ISE and LDAP Attributes Based Authentication

Contents

Introduction

This document describes how to configure Cisco Identity Services Engine (ISE) and use Lightweight Directory Access Protocol (LDAP) objects attributes to authenticate and authorize devices dynamically.

Note: This document is valid for setups that use LDAP as the external identity source for the ISE authentication and authorization.

Contributed by Emmanuel Cano and Mauricio Ramos Cisco Professional Services Engineer.

Edited by Neri Cruz Cisco TAC engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the following topics:

- Basic knowledge of ISE policy sets, authentication, and authorization policies
- Mac Authentication Bypass (MAB)
- Basic knowledge of Radius protocol
- Basic knowledge of Windows server

Components Used

The information on this document is based on the following software and hardware versions:

- Cisco ISE, Version 2.4 patch 11
- Microsoft Windows Server, Version 2012 R2 x64
- Cisco Switch Catalyst 3650-24PD, Version 03.07.05.E (15.2(3)E5)
- Microsoft Windows 7 machine

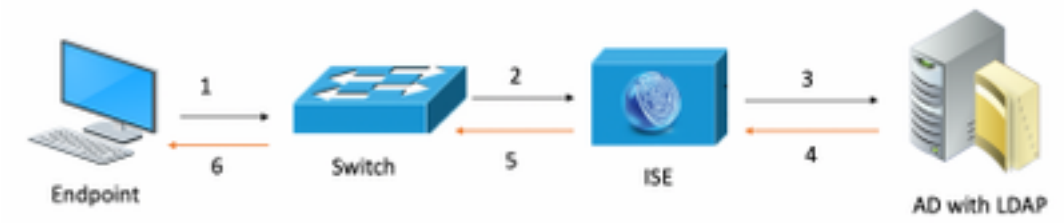
Note: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

This section describes how to configure the network devices, the integration between ISE and LDAP, and finally to configure LDAP attributes to be used in ISE Authorization Policy.

Network Diagram

This image illustrates the network topology that is used:



Here is the traffic flow, as illustrated in the network diagram:

1. The user connects its pc/laptop to the designated switch port.
2. The switch sends a Radius Access-Request for that user to the ISE
3. When the ISE receives the information it queries the LDAP server for the specific user filed, which contains the attributes to be used in the authorization policy conditions.
4. Once the ISE receives the attributes (the switch port, switch name, and device mac address) it compares the information provided by the switch.
5. If the attributes information provided by the switch are the same that those provided by LDAP, the ISE will send a RADIUS Access-Accept with the permissions configured on the authorization profile.

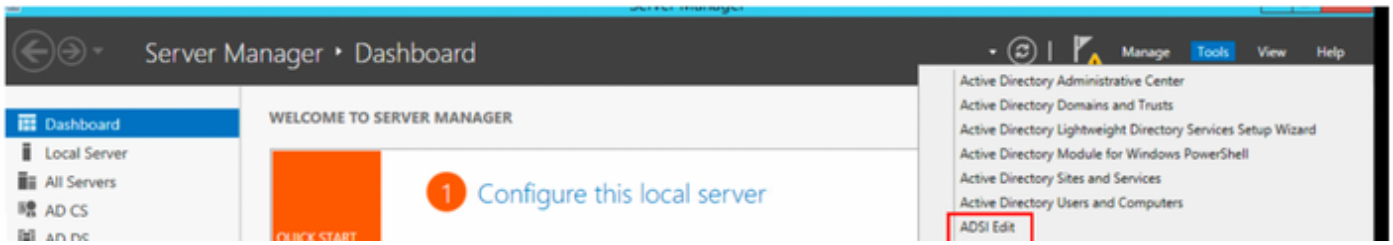
Configurations

Use this section in order to configure the LDAP, switch and the ISE.

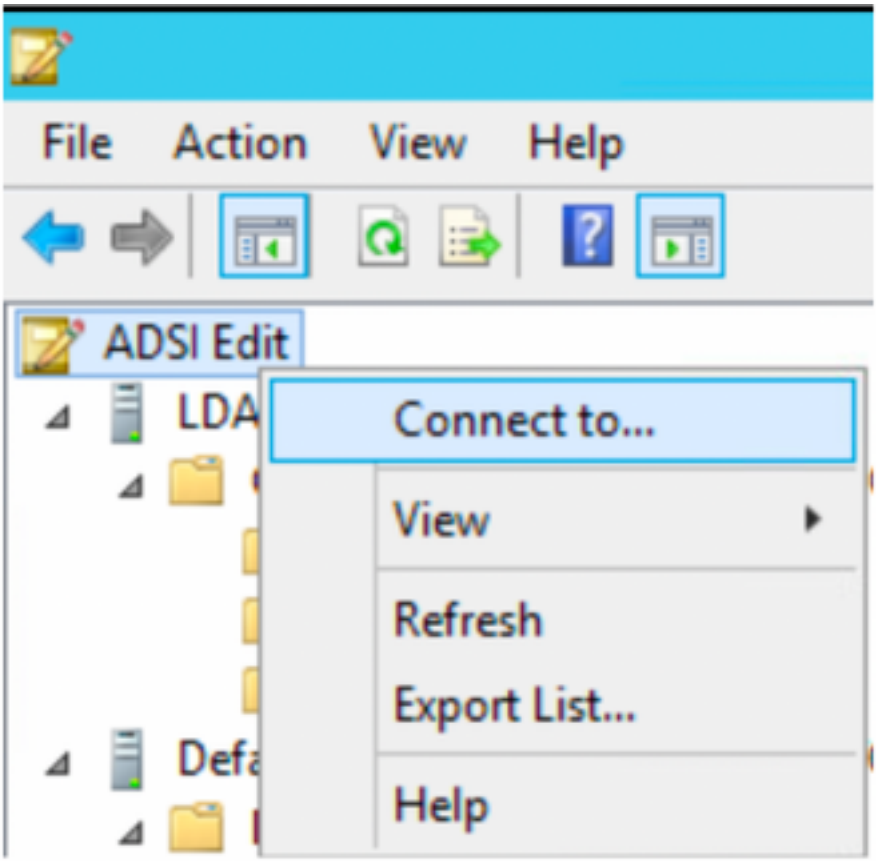
Configure LDAP

Complete the following steps to configure the LDAP server:

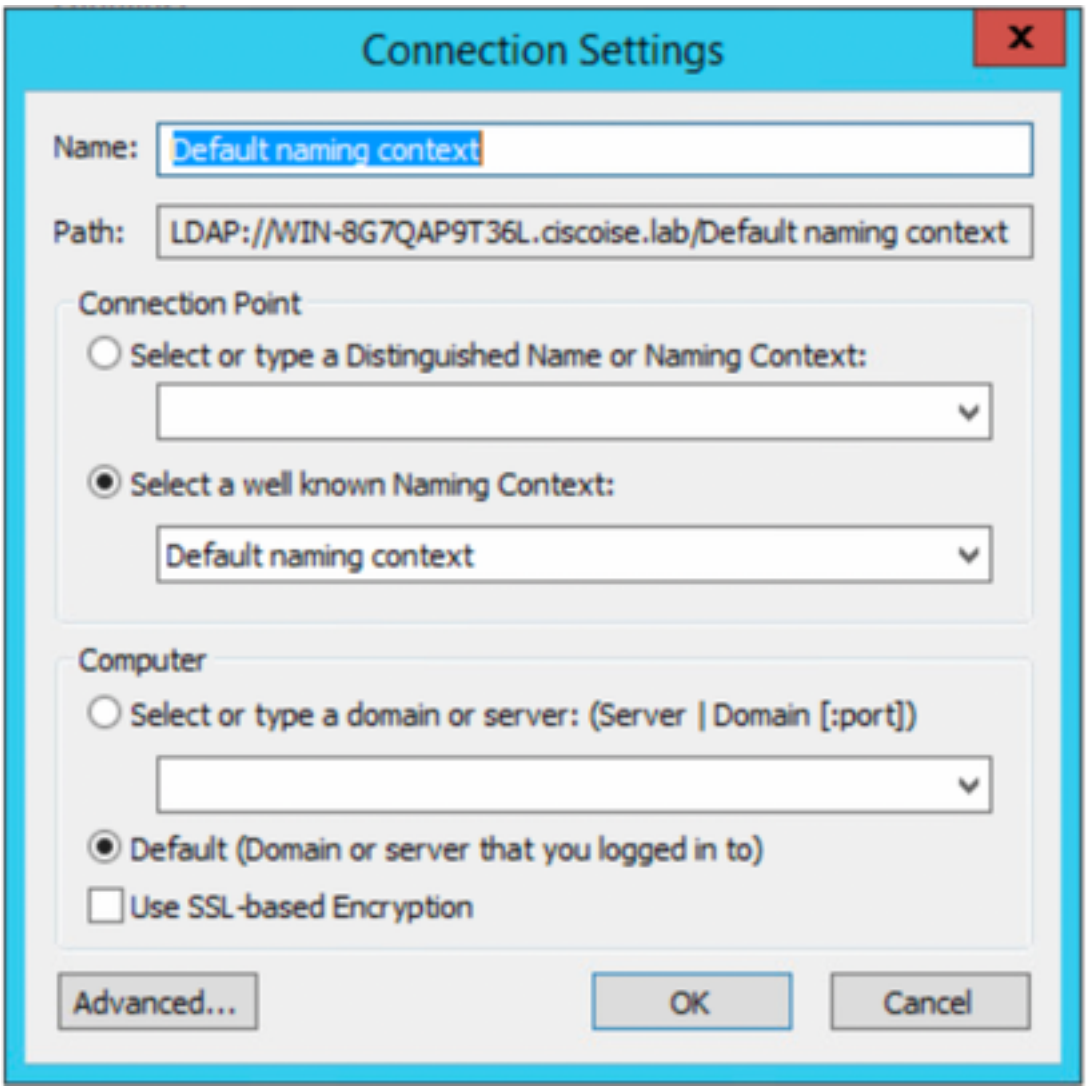
1. Navigate to **Server Manager > Dashboard > Tools > ADSI Edit**



