Autenticación basada en atributos de ISE y LDAP

Contenido

Introducción

Este documento describe cómo configurar Cisco Identity Services Engine (ISE) y utilizar atributos de objetos LDAP (protocolo ligero de acceso a directorios) para autenticar y autorizar dispositivos dinámicamente.

> **Nota: Este documento es válido para configuraciones que utilizan LDAP como origen de identidad externo para la autenticación y autorización de ISE.**

Colaboración de Emmanuel Cano y Mauricio Ramos Ingeniero de Servicios Profesionales de Cisco.

Editado por Neri Cruz, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que conozca los siguientes temas:

- Conocimiento básico de las políticas de ISE, autenticación y autorización
- Omisión de autenticación MAC (MAB)
- Conocimiento básico del protocolo Radius
- Conocimiento básico del servidor Windows

Componentes Utilizados

La información de este documento se basa en las siguientes versiones de software y hardware:

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

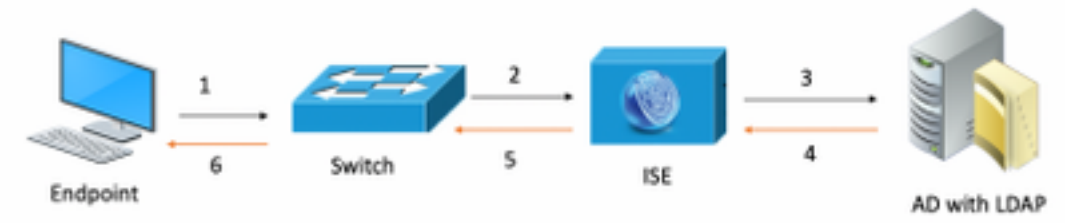
Nota: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuración

Esta sección describe cómo configurar los dispositivos de red, la integración entre ISE y LDAP, y finalmente configurar los atributos LDAP que se utilizarán en la Política de Autorización de ISE.

Diagrama de la red

Esta imagen ilustra la topología de red que se utiliza:



Este es el flujo de tráfico, como se ilustra en el diagrama de red:

1. El usuario conecta su PC/portátil al puerto del switch designado.
2. El switch envía una solicitud de acceso de RADIUS para ese usuario al ISE
3. Cuando el ISE recibe la información, consulta al servidor LDAP para el archivo de usuario específico, que contiene los atributos que se utilizarán en las condiciones de la política de autorización.
4. Una vez que el ISE recibe los atributos (el puerto del switch, el nombre del switch y la dirección mac del dispositivo), compara la información proporcionada por el switch.
5. Si la información de atributos proporcionada por el switch es la misma que la proporcionada por LDAP, el ISE enviará un RADIUS Access-Accept con los permisos configurados en el perfil de autorización.

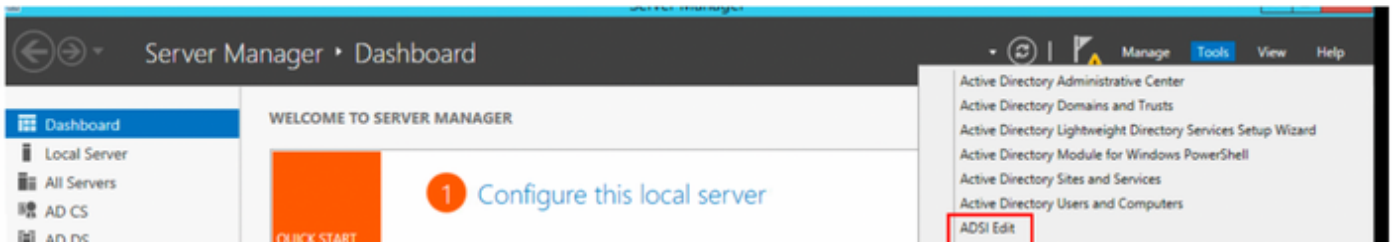
Configuraciones

Utilice esta sección para configurar el LDAP, el switch y el ISE.

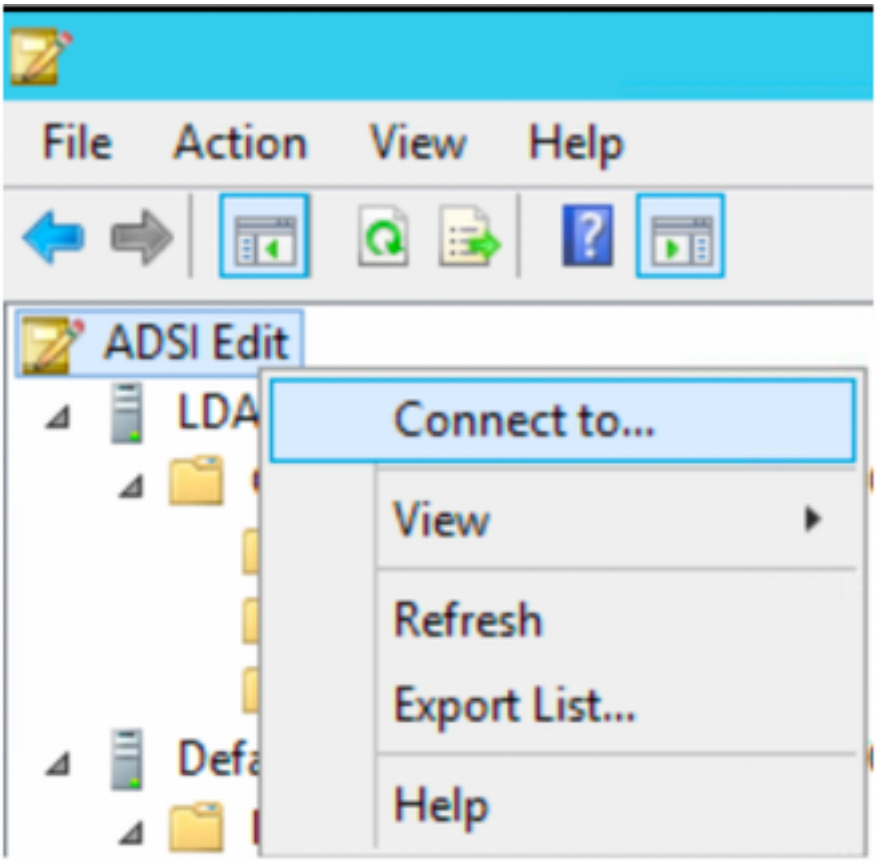
Configurar LDAP

Complete los siguientes pasos para configurar el servidor LDAP:

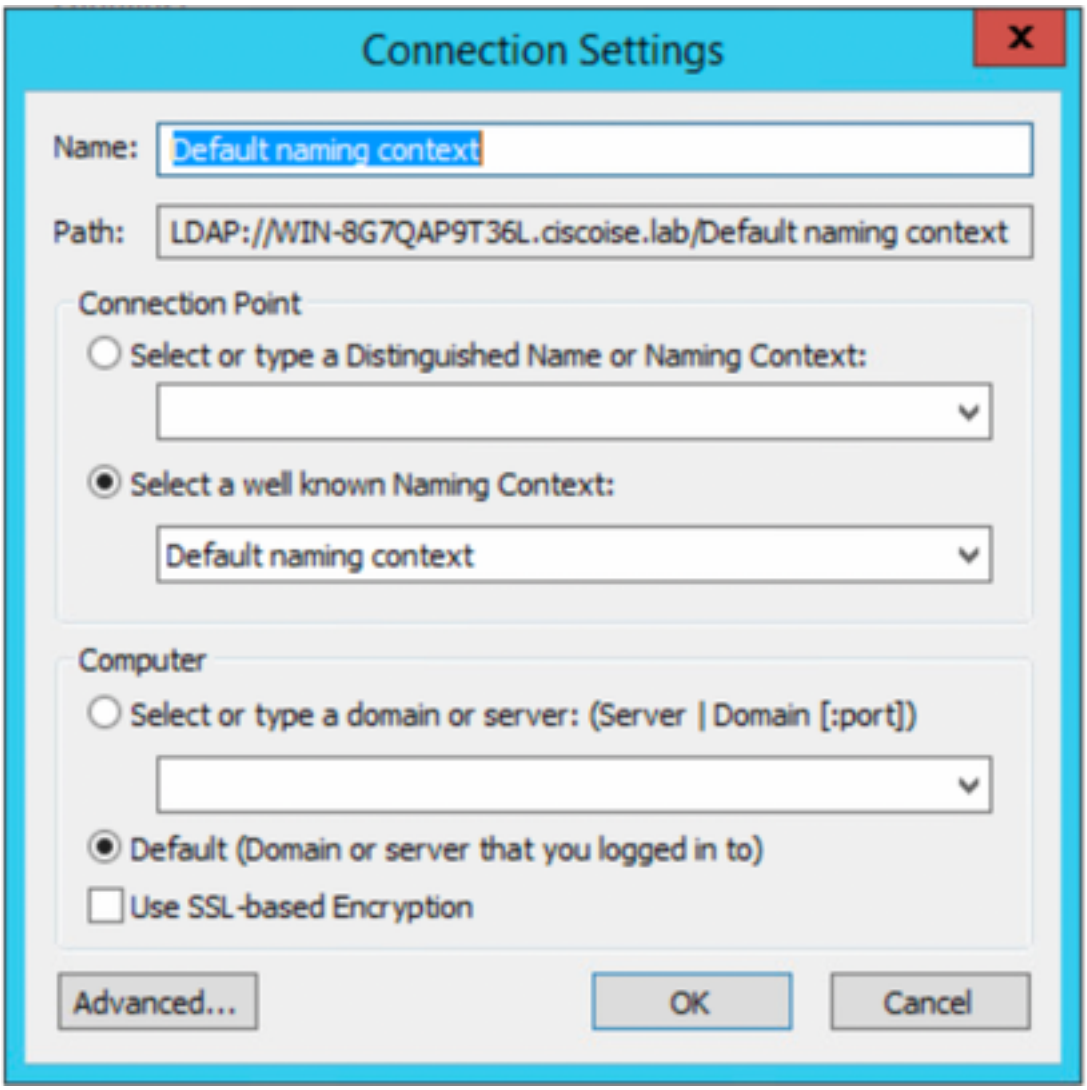
1. Vaya a **Administrador de servidores > Panel > Herramientas > Editar ADSI**



