基于ISE和LDAP属性的身份验证

目录

简介

本文档介绍如何配置思科身份服务引擎(ISE)和使用轻量级目录访问协议(LDAP)对象属性来动态验证和授权设备。

> **注意：本文档对使用LDAP作为ISE身份验证和授权的外部身份源的设置有效。**

作者：Emmanuel Cano和Mauricio Ramos思科专业服务工程师。

由Neri Cruz Cisco TAC工程师编辑。

先决条件

要求

思科建议您了解以下主题：

- ISE策略集、身份验证和授权策略的基本知识
- Mac身份验证绕行(MAB)
- Radius协议的基本知识
- Windows服务器的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本2.4补丁11
- Microsoft Windows Server，版本2012 R2 x64
- 思科交换机Catalyst 3650-24PD版本03.07.05.E(15.2(3)E5)
- Microsoft Windows 7计算机

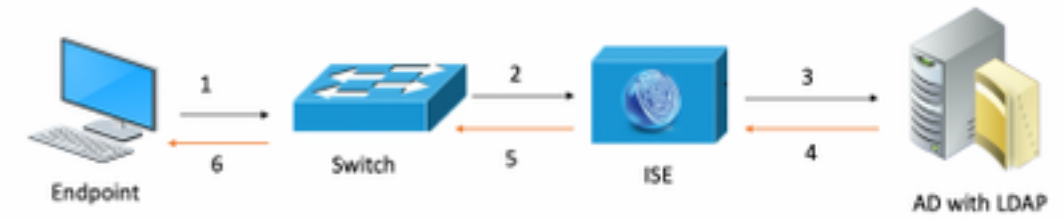
> **注意：**本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

本节介绍如何配置网络设备、ISE与LDAP之间的集成，以及最后如何配置LDAP属性以在ISE授权策略中使用。

网络图

此图显示了所使用的网络拓扑：



以下是流量，如网络图所示：

1. 用户将其pc/笔记本电脑连接到指定的交换机端口。
2. 交换机向ISE发送该用户的Radius访问请求
3. 当ISE收到信息时，它会查询LDAP服务器特定用户字段，该字段包含要在授权策略条件中使用的属性。
4. ISE收到属性（交换机端口、交换机名称和设备MAC地址）后，会比较交换机提供的信息。
5. 如果交换机提供的属性信息与LDAP提供的属性信息相同，ISE将发送RADIUS Access-Accept，其权限在授权配置文件上配置。