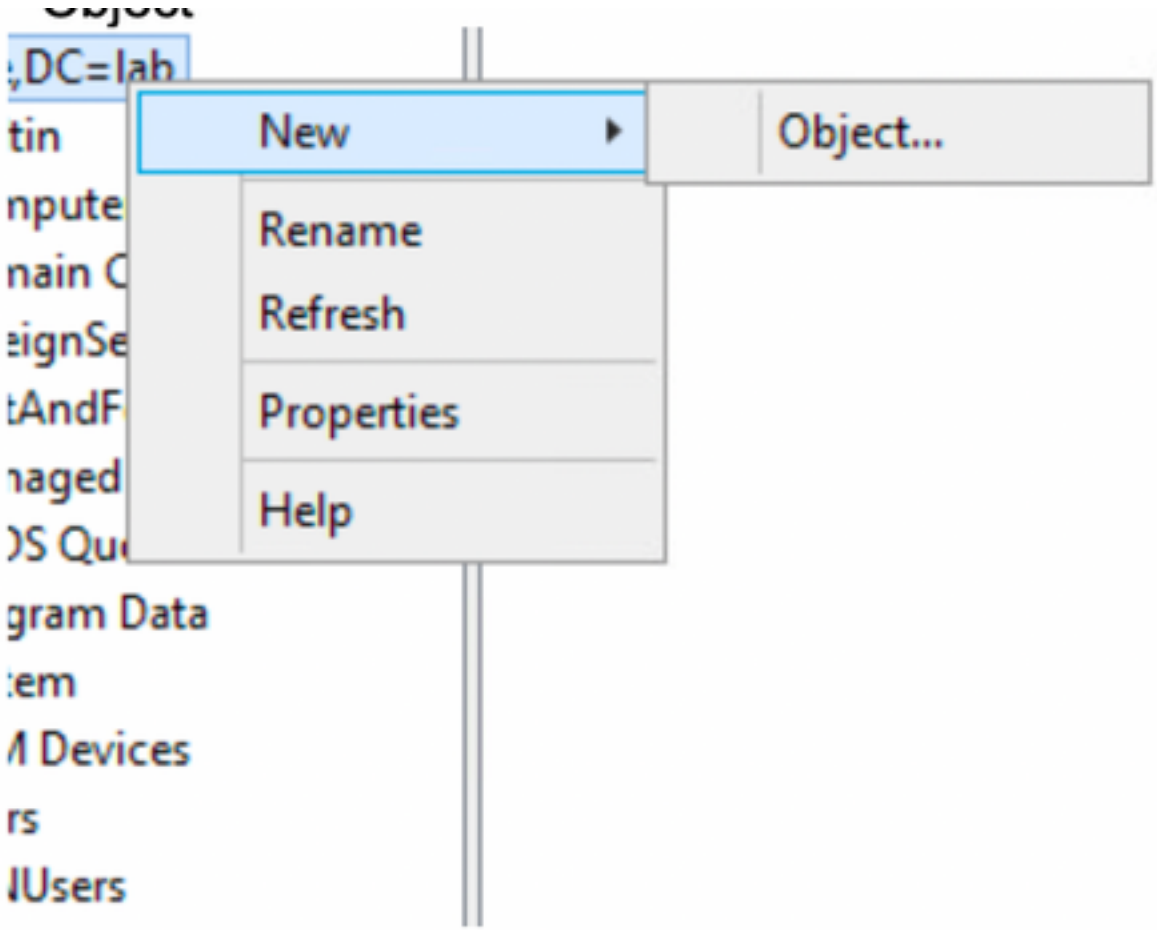
2. Right-click on the ADSI Edit icon and select **Connect to...**



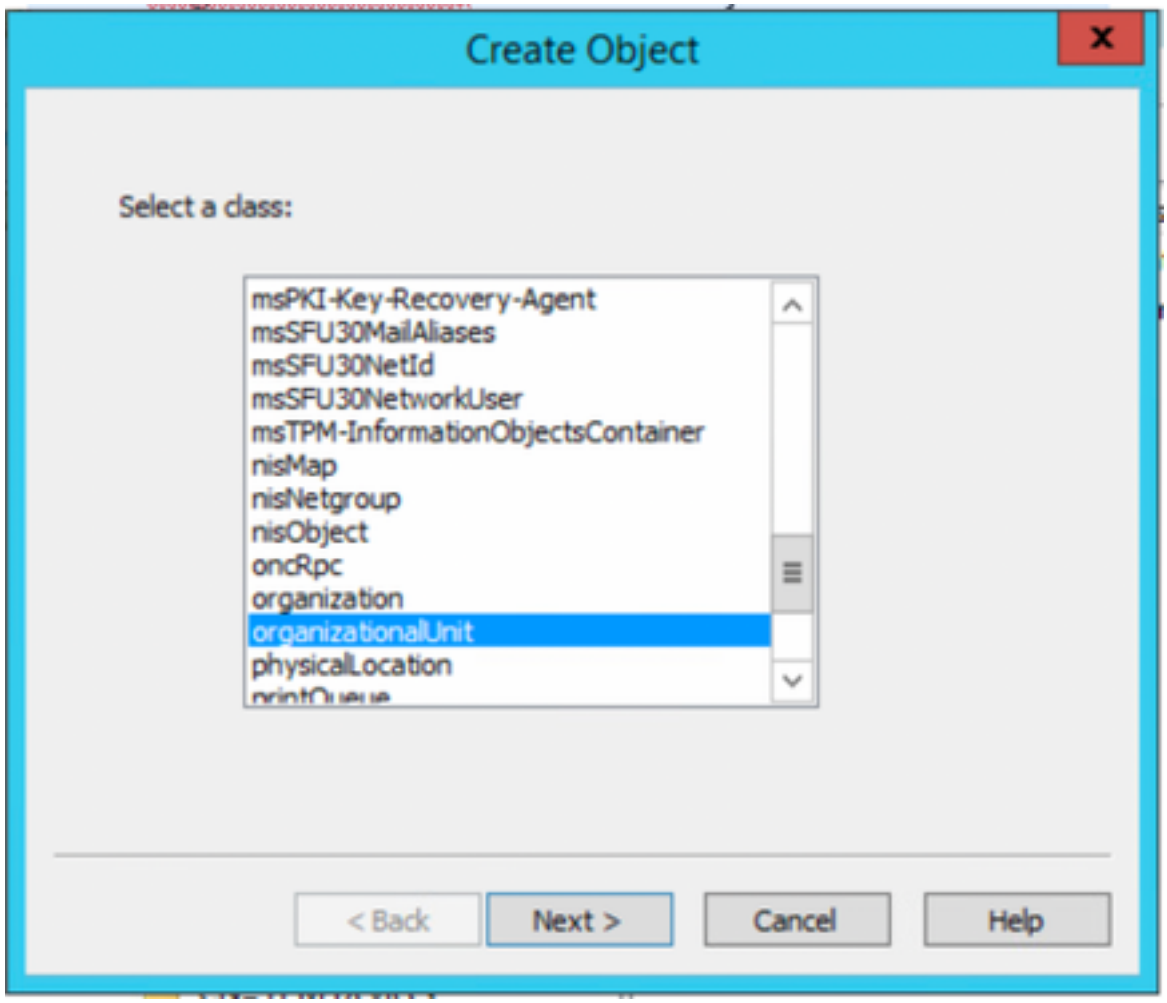
3. Under connection settings define a name and select the **OK** button to start the connection.



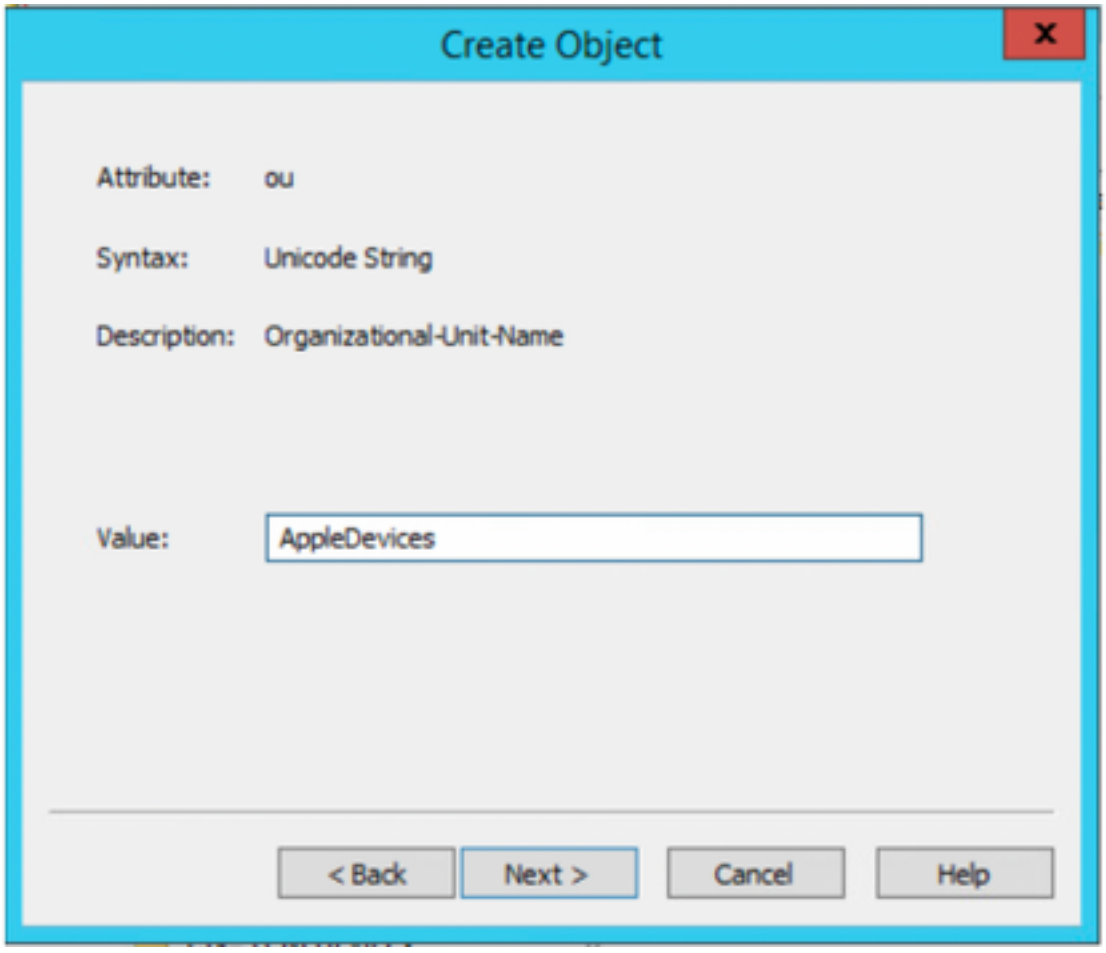
4. Under the same ADSI Edit menu right-click in DC connection (DC=ciscodemo, DC=lab), select **New,** then select option **Object**



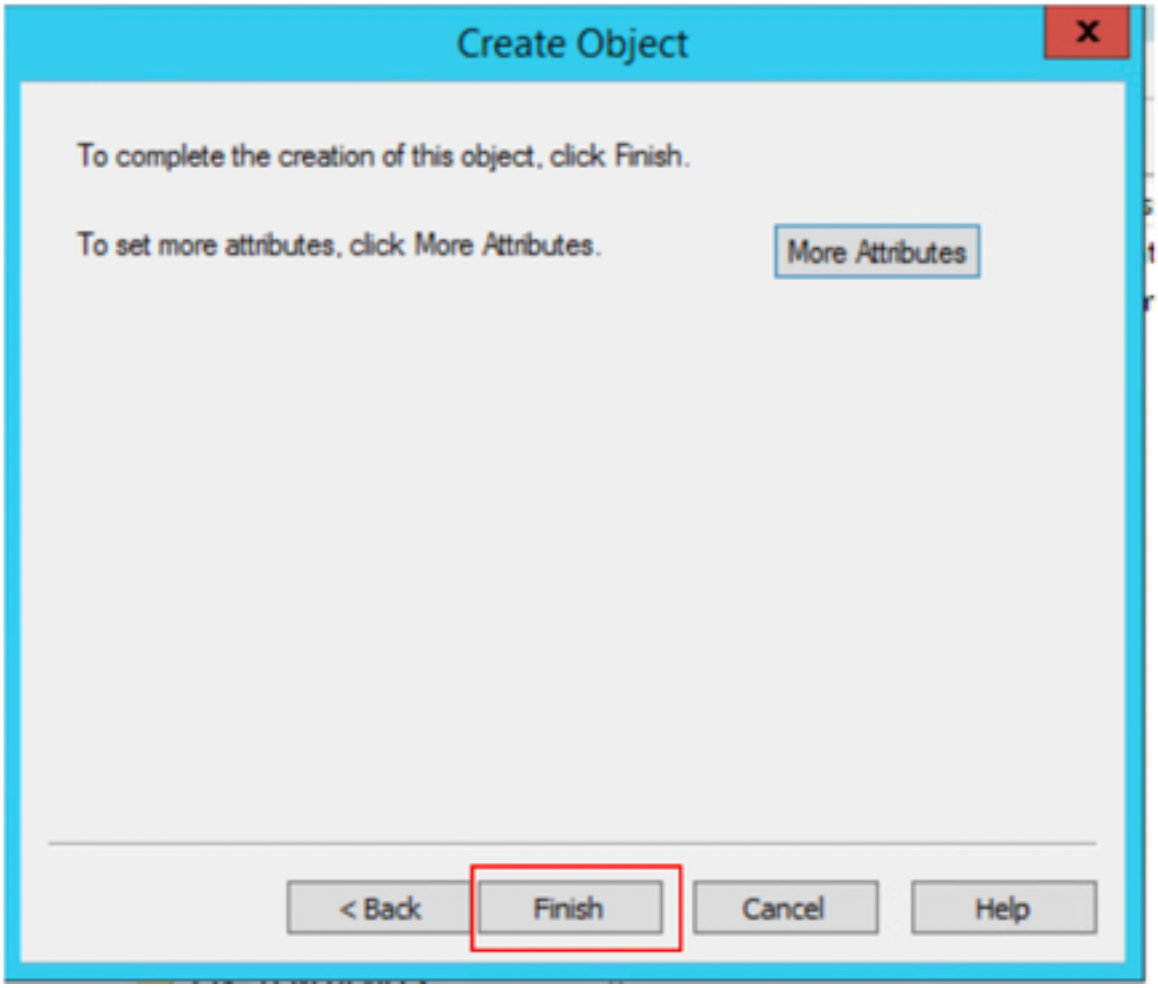
5. Select option **OrganizationalUnit** as the new Object and select **next.**



