

# ISE- und LDAP-Attributbasierte Authentifizierung

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[LDAP konfigurieren](#)

[Switch-Konfiguration](#)

[ISE-Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie die Cisco Identity Services Engine (ISE) konfigurieren und Geräte mithilfe von LDAP-Objektattributen (Lightweight Directory Access Protocol) dynamisch authentifizieren und autorisieren.

**Hinweis:** Dieses Dokument gilt für Einrichtungen, die LDAP als externe Identitätsquelle für die ISE-Authentifizierung und -Autorisierung verwenden.

Beteiligt durch Emmanuel Cano und Mauricio Ramos Cisco Professional Services Engineer.

Editiert von Neri Cruz Cisco TAC Engineer.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, die folgenden Themen zu kennen:

- Grundkenntnisse der ISE-Richtlinien, der Authentifizierungs- und Autorisierungsrichtlinien
- MAB (Mac Authentication Bypass)
- Grundkenntnisse des Radius-Protokolls
- Grundkenntnisse des Windows-Servers

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- 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-Computer

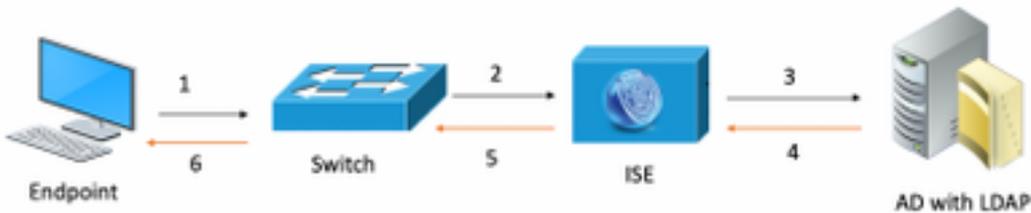
**Hinweis:** Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konfiguration

In diesem Abschnitt wird beschrieben, wie Sie die Netzwerkgeräte konfigurieren, die Integration zwischen ISE und LDAP vornehmen und schließlich LDAP-Attribute für die Verwendung in der ISE-Autorisierungsrichtlinie konfigurieren.

## Netzwerkdiagramm

Dieses Bild zeigt die verwendete Netzwerktopologie:



Hier ist der Datenverkehrsfluss, wie im Netzwerkdiagramm veranschaulicht:

1. Der Benutzer verbindet seinen PC/Laptop mit dem vorgesehenen Switch-Port.
2. Der Switch sendet eine Radius-Zugriffsanforderung für diesen Benutzer an die ISE
3. Wenn die ISE die Informationen erhält, fragt sie den LDAP-Server für das spezifische Benutzerfeld ab, das die Attribute enthält, die in den Autorisierungsrichtlinienbedingungen verwendet werden.
4. Sobald die ISE die Attribute (Switch-Port, Switch-Name und MAC-Adresse des Geräts) erhält, vergleicht sie die vom Switch bereitgestellten Informationen.
5. Wenn die vom Switch bereitgestellten Attributinformationen mit denen von LDAP übereinstimmen, sendet die ISE ein RADIUS Access-Accept mit den im Autorisierungsprofil konfigurierten Berechtigungen.

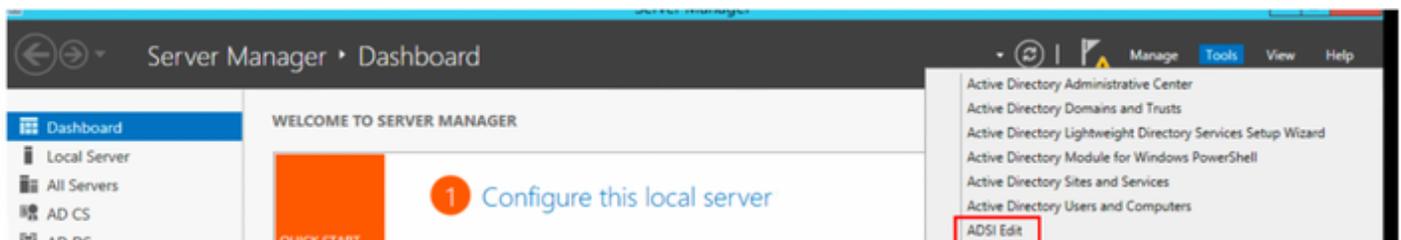
## Konfigurationen

In diesem Abschnitt können Sie LDAP, Switch und ISE konfigurieren.