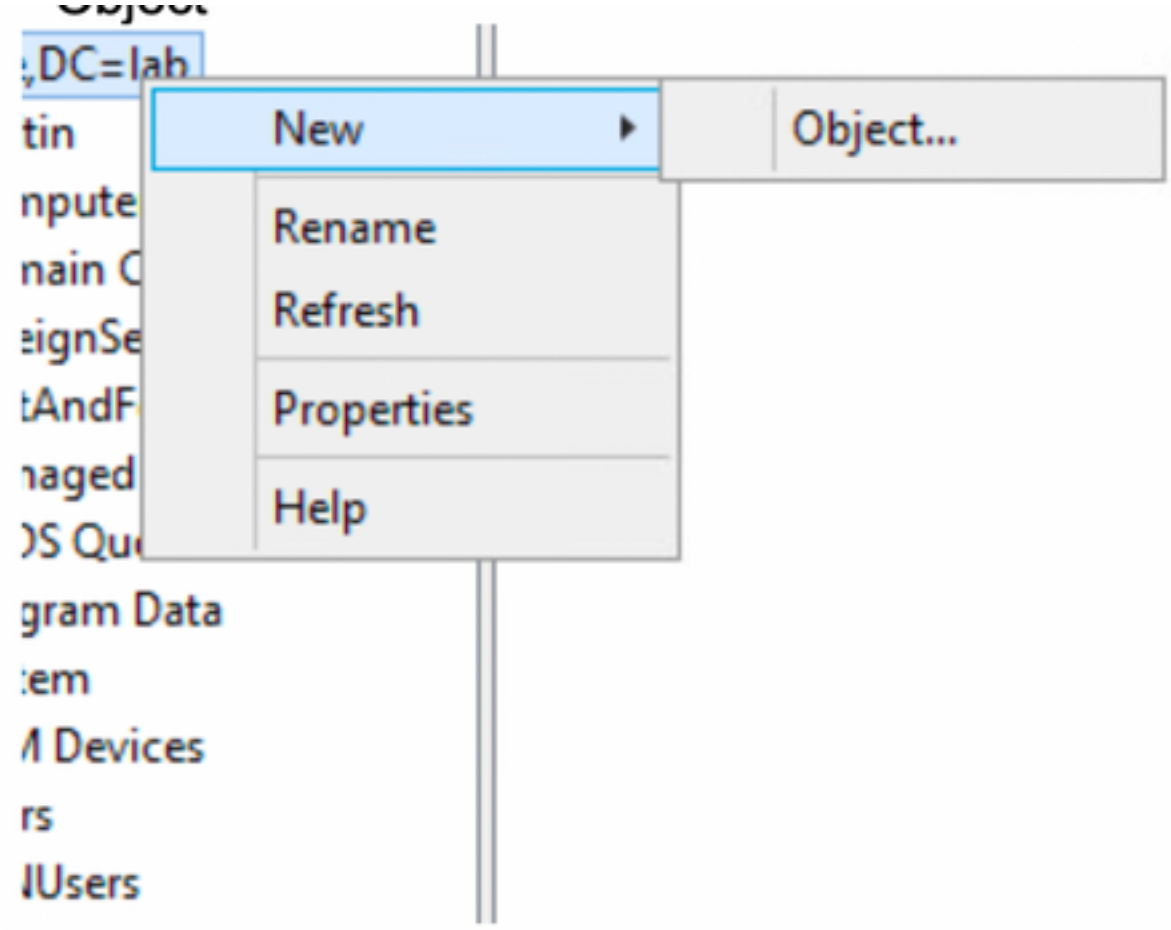
2. Haga clic con el botón derecho del ratón en el icono de edición ADSI y seleccione **Conectar a...**



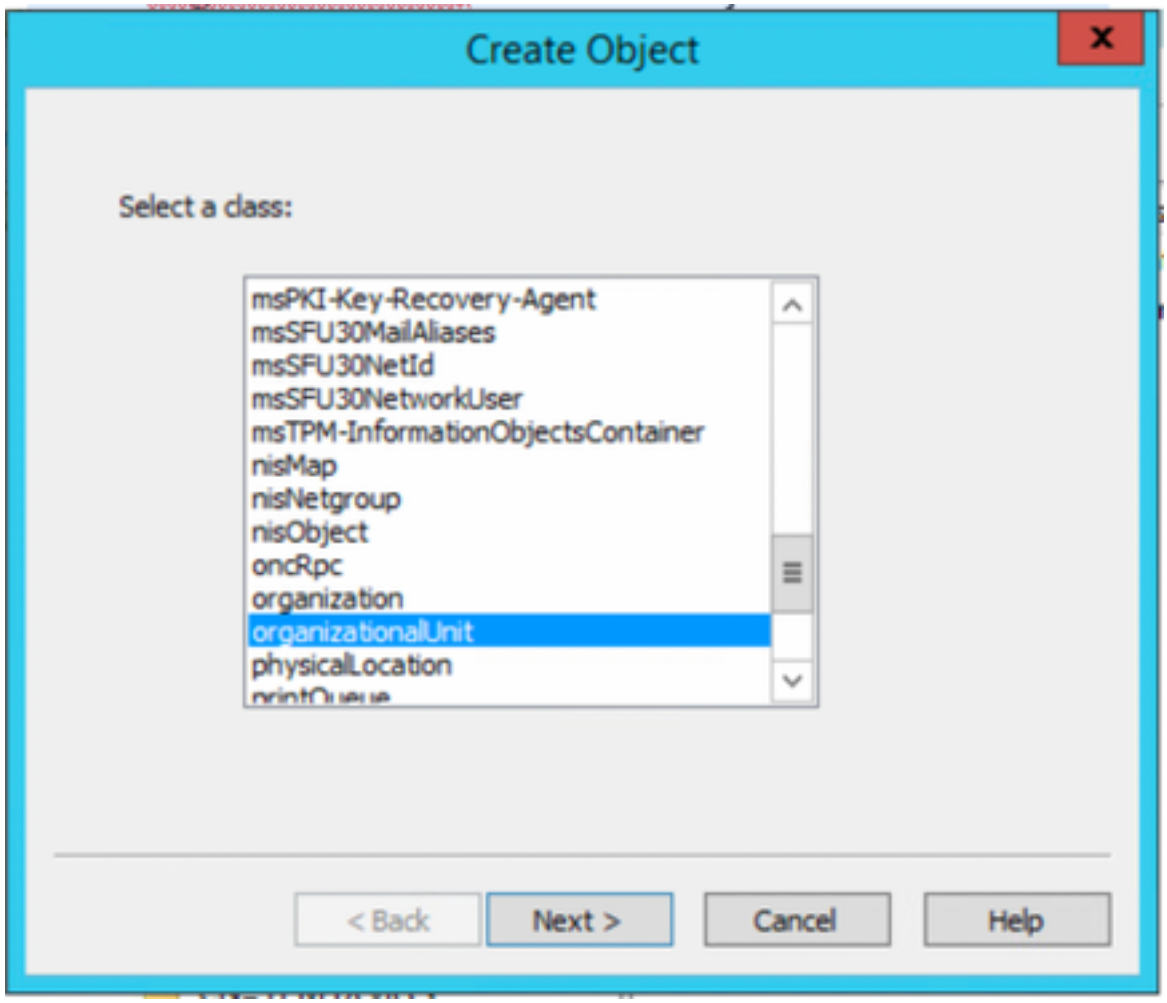
3. En la configuración de conexión, defina un nombre y seleccione el botón **Aceptar** para iniciar la conexión.



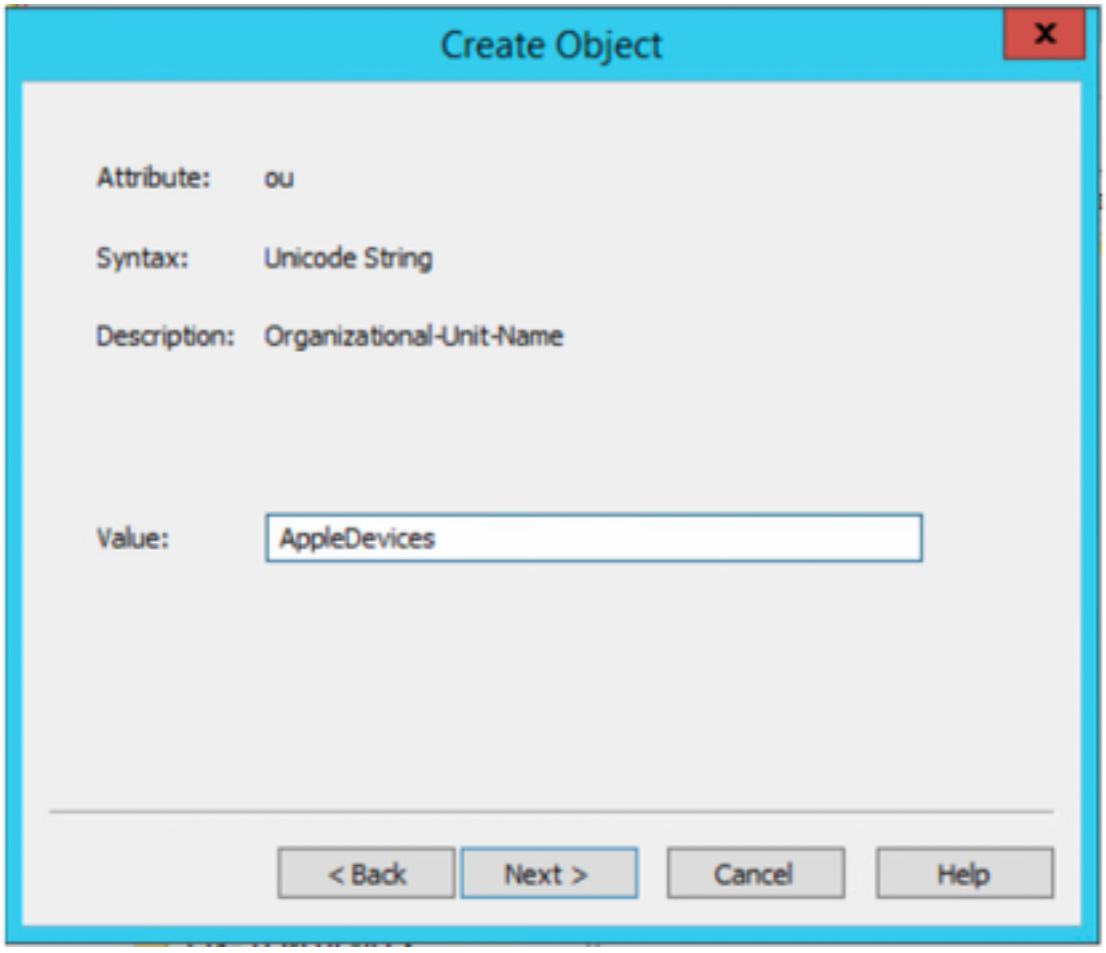
4. En el mismo menú de edición ADSI, haga clic con el botón derecho del ratón en la conexión DC (DC=ciscodemo, DC=lab), seleccione **Nuevo y**, a continuación, seleccione la opción **Objeto**



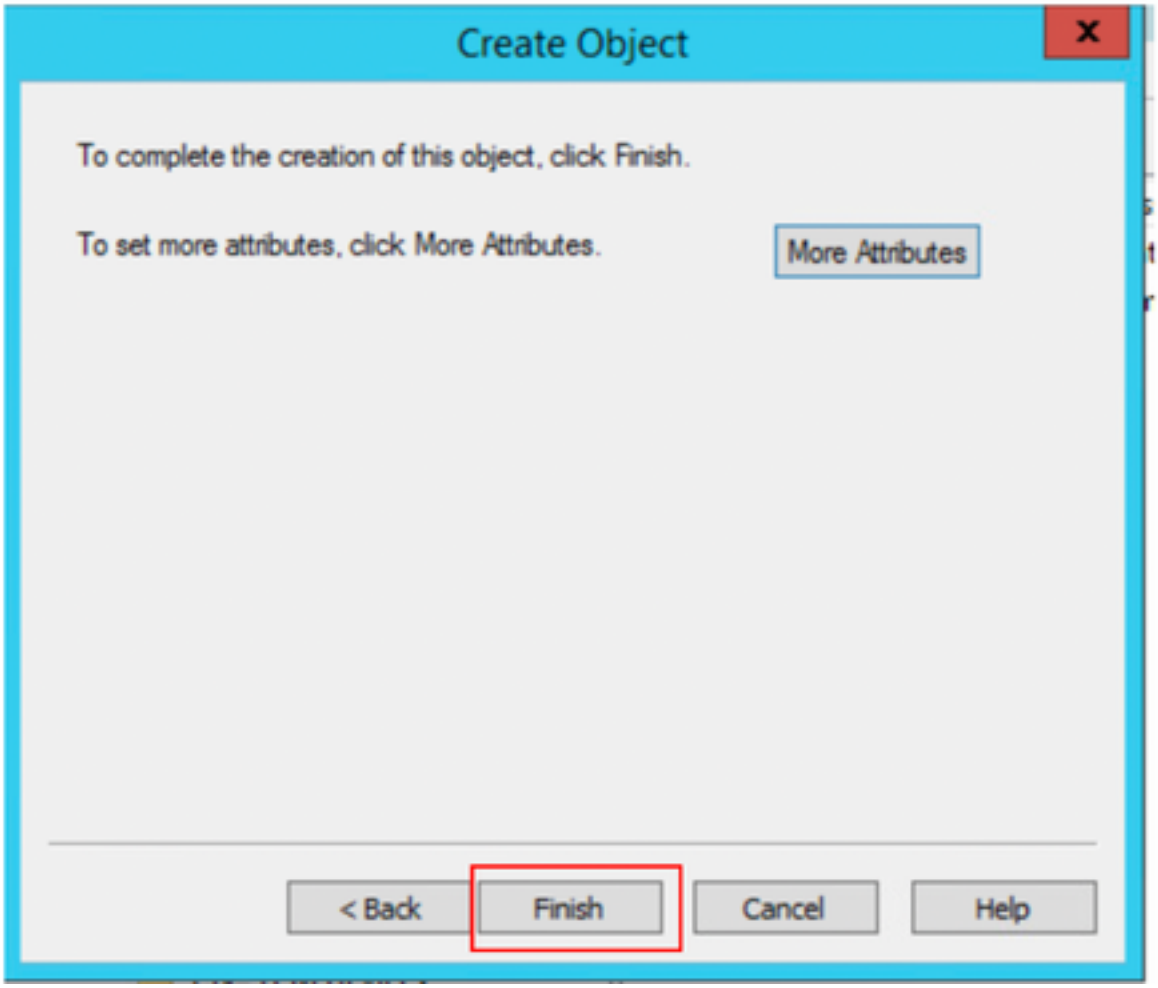
5. Seleccione la opción **OrganizationalUnit** como el nuevo objeto y seleccione **siguiente.**