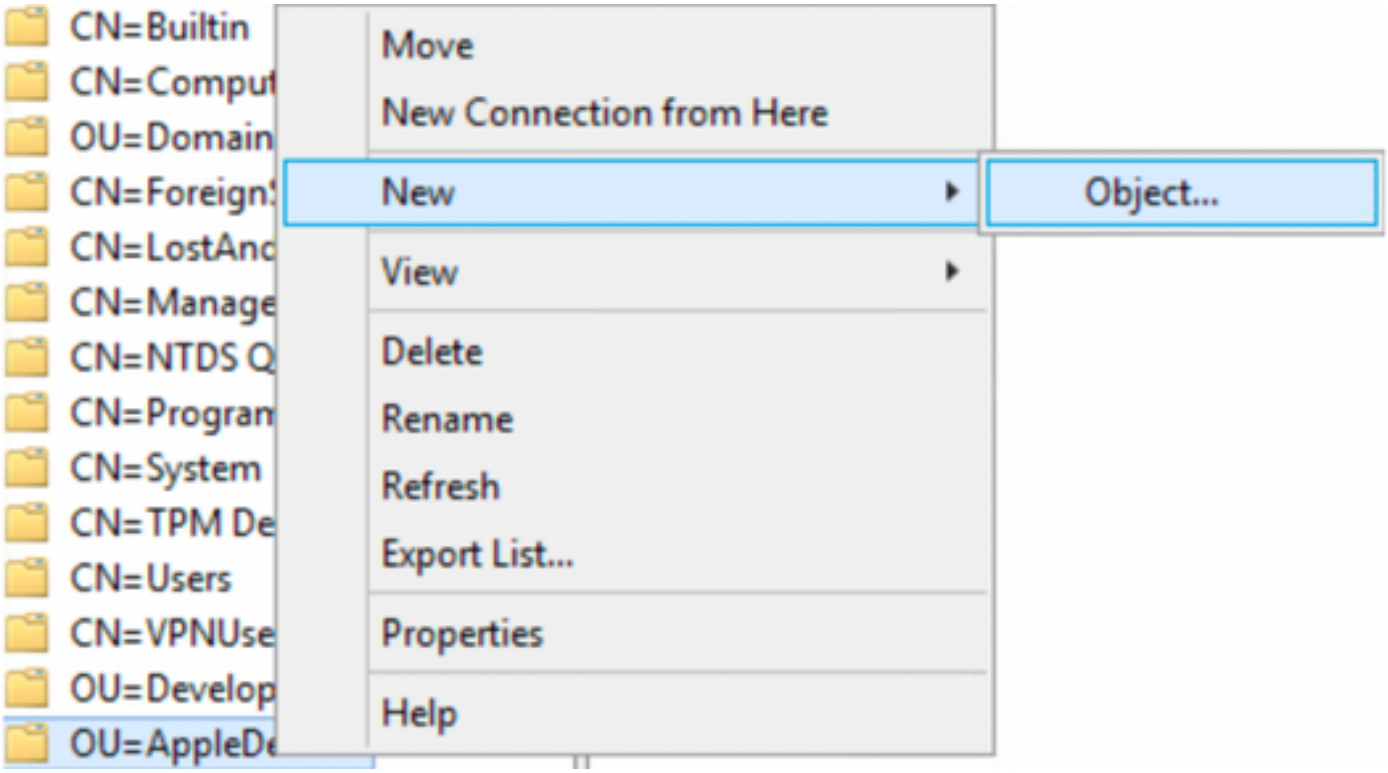
6. Define a name for the new OrganizationalUnit and select **Next**



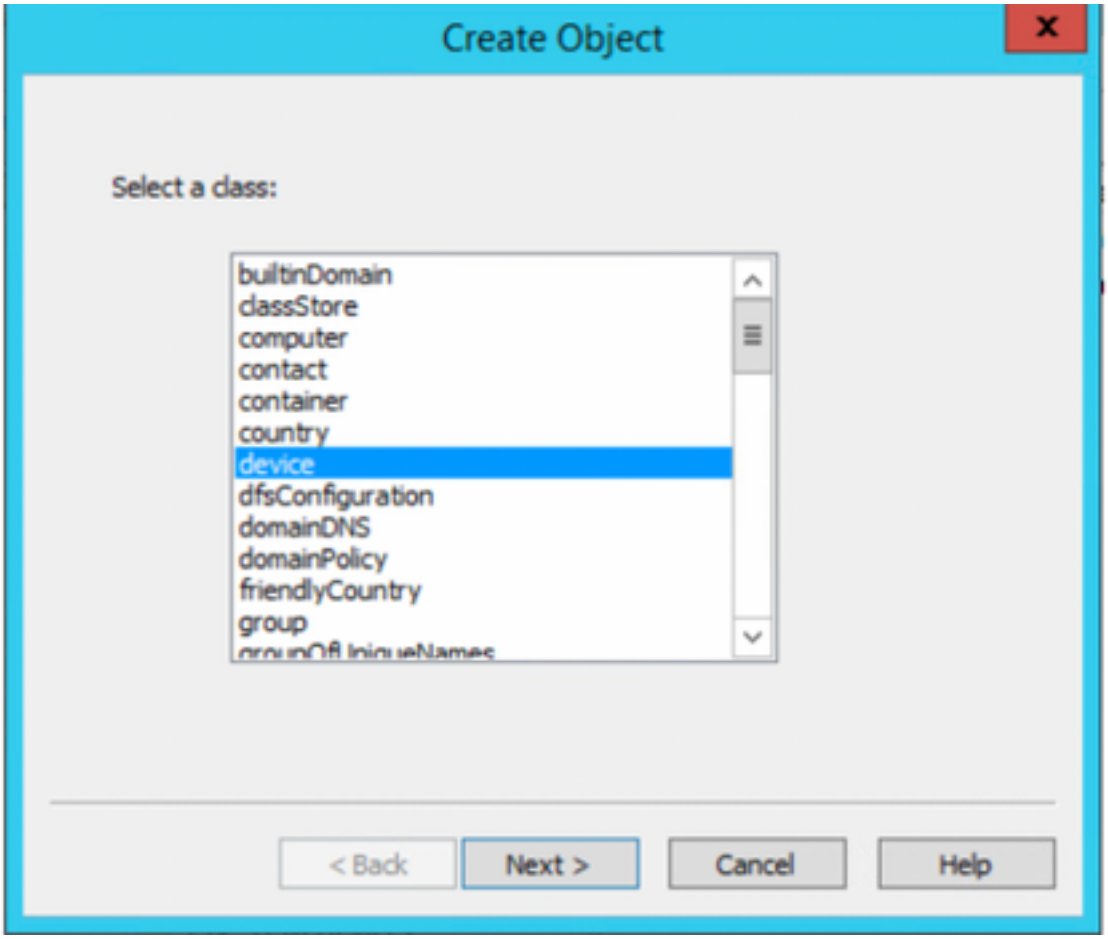
7. Select **Finish in** order to create the new OrganizationalUnit



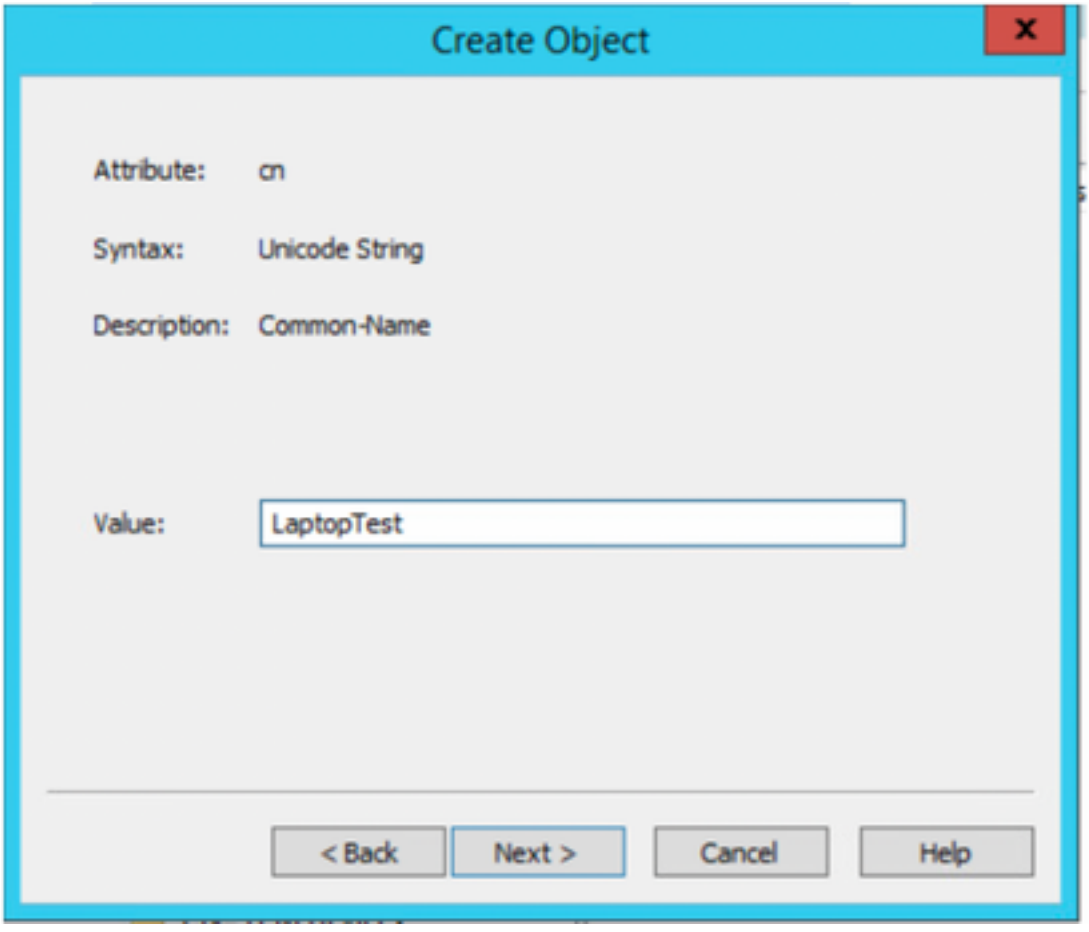
8. Right-click on the OrganizationalUnit that was just created and select **New > Object**



