Autenticação baseada em atributos ISE e LDAP

Contents

Introduction

Este documento descreve como configurar o Cisco Identity Services Engine (ISE) e usar atributos de objetos Lightweight Diretory Access Protocol (LDAP) para autenticar e autorizar dispositivos dinamicamente.

Note: Este documento é válido para configurações que usam LDAP como fonte de identidade externa para autenticação e autorização do ISE.

Contribuído por Emmanuel Cano e Mauricio Ramos, engenheiro de serviços profissionais da Cisco.

Editada pela engenheira do Cisco TAC da Neri Cruz.

Prerequisites

Requirements

A Cisco recomenda que você conheça os seguintes tópicos:

- Conhecimento básico de conjuntos de políticas, autenticação e políticas de autorização do ISE
- Desvio de autenticação Mac (MAB)
- Conhecimento básico do protocolo Radius
- Conhecimento básico do servidor Windows

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de software e hardware:

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

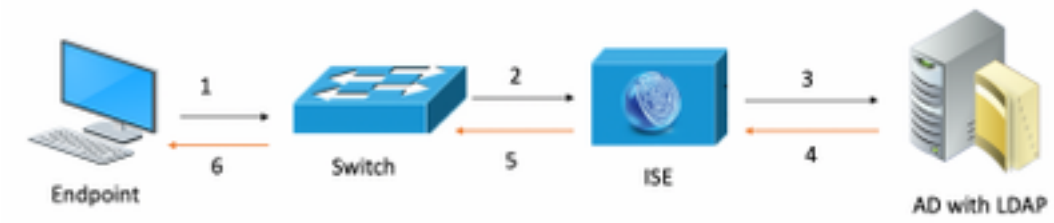
Note: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuração

Esta seção descreve como configurar os dispositivos de rede, a integração entre ISE e LDAP e, finalmente, configurar atributos LDAP a serem usados na política de autorização do ISE.

Diagrama de Rede

Esta imagem ilustra a topologia de rede usada:



Aqui está o fluxo de tráfego, como ilustrado no diagrama de rede:

1. O usuário conecta seu pc/laptop à porta do switch designado.
2. O switch envia uma solicitação de acesso RADIUS para esse usuário ao ISE
3. Quando o ISE recebe as informações, ele consulta o servidor LDAP para o campo de usuário específico, que contém os atributos a serem usados nas condições da política de autorização.
4. Quando o ISE recebe os atributos (a porta do switch, o nome do switch e o endereço mac do dispositivo), ele compara as informações fornecidas pelo switch.
5. Se as informações de atributos fornecidas pelo switch forem as mesmas fornecidas pelo LDAP, o ISE enviará um RADIUS Access-Accept com as permissões configuradas no perfil de autorização.

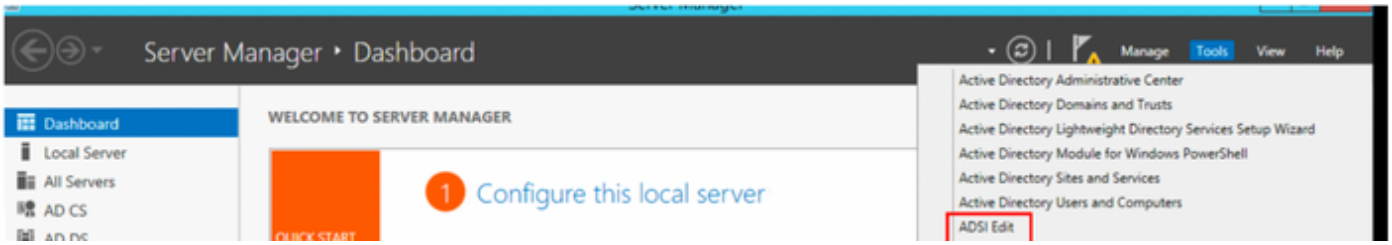
Configurações

Use esta seção para configurar o LDAP, o switch e o ISE.

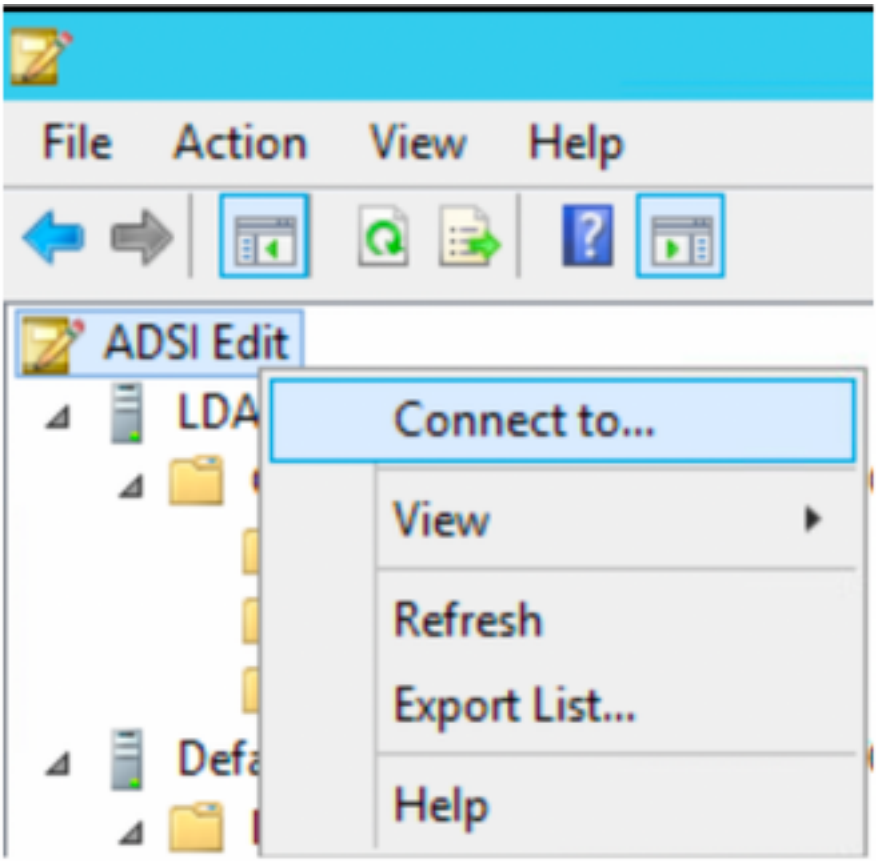
Configurar LDAP

Conclua as seguintes etapas para configurar o servidor LDAP:

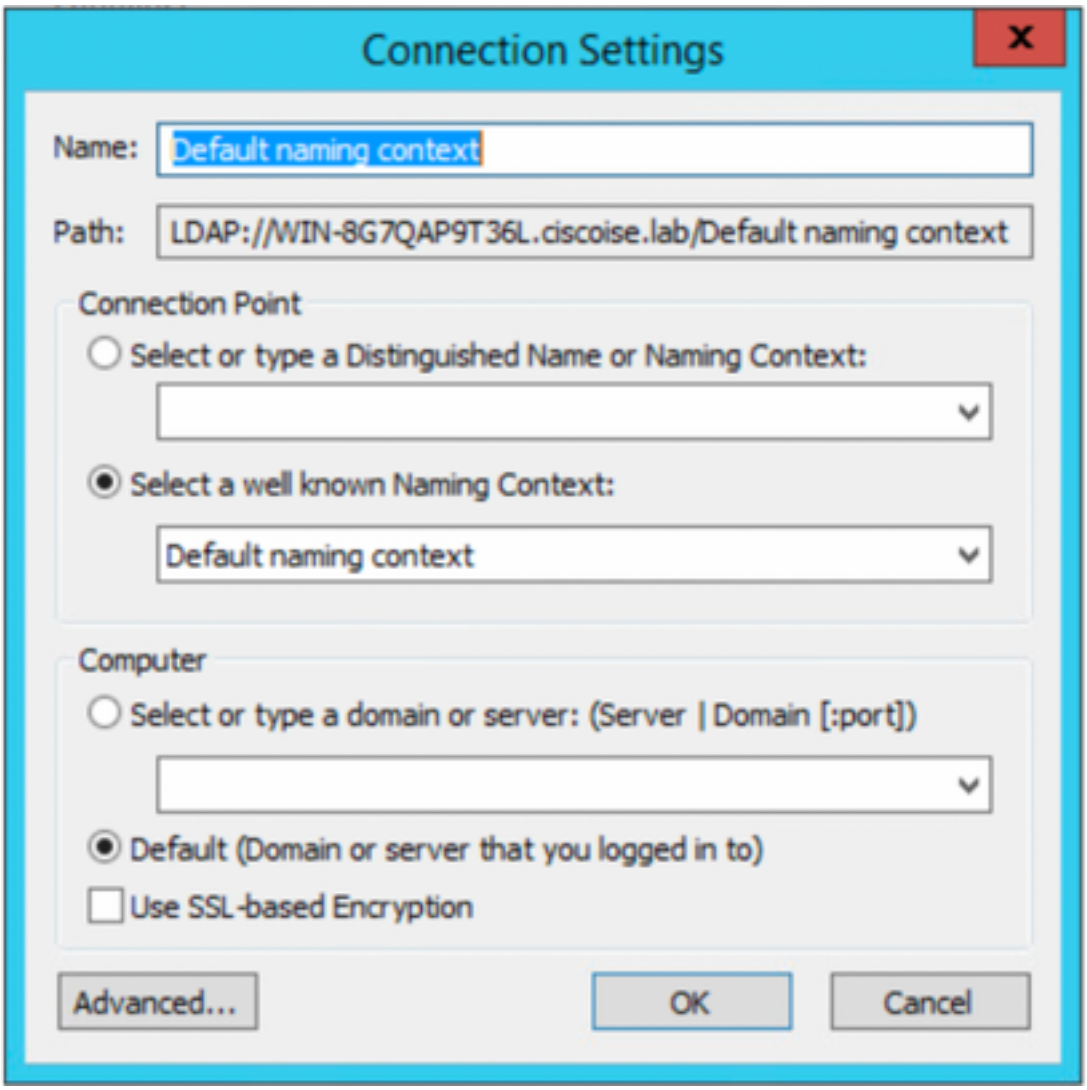
1. Navegue até **Gerenciador de servidores > Painel > Ferramentas > Editar ADSI**



