Op ISE en LDAP gebaseerde verificatie

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Identity Services Engine (ISE) kunt configureren en Lichtgewicht Directory Access Protocol (LDAP) objecten kunt gebruiken om apparaten dynamisch te authenticeren en autoriseren.

Opmerking: Dit document is geldig voor instellingen die LDAP als externe identiteitsbron voor de ISE-verificatie en -vergunning gebruiken.

Bijgedragen door Emmanuel Cano en Mauricio Ramos Cisco Professional Services Engineer.

Bewerkt door Neri Cruz Cisco TAC-ingenieur.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van de volgende onderwerpen:

- Basiskennis van ISE-beleidssets, authenticatie en autorisatiebeleid
- Mac Authentication Bypass (MAB)
- Basiskennis van het protocol van Radius
- Basiskennis van Windows-server

Gebruikte componenten

De informatie over dit document is gebaseerd op de volgende software- en hardwareversies:

- Cisco ISE, versie 2.4, plug-in 11
- Microsoft Windows Server, versie 2012 R2 x64
- Cisco Catalyst 3650-24PD, versie 30.07.05.E (15.2(3)E5)
- Microsoft Windows 7-machine

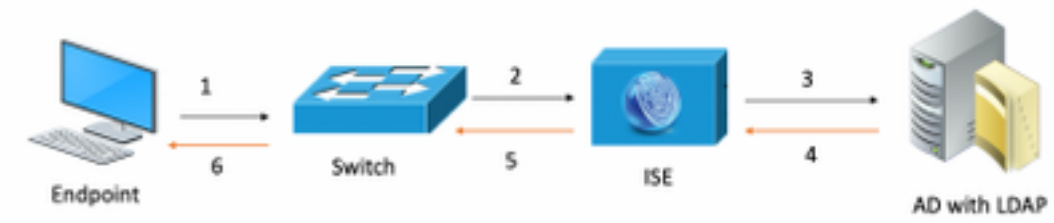
Opmerking: De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configuratie

In dit deel wordt beschreven hoe de netwerkapparaten moeten worden geconfigureerd, hoe de ISE en LDAP moeten worden geïntegreerd, en tenslotte hoe de LBP-eigenschappen moeten worden gevormd die in ISE-autorisatiebeleid moeten worden gebruikt.

Netwerkdiagram

Dit beeld illustreert de netwerktopologie die wordt gebruikt:



Hier is de verkeersstroom, zoals wordt geïllustreerd in het netwerkdiagram:

1. De gebruiker sluit zijn pc/laptop aan op de aangewezen switchpoort.
2. De switch stuurt een RADIUS-toegangsverzoek voor die gebruiker naar ISE
3. Wanneer de ISE de informatie ontvangt, stelt zij de LDAP-server voor het specifieke gebruikersbestand in, die de eigenschappen bevat die in de voorwaarden van het vergunningsbeleid moeten worden gebruikt.
4. Zodra ISE de eigenschappen (de switchpoort, de switchnaam en het apparaatadres) ontvangt, vergelijkt het de informatie die door de schakelaar wordt geleverd.
5. Als de door de schakelaar verschafte attributieinformatie gelijk is aan die van LDAP, zal ISE een RADIUS-toegangsaccepteren sturen met de permissies die zijn ingesteld op het autorisatieprofiel.

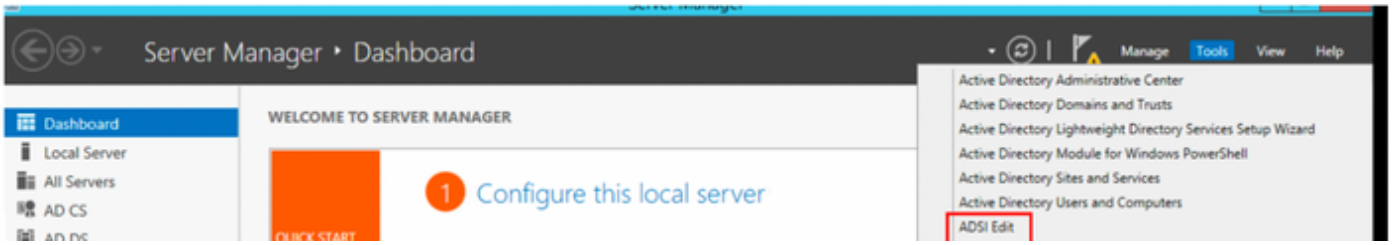
Configuraties

Gebruik dit gedeelte om de LDAP, de schakelaar en de ISE te configureren.

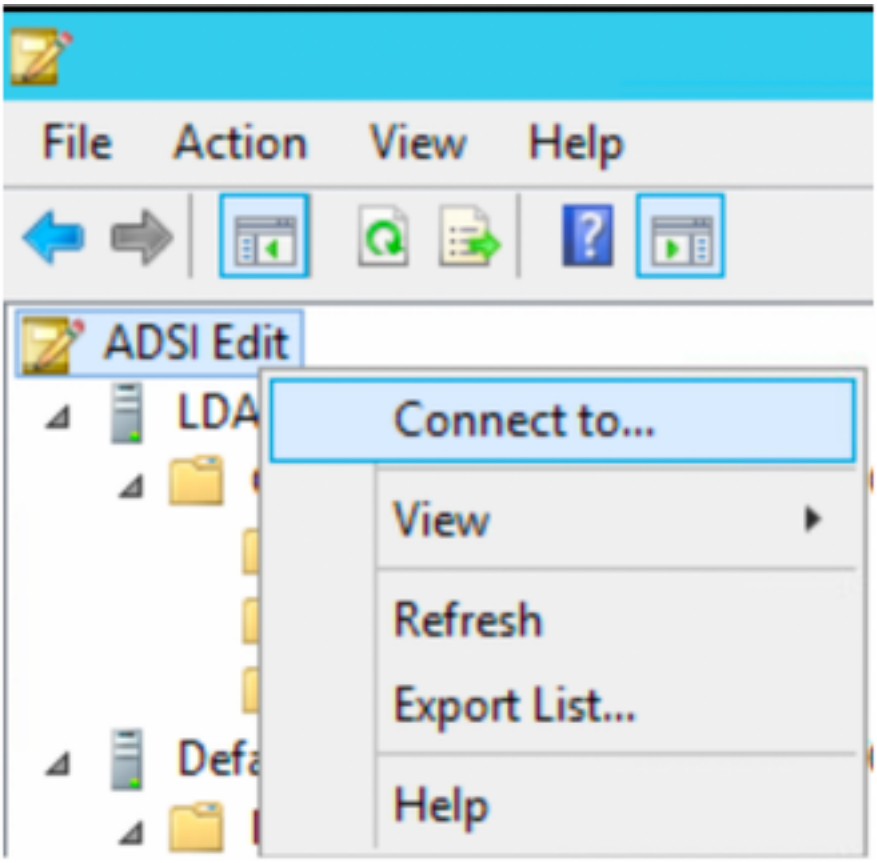
Configureren LDAP

Volg de volgende stappen om de LDAP server te configureren:

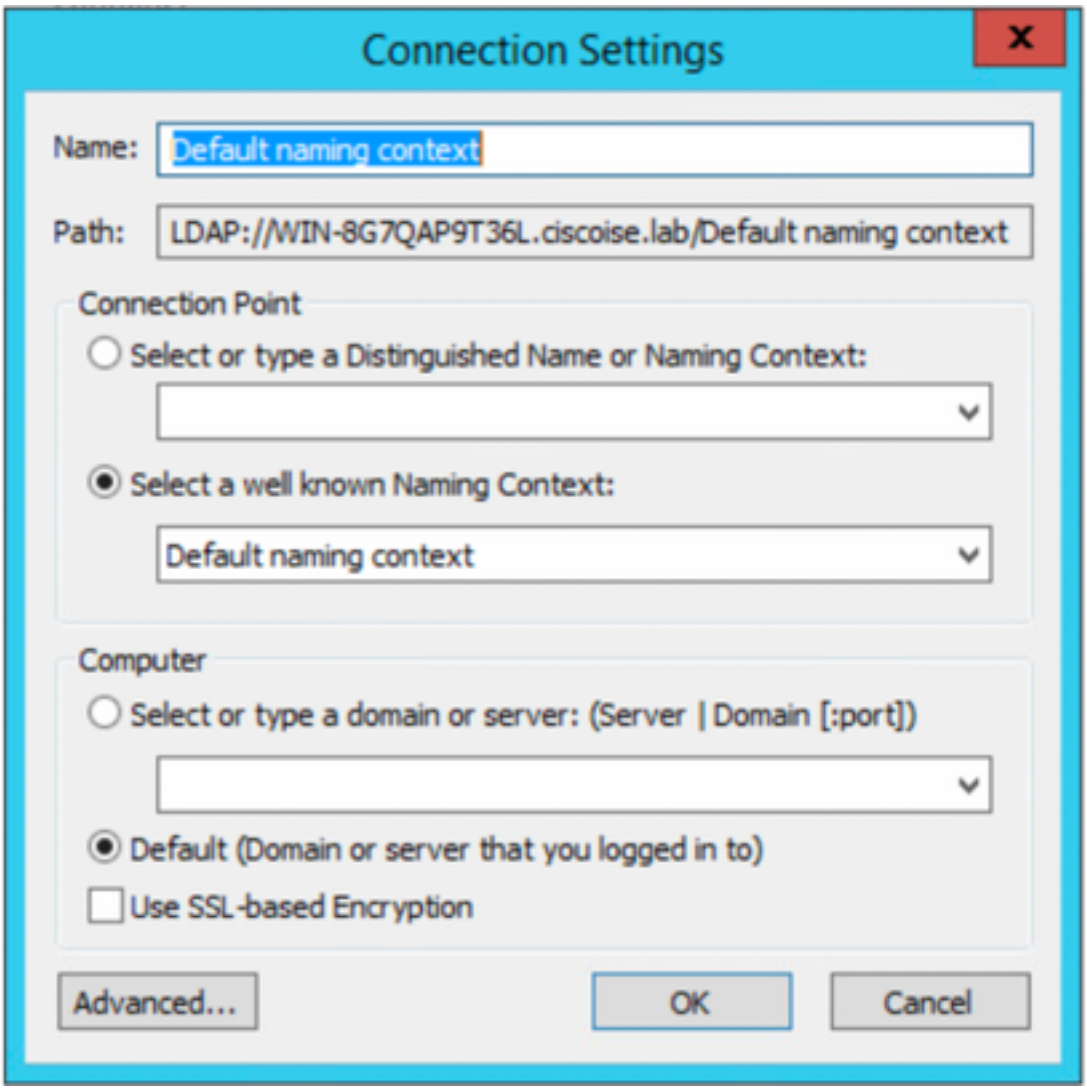
1. Navigatie naar **Server Manager > Dashboard > Gereedschappen > ADSI Bewerken**



