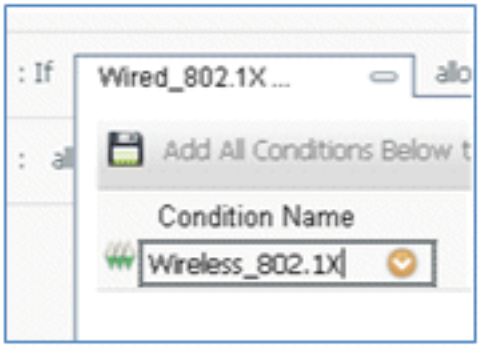
مصدر الهوية: **TestSequence** (هذه هي القيمة التي تم إنشاؤها سابقا)في حالة فشل المصادقة: **رفض**في حالة عدم العثور على المستخدم: **متابعة**في حالة فشل العملية: **إسقاط**



55. انتقل إلى قاعدة **dot1x**، وقم بتغيير هذه القيم:

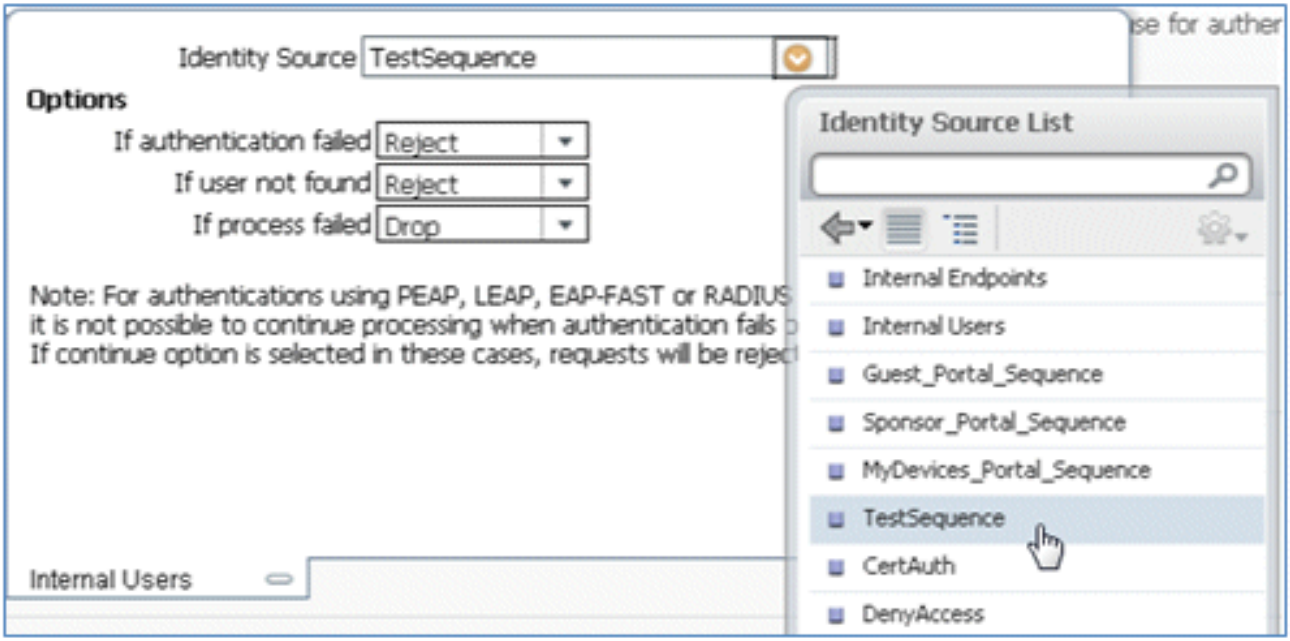






الشرط: **Wireless_802.1X**

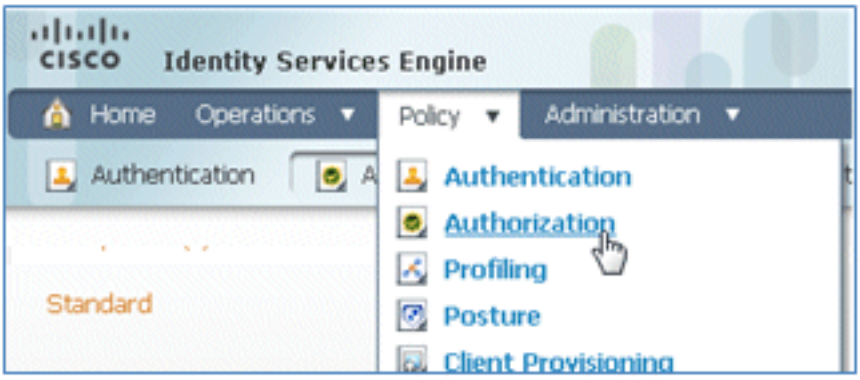
مصدر الهوية: **TestSequence**



طقطقة **حفظ**.

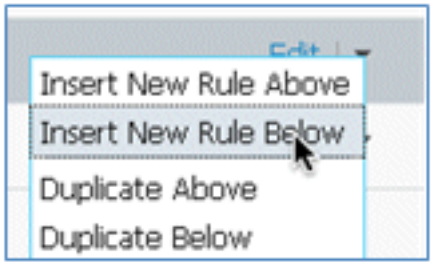
56.

57. انتقل إلى **ISE > السياسة > التفويض**.



تم تكوين القواعد الافتراضية (مثل Black List Default و Profiled و Default) بالفعل من التثبيت، ويمكن58.
تجاهل القواعد الأولى والثانية، وسيتم تحرير القاعدة الافتراضية لاحقا.

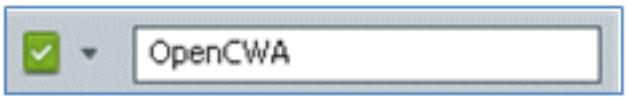
على يمين القاعدة الثانية (إصدارات هواتف Cisco IP)، انقر فوق السهم لأسفل الموجود بجوار التحرير، و59د
إدراج قاعدة جديدة أدناه.



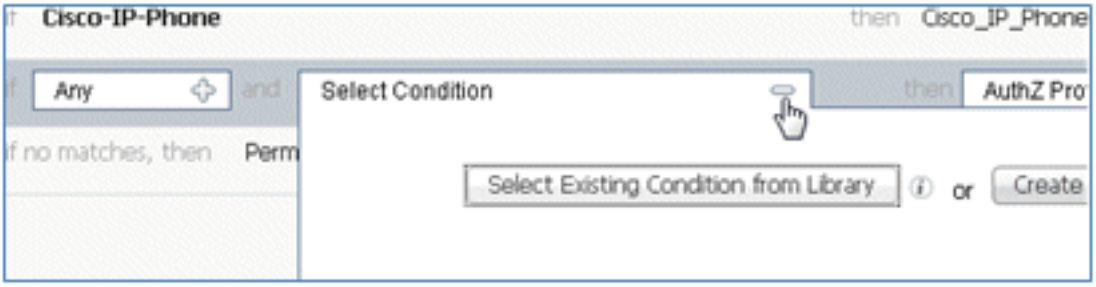
تمت إضافة قاعدة قياسية جديدة
#.

60. قم بتغيير اسم القاعدة من القاعدة القياسية # إلى **OpenCWA**. تهيئ هذه القاعدة عملية التسجيل على

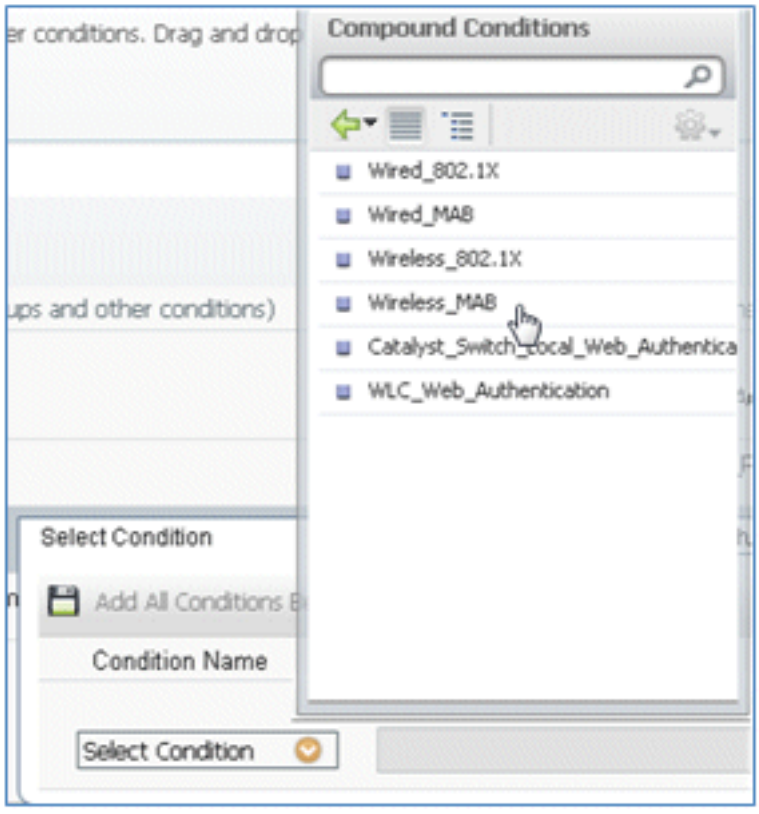
شبكة WLAN المفتوحة (SSID المزدوج) للمستخدمين الذين يأتون إلى شبكة الضيوف من أجل توفير الأجهزة.



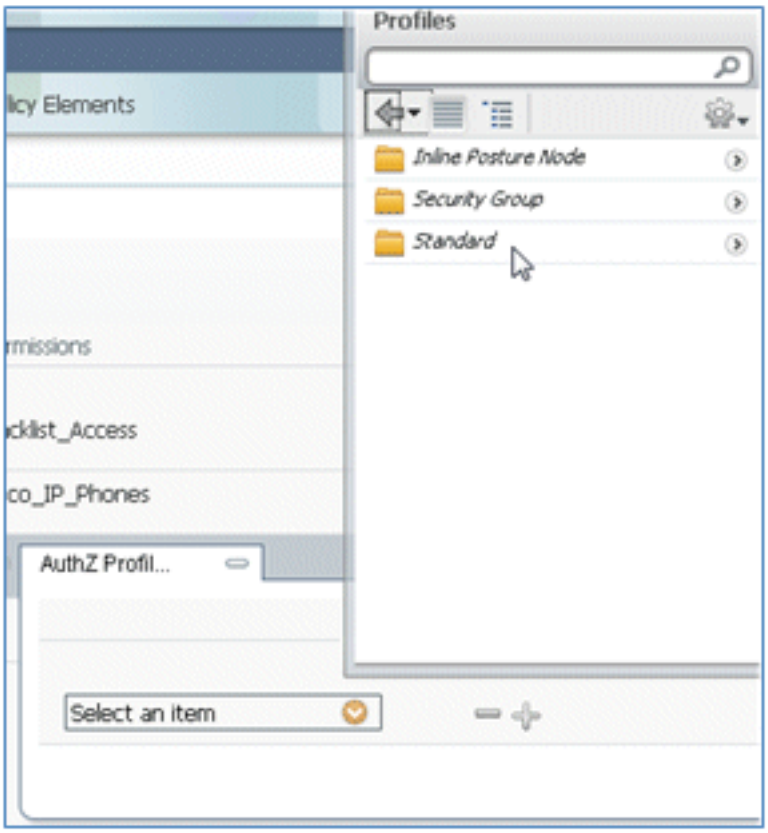
61. انقر علامة الزائد (+) للشرط (الشروط)، وانقر **تحديد الشرط الموجود من المكتبة**.



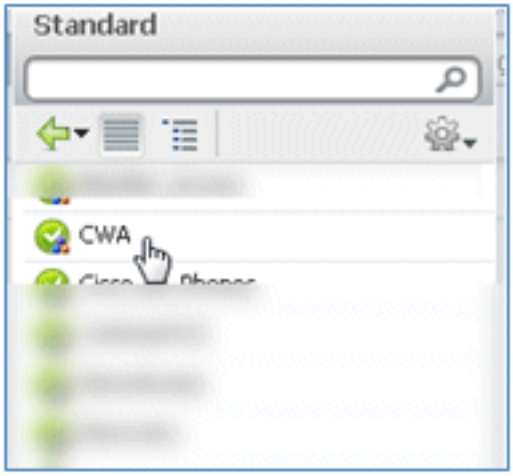
62. حدد **شروط مركبة > Wireless_MAB**.



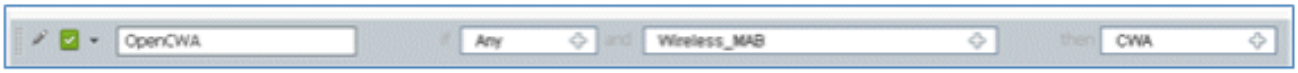
63. في ملف تخصيص AuthZ، انقر علامة الزائد (+)، وحدد **قياسي**.



64. حدد **CWA** القياسي (هذا هو ملف تعريف التخويل الذي تم إنشاؤه سابقا).



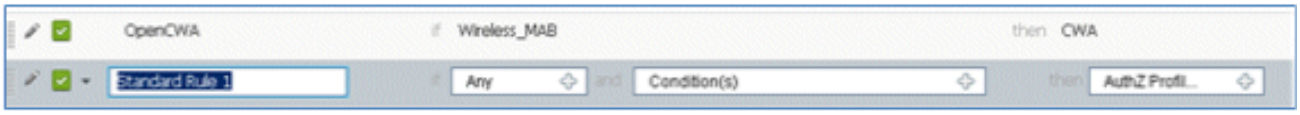
65. تأكد من إضافة القاعدة بالشروط والتفويض الصحيحين.



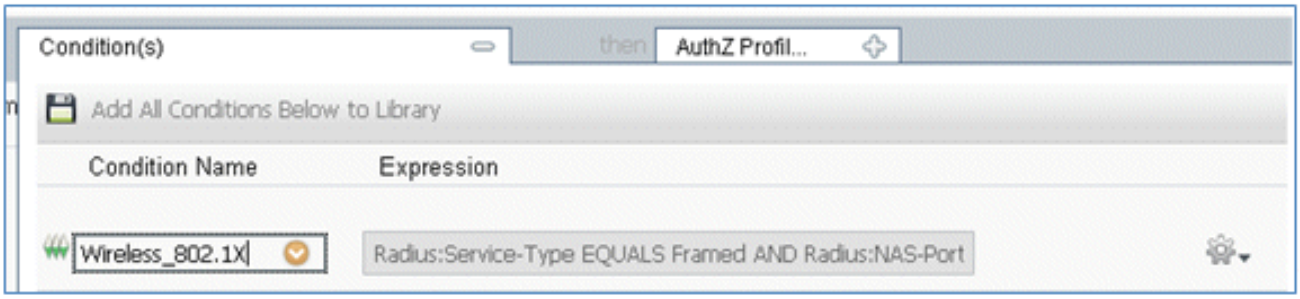
66. انقر فوق **تم** (في الجانب الأيمن من القاعدة).