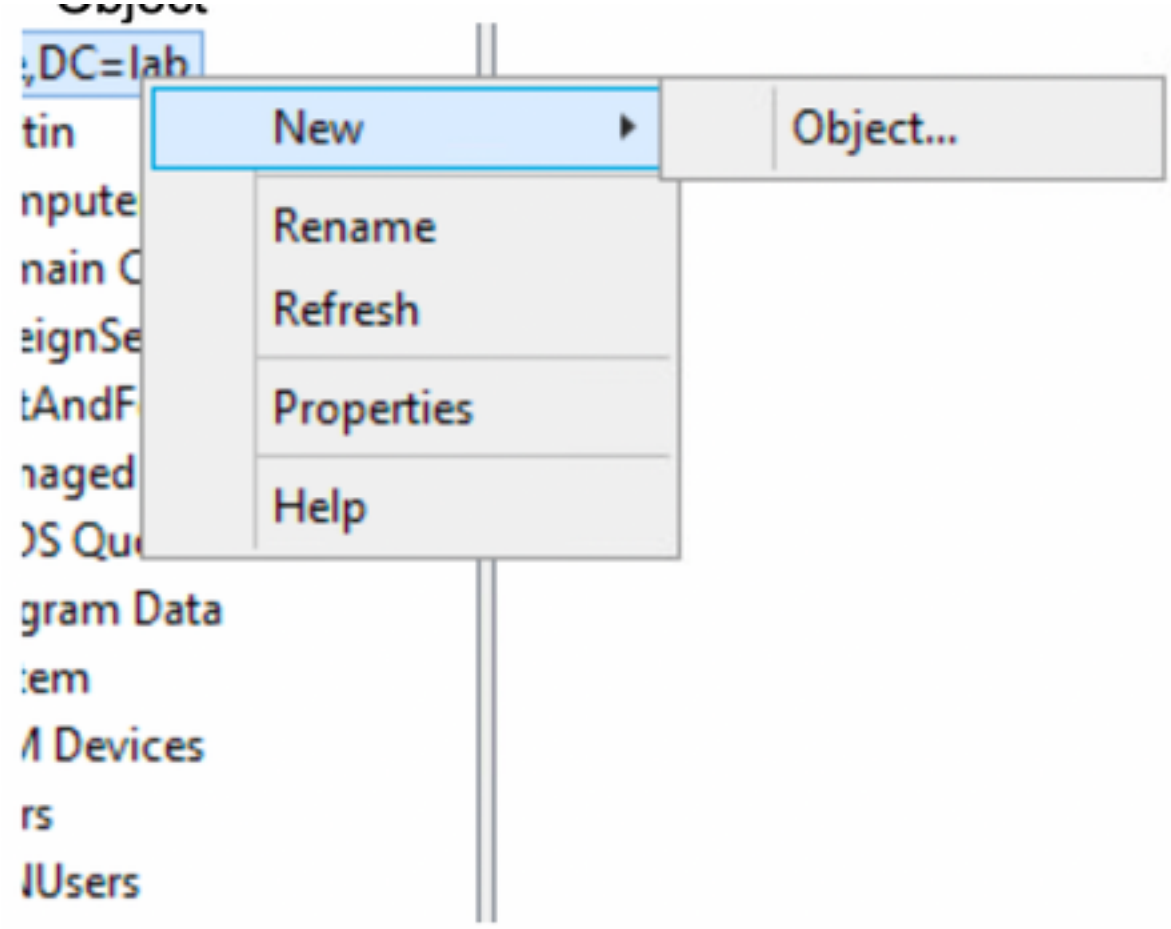
2. Clique com o botão direito do mouse no ícone Editar ADSI e selecione **Conectar a...**



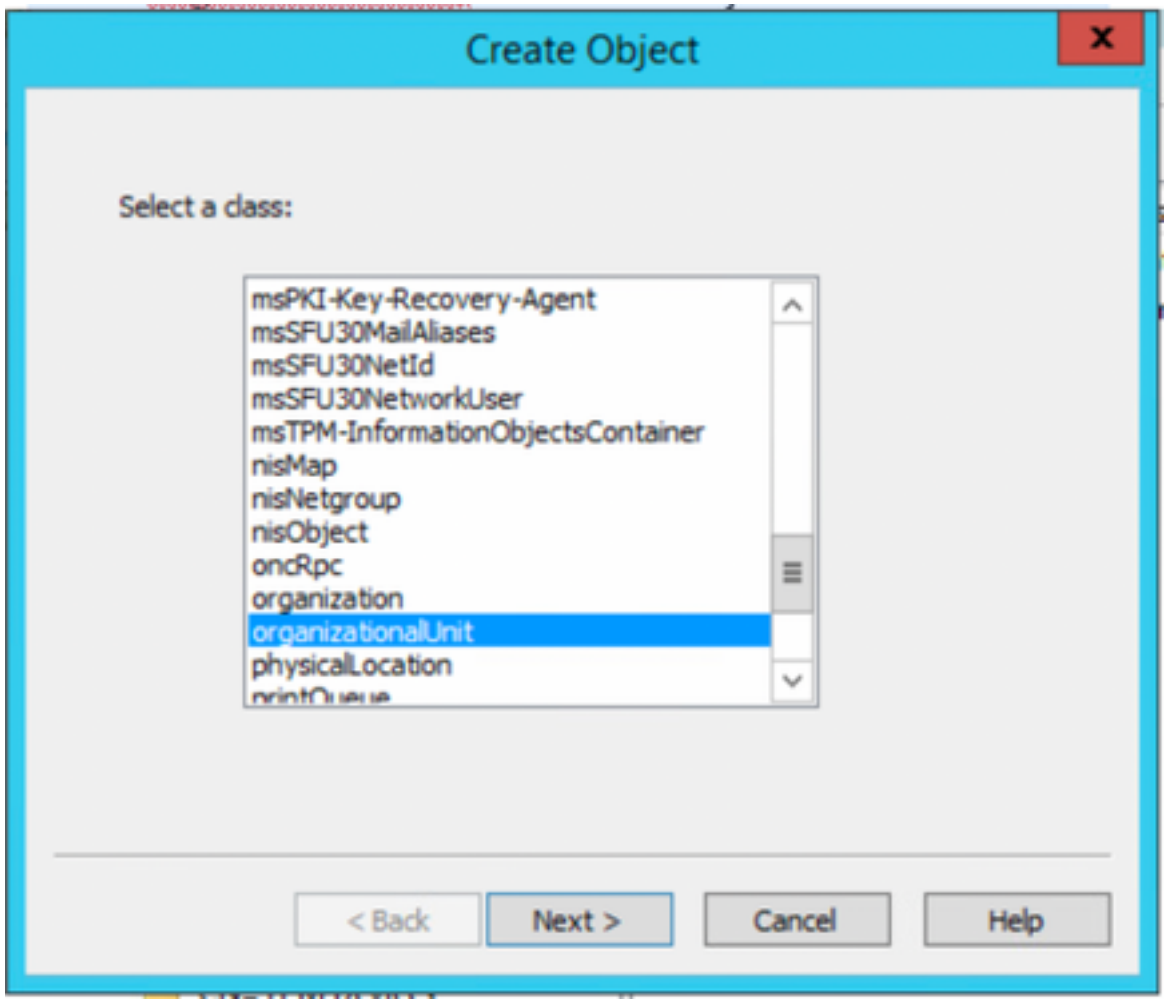
3. Em configurações de conexão, defina um nome e selecione o botão **OK** para iniciar a conexão.



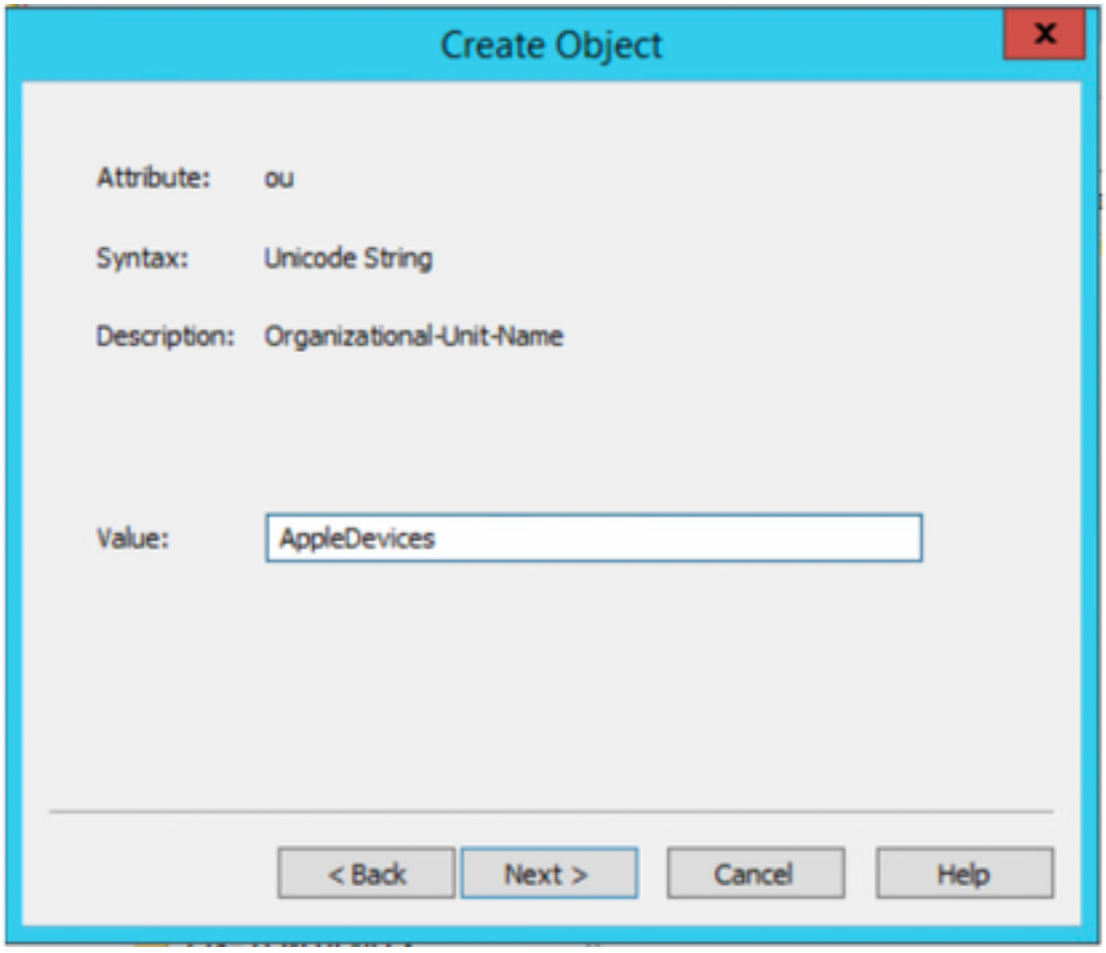
4. No mesmo menu ADSI Edit, clique com o botão direito do mouse em DC connection (DC=ciscodemo, DC=lab), selecione **New (Novo)** e selecione a opção **Object (Objeto)**



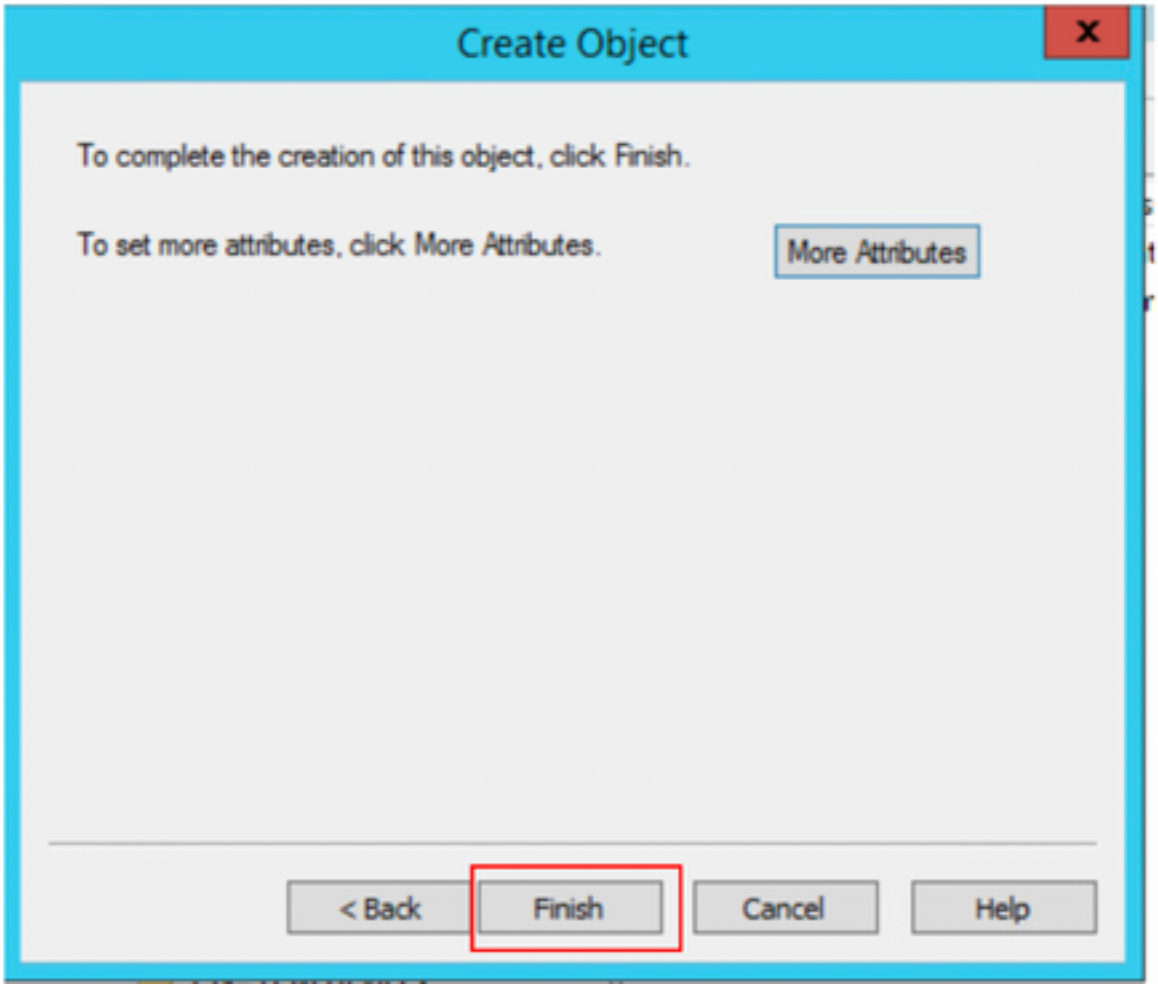
5. Selecione a opção **OrganizationalUnit** como o novo objeto e selecione **avançar.**



