基於ISE和LDAP屬性的身份驗證

目錄

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)和使用輕量級目錄訪問協定(LDAP)對象屬性來動態驗證和授權裝置。

> **附註：本文檔對使用LDAP作為ISE身份驗證和授權的外部身份源的設定有效。**

作者：Emmanuel Cano和Mauricio Ramos Cisco專業服務工程師。

由Neri Cruz Cisco TAC工程師編輯。

必要條件

需求

思科建議您瞭解以下主題：

- ISE策略集、身份驗證和授權策略的基本知識
- Mac Authentication Bypass(MAB)
- Radius通訊協定的基礎知識
- Windows伺服器基礎知識

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- Cisco ISE 2.4版補丁11
- Microsoft Windows Server 2012 R2 x64版
- 思科交換機Catalyst 3650-24PD，版本03.07.05.E(15.2(3)E5)
- Microsoft Windows 7電腦

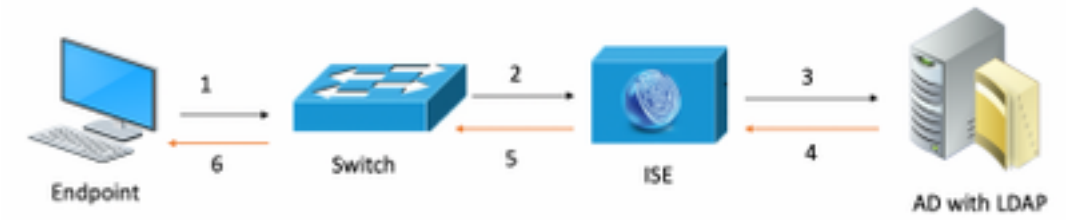
> **附註：** 本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

組態

本節介紹如何配置網路裝置、ISE與LDAP之間的整合，並最終配置要用於ISE授權策略的LDAP屬性。

網路圖表

此圖說明所使用的網路拓撲：



以下是流量傳輸，如網路圖所示：

1. 使用者將其pc/筆記型電腦連線到指定的交換機埠。
2. 交換機向ISE傳送該使用者的Radius訪問請求
3. 當ISE收到資訊時，它將查詢特定使用者欄位的LDAP伺服器，其中包含要在授權策略條件中使用的屬性。
4. ISE收到屬性（交換機埠、交換機名稱和裝置mac地址）後，會比較交換機提供的資訊。
5. 如果交換機提供的屬性資訊與LDAP提供的屬性資訊相同，則ISE將傳送RADIUS Access-Accept，並在授權配置檔案中配置許可權。

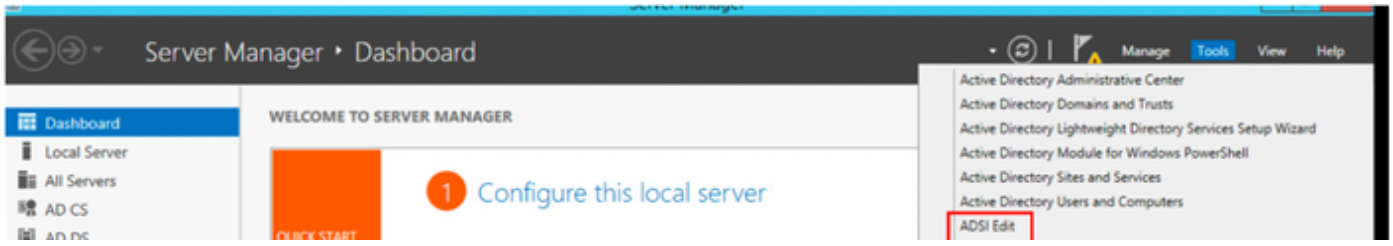
組態

使用本節配置LDAP、交換機和ISE。

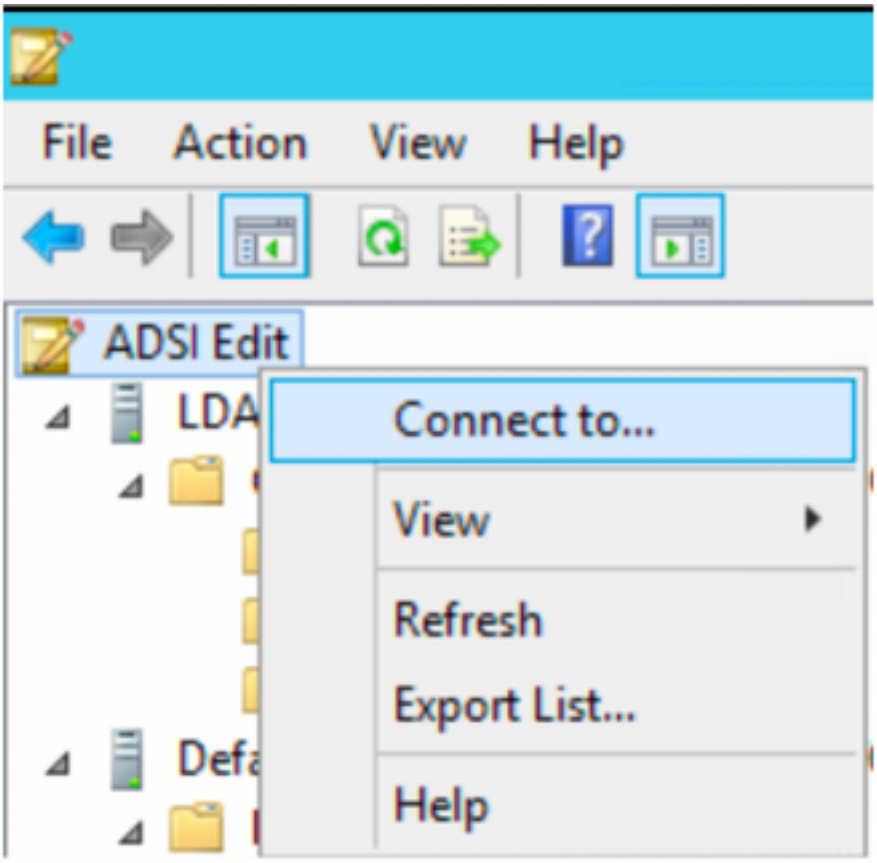
設定 LDAP

完成以下步驟以配置LDAP伺服器：

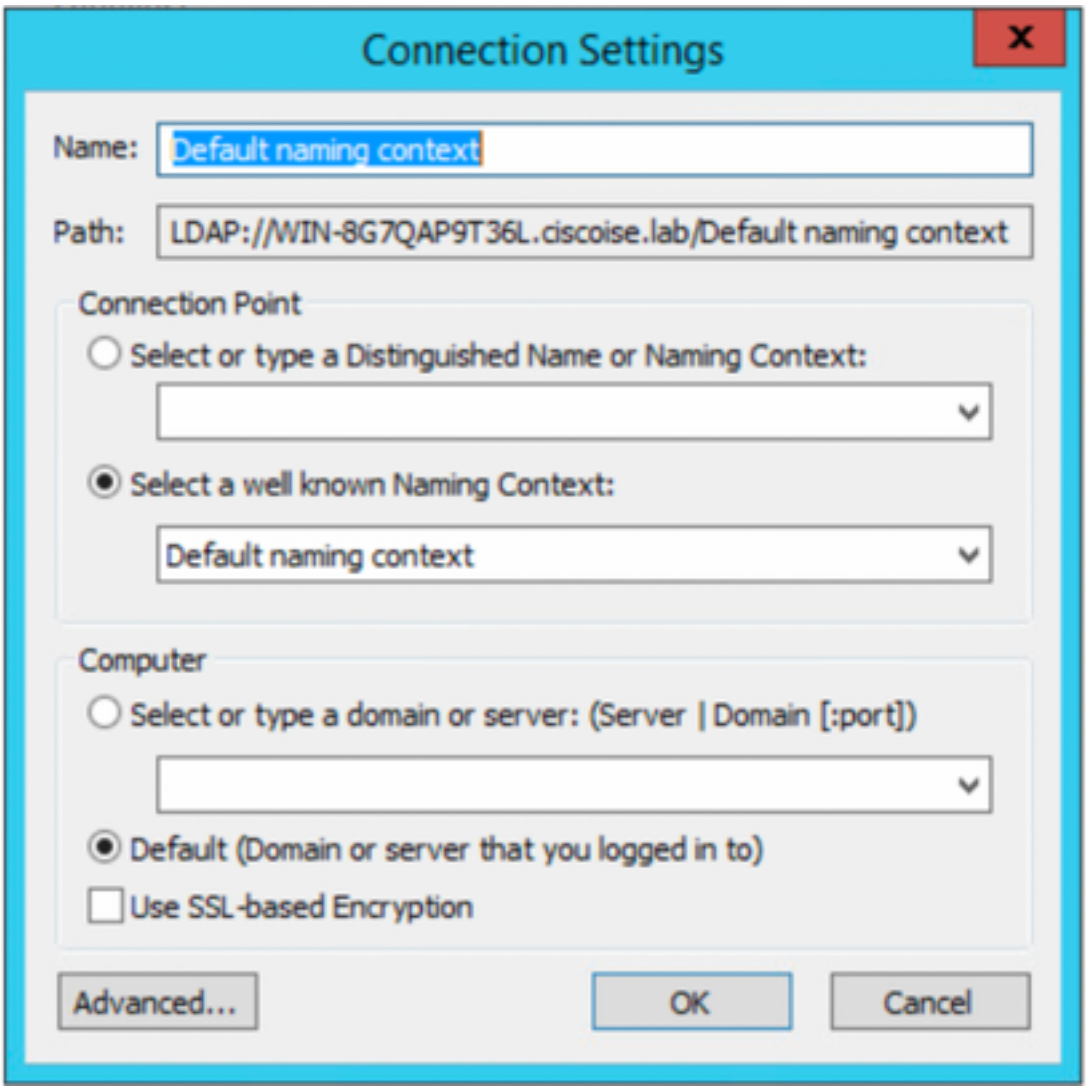
1.導航到**Server Manager > Dashboard > Tools > ADSI Edit**



