

# ةي وهلا تامدخ كرحم عم يكلساللا BYOD

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[طوبولوجيا](#)

[الاصطلاحات](#)

[نظرة عامة على وحدة تحكم الشبكة المحلية اللاسلكية CoA و RADIUS NAC](#)  
[تدفق ميزات RADIUS NAC و CoA لوحدة تحكم الشبكة المحلية \(LAN\) اللاسلكية](#)

[نظرة عامة على تصنيف ISE](#)

[إنشاء مستخدم الهوية الداخلية](#)

[إضافة وحدة تحكم في الشبكة المحلية \(LAN\) اللاسلكية إلى ISE](#)

[تكوين ISE للمصادقة اللاسلكية](#)

[وحدة التحكم في شبكة LAN اللاسلكية ل Bootstrap](#)

[توصيل WLC بشبكة](#)

[إضافة خوادم المصادقة \(ISE\) إلى WLC](#)

[إنشاء الواجهة الديناميكية لموظف WLC](#)

[إنشاء واجهة ديناميكية لضيف WLC](#)

[إضافة 802.1x WLAN](#)

[اختيار الواجهات الديناميكية WLC](#)

[المصادقة اللاسلكية لنظام التشغيل \(iOS \(iPhone/iPad](#)

[إضافة قائمة التحكم في الوصول \(ACL\) لإعادة توجيه الوضع إلى WLC](#)

[تمكين إختبارات إنشاء ملف التعريف على ISE](#)

[تمكين نهج ملف تعريف ISE للأجهزة](#)

[ملف تعريف تخويل ISE لإعادة توجيه اكتشاف الوضع](#)

[إنشاء ملف تعريف تخويل ISE للموظف](#)

[إنشاء ملف تعريف تخويل ISE للمقاول](#)

[نهج التخويل الخاص بوضعية الجهاز/إنشاء ملفات التعريف](#)

[إختبار سياسة إصلاح الوضع](#)

[سياسة التخويل للوصول المميز](#)

[إختبار CoA للوصول المميز](#)

[WLC Guest WLAN](#)

[إختبار الشبكة المحلية اللاسلكية \(WLAN\) للضيف وبوابة الضيوف](#)

[وصول ضيف برعاية ISE Wireless](#)

[ضيف رعاية](#)

[إختبار الوصول إلى بوابة الضيوف](#)

[تكوين الشهادة](#)

[تكامل Windows 2008 Active Directory](#)

[إضافة مجموعات Active Directory](#)  
[إضافة تسلسل مصدر الهوية](#)  
[وصول الضيف الذي ترعاه ISE Wireless مع إعلان مدمج](#)  
[شكلت فسحة بين دعامتين على المفتاح](#)  
[المرجع: المصادقة اللاسلكية لنظام التشغيل Apple Mac OS X](#)  
[المرجع: مصادقة لاسلكية لنظام Microsoft Windows XP](#)  
[المرجع: المصادقة اللاسلكية لنظام التشغيل Microsoft Windows 7](#)  
[معلومات ذات صلة](#)

## [المقدمة](#)

محرك خدمات الهوية من Cisco (ISE) هو خادم سياسات الجيل التالي من Cisco الذي يوفر البنية الأساسية للمصادقة والتفويض لحل Cisco TrustSec. كما يوفر خدمتين حيويتين آخرين:

- تتمثل الخدمة الأولى في توفير طريقة لتوصيف نوع جهاز نقطة النهاية تلقائياً استناداً إلى السمات التي يتلقاها Cisco ISE من مصادر معلومات مختلفة. توفر هذه الخدمة (التي تسمى Profiler) وظائف مكافئة لما قدمته Cisco سابقاً مع جهاز تعريف Cisco NAC.
  - من الخدمات المهمة الأخرى التي يقدمها Cisco ISE مسح التوافق مع نقطة النهاية؛ على سبيل المثال، تثبيت برنامج AV/AS وصلاحية ملف التعريف الخاص به (المعروف باسم Posture). كانت Cisco توفر سابقاً وظيفة الوضع هذه فقط مع جهاز Cisco NAC.
- يوفر Cisco ISE مستوى مكافئ من الوظائف، ويتم دمجها مع آليات مصادقة 802.1X.

يمكن أن توفر Cisco ISE المدمجة مع وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs) آليات تصنيف الأجهزة المحمولة مثل أجهزة iPhone (Apple iDevices)، iPad، و iPod، والهواتف الذكية القائمة على نظام التشغيل Android، وغيرها. بالنسبة لمستخدمي 802.1X، يمكن أن يوفر Cisco ISE نفس مستوى الخدمات مثل إنشاء ملفات التعريف والمسح الضوئي للوضع. كما يمكن دمج خدمات الضيوف على Cisco ISE مع Cisco WLC عن طريق إعادة توجيه طلبات مصادقة الويب إلى Cisco ISE للمصادقة.

يقدم هذا المستند الحل اللاسلكي لجلب الجهاز الخاص بك (BYOD)، مثل توفير وصول مميز بناء على نقاط النهاية المعروفة ونهج المستخدم. لا يوفر هذا المستند الحل الكامل لـ BYOD، ولكنه يعمل على عرض حالة استخدام بسيطة للوصول الديناميكي. وتتضمن أمثلة التكوين الأخرى استخدام بوابة رعاية ISE، حيث يمكن للمستخدم ذي الامتيازات رعاية ضيف لتوفير وصول الضيف اللاسلكي.

## [المتطلبات الأساسية](#)

### [المتطلبات](#)

لا توجد متطلبات خاصة لهذا المستند.

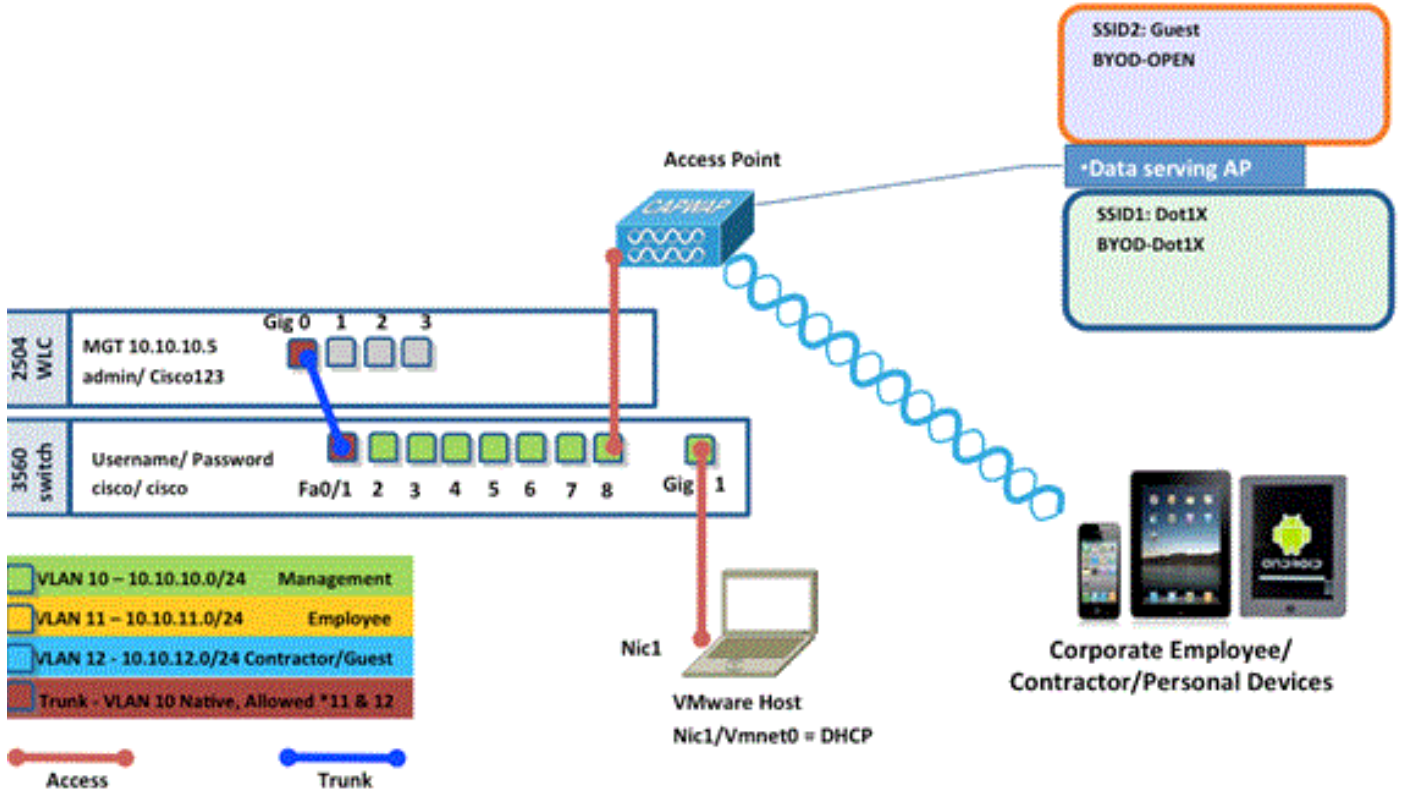
### [المكونات المستخدمة](#)

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

- وحدة التحكم في شبكة LAN اللاسلكية 2504 أو 2106 من Cisco مع إصدار البرنامج 7.2.103
- 8 - Catalyst 3560 منافذ
- WLC 2504
- محرك خدمات تعريف 1.0MR (إصدار صورة خادم VMware)

• خادم Windows 2008 (صورة VMware) — قرص سعة 512 ميجابايت و 20 جيجابايتخدمة Active DirectoryDNSDHCP خدمات الشهادات

## طوبولوجيا



Name	IP Address	Credential
Vmware Host	10.10.10.2	(Machine used to host the ISE 1.0 MR vmware server files)
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)

## الاصطلاحات

راجع اصطلاحات تلميح Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

## نظرة عامة على وحدة تحكم الشبكة المحلية اللاسلكية RADIUS NAC و CoA

يمكن هذا الإعداد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من البحث عن أزواج AV الخاصة بإعادة توجيه URL القادمة من خادم RADIUS ISE. هذا فقط على شبكة WLAN المرتبطة بواجهة مع تمكين إعداد RADIUS NAC. عند تلقي زوج AV من Cisco لإعادة توجيه URL، يتم وضع العميل في حالة POSTURE\_REQD. وهو في الأساس نفس حالة Webauth\_REQD داخليا في جهاز التحكم.

عندما يقرر خادم RADIUS ISE أن العميل متوافق مع Posture\_Compliant، فإنه يصدر إعادة مصادقة CoA. يتم استخدام Session\_ID لربطه معا. مع هذا مصادقة جديدة (reauth) لا يرسل هو ال url-redirect av-pair. نظرا لعدم وجود أزواج AV لإعادة توجيه URL، تعرف وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) أن العميل لم يعد يتطلب الوضع.

إذا لم يتم تمكين إعداد RADIUS NAC، فإن WLC يتجاهل URL Redirect VSA.

CoA-Reauth: يتم تمكين هذا مع إعداد RFC 3576. تمت إضافة قدرة إعادة المصادقة إلى أوامر CoA الحالية التي تم دعمها سابقاً.

يكون إعداد RADIUS NAC حصرياً بشكل متبادل من هذه الإمكانيات، رغم أنها مطلوبة لكي تعمل CoA.

قائمة التحكم في الوصول (ACL) للوضع المسبق: عندما يكون العميل في حالة POSTURE\_REQ، يكون السلوك الافتراضي لمركز التحكم في الشبكة المحلية اللاسلكية (WLC) هو حظر جميع حركات المرور باستثناء DHCP/DNS. يتم تطبيق قائمة التحكم في الوصول (ACL) السابقة للوضعية (والتي يطلق عليها في زوج AV الخاص بقوائم التحكم في الوصول (URL-Redirect-ACL) على العميل، وما هو مسموح به في قائمة التحكم في الوصول هذه هو ما يمكن للعميل الوصول إليه.

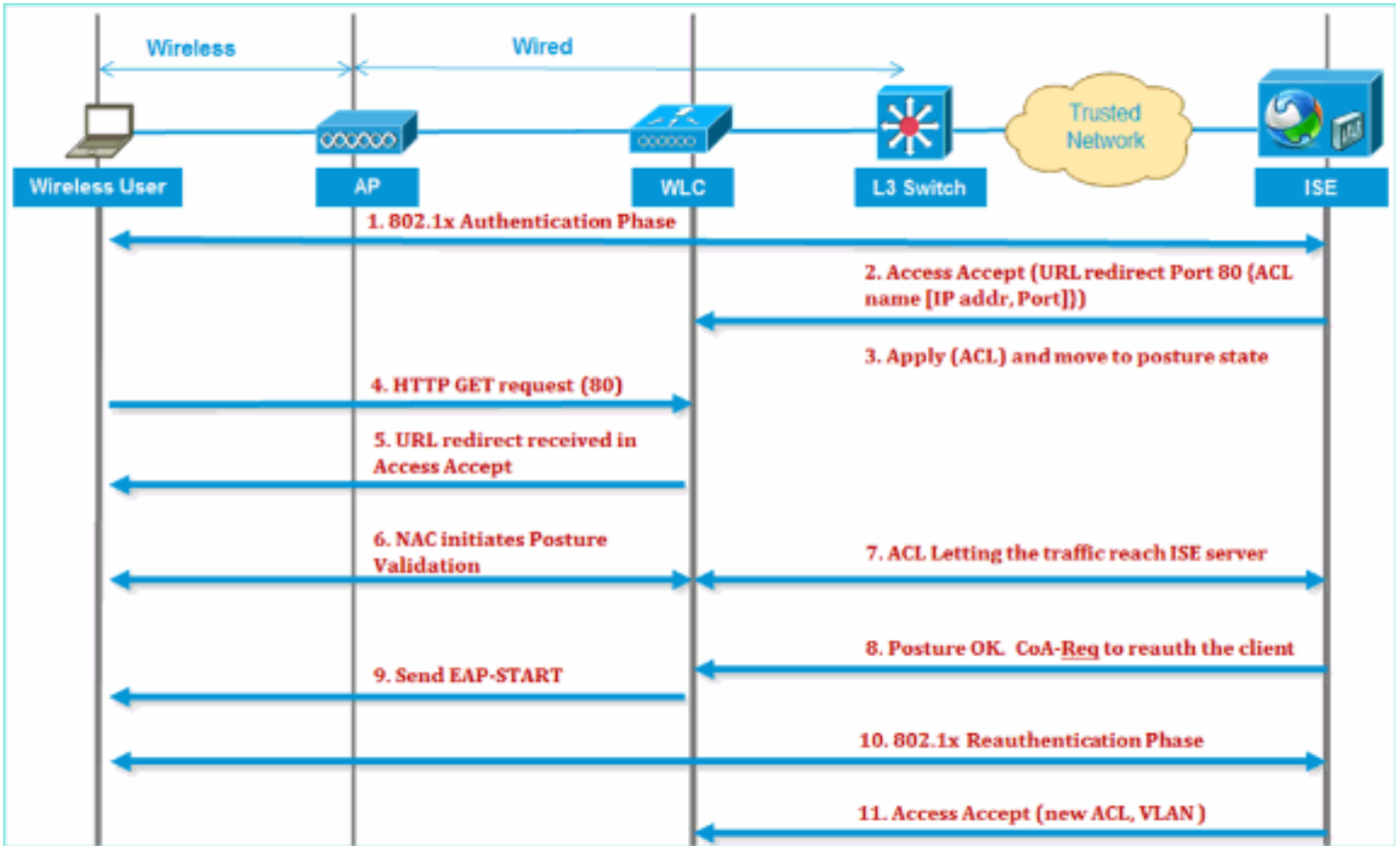
تجاوز قائمة التحكم في الوصول (ACL) السابقة للمصادقة مقابل شبكة VLAN: لا يتم دعم شبكة VLAN الخاصة بالحجر الصحي أو شبكة AuthC التي تختلف عن شبكة VLAN الخاصة ب Access-VLAN في 7.0MR.1. إن يثبت أنت VLAN من السياسة نادل، هو سيكون ال VLAN لجلسة كامل. لا توجد حاجة إلى تغييرات VLAN بعد AuthZ الأول.

## تدفق ميزات RADIUS NAC و CoA لوحدة تحكم الشبكة المحلية (LAN) اللاسلكية

يوفر [الشكل](#) التالي تفاصيل تبادل الرسائل عند مصادقة العميل إلى الخادم الخلفي والتحقق من وضع NAC.

1. تتم مصادقة العميل باستخدام مصادقة dot1x.
2. يحمل "قبول الوصول إلى RADIUS" عنوان URL المعاد توجيهه للمنفذ 80 وقوائم التحكم في الوصول (ACL) السابقة للمصادقة التي تتضمن السماح لعناوين IP والمنافذ، أو شبكة VLAN المعزولة.
3. ستتم إعادة توجيه العميل إلى عنوان URL المتوفر في قبول الوصول، وسيتم وضعه في حالة جديدة حتى يتم التحقق من صحة الوضع. يتحدث العميل في هذه الحالة إلى خادم ISE ويتحقق من صحة نفسه مقابل السياسات التي تم تكوينها على خادم ISE.
4. يقوم عميل NAC على بدء التحقق من صحة الوضع (حركة المرور إلى المنفذ 80): يرسل العميل طلب اكتشاف HTTP إلى المنفذ 80 الذي تقوم وحدة التحكم بإعادة توجيهه إلى URL المتوفر في قبول الوصول. وبدرك مدير البنية الأساسية المحسن (ISE) أن العميل يحاول الوصول إلى العميل والاستجابة له مباشرة. بهذه الطريقة يتعلم العميل حول بروتوكول ISE Server IP، ومن الآن فصاعداً، يتحدث العميل مباشرة مع خادم ISE.
5. يسمح WLC لحركة المرور هذه لأنه تم تكوين قائمة التحكم في الوصول (ACL) للسماح بحركة المرور هذه. في حالة تجاوز شبكة VLAN، يتم ربط حركة مرور البيانات حتى تصل إلى خادم ISE.
6. بمجرد اكتمال تقييم ISE-client، يتم إرسال RADIUS CoA-Req مع خدمة الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يؤدي هذا إلى بدء إعادة مصادقة العميل (إرسال EAP-START). وبمجرد نجاح عملية إعادة المصادقة، يرسل ISE قبول الوصول باستخدام قائمة تحكم في الوصول (ACL) جديدة (إن وجدت) وعدم إعادة توجيه عنوان URL أو شبكة VLAN للوصول.
7. يدعم WLC CoA-Req و Disconnect-Req وفقاً ل RFC 3576. تحتاج وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) إلى دعم CoA-Req لخدمة إعادة المصادقة، وفقاً لمعيار RFC 5176.
8. بدلا من قوائم التحكم في الوصول (ACL) القابلة للتنزيل، يتم استخدام قوائم التحكم في الوصول (ACL) التي تم تكوينها مسبقاً على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يرسل خادم ISE اسم قائمة التحكم في الوصول (ACL) فقط، والذي تم تكوينه بالفعل في وحدة التحكم.
9. يجب أن يعمل هذا التصميم لكل من حالات شبكات VLAN وقوائم التحكم في الوصول (ACL). في حالة تجاوز شبكة VLAN، فما علينا إلا إعادة توجيه المنفذ 80 والسماح (للجسر) ببقية حركة مرور البيانات على شبكة VLAN المعزولة. بالنسبة لقائمة التحكم في الوصول (ACL)، يتم تطبيق قائمة التحكم في الوصول (ACL) السابقة للمصادقة التي تم تلقيها في قبول الوصول.

يوفر هذا الشكل تمثيلا بصريا لتدفق الميزة هذا:



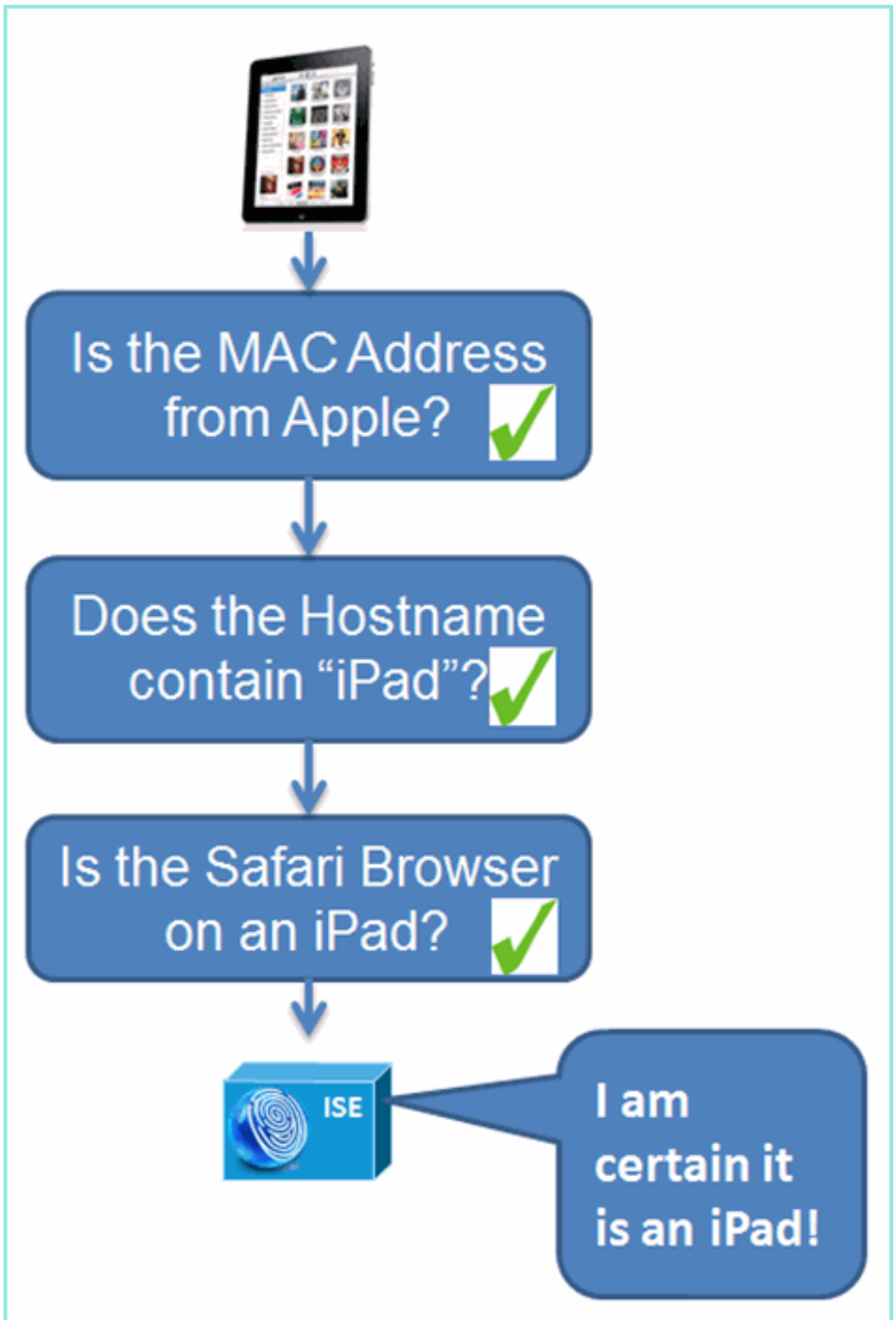
## نظرة عامة على تصنيف ISE

توفر خدمة منشئ ملفات تعريف ISE من Cisco وظائف اكتشاف جميع نقاط النهاية المرفقة على الشبكة لديك وتحديد مكانها وتحديثها، بغض النظر عن أنواع الأجهزة الخاصة بها، لضمان الوصول المناسب إلى شبكة مؤسستك وصيانتها. فهو يقوم في المقام الأول بتجميع سمة أو مجموعة من السمات لكل نقاط النهاية على شبكتك وتصنيفها طبقا لملفات التعريف الخاصة بها.

يتكون منشئ ملفات التعريف من المكونات التالية:

- يحتوي المستشعر على عدد من المسابير. وتلتقط المساطر حزم الشبكة عن طريق الاستعلام عن أجهزة الوصول إلى الشبكة، وإعادة توجيه السمات وقيم سماتها التي يتم تجميعها من نقاط النهاية إلى المحلل.
- يقوم محلل بتقييم نقاط النهاية باستخدام السياسات التي تم تكوينها ومجموعات الهوية لمطابقة السمات وقيم السمات الخاصة بها التي تم تجميعها، والتي تصنف نقاط النهاية إلى المجموعة المحددة وتقوم بتخزين نقاط النهاية مع ملف التعريف المتطابق في قاعدة بيانات Cisco ISE.
- لاكتشاف الجهاز المحمول، من المستحسن استخدام مجموعة من هذه المسابير لتعريف الجهاز بشكل صحيح:

- RADIUS (Call-Station-ID): يوفر عنوان (WI MAC)
  - DHCP (host-name): hostname - اسم المضيف الافتراضي يمكن أن يتضمن نوع الجهاز؛ على سبيل المثال: jsmith-ipad
  - DNS (بحث IP عكسي): FQDN - اسم المضيف الافتراضي يمكن أن يتضمن نوع الجهاز
  - HTTP (وكيل المستخدم): تفاصيل حول نوع جهاز محمول معين
- في هذا المثال على iPad، يلتقط منشئ ملفات التعريف معلومات مستعرض الويب من سمة "وكيل المستخدم"، بالإضافة إلى سمات HTTP الأخرى من رسائل الطلب، وإضافتهم إلى قائمة سمات نقاط النهاية.



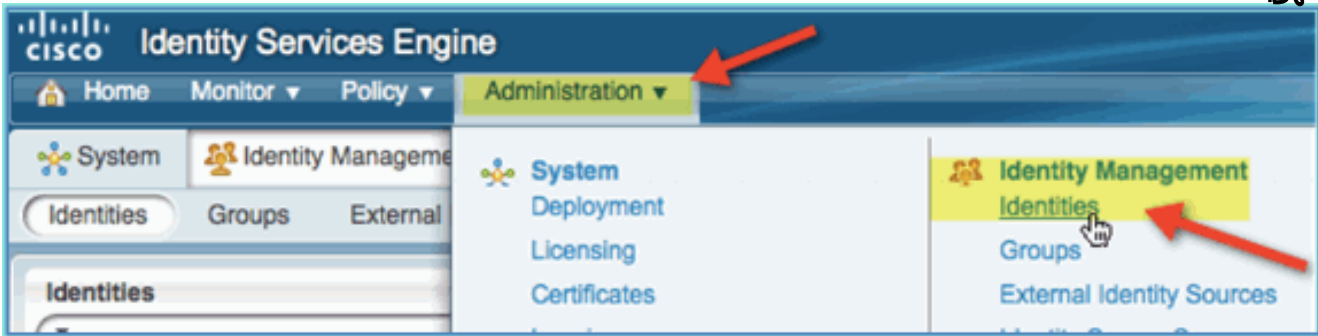
إنشاء مستخدمي الهوية الداخلية

لا يلزم وجود دليل (AD MS Active Directory) لإثبات المفاهيم ببساطة. يمكن استخدام ISE كمخزن الهوية الوحيد، والذي يتضمن التمييز بين وصول المستخدمين إلى الوصول والتحكم في السياسة متعدد المستويات.

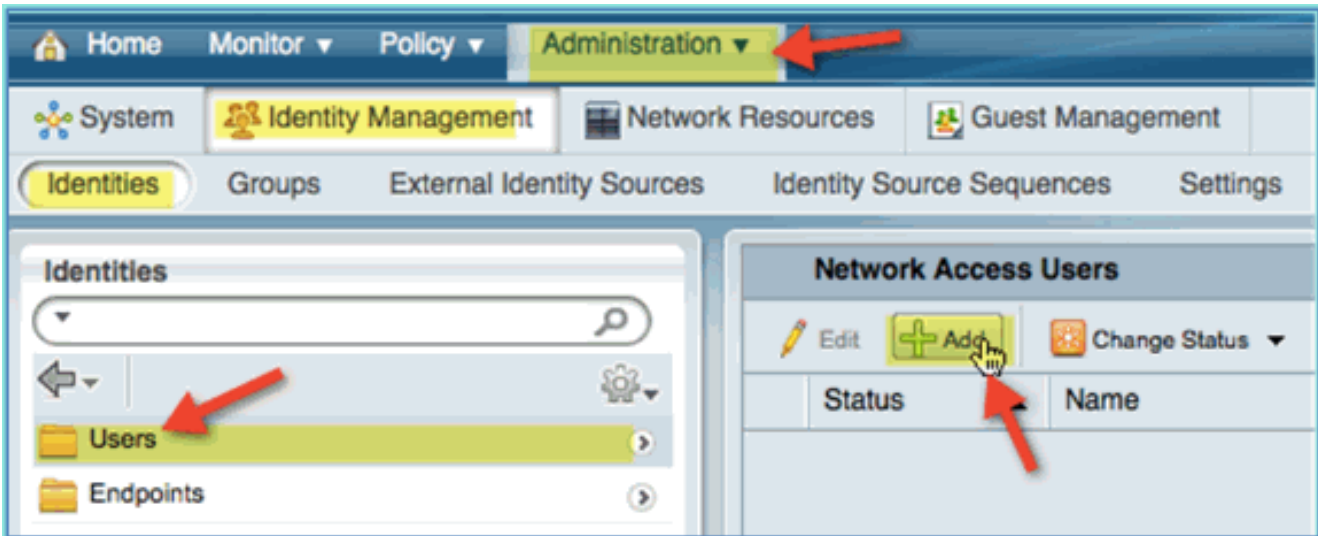
عند إصدار ISE 1.0، باستخدام AD Integration، يمكن أن يستخدم ISE مجموعات AD في سياسات التحويل. في حالة استخدام مخزن مستخدم ISE الداخلي (لا يوجد تكامل AD)، لا يمكن استخدام المجموعات في السياسات المرتبطة بمجموعات هوية الجهاز (الخطأ المعرف الذي سيتم حله في ISE 1.1). وبالتالي، يمكن التمييز بين المستخدمين الأفراد فقط، مثل الموظفين أو المقاولين عند استخدامهم بالإضافة إلى مجموعات هوية الجهاز.

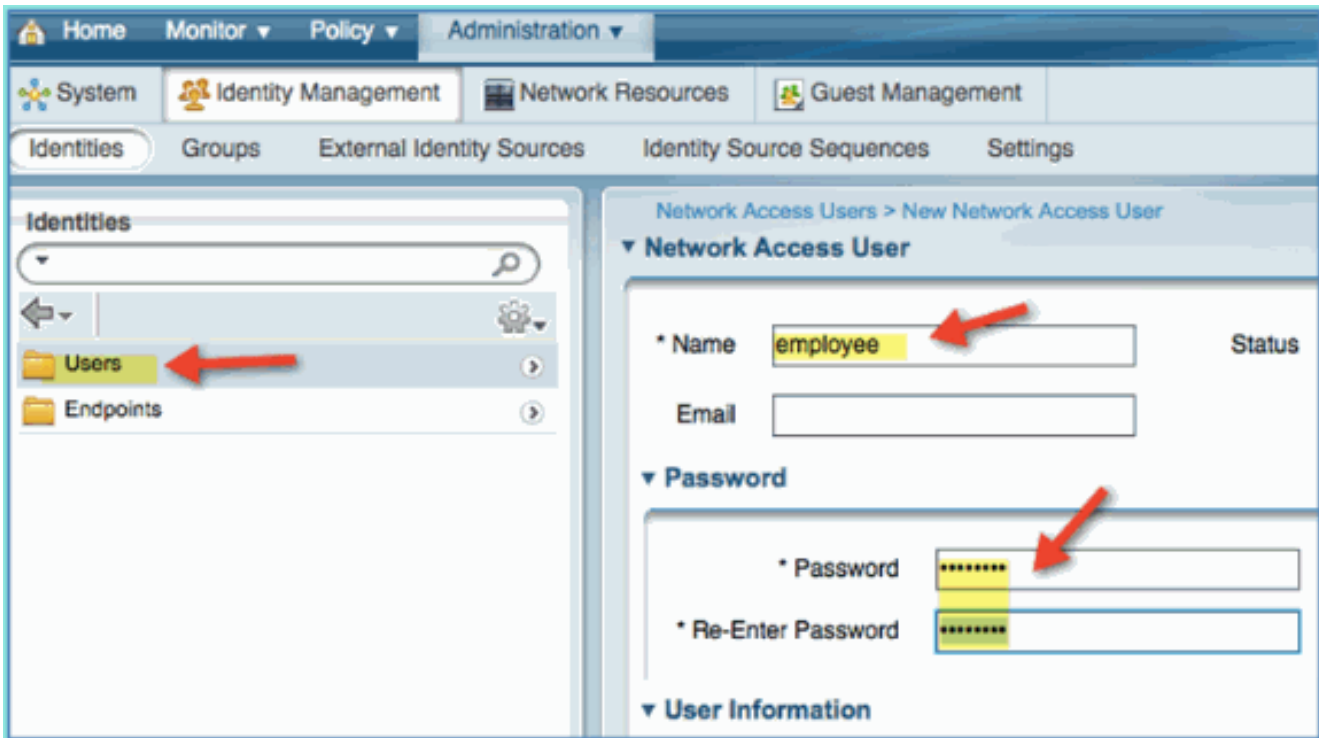
أكمل الخطوات التالية:

1. افتح نافذة المستعرض على عنوان <https://ISEip>.
2. انتقل إلى إدارة < إدارة الهوية > الهويات.

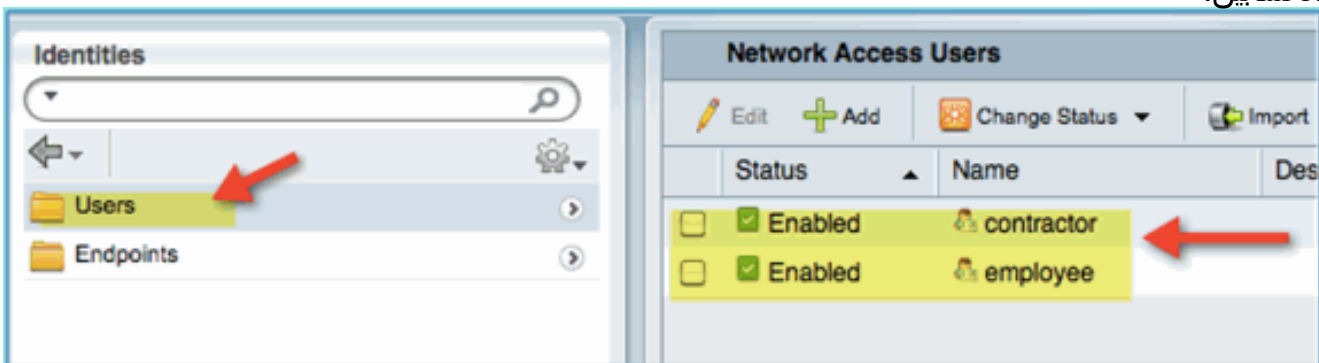


3. حدد مستخدمين، ثم انقر فوق إضافة (مستخدم الوصول إلى الشبكة). أدخل قيم المستخدم هذه وقم بتعيينها إلى مجموعة الموظفين: الاسم: الموظف كلمة المرور: XXXX





4. انقر على إرسال. الاسم: المقاول كلمة المرور: XXXX  
 5. تأكيد إنشاء كلا الحسائين.



## إضافة وحدة تحكم في الشبكة المحلية (LAN) اللاسلكية إلى ISE

يجب أن يكون لأي جهاز يقوم ببدء طلبات RADIUS إلى ISE تعريف في ISE. يتم تحديد أجهزة الشبكة هذه استناداً إلى عنوان IP الخاص بها. يمكن أن تحدد تعريفات جهاز شبكة ISE نطاقات عناوين IP وبالتالي السماح للتعريف بتمثيل أجهزة فعلية متعددة.

وبعيداً عما هو مطلوب لاتصال RADIUS، تحتوي تعريفات جهاز شبكة ISE على إعدادات لاتصال ISE/الجهاز الآخر، مثل SSH و SNMP.

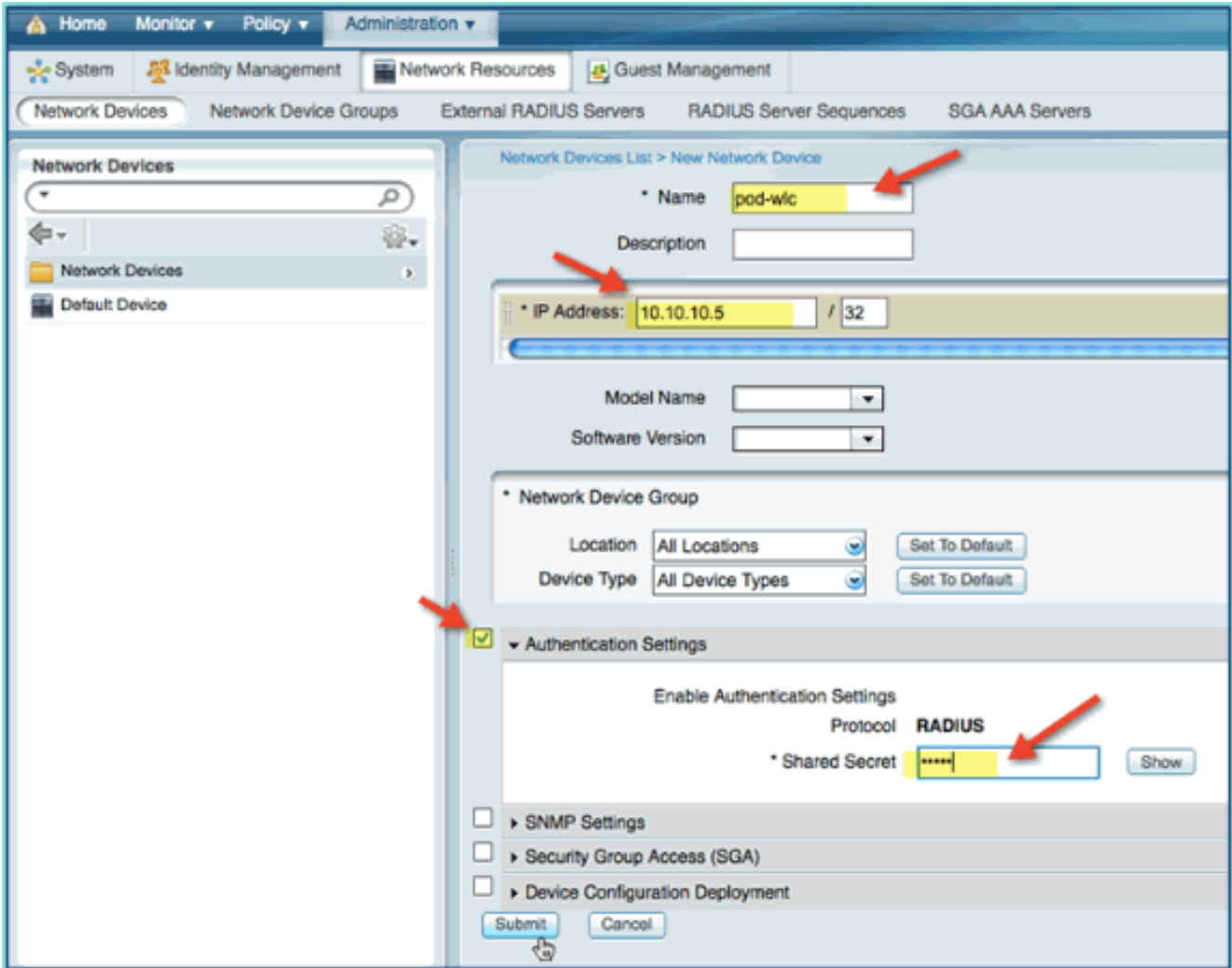
هناك جانب آخر مهم لتعريف جهاز الشبكة وهو تجميع الأجهزة بشكل مناسب حتى يمكن الاستفادة من هذا التجميع في سياسة الوصول إلى الشبكة.

في هذا التمرين، يتم تكوين تعريفات الأجهزة المطلوبة لمختبرك.

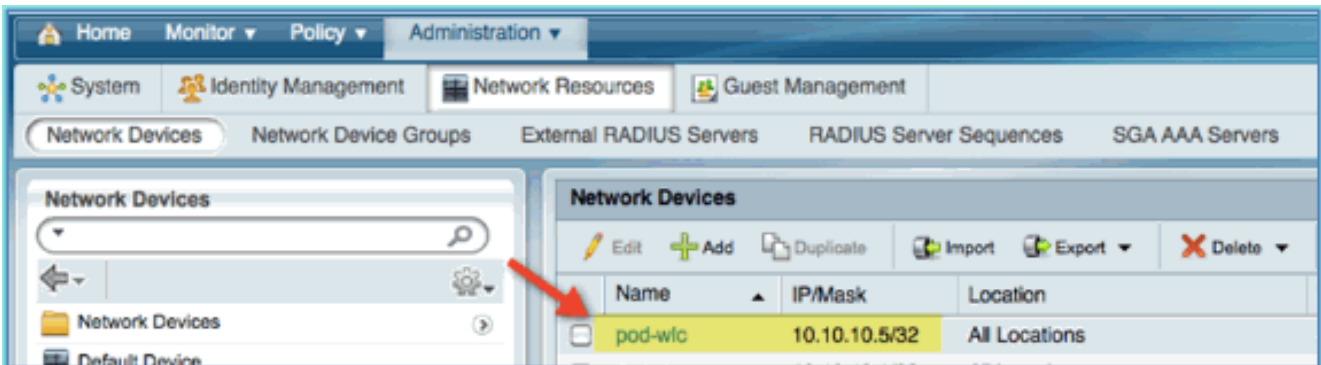
أكمل الخطوات التالية:

1. من ISE انتقل إلى الإدارة < موارد الشبكة > أجهزة الشبكة.





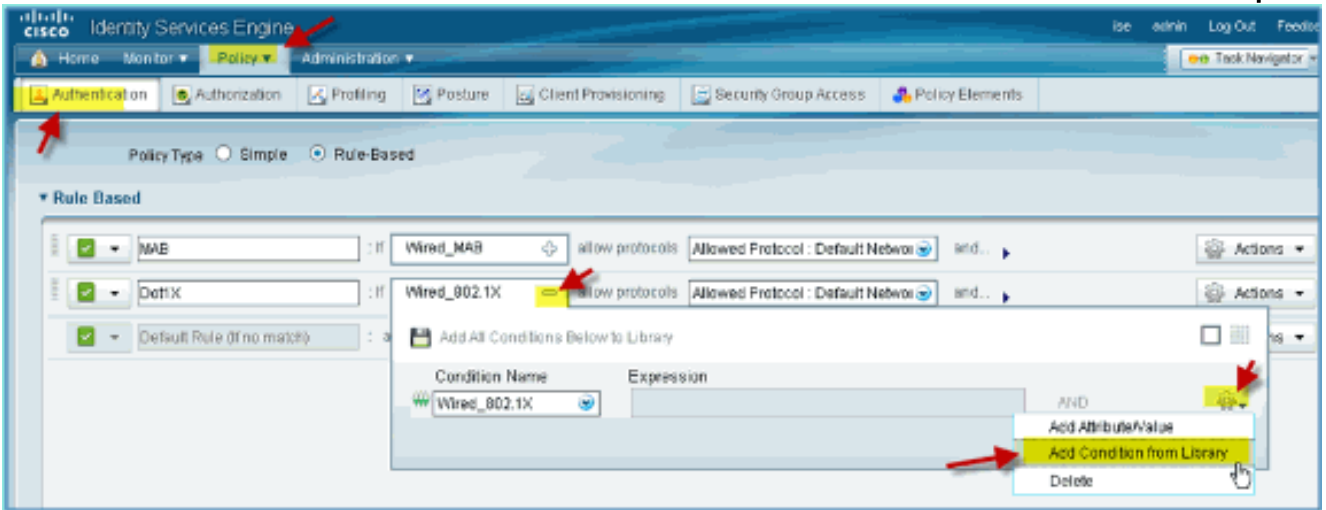
2. من أجهزة الشبكة، انقر فوق إضافة. دخلت عنوان، قناع تدقيق صحة هوية إعداد، بعد ذلك دخلت "cisco" ل يشارك سر.
3. قم بحفظ إدخال WLC، وتأكد وحدة التحكم في القائمة.



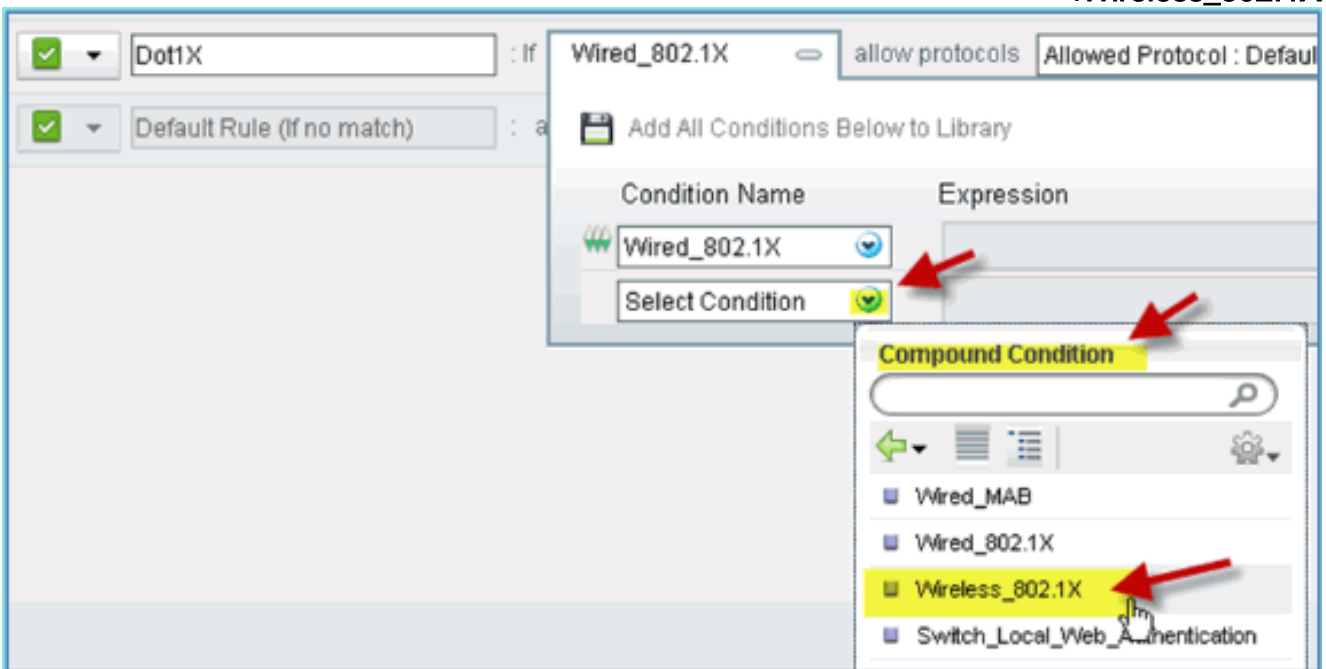
## تكوين ISE للمصادقة اللاسلكية

يلزم تكوين ISE لمصادقة عملاء شبكة 802.1x اللاسلكية واستخدام Active Directory كمخزن للهوية. أكمل الخطوات التالية:

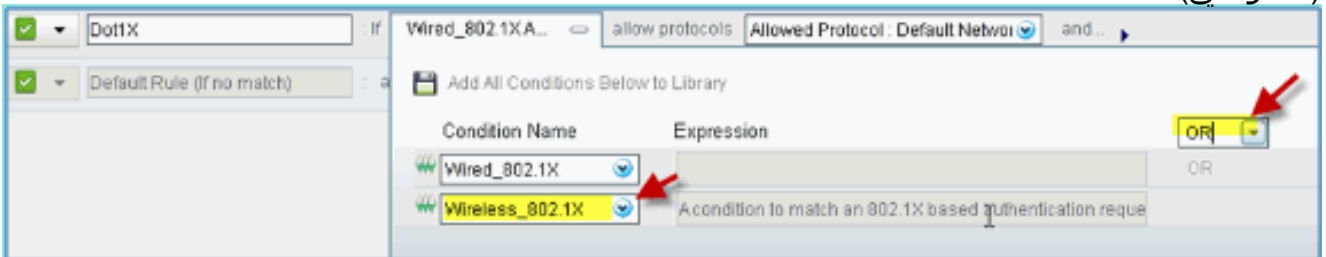
1. من ISE انتقل إلى السياسة < المصادقة.
2. انقر لتوسيع النقطة 1x > Wired\_802.1X (-).
3. انقر على أيقونة العتاد لإضافة حالة من

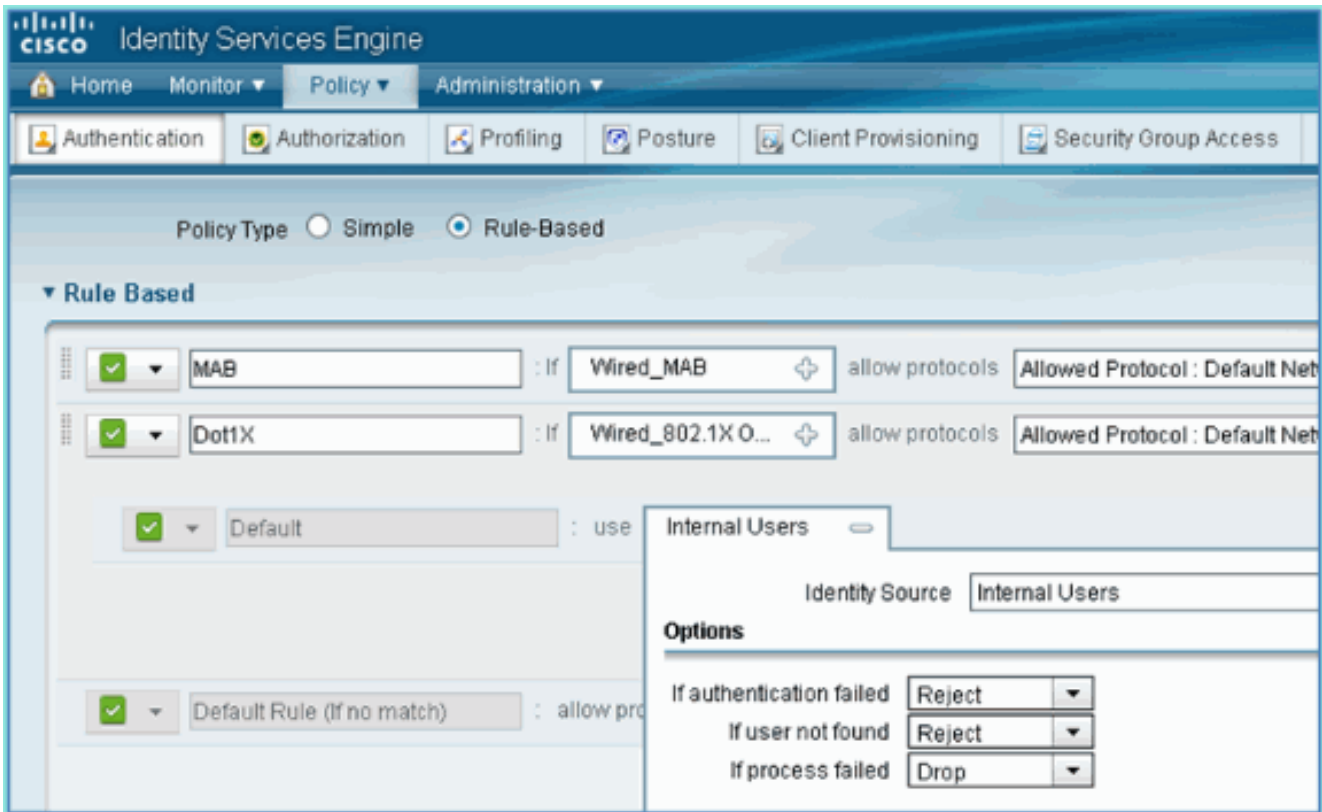


4. من القائمة المنسدلة لتحديد الشرط، أختار شرط مركب < Wireless\_802.1X



5. قم بتعيين الشرط Express إلى OR.  
6. قم بتوسيع خيار بعد السماح بالبروتوكولات، وقبول المستخدمين الداخليين الافتراضيين (الافتراضي).





7. أترك كل شيء آخر في الوضع الافتراضي. انقر فوق حفظ" لإكمال الخطوات.

## وحدة التحكم في شبكة LAN اللاسلكية ل Bootstrap

### توصيل WLC بشبكة

كما يتوفر دليل نشر وحدة تحكم الشبكة المحلية (LAN) اللاسلكية Cisco 2500 في [دليل نشر وحدة التحكم اللاسلكية من السلسلة Cisco 2500 Series](#).

### تكوين وحدة التحكم باستخدام معالج بدء التشغيل

```
(Cisco Controller)
Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
:(no configuration loaded System Name [Cisco_d9:24:44] (31 characters max --
ISE-Podx Enter Administrative User Name (24 characters max): admin
Enter Administrative Password
to 24 characters): Cisco123 3)
Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: no
.Warning! The default WLAN security policy requires a RADIUS server
.Please see documentation for more details
```

```
Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
    Enable Auto-RF [YES][no]: yes
Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
!Configuration saved
...Resetting system with new configuration
    .Restarting system
```

## تكوين المحول المجاور

يتم توصيل وحدة التحكم بمنفذ Ethernet على المحول المجاور (Fast Ethernet 1). يتم تكوين منفذ المحول المجاور كخط اتصال 802.1Q ويسمح لجميع شبكات VLAN على خط الاتصال. ال VLAN أهلي طبيعي 10 يسمح الإدارة قارن من ال WLC أن يكون ربطت.

ال 802.1Q مفتاح تشكيل ميناء كما يلي:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

## إضافة خوادم المصادقة (ISE) إلى WLC

يلزم إضافة ISE إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتمكين 802.1X وميزة CoA لنقاط النهاية اللاسلكية.

أكمل الخطوات التالية:

1. افتح مستعرض، ثم اتصل ب WLC pod (باستخدام HTTP الآمن) < https://wlc.
2. انتقل إلى التأمين < المصادقة < جديد.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

### RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret \*\*\*\*\*

Confirm Shared Secret \*\*\*\*\*

Key Wrap  (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  Enable

Management  Enable

IPSec  Enable

3. قم بإدخال القيم التالية: عنوان IP للخادم: 10.10.10.70 (مهمة الفحص) سر مشترك: Cisco دعم RFC 3576 CoA): ممكن (افتراضي) كل شيء آخر: الافتراضي
4. انقر فوق تطبيق للمتابعة.
5. حدد محاسبة RADIUS < إضافة جديد.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT C

### Security RADIUS Accounting Servers > New

AAA

- General
- RADIUS
  - Authentication
  - Accounting
  - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

Local EAP

Priority Order

Certificate

Server Index (Priority) 2

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret \*\*\*\*\*

Confirm Shared Secret \*\*\*\*\*

Port Number 1813

Server Status Enabled

Server Timeout 2 seconds

Network User  Enable

IPSec  Enable

6. قم بإدخال القيم التالية: عنوان IP للخادم: 10.10.10.70 سر مشترك: Cisco كل شيء آخر: الافتراضي
7. طغقة يطبق، بعد ذلك ينقذ التشكيل ل ال WLC.

## إنشاء الواجهة الديناميكية لموظف WLC

أتمت هذا steps in order to أضفت قارن حركي جديد ل ال WLC وخورطتها إلى الموظف VLAN:

1. من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى وحدة التحكم < الواجهات. ثم انقر فوق

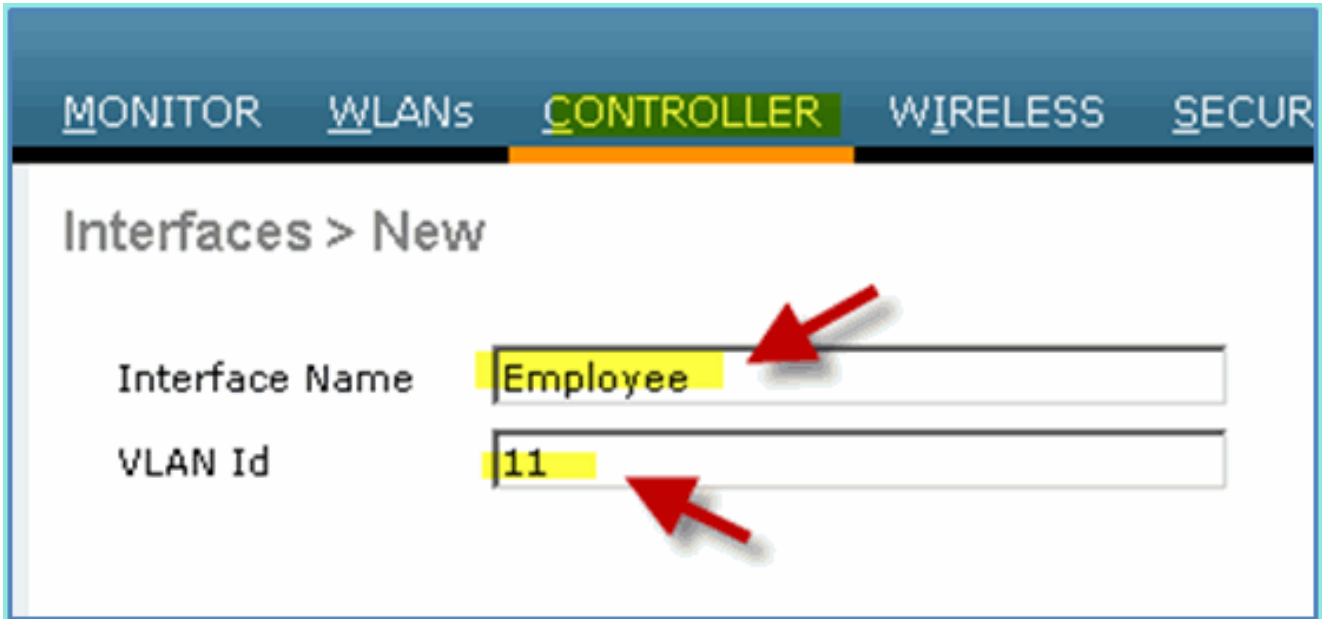
جديد.



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
<a href="#">management</a>	untagged	10.10.10.5	Static	Enabled
<a href="#">virtual</a>	N/A	1.1.1.1	Static	Not Supported

2. من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى وحدة التحكم < الواجهات. أدخل ما يلي: اسم الواجهة: الموظف معرف شبكة: VLAN:

11



Interface Name: Employee

VLAN Id: 11

3. أدخل ما يلي لواجهة الموظف: رقم المنفذ: 1 معرف شبكة: VLAN: 11 عنوان IP: 10.10.11.5 NetMask:

255.255.255.0 البوابة: 10.10.11.1 بروتوكول DHCP:

10.10.10.10

## Configuration

Quarantine   
Quarantine Vlan Id

## Physical Information

Port Number   
Backup Port   
Active Port   
Enable Dynamic AP Management

## Interface Address

VLAN Identifier   
IP Address   
Netmask   
Gateway

## DHCP Information

Primary DHCP Server   
Secondary DHCP Server

4. تأكد من إنشاء الواجهة الديناميكية للموظف الجديد.

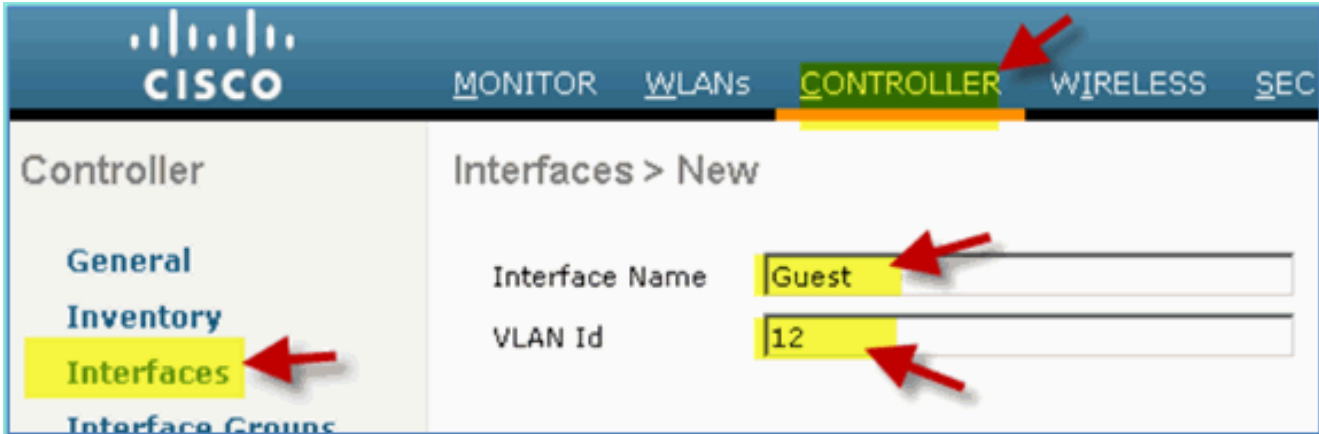
CISCO		MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMA
Controller	Interfaces							
General								
Inventory								
Interfaces								
Interface Groups								
Multicast								
	Interface Name	VLAN Identifier	IP Address	Interface Type				
	employee	11	10.10.11.5	Dynamic				
	management	untagged	10.10.10.5	Static				
	virtual	N/A	1.1.1.1	Static				

## إنشاء واجهة ديناميكية لضيف WLC

أتمت هذا steps in order to أضفت قارن ديناميكي جديد ل ال WLC وخرائطها إلى Guest VLAN:

1. من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى وحدة التحكم < الواجهات >. ثم انقر فوق جديد.

2. من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى وحدة التحكم < الواجهات >. أدخل ما يلي: اسم الواجهة: الضيفمعرف شبكة: VLAN: 12



3. دخلت هذا ل ضيف قارن: رقم المنفذ: 1 معرف شبكة: VLAN: 12 عنوان NetMask: 10.10.12.5 IP:  
DHCP: 10.10.12.1 البوابة: 255.255.255.0  
10.10.10.10



## Configuration

Quarantine

Quarantine Vlan Id

## Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

## Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

## DHCP Information

Primary DHCP Server

Secondary DHCP Server

## Access Control List

ACL Name

*Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.*

4. تأكد من إضافة واجهة الضيف.

CISCO				
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS				
Controller	Interfaces			
General				
Inventory				
Interfaces				
Interface Groups				
Multicast				
Internal DHCP Server				
Interface Name	VLAN Identifier	IP Address	Interface Type	
employee	11	10.10.11.5	Dynamic	
quest	12	10.10.12.5	Dynamic	
management	untagged	10.10.10.5	Static	
virtual	N/A	1.1.1.1	Static	

## إضافة WLAN 802.1x

من شريط التمهيد الأولي لـ WLC، قد يكون هناك شبكة WLAN افتراضية تم إنشاؤها. إذا كان الأمر كذلك، فعليك بتعديله أو إنشاء شبكة WLAN جديدة لدعم مصادقة 802.1X اللاسلكية كما هو موضح في الدليل.

أكمل الخطوات التالية:

1. من WLC، انتقل إلى WLAN < إنشاء

جديد.



2. بالنسبة للشبكة المحلية اللاسلكية (WLAN)، أدخل ما يلي: اسم ملف التعريف: pod1xSSID: نفس



3. لإعدادات WLAN < علامة التبويب "عام"، أستخدم ما يلي: سياسة الراديو: الكلالواجهة/المجموعة: الإدارة كل شيء آخر، الافتراضي

## WLANs &gt; Edit 'pod1x'

## General

## Security

## QoS

## Advanced

Profile Name pod1x

Type WLAN

SSID pod1x

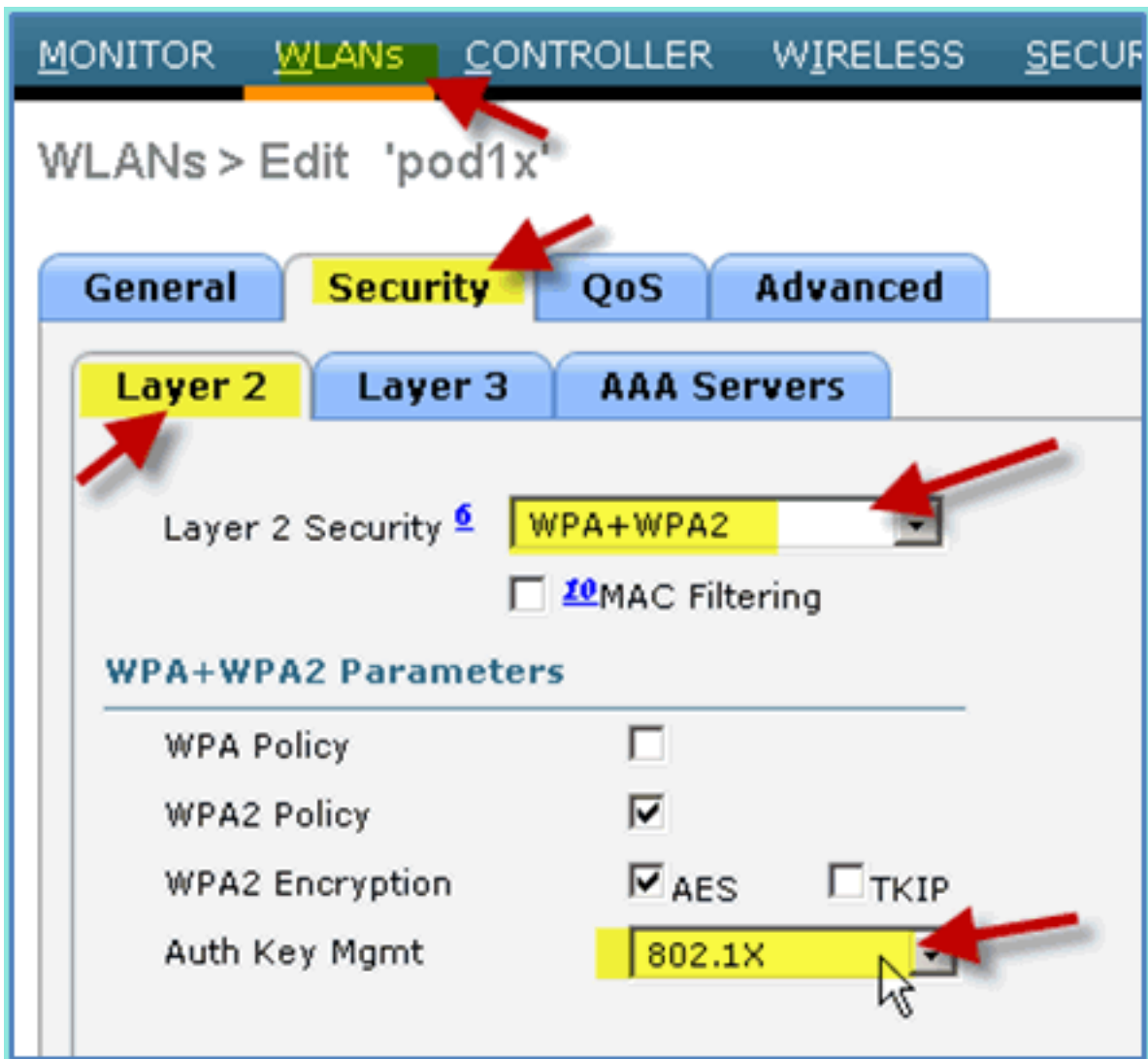
Status  EnabledSecurity Policies [WPA2][Auth(802.1X)]  
(Modifications done under security tab w

Radio Policy All

Interface/Interface Group(G) management

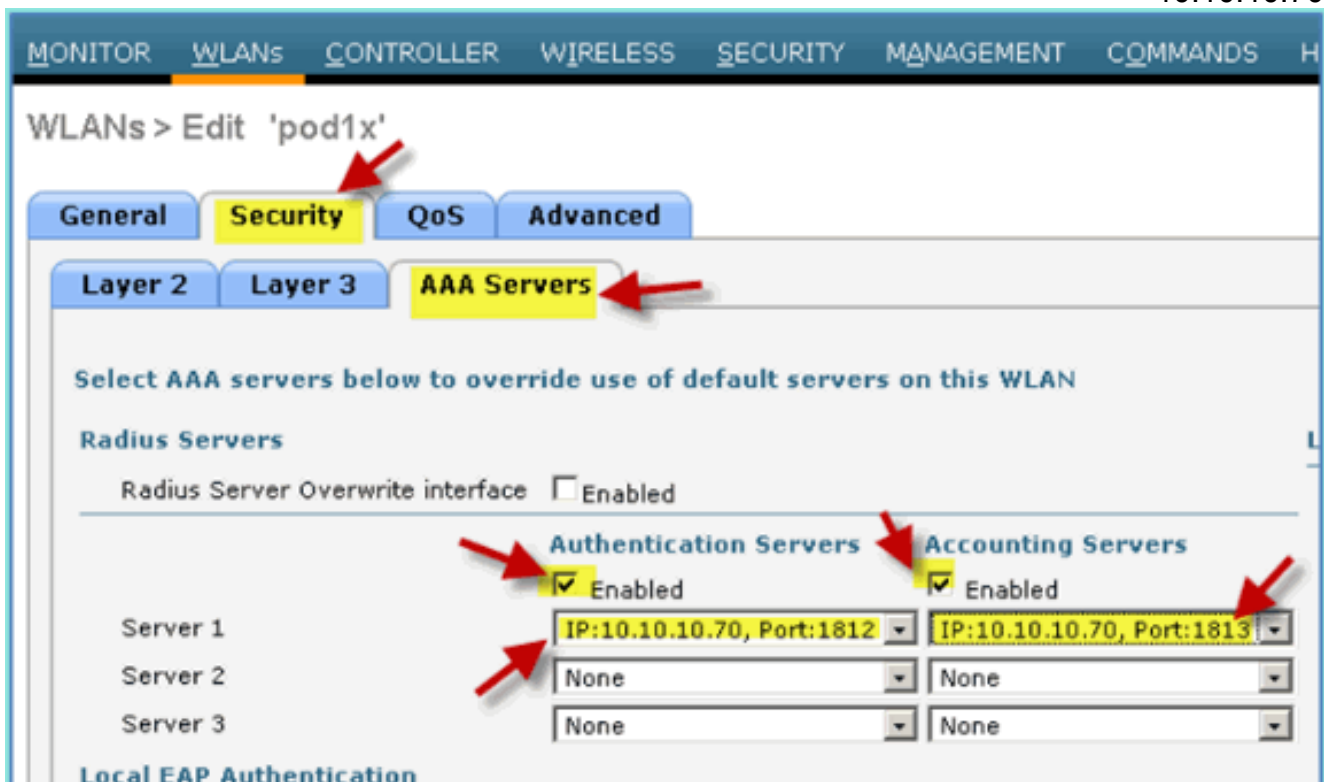
Multicast Vlan Feature  EnabledBroadcast SSID  Enabled

4. للشبكة المحلية اللاسلكية (WLAN) < صفحة التأمين < الطبقة 2، قم بضبط التالي: تأمين الطبقة  
WPA+WPA2:2 سياسة / تشفير WPA2: ممكن / إدارة مفتاح المصادقة:



802.1X

5. بالنسبة للشبكة المحلية اللاسلكية (WLAN) < علامة التبويب "أمان" > خوادم AAA، قم بتعيين ما يلي: واجهة الكتابة فوق خادم الراديو: معطلة خوادم المصادقة/المحاسبة: ممكنة الخادم 1: 10.10.10.70



6. بالنسبة للشبكة المحلية اللاسلكية (WLAN) < علامة التبويب خيارات متقدمة، قم بتعيين ما يلي: السماح بتجاوز

AAA: ممكن حالة NAC RADIUS  
(محدد)

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'pod1x'

General Security QoS **Advanced**

**Allow AAA Override**  Enabled

Coverage Hole Detection  Enabled

Enable Session Timeout  1800  
Session Timeout (secs)

Aironet IE  Enabled

Diagnostic Channel  Enabled

IPv6 Enable

Override Interface ACL

P2P Blocking Action

Client Exclusion  Enabled 60  
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling  Enabled

DHCP

DHCP Server  Override

DHCP Addr. Assignment  Required

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select

7. رجوع إلى الشبكة المحلية اللاسلكية (WLAN) < علامة التبويب "عام" > تمكين شبكة WLAN (خانة الاختيار).

WLANs > Edit 'pod1x'

**General** Security QoS Advanced

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

## اختبار الواجهات الديناميكية WLC

تحتاج إلى إجراء فحص سريع لواجهات الموظفين والضيوف الصحيحة. أستخدم أي جهاز للاقتران بشبكة WLAN، ثم قم بتغيير تعيين واجهة WLAN.

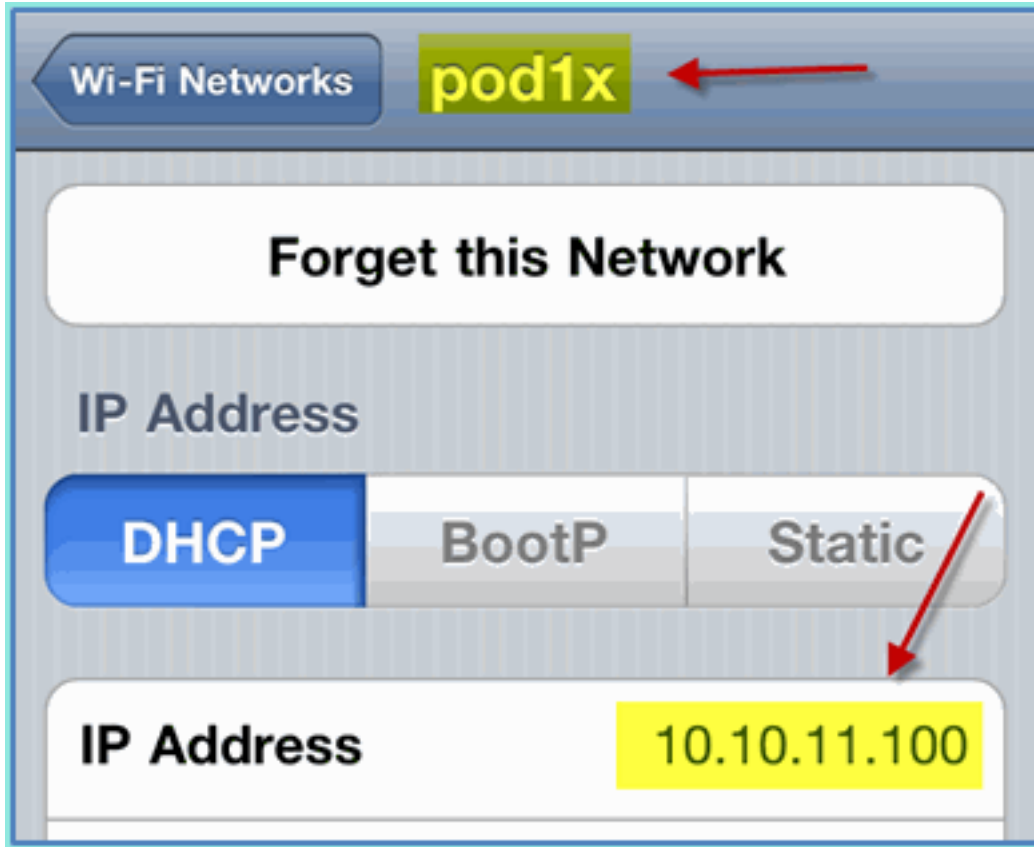
1. من WLC، انتقل إلى WLAN > WLANs. انقر لتحرير SSID الآمن الذي تم إنشاؤه في التمرين السابق.
2. قم بتغيير مجموعة الواجهة/الواجهة إلى الموظف، ثم انقر فوق تطبيق.

The screenshot shows the Cisco WLAN configuration page for a profile named 'pod1x'. The interface includes a navigation menu on the left with 'WLANs' and 'Advanced' options. The main content area has tabs for 'General', 'Security', 'QoS', and 'Advanced', with 'General' selected. The configuration details are as follows:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security to
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	employee
Broadcast SSID	guest management <input checked="" type="checkbox"/> Enabled

Red arrows point to the 'WLANs' menu item, the 'WLANs' tab, the 'General' tab, and the 'management' dropdown menu.

3. إن شكلت بشكل صحيح، يستلم أداة عنوان من الموظف (10.10.11.0/24 VLAN). يوضح هذا المثال جهاز iOS الذي يحصل على عنوان IP



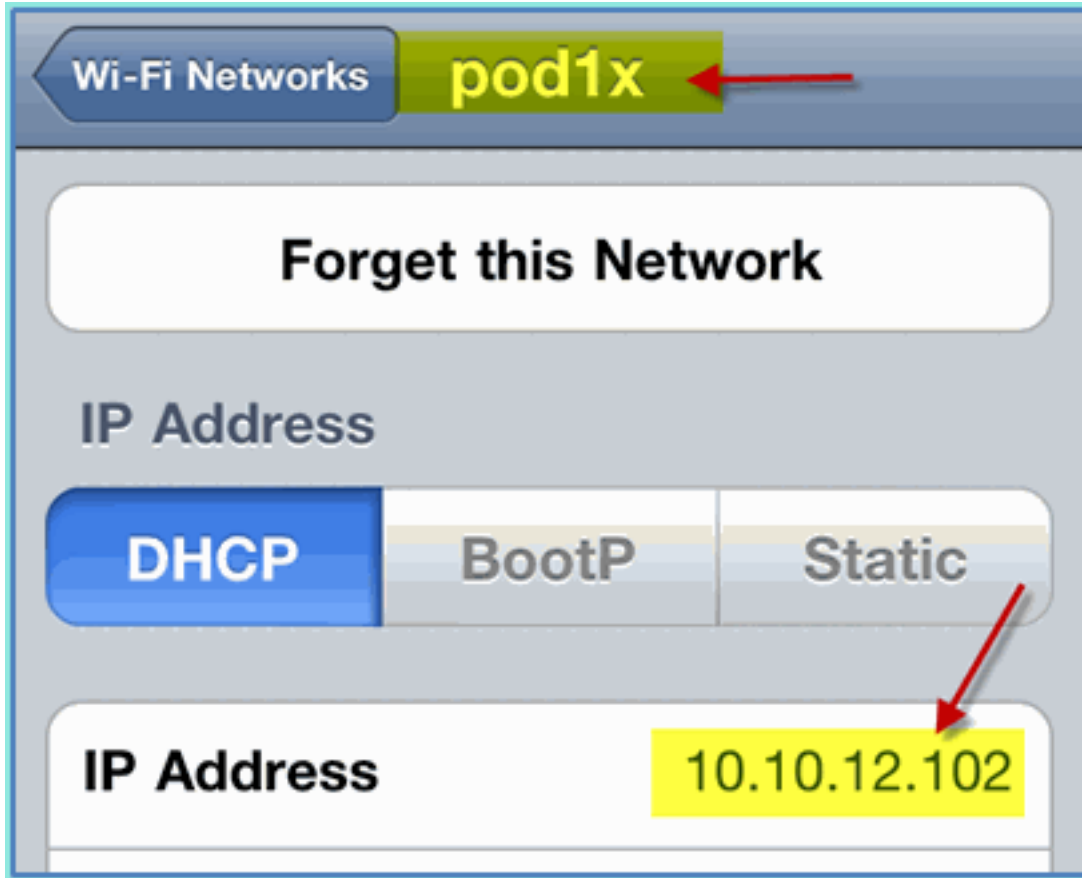
جديد.  
4. بمجرد تأكيد الواجهة السابقة، قم بتغيير تعيين واجهة شبكة WLAN إلى Guest، ثم انقر فوق تطبيق.



The screenshot displays the Cisco WLC configuration interface. At the top, the navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar shows a tree view with 'WLANs' and 'Advanced' options. The main content area is titled 'WLANs > Edit 'pod1x''. Below this, there are four tabs: 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active, showing the following configuration details:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under se
Radio Policy	All
Interface/Interface Group(G)	quest
Multicast Vlan Feature	quest
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

5. إن شكلت بشكل صحيح، يستلم أداة عنوان من الضيف (10.10.12.0/24 VLAN). يوضح هذا المثال جهاز iOS الذي يحصل على عنوان IP



جديد.

6. هام: قم بتغيير تعيين الواجهة مرة أخرى إلى الإدارة الأصلية.
7. طققة يطبق ويحفظ التشكيل ل ال WLC.

## المصادقة اللاسلكية لنظام التشغيل (iOS (iPhone/iPad

أربط عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال SSID مصدق عليه لمستخدم داخلي (أو مستخدم AD مدمج) باستخدام جهاز يعمل بنظام التشغيل iOS مثل iPhone أو iPad أو iPod. تخطي هذه الخطوات إذا لم تكن قابلة للتطبيق.

1. على جهاز iOS، انتقل إلى إعدادات WLAN. قم بتمكين WiFi ثم حدد SSID 802.1X الذي تم إنشاؤه في القسم السابق.
2. توفير هذه المعلومات للاتصال: اسم المستخدم: موظف (داخلي - موظف) أو مقاول (داخلي - مقاول) كلمة



المرون: XXXX



3. انقر لقبول شهادة ISE.
4. تأكد من أن جهاز iOS يحصل على عنوان IP من واجهة الإدارة



5. على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) < مراقبة > العملاء، تحقق من معلومات نقطة النهاية بما في ذلك الاستخدام والحالة ونوع EAP.

(VLAN10)

Monitor

- Summary
- ▶ Access Points
- ▶ Cisco CleanAir
- ▶ Statistics
- ▶ CDP
- ▶ Rogues
- Clients
- Multicast

Clients > Detail



Client Properties

MAC Address	5c:59:48:40:82:8d
IP Address	10.10.10.102
Client Type	Regular
User Name	aduser
Port Number	1
Interface	management
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN
AAA Override ACL Name	none

6. وبالمثل، يمكن توفير معلومات العميل بواسطة Monitor > ISE < صفحة المصادقة.

Time	Status	Details	Username	Endpoint ID	Network Device	Authorization Profiles	Ident
Jul 13,11 04:39:36.573 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
Jul 13,11 04:38:46.285 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	

7. انقر فوق رمز التفاصيل للتنقل لأسفل إلى جلسة العمل للحصول على معلومات تفصيلية حول جلسة العمل.

**AAA Protocol > RADIUS Authentication Detail**

RADIUS Audit Session ID : 0a0a0a050000000d4e1e2a45  
 AAA session ID : ise/99967658/11  
 Date : July 13,2011

Generated on July 13, 2011 4:41:11 PM PDT

**Authentication Summary**

Logged At: July 13,2011 4:39:36.573 PM  
**RADIUS Status: Authentication succeeded**  
 NAS Failure:  
 Username: aduser  
 MAC/IP Address: 5C:59:48:40:82:8D  
 Network Device: WLC : 10.10.10.5  
 Allowed Protocol: Default Network Access  
 Identity Store: AD1  
 Authorization Profiles: PermitAccess  
 SGA Security Group:  
**Authentication Protocol : PEAP(EAP-MSCHAPv2)**

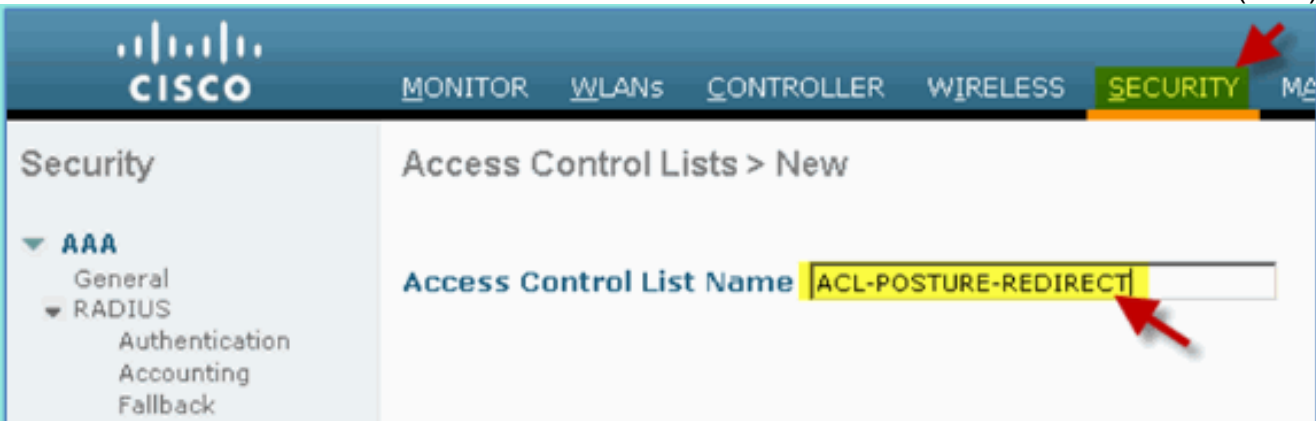
## إضافة قائمة التحكم في الوصول (ACL) لإعادة توجيه الوضع إلى WLC

تم تكوين قائمة التحكم في الوصول (ACL) لإعادة توجيه الوضع على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، حيث يستخدم ISE لتقييد العميل للوضع. تتيح قائمة التحكم في الوصول (ACL) بشكل فعال وعلى أقل تقدير حركة المرور بين ISE. يمكن إضافة القواعد الاختيارية في قائمة التحكم في الوصول (ACL) هذه إذا لزم الأمر.

1. انتقل إلى WLC < الأمان < قوائم التحكم في الوصول < قوائم التحكم في الوصول. طقطقت جديد.



2. توفير اسم (ACL-Posture-Redirect) لقائمة التحكم في الوصول (ACL).



3. انقر فوق إضافة قاعدة جديدة لقائمة التحكم في الوصول (ACL) الجديدة. قم بتعيين القيم التالية إلى تسلسل قائمة التحكم بالوصول (#1) ACL. انقر فوق تطبيق عند الانتهاء. المصدر: أيا الوجهة: عنوان IP 10.10.10.70، 255.255.255.255 البروتوكول: أيا العمل: الترخيص



MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

### Access Control Lists > Rules > Edit

Sequence: 1

Source: Any

Destination: IP Address

IP Address: 10.10.10.70

Netmask: 255.255.255.255

Protocol: Any

DSCP: Any

Direction: Any

Action: Permit

4. تم إضافة تسلسل التأكيد.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. انقر فوق إضافة قاعدة جديدة. قم بتعيين القيم التالية إلى تسلسل قائمة التحكم بالوصول (ACL) #2. انقر فوق تطبيق عند الانتهاء. المصدر: عنوان IP 10.10.10.70، الوجهة: أيا لبروتوكول: أيا لعمل: الترخيص

Sequence: 2

Source: IP Address

IP Address: 10.10.10.70

Netmask: 255.255.255.255

Destination: Any

Protocol: Any

DSCP: Any

Direction: Any

Action: Permit

6. تم إضافة تسلسل التأكيد.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any

7. قم بتعيين القيم التالية إلى تسلسل قائمة التحكم بالوصول (#3) ACL. انقر فوق تطبيق عند الانتهاء. المصدر: أيالوجهة: أيالبروتوكول: UDPمنفذ المصدر: DNSأىغاية ميناء: أيالعمل:

Sequence: 3

Source: Any

Destination: Any

Protocol: UDP

Source Port: DNS

Destination Port: Any

DSCP: Any

Direction: Any

Action: Permit

الترخيص

8. تم إضافة تسلسل التأكيد.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<a href="#">1</a>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
<a href="#">2</a>	Permit	0.0.0.0 /	255.255.255.255 /	Any	Any	Any	Any	Any
<a href="#">3</a>	Permit	10.10.10.70 /	0.0.0.0 /	UDP	DNS	Any	Any	Any

9. انقر فوق إضافة قاعدة جديدة. قم بتعيين القيم التالية إلى تسلسل قائمة التحكم بالوصول (#4) ACL. انقر فوق تطبيق عند الانتهاء. المصدر: أيالوجهة: أيالبروتوكول: UDPمنفذ المصدر: أيغاية ميناء: أيالعمل: الترخيص

Sequence

Source

Destination

Protocol

Source Port

Destination Port

DSCP

Direction

Action

10. تم إضافة تسلسل التأكيد.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<a href="#">1</a>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
<a href="#">2</a>	Permit	0.0.0.0 /	255.255.255.255 /	Any	Any	Any	Any	Any
<a href="#">3</a>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
<a href="#">3</a>	Permit	255.255.255.255 /	0.0.0.0 /	Any	Any	Any	Any	Any
<a href="#">3</a>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
<a href="#">3</a>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
<a href="#">4</a>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Any
<a href="#">4</a>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Any

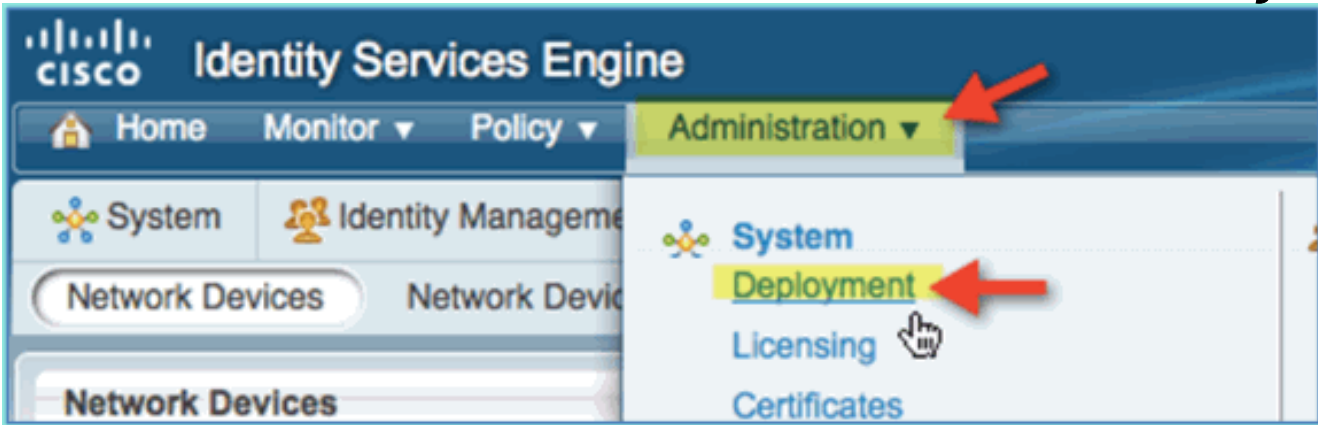
11. حفظ تكوين WLC الحالي.

## تمكين إختبارات إنشاء ملف التعريف على ISE

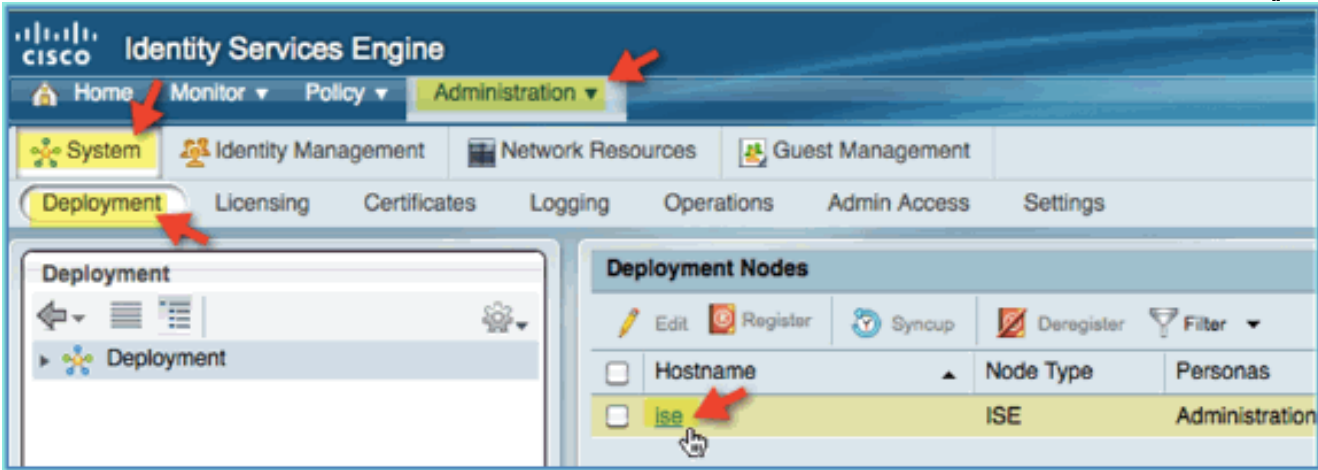
يلزم تكوين ISE على هيئة إختبارات لتخصيص نقاط النهاية بشكل فعال. بشكل افتراضي، تلك الخيارات معطلة. يوضح

هذا القسم كيفية تكوين ISE لتكون تجارب.

1. من إدارة ISE، انتقل إلى الإدارة < النظام > النشر.



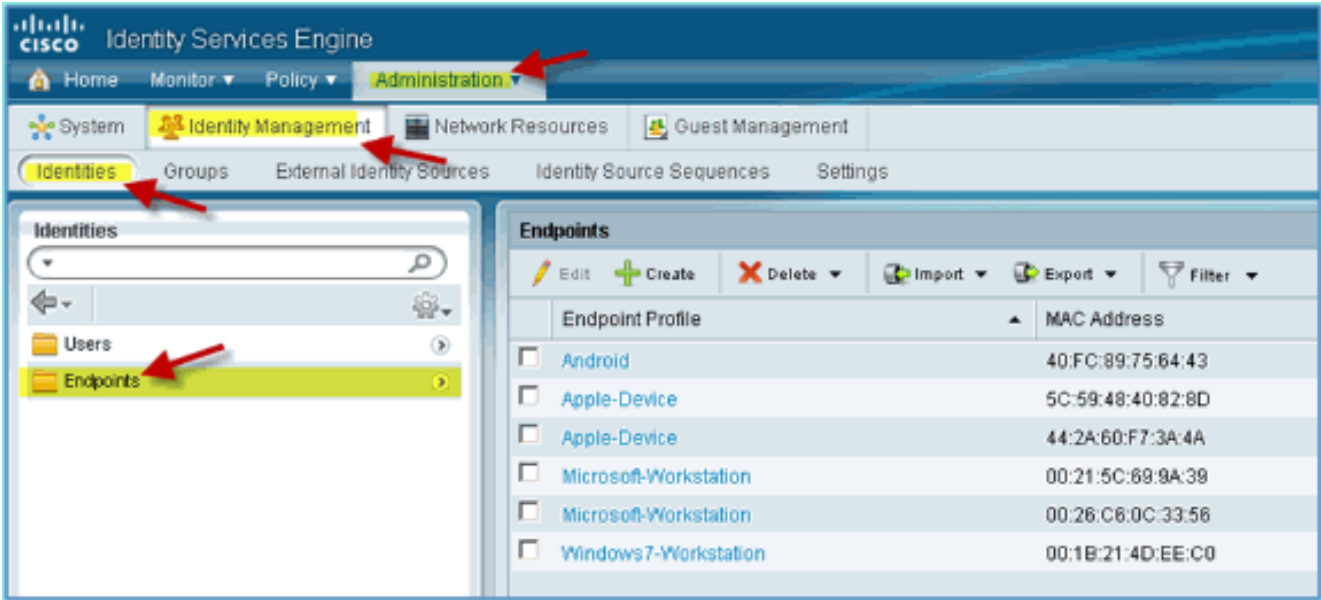
2. أختار ISE. قطعة يحرق ISE مضيف.



3. من صفحة تحرير العقدة، حدد تكوين إنشاء ملفات التعريف ثم قم بتكوين ما يلي: DHCP: ممكن، الكل (أو الافتراضي) DHCPspan: ممكن، الكل (أو تقصير) http: ممكن، الكل (أو الافتراضي) RADIUS: ممكن، غير متاح DNS: ممكن، غير متوفر

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main navigation bar includes 'Home', 'Monitor', 'Policy', and 'Administration'. The 'Administration' tab is active, and the 'Deployment' sub-tab is selected. The left sidebar shows the 'Deployment' menu. The main content area is titled 'Edit Node' and shows the 'Profiling Configuration' section. The configuration is organized into sections for DHCP, DHCPSPAN, HTTP, RADIUS, and DNS. Each section has a checked checkbox and a dropdown menu for 'Interface' set to 'All'. The DHCP section also has a 'Port' field set to 67 and a 'Description' field set to 'DHCP'. The DHCPSPAN section has a 'Description' field set to 'DHCPSPAN'. The HTTP section has a 'Description' field set to 'HTTP'. The RADIUS section has a 'Description' field set to 'RADIUS'. The DNS section is partially visible. At the bottom, there are 'Save' and 'Reset' buttons. Red arrows point to the 'Interface' dropdown menu in each section.

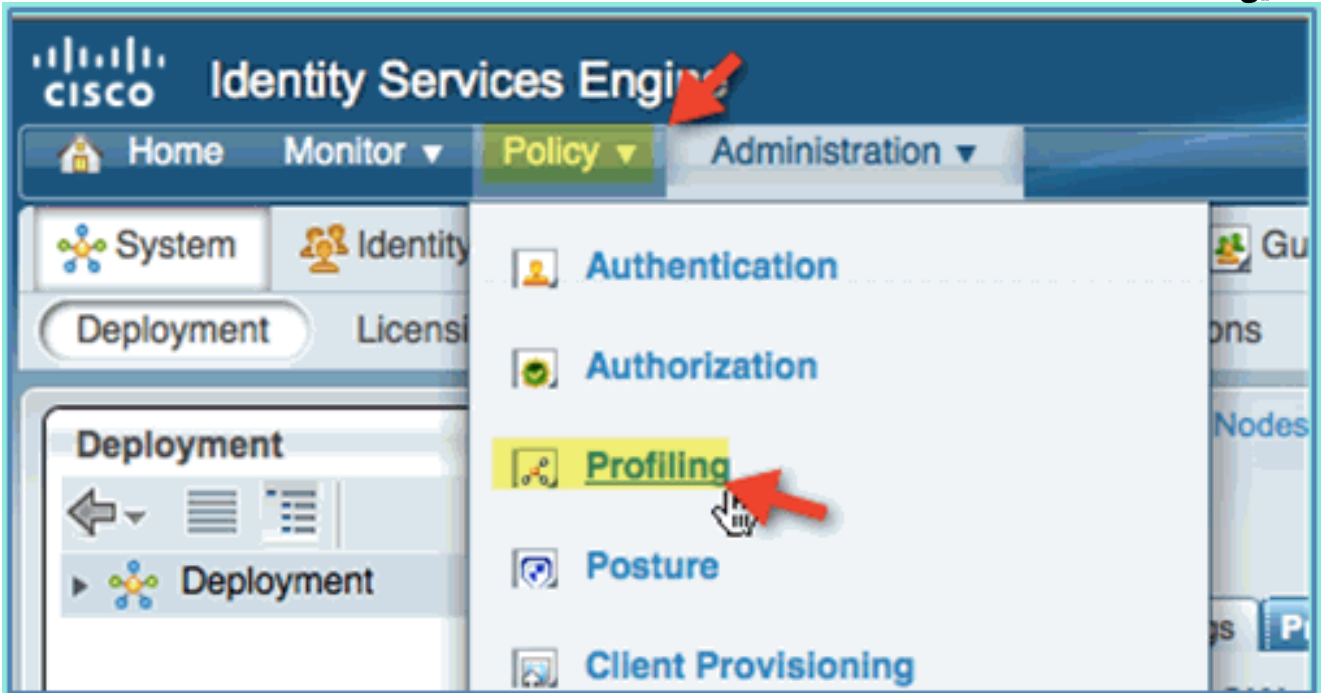
4. إعادة ربط الأجهزة (iPhone/iPads/Droids/Mac، وما إلى ذلك).
5. تأكيد هويات نقاط نهاية ISE. انتقل إلى إدارة < إدارة الهوية > الهويات. انقر فوق نقاط النهاية لسرد ما تم توضيحه. ملاحظة: البيانات الأولية مقدمة من اختبارات RADIUS.



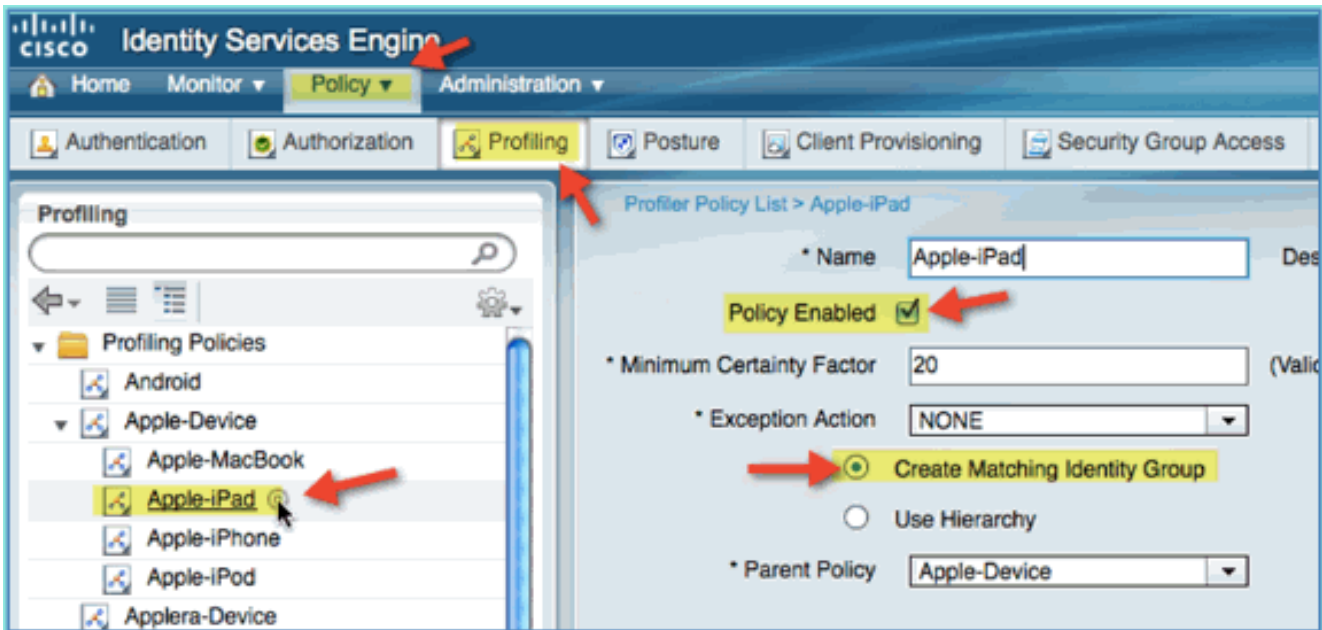
## تمكين نهج ملف تعريف ISE للأجهزة

وخارج هذا المربع، يوفر ISE مكتبة من مختلف ملفات تعريف نقاط النهاية. أكمل الخطوات التالية لتمكين توصيفات الأجهزة:

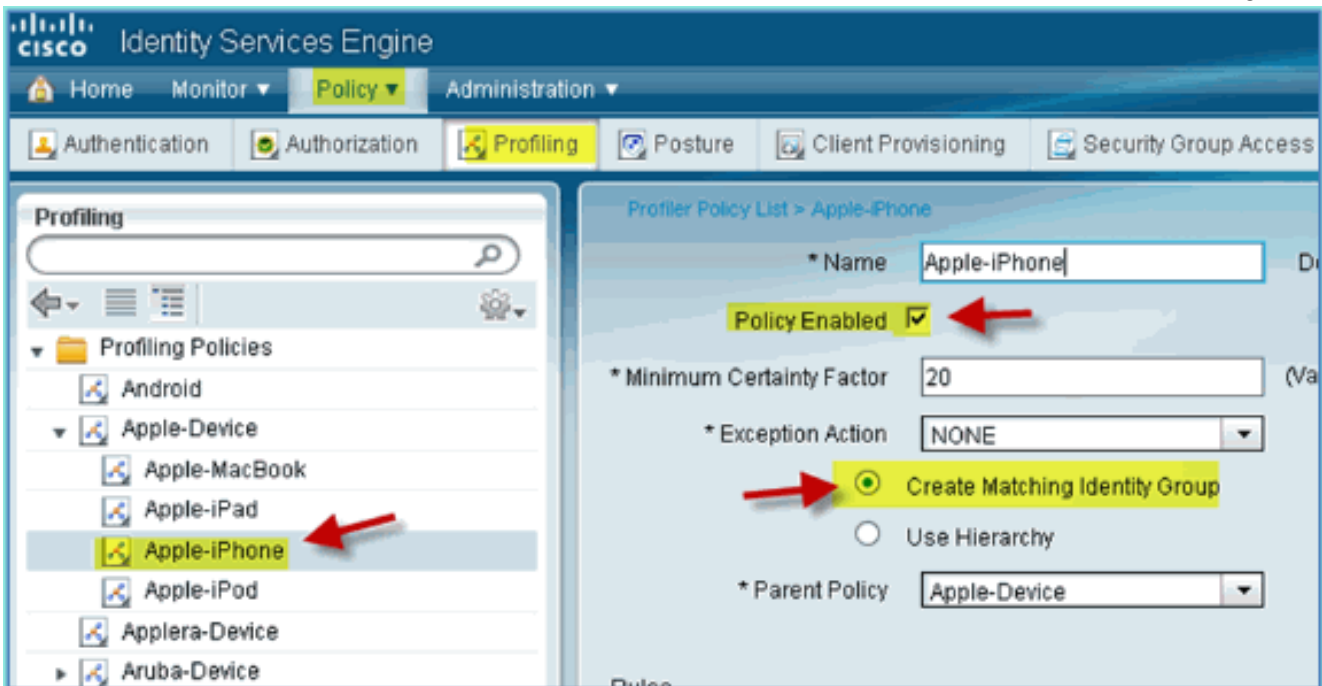
1. من ISE، انتقل إلى السياسة < التحليل.



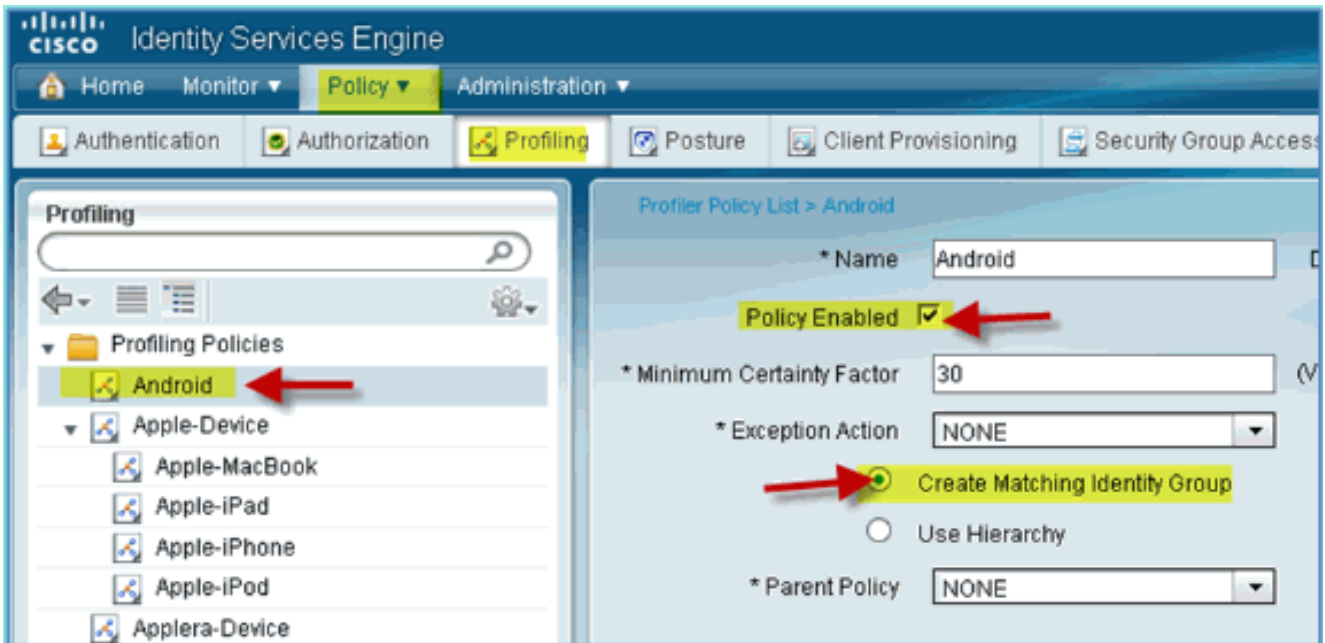
2. من الجزء الأيسر، قم بتوسيع نهج تحديد الملفات.
3. انقر فوق جهاز Apple > Apple iPad، واضبط ما يلي: تم تمكين النهج: ممكن إنشاء مجموعة هوية مطابقة: محددة



4. انقر فوق جهاز Apple > Apple iPhone، قم بتعيين ما يلي: تم تمكين النهج: ممكن إنشاء مجموعة هوية مطابقة: محددة



5. طقطقت Android، ثبت التالي: تم تمكين النهج: ممكن إنشاء مجموعة هوية مطابقة: محددة



## ملف تعريف تخويل ISE لإعادة توجيه اكتشاف الوضع

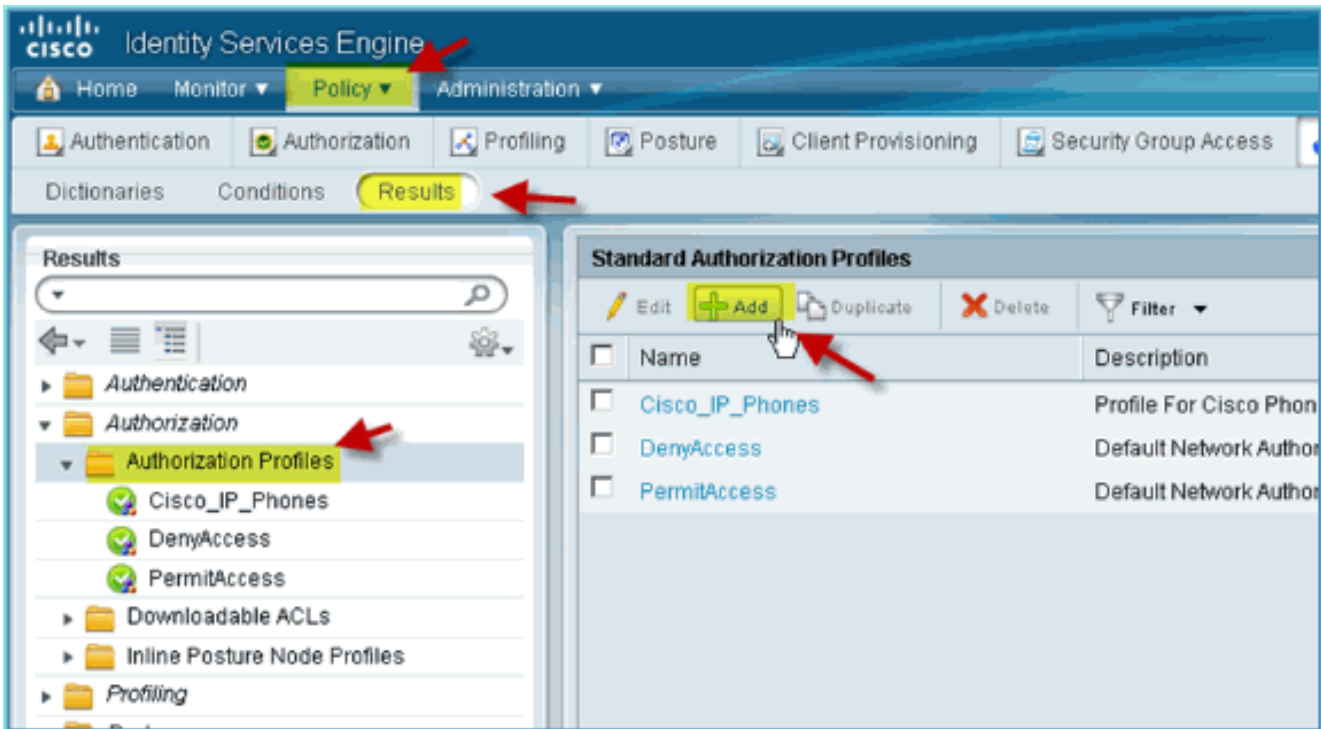
أكمل هذه الخطوات لتكوين إعادة توجيه وضع نهج التخويل الذي يسمح بإعادة توجيه الأجهزة الجديدة إلى ISE لاكتشاف المناسب والتنميط:

1. من ISE، انتقل إلى السياسة < عناصر السياسة > التناج.

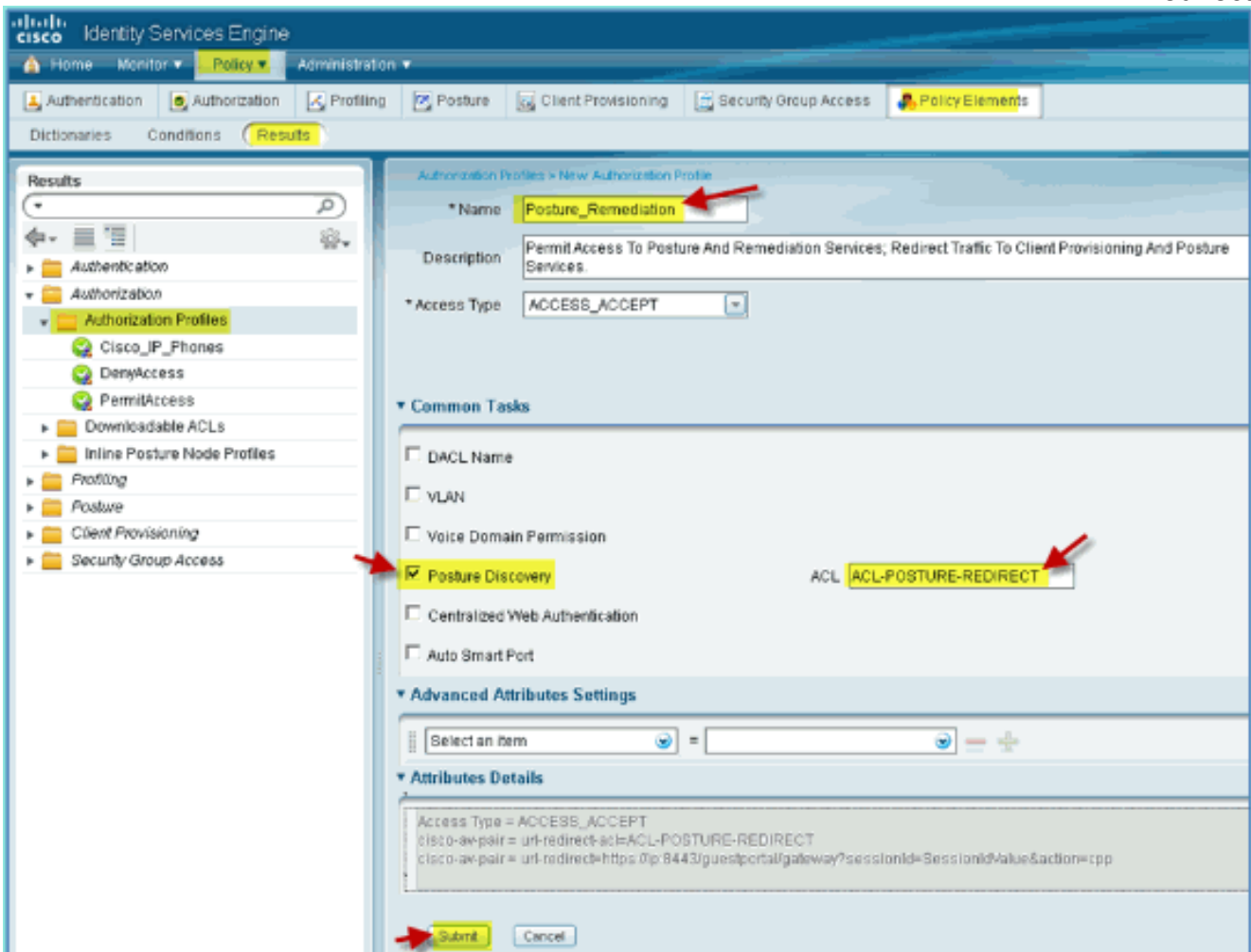




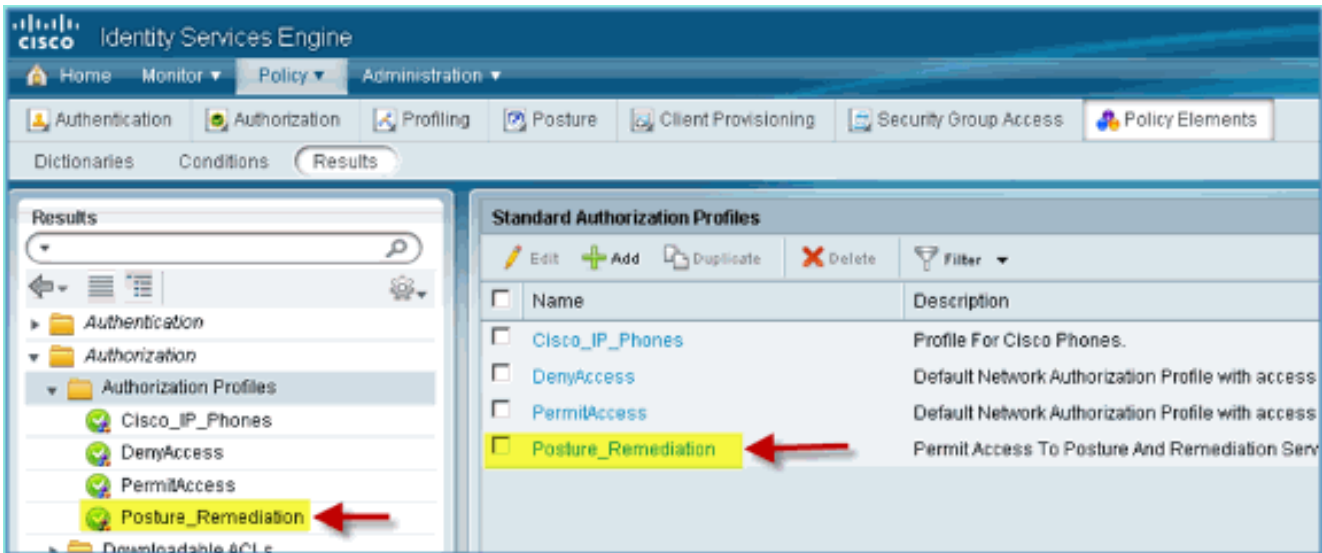
2. توسيع التفويض. انقر على توصيفات التحويل (اللوحة اليسرى) وانقر إضافة.



3. قم بإنشاء ملف تعريف التحويل على النحو التالي: الاسم: Posture\_remediation نوع الوصول: access\_accept الأدوات الشائعة: إكتشاف الوضع، ممكن اكتشاف الوضع، قائمة التحكم في الوصول (-ACL) Posture-Redirect



4. انقر فوق إرسال لإكمال هذه المهمة.  
5. تأكد من إضافة ملف تعريف التحويل الجديد.

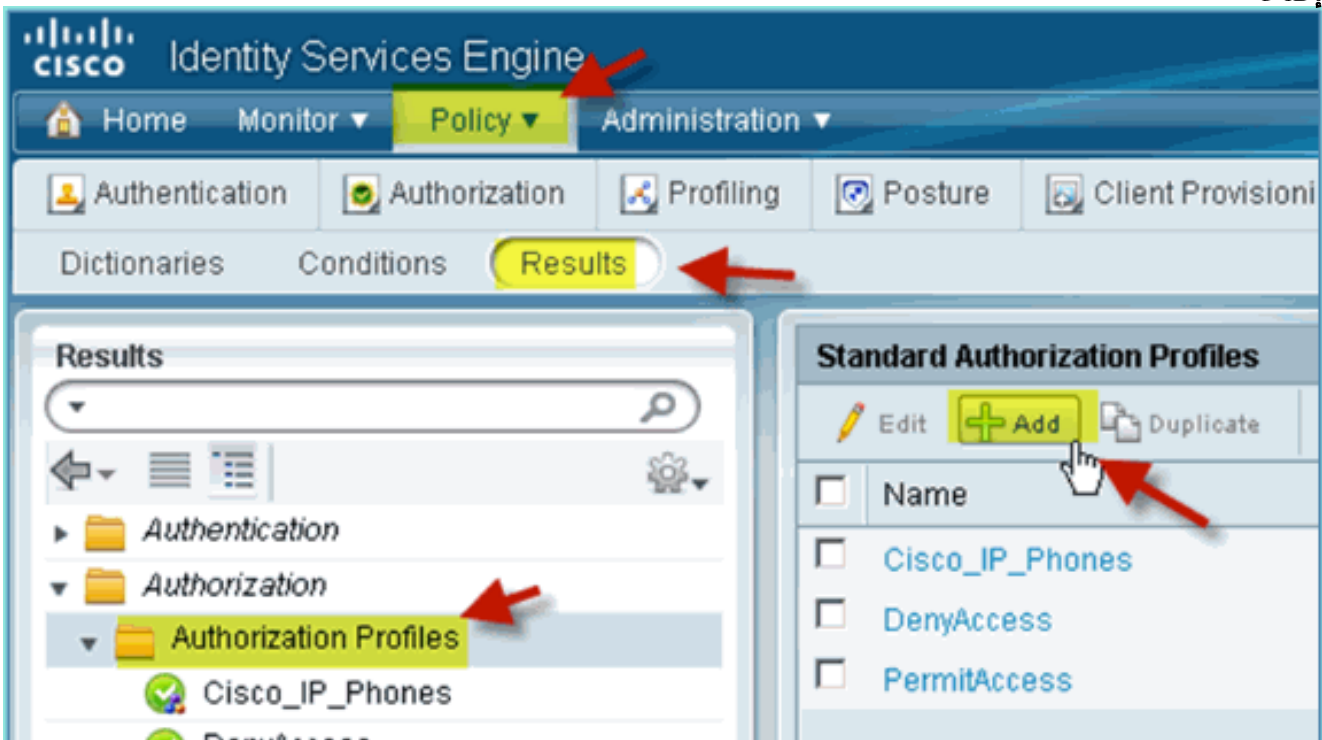


## إنشاء ملف تعريف تخويل ISE للموظف

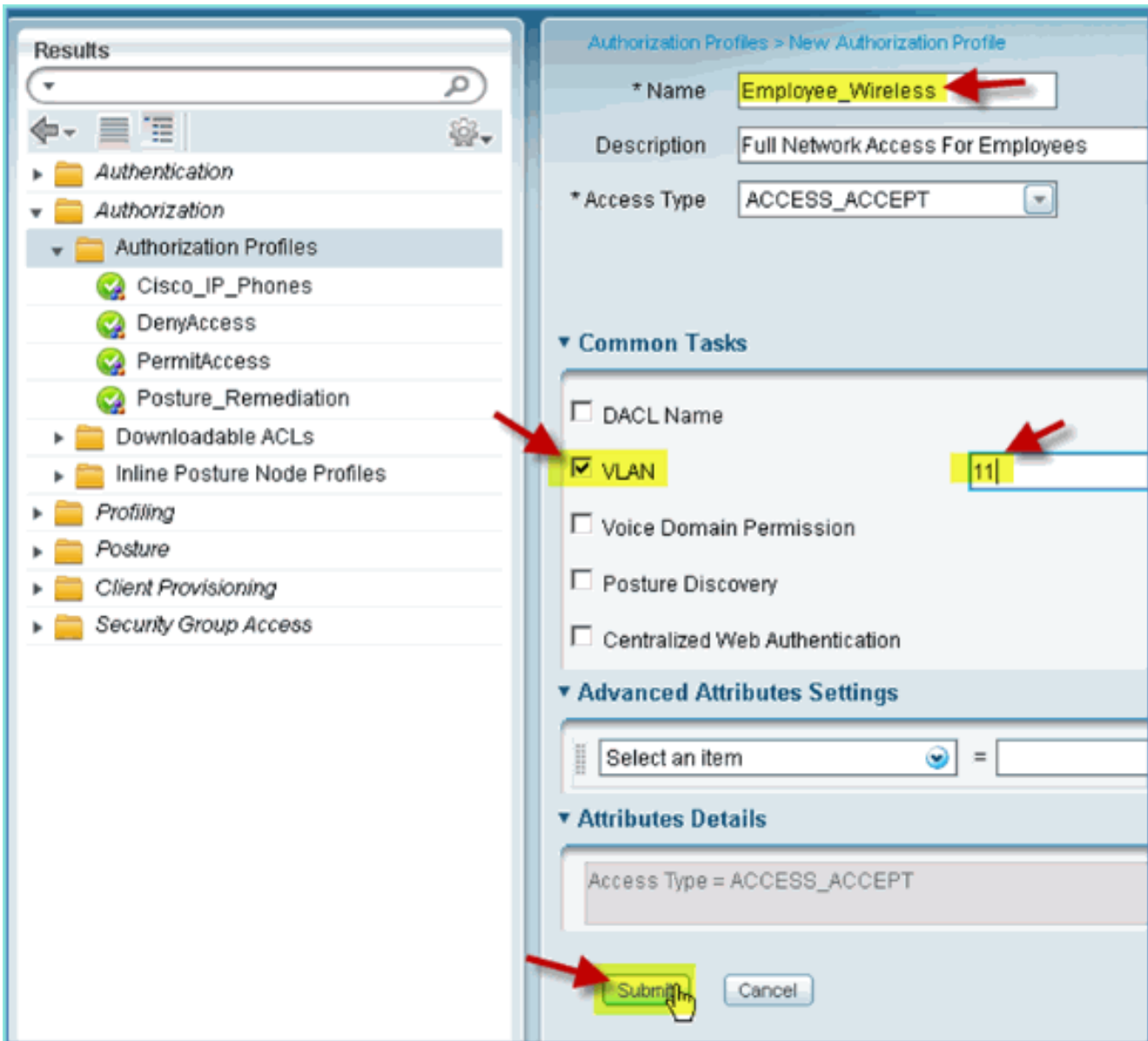
إن إضافة ملف تعريف تخويل لموظف يسمح لشركة خدمات البنية الأساسية (ISE) بتخويل الوصول والسماح به باستخدام السمات المعينة. يتم تعيين الموظف VLAN 11 في هذه الحالة.

أكمل الخطوات التالية:

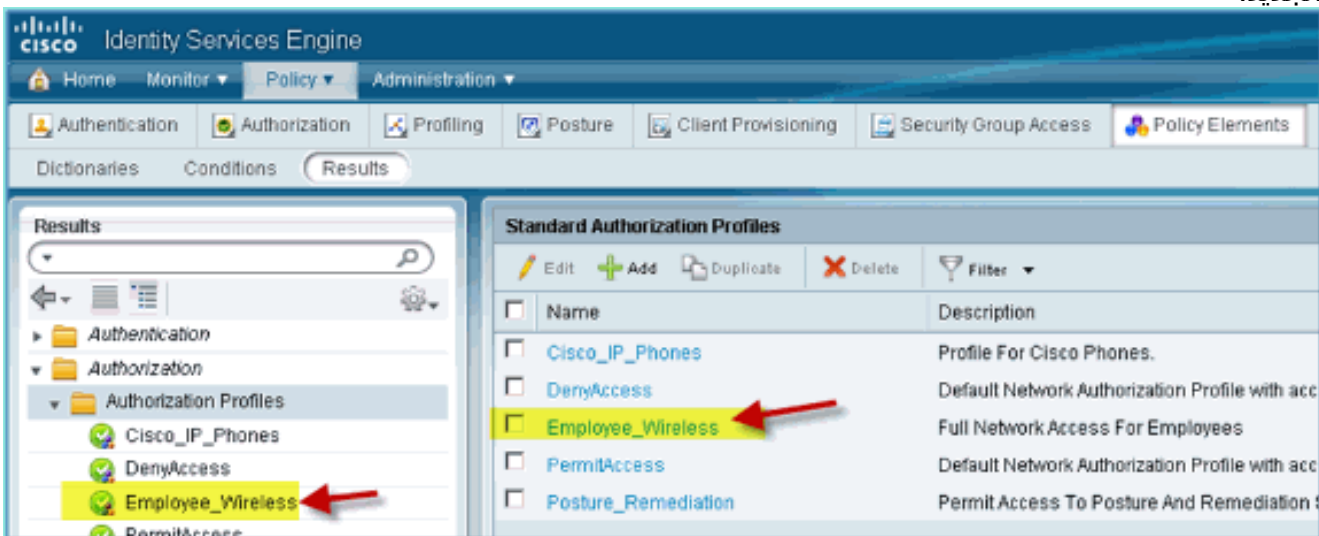
1. من ISE، انتقل إلى السياسة > النتائج. قم بتوسيع التفويض، ثم انقر على توصيفات التخويل وانقر على إضافة.



2. أدخل ما يلي لملف تعريف تخويل الموظف: الاسم: EMPLOYEE\_WIRELESS المهام المشتركة: VLAN، يمكن VLAN، القيمة الفرعية 11  
3. انقر فوق إرسال لإكمال هذه المهمة.



4. تأكد من إنشاء ملف تعريف تخويل الموظف الجديد.

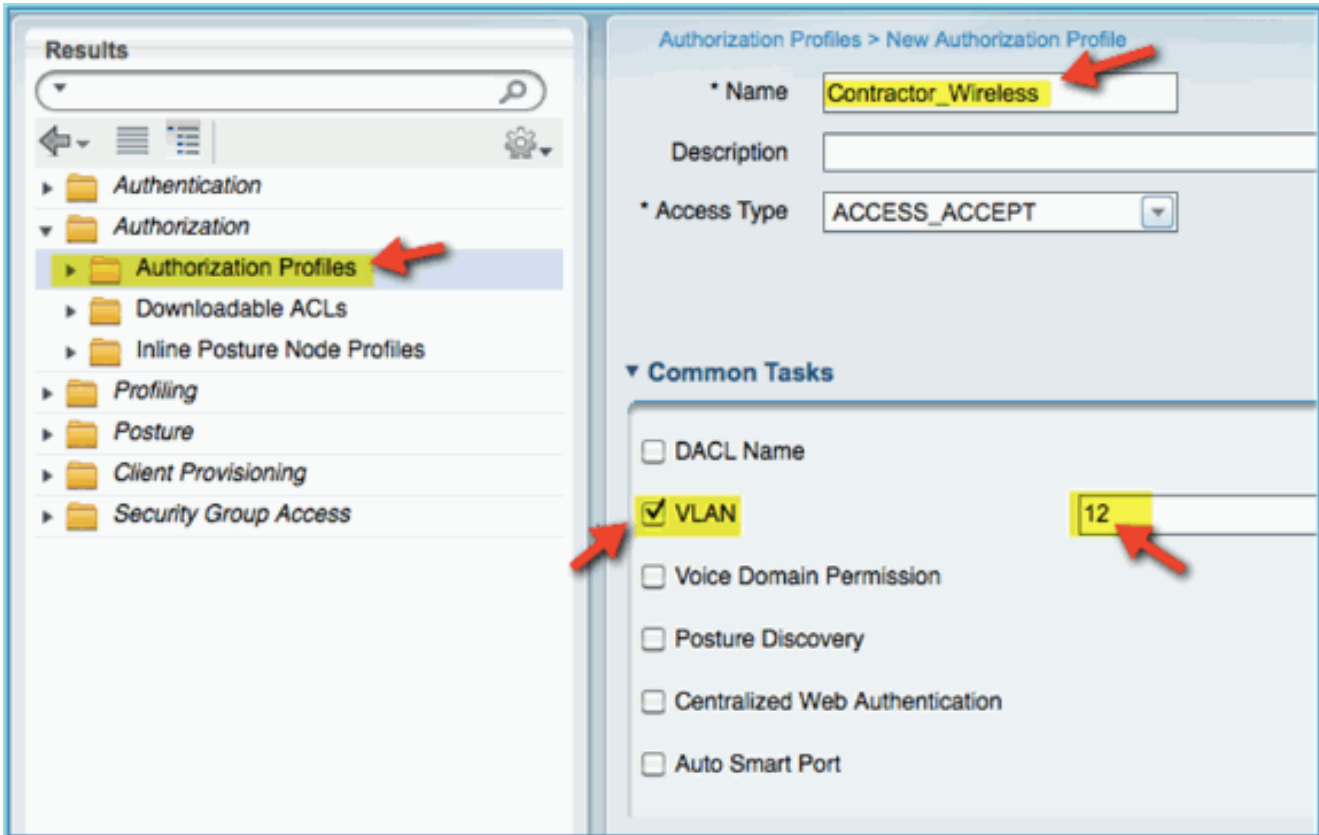


## إنشاء ملف تعريف تخويل ISE للمقاول

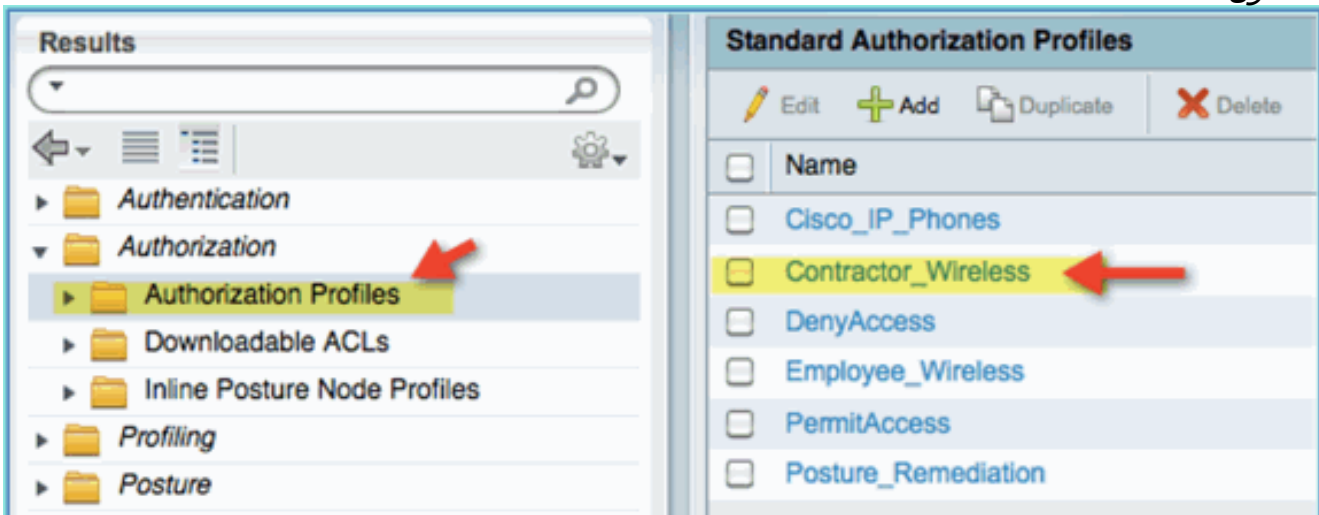
إن إضافة ملف تعريف تخويل للمتعاقدين يسمح لشركة خدمات البنية الأساسية (ISE) بتفويض الوصول والسماح به باستخدام السمات المعنية. يتم تخصيص شبكة VLAN 12 الخاصة بالمتعاقدين في هذه الحالة.

1. من ISE، انتقل إلى السياسة < النتائج. قم بتوسيع التفويض، ثم انقر على توصيفات التحويل وانقر على إضافة.
2. أدخل ما يلي لملف تعريف تحويل الموظف: الاسم: EMPLOYEE\_WIRELESS المهام المشتركة: VLAN، القيمة الفرعية

12



3. انقر فوق إرسال لإكمال هذه المهمة.
4. تأكد من إنشاء ملف تعريف تفويض المقاول.



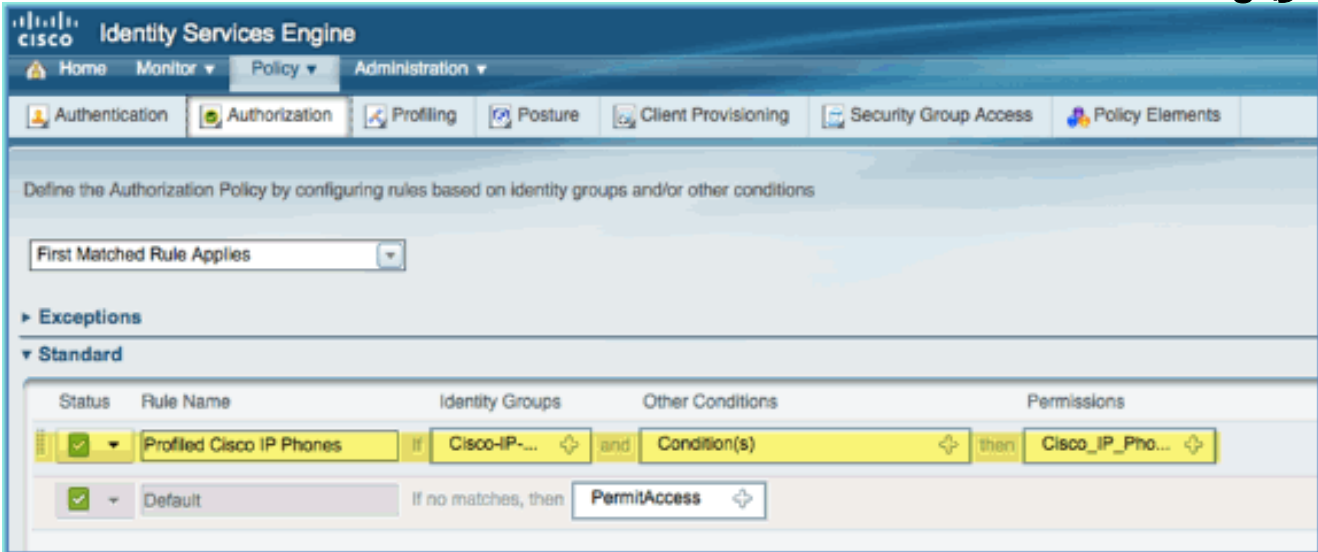
## نهج التحويل الخاص بوضعية الجهاز/إنشاء ملفات التعريف

لا يعرف سوى القليل من المعلومات حول الجهاز الجديد عند دخوله لأول مرة إلى الشبكة، وسيقوم المسؤول بإنشاء السياسة المناسبة للسماح بتعريف نقاط النهاية غير المعروفة قبل السماح بالوصول. وفي هذه العملية، سيتم إنشاء سياسة التحويل بحيث تتم إعادة توجيه جهاز جديد إلى ISE لتقييم الوضع (لأن الأجهزة المحمولة لا تحتاج إلى استخدام أية برامج، وبالتالي فإن عملية تحديد الهوية هي المهمة فقط)، وسيتم إعادة توجيه نقاط النهاية إلى بوابة ISE الأسيرة

والتعرف عليها.

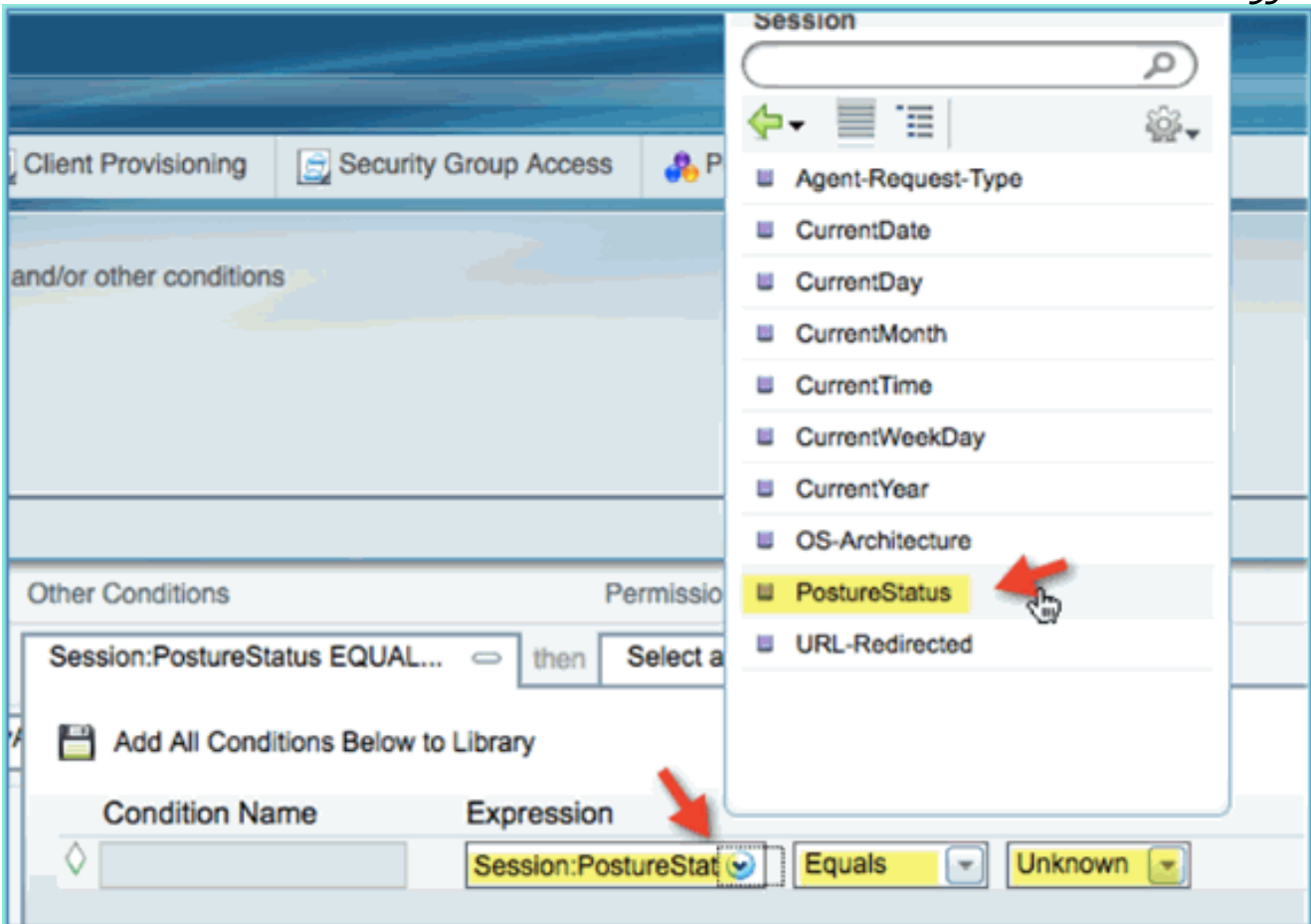
أكمل الخطوات التالية:

1. من ISE، انتقل إلى نهج < تفويض.

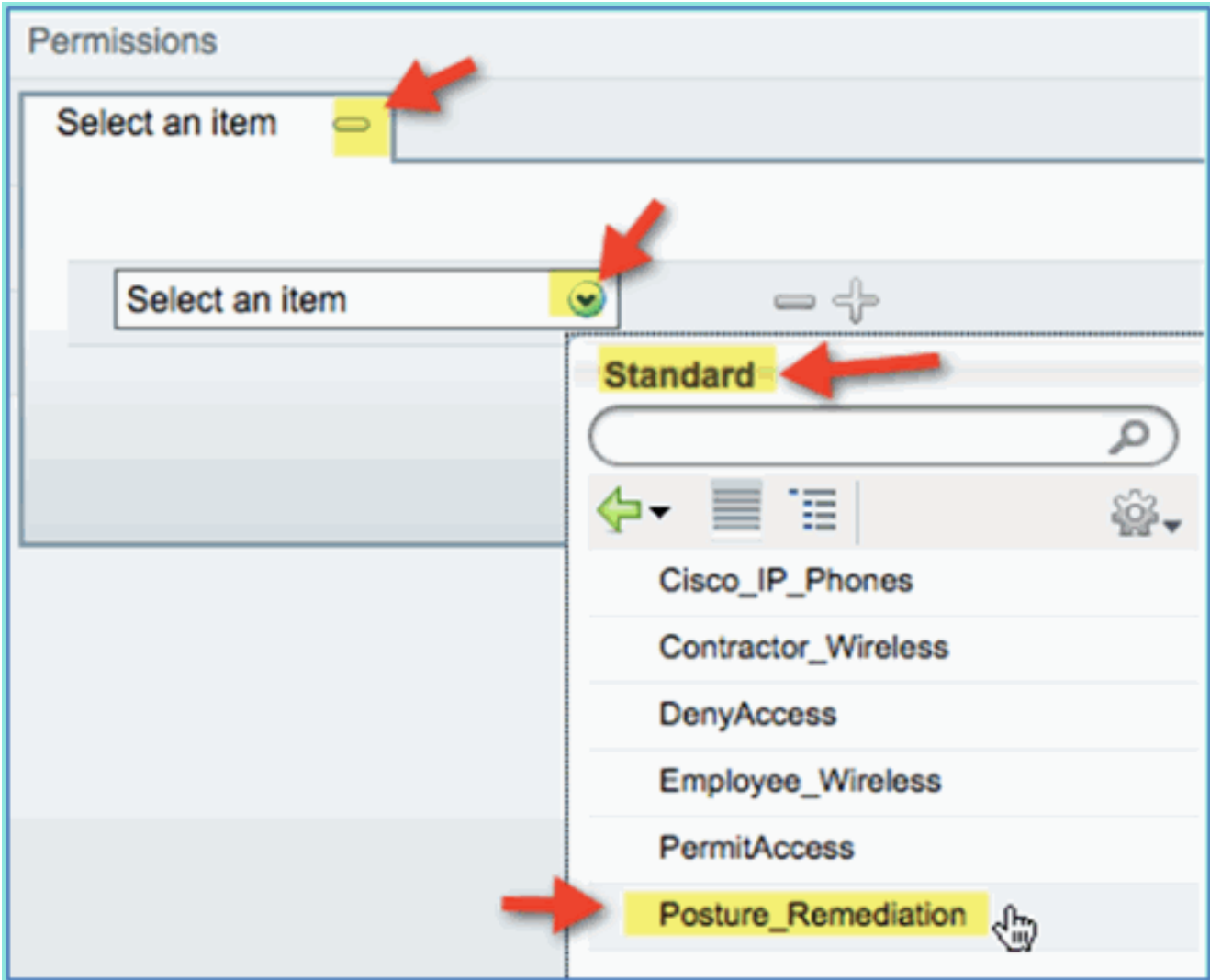


2. هناك سياسة لهواتف Cisco IP الموزعة. هذا خارج الصندوق. تحرير هذا كنهج الوضع.

3. أدخل القيم التالية لهذا النهج: اسم القاعدة: Posture\_remediation مجموعة الهوية: أي شروط أخرى < إنشاء جديد: (متقدم) جلسة < PostureStatusPostureStatus < يساوي: غير معروف



4. قم بتعيين التالي للأذونات: أذون < قياسية: Posture\_Remediation

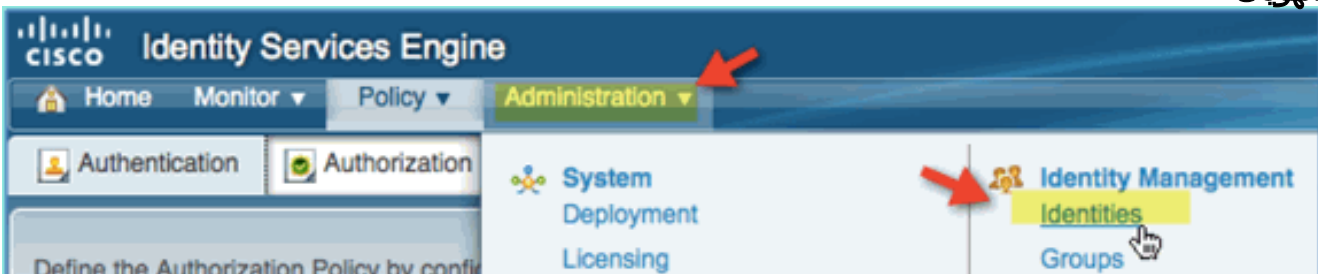


5. قطعة حفظ. ملاحظة: يمكن بدلا من ذلك إنشاء عناصر سياسات مخصصة لإضافة سهولة الاستخدام.

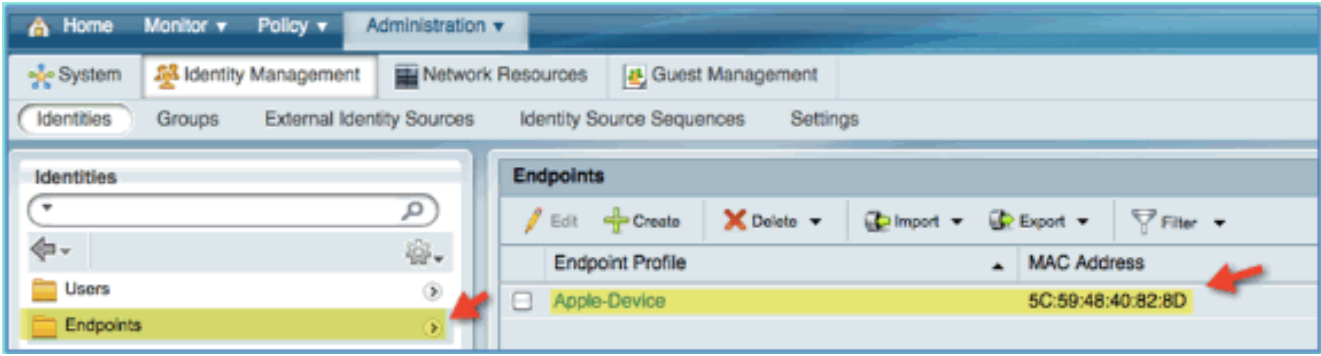
## إختبار سياسة إصلاح الوضع

ولتبسيط العرض التوضيحي يمكن القيام به لإظهار أن ISE يقوم بتحديد ملامح جهاز جديد بشكل صحيح استنادا إلى نهج الوضع.

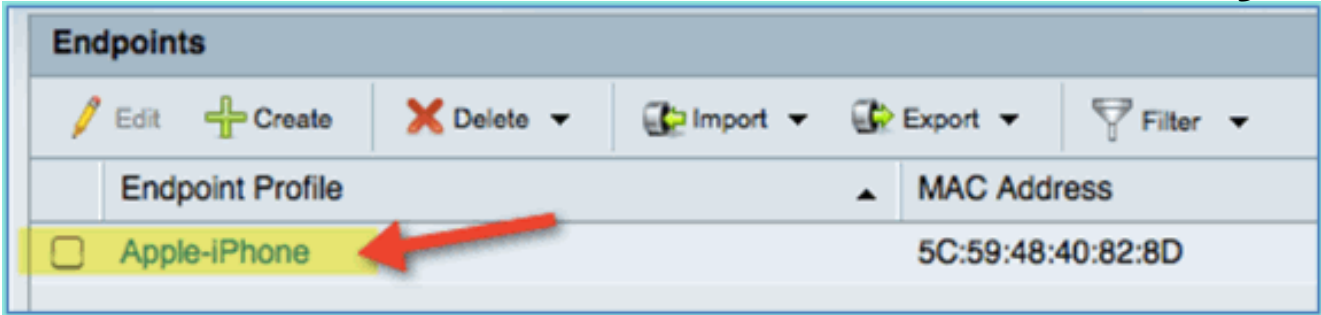
1. من ISE، انتقل إلى إدارة < إدارة الهوية > الهويات.



2. انقر نقاط النهاية. إقران جهاز وتوصيله (أي فون في هذا المثال).



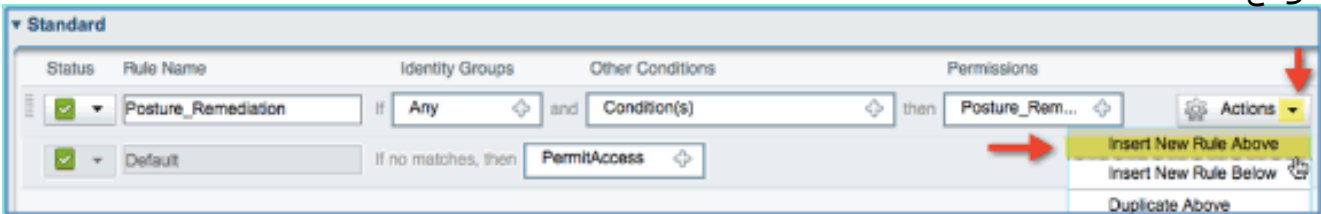
3. قم بتحديث قائمة نقاط النهاية. لاحظوا اية معلومات تعطى.
4. من جهاز نقطة النهاية، تصفح إلى URL: http://www:10.10.10.10 تمت إعادة توجيه الجهاز. قبول أية مطالبة للشهادات.
5. بعد إعادة توجيه الجهاز المحمول بالكامل، من ISE قم بتحديث قائمة نقاط النهاية مرة أخرى. لاحظوا ما تغير. نقطة النهاية السابقة (على سبيل المثال، Apple-Device) يجب أن تكون قد تغيرت إلى 'Apple-iPhone'. السبب هو أن تحقيق HTTP يحصل بشكل فعال على معلومات وكيل المستخدم، كجزء من عملية إعادة التوجيه إلى المدخل المأهول.



## سياسة التحويل للوصول المميز

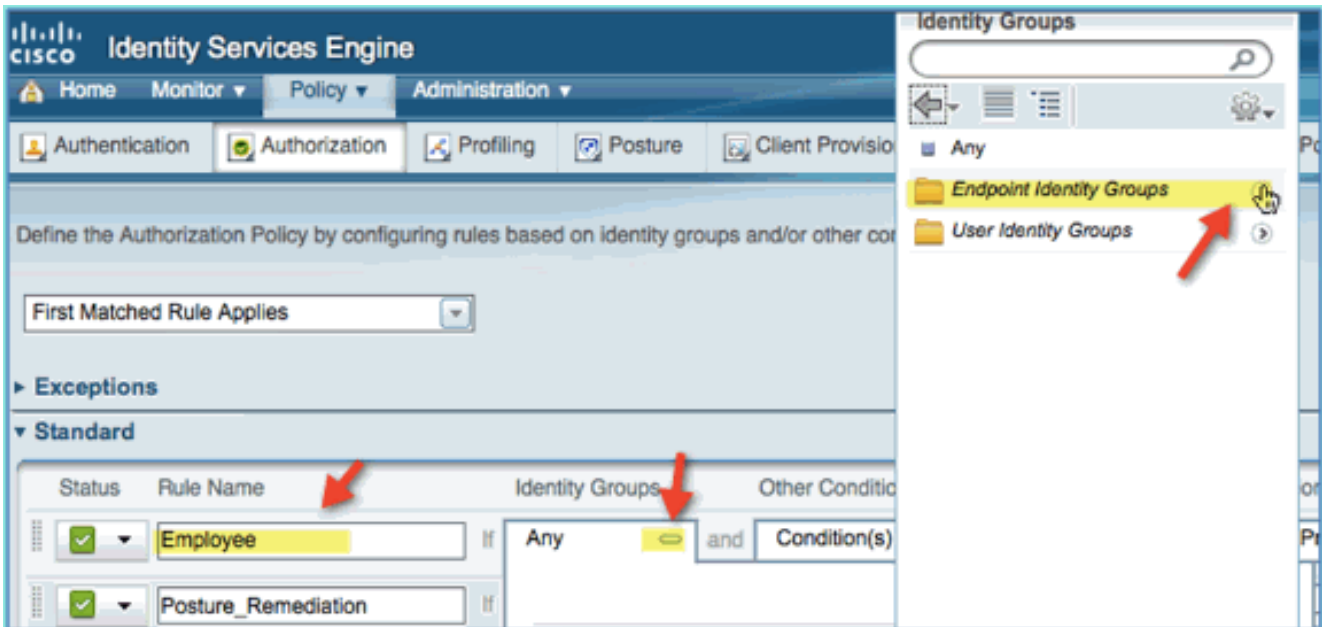
بعد إختبار تفويض الوضع بنجاح، استمر في إنشاء سياسات لدعم الوصول المميز للموظف والمتعهد باستخدام أجهزة معروفة وتعيين شبكة VLAN مختلف محدد لدور المستخدم (في هذا السيناريو، الموظف والمتعهد).  
أكمل الخطوات التالية:

1. انتقل إلى ISE < نهج < تفويض.
2. إضافة/إدراج قاعدة جديدة فوق نهج/سطر إصلاح الوضع.

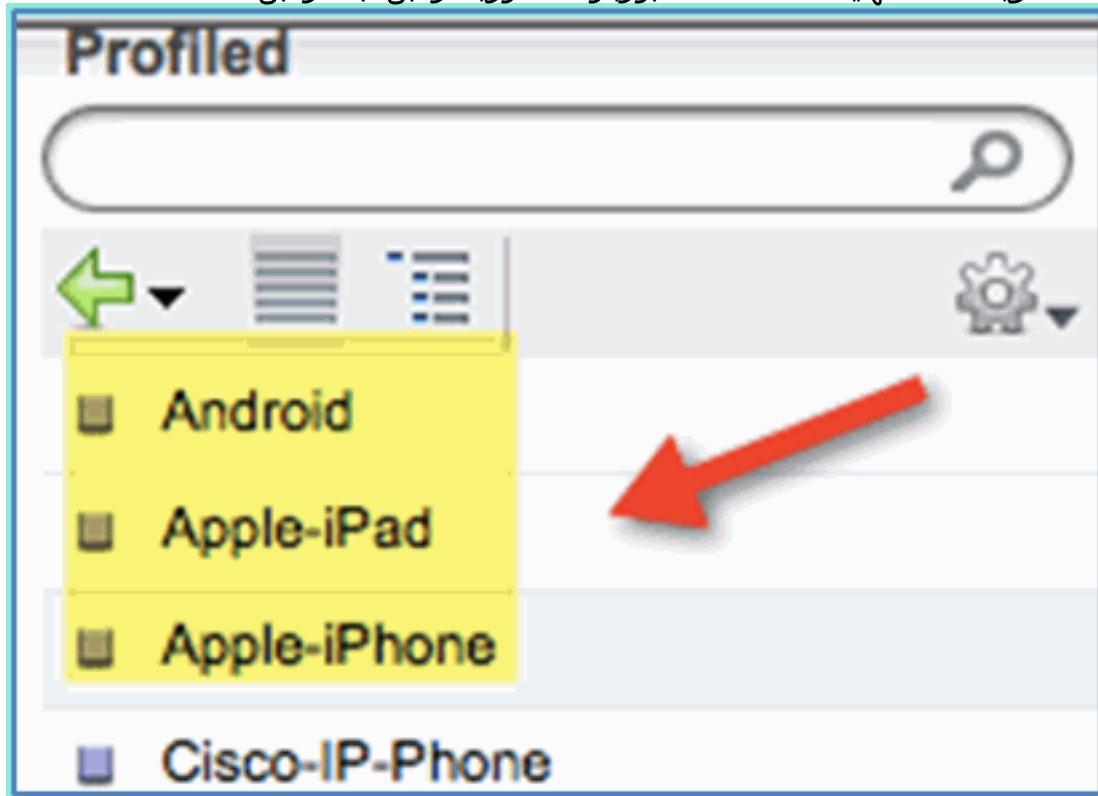


3. أدخل القيم التالية لهذا النهج: اسم القاعدة: الموظف مجموعات الهوية (التوسيع): مجموعات هوية نقاط النهاية

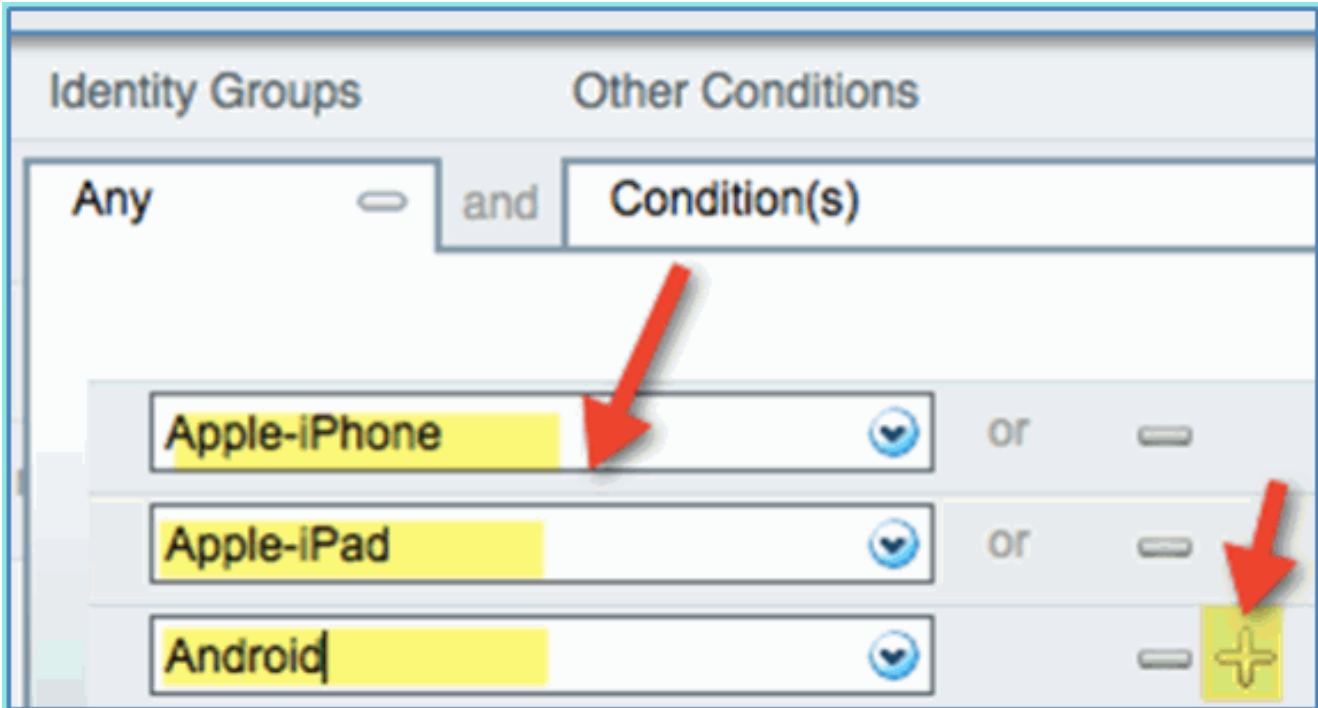




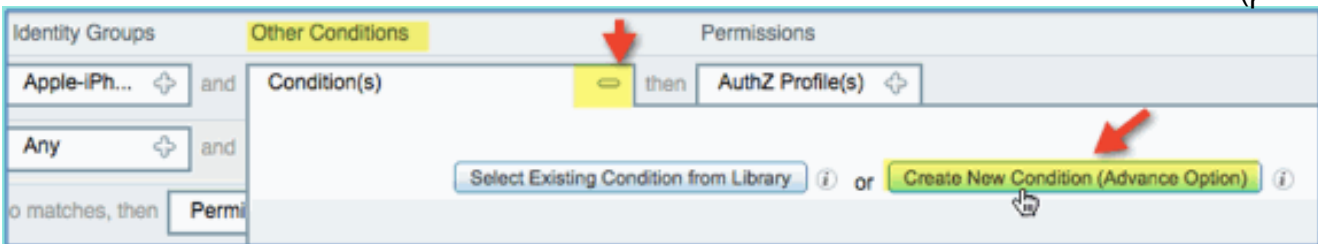
مجموعات هوية نقطة النهاية: PROFILED بروبارت: أندرويد أو أبل-آباد أو أبل-



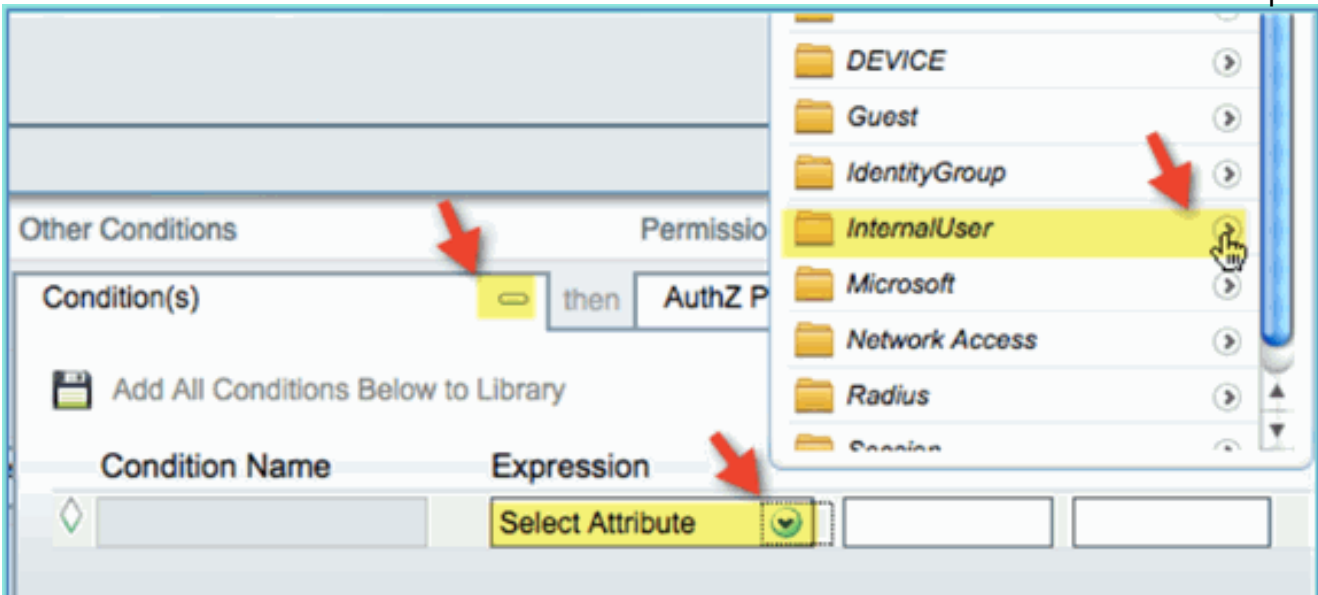
4. لتحديد أنواع أجهزة إضافية، انقر فوق + وقم بإضافة المزيد من الأجهزة (إذا لزم الأمر): مجموعات هوية نقطة  
النهاية: PROFILED بروبارت: أندرويد أو أبل-آباد أو أبل-  
أيفون



5. حدد قيم الأذونات التالية لهذا النهج: شروط أخرى (توسيع): إنشاء شرط جديد (خيار متقدم)



شرط < تعبير (من القائمة): InternalUser < اسم



InternalUser < الاسم:  
الموظف

Other Conditions Permissions

Select Attribute then AuthZ Profile(s)

Add All Conditions Below to Library

Condition Name Expression

InternalUser:Name Equals employee

6. إضافة شرط ل Posture جلسة متوافق:أذون < توصيفات < قياسي:  
EMPLOYEE\_Wireless

Permissions

AuthZ Profile(s)

Select an item

Standard

Cisco\_IP\_Phones

Contractor\_Wireless

DenyAccess

Employee\_Wireless

PermitAccess

Posture\_Remediation

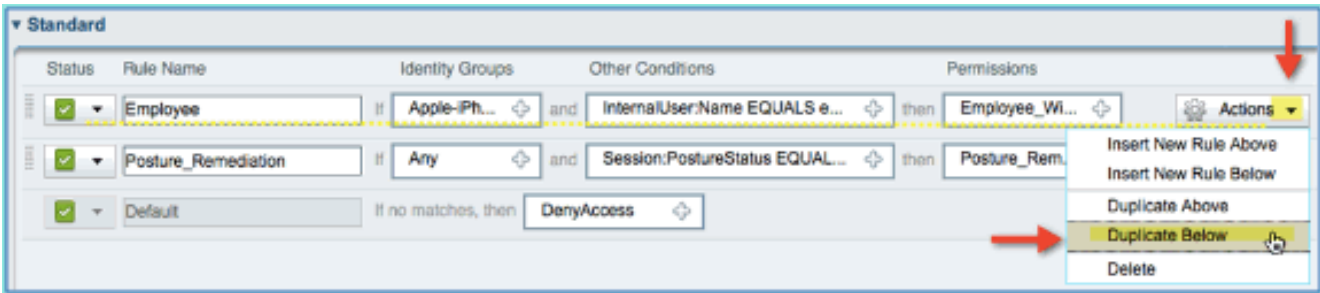
7. قطعة حفظ. تأكد من إضافة النهج بشكل صحيح.

Standard

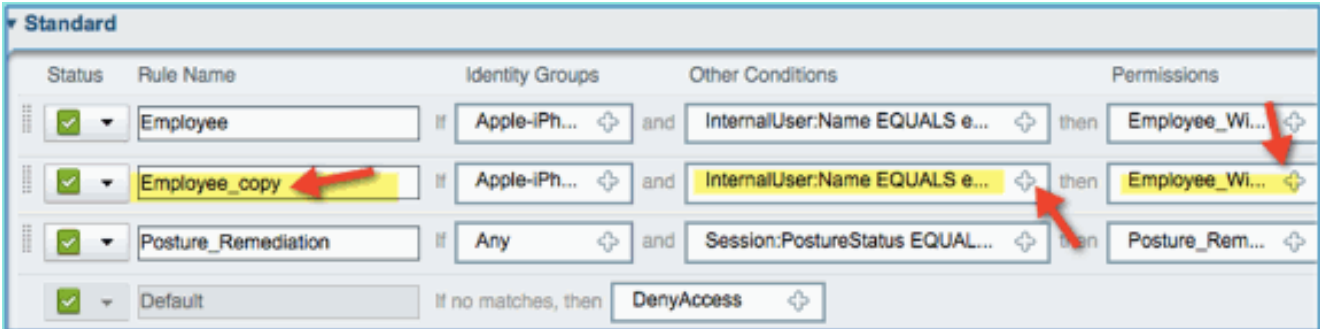
Status	Rule Name	Identity Groups	Other Conditions	Permissions
	Employee	Apple-iPh...	and InternalUser:Name EQUALS e...	then Employee_Wi...
	Posture_Remediation	Any	and Session:PostureStatus EQUAL...	then Posture_Rem...
	Default	If no matches, then	DenyAccess	

8. المتابعة بإضافة سياسة "المقاول". في هذا المستند، يتم تكرار النهج السابق من أجل تسريع العملية (أو، يمكنك التكوين يدويا للممارسة الجيدة). من نهج الموظف < الإجراءات، انقر فوق تكرار

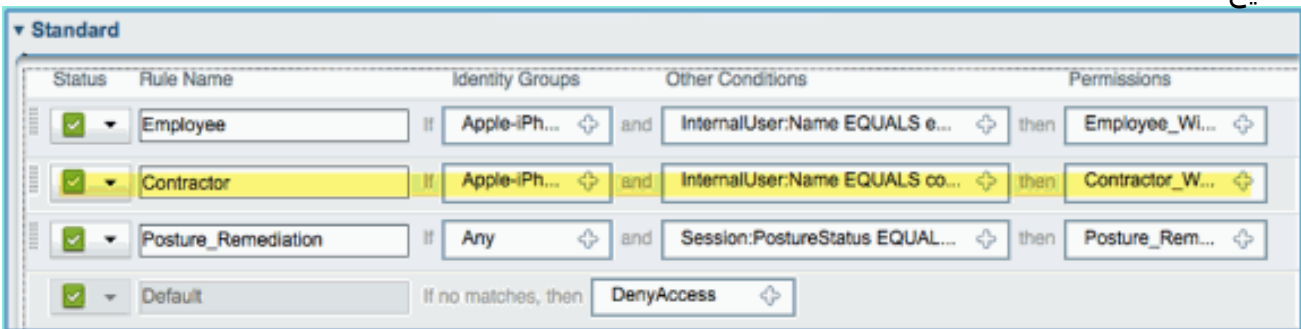
أدناه.



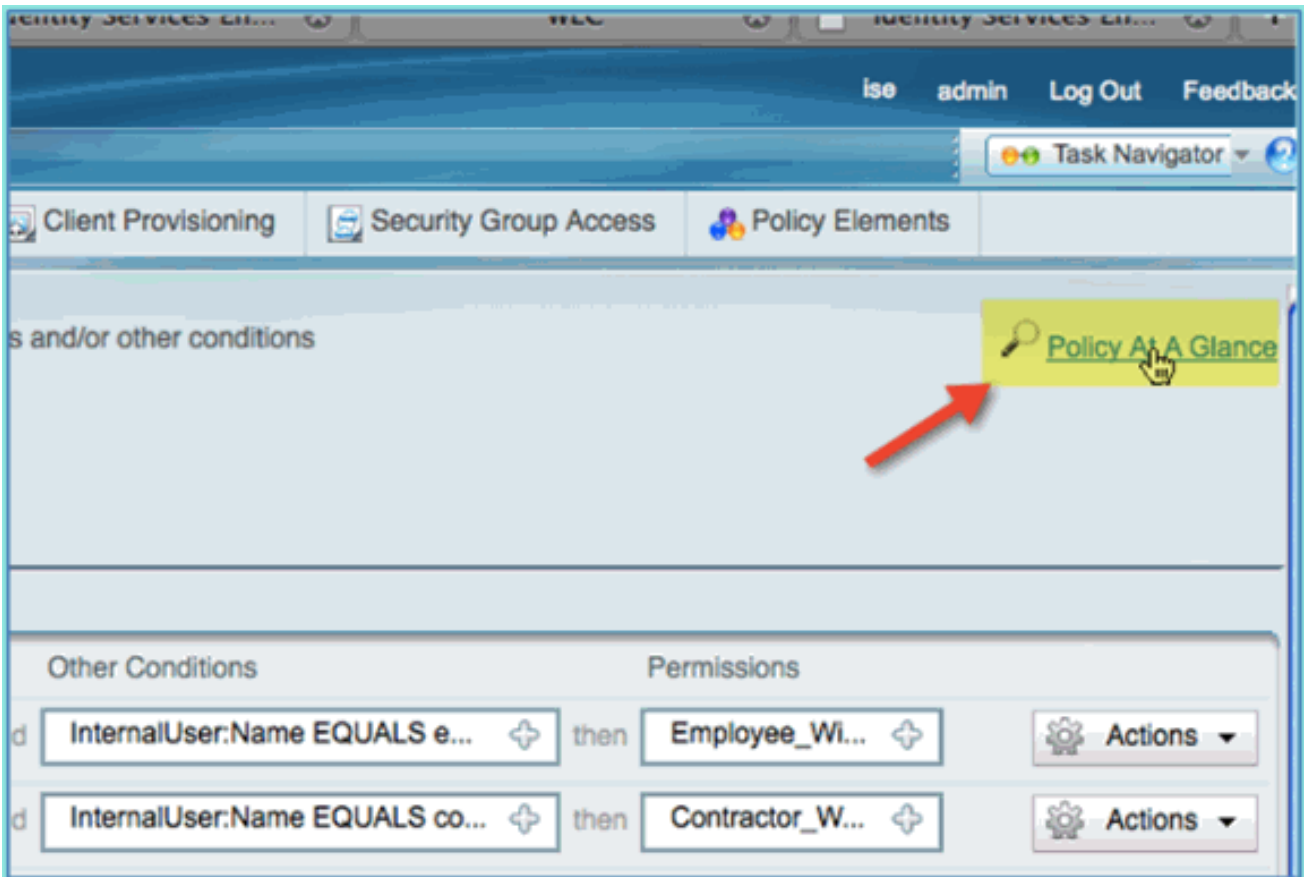
9. تحرير الحقول التالية لهذا النهج (نسخة مكررة): اسم القاعدة: المقاولشروط أخرى < InternalUser > Name: Contractor الأذونات: Contractor\_Wireless



10. قطعة حفظ. تأكد من تكوين النسخة المكررة السابقة (أو النهج الجديد) بشكل صحيح.



11. لمعاينة السياسات، انقر نظرة على النهج.



توفر السياسة في نظرة سريعة ملخصا موحدًا وبسهل الاطلاع على السياسات.

Authorization Policy At A Glance				
First Matched Rule Applies				
Exceptions				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
			No data available	
Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Employee	Android OR Apple-iPad OR Apple-iphone	InternalUser:Name EQUALS employee	Employee_Wireless
Enabled	Contractor	Android OR Apple-iPad OR Apple-iphone	InternalUser:Name EQUALS contractor	Contractor_Wireless
Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
Enabled	Default	Any		DenyAccess

## إختبار CoA للوصول المميز

وقد حان الوقت لاختبار ملفات تعريف التحويل والسياسات المعدة لتمييز الوصول. مع وجود شبكة محلية لاسلكية (WLAN) مؤمنة واحدة، سيتم تعيين شبكة VLAN للموظف وسيكون المقابل لشبكة VLAN للمقاول. يستخدم آبل أي فون/ iPad في الأمثلة التالية.

أكمل الخطوات التالية:

1. اتصل بالشبكة المحلية اللاسلكية (WLAN) الآمنة (POD1x) مع الجهاز المحمول واستخدم بيانات الاعتماد التالية: اسم المستخدم: الموظف كلمة المرور:

Enter the password for "pod1x"

**Cancel** **Enter Password**

**Username** employee

**Password** ●●●●●●3

**Mode** Automatic >

1 2 3 4 5 6 7 8 9 0

XXXX

2. انقر فوق الانضمام. تأكد من أن الموظف قد تم تعيينه لشبكة VLAN 11 (شبكة VLAN للموظف).



3. انقر على تجاهل هذه الشبكة. تأكد بالنقر فوق



انسى.

4. انتقل إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وقم بإزالة إتصالات العميل الموجودة (إذا كان نفس المستخدم قد تم استخدامه في الخطوات السابقة). انتقل إلى شاشة < عملاء > عنوان MAC، ثم انقر إزالة.



Monitor

Clients

Summary

Current Filter

▶ Access Points

▶ Cisco CleanAir

▶ Statistics

▶ CDP

▶ Rogues

Clients

Multicast

Client MAC Addr

44:2a:60:f7:3a:4a

5c:59:48:40:82:8d

Status	Auth	Port	WGB
Associated	Yes	1	No
Associated	No	1	No

LinkTest

Disable

Remove

802.11aTSM

802.11b/gTSM

5. طريقة أخرى مؤكدة لمسح جلسات العميل السابقة هي تعطيل/تمكين شبكة WLAN. انتقل إلى > WLC WLAN > WLANs، ثم انقر فوق الشبكة المحلية اللاسلكية (WLAN) للتحريك. **enabled** uncheck < تطبيق (أن يعجز). حدد المربع تمكين < تطبيق (لإعادة التمكين).

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The main content area is titled 'WLANs > Edit 'pod1x''. On the left, a sidebar shows a tree view with 'WLANs' and 'Advanced' items. The 'WLANs' item is highlighted with a red arrow. The main content area has tabs for 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active, showing the following configuration:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)]

A red arrow points to the 'Enabled' checkbox in the 'Status' row. Below the 'Security Policies' row, there is a note: '(Modifications done under security tab will s

6. العودة إلى الجهاز المحمول. اتصل مرة أخرى بنفس شبكة WLAN باستخدام بيانات الاعتماد التالية: اسم المستخدم: المقاول كلمة المرور:

Enter the password for "pod1x"

**Cancel** **Enter Password**

**Username** contractor ←

**Password** ●●●●●●●● | ←

**Mode** Automatic >

1 2 3 4 5 6 7 8 9 0

XXXX

7. انقر فوق الانضمام. أكدت أن المقاول عينت مستعمل VLAN 12 (مقاول/ضيف



(VLAN

8. يمكنك النظر إلى عرض سجل ISE في الوقت الفعلي في ISE < مراقبة > التكاليف. يجب أن ترى المستخدمين الفرديين (الموظف أو المقاول) يحصلون على توصيفات تخويل مختلفة (Employee\_WirelessvsContractor\_Wireless) في شبكات VLAN مختلفة.

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Aug 02,11 03:40:18.331 PM	✓		employee	5C:59:48:40:82:8D		wlc		Employee_Wireless
Aug 02,11 03:38:33.663 PM	✓		contractor	5C:59:48:40:82:8D		wlc		Contractor_Wireless

## WLC Guest WLAN

أتمت هذا steps in order to أضفت ضيف WLAN أن يسمح ضيف أن ينفذ ال ISE Sponsors Guest مدخل:

1. من WLC، انتقل إلى شبكات WLAN > WLAN < إضافة جديد.
2. دخلت التالي للضيف للضيف جديد WLAN: اسم ملف التعريف: pod1guestSSID: pod1guest



3. قطعة يطبق.
4. أدخل ما يلي أسفل Guest WLAN < علامة التبويب "عام": الحالة: معظم مجموعة الواجهة/الواجهة: ضيف

WLANs &gt; Edit 'pod1guest'

General

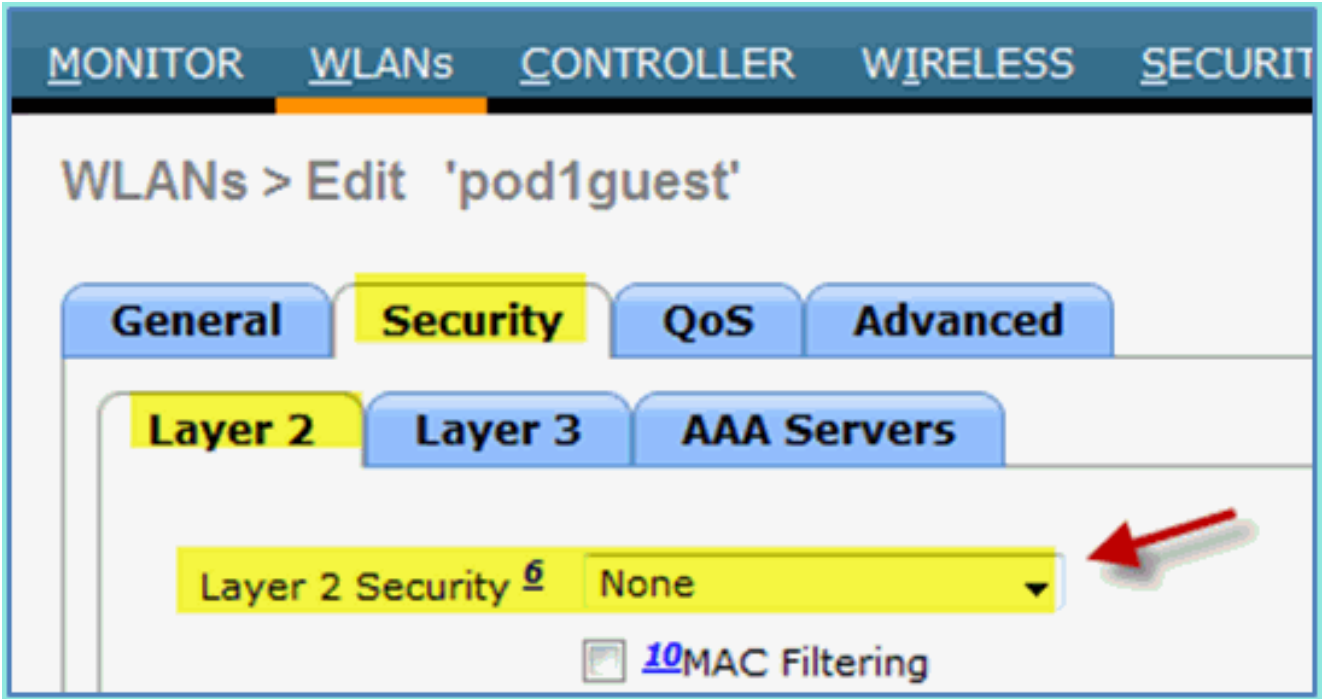
Security

QoS

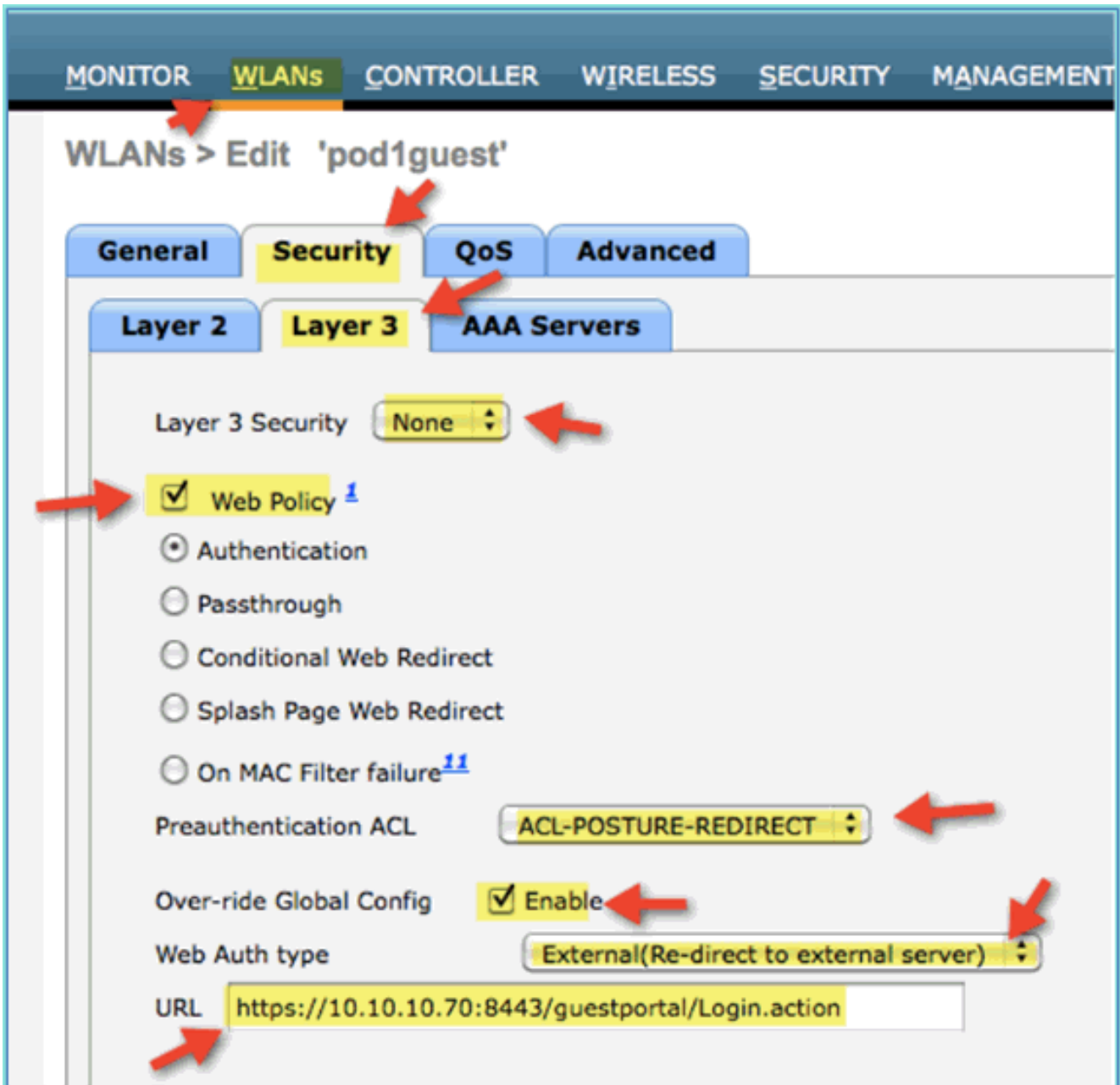
Advanced

Profile Name	pod1guest
Type	WLAN
SSID	pod1guest
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security
Radio Policy	All
Interface/Interface Group(G)	guest
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

5. انتقل إلى شبكة WLAN للضيف < التأمين < الطبقة 2 وأدخل ما يلي: أمان الطبقة 2: لا يوجد



6. انتقل إلى شبكة WLAN للضيف < التأمين < صفحة الطبقة 3 وأدخل التالي: أمان الطبقة 3: لا يوجد نهج ويب: ممكن القيمة الفرعية لنهج الويب: المصادقة قائمة التحكم في الوصول (ACL) لما قبل المصادقة: ACL- Posture-Redirect نوع مصادقة الويب: خارجي (إعادة التوجيه إلى خادم خارجي): URL: <https://10.10.10.70:8443/guestportal/Login.action>



7. طقطقة يطبق.

8. تأكد من حفظ تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

## إختبار الشبكة المحلية اللاسلكية (WLAN) للضيف وبوابة الضيوف

الآن، يمكنك إختبار تكوين شبكة WLAN الضيف. يجب أن تعيد توجيه الضيوف إلى بوابة ضيف ISE.

أكمل الخطوات التالية:

1. من جهاز iOS مثل iPhone، انتقل إلى شبكات Wi-Fi < تمكين. ثم حدد شبكة ضيف

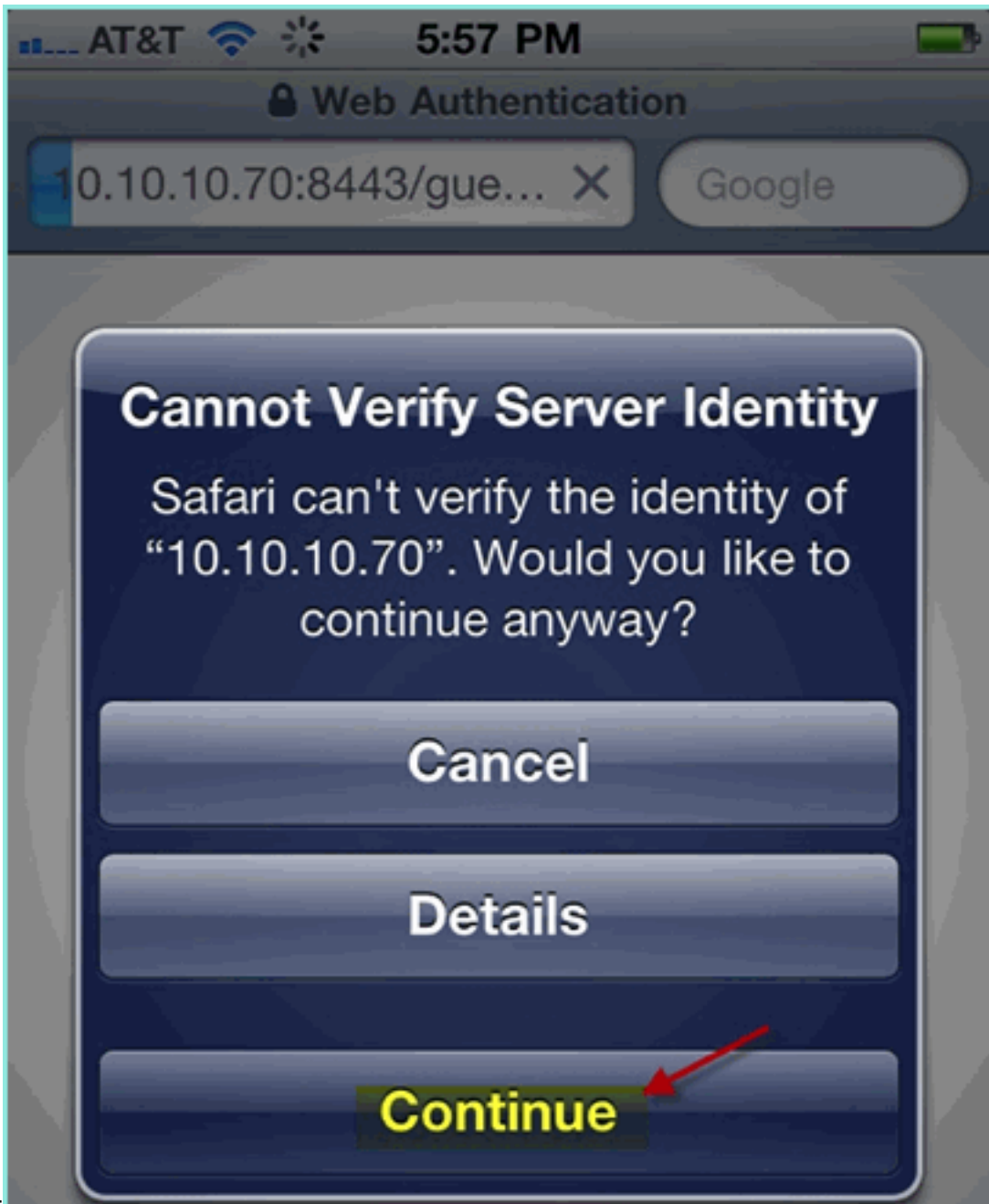




.POD  
2. يجب أن يظهر جهاز iOS الخاص بك عنوان IP صالح من شبكة VLAN الضيف  
(24/10.10.12.0).



3. افتح مستعرض Safari واتصل ب: <http://10.10.10.10> URL تظهر إعادة توجيه مصادقة ويب.
4. انقر فوق متابعة حتى تصل إلى صفحة مدخل ضيف



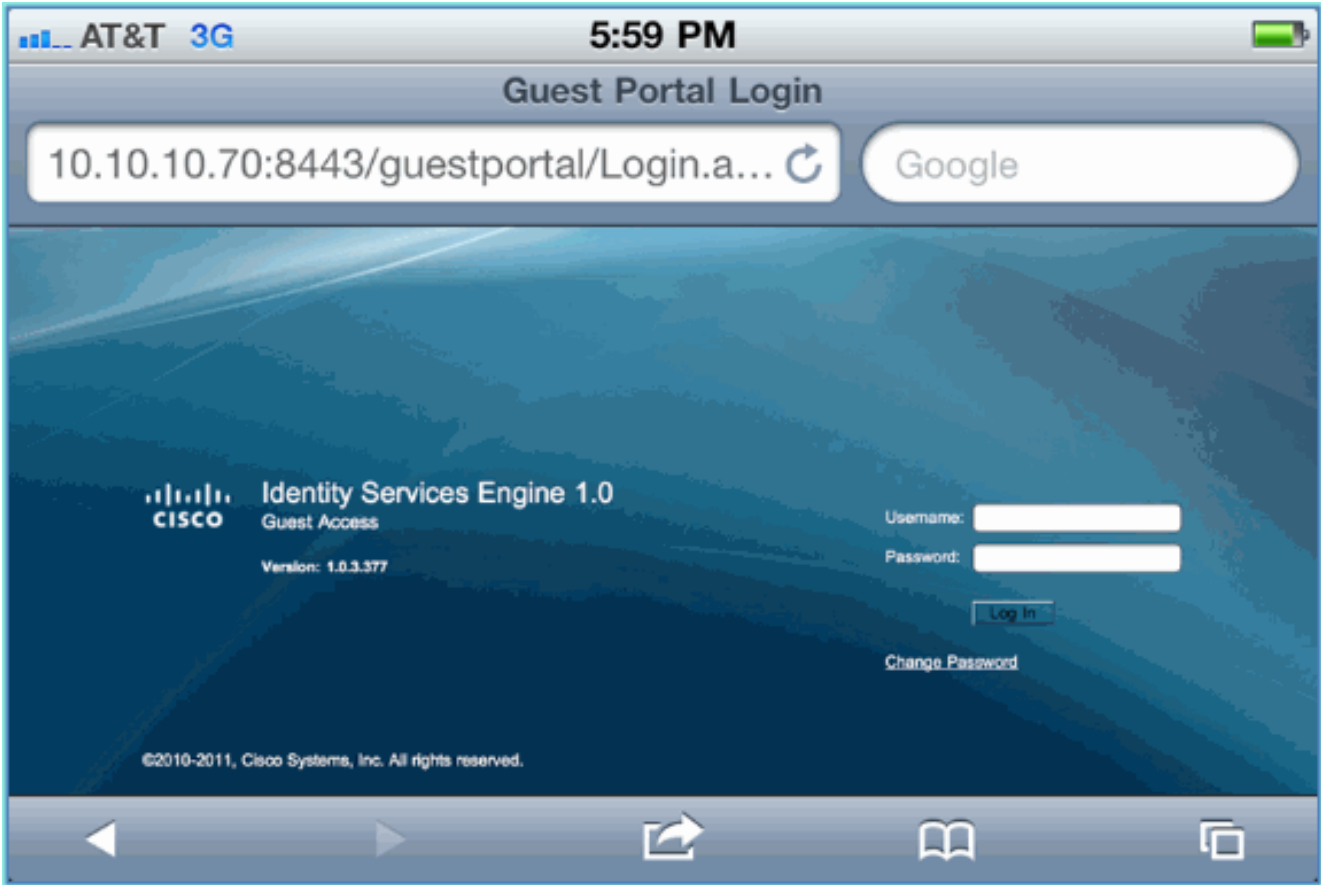
توضح لقطة

.ISE

الشاشة التالية جهاز iOS على تسجيل دخول Guest Portal. هذا يؤكد أن الإعداد الصحيح لـ WLAN و ISE

Guest Portal

نشط.

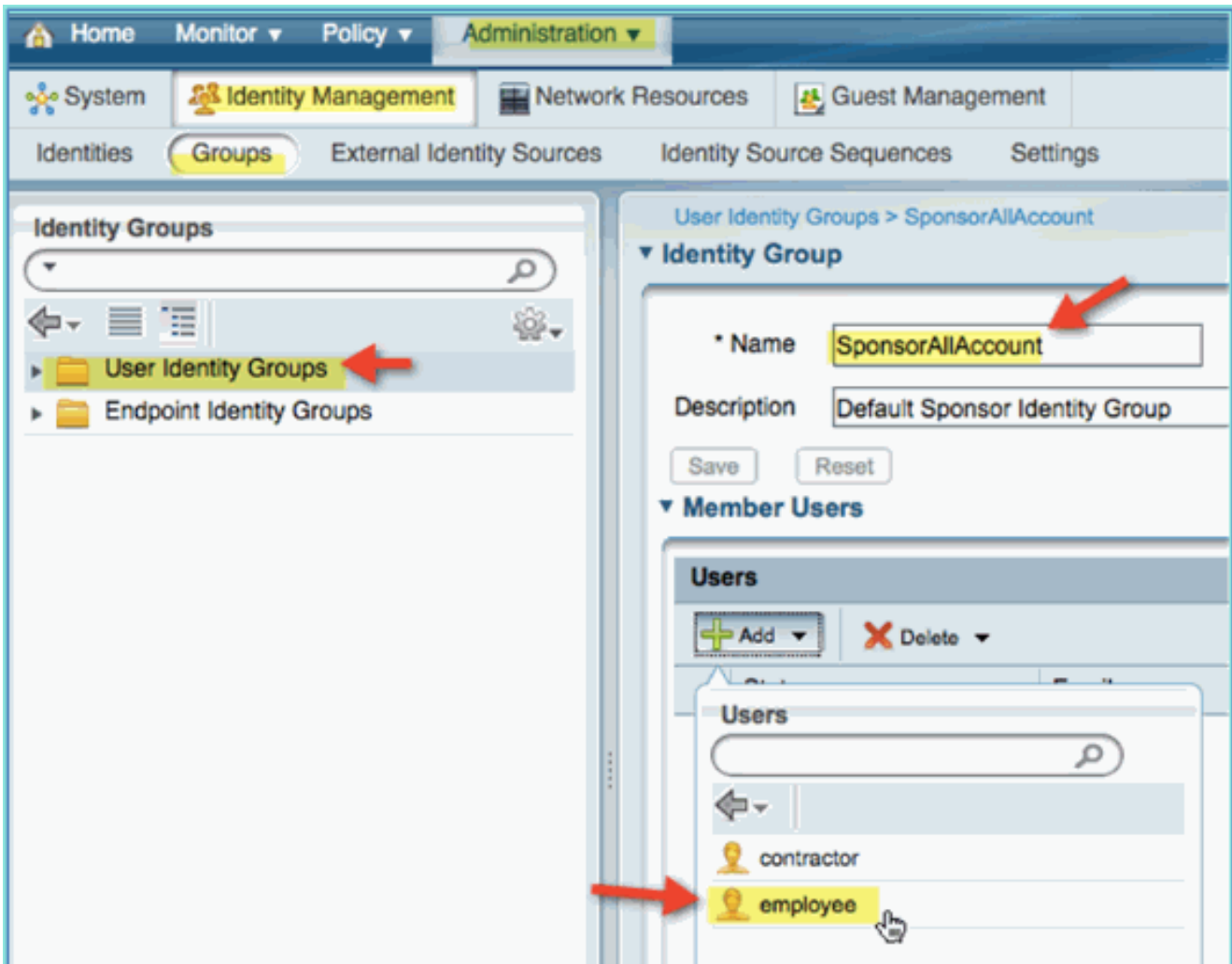


## وصول ضيف برعاية ISE Wireless

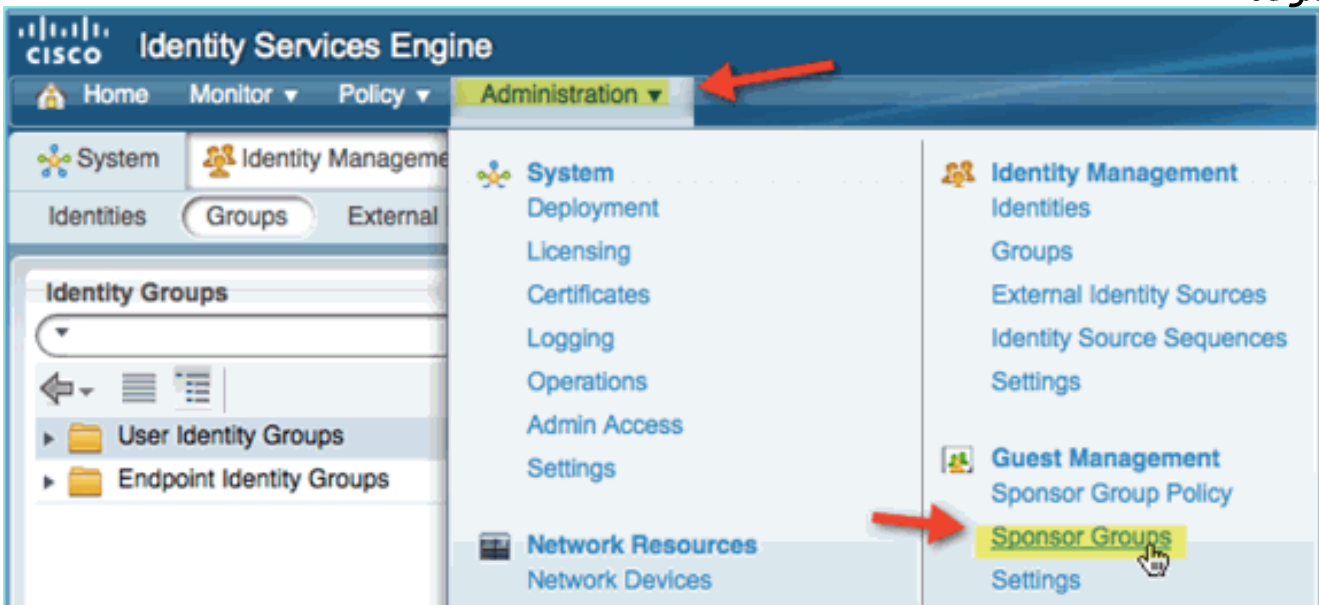
يمكن تهيئة ISE للسماح برعاية الضيوف. في هذه الحالة، ستقوم بتكوين نهج ضيف ISE للسماح إما للمستخدمين الداخليين أو مستخدمي مجال AD (في حالة دمجهم) برعاية الوصول للضيف. كما ستقوم بتكوين ISE للسماح للجهات الراعية بعرض كلمة مرور الضيف (إختيارية)، وهو ما يساعد هذا المختبر.

أكمل الخطوات التالية:

1. إضافة مستخدم موظف إلى مجموعة SponsorAllAccount. هناك طرق مختلفة للقيام بذلك: انتقل مباشرة إلى المجموعة، أو قم بتحرير المستخدم وتعيين المجموعة. لهذا المثال، انتقل إلى إدارة < إدارة الهوية > مجموعات < مجموعات هوية المستخدم. ثم انقر فوق SponsorAllAccount وقم بإضافة مستخدم موظف.



2. انتقل إلى إدارة < إدارة الضيوف > مجموعات الرعاية.



3. انقر فوق تحرير، ثم اختر SponsorAllAccounts.

**CISCO Identity Services Engine**

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

### Guest Sponsor Groups

Edit Add Delete Filter

<input type="checkbox"/>	Sponsor Group Name	Description
<input checked="" type="checkbox"/>	SponsorAllAccounts	Default SponsorGroup
<input type="checkbox"/>	SponsorGroupGrpAccounts	Default SponsorGroup

4. حدد مستويات التحويل، ثم قم بتعيين ما يلي: عرض كلمة مرور الضيف:  
نعم

**CISCO Identity Services Engine**

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Sponsor Group List > SponsorAllAccounts

General Authorization Levels Guest Roles Time Profiles

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

Save Reset

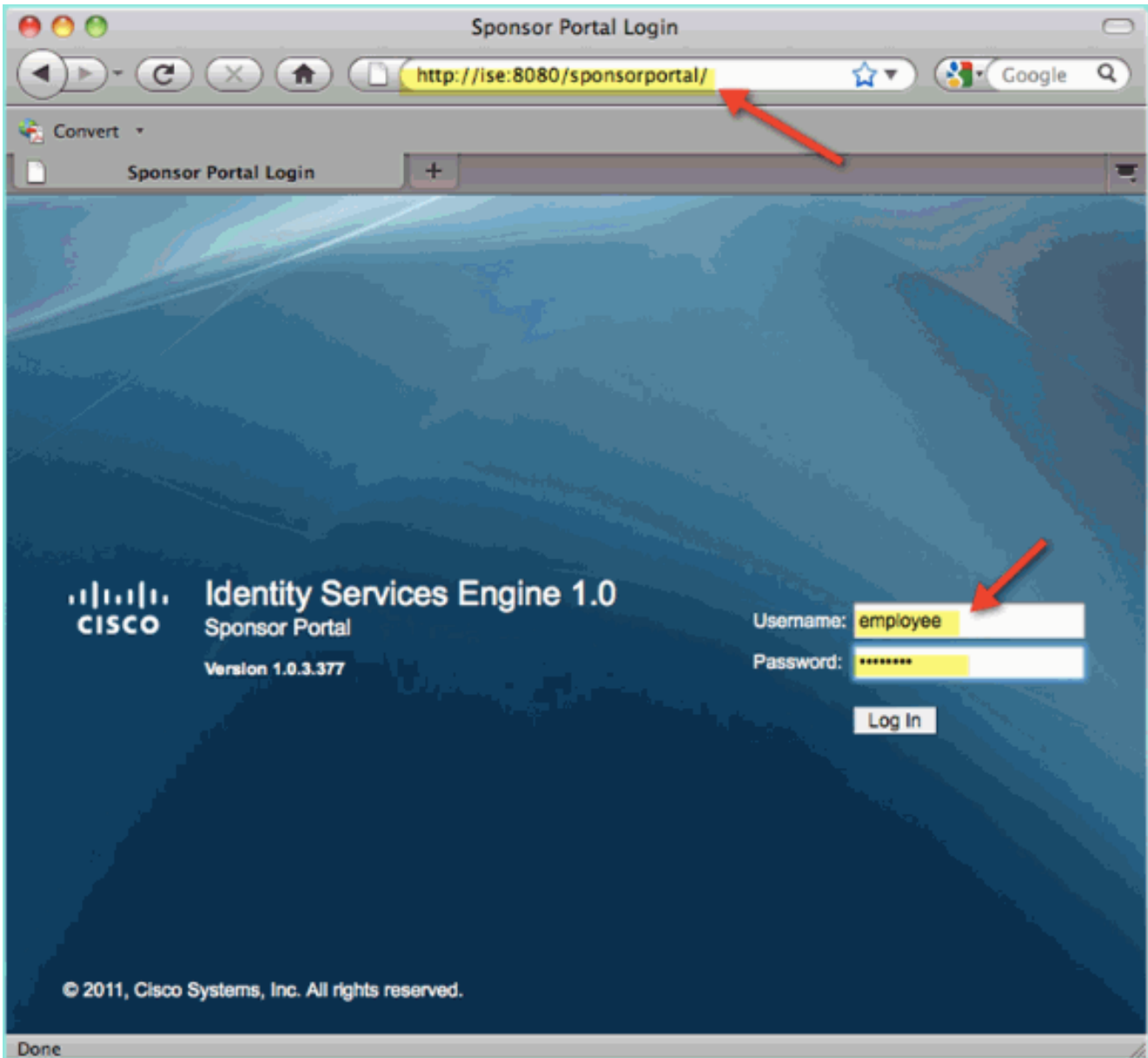
5. طقطقة حفظ in order to أتمت هذا مهمة.

## ضيف رعاية

في السابق، قمت بتكوين نهج الضيوف والمجموعات المناسبة للسماح لمستخدم مجال AD بتبني الضيوف المؤقتين. بعد ذلك، ستدخل إلى "بوابة الكفيل" وتنشئ وصولاً مؤقتاً للضيف.

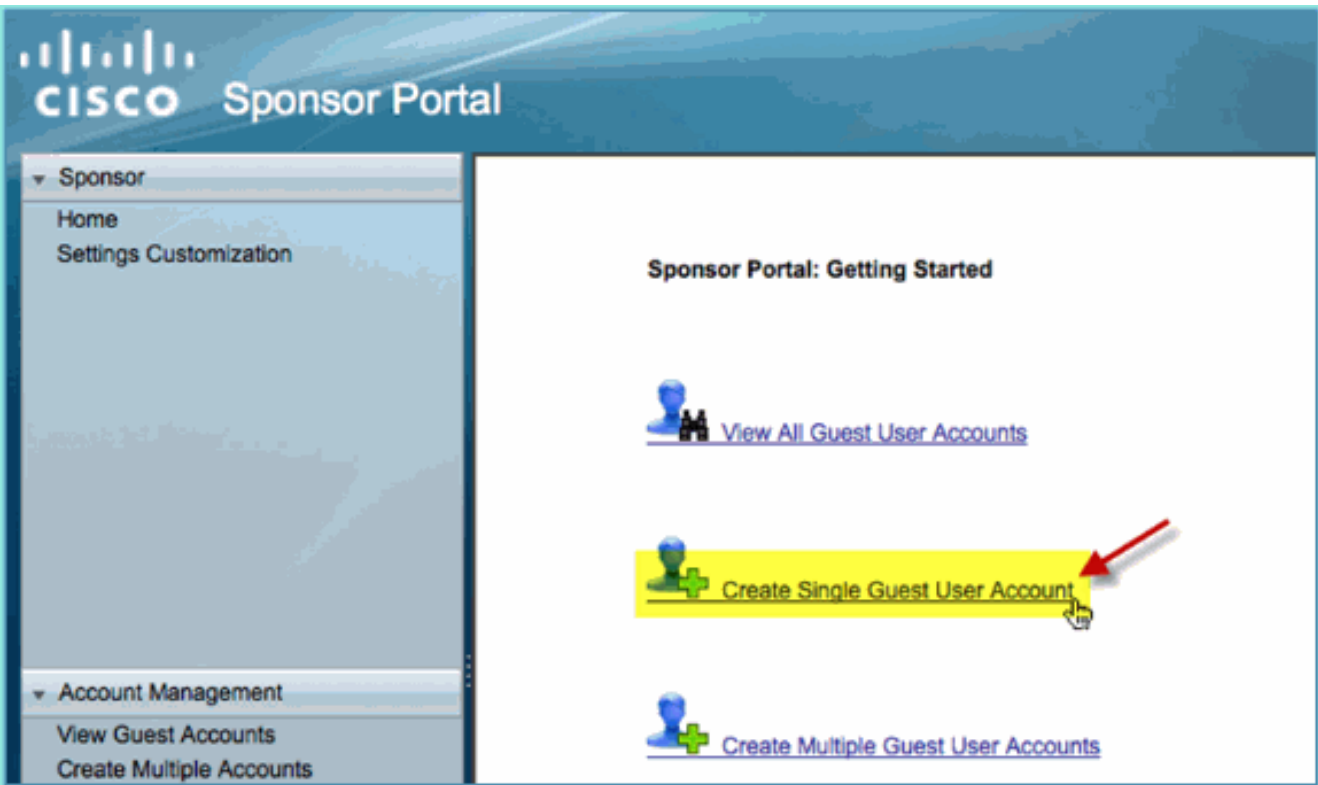
أكمل الخطوات التالية:

1. من متصفح، انتقل إلى أي من عناوين URL هذه: <http://<ise ip>:8080/sponsorportal> أو <https://<ise ip>:8443/sponsorportal>. بعد ذلك، سجل الدخول بما يلي: اسم المستخدم: المستخدم (Active Directory)، الموظف (المستخدم الداخلي) كلمة المرور: XXXX



2. من صفحة الكفيل، انقر فوق إنشاء حساب مستخدم ضيف واحد.





3. بالنسبة للضيف المؤقت، أضف ما يلي: الاسم الأول: مطلوب (على سبيل المثال، Sam) اسم العائلة: مطلوب (على سبيل المثال، Jones) دور المجموعة: ضيف ملف تعريف الوقت: DefaultOneHour المنطقة الزمنية: أي/افتراضي

## Create Guest Account

First Name:

Sam

Last Name:

iAm

Email Address:

Phone Number:

Company:

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role:

Guest

Time Profile:

DefaultOneHour

Timezone:

EST

⚙ = Required fields

Submit

Cancel

4. انقر على إرسال.

5. يتم إنشاء حساب ضيف استنادا إلى إدخالك السابق. لاحظ أن كلمة المرور مرئية (من تمرين سابق) بدلا من التجزئة \*\*\*.

6. أترك هذه النافذة مفتوحة لتظهر اسم المستخدم وكلمة المرور للضيف. سوف تستخدمها لاختبار تسجيل دخول مدخل الضيف (التالي).



## Successfully Created Guest Account siam0002

Username: siam0002  
Password: 5\_5g6d7Kx  
First Name: Sam  
Last Name: iAm  
Email Address:  
Phone Number:  
Company:  
Status: AWAITING INITIAL LOGIN  
Suspended: false  
Optional Data 1:  
Optional Data 2:  
Optional Data 3:  
Optional Data 4:  
Optional Data 5:  
Group Role: Guest  
Time Profile: DefaultOneHour

Timezone: EST

Account Start Date: 2011-07-15 13:56:04 EST

Account Expiration Date: 2011-07-15 14:56:04 EST

Email

Print

Create Another Account

View All Accounts

## إختبار الوصول إلى بوابة الضيوف

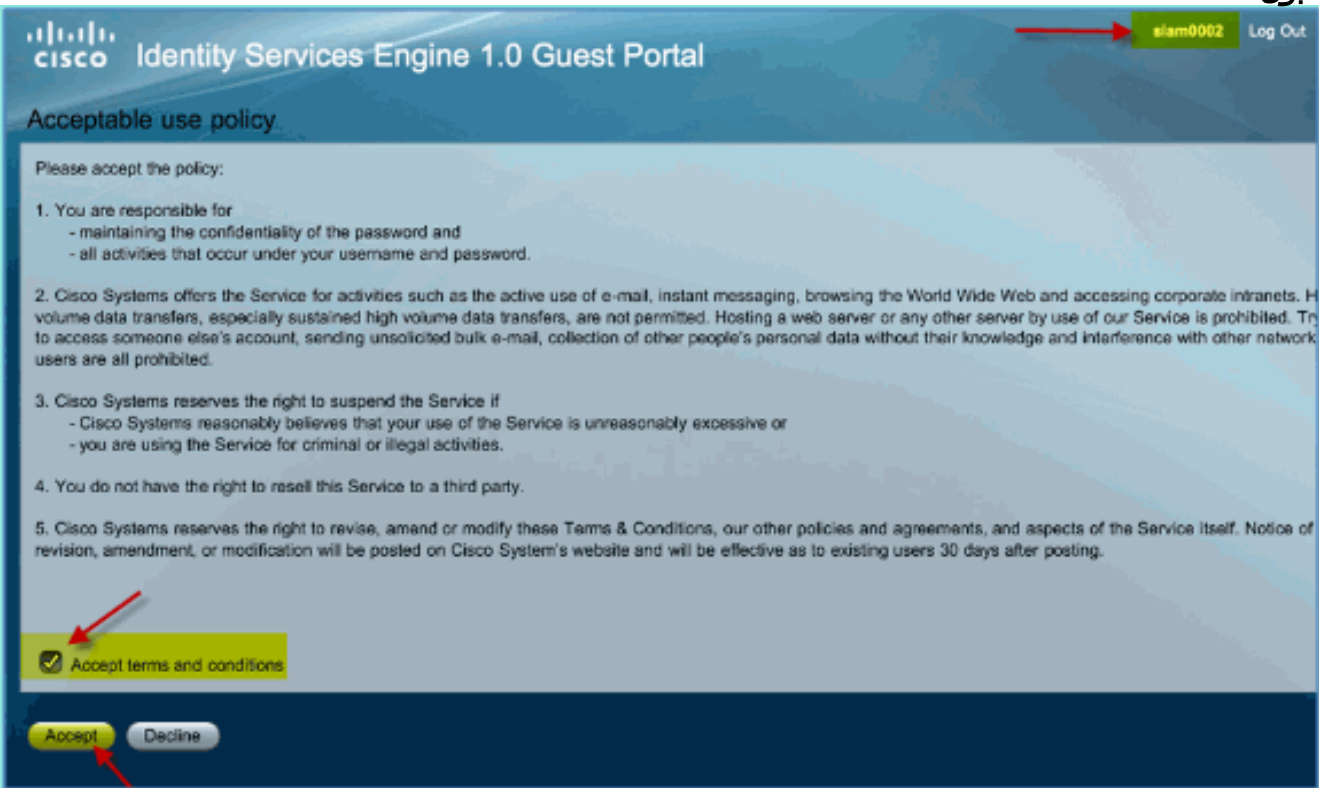
باستخدام حساب الضيف الجديد الذي تم إنشاؤه من قبل مستخدم/كفيل الإعلان، حان الوقت لاختبار مدخل الضيف والوصول إليه.

أكمل الخطوات التالية:

1. على جهاز مفضل (في هذه الحالة iPad / iOS من Apple)، اتصل ب SSID ضيف Pod وتحقق من عنوان IP والاتصال.
2. أستخدم المستعرض وحاول التنقل إلى <http://www.Guest>. تتم إعادة توجيهك إلى صفحة تسجيل الدخول إلى مدخل.



3. قم بتسجيل الدخول باستخدام حساب الضيف الذي تم إنشاؤه في التمرين السابق. في حالة نجاح هذه العملية، تظهر صفحة نهج الاستخدام المقبول.
4. تحقق من شروط وأحكام القبول، ثم انقر فوق قبول.



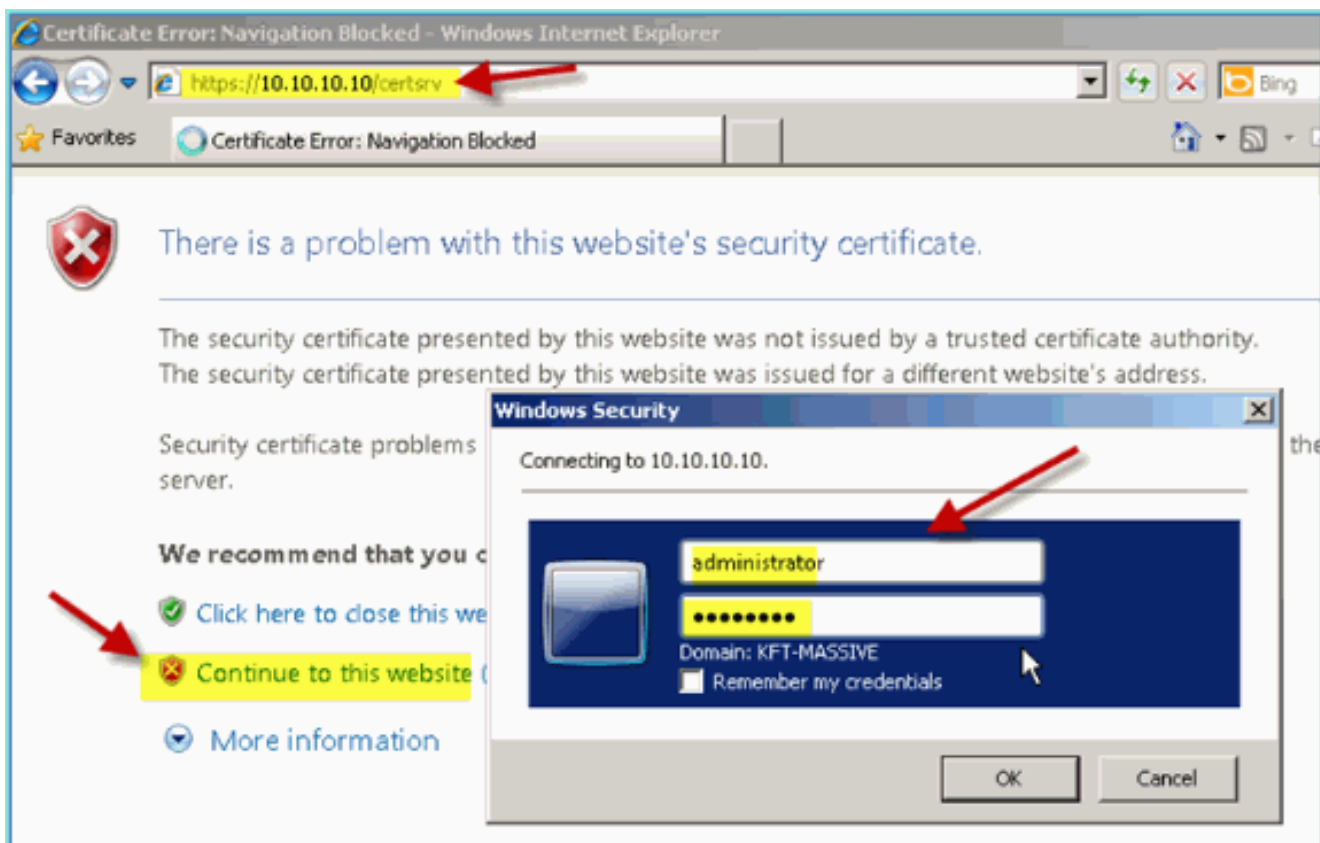
يتم إكمال عنوان URL الأصلي، ويتم السماح بالوصول إلى نقطة النهاية كضيف.

## تكوين الشهادة

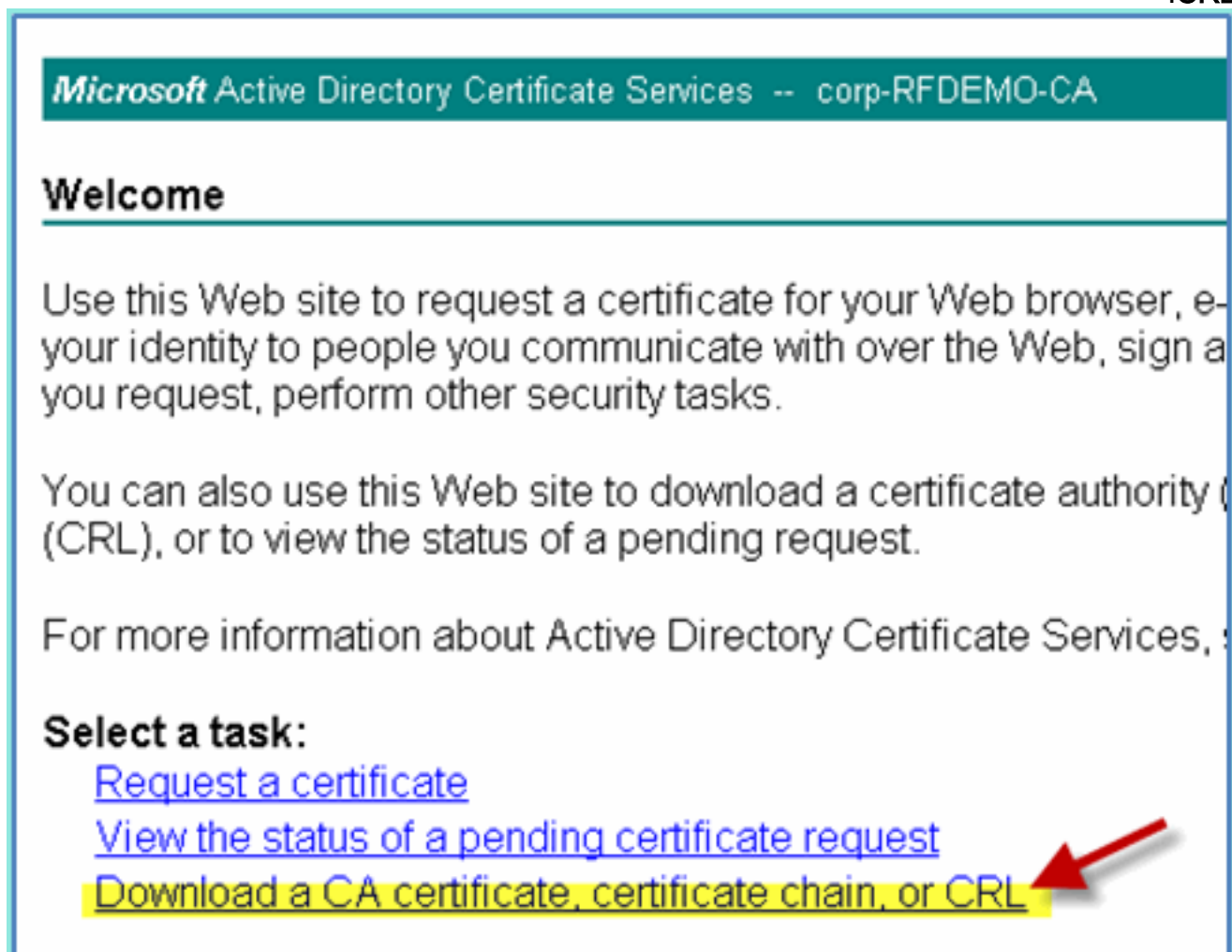
من أجل تأمين الاتصالات مع ISE، حدد ما إذا كان الاتصال متصلًا بالمصادقة أو لإدارة ISE. على سبيل المثال، للتكوين باستخدام واجهة مستخدم ISE على الويب، يلزم تكوين شهادات X.509 وسلاسل ائتمان الشهادات لتمكين التشفير غير المتماثل.

أكمل الخطوات التالية:

1. من الكمبيوتر المتصل السلكي، افتح نافذة مستعرض إلى <https://AD/certsrv>. ملاحظة: استخدم بروتوكول HTTP الآمن. ملاحظة: استخدم Mozilla Firefox أو MS Internet Explorer للوصول إلى ISE.
2. سجل الدخول كمسؤول/Cisco123.



3. انقر على تنزيل شهادة CA أو سلسلة شهادات أو .CRL



4. انقر على تنزيل شهادة المرجع المصدق واحفظها (لاحظ موقع

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

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install the certificate on your computer.

To download a CA certificate, certificate chain, or CRL, select the type of file you want to download:

**CA certificate:**

Current [corp-RFDEMO-CA]

**Encoding method:**

DER  
 Base 64

[Download CA certificate](#)  
[Download CA certificate chain](#)  
[Download latest base CRL](#)  
[Download latest delta CRL](#)

(الحفظ)

5. افتح نافذة مستعرض على Pod-ISE <https://>.
6. انتقل إلى إدارة < نظام < شهادات < شهادات مرجع شهادات.

**CISCO Identity Services Engine**

Home Monitor Policy Administration

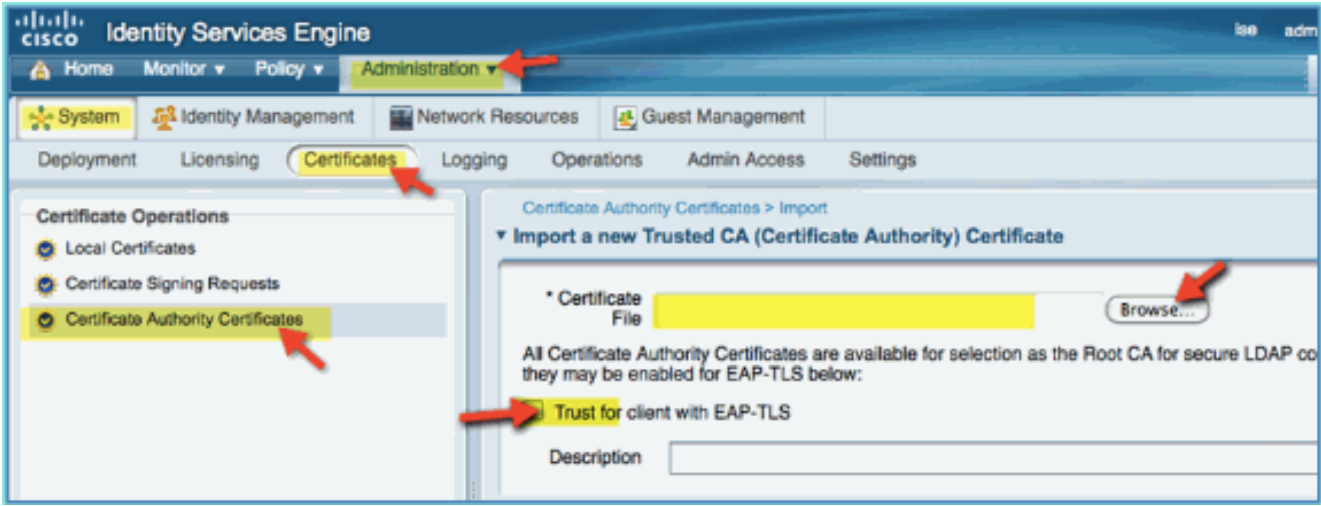
Metrics

Active Endpoints

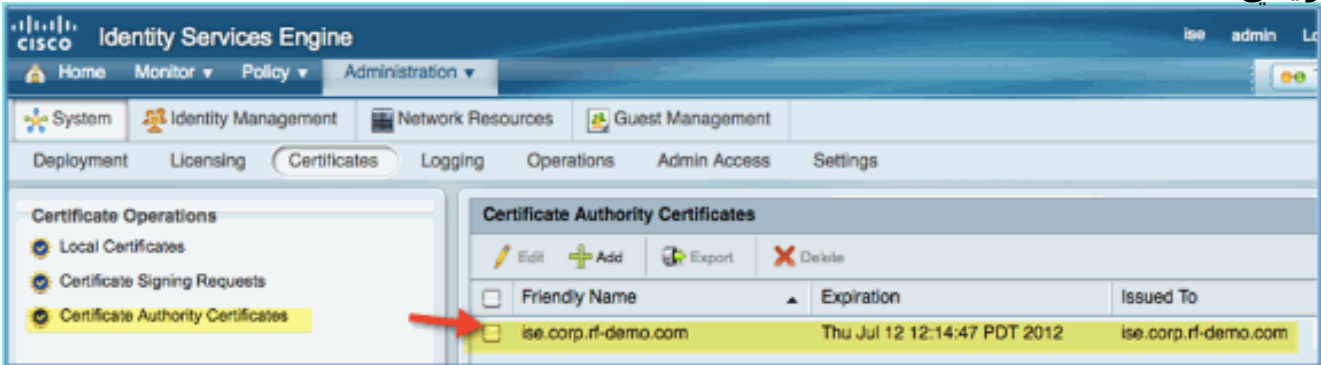
0

System  
Deployment  
Licensing  
**Certificates**

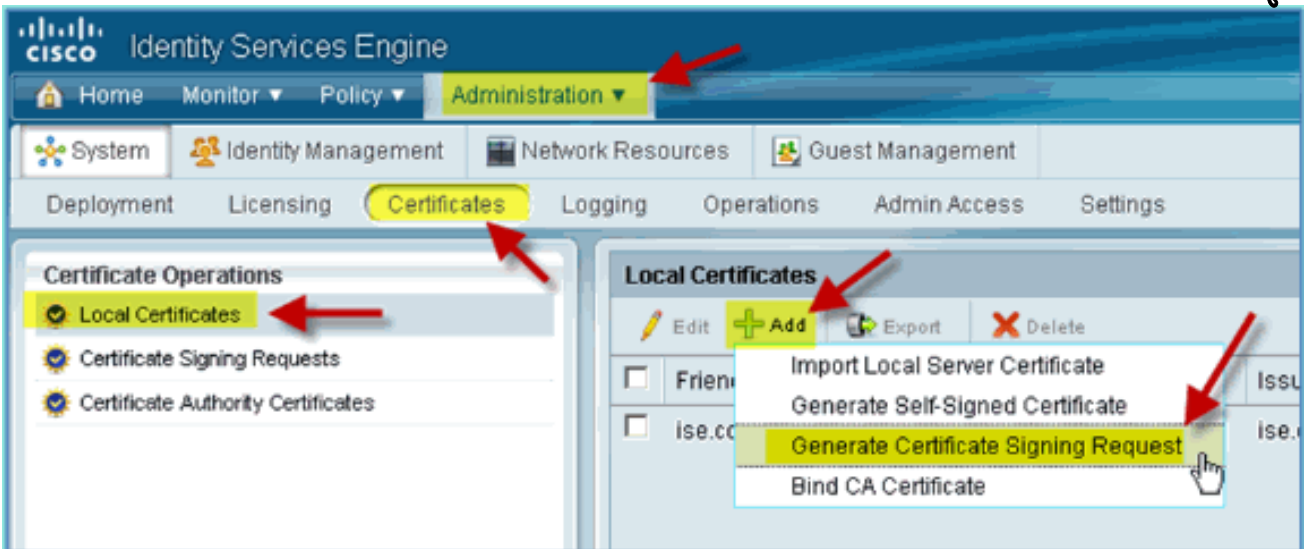
7. حدد عملية شهادات المرجع المصدق واستعرض إلى شهادة المرجع المصدق التي تم تنزيلها سابقا.
8. حدد ثقة للعميل مع EAP-TLS، ثم أرسل.



9. تأكد من إضافة المرجع المصدق كمرجع مصدق رئيسي.



10. من متصفح، انتقل إلى إدارة < نظام < شهادات < شهادات مرجع الشهادات.  
11. انقر فوق إضافة، ثم إنشاء طلب توقيع شهادة.



12. إرسال هذه القيم: موضوع الشهادة: cn=ise.corp.rf-demo.com طول المفتاح: 2048

Local Certificates > Generate Certificate Signing Request

▼ Generate Certificate Signing Request

**Certificate**

\* Certificate Subject

\* Key Length

Digest to Sign With SHA1

13. تطلبك ISE بأن تتوفر CSR في صفحة CSR. وانقر فوق OK.



14. حدد CSR من صفحة ISE CSR وانقر فوق تصدير.  
 15. قم بحفظ الملف في أي موقع (على سبيل المثال، التنزيلات، إلخ)  
 16. سيتم حفظ الملف باسم \*.pem.

CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Deployment Licensing Certificates Logging Operations Admin Access Settings

Certificate Operations

- Local Certificates
- Certificate Signing Requests
- Certificate Authority Certificates

Certificate Signing Requests

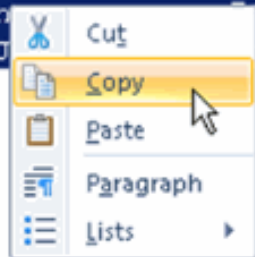
Export Delete

Friendly Name	Certificate Subject	Key Length
<input checked="" type="checkbox"/> ise.corp.rf-demo.com	CN=ise.corp.rf-demo.com	2048

17. حدد موقع ملف CSR وتحريره باستخدام Notepad/Wordpad/TextEdit.  
 18. أنسخ المحتوى (حدد الكل < نسخ).



```
-----BEGIN CERTIFICATE REQUEST-----
MIICyTCCAAbECAQAwHzEdMBSGA1UEAxMUaXNlLmNvcnAucmYtZGVtby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXaeWDSqfI64K59dyRLm8JAXan
WYTAAJ6S/Ke206ws/K3BFAFJQhndQQ0hYVmGcJLVN03pXtRln/q/HBuglLIItIvbe
86FADPq3kUNb48UHcdr9b5rUs7B8T5E6banZia6eHSXjIzX4f0U7mVOrzALeAPDK
HXU+/y/gleyNL6P8zC4bvi/SZXhZp1OvTQpi+8lh14M5ROChhbPUnB3EGVaIVRiN
wYn8Ojvejbtg//k0CItGARlG2IFbBbgUpkMVhDQOgixp3wrlm3hi9JXgffEI4EO
sirLrhvMSuSNESnIVWYrRLz5Xt4dMct+bu08xaEYPqoukYjxsA9gn0bRDMJAgMB
AAGgZTBjBgkqhkiG9w0BCQ4xVjBUMAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQU2jmj
715rSw0yVb/vlWAYkK/YBwkWewYDVR0lBAwwCgYIKwYBBQUHAWewEQYJYIZIAYb4
QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUAA4IBAQBz4YPO9sN7WF2HtG+48300mw9q
gA/MMZsTioEPekcunm+ZFtlAXajB32uwHHillc9Rn93TgOWPFxKEX9E89fzSWDK
J4qsQM7KEYOpQt4bia07188Lm6BBTk9mRhiTBw8F3dx0tlzfgiHc72kjWvxsgg/c
kSa7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42riz7vK0g0nkWRHF52uiu3AkP
LPKQ72N2XYIXfu0jdgOAJjmsk6T9nLABVYQ6n...KDJTHchcwx6Ilk/
V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJ...W1ZuB6drHg9
-----END CERTIFICATE REQUEST-----
```



19. افتح نافذة المستعرض على <https://<Pod-AD>/certsrv>
20. انقر على طلب شهادة.

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

### Welcome

Use this Web site to request a certificate for your Web browser to communicate with over the Web, sign and encrypt messages.

You can also use this Web site to download a certificate automatically for a pending request.

For more information about Active Directory Certificate Services, click the following link:

#### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

**Microsoft Active Directory Certificate Services -- corp**

## Request a Certificate

Select the certificate type:  
[User Certificate](#)

Or, submit an **advanced certificate request**



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

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM source (such as a Web server) in the Saved Request box.

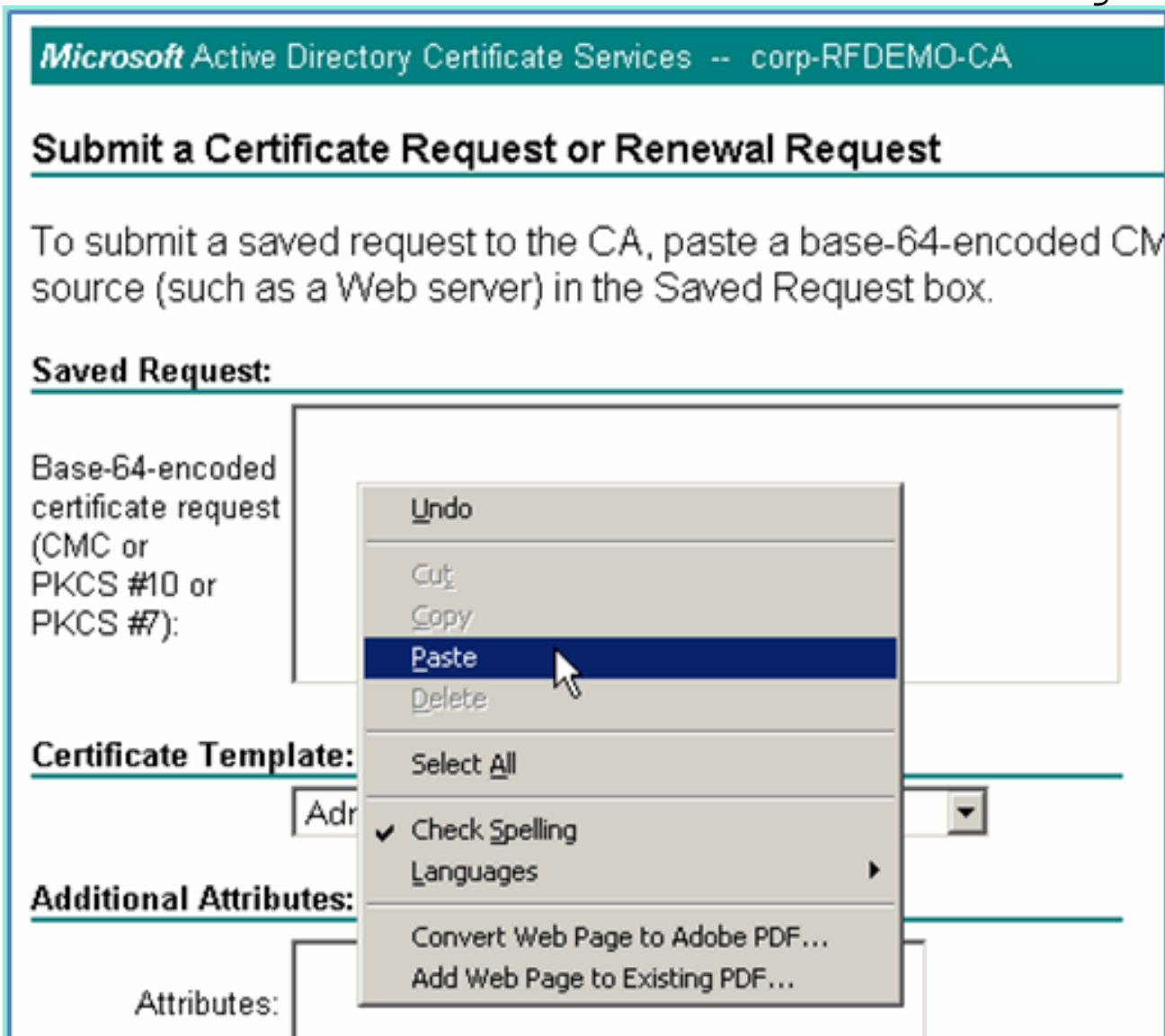
**Saved Request:**

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

**Certificate Template:**

Additional Attributes:

Attributes:



23. حدد خادم ويب كقالب الشهادة، ثم انقر على إرسال.

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

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM source (such as a Web server) in the Saved Request box.

**Saved Request:**

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

```
gA/MMZsTioEPekcunnm+ZFt1AXajB32uwHH11c9  
J4qsQM7KEYOpQt4bia071S8Lm6BBTk9mRhiTBwSF  
kSa7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42  
LPKQ72N2XYIXfu0jdgoaJjmsk6T9nLABVYQ6nKQx  
V5QYBOjTYHXIPG8/ned9z3MOi2d2sm4XNS2bJfO/  
-----END CERTIFICATE REQUEST-----
```

**Certificate Template:**

Web Server

**Additional Attributes:**

Attributes:

Submit >

24. حدد DER المرمز، ثم انقر تنزيل الشهادة.

## Certificate Issued

The certificate you requested was issued to you.



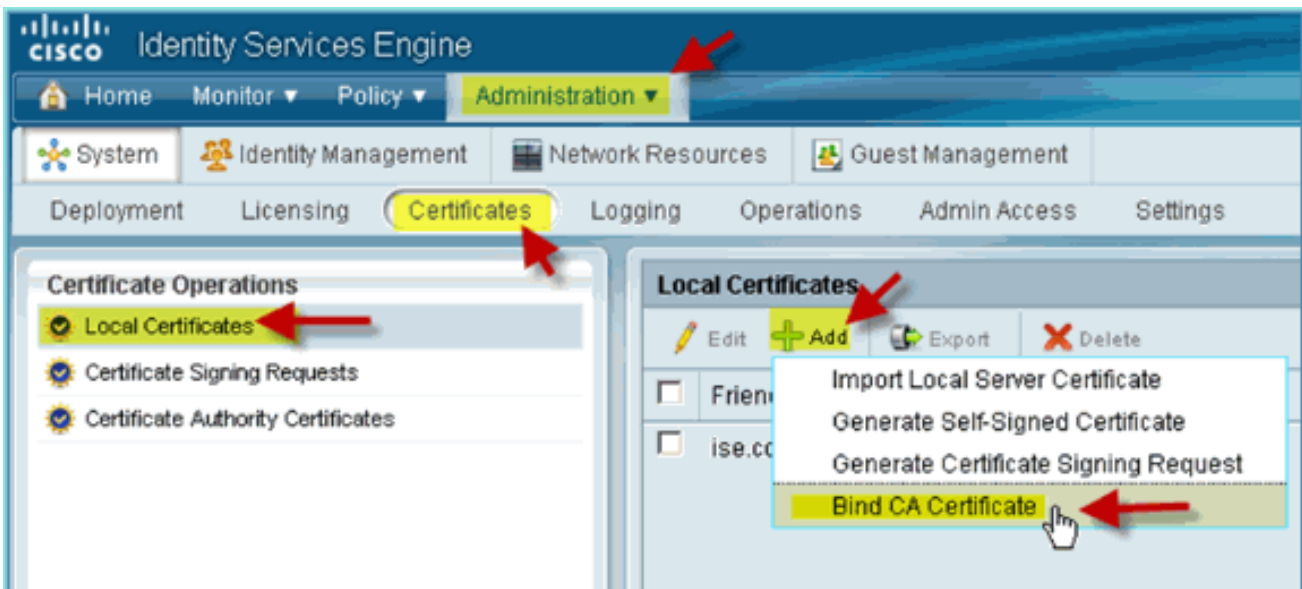
25. حفظ الملف في موقع معروف (على سبيل المثال، التنزيلات)

26. انتقل إلى إدارة < نظام < شهادات < شهادات مرجع

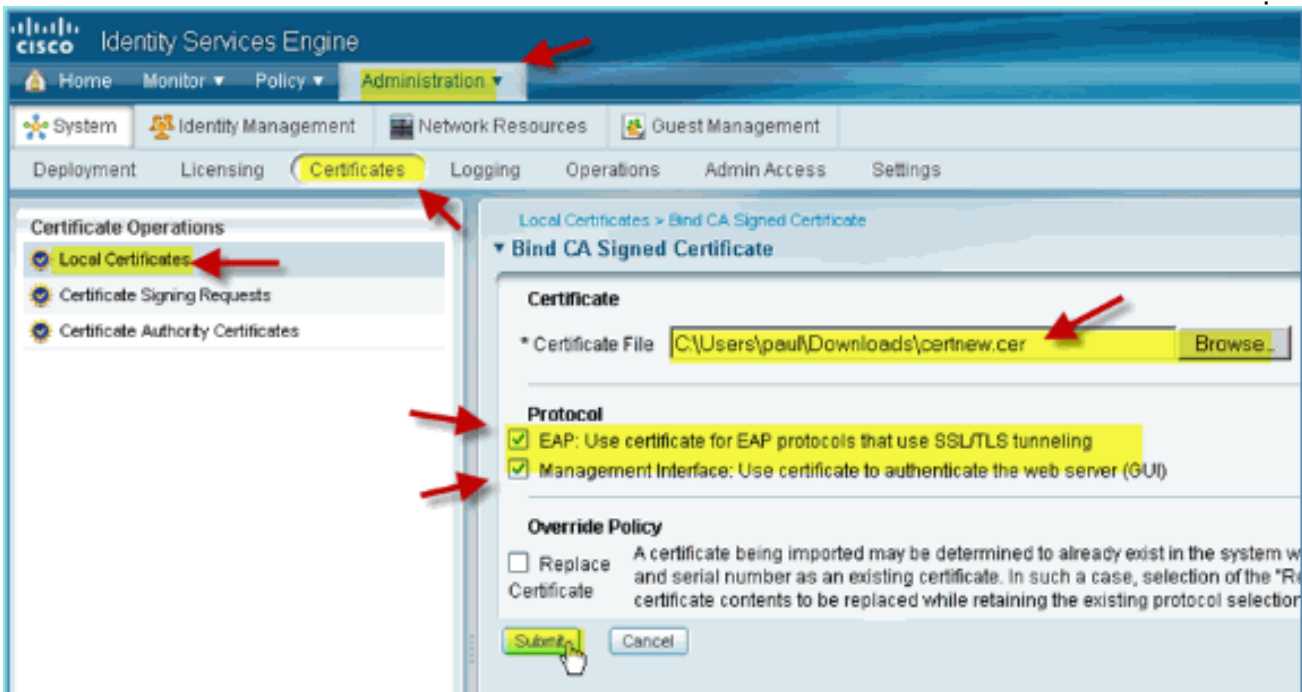


شهادات.

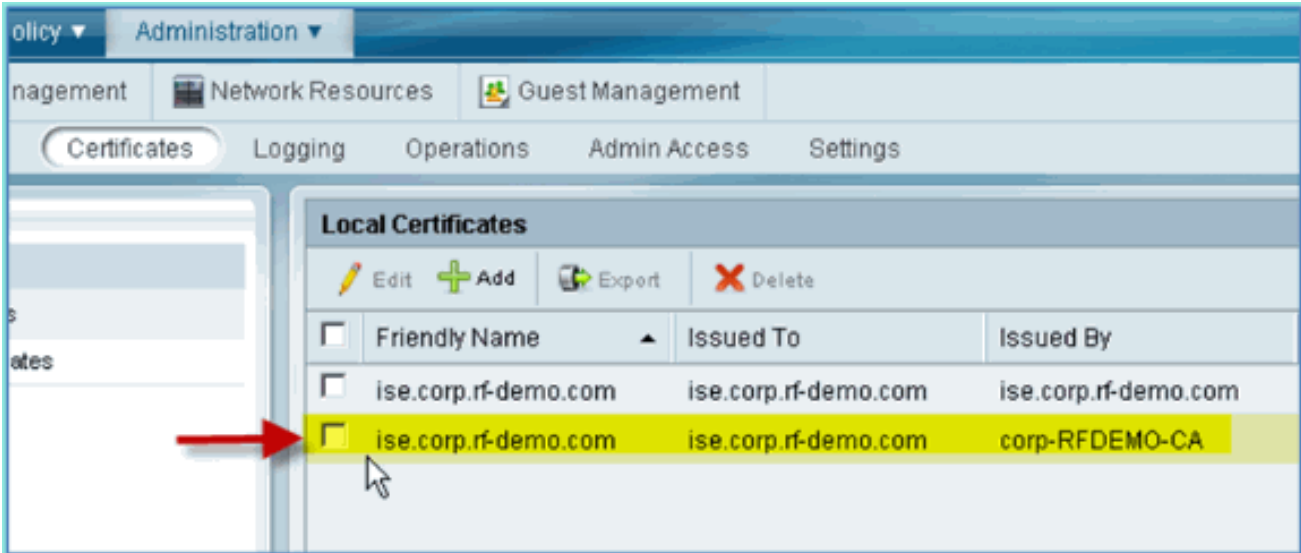
27. انقر على إضافة < ربط شهادة المرجع المصدق.



28. تصفح إلى شهادة المرجع المصدق التي تم تنزيلها سابقاً.



29. حدد كل من بروتوكول EAP وواجهة الإدارة، ثم انقر على إرسال.  
30. تأكد من إضافة المرجع المصدق كمرجع مصدق رئيسي.

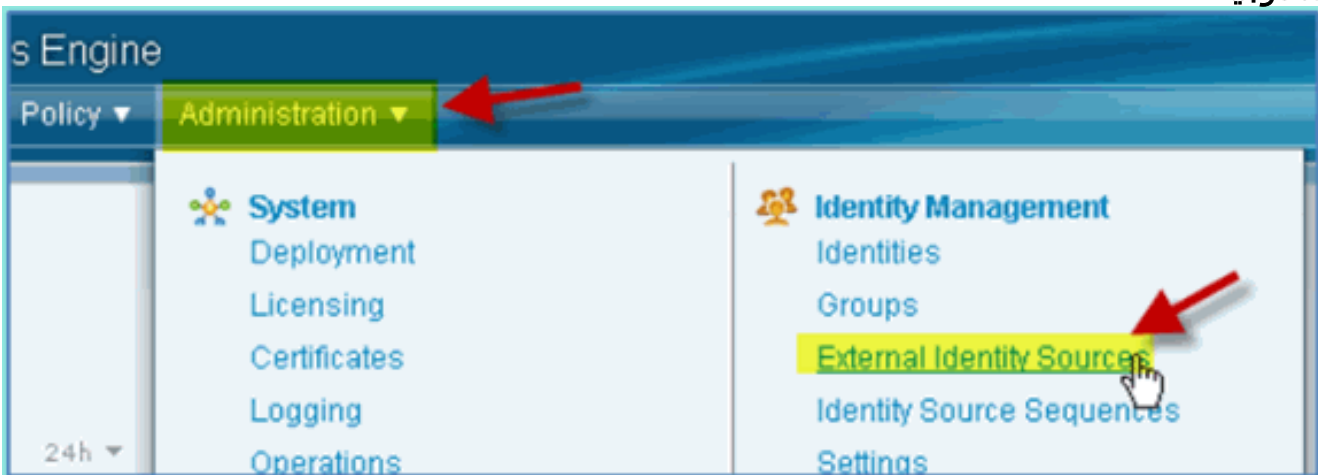


## تكمال Windows 2008 Active Directory

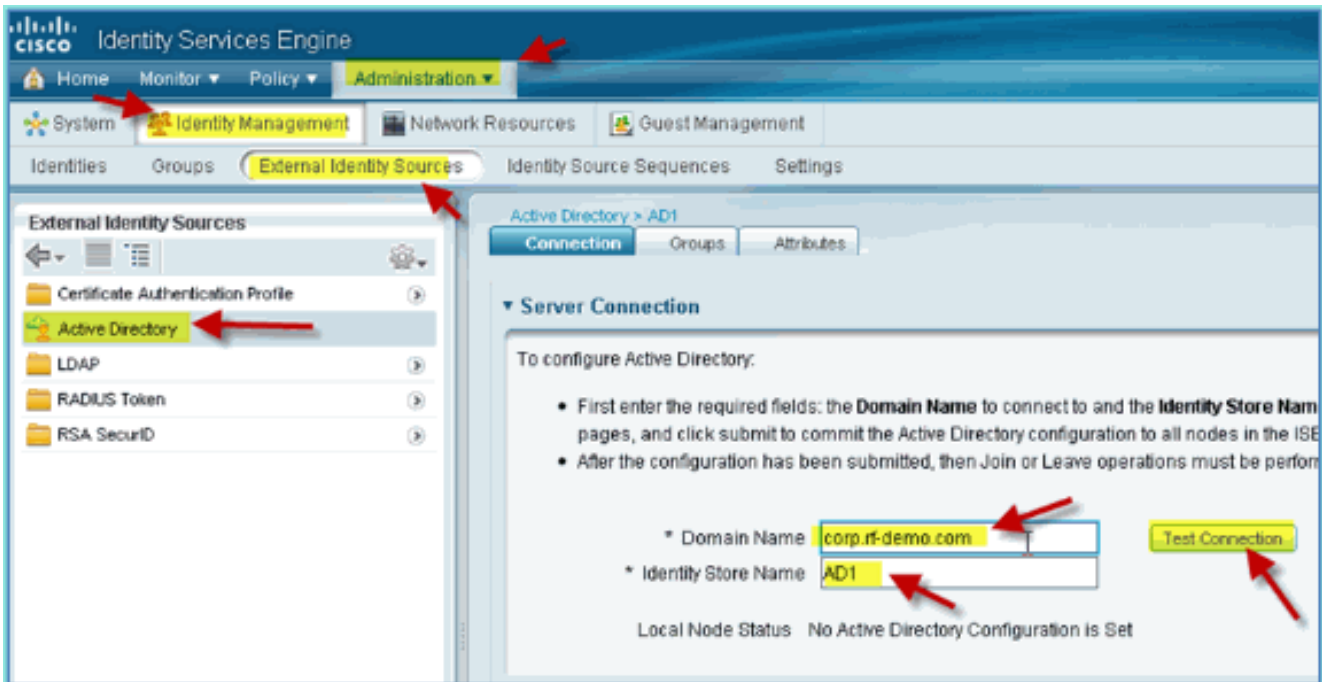
يمكن أن يتصل ISE مباشرة مع Active Directory (AD) لمصادقة المستخدم/الجهاز أو لاسترداد سمات مستخدم معلومات التحويل. من أجل الاتصال ب AD، يجب أن يكون ISE "منضمًا" إلى مجال AD. في هذا التمرين سنتنضم إلى ISE إلى مجال AD، وتأكد من أن اتصال AD يعمل بشكل صحيح.

أكمل الخطوات التالية:

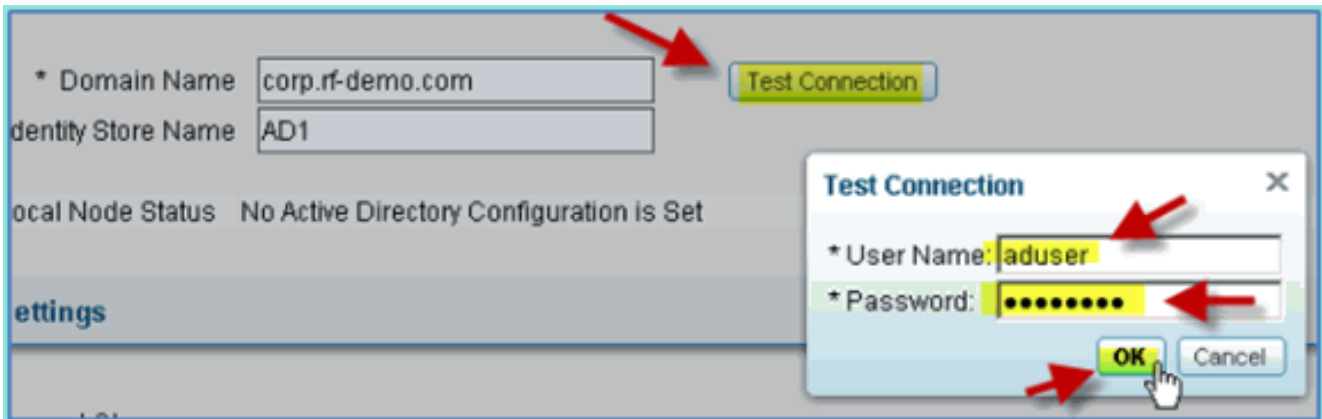
1. من أجل الانضمام إلى ISE إلى مجال AD، انتقل من ISE إلى الإدارة < إدارة الهوية < مصادر الهوية الخارجية.



2. من الجزء الأيسر (مصادر الهوية الخارجية)، حدد **Active Directory**.
3. على الجانب الأيمن، حدد علامة التبويب **توصيل** وأدخل ما يلي: اسم المجال: corp.rf-demo.com اسم مخزن الهوية: AD1



4. انقر على إختبار الاتصال. (دخلت aduser/Cisco123 (AD username) بعد ذلك طقطقت .ok



5. تأكد من أن إختبار الحالة نجح.

6. حدد إظهار السجل التفصيلي وملاحظة التفاصيل المفيدة لاستكشاف الأخطاء وإصلاحها. انقر فوق موافق" للمتابعة.

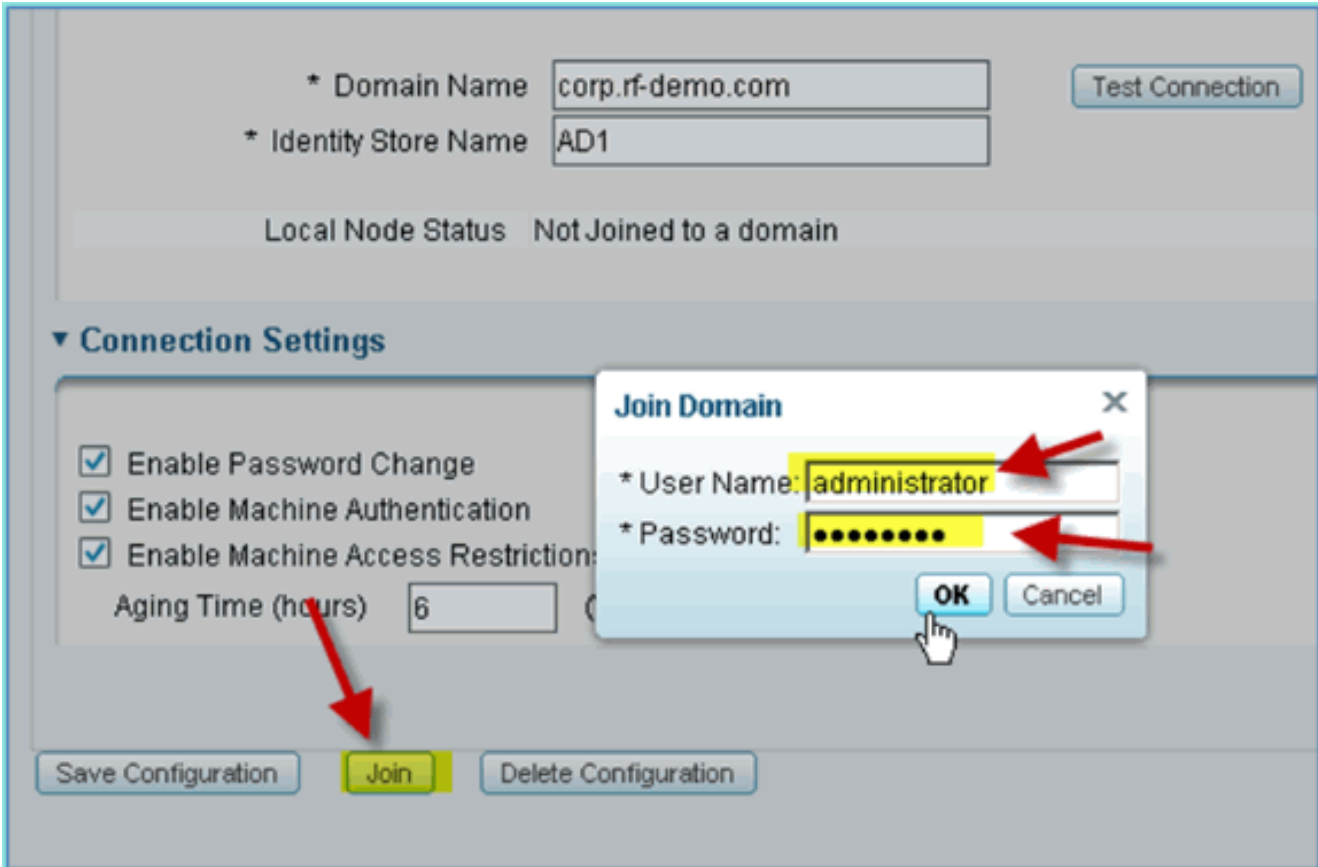


7. انقر على حفظ التكوين.

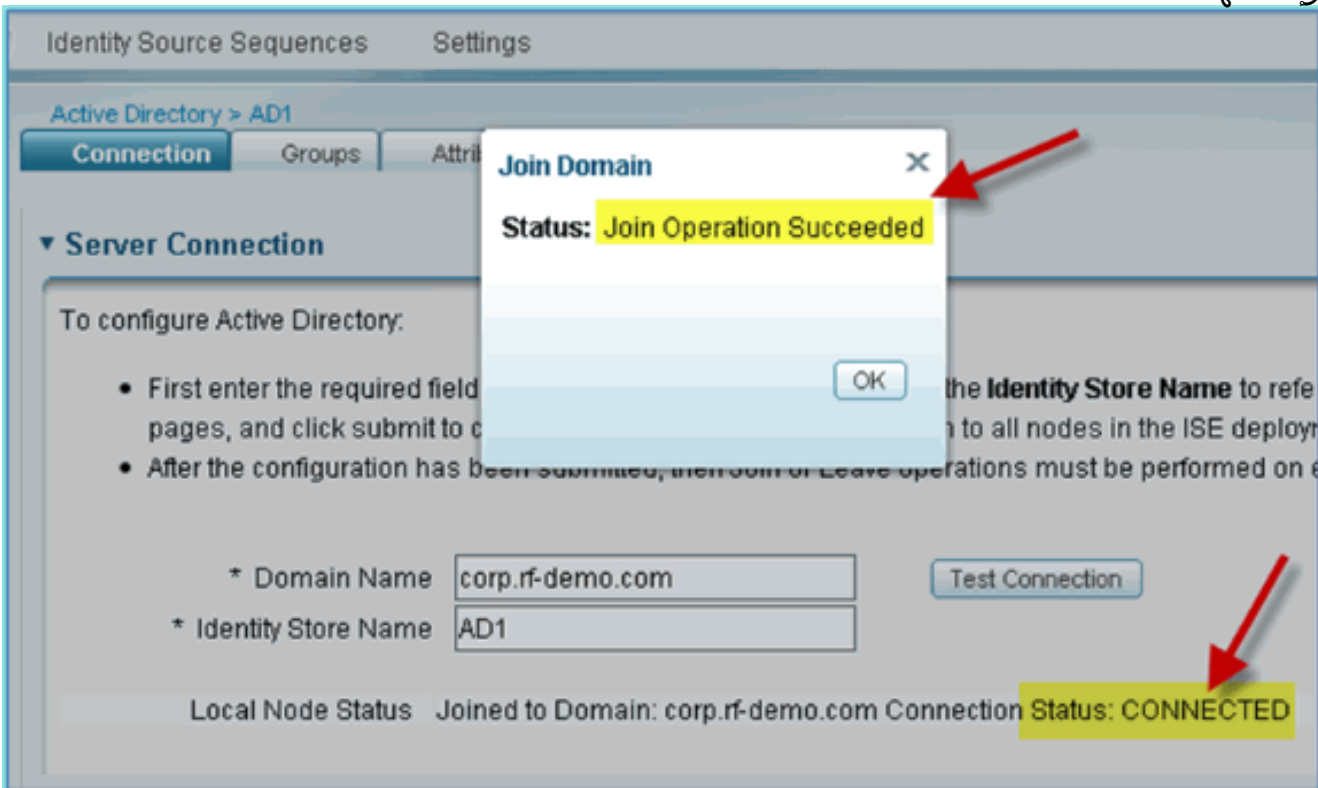


8. انقر فوق الانضمام. أدخل مستخدم الإعلان (administrator/Cisco123)، ثم انقر فوق موافق.





9. تأكد من نجاح عرض حالة عملية الانضمام، ثم انقر فوق موافق للمتابعة. تظهر حالة اتصال الخادم متصلة. إذا تغيرت هذه الحالة في أي وقت، يساعد "اتصال الاختبار" في أكتشاف أخطاء عمليات AD وإصلاحها.



## إضافة مجموعات Active Directory

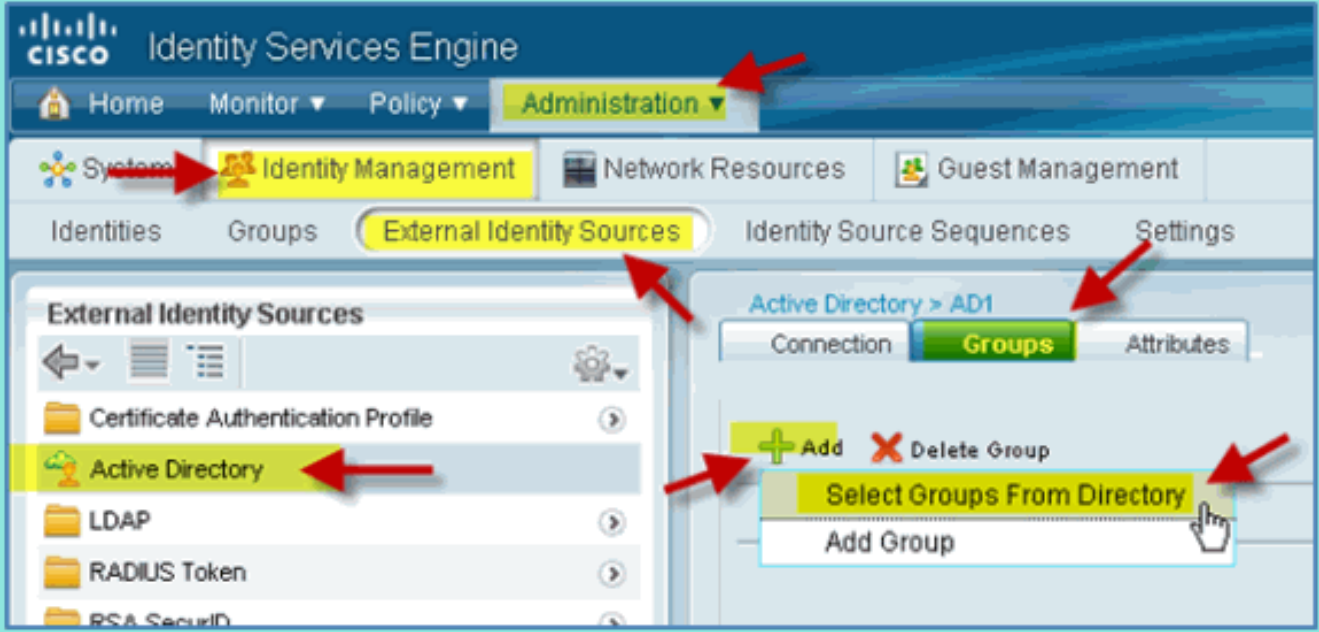
عند إضافة مجموعات AD، يتم السماح بتحكم أكثر دقة في سياسات ISE. على سبيل المثال، يمكن التمييز بين مجموعات الإعلان (AD) حسب الأدوار الوظيفية، مثل مجموعات الموظفين أو المقاولين، دون حدوث الخطأ ذي الصلة

في ممارسات ISE 1.0 السابقة حيث كانت السياسات تقتصر على المستخدمين فقط.

في هذا المختبر، يتم استخدام مستخدمي المجال و/أو مجموعة الموظفين فقط.

أكمل الخطوات التالية:

1. من ISE، انتقل إلى الإدارة < إدارة الهوية < مصادر الهوية الخارجية.
2. حدد Active Directory < علامة التبويب مجموعات.
3. انقر فوق +إضافة، ثم حدد مجموعات من الدليل.



4. في نافذة المتابعة (حدد مجموعات الدليل)، اقبل الافتراضيات للمجال (corp-rf-demo.com) ومرشح (\*). ثم انقر فوق إستراداد المجموعات.

## Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to reat Use \* for wildcard search (i.e. admin\*). Search filter applies to group name and not th

Domain:

Filter:

**Retrieve Groups..**

Number of Grou

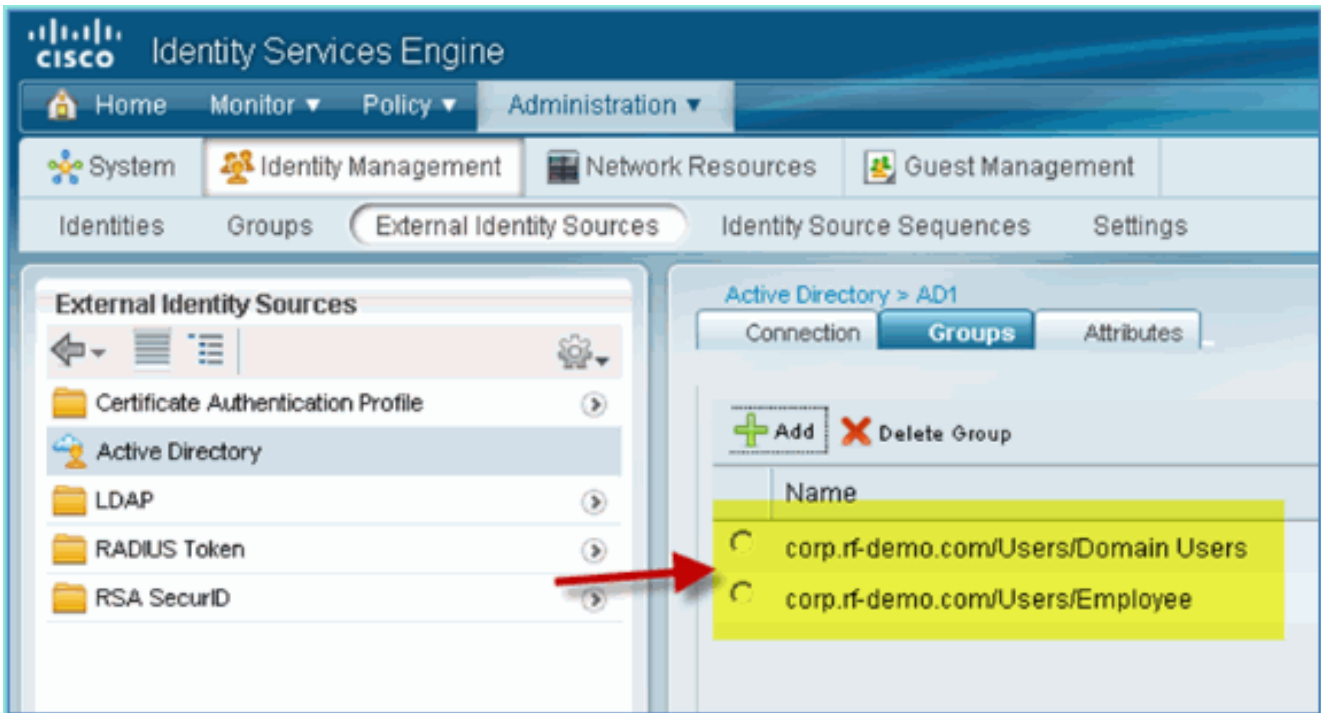
- | <input type="checkbox"/> | Name                                      |
|--------------------------|---|
| <input type="checkbox"/> | corp.rf-demo.com/Users/DnsUpdateProxy     |
| <input type="checkbox"/> | corp.rf-demo.com/Users/Domain Admins      |
| <input type="checkbox"/> | corp.rf-demo.com/Users/Domain Computers   |
| <input type="checkbox"/> | corp.rf-demo.com/Users/Domain Controllers |
| <input type="checkbox"/> | corp.rf-demo.com/Users/Domain Guests      |
| <input type="checkbox"/> | corp.rf-demo.com/Users/Domain Users       |
| <input type="checkbox"/> | corp.rf-demo.com/Users/Employee           |
| <input type="checkbox"/> | corp.rf-demo.com/Users/Enterprise Admins  |

5. حدد المربعات لمستخدمي المجال و مجموعات الموظفين. طققة ok عندما إنتهيت.

<input type="checkbox"/>	corp.rf-demo.com/Users/Domain Computers	GLOBAL
<input type="checkbox"/>	corp.rf-demo.com/Users/Domain Controllers	GLOBAL
<input type="checkbox"/>	corp.rf-demo.com/Users/Domain Guests	GLOBAL
<input checked="" type="checkbox"/>	corp.rf-demo.com/Users/Domain Users	GLOBAL
<input checked="" type="checkbox"/>	corp.rf-demo.com/Users/Employee	GLOBAL
<input type="checkbox"/>	corp.rf-demo.com/Users/Enterprise Admins	UNIVERSAL
<input type="checkbox"/>	corp.rf-demo.com/Users/Enterprise Read-only Domain Controllers	UNIVERSAL
<input type="checkbox"/>	corp.rf-demo.com/Users/Group Policy Creator Owners	GLOBAL
<input type="checkbox"/>	corp.rf-demo.com/Users/RAS and IAS Servers	LOCAL
<input type="checkbox"/>	corp.rf-demo.com/Users/Read-only Domain Controllers	GLOBAL
<input type="checkbox"/>	corp.rf-demo.com/Users/Schema Admins	UNIVERSAL

**OK** Cancel

6. تأكد من إضافة المجموعات إلى القائمة.

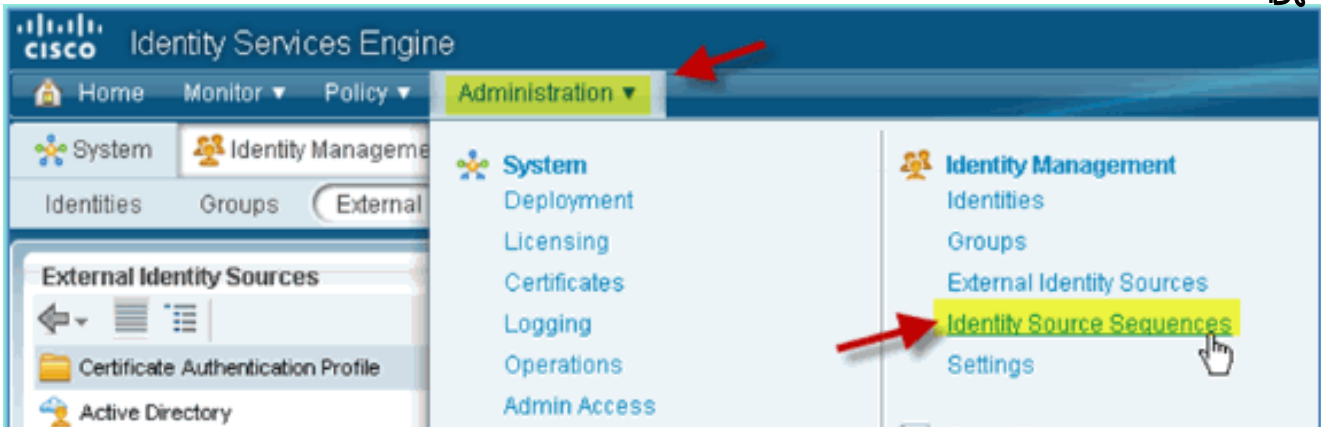


## إضافة تسلسل مصدر الهوية

وبشكل افتراضي، يتم تعيين ISE لاستخدام المستخدمين الداخليين لمخزن المصادقة. في حالة إضافة AD، يمكن إنشاء ترتيب تسلسل ذو أولوية لتضمين AD الذي سيستخدمه ISE للتحقق من المصادقة.

أكمل الخطوات التالية:

1. من ISE، انتقل إلى إدارة < إدارة الهوية > تسلسلات مصدر الهوية.



2. انقر فوق +إضافة لإضافة تسلسل جديد.

The screenshot shows the Cisco Identity Services Engine Administration interface. The top navigation bar includes 'Home', 'Monitor', 'Policy', and 'Administration'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', and 'Guest Management'. The main content area is titled 'Identity Source Sequences' and contains a table with columns for 'Name', 'Description', and 'Identity Stores'. The table lists two built-in sequences: 'Guest\_Portal\_Sequence' and 'Sponsor\_Portal\_Sequence'. Above the table, there are action buttons: 'Edit', 'Add', 'Duplicate', and 'Delete'. A red arrow points to the 'Add' button.

Name	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

3. أدخل الاسم الجديد: **AD\_Internal**. إضافة كافة المصادر المتاحة إلى الحقل المحدد. ثم قم بإعادة الترتيب حسب الحاجة بحيث يتم نقل AD1 إلى أعلى القائمة. انقر على إرسال.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > New Identity Source Sequence

**▼ Identity Source Sequence**

\* Name

Description

**▼ Certificate Based Authentication**

Select Certificate Authentication Profile

**▼ Authentication Search List**

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
	AD1
	Internal Users
	Internal Endpoints

**▼ Advanced Search List Settings**

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

4. تأكد من إضافة التسلسل إلى القائمة.

CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Identities Groups External Identity Sources **Identity Source Sequences** Settings

**Identity Source Sequences**

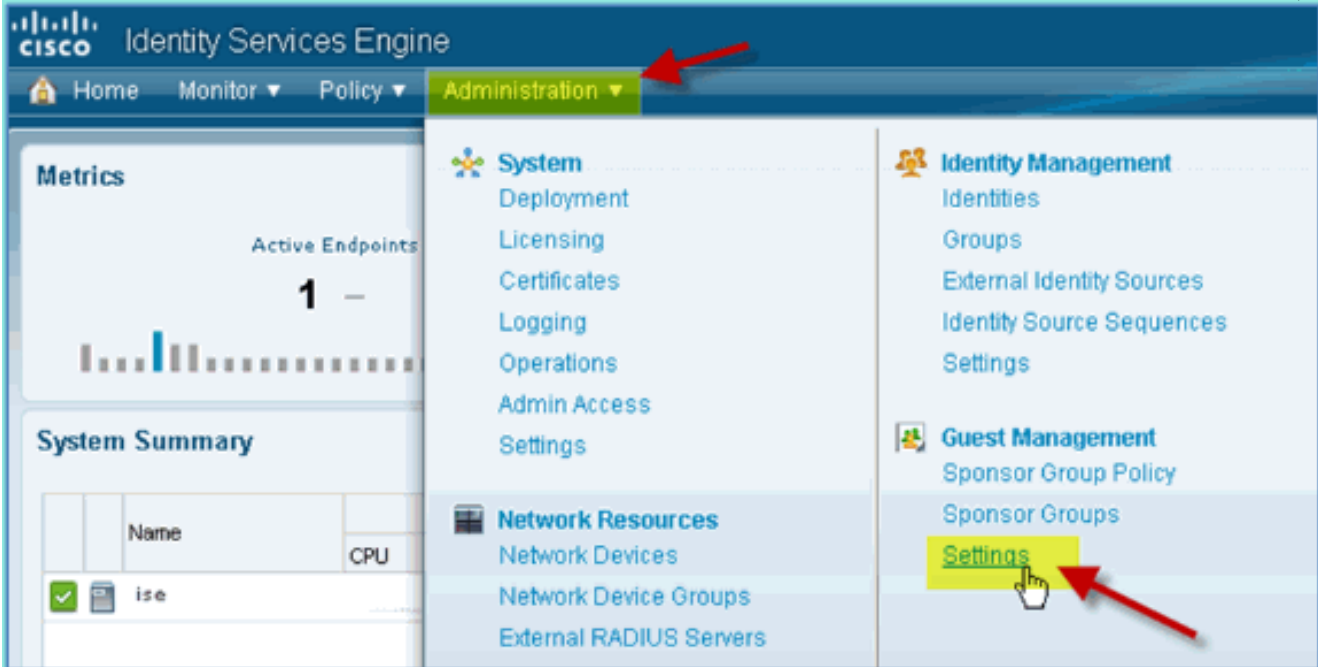
Edit Add Duplicate Delete Filter

Name	Description	Identity Stores
AD_Internal		AD1,Internal Endpoints,Internal Users
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

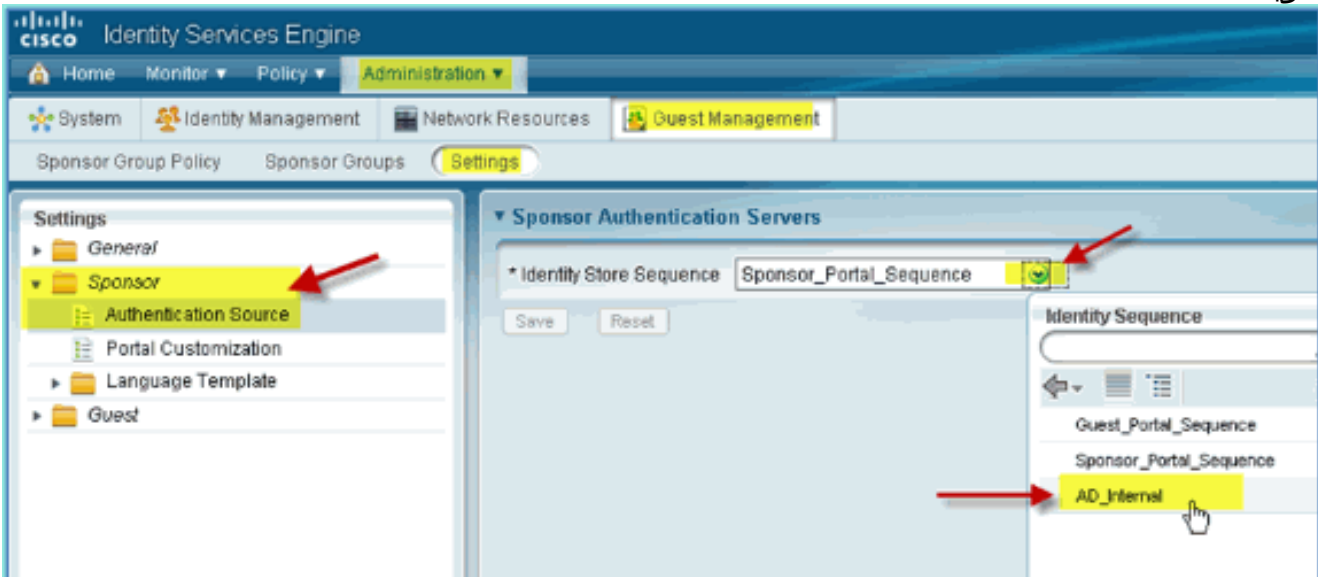
## وصول الضيف الذي ترعاه ISE Wireless مع إعلان مدمج

يمكن تكوين ISE للسماح برعاية الضيوف بواسطة سياسات للسماح لمستخدمي مجال AD برعاية الوصول للضيف.  
أكمل الخطوات التالية:

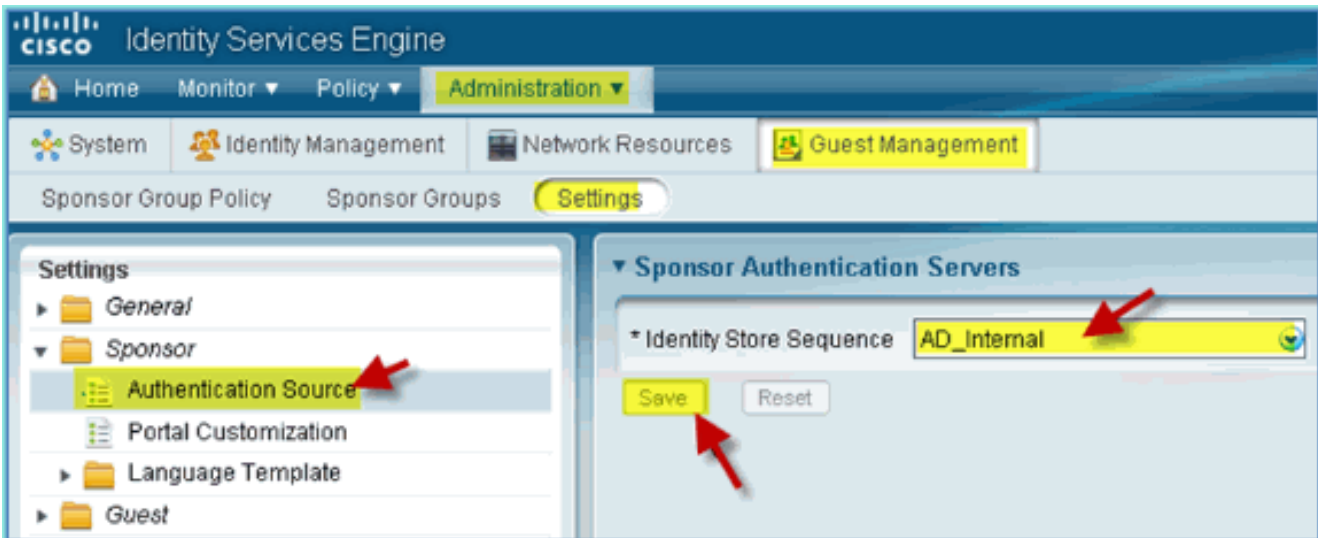
1. من ISE، انتقل إلى الإدارة < إدارة الضيوف > الإعدادات.



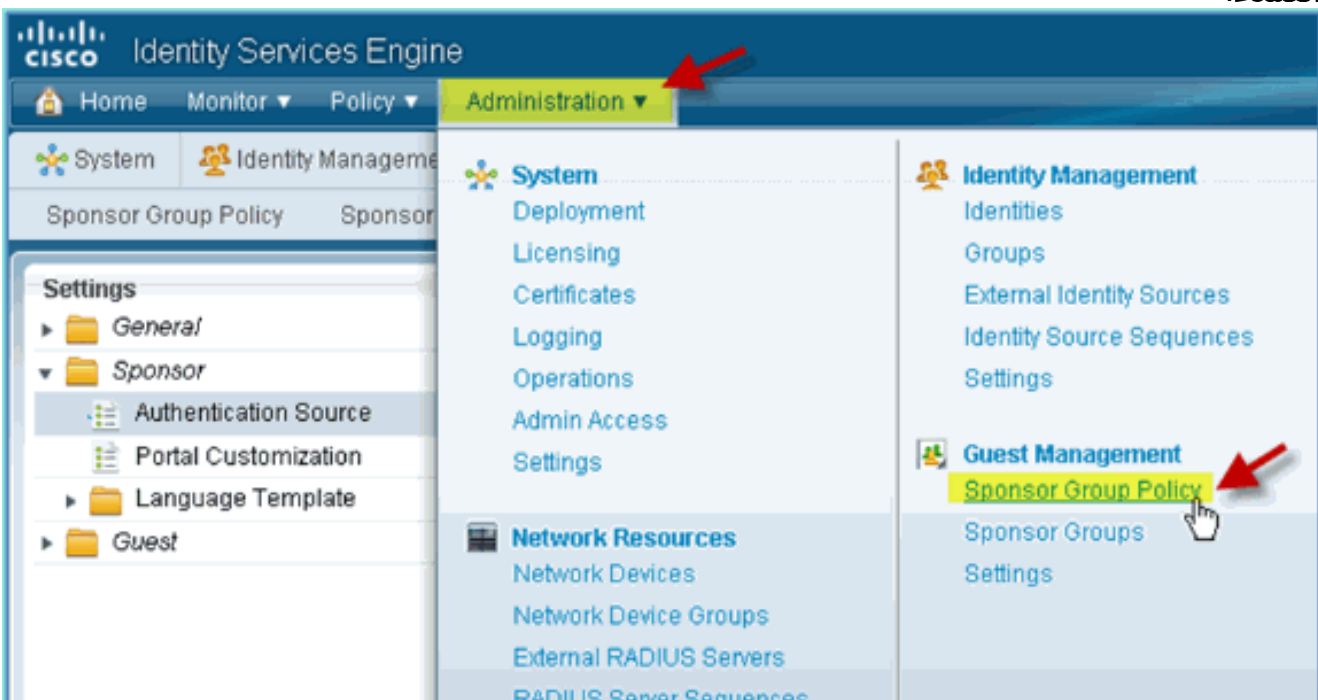
2. قم بتوسيع الكفيل، وانقر مصدر المصادقة. ثم حدد AD\_Internal كتسلسل مخزن هوية.



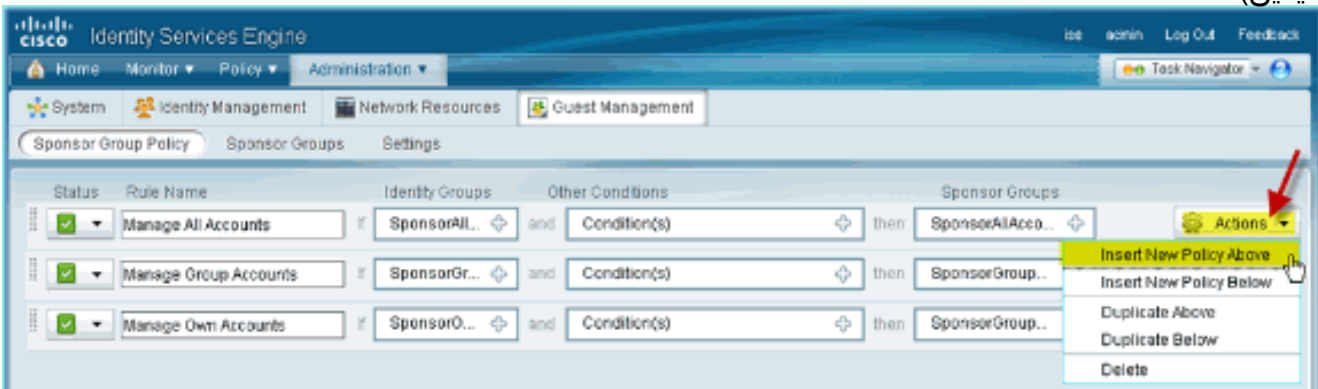
3. تأكيد AD\_Internal كتسلسل مخزن الهويات. قطعة حفظ.



4. انتقل إلى إدارة < إدارة الضيوف > سياسة مجموعة العملاء.



5. قم بإدراج نهج جديد فوق القاعدة الأولى (انقر فوق رمز الإجراءات من اليمين).



6. بالنسبة لنهج مجموعة الكفيل الجديد، قم بإنشاء ما يلي: اسم القاعدة: مستخدمو المجال/مجموعات الهوية: أي شروط أخرى: (إنشاء جديد/متقدم) < AD1

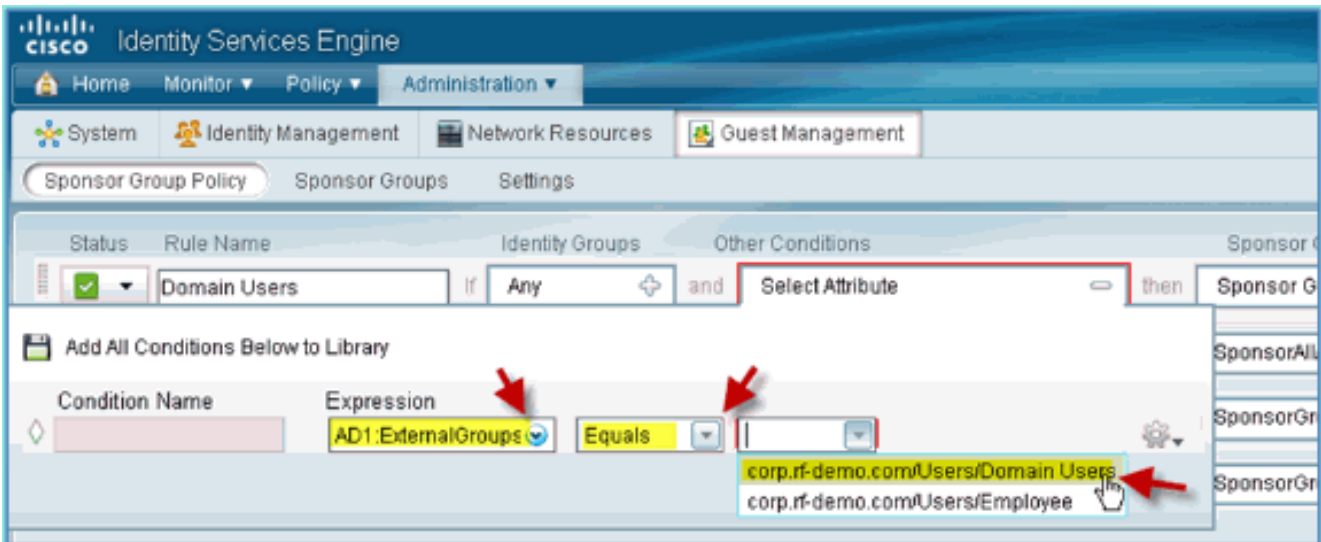


CISCO Identity Services Engine Administration console. The 'Administration' tab is active. The 'Sponsor Group Policy' section is selected, showing a rule named 'Domain Users'. The rule status is 'On' (checked). The rule expression is 'Select Attribute'. A 'Dictionaries' dropdown menu is open, showing a list of dictionaries: 'AD1', 'Airespace', and 'CERTIFICATE'. The 'AD1' dictionary is selected. Red arrows point to the 'Select Attribute' dropdown and the 'AD1' folder.

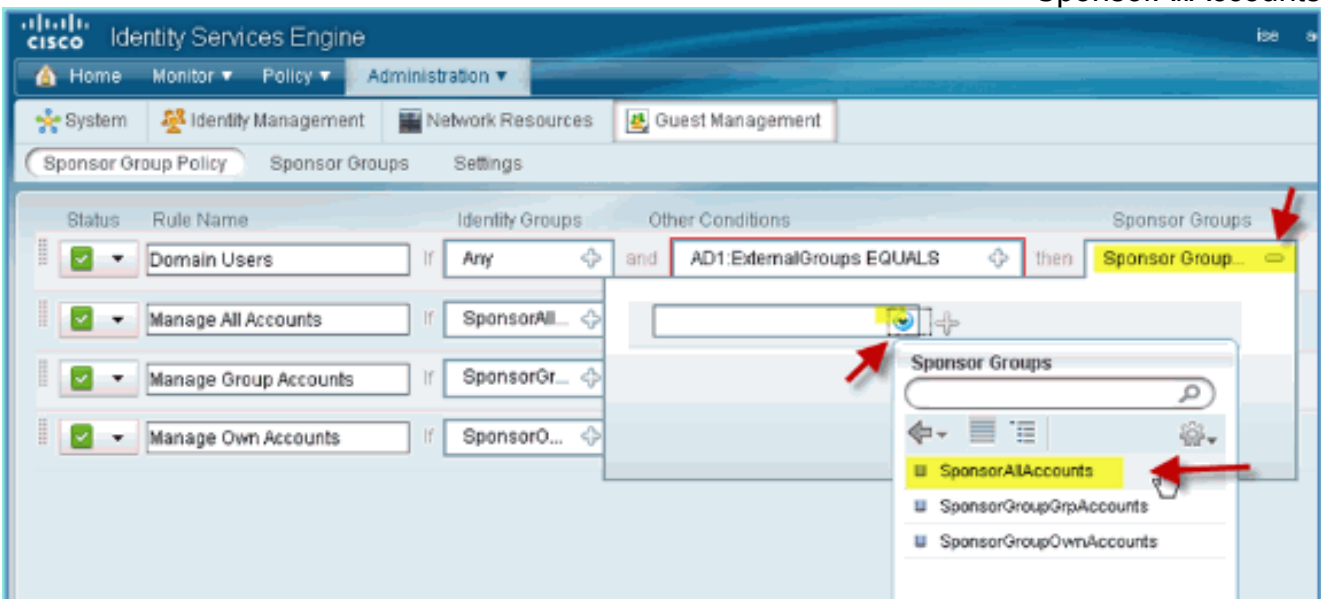
AD1: المجموعات الخارجية

CISCO Identity Services Engine Administration console. The 'Administration' tab is active. The 'Sponsor Group Policy' section is selected, showing a rule named 'Domain Users'. The rule status is 'On' (checked). The rule expression is 'Select Attribute'. A dropdown menu is open, showing a list of dictionaries: 'AD1', 'Airespace', and 'CERTIFICATE'. The 'AD1' dictionary is selected. The 'ExternalGroups' folder is highlighted. Red arrows point to the 'Domain Users' rule name, the 'Select Attribute' dropdown, and the 'ExternalGroups' folder.

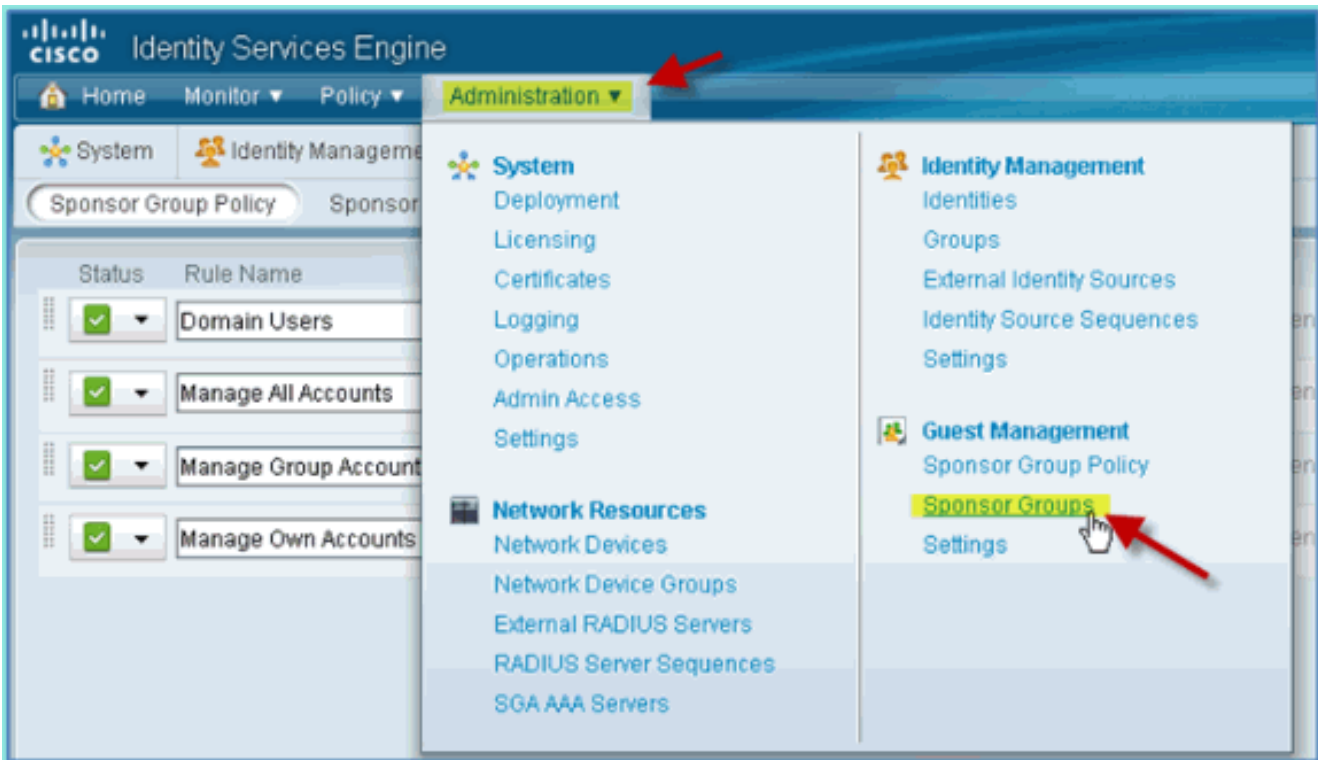
مجموعات AD1 الخارجية < يساوي > مستخدمى -corp.rf demo.com/Users/Domain



7. في مجموعات الكفيل، قم بتعيين ما يلي: مجموعات الكفيل:  
SponsorAllAccounts

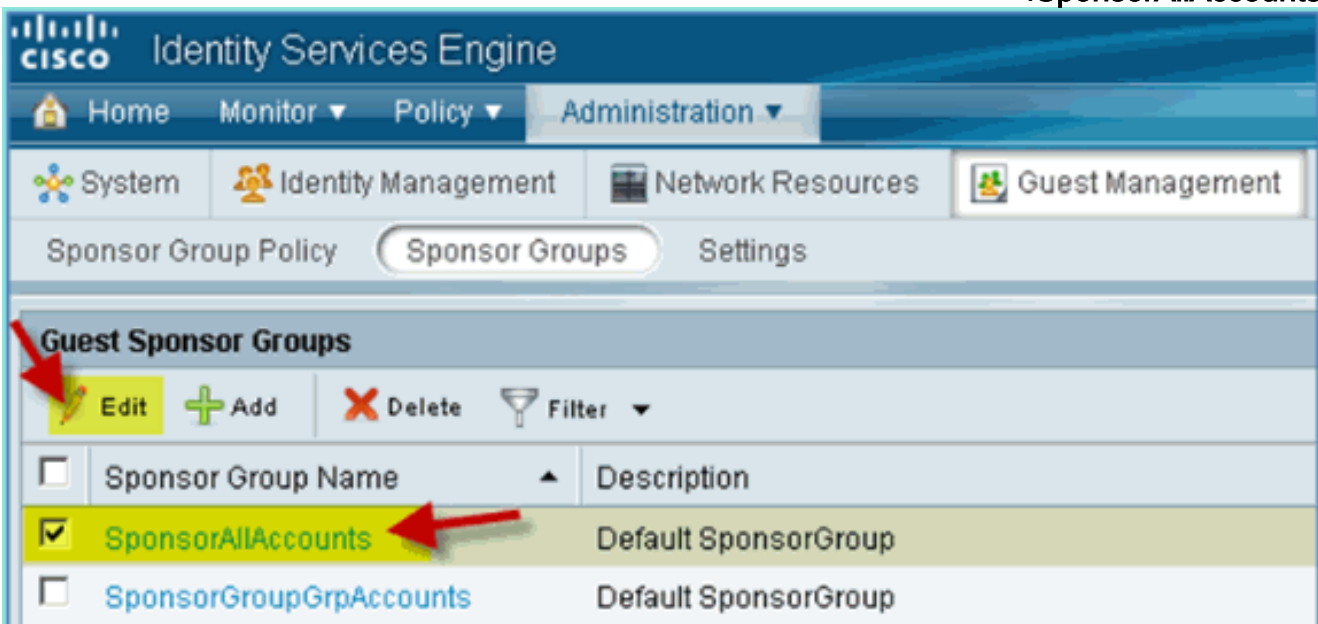


8. انتقل إلى إدارة < إدارة الضيوف > مجموعات الرعاية.



9. حدد لتحرير <

.SponsorAllAccounts



10. حدد مستويات التحويل، ثم قم بتعيين ما يلي: عرض كلمة مرور الضيف:  
نعم

**CISCO Identity Services Engine**

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Sponsor Group List > SponsorAllAccounts

General Authorization Levels Guest Roles Time Profiles

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

Save Reset

## شكلت فسحة بين دعامتین علی المفتاح

شكلت فسحة بين دعامتین - ISE mgt/probe قارن L2 مجاور إلى WLC إدارة قارن. المفتاح يستطيع كنت شكلت أن يجسر و آخر قارن، مثل موظف و ضیف قارن VLANs.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface
```

## المرجع: المصادقة اللاسلكية لنظام التشغيل Apple Mac OS X

يمكنك الاقتران بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال بطاقة SSID مصدق عليها كمستخدم داخلي (أو مستخدم إعلانات مدمج) باستخدام كمبيوتر محمول لاسلكي من طراز Apple Mac OS X. التخطي إذا لم

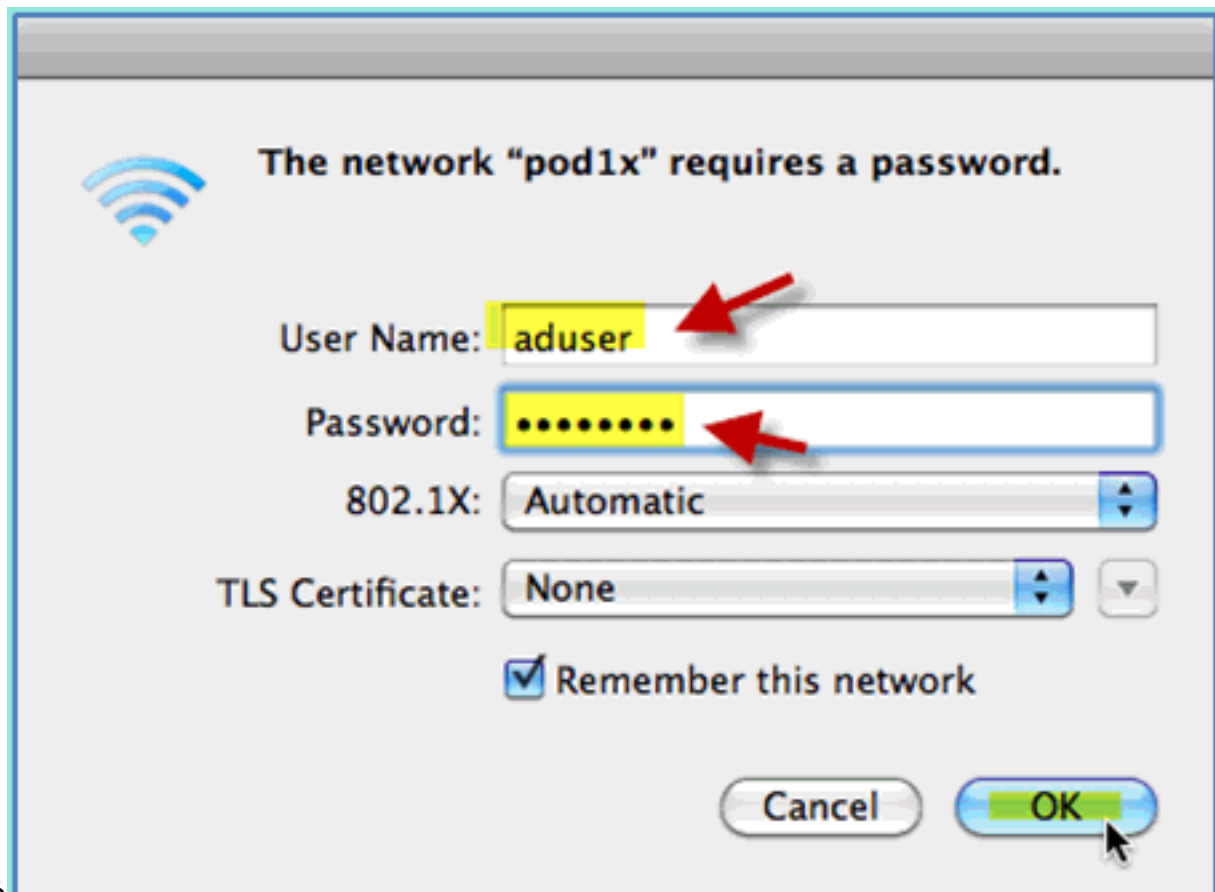
يكن قابلا للتطبيق.

1. على Mac، انتقل إلى إعدادات WLAN. تمكين WiFi ثم تحديد PoD SSID الممكن لـ 802.1X والذي تم



إنشأؤه في التمرين السابق وتوصيله.

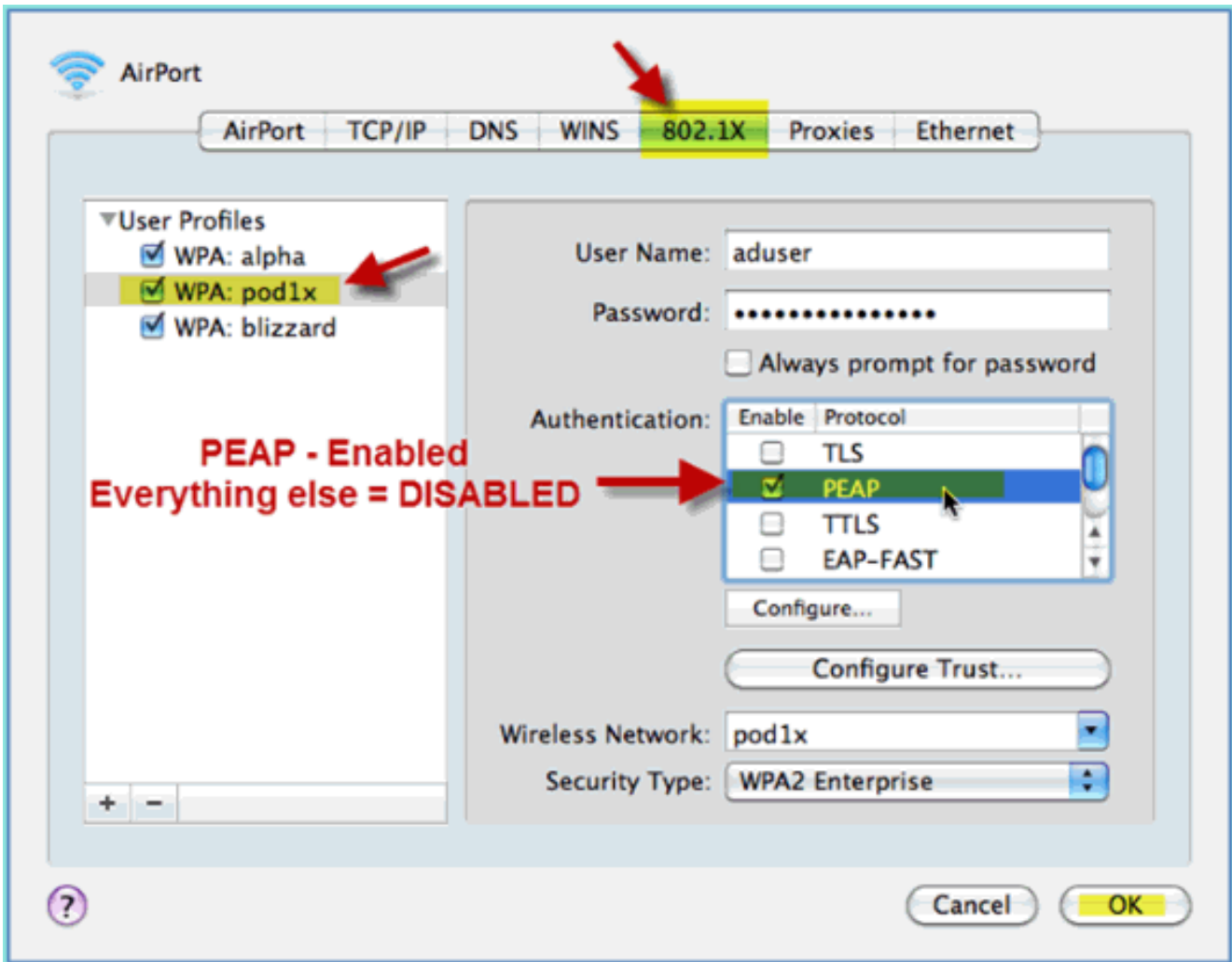
2. توفير المعلومات التالية للاتصال: اسم المستخدم: المستخدم (إذا كان يستخدم AD)، الموظف (داخلي - الموظف)، المقاول (داخلي - المقاول) كلمة المرور: XXXX معيار 802.1X: 802.1X معيار: TLS: تلقائياً شهادة:



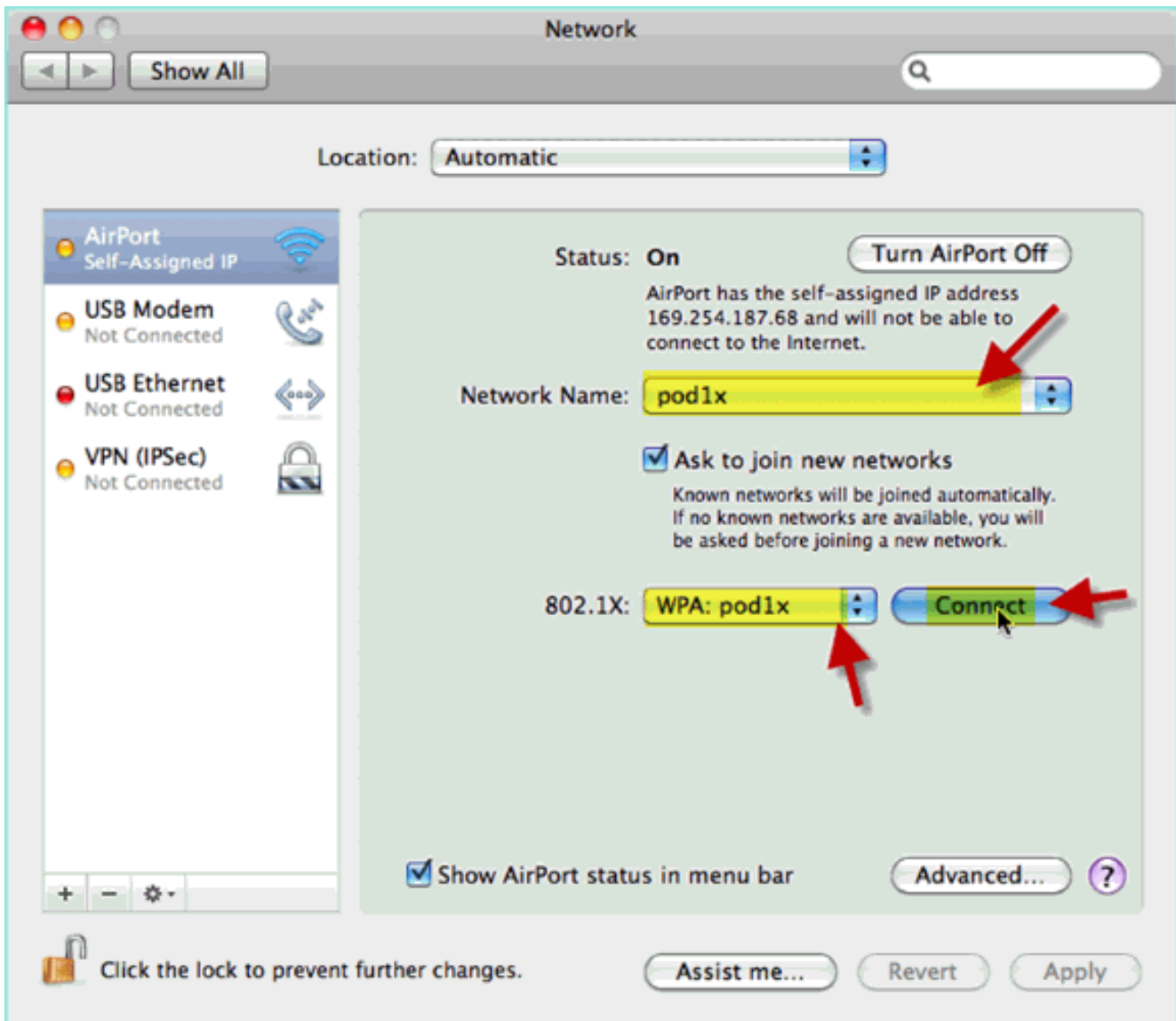
في هذا الوقت، قد لا يتصل الكمبيوتر المحمول. بالإضافة إلى ذلك، يمكن أن يقوم ISE برمي حدث فاشل كما يلي:

Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain

3. انتقل إلى تفضيل النظام < الشبكة < المطار < إعداد 802.1X واضبط مصادقة توصيف POD SSID/ WPA الجديد على النحو التالي: TLS: معطل PEAP: ممكن TTLS: معطل EAP-FAST: معطل

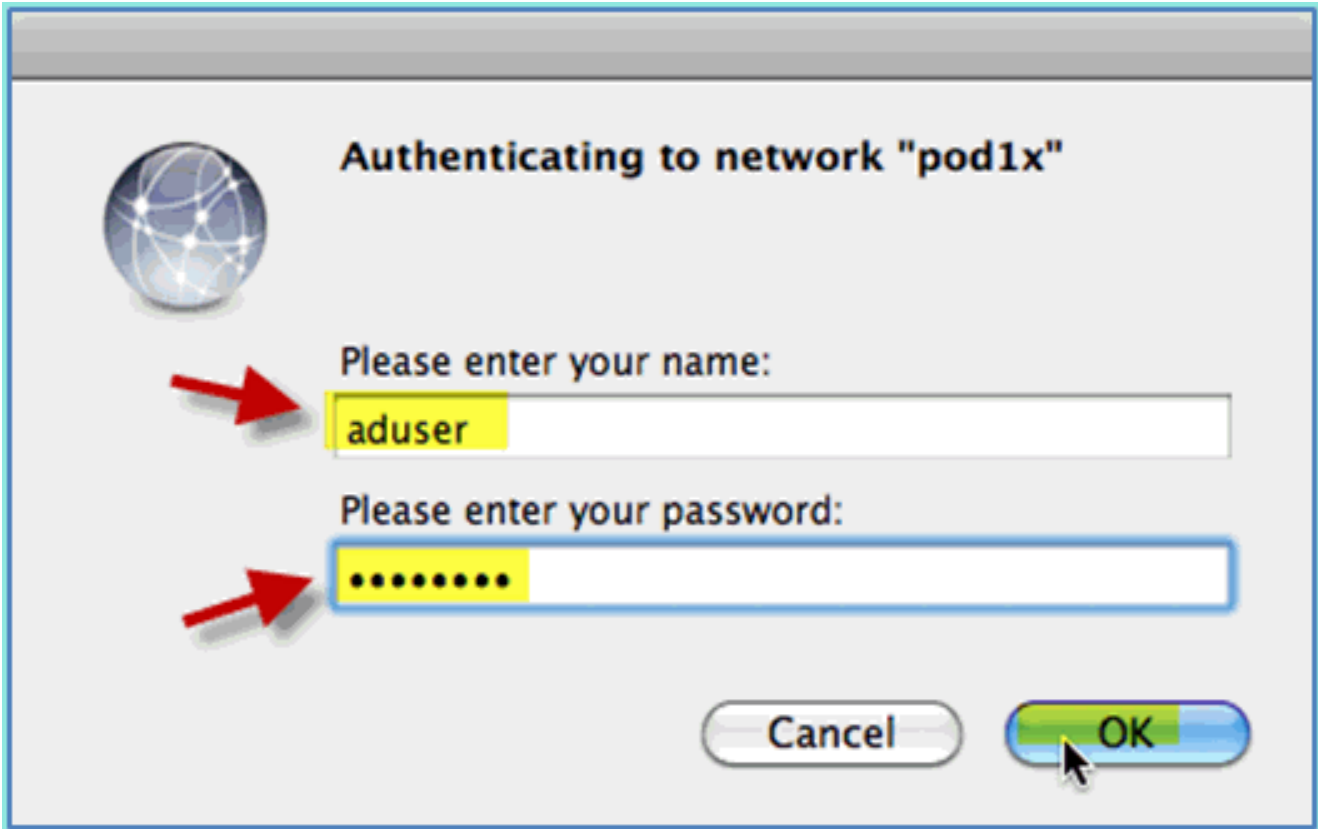


4. انقر فوق **موافق** للمتابعة والسماح بحفظ الإعداد.
5. على شاشة الشبكة، حدد SSID + توصيف WPA 802.1X المناسب وانقر على **توصيل**.

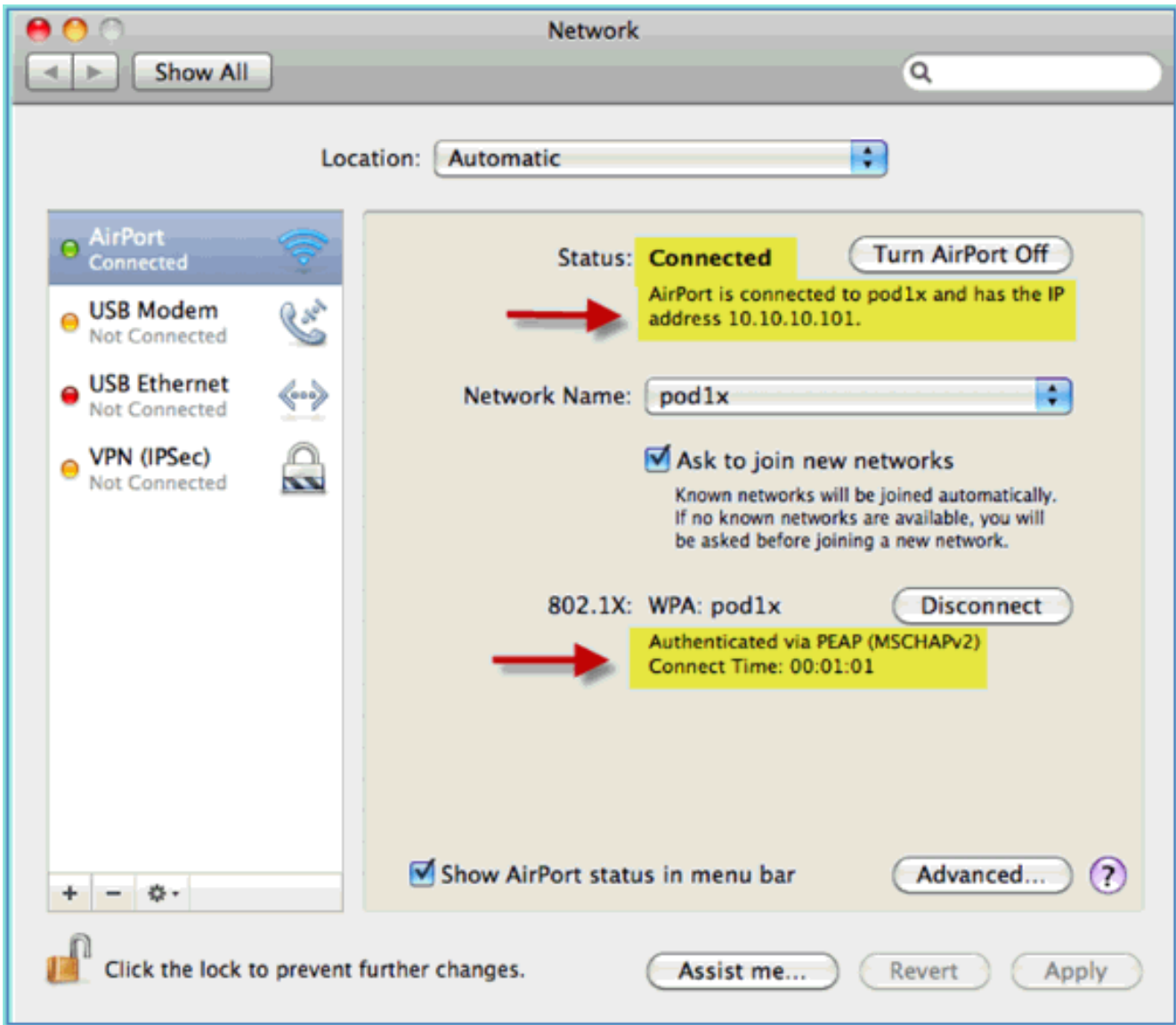


6. قد يطلب النظام اسم مستخدم وكلمة مرور. أدخل مستخدم الإعلان وكلمة المرور (aduser/xxxx). ثم انقر على موافق.





يجب على العميل إظهار متصل عبر PEAP بعنوان IP صالح.

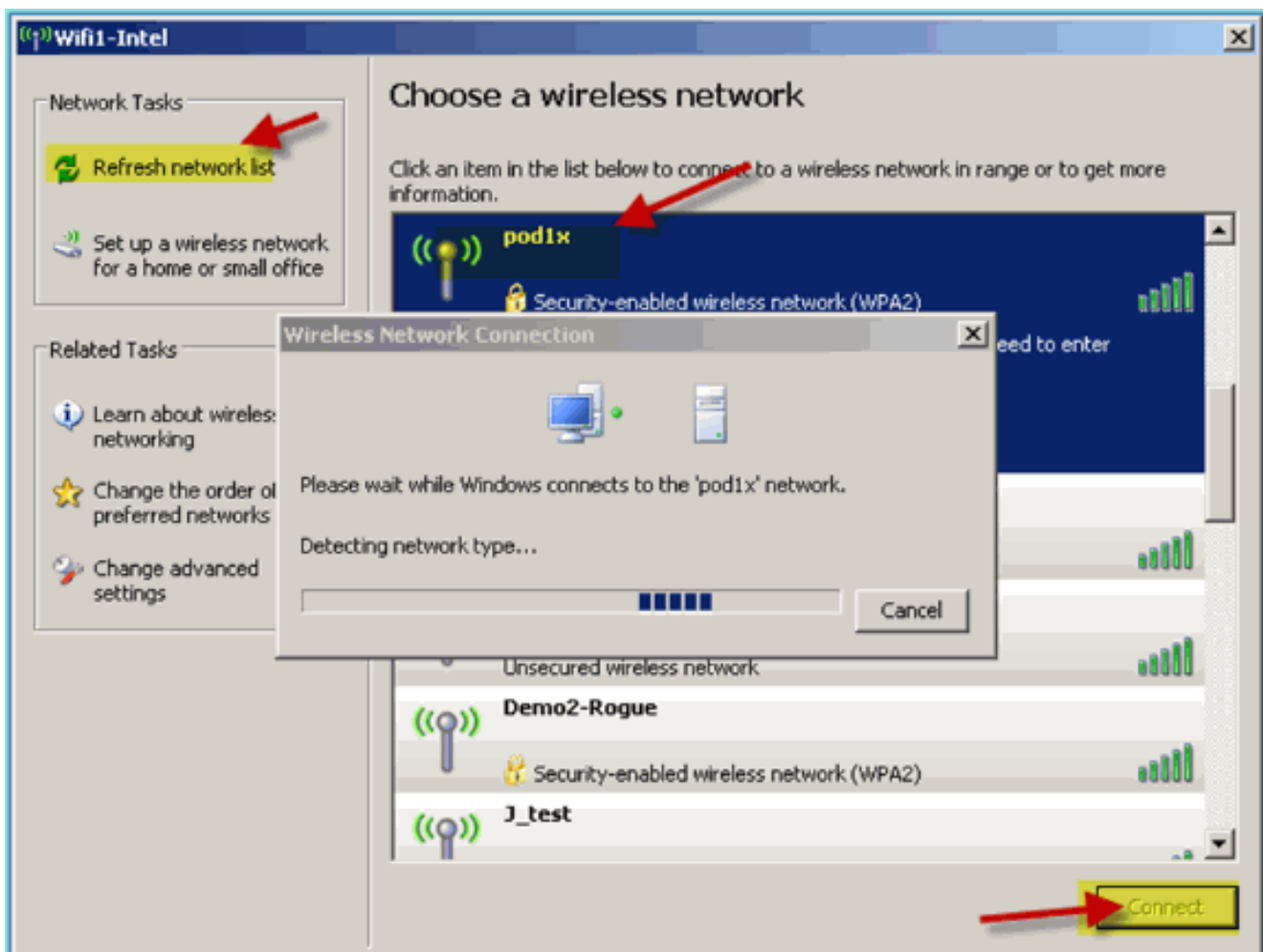


## المرجع: مصادقة لاسلكية لنظام Microsoft Windows XP

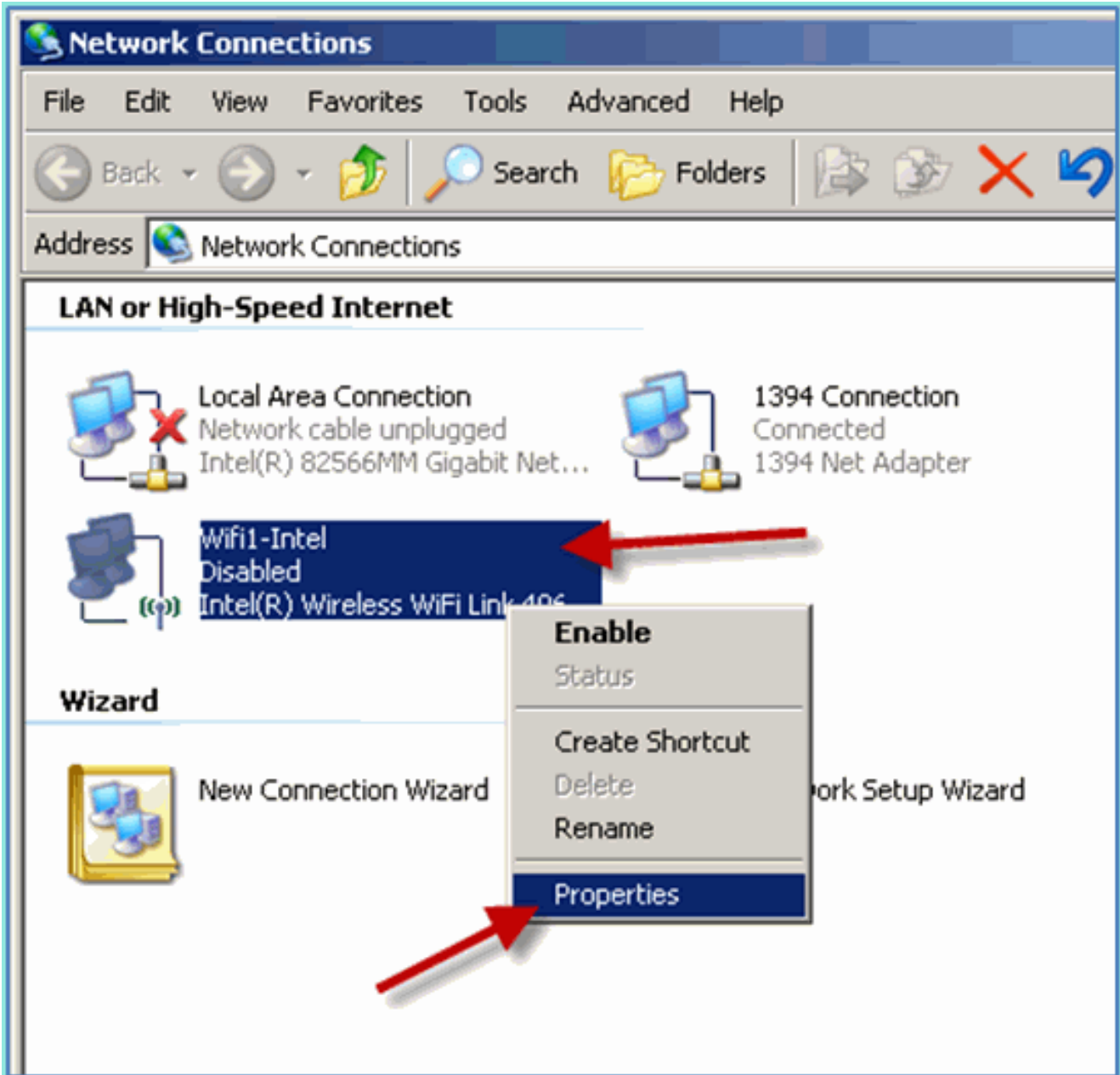
يمكنك الاقتران بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) عبر معرف SSID مصدق كمستخدم داخلي (أو مستخدم إعلانات مدمج) باستخدام كمبيوتر محمول لاسلكي يعمل بنظام التشغيل Windows XP. التخطي إذا لم يكن قابلاً للتطبيق.

أكمل الخطوات التالية:

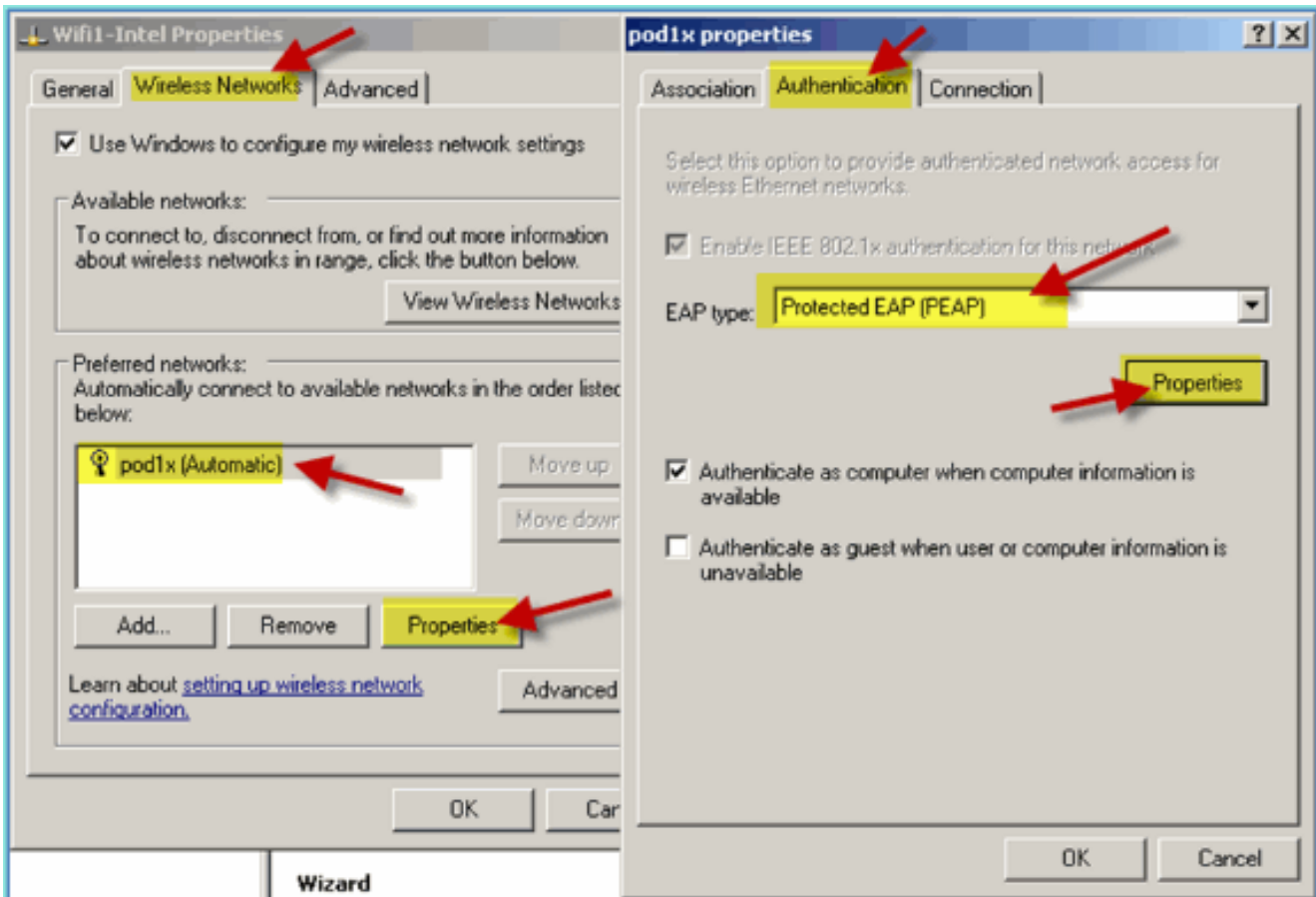
1. على الكمبيوتر المحمول، انتقل إلى إعدادات WLAN. مكن WiFi واتصل بمعرف SSID الممكن لـ 802.1X الذي تم إنشاؤه في التمرين السابق.



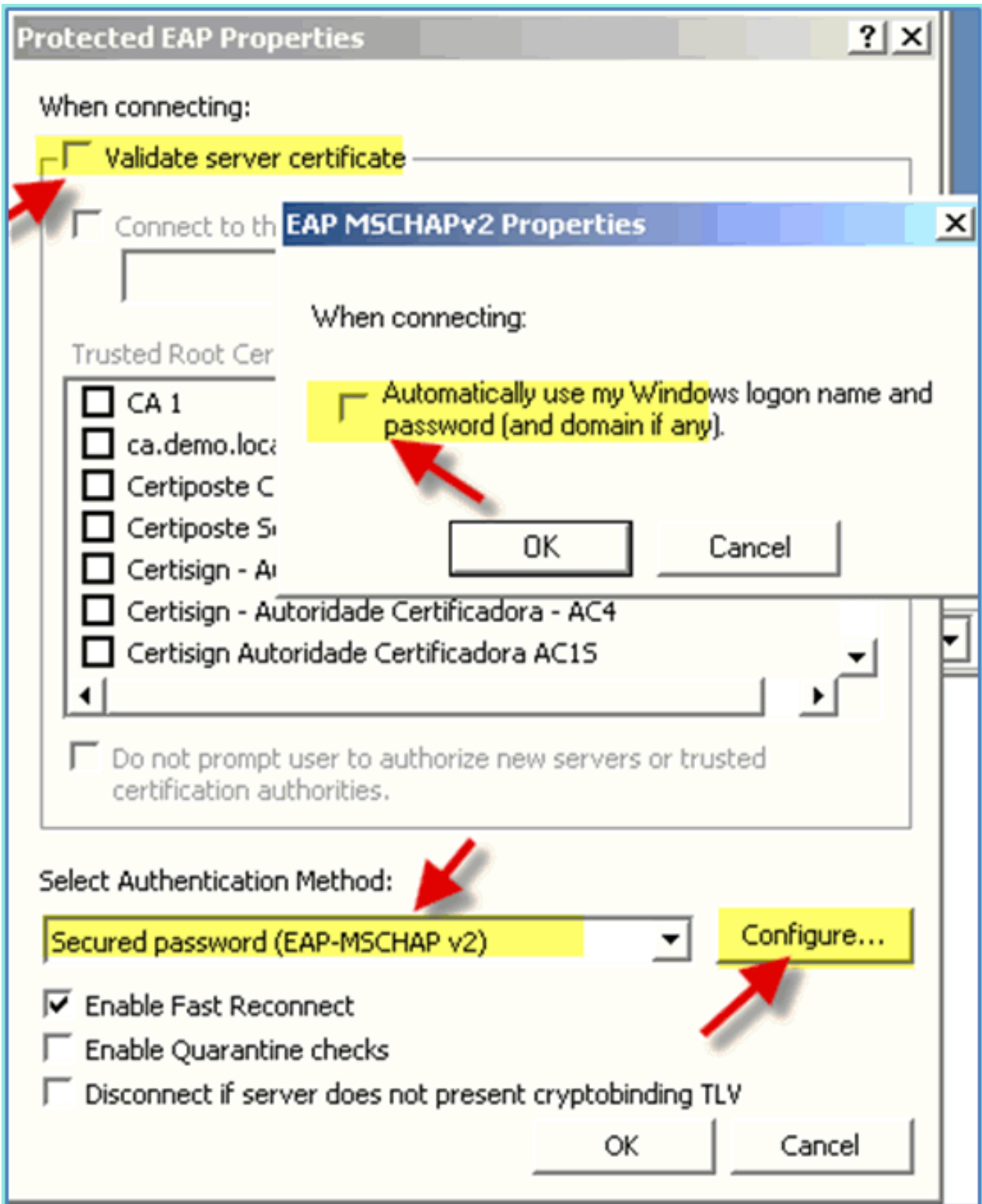
2. الوصول إلى خصائص شبكة واجهة .WiFi



3. انتقل إلى علامة تبويب الشبكات اللاسلكية. حدد خصائص شبكة SSID الخاصة بـ Pod < علامة تبويب مصادقة < نوع EAP = EAP محمي (PEAP).



4. انقر على خصائص EAP.
5. قم بتعيين ما يلي: التحقق من شهادة الخادم: معطل أسلوب المصادقة: كلمة المرور المؤمنة (EAP-MSCHAP) (v2)

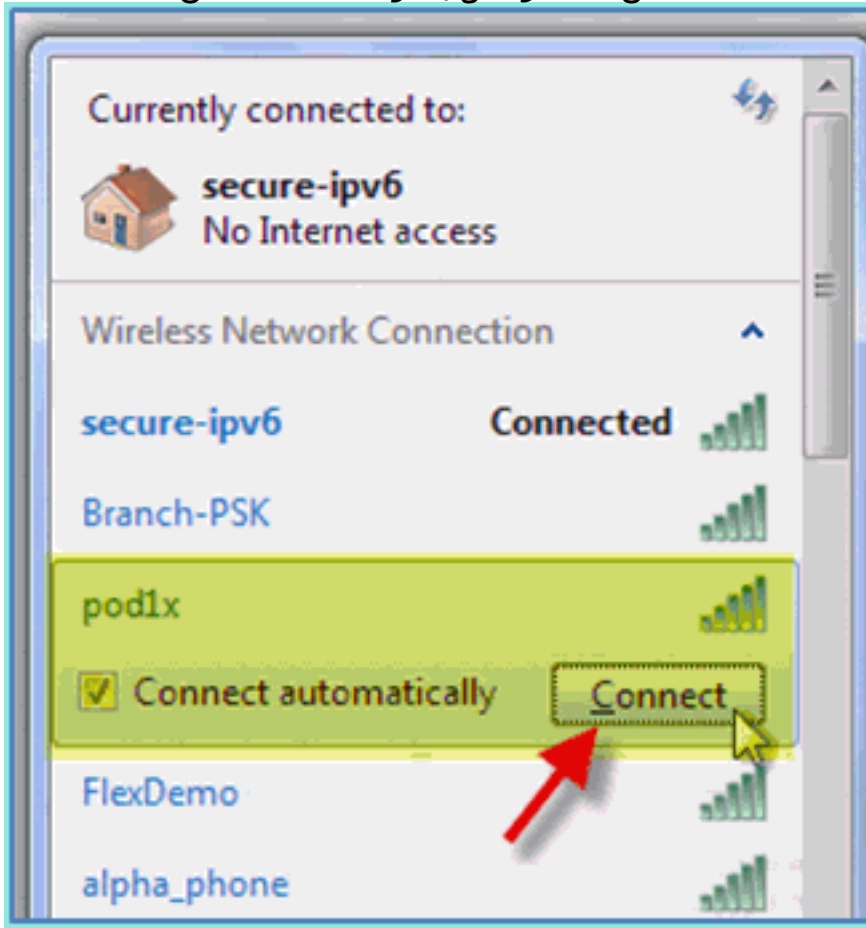


6. انقر فوق موافق" في جميع الإطارات لإكمال مهمة التكوين هذه.
7. يطلب عميل Windows XP اسم المستخدم وكلمة المرور. في هذا مثال، هو aduser/xxxx.
8. تأكيد اتصال الشبكة، عنوانة (v4 IP).

## [المرجع: المصادقة اللاسلكية لنظام التشغيل Microsoft Windows 7](#)

يمكنك الاقتران بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) عبر معرف SSID مصدق كمستخدم داخلي (أو مستخدم إعلانات مدمج) باستخدام كمبيوتر محمول لاسلكي يعمل بنظام التشغيل Windows 7.

1. على الكمبيوتر المحمول، انتقل إلى إعدادات WLAN. مكن WiFi واتصل بمعرف SSID الممكن لـ 802.1X



الذي تم إنشاؤه في التمرين السابق.

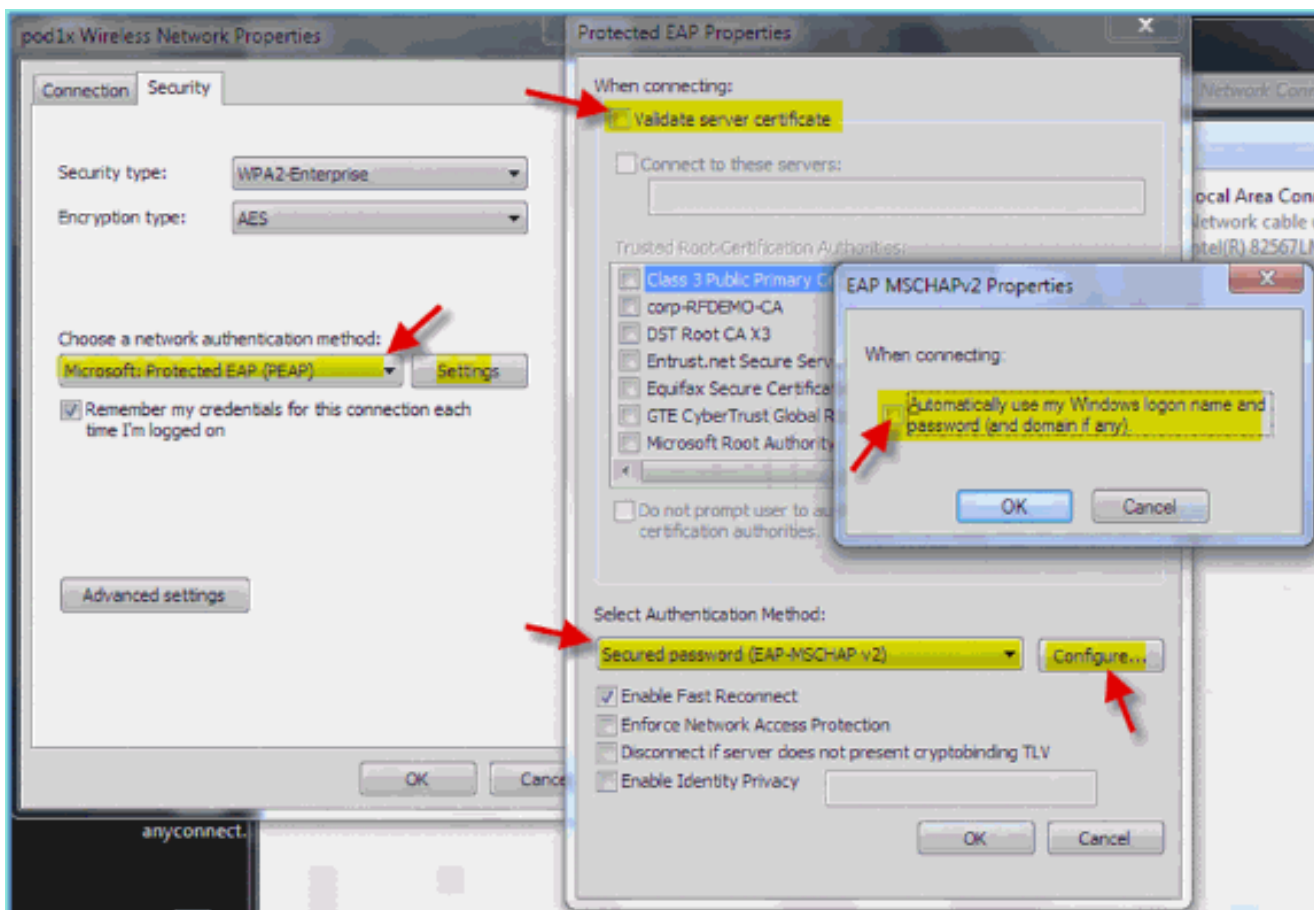
2. الوصول إلى إدارة اللاسلكي وتحرير توصيف POD اللاسلكي الجديد.

3. قم بتعيين ما يلي: أسلوب المصادقة: PEAP تذكر بيانات الاعتماد الخاصة بي...: معطالاتحقق من شهادة الخادم

(الإعداد المتقدم): معطالأسلوب المصادقة (إعداد البروتوكول): EAP-MSCHAP v2 استخدام تسجيل الدخول

إلى Windows تلقائياً...:

معطل



## معلومات ذات صلة

• [الدعم التقني والمستندات - Cisco Systems](#)



ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت  
ملاعلاء انء مچي ف ني مدخت سمل معد و ت م مي دقت لة يرش بل او  
امك ة قيق دن نوك ت نل ةللأل مچرت ل ضف أن ة ظحال م چرني . ة صاأل م هت بل ب  
Cisco ي لخت . فرت م مچرت م امدقي ي تل ةل ة فارت حال ة مچرت ل عم ل األ و ه  
ى ل إأمء اد ة وچرل اب ي صؤت و ت ا مچرت ل هذه ة ق دن ع اه تي ل وئ س م Cisco  
Systems (رفو تم طبارل) ي ل صأل ا يزي ل چن إل دن تسمل ا