

# ل ٲٲ كل سل ال ال ال BYOD ٲٲ ن ق ت ر ش ن ل ل ل د FlexConnect

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [طوبولوجيا](#)
- [تسجيل الجهاز وتوفير ملتمس](#)
- [بوابة تسجيل الأصول](#)
- [بوابة التسجيل الذاتي](#)
- [المصادقة والإمداد](#)
- [الإمداد بنظام التشغيل \(iOS \(iPhone/iPad/iPod](#)
- [توفير ل Android](#)
- [التسجيل الذاتي لبطاقة BYOD اللاسلكية المزودة لشبكة SSID](#)
- [التسجيل الذاتي لبطاقة BYOD اللاسلكية أحادية SSID](#)
- [تكوين الميزة](#)
- [تكوين شبكة WLAN](#)
- [تكوين نقطة الوصول عبر الإنترنت FlexConnect](#)
- [تكوين ISE](#)
- [تجربة المستخدم - توفير نظام التشغيل iOS](#)
- [SSID مزدوج](#)
- [SSID واحد](#)
- [تجربة المستخدم - توفير Android](#)
- [SSID مزدوج](#)
- [بوابة أجهزتي](#)
- [المرجع - الشهادات](#)
- [معلومات ذات صلة](#)

## المقدمة

أصبحت الأجهزة المحمولة أكثر قوة من الناحية الحسابية وأكثر شيوعاً 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 AD) للشركة وينزل شهادة بعنوان MAC مدمج لاسم مستخدم iPad إلى iPad، بالإضافة إلى ملف تعريف ملحق يفرض استخدام بروتوكول المصادقة المتوسع - أمان طبقة النقل (EAP-TLS) كطريقة لاتصال dot1x. استنادا إلى سياسة التحويل 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:

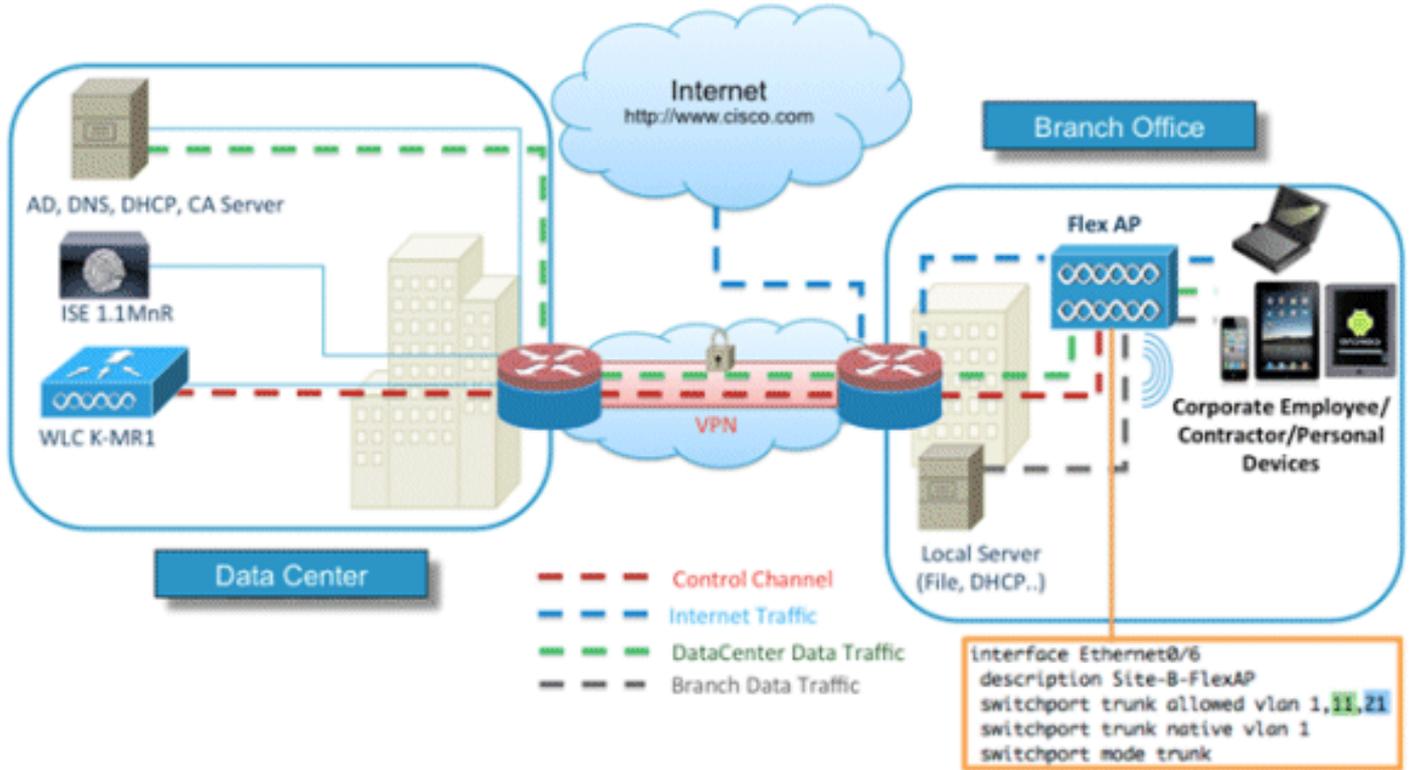
- المحولات Cisco Catalyst Switches
- وحدات التحكم في الشبكة المحلية اللاسلكية (WLAN) من Cisco
- برنامج (Cisco WLAN Controller) (WLC) الإصدار 7.2.110.0 والإصدارات الأحدث
- نقاط الوصول من شبكة 802.11n في وضع FlexConnect
- برنامج Cisco ISE الإصدار 1.1.1 والإصدارات الأحدث
- Windows 2008 AD مع جهة منح الشهادة (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 بوحدة 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

## 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 ISE و WLC. يتم توصيل نقطة الوصول FlexConnect بشبكة لاختبار التحويل المحلي باستخدام شبكات VLAN متعددة.

## تسجيل الجهاز وتوفير ملتمس

يجب تسجيل الجهاز بحيث يمكن للمطالب الأصلي الخاص به توفير مصادقة dot1x. استناداً إلى نهج المصادقة الصحيح، تتم إعادة توجيه المستخدم إلى صفحة الضيف ويتم 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) مدعوماً للتوفير، تتم إعادة توجيه المستخدم إلى مدخل تسجيل الأصول لوضع علامة على ذلك الجهاز للوصول إلى مجرى مصادقة (MAC MAB). إذا كان نظام التشغيل مدعوماً، 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 تحويل 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 ارتباط موجود على الصفحة للموظف بتنزيل معالج (Client Pilot) (SPW).

ملاحظة: ارجع إلى مقالة [Cisco FlexConnect Feature Matrix](#) لعرض أحدث مصفوفة ميزة BYOD ل FlexConnect.

## 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 مسبق.
- 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 المعلومات 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 لمعرفة 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 ضيفاً، فإنه يعيد توجيهه المستخدم إلى صفحة ضيف تسجيل جهاز الموظف.
5. يتم ملء عنوان MAC مسبقاً في صفحة ضيف تسجيل الأجهزة لمعرفة الجهاز. يدخل المستخدم وصفاً ويقبل سياسة الاستخدام المقبول (AUP) إذا لزم الأمر.
6. يحدد المستخدم قبولاً 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) وبمصادق مع EAP-TLS (أو طريقة تحويل 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.

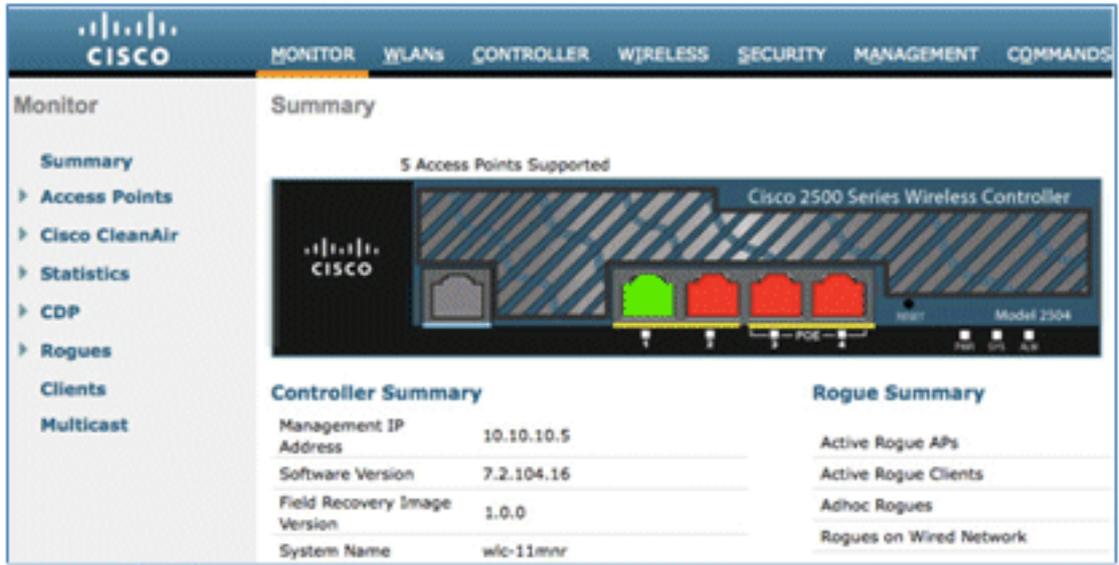
هذه هي عملية التسجيل الذاتي لمعرفة SSID اللاسلكي الفردي لترتيب BYOD:

1. يرتبط المستخدم ب CORP.
2. يدخل المستخدم اسم مستخدم وكلمة مرور للموظف في طلب مصادقة PEAP.
3. يصادق ISE المستخدم، واستناداً إلى أسلوب PEAP، يوفر سياسة تحويل 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 مسبقاً في صفحة ضيف تسجيل الأجهزة لمعرفة الجهاز. يقوم المستخدم بإدخال وصف ويقبل بروتوكول AUP.
6. يحدد المستخدم قبولاً 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 وبمصادق مع EAP-TLS.

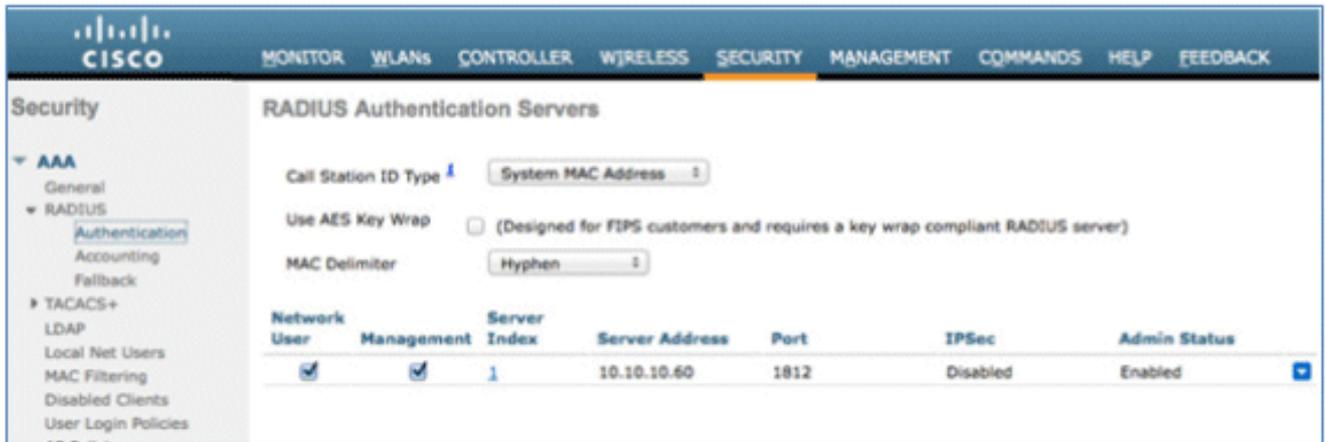
## تكوين الميزة

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 (WLC) اللاسلكية.



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

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

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

### RADIUS Authentication Servers > Edit

Server Index	1
Server Address	10.10.10.60
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

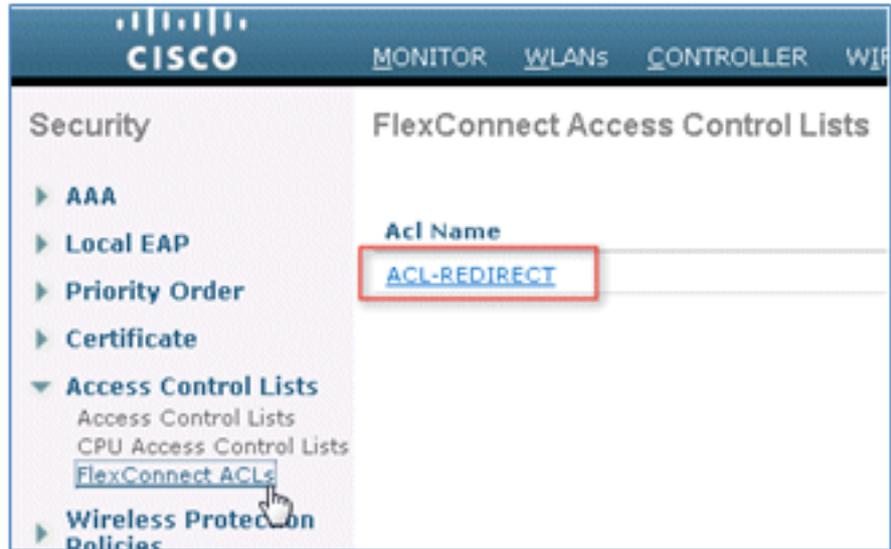
4. قم بإضافة خادم ISE نفسه كخادم محاسبة RADIUS.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANA

### RADIUS Accounting Servers > Edit

Server Index	1
Server Address	10.10.10.60
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

قم بإنشاء قائمة تحكم في الوصول (ACL) سابقة للمصادقة ل WLC لاستخدامها في سياسة ISE لاحقاً. 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).



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 set ip (عنوان 255.255.255.255 NetMask / ISE). تعيين إجراء للسماح.

Access Control Lists > Rules > Edit

Sequence: 1

Source: Any

Destination: IP Address

IP Address: 10.10.10.60

Netmask: 255.255.255.255

Protocol: Any

DSCP: Any

Direction: Any

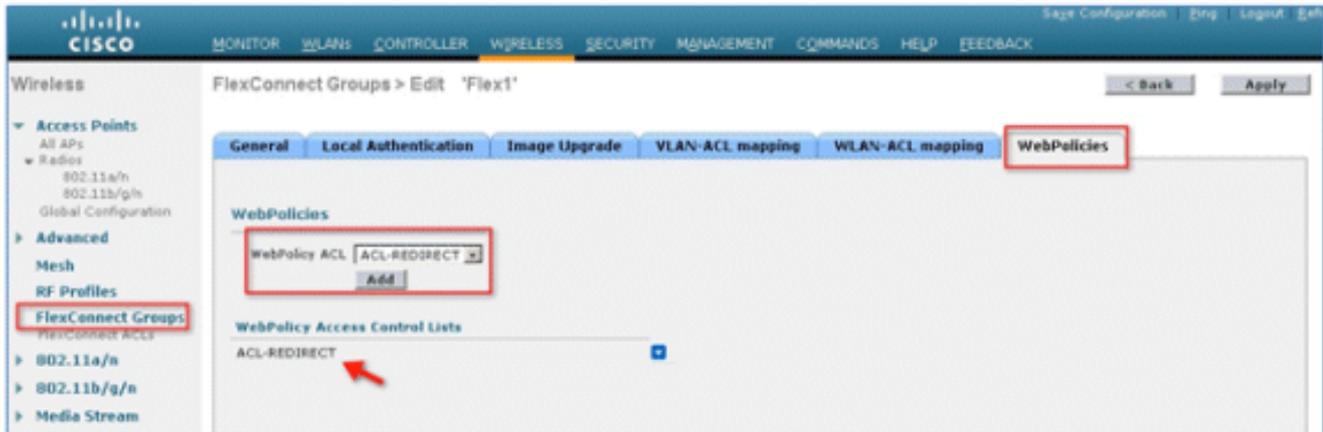
Action: Permit

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

General								
Access List Name		ACL-REDIRECT						
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.60 / 255.255.255.255	Any	Any	Any	Any	<input checked="" type="checkbox"/>
2	Permit	10.10.10.60 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	<input checked="" type="checkbox"/>

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 مسبقاً. تأكد من أنه يقوم بملء حقل قوائم التحكم في الوصول إلى WebPolicy.



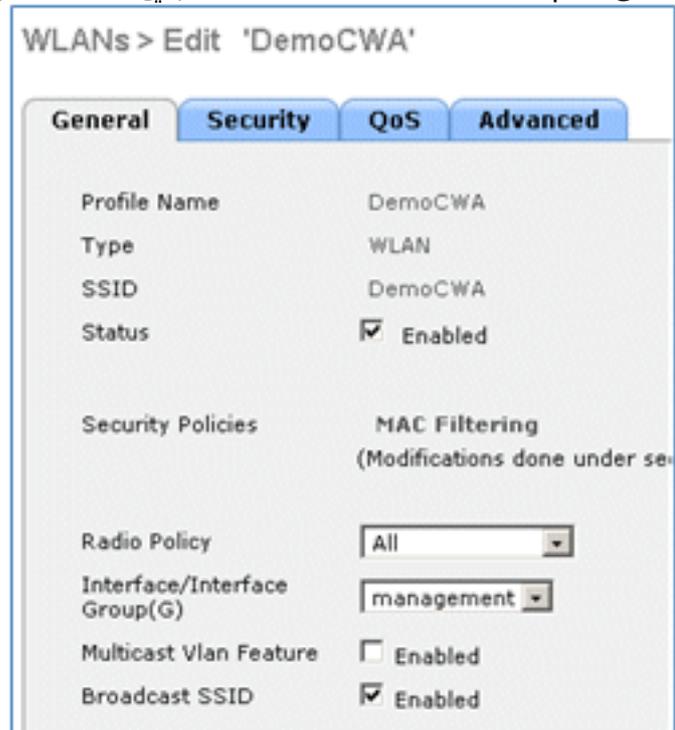
8. طغقة يطبق ويحفظ تشكيل.