67. على يمين نفس القاعدة، انقر فوق السهم لأسفل المجاور للتحرير، وحدد **إدراج قاعدة جديدة أدناه**.

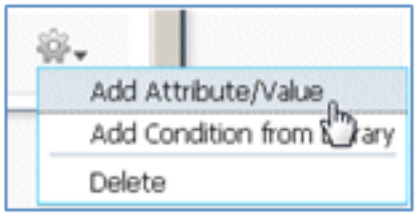
68. قم بتغيير اسم القاعدة من القاعدة القياسية # إلى **قاعدة PEAPrule** (في هذا المثال). هذه القاعدة خاصة ب PEAP (يستخدم أيضا لسيناريو SSID المفرد) للتحقق من أن مصادقة 802.1X دون تأمين طبقة النقل (TLS) وأن تزويد ملتمس الشبكة يتم بدؤه مع ملف تعريف تخويل التوفير الذي تم إنشاؤه سابقا.



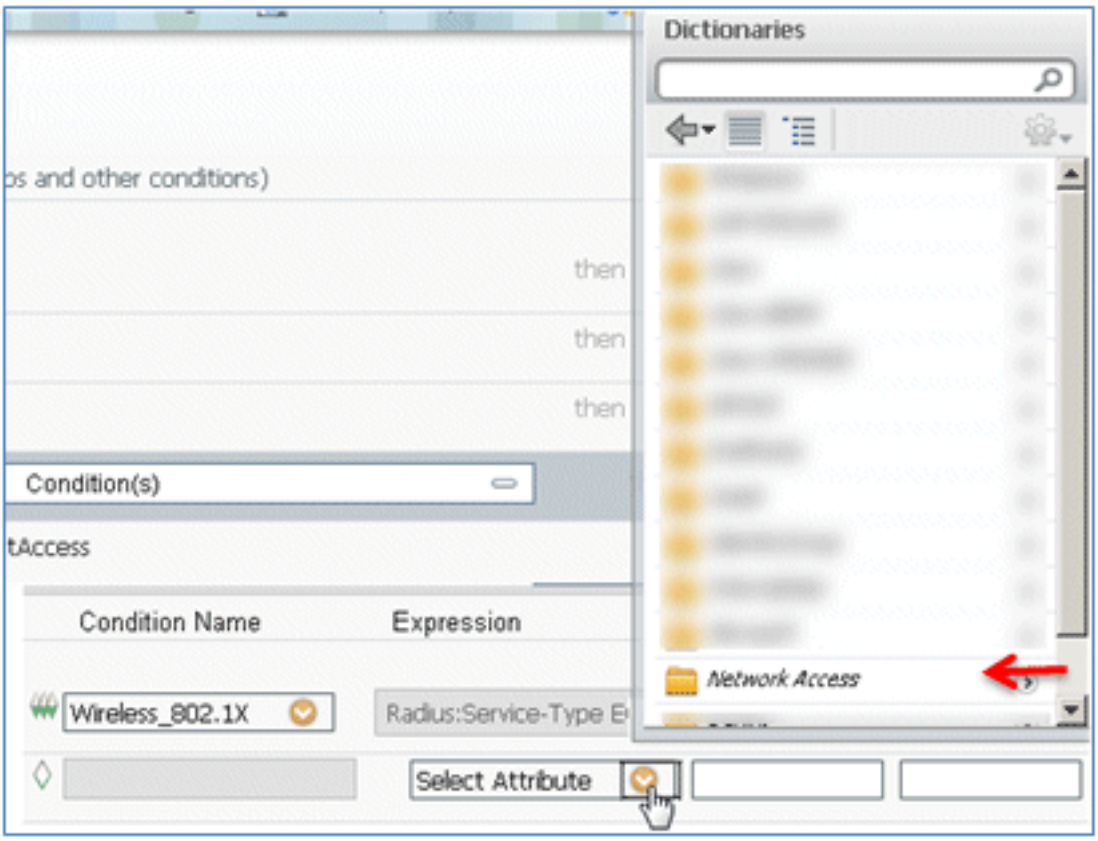
69. قم بتغيير الشرط إلى **Wireless_802.1X**.



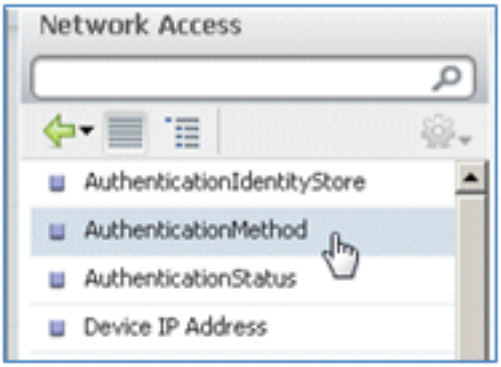
70. انقر أيقونة التروس على الجانب الأيمن من الشرط، وحدد **إضافة سمة/قيمة**. هذا شرط 'and'، وليس شرط 'or'.



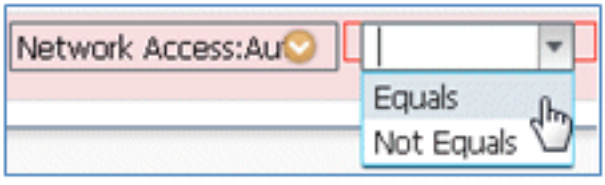
71. حدد موقع **الوصول إلى الشبكة** وحدده.



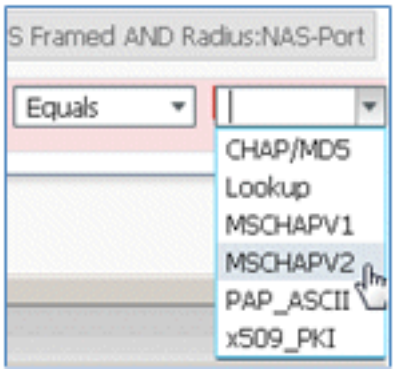
72. حدد **AuthenticationMethod**، وأدخل القيم التالية:



AuthenticationMethod: **يساوي**

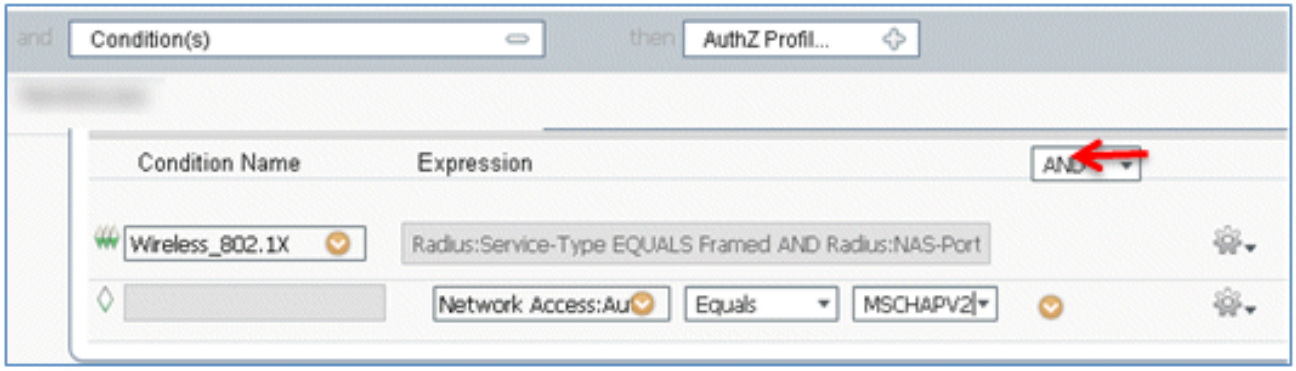


حدد **MSCHAPV2**.

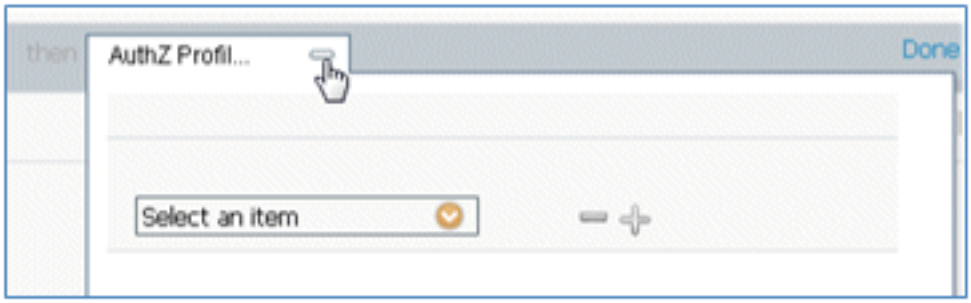


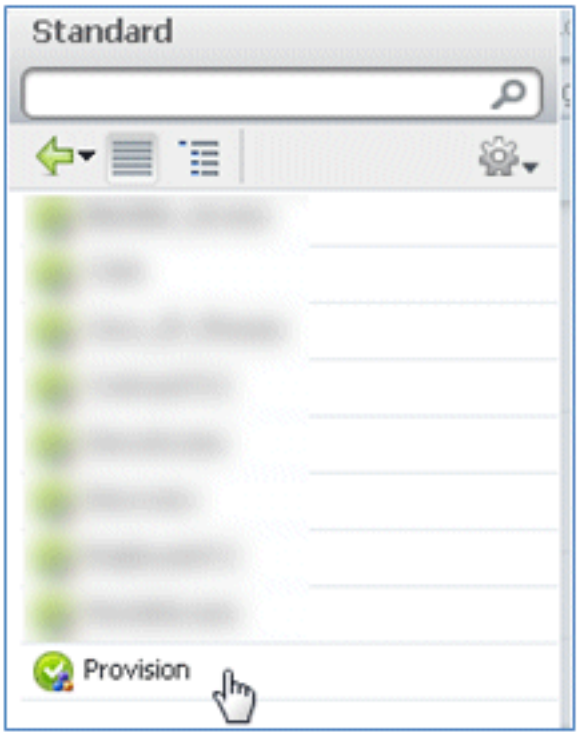
هذا مثال على القاعدة، تأكد من أن الشرط هو

و.



في ملف تعريف AuthZ، حدد **Standard > Provision** (هذا هو ملف تعريف التخويل الذي تم إنشاؤه سابقًا).

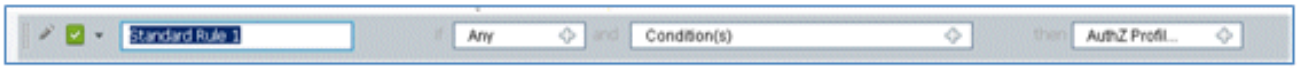




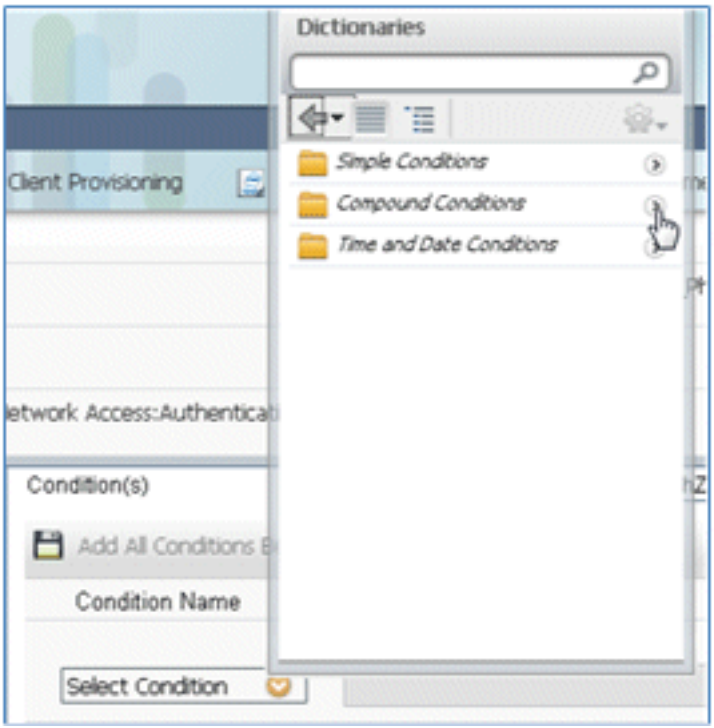
74. طقطقة **تم**.

75. على يمين قاعدة PEARule، انقر السهم لأسفل الموجود بجوار التحرير وحدد **إدراج قاعدة جديدة أدناه**.

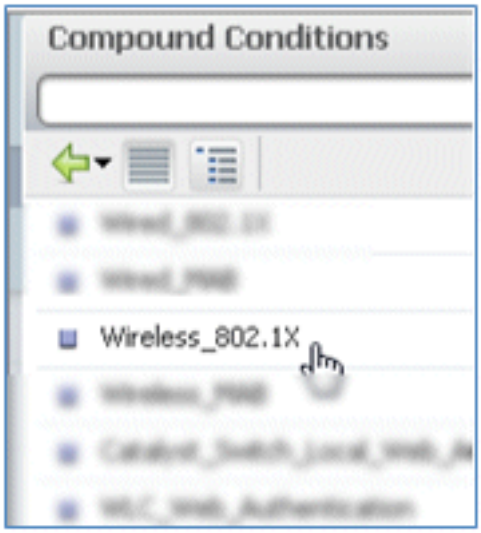
76. قم بتغيير اسم القاعدة من رقم القاعدة القياسية إلى **AllowRule** (في هذا المثال). سيتم إستخدام هذه القاعدة للسماح بالوصول إلى الأجهزة المسجلة ذات الشهادات المثبتة.



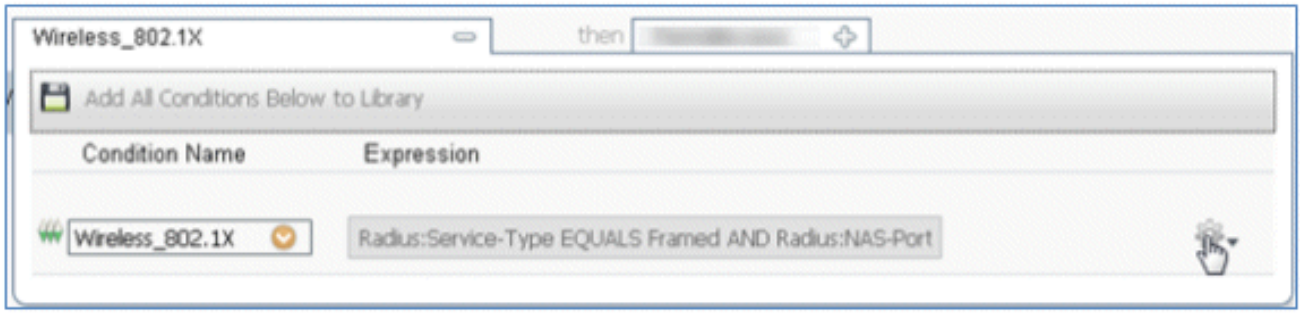
77. تحت شرط (شروط)، حدد **شروط مركبة**.