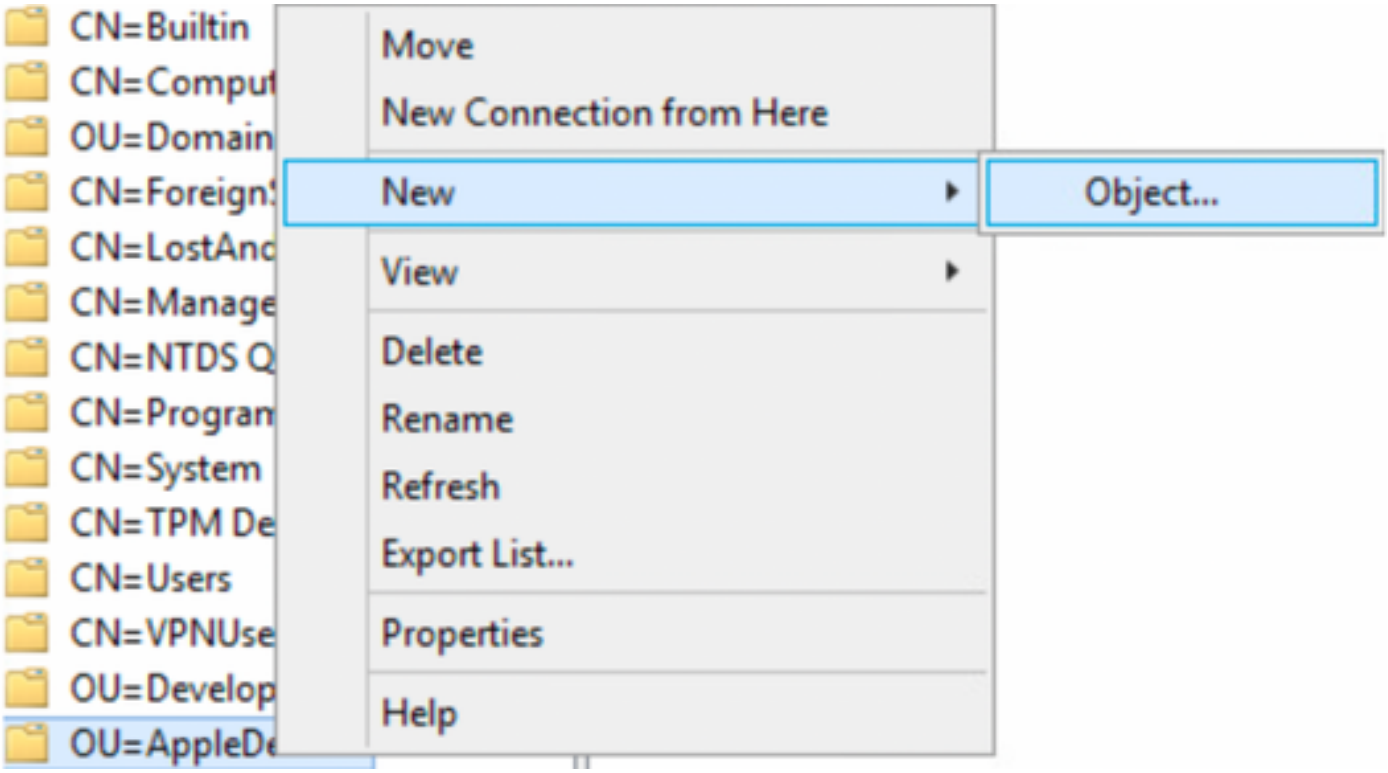
6. Defina un nombre para la nueva OrganizationalUnit y seleccione **Siguiente**



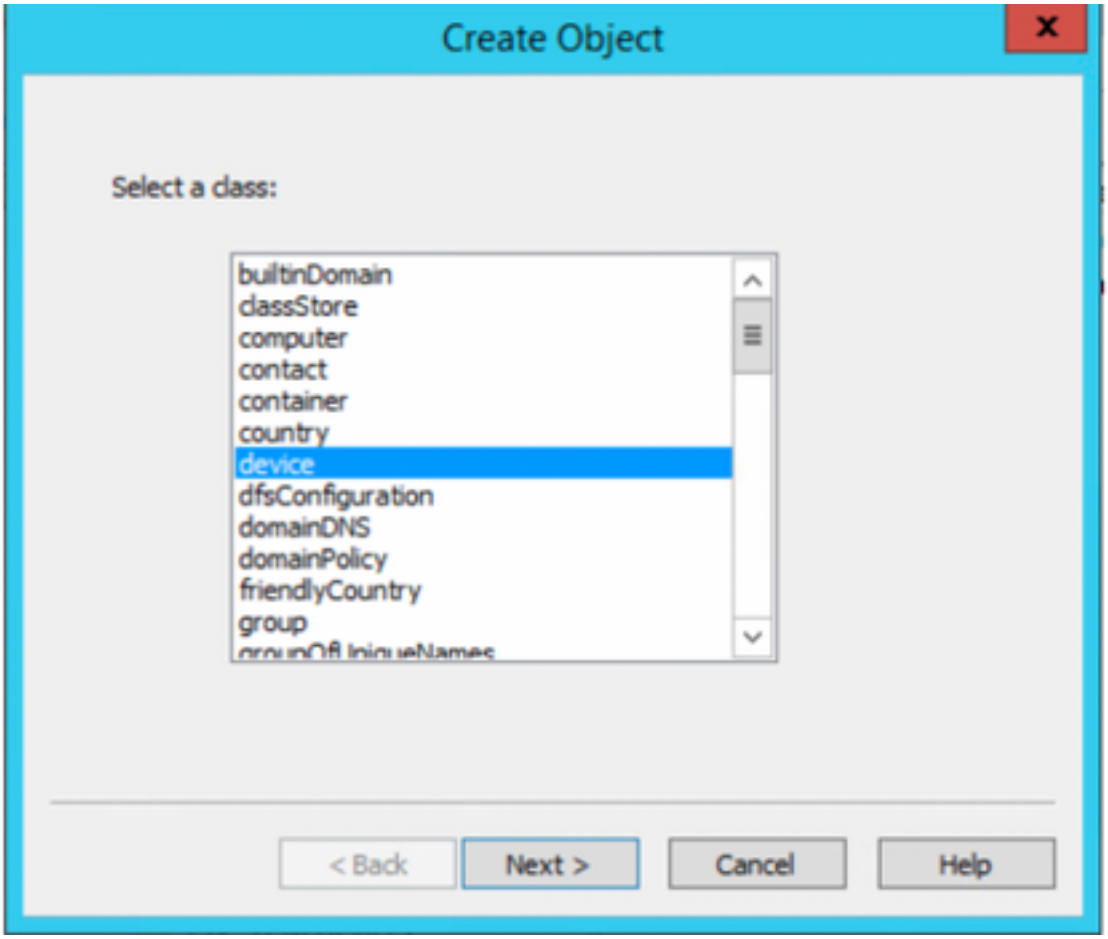
7. Seleccione **Finalizar** para crear la nueva unidad organizativa



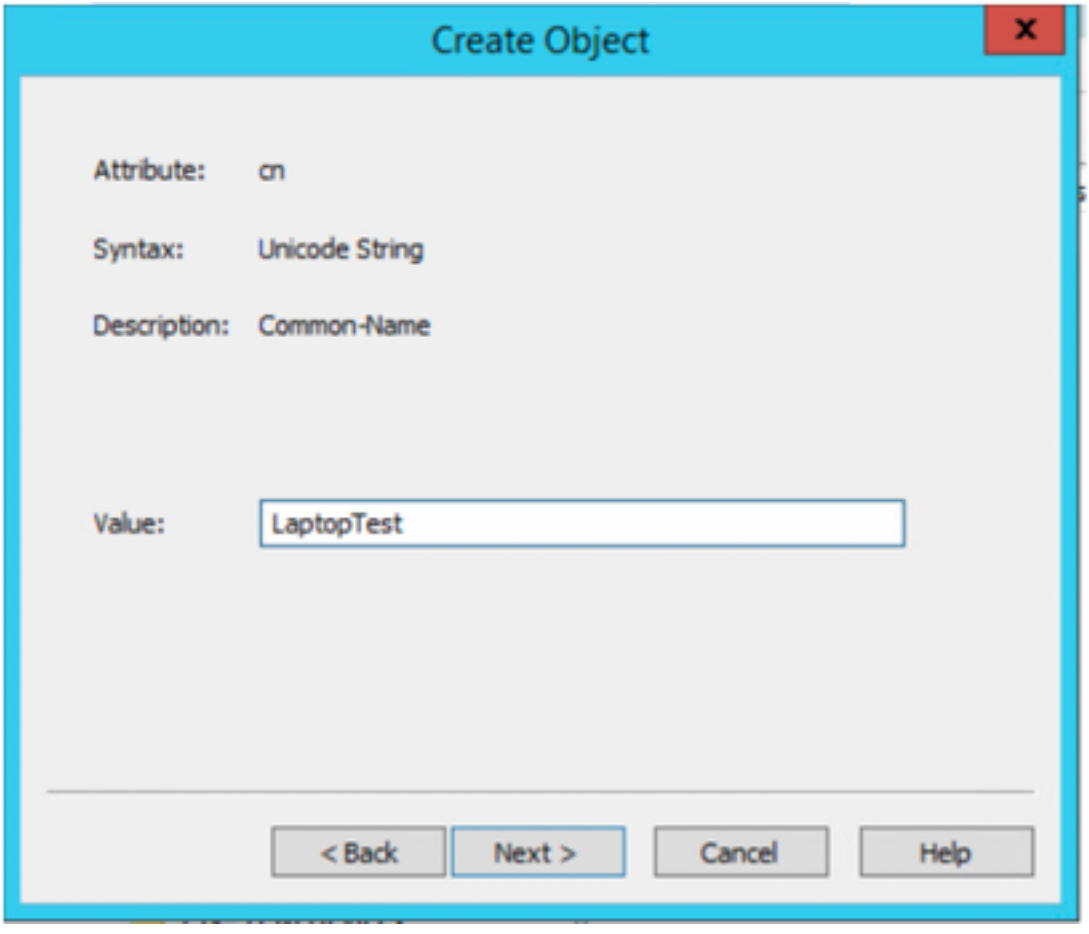
8. Haga clic con el botón derecho del ratón en OrganizationalUnit que se acaba de crear y seleccione **New > Object**