## تكوين شبكة WLAN

أتمت هذا steps in order to شكلت ال WLAN:

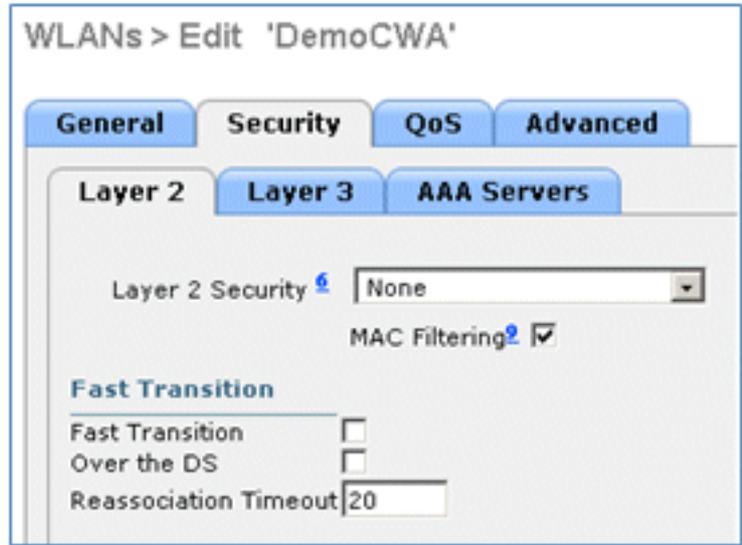
1. إنشاء WLAN SSID مفتوح لمثال SSID المزدوج:

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



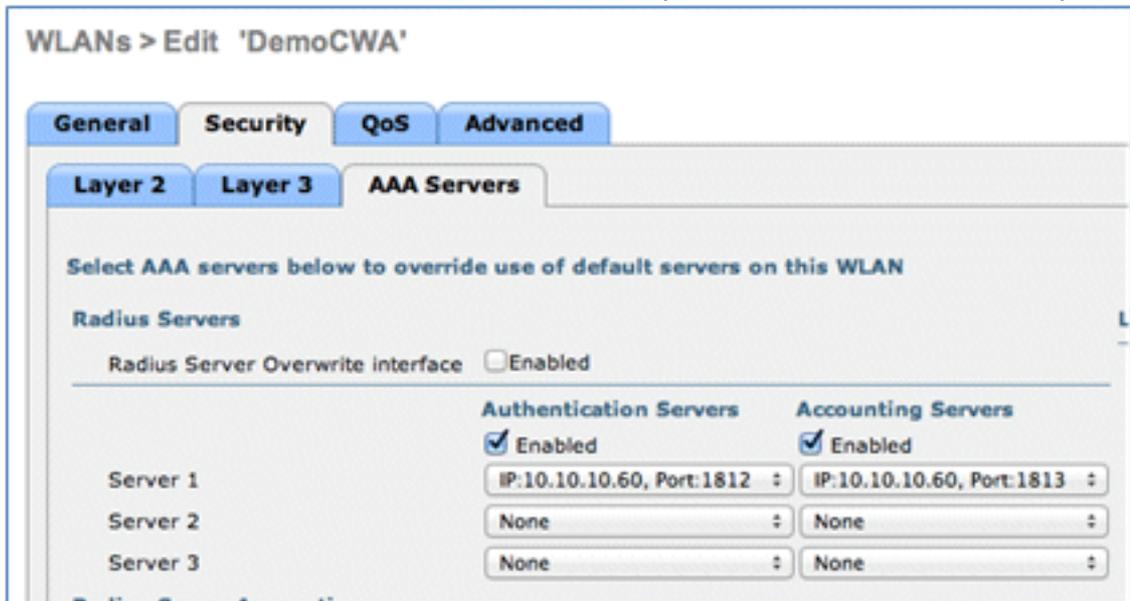
2. انتقل إلى صفحة التأمين < صفحة الطبقة 2، واضبط الخصائص التالية:

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: **ممكناً** خادم 1: **<عنوان IP ISE>**

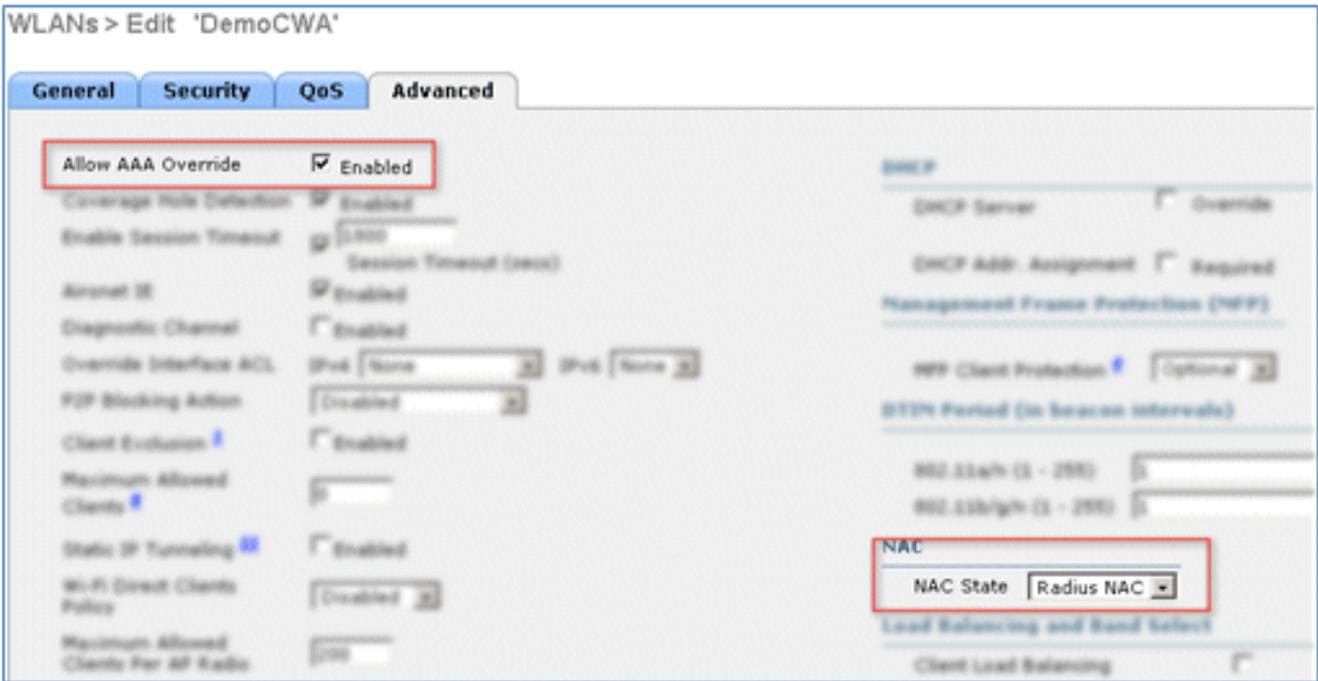


4. قم بالتمرير لأسفل من علامة التبويب **خوادم AAA**. تحت ترتيب أولوية المصادقة لمستخدم مصادقة الويب، تأكد من استخدام **RADIUS** للمصادقة وعدم استخدام الآخرين.

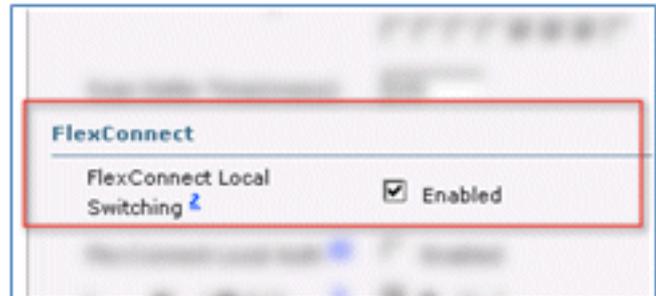


5. انتقل إلى علامة التبويب **خيارات متقدمة**، وقم بضبط السمات التالية:

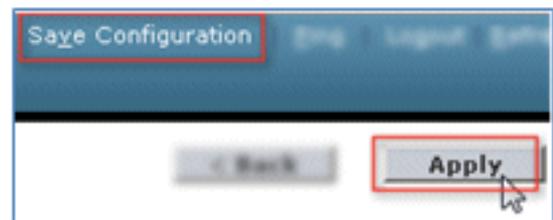
السماح بتجاوز AAA: **ممكناً** **NAC: RADIUS NAC**



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



7. طققة يطبق ويحفظ تشكيل.



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

WLANs > Edit 'Demo1x'

General Security QoS Advanced

Profile Name Demo1x  
 Type WLAN  
 SSID Demo1x  
 Status  Enabled

Security Policies [WPA2][Auth(802.1X)]  
 (Modifications done under secu

Radio Policy All  
 Interface/Interface Group(G) management  
 Multicast Vlan Feature  Enabled  
 Broadcast SSID  Enabled

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: 802.1X: تمكين

WLANs > Edit 'Demo1x'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security WPA+WPA2  
 MAC Filtering

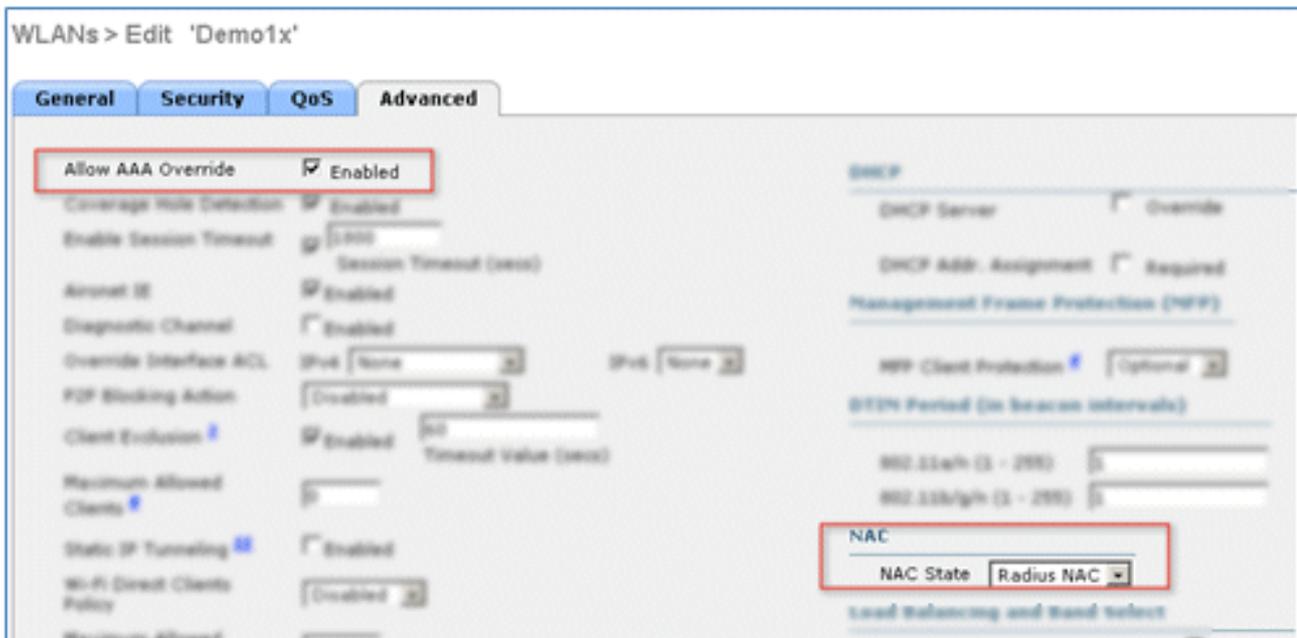
Fast Transition  
 Fast Transition   
 Over the DS   
 Reassociation Timeout 20

WPA+WPA2 Parameters  
 WPA Policy   
 WPA2 Policy   
 WPA2 Encryption  AES  TKIP

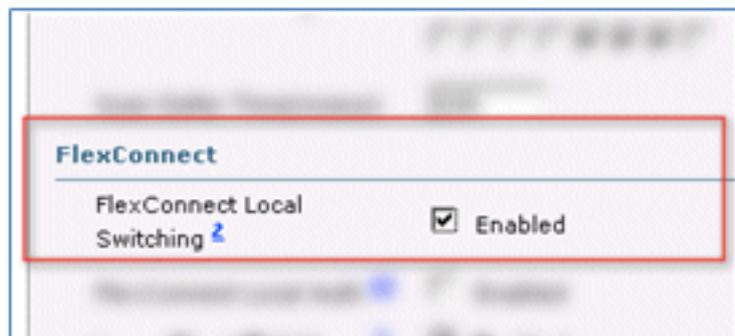
Authentication Key Management  
 802.1X  Enable  
 CCKM  Enable  
 PSK  Enable

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

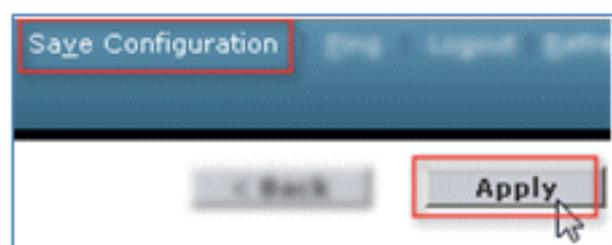
السماح بتجاوز AAA: ممكنة NAC: RADIUS NAC



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



12. قطعة يطبق ويحفظ تشكيل.



13. تأكد من إنشاء كل من شبكات WLAN الجديدة.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	BLX	BLX	Disabled	[WPA2][Auth(802.1X)]
2	WLAN	Demo1x	Demo1x	Enabled	[WPA2][Auth(802.1X)]
4	WLAN	DemoCWA	DemoCWA	Enabled	MAC Filtering
5	WLAN	Flex	Flex	Disabled	Web-Auth

## 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 الهدف.

AP Name	AP Model
<a href="#">Site-B-FlexAP</a>	AIR-LAP1262N-A-K

2. انقر فوق علامة التبويب FlexConnect.

General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
---------	-------------	------------	-------------------	-----------	-------------	----------

3. مكنت دعم VLAN (صندوق يكون محددًا)، ثبت ال VLAN id أهلي طبيعي، وطبقة VLAN يخطط.

VLAN Support

Native VLAN ID  **VLAN Mappings**

FlexConnect Group Name Not Configured

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

MONITOR WLANs CONTROLLER WIRELESS SECURITY M...

All APs > Site-B-FlexAP > VLAN Mappings

AP Name Site-B-FlexAP

Base Radio MAC e8:04:62:0a:68:80

WLAN Id	SSID	VLAN ID
3	Demo1x	21
4	DemoCWA	21

5. طقطقة يطبق ويحفظ تشكيل.

## تكوين ISE

أتمت هذا steps in order to شكلت ال ISE:

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

Identity Services Engine

Username

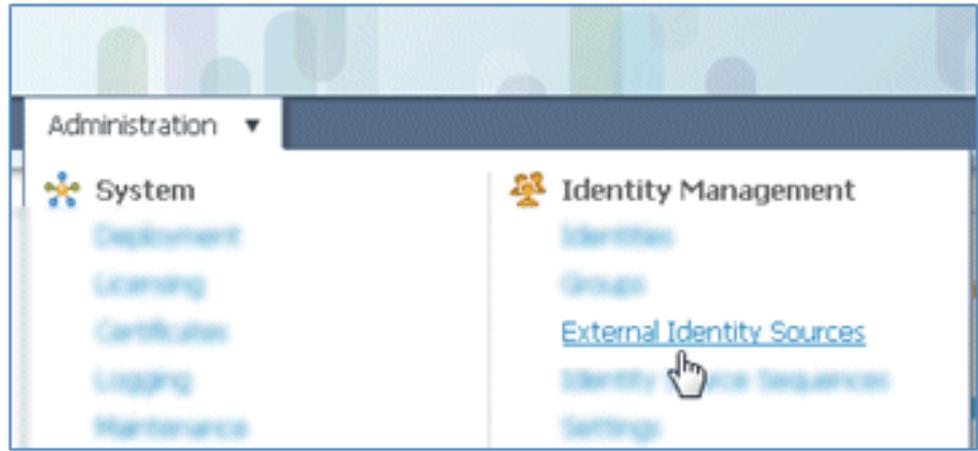
Password

Remember username

[Problem logging in?](#)

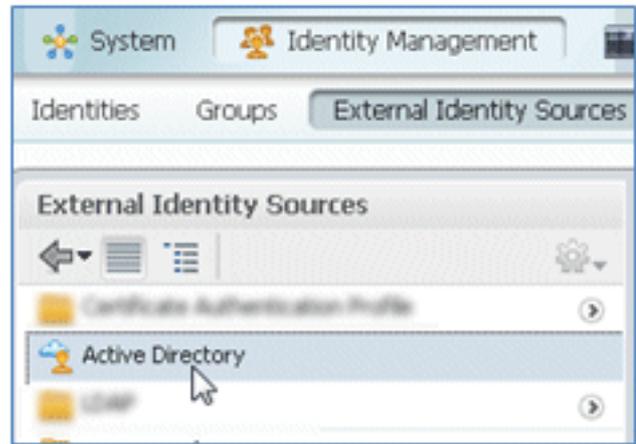
© 2012 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. CISCO

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



انقر فوق **Active Directory**.

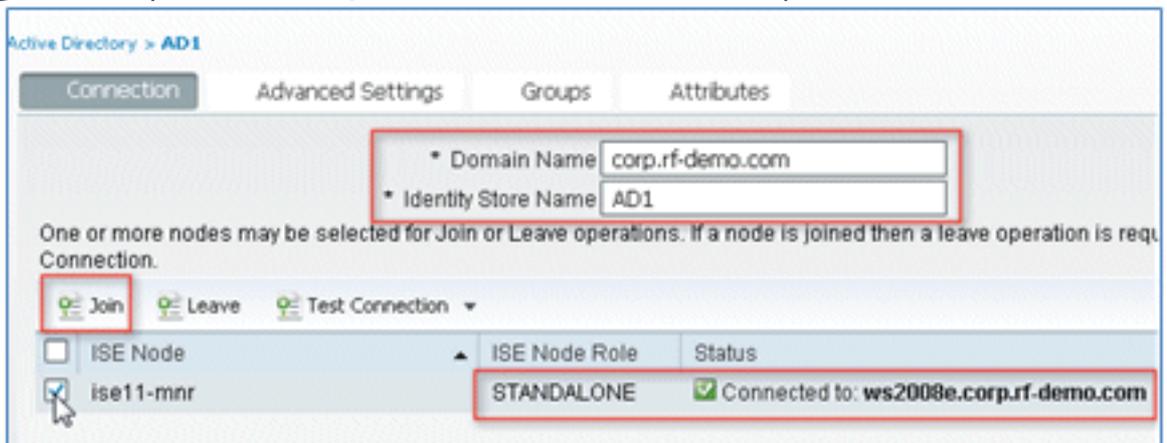
.3



في علامة تبويب التوصليل:

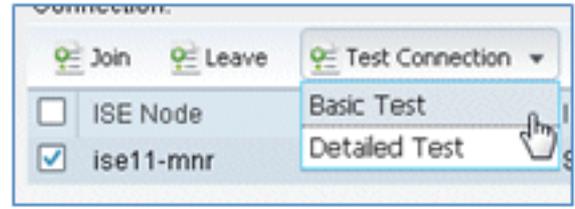
.4

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).

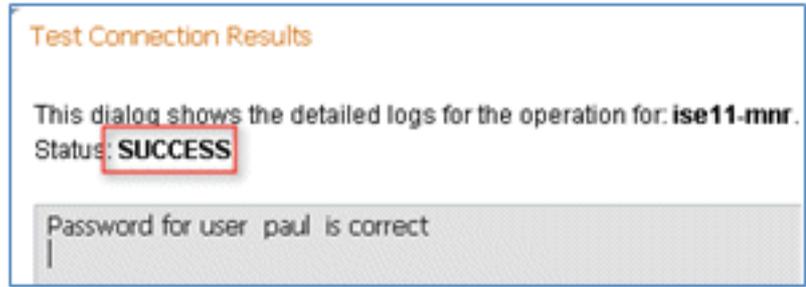


.5

قم بإجراء اختبار اتصال أساسي ب AD مع مستخدم المجال الحالي.

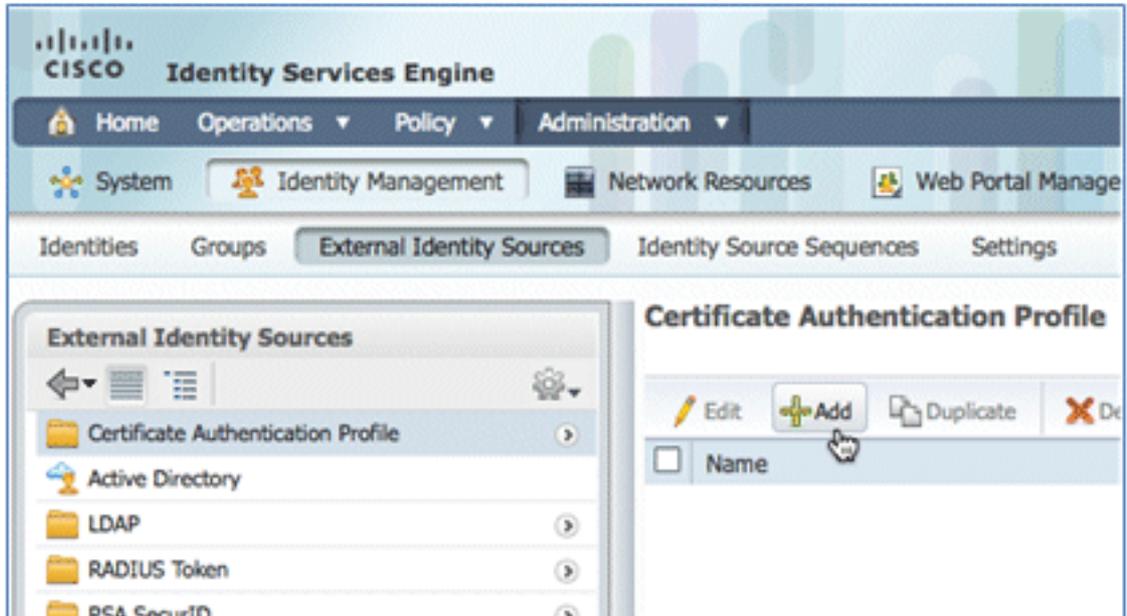


6. إذا نجح التوصل ب AD، سيؤكد حوار أن كلمة المرور صحيحة.



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).



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

Certificate Authentication Profiles List > New Certificate Authentication Profile

### Certificate Authentication Profile

\* Name

Description

Principal Username X509 Attribute

Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

LDAP/AD Instance Name

تأكد من إضافة CAP الجديد.