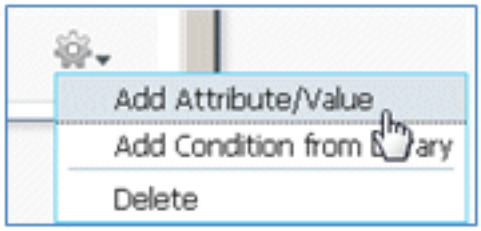
78. حدد **Wireless_802. 1X**.



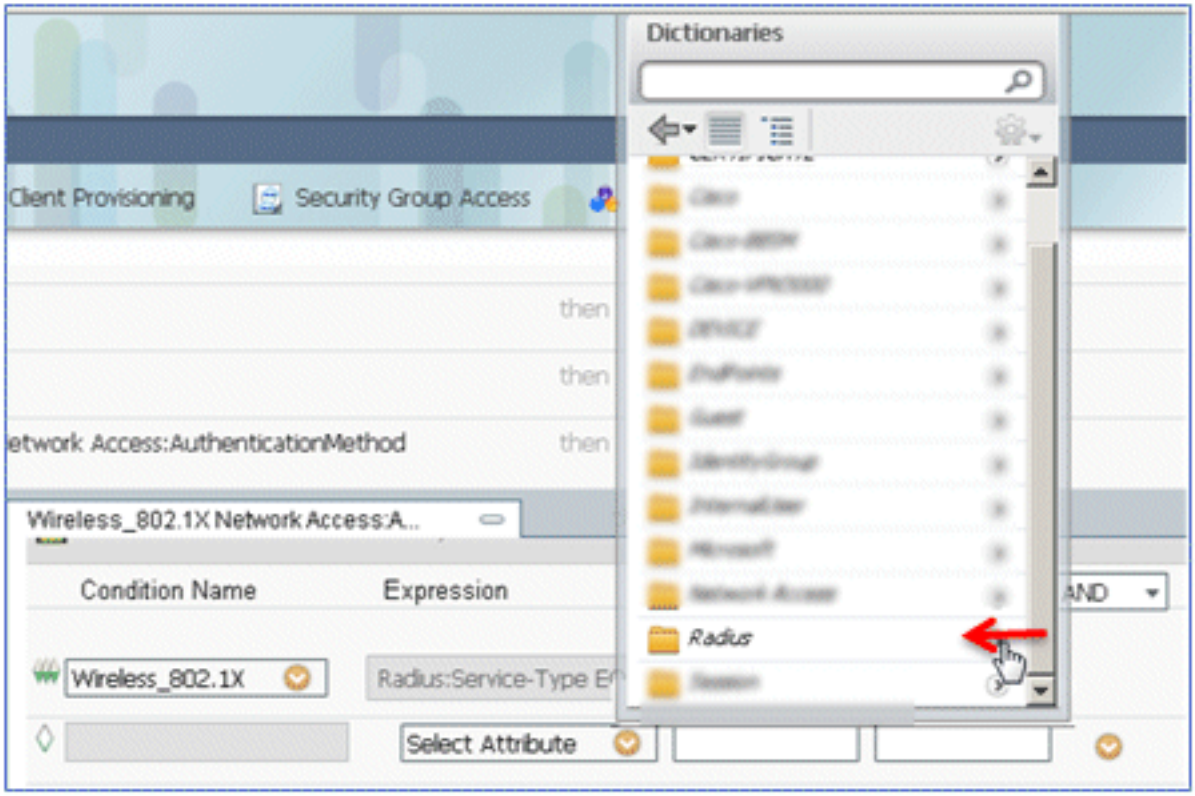
79. إضافة سمة AND.



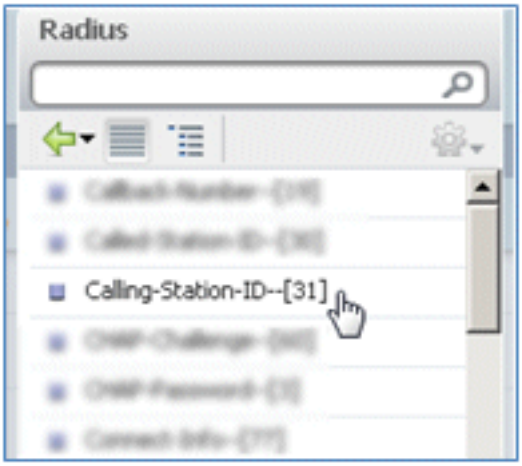
80. انقر أيقونة التروس على الجانب الأيمن من الشرط، وحدد **إضافة سمة/قيمة**.



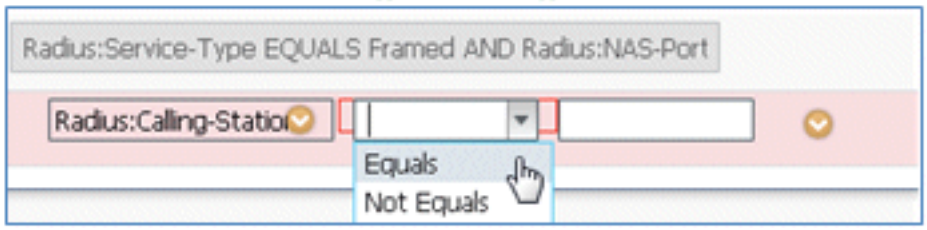
.81 حدد موقع **RADIUS** وحدده.



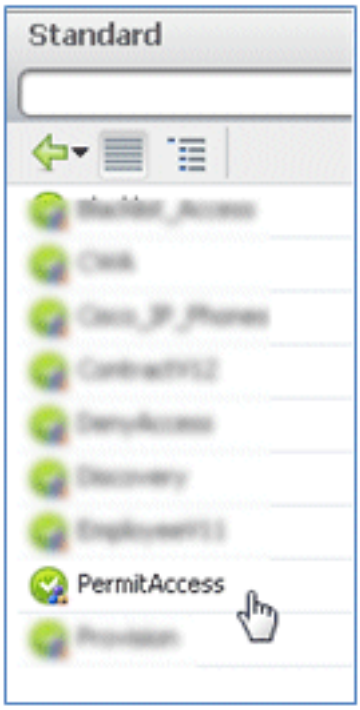
.82 حدد **31]—[Call-Station-ID**.



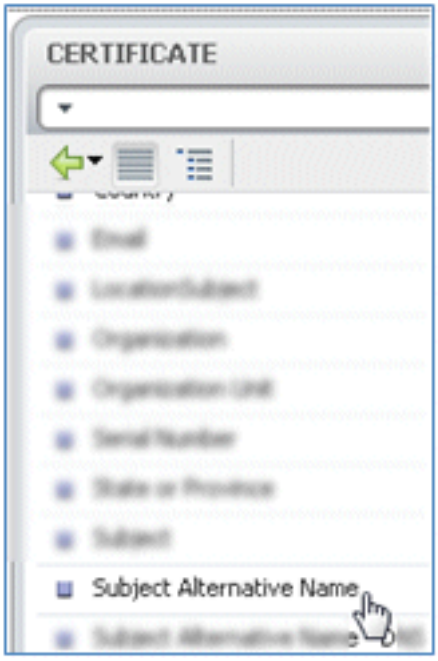
.83 حدد **يساوي**.



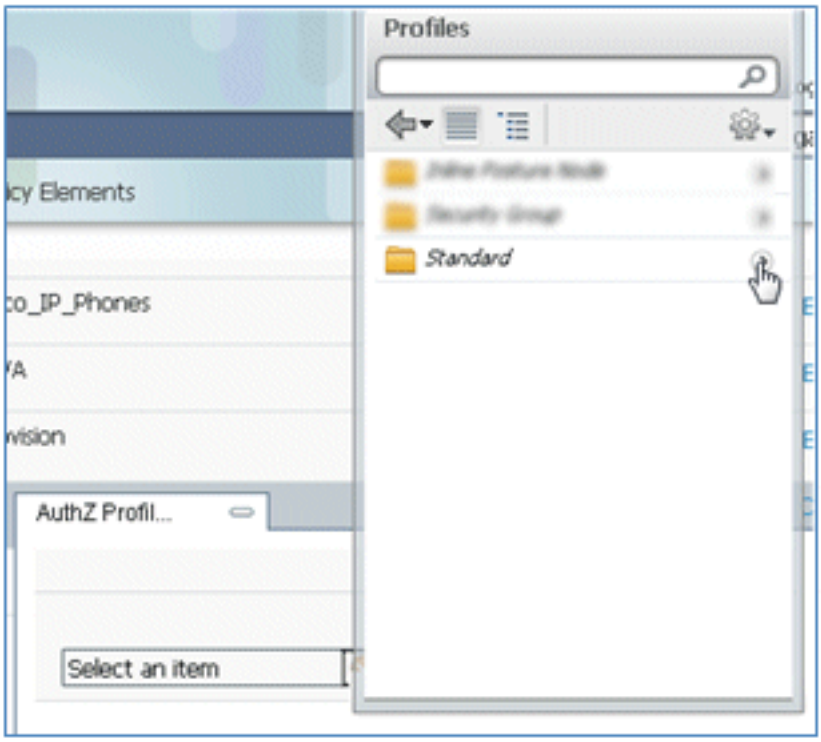
84. انتقل إلى **CERTIFICATE**، وانقر فوق السهم الأيمن.



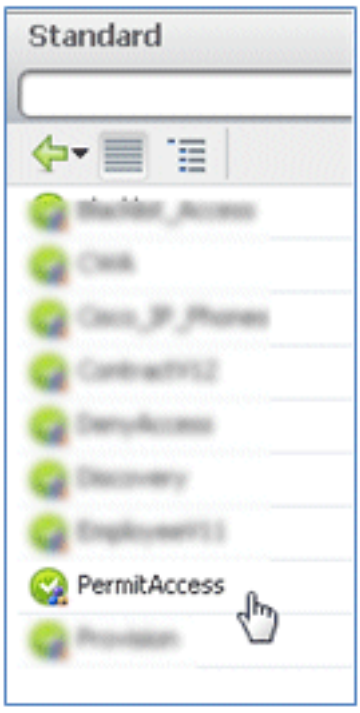
85. حدد **الاسم البديل للموضوع**.



86. بالنسبة لملف تعريف AuthZ، حدد **قياسي**.



87. حدد **السماح بالوصول**.

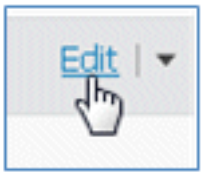


88. طقطقة **تم**.

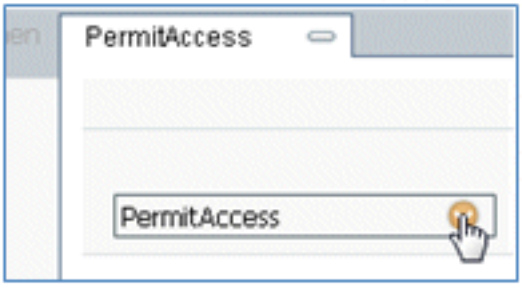
هذا مثال على القاعدة:

89. حدد موقع القاعدة الافتراضية لتغيير PermitAccess إلى DenyAccess.

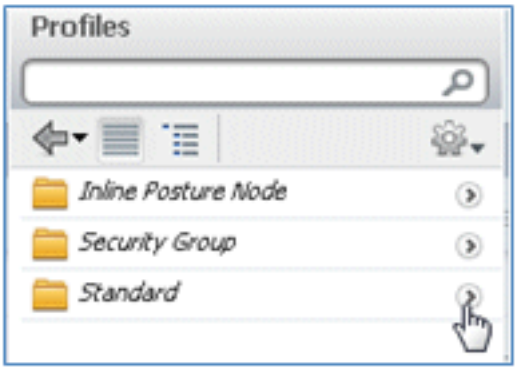
90. انقر فوق **تحرير** لتحرير القاعدة الافتراضية.



91. انتقل إلى ملف تعريف AuthZ الحالي ل PermitAccess.



92. حدد **قياسي**.



93. حدد **DenyAccess**.

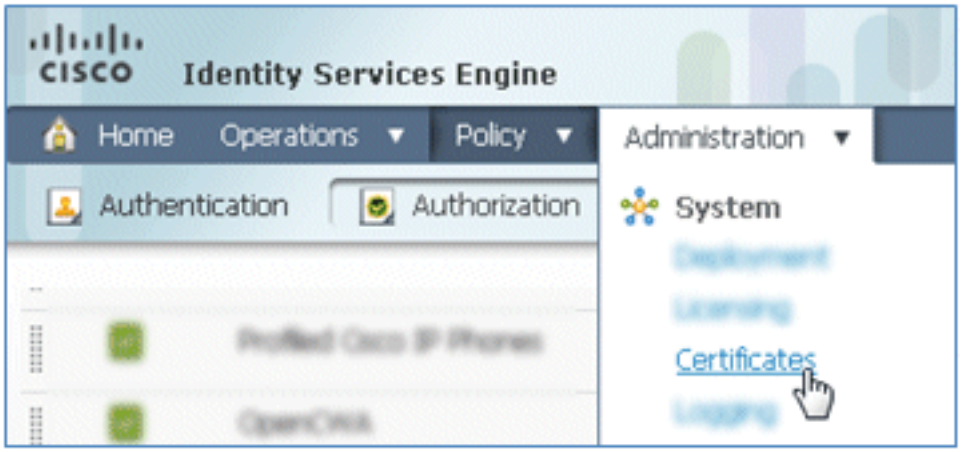
94. تأكد من أن القاعدة الافتراضية تحتوي على DenyAccess إذا لم يتم العثور على تطابقات.

95. طقطقة **تم**.

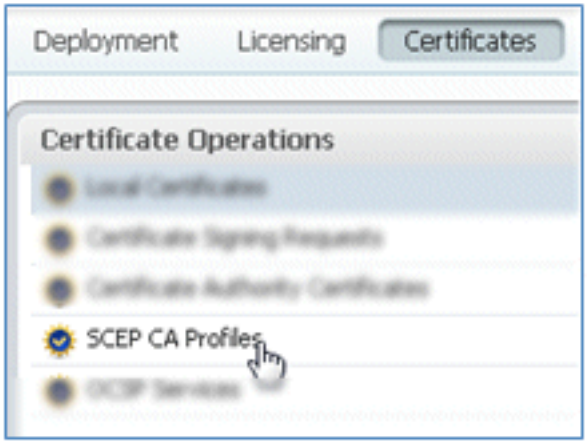
هذا مثال على القواعد الأساسية المطلوبة لهذا الاختبار، وهي تنطبق إما على سيناريو SSID واحد أو سيناريو SSID مزدوج.

96. طقطقة **حفظ**.

97. انتقل إلى **ISE>الإدارة>النظام>الشهادات** لتكوين خادم ISE باستخدام ملف تعريف SCEP.



98. في عمليات الترخيص، انقر على **توصيفات SCEP CA**.