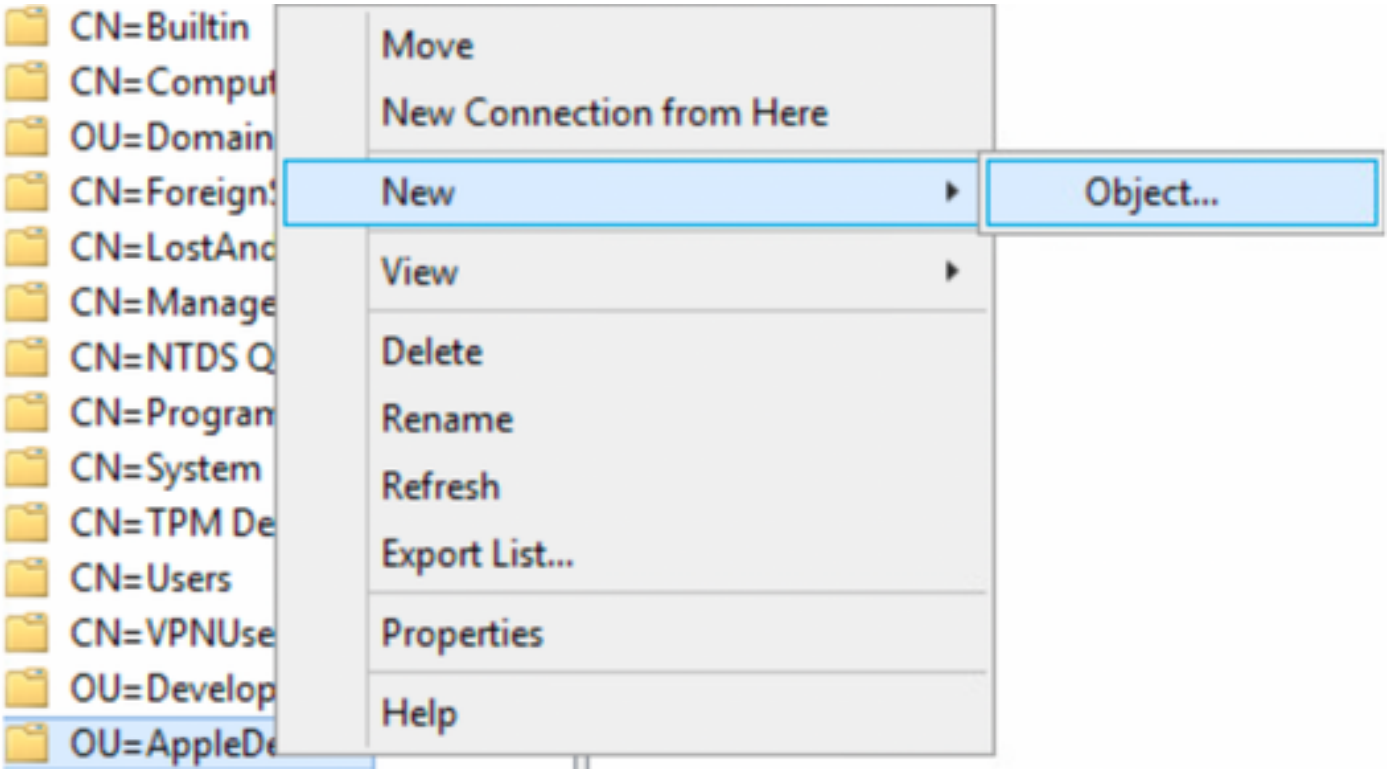
6. Defina um nome para a nova OrganizationalUnit e selecione **Next**



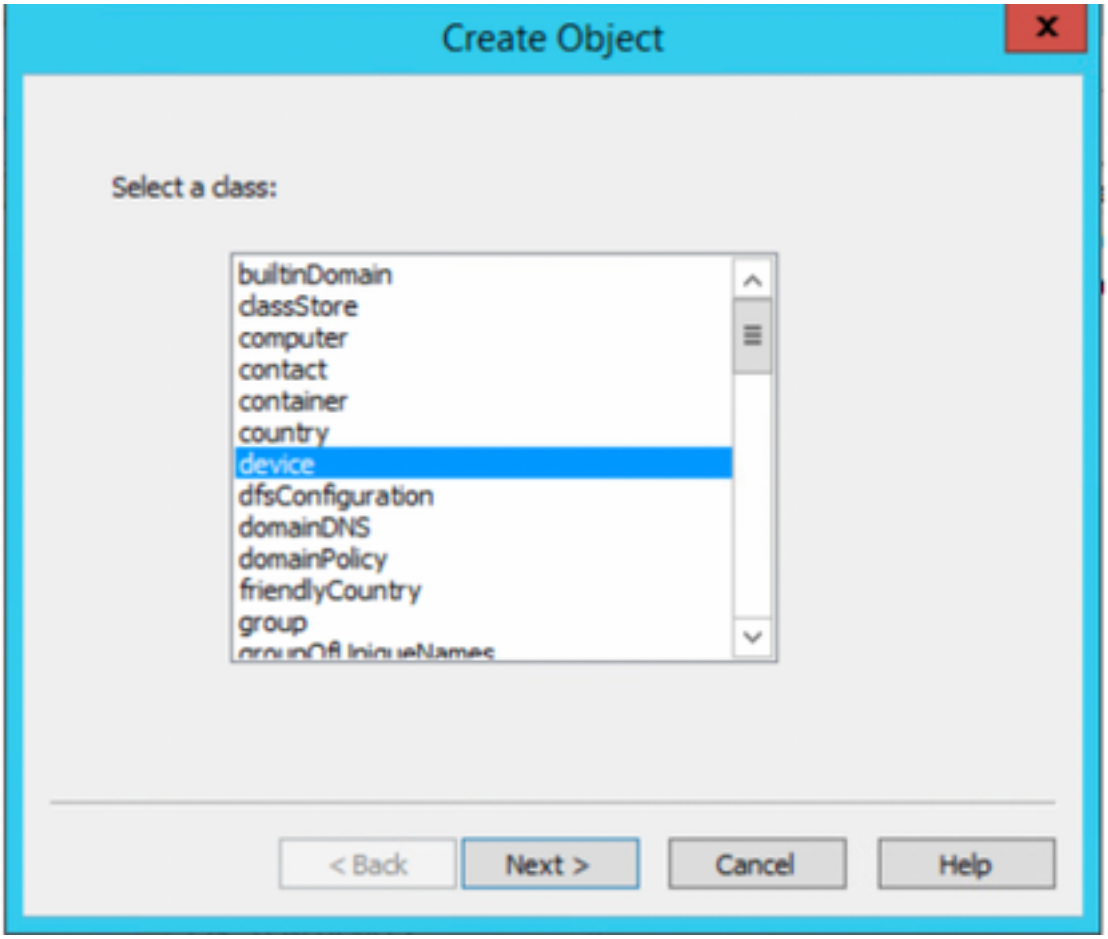
7. Selecione **Concluir** para criar a nova Unidade Organizacional



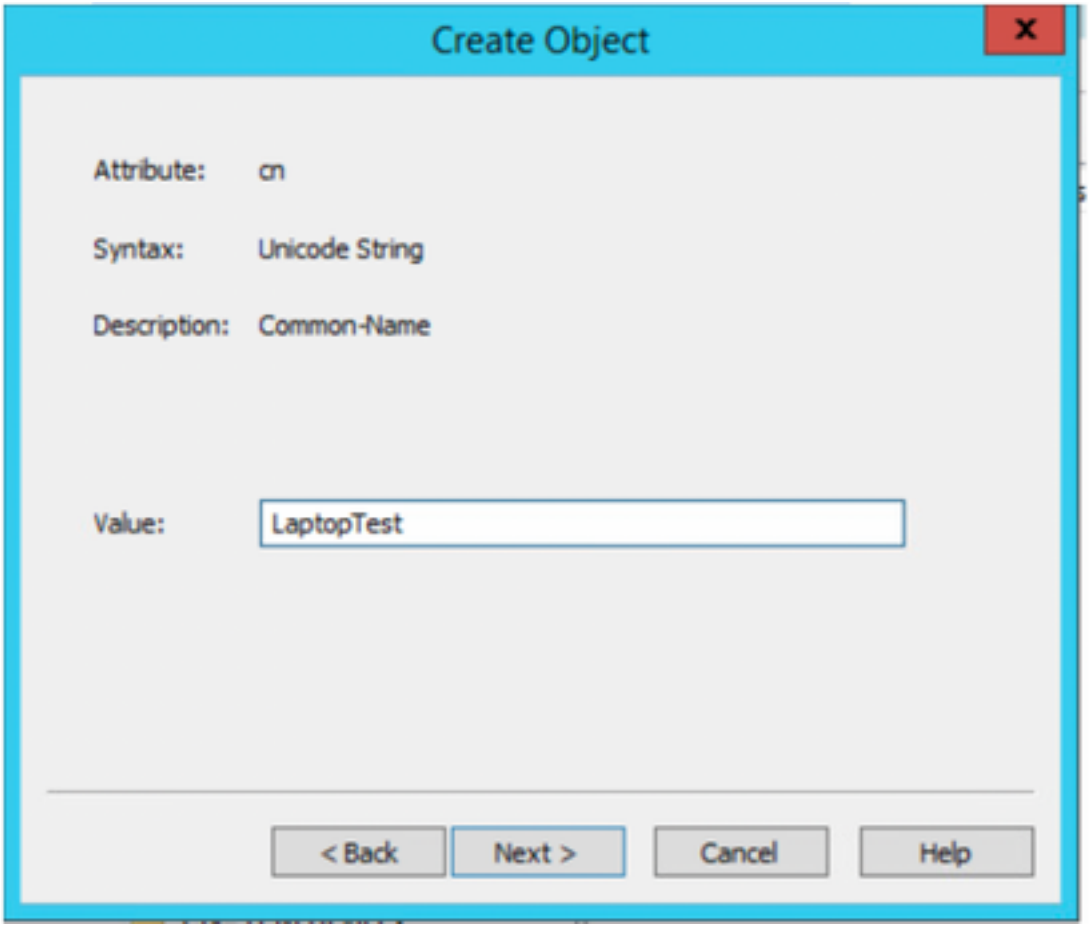
8. Clique com o botão direito do mouse na OrganizationalUnit que acabou de ser criada e selecione **New > Object**