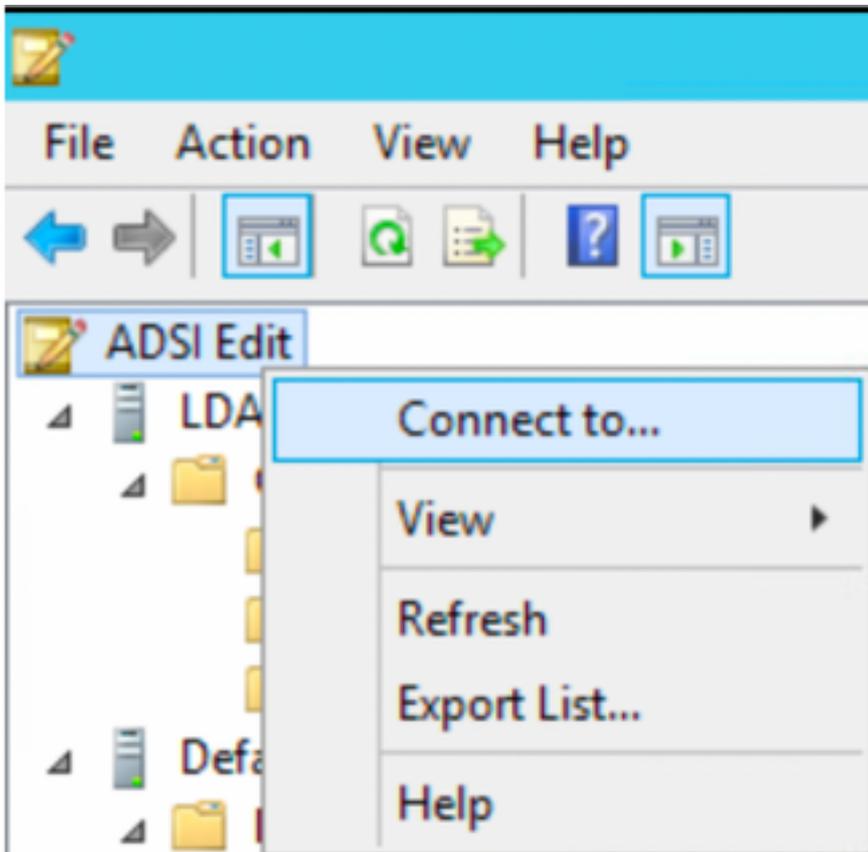
### Konfiguration LDAP

Führen Sie die folgenden Schritte aus, um den LDAP-Server zu konfigurieren:

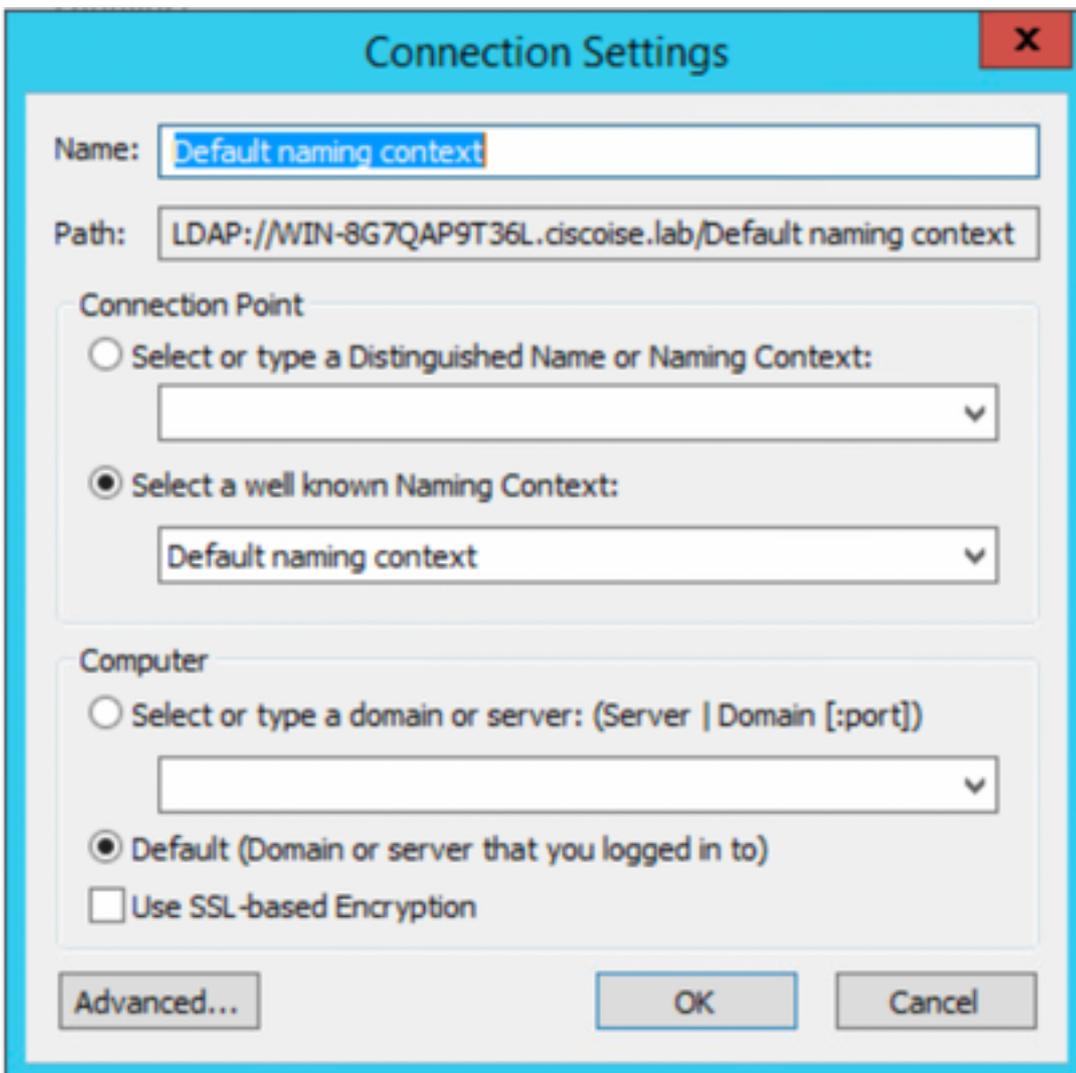
1. Navigieren Sie zu **Server Manager > Dashboard > Tools > ADSI Edit**.