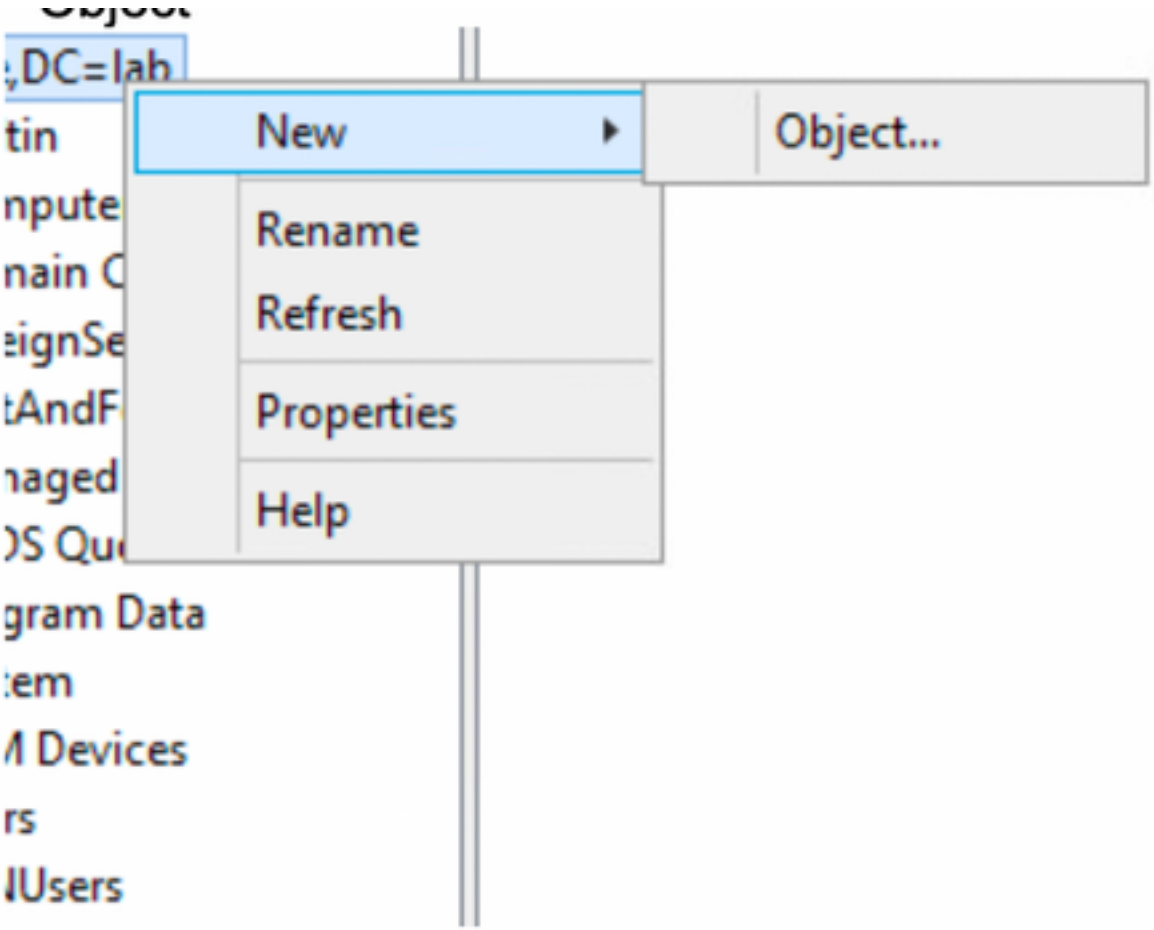
2.按一下右鍵ADSI Edit圖示，然後選擇**Connect to...**



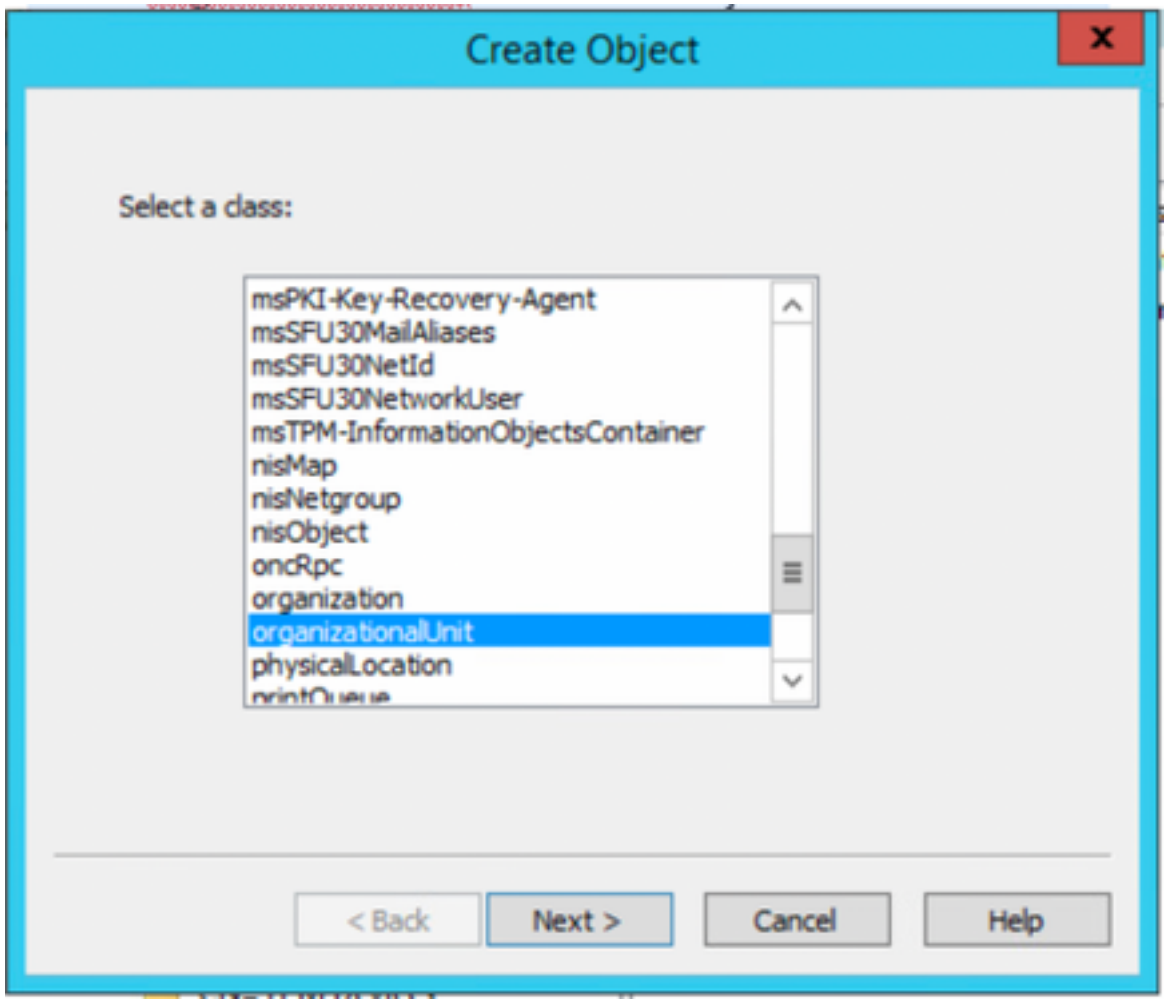
3.在「連線設定」下，定義名稱並選擇**確定**按鈕以啟動連線。



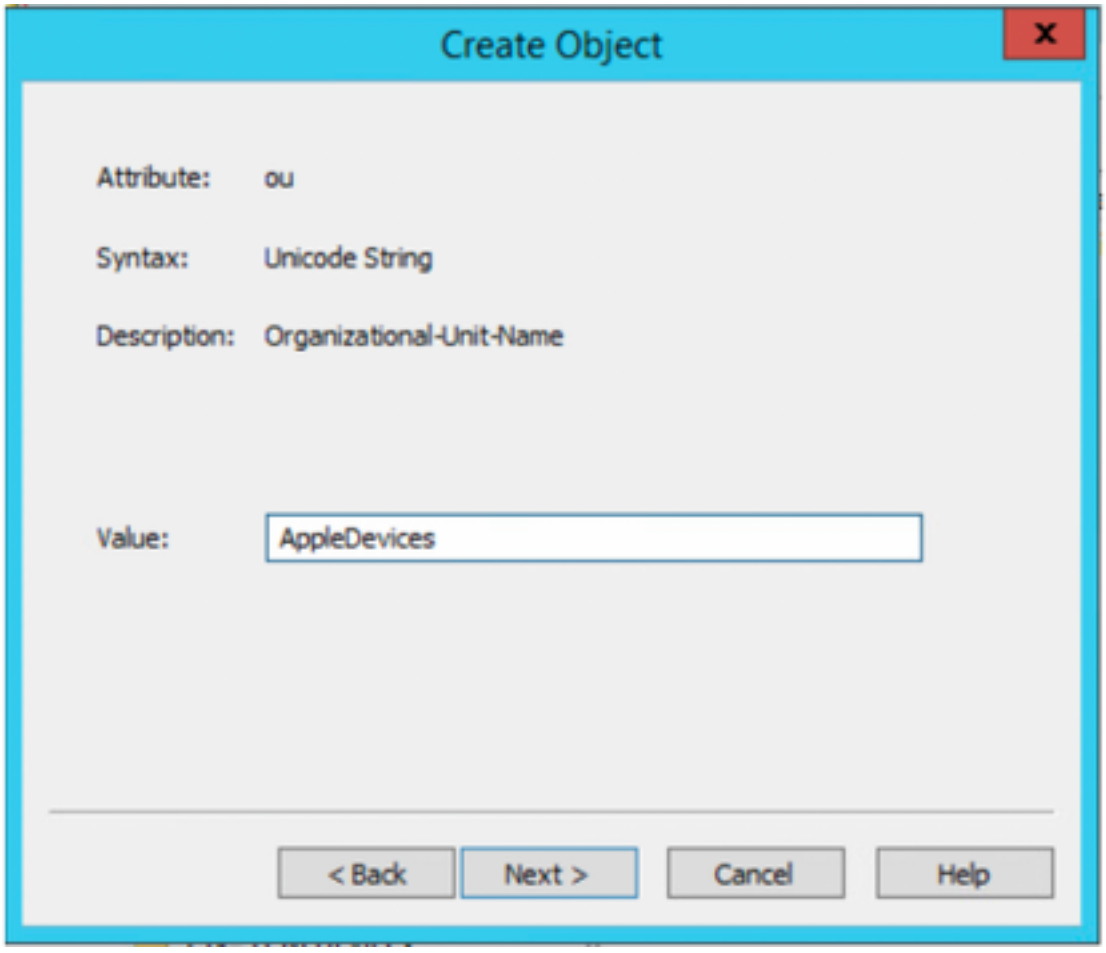
4.在同一ADSI Edit選單下，按一下右鍵DC連線(DC=ciscodemo， DC=lab)，選擇**New，然**後選擇選項**Object**



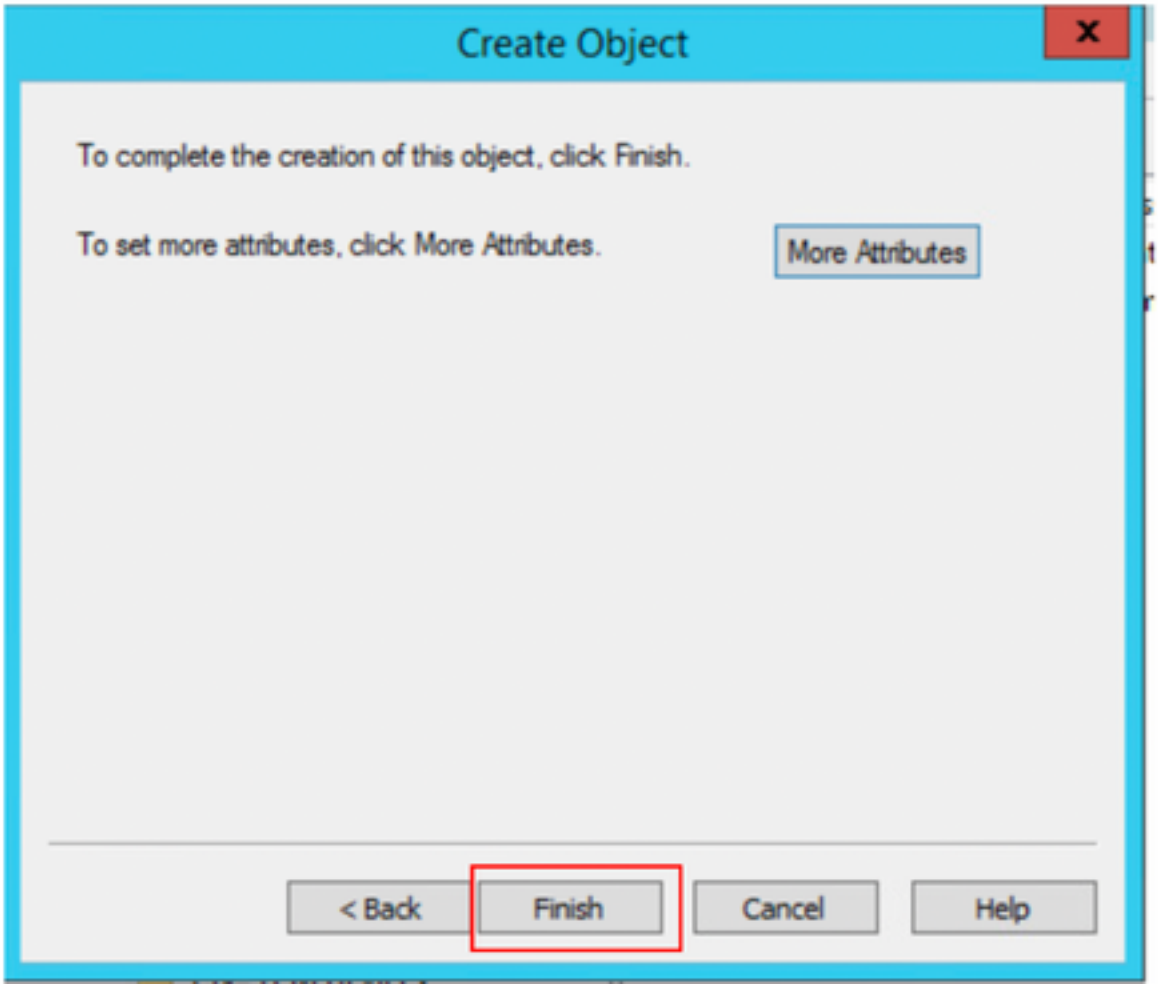
5.選擇選項**OrganizationalUnit**作為新對象，然後選擇「下一**步**」。