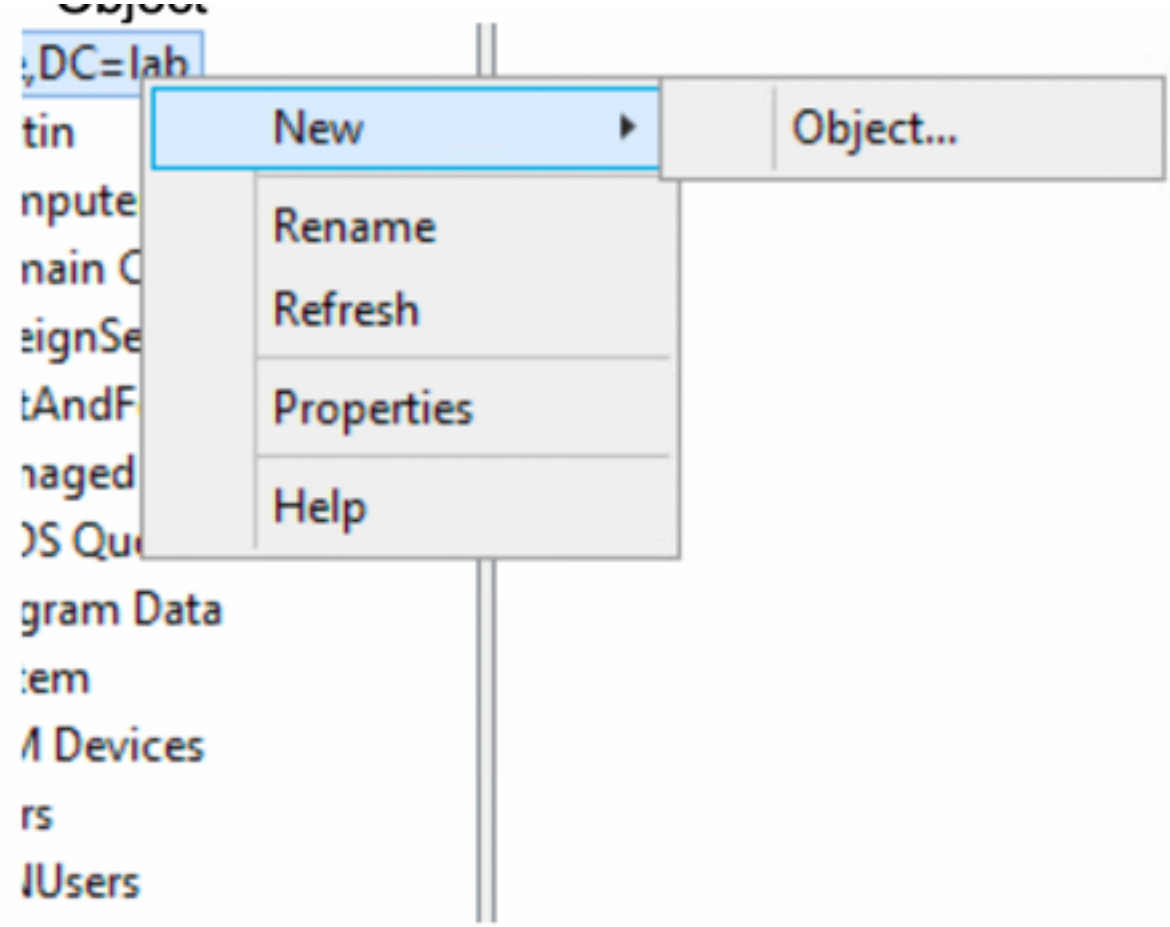
2. Klik met de rechtermuisknop op het pictogram ADSI Bewerken en selecteer **Connect met...**



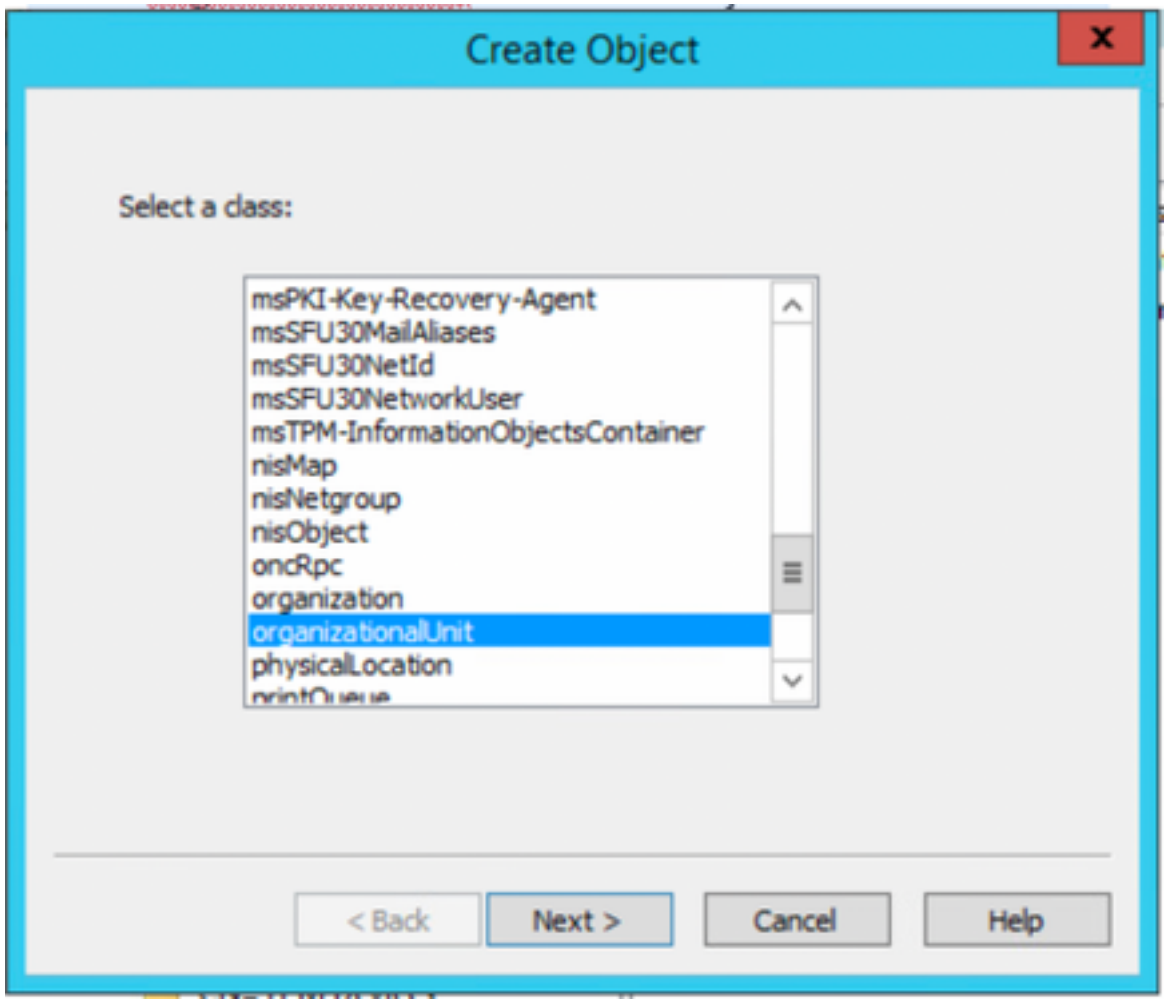
3. Onder verbindingsinstellingen definieer een naam en selecteer de knop **OK** om de verbinding te starten.



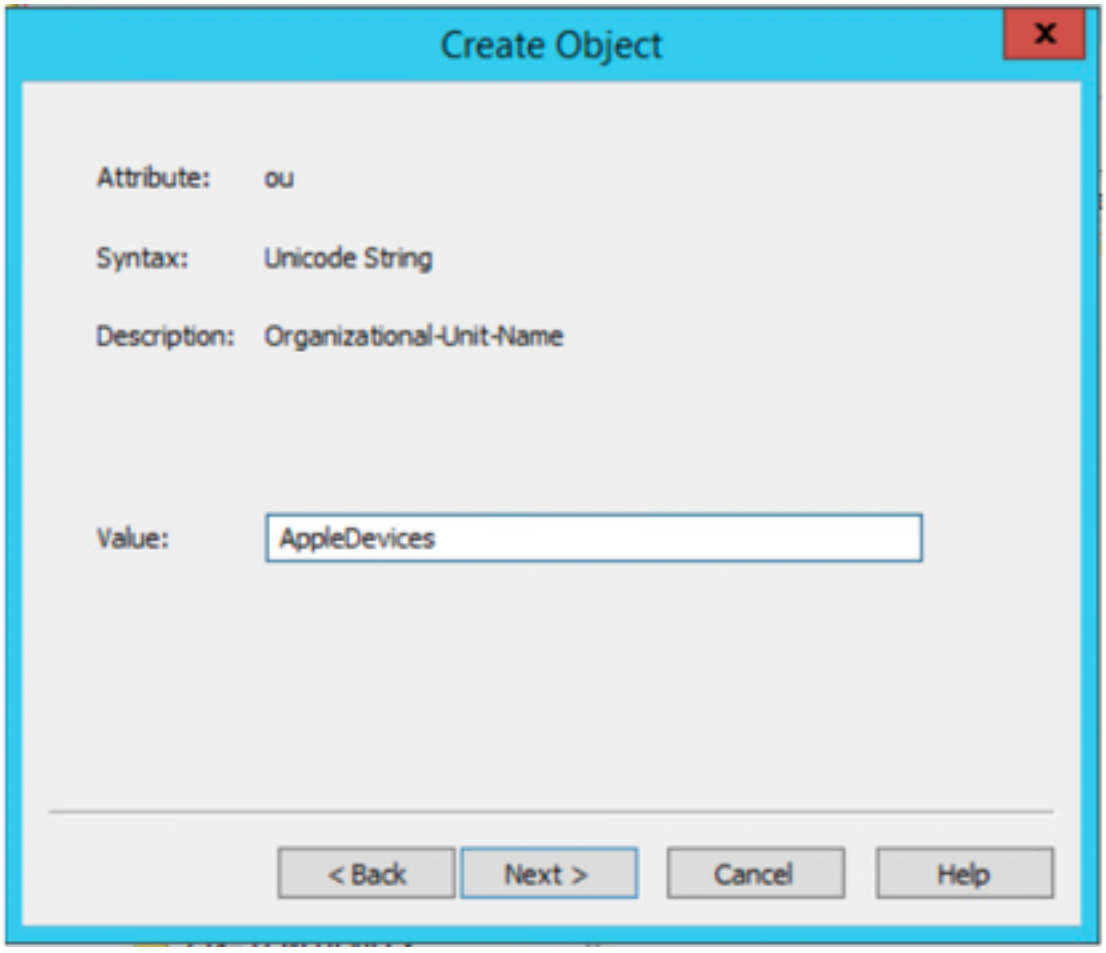
4. Onder hetzelfde menu ADSI Bewerken, klik met de rechtermuisknop in DC-verbinding (DC=ciscodemo, DC=lab), selecteer **Nieuw,** selecteer vervolgens optie **object**



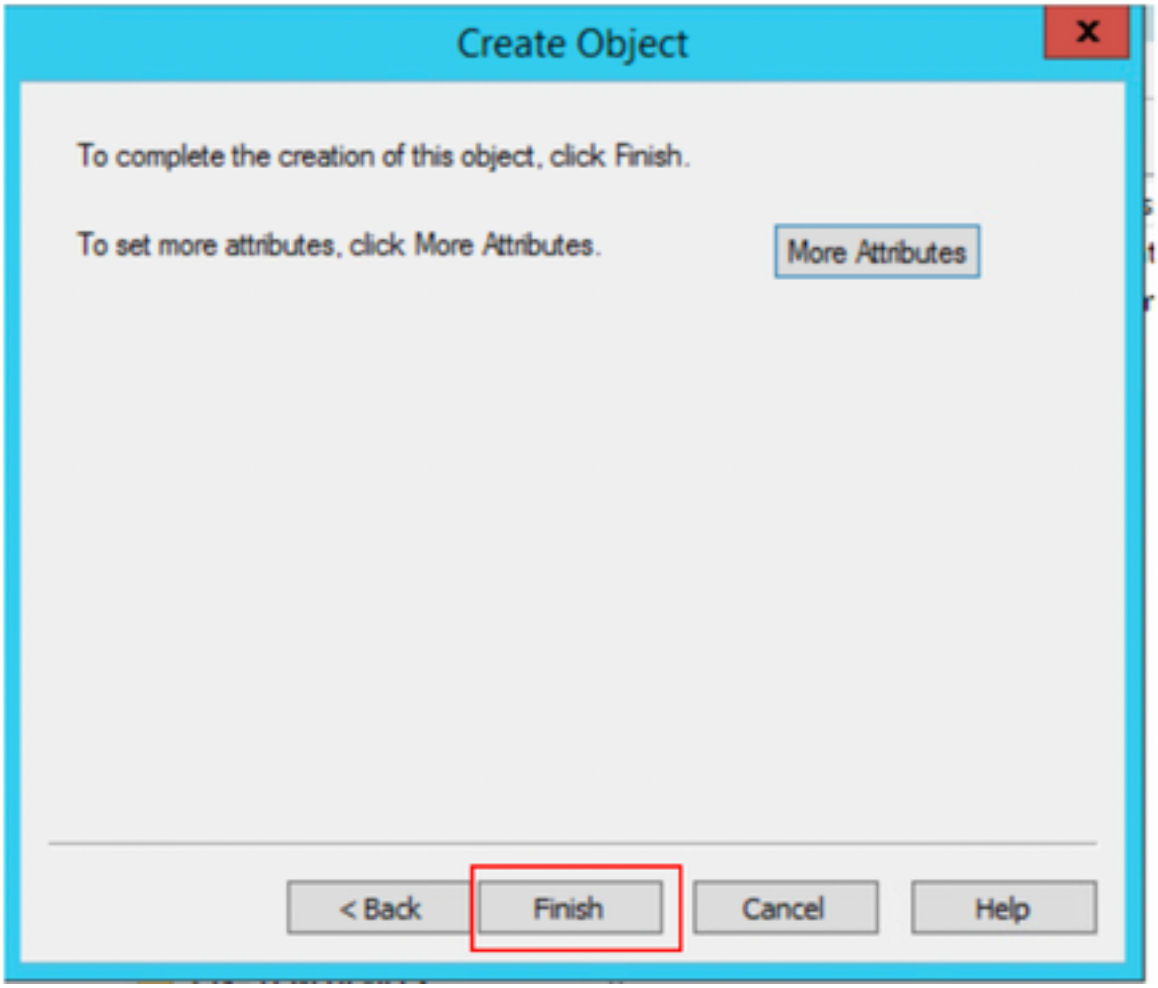
5. Selecteer optie **OrganisatorischeEenheid** als het nieuwe object en selecteer **het volgende.**