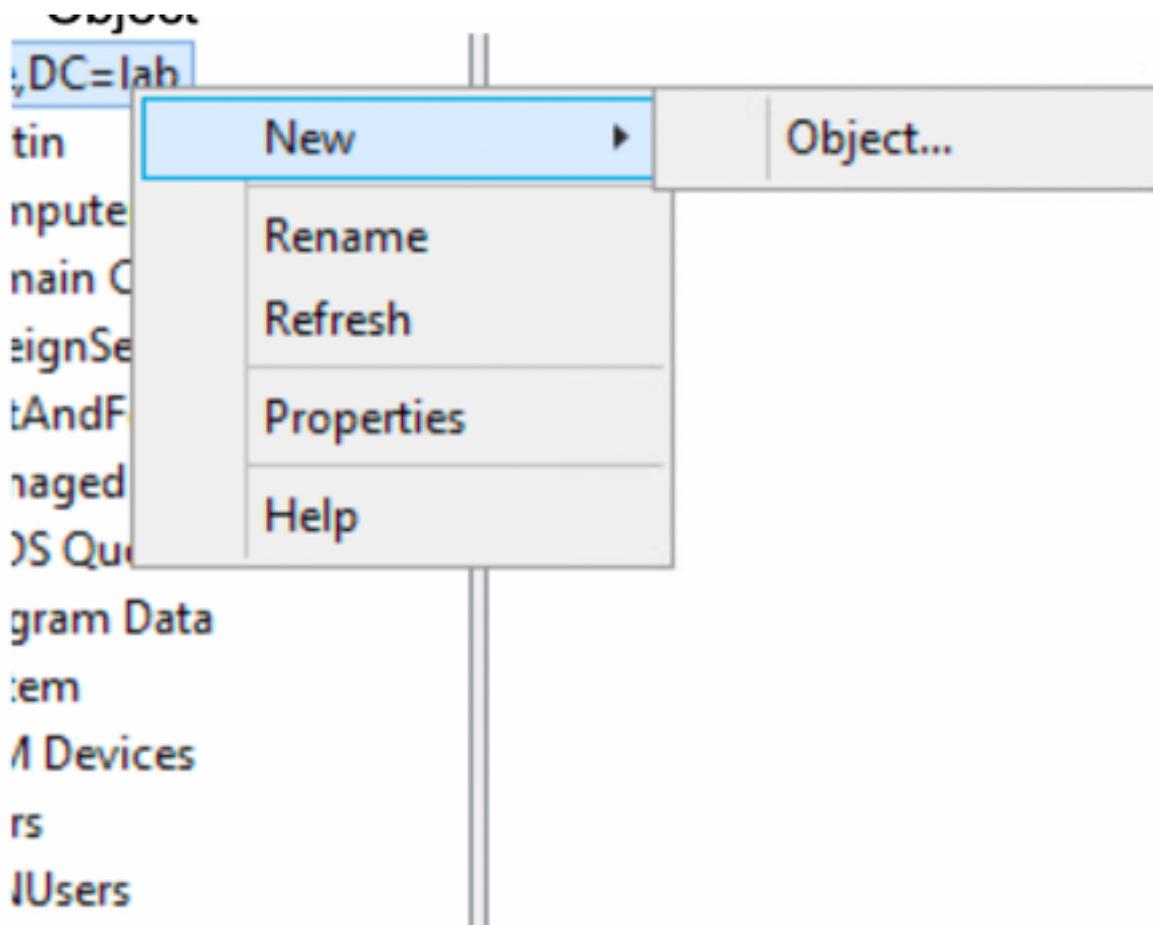
2. Klicken Sie mit der rechten Maustaste auf das Symbol ADSI Edit, und wählen Sie **Connect to.. (Verbinden mit)** aus.