.9

CISCO Identity Services Engine

Home Operations Policy Administration

System Identity Management Network Resources Web Portal Management

Identities Groups External Identity Sources Identity Source Sequences Settings

### External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

### Certificate Authentication Profile

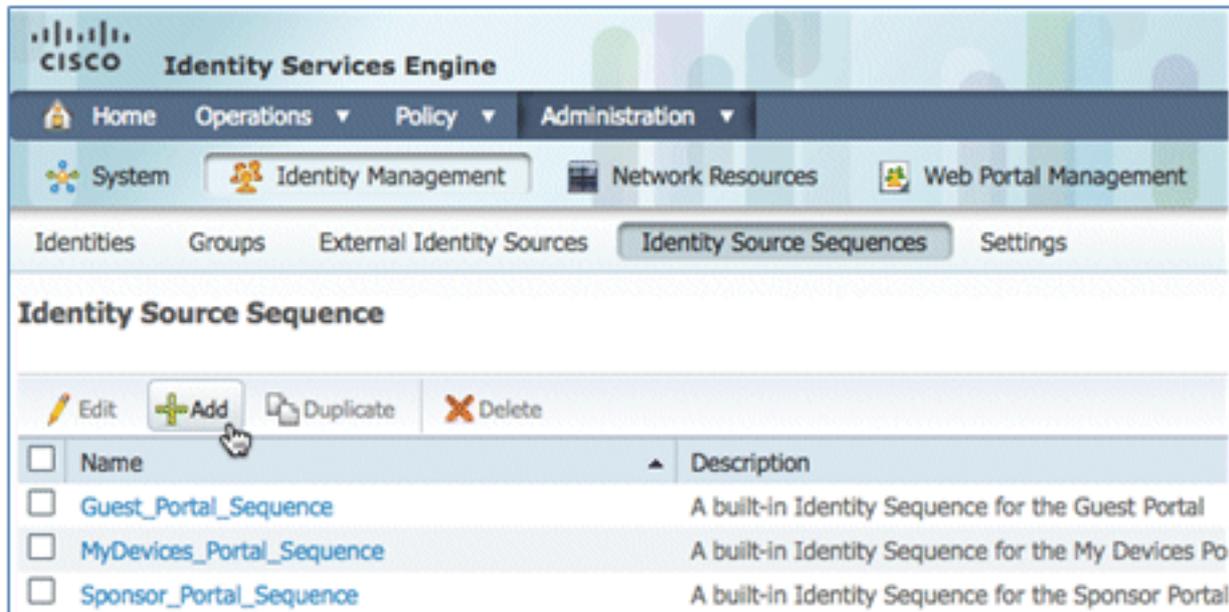
Edit Add Duplicate Delete

Name

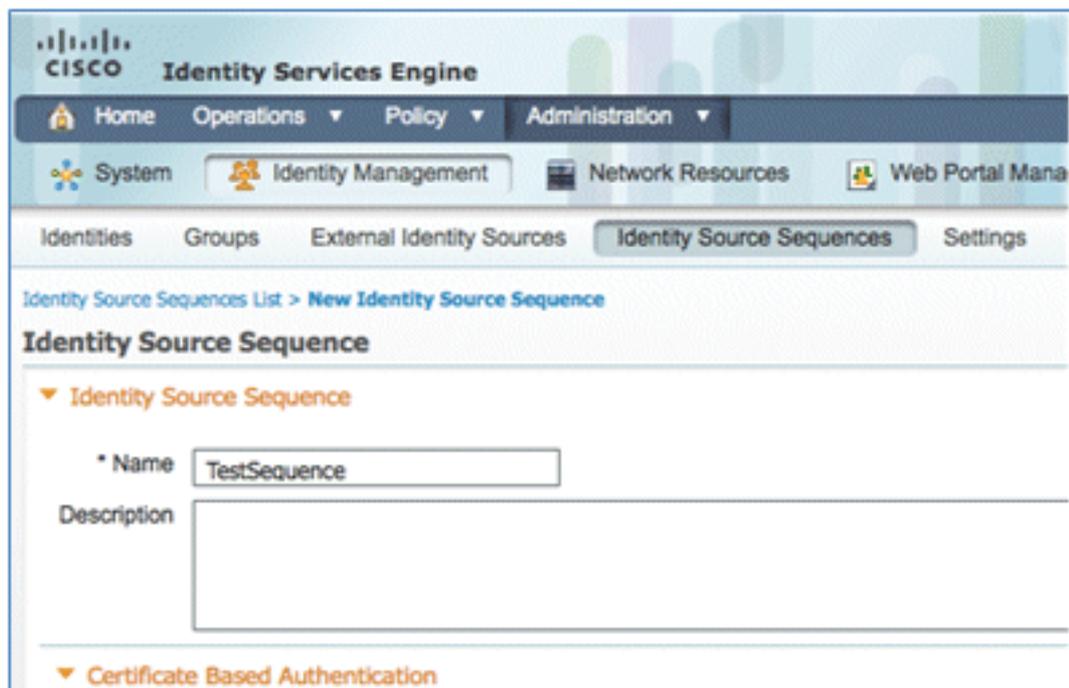
CertAuth

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

.10

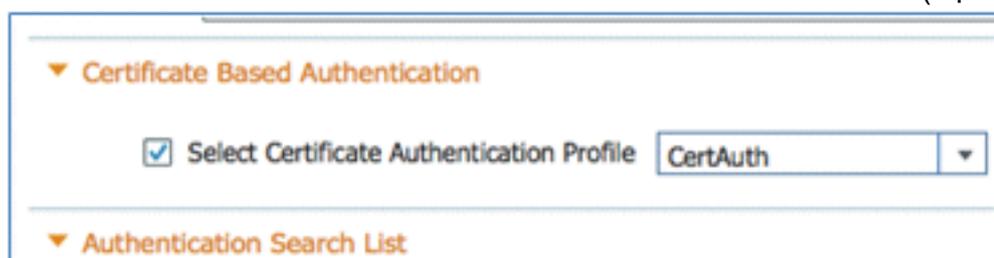


11. إعطاء التسلسل اسم TestSequence (في هذا المثال).



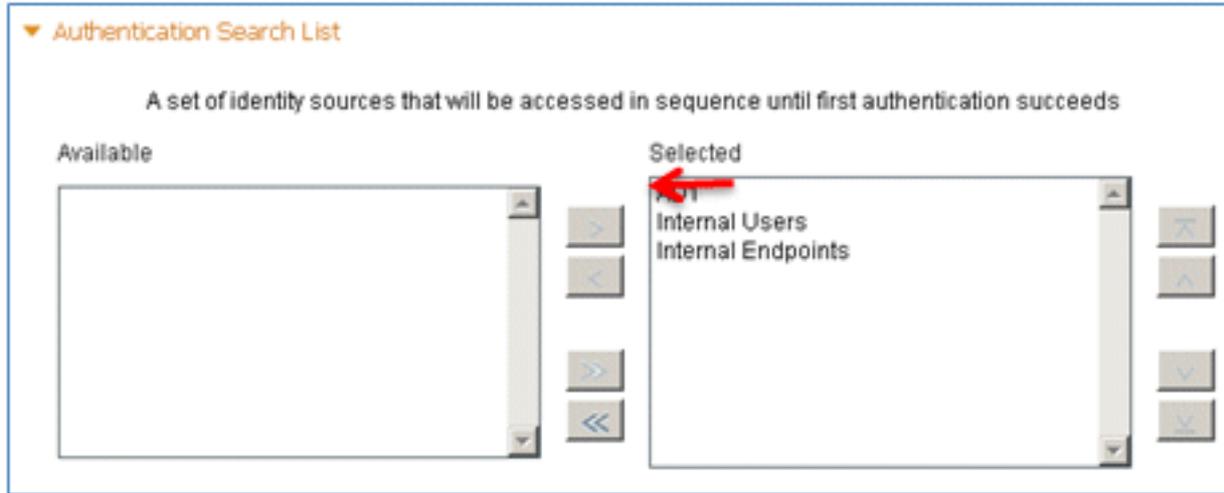
12. قم بالتمرير لأسفل إلى المصادقة المستندة إلى الشهادة:

يمكن تحديد توصيف مصادقة الشهادة (خانة الاختيار). حدد CertAuth (أو ملف تعريف CAP آخر تم إنشاؤه مسبقاً).



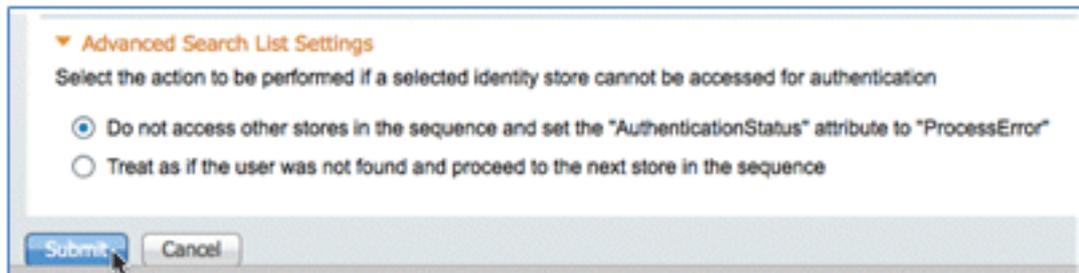
13. قم بالتمرير إلى قائمة البحث عن المصادقة:

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



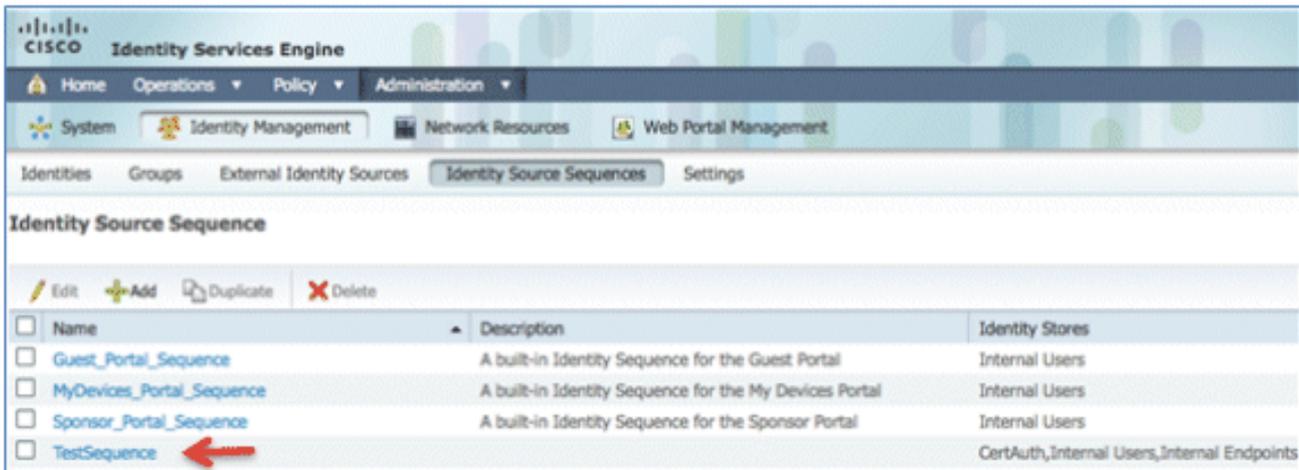
.14

طقطقة يسلم in order to أنفذت.

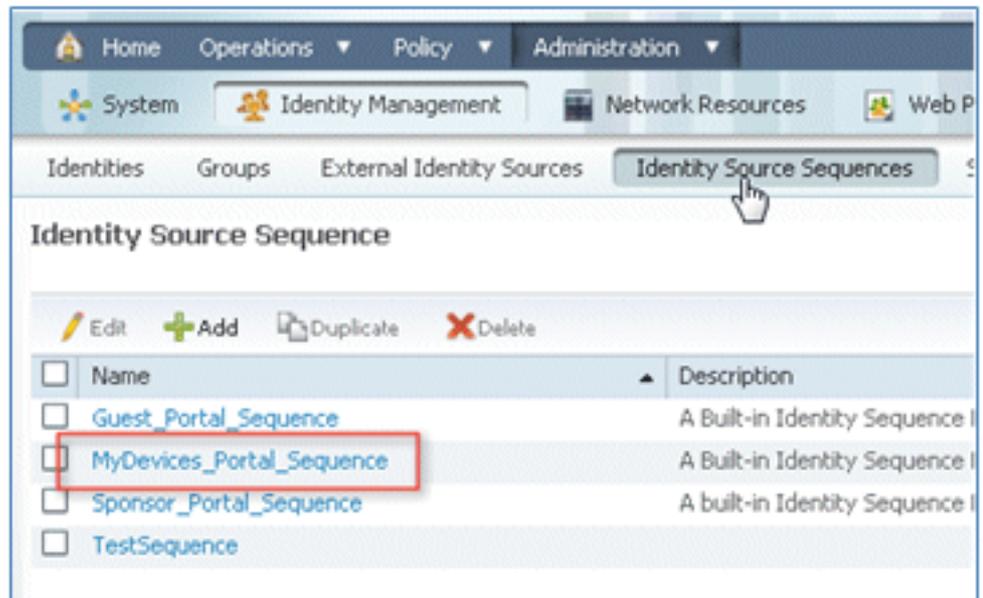


.15

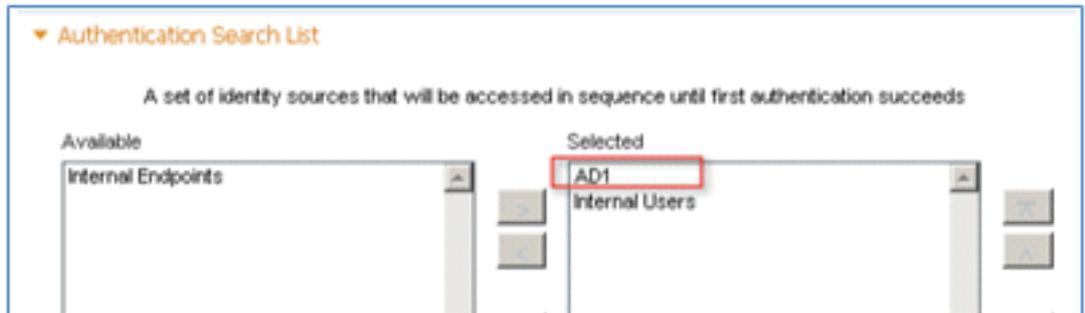
تأكد من إضافة تسلسل مصدر الهوية الجديد.



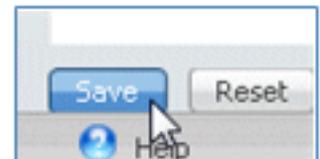
.16 استخدم الإعلان لمصادقة بوابة الأجهزة الخاصة بي. انتقل إلى ISE < الإدارة < إدارة الهوية < Identity Source Sequence، وقم بتحرير MyDevices\_Portal\_Sequence.



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



18. طغطة 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.

Name	Description	Identity Stores
Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users,AD1

in order to أضفت ال WLC إلى شبكة منفذ أداة (WLC)، انتقل إلى إدارة <شبكة مورد> شبكة أداة، وطفظة يضيف.



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

Network Devices List > New Network Device

### Network Devices

\* Name

Description

---

\* IP Address:  /

---

Model Name

Software Version

---

\* Network Device Group

Location

Device Type

قم بالتمرير لأسفل إلى إعدادات المصادقة، وأدخل "السر المشترك". يجب أن يطابق هذا السر المشترك مر4. ال WLC RADIUS.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

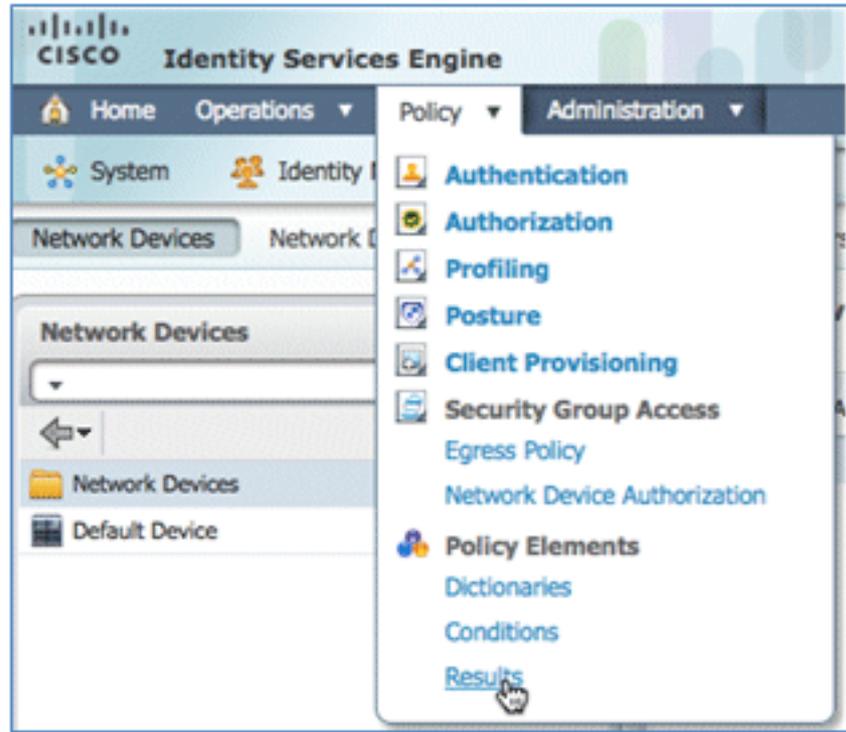
Key Input Format  ASCII  HEXADECIMAL

SNMP Settings

SGA Attributes

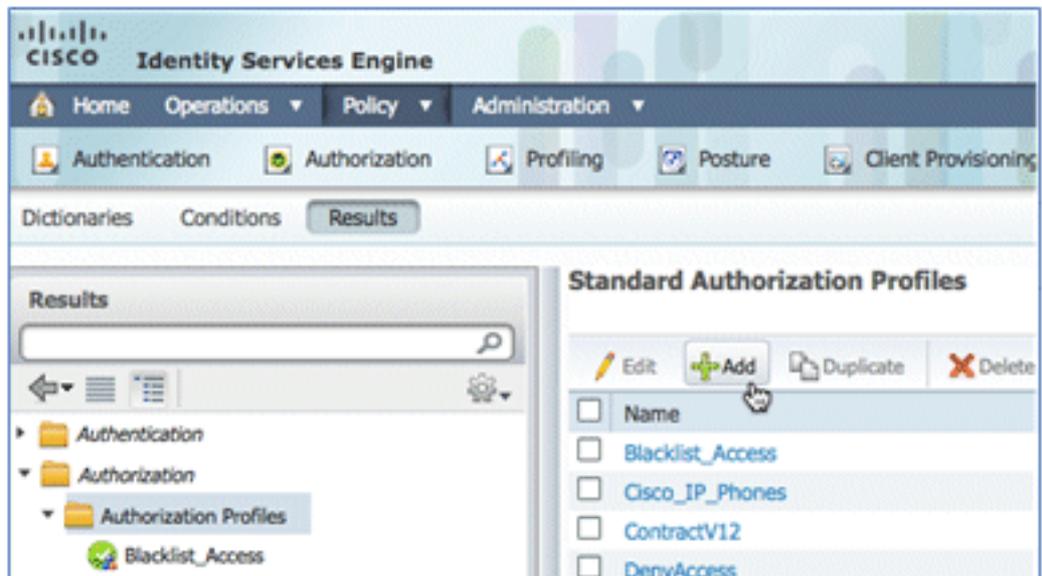
.25 انقر على إرسال.

.26 انتقل إلى ISE < السياسة < عناصر السياسة < النتائج.



.27

قم بتوسيع النتائج والتفويض، وانقر توصيفات التفويض، وانقر إضافة لتوصيف جديد.



28. امنح ملف التخصيص هذا القيم:

الاسم: CWA

Authorization Profiles > New Authorization Profile

**Authorization Profile**

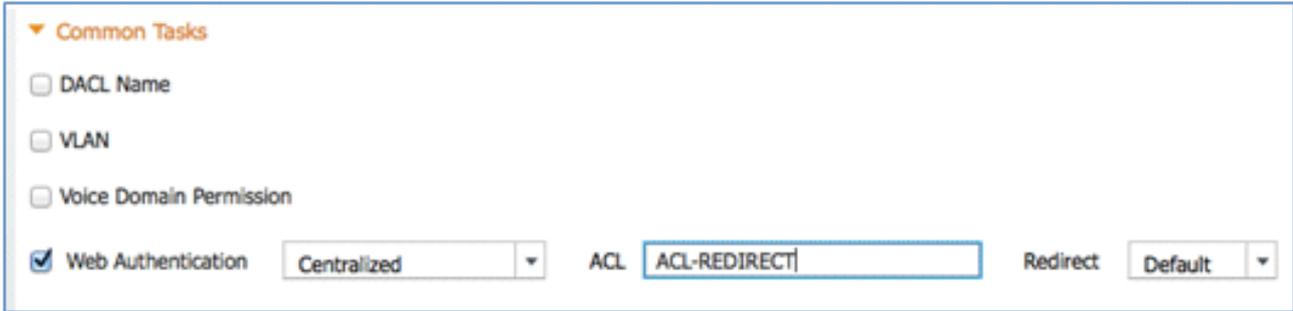
\* Name

Description

\* Access Type

تمكين مصادقة الويب (تم تحديد المربع):

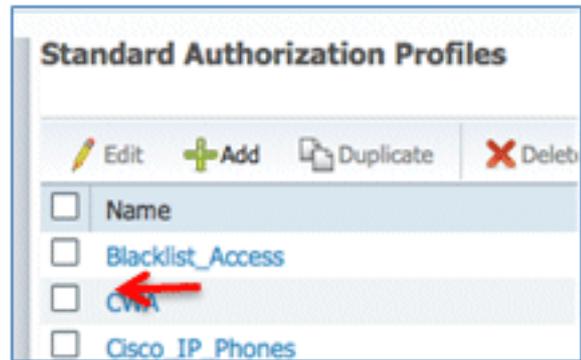
مصادقة الويب: مركز قائمة التحكم في الوصول (ACL-Redirect): ACL (يجب أن يتطابق هذا مع اسم قائمة التحكم في الوصول (ACL) للمصادقة المسبقة لـ WLC). إعادة التوجيه: الافتراضي



Common Tasks

- DACL Name
- VLAN
- Voice Domain Permission
- Web Authentication  ACL  Redirect

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

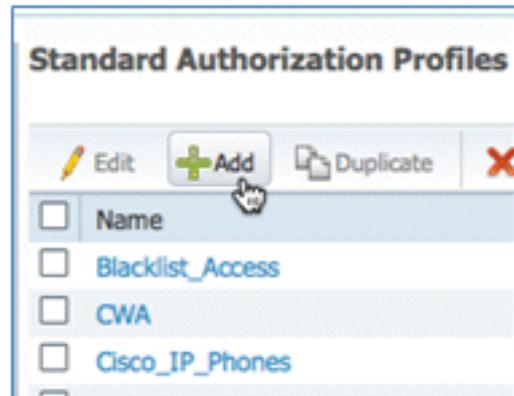


Standard Authorization Profiles

Edit Add Duplicate Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	Blacklist_Access
<input checked="" type="checkbox"/>	CWA
<input type="checkbox"/>	Cisco_IP_Phones

30. انقر على إضافة لإنشاء ملف تعريف تخويل جديد.



