المصادقة المستندة إلى سمات ISE و LDAP

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين محرك خدمات الهوية من Cisco (ISE) واستخدام سمات كائنات بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP) للمصادقة على الأجهزة وتخويلها بشكل ديناميكي.

ملاحظة: هذا المستند صالح للإعدادات التي تستخدم LDAP كمصدر هوية خارجي لمصادقة ISE والتخويل.

ساهم به إيمانويل كانو وماوريسيو راموس مهندس الخدمات الاحترافية من سيسكو.

قام بتحرير هذا الدرس مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بمجموعات سياسات ISE والمصادقة وسياسات التخويل
- تجاوز مصادقة MAC (MAB)
- معرفة أساسية ببروتوكول RADIUS
- معرفة أساسية بخادم Windows

المكونات المستخدمة

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

- Cisco ISE، الإصدار 2.4 تصحيح 11
- Microsoft Windows Server، الإصدار 2012 R2 x64
- محول Catalyst 3650-24PD من Cisco، الإصدار 03.07.05.E (15.2(3)E5)
- جهاز Microsoft Windows 7

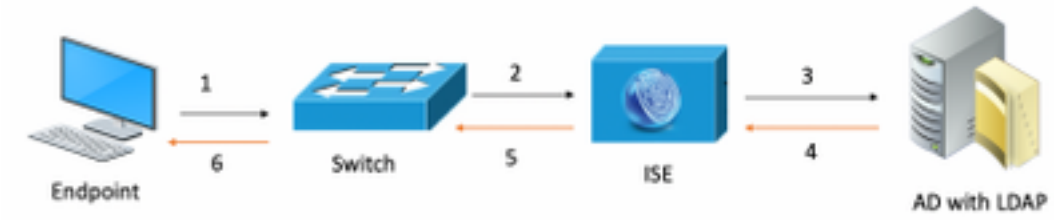
ملاحظة: تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

يصف هذا القسم كيفية تكوين أجهزة الشبكة، والتكامل بين ISE و LDAP، وأخيرا لتكوين سمات LDAP التي سيتم إستخدامها في نهج تخويل ISE.

الرسم التخطيطي للشبكة

يوضح هذا الصورة مخطط الشبكة الذي يتم إستخدامه:



وفيما يلي تدفق حركة المرور، كما هو موضح في الرسم التخطيطي للشبكة:

1. يقوم المستخدم بتوصيل الكمبيوتر/الكمبيوتر المحمول الخاص به بمنفذ المحول المخصص.
2. يرسل المفتاح طلب وصول RADIUS لذلك المستخدم إلى ISE
3. عندما يستلم ISE المعلومات يستعلم خادم LDAP عن المستخدم المحدد الذي تم تسجيله، والذي يحتوي على السمات التي سيتم إستخدامها في شروط نهج التخويل.
4. ما إن يستلم ال ise السمة (المفتاح ميناء، مفتاح إسم، وجهاز {upper}mac address) وه يقارن المعلومة يزود بالمفتاح.
5. إذا كانت معلومات السمات المقدمة من المحول هي نفسها المعلومات المقدمة من قبل LDAP، سيقوم ISE بإرسال قبول وصول RADIUS باستخدام الأذونات التي تم تكوينها على ملف تعريف التخويل.

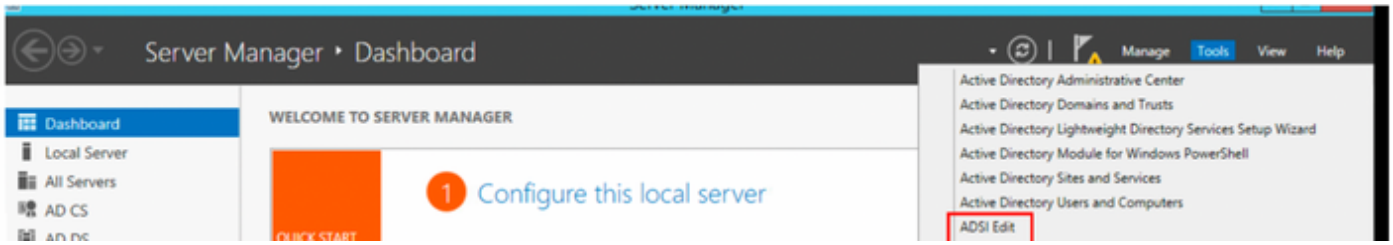
التكوينات

استعملت هذا قسم in order to شكلت ال LDAP، مفتاح و ال ISE.

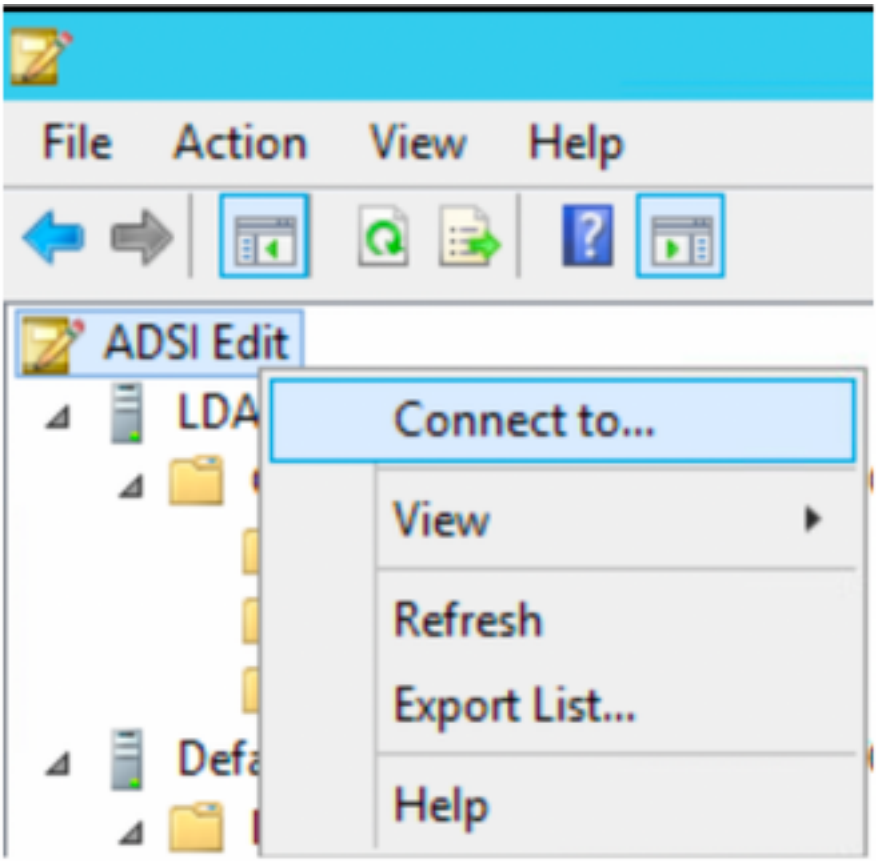
التكوين LDAP

أكمل الخطوات التالية لتكوين خادم LDAP:

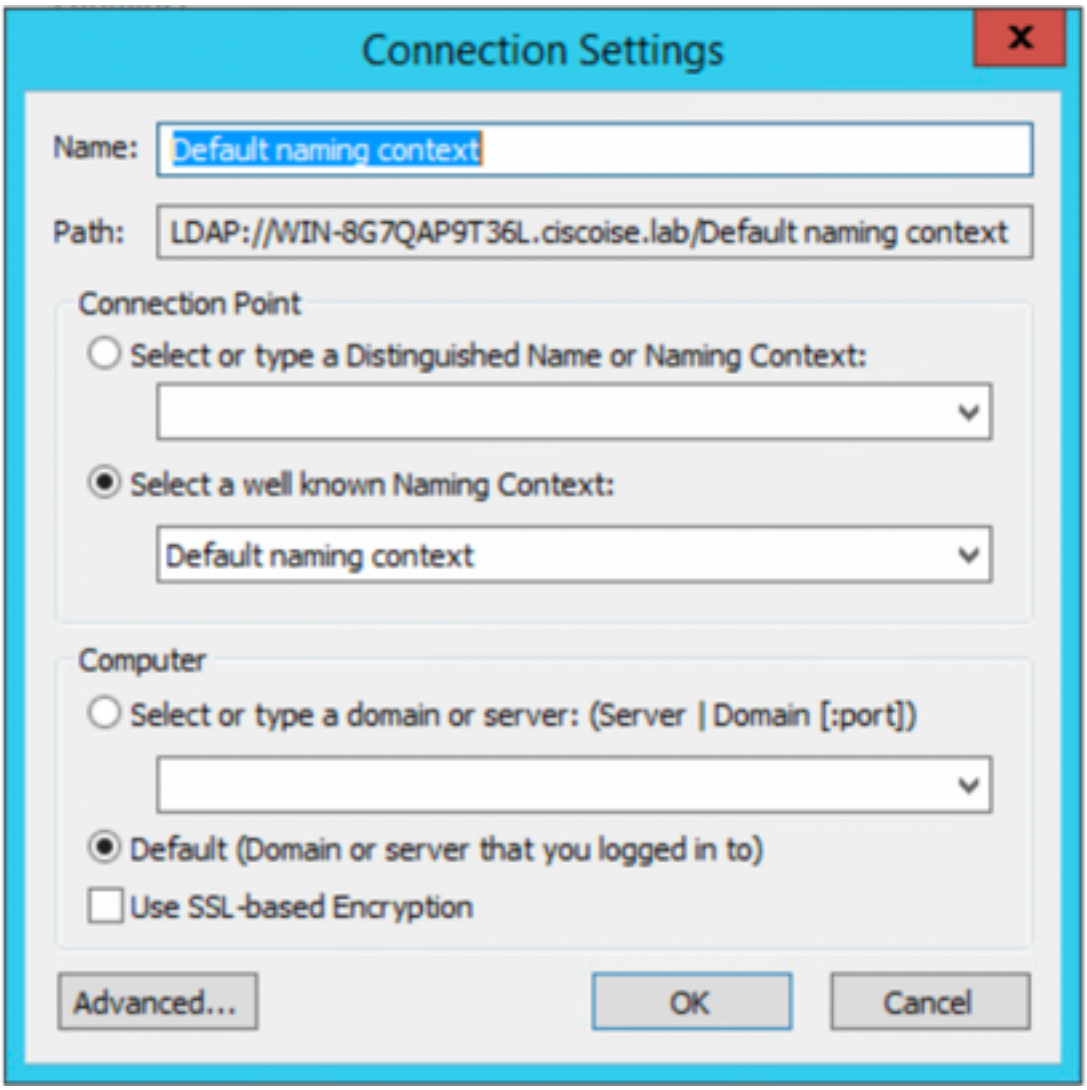
1. انتقل إلى **مدير الخادم > لوحة المعلومات > أدوات > تحرير ADSI**



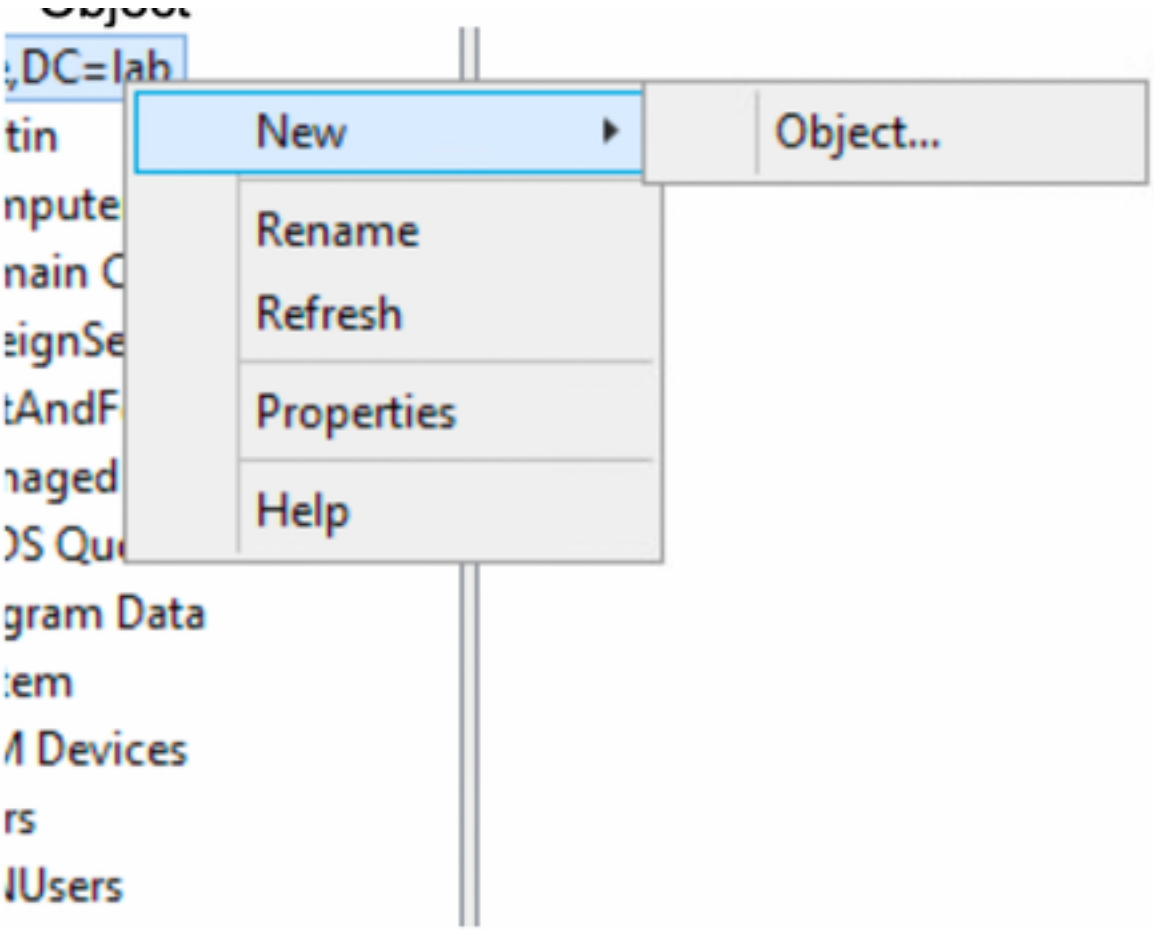
2. انقر بزر الماوس الأيمن على رمز تحرير ADSI وحدد **الاتصال ب...**



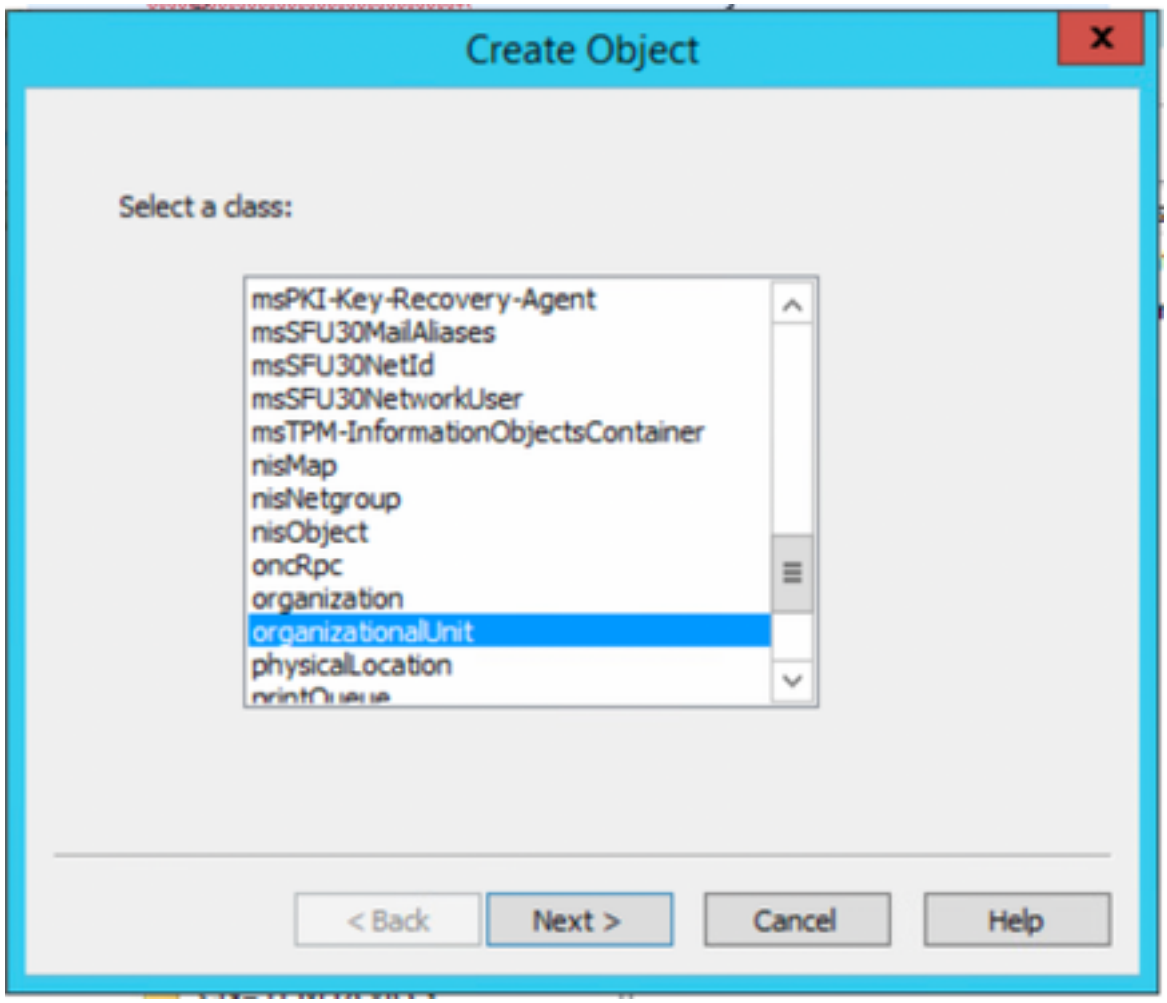
3. تحت إعدادات التوصيل قم بتعريف اسم وحدد الزر **موافق** لبدء الاتصال.



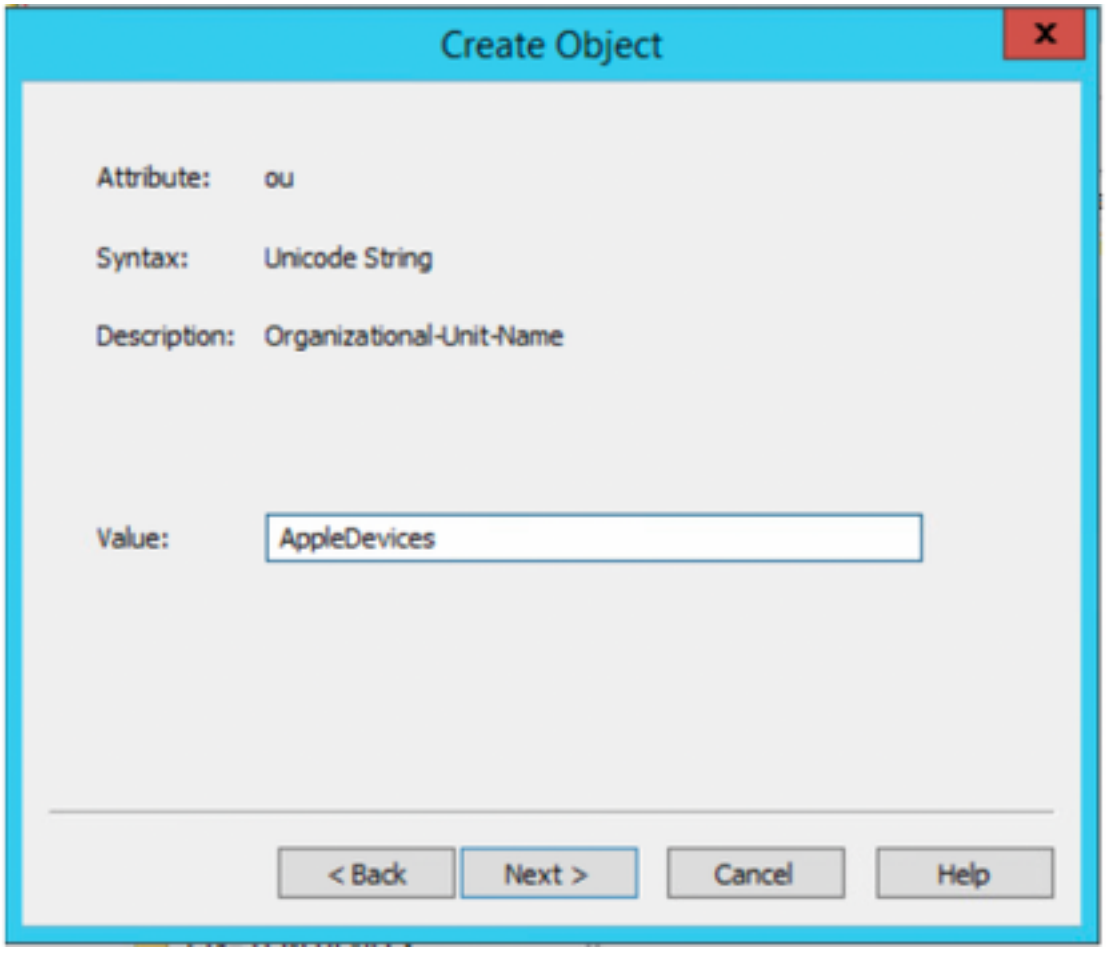
4. تحت نفس قائمة تحرير ADSI انقر بزر الماوس الأيمن في اتصال DC (DC=CiscoDemo، DC=lab)، حدد **جديد**، ثم حدد خيار **كائن**



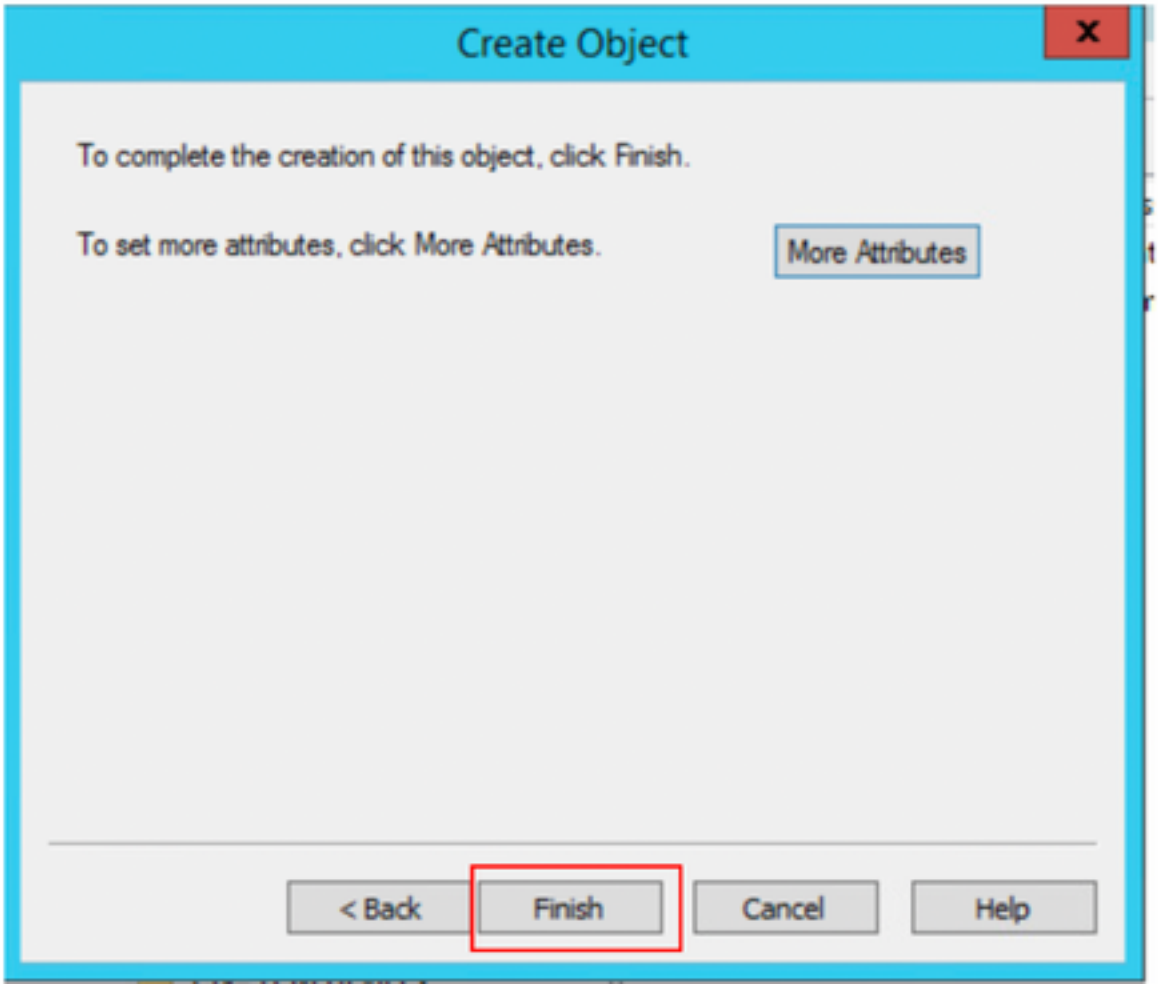
5. حدد خيار **الوحدة التنظيمية** كائن جديد وحدد **التالي**.



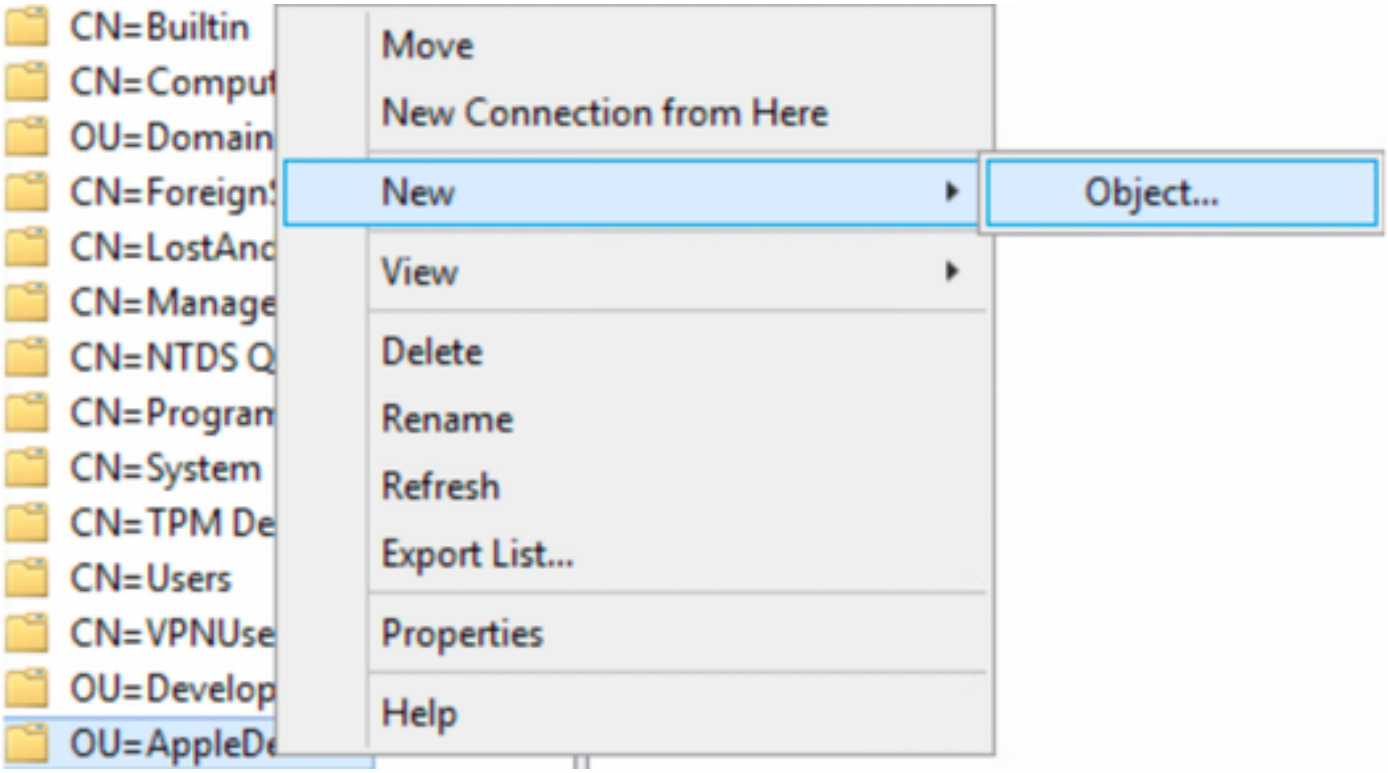
6. تحديد اسم للوحدة التنظيمية الجديدة وتحديد **التالي**



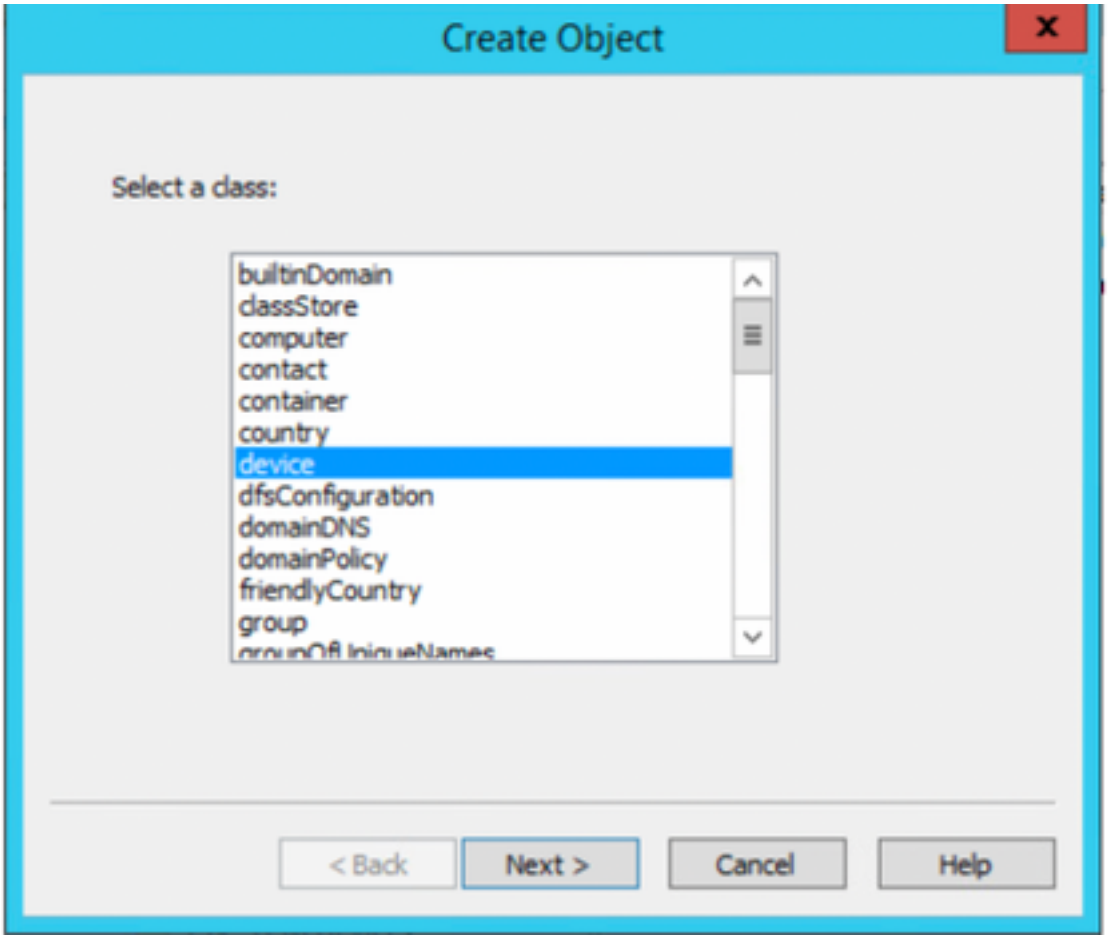
7. حدد **إنهاء** لإنشاء الوحدة التنظيمية الجديدة



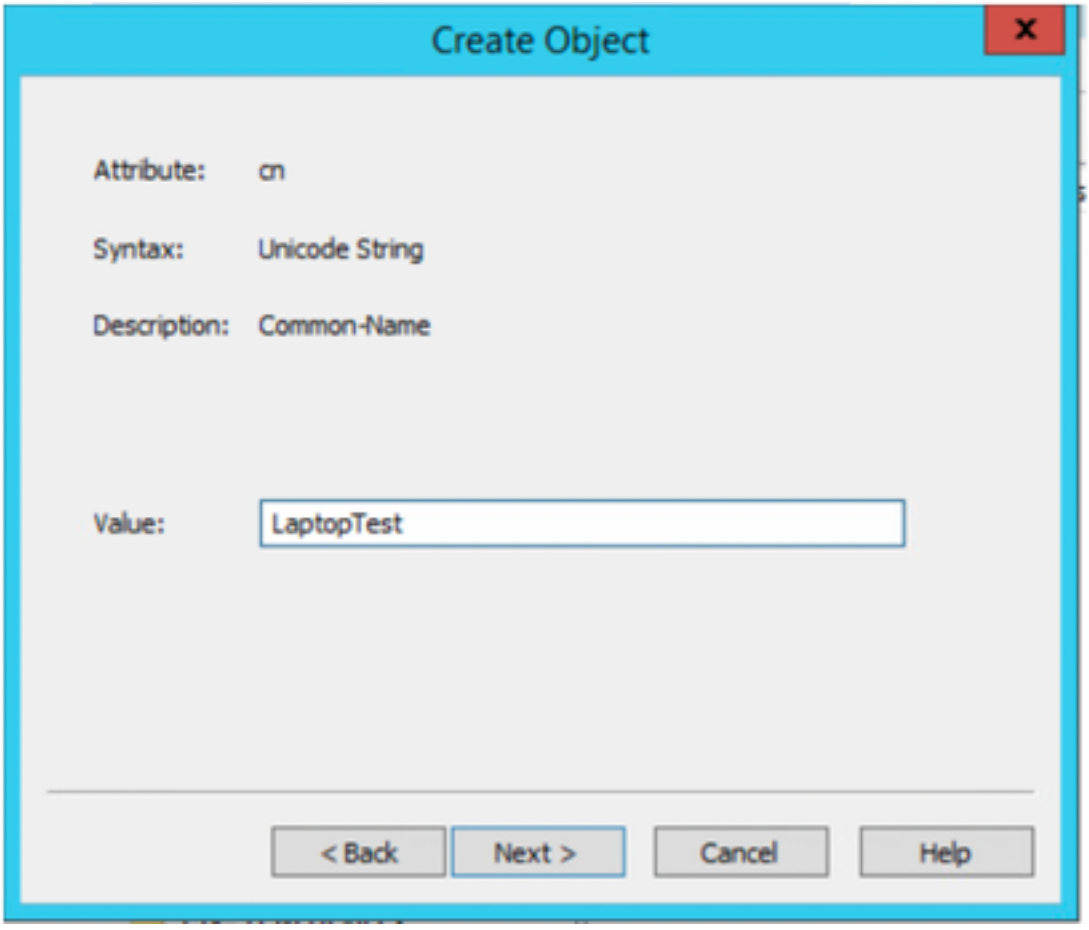
8. انقر بزر الماوس الأيمن فوق الوحدة التنظيمية التي تم إنشاؤها للتو وحدد **جديد > كائن**



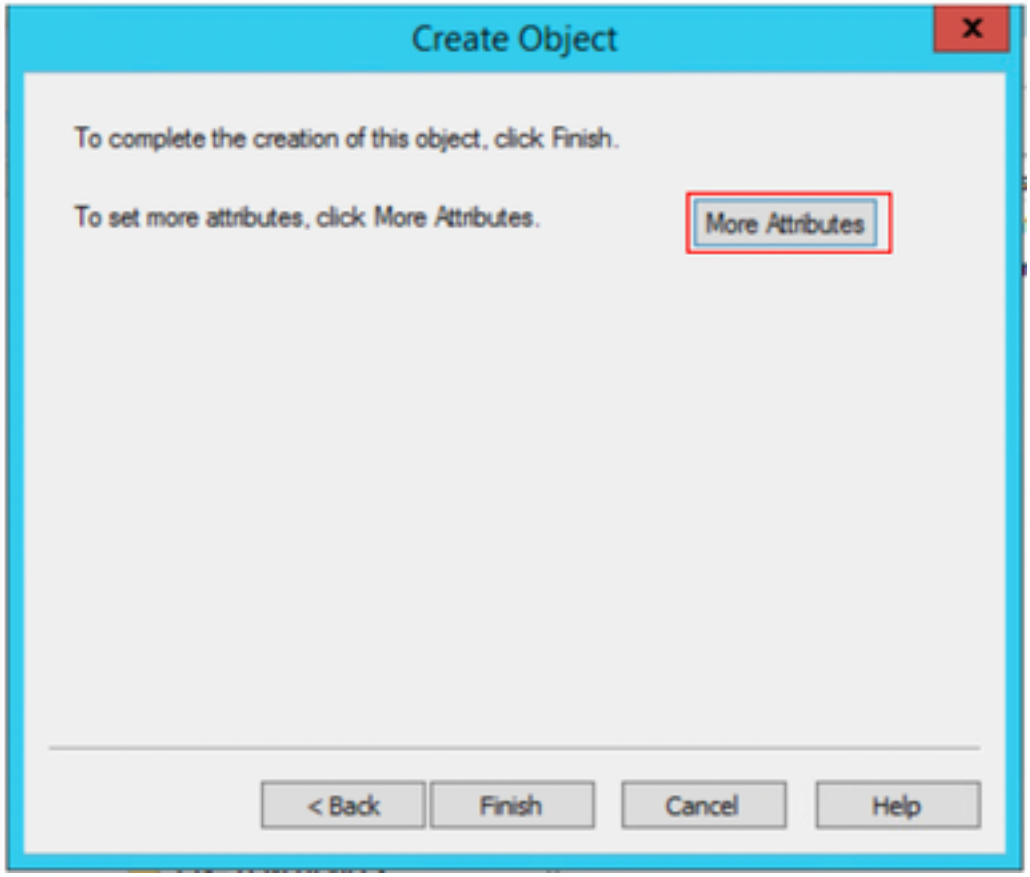
9.حدد **الوجهة** كفئة كائن وحدد **التالي**



10.حدد اسما في حقل القيمة وحدد **التالي**

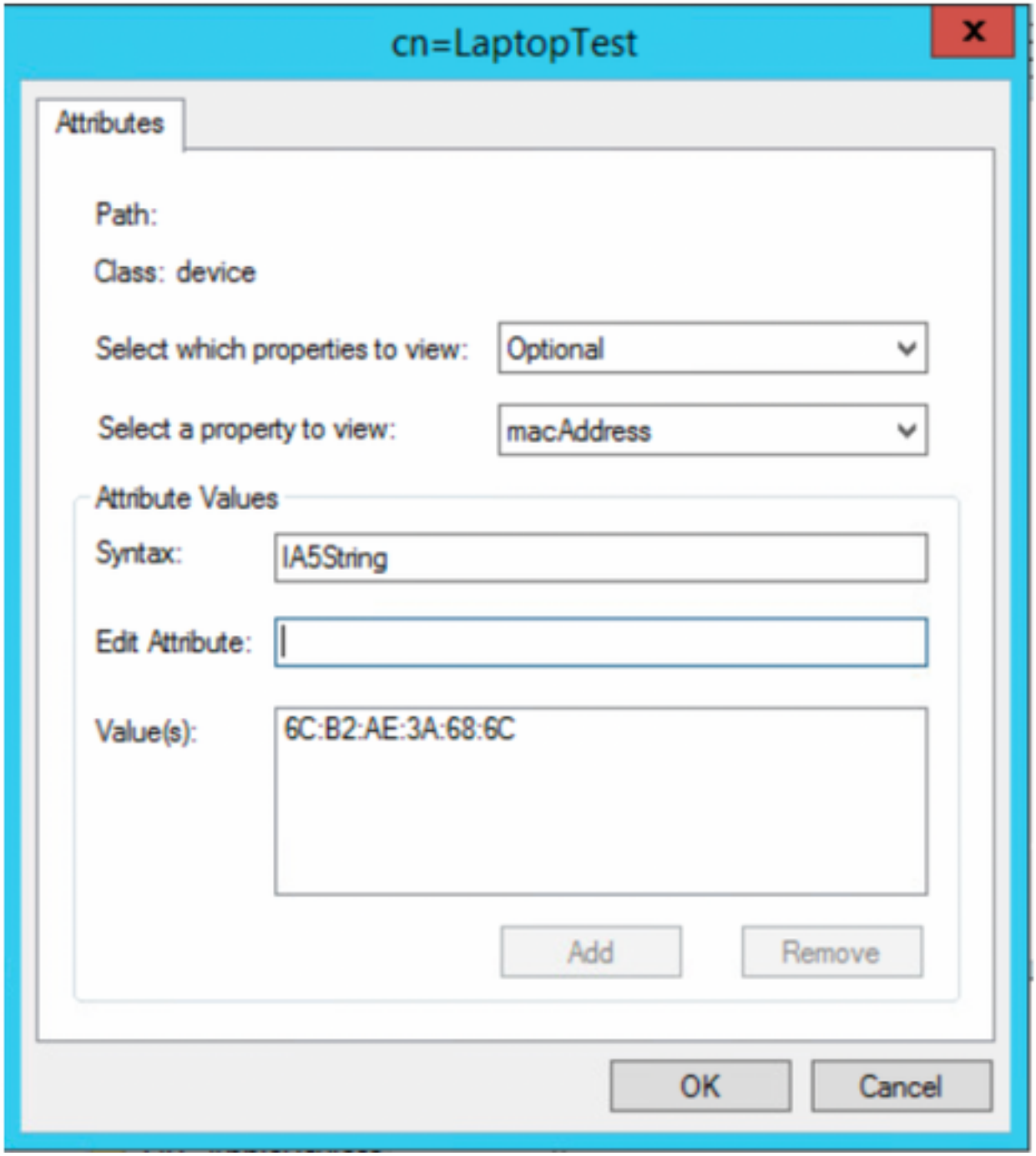


11. حدد الخيار **المزيد من السمات**



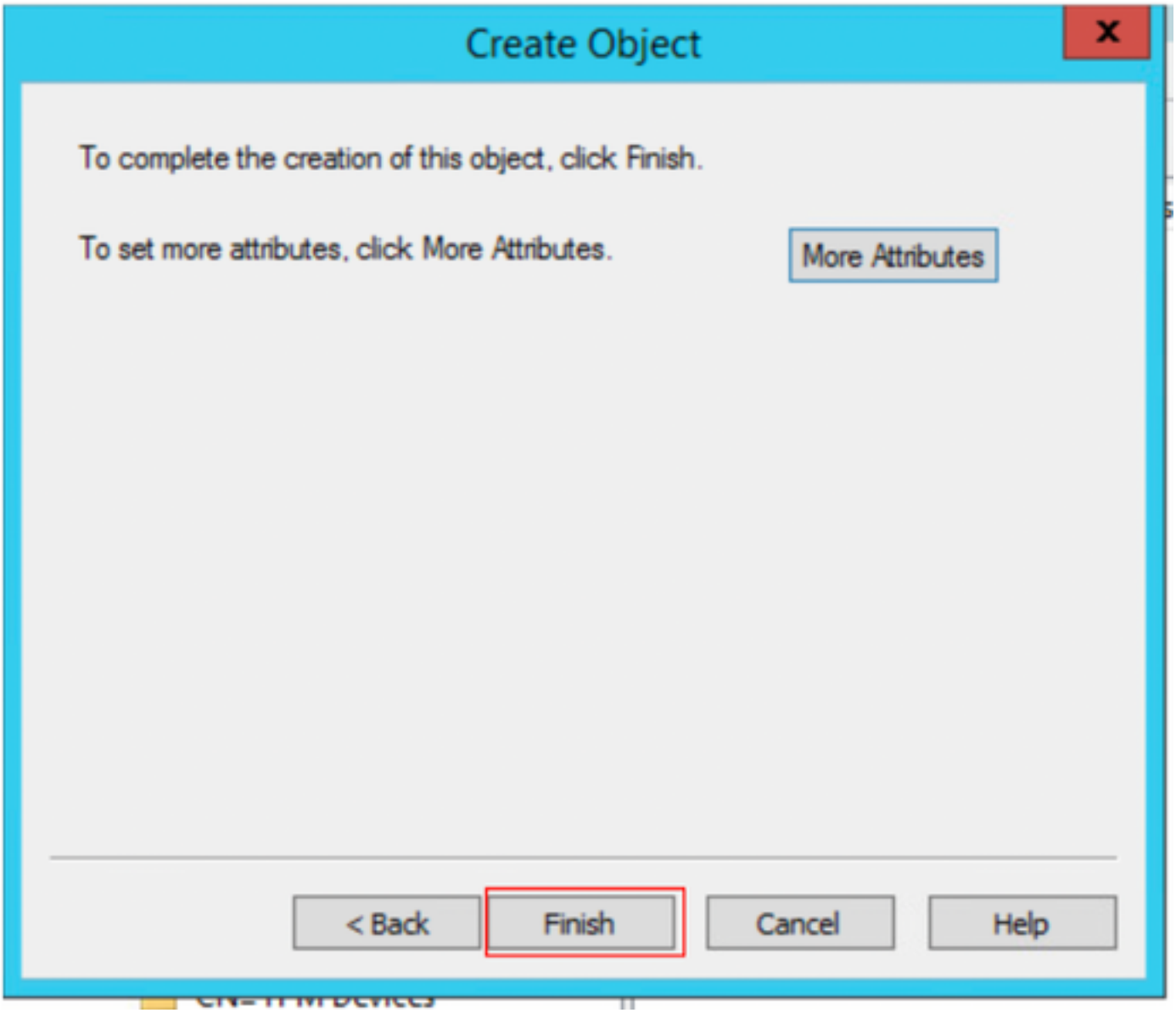
11. للحصول على القائمة المنسدلة، **حدد خاصية العرض**، حدد خيار **MacAddress**، ثم قم بتعريف عنوان Mac لنقطة النهاية الذي سيتم مصادقته ضمن حقل **تحرير السمة** وحدد **إضافة** زر لحفظ عنوان MAC للجهاز.

ملاحظة: أستخدم فواصل بين الأنظمة الثمانية لعناوين MAC.

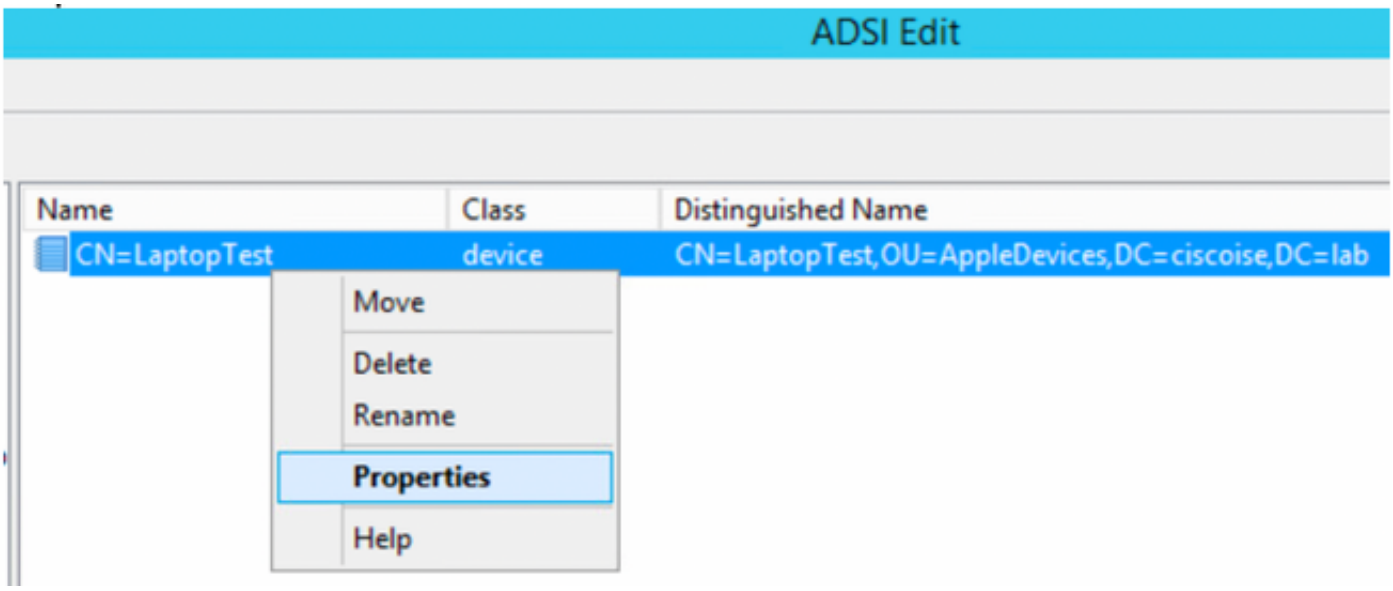


12. حدد **موافق** لحفظ المعلومات ومتابعة تكوين كائن الجهاز

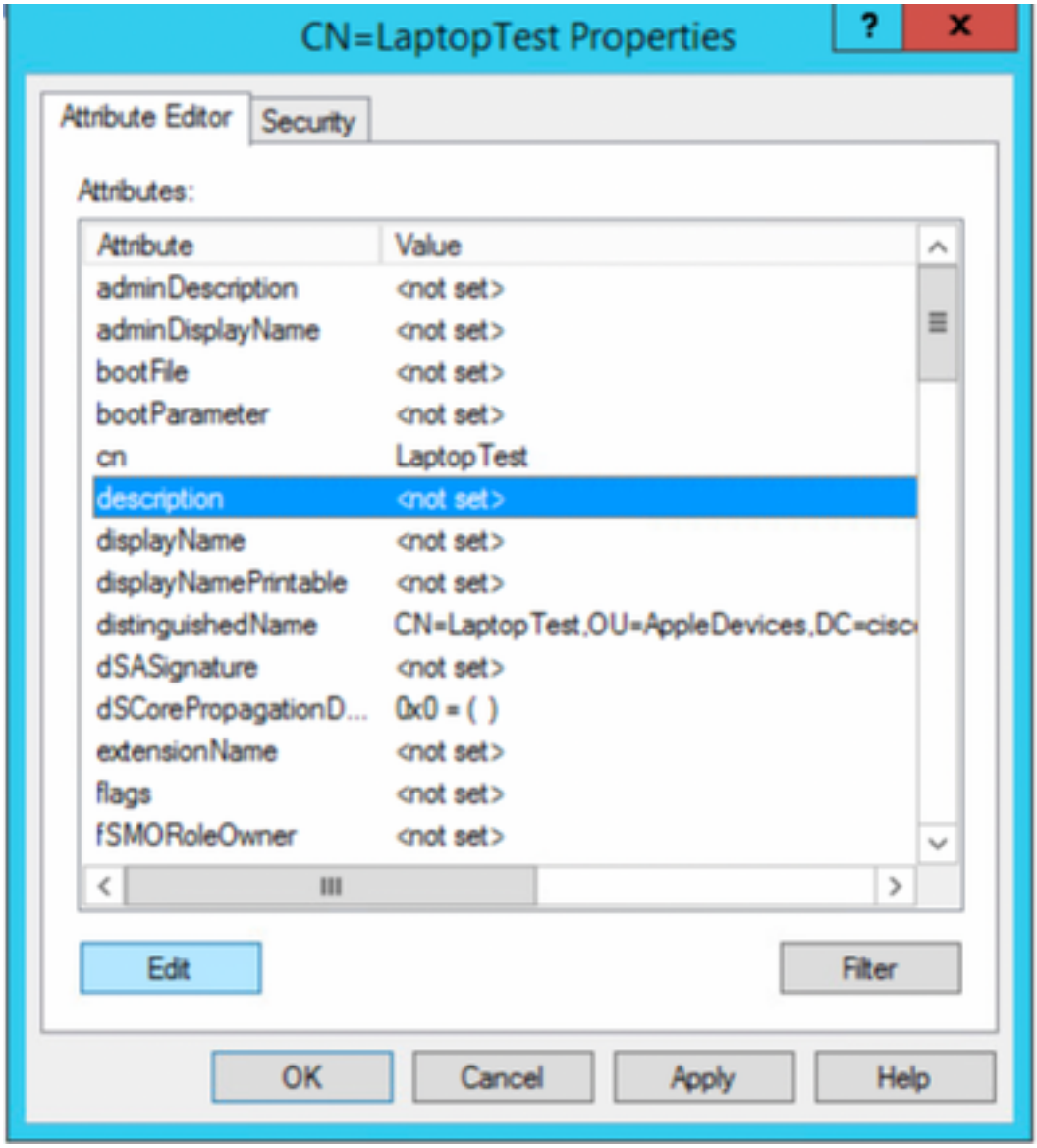
13. حدد **إنهاء** لإنشاء كائن الجهاز الجديد



14. انقر بزر الماوس الأيمن على كائن الجهاز وحدد **خصائص** الخيار

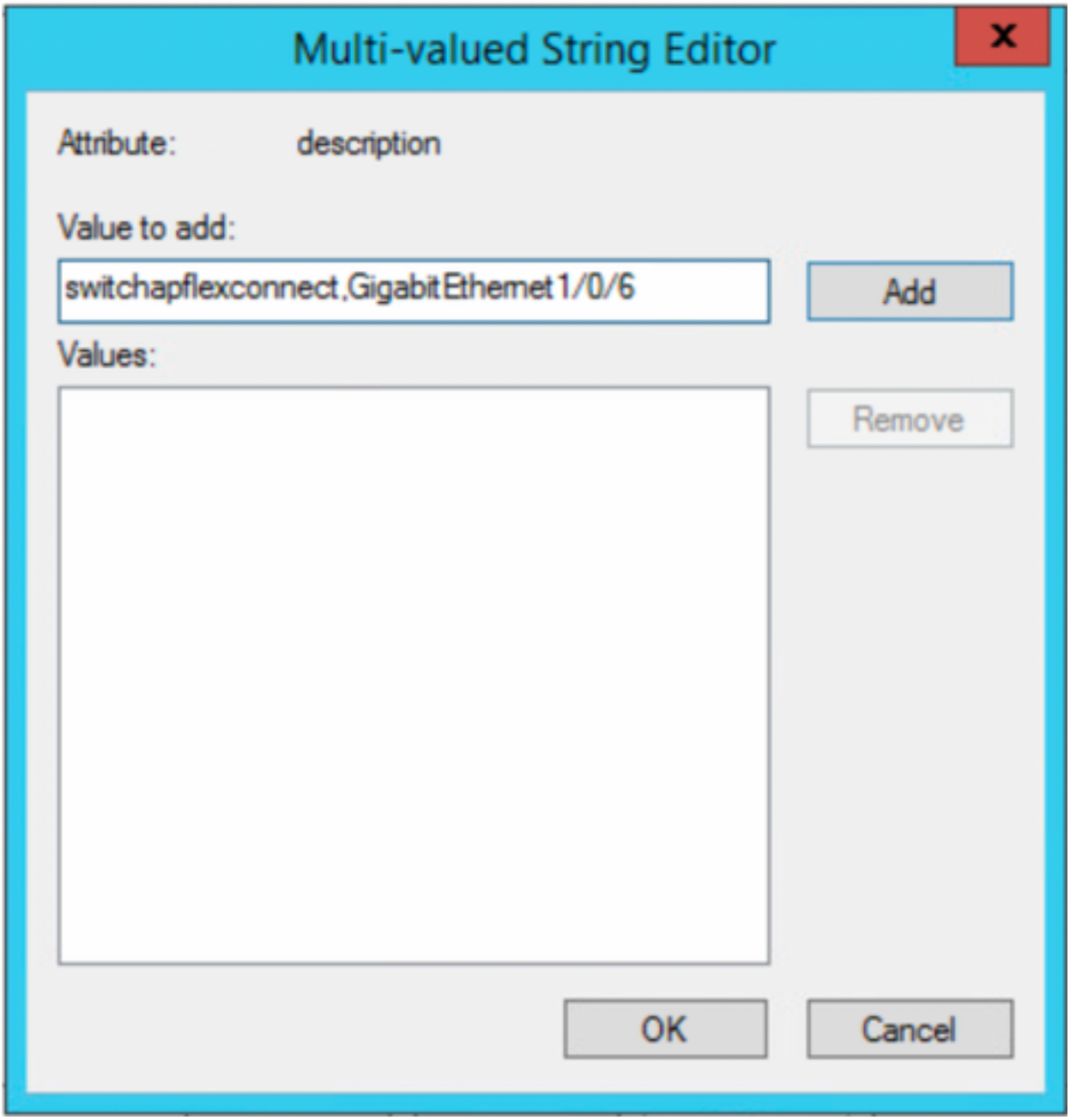


15. حدد **وصف** الخيار وحدد **تحرير** من أجل تحديد اسم المحول ومنفذ المحول حيث سيتم



توصيل الجهاز.

16. حدد اسم المحول ومنفذ المحول، يرجى التأكد من إستخدام فاصلة لفصل كل قيمة. حدد **إضافة** ثم **موافق** لحفظ المعلومات.



- **SwitchapflexConnect وه اسم المحول.**
- **GigabitEthernet1/0/6 وه المحول-port الذي يتم توصيل نقطة النهاية به.**

ملاحظة: من الممكن إستخدام نصوص تنفيذية إضافة خصائص إلى حقل معين، على أي حال، لهذا المثال نحن نقوم بتعريف القيم يدوياً

ملاحظة: تكون السمة AD حساسة لحالة الأحرف، إذا كنت تستخدم جميع عناوين MAC في حالة الأحرف الأقل ISE التي يتم تحويلها إلى حالة عليا أثناء استعلام LDAP. لتجنب هذا السلوك، قم بتعطيل البحث عن مضيف العملية ضمن البروتوكولات المسموح بها. يمكن العثور على التفاصيل في هذا الارتباط: https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

تكوين المبدّل

يصف ما يلي تكوين اتصال 802.1x بين ISE والمحول.

```
aaa new-model ! aaa group server radius ISE server name ISE deadtime 15 ! aaa authentication
dot1x default group ISE aaa authorization network default group ISE aaa accounting update
newinfo aaa accounting dot1x default start-stop group ISE ! aaa server radius dynamic-author
client 10.81.127.109 server-key XXXXabc ! aaa session-id common switch 1 provision ws-c3650-24pd
```

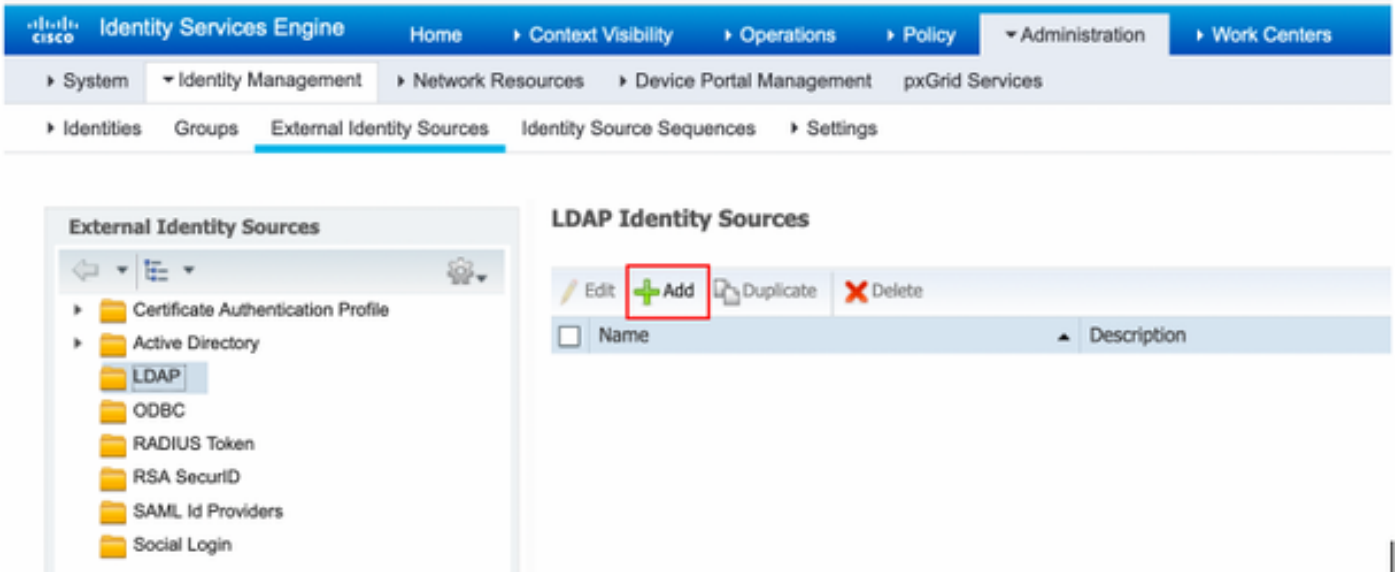
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access authentication event fail action next-method authentication event server
dead action authorize vlan 127 authentication event server alive action reinitialize
authentication host-mode multi-domain authentication open authentication order dot1x mab
authentication priority dot1x mab authentication port-control auto authentication periodic
authentication timer reauthenticate server authentication timer inactivity server dynamic
authentication violation restrict mab dot1x pae authenticator dot1x timeout tx-period 10
spanning-tree portfast ! radius server ISE address ipv4 10.81.127.109 auth-port 1812 acct-port
1813 automate-tester username radiustest idle-time 5 key XXXXabc !
```

ملاحظة: قد يلزم تعديل تكوين الواجهة والتكوين العام في بيئتك

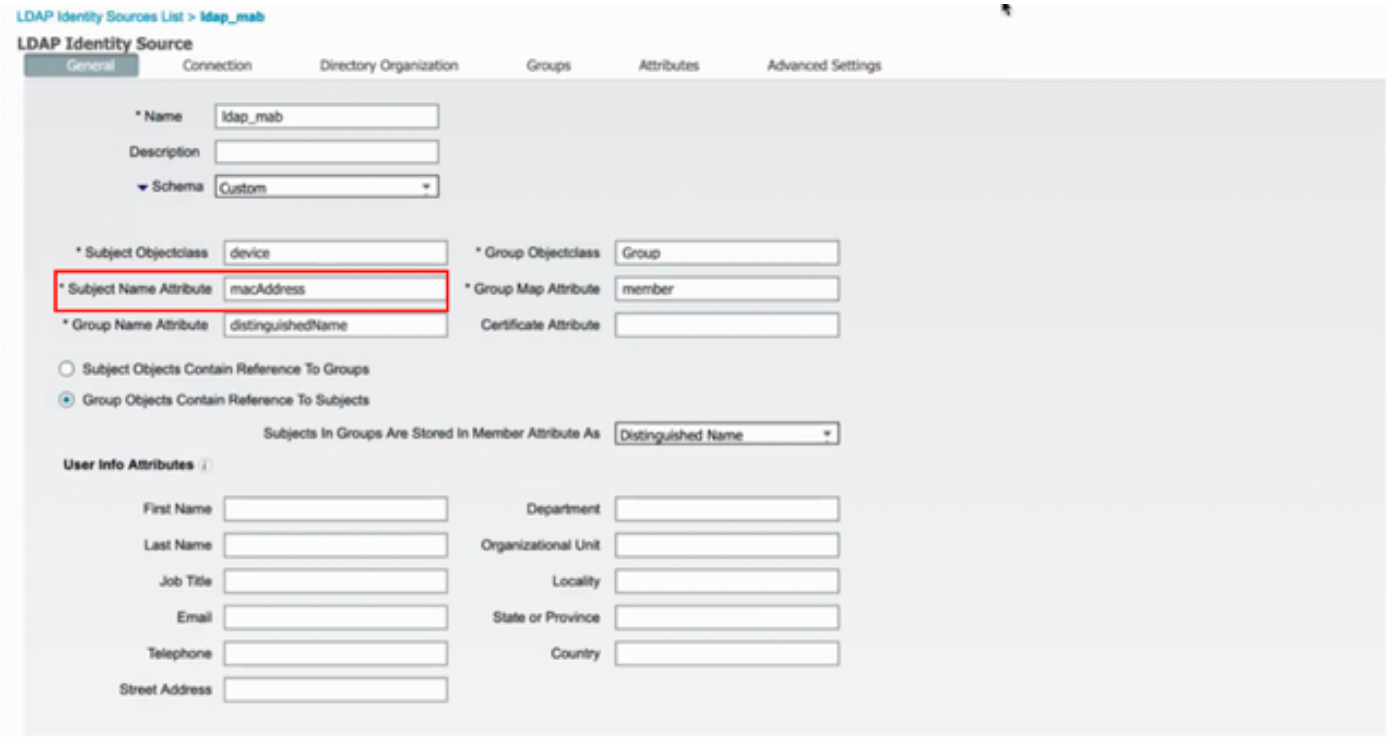
تكوين ISE

يصف التالي التكوين على ISE للحصول على السمات من خادم LDAP وتكوين سياسات ISE.

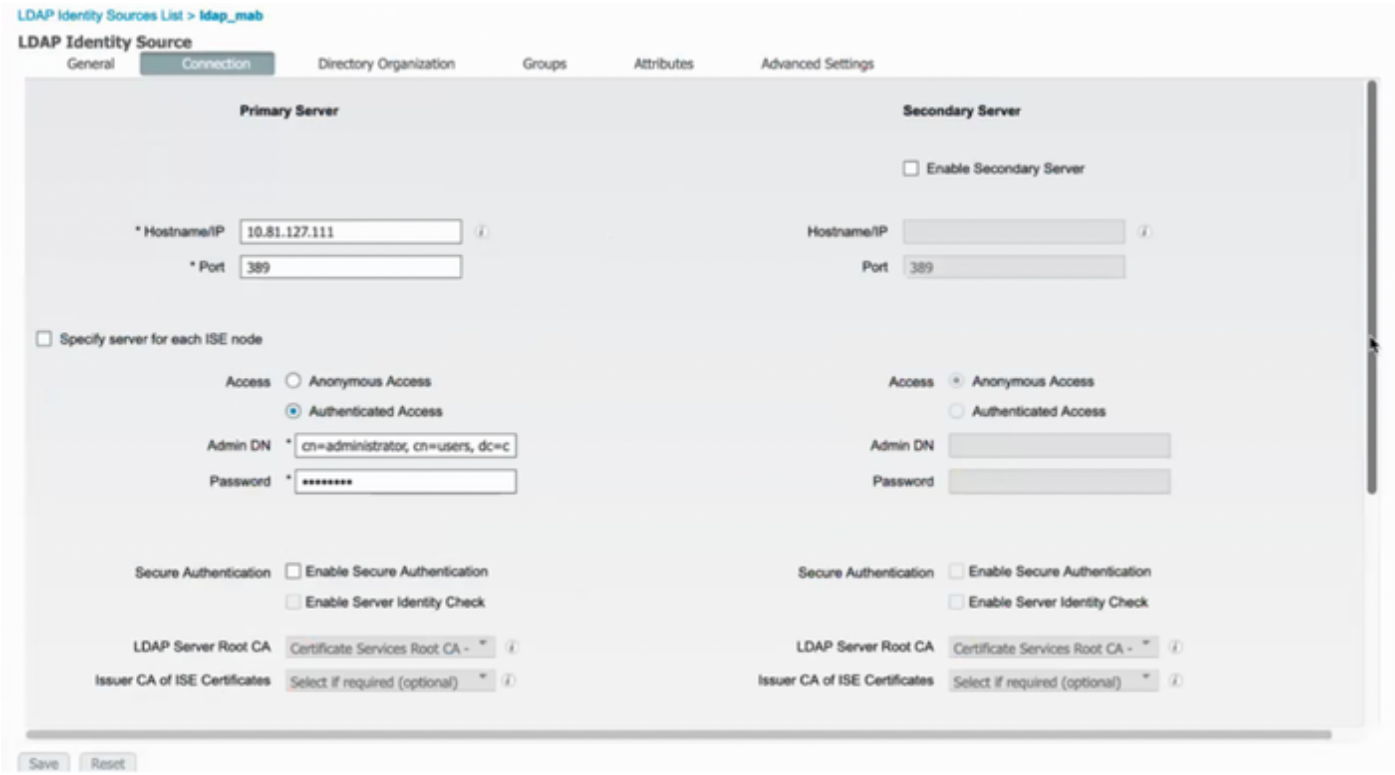
1. على ISE، انتقل إلى **إدارة->إدارة الهوية->مصادر الهوية الخارجية** وحدد مجلد **LDAP** وانقر على **إضافة** لإنشاء اتصال جديد مع LDAP



2.تحت علامة التبويب **عام** قم بتعريف اسم وحدد عنوان MAC كسمة اسم الموضوع

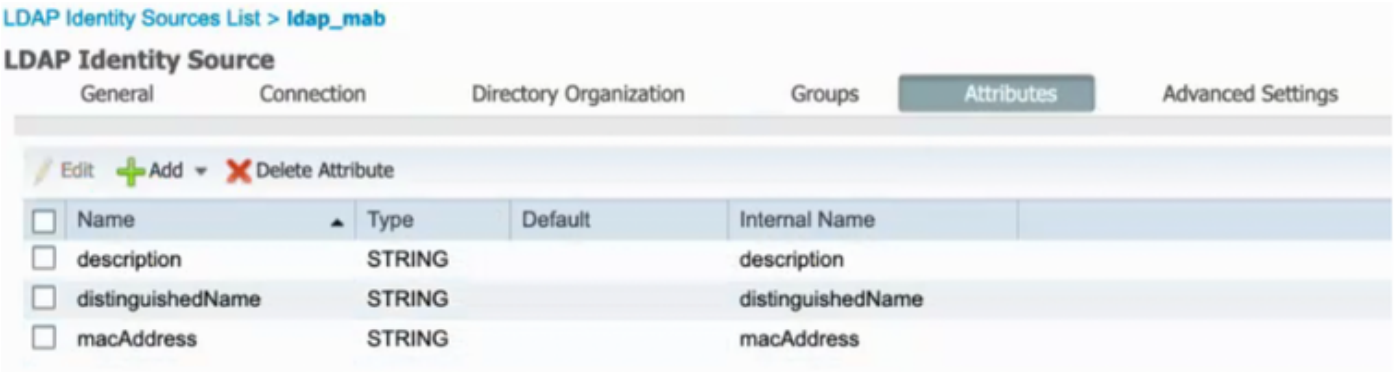


3. تحت **علامة** تبويب **التوصيل**، قم بتكوين عناوين IP و admin DN وكلمة المرور من خادم LDAP للحصول على اتصال ناجح.

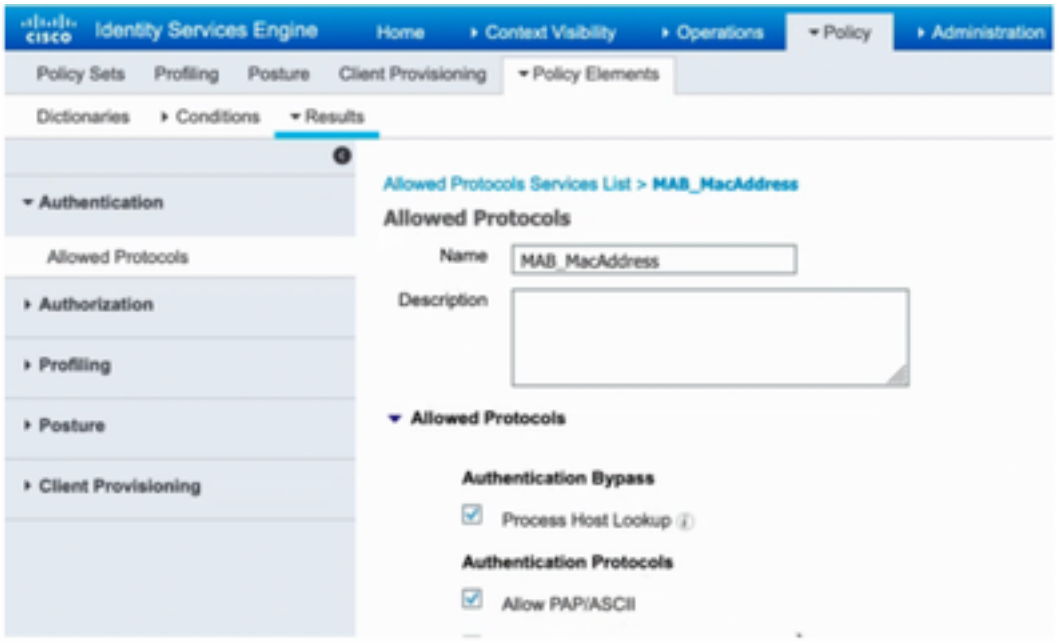


ملاحظة: المنفذ 389 هو المنفذ الافتراضي المستخدم.

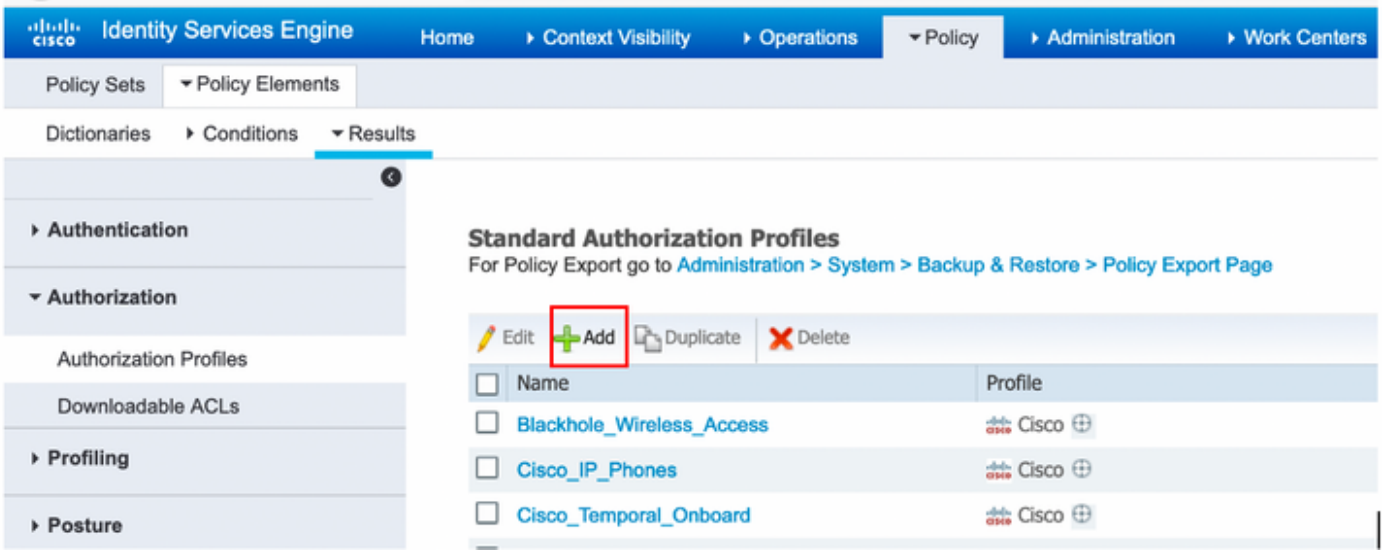
4. تحت علامة التبويب **سمات**، قم بتحديد سمات MacAddress والوصف، سيتم استخدام هذه السمات في نهج التخويل

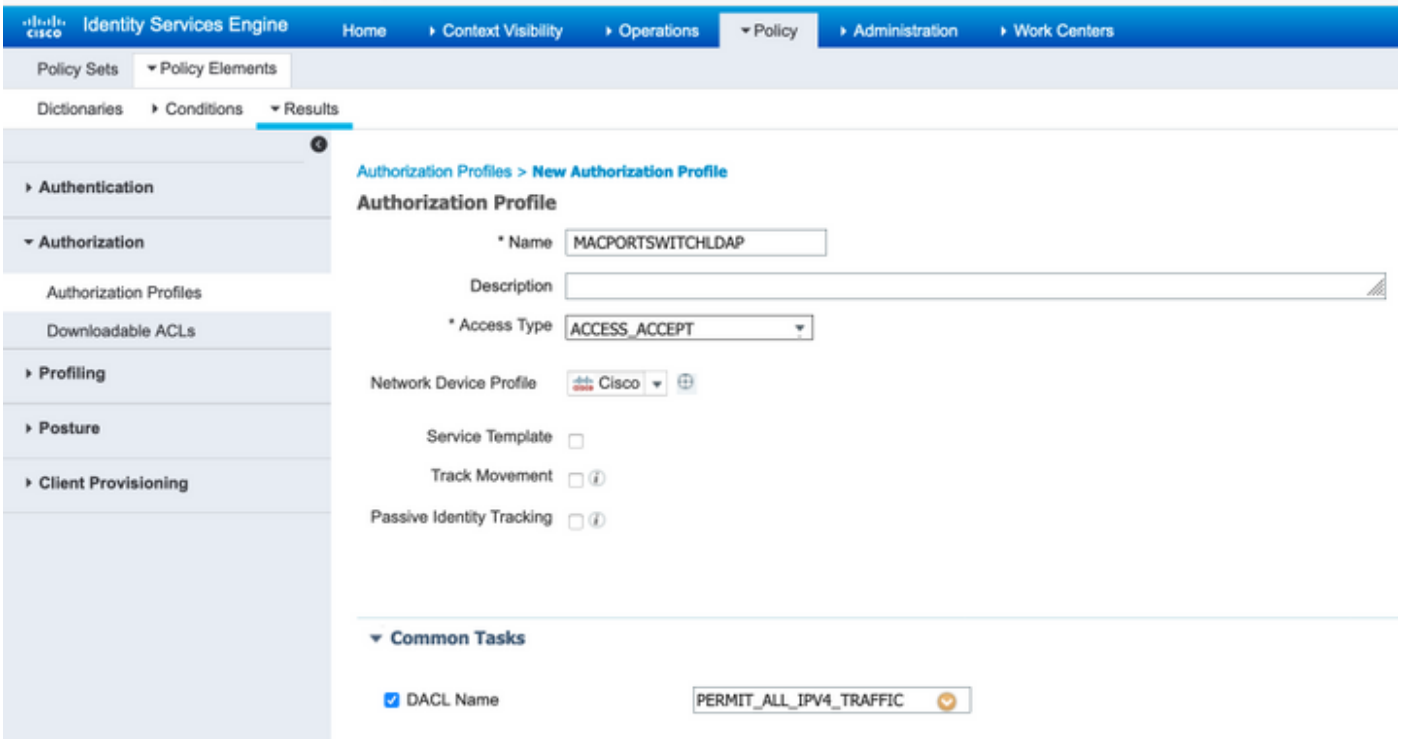


5. من أجل إنشاء بروتوكول مسموح به انتقل إلى **السياسة->عناصر السياسة->النتائج->المصادقة->البروتوكولات المسموح بها.** قم بتحديد البحث عن مضيف العملية ثم قم بالسماح ب PAP/ASCII كالبروتوكولات الوحيدة المسموح بها. أخيرا حدد **حفظ**

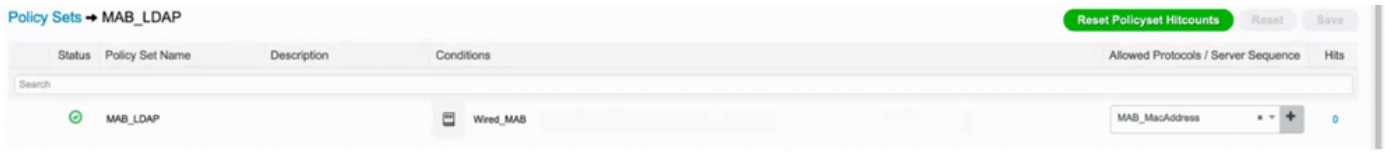


6. من أجل إنشاء ملف تعريف تخويل، انتقل إلى **Policy->Policy Elements->Results->Authorization->Authorization Profile. حدد إضافة** وقم بتعريف الأذون التي سيتم تعيينها إلى نقطة النهاية.

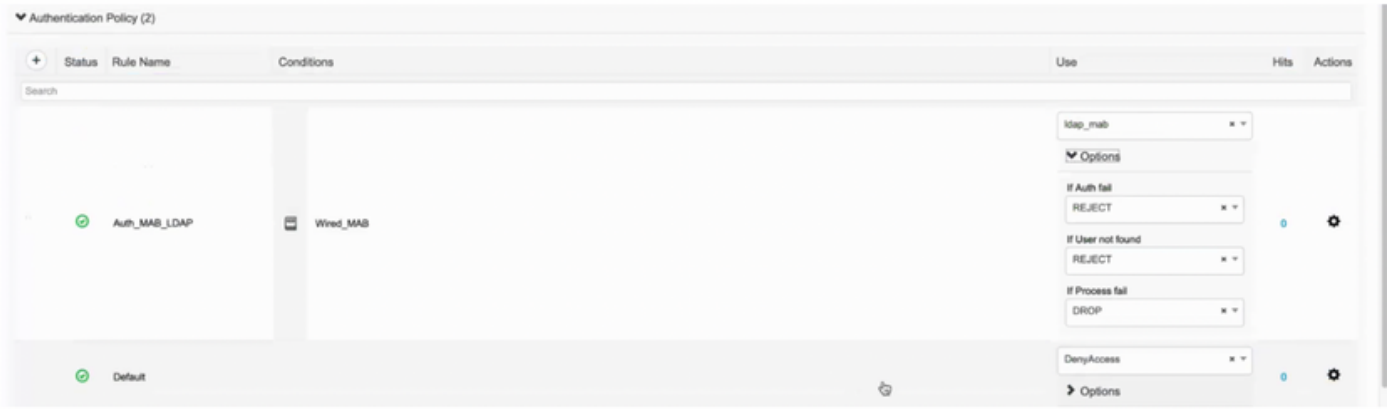




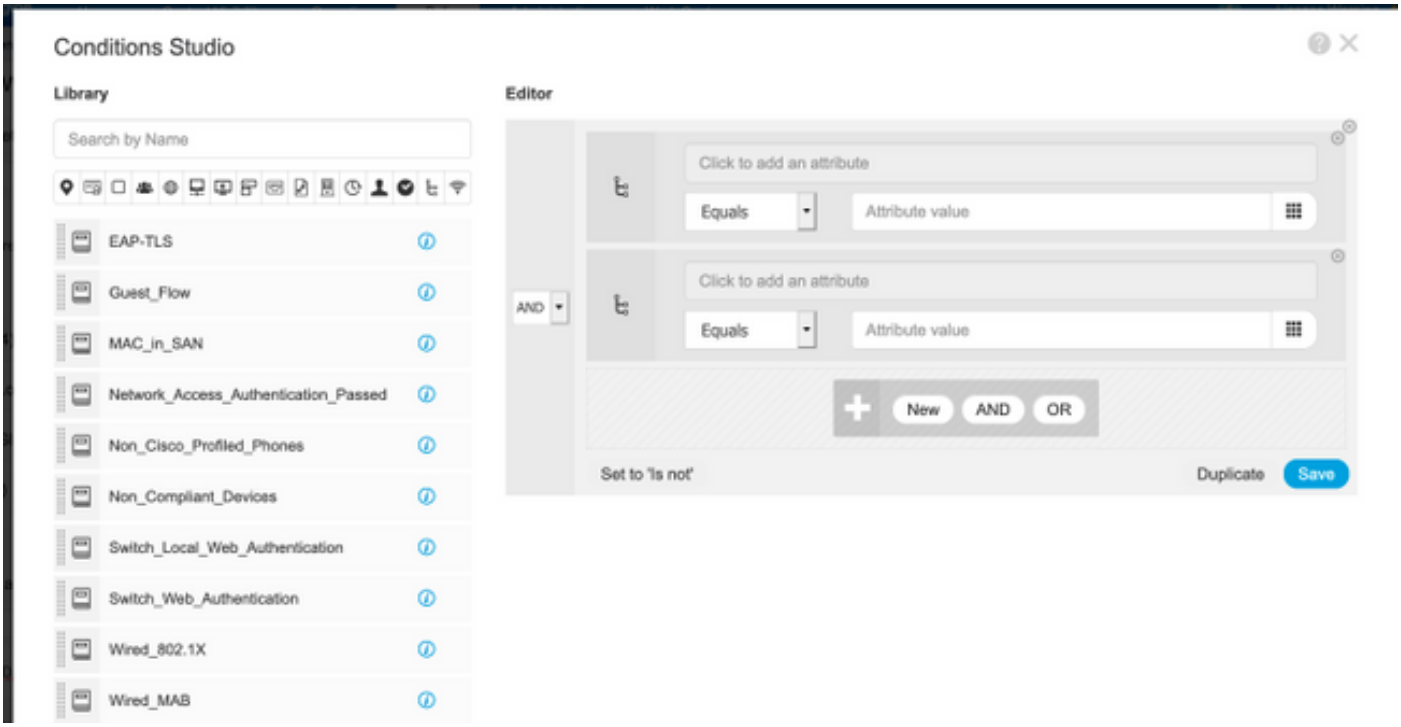
7.انتقل إلى مجموعة النهج> وقم بإنشاء مجموعة نهج باستخدام الشرط المحدد مسبقا Wired_MAB والبروتوكول المسموح به الذي تم إنشاؤه في الخطوة 5.

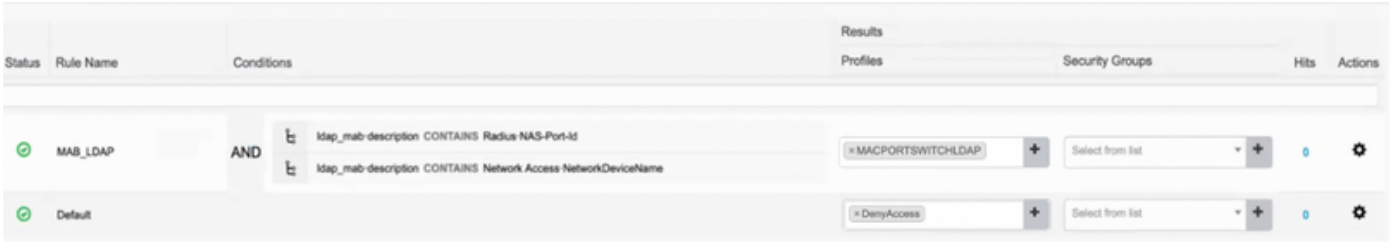


8. بموجب مجموعة النهج الجديدة، قم بإنشاء سياسة مصادقة باستخدام اتصال **LDAP** ومكتبة **Wired_MAB** المحددة مسبقا كتسلسل مصدر هوية خارجي



9. بموجب **نهج التخويل**، قم بتحديد اسم وإنشاء شرط مركب باستخدام وصف سمة LDAP و RADIUS NAS-Port-ID و NetworkDeviceName. أخيرا، أضف ملف تعريف التخويل الذي تم إنشاؤه في الخطوة 6.





بعد تطبيق التكوين، يجب أن تكون قادرا على الاتصال بالشبكة دون تدخل من المستخدم.

التحقق من الصحة

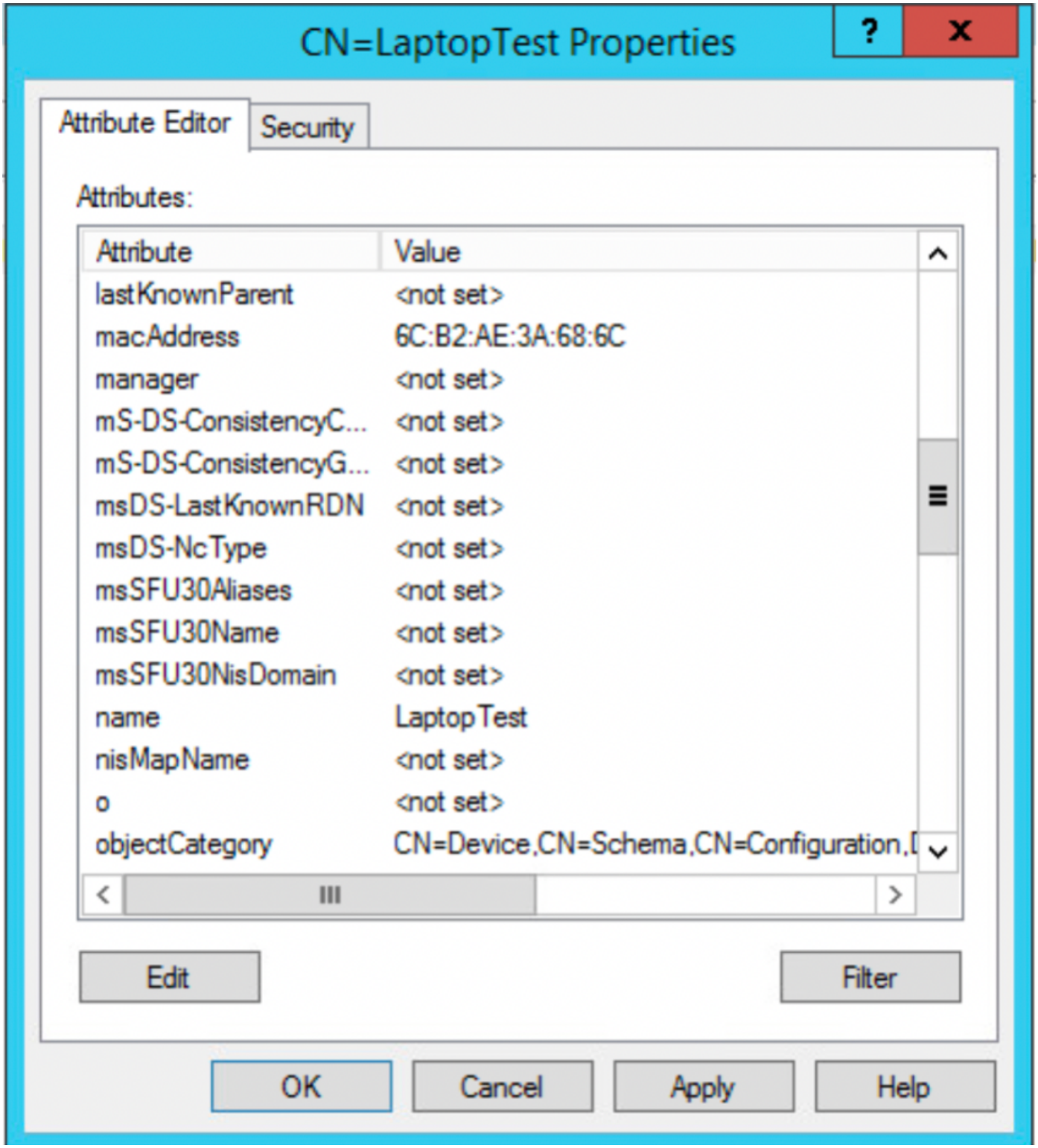
ويجب الاتصال بمنفذ المحول المخصص، يمكنك كتابة **لفاصيلا** show **authentication session** GigabitEthernet X/X/X للتحقق من حالة المصادقة والتفويض الخاصة بالجهاز.

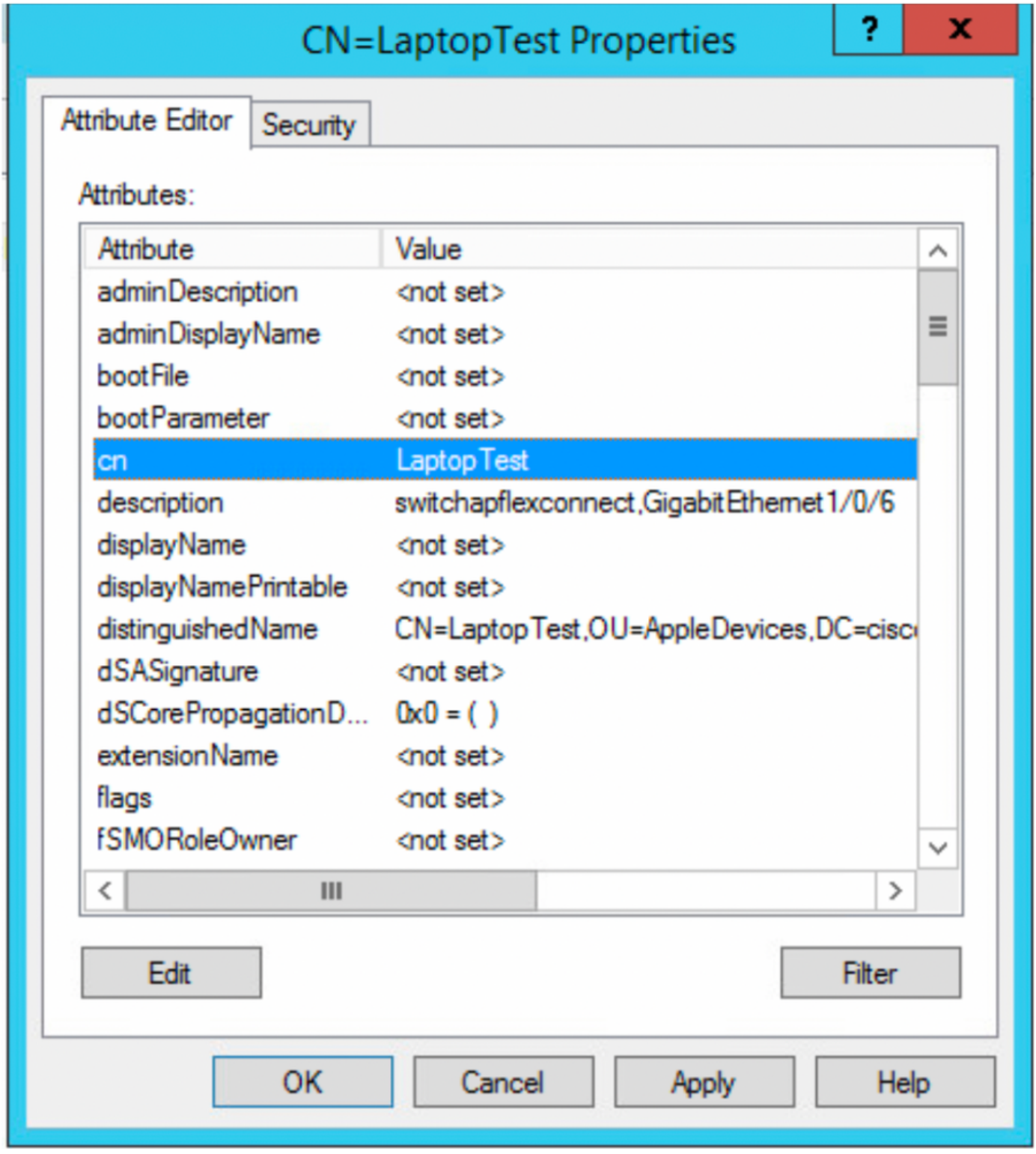
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID:
0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-
B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir:
both Session timeout: N/A Restart timeout: N/A Common Session ID: 0A517F65000013DA87E85A24 Acct
session ID: 0x000015D9 Handle: 0x9300005C Current Policy: Policy_Gi1/0/6 Local Policies: Service
Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Security Policy: Should Secure
Security Status: Link Unsecure Method status list: Method State mab Authc Success
```

على ISE، يمكنك إستخدام سجلات Radius Live للتأكيد.

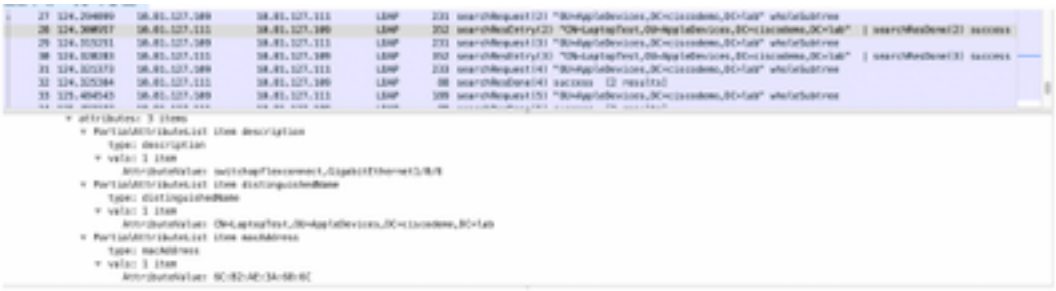
استكشاف الأخطاء وإصلاحها

على خادم LDAP، تحقق من أن الجهاز الذي تم إنشاؤه يحتوي على عنوان MAC واسم المحول المناسب ومنفذ المحول الذي تم تكوينه


CN=LaptopTest Properties
?
X
Attribute Editor
Security
Attributes:
Attribute
Value
lastKnownParent
<not set>
macAddress
6C:B2:AE:3A:68:6C
manager
<not set>
mS-DS-ConsistencyC...
<not set>
mS-DS-ConsistencyG...
<not set>
msDS-LastKnownRDN
<not set>
msDS-NcType
<not set>
msSFU30Aliases
<not set>
msSFU30Name
<not set>
msSFU30NisDomain
<not set>
name
LaptopTest
nisMapName
<not set>
o
<not set>
objectCategory
CN=Device,CN=Schema,CN=Configuration,
Edit
Filter
OK
Cancel
Apply
Help



على ISE، أنت يستطيع أخذ ربط على قبض (انتقل إلى **العمليات->تحريت->أداة التشخيص->TCP** (**مقابل TCP**) in order to دقق القيمة قيد الارسال من LDAP إلى ISE



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).