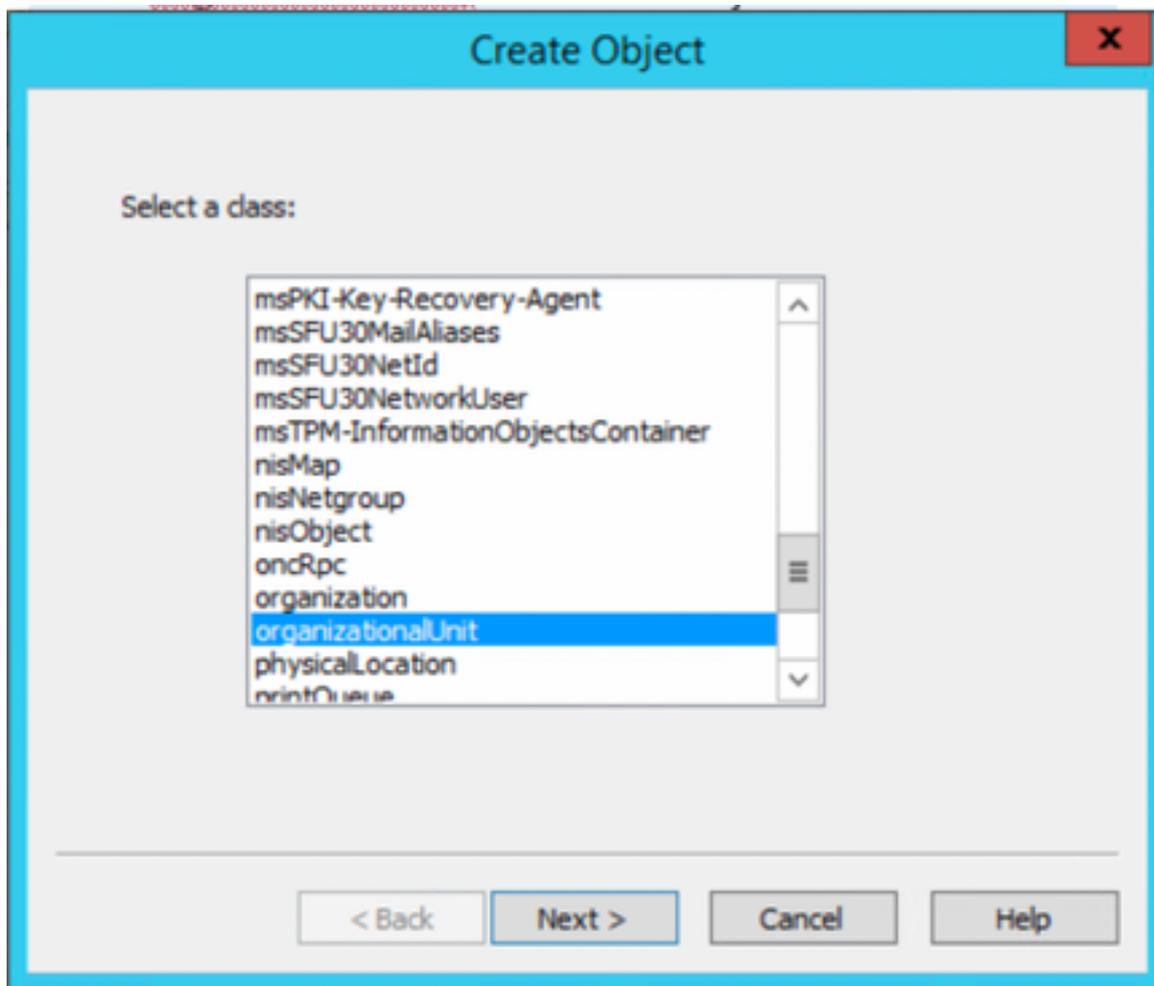
3. Definieren Sie unter Verbindungseinstellungen einen Namen, und wählen Sie die Schaltfläche OK, um die Verbindung zu starten.