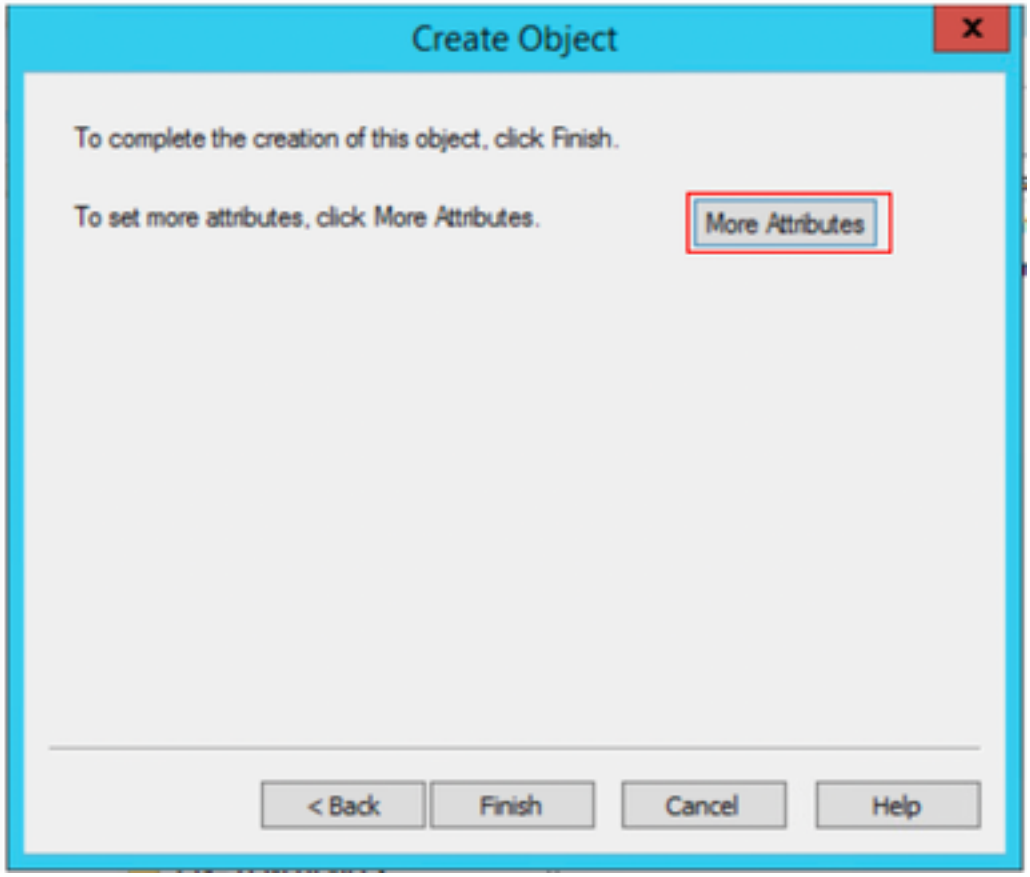
9.Select **device** as object class and select **next**



10.Define a name in the Value field and select **Next**

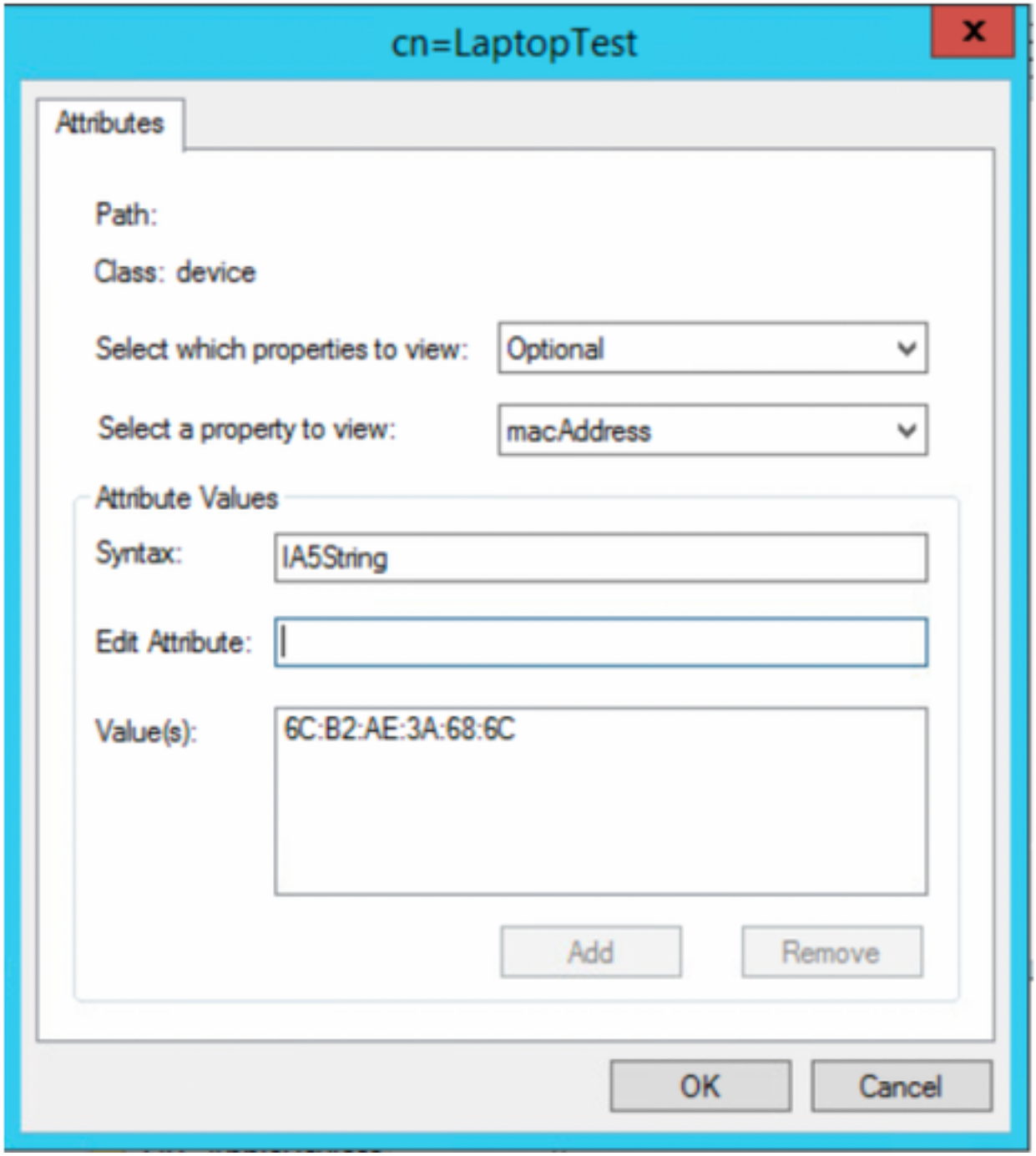


11. Select the option **More Attributes**



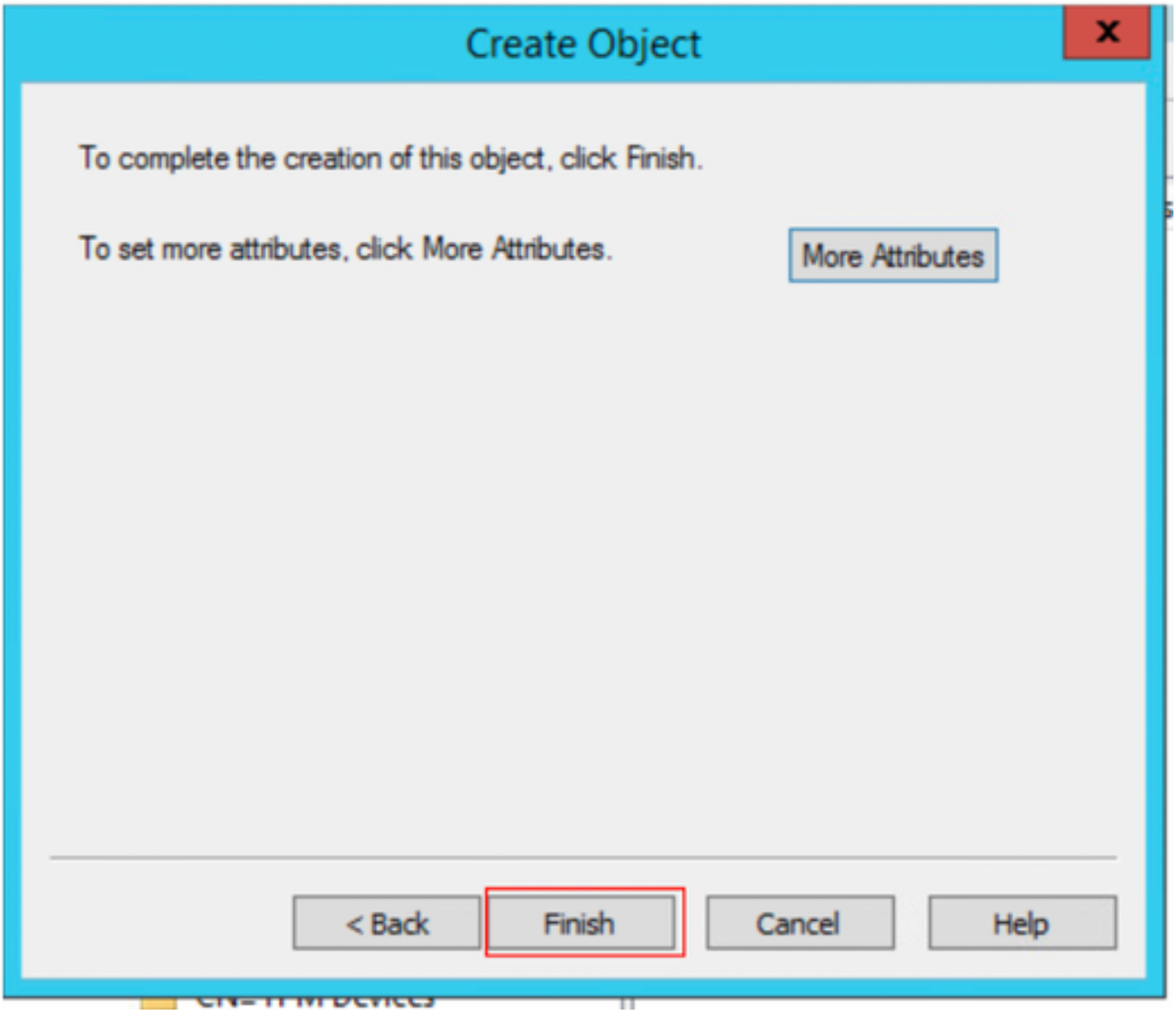
11. For the drop-down menu, **Select a property to view**, select option **macAddress,** then define the endpoint Mac address that will be authenticated under the **Edit attribute** field and select the **Add button to save the device mac address.**

Note: Use a double colon instead of dots or hyphen between mac address octets.