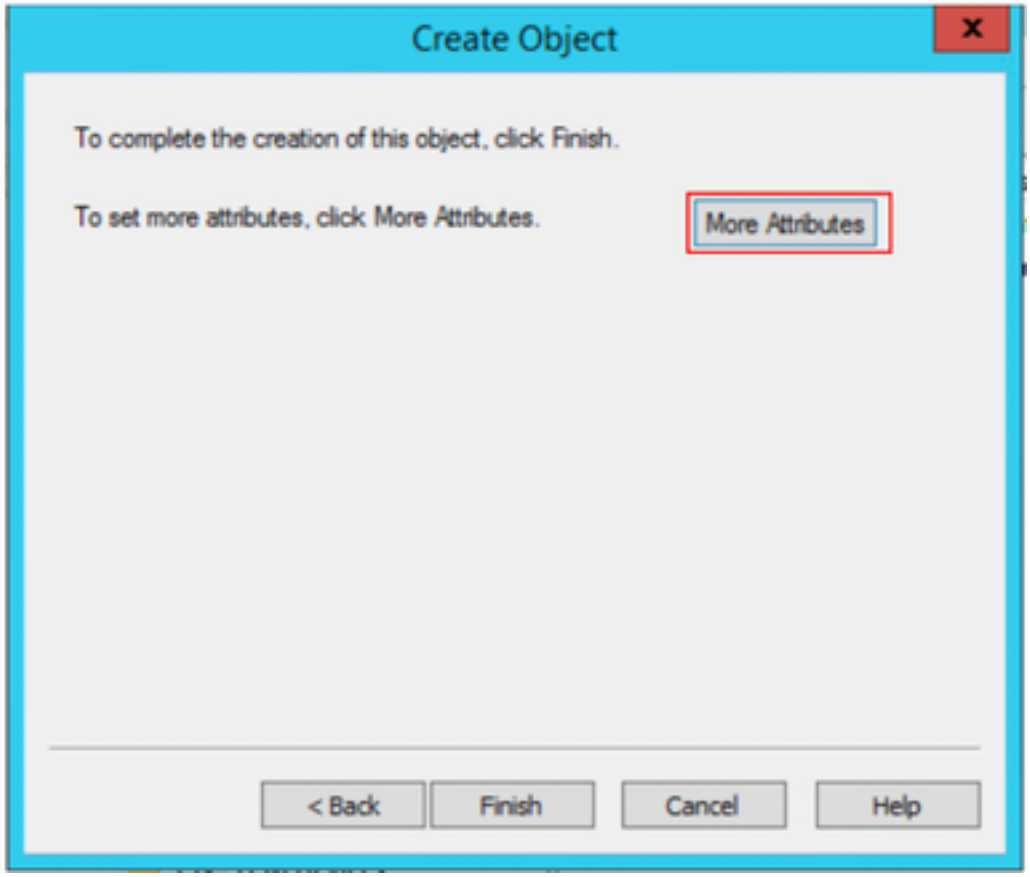
9. Seleccione **dispositivo** como clase de objeto y seleccione **siguiente**



10.Defina un nombre en el campo Valor y seleccione **Siguiente**

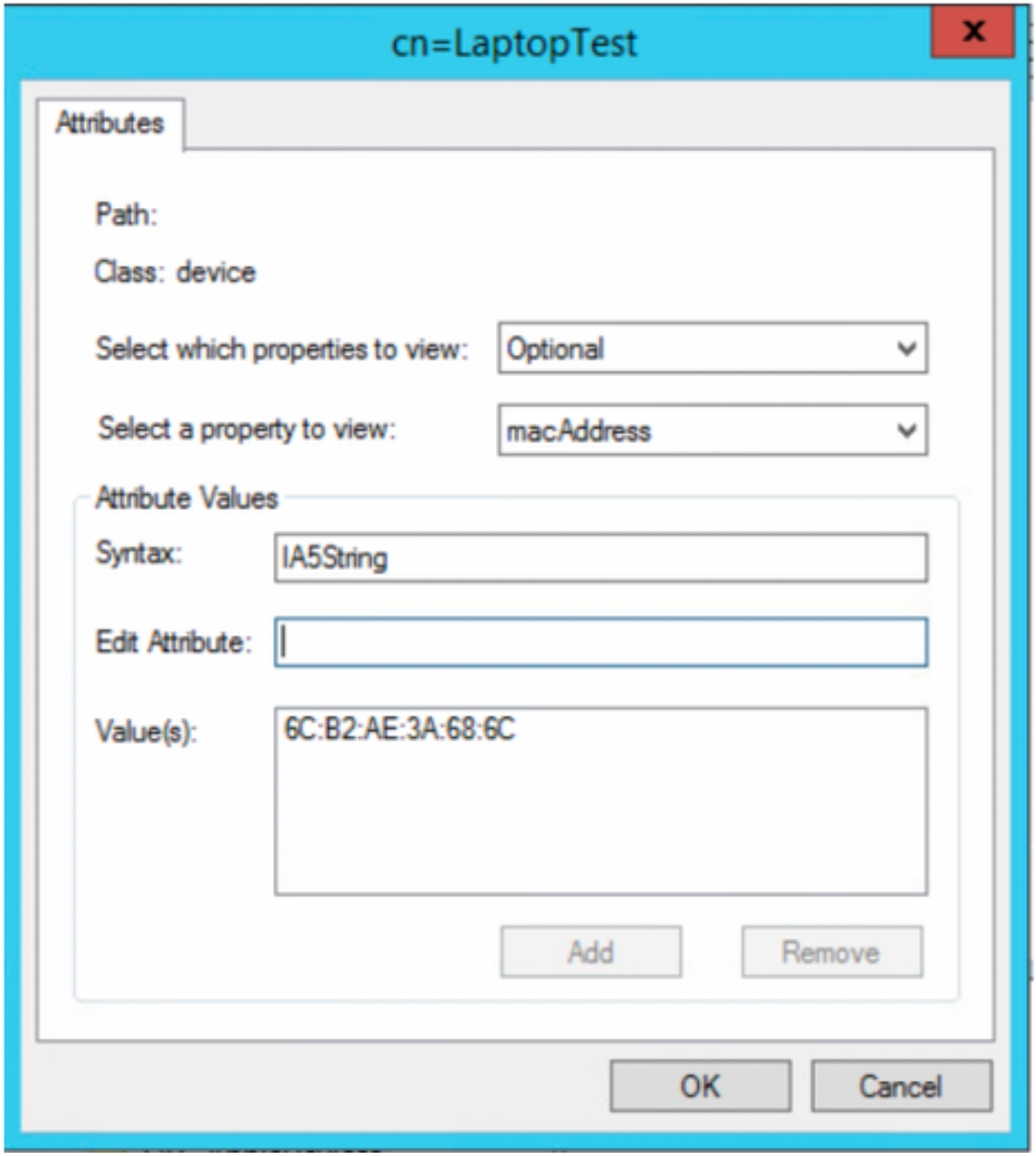


11. Seleccione la opción **Más atributos**



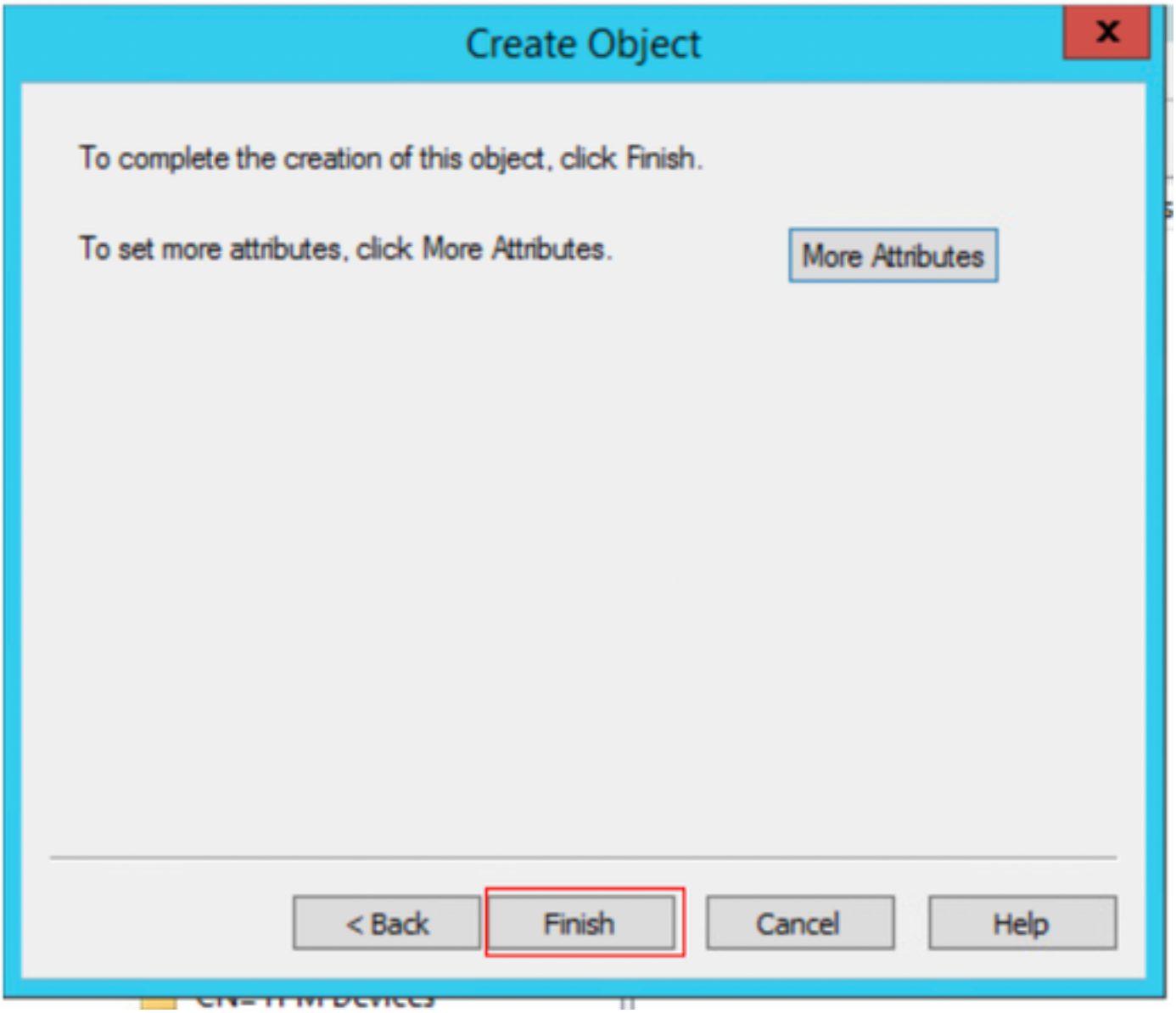
11. Para el menú desplegable, **Seleccione una propiedad para ver**, seleccione la opción **macAddress,** luego defina la dirección MAC del terminal que se autenticará en el campo **Edit attribute** y seleccione el **Agregar** botón para guardar la dirección mac del dispositivo.

Nota: Utilice dos puntos en lugar de puntos o guiones entre octetos de dirección mac.