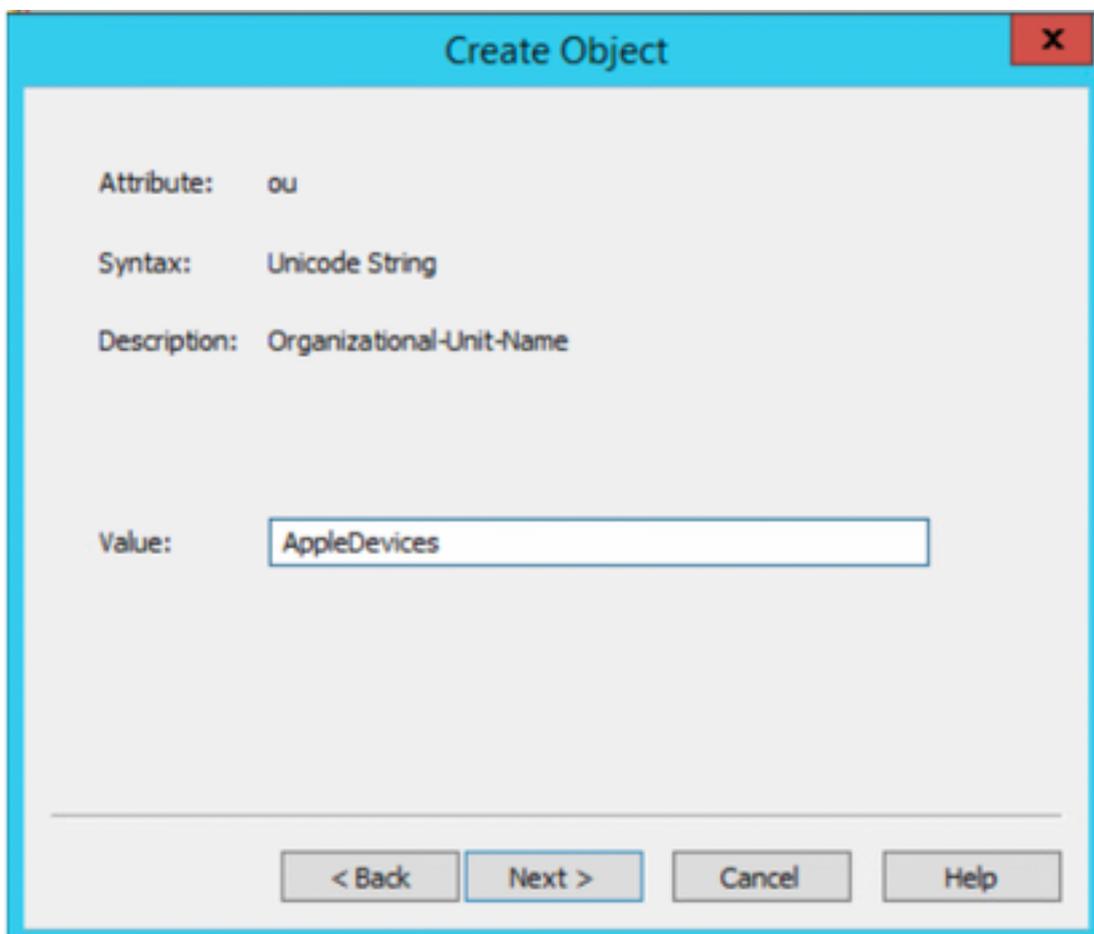
4. Klicken Sie im Menü ADSI Edit (ADSI-Bearbeiten) mit der rechten Maustaste in die Verbindung für das Rechenzentrum (DC=ciscodemo, DC=lab), wählen Sie **Neu**, und wählen Sie dann die Option **Objekt**



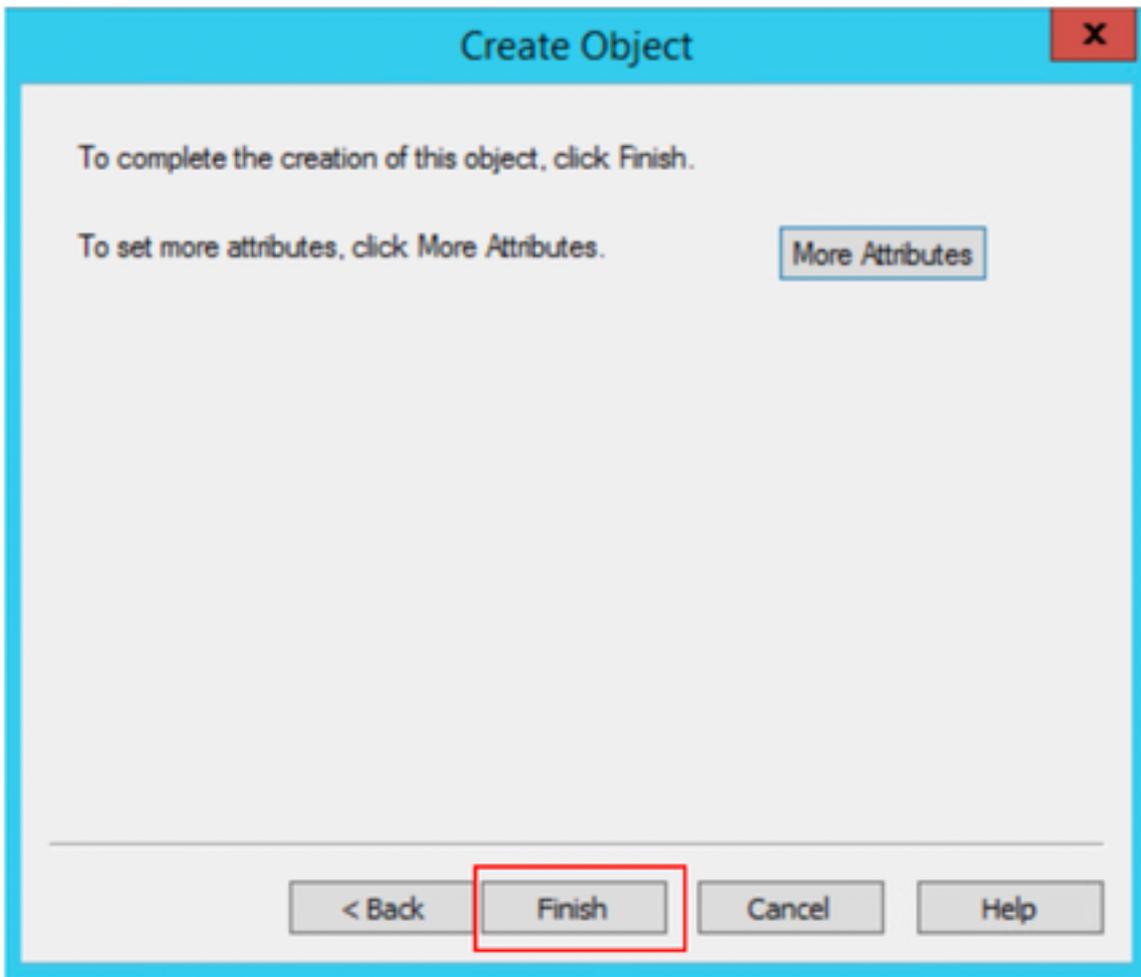
5. Wählen Sie die Option **OrganizationalUnit** als neues Objekt aus, und wählen Sie **als Nächstes** aus.