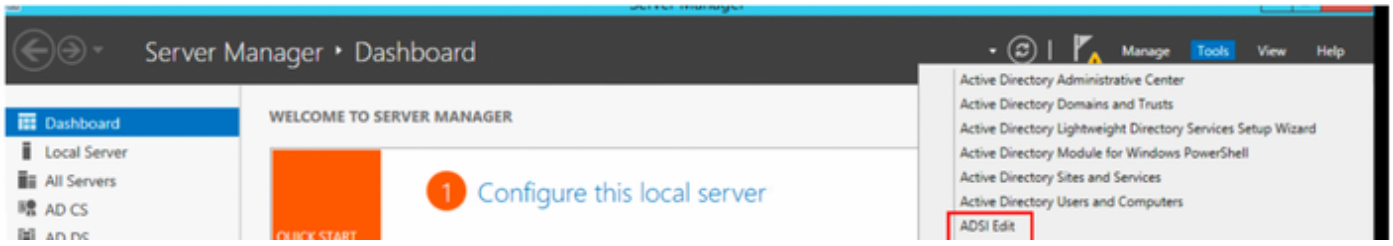
配置

使用此部分配置LDAP、交换机和ISE。

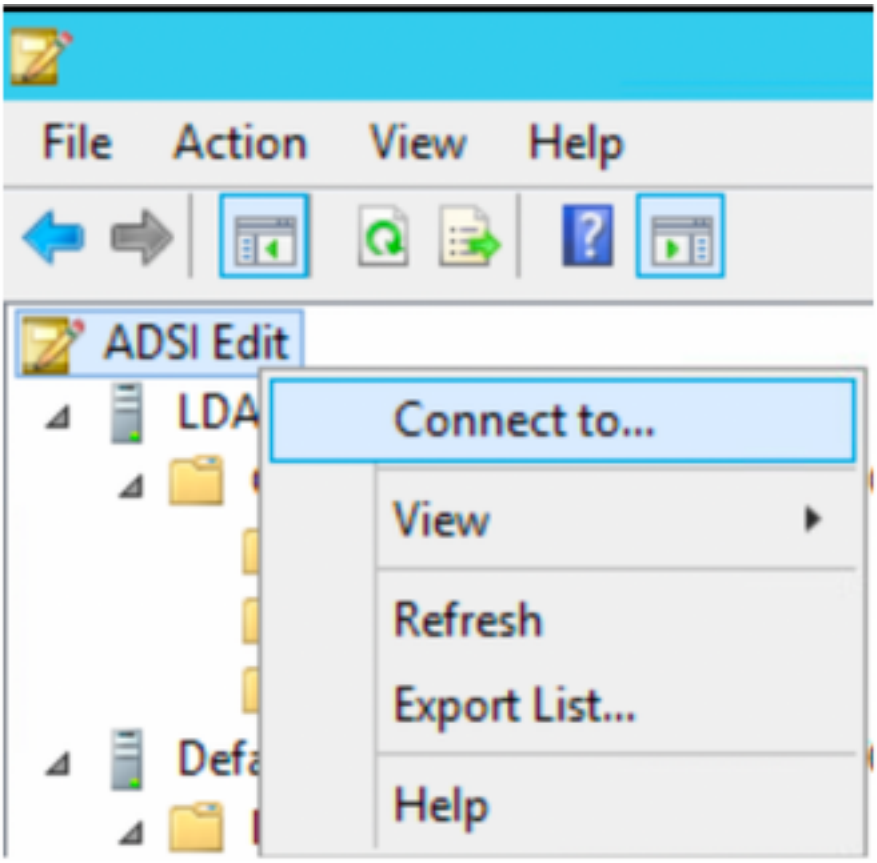
配置 LDAP

完成以下步骤以配置LDAP服务器：

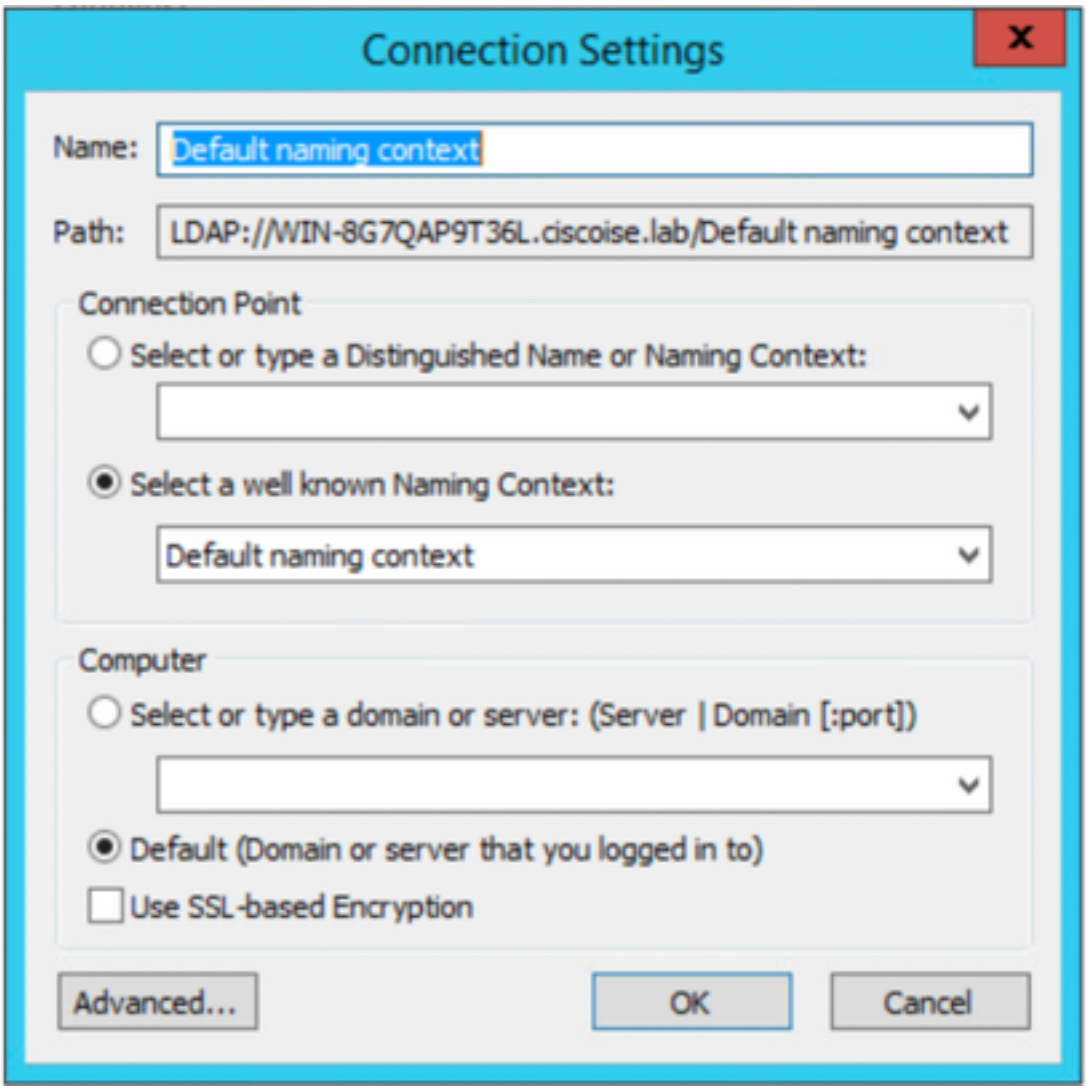
1.导航至“服务器**管理器”>“控制面板”>“工具”>“ADSI编辑”**



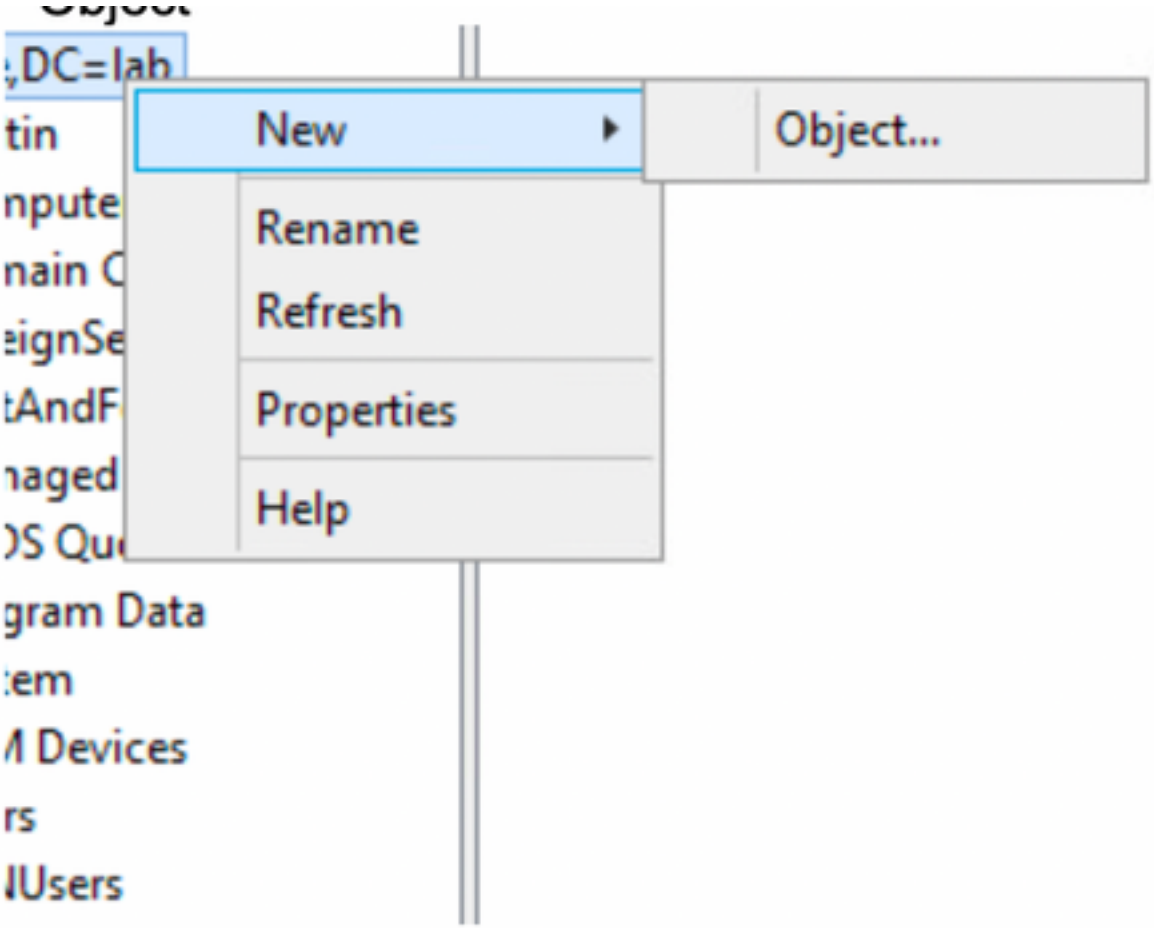
2.右键单击ADSI Edit图标并选择“连**接到……”**



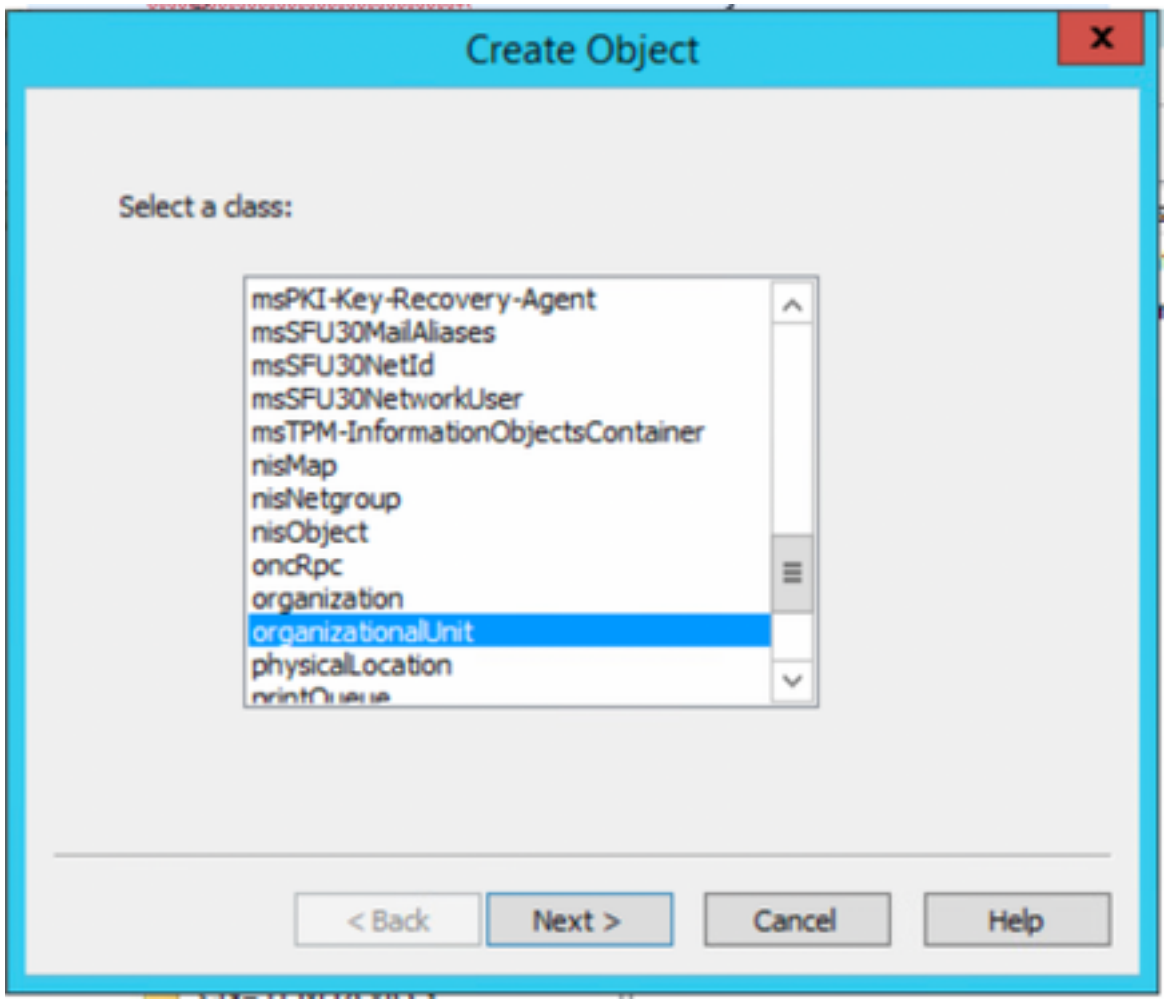
3.在“连接设置”下定义一个名称，然后选**择“**确定”按钮以启动连接。



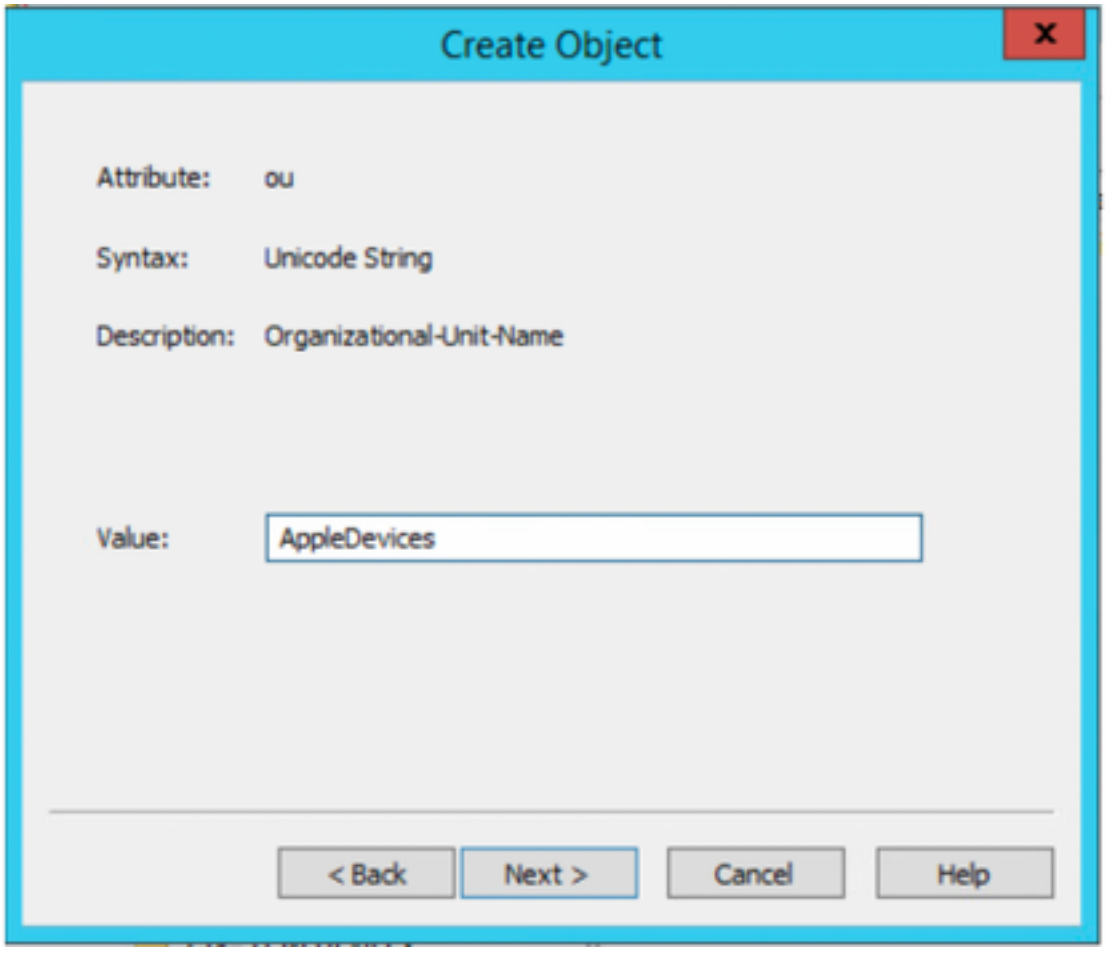
4.在DC连接中的同一ADSI Edit菜单下，右键单击(DC=ciscodemo， DC=lab)，选择New，**然后选择**Object选**项**



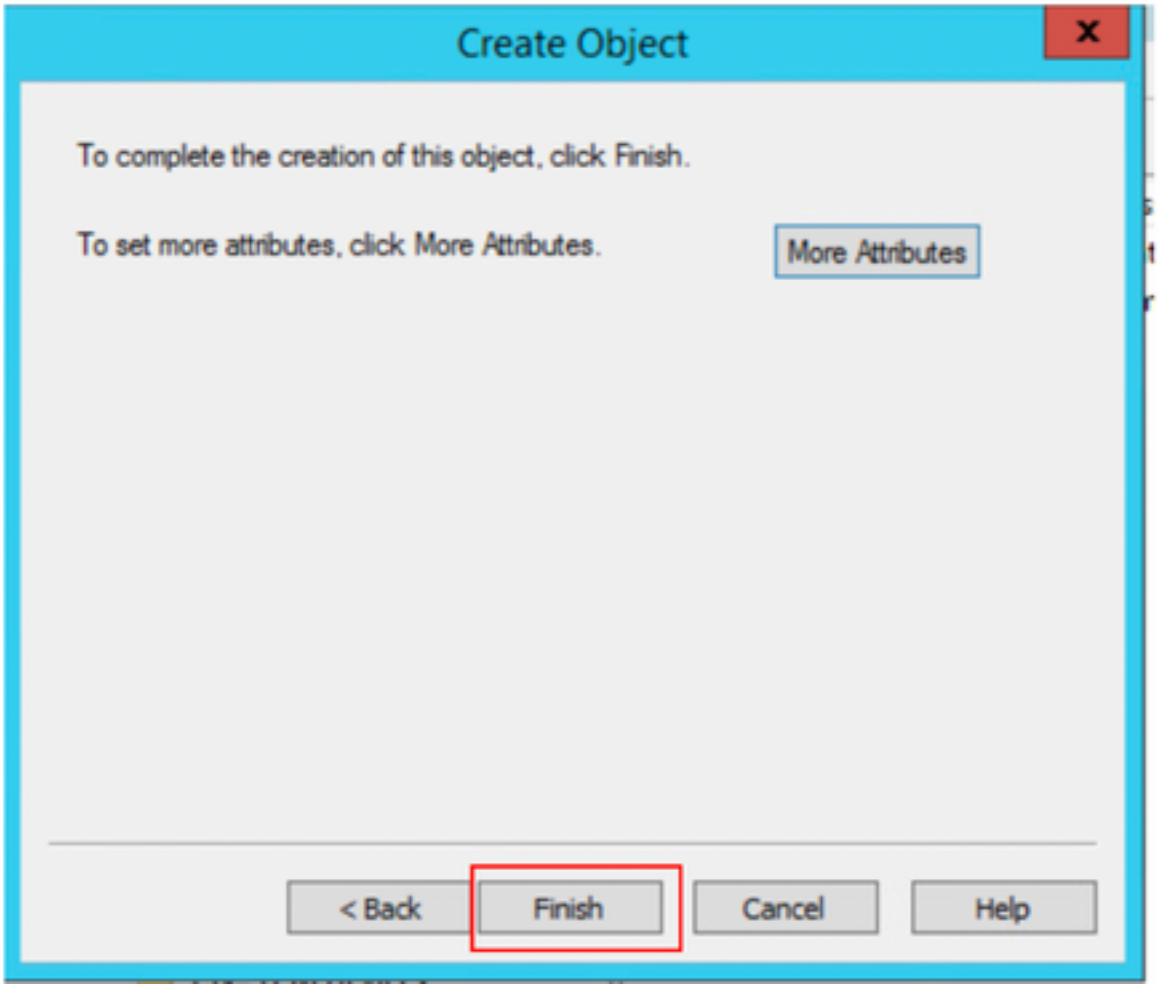
5.选择选项**OrganizationalUnit**作为新对象，然后选**择下一步。**