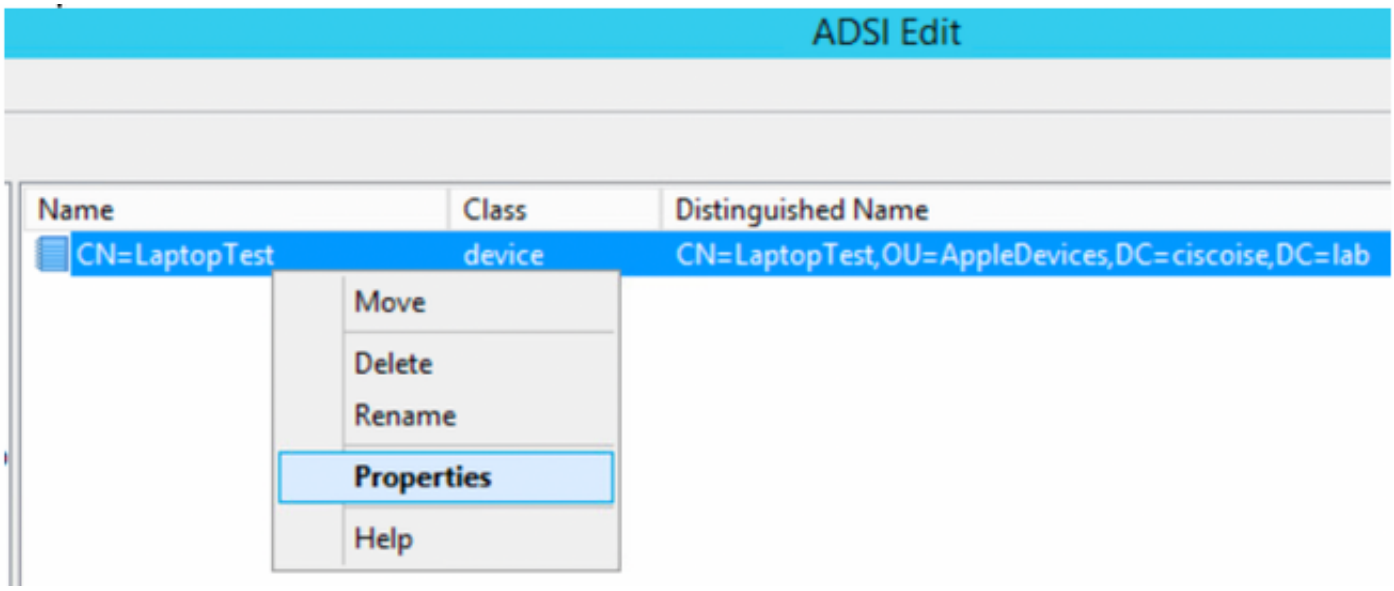


12. Select **OK** in order to save the information and continue with device object configuration

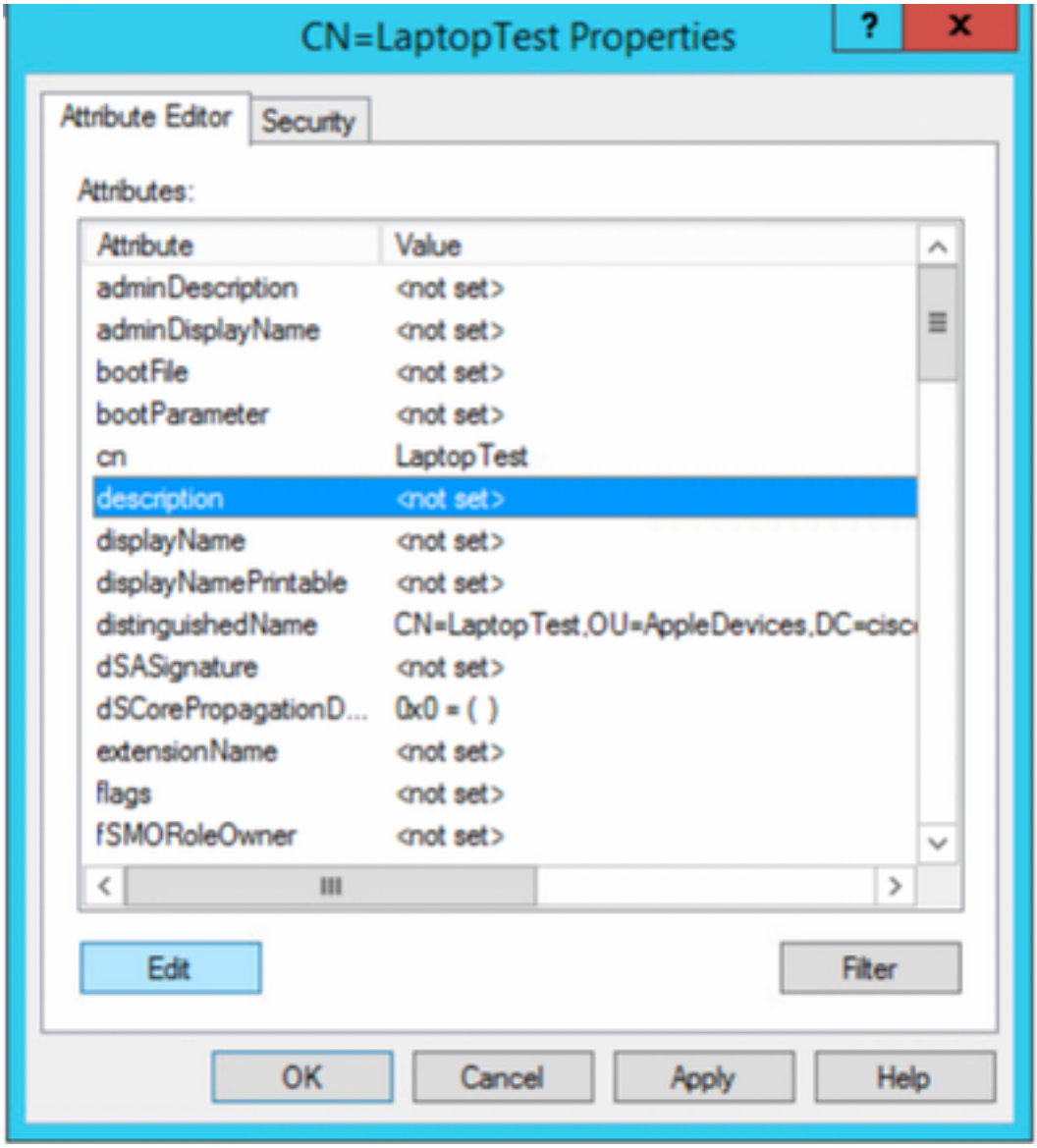
13. Select F**inish** in order to create the new device Object



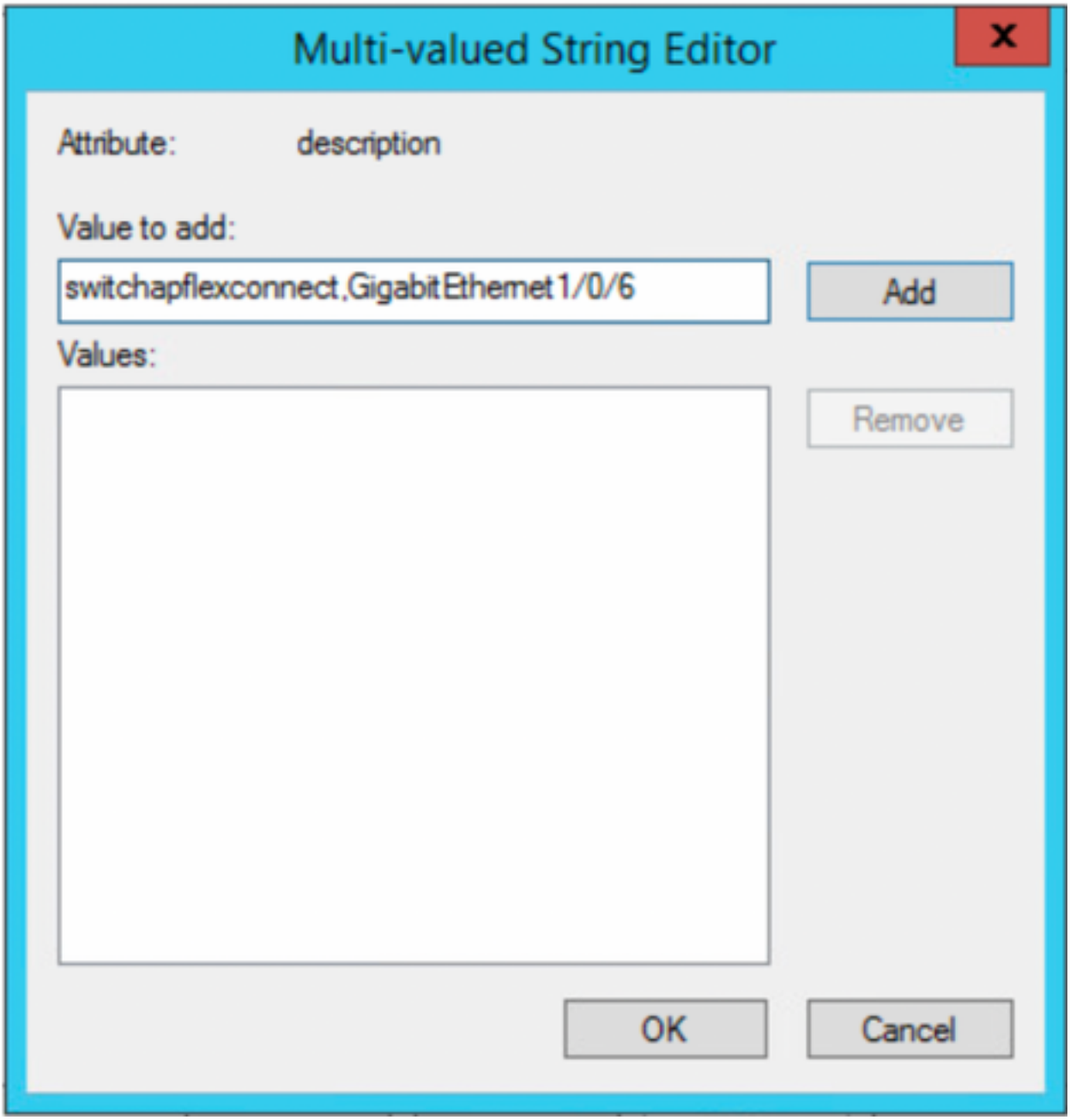
14. Right-click on the device object and select option **Properties**



15. Select option **description** and select **Edit** in order to define the switch name and switch-port where the device will be connected.



16. Define the switch name and switch-port, please make sure you use a comma to separate each value. Select **Add** and then **Ok** to save the information.



- **Switchapflexconnect is the switch name.**
- **GigabitEthernet1/0/6 is the switch-port where the endpoint is connected to.**

Note: It is possible to use scripts in order to add attributes to a specific field, however, for this example we are defining the values manually

Note: AD-attribute is case sensitive, if you use all Mac addresses in lower case ISE converts to upper case during the LDAP query. In order to avoid this behavior, Disable Process Host Lookup under allowed protocols. Details can be found in this link: https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

Switch Configuration

The following describes the configuration for 802.1x communication between ISE and the switch.

```
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
```

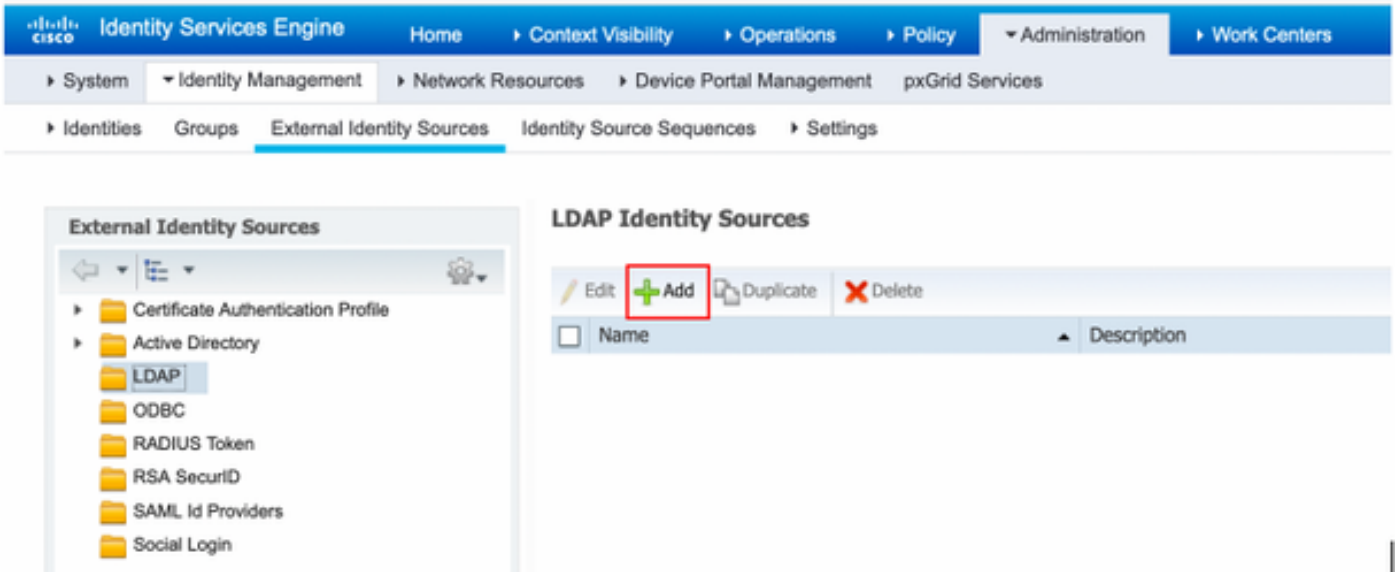
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access 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 !
```

Note: Global and interface configuration may need to be adjusted in your environment

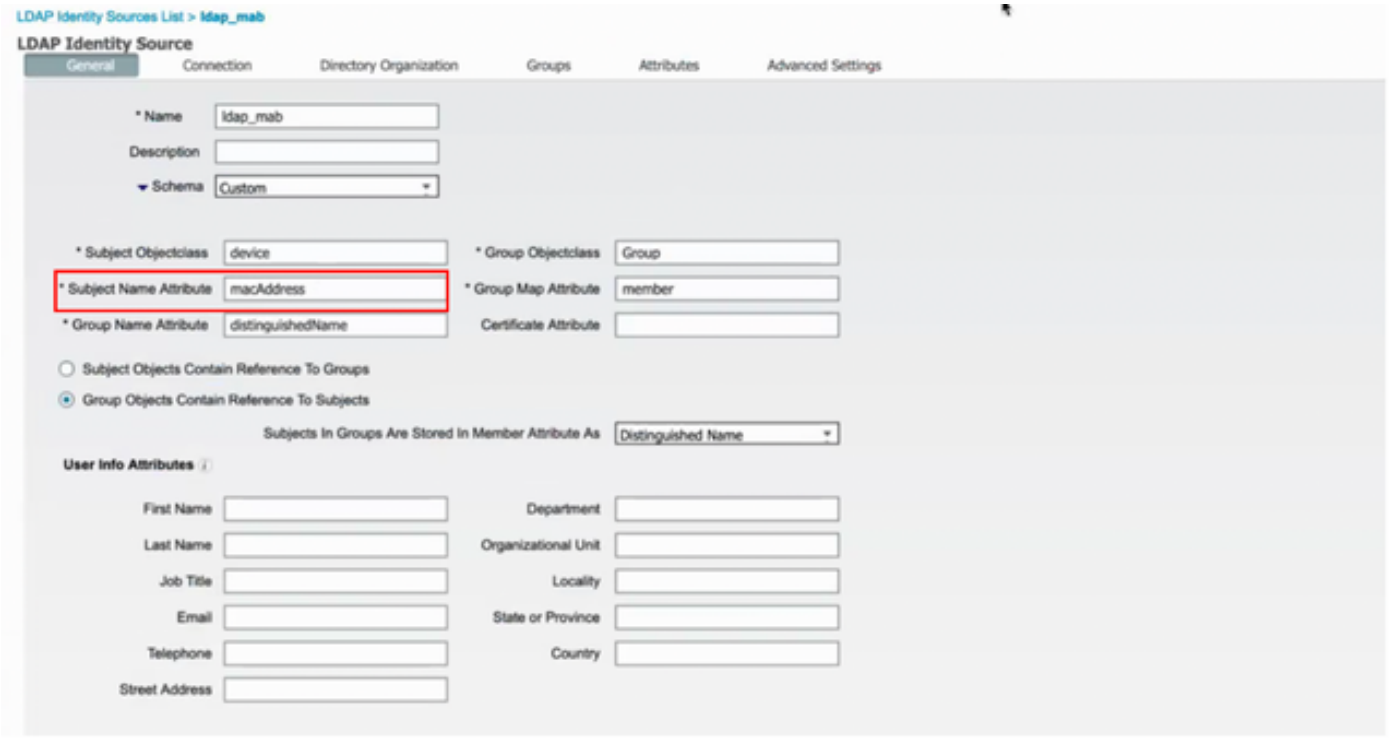
ISE Configuration

The following describes the configuration on ISE to get the attributes from the LDAP server and to configure the ISE policies.

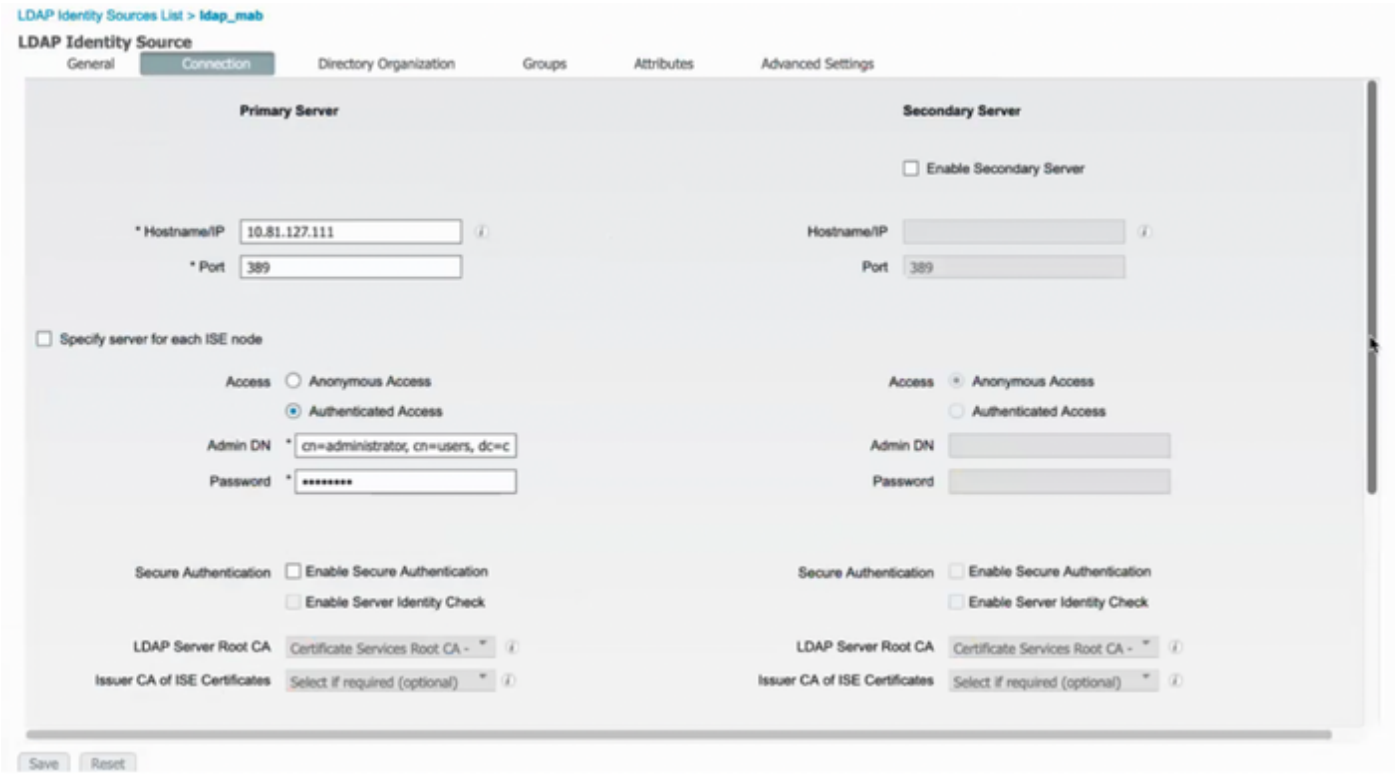
1. On ISE, go to **Administration->Identity Management->External Identity Sources** and select the **LDAP** folder and click on **Add** in order to create a new connection with LDAP



2.Under **General** tab define a name and select the mac address as the Subject Name Attribute

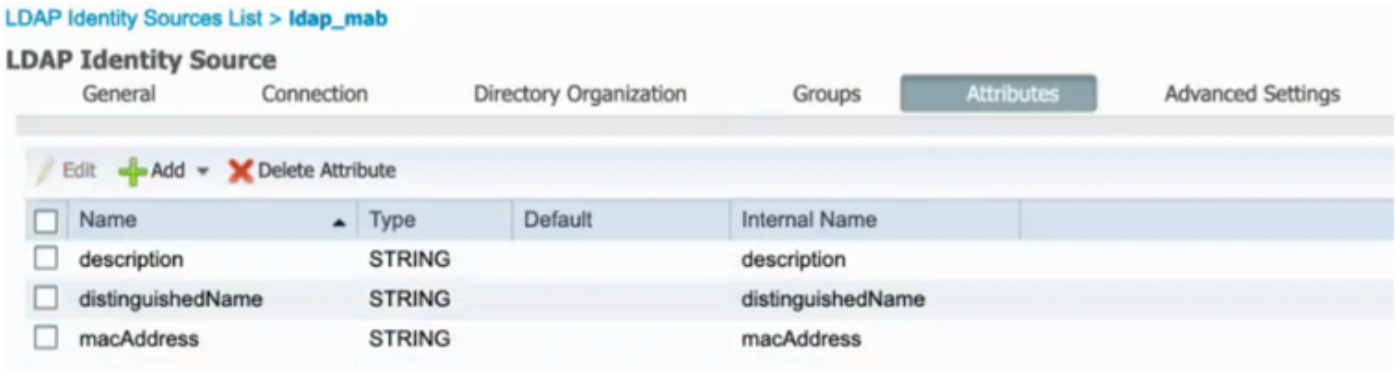


3. Under **Connection** tab configure the IP addres, admin DN, and password from the LDAP server to get a successful connection.

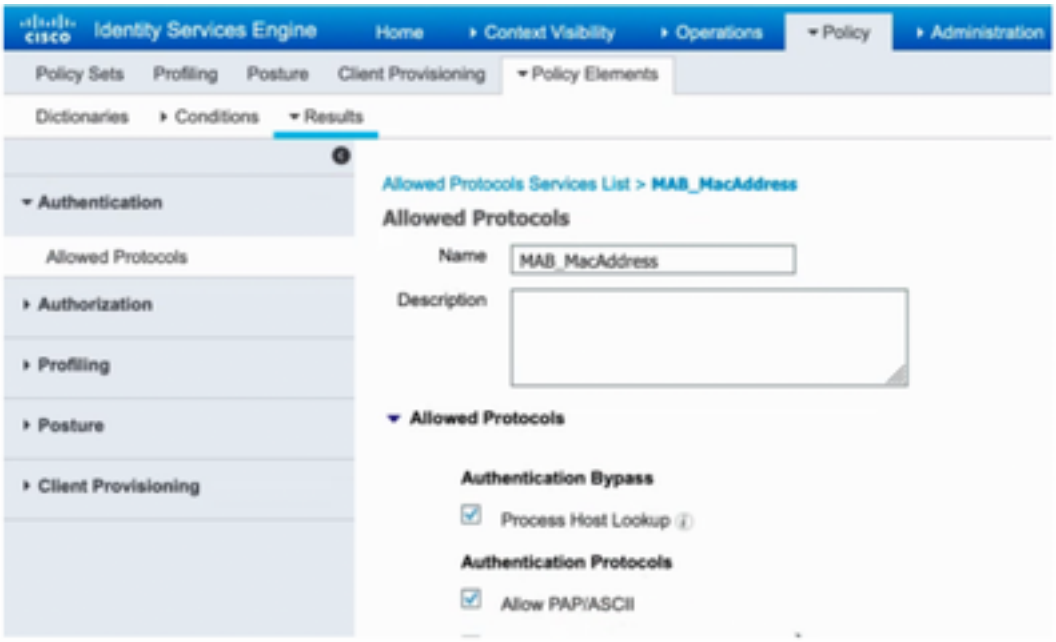


Note: Port 389 is the default port used.

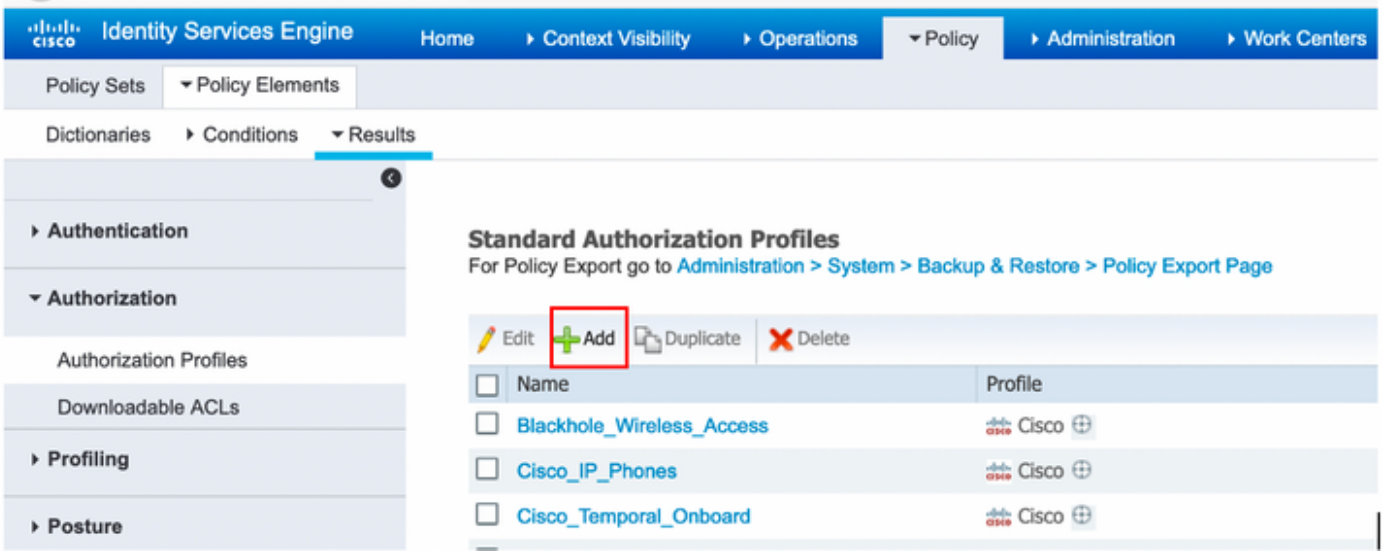
4. Under **Attributes** tab select the the macAddress and description attributes, these attributes will be used in the authorization policy

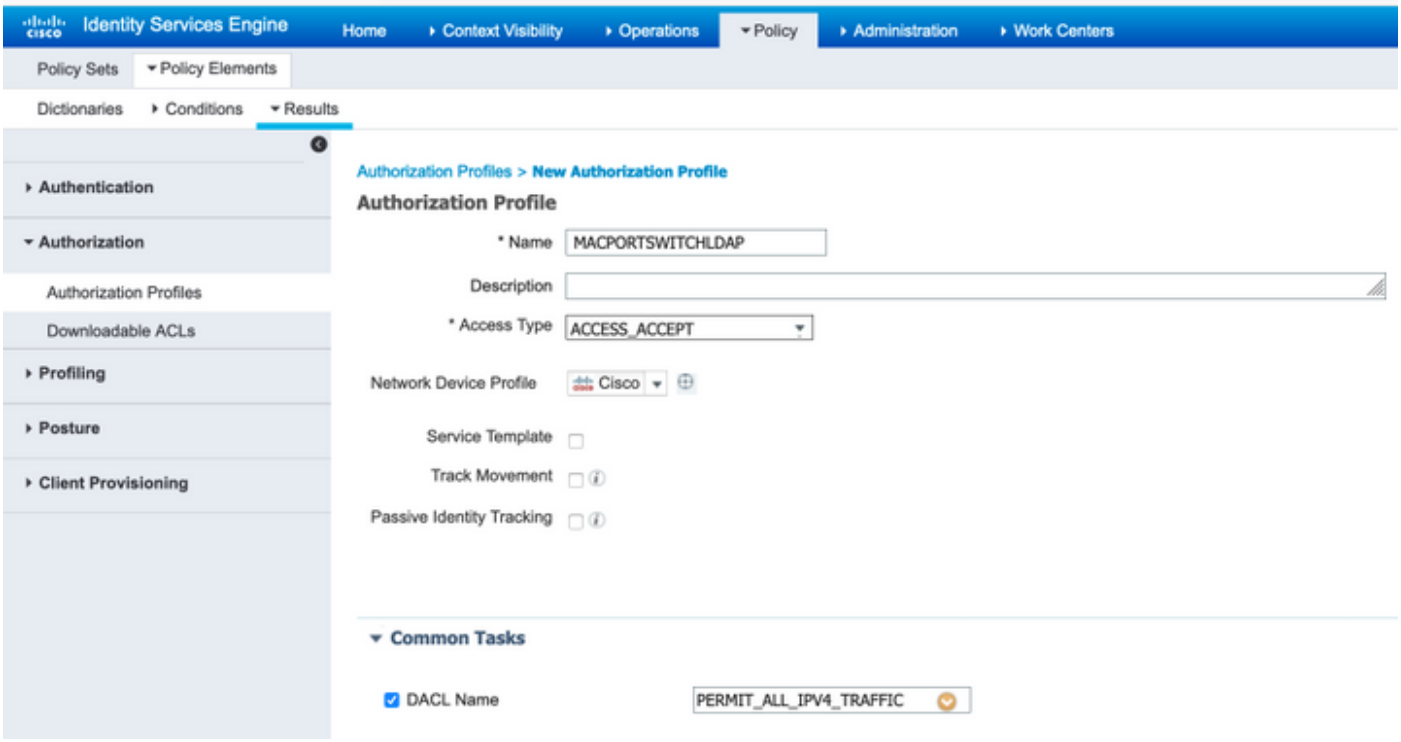


5. In order to create an allowed protocol permitted go to **Policy->Policy Elements->Results->Authentication->Allowed Protocols.** Define and select Process Host Lookup and Allow PAP/ASCII as the only allowed protocols. Finally select **Save**

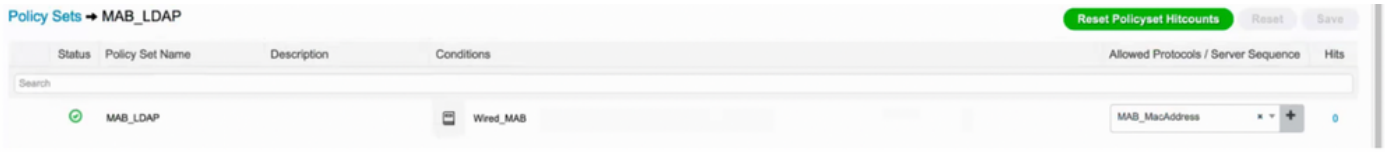


6. In order to create an authorization profile, go to **Policy->Policy Elements->Results->Authorization->Authorization Profiles.** Select **Add** and define the permissions will be assigned to the endpoint.

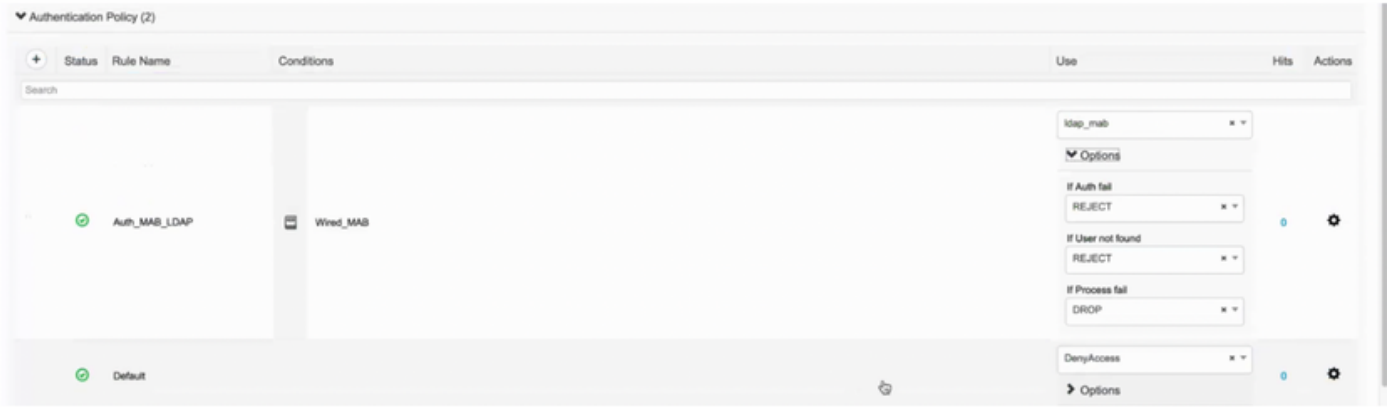




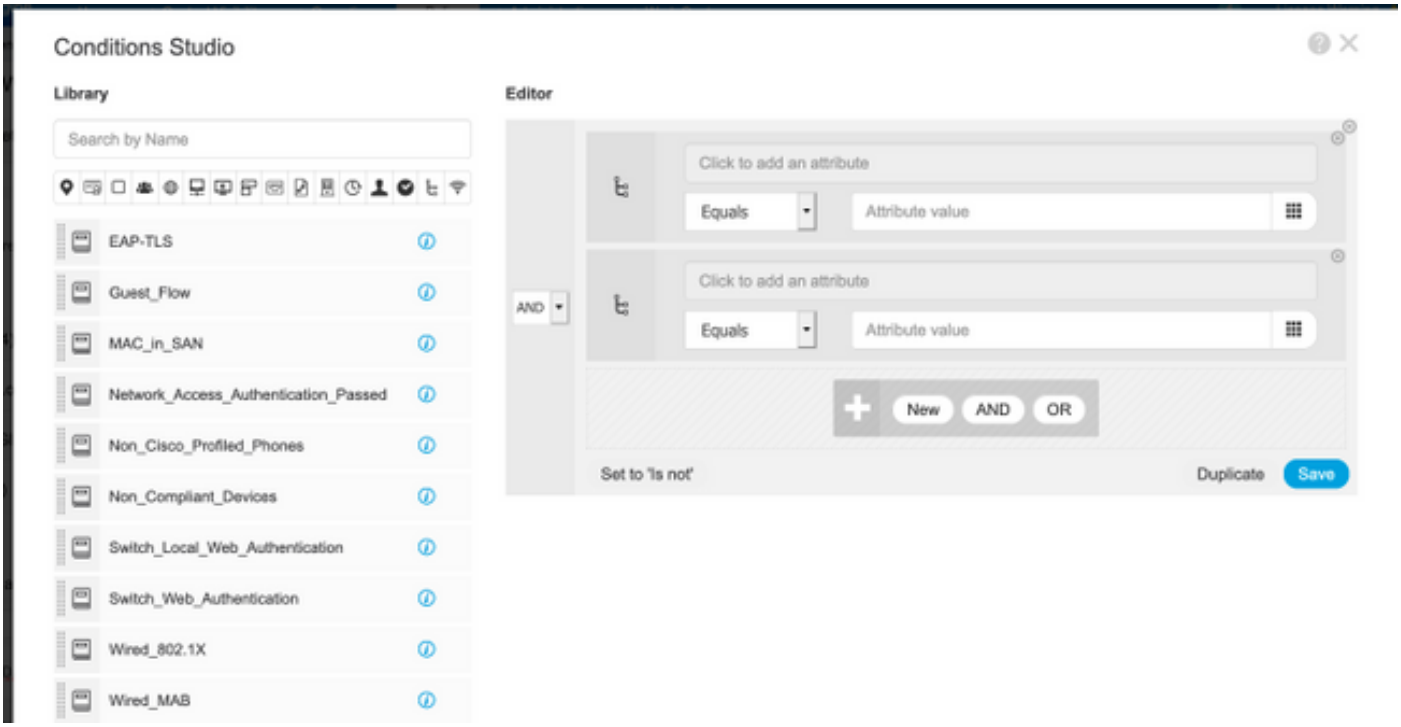
7.Go to Policy-> Policy Set and create a policy set using the predefined condition Wired_MAB and the Allowed Protocol created in step 5.

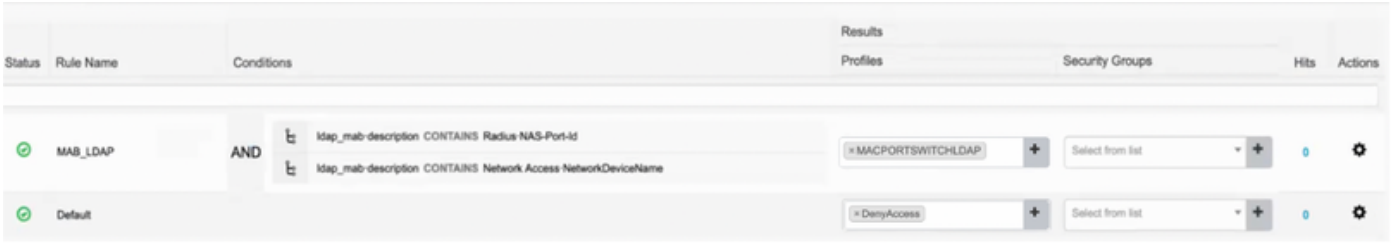


8.Under the new Policy set created create an authentication policy using the predefined **Wired_MAB** Library and **LDAP** connection as external identity source sequence



9. Under **Authorization Policy** define a name and create a compound condition using LDAP Attribute description, Radius NAS-Port-Id and NetworkDeviceName. Finally, add the Authorization profile created in step 6.





After you apply the configuration, you should be able to connect to the network without user intervention.

Verify

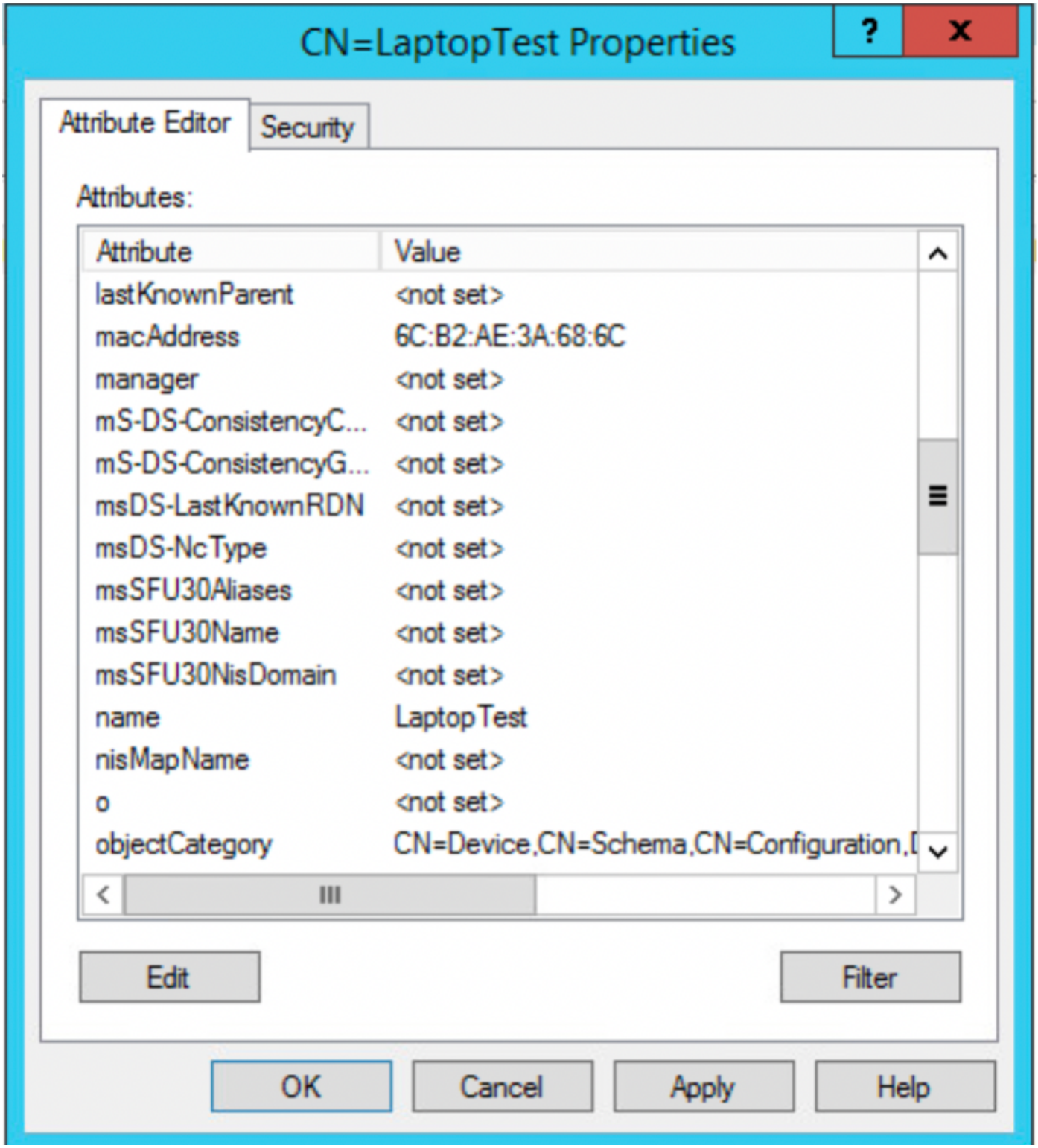
Once connected to the designated switch-port you can type **show authentication session interface GigabitEthernet X/X/X details** to validate the authentication and authorization status of the device.

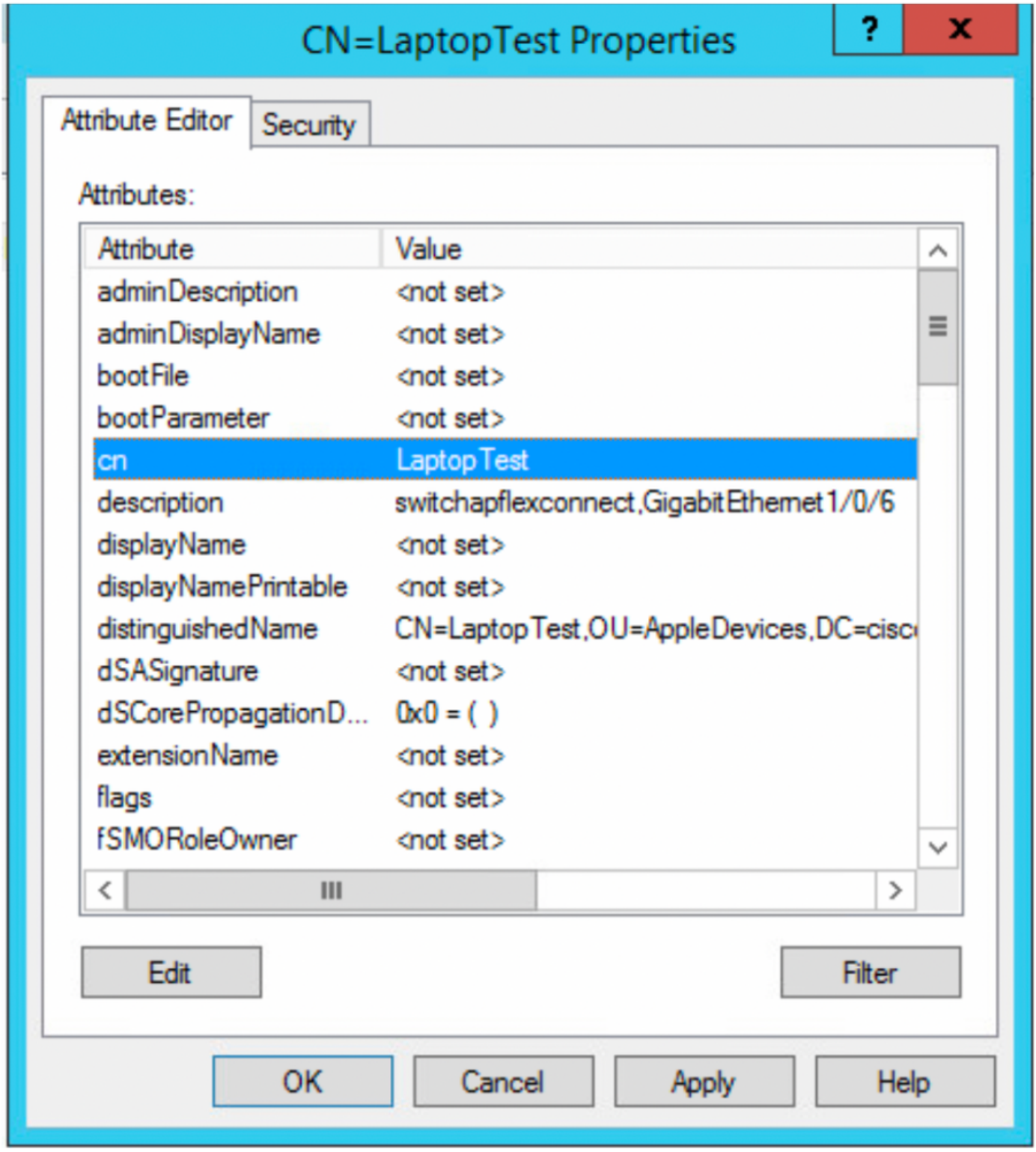
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session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

On ISE you can use Radius Live Logs for confirmation.

Troubleshoot

On the LDAP server, Validate that the device created has Mac address, proper switch name, and switch-port configured


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



On ISE, you can take a packet capture (Go to **Operations->Troubleshoot->Diagnostic Tool->TCP Dumps**) in order to validate the values are being sent from LDAP to ISE