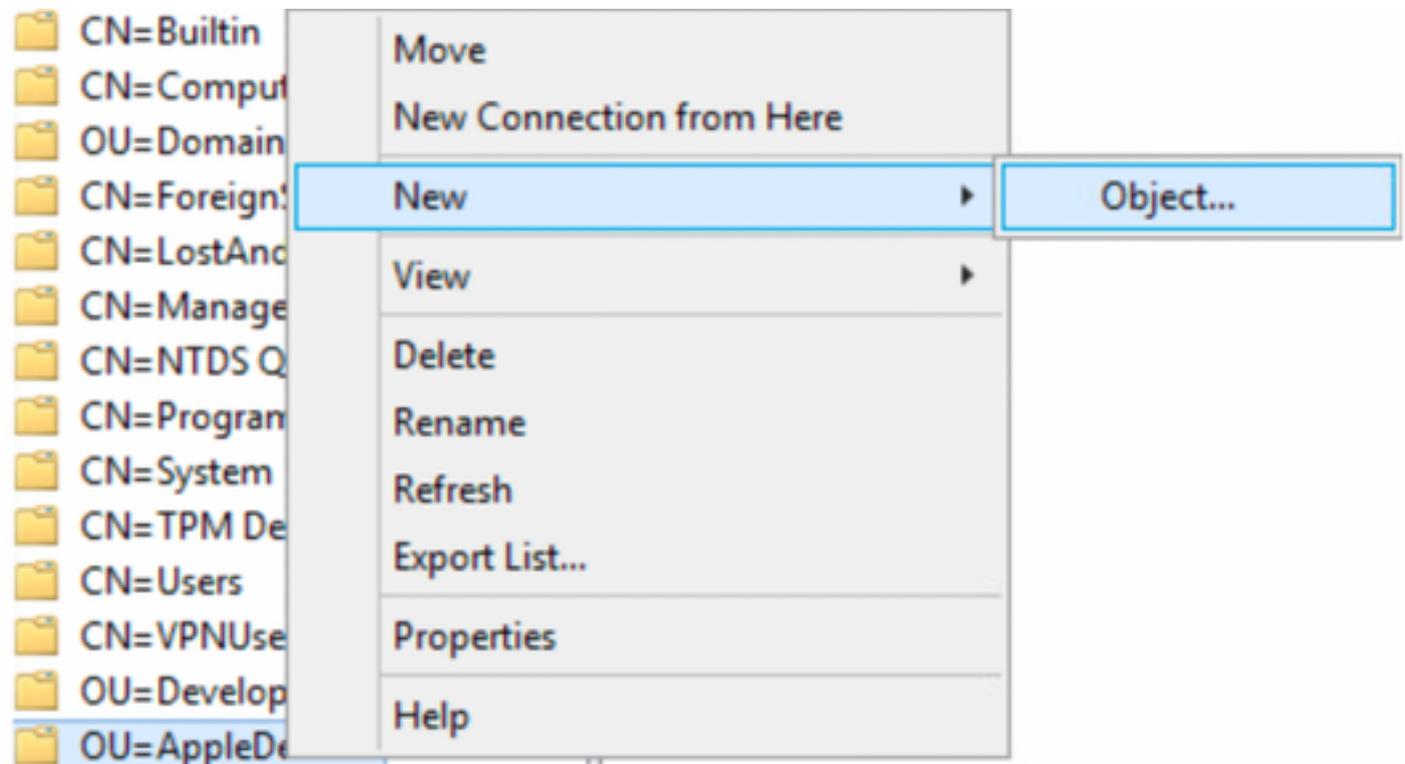
6. Definieren Sie einen Namen für die neue Organisationseinheit, und wählen Sie **Weiter**