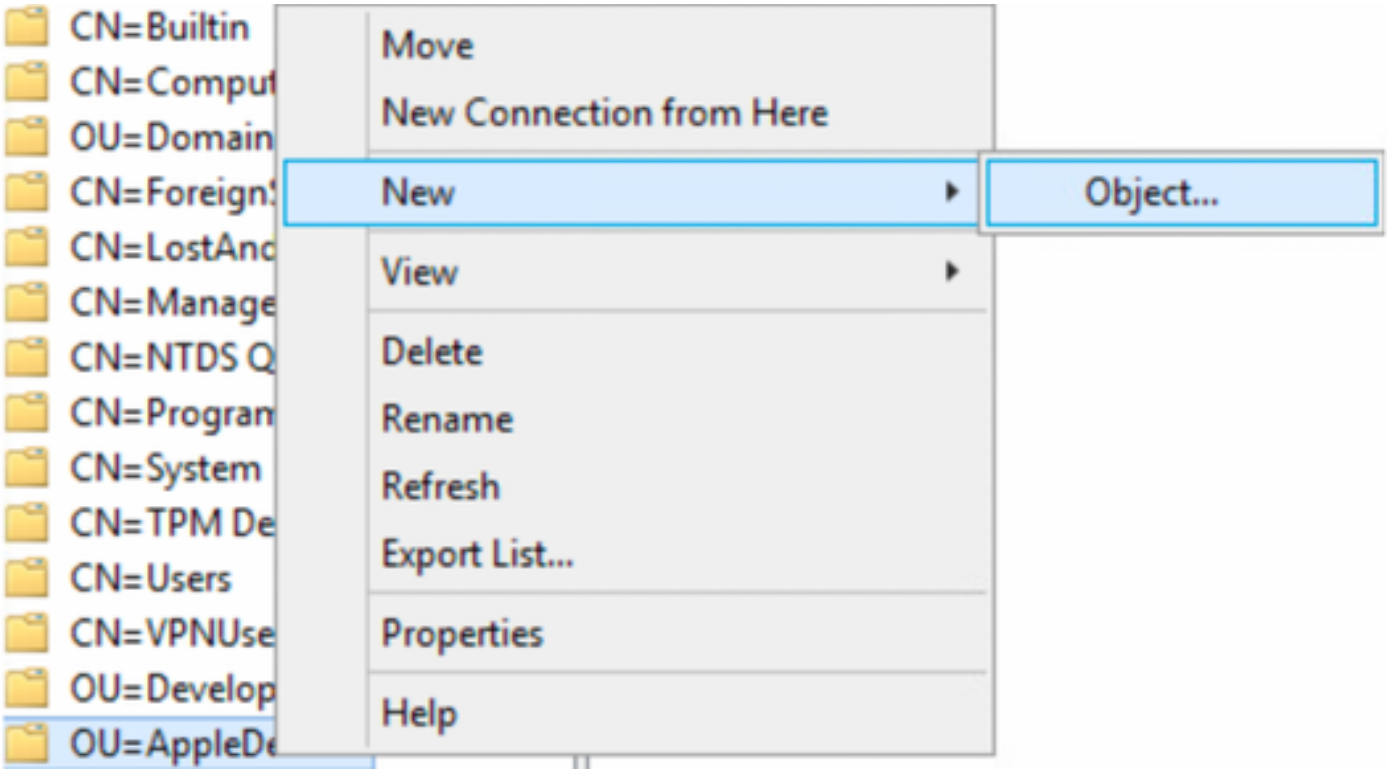
6. Bepaal een naam voor de nieuwe Organisatorische Eenheid en selecteer **Volgende**



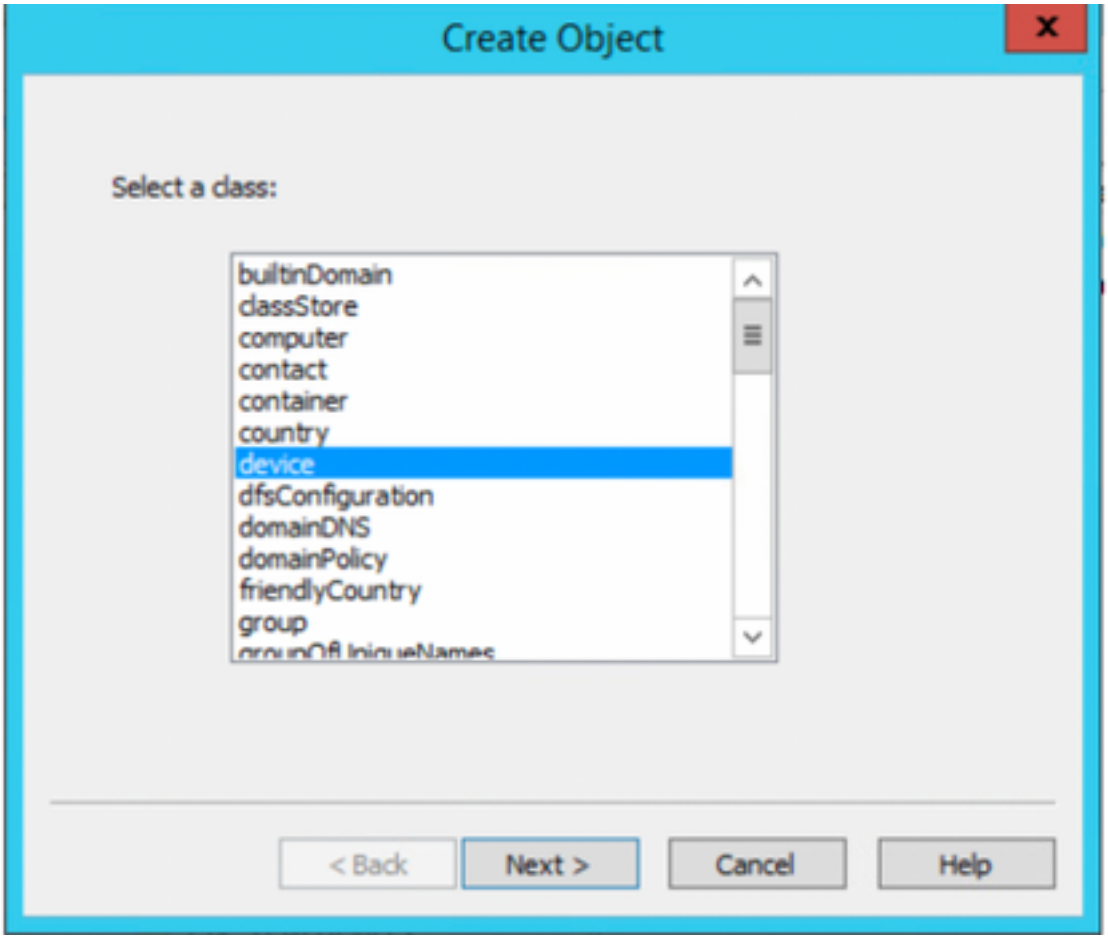
7. Selecteer **Voltooien** om de nieuwe organisatorische eenheid te creëren



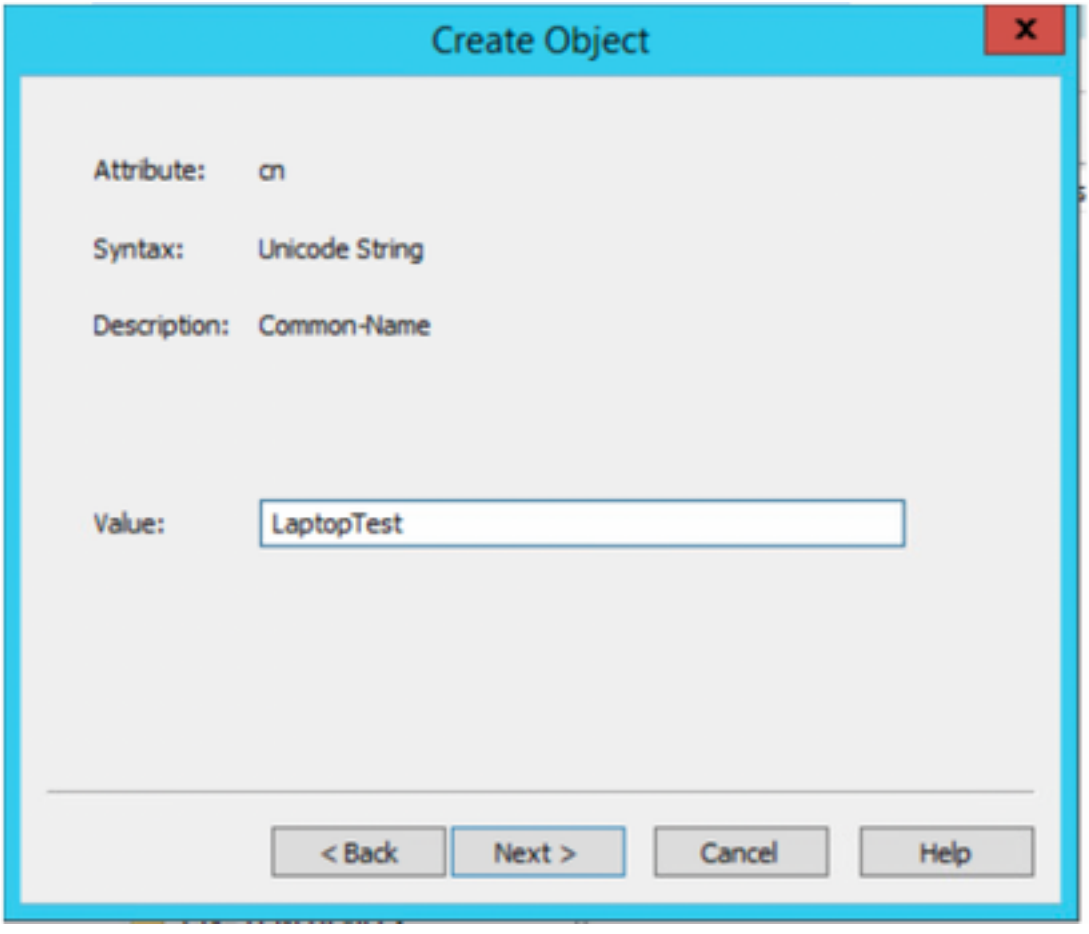
8. Klik met de rechtermuisknop op de organisatorische eenheid die net is gemaakt en selecteer **Nieuw > object**