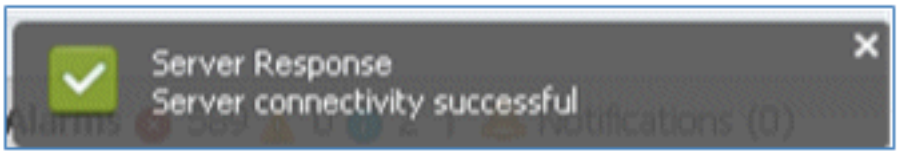
99. انقر فوق **إضافة (Add)**.

100. أدخل القيم التالية لملف التعريف هذا:

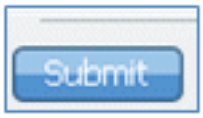
الاسم: **MySCEP** (في هذا المثال)/url: **https://*<ca-server>*/CertSrv/mscep** (تحقق من تكوين خادم CA لديك للحصول على العنوان الصحيح.)

101. انقر على **إختبار الاتصال** لاختبار اتصال اتصال SCEP.

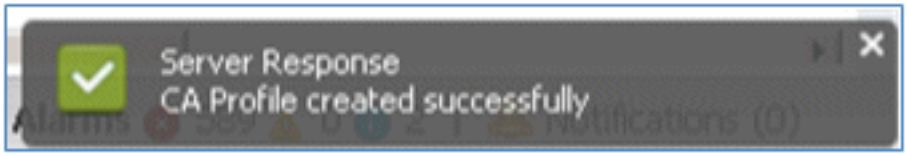
102. توضح هذه الاستجابة أن اتصال الخادم ناجح.



103. انقر على **إرسال**.



104. يستجيب الخادم بأن ملف تعريف المرجع المصدق قد تم إنشاؤه بنجاح.



105. تأكد من إضافة ملف تعريف SCEP CA.

تجربة المستخدم - توفير نظام التشغيل iOS

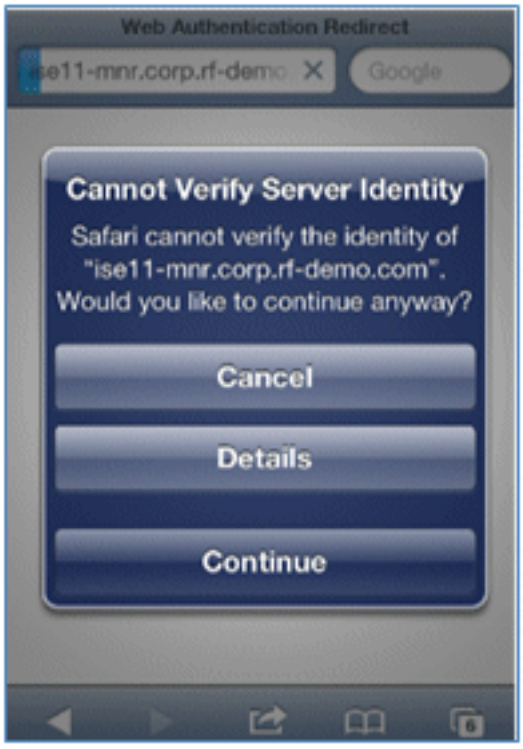
SSID مزدوج

يغطي هذا القسم SSID المزدوج ويصف كيفية الاتصال بالضيف المراد توفيره وكيفية الاتصال بشبكة محلية لاسلكية (WLAN) بسرعة 802.1x.

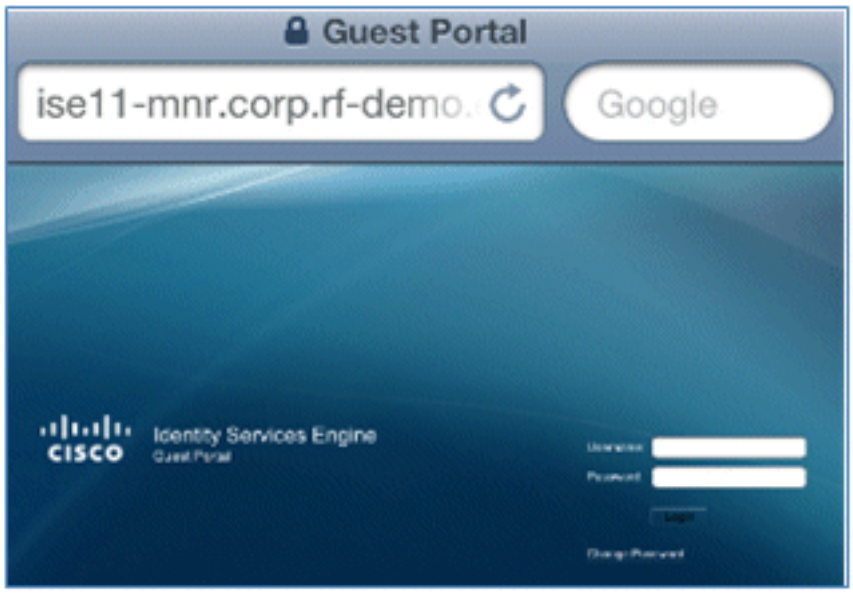
أكمل الخطوات التالية لتوفير نظام التشغيل iOS في سيناريو SSID المزدوج:

1. على جهاز iOS، انتقل إلى **شبكات Wi-Fi**، وحدد **DemoCWA** (يشكل شبكة WLAN مفتوحة على WLC).

2. افتح مستعرض Safari على جهاز iOS، وقم بزيارة URL قابل للوصول (على سبيل المثال، خادم ويب داخلي/خارجي). يقوم ISE بإعادة توجيهك إلى البوابة. انقر فوق **متابعة**.



3. تتم إعادة توجيهك إلى "بوابة الضيوف" لتسجيل الدخول.



4. قم بتسجيل الدخول باستخدام حساب مستخدم وكلمة مرور AD. قم بتثبيت ملف تعريف المرجع المصدق عند طلبها.

5. انقر على **تثبيت** الشهادة الموثوق بها لخادم CA.

6. انقر على **تم** بمجرد أن يتم تثبيت ملف التخصيص بالكامل.

7. ارجع إلى المستعرض، وانقر فوق **تسجيل**. دون معرف الجهاز الذي يحتوي على عنوان MAC للجهاز.

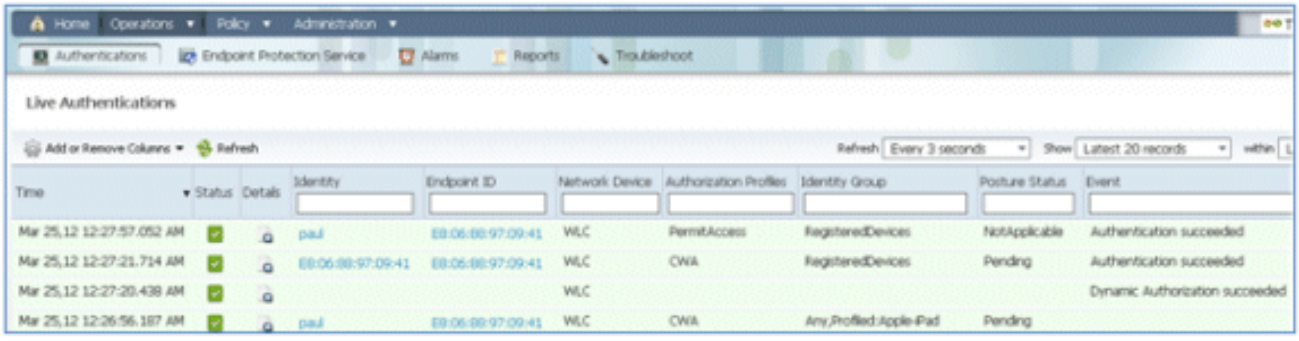
8. انقر على **تثبيت** لتثبيت التوصيف الذي تم التحقق منه.

9. انقر على **تثبيت الآن**.

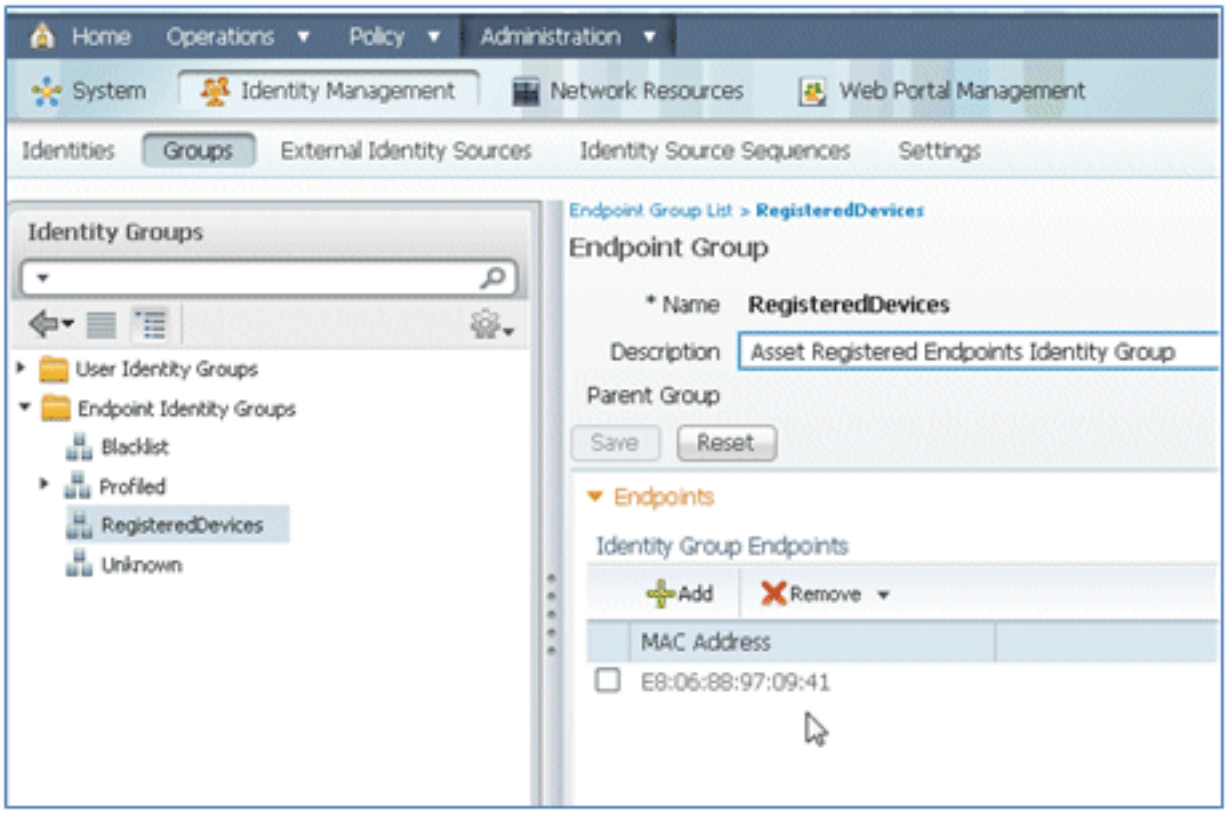
10. بعد اكتمال العملية يؤكد توصيف WirelessSP تثبيت التوصيف. طقطقة **تم**.

انتقل إلى **شبكات Wi-Fi**، وقم بتغيير الشبكة إلى **العرض التوضيحي1x**. جهازك متصل الآن ويستخدم TLS11.

على ISE، انتقل إلى **العمليات > المصادقة**. تظهر الأحداث العملية التي يتم فيها توصيل الجهاز بشبكة الضيف12. المفتوحة، ويمر بعملية التسجيل باستخدام تزويد مقدم الطلب، ويتم السماح بالوصول بعد التسجيل.



انتقل إلى ISE > إدارة > إدارة الهوية > **مجموعات > مجموعات هوية نقطة النهاية** > الأجهزة المسجلة. تم13. إضافة عنوان MAC إلى قاعدة البيانات.

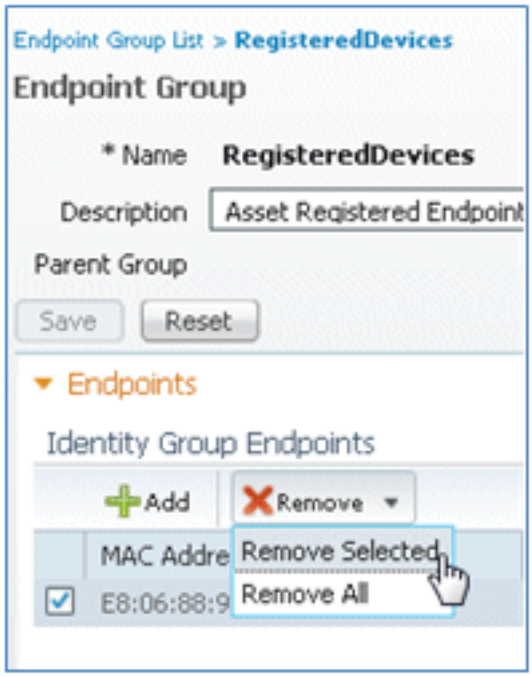


SSID واحد

يغطي هذا القسم Single SSID ويصف كيفية الاتصال مباشرة بشبكة محلية لاسلكية 802.1x، وتوفير AD username/كلمة المرور لمصادقة PEAP، والتزويد من خلال حساب ضيف، وإعادة الاتصال ب TLS.

أكمل الخطوات التالية لتوفير نظام التشغيل iOS في سيناريو SSID واحد:

1. إذا كنت تستخدم جهاز iOS نفسه، فقم بإزالة نقطة النهاية من الأجهزة المسجلة.



2. على جهاز iOS، انتقل إلى **الإعدادات > الجنرالات > ملفات التعريف**. أزل التوصيفات المثبتة في هذا المثال.

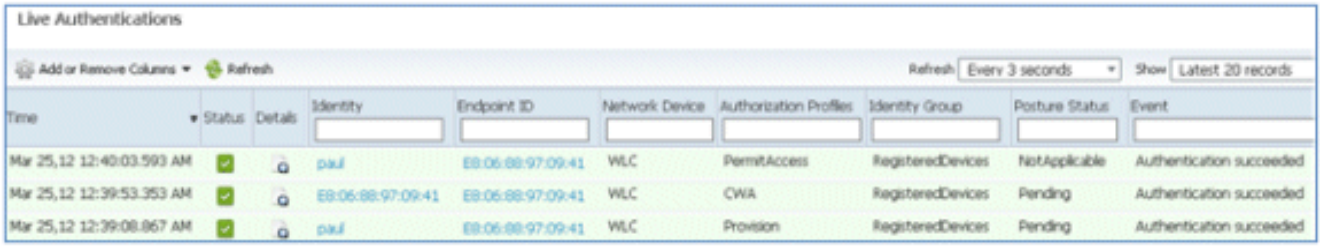
3. انقر على **إزالة** لإزالة التوصيفات السابقة.

4. قم بالاتصال مباشرة بالمحول 802.1x باستخدام الجهاز (الممسوح) الموجود أو جهاز iOS جديد.