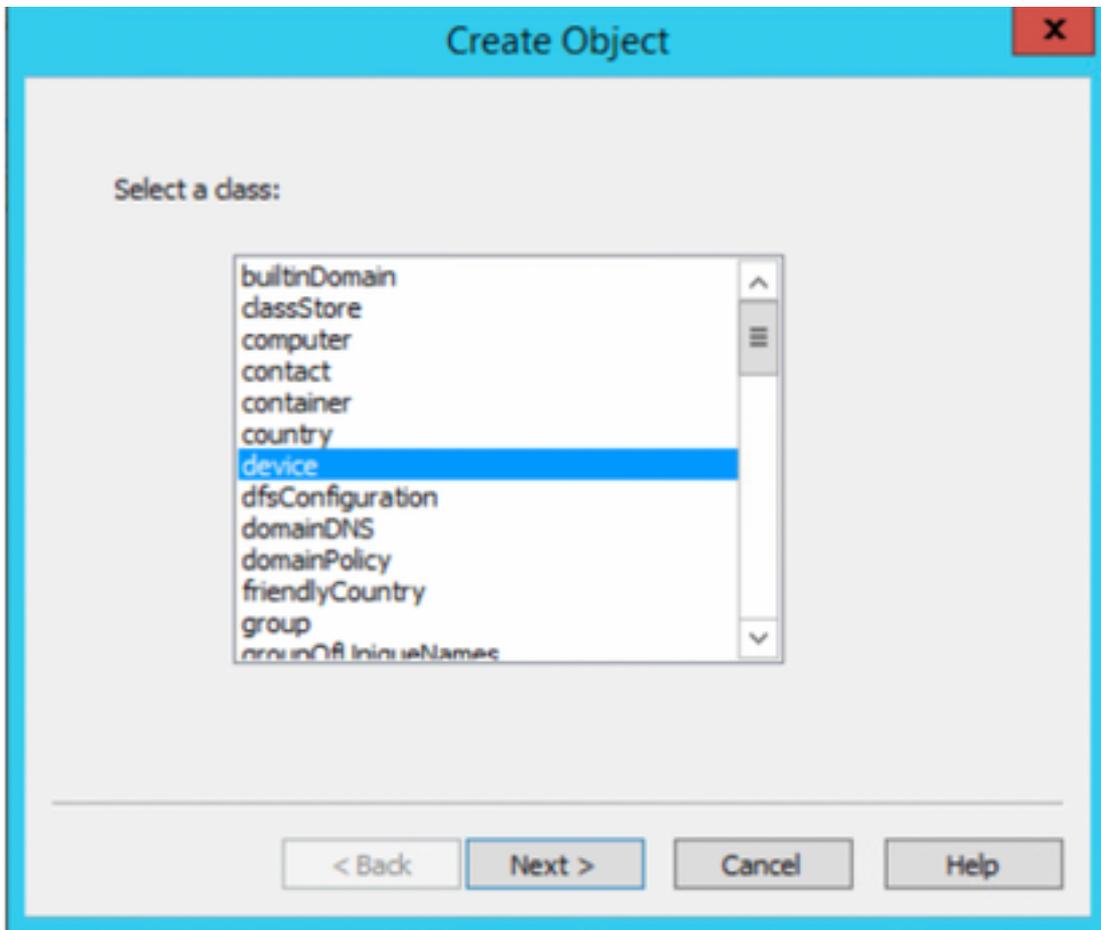
7. Wählen Sie **Fertig stellen**, um die neue Organisationseinheit zu erstellen.



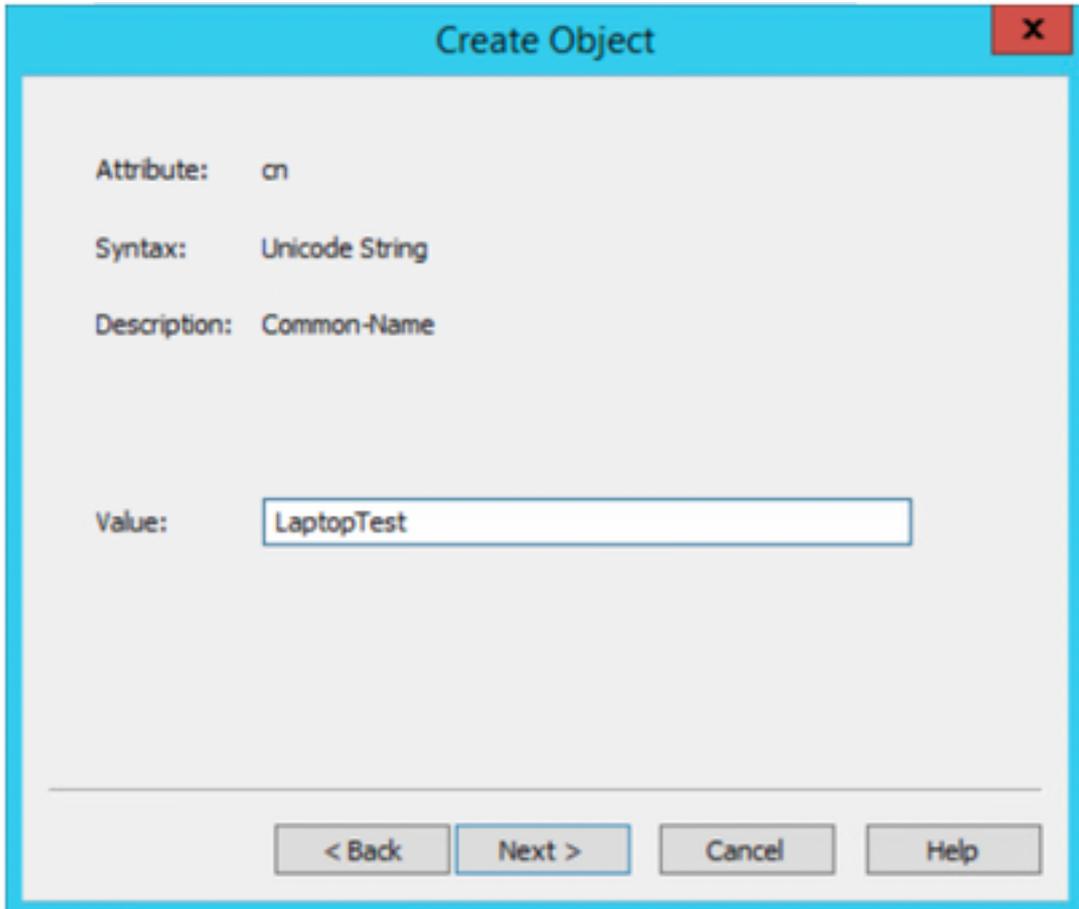
8. Klicken Sie mit der rechten Maustaste auf die gerade erstellte Organisationseinheit, und wählen Sie **Neu > Objekt**