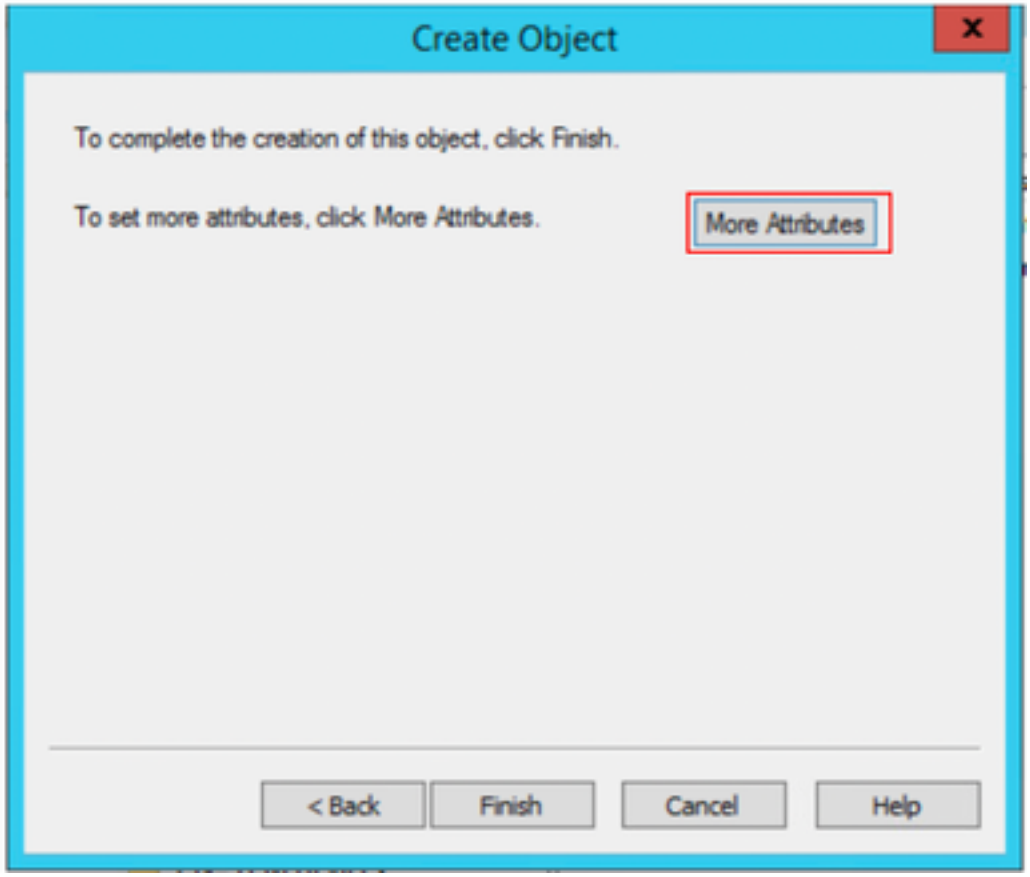
9. Selecteer **apparaat** als doelklasse en selecteer **Volgende**



10.Defineer een naam in het veld Waarde en selecteer **Volgende**

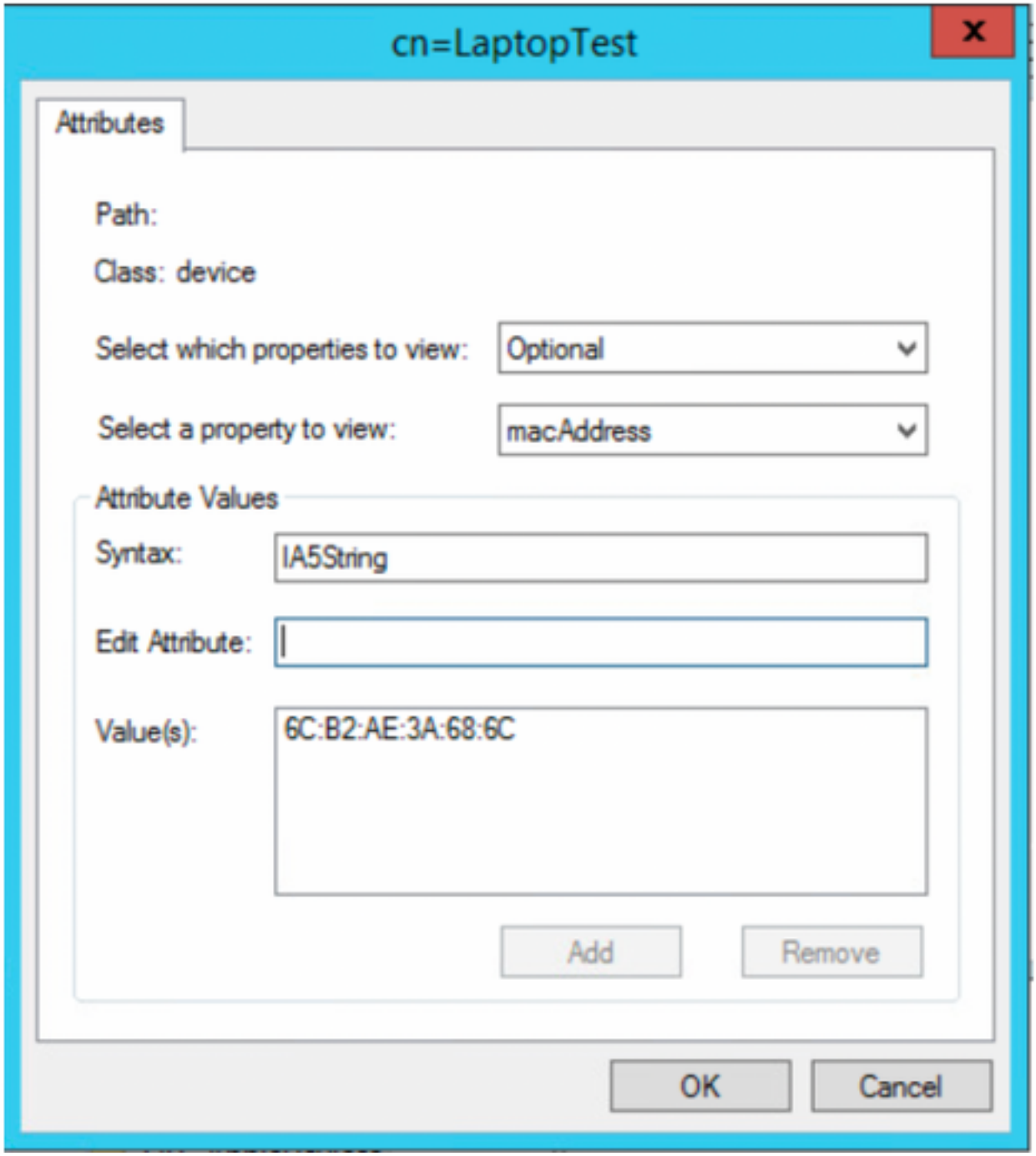


1. Selecteer de optie **Meer kenmerken**



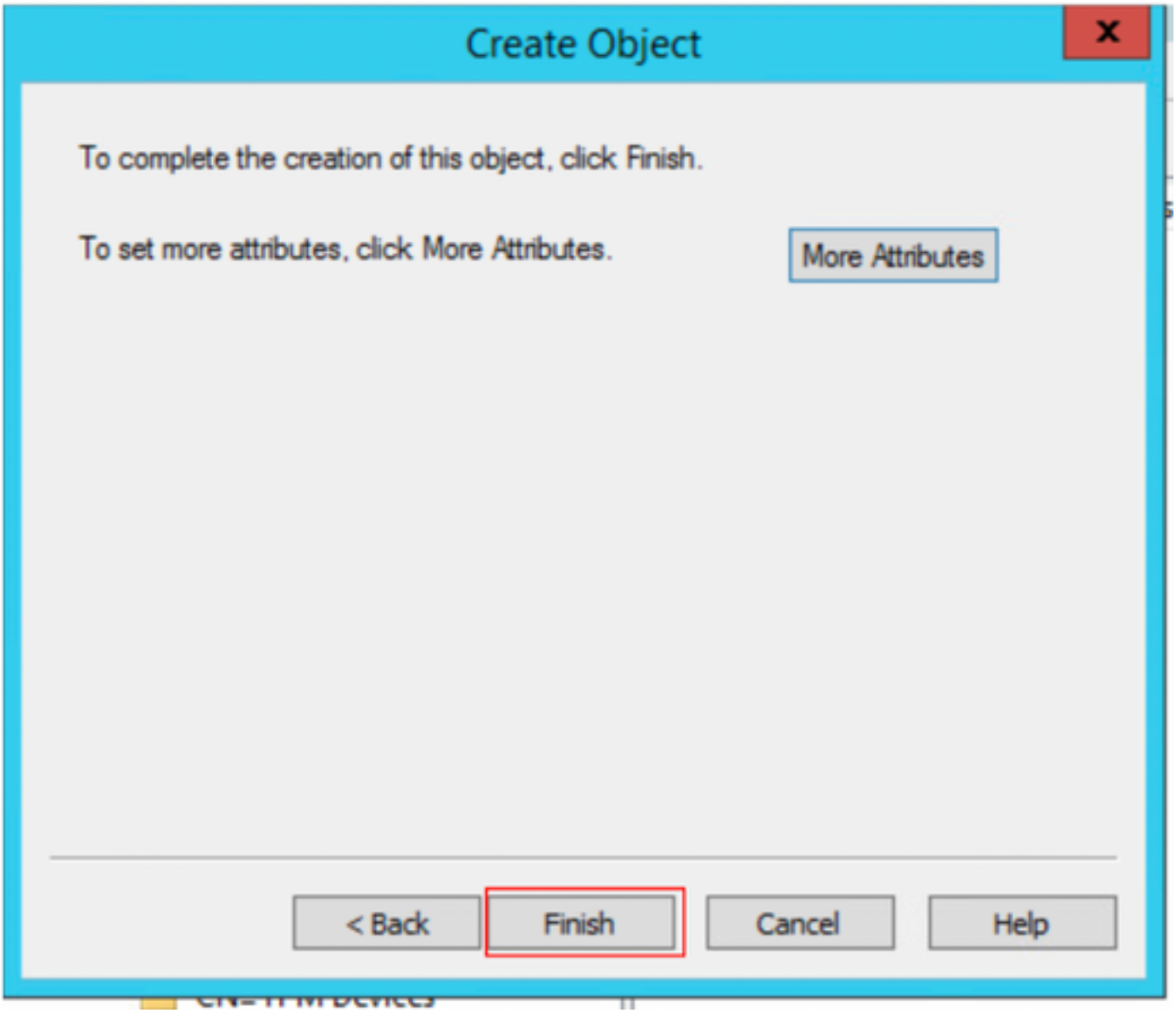
11. Voor het vervolgkeuzemenu **Selecteer een eigenschap die u wilt bekijken**, selecteer optie **macAddress** en definieer vervolgens het endpointadres dat voor authentiek zal zijn onder het veld **Eigenschappen** en selecteer de optie **Voeg** knop toe om het adres van het apparaat op te slaan.

Opmerking: Gebruik een dubbele kolom in plaats van een koppelteken tussen de hoofdadressen en de koppeltekens tussen de hoofdletters.

