الوصول إلى الإدارة ل AireOS WLC من خلال Microsoft NPS

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل إدارة منفذ ل AireOS WLC GUI و CLI من خلال ال مايكروسوفت شبكة سياسة خادم (NPS).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة حلول الأمان اللاسلكية
- مفاهيم المصادقة والتفويض والمحاسبة (AAA) و RADIUS
- معرفة أساسية بخادم Microsoft Server 2012
- تثبيت Microsoft NPS و Active Directory (AD)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مكونات البرامج والأجهزة التالية.

- وحدة تحكم AireOS (5520) في 8.8.120.0
- نظام التشغيل Microsoft Server 2012

ملاحظة: يهدف هذا المستند إلى إعطاء القارئ مثال للتكوين المطلوب على خادم Microsoft المقدم في Microsoft Windows لتمكين الوصول إلى إدارة WLC. تم إختبار تكوين خادم Microsoft Windows المقدم في هذا المستند في المعمل وتبين أنه يعمل كما هو متوقع. إذا واجهت مشكلة في التكوين، فاتصل ب Microsoft للحصول على تعليمات. ال يدعم مركز المساعدة التقنية (TAC) من Cisco تكوين خادم Microsoft Windows. يمكن العثور على أدلة تكوين وتثبيت نظام التشغيل Microsoft Windows 2012 على Microsoft Tech Net.

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

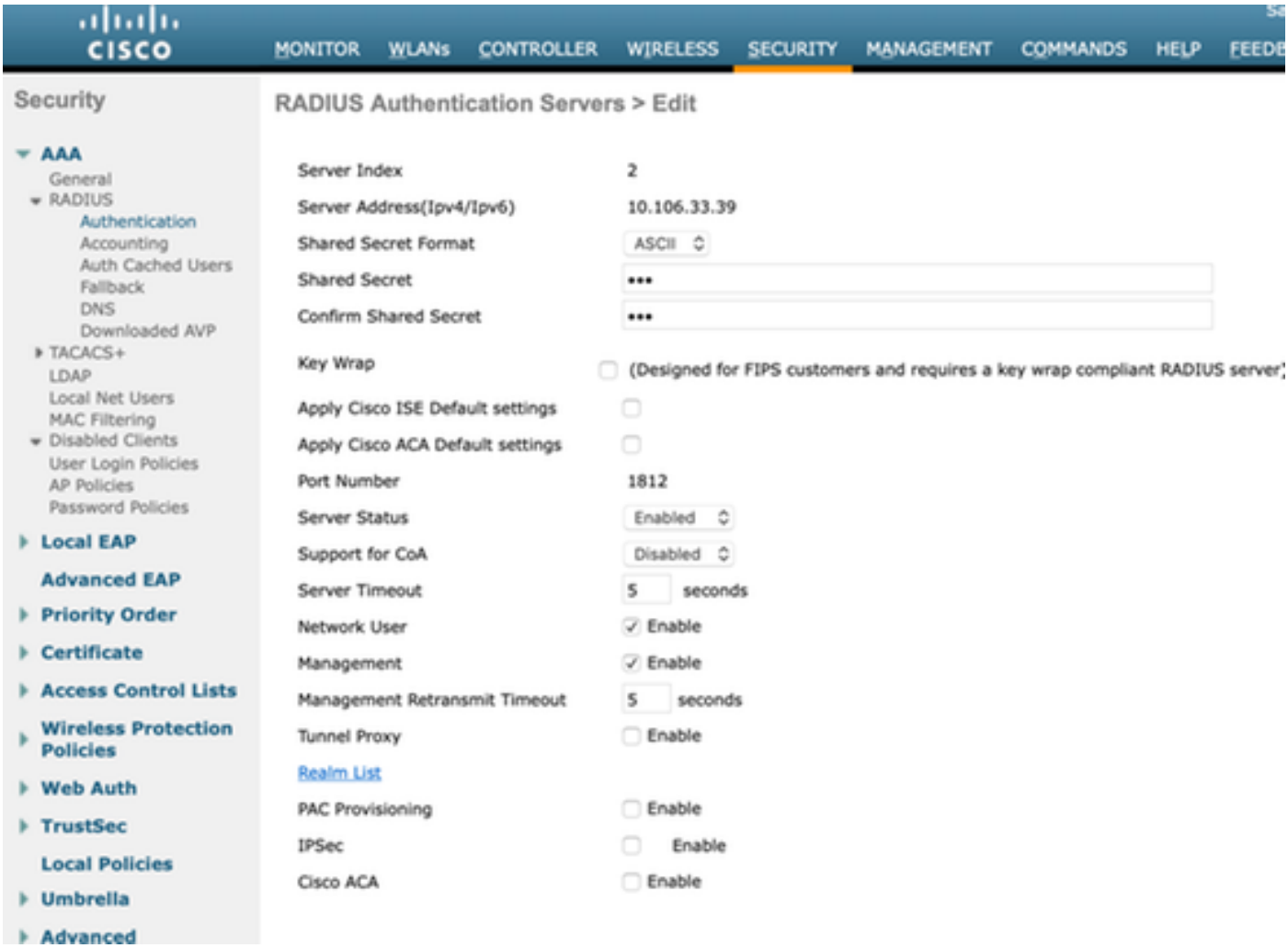
عند الوصول إلى WLC CLI/GUI، تتم مطالبة المستخدم بإدخال بيانات الاعتماد لتسجيل الدخول بنجاح. يمكن التحقق من بيانات الاعتماد مقابل قاعدة بيانات محلية أو خادم AAA خارجي. في هذا المستند، يتم استخدام Microsoft NPS كخادم مصادقة خارجي.

التكوينات

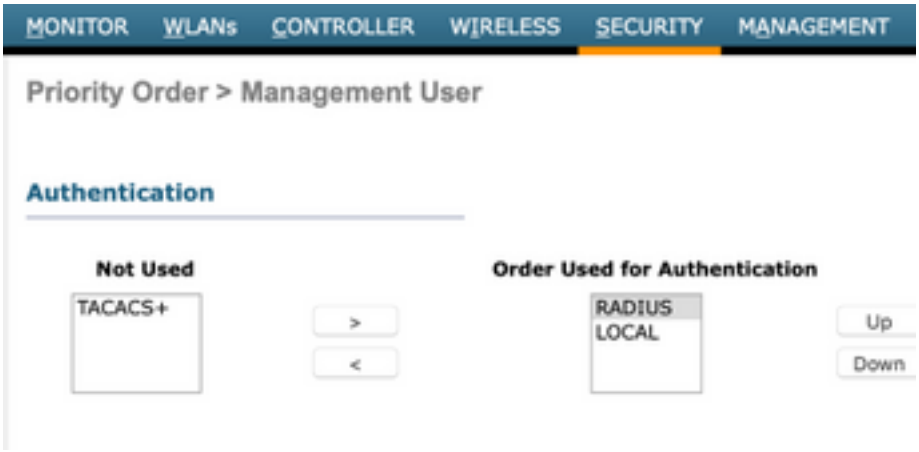
في هذا المثال، تم تكوين إثنين من المستخدمين على مزيج AAA (NPS). وLogUser وAdmin. يتمتع LogInUser بالوصول للقراءة فقط بينما يتم منح AdminUser حق الوصول الكامل.

تكوين وحدة التحكُّم في شبكة LAN اللاسلكية (WLC)

الخطوة 1. إضافة خادم RADIUS على وحدة التحكم. انتقل إلى **المصادقة > RADIUS > التأمين**. انقر فوق **جديد** لإضافة الخادم. تأكد من تمكين خيار **الإدارة** بحيث يمكن إستخدام هذا الخادم للوصول إلى الإدارة، كما هو موضح في هذه الصورة.



الخطوة 2. انتقل إلى **الأمان > ترتيب الأولوية > مستخدم الإدارة**. تأكد من تحديد RADIUS كأحد أنواع المصادقة.

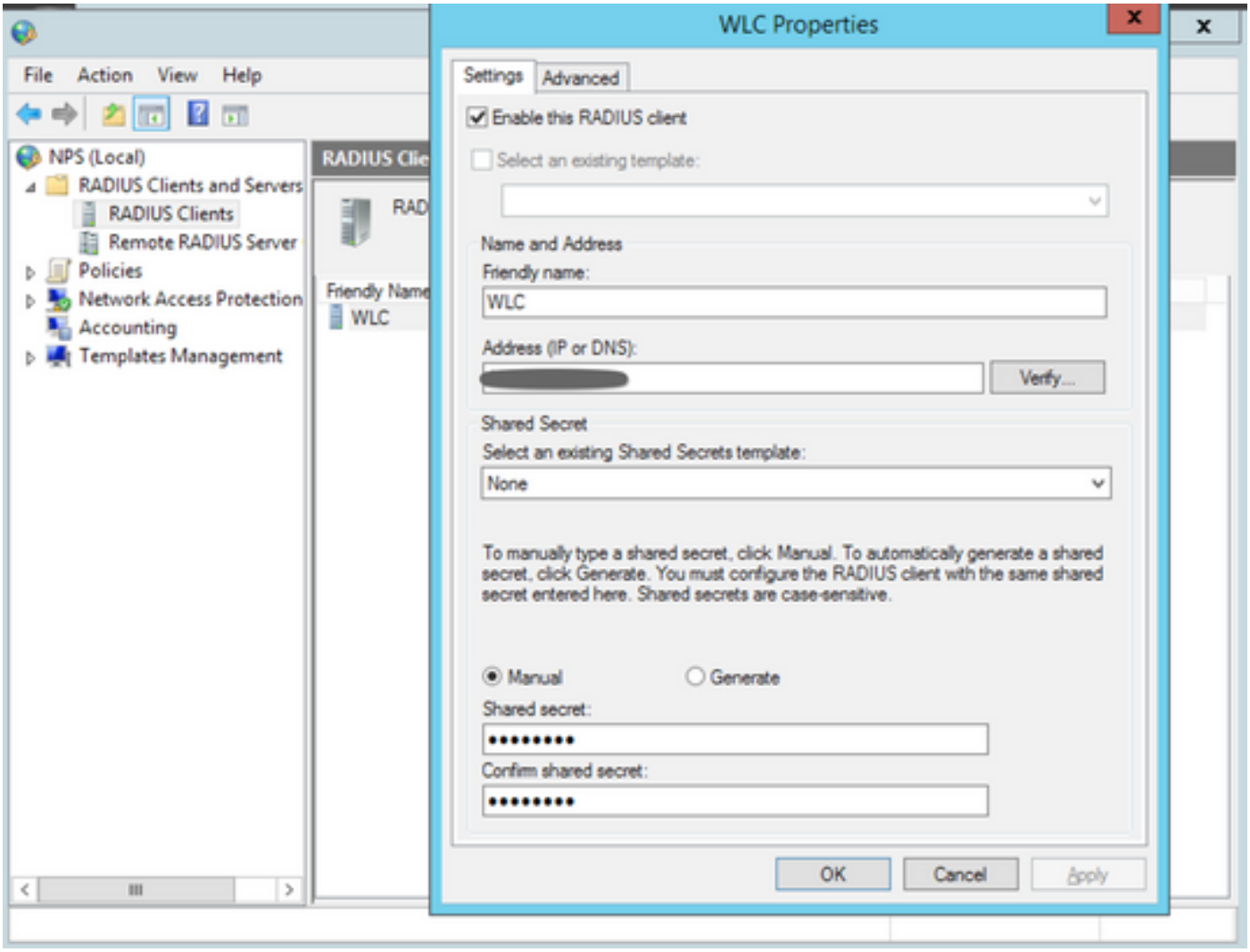


ملاحظة: إذا تم تحديد RADIUS كأولوية أولى في أمر المصادقة، فسيتم إستخدام بيانات الاعتماد المحلية للمصادقة فقط إذا كان خادم RADIUS غير قابل للوصول إليه. إذا تم تحديد RADIUS كأولوية ثانية، فسيتم التحقق من بيانات اعتماد RADIUS أوالا مقابل قاعدة البيانات المحلية ثم بعد ذلك، فحصها مقابل خوادم RADIUS التي تم تكوينها.

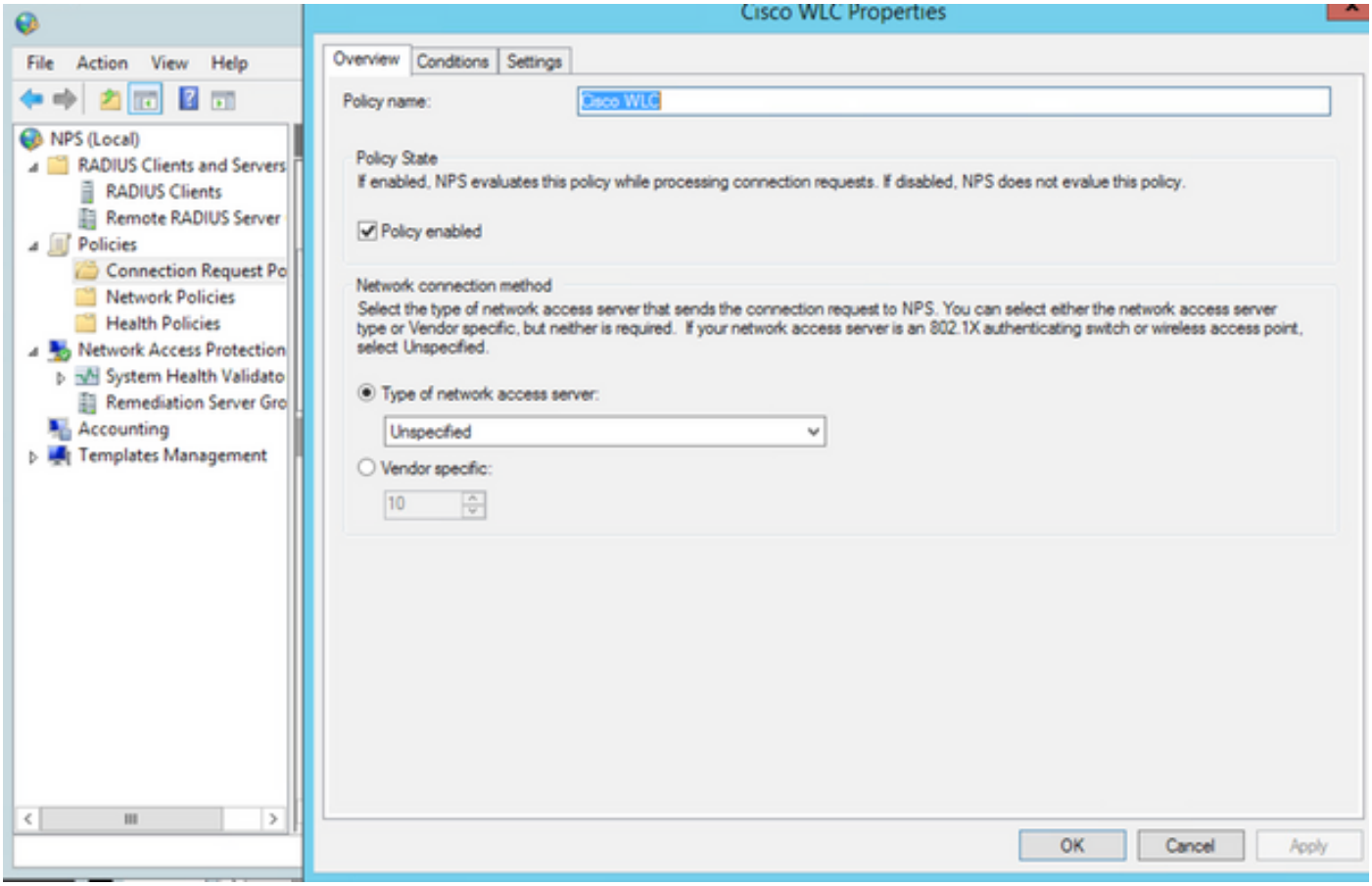
تكوين Microsoft NPS

الخطوة 1. افتح خادم Microsoft NPS. انقر بزر الماوس الأيمن فوق **عملاء RADIUS**. انقر فوق **جديد** لإضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل RADIUS.

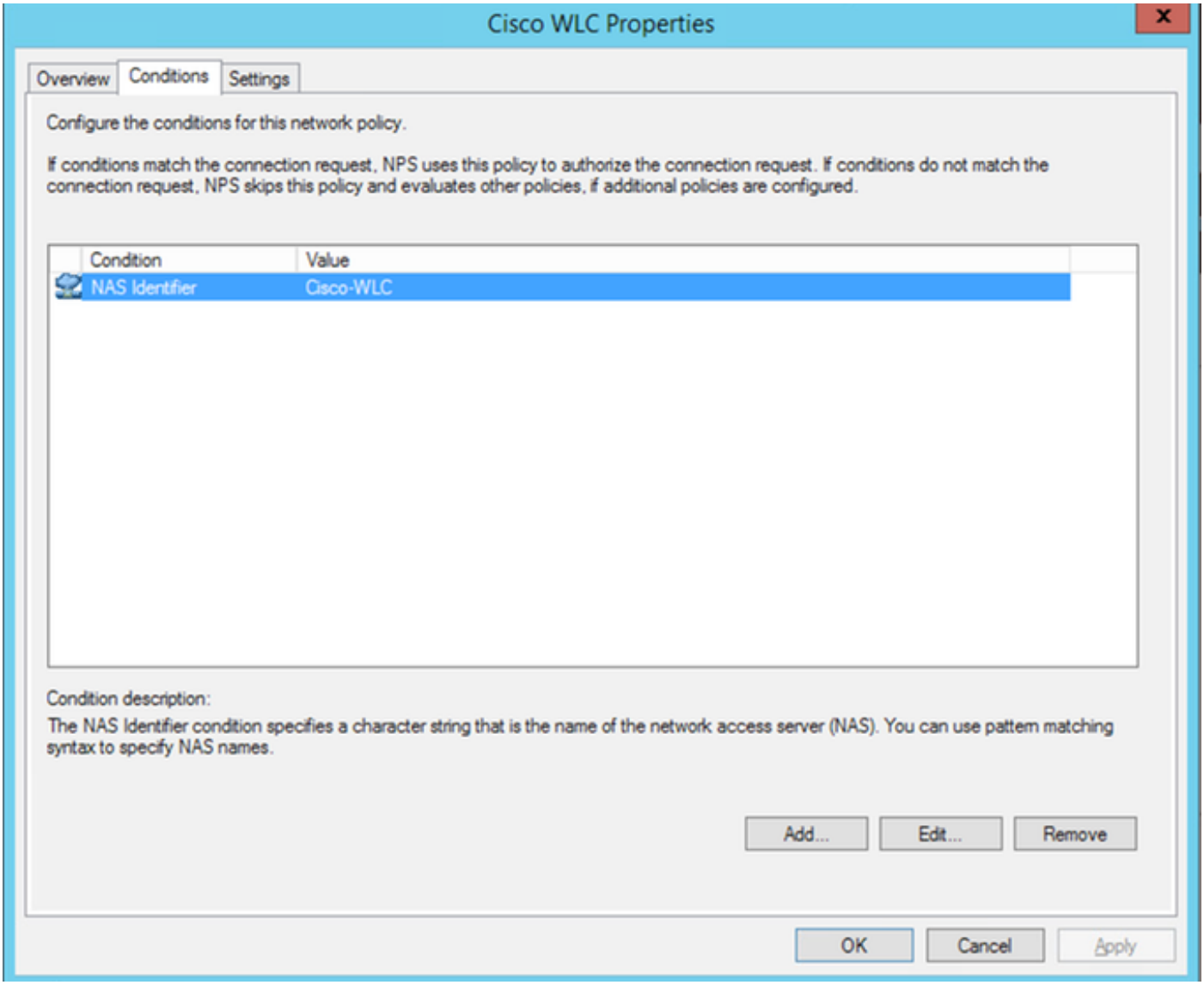
أدخل التفاصيل المطلوبة. الرجاء التأكد من أن السر المشترك هو نفسه الذي تم تكوينه على وحدة التحكم أثناء إضافة خادم RADIUS.



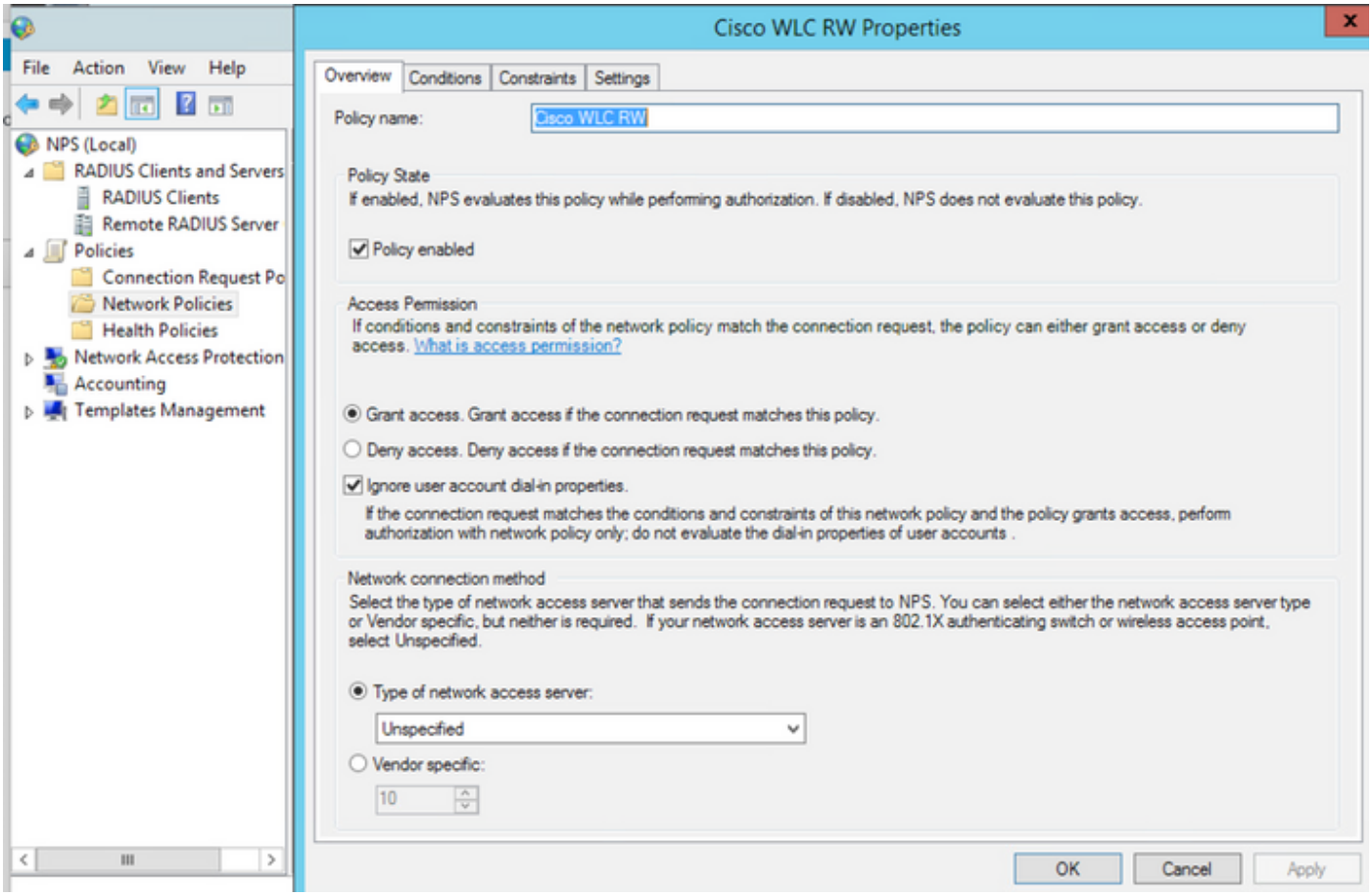
الخطوة 2. انتقل إلى **السياسات > نهج طلب الاتصال**. انقر بزر الماوس الأيمن لإضافة نهج جديد، كما هو موضح في الصورة.



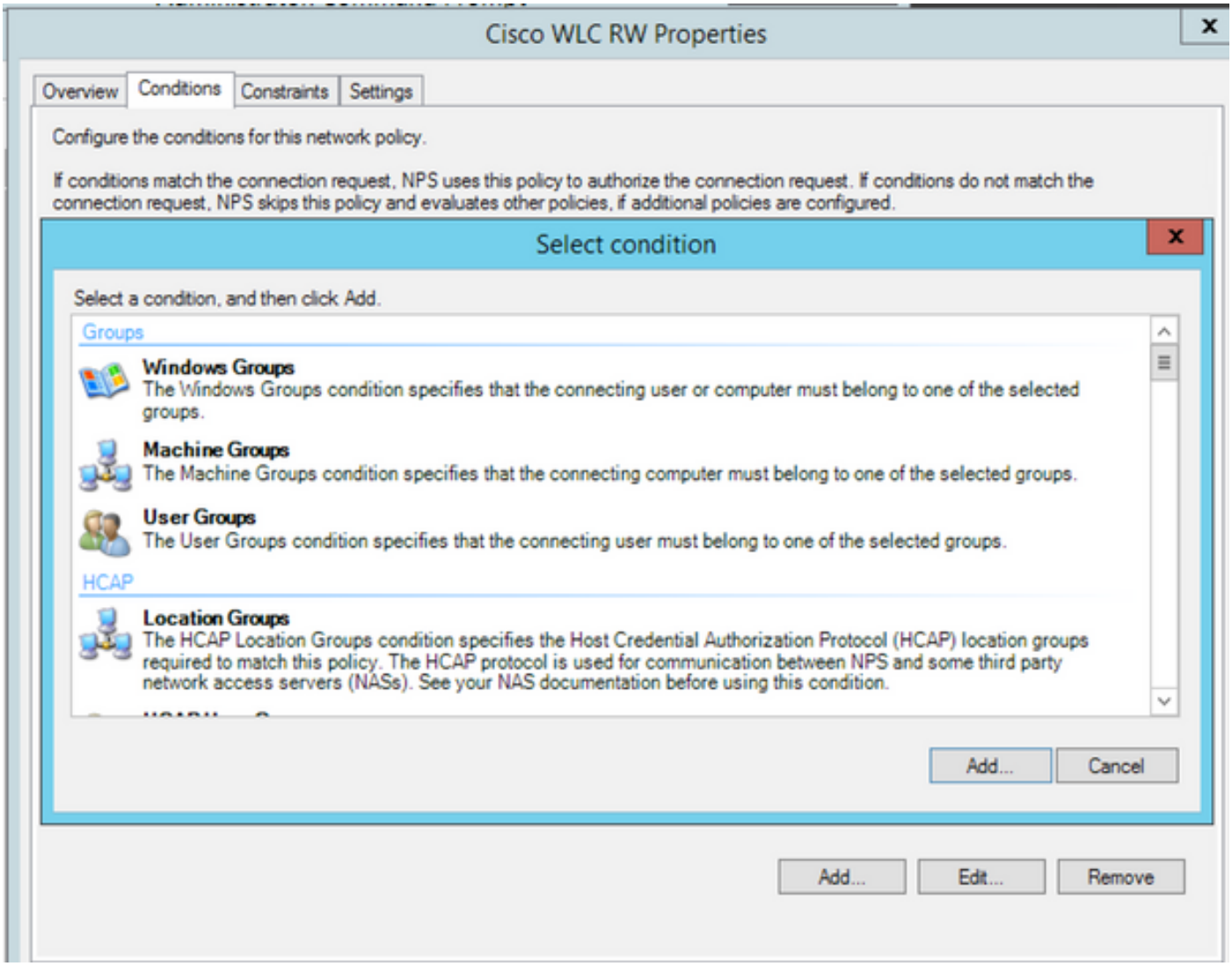
الخطوة 3. تحت علامة التبويب **شروط**، حدد **معرف NAS** كشرط جديد. عند المطالبة، أدخل اسم المضيف لوحدة التحكم كقيمة، كما هو موضح في الصورة.



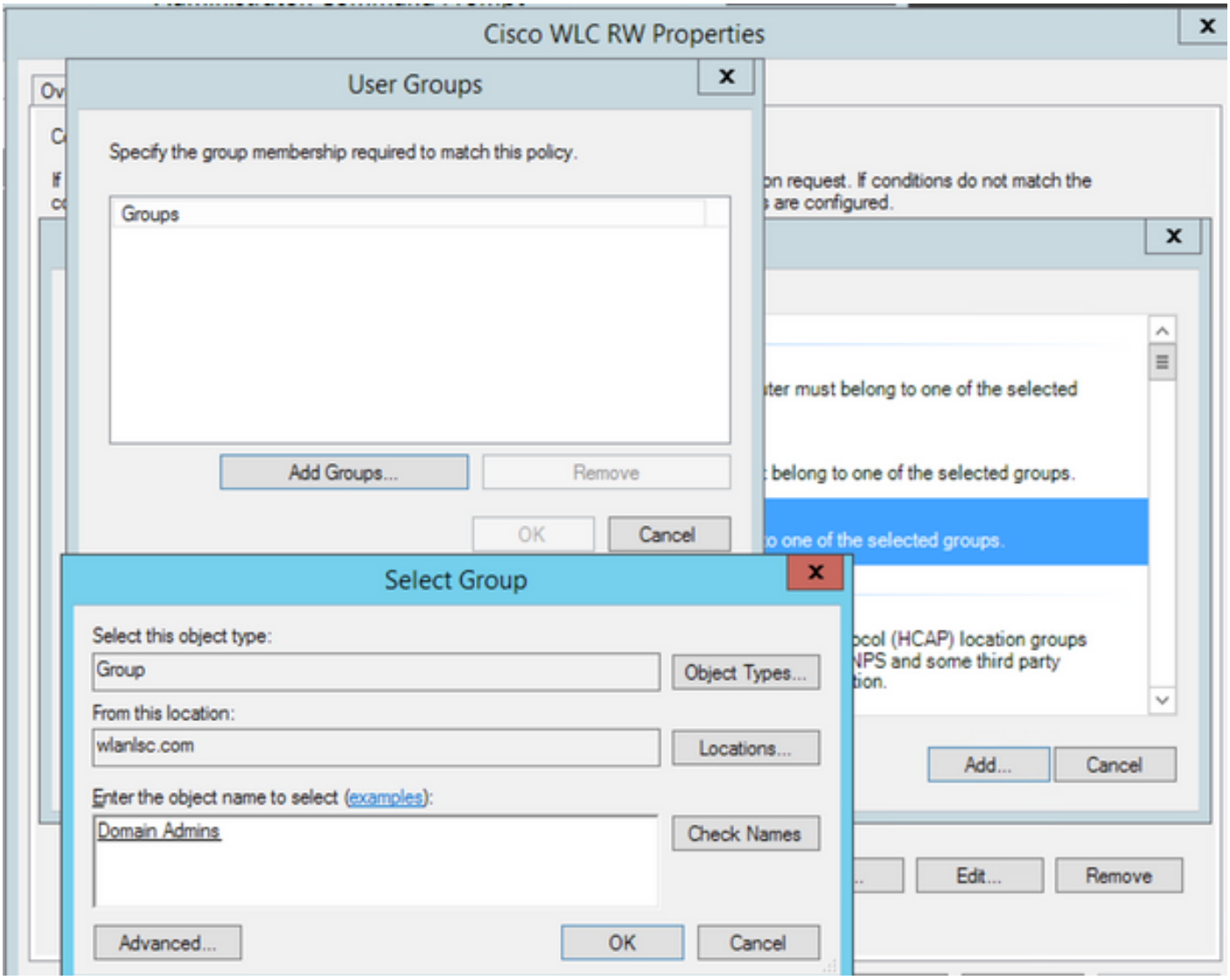
الخطوة 4. انتقل إلى **السياسات > سياسات الشبكة**. انقر بزر الماوس الأيمن لإضافة نهج جديد. في هذا المثال، يتم تسمية السياسة باسم **Cisco WLC RW** وهو ما يشير إلى إستخدام السياسة لتوفير الوصول الكامل (للقراءة والكتابة). تأكد من تكوين السياسة كما هو موضح هنا.



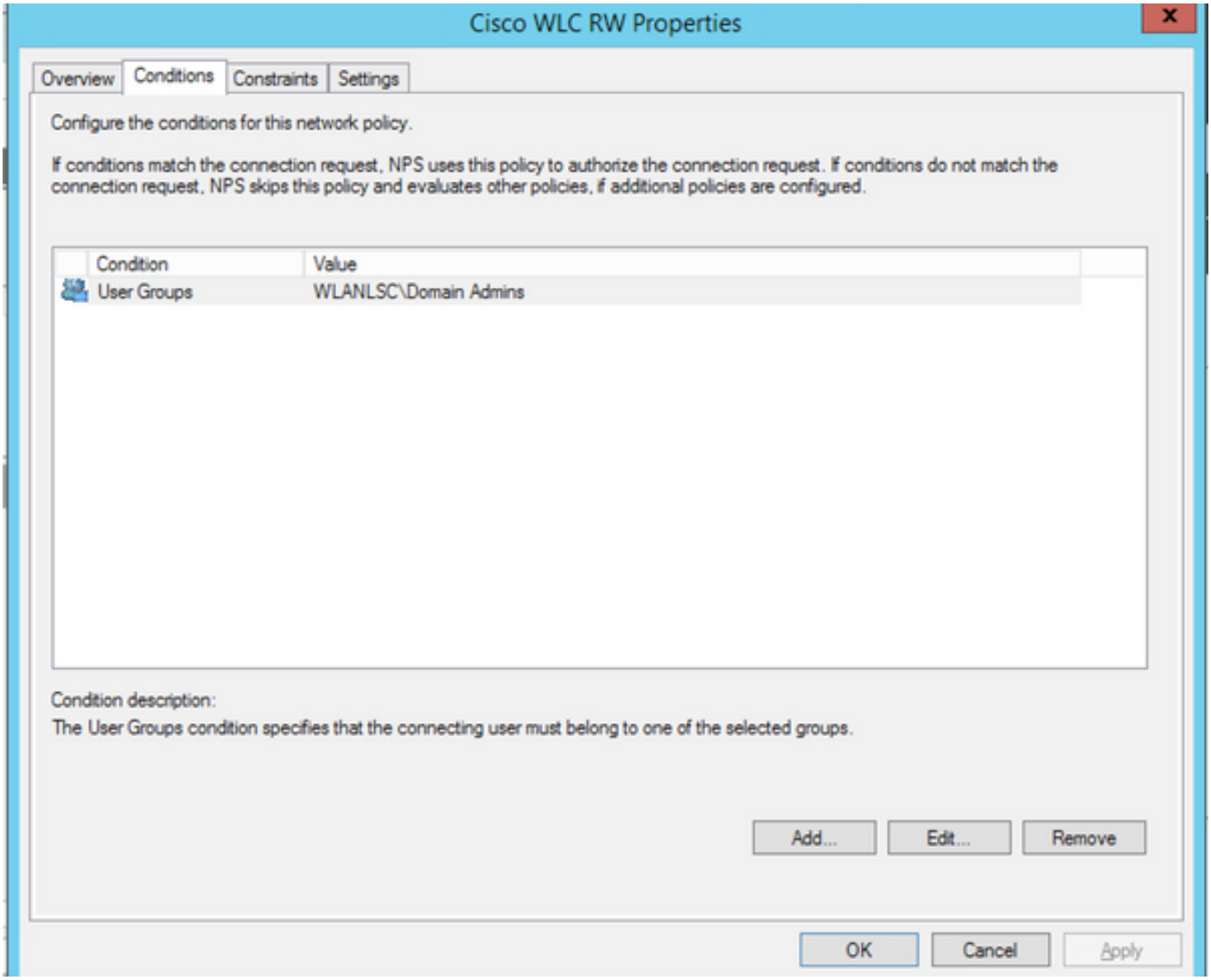
الخطوة 5. تحت علامة التبويب **الشروط**، انقر فوق **إضافة**. حدد **مجموعات المستخدمين** وانقر فوق **إضافة**، كما هو موضح في الصورة.



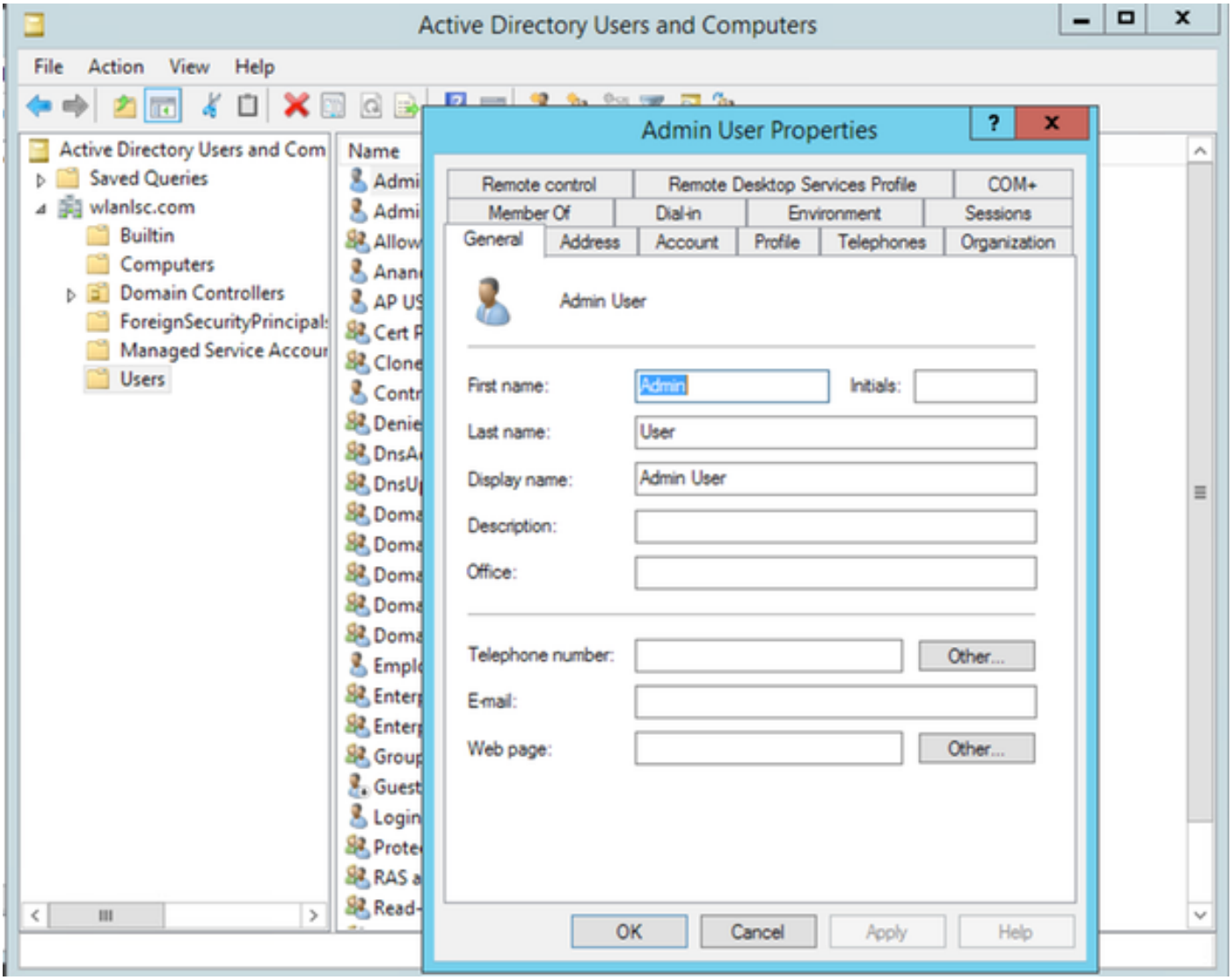
الخطوة 6. انقر فوق **إضافة مجموعات** في الشاشة التي تظهر. في نافذة **تحديد مجموعة** التي تظهر، حدد **نوع الكائن** المرغوب و **الموقع** وأدخل اسم الكائن المطلوب، كما هو موضح في الصورة.

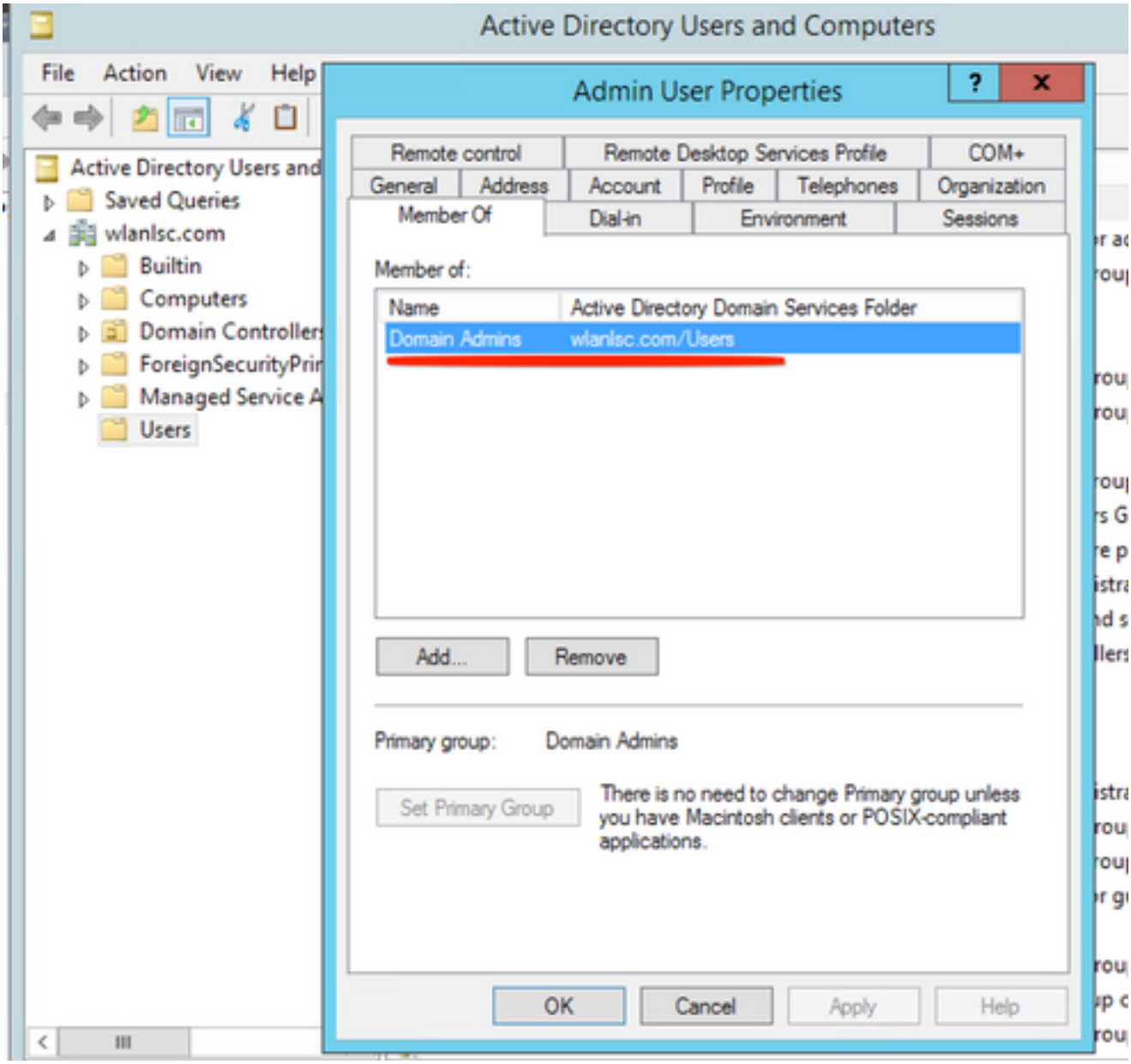


إذا تمت إضافة الشرط بشكل صحيح، فيجب أن يبدو كما هو موضح هنا.

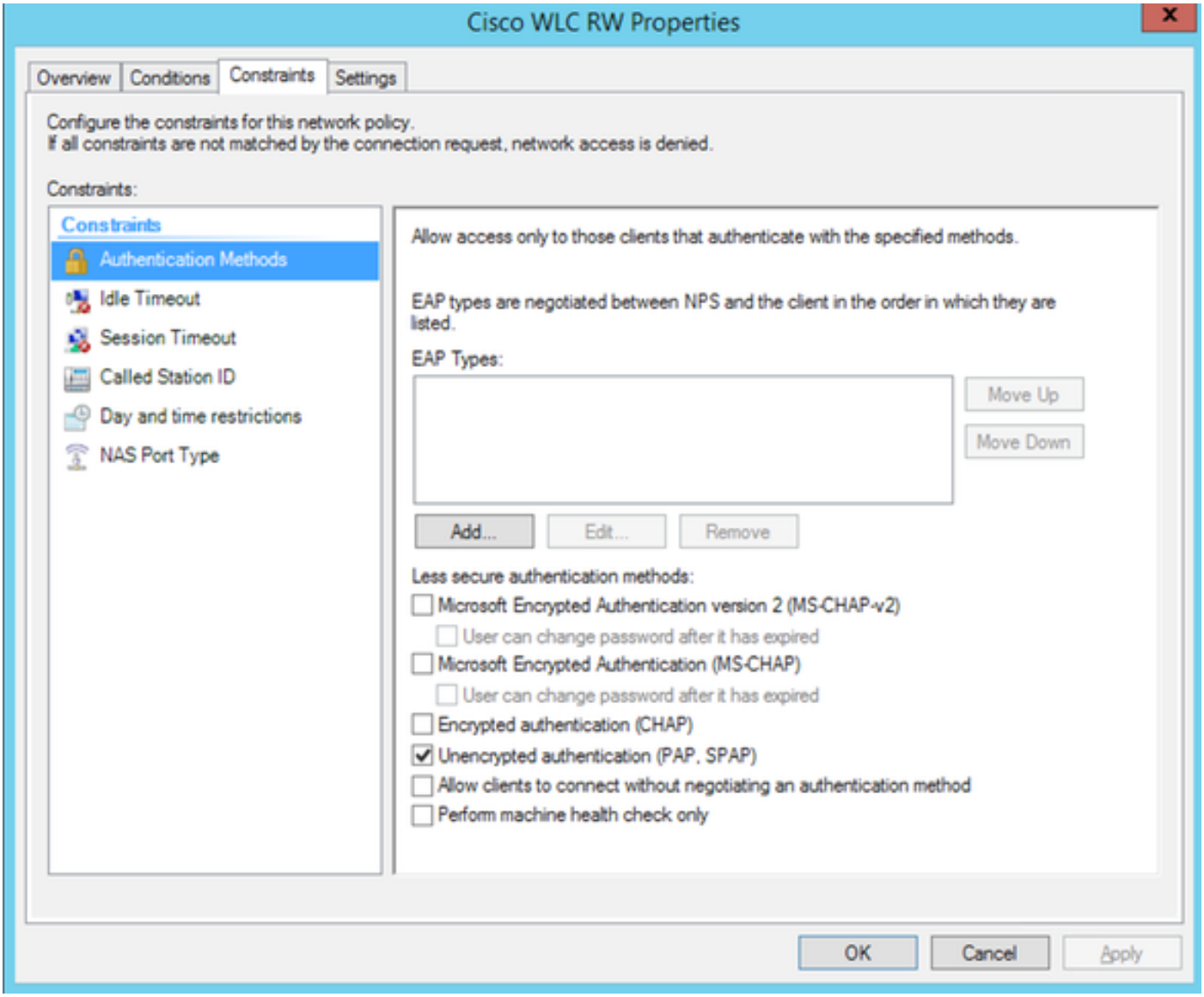


ملاحظة: لمعرفة تفاصيل الموقع واسم الكائن، افتح Active Directory وابحث عن اسم المستخدم المطلوب. في هذا المثال، يتكون **مسؤولو المجال** من مستخدمين يتم منحهم حق الوصول الكامل. **AdminUser** هو جزء من اسم الكائن هذا.

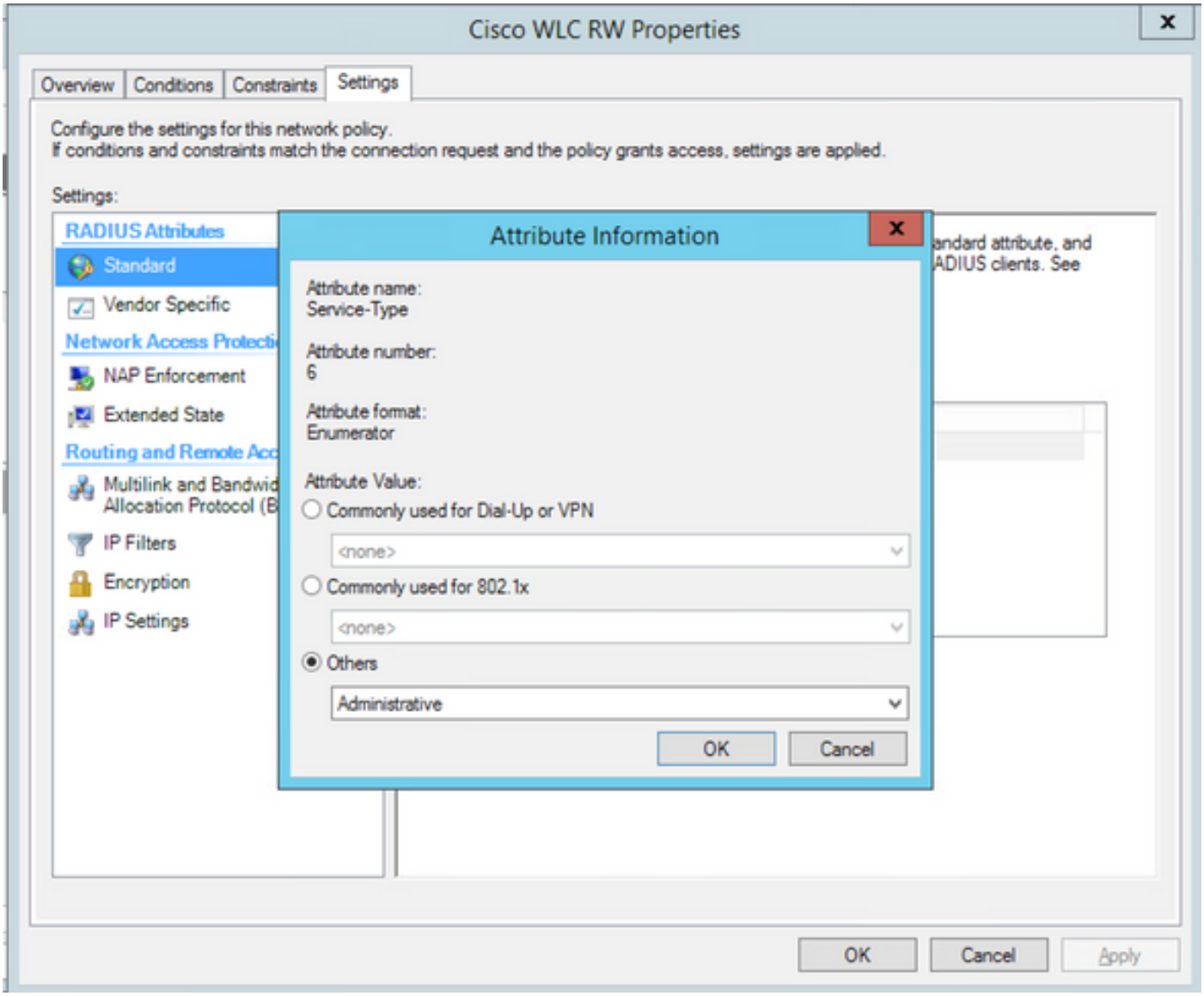

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
wlanlsc.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Admin User Properties
Remote control
Remote Desktop Services Profile
COM+
Member Of
Dial-in
Environment
Sessions
General
Address
Account
Profile
Telephones
Organization
Admin User
First name:
Admin
Initials:
Last name:
User
Display name:
Admin User
Description:
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...
OK
Cancel
Apply
Help



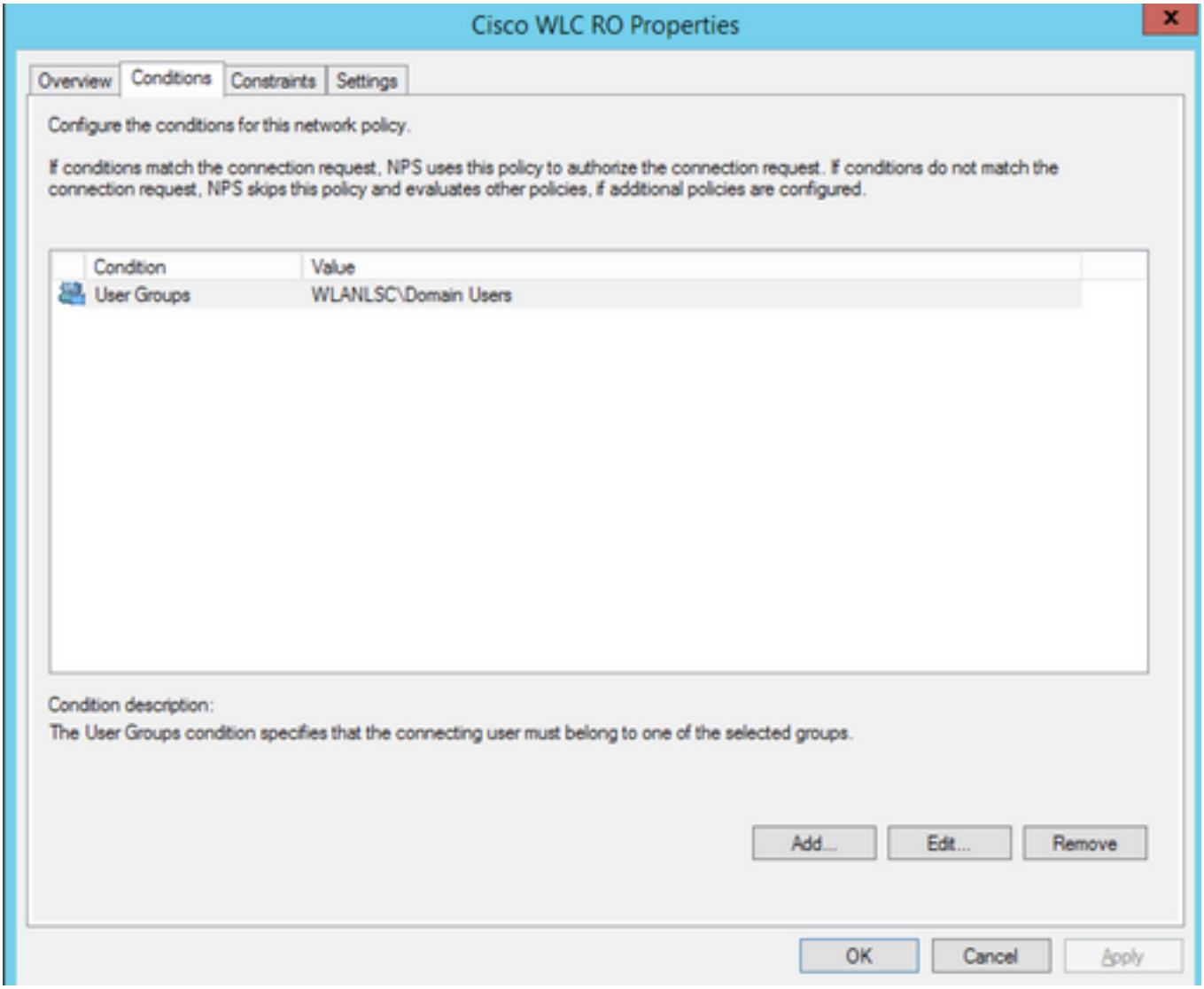
الخطوة 7. تحت علامة التبويب **قيود**، انتقل إلى **طرق المصادقة** وتأكد من أنه **تم التحقق من المصادقة غير المشفرة** فقط.

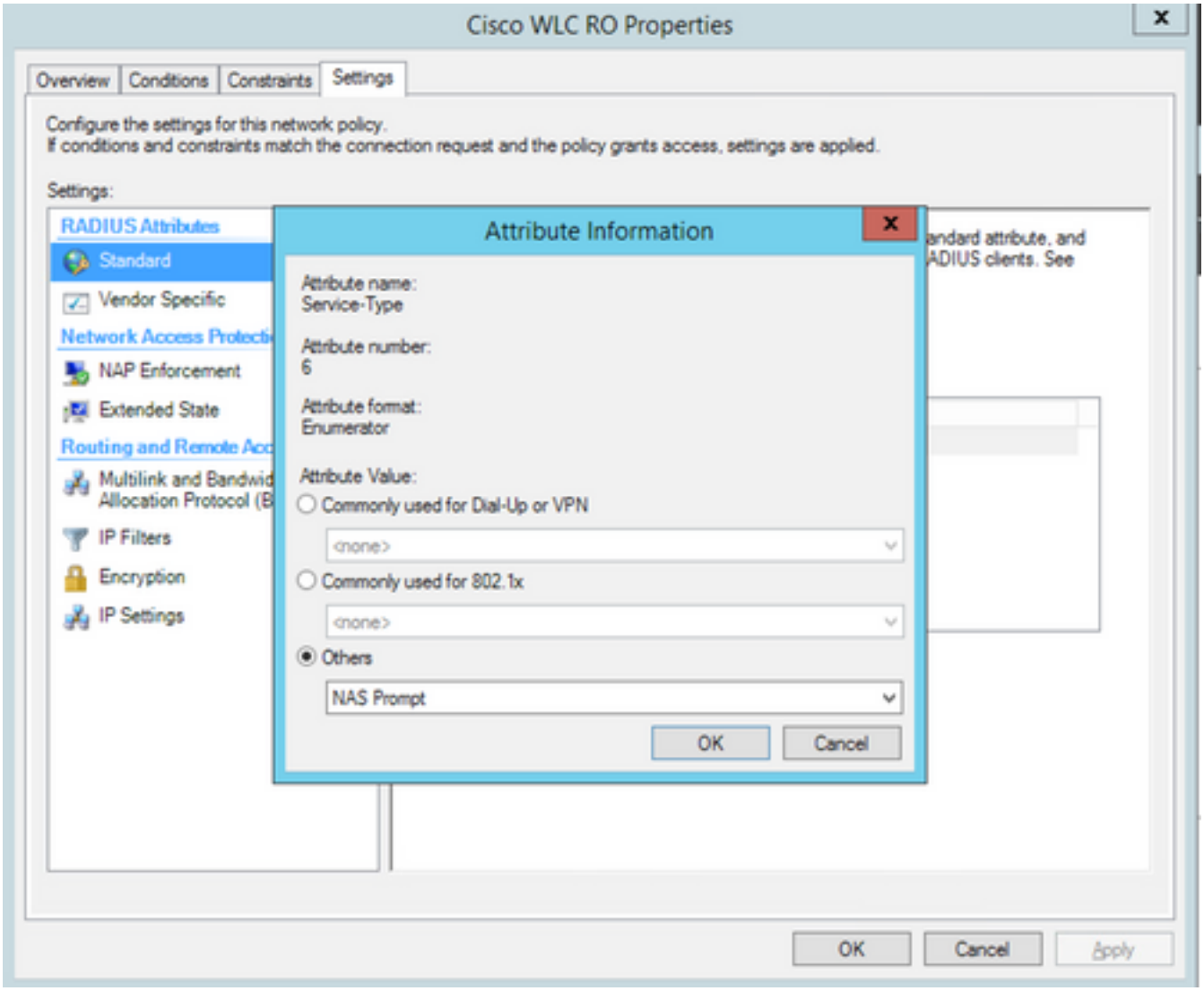


الخطوة 8. تحت صفحة **الإعدادات**، تصفح إلى **خصائص RADIUS > قياسي**. انقر فوق **إضافة** لإضافة سمة جديدة، **نوع الخدمة**. من القائمة المنسدلة، حدد **Administrative** لتوفير وصول كامل للمستخدمين المعينين لهذا النهج. انقر فوق تطبيق لحفظ التغييرات، كما هو موضح في الصورة.



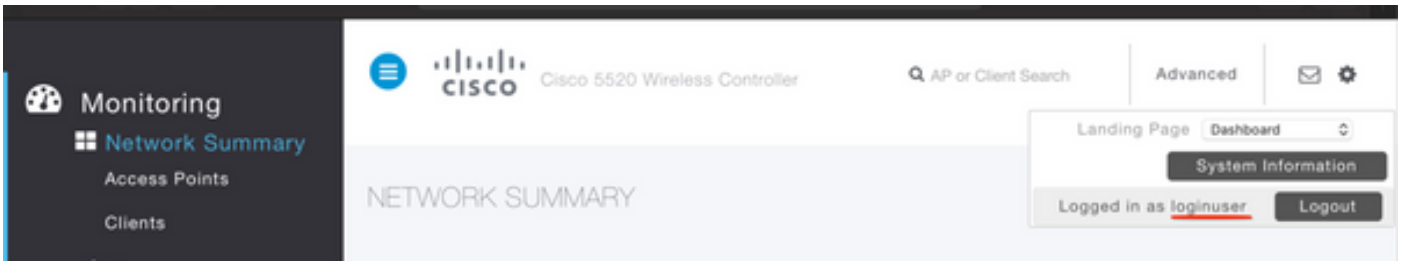
ملاحظة: إذا كنت ترغب في منح وصول للقراءة فقط لمستخدمين محددين، فحدد مطالبة NAS من القائمة المنسدلة. في هذا المثال، يتم إنشاء سياسة أخرى باسم **Cisco WLC RO** لتوفير وصول للقراءة فقط للمستخدمين تحت اسم كائن **مستخدمي المجال**.

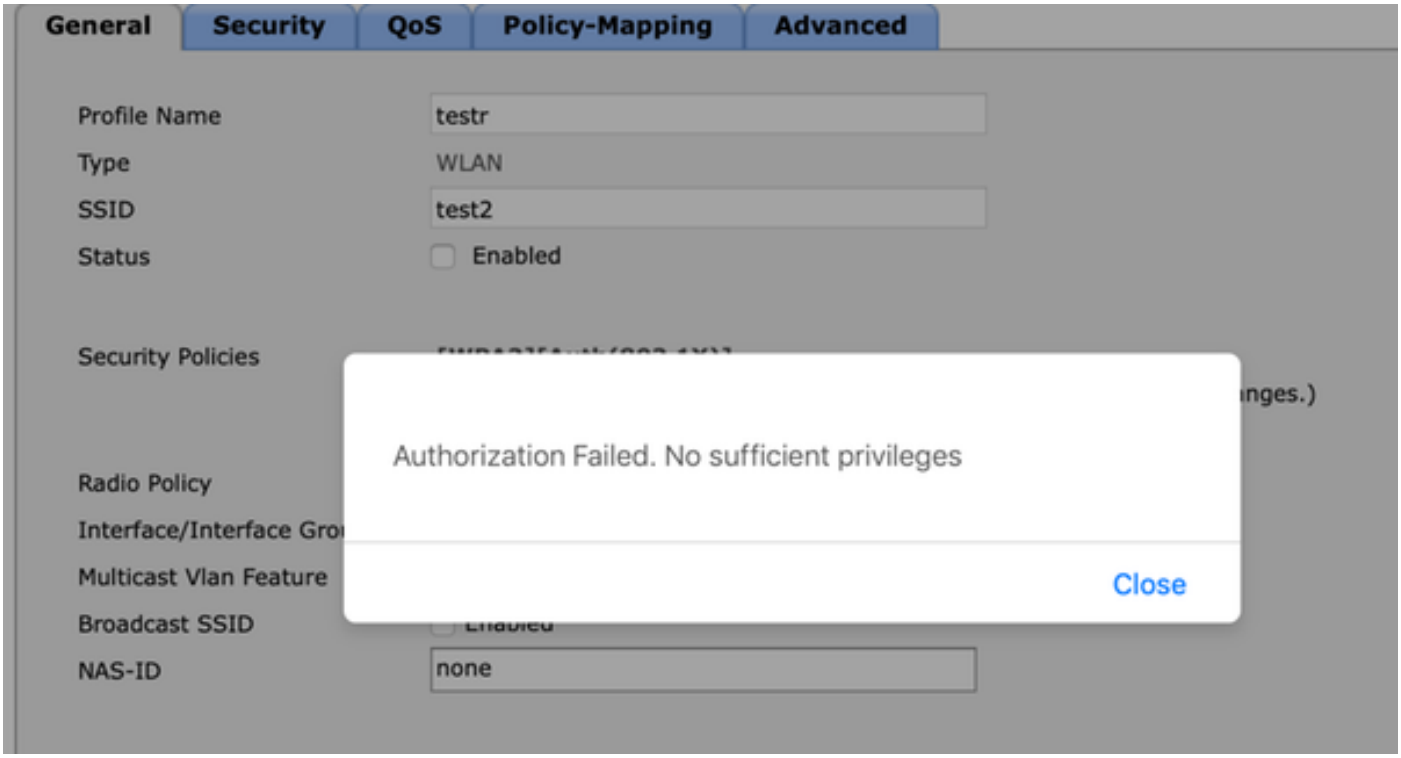

Cisco WLC RO Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
User Groups
WLANLSC\Domain Users
Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Add...
Edit...
Remove
OK
Cancel
Apply



التحقق من الصحة

1. عند إستخدام بيانات اعتماد **مستخدم** السجل، لا يسمح للمستخدم بتكوين أي تغييرات على وحدة التحكم.

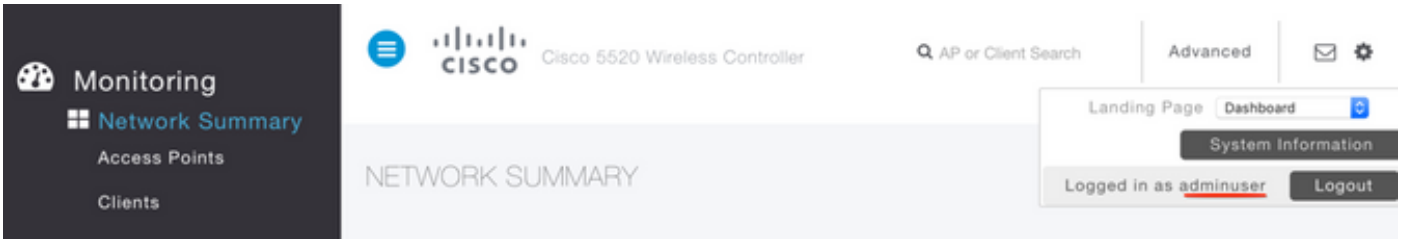




من **debug aaa all enable**، يمكنك أن ترى قيمة سمة نوع الخدمة في إستجابة التفويض هي 7 والتي تطابق موجه NAS.

```
*aaaQueueReader: Dec 07 22:20:14.664: 30:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 14) to 10.106.33.39:1812 from server queue 0, proxy state
30:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:20:14.664: 00000000: 01 0e 00 48 47 f8 f3 5c 58 46 98 ff 8e f8 20 7a
...HG..\XF.....z
*aaaQueueReader: Dec 07 22:20:14.664: 00000010: f6 a1 f1 d1 01 0b 6c 6f 67 69 6e 75 73 65 72 02
......loginuser.
*aaaQueueReader: Dec 07 22:20:14.664: 00000020: 12 c2 34 69 d8 72 fd 0c 85 aa af 5c bd 76 96 eb
..4i.r.....\.v..
*aaaQueueReader: Dec 07 22:20:14.664: 00000030: 60 06 06 00 00 00 07 04 06 0a 6a 24 31 20 0b 43
`.........j$1..C
*aaaQueueReader: Dec 07 22:20:14.664: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
:
:
*radiusTransportThread: Dec 07 22:20:14.668: 30:01:00:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:14
*radiusTransportThread: Dec 07 22:20:14.668: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:20:14.668: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:20:14.668: structureSize.............................304
*radiusTransportThread: Dec 07 22:20:14.668:
protocolUsed.................................0x00000001
*radiusTransportThread: Dec 07 22:20:14.668:
proxyState...................................30:01:00:00:00:00-00:00
*radiusTransportThread: Dec 07 22:20:14.668: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:20:14.668: AVP[01] Service-
Type.............................0x00000007 (7) (4 bytes)
*radiusTransportThread: Dec 07 22:20:14.668: AVP[02]
Class.................................DATA (44 bytes)
```

2. عند إستخدام بيانات اعتماد **المستخدم المسؤول**، يجب أن يتمتع المستخدم بحق الوصول الكامل مع القيمة **نوع الخدمة** 6، والتي تتوافق مع **Administrative**.




```
*aaaQueueReader: Dec 07 22:14:27.439: AuthenticationRequest: 0x7fba240c2f00
*aaaQueueReader: Dec 07 22:14:27.439: Callback.....................................0xa3c13ccb70
*aaaQueueReader: Dec 07 22:14:27.439:
proxyState.....................................2E:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:14:27.439: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:14:27.439: AVP[01] User-Name.............................adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:14:27.439: AVP[04] Nas-Ip-
Address.........................0x0a6a2431 (174728241) (4 bytes)
*aaaQueueReader: Dec 07 22:14:27.439: AVP[05] NAS-Identifier.........................Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:14:27.442: 2e:01:00:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:13
*radiusTransportThread: Dec 07 22:14:27.442: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:14:27.442: structureSize.............................304
*radiusTransportThread: Dec 07 22:14:27.442:
protocolUsed.................................0x00000001
*radiusTransportThread: Dec 07 22:14:27.442:
proxyState.....................................2E:01:00:00:00:00-00:00
*radiusTransportThread: Dec 07 22:14:27.442: AVP[01] Service-
Type.............................0x00000006 (6) (4 bytes)
*radiusTransportThread: Dec 07 22:14:27.442: AVP[02]
Class.....................................DATA (44 bytes)
```

استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء إدارة الوصول إلى WLC عبر NPS وإصلاحها، قم بتشغيل الأمر **debug aaa all enable**.

1. يتم عرض السجلات عند إستخدام بيانات اعتماد غير صحيحة هنا.

```
*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 15) to 10.106.33.39:1812 from server queue 0, proxy state
32:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:36:39.753: 00000000: 01 0f 00 48 b7 e4 16 4d cc 78 05 32 26 4c ec 8d
...H...M.x.2&L..
*aaaQueueReader: Dec 07 22:36:39.753: 00000010: c7 a0 5b 72 01 0b 6c 6f 67 69 6e 75 73 65 72 02
..[r..loginuser.
*aaaQueueReader: Dec 07 22:36:39.753: 00000020: 12 03 a7 37 d4 c0 16 13 fc 73 70 df 1f de e3 e4
...7.....sp.....
*aaaQueueReader: Dec 07 22:36:39.753: 00000030: 32 06 06 00 00 00 07 04 06 0a 6a 24 31 20 0b 43
2.........j$1..C
*aaaQueueReader: Dec 07 22:36:39.753: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 User entry not found in the Local FileDB
for the client.
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Counted 0 AVPs (processed 20
bytes, left 0)
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Access-Reject received from
```

```
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:15
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Did not find the macaddress to be
deleted in the RADIUS cache database
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Returning AAA Error
'Authentication Failed' (-4) for mobile 32:01:00:00:00:00 serverIdx 1
*radiusTransportThread: Dec 07 22:36:39.763: AuthorizationResponse: 0x7fbaebebf860
*radiusTransportThread: Dec 07 22:36:39.763: structureSize.............................136
*radiusTransportThread: Dec 07 22:36:39.763: resultCode.................................-4
*radiusTransportThread: Dec 07 22:36:39.763:
protocolUsed.............................0xffffffff
*radiusTransportThread: Dec 07 22:36:39.763: Packet contains 0 AVPs:
*emWeb: Dec 07 22:36:39.763: Authentication failed for loginuser
```

2. يتم عرض السجلات التي يتم فيها إستخدام نوع الخدمة مع قيمة أخرى غير Administrative (value=6) وأ NAS (value=7) كما يلي. في مثل هذه الحالة، يفشل تسجيل الدخول حتى إذا نجحت المصادقة.

```
*aaaQueueReader: Dec 07 22:46:31.849: AuthenticationRequest: 0x7fba240c56a8
*aaaQueueReader: Dec 07 22:46:31.849: Callback.....................................0xa3c13ccb70
*aaaQueueReader: Dec 07 22:46:31.849: protocolType.................................0x00020001
*aaaQueueReader: Dec 07 22:46:31.849:
proxyState.....................................39:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:46:31.849: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:46:31.849: AVP[01] User-Name.................................adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[02] User-Password.............................[...]
*aaaQueueReader: Dec 07 22:46:31.849: AVP[03] Service-
Type............................0x00000007 (7) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[04] Nas-Ip-
Address............................0x0a6a2431 (174728241) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[05] NAS-Identifier............................Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:46:31.853: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:46:31.853: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:46:31.853: structureSize.............................304
*radiusTransportThread: Dec 07 22:46:31.853: resultCode.................................0
*radiusTransportThread: Dec 07 22:46:31.853:
protocolUsed.................................0x00000001
*radiusTransportThread: Dec 07 22:46:31.853: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:46:31.853: AVP[01] Service-
Type............................0x00000001 (1) (4 bytes)
*radiusTransportThread: Dec 07 22:46:31.853: AVP[02]
Class.....................................DATA (44 bytes)
*emWeb: Dec 07 22:46:31.853: Authentication succeeded for adminuser
```

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).