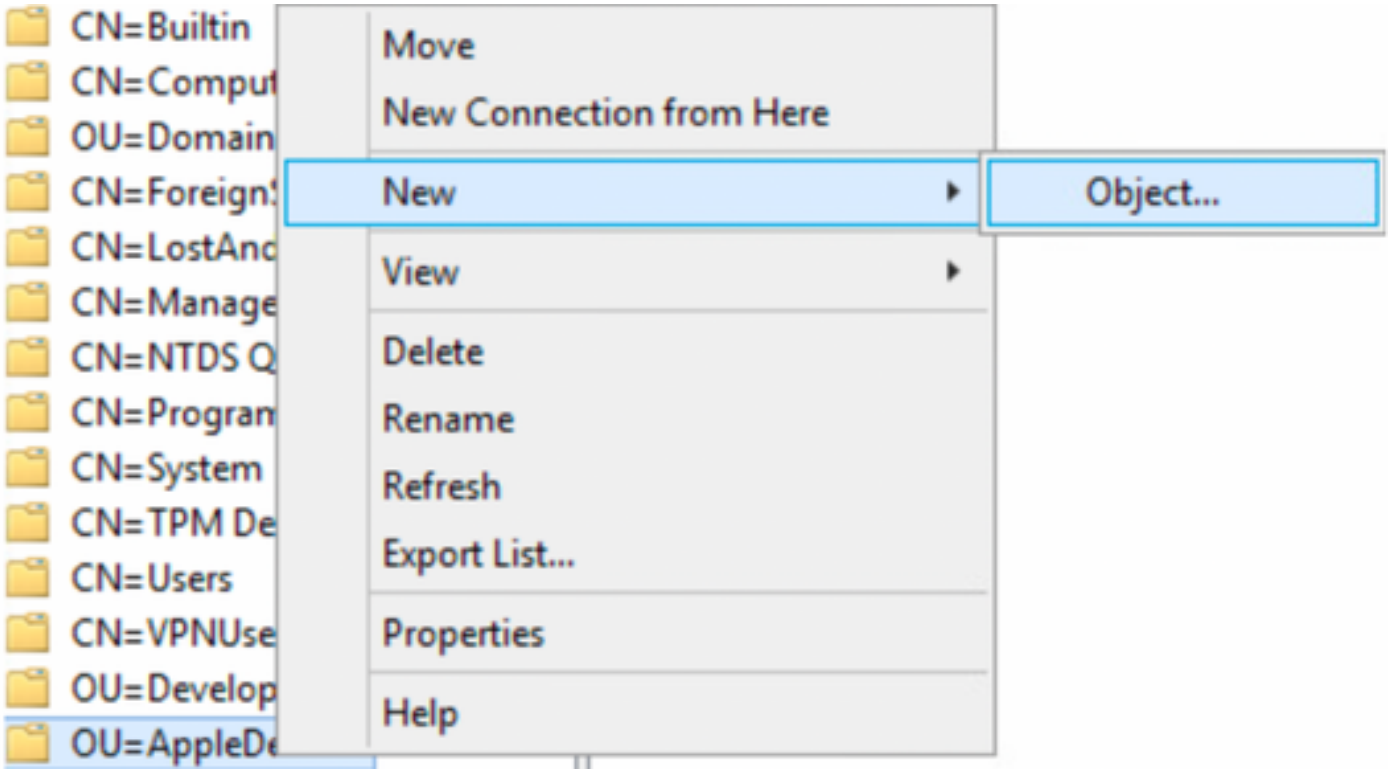
6.为新组织单位定义名称并选择“下一**步**”



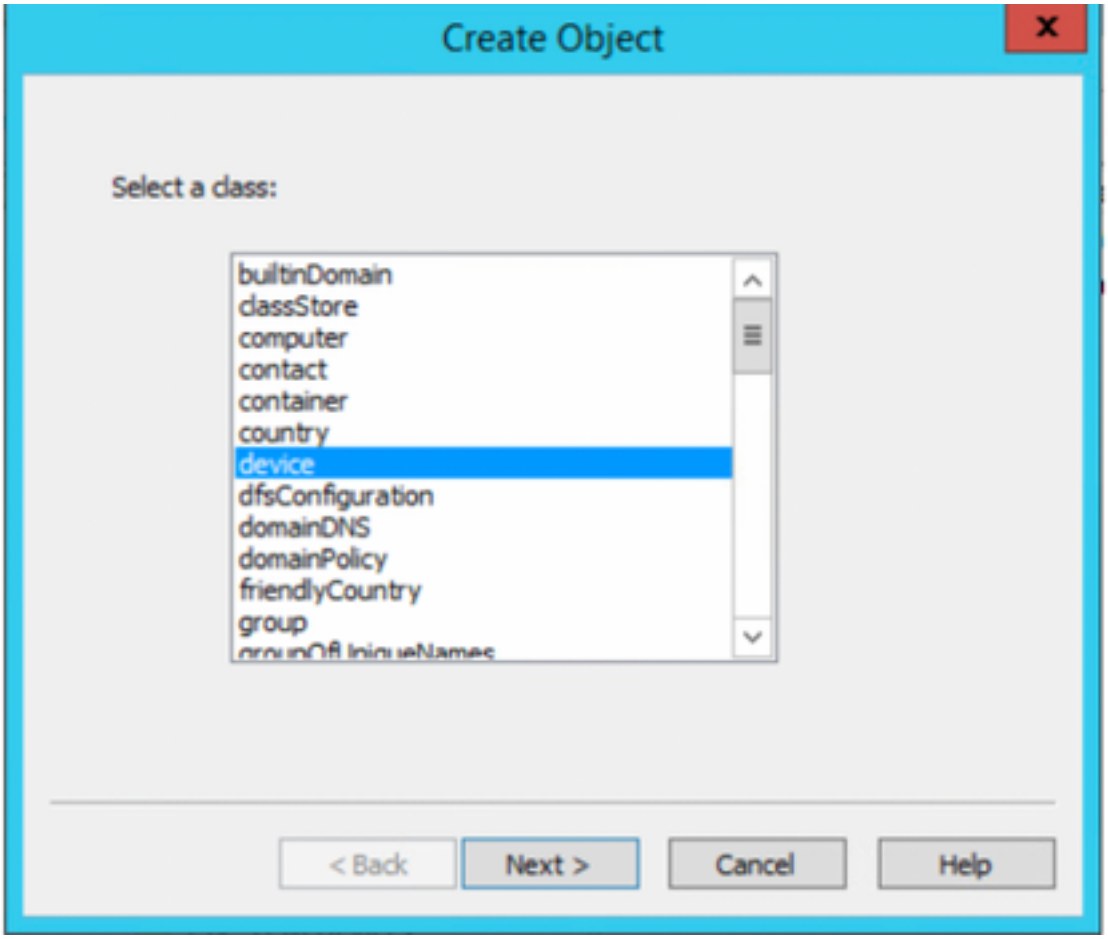
7.选择“**完成**”以创建新的组织单位



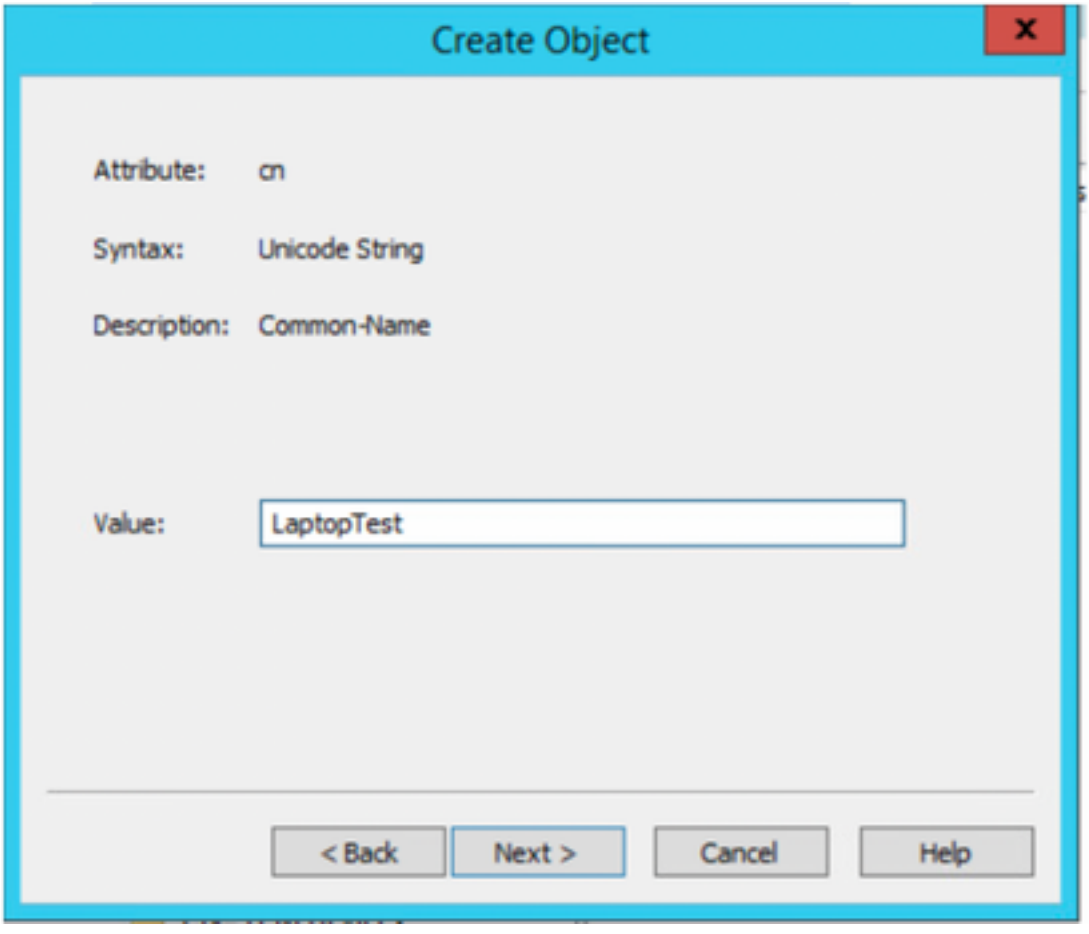
8.右键单击刚创建的OrganizationalUnit，然后选择“新建”**>“对象”**