Standard Authorization Profiles

Edit Add Duplicate Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	Blacklist_Access
<input type="checkbox"/>	CWA
<input type="checkbox"/>	Cisco_IP_Phones

31. امنح ملف التخصيص هذا القيم:

الاسم: الاعتماد

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name

Description

\* Access Type

تمكين مصادقة الويب (تم تحديد المربع):

قيمة مصادقة الويب: توفير الطالب

Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication  ACL

Auto Smart Port

Filter-ID

Centralized  
Device Registration  
Posture Discovery  
Supplicant Provisioning

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

Common Tasks

DACL Name

VLAN

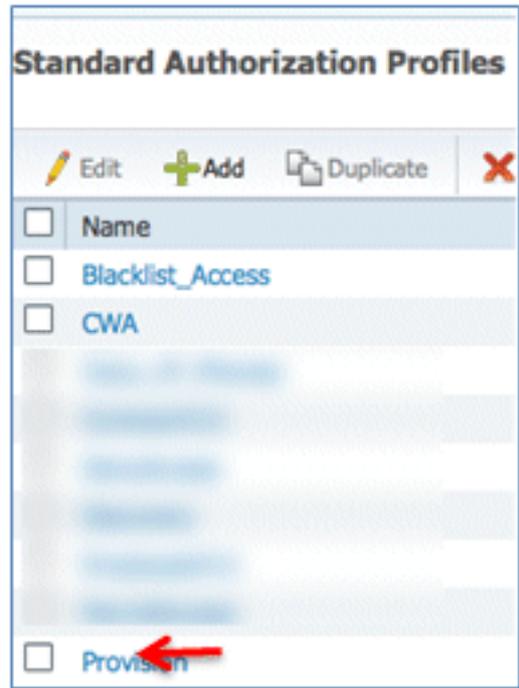
Voice Domain Permission

Web Authentication  ACL

Auto Smart Port

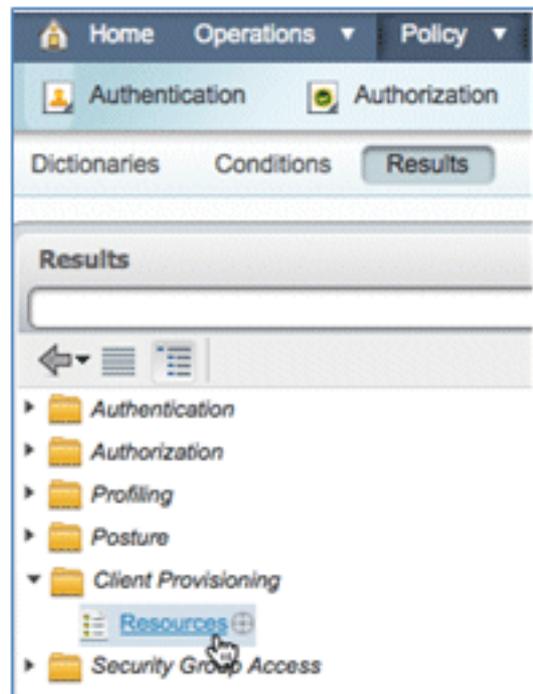
.32

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



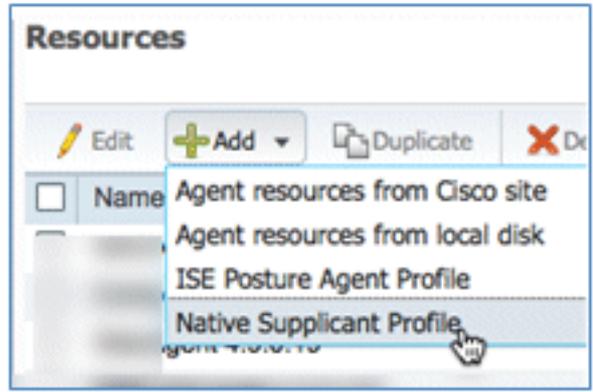
.33

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 التوضيحي 1x (هذه القيمة من تكوين شبكة WLC 802.1x  
WLAN) البروتوكول المسموح به: TLS حجم المفتاح: 1024

37. انقر على إرسال.

38. طقطقة حفظ.

\* Allowed Protocol

\* Key Size

.39

تأكد من إضافة ملف التعريف الجديد.

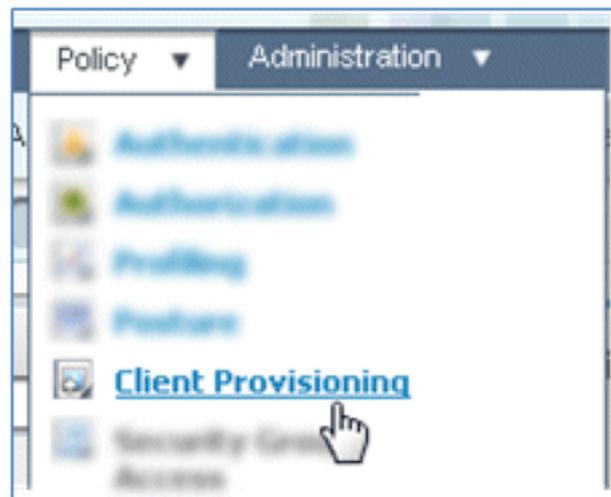
**Resources**

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	WirelessS...	NativeSPProfile

.40

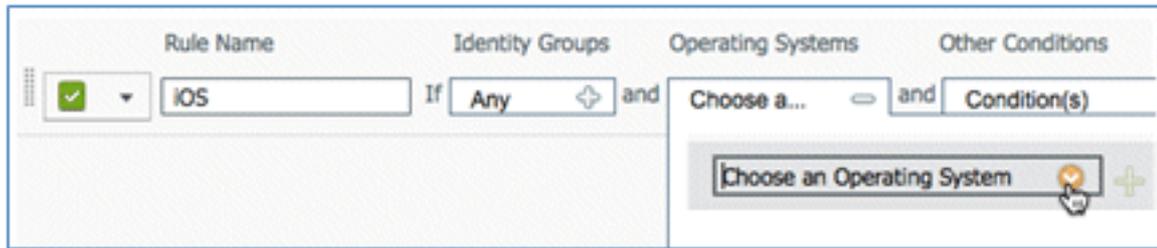
انتقل إلى السياسة > إمداد العميل.



.41

أدخل هذه القيم لقاعدة توفير أجهزة iOS:

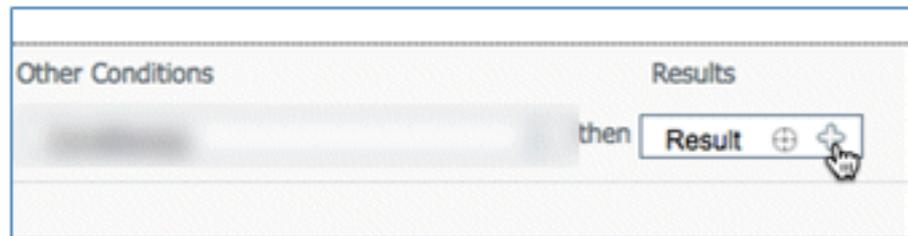
اسم القاعدة: iOSمجموعات الهوية: أي



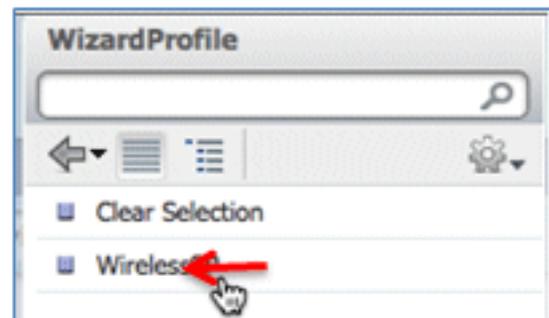
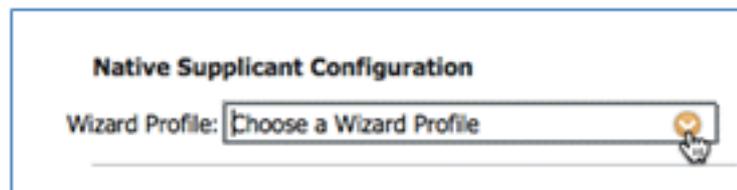
أنظمة التشغيل: نظام التشغيل Mac iOS All

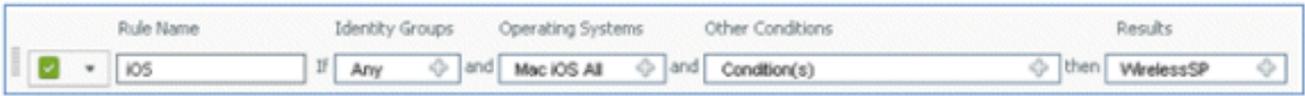


النتائج: WirelessSP (هذا هو ملف تعريف الطالب الأصلي الذي تم إنشاؤه سابقاً)



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





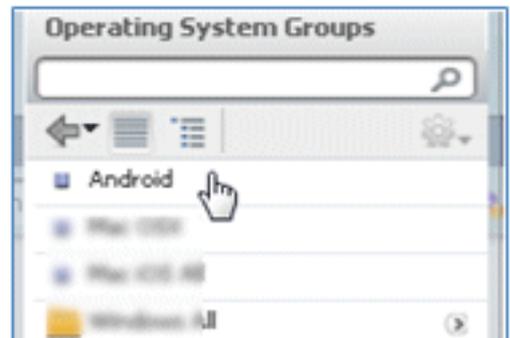
43. على الجانب الأيمن من القاعدة الأولى، حدد قائمة الإجراءات المنسدة، وحدد تكرار أدناه (أو أعلى).



44. قم بتغيير اسم القاعدة الجديدة إلى Android.

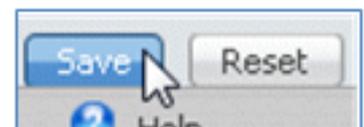


45. قم بتغيير أنظمة التشغيل إلى Android.

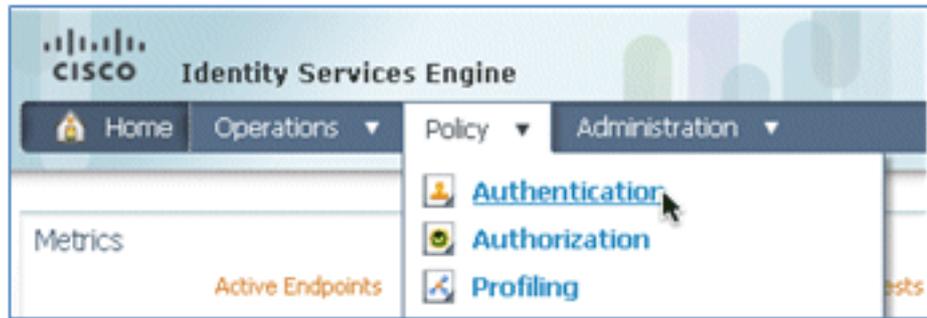


46. أترك القيم الأخرى بدون تغيير.

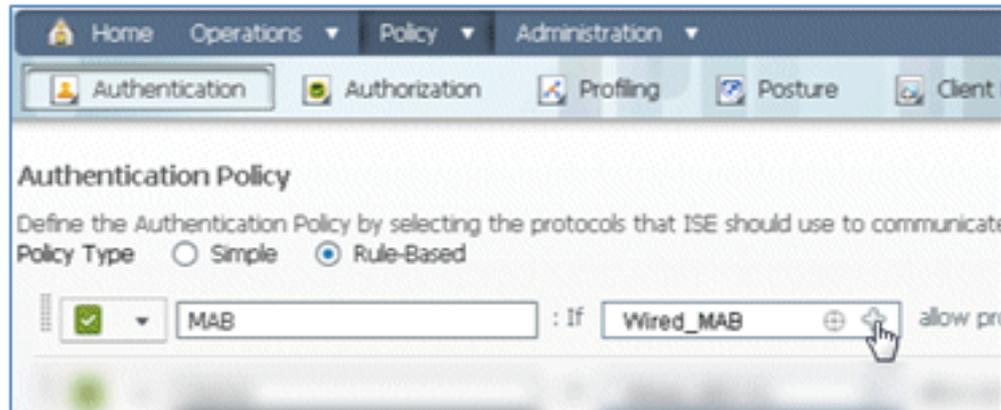
47. انقر فوق حفظ (الشاشة اليسرى السفلى).



48. انتقل إلى ISE < السياسة < المصادقة.



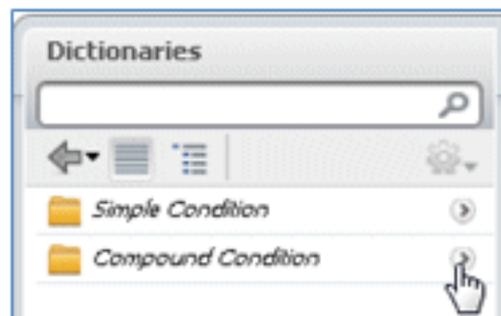
49. قم بتعديل الشرط ليضم wireless\_mab، ثم قم بتوسيع wired\_mab.



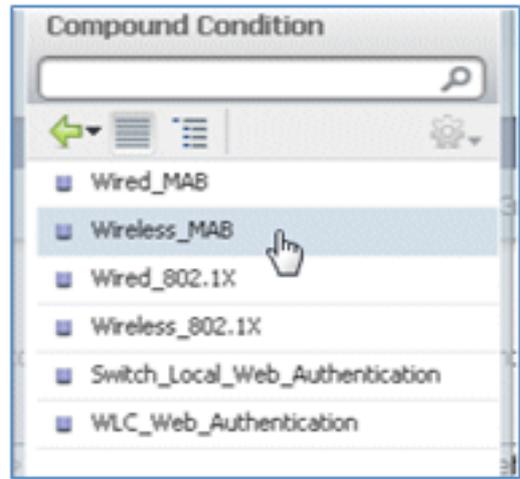
50. انقر فوق القائمة المنسدلة اسم الشرط.



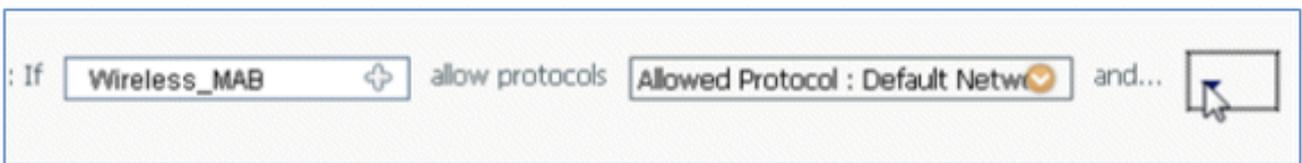
51. حدد القواميس < شرط مركب.



52. حدد Wireless\_MAB.

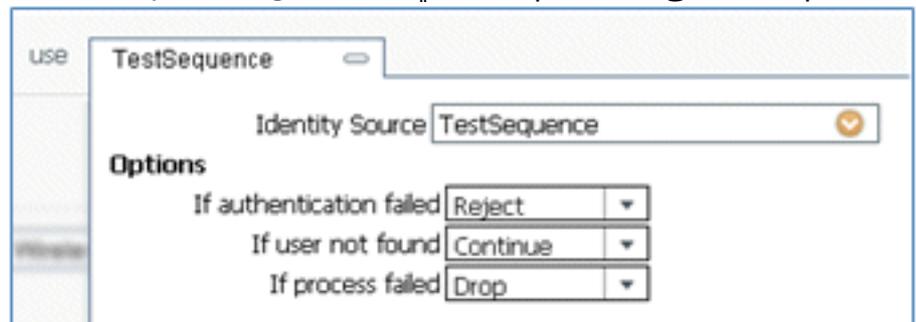


.53 إلى يمين القاعدة، حدد السهم للتوسيع.

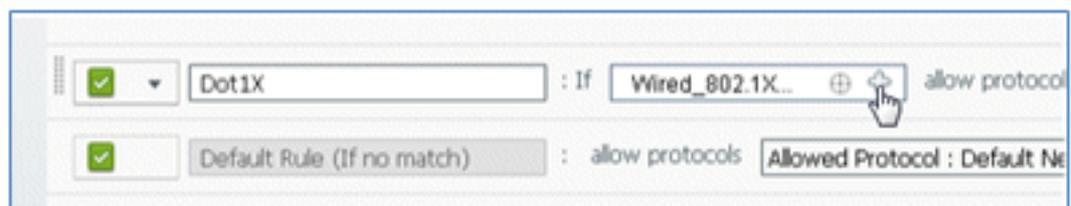


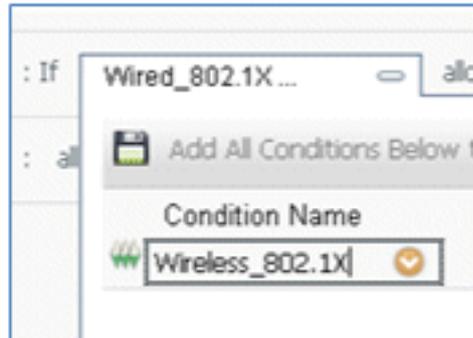
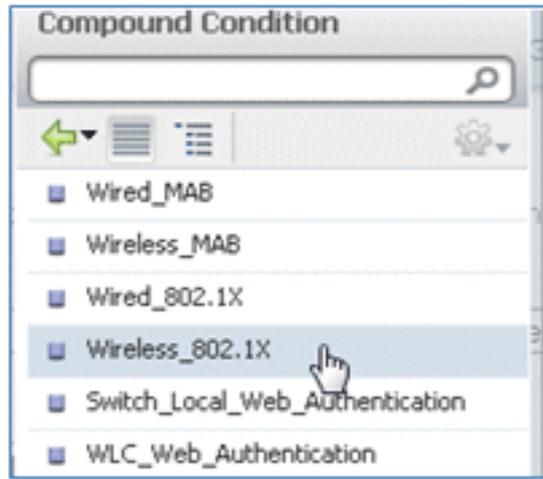
.54 حدد هذه القيم من القائمة المنسدلة:

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



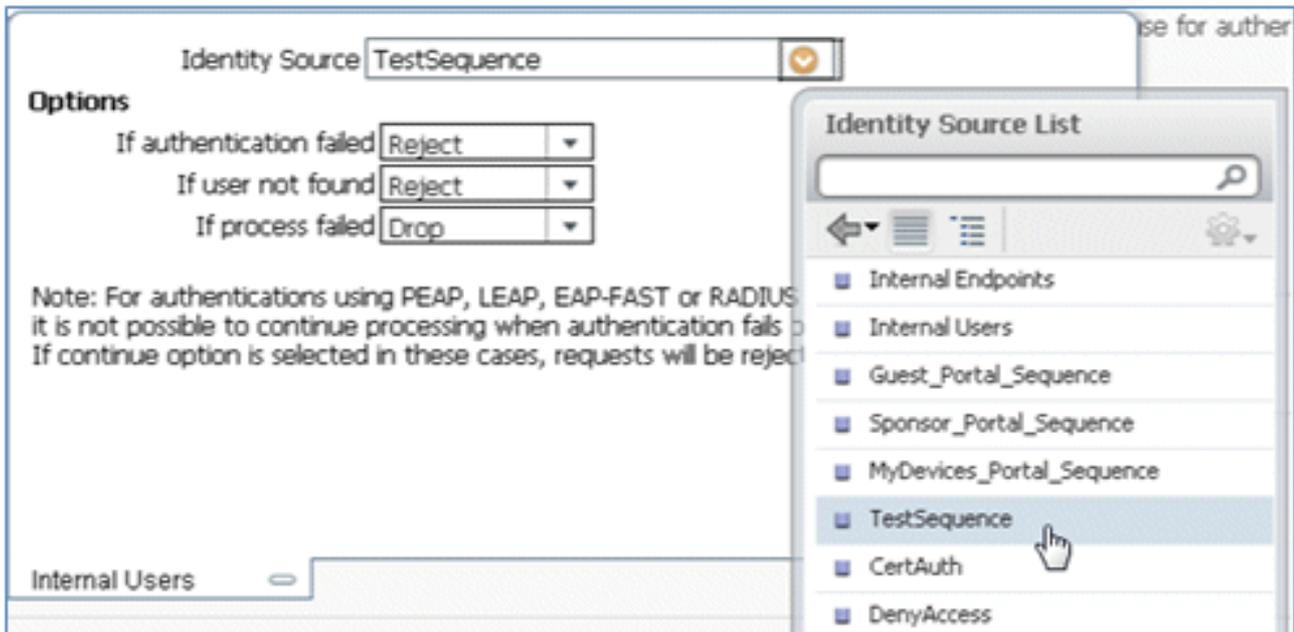
.55 انتقل إلى قاعدة dot1x، وقم بتغيير هذه القيم:





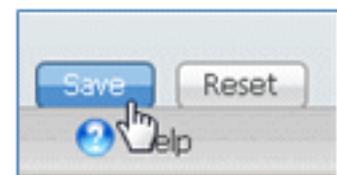
الشرط: Wireless\_802.1X

مصدر الهوية: TestSequence

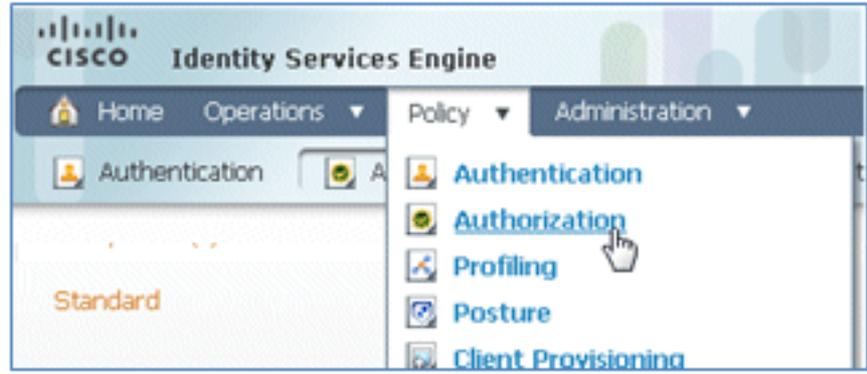


.56

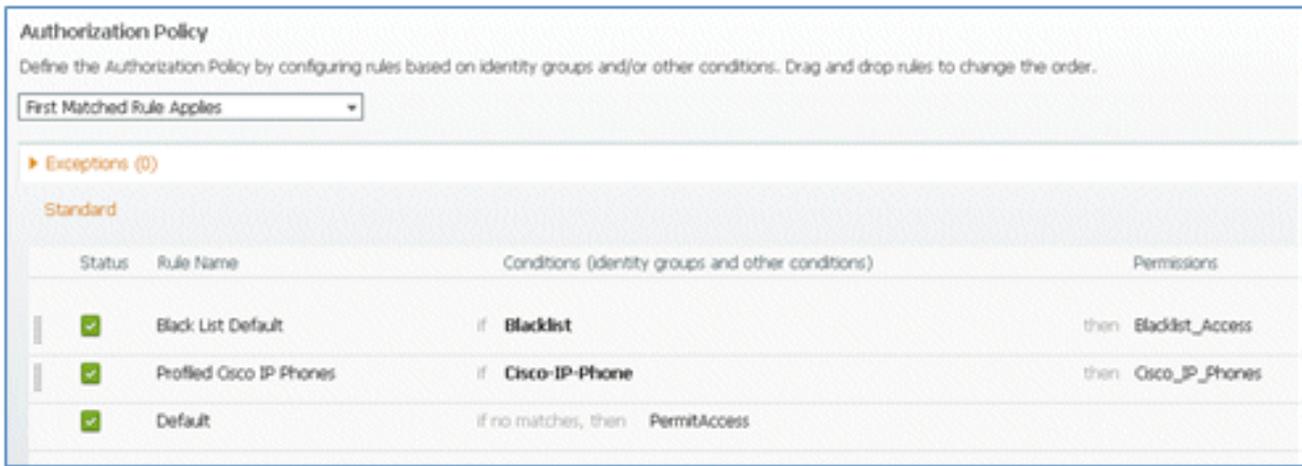
طقطقة حفظ.



.57. انتقل إلى ISE < السياسة > التفويض.



تم تكوين القواعد الافتراضية (مثل Black List Default و Profiled و Default) بالفعل من التثبيت، ويمكن 58. تجاهل القواعد الأولى والثانية، وسيتم تحرير القاعدة الافتراضية لاحقاً.



على يمين القاعدة الثانية (إصدارات هواتف Cisco IP)، انقر فوق السهم لأسفل الموجود بجوار التحرير، و59 إدراج قاعدة جديدة أدناه.

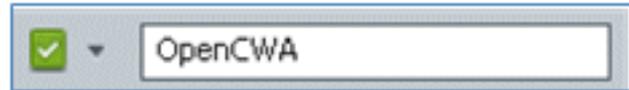


تمت إضافة قاعدة قياسية جديدة #.

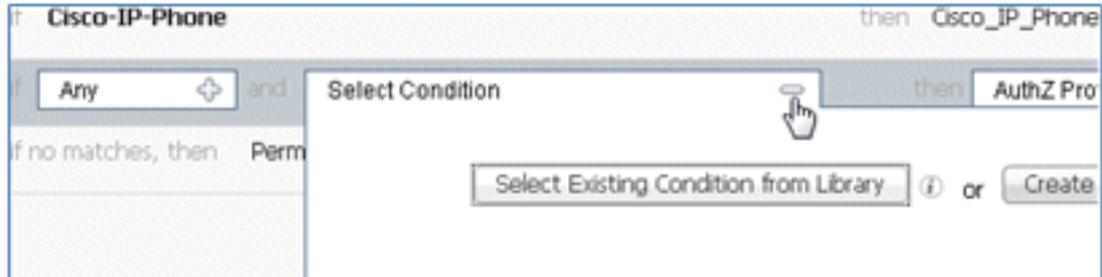


60. قم بتغيير اسم القاعدة من القاعدة القياسية # إلى OpenCWA. تهيئ هذه القاعدة عملية التسجيل على

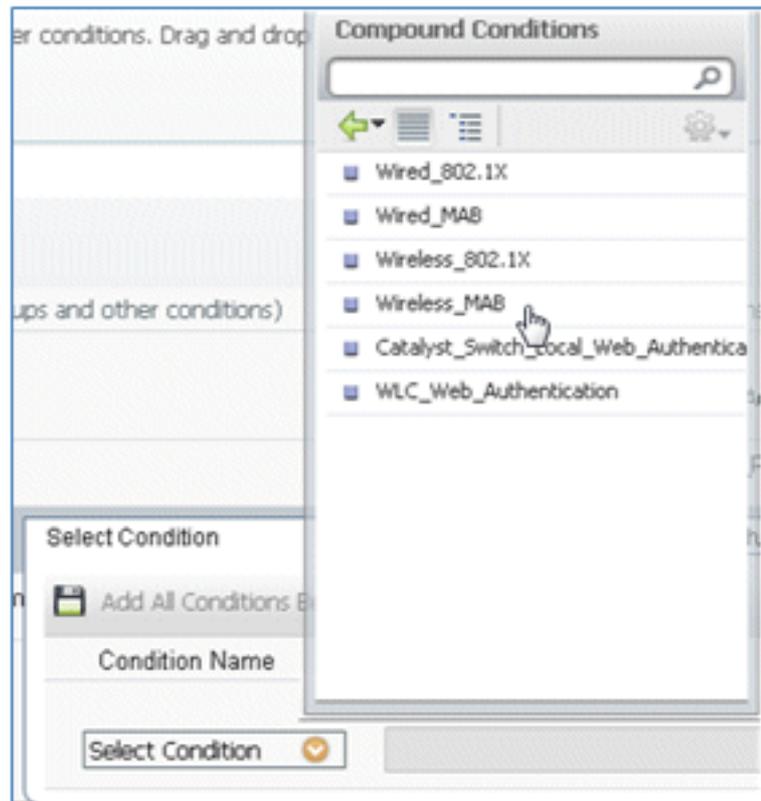
شبكة WLAN المفتوحة (SSID المزدوج) للمستخدمين الذين يأتون إلى شبكة الضيوف من أجل توفير الأجهزة.



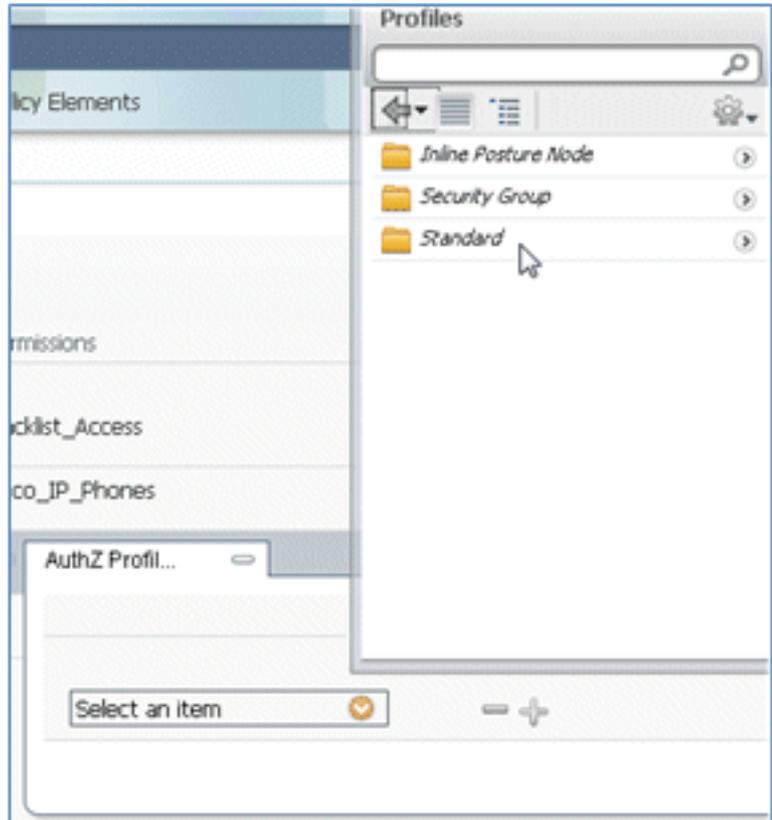
61. انقر علامة الزائد (+) للشرط (الشروط)، وانقر تحديد الشرط الموجود من المكتبة.



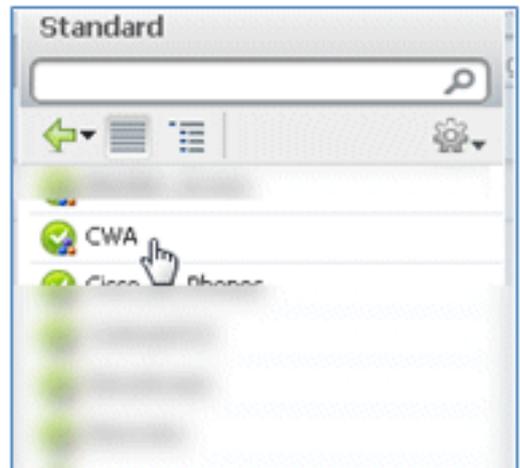
62. حدد شروط مركبة < Wireless\_MAB.



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



64. حدد CWA القياسي (هذا هو ملف تعريف التحويل الذي تم إنشاؤه سابقاً).



65. تأكد من إضافة القاعدة بالشروط والتفويض الصحيحين.



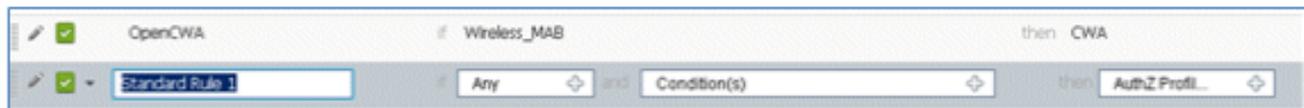
66. انقر فوق تم (في الجانب الأيمن من القاعدة).



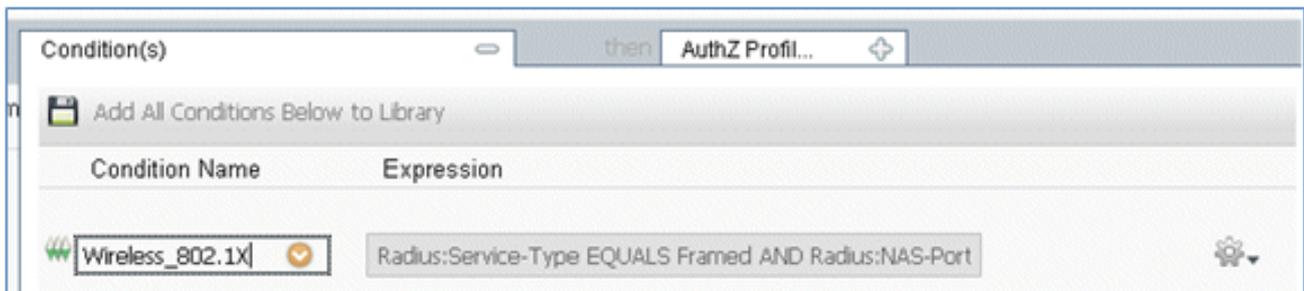
67. على يمين نفس القاعدة، انقر فوق السهم لأسفل المجاور للتحريك، وحدد إدراج قاعدة جديدة أدناه.



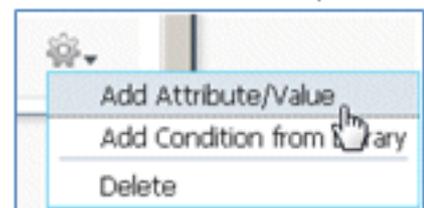
68. قم بتغيير اسم القاعدة من القاعدة القياسية # إلى قاعدة PEAPrule (في هذا المثال). هذه القاعدة خاصة ب PEAP (يستخدم أيضا لسيناريو SSID المفرد) للتحقق من أن مصادقة 802.1X دون تأمين طبقة النقل (TLS) وأن تزويد ملتزم الشبكة يتم بدؤه مع ملف تعريف تحويل التوفير الذي تم إنشاؤه سابقا.



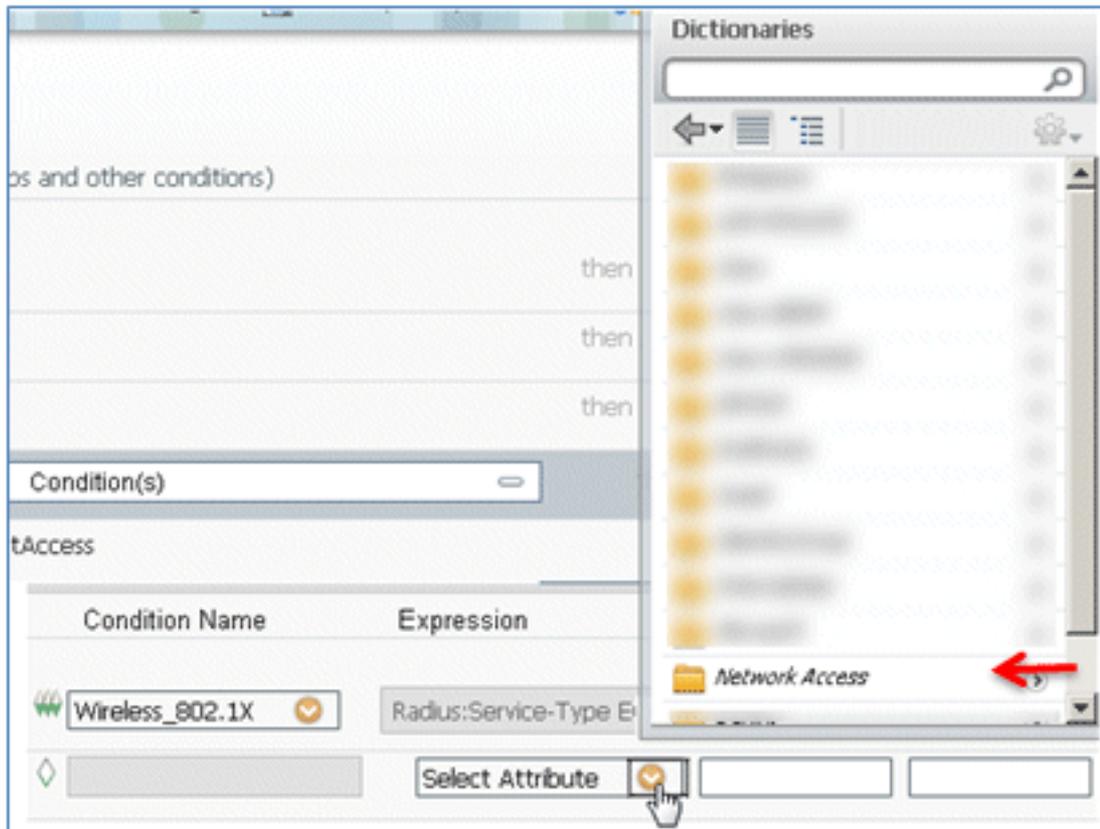
69. قم بتغيير الشرط إلى Wireless\_802.1X.



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

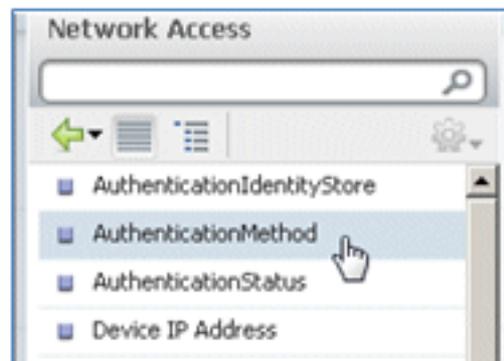


71. حدد موقع الوصول إلى الشبكة وحدده.

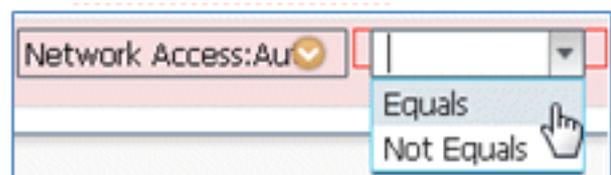


.72

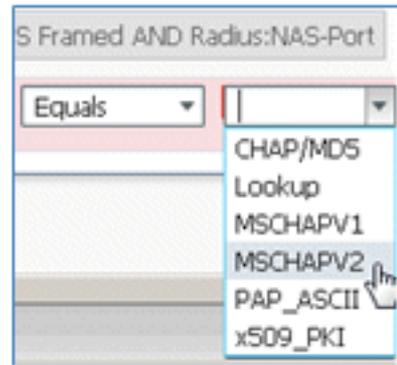
حدد AuthenticationMethod، وأدخل القيم التالية:



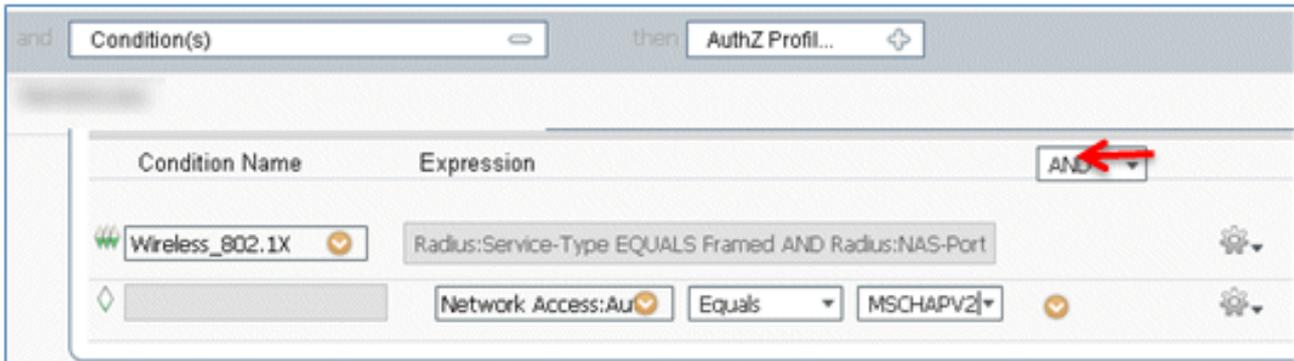
AuthenticationMethod: يساوي



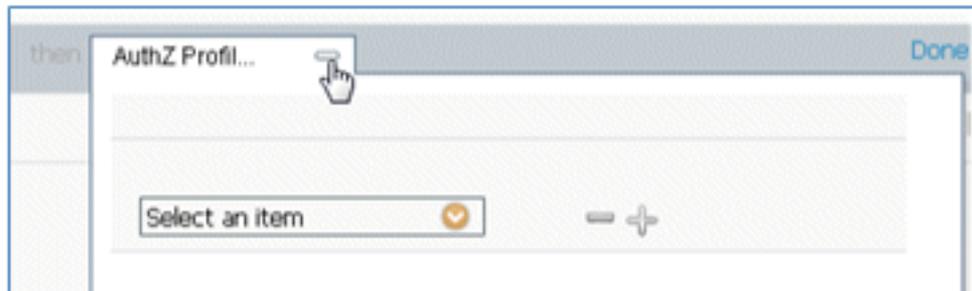
حدد MSCHAPV2.

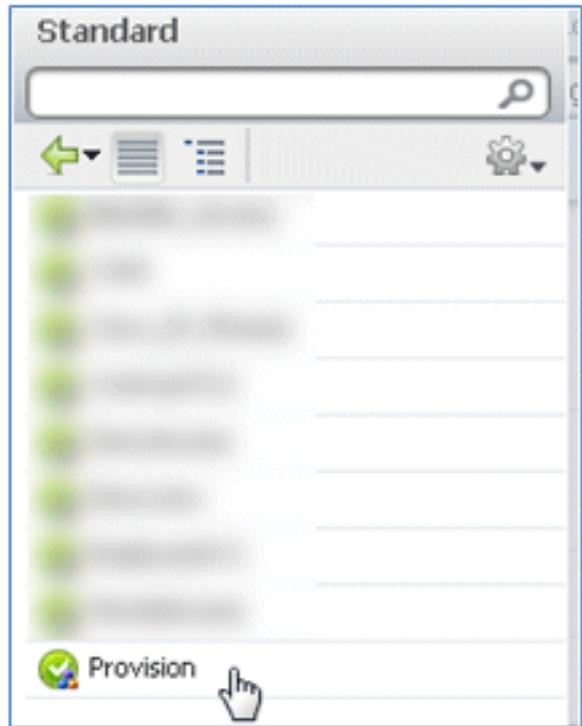


هذا مثال على القاعدة، تأكد من أن الشرط هو و.