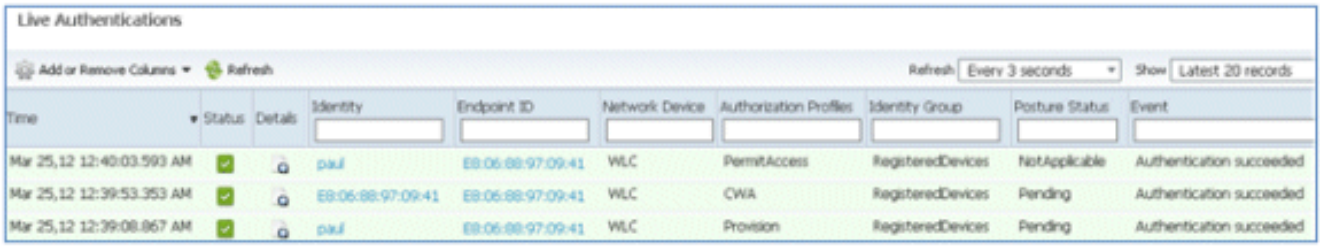
5. ربطت إلى **dot1x**، دخلت username وكلمة، وطقطقة **يتلاقى**.

6. كرر الخطوات 90 وما إلى ذلك من قسم تكوين ISE حتى يتم تثبيت التوصيفات المناسبة بالكامل.

7. انتقل إلى **ISE > العمليات > عمليات المصادقة** لمراقبة العملية. يوضح هذا المثال العميل المتصل مباشرة بشبكة 802.1X المحلية اللاسلكية (WLAN) أثناء تزويدها، ثم قطعها، وإعادة إتصالها بشبكة WLAN نفسها باستخدام قوائم التحكم في الوصول إلى النقل (TLS).



8. انتقل إلى **WLC > شاشة > [Client MAC]**. في تفاصيل العميل، لاحظ أن العميل في حالة RUN، وتم تعيين تحويل البيانات الخاص به على محلي، وأن المصادقة مركزية. ويصدق هذا على العملاء الذين يقومون بالاتصال بنقطة الوصول FlexConnect AP.



تجربة المستخدم - توفير Android

SSID مزدوج

يغطي هذا القسم SSID المزدوج ويصف كيفية الاتصال بالضيف المراد توفيره وكيفية الاتصال بشبكة محلية لاسلكية (WLAN) بسرعة 802.1x.

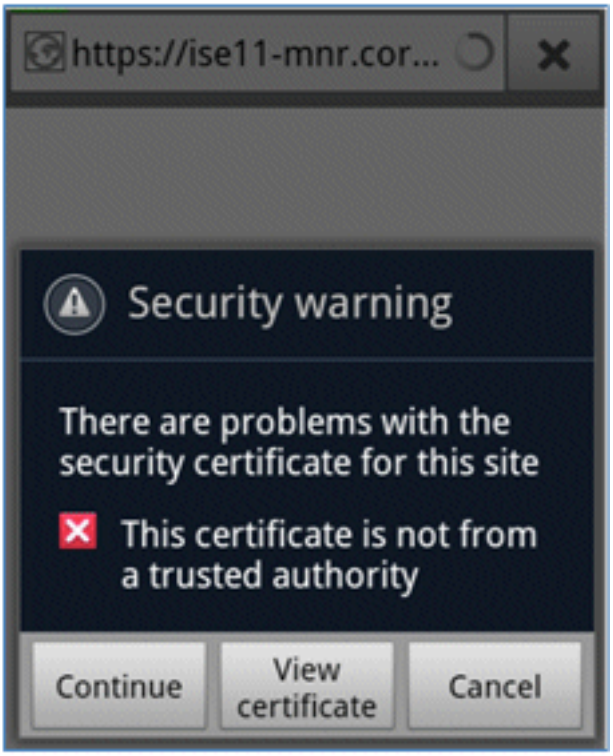
عملية الاتصال لجهاز Android تشبه كثيرا عملية الاتصال بجهاز iOS (معرف SSID أحادي أو مزدوج). ومع ذلك،

فالفرق المهم هو أن جهاز الأندرويد يتطلب الدخول إلى الإنترنت من أجل الوصول إلى سوق جوجل (الآن جوجل بلاي) وتنزيل مقدم الطلب.

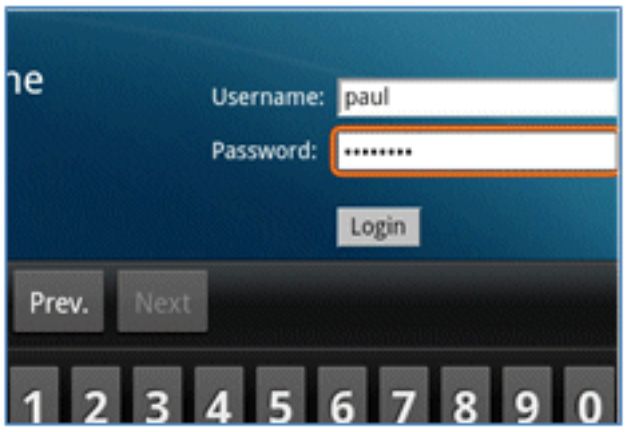
أكمل هذه الخطوات لتوفير جهاز يعمل بنظام التشغيل Android (مثل Samsung Galaxy في هذا المثال) في سيناريو SSID المزدوج:

1. في جهاز Android، أستخدم Wi-Fi للاتصال ب **DemoCWA**، وافتح شبكة WLAN للضيف.

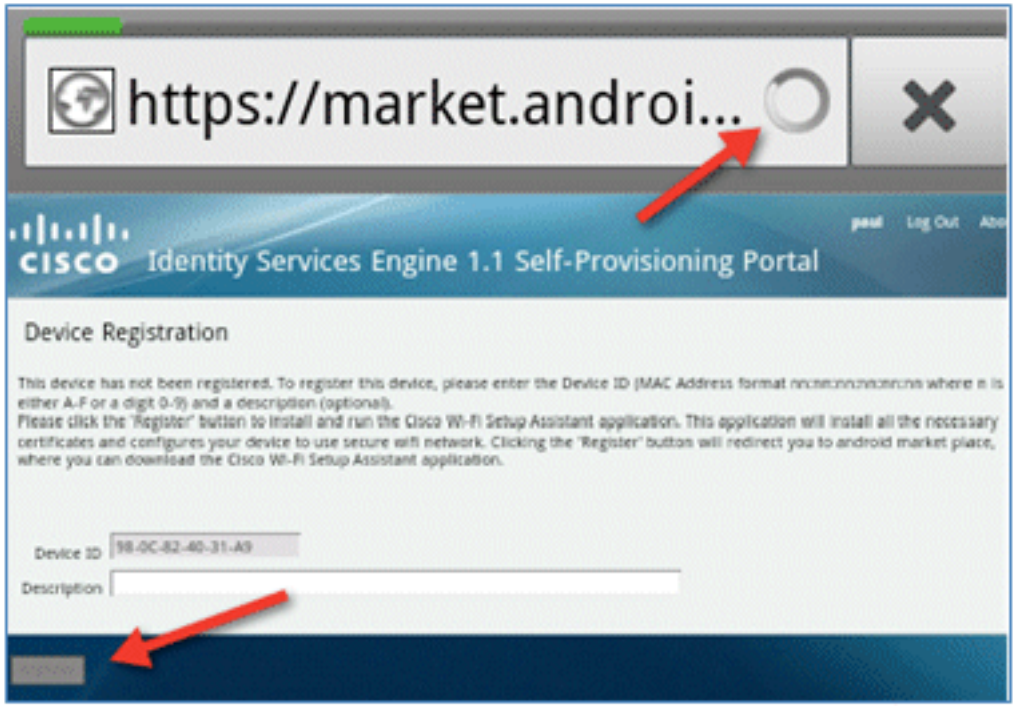
2. قبول أي شهادة للاتصال ب ISE.



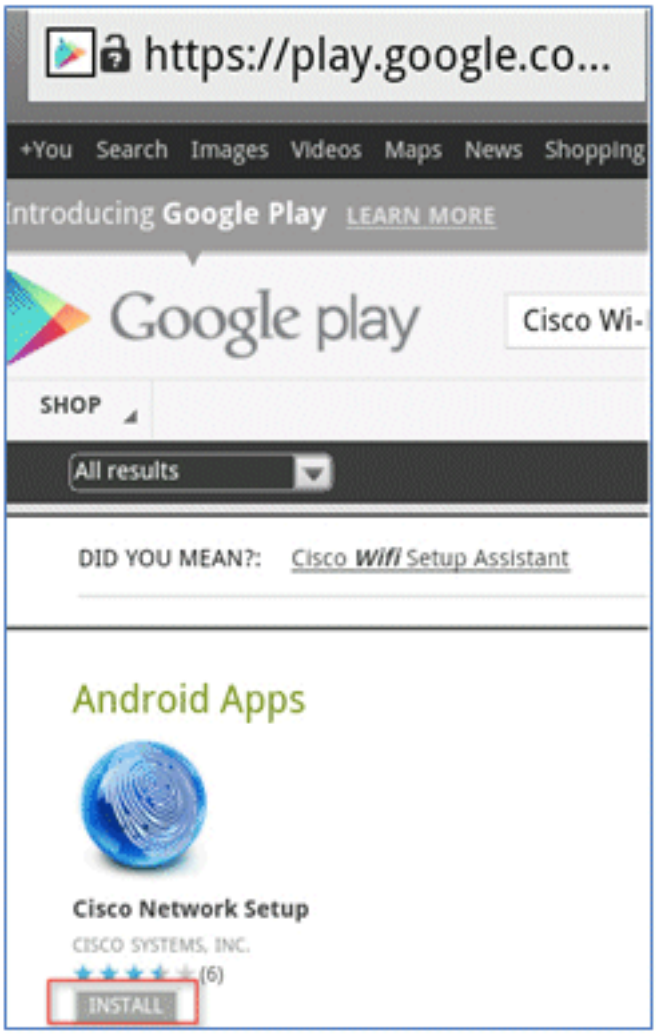
3. أدخل اسم مستخدم وكلمة مرور في مدخل الضيف لتسجيل الدخول.



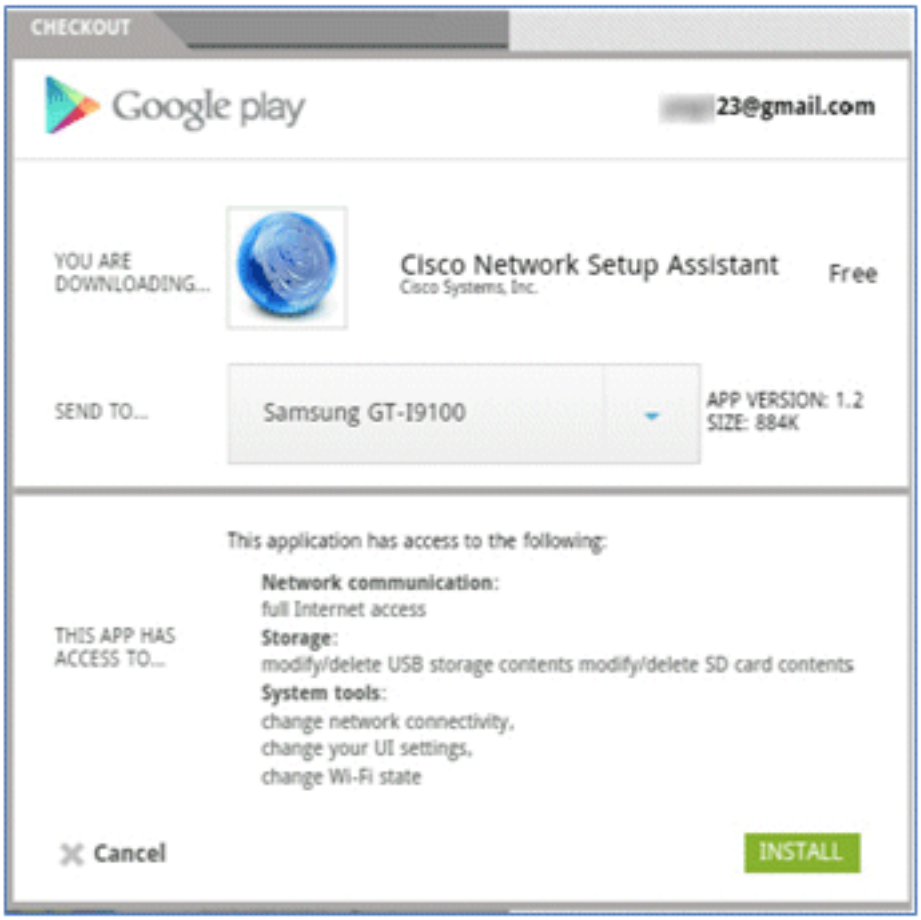
طقطقة **سجل**. ويحاول الجهاز الوصول إلى الإنترنت من أجل الوصول إلى سوق جوجل. قم بإضافة أي قواعد4. إضافية إلى قائمة التحكم بالوصول (ACL) السابقة للمصادقة (مثل إعادة توجيه قائمة التحكم في الوصول) في وحدة التحكم للسماح بالوصول إلى الإنترنت.



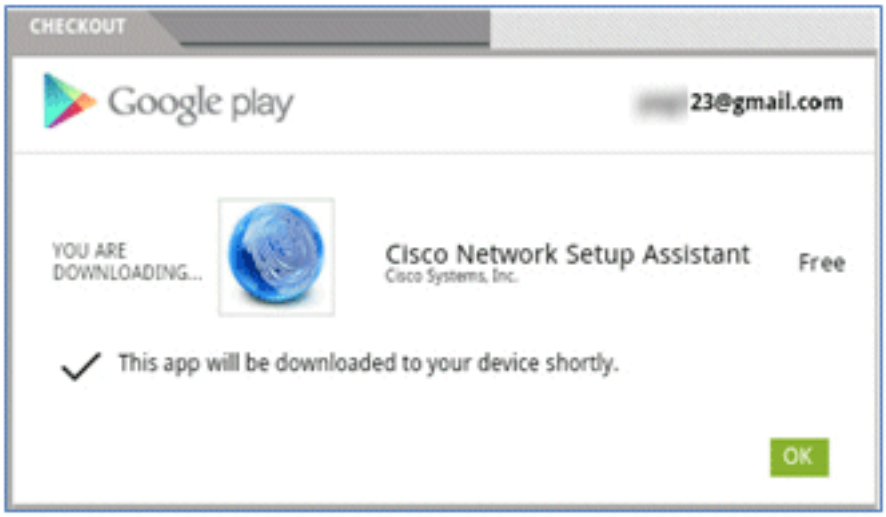
غوغل تدرج إعداد شبكة Cisco على أنه تطبيق يعمل بنظام التشغيل Android. انقر على **تثبيت**. 5.