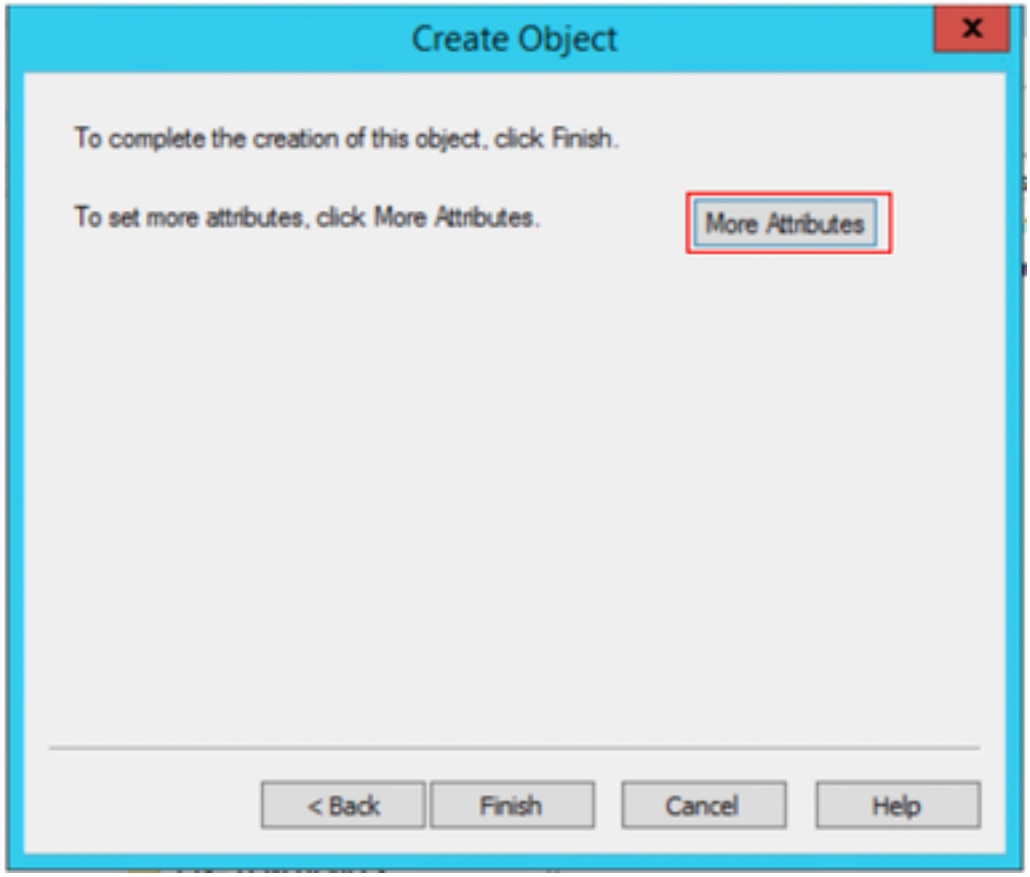
9.选择**设备**作为对象类并选择 **下一步**



10.在“值”字段中定义名称并选择“下一**步**”

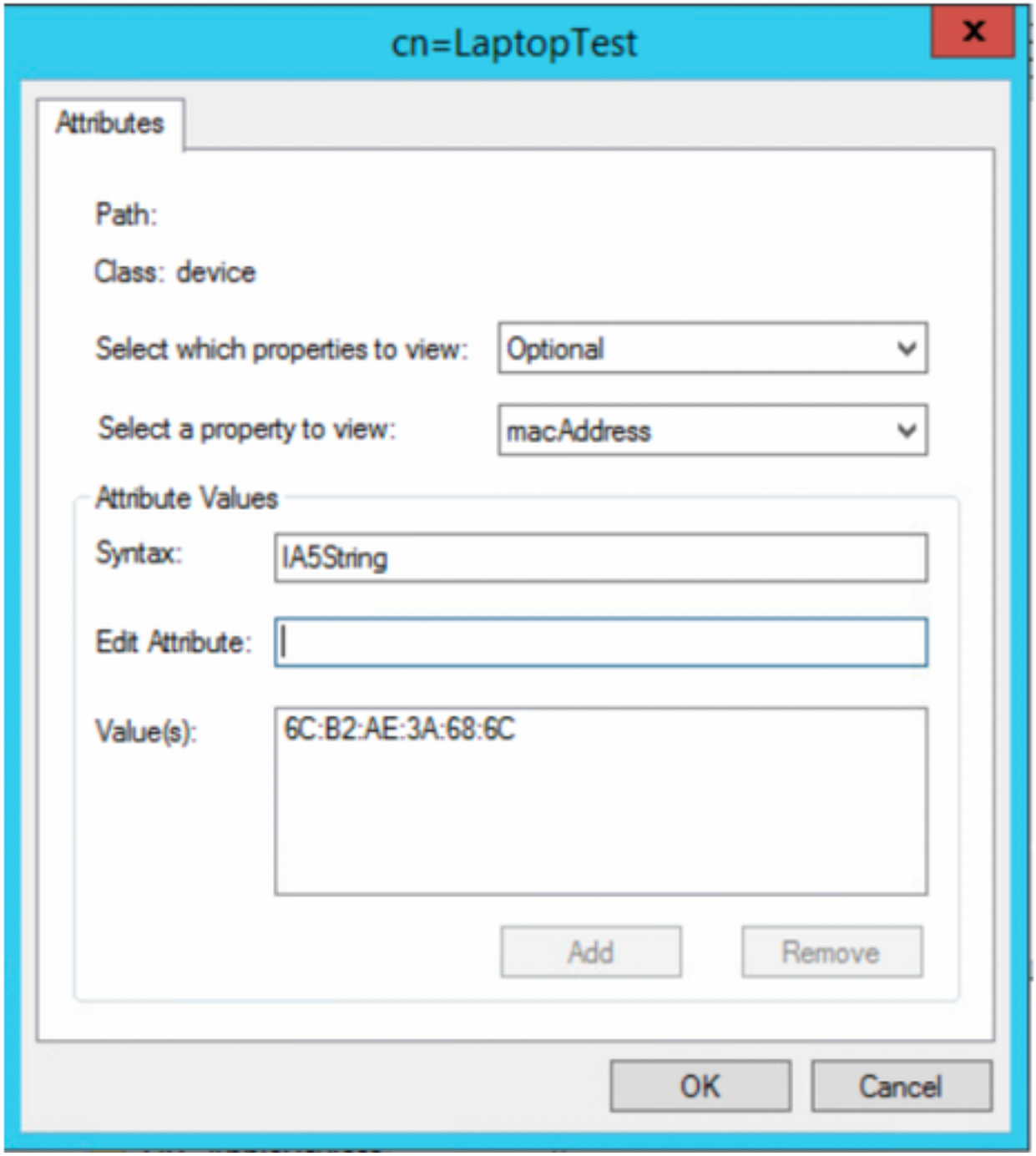


11.选择“更多属性”**选项**



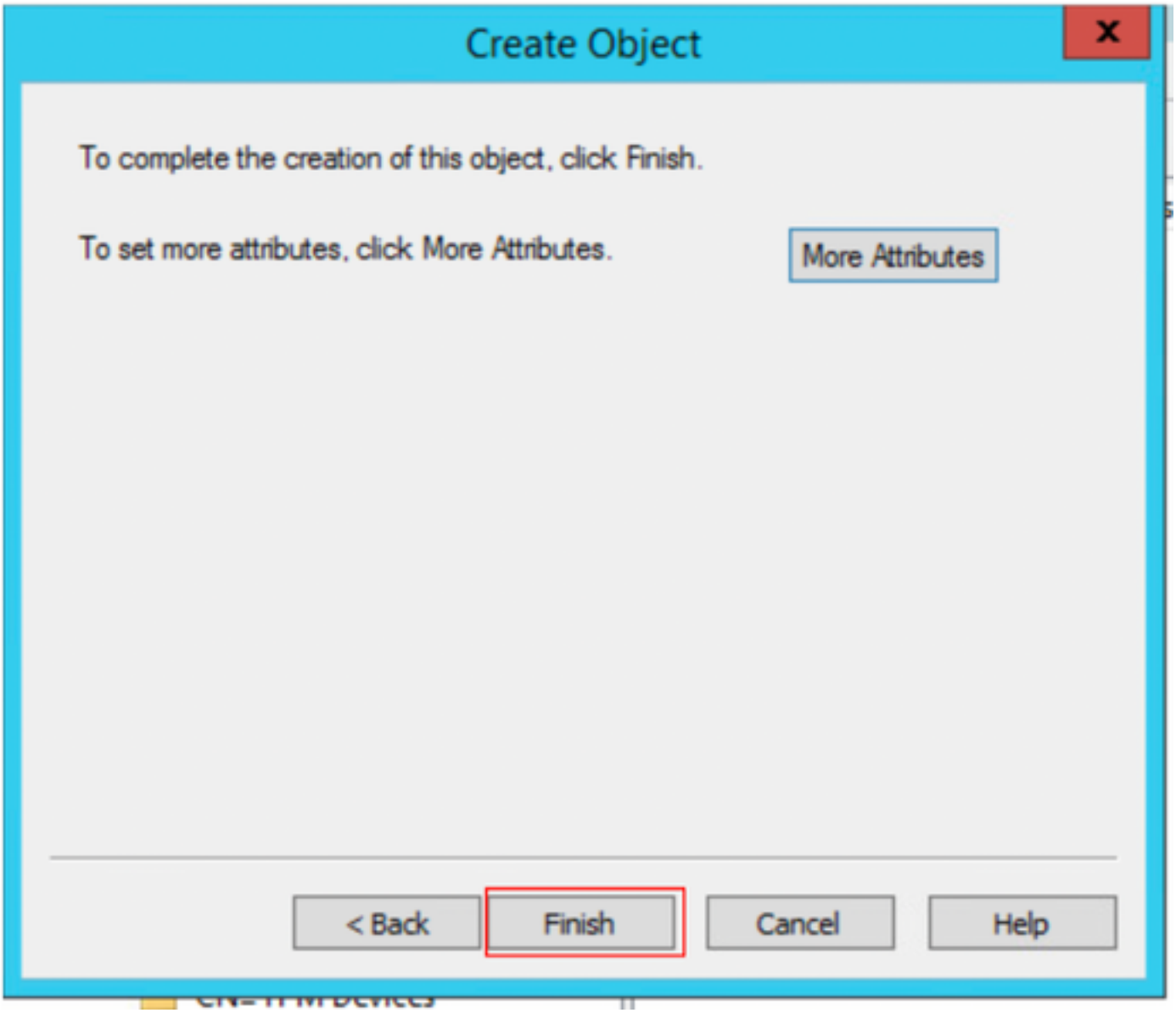
11.对于下拉菜单，**选择要查看的**属性，选**择选项macAddress，**然后在“编辑属性”字段下定义要验证的终**端Mac地址，并选**择 **添加**按钮以保存设备MAC地址。