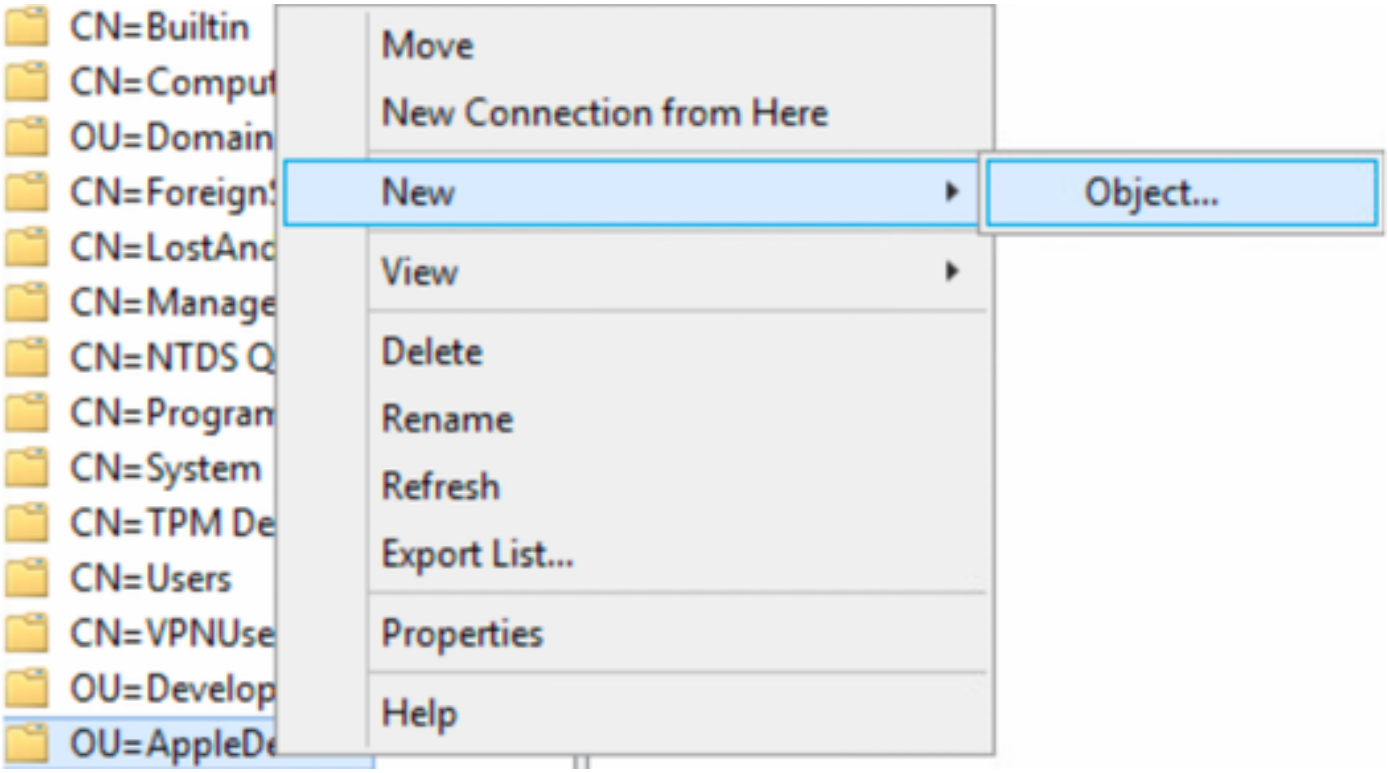
6.定義新OrganizationalUnit的名稱，然後選擇「下一步」



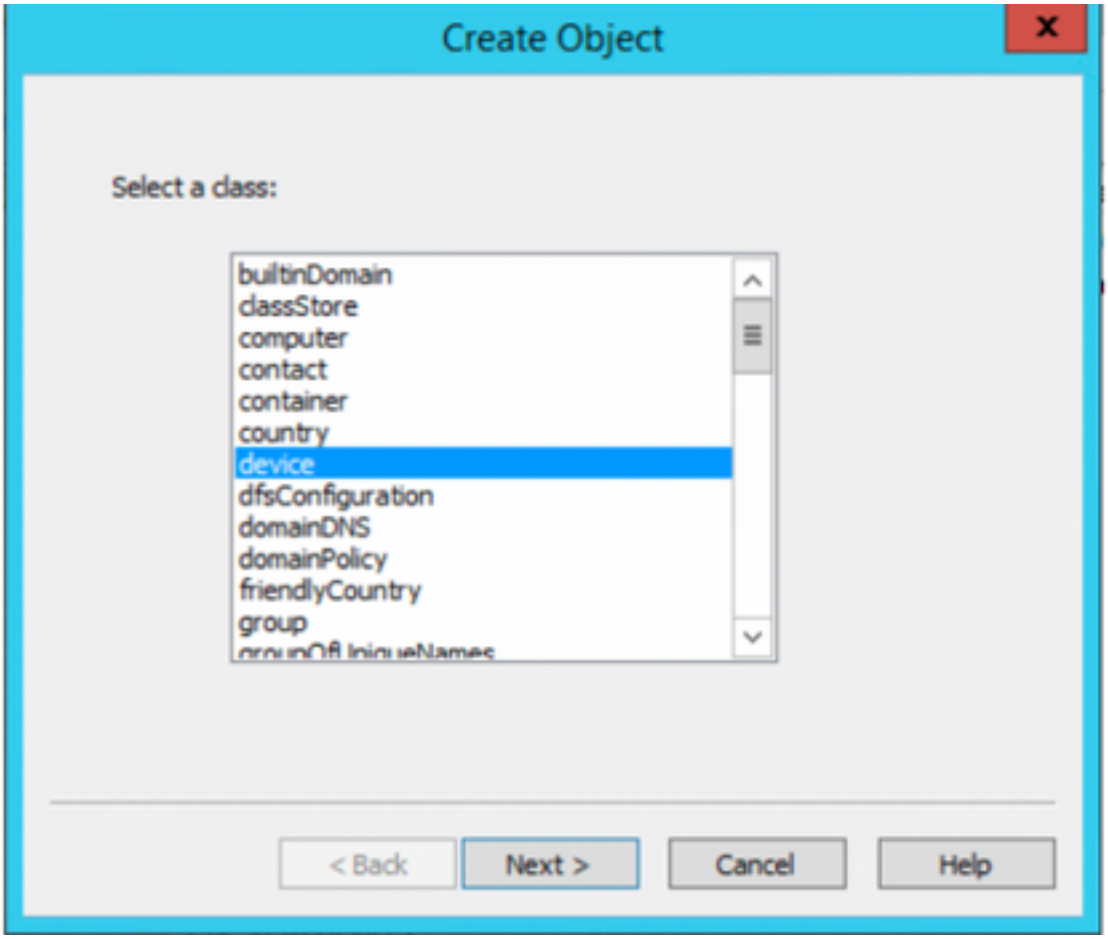
7.選擇「**完成**」以建立新的組織單位



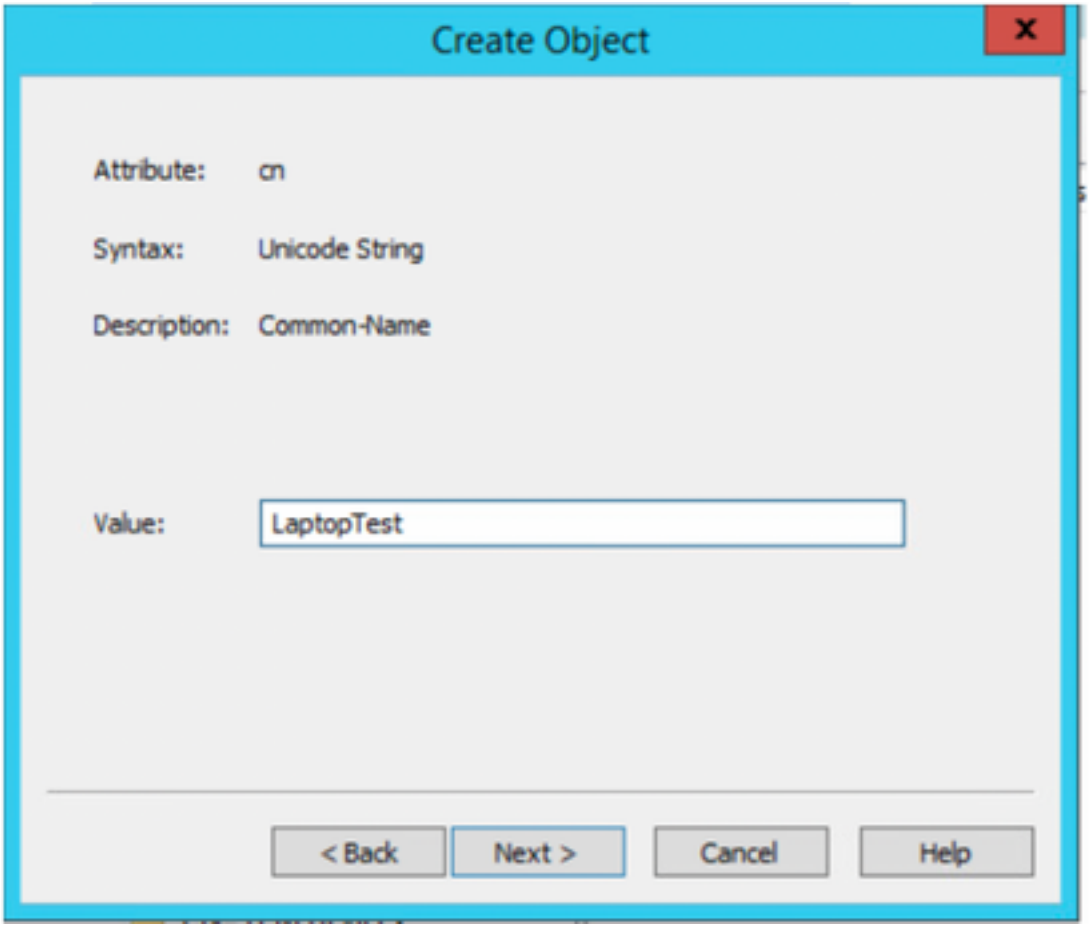
8.按一下右鍵剛建立的OrganizationalUnit，然後選擇**New > Object**