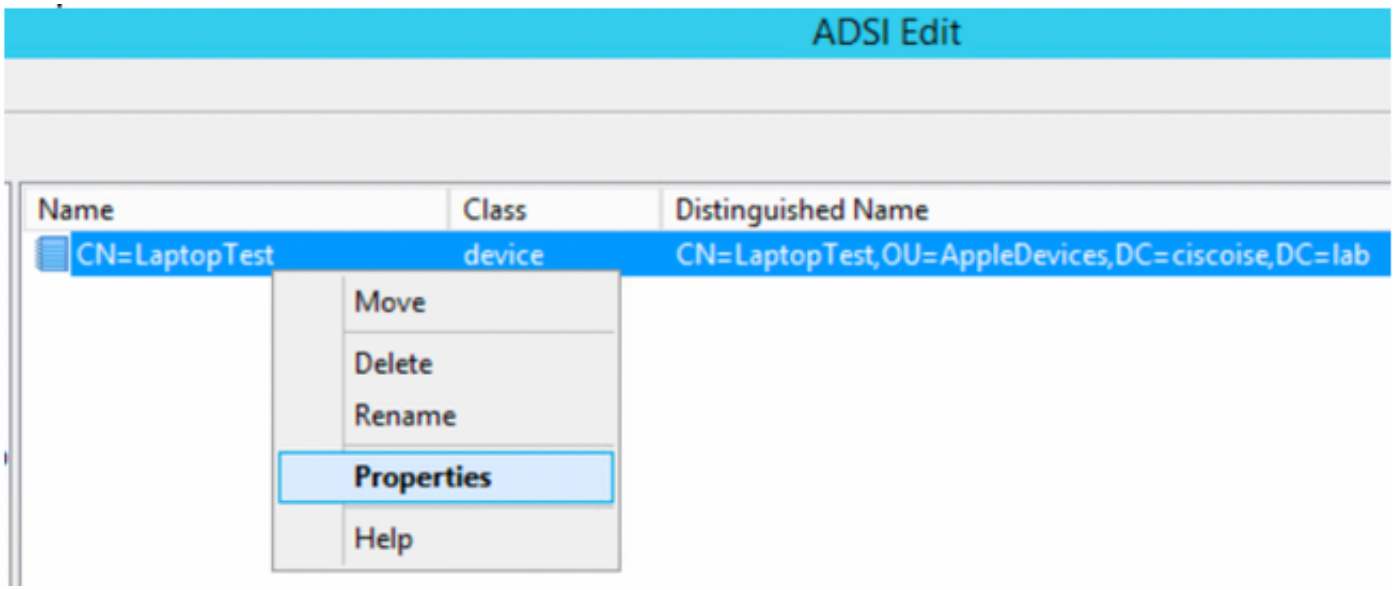


12. Seleccione **OK** para guardar la información y continuar con la configuración del objeto del dispositivo

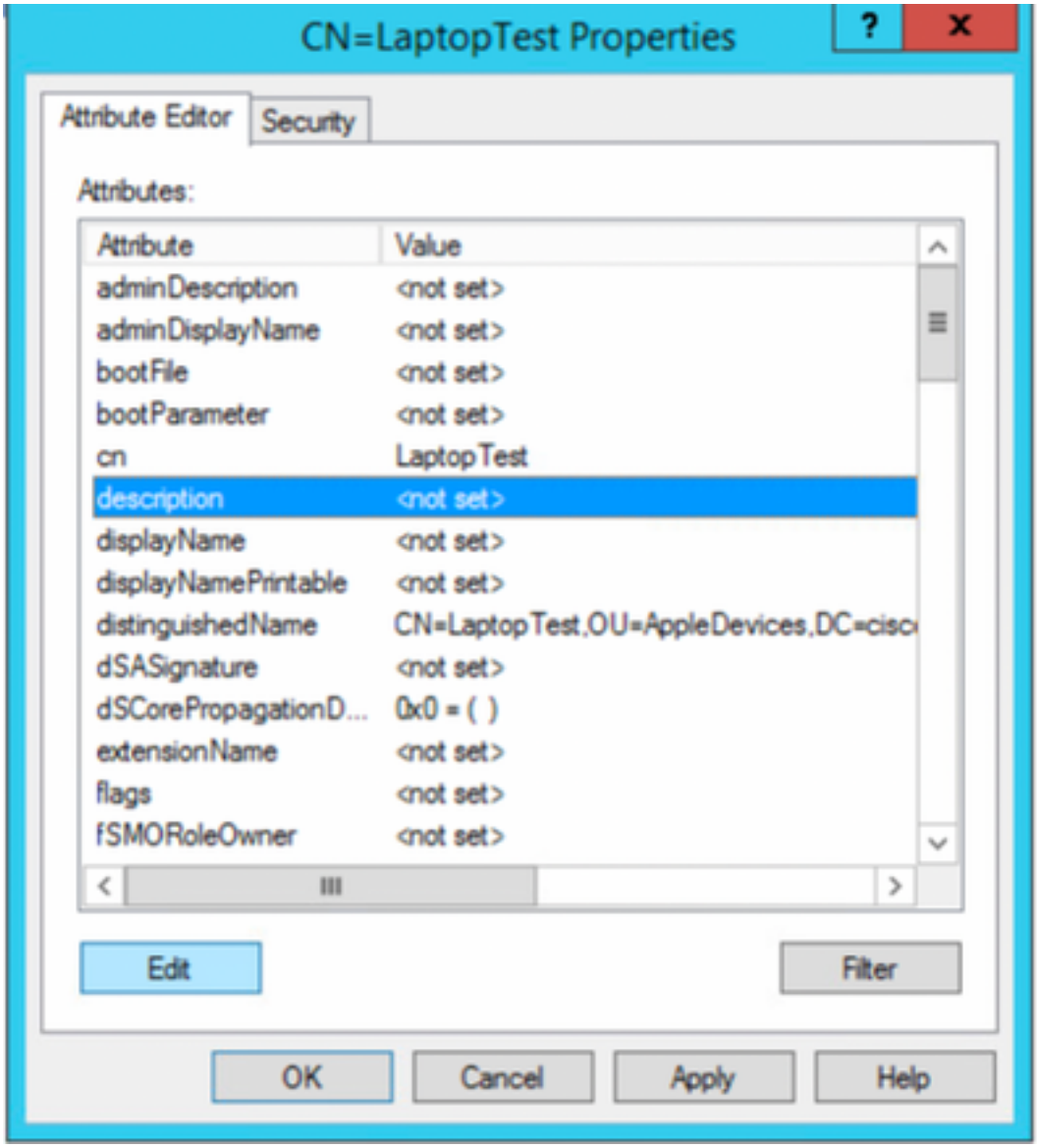
13. Seleccione **Finish** para crear el nuevo objeto de dispositivo



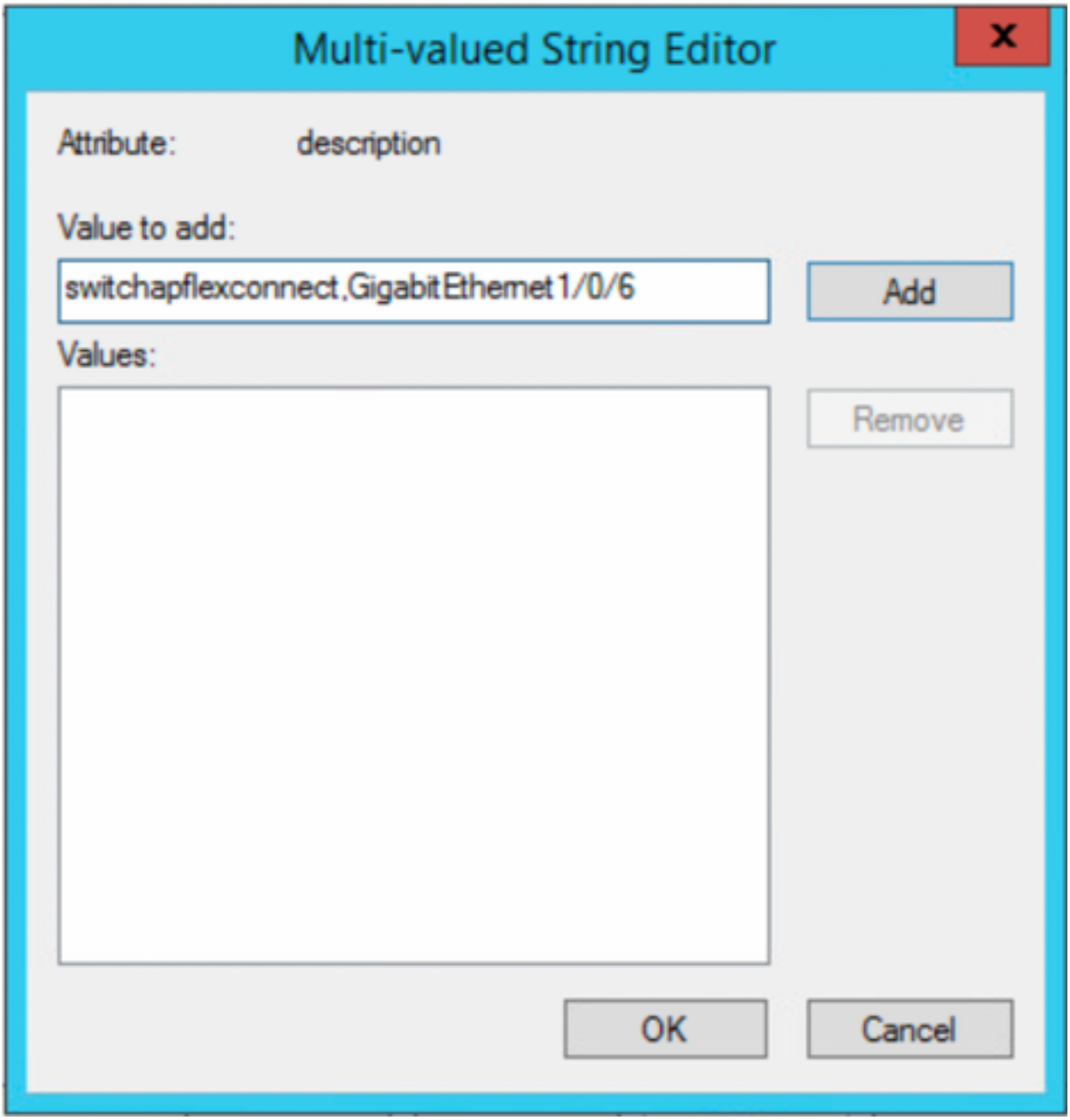
14. Haga clic con el botón derecho del ratón en el objeto del dispositivo y seleccione la opción **Propiedades**



15. Seleccione la **descripción de** la opción y seleccione **Editar** para definir el nombre del switch y el puerto del switch donde se conectará el dispositivo.



16. Defina el nombre del switch y el puerto del switch; asegúrese de utilizar una coma para separar cada valor. Seleccione **Add** y luego **Ok** para guardar la información.