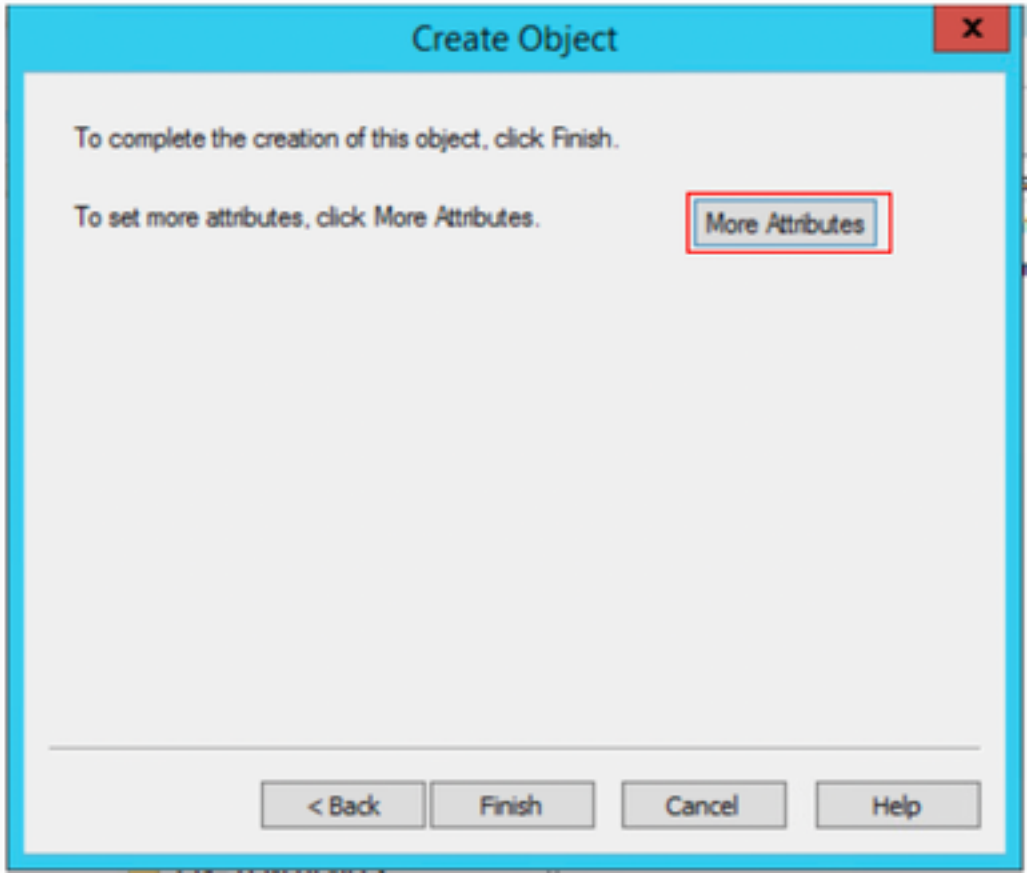
9.Selecione **dispositivo** como classe de objeto e selecione **próximo**



10.Defina um nome no campo Valor e selecione **Avançar**

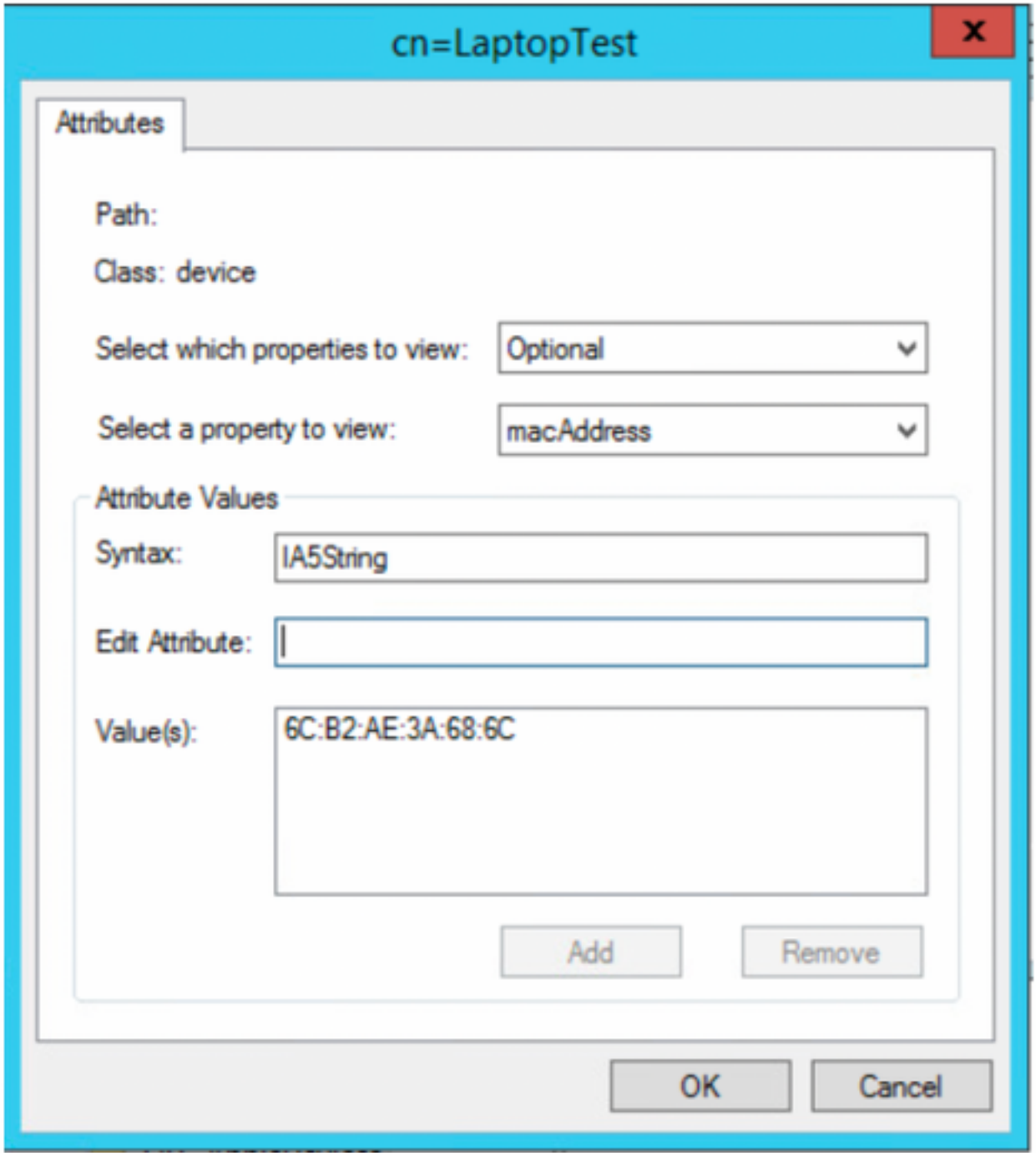


11. Selecione a opção **Mais atributos**



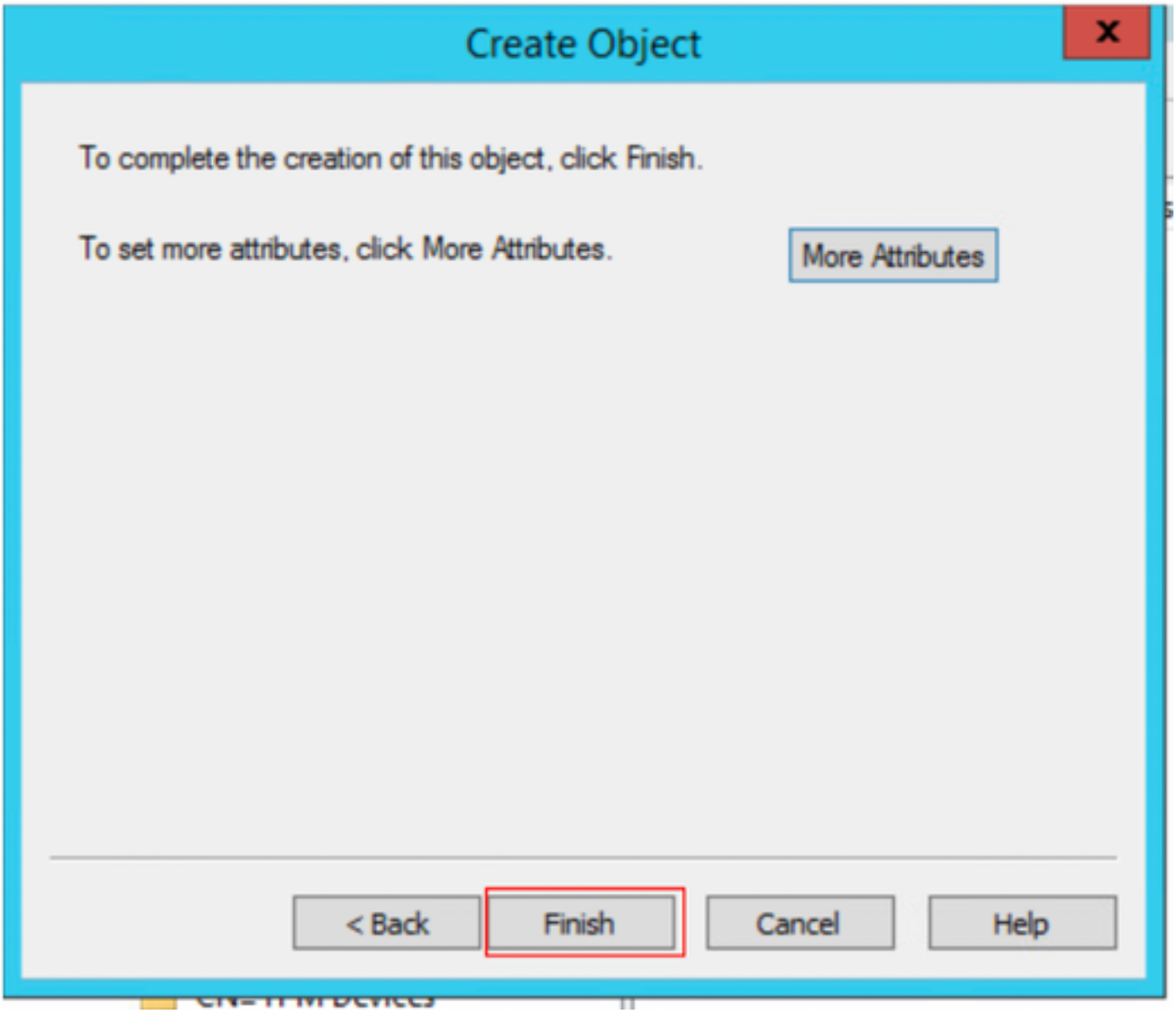
11. No menu suspenso, **selecione uma propriedade para exibir**, selecione a opção **macAddress,** defina o endereço Mac do endpoint que será autenticado no campo **Editar atributo** e selecione o **Adicionar** botão para salvar o endereço mac do dispositivo.

Observação: use dois-pontos em vez de pontos ou hífen entre octetos de endereços mac.