注意: 在mac地址八位组之间使用双冒号，而不是点或连字符。

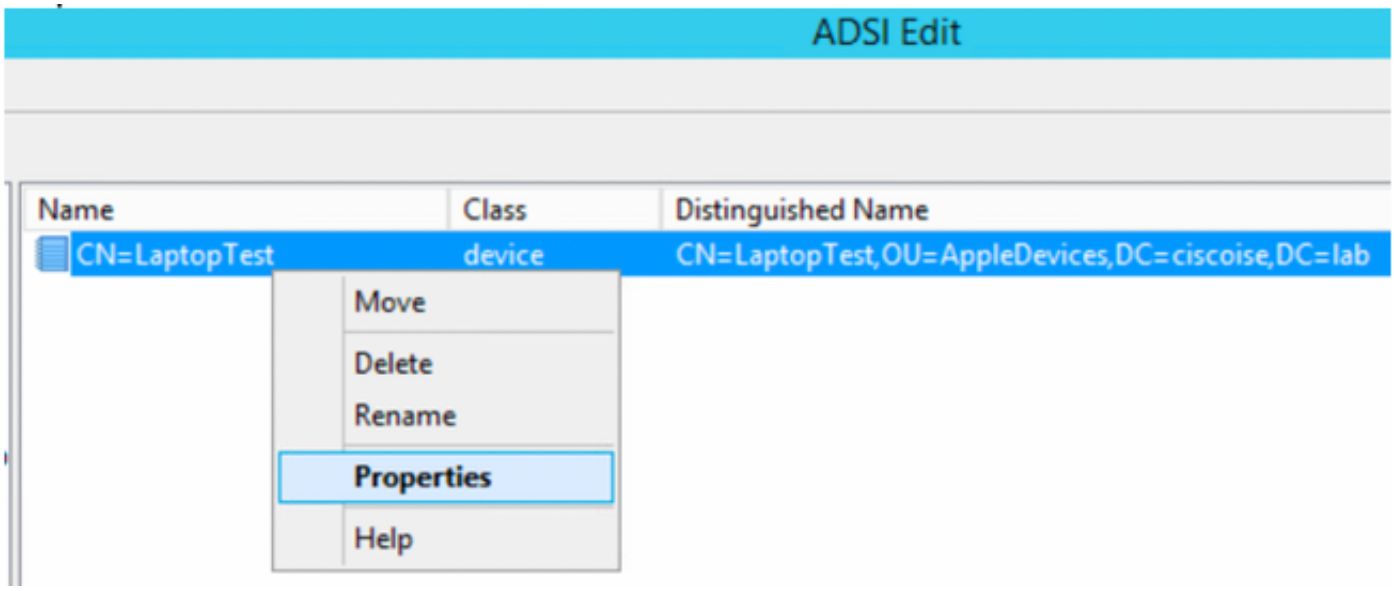


12.选择**OK**以保存信息并继续设备对象配置

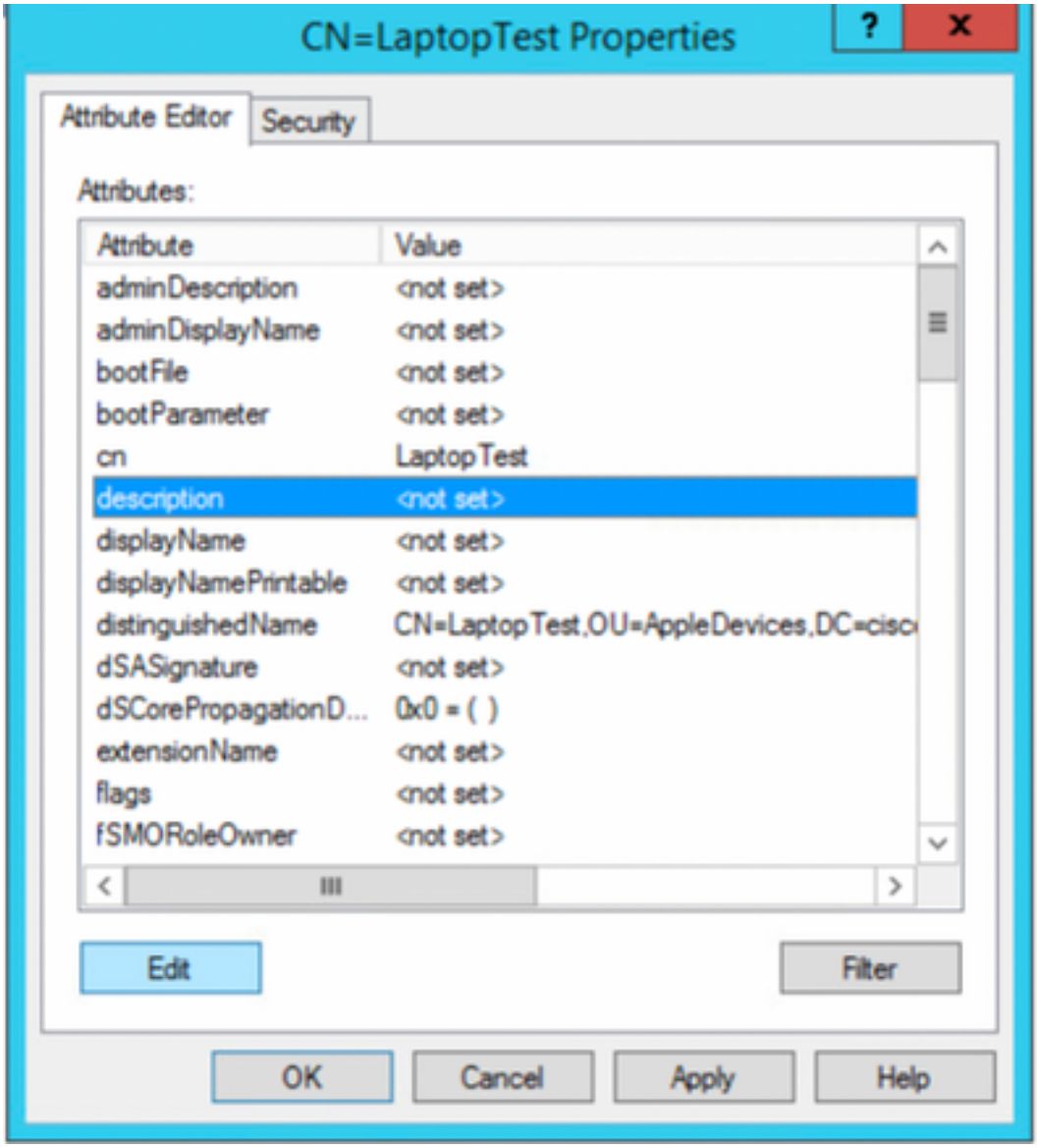
13.选择“完**成**”以创建新设备对象



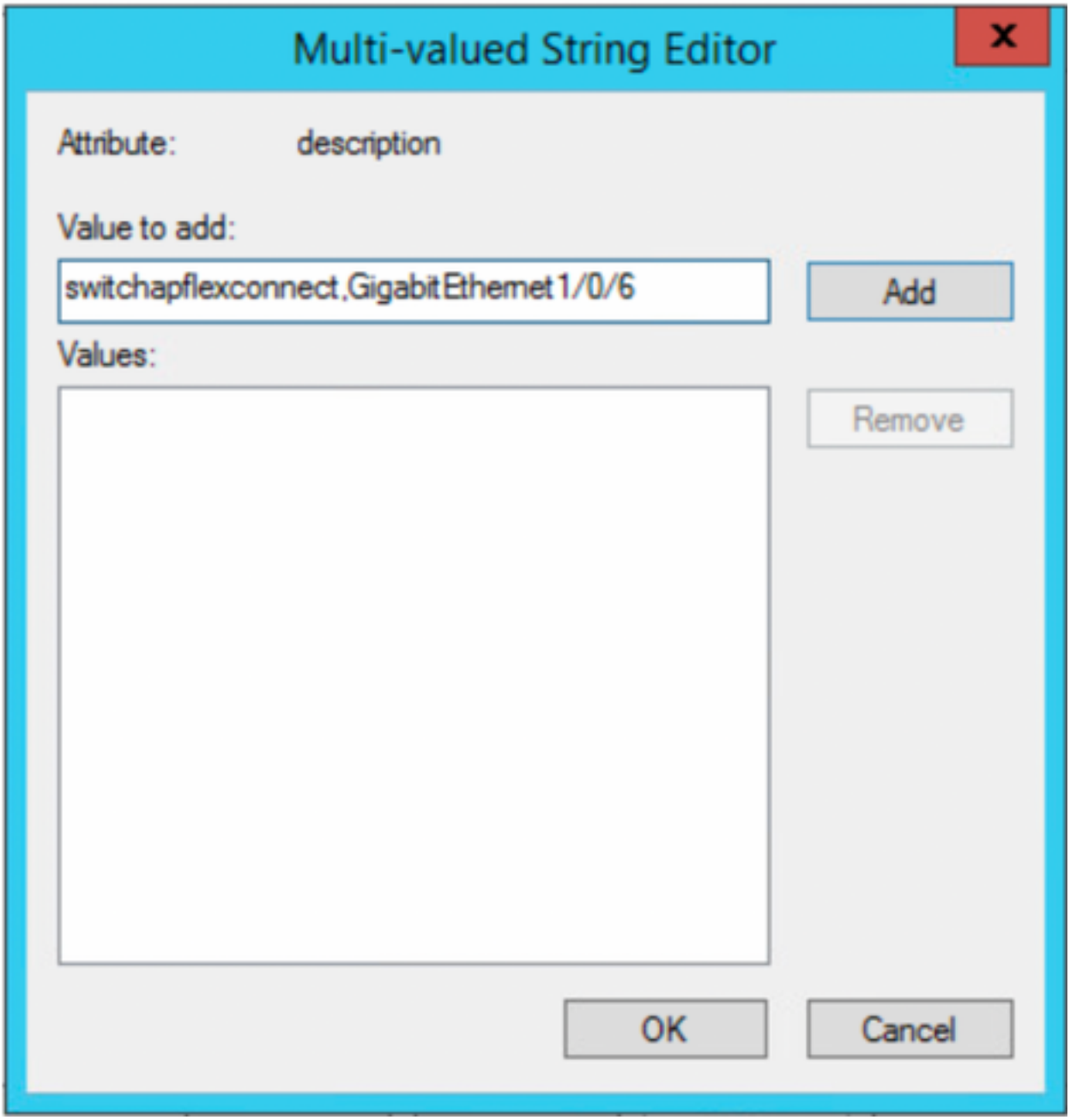
14.右键单击设备对象并选择“属性”选项



15.选择选项**说明**并选择**编辑**，以定义将连接设备的交换机名称和交换机端口。



16.定义交换机名称和交换机端口，请确保使用逗号分隔每个值。选择**添加**，然后**选择**确定以保存信息。



- **Switchapflexconnect是交换机名称。**
- **GigabitEthernet1/0/6是终端连接到的交换机端口。**

注意：可以使用脚本将属性添加到特定字段，但是，在本例中，我们将手动定义值

注意：AD属性区分大小写，如果在LDAP查询期间使用ISE转换为大写的所有Mac地址。为避免此行为，请在允许的协议下禁用进程主机查找。详细信息可在以下链接中找到：https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