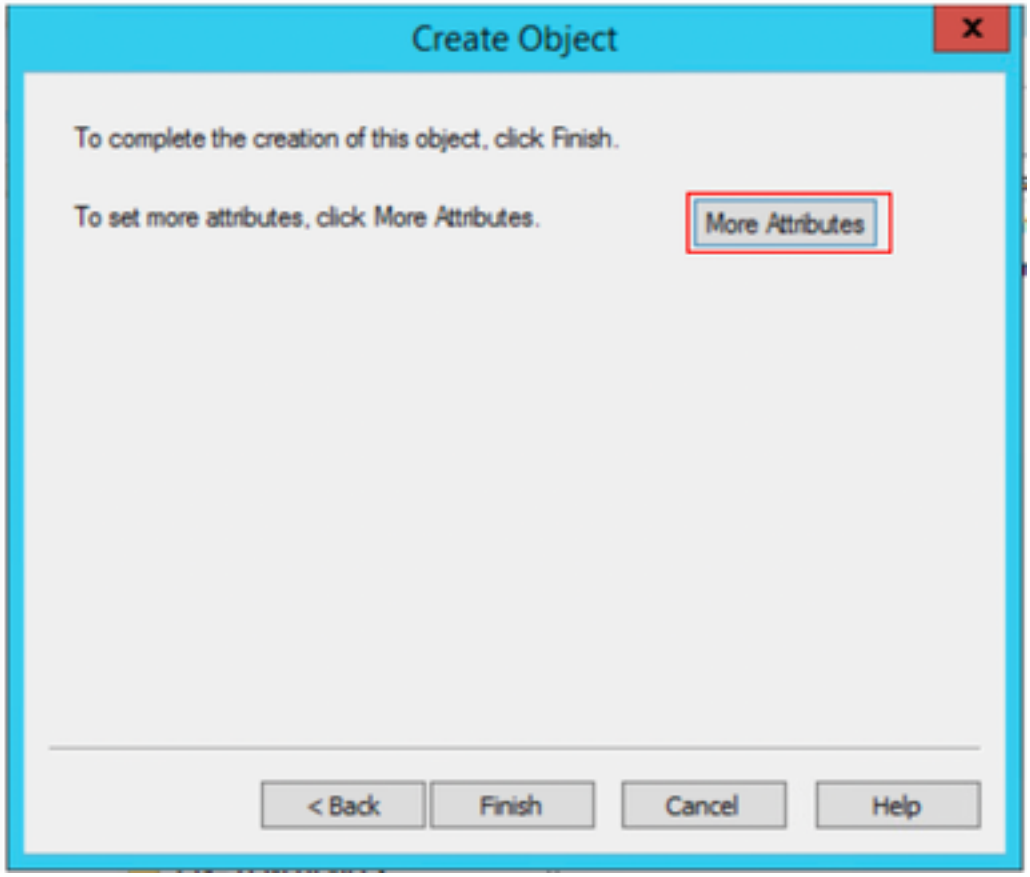
9.選擇**device**作為對象類，然後選擇 **下一頁**



10.在「值」(Value)欄位中定義名稱，然後選擇「下一個」(**Next)**

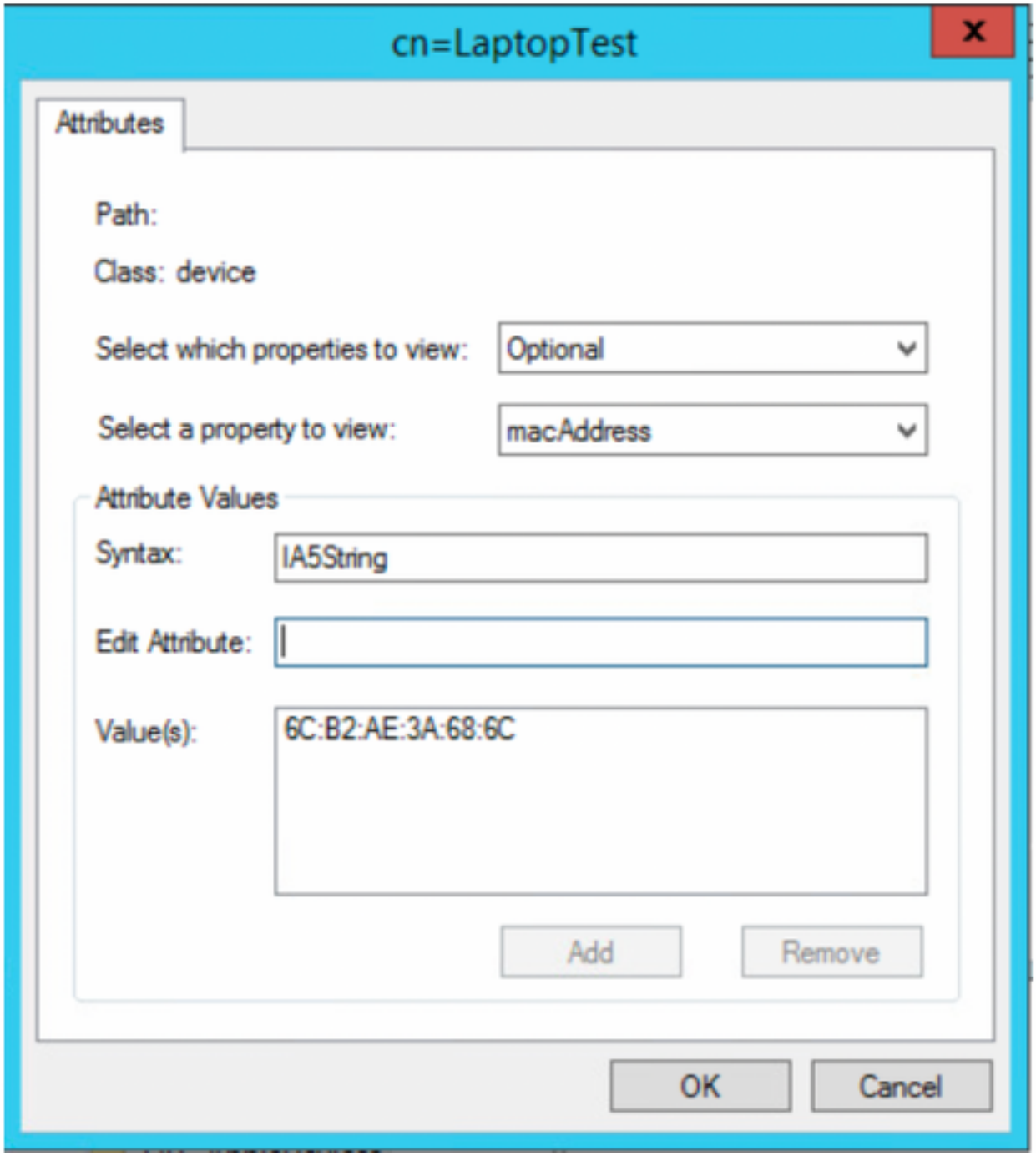


11.選擇選項**更多屬性**



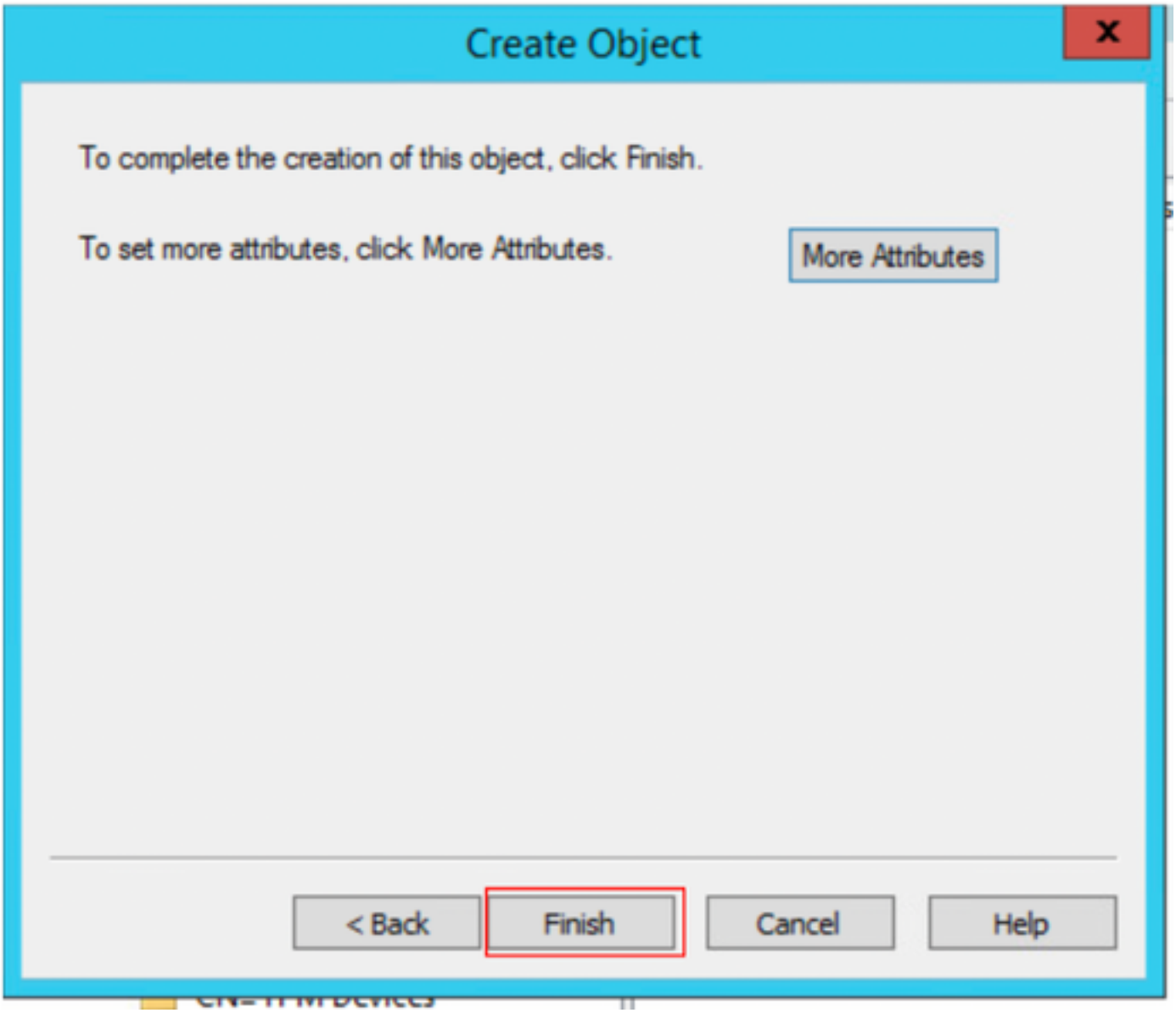
11.對於下拉選單，**選擇要檢視的屬性**，選擇選項**macAddress**，然後在**Edit attribute**欄位下定義要驗證的終端Mac地址，然後選擇 **Add**按鈕儲存裝置MAC地址。

注意:在mac地址八位元之間使用雙冒號代替點或連字元。

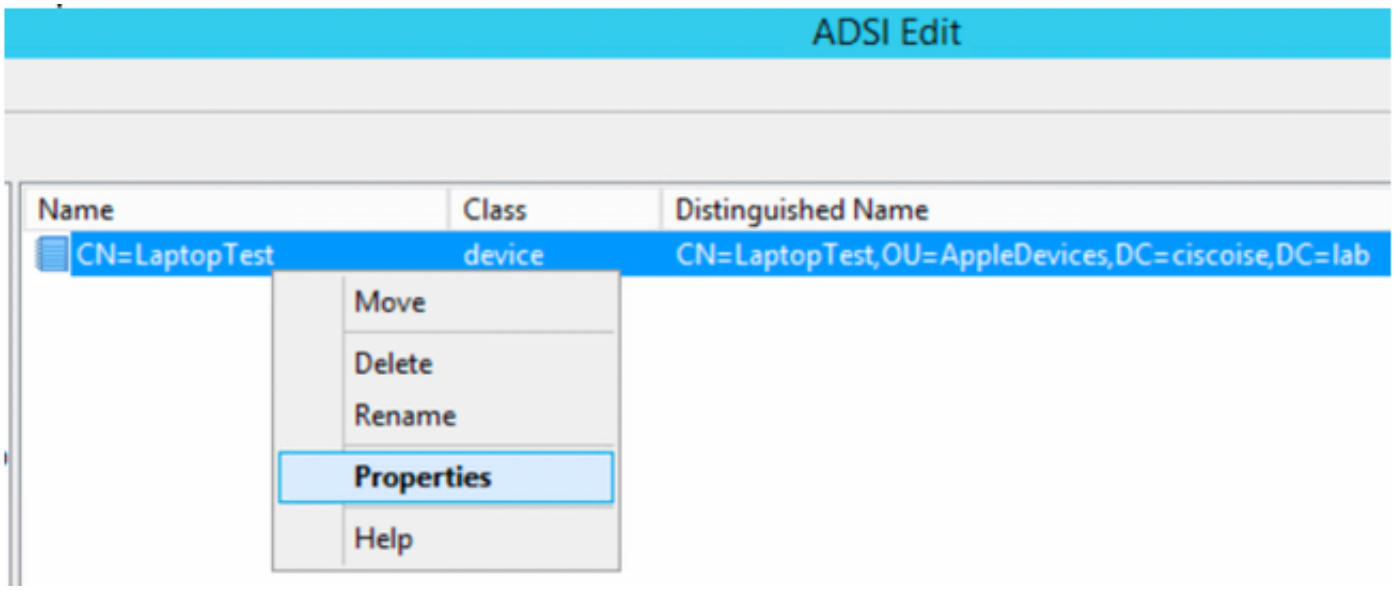


12.選擇**OK**以儲存資訊並繼續配置裝置對象

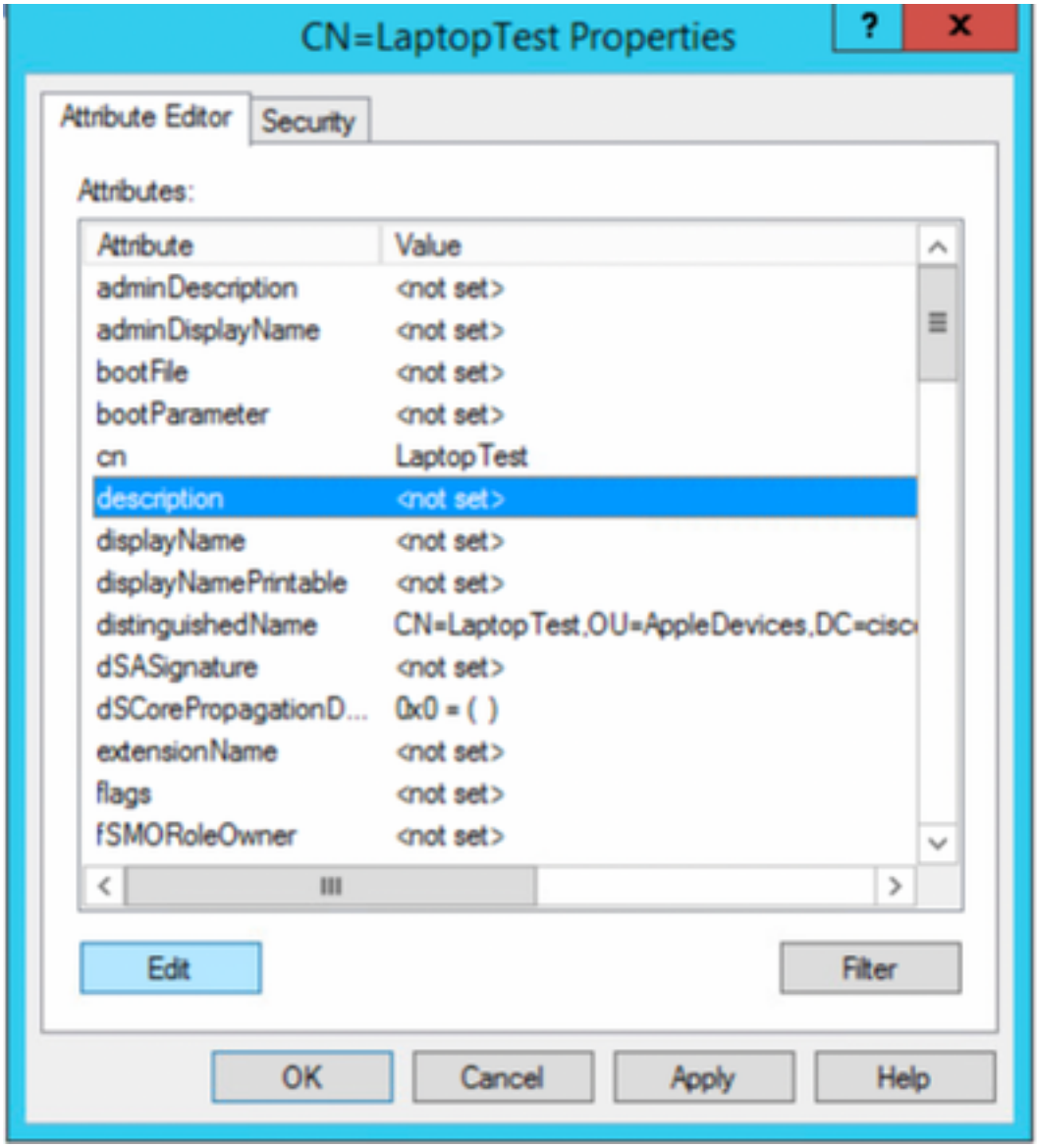
13.選擇**完成**以建立新的裝置對象



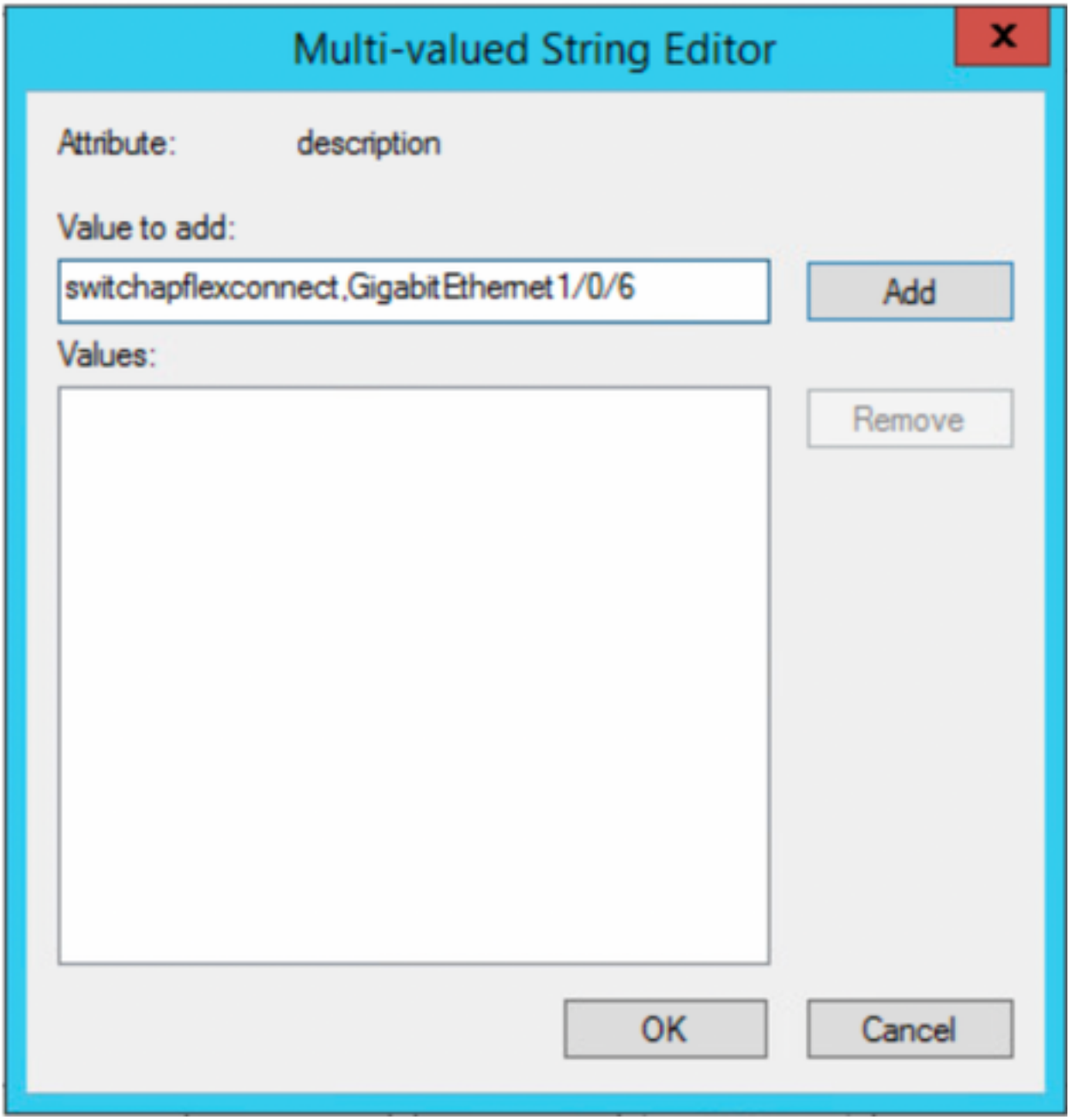
14.按一下右鍵裝置對象並選擇選項**Properties**



15.選擇**description**選項，然後選擇**Edit**以定義交換器名稱和裝置所連線的交換器連線埠。



16.定義交換機名稱和交換機埠，請確保使用逗號分隔每個值。選擇**Add**，然後選擇**Ok**以儲存資訊。



- **Switchapflexconnect是交換機名稱。**
- **GigabitEthernet1/0/6是終端所連線的交換機埠。**

附註：可以使用指令碼將屬性新增到特定欄位，但是，對於本示例，我們正在手動定義這些值

附註：AD屬性區分大小寫，如果您在LDAP查詢期間使用小寫形式的所有Mac地址，則ISE會轉換為大寫。為了避免此行為，請在允許的協定下禁用進程主機查詢。詳細資訊可以在以下連結中找到：https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

交換器組態

ISE802.1x

```
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
```

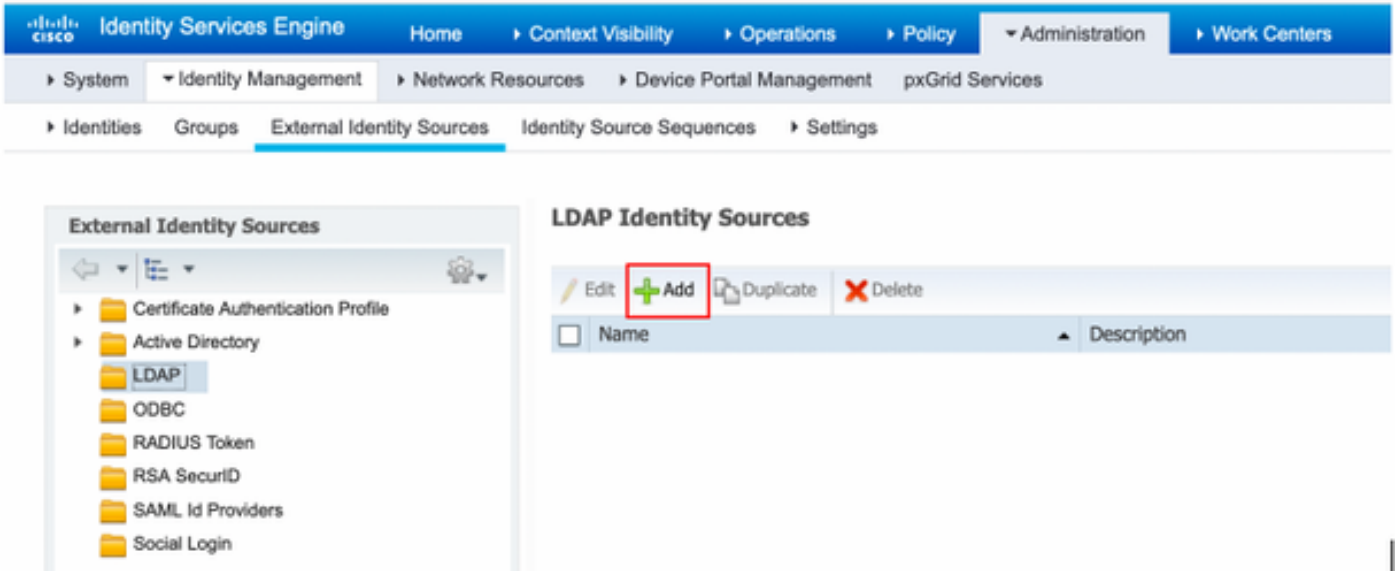
```
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access authentication event fail action next-method authentication event server
dead action authorize 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 !
```

附註：可能需要在您的環境中調整全域性和介面配置

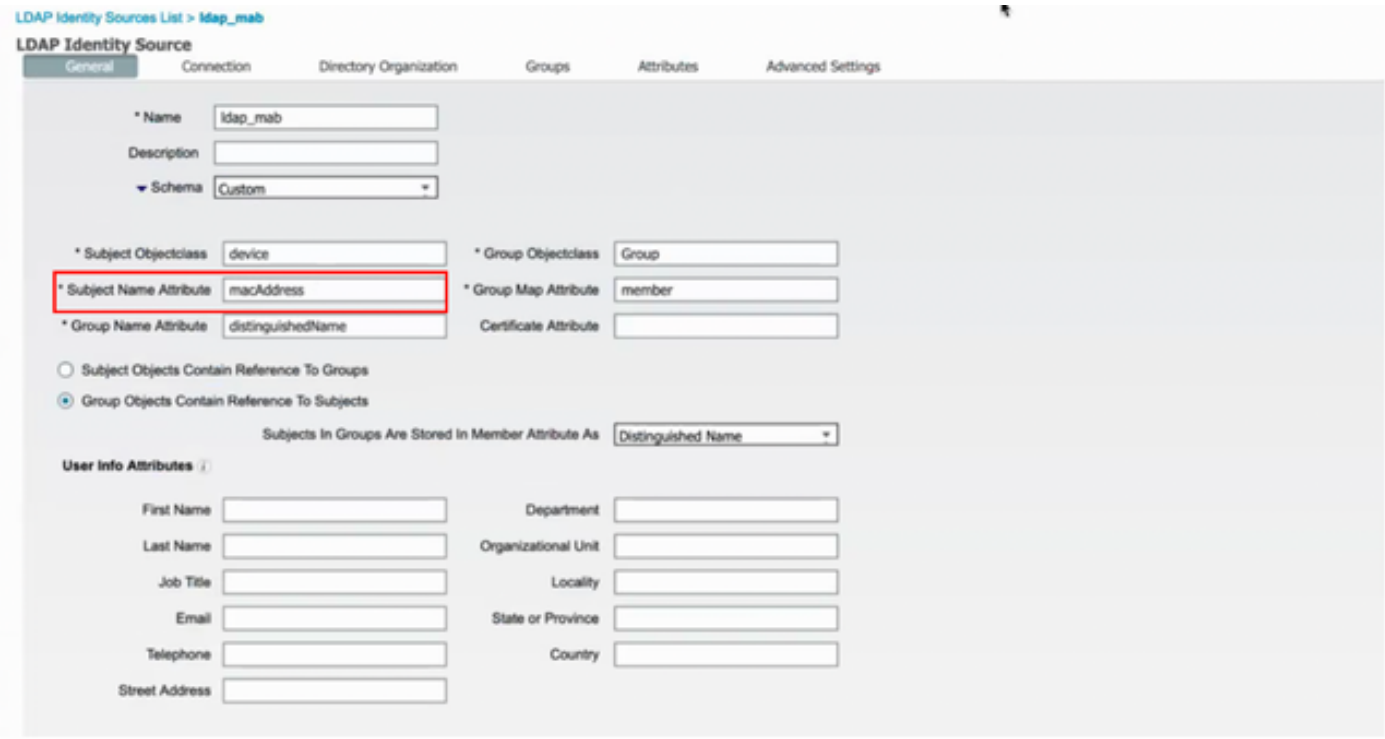
ISE 組態

以下說明在ISE上配置從LDAP伺服器獲取屬性並配置ISE策略。

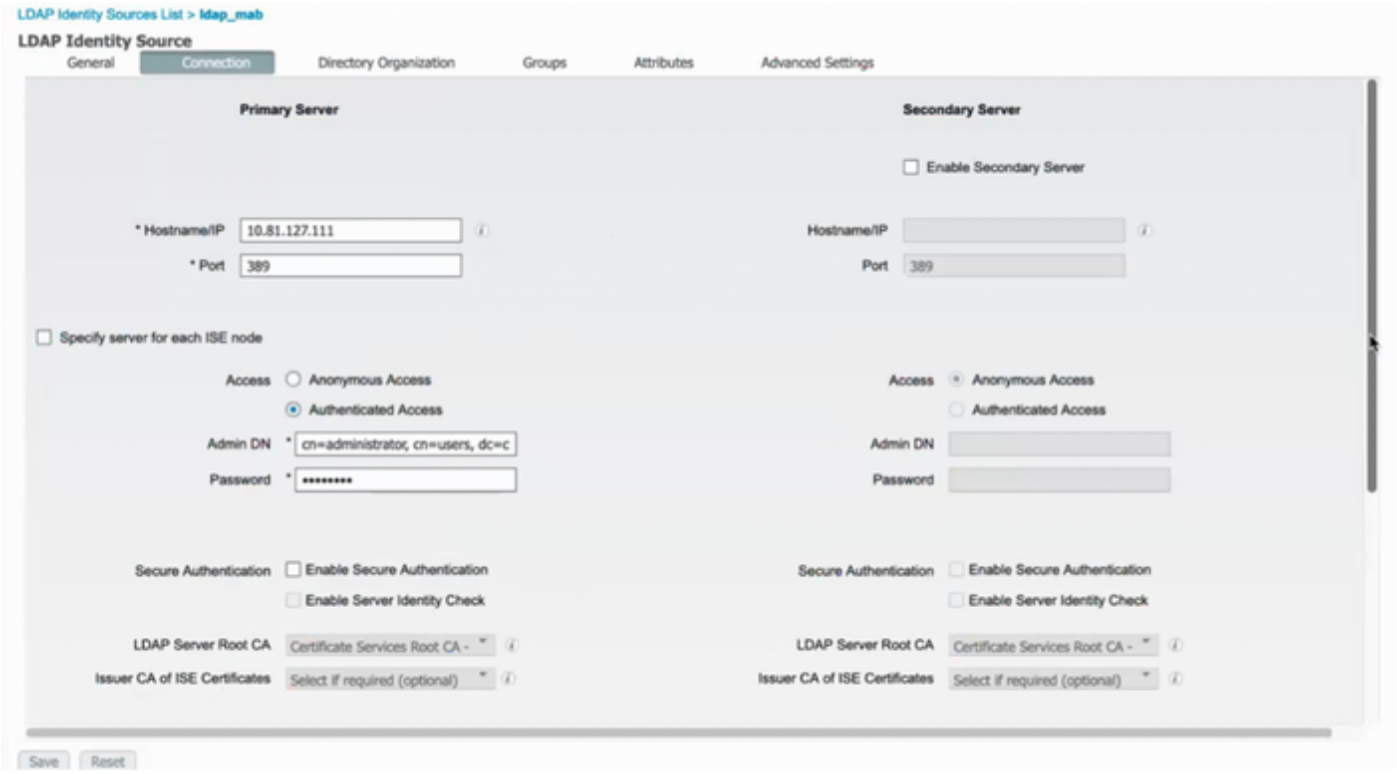
1. 在ISE上，轉至**管理 — >身份管理 — >外部身份源**，選擇**LDAP**資料夾，然後按一下**Add**以建立與LDAP的新連線



2.在**General**頁籤下，定義名稱，然後選擇mac地址作為主題名稱屬性

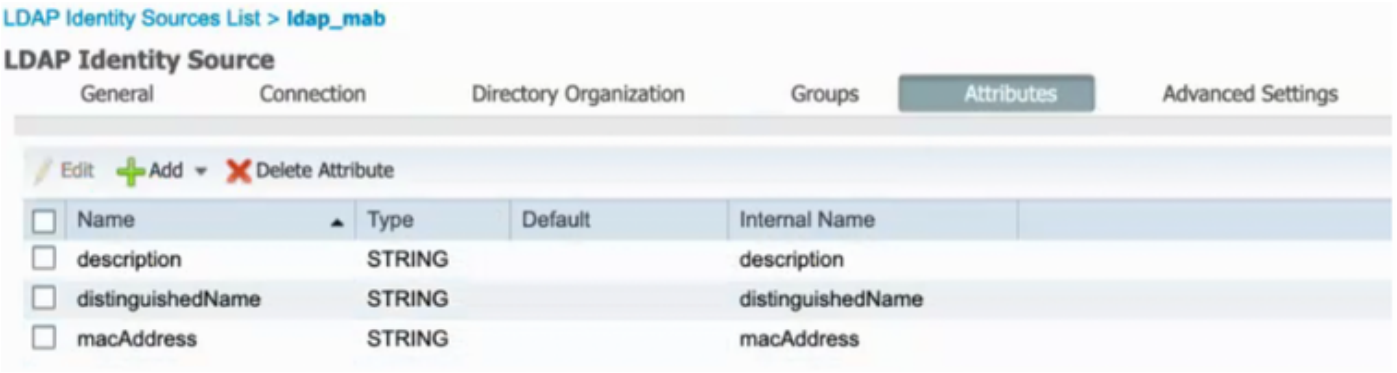


3.在**Connection**頁籤下，從LDAP伺服器配置IP地址、管理員DN和密碼以成功連線。

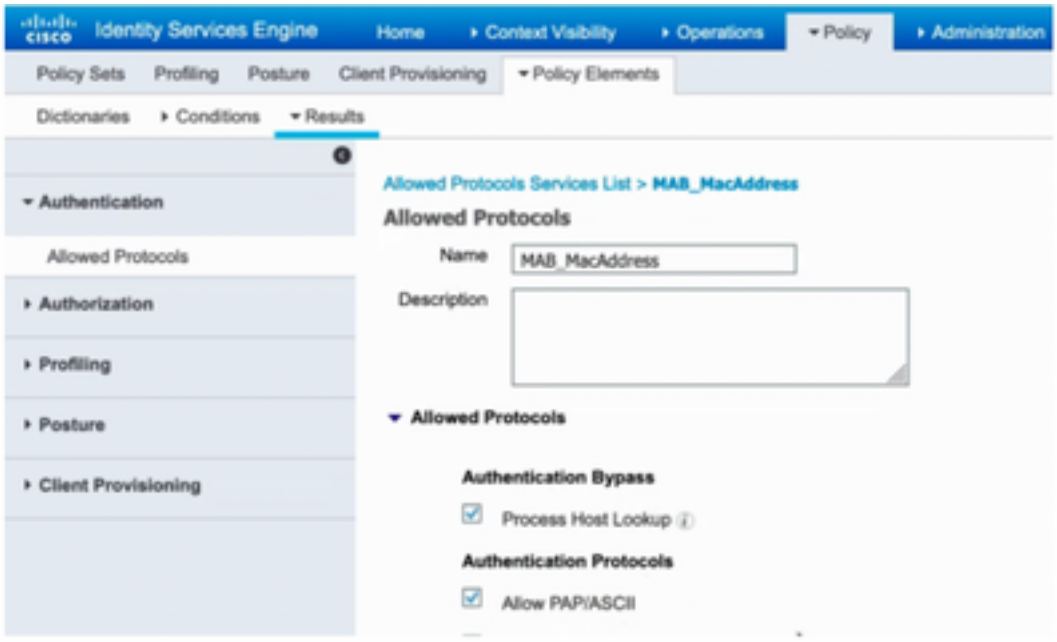


附註：埠389是使用的預設埠。

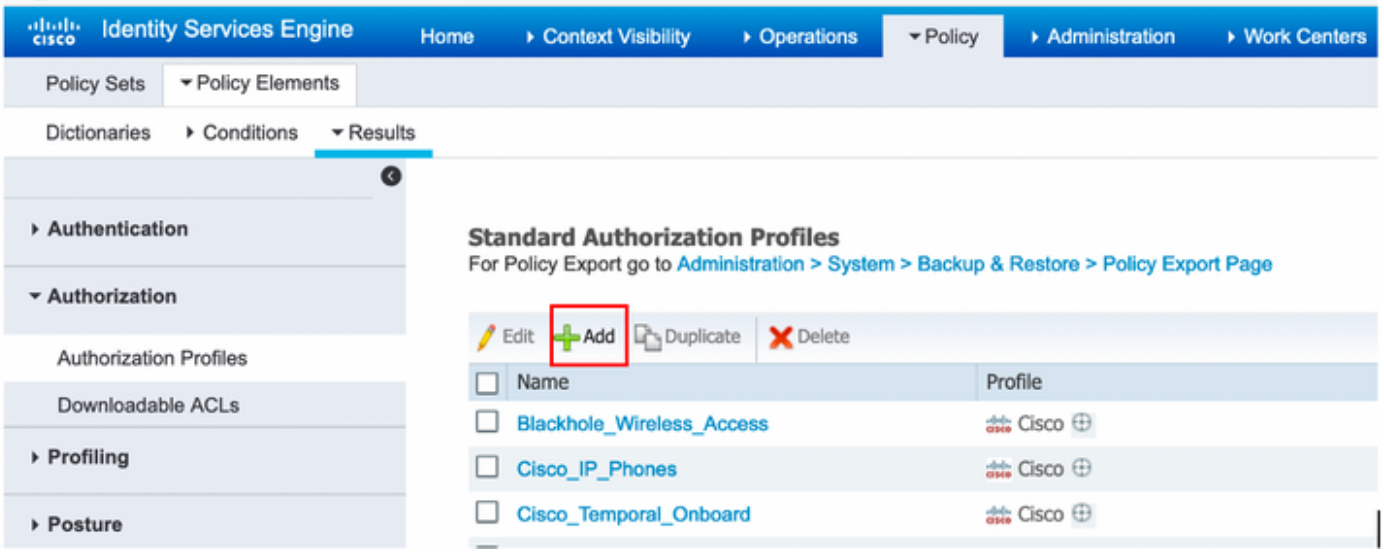
4.在**Attributes**頁籤下，選擇macAddress和description屬性，這些屬性將在授權策略中使用

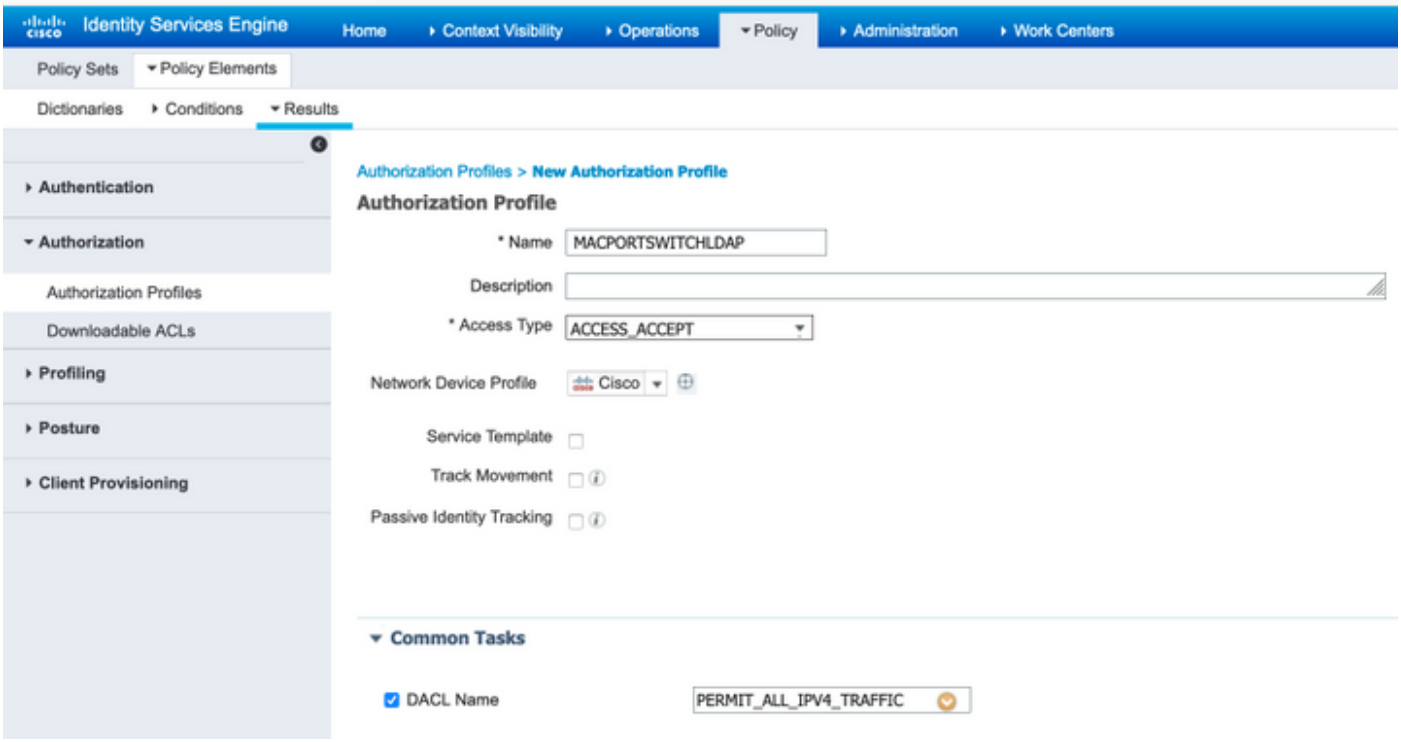


5.要建立允許的協定，請轉至**策略 — >策略元素 — >結果 — >身份驗證 — >允許的協定。**定義並選擇進程主機查詢和允許PAP/ASCII作為唯一允許的協定。最後選擇**儲存**

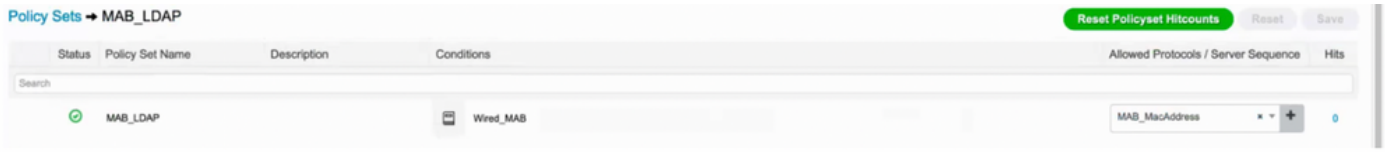


6.要建立授權配置檔案，請轉到**策略 — >策略元素 — >結果 — >授權 — >授權配置檔案。選擇Add**並定義將分配給終結點的許可權。

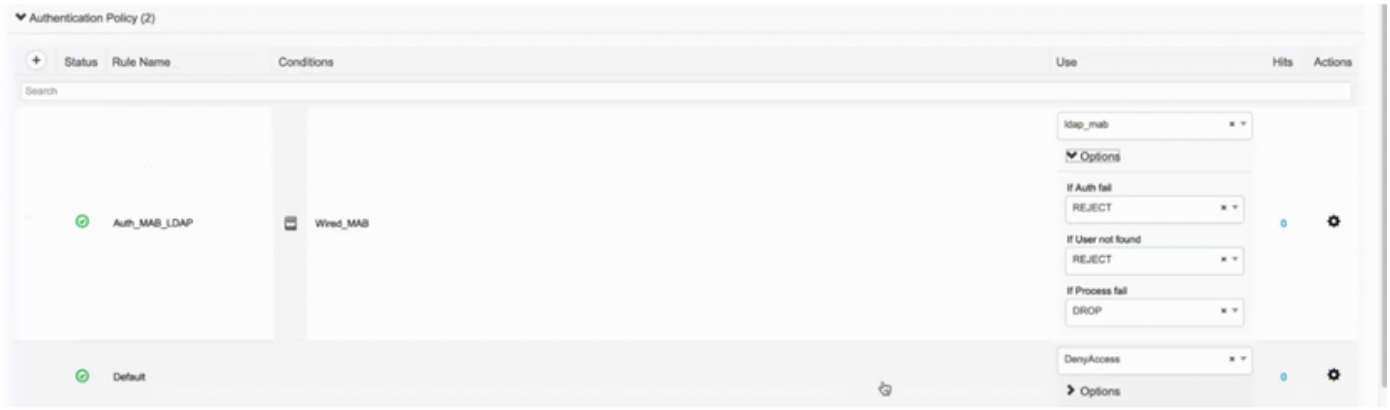




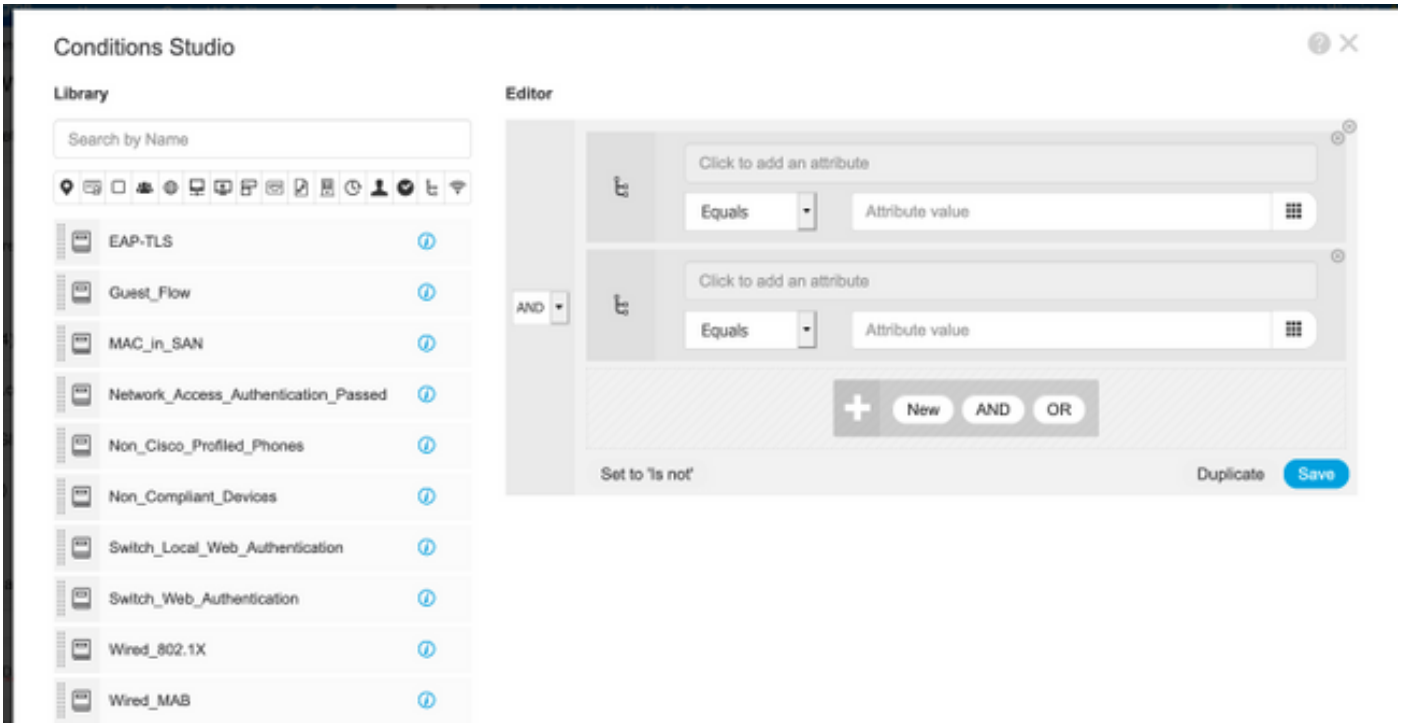
7.轉至Policy-> Policy Set，使用預定義條件Wired_MAB和步驟5中建立的允許協定建立策略集。

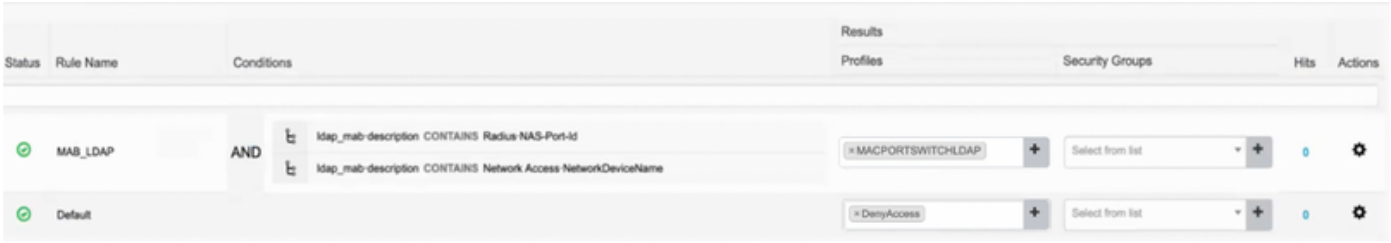


8.在新建立的策略集下，使用預定義的**Wired_MAB庫和LDAP連線作為外部身份源序列建立身份驗證策略**



9.在**授權策略**下，使用LDAP屬性說明、Radius NAS-Port-Id和NetworkDeviceName定義名稱並建立複合條件。最後，新增在步驟6中建立的授權配置檔案。





套用組態後，您應該能夠連線到網路，無需使用者干預。

驗證

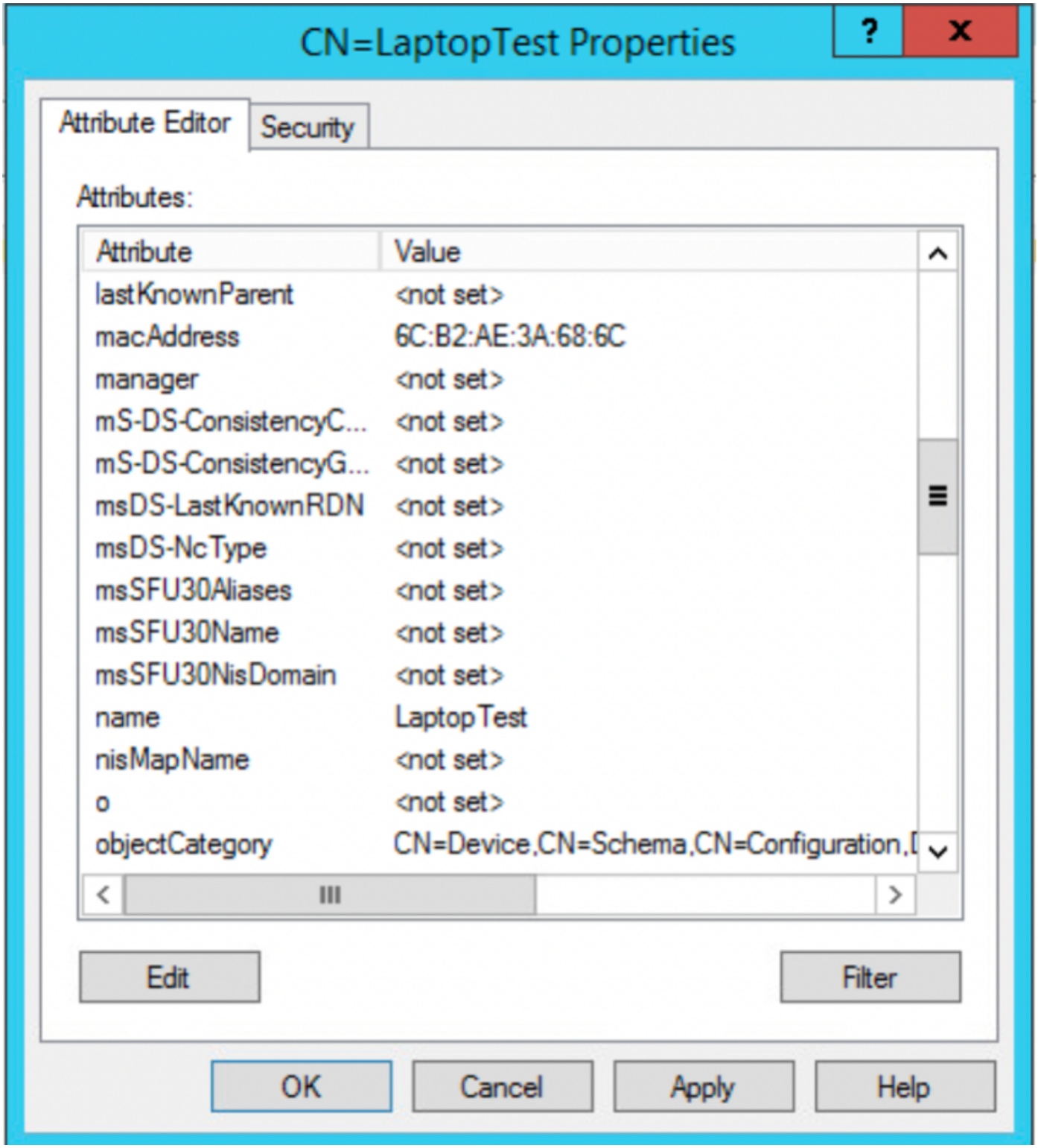
連線到指定的交換機埠後，可以鍵入**show authentication session interface GigabitEthernet X/X/X details**以驗證裝置的身份驗證和授權狀態。

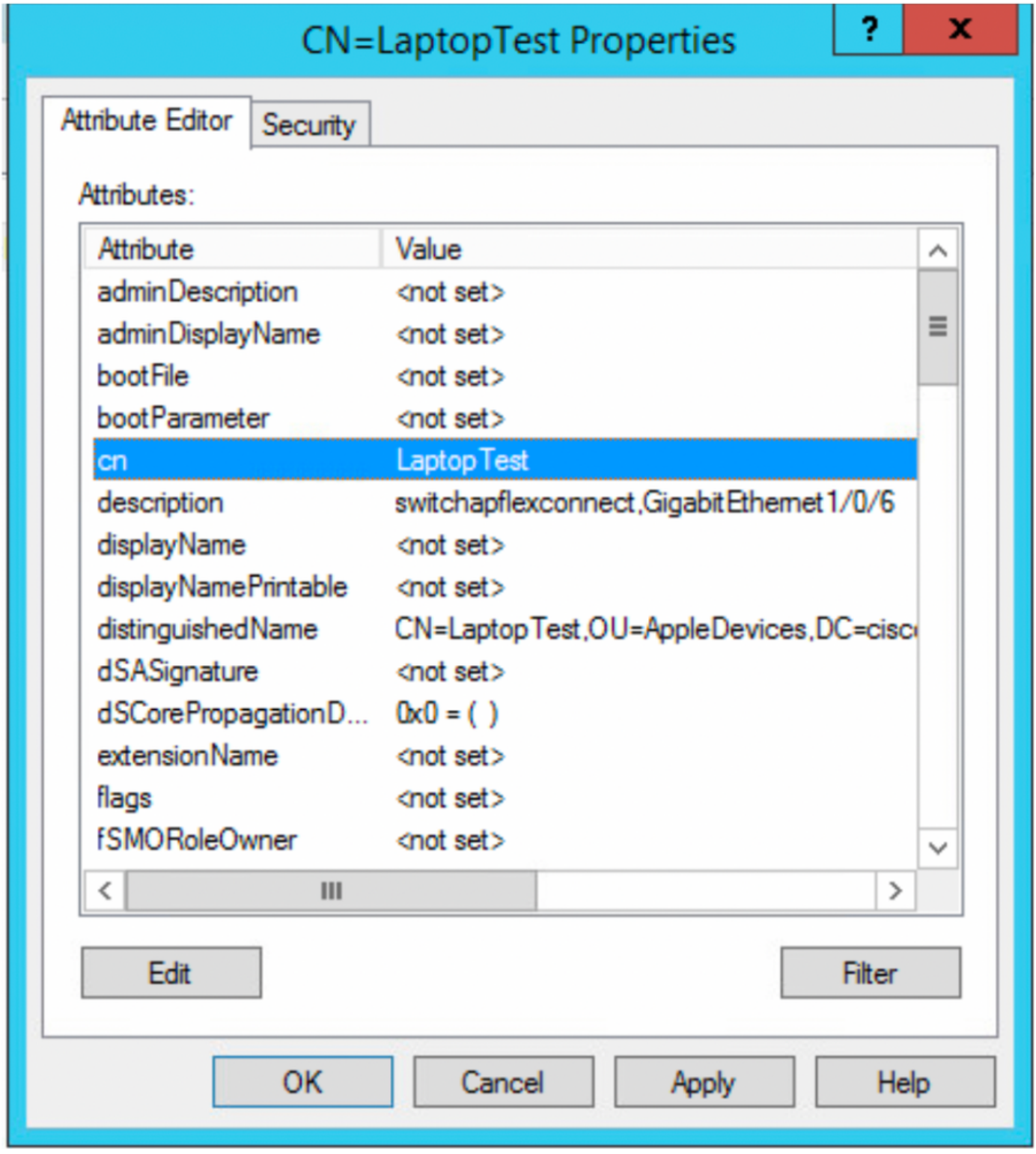
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session 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
```

在ISE上，您可以使用Radius即時日誌進行確認。

疑難排解

在LDAP伺服器上，驗證建立的裝置是否配置了Mac地址、正確的交換機名稱和交換機埠


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



在ISE上，您可以進行資料包捕獲(轉至**操作 — >故障排除 — >診斷工具 — >TCP轉儲**)以驗證從LDAP傳送到ISE的值