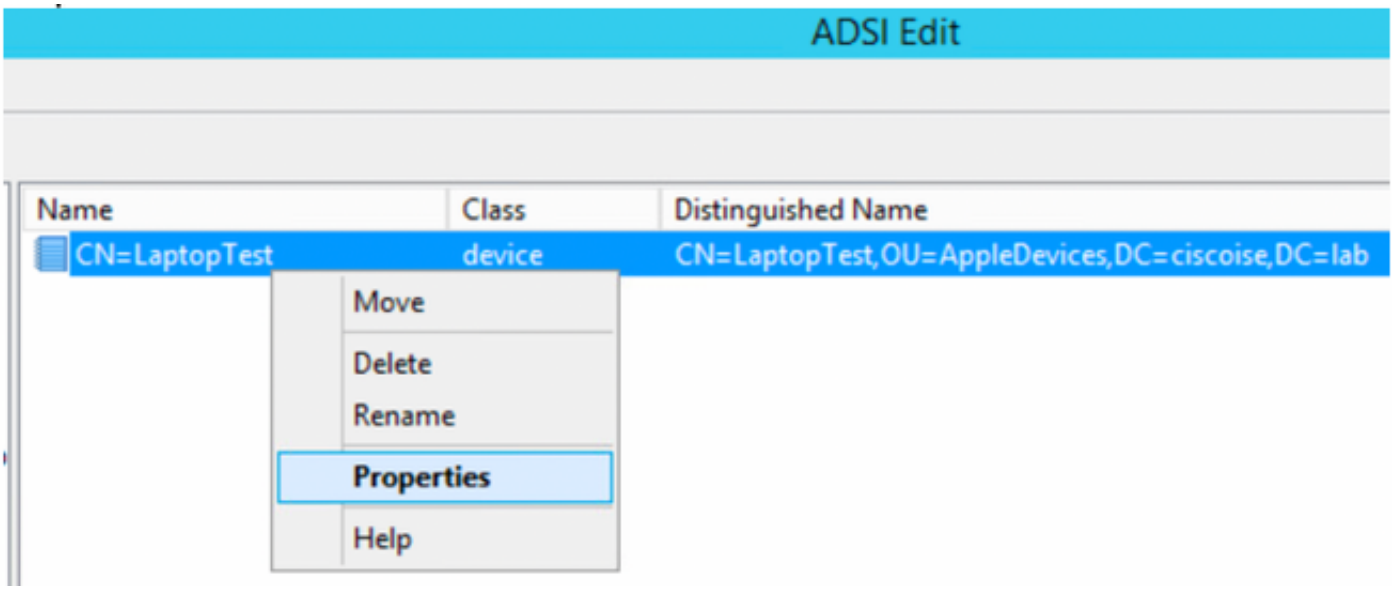


12. Selecione **OK** para salvar as informações e continuar com a configuração do objeto de dispositivo

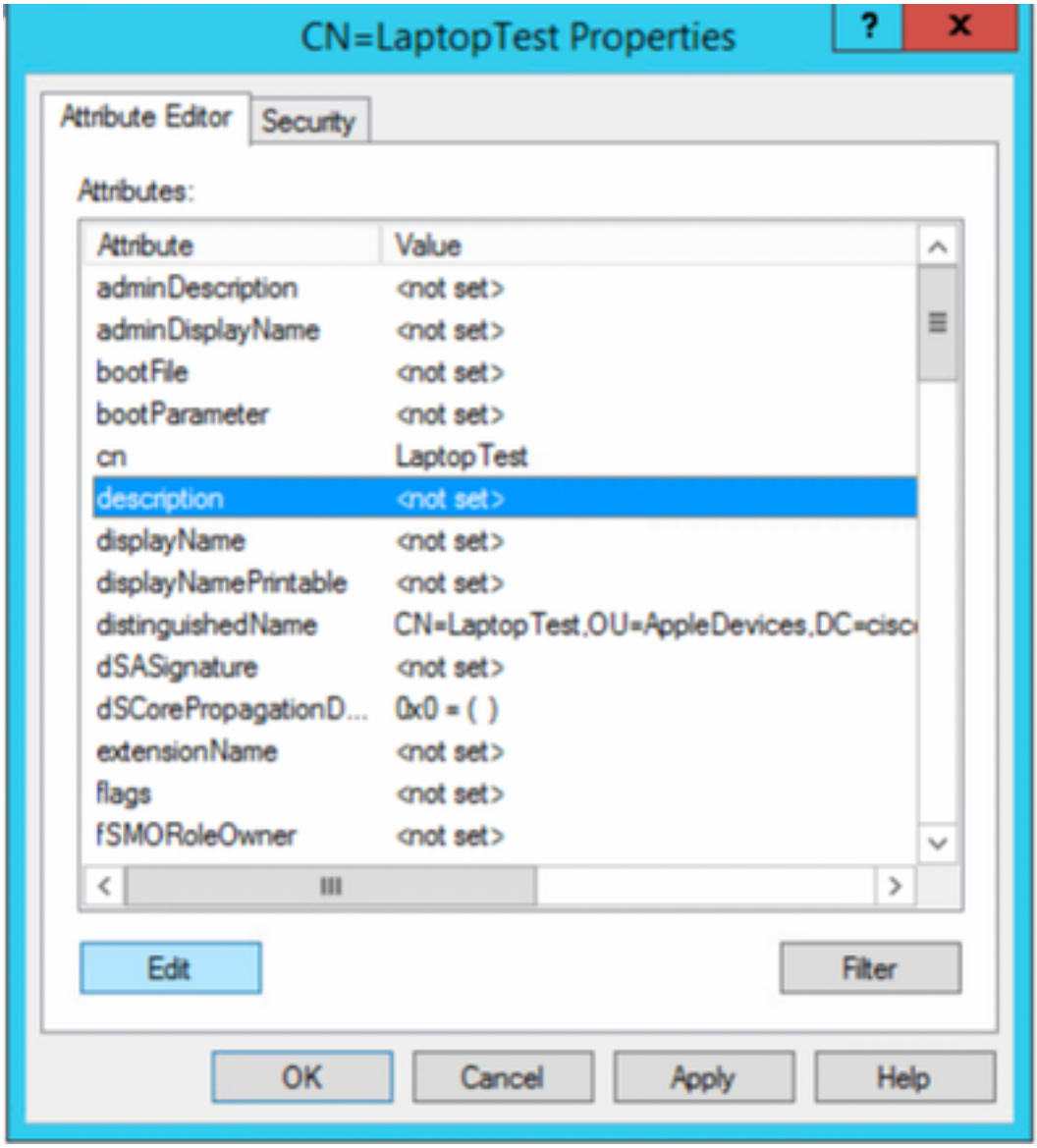
13. Selecione **Concluir** para criar o novo dispositivo Object



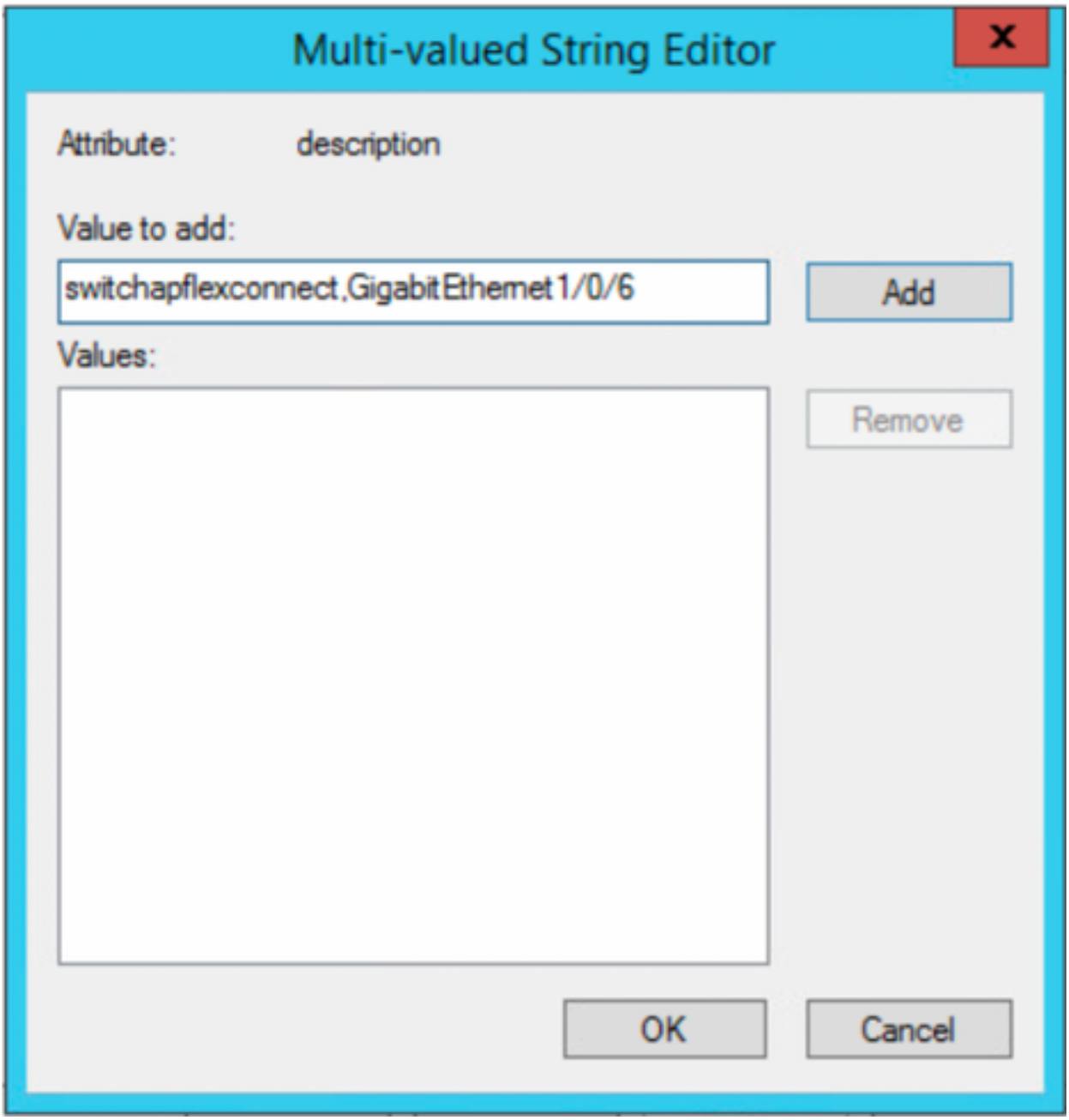
14. Clique com o botão direito do mouse no objeto do dispositivo e selecione a opção **Propriedades**



15. Selecione a **descrição** da opção e selecione **Editar** para definir o nome do switch e a porta do switch onde o dispositivo será conectado.



16. Defina o nome do switch e a porta do switch. Certifique-se de usar uma vírgula para separar cada valor. Selecione **Adicionar** e **Ok** para salvar as informações.