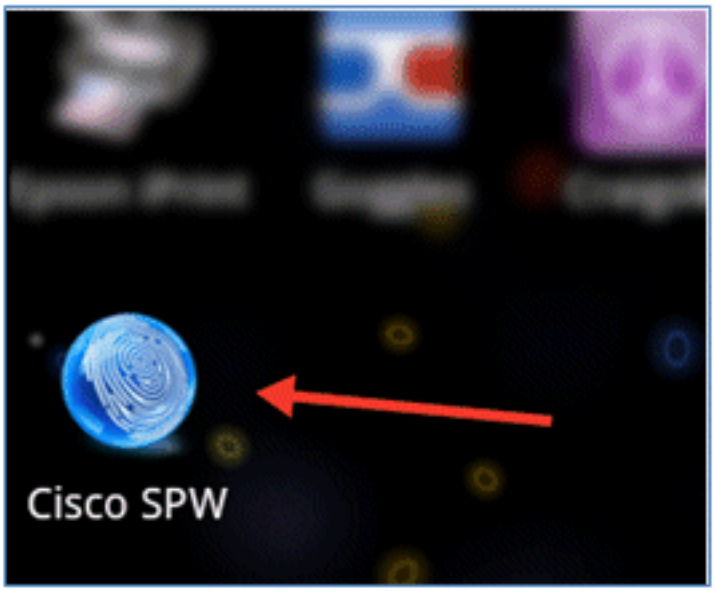
6. قم بتسجيل الدخول إلى Google، وانقر فوق **تثبيت**.



7. وانقر فوق **OK**.



8. على جهاز Android، ابحث عن تطبيق **Cisco SPW** المثبت، وافتحه.



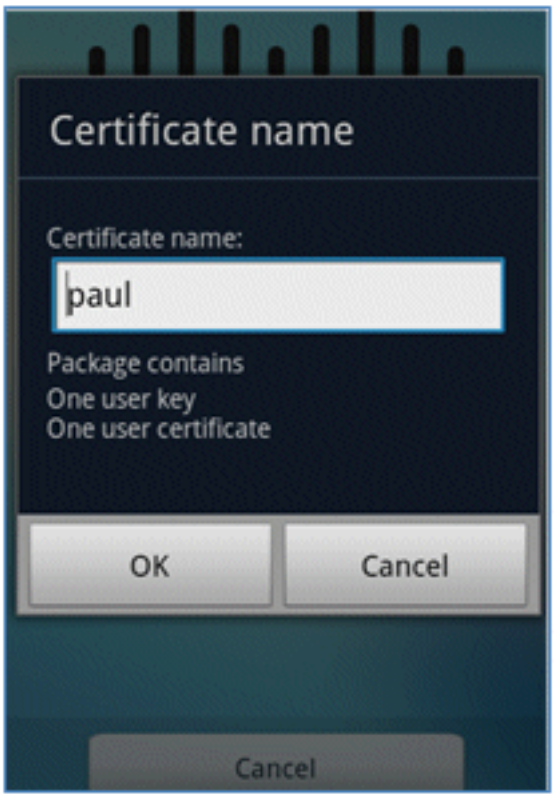
9. تأكد من أنك لا تزال تسجل دخولك إلى "مدخل الضيف" من جهاز Android الخاص بك.

10. انقر على **بدء** لبدء مساعد إعداد Wi-Fi.

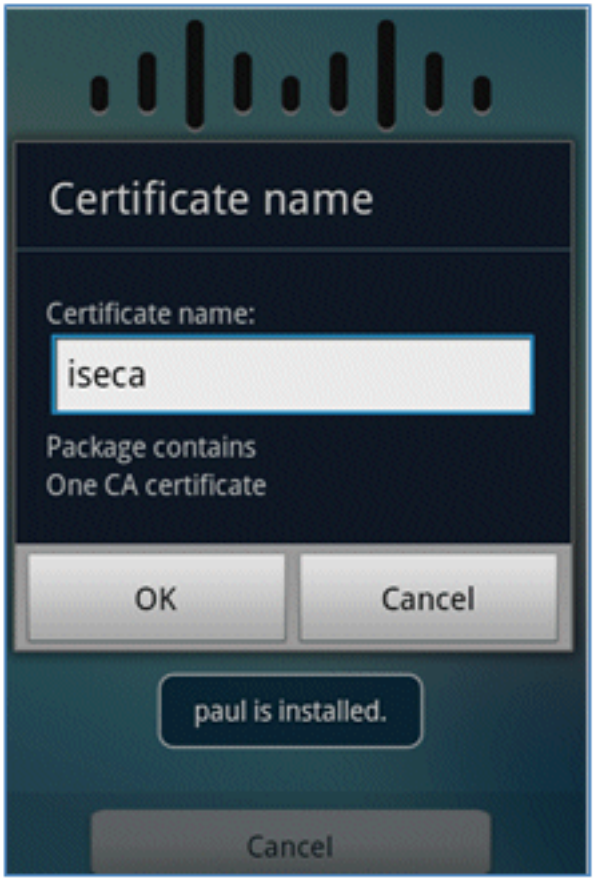
11. يبدأ SPW من Cisco في تثبيت الشهادات.

12. عند المطالبة، قم بتعيين كلمة مرور لتخزين بيانات الاعتماد.

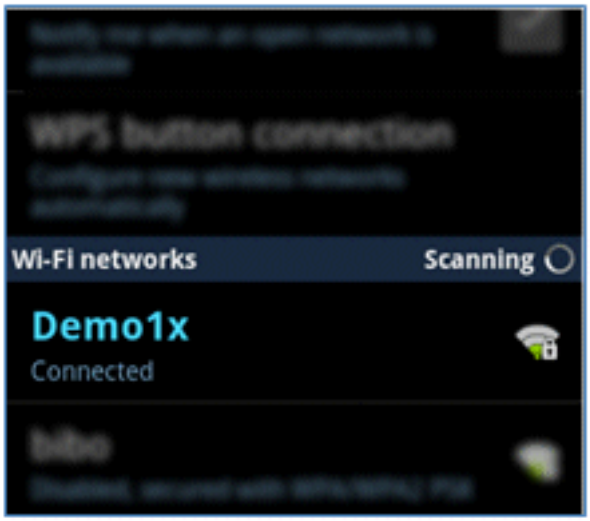
13. يرجع Cisco SPW باسم شهادة، يحتوي على مفتاح المستخدم وشهادة المستخدم. طقطقة ok in order to أكدت.



14. يستمر SPW من Cisco ويطلب اسم شهادة آخر، يحتوي على شهادة CA. أدخل الاسم **iseca** (في هذا المثال)، ثم انقر فوق **موافق** للمتابعة.



15. جهاز Android متصل الآن.

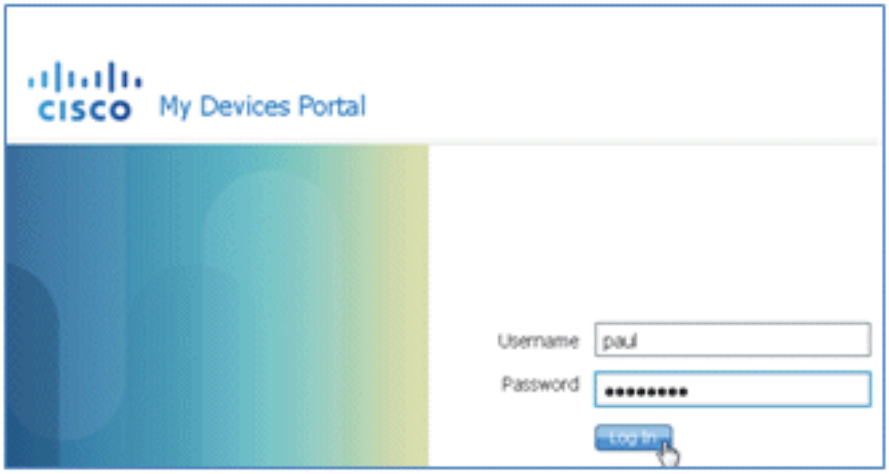


بوابة أجهزتي

يسمح "مدخل الأجهزة الخاصة بي" للمستخدمين بإدراج الأجهزة المسجلة سابقا في القائمة السوداء في حالة فقد الجهاز أو سرقته. كما أنها تسمح للمستخدمين بإعادة الانضمام إذا لزم الأمر.

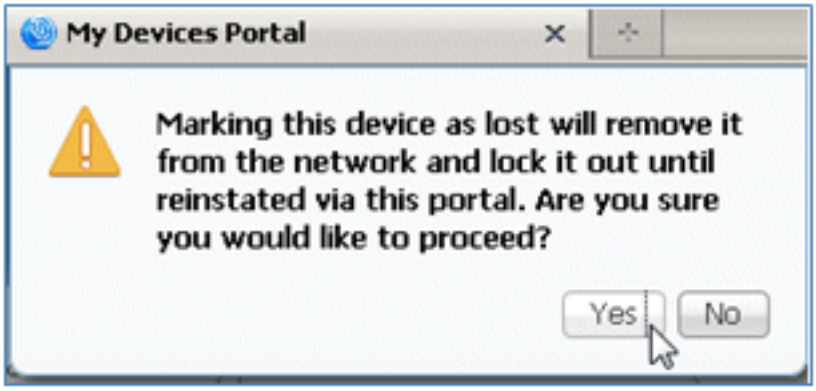
أتمت هذا steps in order to عددت أداة:

1. لتسجيل الدخول إلى بوابة الأجهزة الخاصة بي، افتح مستعرض، واتصل ب https://ise-server:8443/mydevices (لاحظ رقم المنفذ 8443)، ثم قم بتسجيل الدخول باستخدام حساب AD.



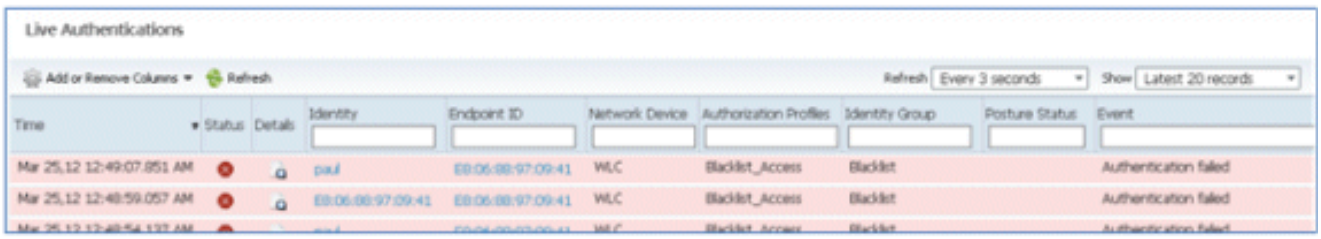
2. حدد موقع الجهاز تحت معرف الجهاز، وانقر فوق **فقدان؟** لبدء إدخال القائمة السوداء للجهاز.

3. عندما يطلب ISE تحذيرا، انقر فوق **نعم** للمتابعة.

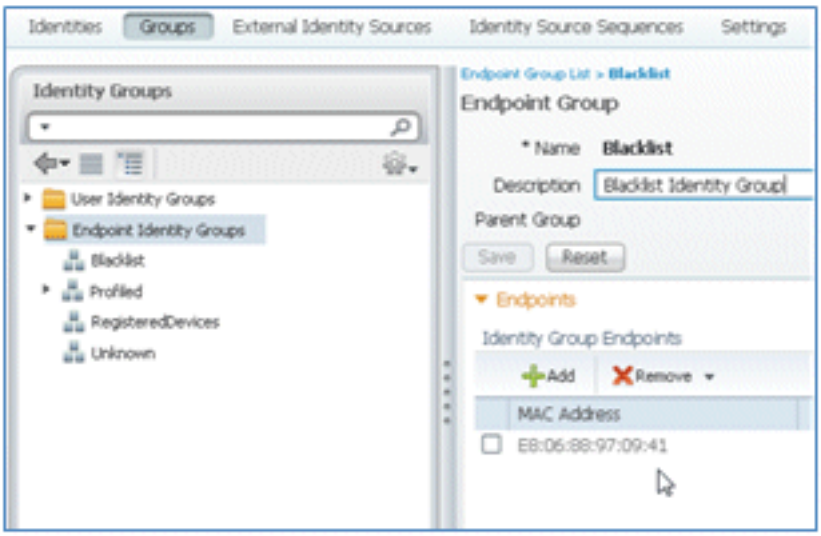


4. يؤكد ISE أن الجهاز تم وضع علامة **LOST عليه**.

5. يتم الآن حظر أي محاولة للاتصال بالشبكة بواسطة الجهاز المسجل مسبقا، حتى في حالة تثبيت شهادة صالحة. هذا مثال على جهاز مدرج في القائمة السوداء يفشل في المصادقة:



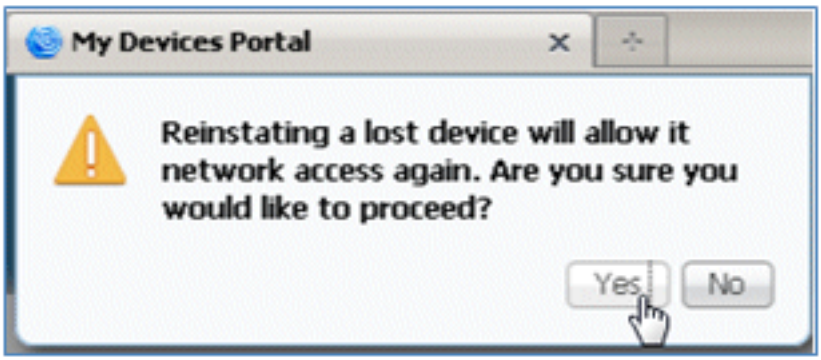
6. يمكن أن ينتقل المسؤول إلى ISE > إدارة > إدارة الهوية > **مجموعات**، انقر فوق **مجموعات هوية نقطة النهاية**>القائمة السوداء، وانظر الجهاز مدرجا في القائمة السوداء.



أكمل الخطوات التالية لإعادة إدخال جهاز مدرج في القائمة السوداء:

1. من بوابة "أجهزتي"، انقر فوق **إعادة الحالة** لذلك الجهاز.

2. عندما يطلب ISE تحذيرا، انقر فوق **نعم** للمتابعة.



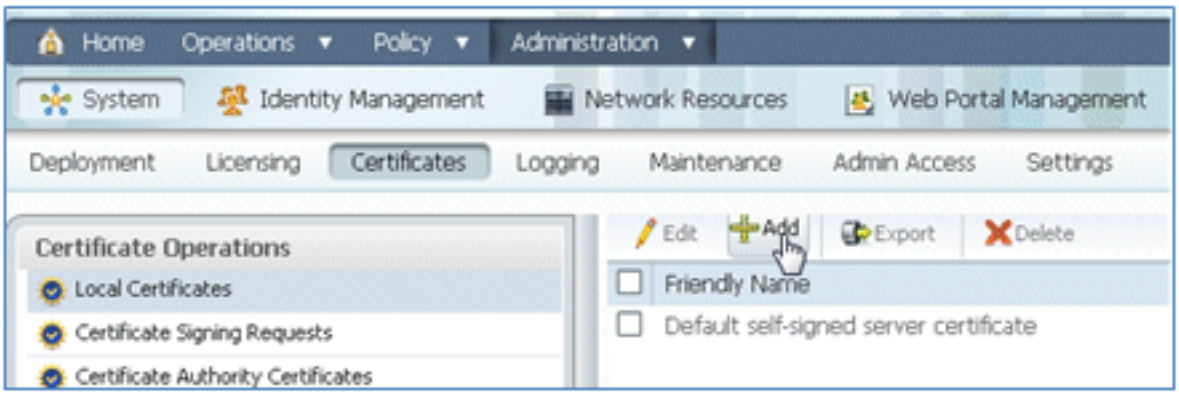
3. يؤكد ISE على إعادة الجهاز بنجاح. قم بتوصيل الجهاز الذي تمت إعادته بالشبكة لاختبار السماح الآن للجهاز.