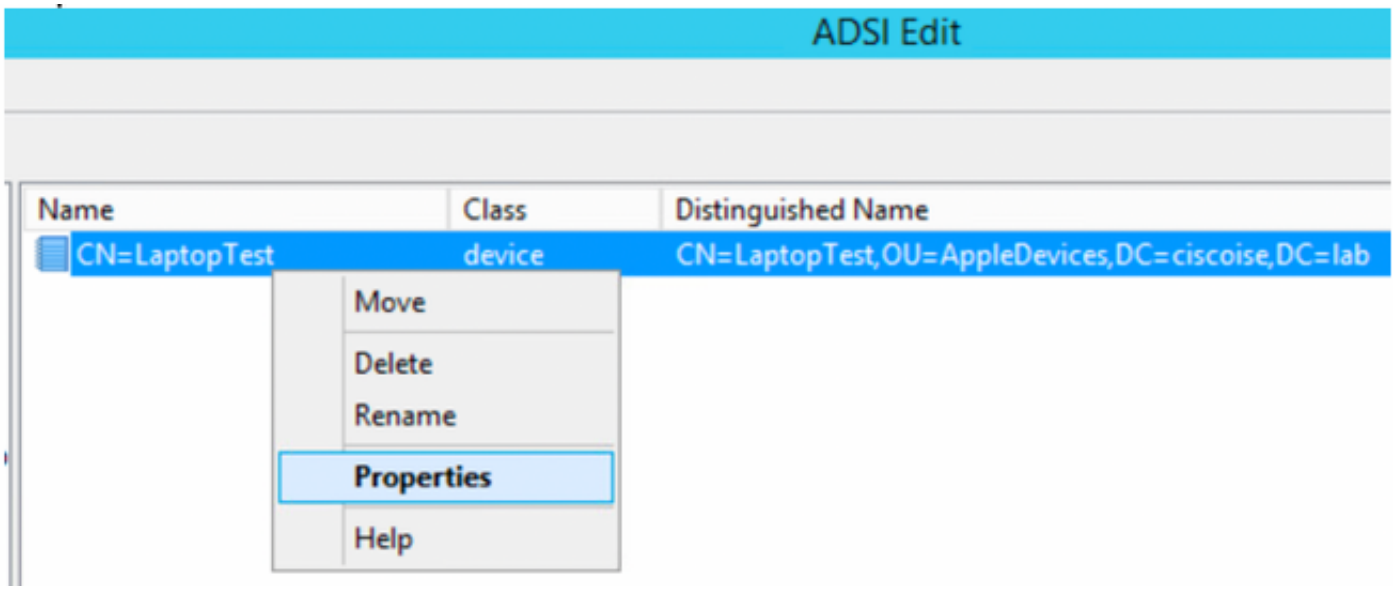


12. Selecteer **OK** om de informatie op te slaan en door te gaan met de configuratie van apparaatobjecten

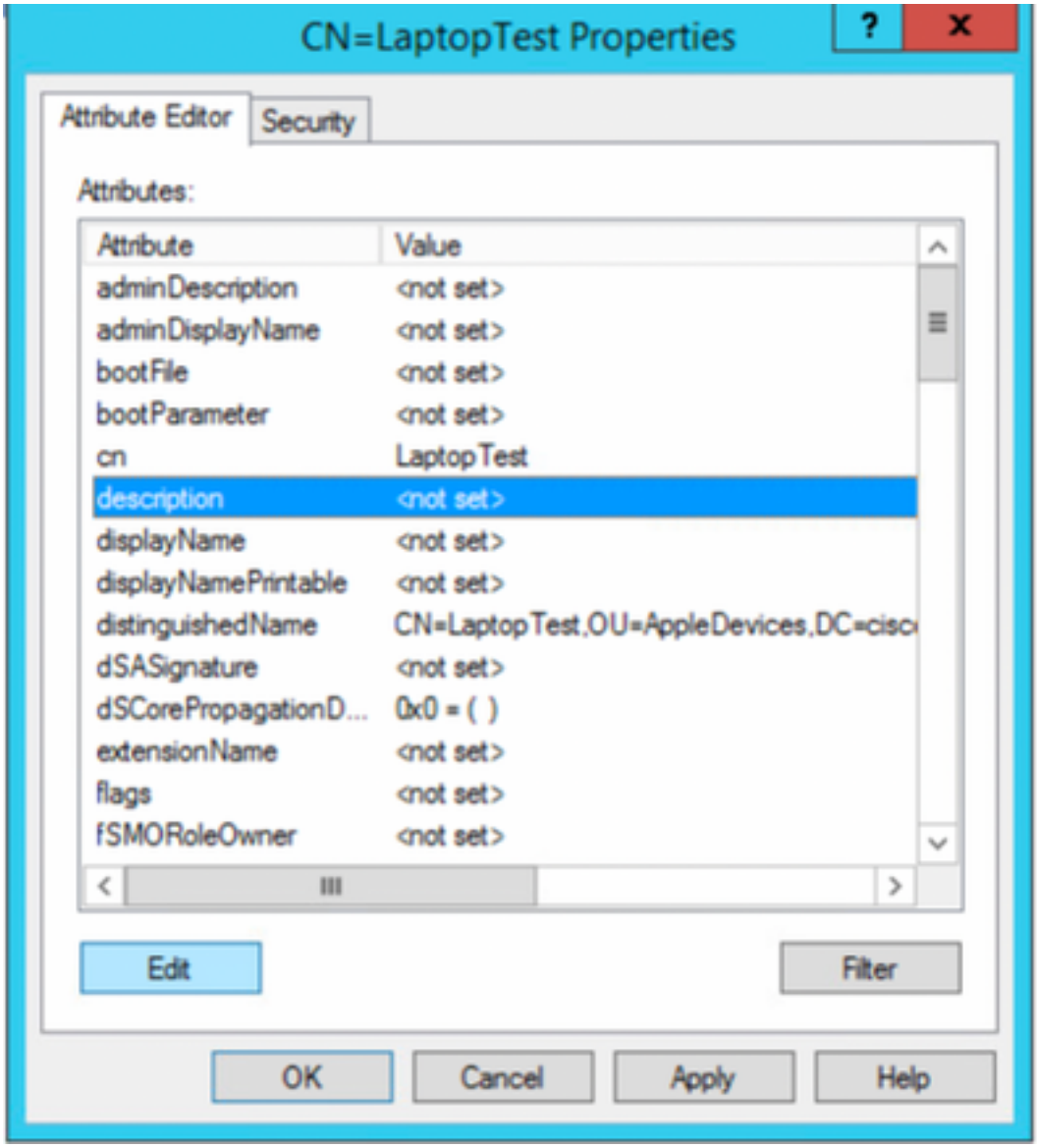
13. Selecteer **Voltooien** om het nieuwe apparaatobject te maken



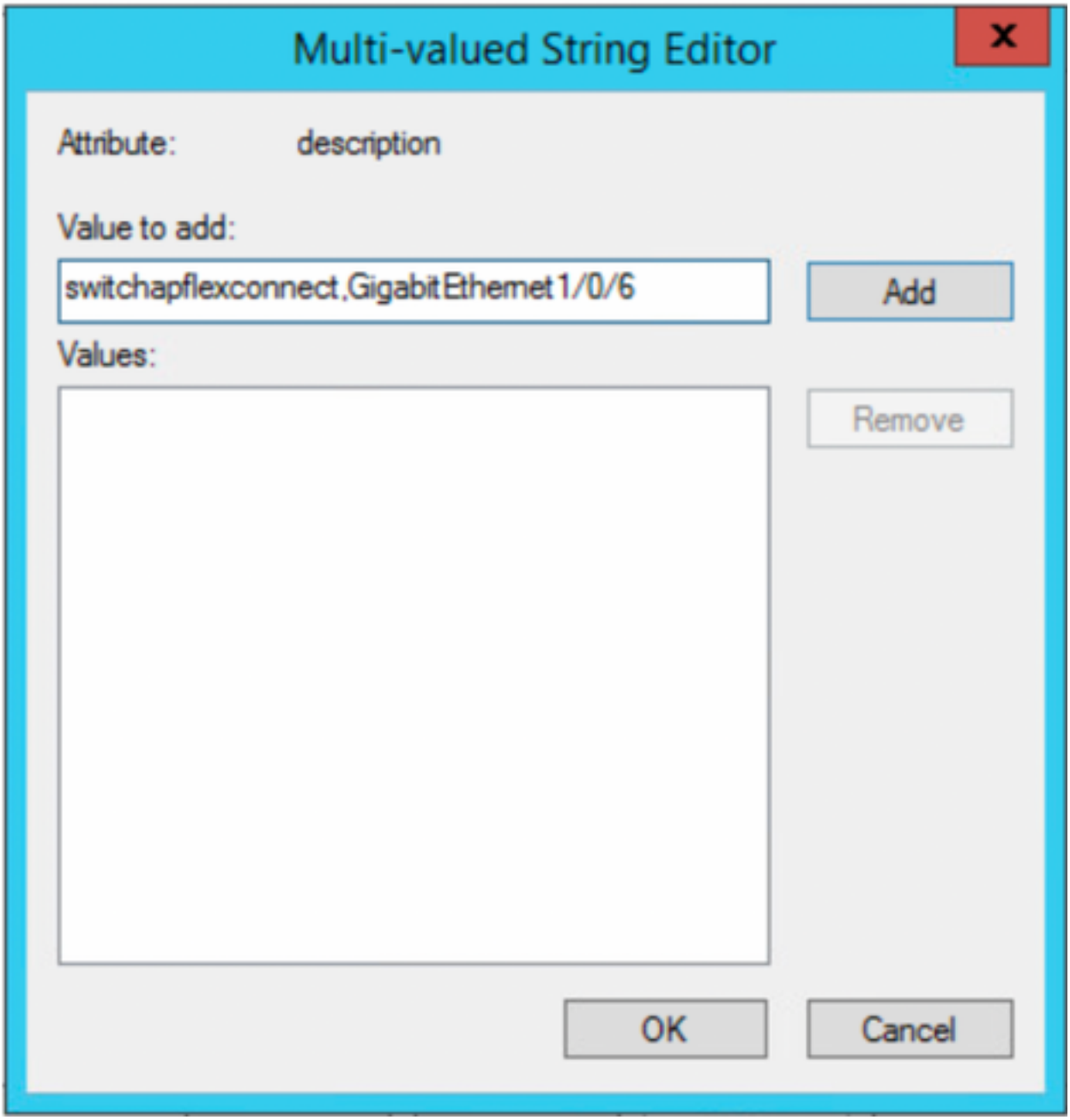
14. Klik met de rechtermuisknop op het apparaatobject en selecteer **Optieeigenschappen**



15. Selecteer de **beschrijving van de** optie en selecteer **Bewerken** om de naam van de schakelaar en de switchpoort te definiëren waar het apparaat met elkaar verbonden zal zijn.



16. Defineer de naam van de schakelaar en de schakelaar-poort, zorg ervoor dat u een komma gebruikt om elke waarde te scheiden. Selecteer **Add** en vervolgens **OK** om de informatie op te slaan.