- **Switchapflexconnect é o nome do switch.**
- **GigabitEthernet1/0/6 é a porta do switch ao qual o endpoint está conectado.**

Note: É possível usar scripts para adicionar atributos a um campo específico, no entanto, para este exemplo, estamos definindo os valores manualmente

Note: O atributo AD diferencia maiúsculas de minúsculas, se você usar todos os endereços Mac em minúsculas, o ISE converte em maiúsculas durante a consulta LDAP. Para evitar esse comportamento, Desative a pesquisa de host de processo em protocolos permitidos. Os detalhes podem ser encontrados neste link: https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

Configuração do Switch

O seguinte descreve a configuração para comunicação 802.1x entre o ISE e o 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
```

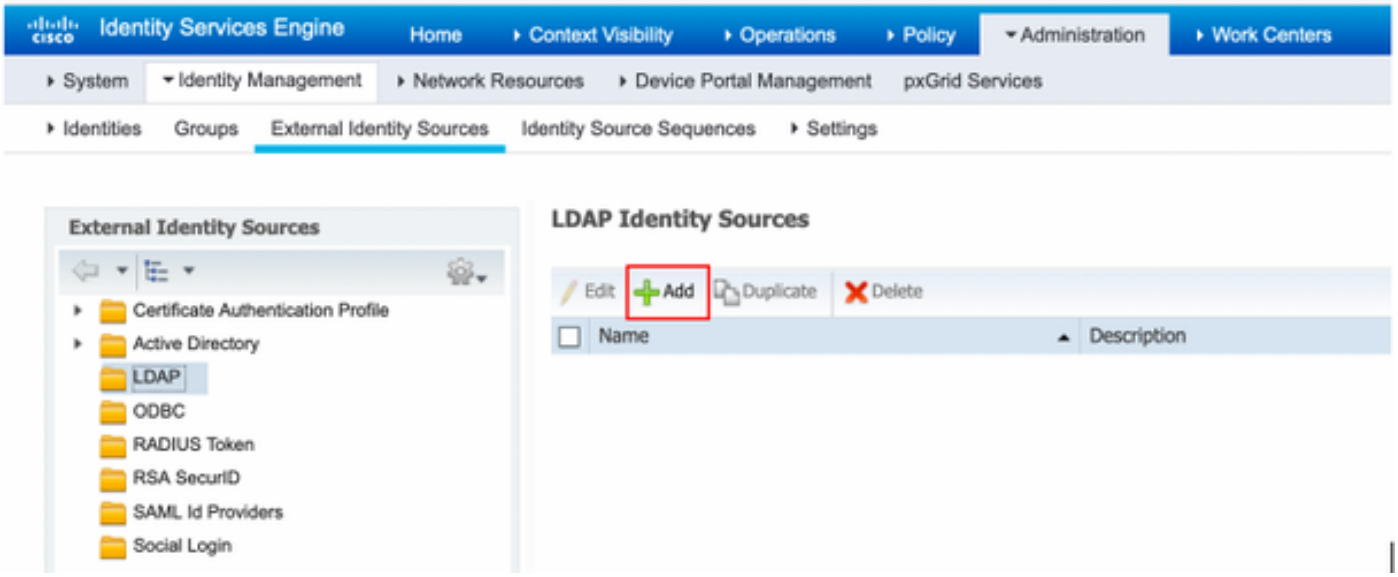
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access 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: A configuração global e da interface pode precisar ser ajustada em seu ambiente

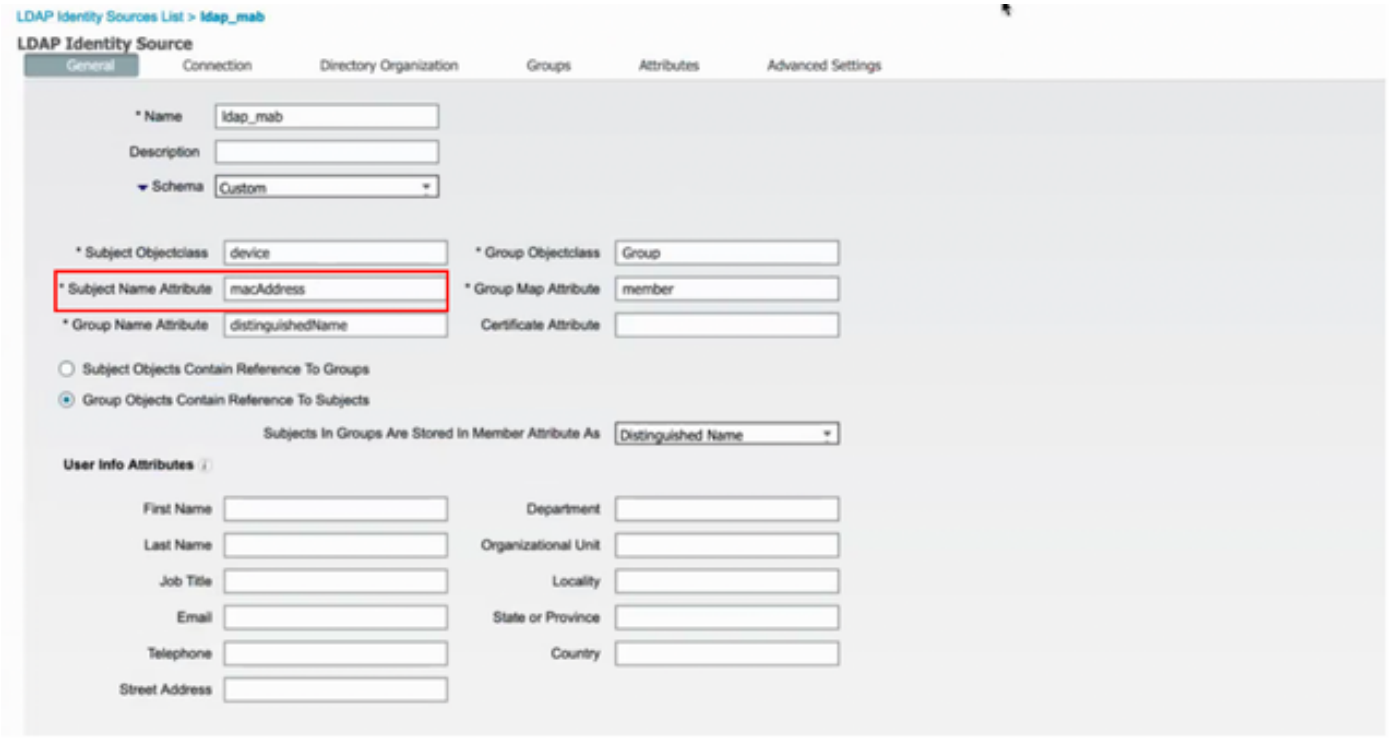
Configuração do ISE

O seguinte descreve a configuração no ISE para obter os atributos do servidor LDAP e configurar as políticas do ISE.

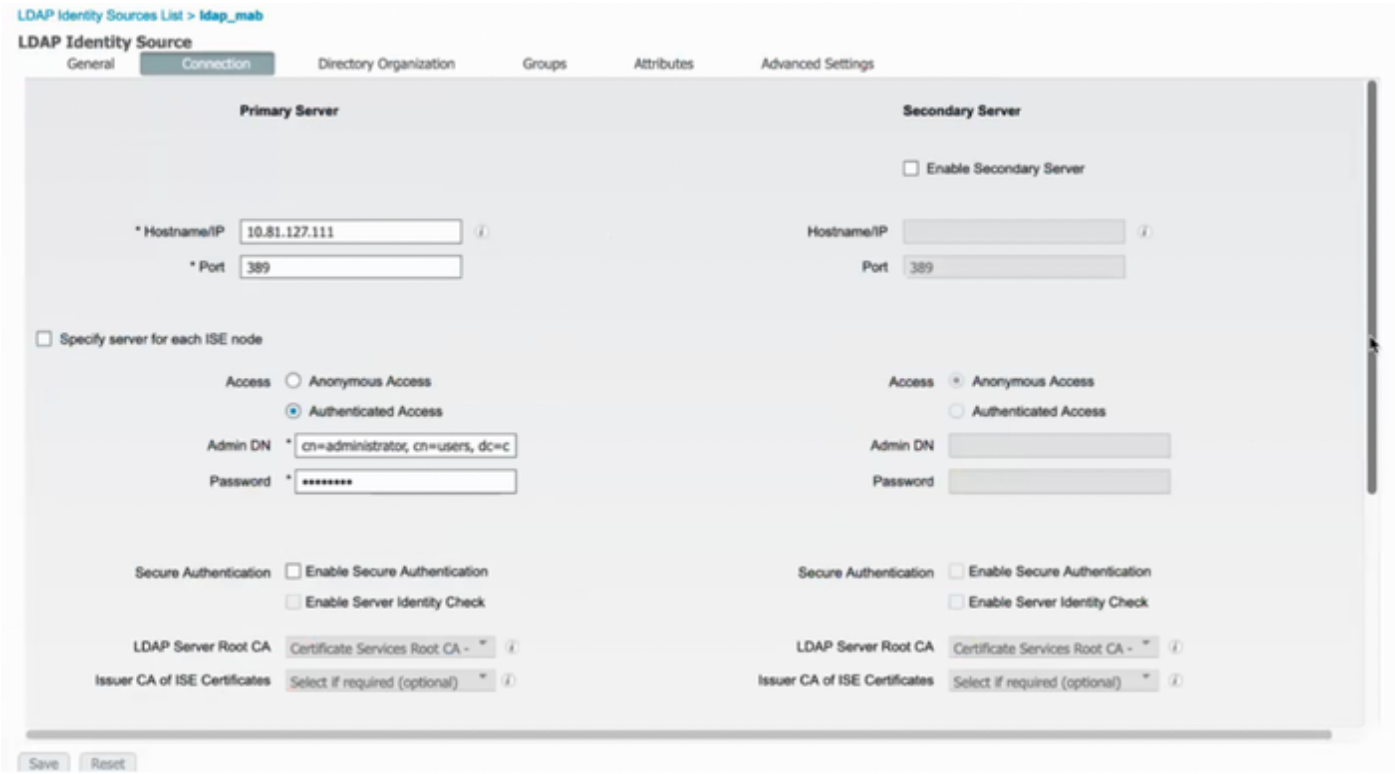
1. No ISE, vá para **Administration->Identity Management->External Identity Sources** e selecione a pasta **LDAP** e clique em **Add** para criar uma nova conexão com LDAP