في ملف تعريف AuthZ، حدد Standard > Provision (هذا هو ملف تعريف التحويل الذي تم إنشاؤه سابقاً).





.74

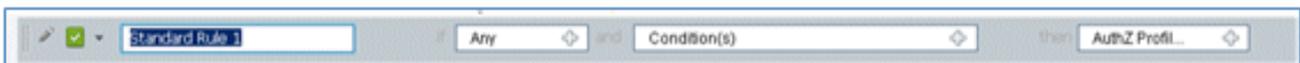
طققة تم.



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



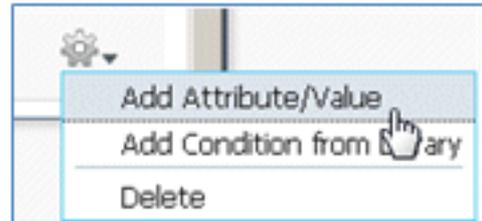
.76 قم بتغيير اسم القاعدة من رقم القاعدة القياسية إلى AllowRule (في هذا المثال). سيتم استخدام هذه القاعدة للسماح بالوصول إلى الأجهزة المسجلة ذات الشهادات المثبتة.



.77

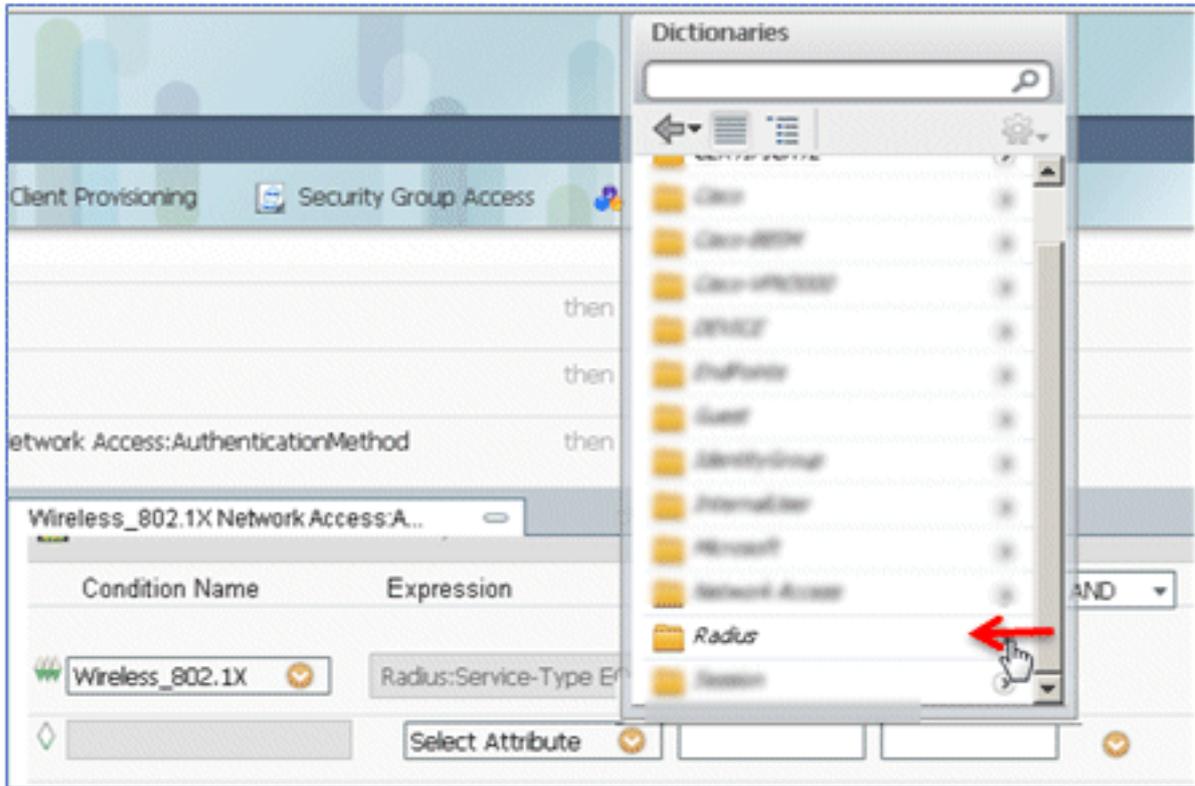
تحت شرط (شروط)، حدد شروط مركبة.





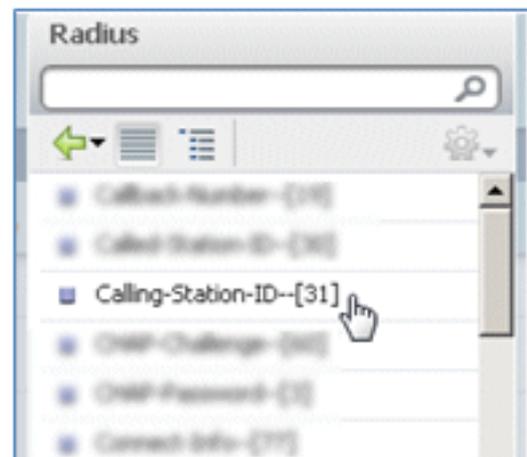
.81

حدد موقع RADIUS وحدده.



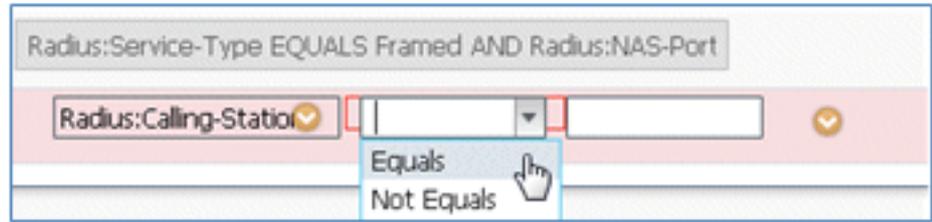
.82

حدد [31]—[Call-Station-ID].



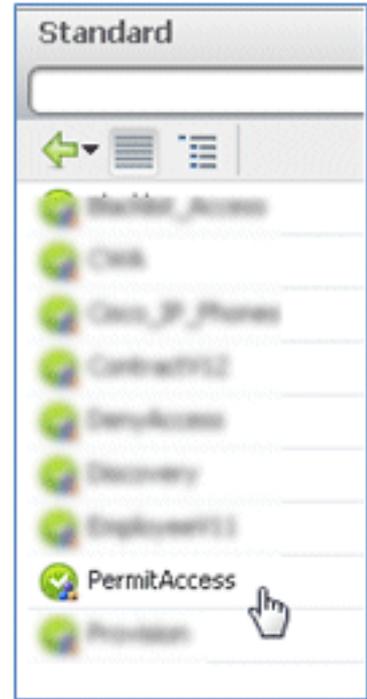
.83

حدد يساوي.



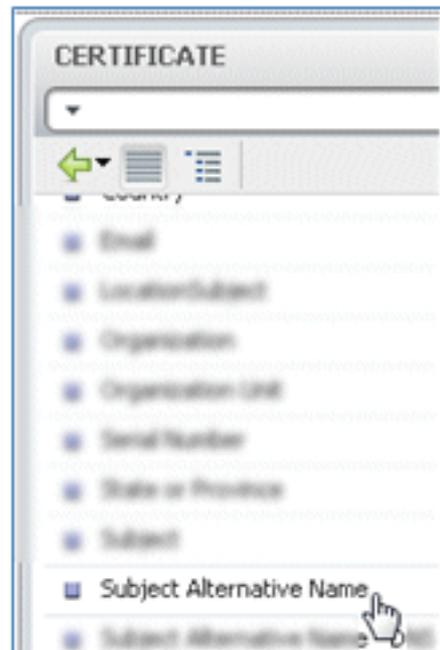
.84

انتقل إلى CERTIFICATE، وانقر فوق السهم الأيمن.



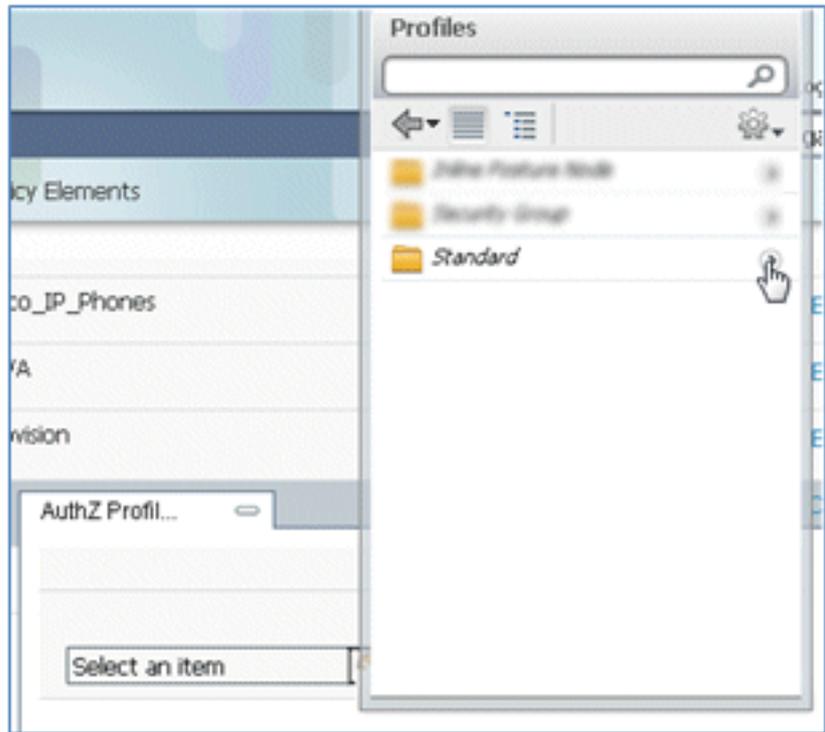
.85

حدد الاسم البديل للموضوع.



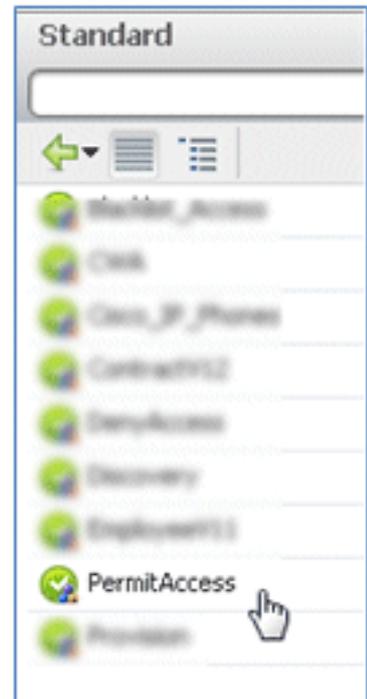
.86

بالنسبة لملف تعريف AuthZ، حدد قياسي.



.87

حدد السماح بالوصول.



.88

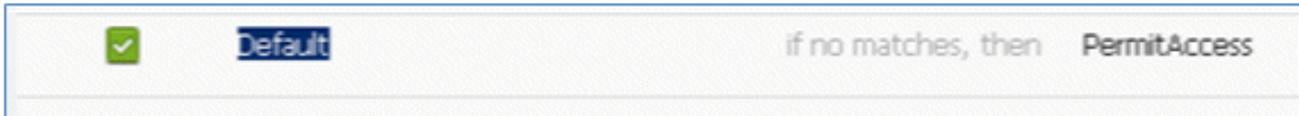
طقطقة تم.



هذا مثال على القاعدة:

OpenCMA	Wireless_MQ2	then: Deny
PEAPRule	Wireless_802.1X (1): Network Access:AuthenticationMethod EQUALS PEAP(2)	then: Permit
AllowRule	Wireless_802.1X Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name	then: PermitAccess

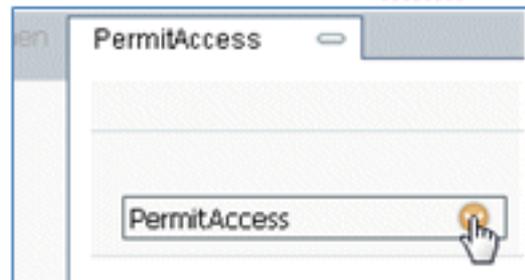
89. حدد موقع القاعدة الافتراضية لتغيير PermitAccess إلى DenyAccess.



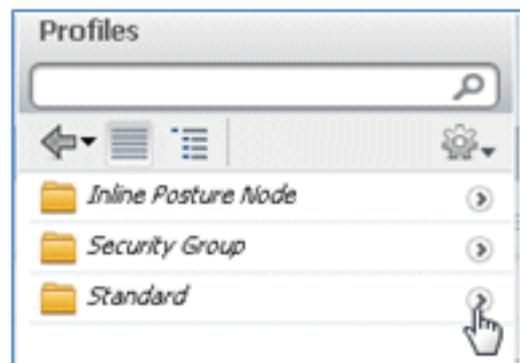
90. انقر فوق تحرير لتحرير القاعدة الافتراضية.



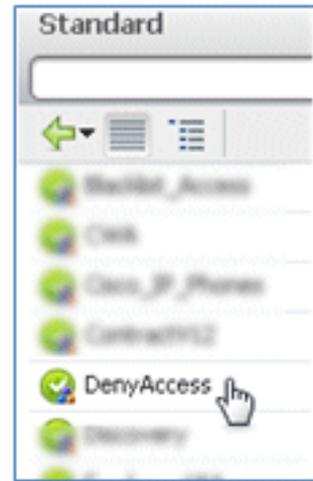
91. انتقل إلى ملف تعريف AuthZ الحالي ل PermittAccess.



92. حدد قياسي.



93. حدد DenyAccess.



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



95. طغطة تم.



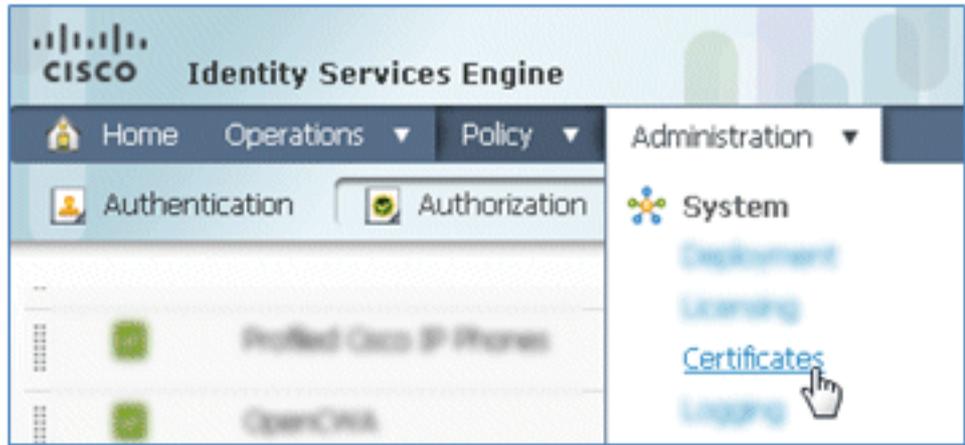
هذا مثال على القواعد الأساسية المطلوبة لهذا الاختبار، وهي تنطبق إما على سيناريو SSID واحد أو سيناريو SSID مزدوج.

<input checked="" type="checkbox"/>	OpenCWA	if Wireless_MAB	then CWA
<input checked="" type="checkbox"/>	PEAPrule	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 )	then Provision
<input checked="" type="checkbox"/>	AllowRule	if (Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name )	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

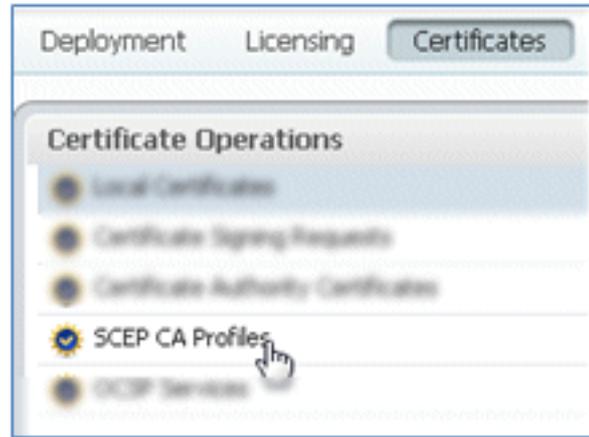
96. طغطة حفظ.



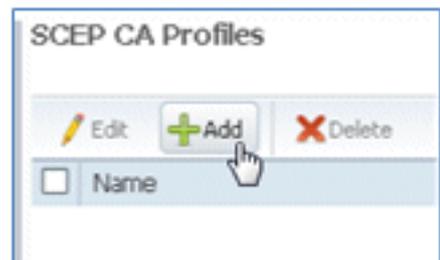
97. انتقل إلى ISE <الإدارة> النظام <الشهادات لتكوين خادم ISE باستخدام ملف تعريف SCEP.



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) `https://<ca-server>/CertSrv/mscep` /url: (تحقق من تكوين خادم CA لديك للحصول على العنوان الصحيح).

SEP Certificate Authority Certificates > New SCEP Profile

Edit Certificate

SEP Certificate Authority

\* Name

Description

\* URL

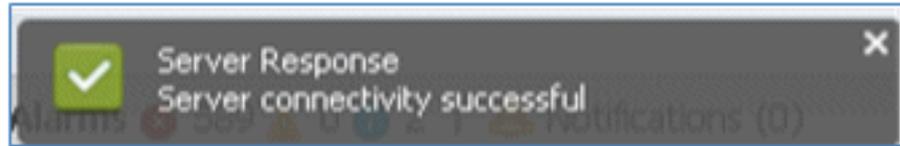
.101

انقر على إختبار الاتصال لاختبار اتصال اتصال SCEP.



.102

توضح هذه الاستجابة أن اتصال الخادم ناجح.



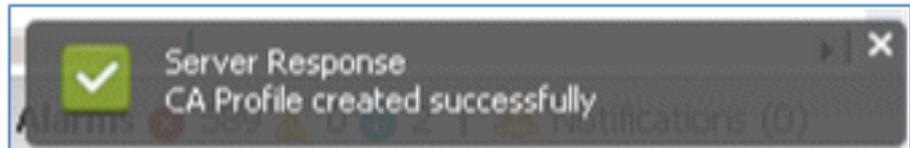
.103

انقر على إرسال.



.104

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



.105. تأكد من إضافة ملف تعريف SCEP CA.

SCEP CA Profiles			
Name	Description	URL	CA Cert Name
<input type="checkbox"/> MySCEP		https://10.10.10.10/cartm/mscep	RFDemo-MSCE

## تجربة المستخدم - توفير نظام التشغيل iOS

### SSID مزدوج

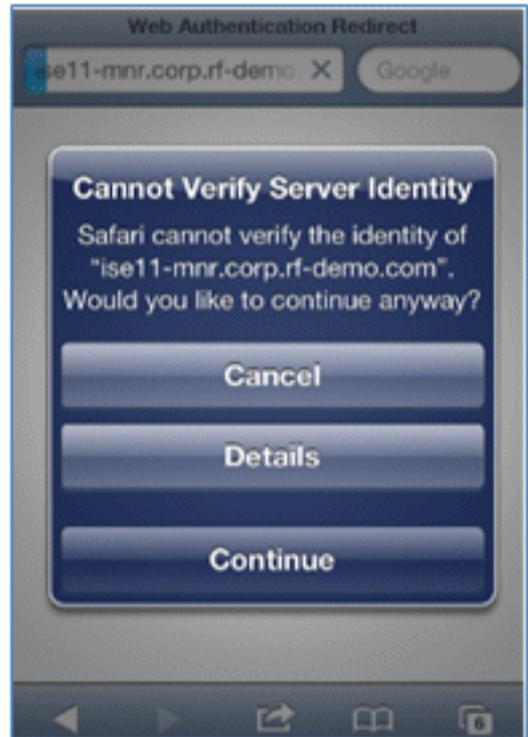
يغطي هذا القسم SSID المزدوج ووصف كيفية الاتصال بالضيف المراد توفيره وكيفية الاتصال بشبكة محلية لاسلكية (WLAN) بسرعة 802.1x.