المرجع - الشهادات

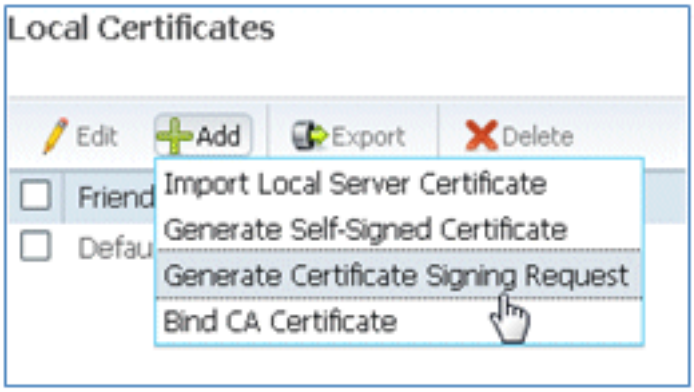
لا يتطلب ISE شهادة جذر CA صالحة فحسب، بل يحتاج أيضا إلى شهادة صالحة موقعة بواسطة CA.

أتمت هذا steps in order to أضفت، ربطت، واستوردت جديد مرجع مصدق ثقة:

1. انتقل إلى ISE > إدارة > النظام > **الشهادات**، وانقر **شهادات محلية**، وانقر إضافة.



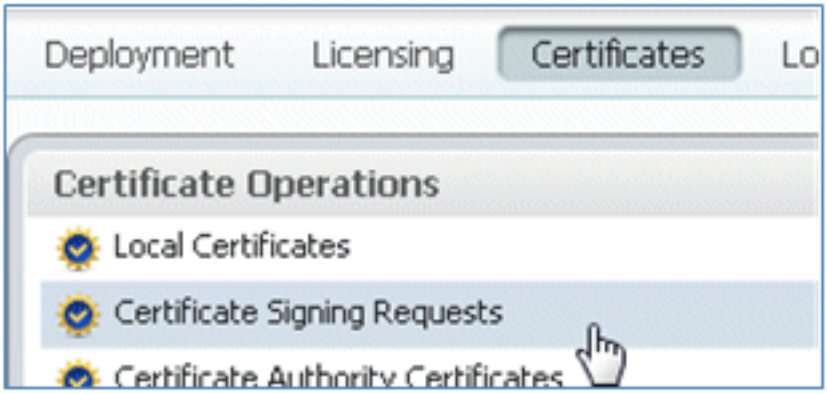
2. حدد **إنشاء طلب توقيع الشهادة** (CSR).



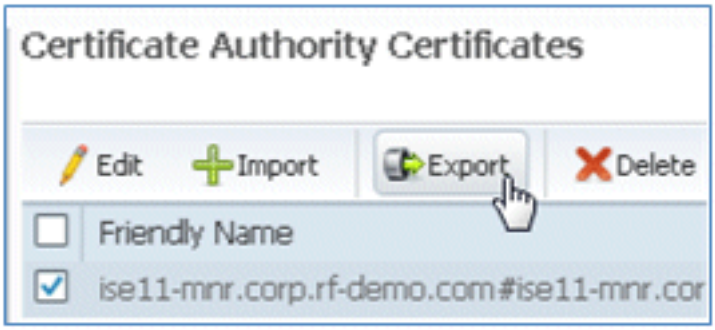
3. أدخل موضوع الشهادة **CN=<***ISE-Server Hostname.FQDN***>**. للحقول الأخرى، يمكنك إستخدام القيم الافتراضية أو القيم المطلوبة من قبل إعداد المرجع المصدق. انقر على **إرسال**.

4. يتحقق ISE من إنشاء CSR.

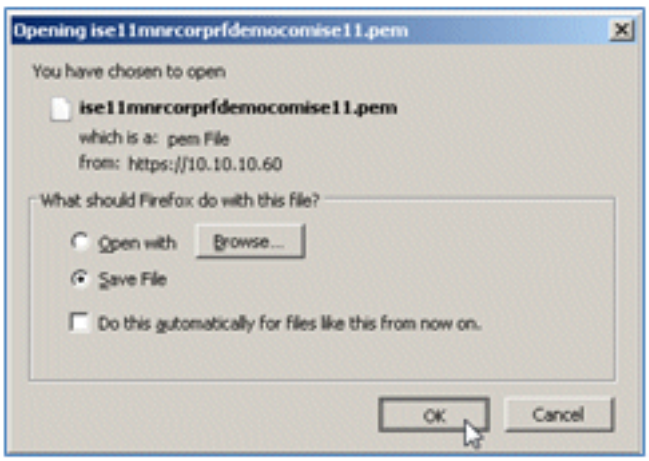
5. للوصول إلى CSR، انقر على عمليات **طلبات توقيع الشهادة**.



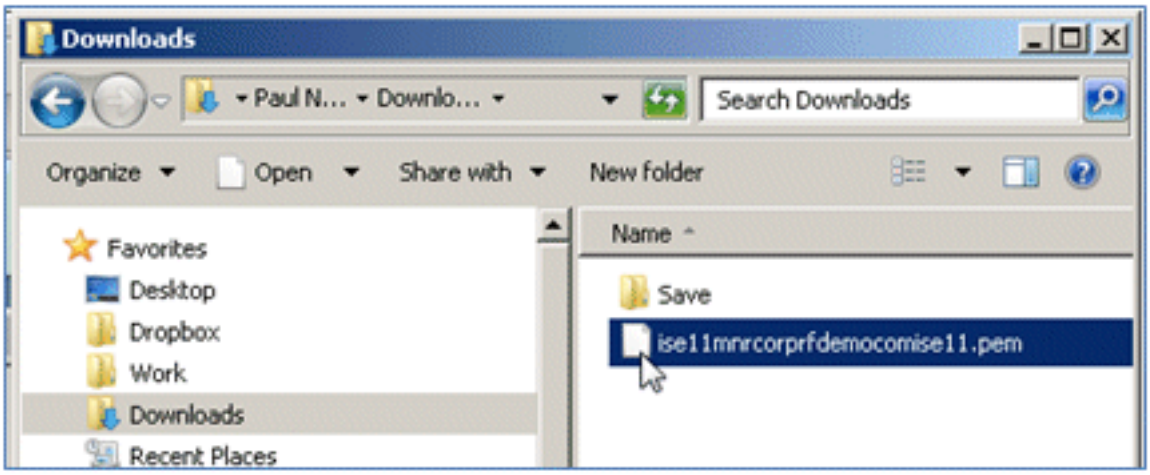
6. حدد CSR الذي تم إنشاؤه مؤخرا، ثم انقر فوق **تصدير**.



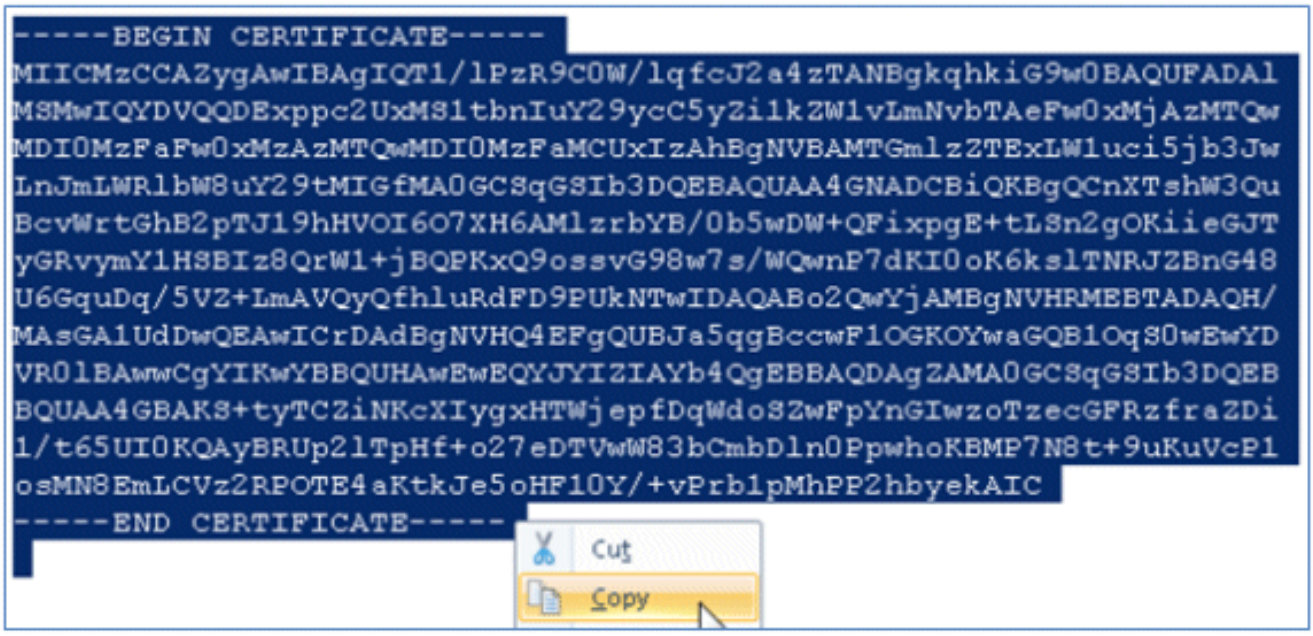
7. يقوم ISE بتصدير CSR إلى ملف .pem. انقر فوق **حفظ الملف**، ثم انقر فوق **موافق** لحفظ الملف على الجهاز المحلي.



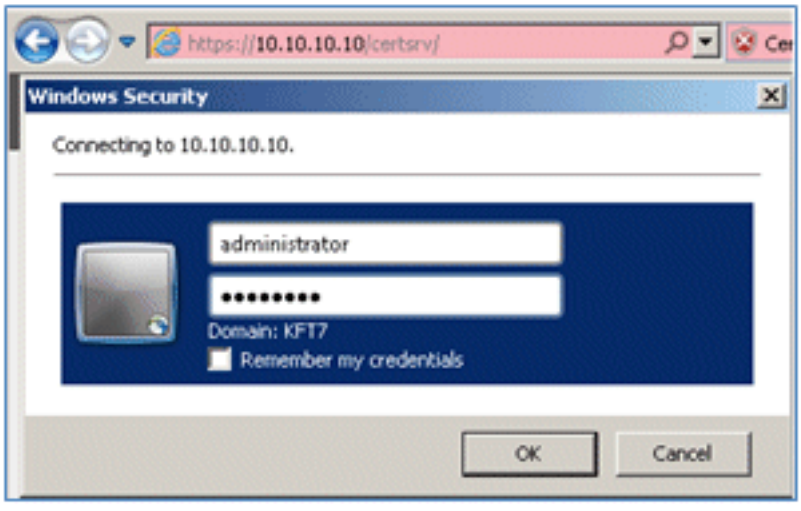
8. حدد مكان وافتح ملف شهادة ISE باستخدام محرر نصي.



9. نسخ محتوى الشهادة بالكامل.

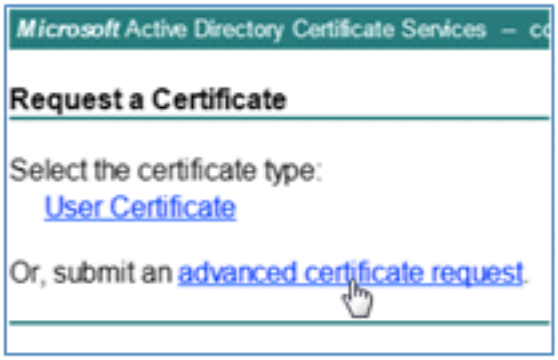


10. اتصل بخادم CA، وسجل الدخول باستخدام حساب مسؤول. الخادم هو مرجع مصدق Microsoft 2008 في https://10.10.10.10/certsrv (في هذا المثال).

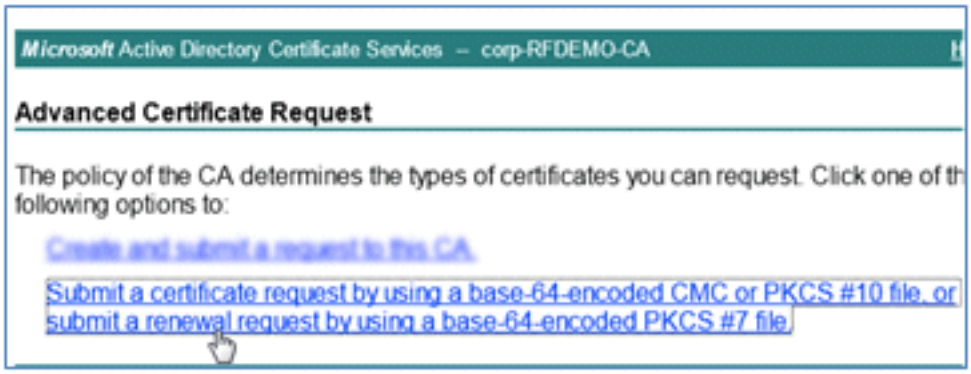


11. انقر على **طلب شهادة**.

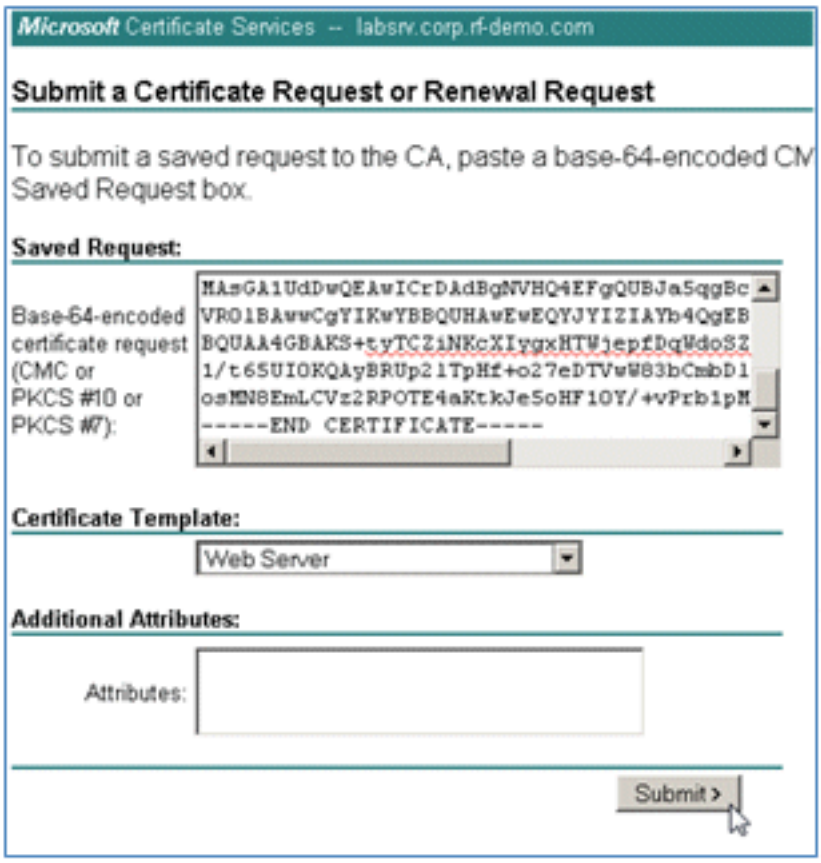
12. انقر على **طلب شهادة متقدمة**.



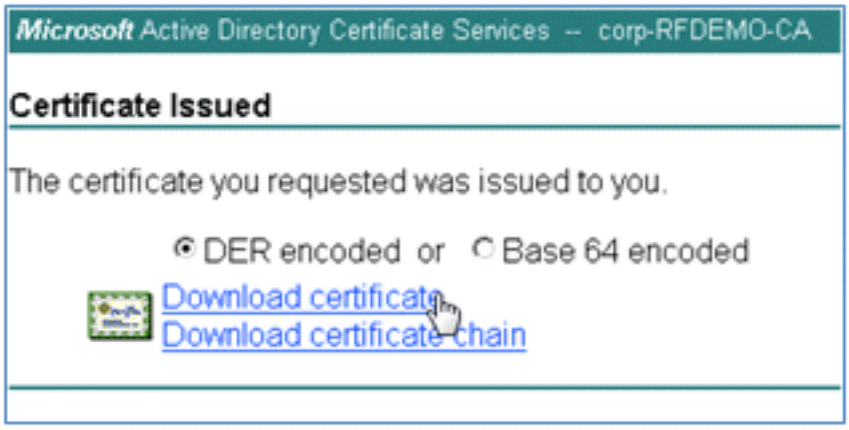
13. انقر على الخيار الثاني **لإرسال طلب شهادة باستخدام CMC مرمز بالأساس 64 أو ...** .



الصق المحتوى من ملف شهادة pem.) ISE) في حقل الطلب المحفوظ، وتأكد من أن قالب الشهادة هو **خادم ويب**، وانقر **إرسال**.

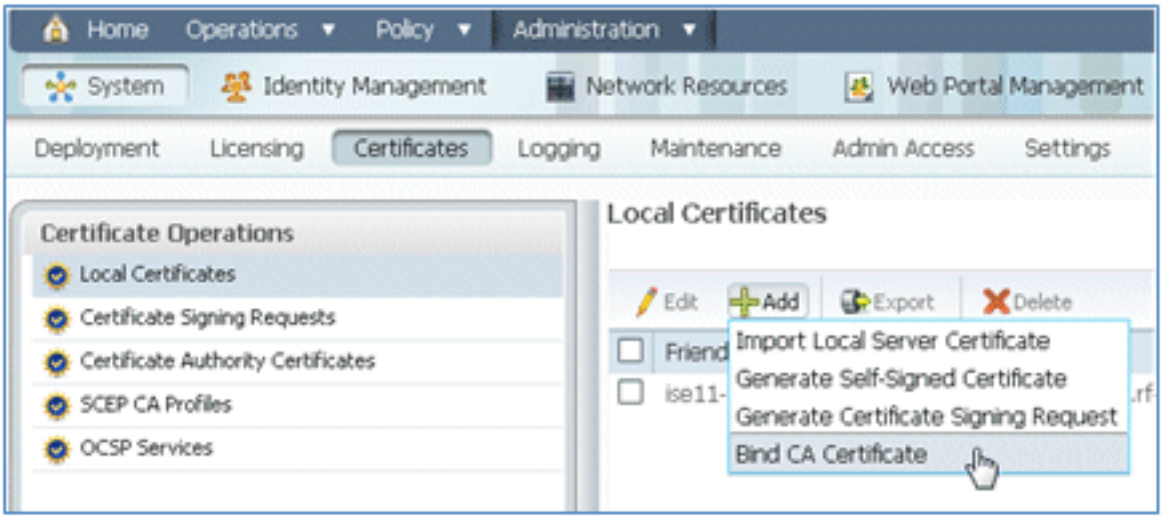


15. انقر على **تنزيل الشهادة**.

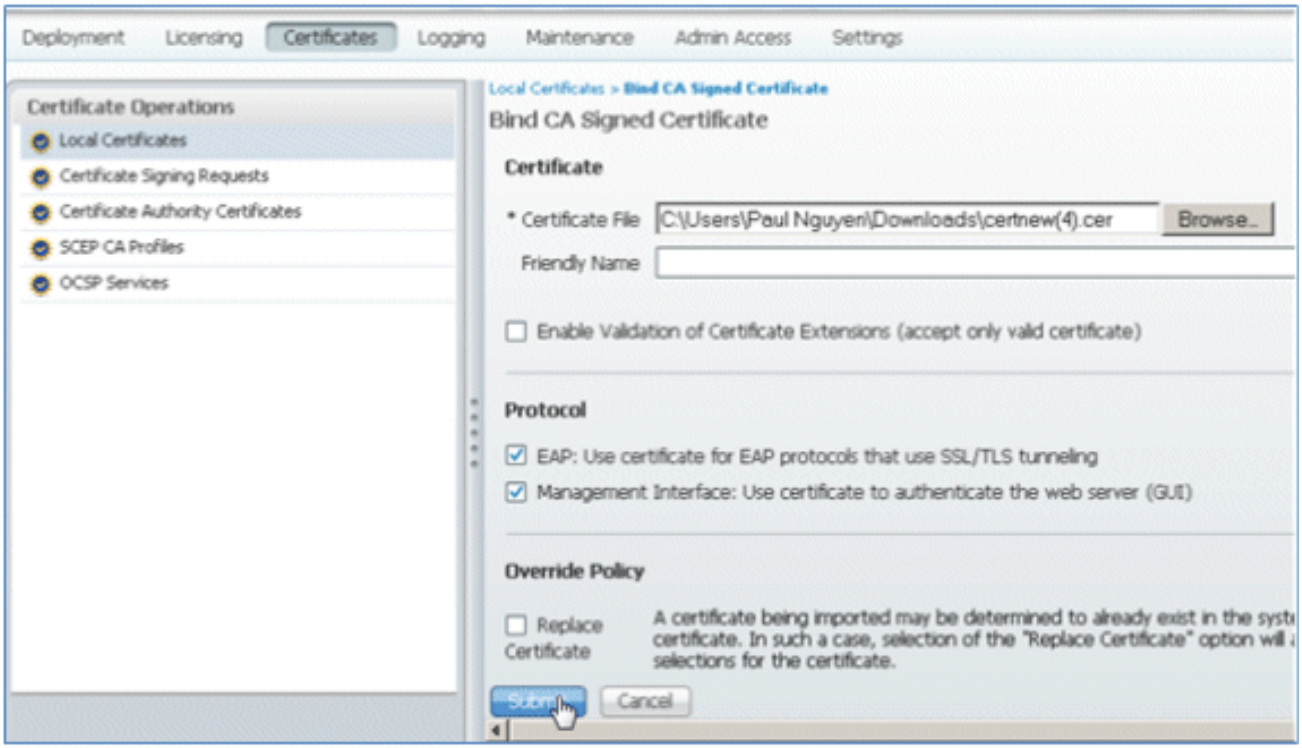


16. قم بحفظ ملف certnew.cer؛ سيتم إستخدامه لاحقا للربط مع ISE.

17. من **شهادات ISE**، انتقل إلى **شهادات محلية**، وانقر **إضافة > ربط شهادة CA**.



18. تصفح إلى الشهادة التي تم حفظها على الجهاز المحلي في الخطوة السابقة، وقم بتمكين كل من **EAP** و**بروتوكولات واجهة الإدارة** (المربعات محددة)، وانقر **إرسال**. قد يستغرق ISE عدة دقائق أو أكثر لإعادة تشغيل الخدمات.

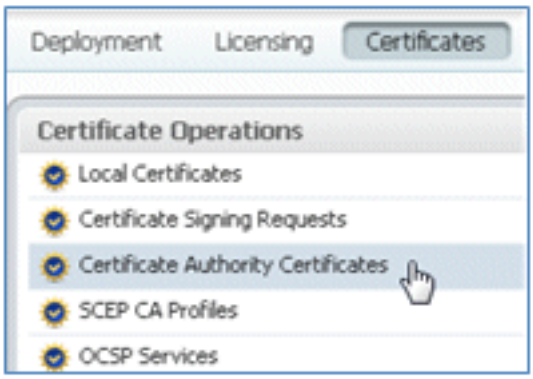


19. ارجع إلى صفحة تنزيل (https://CA/certsrv/CA)، وانقر فوق **تنزيل شهادة CA أو سلسلة الشهادات أو CRL**.

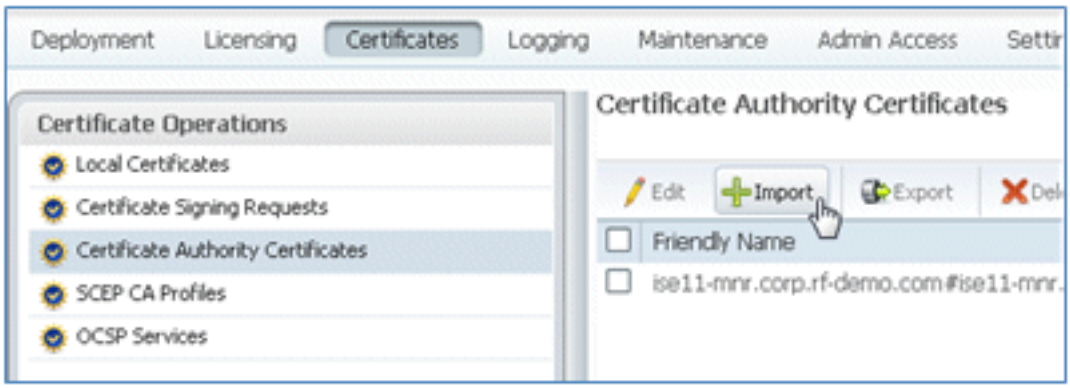
20. انقر على **تنزيل شهادة المرجع المصدق**.

21. **قم بحفظ** الملف على الجهاز المحلي.

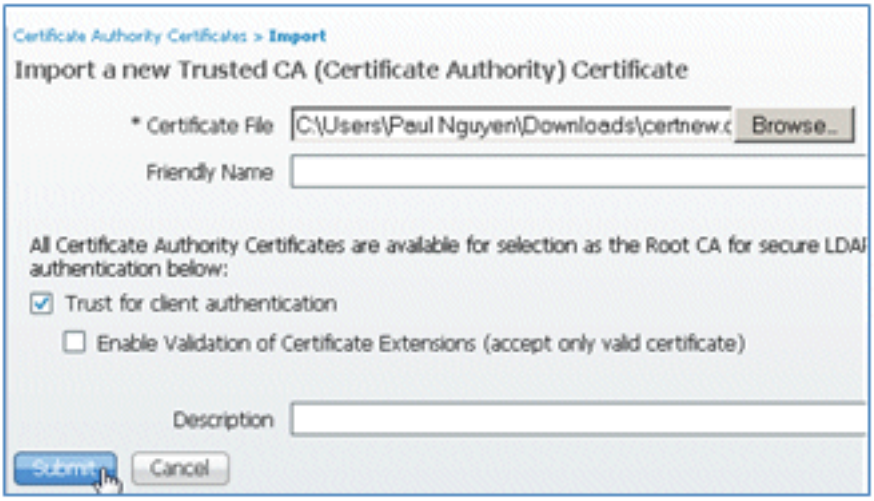
22. مع وجود خادم ISE عبر الإنترنت، انتقل إلى **الشهادات**، وانقر فوق **شهادات المرجع المصدق**.



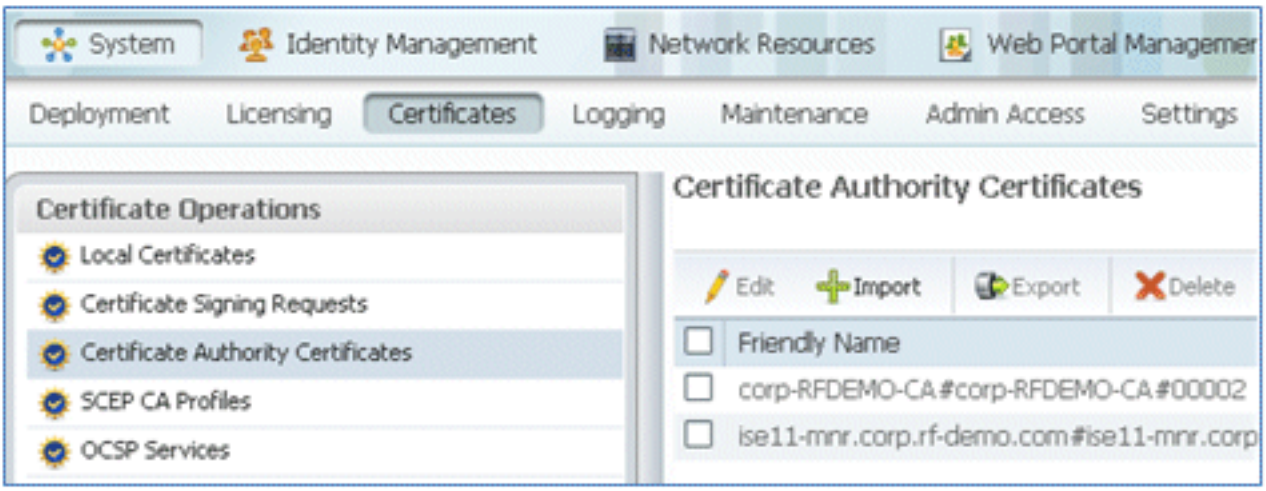
23. انقر فوق **استيراد**.



24. استعرض شهادة CA، وقم بتمكين **الثقة لمصادقة العميل** (المربع محدد)، وانقر **إرسال**.



25. تأكد من إضافة شهادة مرجع مصدق ثقة جديدة.



معلومات ذات صلة

- دليل تثبيت أجهزة محرك خدمات الهوية من Cisco، الإصدار 1.0.4
- سلسلة وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية 2000 من Cisco
- سلسلة وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية 4400 من Cisco
- السلسلة Cisco Aironet 3500 Series
- دليل نشر وحدة التحكم الفرعية اللاسلكية Flex 7500
- احصل على الجهاز الخاص بك - مصادقة الجهاز الموحد واختبار الوصول المتناسق
- BYOD اللاسلكي مع محرك خدمات الهوية
- الدعم التقني والمستندات - Cisco Systems

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).