- **Switchapflexverbinding is de naam van de schakelaar.**
- **Gigabit Ethernet1/0/6 is de switch-poort waarop het eindpunt is aangesloten.**

Opmerking: Het is mogelijk om scripts te gebruiken om eigenschappen aan een specifiek veld toe te voegen, maar in dit voorbeeld definiëren we handmatig de waarden

Opmerking: AD-attribuut is hoofdlettergevoelig, als u alle adressen van Mac gebruikt in het lagere geval ISE converteert naar hoofdletters tijdens de LDAP query. Om dit gedrag te vermijden, dient Proceshost-account uit te schakelen onder toegestane protocollen. Zie voor meer informatie deze link: https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

Switch-configuratie

Hieronder wordt de configuratie beschreven voor 802.1x-communicatie tussen ISE en de 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
```

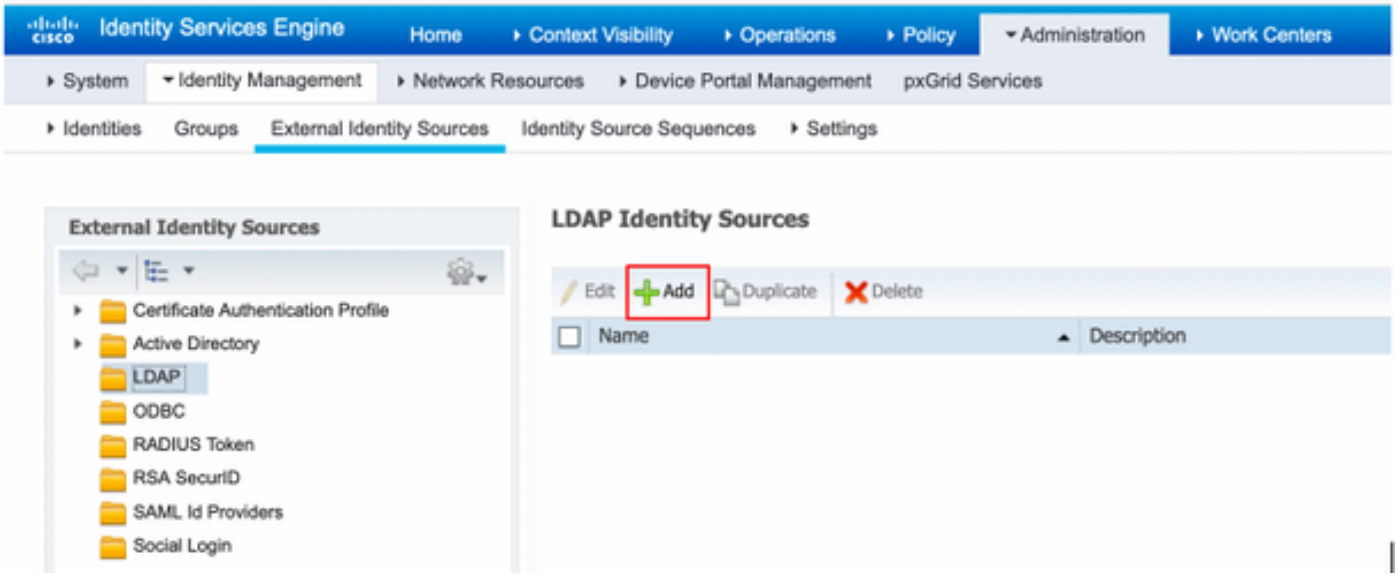
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access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

Opmerking: De configuratie van de aarde en de interface moet in uw omgeving mogelijk worden aangepast

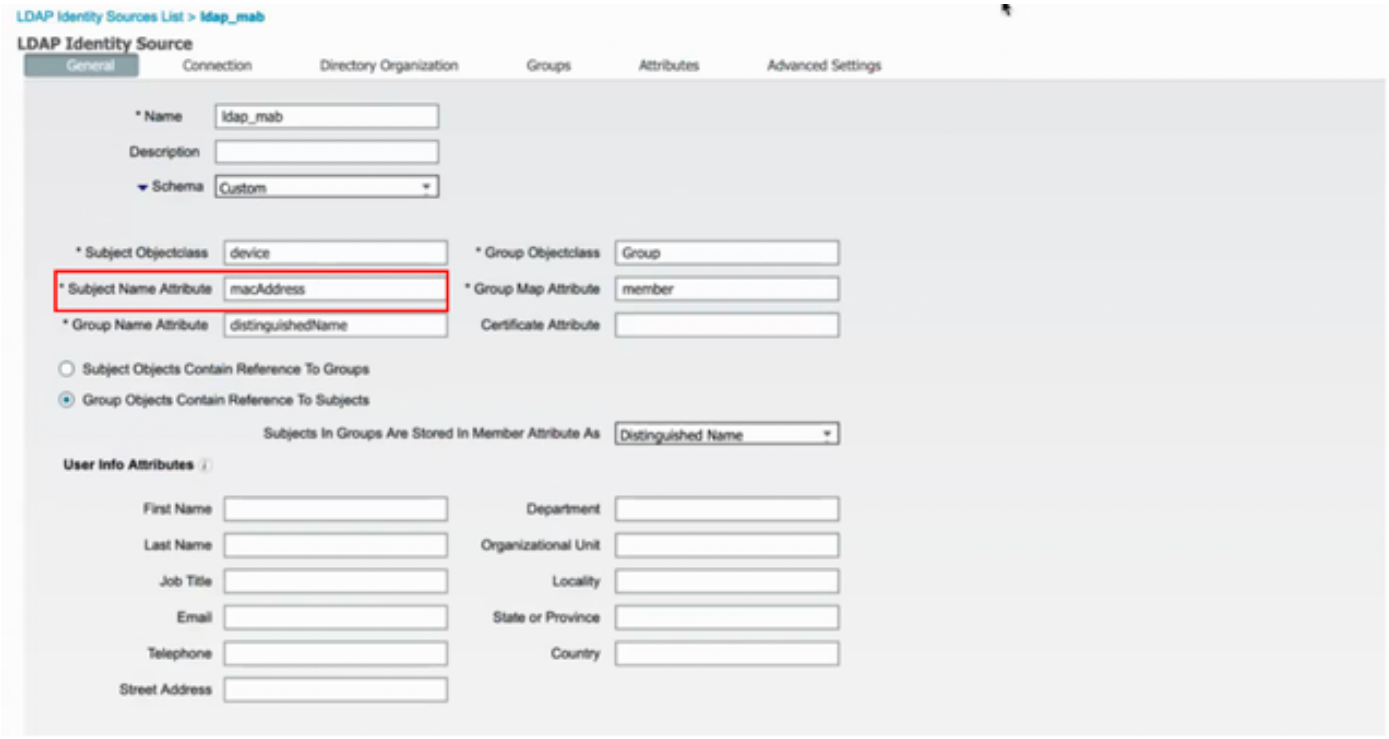
ISE-configuratie

Hieronder wordt de configuratie op ISE beschreven om de eigenschappen van de LDAP-server te verkrijgen en het ISE-beleid te configureren.

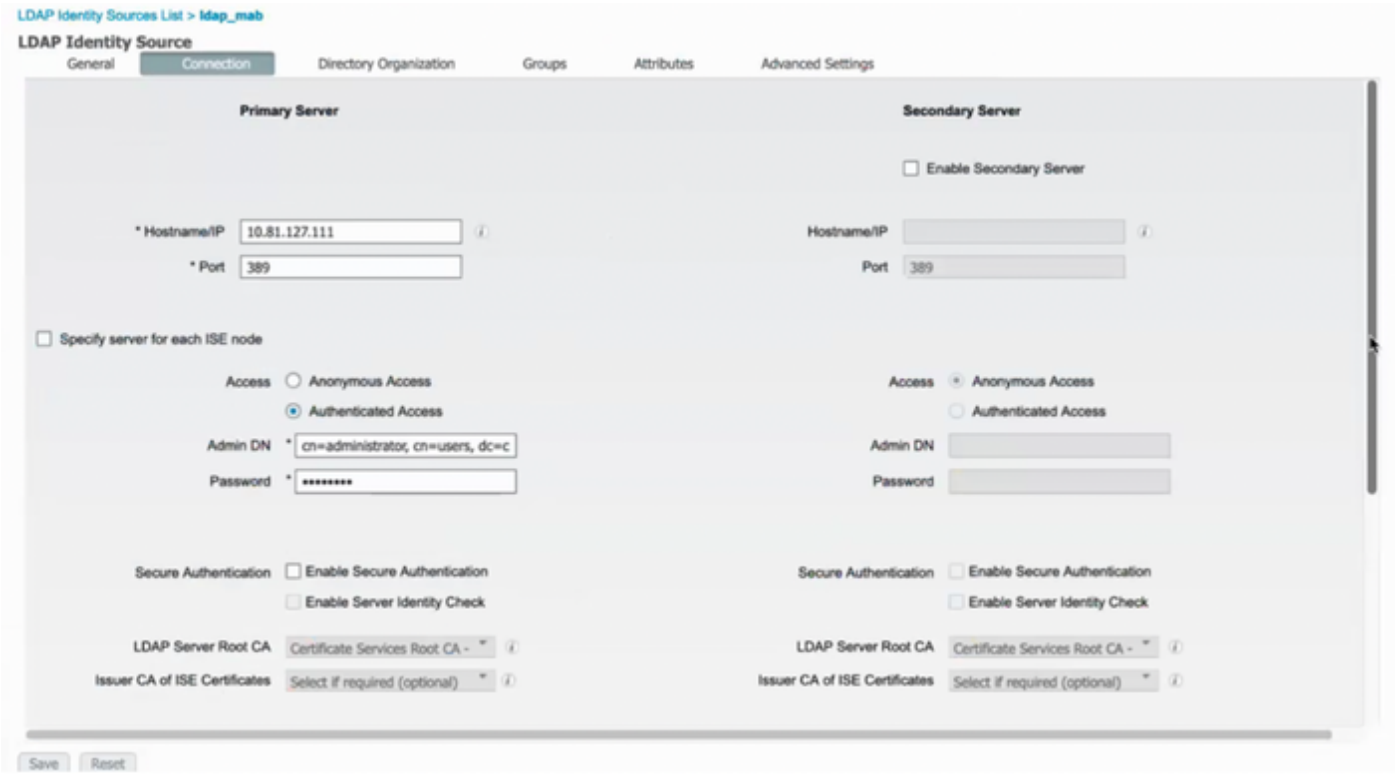
1. Ga op ISE naar **Administratie->identiteitsbeheer->Externe identiteitsbronnen** en selecteer de **LDAP**-map en klik op **Toevoegen** om een nieuwe verbinding met LDAP te maken



2.Onder **het** tabblad **General** definieert een naam en selecteert u het mac-adres als de eigenschap Onderwerp

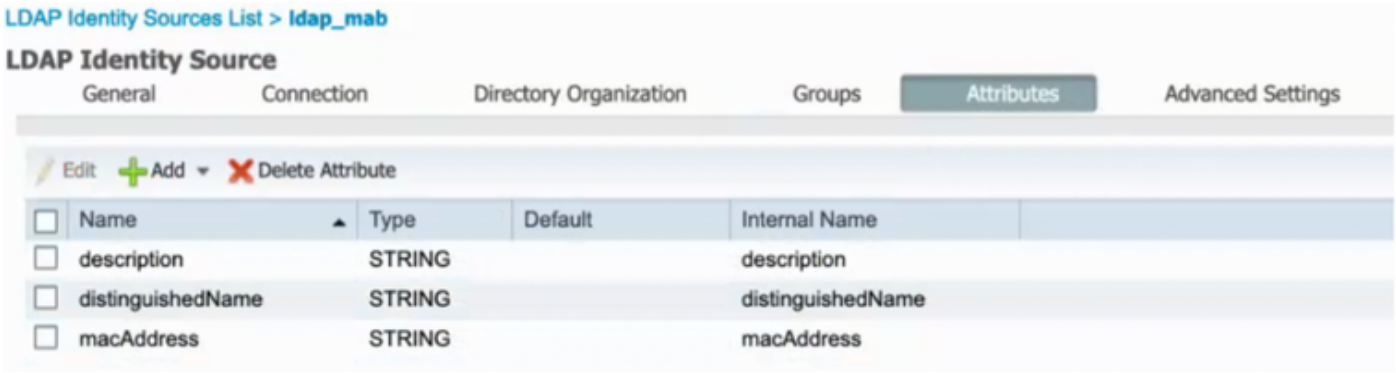


3. Onder het tabblad **Connection** moet u het IP-adres, admin DN en wachtwoord instellen vanaf de LDAP-server om een succesvolle verbinding te maken.

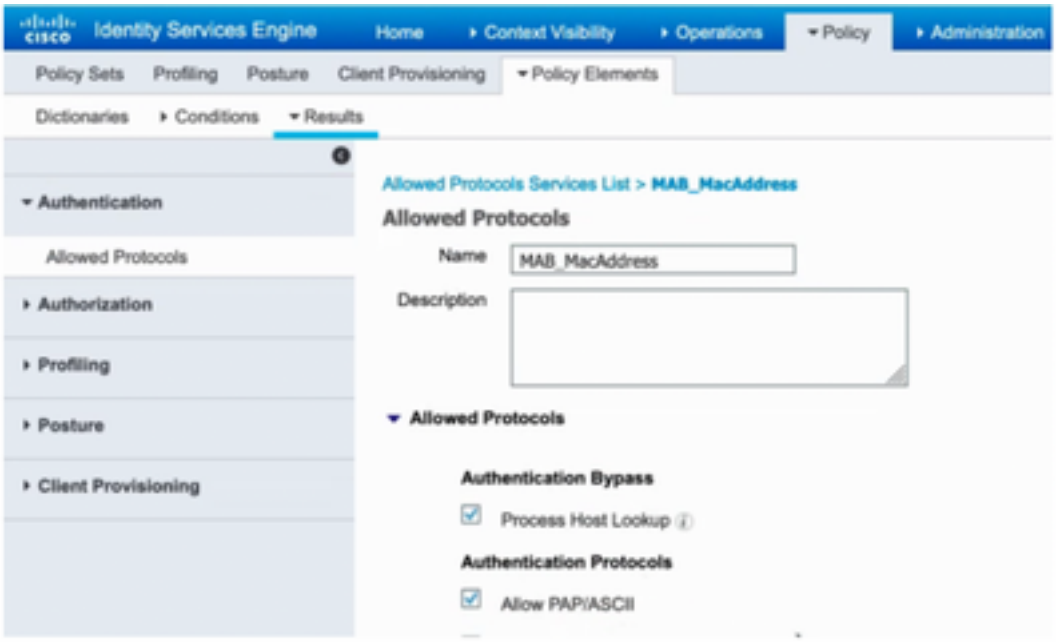


Opmerking: Port 3890 is de standaardpoort die wordt gebruikt.

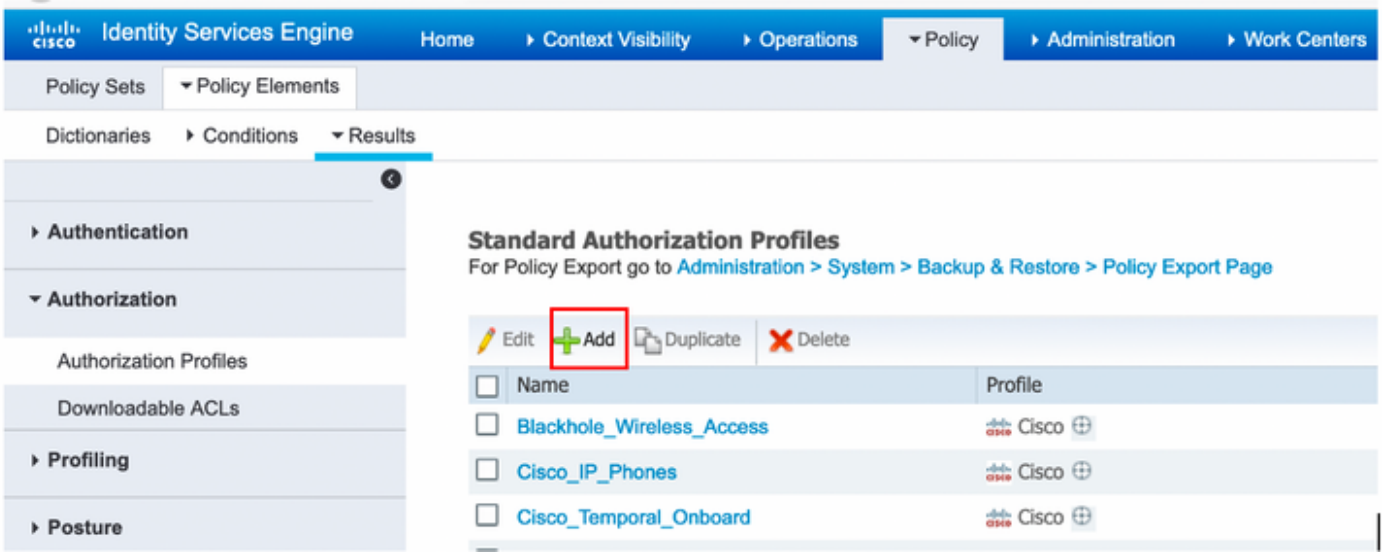
4. Onder tabblad **Eigenschappen** selecteert u de eigenschappen hoofdletter Adres en beschrijving van het autorisatiebeleid.

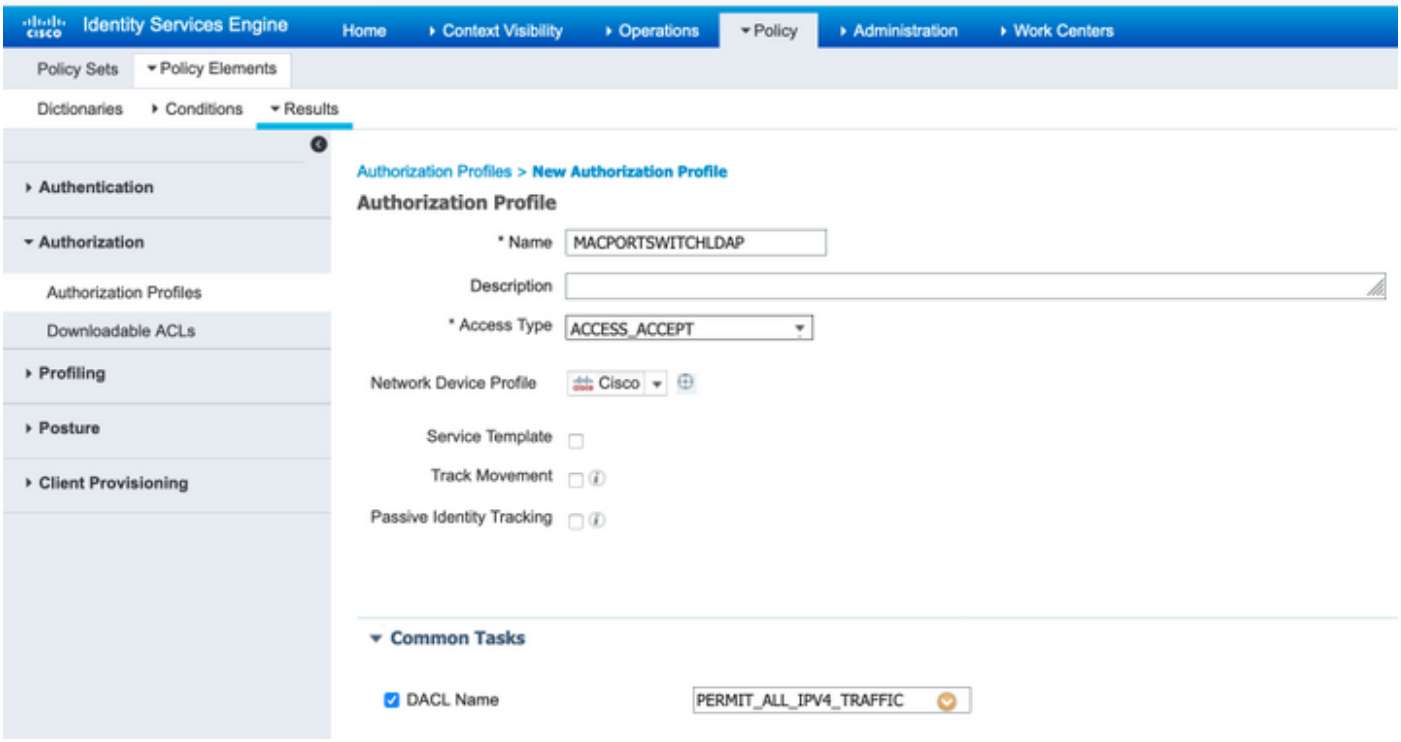


5. Om een geautoriseerd protocol te maken, gaat u naar **Beleidselementen->Resultaten->Verificatie->Geoorloofde protocollen.** Defineer en selecteer Host Lookup verwerken en sta PAP/ASCII toe als de enige toegestane protocollen. Selecteer ten slotte **Opslaan**

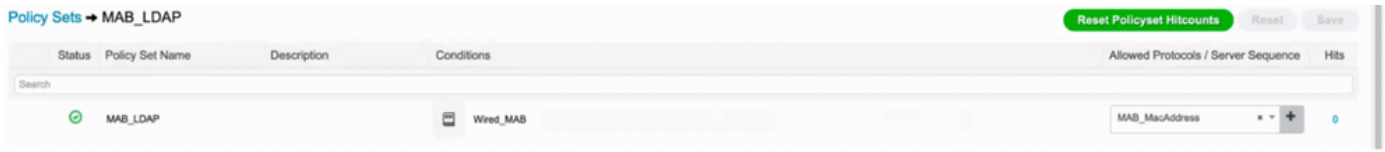


6. Om een vergunningsprofiel te maken, gaat u naar **Gegevens uit het beleid->Gegevens->Vergunningsprofielen.** Selecteer **Add** en definieer de permissies die aan het eindpunt worden toegewezen.

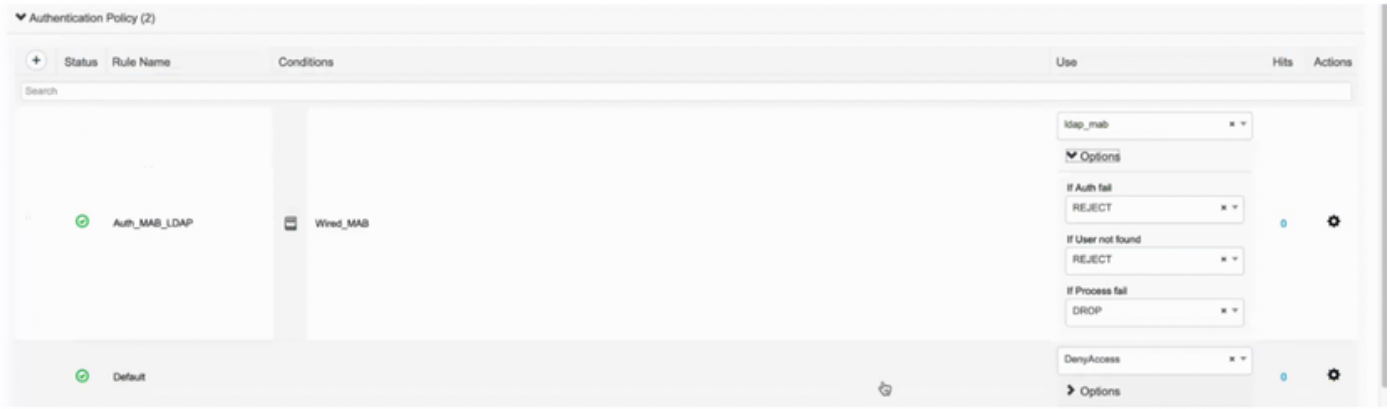




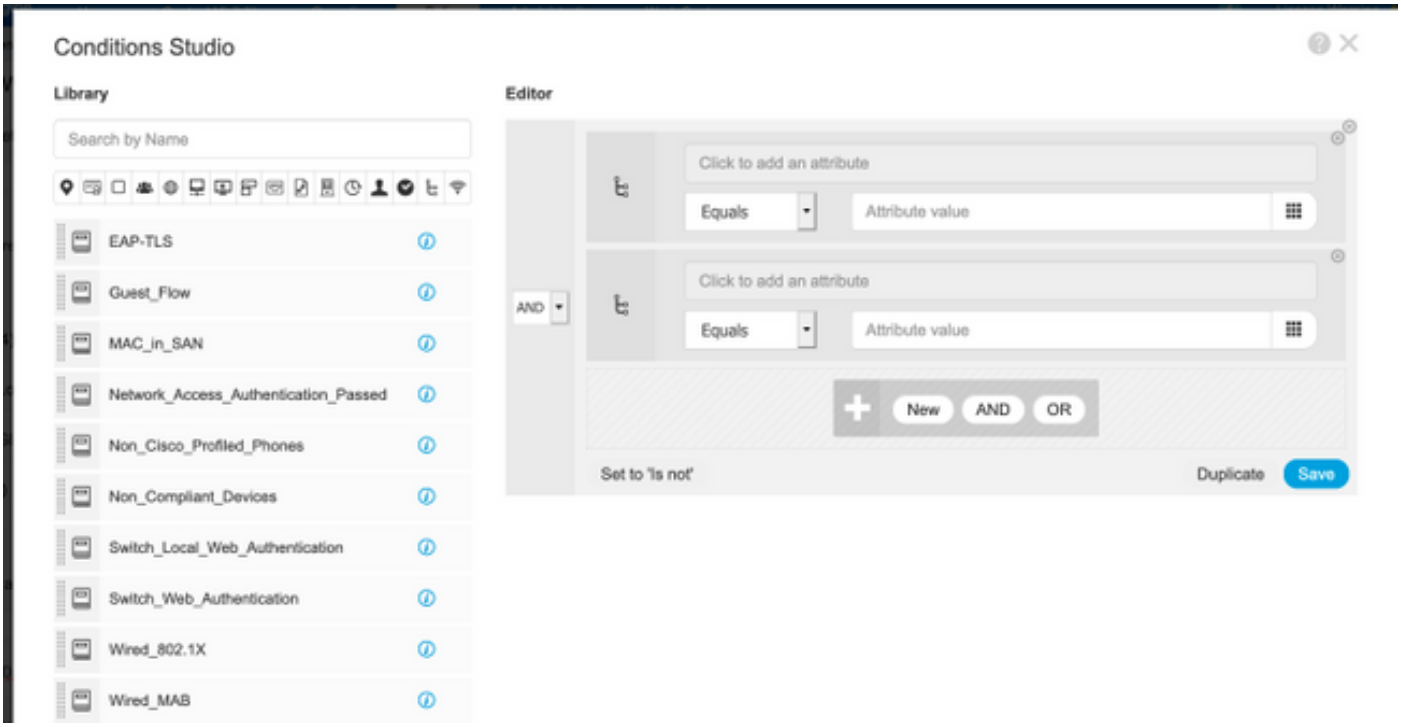
7.Ga naar Policy Suite en maak een beleidsset aan de hand van de vooraf gedefinieerde conditie Wired_MAB en het toegestane protocol dat in stap 5 is gemaakt.

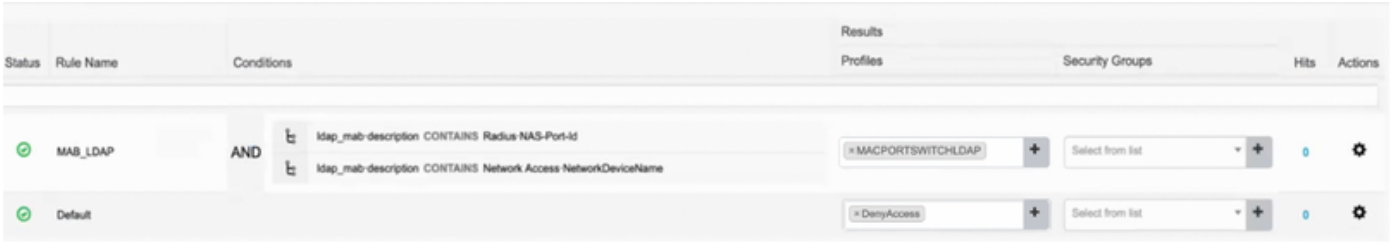