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

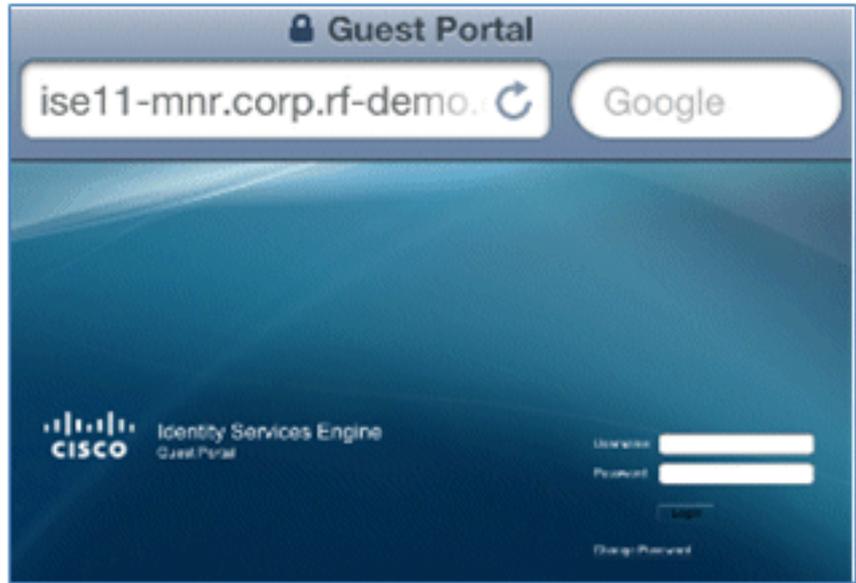
1. على جهاز iOS، انتقل إلى شبكات Wi-Fi، وحدد DemoCWA (يشكل شبكة WLAN مفتوحة على WLC).



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.



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



انقر على تثبيت الشهادة الموثوق بها لخادم CA. 5.



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



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.



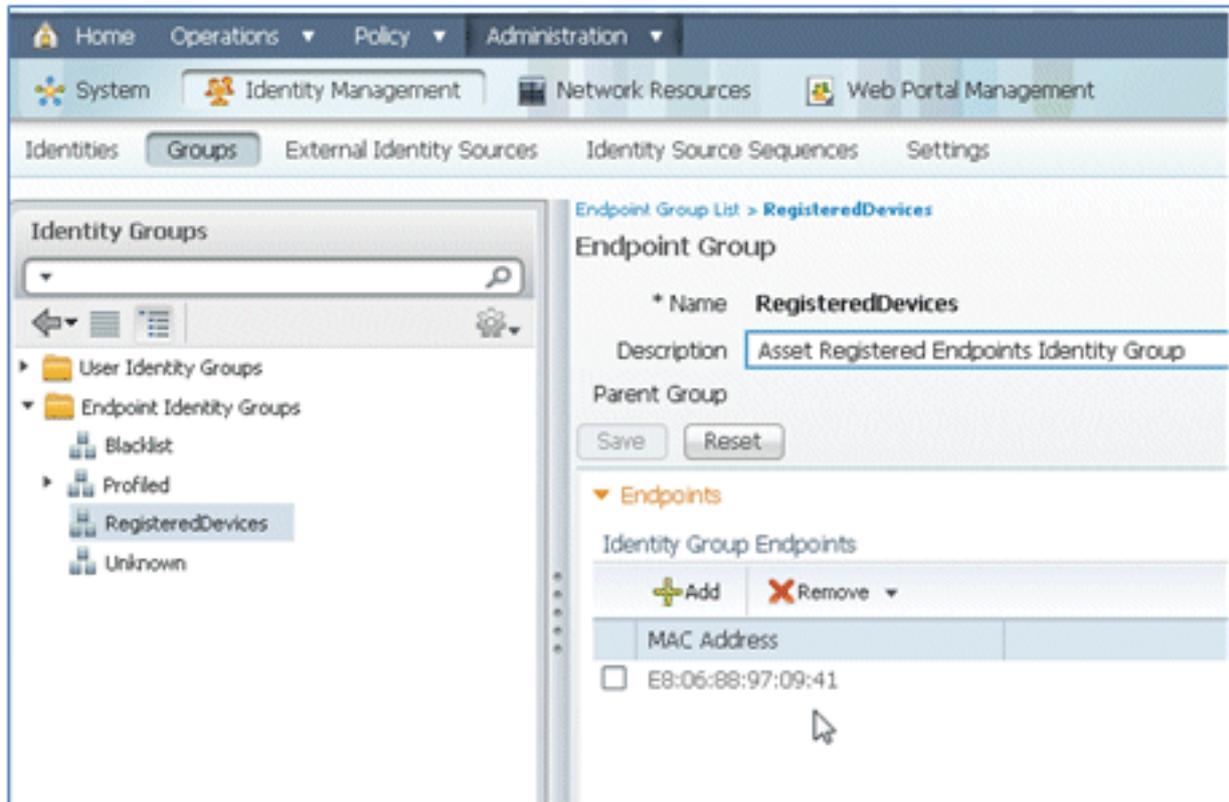
انتقل إلى شبكات Wi-Fi، وقم بتغيير الشبكة إلى العرض التوضيحي 1x. جهازك متصل الآن ويستخدم TLS1.1.



على ISE، انتقل إلى العمليات < المصادقة. تظهر الأحداث العملية التي يتم فيها توصيل الجهاز بشبكة الضيف 12. المفتوحة، وبمر بعملية التسجيل باستخدام تزويد مقدم الطلب، ويتم السماح بالوصول بعد التسجيل.

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:27:57.052 AM	✓		paul	EB-06-98-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:27:21.714 AM	✓		EB-06-98-97-09-41	EB-06-98-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:27:20.438 AM	✓				WLC				Dynamic Authorization succeeded
Mar 25,12 12:26:56.187 AM	✓		paul	EB-06-98-97-09-41	WLC	CWA	Any_Profiled_Apple_Pad	Pending	

انتقل إلى ISE < إدارة < إدارة الهوية < مجموعات < مجموعات هوية نقطة النهاية < الأجهزة المسجلة. تمثنا. إضافة عنوان MAC إلى قاعدة البيانات.

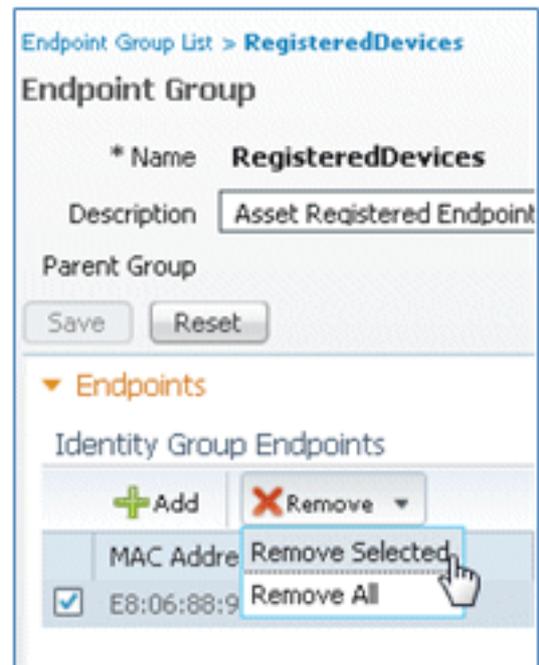


## SSID واحد

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، وطققة 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).

Live Authentications									
Add or Remove Columns Refresh Refresh Every 3 seconds Show Latest 20 records									
Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12:40:03.593 AM	✓	🔒	paul	EB:06:98:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12:39:53.353 AM	✓	🔒	EB:06:98:97:09:41	EB:06:98:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12:39:08.967 AM	✓	🔒	paul	EB:06:98:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

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.

Live Authentications									
Add or Remove Columns Refresh Refresh Every 3 seconds Show Latest 20 records									
Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12:40:03.593 AM	✓	🔒	paul	EB:06:98:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12:39:53.353 AM	✓	🔒	EB:06:98:97:09:41	EB:06:98:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12:39:08.967 AM	✓	🔒	paul	EB:06:98:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

## 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،

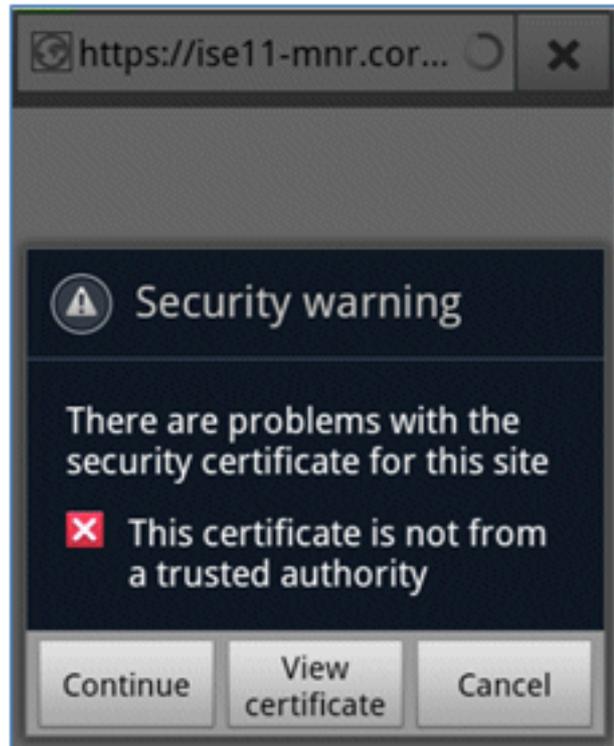
فالفارق المهم هو أن جهاز الأندرويد يتطلب الدخول إلى الإنترنت من أجل الوصول إلى سوق جوجل (الآن جوجل بلاي) وتنزيل مقدم الطلب.

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

1. في جهاز Android، استخدم Wi-Fi للاتصال بـ DemoCWA، وافتح شبكة WLAN للضيف.



2. قبول أي شهادة للاتصال بـ ISE.



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

Username: paul

Password: .....

Login

Prev. Next

1 2 3 4 5 6 7 8 9 0

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

https://market.androi...

CISCO Identity Services Engine 1.1 Self-Provisioning Portal

Device Registration

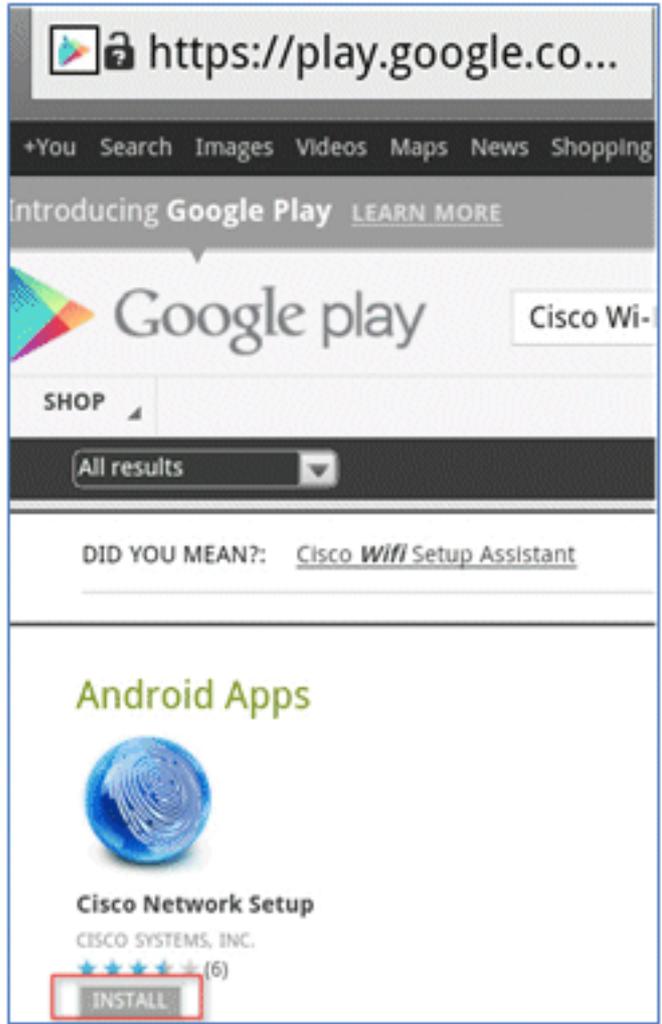
This device has not been registered. To register this device, please enter the Device ID (MAC Address format nnnn-nnnn-nnnn-nnnn where n is either A-F or a digit 0-9) and a description (optional). Please click the "Register" button to install and run the Cisco Wi-Fi Setup Assistant application. This application will install all the necessary certificates and configures your device to use secure wifi network. Clicking the "Register" button will redirect you to android market place, where you can download the Cisco Wi-Fi Setup Assistant application.

Device ID: 98-0C-82-40-31-A9

Description:

Register

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



.6

قم بتسجيل الدخول إلى Google، وانقر فوق تثبيت.



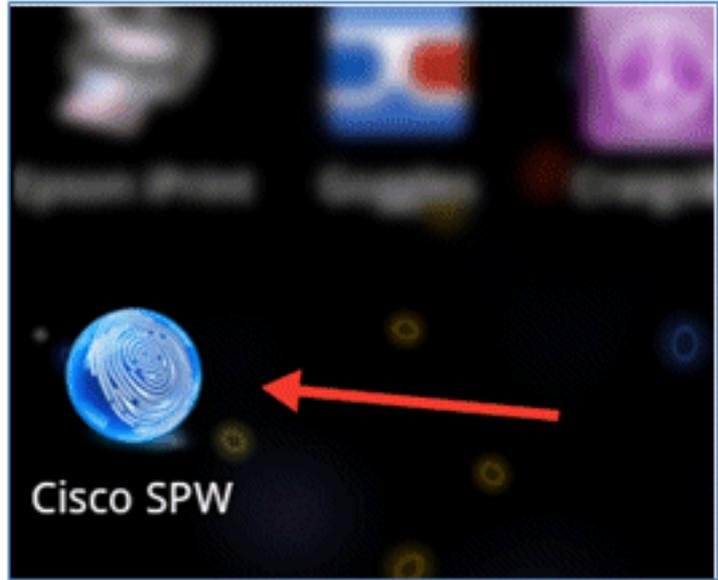
.7

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

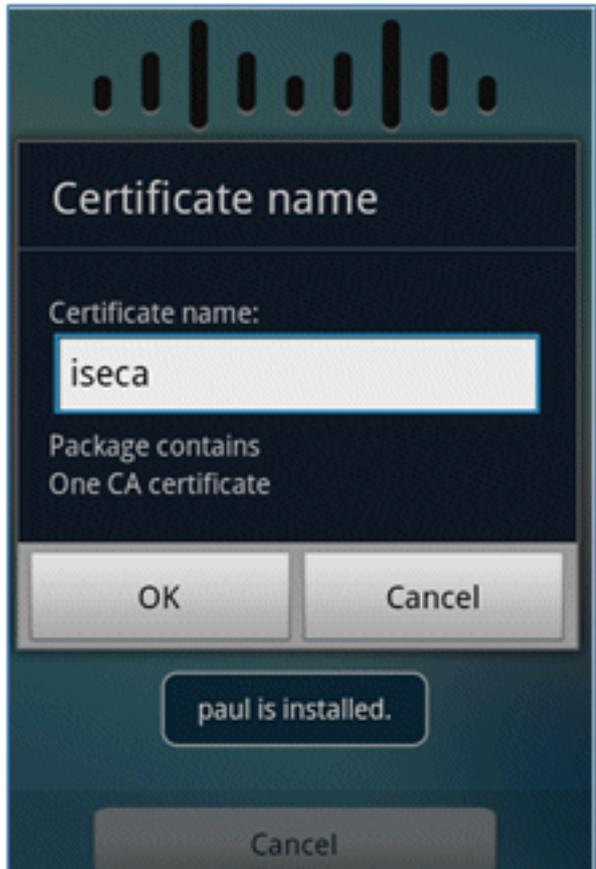
عند المطالبة، قم بتعيين كلمة مرور لتخزين بيانات الاعتماد.



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

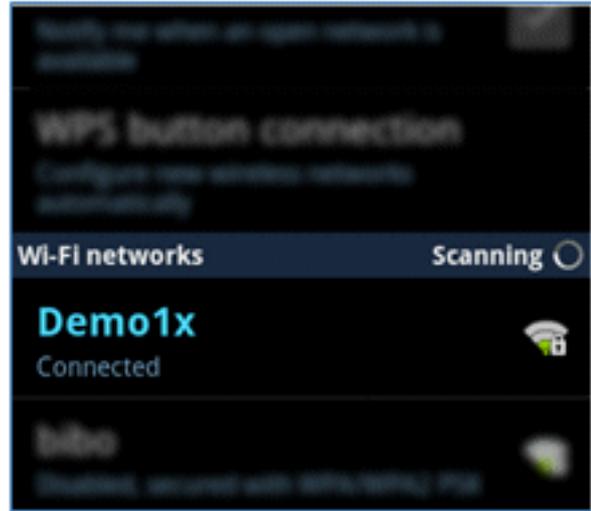


يستمر SPW من Cisco ويطلب اسم شهادة آخر، يحتوي على شهادة CA. أدخل الاسم iseca (في هذا 14. المثال)، ثم انقر فوق موافق للمتابعة.



.15

جهاز Android متصل الآن.

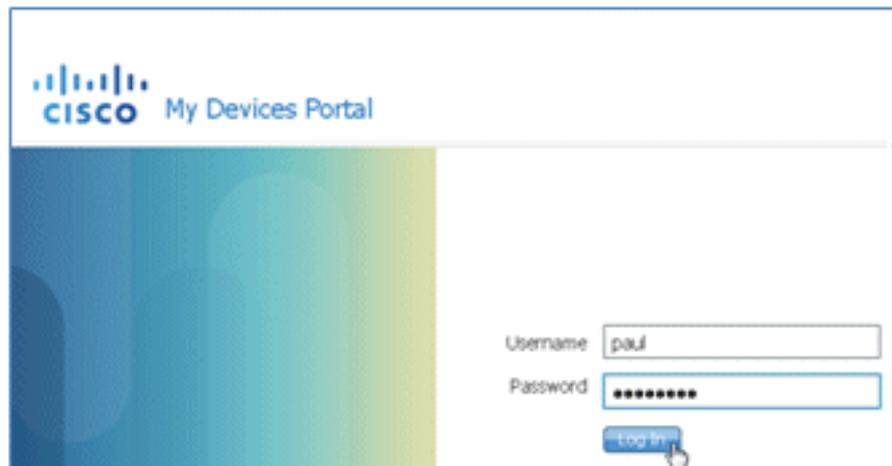


## بوابة أجهزتي

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

أتمت هذا steps in order to 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.

### Add a New Device

To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

\* Device ID

Description

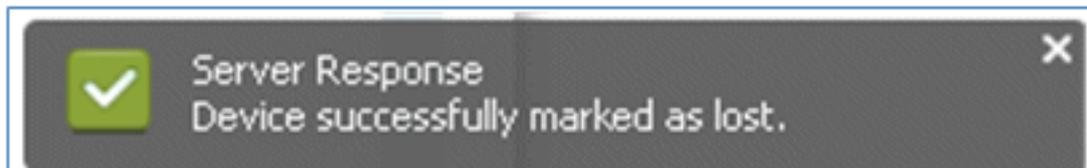
#### Your Devices

State	Device ID	Description	Action
	EB:06:88:97:09:41		<a href="#">Edit</a>   <a href="#">Log2</a>

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



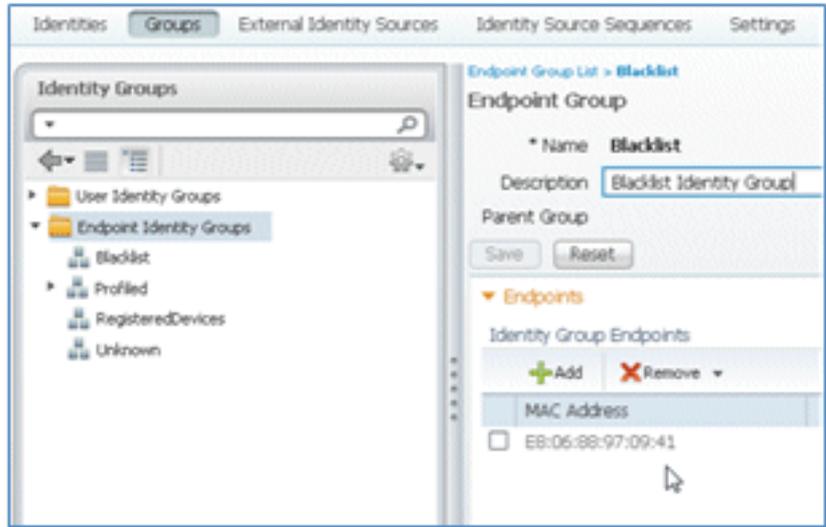
4. يؤكد ISE أن الجهاز تم وضع علامة LOST عليه.



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:

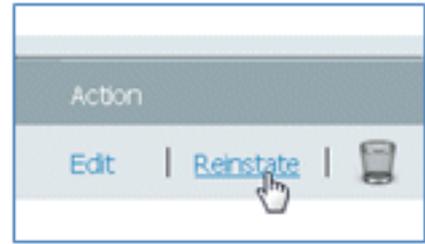
Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12:49:07.851 AM	Failed		pauf	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:59.057 AM	Failed		EB:06:88:97:09:41	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:54.137 AM	Failed		pauf	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed

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:

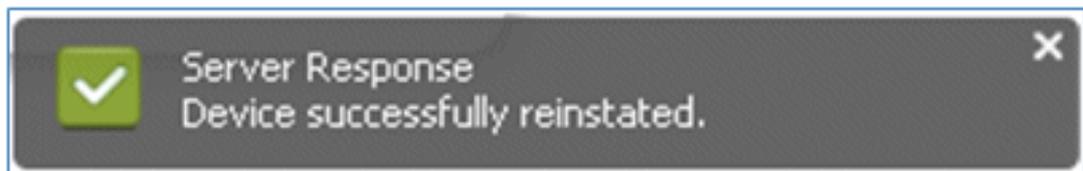
1. من بوابة "أجهزتي"، انقر فوق إعادة الحالة لذلك الجهاز.