2.Na guia **Geral**, defina um nome e selecione o endereço mac como Atributo do Nome do Assunto

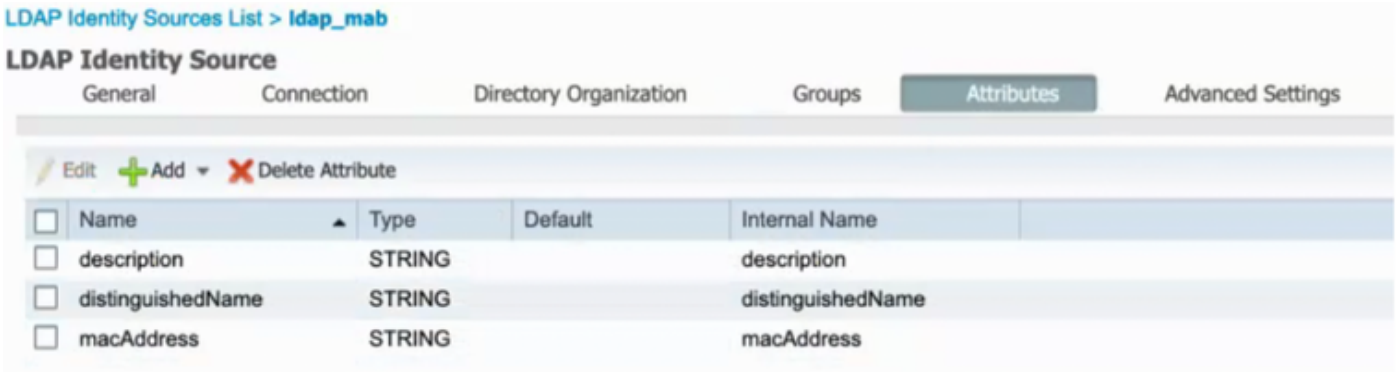


3. Na guia **Connection**, configure o endereço IP, o DN do administrador e a senha do servidor LDAP para obter uma conexão bem-sucedida.

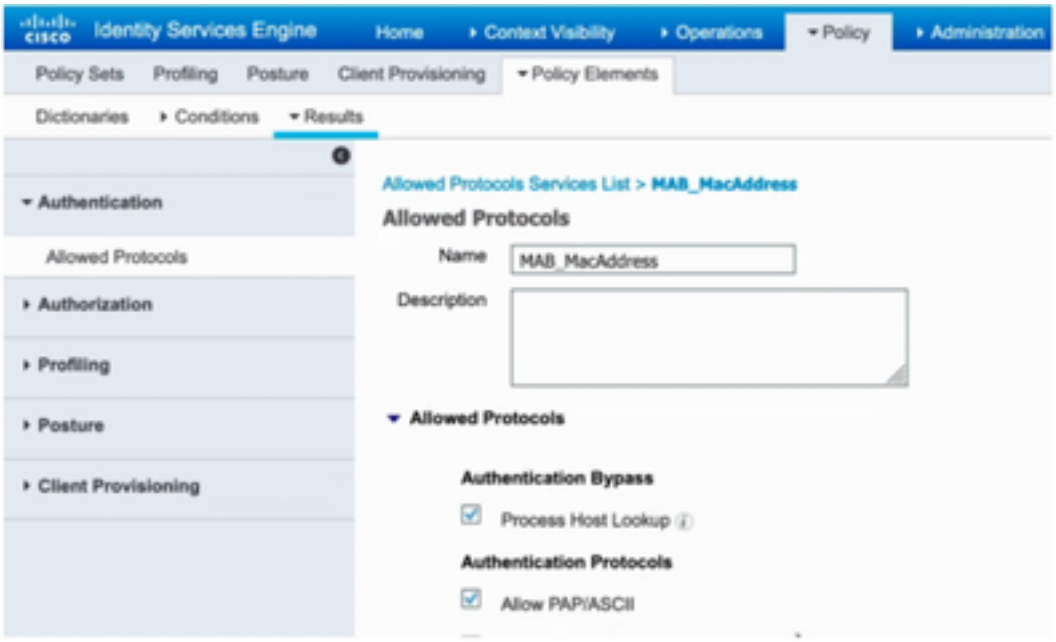


Note: A porta 389 é a porta padrão usada.

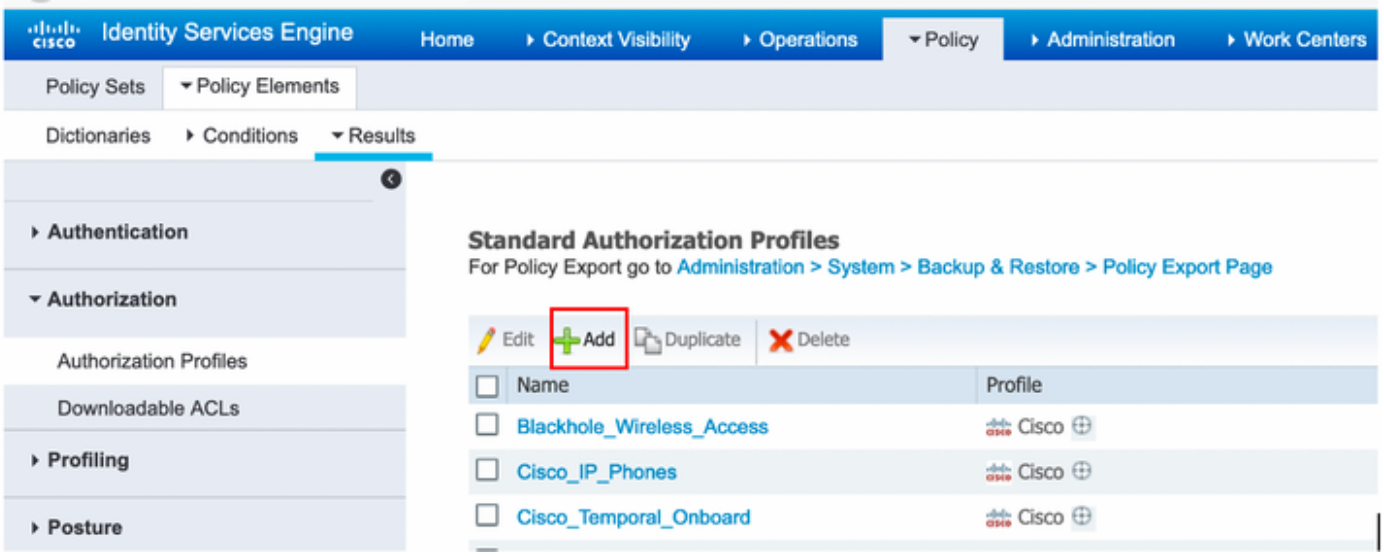
4. Na guia **Attributes** selecione os atributos macAddress e description, esses atributos serão usados na política de autorização

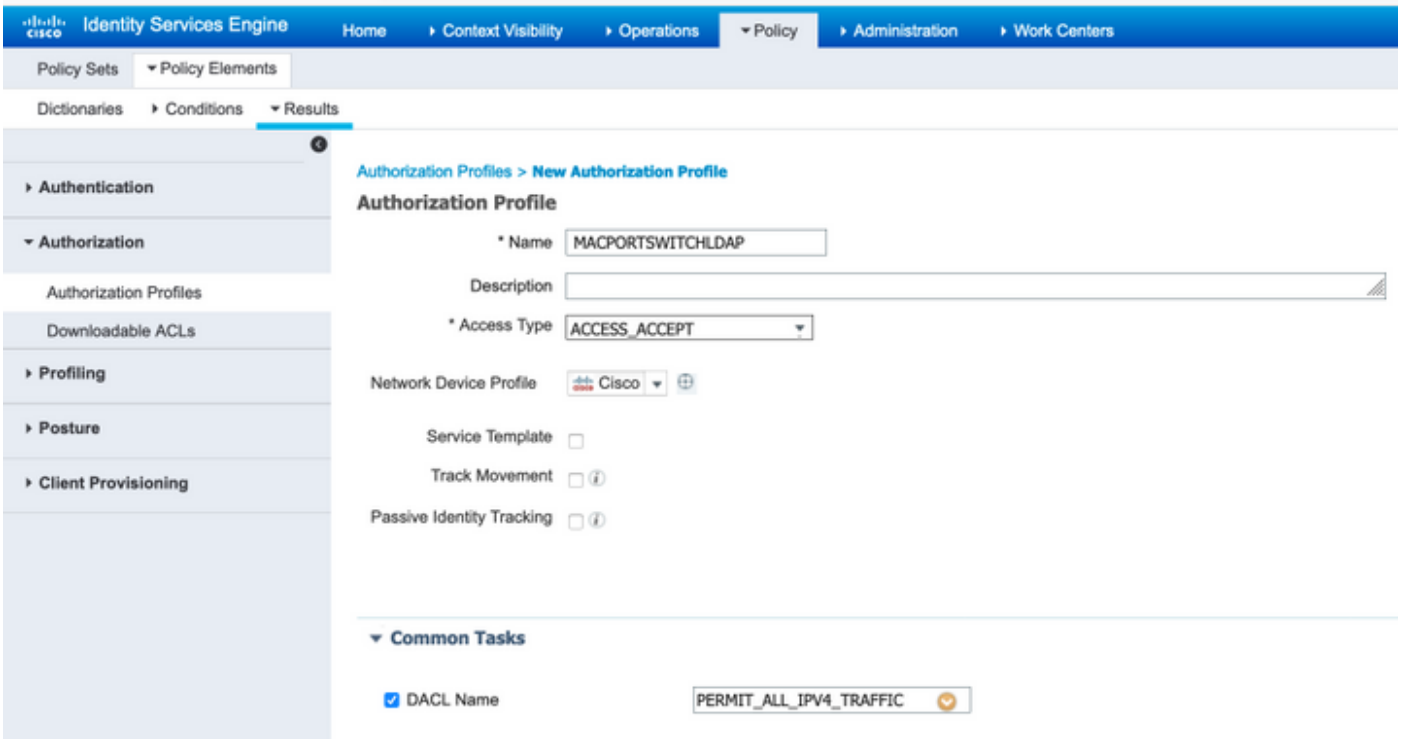


5. Para criar um protocolo permitido, vá para **Policy->Policy Elements->Results->Authentication->Allowed Protocols.** Defina e selecione Process Host Lookup e Allow PAP/ASCII como os únicos protocolos permitidos. Finalmente, selecione **Salvar**

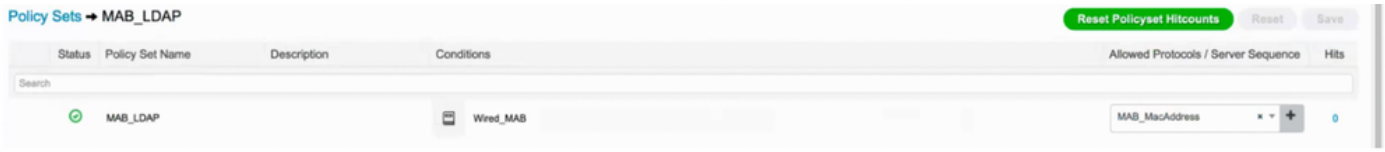


6. Para criar um perfil de autorização, vá para **Policy->Policy Elements->Results->Authorization->Authorization Profiles.** Selecione **Adicionar** e defina as permissões que serão atribuídas ao ponto final.

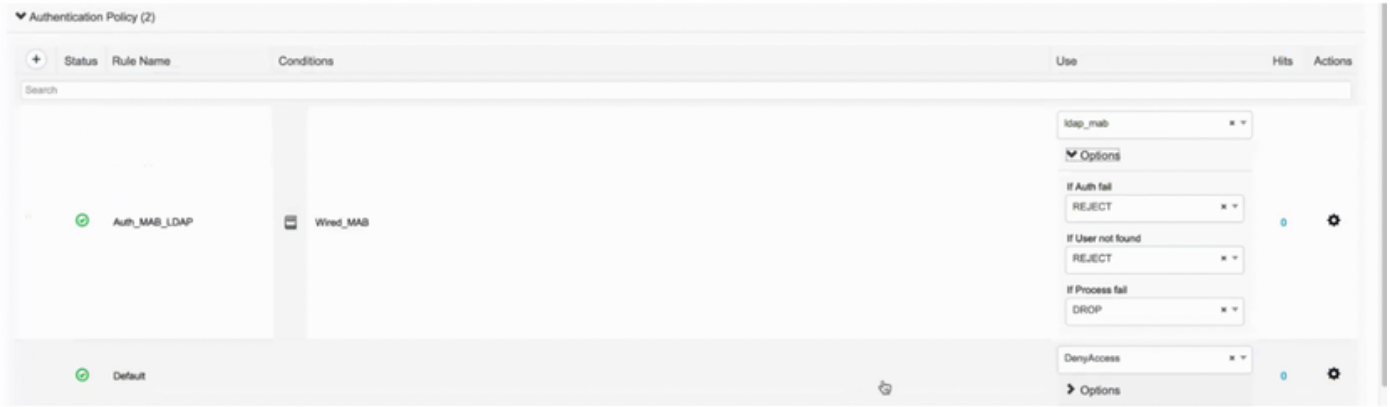




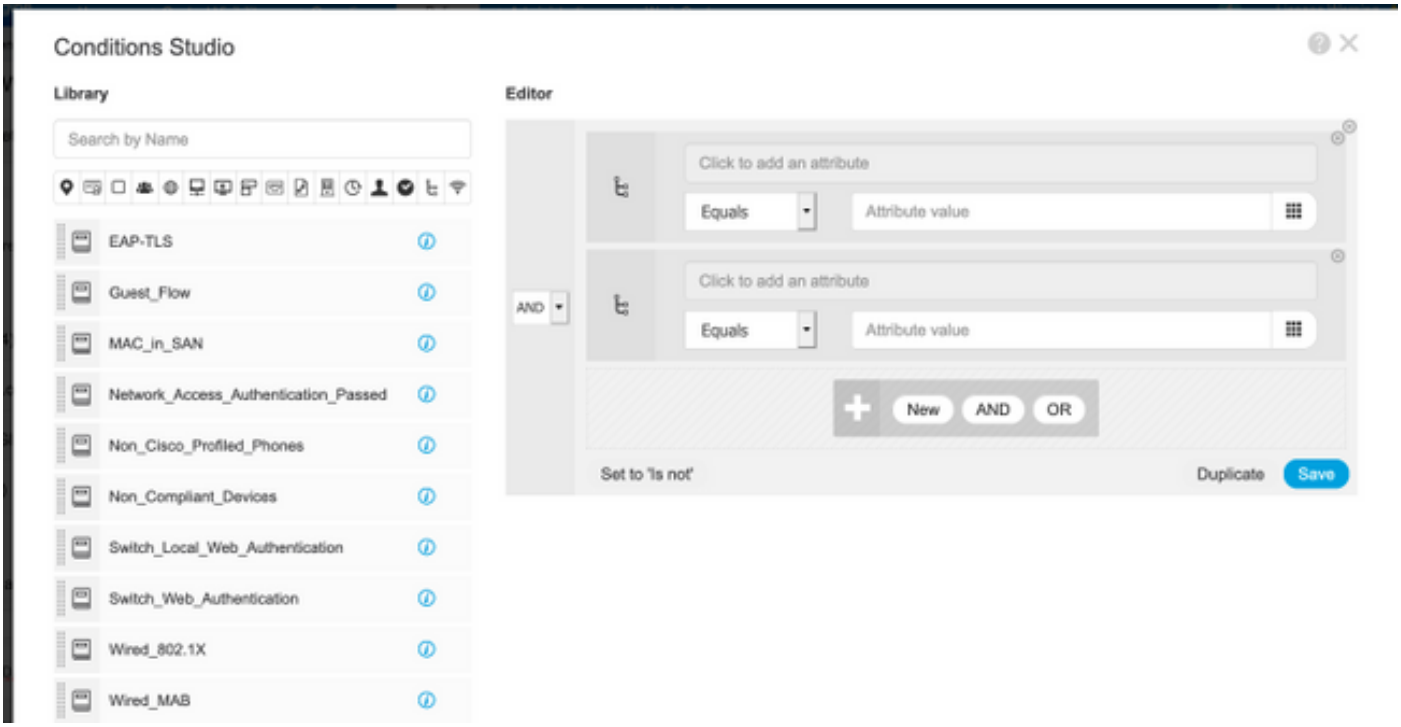
7.Vá para Policy-> Policy Set e crie um conjunto de políticas usando a condição predefinida Wired_MAB e o Allowed Protocol criado na etapa 5.

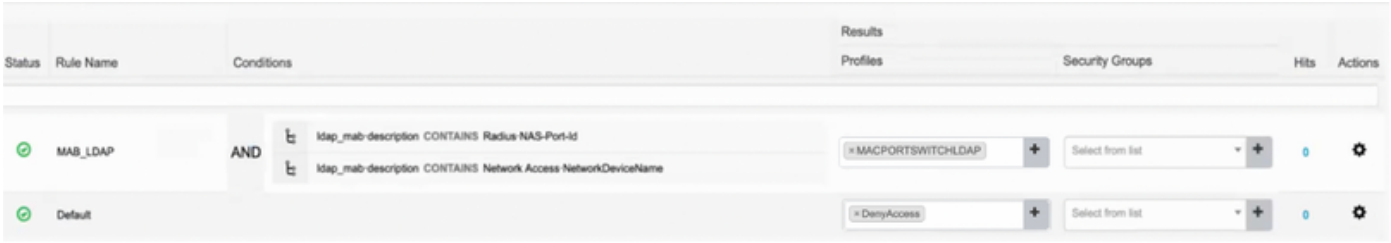


8.No novo conjunto de políticas criado, crie uma política de autenticação usando a biblioteca **Wired_MAB** predefinida e a conexão **LDAP** como sequência de origem de identidade externa



9. Em **Authorization Policy**, defina um nome e crie uma condição composta usando a descrição de atributo LDAP, Radius NAS-Port-Id e NetworkDeviceName. Finalmente, adicione o perfil de autorização criado na etapa 6.





Depois de aplicar a configuração, você deve ser capaz de se conectar à rede sem intervenção do usuário.

Verificar

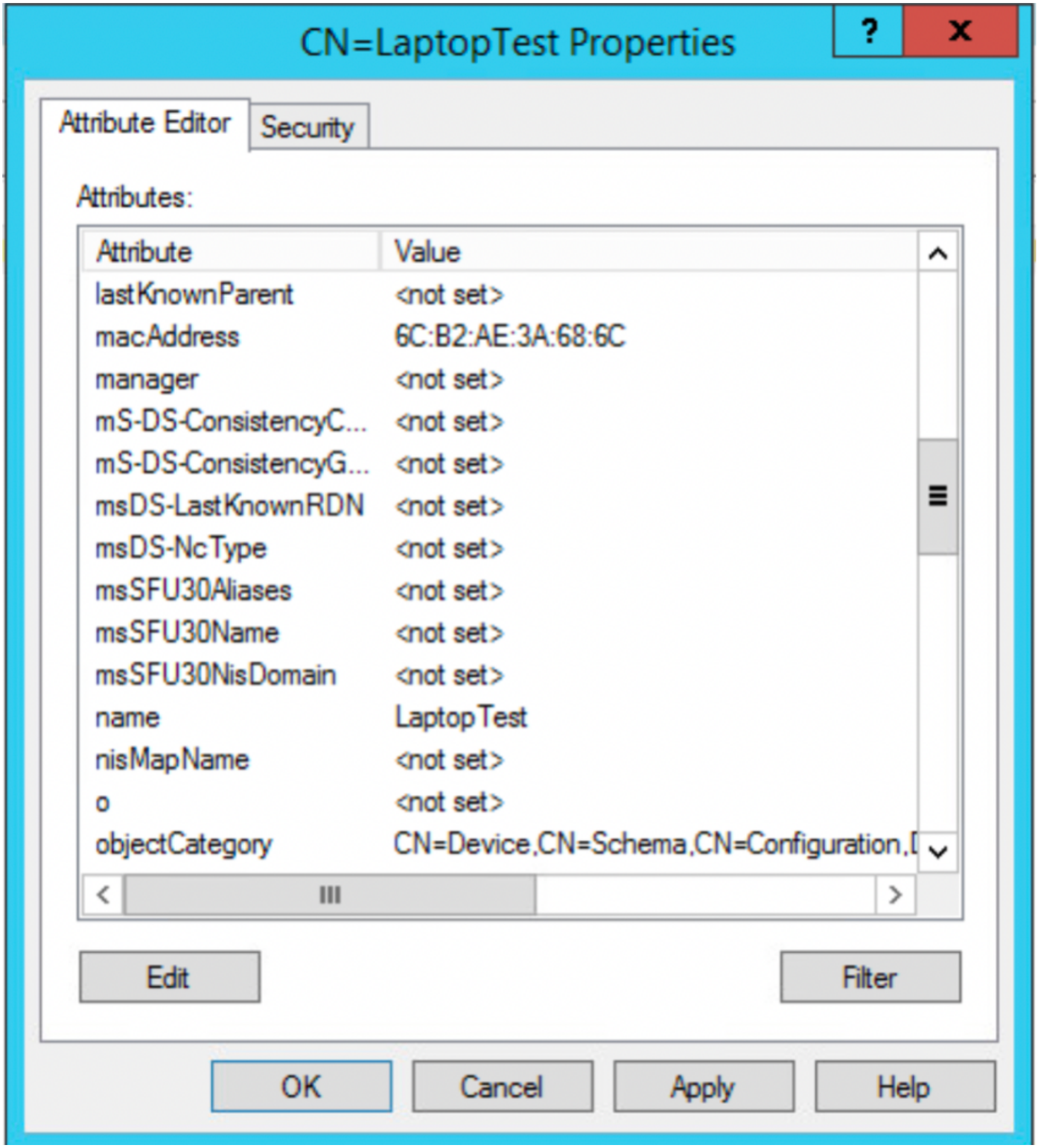
Depois de conectado à porta do switch designado, você pode digitar **show authentication session interface GigabitEthernet X/X/X** para validar o status de autenticação e autorização do dispositivo.

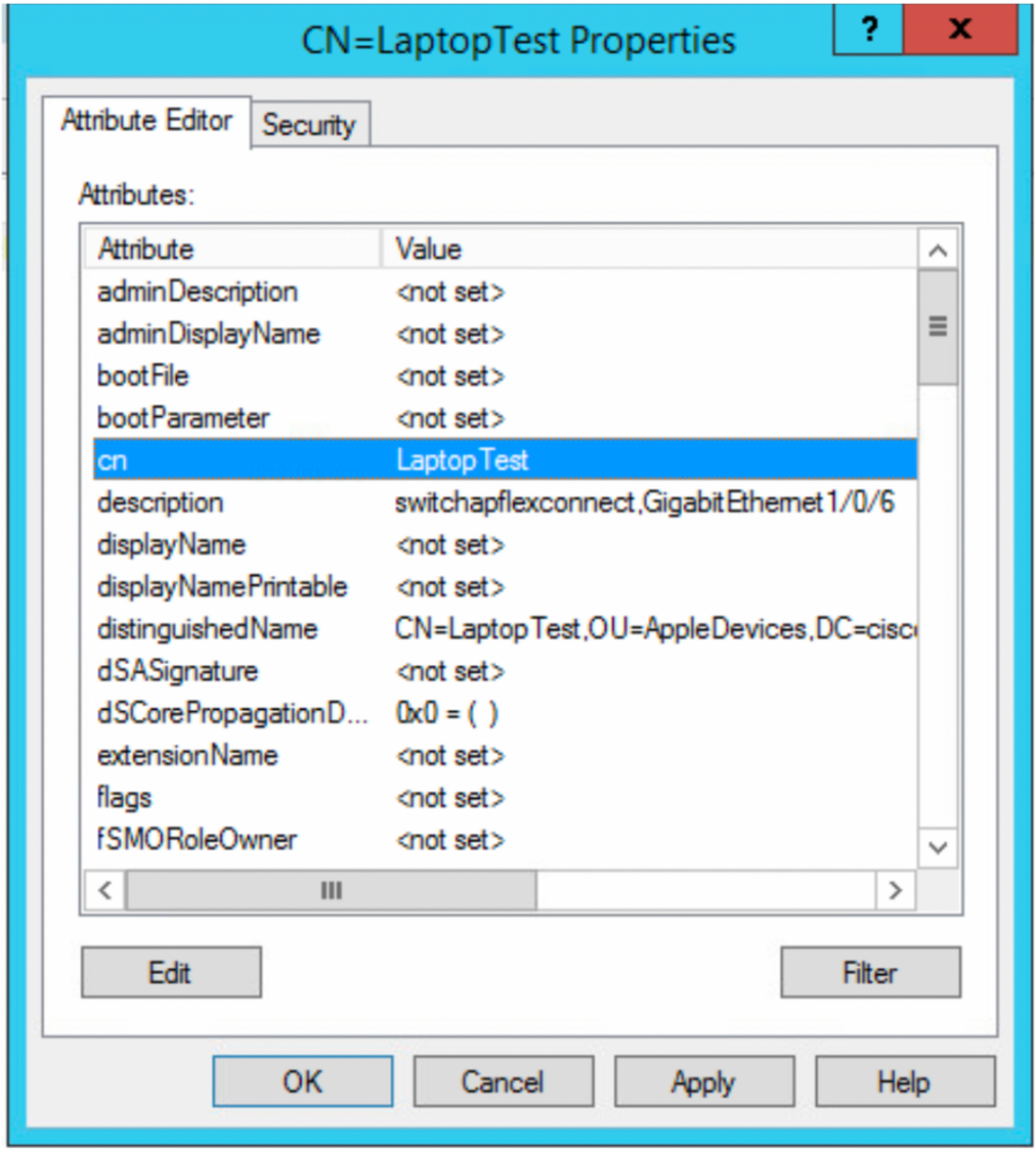
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session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

No ISE, você pode usar os registros ao vivo do Radius para confirmação.

Troubleshoot

No servidor LDAP, verifique se o dispositivo criado tem endereço Mac, nome de switch apropriado e porta de switch configurados


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



No ISE, você pode capturar um pacote (Vá para **Operations->Troubleshoot->Diagnostic Tool->TCP Dumps**) para validar os valores que estão sendo enviados do LDAP ao ISE