8. In het kader van de nieuwe beleidsset werd een verificatiebeleid gecreëerd dat gebruik maakte van de vooraf gedefinieerde sequentie **Wired_MAB** Library en **LDAP** als externe identiteitsbron



9. Onder **Automation Policy** wordt een naam gedefinieerd en een samengestelde voorwaarde gemaakt met behulp van de beschrijving van de LFI-kenmerken, de NAS-poorts-ID en de NetworkDevices-Name. Voeg ten slotte het machtigingsprofiel toe dat in stap 6 is gemaakt.





Nadat u de configuratie hebt toegepast, dient u in staat te zijn verbinding te maken met het netwerk zonder tussenkomst van de gebruiker.

Verifiëren

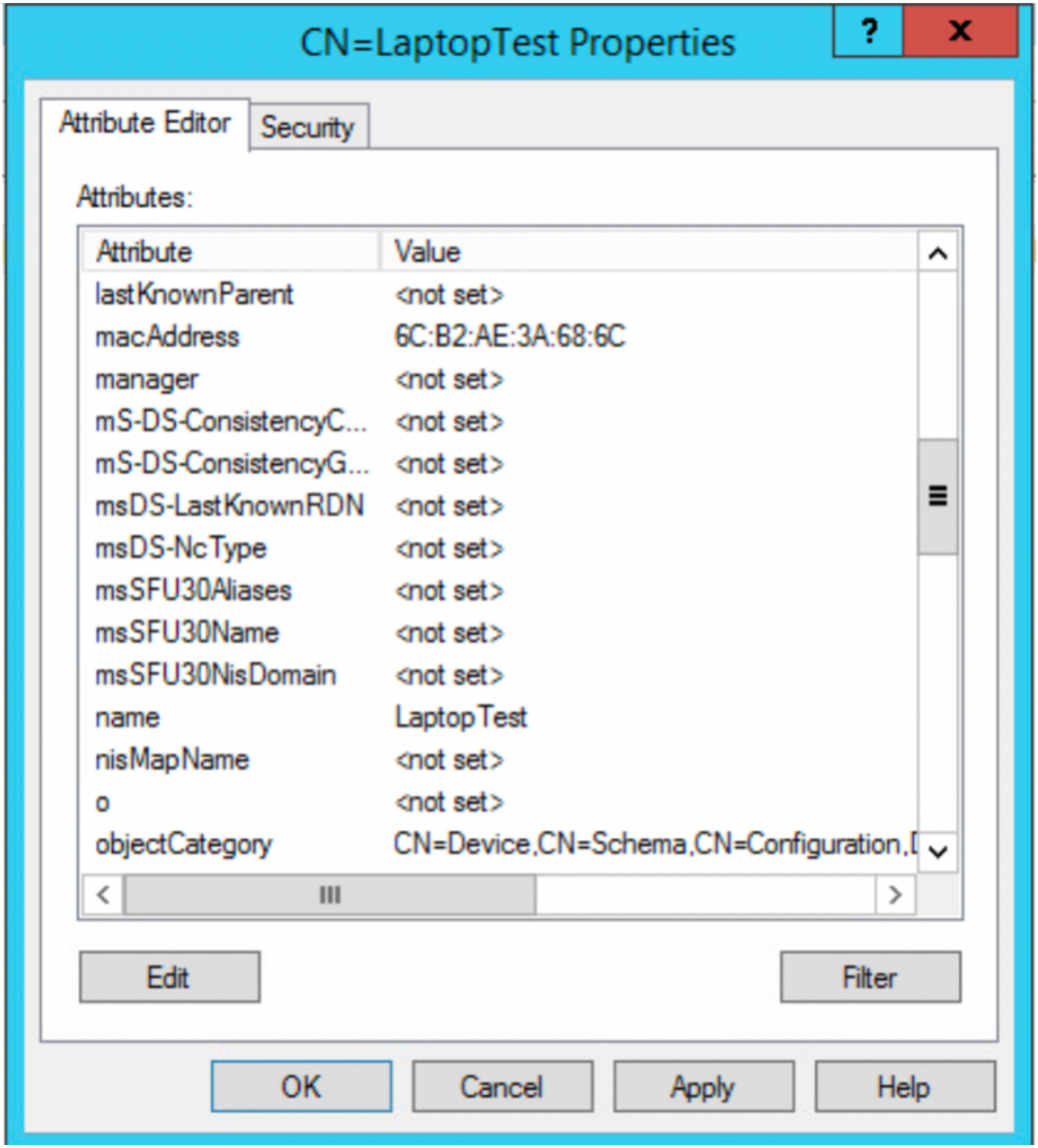
Nadat u is aangesloten op de aangewezen schakelaar-poort kunt u **authenticatiesessie-interface Gigabit Ethernet X/X/X details** typen om de authenticatie- en autorisatiestatus van het apparaat te valideren.

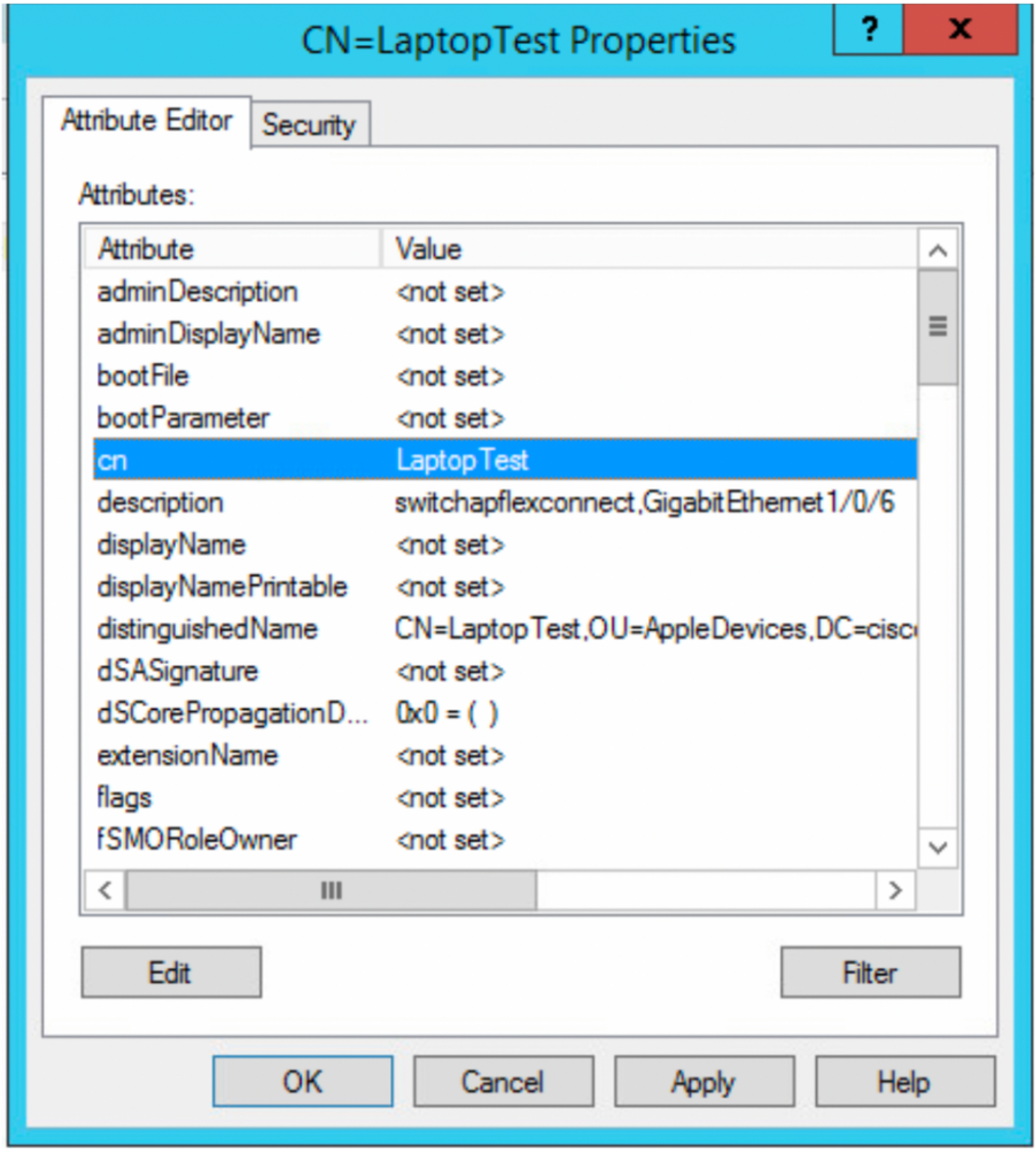
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session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

Op ISE kunt u Live Logs voor bevestiging gebruiken.

Problemen oplossen

Bevestig op de LDAP server dat het gemaakte apparaat een Mac adres, een juiste naam en een schakelaar-poort heeft


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



Op ISE kunt u een pakketvastlegging (Ga naar **Operations->Troubleshoot ->Diagnostisch Tool-TCP-bulten**) uitvoeren om te valideren dat de waarden van LDAP naar ISE worden verzonden