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.

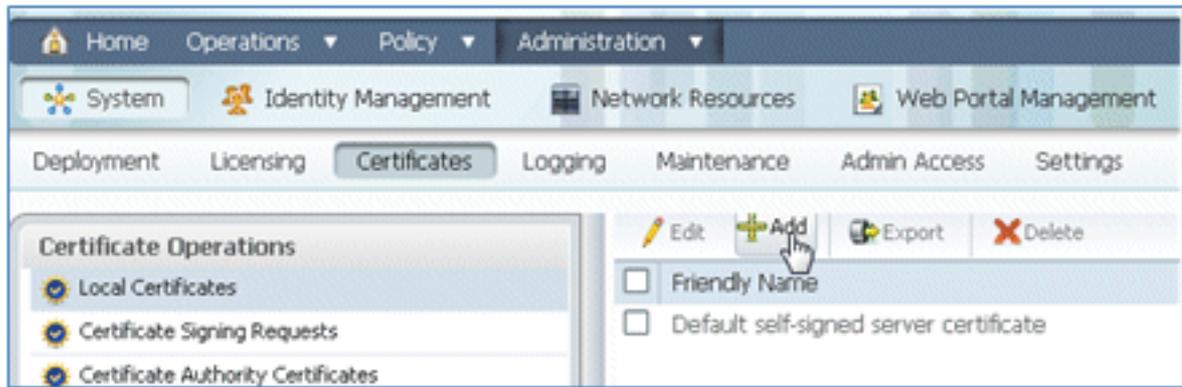


## المرجع - الشهادات

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.



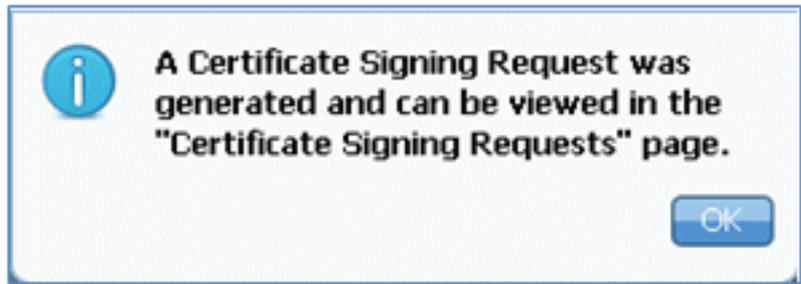
2. حدد إنشاء طلب توقيع الشهادة (CSR).



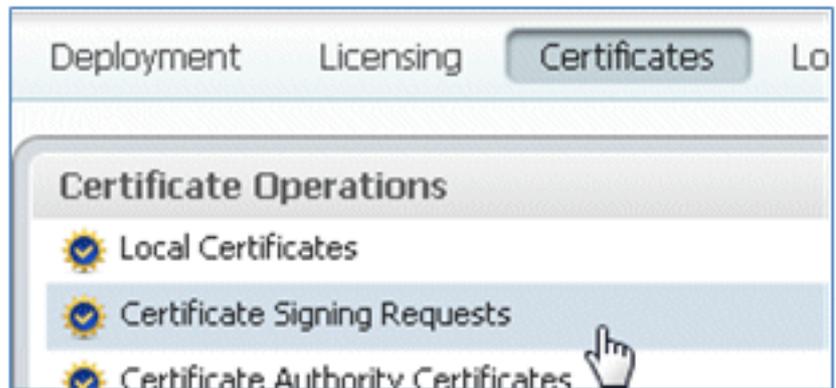
3. أدخل موضوع الشهادة <CN=<ISE-Server Hostname.FQDN. للحقول الأخرى، يمكنك استخدام القيم الافتراضية أو القيم المطلوبة من قبل إعداد المرجع المصدق. انقر على إرسال.



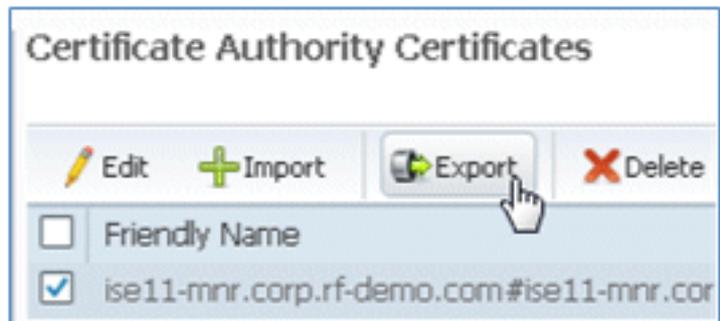
4. يتحقق ISE من إنشاء CSR.



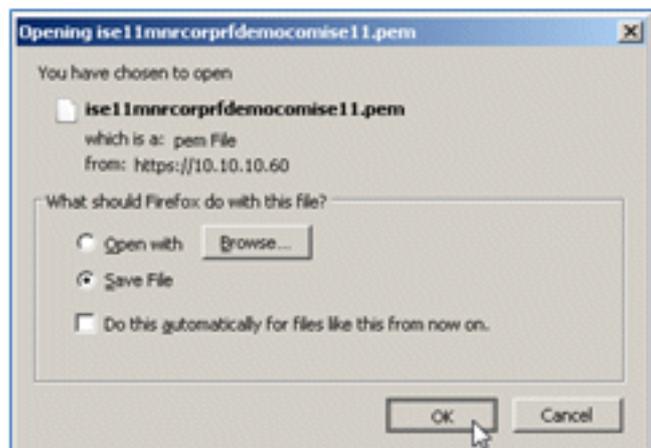
5. للوصول إلى CSR، انقر على عمليات طلبات توقيع الشهادة.



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



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

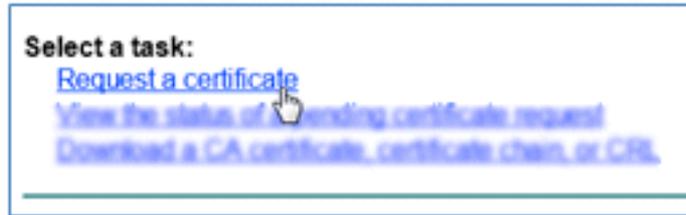


8. حدد مكان وافتح ملف شهادة ISE باستخدام محرر نصي.



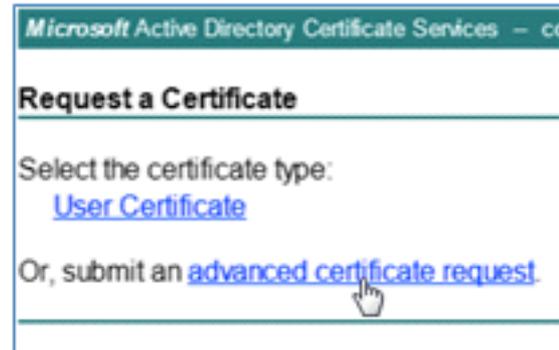
.11

انقر على طلب شهادة.



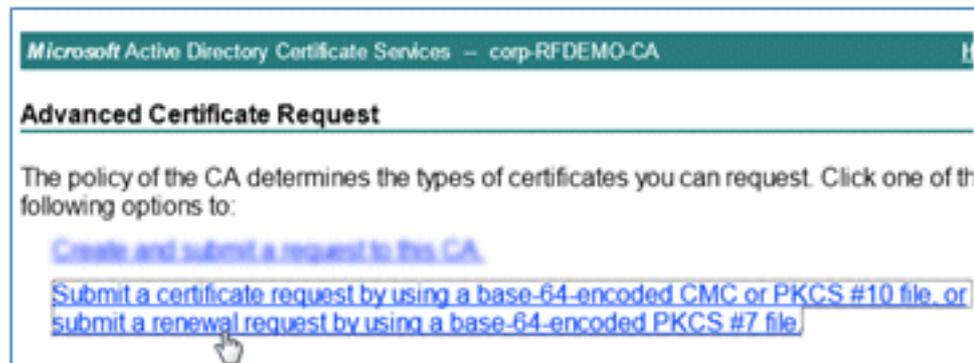
.12

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 **كلام** ويب، وانقر إرسال.

Microsoft Certificate Services -- labsrv.corp.rf-demo.com

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
MAAGAlUdDwQEAvICrDAdBgNVHQ4EFgQUBJa5qgBc
VRO1BAwwCgYIKwYBBQUHAWewEQYJYIZIAAYb4QgEB
BQUAA4GBAKS+tyTCZiNKcXIygxHTWjepfDqVdo8Z
1/t.65UIOKQayBRUp2.1TpHf+o27eDTVw#83bCmbD1
osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pM
-----END CERTIFICATE-----
```

**Certificate Template:**

Web Server

**Additional Attributes:**

Attributes:

Submit >

.15

انقر على تنزيل الشهادة.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)

.16

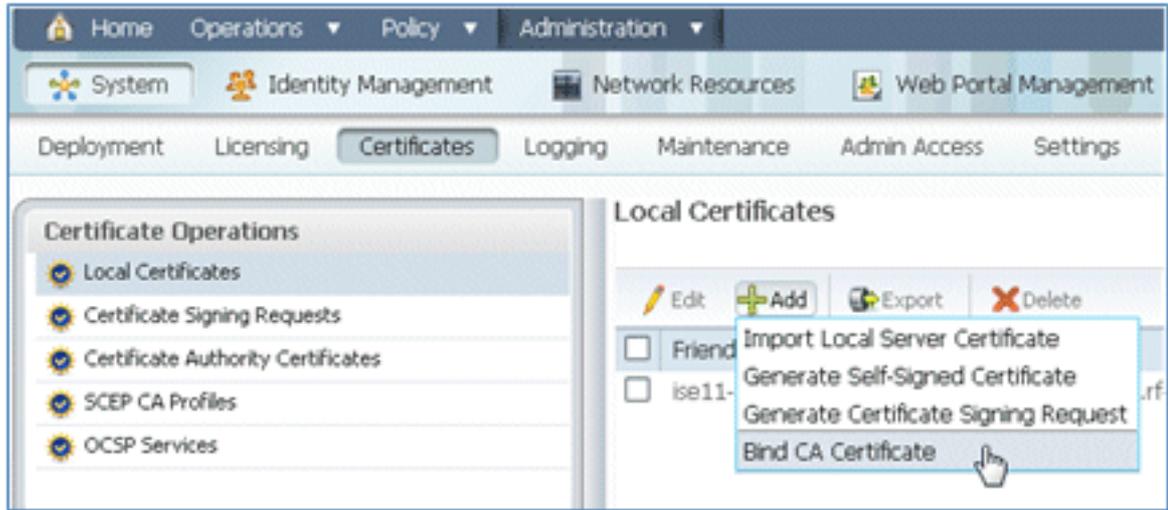
قم بحفظ ملف certnew.cer؛ سيتم استخدامه لاحقاً للربط مع ISE.

Do you want to open or save certnew.cer (921 bytes) from 10.10.10.10?

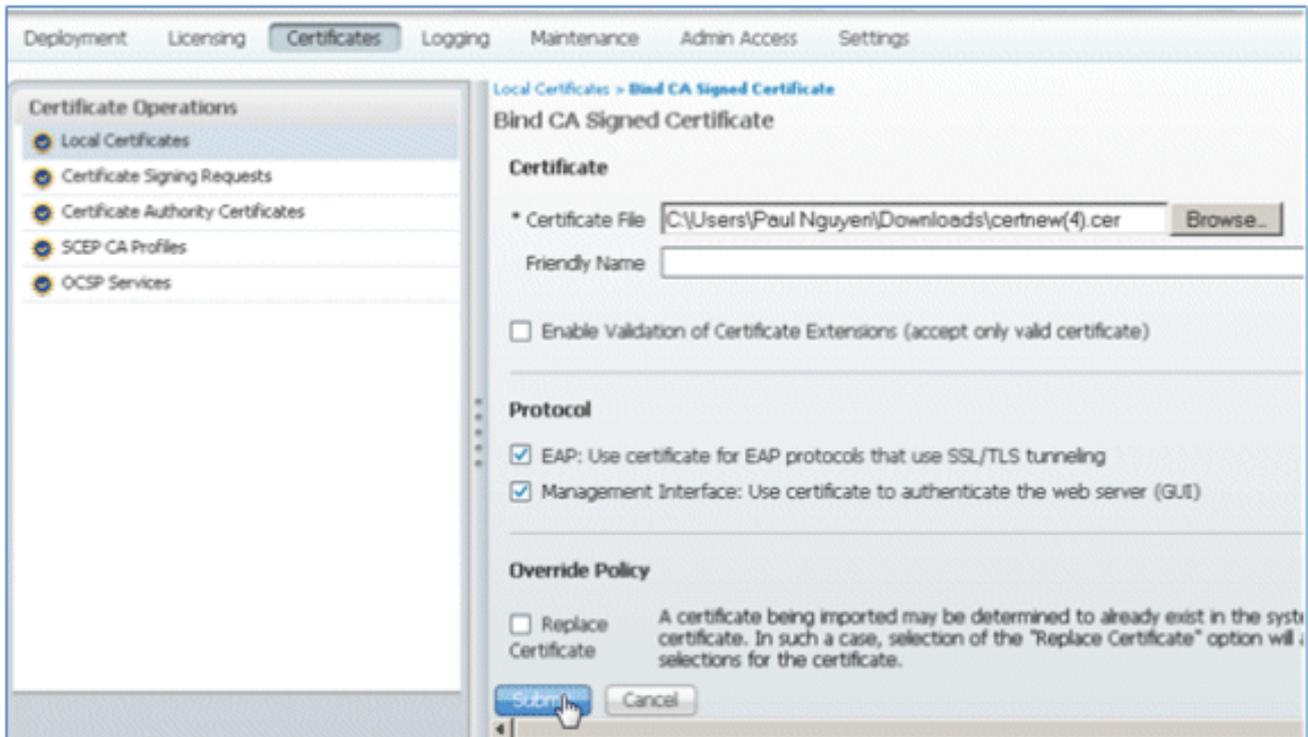
Open Save

.17

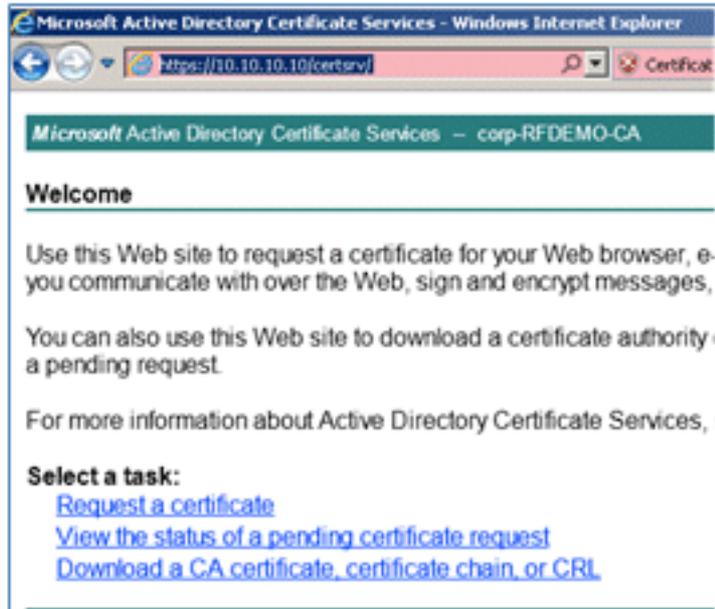
من شهادات ISE، انتقل إلى شهادات محلية، وانقر إضافة < ربط شهادة CA.



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.



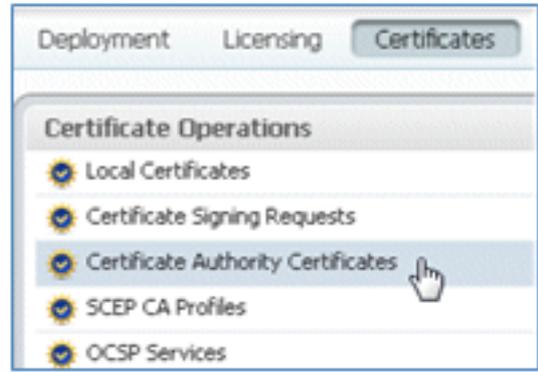
.21

قم بحفظ الملف على الجهاز المحلي.



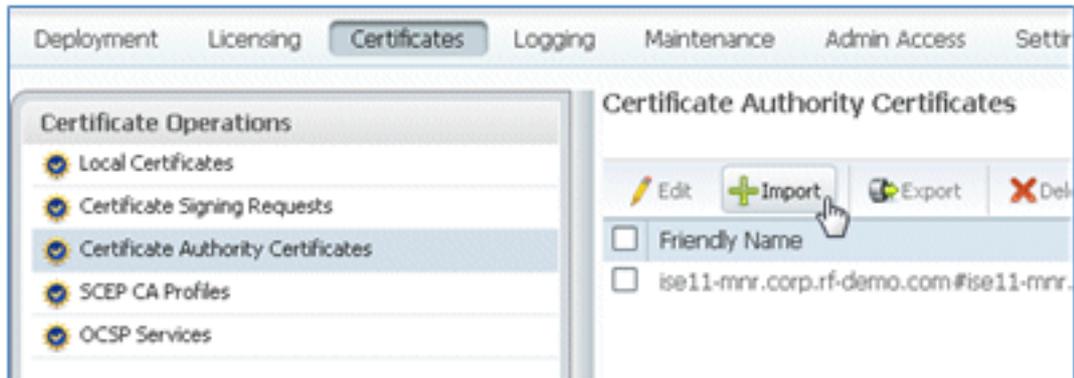
.22

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



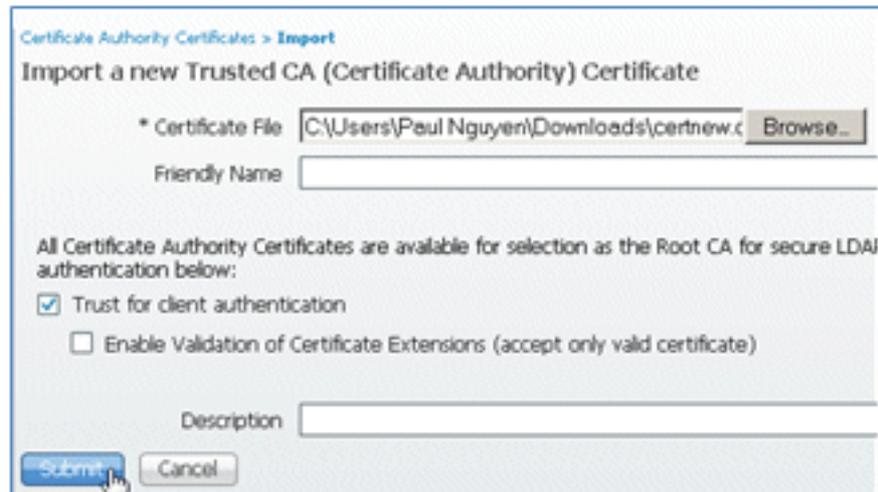
.23

انقر فوق استيراد.



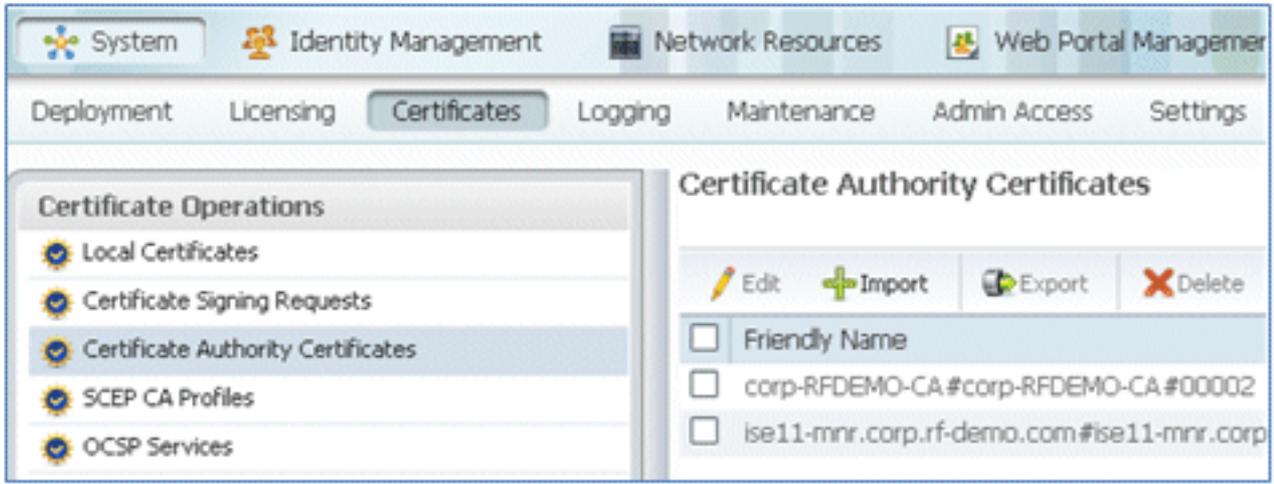
.24

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](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف ا ن ا ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (رف و ت م ط بار ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا