تكوين تعيين VLAN الديناميكي باستخدام WLCs استناد إلى ISE إلى خريطة مجموعة Active Directory

المحتويات

المقدمة

يصف هذا وثيقة مفهوم VLAN حركي تعيين.

المتطلبات الأساسية

يصف المستند كيفية تكوين خادم وحدة تحكم الشبكة المحلية (WLC) اللاسلكية ومحرك خدمات الهوية (ISE) من أجل تخصيص عملاء شبكة LAN اللاسلكية (WLAN) في شبكة VLAN معينة بشكل ديناميكي.

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بوحدات التحكم في الشبكة المحلية (LAN) اللاسلكية (WLCs) ونقاط الوصول في الوضع Lightweight (LAPs)
- المعرفة الوظيفية لخادم المصادقة والتفويض والمحاسبة (AAA) مثل ISE
- معرفة دقيقة بالشبكات اللاسلكية ومشكلات الأمان اللاسلكي
- معرفة وظيفية قابلة للتكوين لتعيين شبكة VLAN الديناميكية
- الفهم الأساسي لخدمات Microsoft Windows AD، بالإضافة إلى وحدة التحكم بالمجال

ومفاهيم DNS
- لديهم معرفة أساسية ببروتوكول نقطة الوصول (CAPWAP) من حيث التحكم والإمداد

المكونات المستخدمة

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

- Cisco 5520 Series WLC الذي يشغل البرنامج الثابت، الإصدار 8.8.111.0
- cisco 4800 sery AP
- طالب Windows الأصلي و AnyConnect NAM
- Cisco Secure ISE، الإصدار 2.3.0.298
- تم تكوين Microsoft Windows 2016 Server كوحدة تحكم بالمجال
- محول سلسلة Cisco 3560-CX الذي يشغل الإصدار 15.2(4)E1

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

الاصطلاحات

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

التعيين الديناميكي لشبكة VLAN مع خادم RADIUS

في معظم أنظمة WLAN، يكون لكل شبكة WLAN سياسة ثابتة تنطبق على جميع العملاء المرتبطين بمعرف مجموعة الخدمة (SSID) أو WLAN في مصطلحات وحدة التحكم. وعلى الرغم من أنها فعالة، إلا أن هذه الطريقة لها قيود لأنها تتطلب من العملاء الاقتران ب SSIDs مختلفة لوراثة حقوق الخدمة (QoS) ونهج الأمان المختلفة.

عناوين حلول شبكات WLAN من Cisco التي تحدد بواسطة دعم شبكات الهوية. وهذا يسمح للشبكة بالإعلان عن معرف SSID واحد ولكنه يسمح لمستخدمين محددين بتوريث حقوق الخدمة (QoS) المختلفة وسمات VLAN و/أو سياسات الأمان المستندة إلى بيانات اعتماد المستخدم.

تعيين VLAN الديناميكي هو أحد تلك الميزات التي تضع مستخدم السلكي في شبكة VLAN معينة بناء على بيانات الاعتماد التي قدمها المستخدم. تتم معالجة هذه المهمة لتعيين مستخدمين لشبكة VLAN معينة بواسطة خادم مصادقة RADIUS، مثل Cisco ISE. يمكن إستخدام هذا، على سبيل المثال، للسماح للضيف اللاسلكي بالبقاء على شبكة VLAN نفسها أثناء انتقالها داخل شبكة مجمع.

يصادق خادم Cisco ISE المستخدمين اللاسلكيين مقابل قاعدة بيانات واحدة من بين قواعد

بيانات متعددة محتملة، تتضمن قاعدة بياناته الداخلية. على سبيل المثال:

- قاعدة بيانات داخلية
- الدليل النشط
- البروتوكول العام الخفيف للوصول إلى الدليل (LDAP)
- قواعد بيانات ارتباطية متوافقة مع اتصال قاعدة البيانات المفتوحة (ODBC)
- خوادم SecureID المميزة من Rivest و Shamir و Adelman (RSA)
- خوادم الرمز المميز المتوافقة مع RADIUS

تسرد [بروتوكولات مصادقة Cisco ISE ومصادر الهوية الخارجية المدعومة](#) مختلف بروتوكولات المصادقة المدعومة بواسطة قواعد بيانات ISE الداخلية والخارجية.

يركز هذا المستند على مصادقة المستخدمين اللاسلكيين الذين يستخدمون قاعدة بيانات Windows Active Directory الخارجية.

بعد نجاح المصادقة، يسترجع ISE معلومات المجموعة الخاصة بذلك المستخدم من قاعدة بيانات Windows ويربط المستخدم بملف تعريف التخويل الخاص.

عندما يحاول العميل أن يقترن مع نقطة وصول في الوضع Lightweight مسجلة مع وحدة تحكم، فإن نقطة الوصول في الوضع Lightweight تمرر بيانات اعتماد المستخدم إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام التعليمات الخاصة بأسلوب EAP ذي الصلة.

ترسل WLC بيانات الاعتماد هذه إلى ISE باستخدام بروتوكول RADIUS (الذي يتضمن EAP) ويمرر ISE بيانات اعتماد المستخدمين إلى AD للتحقق بمساعدة بروتوكول Kerberos.

يقوم AD بالتحقق من صحة بيانات اعتماد المستخدم وعند نجاح المصادقة، يقوم بإعلام ISE.

بمجرد نجاح المصادقة، يقوم خادم ISE بتمرير سمات معينة لفرق عمل هندسة الإنترنت (IETF) إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تحدد سمات RADIUS هذه معرف VLAN الذي يجب تعيينه للعميل اللاسلكي. الـ SSID (WLAN، فيما يتعلق بـ WLC) العميل لأنه يتم تعيين المستخدم دائما لمعرف VLAN هذا المحدد مسبقا.

سمات مستخدم RADIUS المستخدمة لتعيين معرف VLAN هي:

- IETF 64 (نوع النفق)—تثبت هذا إلى VLAN
- IETF 65 (نوع متوسط للنفق)—تعيين هذا إلى 802
- IETF 81 (معرف مجموعة النفق الخاصة)—تثبت هذا إلى VLAN id

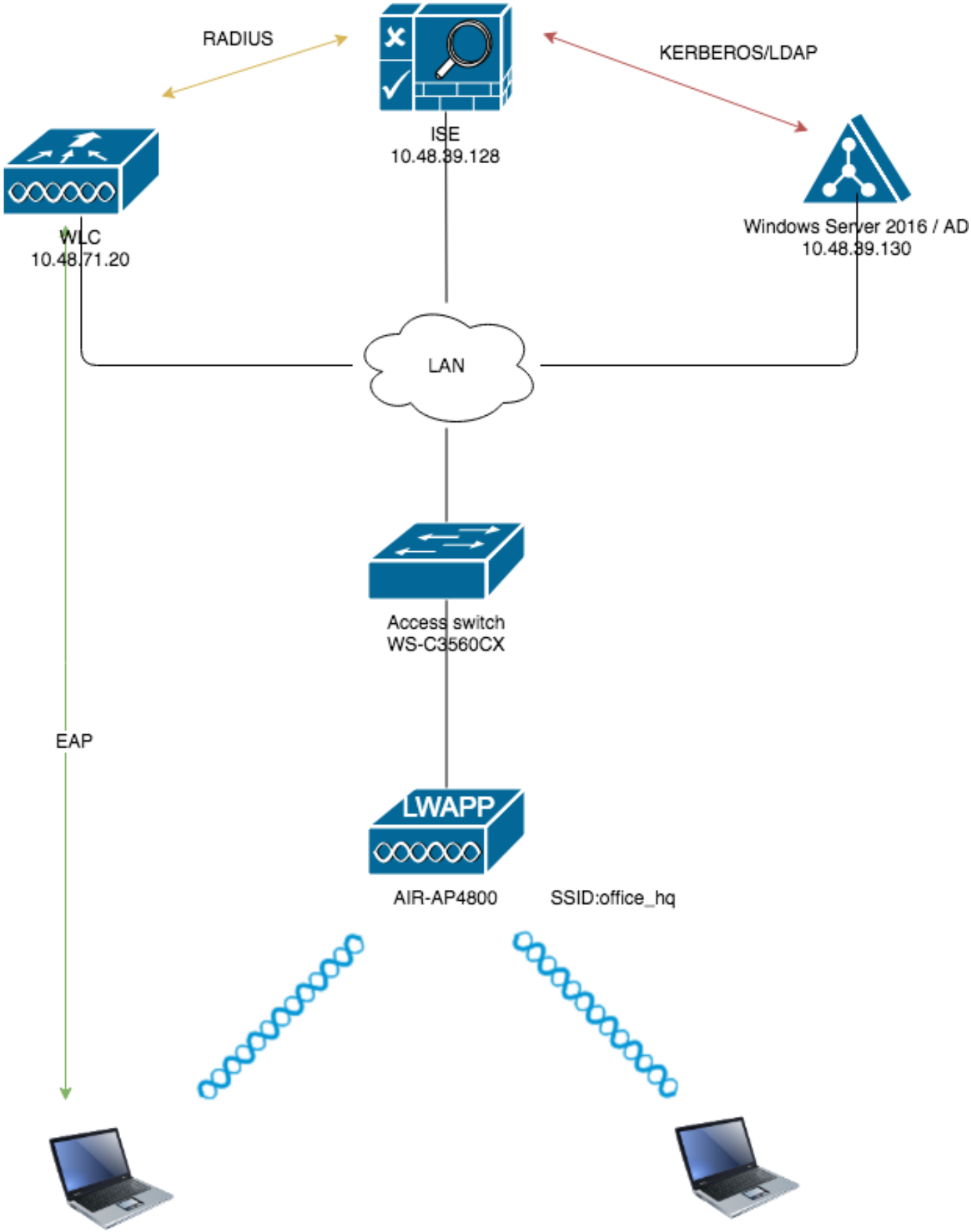
معرف شبكة VLAN هو 12 بت وأي قيمة بين 1 و 4094، شاملة. لأن Tunnel-Private-Group-ID هو من النوع سلسلة، كما هو محدد في RFC2868 للاستخدام مع IEEE 802.1X، يتم تشفير قيمة العدد الصحيح لمعرف VLAN كسلسلة. عندما يتم إرسال سمات النفق هذه، فمن الضروري أن تملأ في حقل علامة التمييز.

كما تمت الإشارة في RFC 2868، القسم 3.1: حقل العلامة عبارة عن نظام ثماني واحد بطول ويقصد به توفير وسيلة لتجميع السمات في نفس الحزمة التي تشير إلى نفس النفق. القيم الصالحة لهذا الحقل هي 0x01 حتى 0x1F، شاملة. إذا كان حقل العلامة غير مستخدم، يجب أن يكون صفر (0x00). راجع RFC 2868 للحصول على مزيد من المعلومات حول جميع سمات RADIUS.

التكوين

يوفر هذا القسم المعلومات اللازمة لتكوين الميزات الموضحة في المستند.

الرسم التخطيطي للشبكة

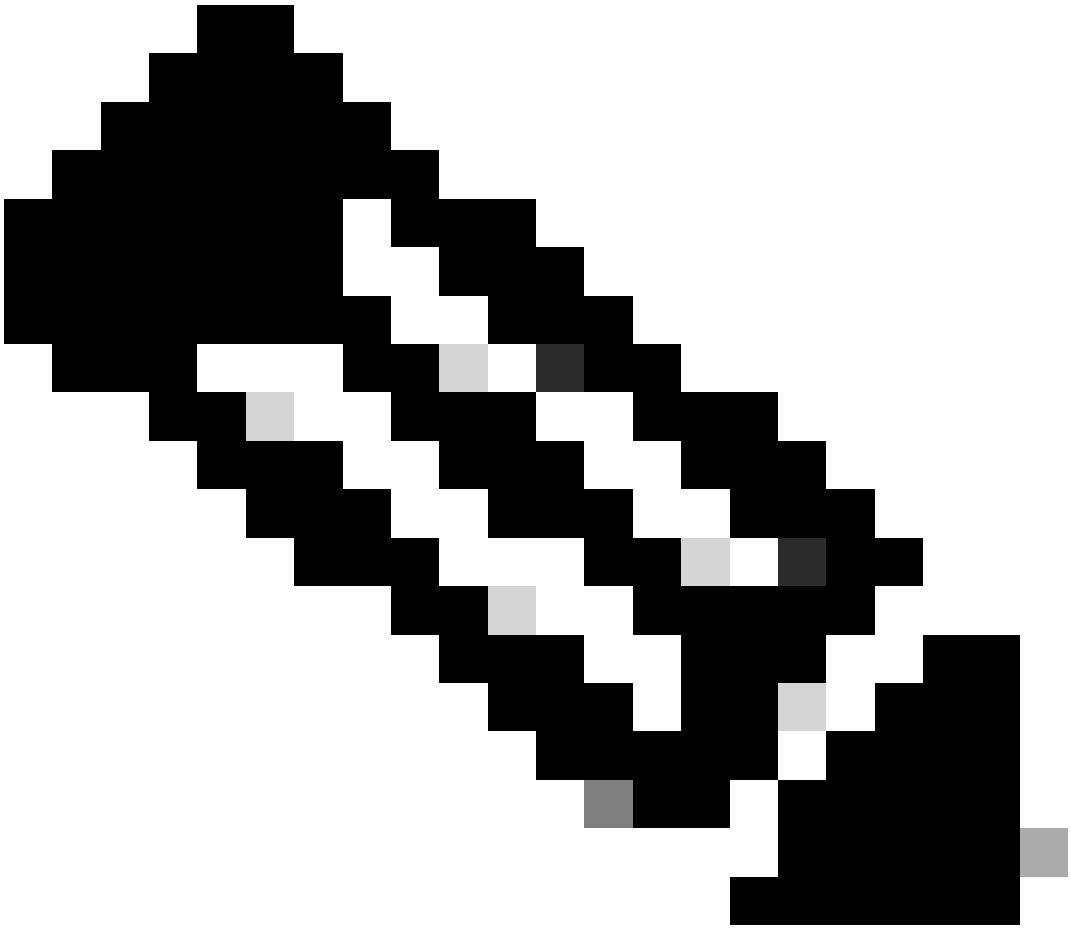


التكوينات

هذه هي تفاصيل تكوين المكونات المستخدمة في هذا المخطط:

- عنوان IP الخاص بخادم ISE (RADIUS) وه 10.48.39.128.
- عنوان واجهة الإدارة و AP-Manager الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وه 10.48.71.20.
- يتواجد خادم DHCP في شبكة LAN ويتم تكوينه لتجمعات العملاء المقابلة؛ والي يتم عرضه في المخطط.
- يتم إستخدام شبكة VLAN1478 وشبكة VLAN1477 عبر هذه التكوين. يتم تكوين VLAN1477 ويتم تكوين المستخدمين من قسم التسويق من أجل وضعهم في شبكة VLAN1478 بواسطة خادم RADIUS المستخدمين من قسم HR من أجل وضعهم في شبكة VLAN1478 عندما يتصل كل المستخدمين بنفس SSID — office_hq.

  VLAN1477: 192.168.77.0/24. البوابة: 192.168.77.1 VLAN1478: 192.168.78.0/24. البوابة: 192.168.78.1
- يستخدم هذا المستند 802.1xPEAP-mschapv2كآلية أمان.



ملاحظة: توصي Cisco باستخدام طرق المصادقة المتقدمة، مثل مصادقة EAP-FAST و

EAP-TLS، لتأمين شبكة WLAN.

يتم وضع هذه الافتراضات قبل تنفيذ هذا التكوين:

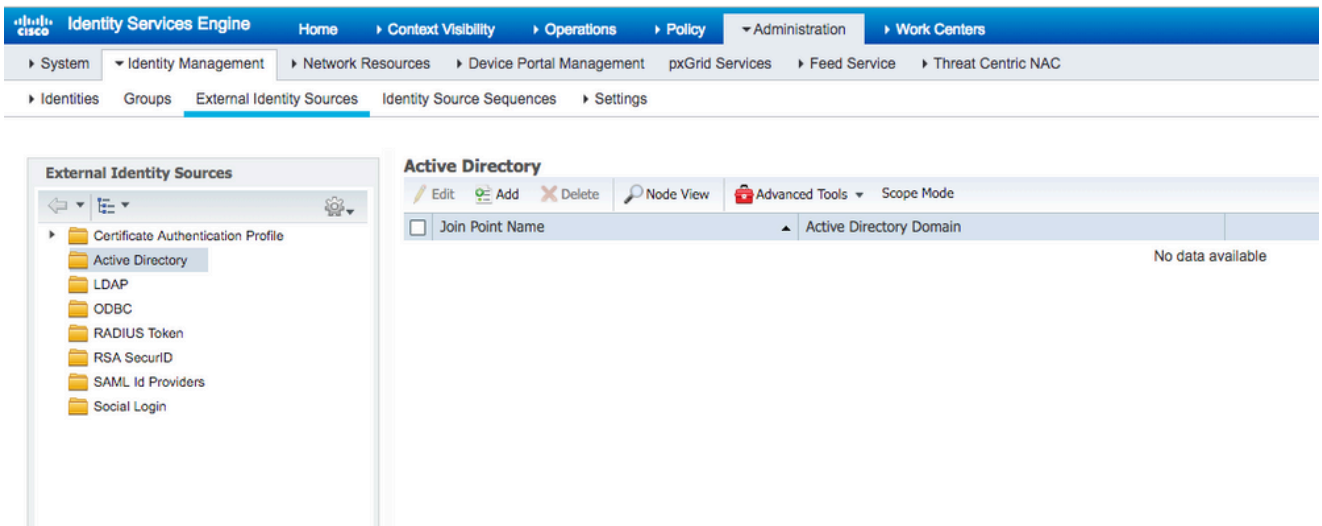
- ال{upper}lap مسجل بالفعل مع ال WLC
- تم تعيين نطاق DHCP لخادم DHCP
- يوجد اتصال الطبقة 3 بين جميع الأجهزة في الشبكة
- يناقش المستند التكوين المطلوب على الجانب اللاسلكي ويفترض أن الشبكة اللاسلكية في موضعها
- تم تكوين المستخدمين والمجموعات الخاصة على AD

من أجل إنجاز تعيين شبكة VLAN الديناميكية باستخدام قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs) استنادا إلى تعيين ISE إلى مجموعة AD، يجب تنفيذ هذه الخطوات:

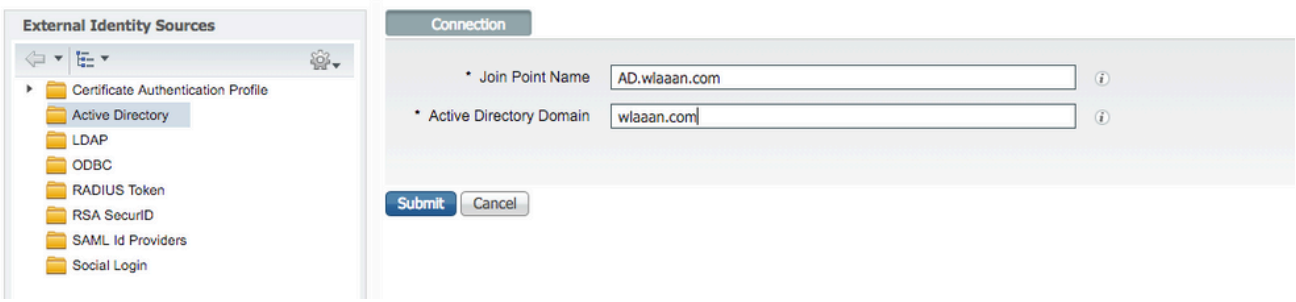
1. دمج ISE إلى AD وتكوين سياسات المصادقة والتفويض للمستخدمين على ISE.
2. تكوين WLC لدعم مصادقة dot1x وتجاوز AAA ل SSID 'office_hq'.
3. تكوين ملتمس العميل النهائي.

دمج وتهيئة سياسات المصادقة والتفويض للمستخدمين على ISE إلى AD ISE

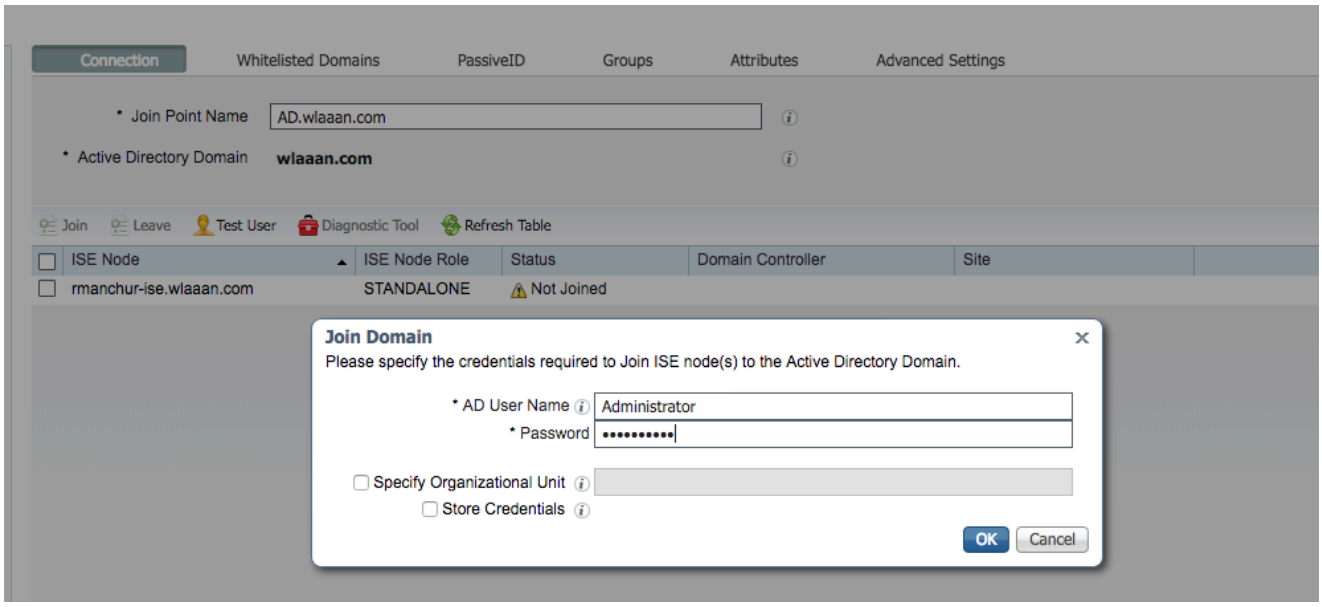
1. تسجيل الدخول إلى واجهة ISE Web UI باستخدام حساب مسؤول.
2. انتقل إلىAdministration > Identity management > External Identity Sources > Active directory.



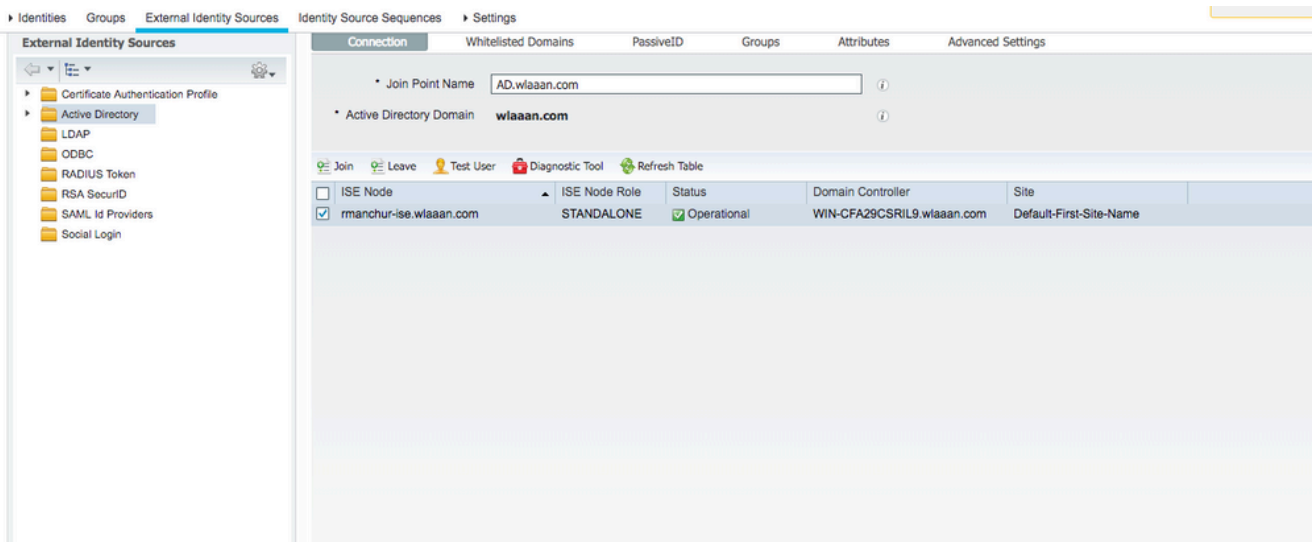
3. انقر فوق إضافة وأدخل اسم المجال واسم مخزن الهوية من إعدادات "اسم نقطة الانضمام ل Active Directory". في المثال، يتم تسجيل ISE في المجالwlaaan.comويتم تحديد نقطة الاتصال كAD.wlaaan.com- اسم اه محليا إلى ISE.



4. في حالة وجود أي مشاكل لديك في عملية التسجيل، يمكنك إستخدامDiagnostic Tool in order to ركضت الاختبارات المطلوبة لاتصال AD.

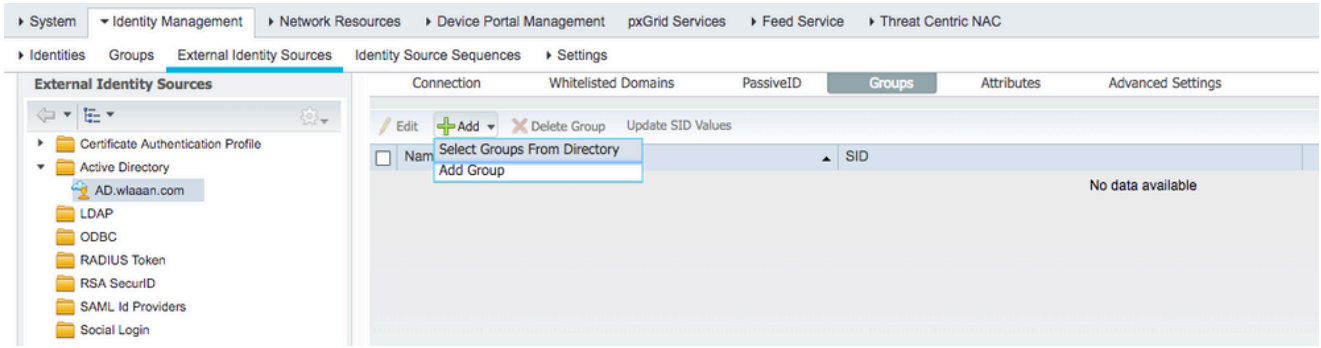


5. بعد هذه النقطة، يجب أن يكون لديك ISE مسجل بنجاح في AD.

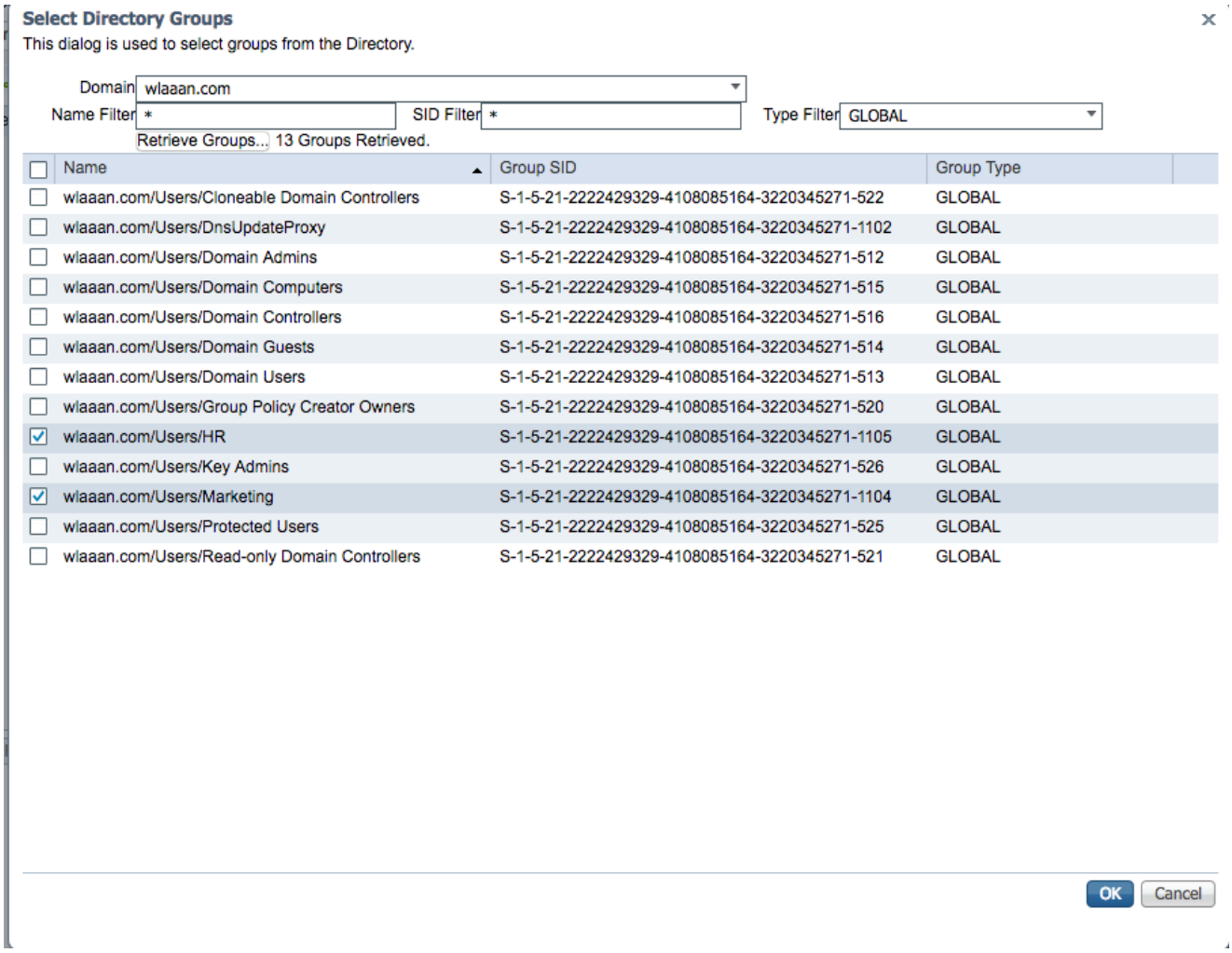


في حالة وجود أي مشاكل لديك في عملية التسجيل، يمكنك إستخدامDiagnostic Tool in order to ركضت الاختبارات المطلوبة لاتصال AD.

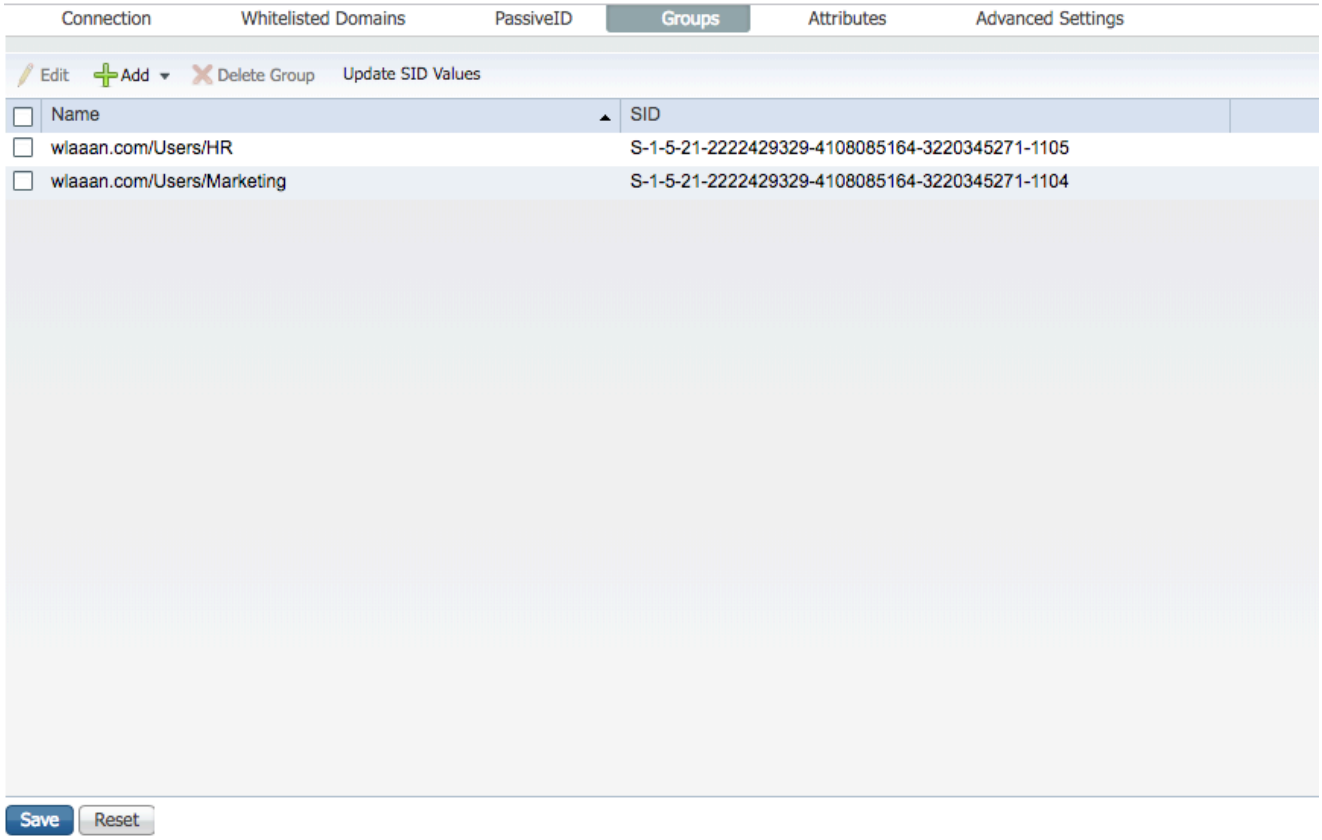
6. يجب إسترداد مجموعات الدلائل النشطة التي يتم إستخدامها لتعيين ملفات تعريف التخويل الخاصة. انتقل إلىAdministration > Identity management > External Identity Sources > Active directory > > Groups ، ثم انقر فوقAddواخترSelect Groups from Active Directory.



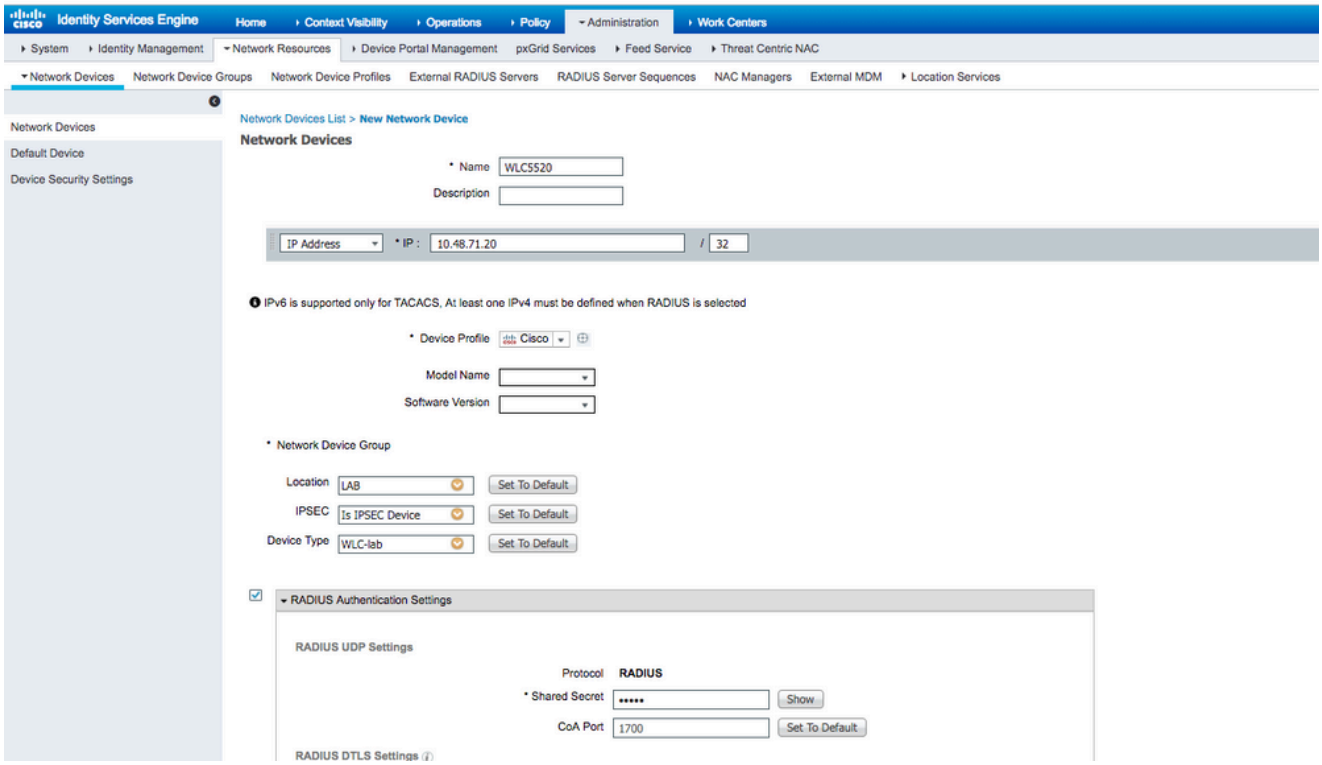
7. تفتح نافذة منبثقة جديدة حيث يمكنك تحديد عامل تصفية لاسترداد مجموعة (مجموعات) معينة أو إسترداد جميع المجموعات من AD.
أختر المجموعات المعنية من قائمة مجموعة AD واضغطOK.



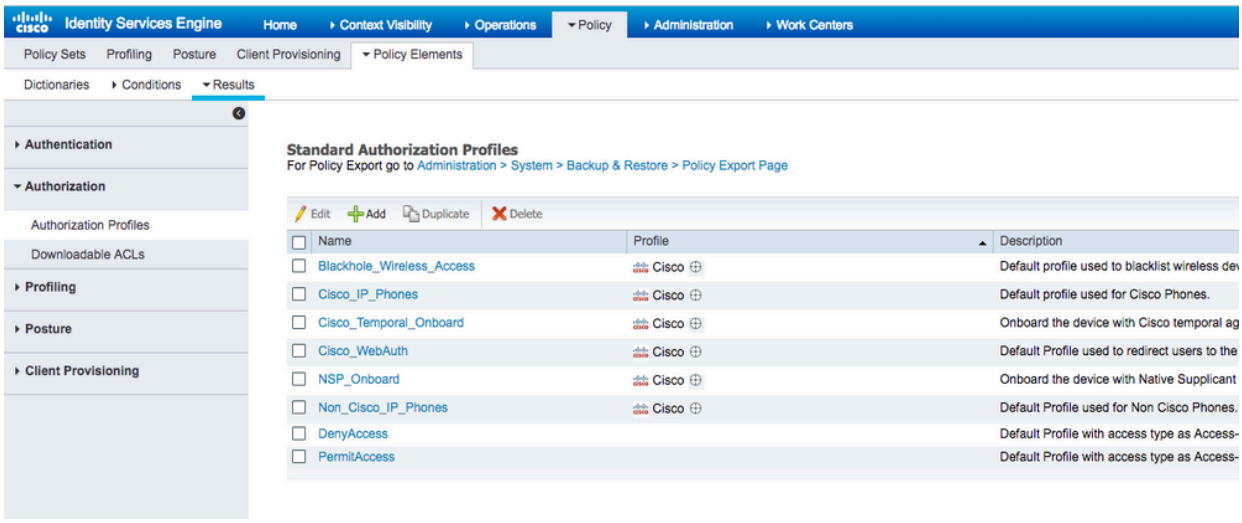
8. تتم إضافة المجموعات المعنية إلى ISE ويمكن حفظها. اضغطSave.



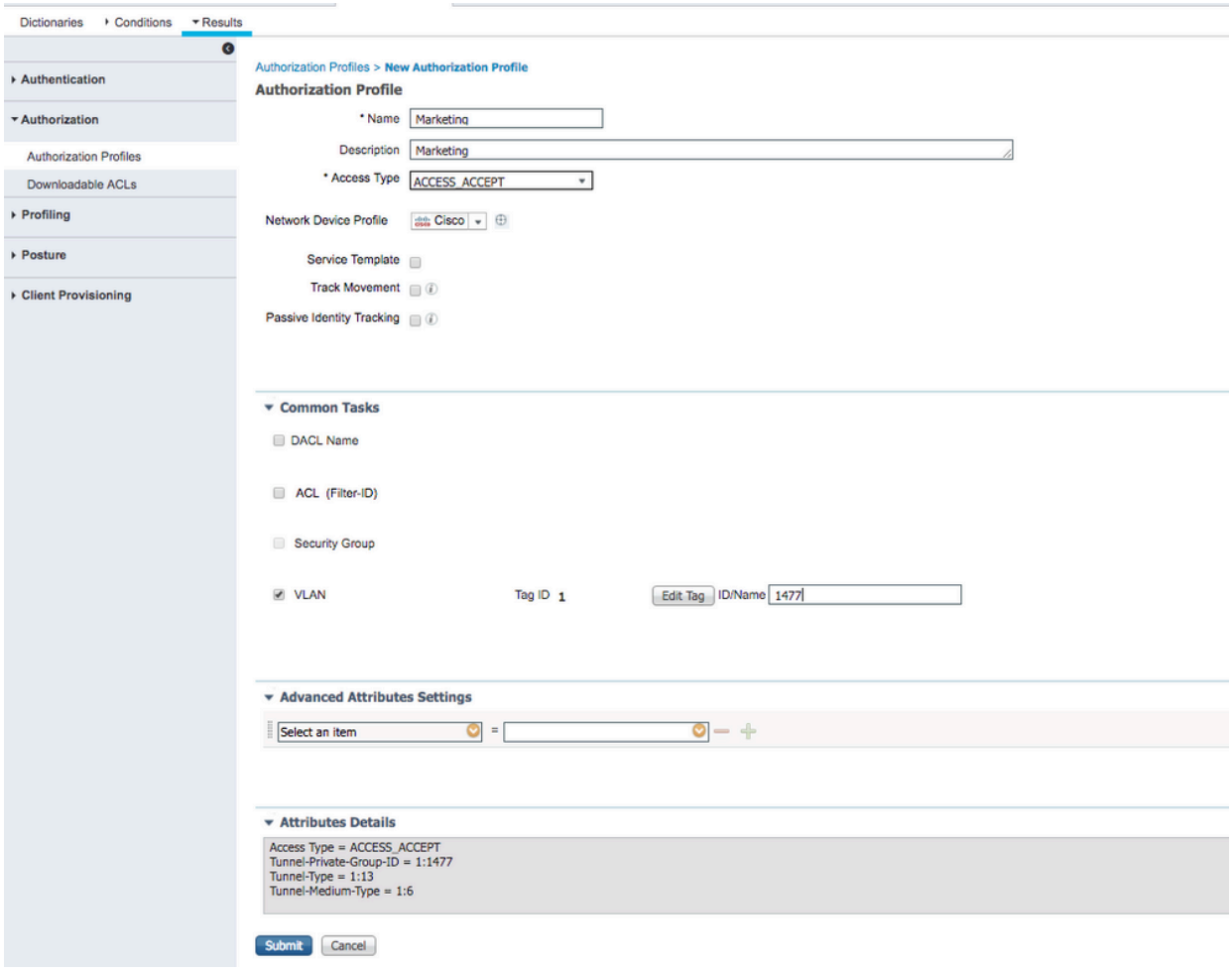
9. إضافة WLC إلى قائمة جهاز شبكة ISE - انتقل إلىAdministration > Network Resources > Network DevicesواضغطAdd.
تكوين كامل، من خلال توفير عنوان IP لإدارة WLC وسر RADIUS المشترك بين WLC و ISE.



10. الآن بعد انضمامك إلى ISE إلى AD وإضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إلى قائمة الأجهزة، يمكنك بدء تكوين سياسات المصادقة والتفويض للمستخدمين.
    - قم بإنشاء ملف تعريف تفويض لتعيين المستخدمين من التسويق إلى VLAN1477 ومن مجموعة HR إلى VLAN1478.
      انتقل إلىPolicy > Policy Elements > Results > Authorization > Authorization profilesوانقر فوق الزرAddلإنشاء ملف تخصيص جديد.

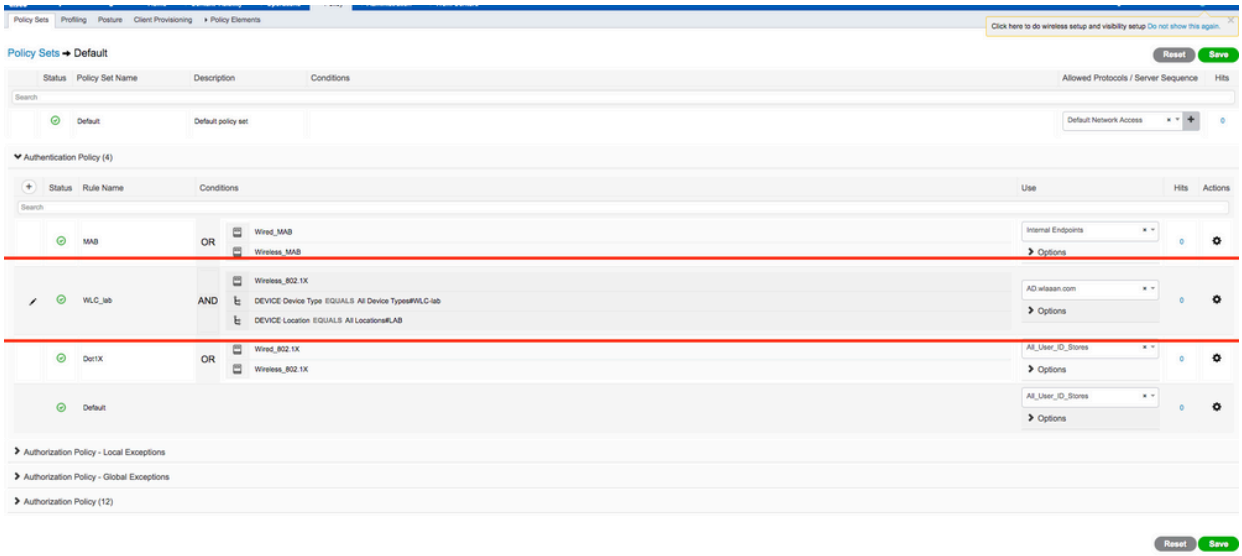


    - أكمل تكوين ملف تعريف التخويل باستخدام معلومات شبكة VLAN للمجموعة المعنية؛ يوضح المثالMarketingإعدادات تكوين المجموعة.

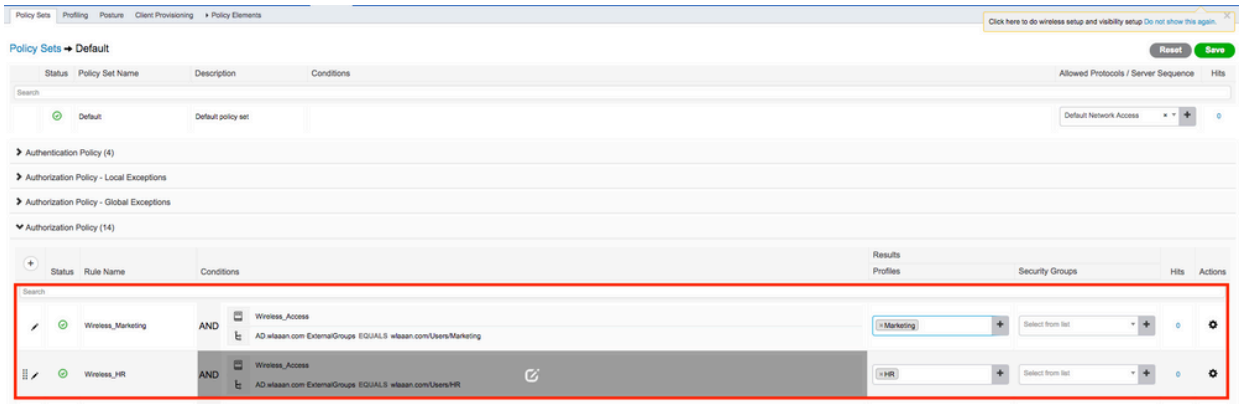


يجب إجراء تكوين مماثل للمجموعات الأخرى ويجب تكوين سمات علامة VLAN المقابلة.

- بعد تكوين توصيفات التخويل، يمكنك تحديد سياسات المصادقة للمستخدمين اللاسلكيين. يمكن القيام بذلك إما من خلال تكوينCustomمجموعة النهج أو تعديلهاDefault. في هذا المثال، تم تعديل مجموعة النهج الافتراضية. انتقل إلىPolicy > Policy Sets > Default. افتراضيdot1xنوع المصادقة، يستخدم ISEAll_User_ID_Stores، على الرغم من أنه يعمل حتى مع الإعدادات الافتراضية الحالية نظرا لأن AD هو جزء من قائمة مصدر الهوية لAll_User_ID_Stores، يستخدم هذا المثال قاعدة أكثر تحديداWLC_labلوحدة التحكم المعمولية المعينة ويستخدم AD كمصدر وحيد للمصادقة.

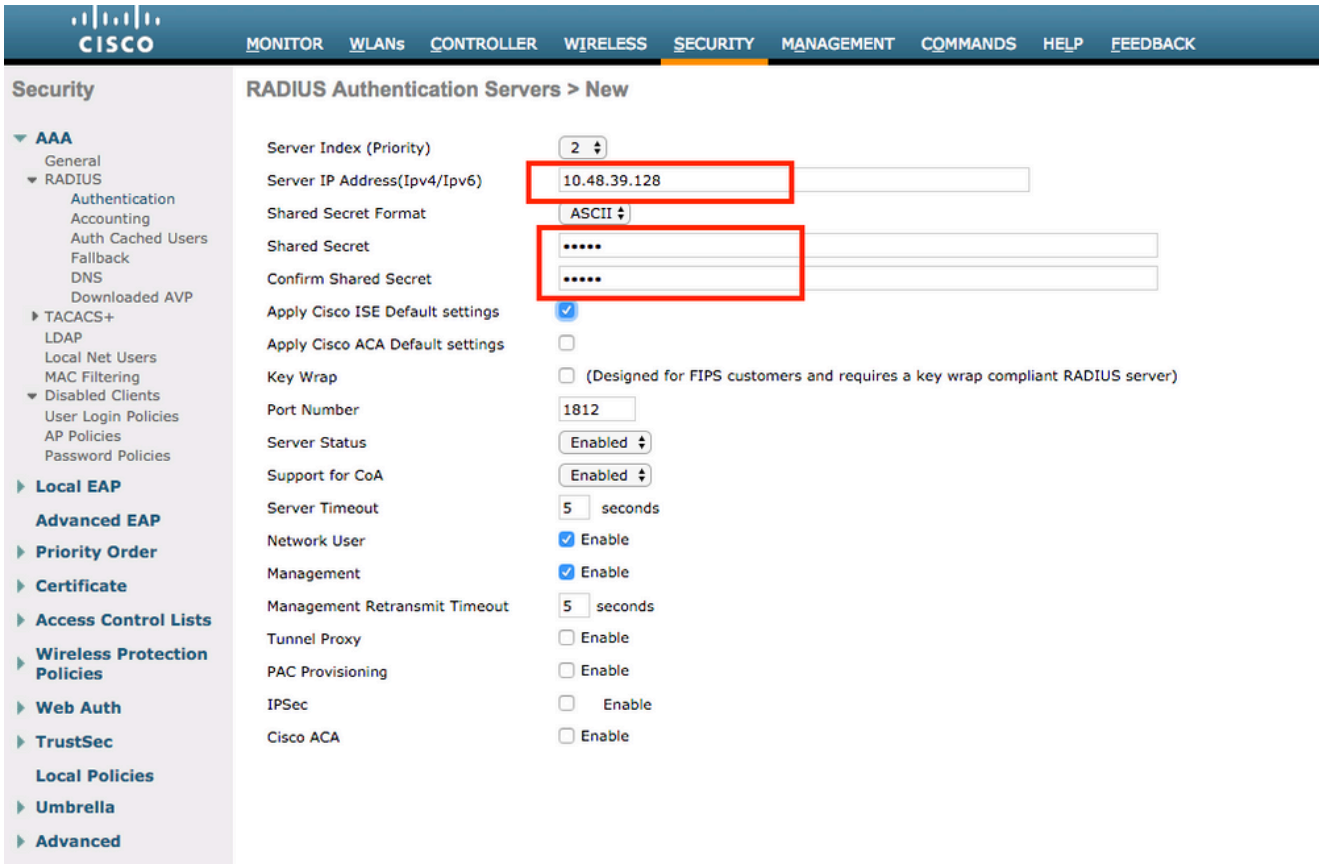


- يجب عليك الآن إنشاء سياسات تخويل للمستخدمين الذين يقومون بتعيين ملفات تعريف تخويل خاصة استنادا إلى عضوية المجموعة. انتقل إلىAuthorization policyالقسم وقم بإنشاء سياسات من أجل تحقيق هذا المتطلب.

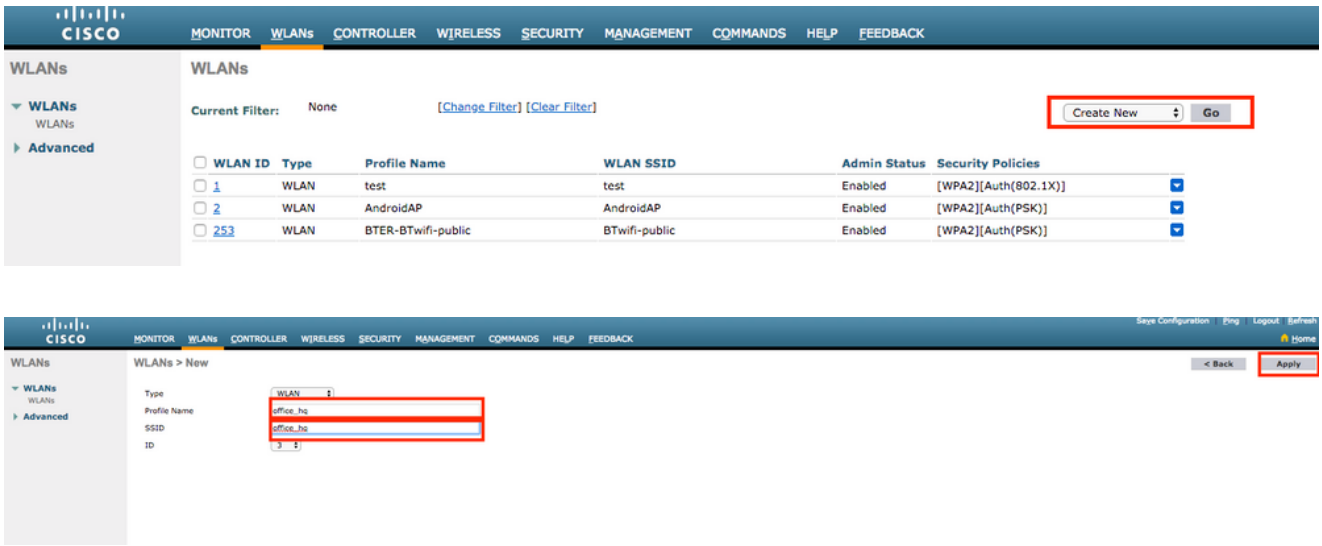


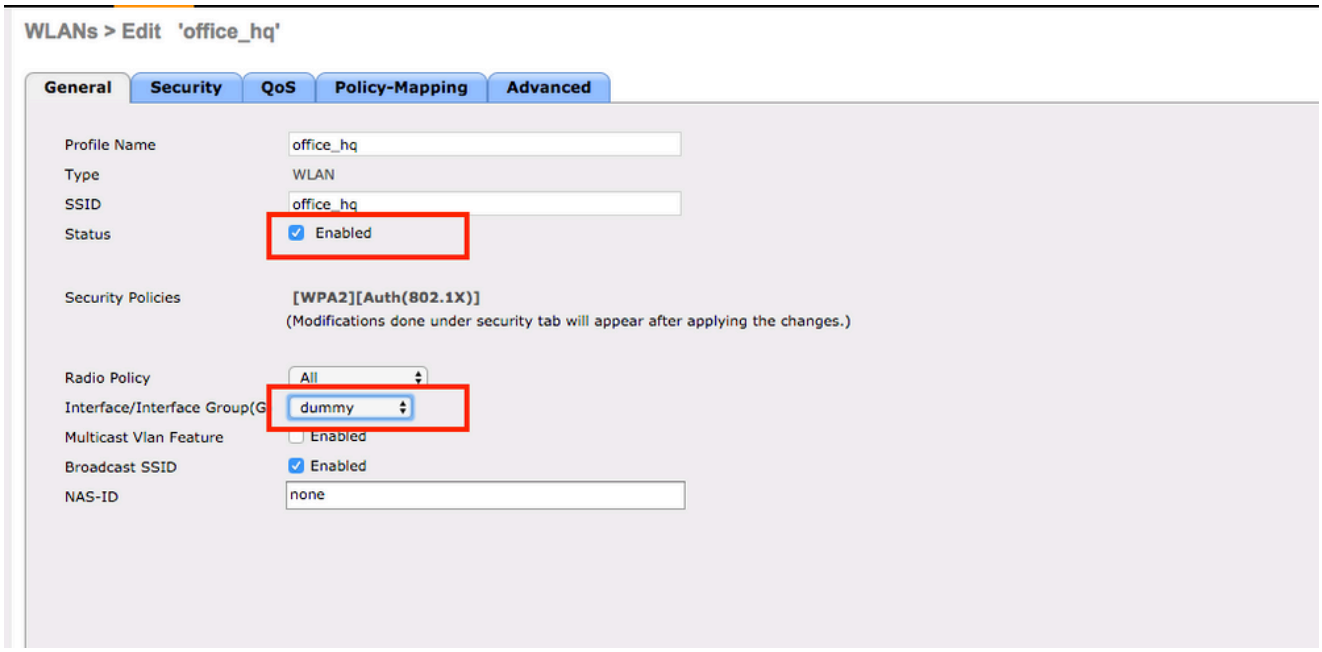
تكوين WLC لدعم مصادقة dot1x وتجاوز AAA ل SSID 'office_hq'

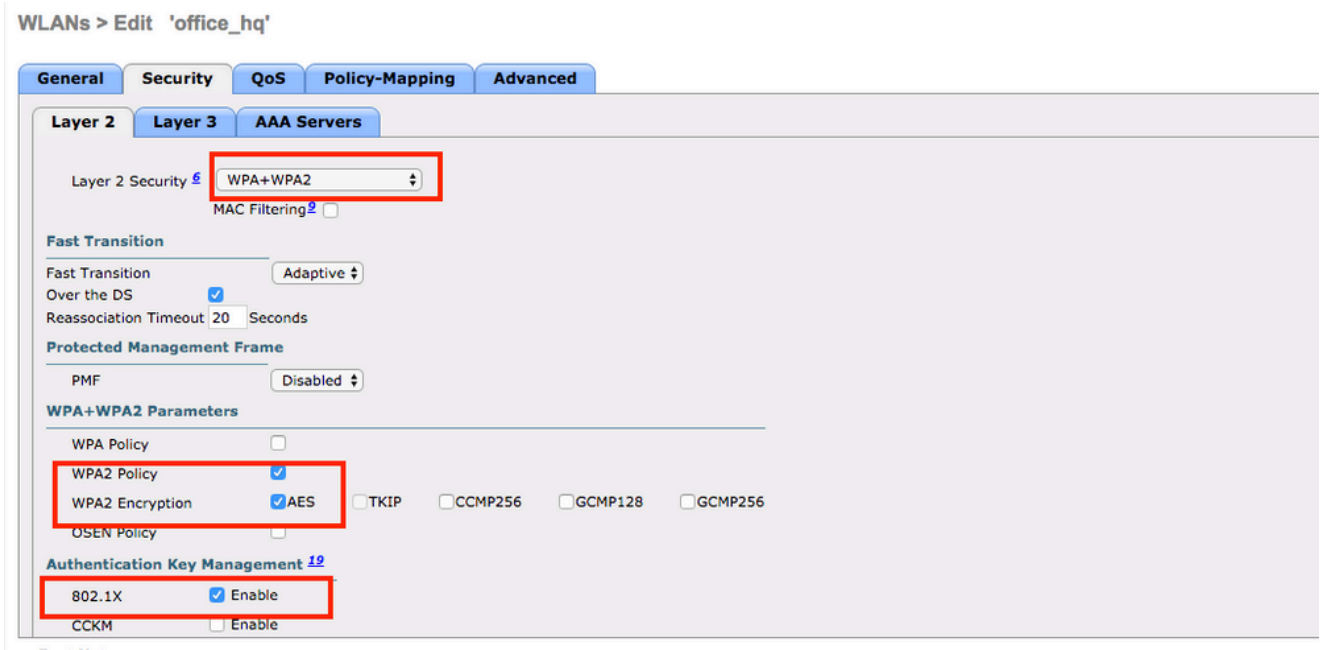
1. تكوين ISE كخادم مصادقة RADIUS على WLC. انتقل إلىSecurity > AAA > RADIUS > Authenticationقسم في واجهة مستخدم الويب ووفر عنوان ISE IP والمعلومات السرية المشتركة.

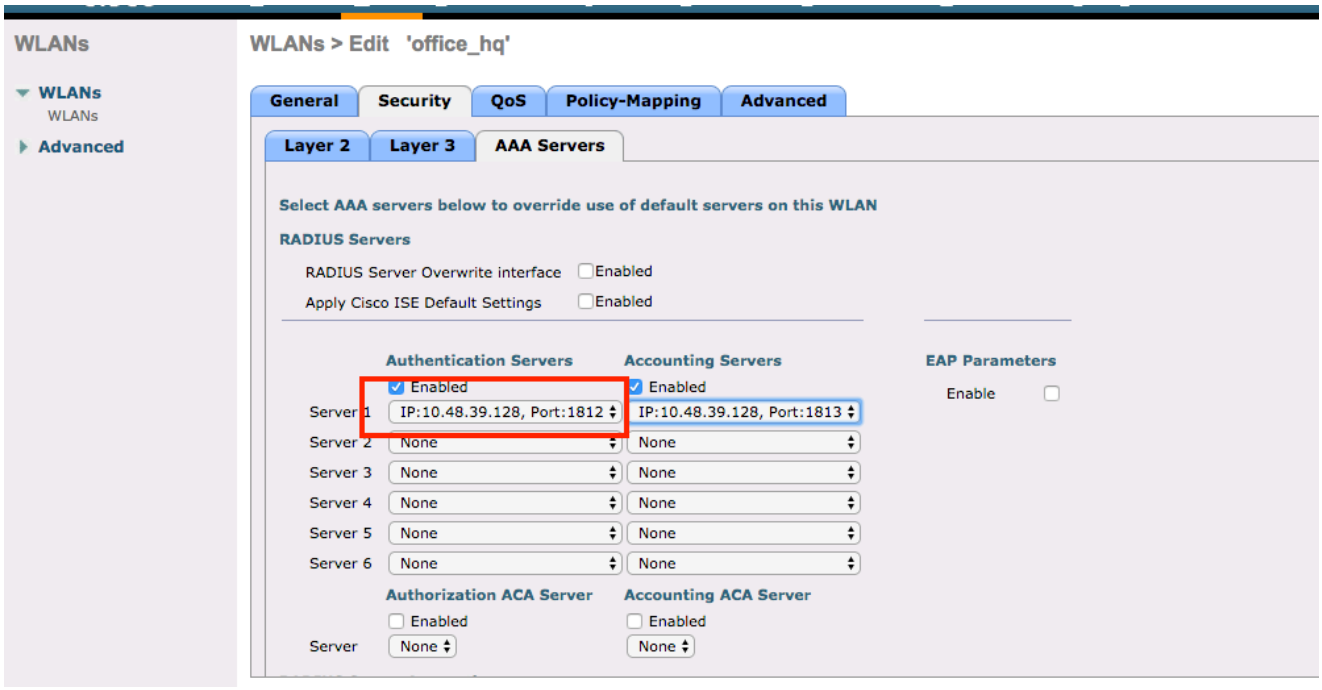


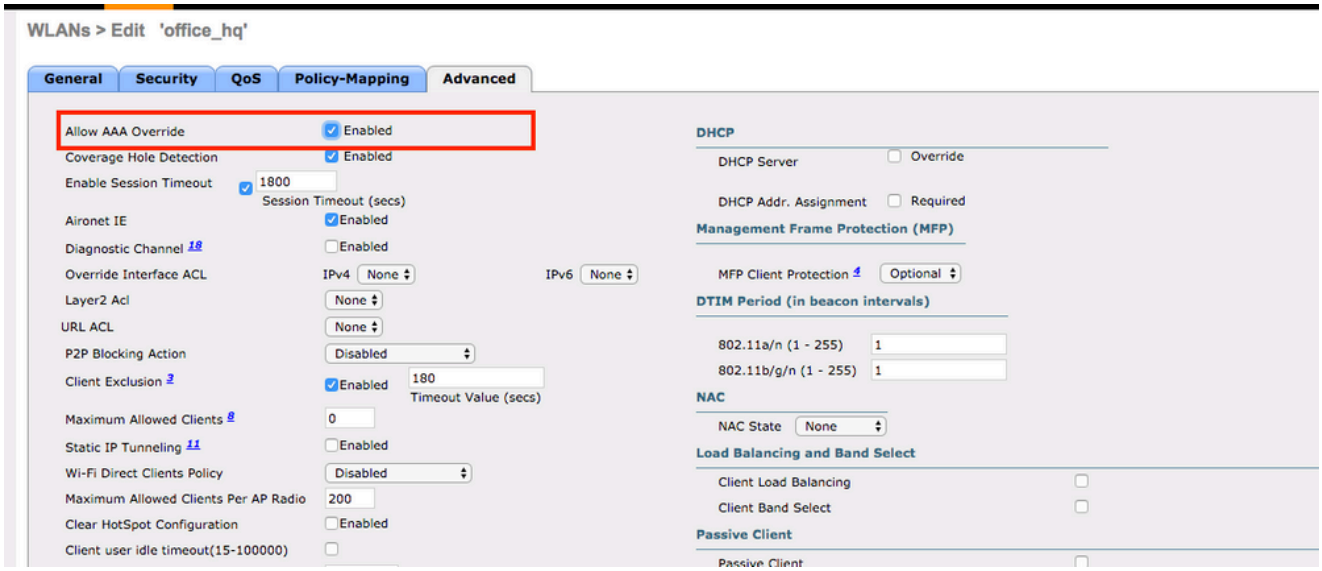
2. قم بتكوين SSIDoffice_hqضمن القسم الموجودWLANsعلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)؛ يقوم هذا المثال بتكوين SSIDWPA2/AES+dot1xبتجاوز AAA. يتم إختياراالواجهةDummyللشبكة المحلية اللاسلكية (WLAN) نظرا لأنه يتم تخصيص شبكة VLAN المناسبة عبر RADIUS على أية حال. يجب إنشاء هذه الواجهة الوهمية على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وإعطائها عنوان IP، ولكن لا يجب أن يكون عنوان IP صالحا ولا يمكن إنشاء شبكة VLAN التي يتم وضعها فيها في محول الوصلة حتى إذا لم يتم تعيين شبكة VLAN، فلن يتمكن العميل من الذهاب إلى أي مكان.



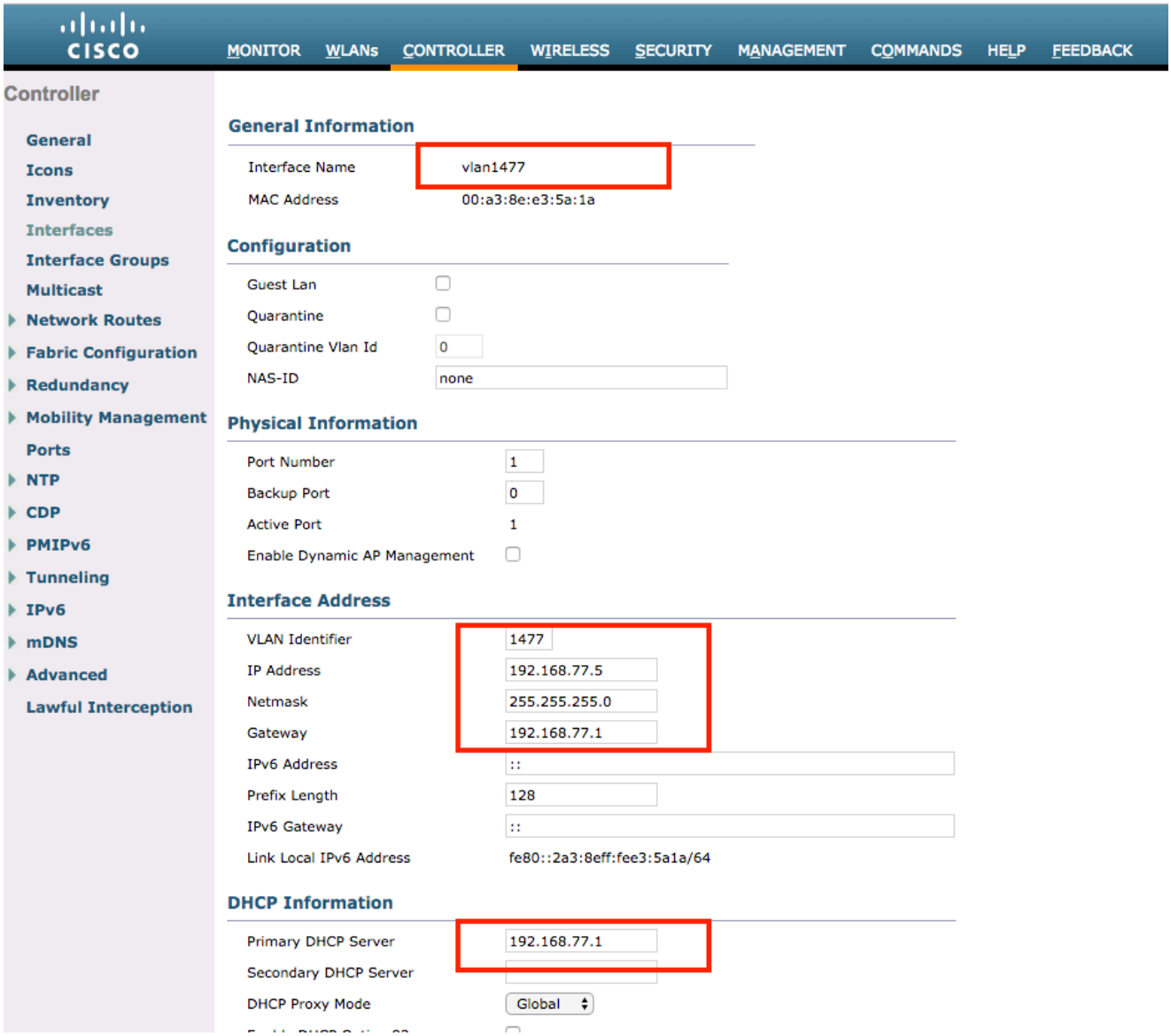

WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
office_hq
Type
WLAN
SSID
office_hq
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G
dummy
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none


WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Adaptive
Over the DS
Reassociation Timeout
20
Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable





3. أنت ينبغي أيضا خلقت قارن حرك على ال WLC ل مستعمل VLANs. انتقل إلىController > Interfacesقائمة واجهة المستخدم. ال WLC يستطيع فقط مدت VLAN يستلم عبر AAA إن يتلقى هو قارن حرك في أن VLAN.



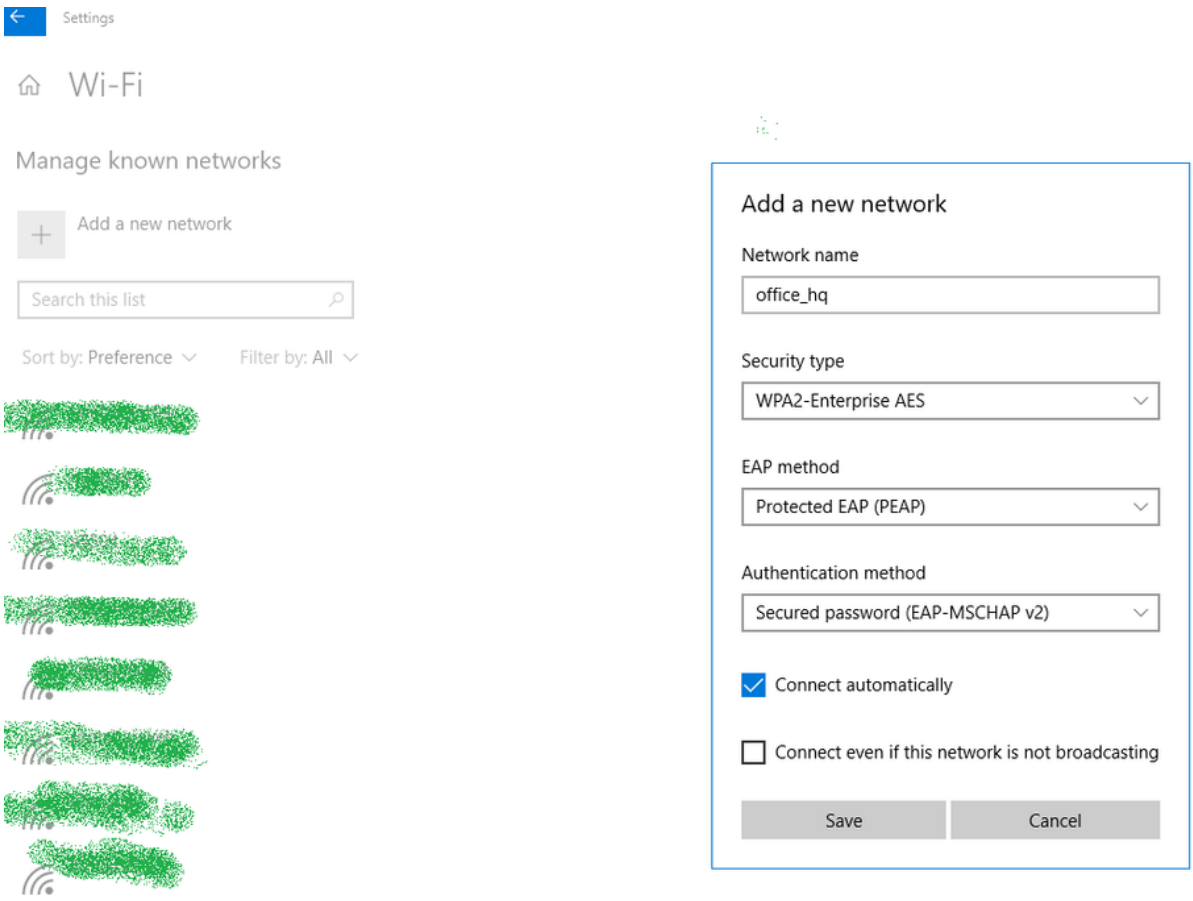
التحقق من الصحة

أستخدم المطالبة الأصلية لنظام التشغيل Windows 10 و AnyConnect NAM لاختبار الاتصالات.

بما أنك تستخدم مصادقة EAP-PEAP وأن ISE يستخدم شهادة موقعة ذاتيا (SSC)، يجب أن توافق على تحذير شهادة أو تعطيل التحقق من الشهادة. في بيئة الشركات، يجب عليك إستخدام شهادة موقعة وموثوق بها في ISE وضمان حصول أجهزة المستخدم النهائي على الشهادة الجذر المناسبة المثبتة ضمن قائمة CA الموثوق بها.

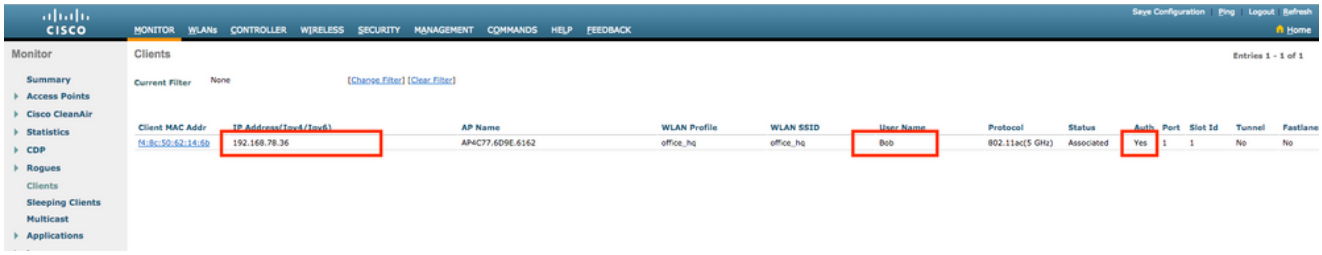
إختبار الاتصال بنظام التشغيل Windows 10 والمطالب الأصلي:

1. افتحNetwork & Internet settings > Wi-Fi > Manage known networksوقم بإنشاء ملف تعريف شبكة جديد بالضغط علىAdd new networkالزر؛ قم بتعبئة المعلومات المطلوبة.



2. تحقق من سجل المصادقة عند دخول ISE وتأكد من تحديد ملف التعريف الصحيح للمستخدم.

3. تحقق من إدخال العميل على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وتأكد من تعيينه لشبكة VLAN اليمنى ومن أنه في حالة التشغيل.



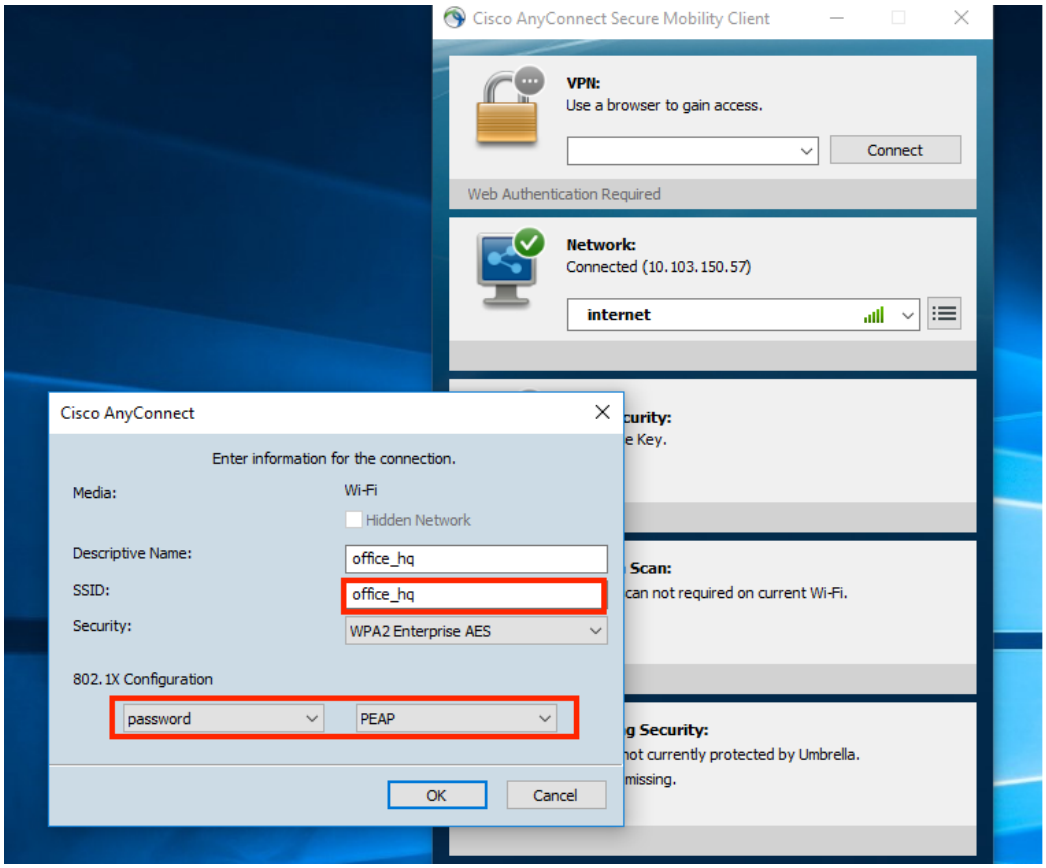
4. من واجهة سطر أوامر (CLI) عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، يمكن التحقق من حالة العميل باستخدامshow client dertails
:

```
show client detail f4:8c:50:62:14:6b
Client MAC Address.............................. f4:8c:50:62:14:6b
```

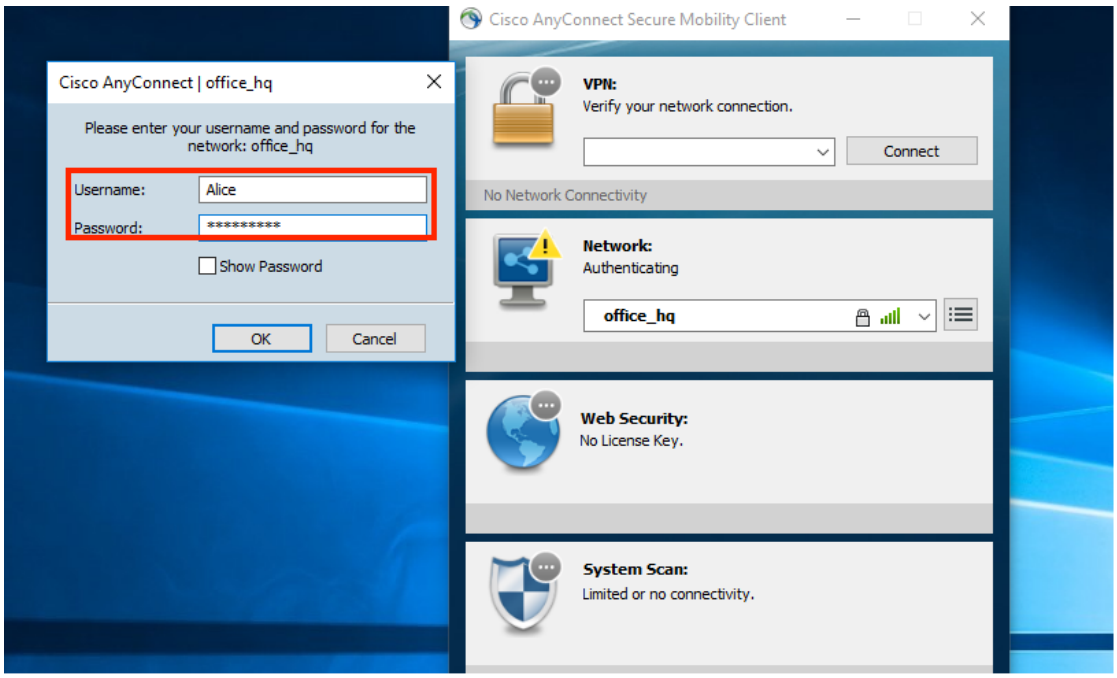
```
Client Username ..............................  Bob
Client Webauth Username ......................  N/A
Hostname: ....................................
Device Type: .................................  Intel-Device
AP MAC Address................................  70:69:5a:51:4e:c0
AP Name.......................................  AP4C77.6D9E.6162
AP radio slot Id..............................  1
Client State..................................  Associated
User Authenticated by ........................  RADIUS Server
Client User Group.............................  Bob
Client NAC OOB State..........................  Access
Wireless LAN Id...............................  3
Wireless LAN Network Name (SSID).............  office_hq
Wireless LAN Profile Name.....................  office_hq
Hotspot (802.11u).............................  Not Supported
Connected For ................................  242 secs
BSSID.........................................  70:69:5a:51:4e:cd
Channel.......................................  36
IP Address....................................  192.168.78.36
Gateway Address...............................  192.168.78.1
Netmask.......................................  255.255.255.0
...
Policy Manager State..........................  RUN
...
EAP Type......................................  PEAP
Interface.....................................  vlan1478
VLAN..........................................  1478
Quarantine VLAN...............................  0
Access VLAN...................................  1478
```

إختبار الاتصال ب Windows 10 و AnyConnect NAM:

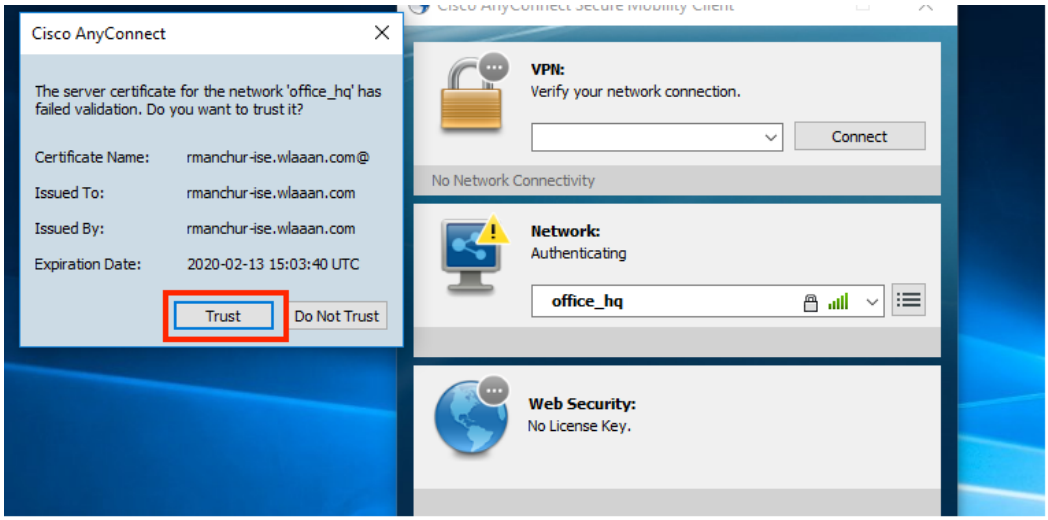
1. أختر SSID من قائمة SSID المتاحة ونوع مصادقة EAP الخاص (في هذه المثال PEAP) ونموذج المصادقة الداخلية.



2. قم بتوفير اسم المستخدم وكلمة المرور لمصادقة المستخدم.

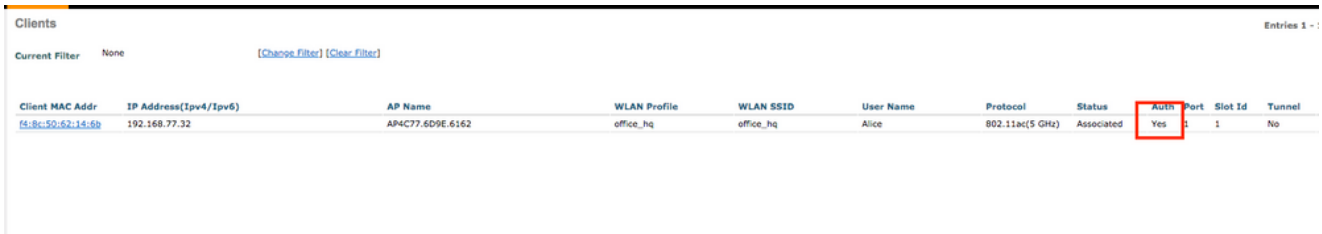


3. ونظرا لأن ISE يقوم بإرسال SSC إلى العميل، فيجب عليك إختيار الثقة في الشهادة يدويا (في بيئة الإنتاج يوصى بشدة بتثبيت الشهادة الموثوق بها على ISE).



4. تحقق من سجلات المصادقة على ISE وتأكد من تحديد ملف تعريف التخويل الصحيح للمستخدم.

5. تحقق من إدخال العميل على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وتأكد من تعيينه لشبكة VLAN الميمنى ومن أنه في حالة التشغيل.



6. من واجهة سطر أوامر (CLI) عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، يمكن التحقق من حالة العميل باستخدامshow client dertails
:

```
Client MAC Address..............................  f4:8c:50:62:14:6b
Client Username ................................  Alice
Client Webauth Username ........................  N/A
Hostname: ......................................
Device Type: ...................................  Intel-Device
AP MAC Address..................................  70:69:5a:51:4e:c0
AP Name.........................................  AP4C77.6D9E.6162
```

```
AP radio slot Id..................................... 1
Client State..................................... Associated
User Authenticated by ........................... RADIUS Server
Client User Group................................ Alice
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 3
Wireless LAN Network Name (SSID)................. office_hq
Wireless LAN Profile Name........................ office_hq
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 765 secs
BSSID............................................ 70:69:5a:51:4e:cd
Channel.......................................... 36
IP Address....................................... 192.168.77.32
Gateway Address.................................. 192.168.77.1
Netmask.......................................... 255.255.255.0
...
Policy Manager State............................. RUN
...
Policy Type...................................... WPA2
Authentication Key Management.................... 802.1x
Encryption Cipher................................ CCMP-128 (AES)
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... PEAP
Interface........................................ vlan1477
VLAN............................................. 1477
```

استكشاف الأخطاء وإصلاحها

1. استعملت in ordertest aaa radius username

   password

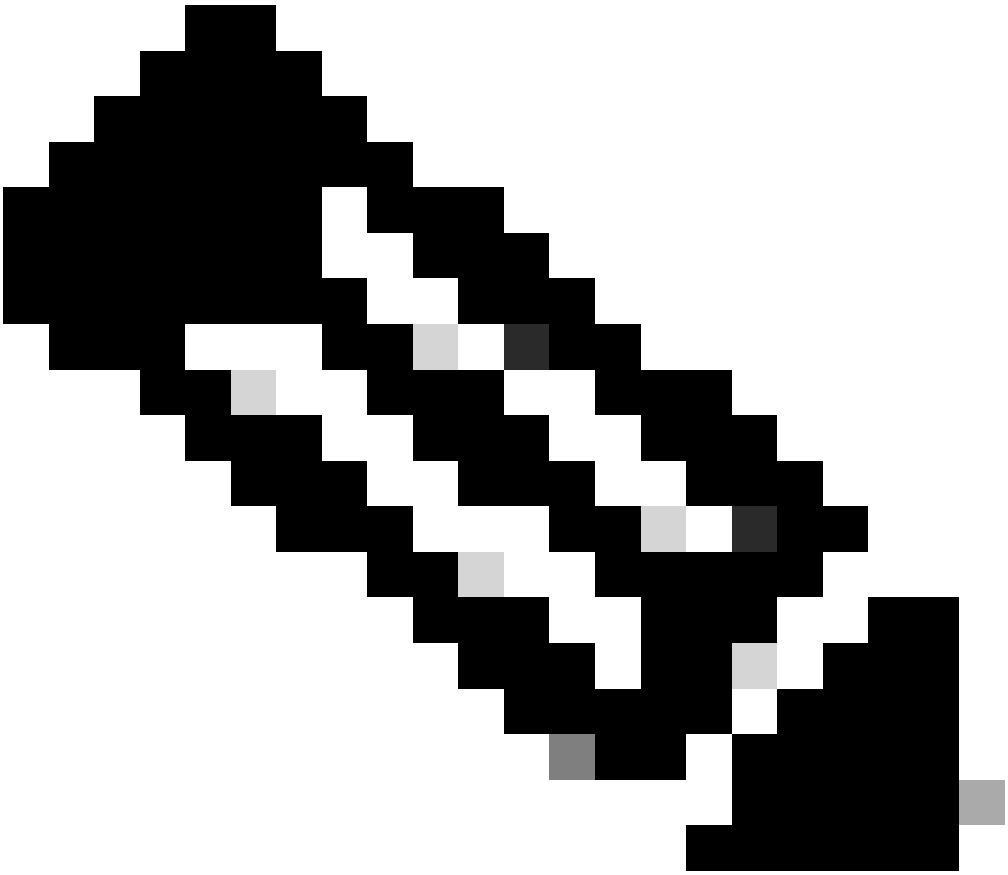
   wlan-id

to اختبرت ال RADIUS توصيل بين WLC و ISEtest aaa show radiusin order to عرضت النتائج.

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id.......................................... 2
  ApGroup Name..................................... none

  Attributes                    Values
  ----------                    ------
  User-Name                     Alice
  Called-Station-Id             00-00-00-00-00-00:AndroidAP
  Calling-Station-Id            00-11-22-33-44-55
  Nas-Port                      0x00000001 (1)
```

```
  Nas-Ip-Address                  10.48.71.20
  NAS-Identifier                  0x6e6f (28271)
  Airespace / WLAN-Identifier     0x00000002 (2)
  User-Password                   cisco!123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Cisco / Audit-Session-Id        1447300a0000003041d5665c
  Acct-Session-Id                 5c66d541/00:11:22:33:44:55/743


test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none
Radius Test Response

Radius Server            Retry Status
-------------            ----- ------
10.48.39.128             1     Success

Authentication Response:
  Result Code: Success

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  State                           ReauthSession:1447300a0000003041d5665c
  Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x000005c5 (1477)


(Cisco Controller) >
```

2. استعملت ال debug client
   in order to تحريت السلكي زبون موصولية إصدار.
3. أستخدمdebug aaa all enableالأمر السكشاف أخطاء المصادقة والتفويض وإصلاحها على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).



ملاحظة: أستخدم هذا الأمر فقط مع debug mac addr لتحديد الإخراج استنادا إلى عنوان MAC الذي يتم تصحيح الأخطاء له.

4. ارجع إلى سجلات ISE المباشرة وسجلات الجلسات لتحديد مشاكل حالات فشل المصادقة ومشاكل إتصالات AD.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).