- **Switchapflexconnect es el nombre del switch.**
- **GigabitEthernet1/0/6 es el puerto del switch al que se conecta el terminal.**

Nota: Es posible utilizar secuencias de comandos para agregar atributos a un campo específico, sin embargo, para este ejemplo estamos definiendo los valores manualmente

Nota: El atributo AD distingue entre mayúsculas y minúsculas, si utiliza todas las direcciones Mac en minúsculas, ISE se convierte en mayúsculas durante la consulta LDAP. Para evitar este comportamiento, inhabilite Process Host Lookup bajo los protocolos permitidos. Encontrará detalles en este enlace: https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

Configuración del switch

A continuación se describe la configuración para la comunicación 802.1x entre ISE y el 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
```

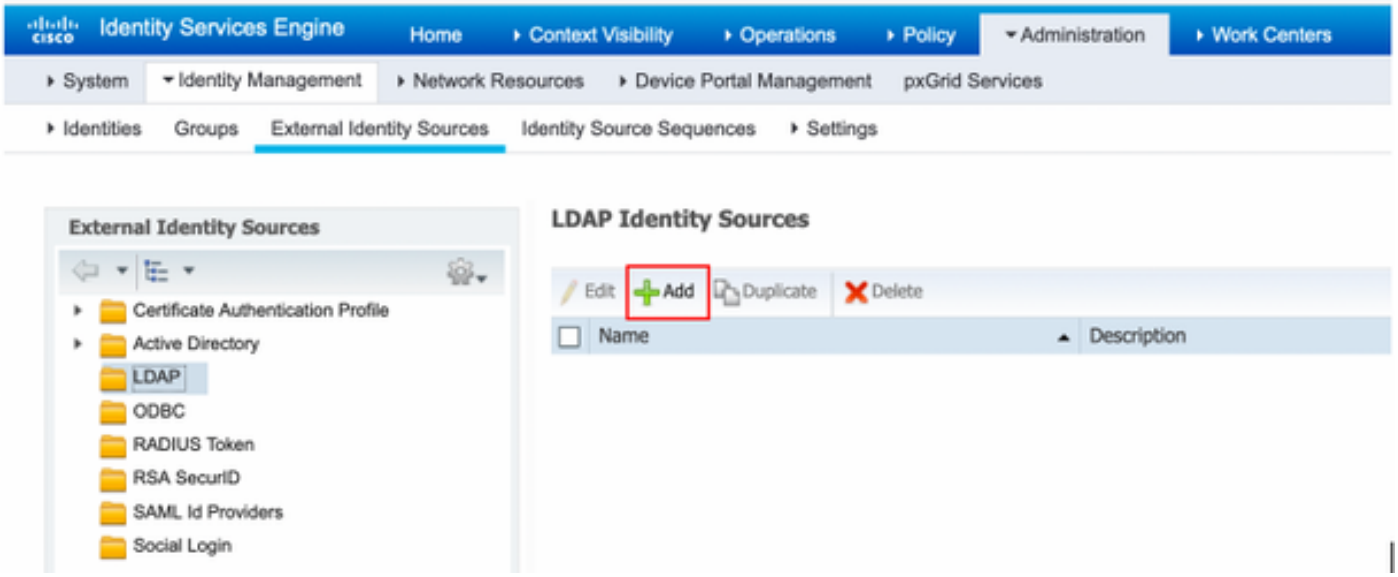
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access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

Nota: Es posible que sea necesario ajustar la configuración global e de interfaz en su entorno

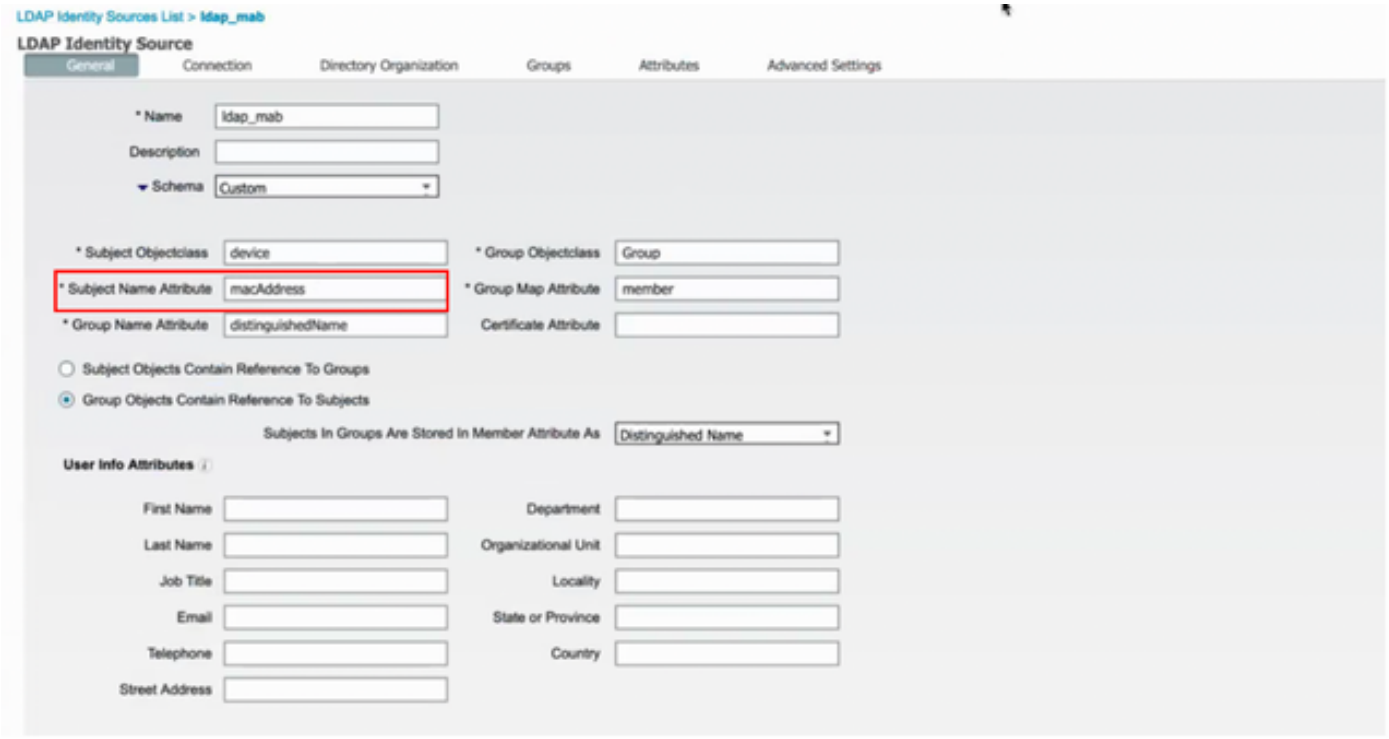
Configuración de ISE

A continuación se describe la configuración en ISE para obtener los atributos del servidor LDAP y configurar las políticas de ISE.

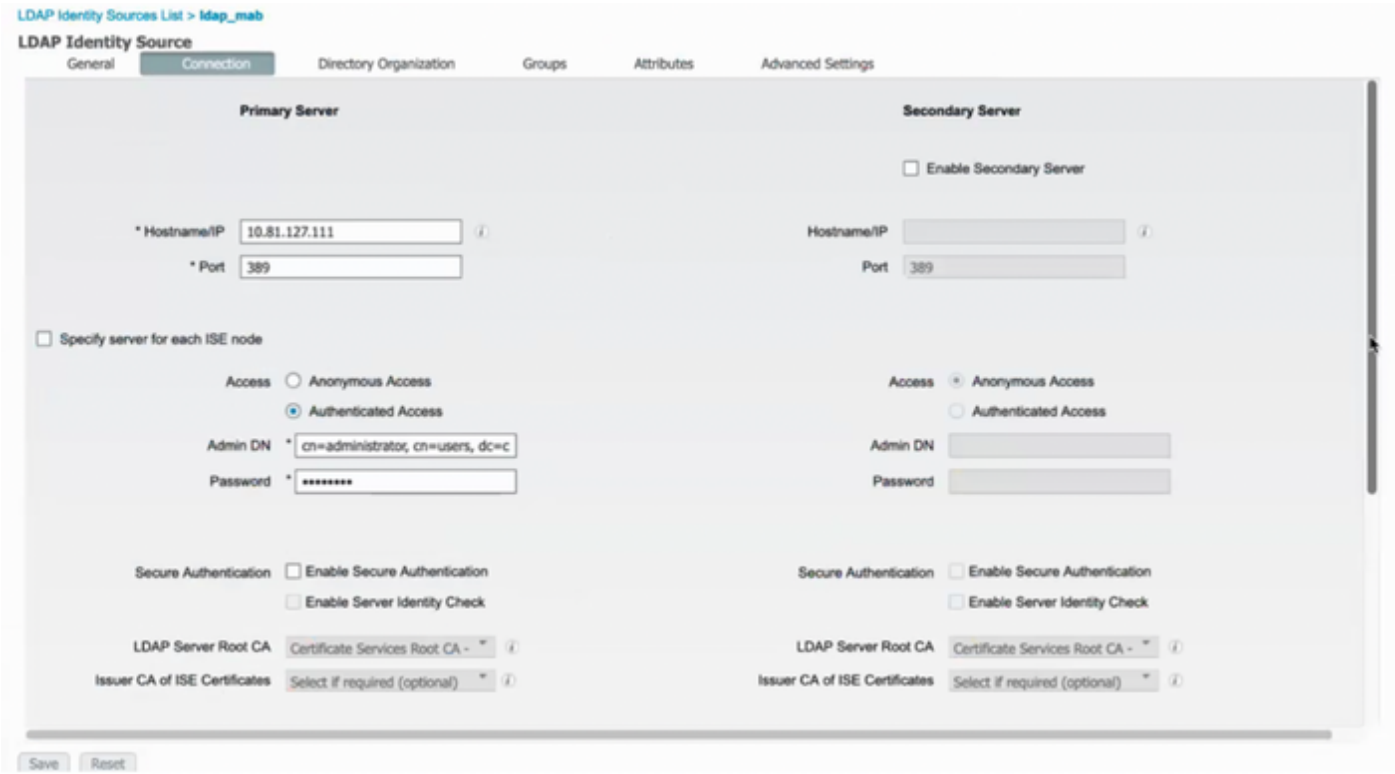
1. En ISE, vaya a **Administration->Identity Management->External Identity Sources** y seleccione la **carpeta LDAP** y haga clic en **Add** para crear una nueva conexión con LDAP