交换机配置

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
```

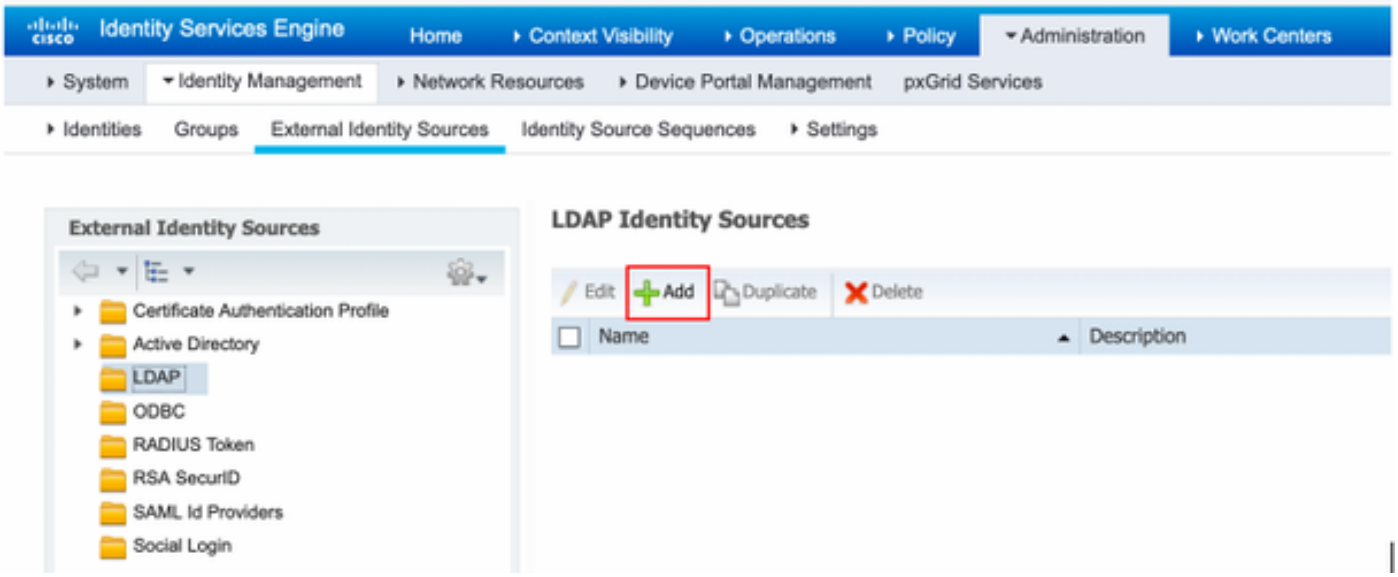
```
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access authentication event fail action next-method authentication event server
dead action authorize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

注意：可能需要在您的环境中调整全局和接口配置

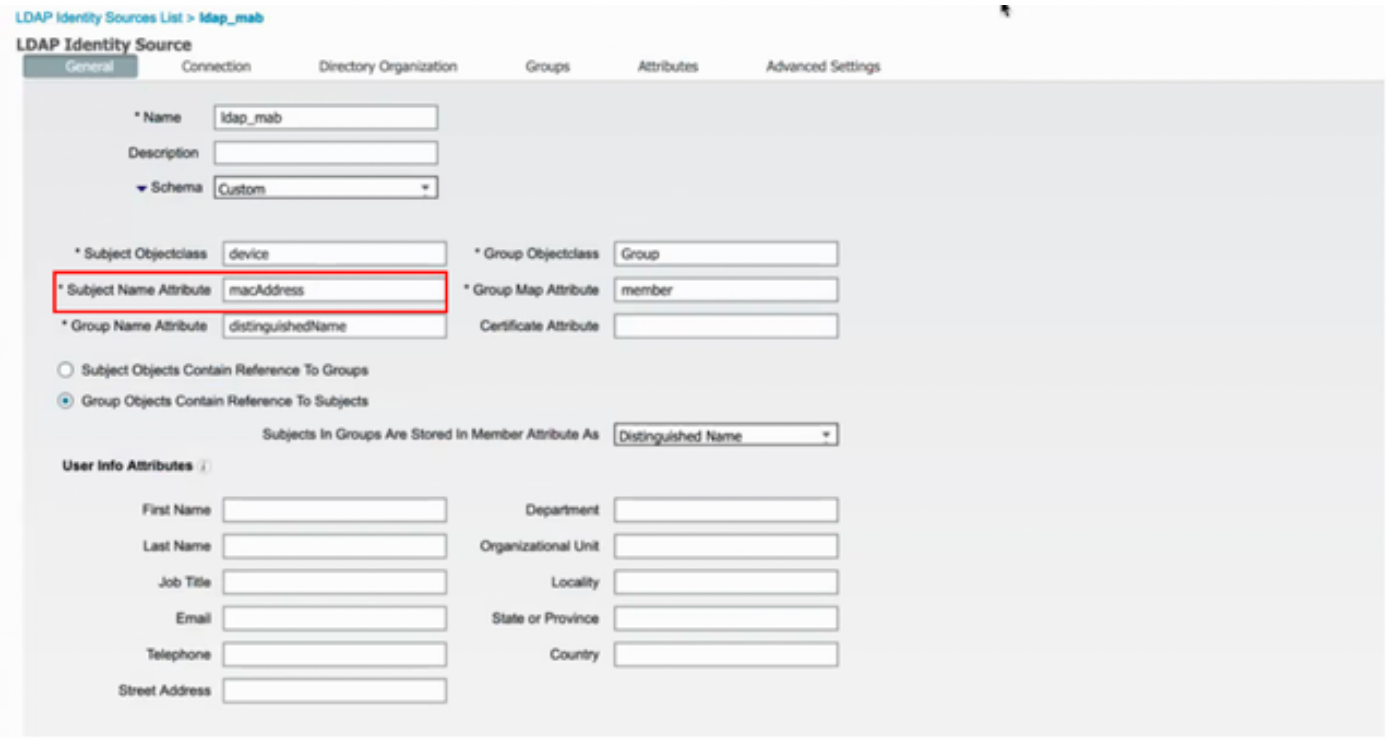
ISE配置

以下描述ISE上的配置，以从LDAP服务器获取属性并配置ISE策略。

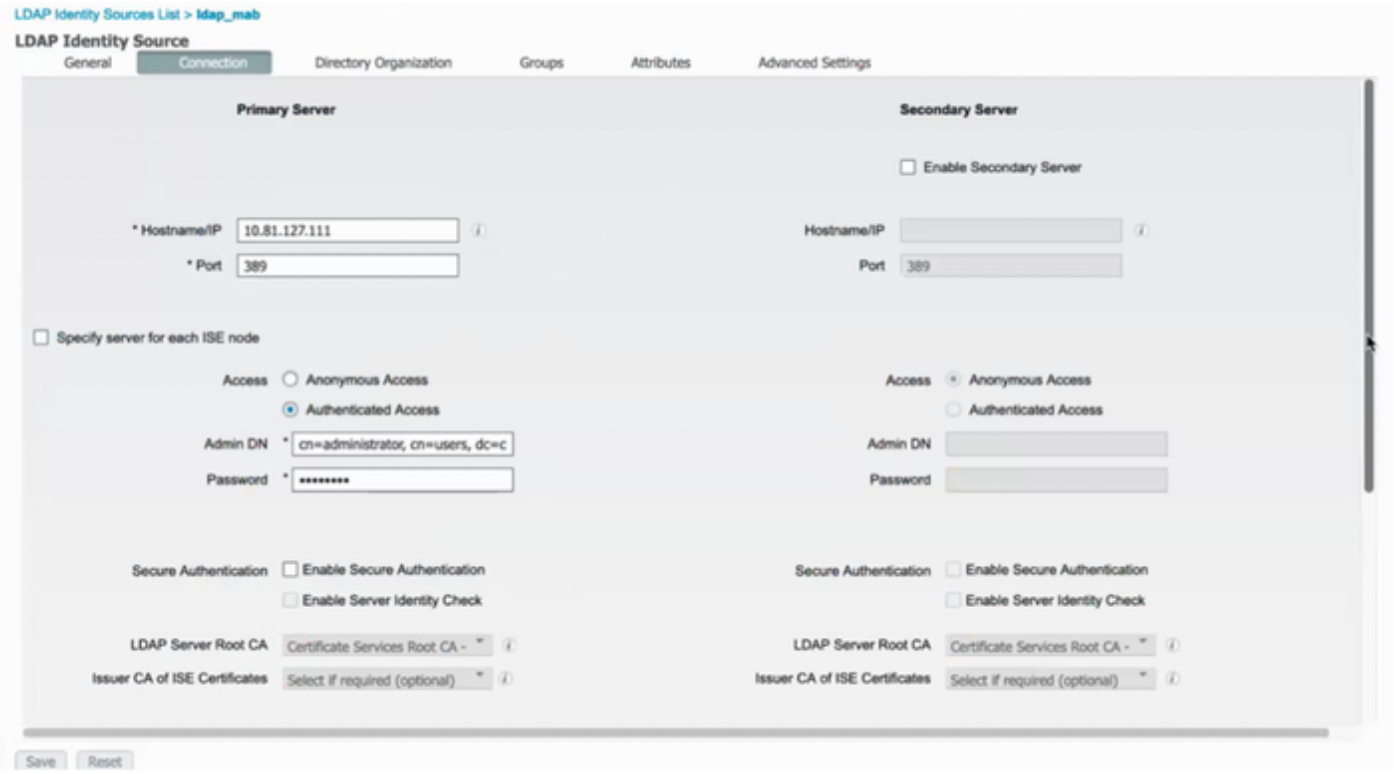
1. 在ISE上，转到**Administration -> Identity Management -> External Identity Sources**并选择**LDAP**文件夹，然后单击**Add** 以创建与LDAP的新连接



2.在“常规”选项卡下定义一个名称，并选择mac地址作为“主题名称属性”

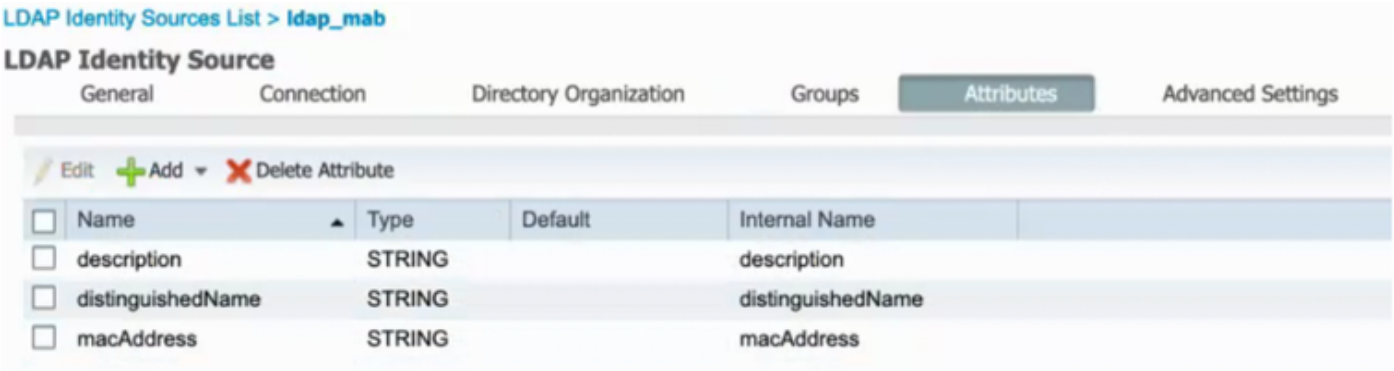


3.在“连接”**选项卡**下，配置LDAP服务器的IP地址、管理DN和密码，以便成功连接。

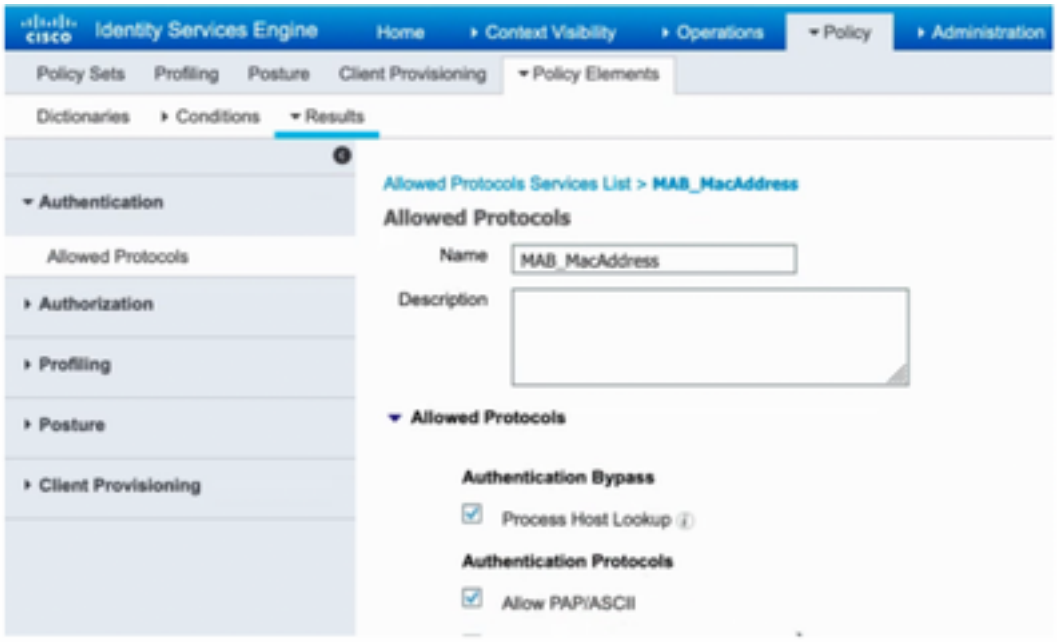


注意：端口389是使用的默认端口。

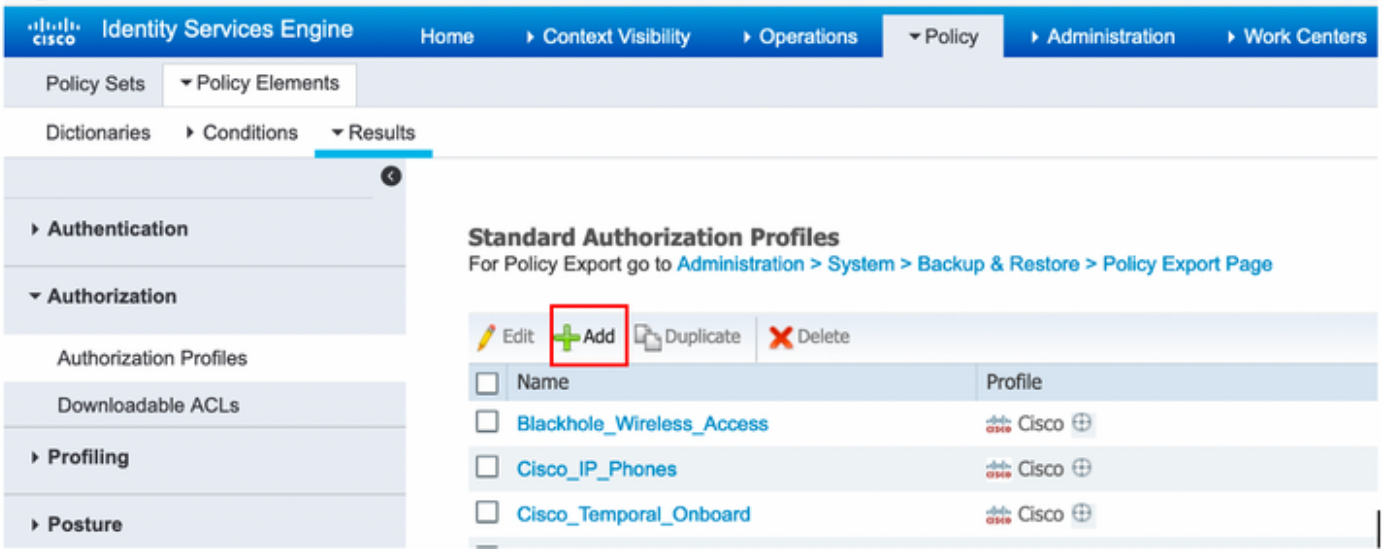
4.在“属性”选**项**卡下，选择macAddress和说明属性，这些属性将用于授权策略

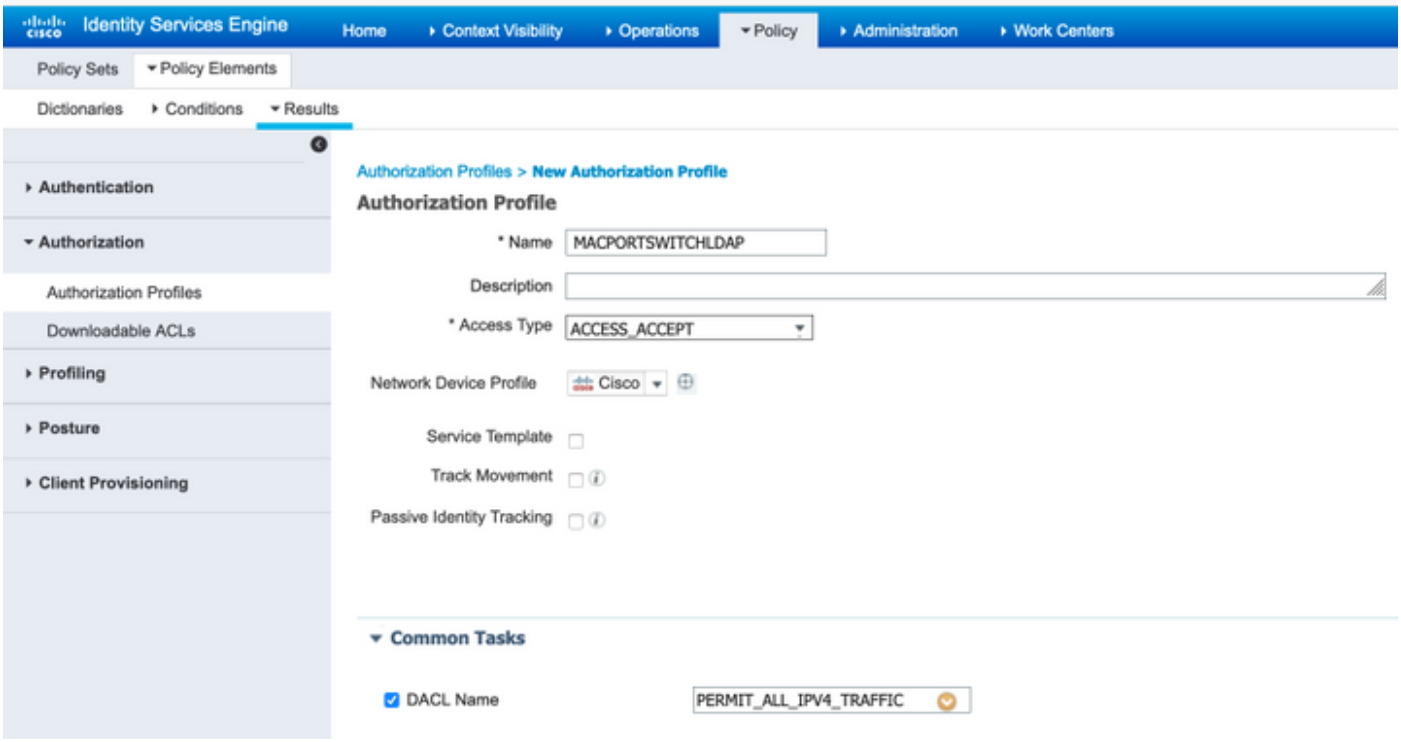


5.要创建允许的协议，请转到**Policy->Policy Elements->Results->Authentication->Allowed Protocols。**定义并选择进程主机查找和允许PAP/ASCII作为唯一允许的协议。最后选择“**保存”**

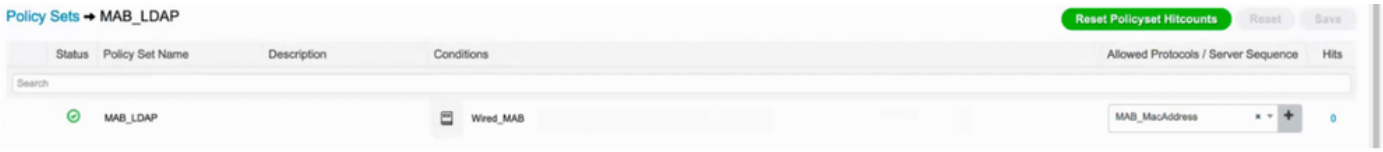


6.要创建授权配置文件，请转至**Policy->Policy Elements->Results->Authorization->Authorization Profiles。选择Add**并定义将分配给终端的权限。

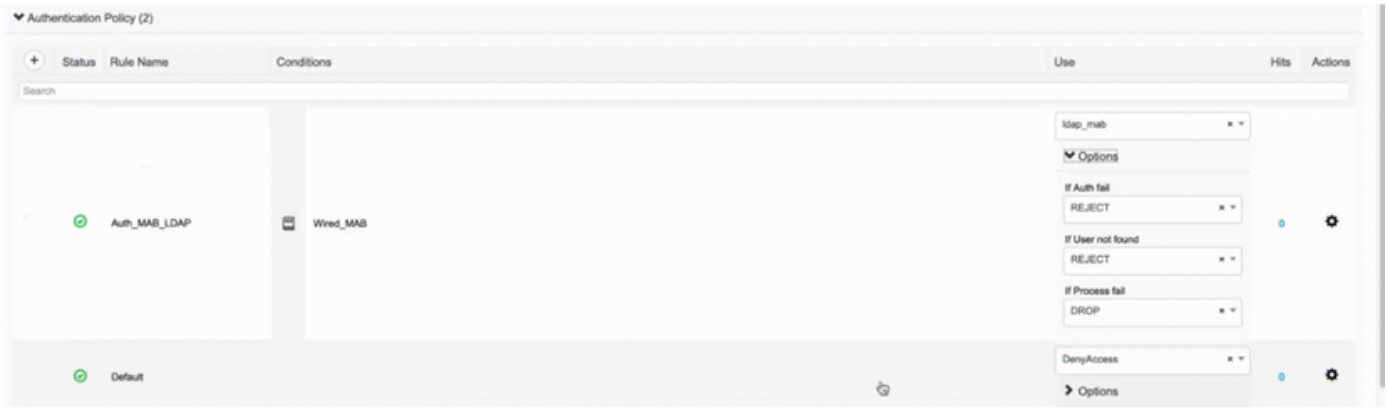




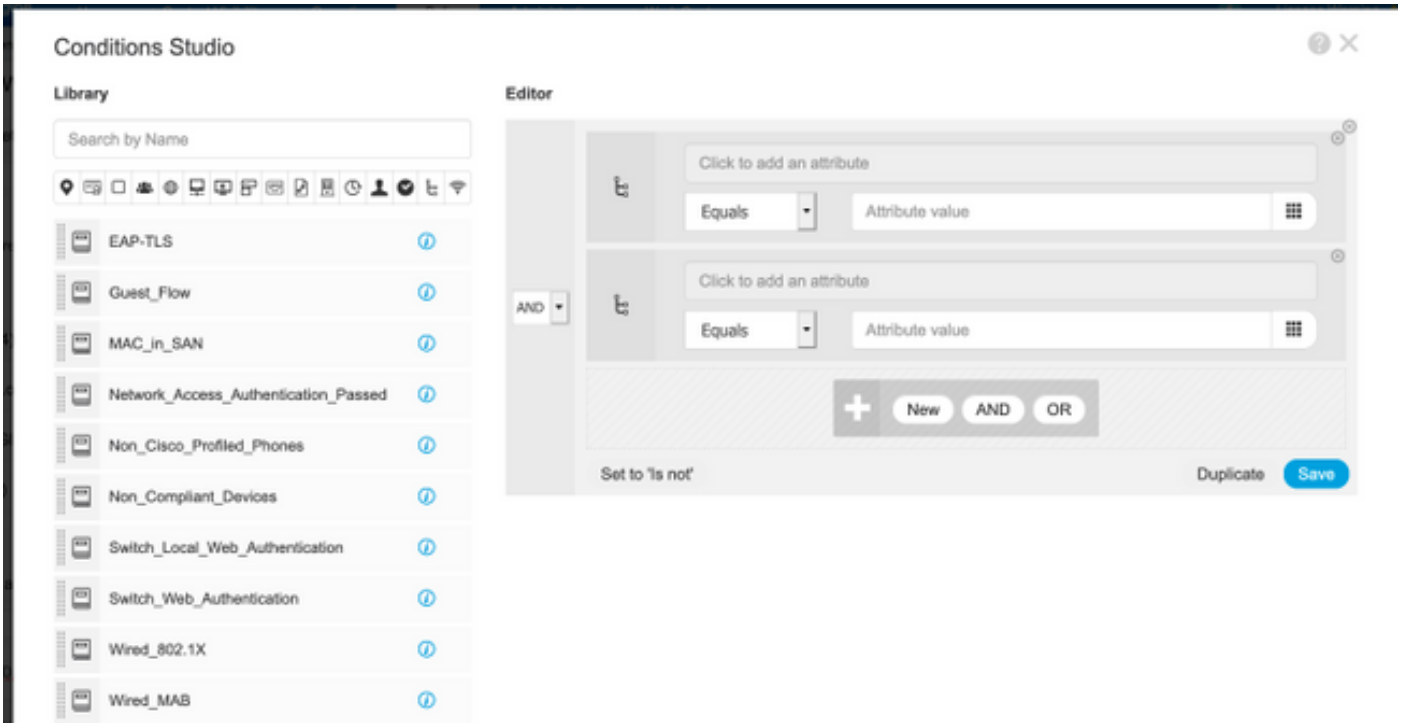
7.转到Policy-> Policy Set，使用预定义条件Wired_MAB和步骤5中创建的Allowed Protocol创建策略集。

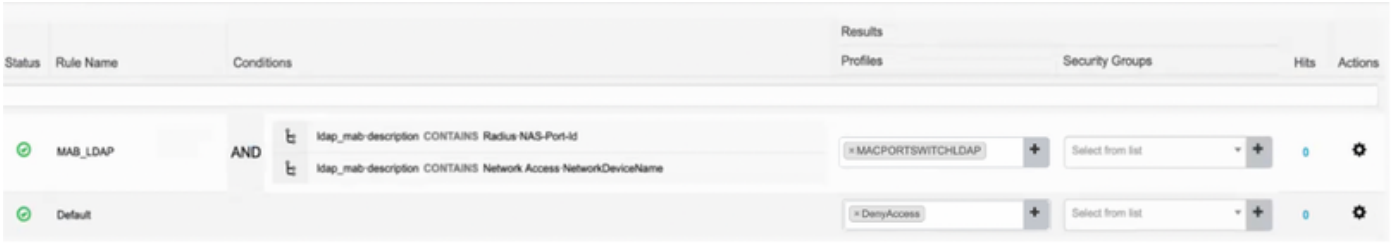


8.在新创建的策略集下，使用预定义的Wired_MAB库和LDAP连**接作为外**部身份**源序**列创建身份验证策略



9.在授权策**略下**，使用LDAP属性说明、Radius NAS-Port-Id和NetworkDeviceName定义名称并创建复合条件。最后，添加在步骤6中创建的授权配置文件。





应用配置后，您应该能够连接到网络，而无需用户干预。

验证

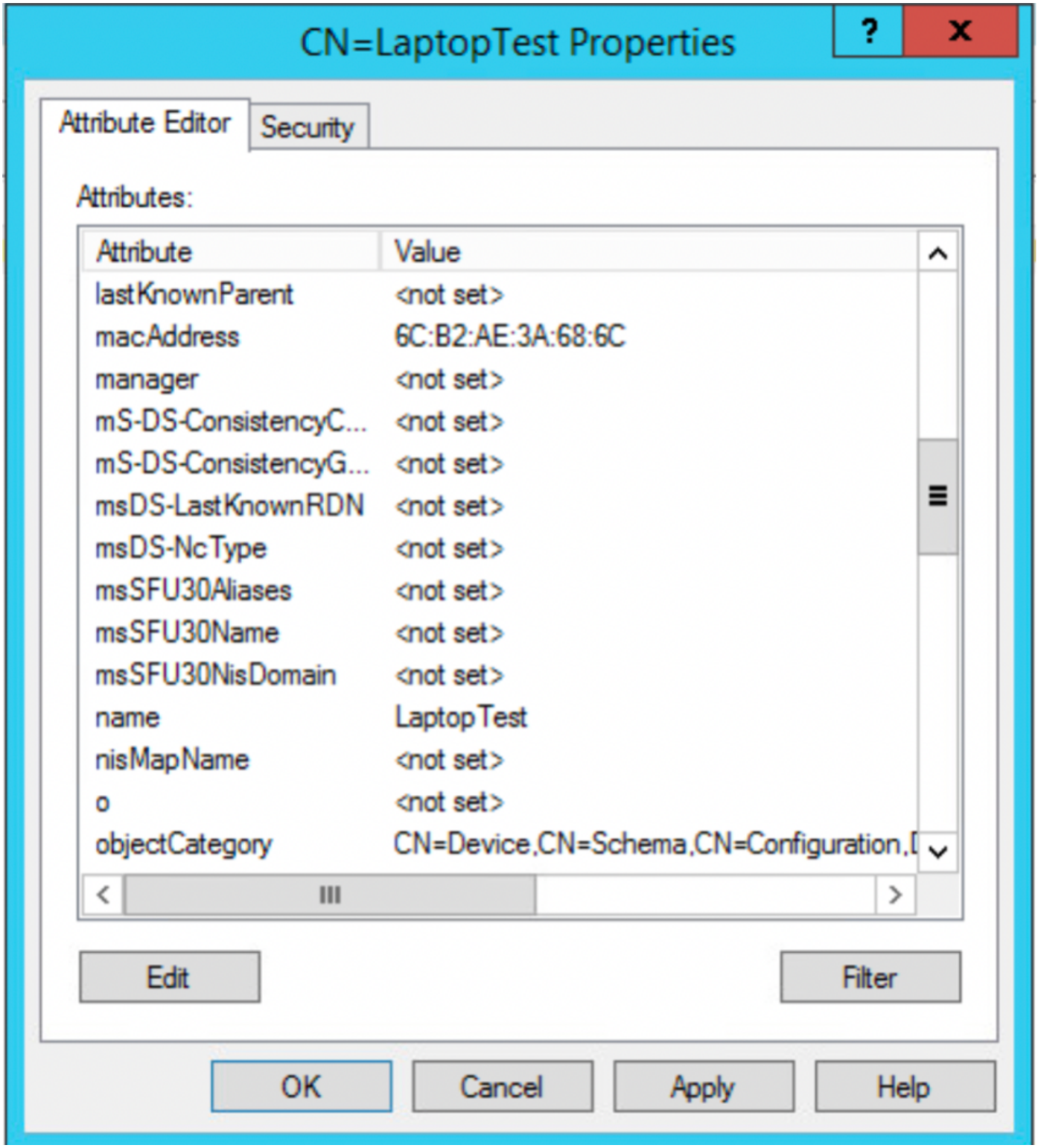
连接到指定的交换机端口后，您可以键入**show authentication session interface GigabitEthernet X/X/X details** ，以验证设备的身份验证和授权状态。

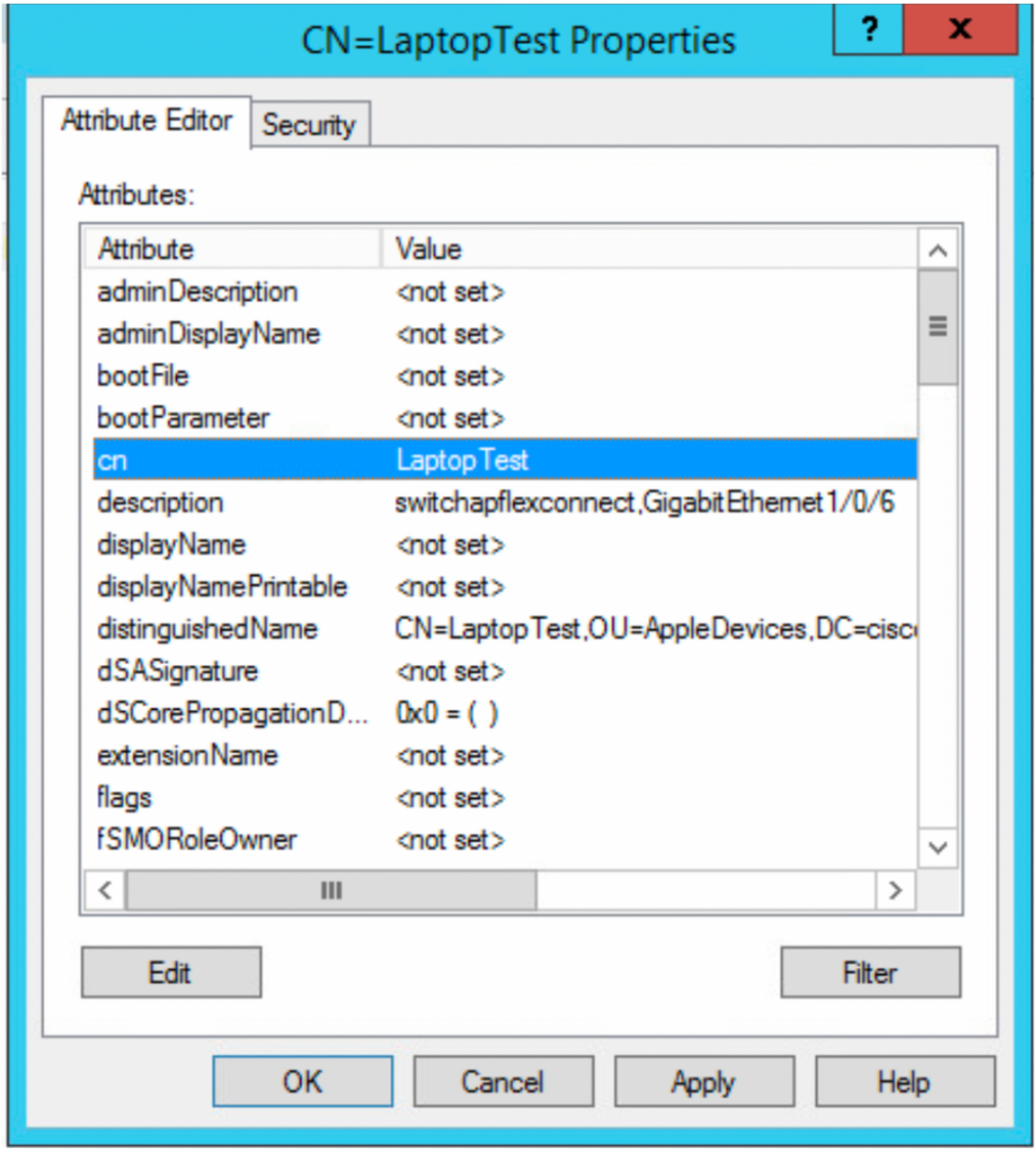
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session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

故障排除

在LDAP服务器上，验证创建的设备是否配置了Mac地址、正确的交换机名称和交换机端口


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，您可以执行数据包捕获(转到**操作 — >故障排除 — >诊断工具 — >TCP转储**)以验证从LDAP发送到ISE的值