2.En la ficha **General**, defina un nombre y seleccione la dirección mac como atributo del nombre del sujeto

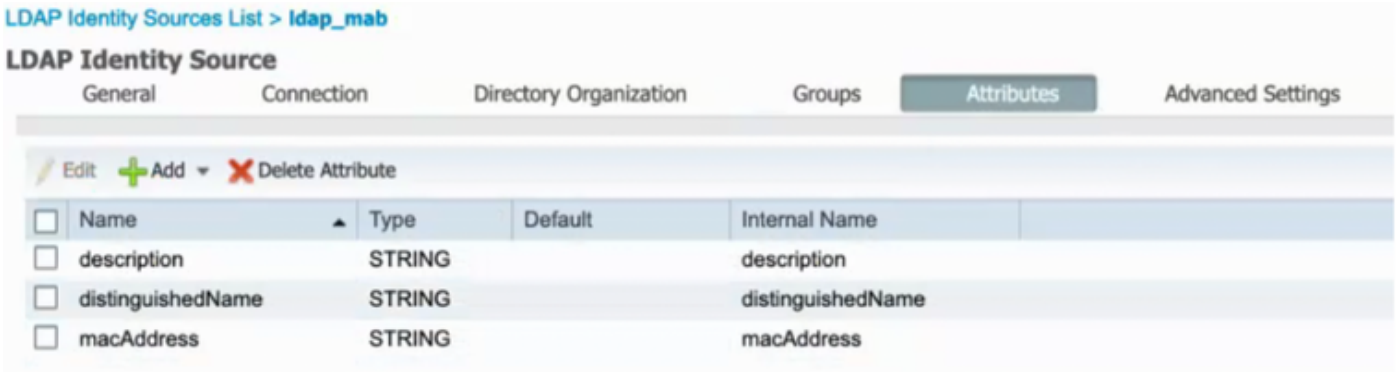


3. En la pestaña **Connection**, configure la dirección IP, el DN de administrador y la contraseña del servidor LDAP para obtener una conexión correcta.

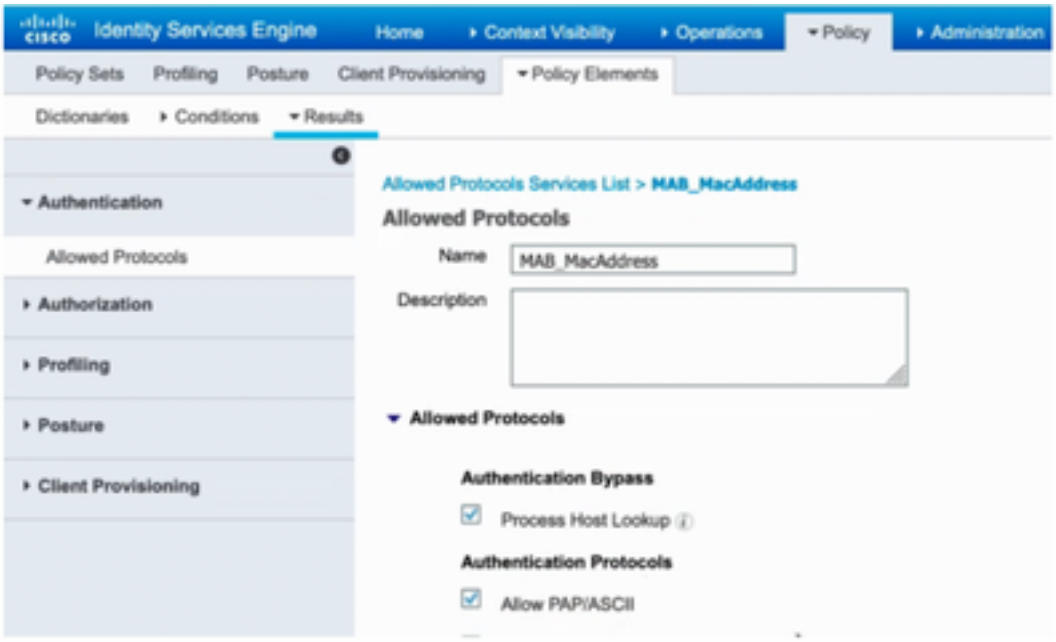


Nota: El puerto 389 es el puerto predeterminado utilizado.

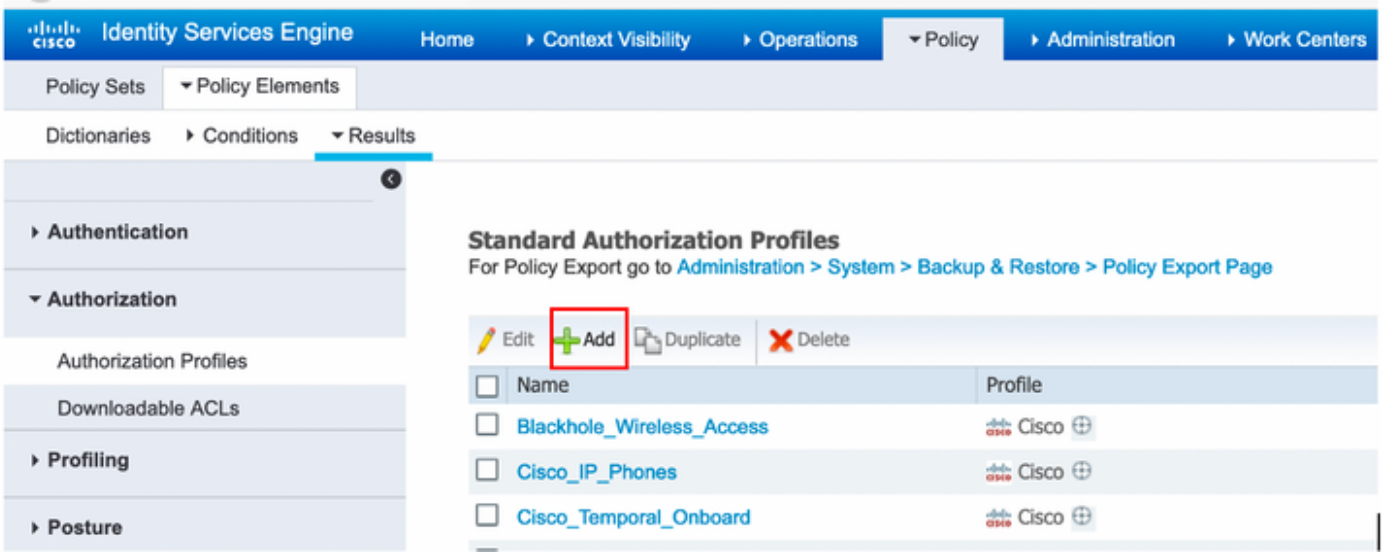
4. En la pestaña **Atributos** seleccione los atributos macAddress y description, estos atributos se utilizarán en la política de autorización

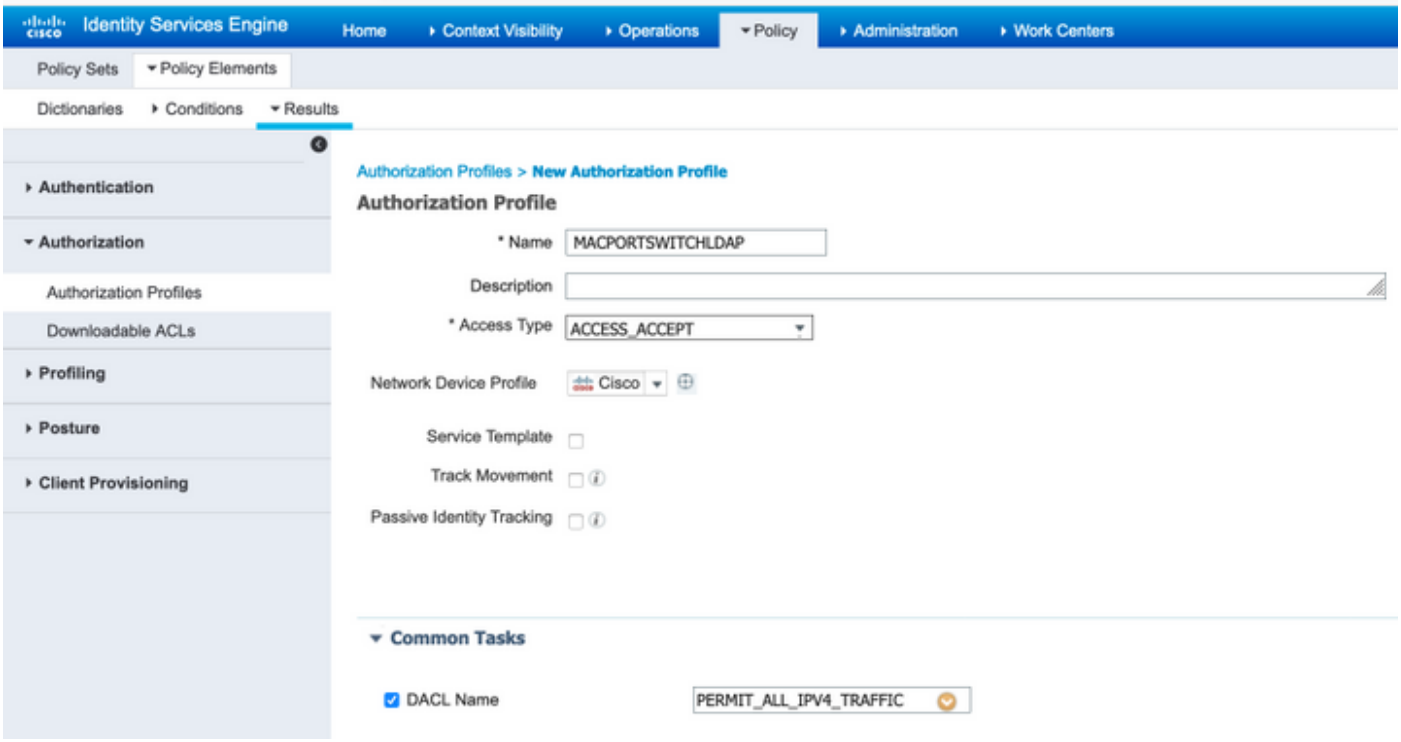


5. Para crear un protocolo permitido, vaya a **Política->Elementos de política->Resultados->Autenticación->Protocolos permitidos.** Defina y seleccione Process Host Lookup y Allow PAP/ASCII como los únicos protocolos permitidos. Por último, seleccione **Guardar**

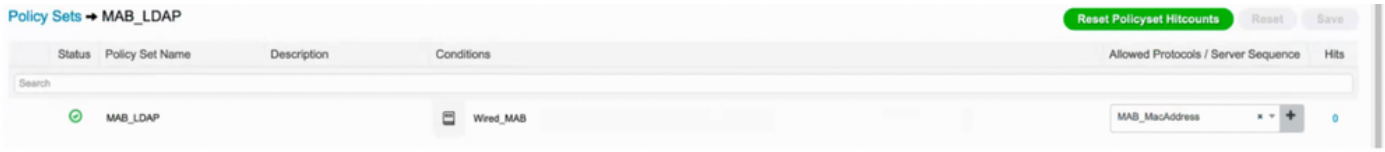


6. Para crear un perfil de autorización, vaya a **Política->Elementos de política->Resultados->Autorización->Perfiles de autorización.** Seleccione **Add** y defina los permisos que se asignarán al extremo.

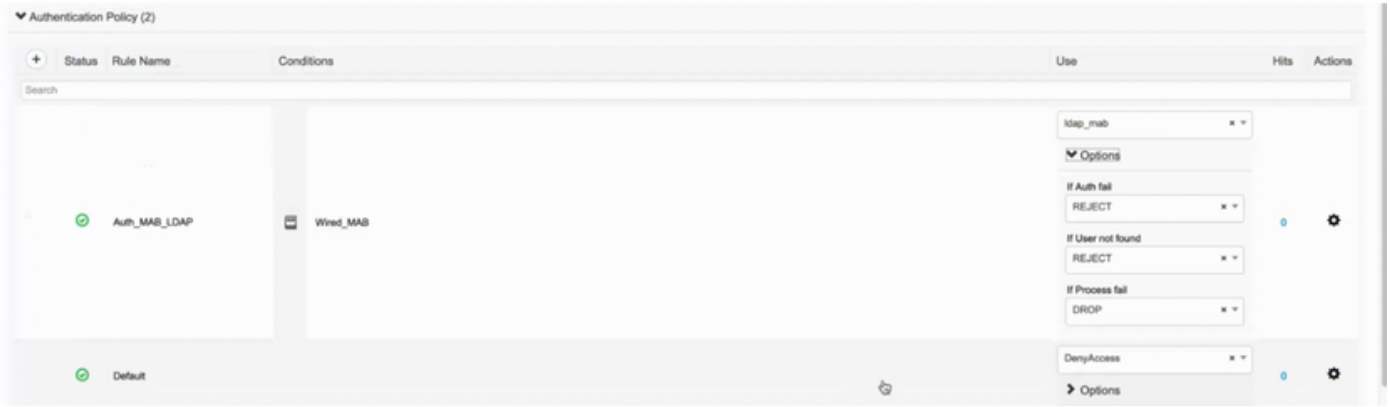




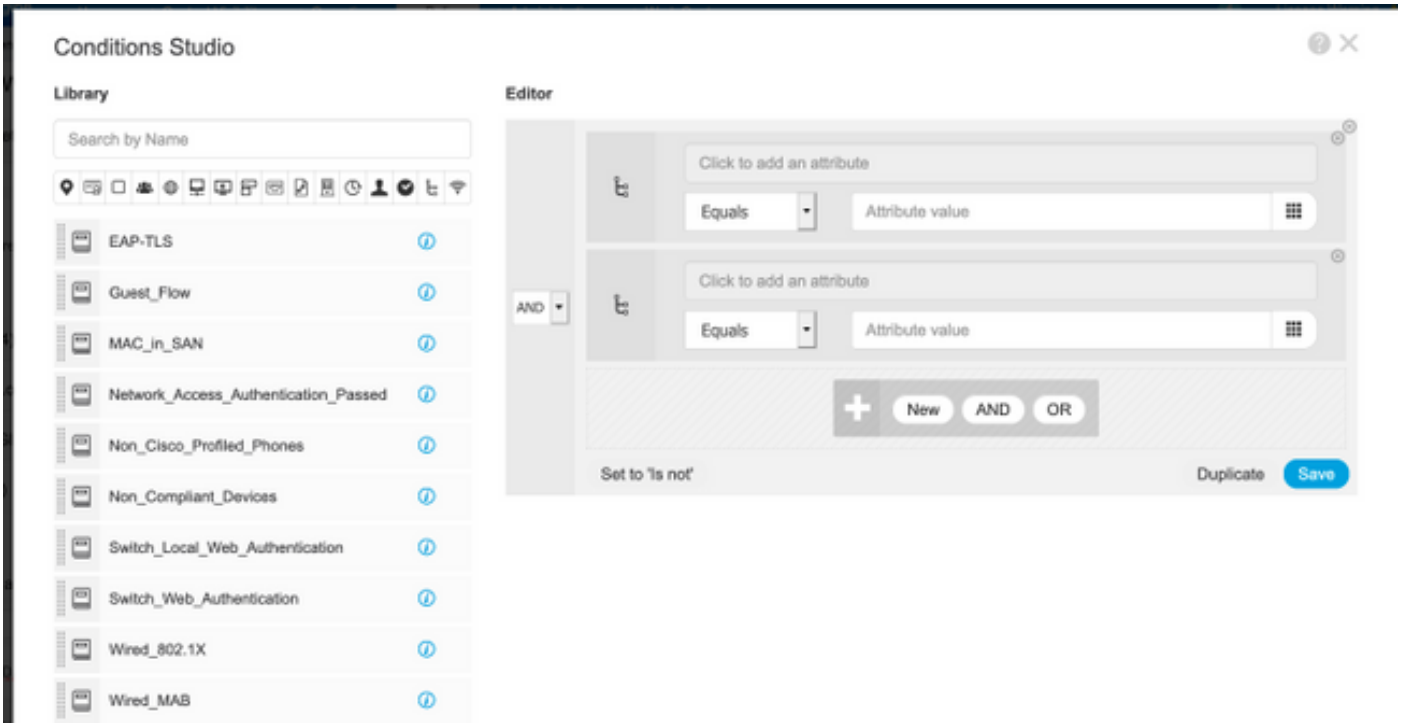
7. Vaya a Policy-> Policy Set y cree un conjunto de políticas utilizando la condición predefinida Wired_MAB y el Allowed Protocol creado en el paso 5.

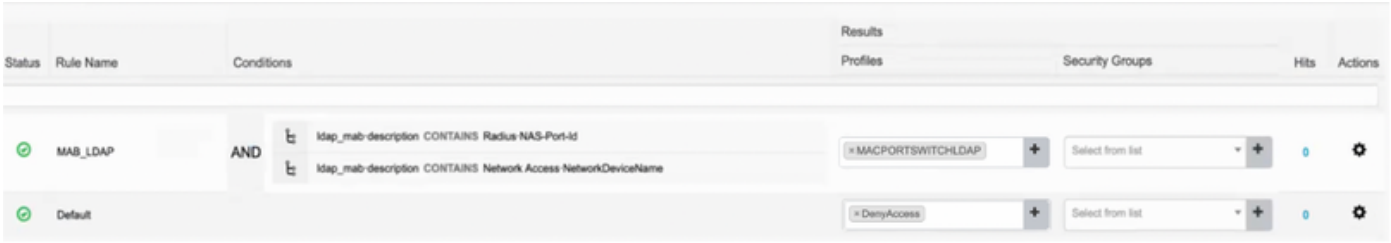


8.En el nuevo conjunto de políticas creado, cree una política de autenticación utilizando la biblioteca **Wired_MAB** y la conexión **LDAP** como secuencia de origen de identidad externa



9. Bajo **Política de Autorización** defina un nombre y cree una condición compuesta usando la descripción del atributo LDAP, Radius NAS-Port-Id y NetworkDeviceName. Por último, agregue el perfil de autorización creado en el paso 6.





Después de aplicar la configuración, debe poder conectarse a la red sin intervención del usuario.

Verificación

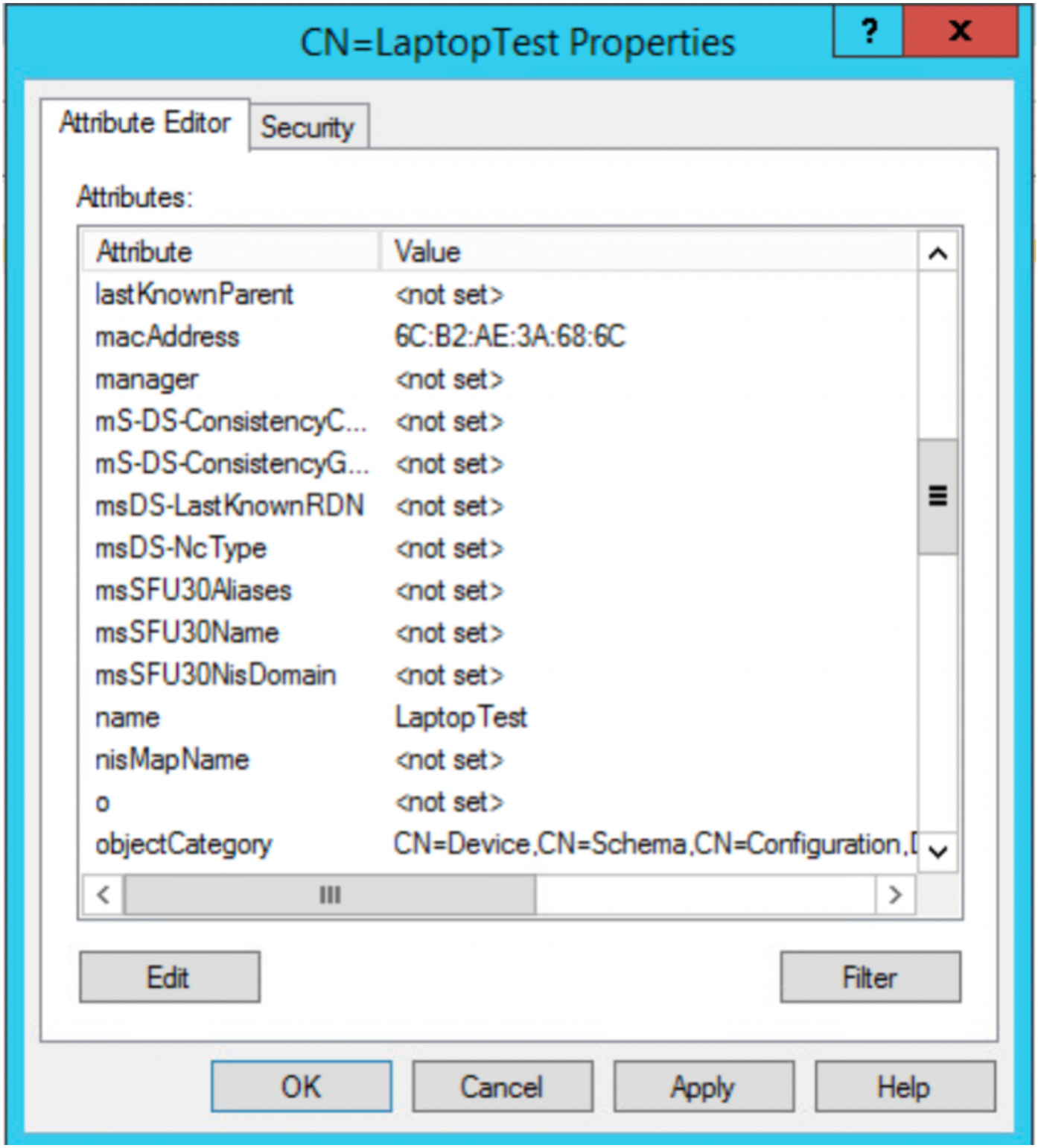
Una vez conectado al puerto del switch designado, puede escribir **show authentication session interface GigabitEthernet X/X/X** para validar el estado de autenticación y autorización del dispositivo.

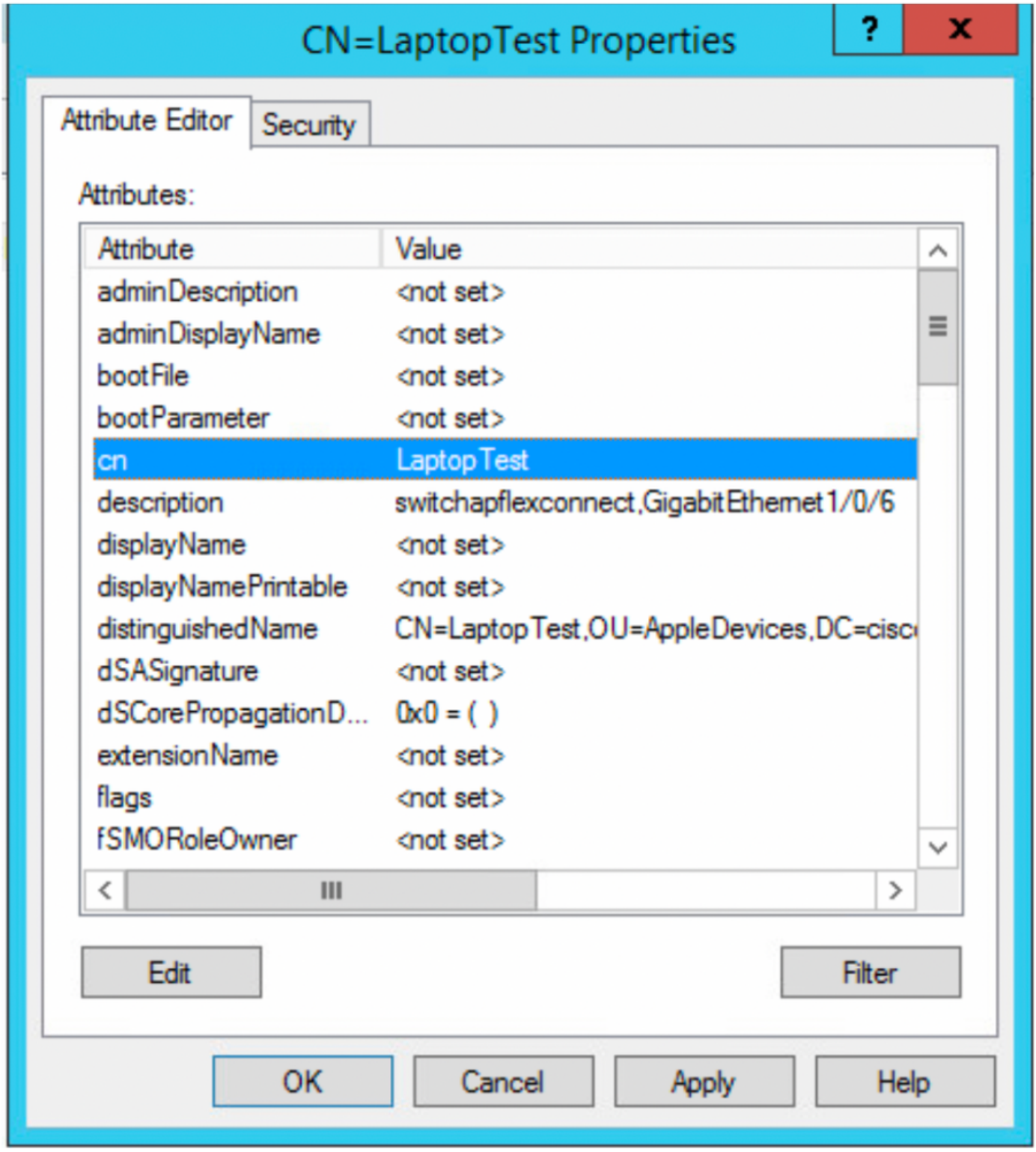
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session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

En ISE puede utilizar Registros en directo de Radius para obtener confirmación.

Troubleshoot

En el servidor LDAP, Valide que el dispositivo creado tenga la dirección Mac, el nombre de switch adecuado y el puerto del 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



En ISE, puede tomar una captura de paquetes (vaya a **Operaciones->Solución de problemas->Herramienta de diagnóstico->Vaciados TCP**) para validar los valores que se envían de LDAP a ISE