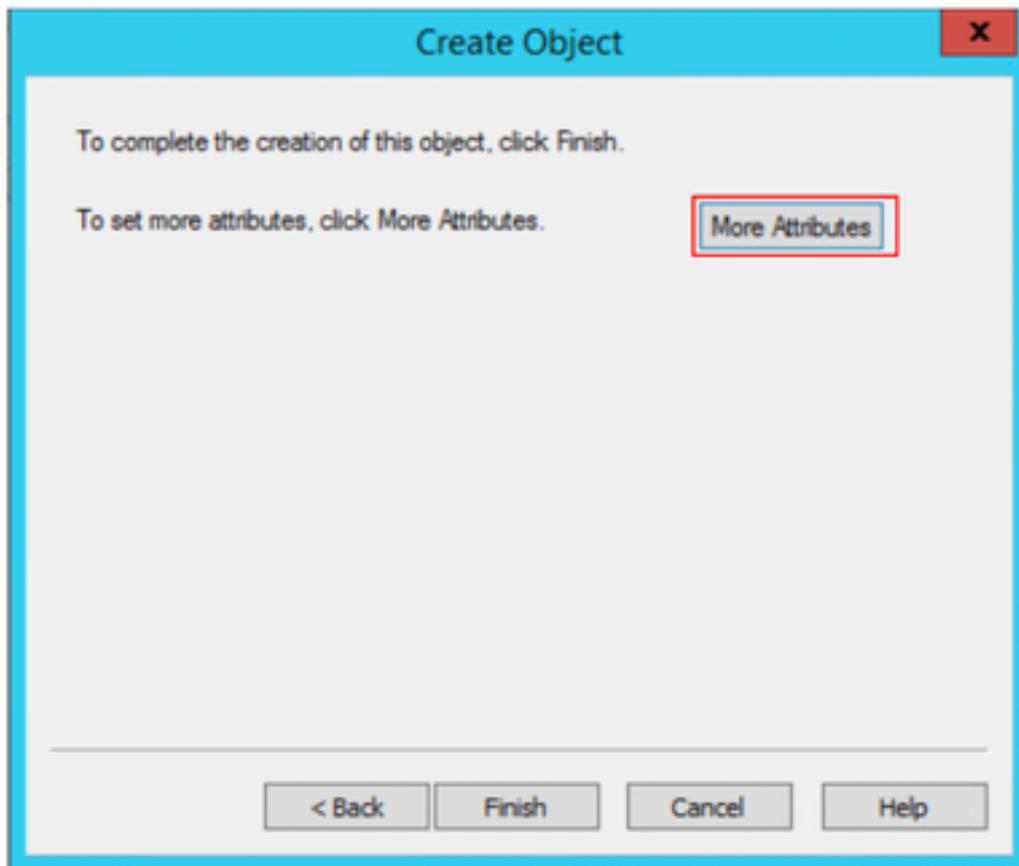
9. Wählen Sie das **Gerät** als Objektklasse aus, und wählen Sie **Nächste**



10. Definieren Sie einen Namen im Feld Wert, und wählen Sie **Weiter** aus.



11. Wählen Sie die Option **More Attributes (Mehr Attribute)** aus.



11. Wählen Sie im Dropdown-Menü **eine anzuzeigende Eigenschaft aus**, wählen Sie die Option **MACAddress aus**, definieren Sie dann die MAC-Adresse des Endpunkts, die im Feld **Edit**-Attribut authentifiziert wird, und wählen Sie die Schaltfläche **hinzufügen**, um die MAC-Adresse des Geräts zu speichern.

**Hinweis:** Verwenden Sie einen doppelten Doppelpunkt anstelle von Punkten oder Bindestrich zwischen MAC-Adressenoctets.

cn=LaptopTest

Attributes

Path:

Class: device

Select which properties to view: Optional

Select a property to view: macAddress

Attribute Values

Syntax: IA5String

Edit Attribute: |

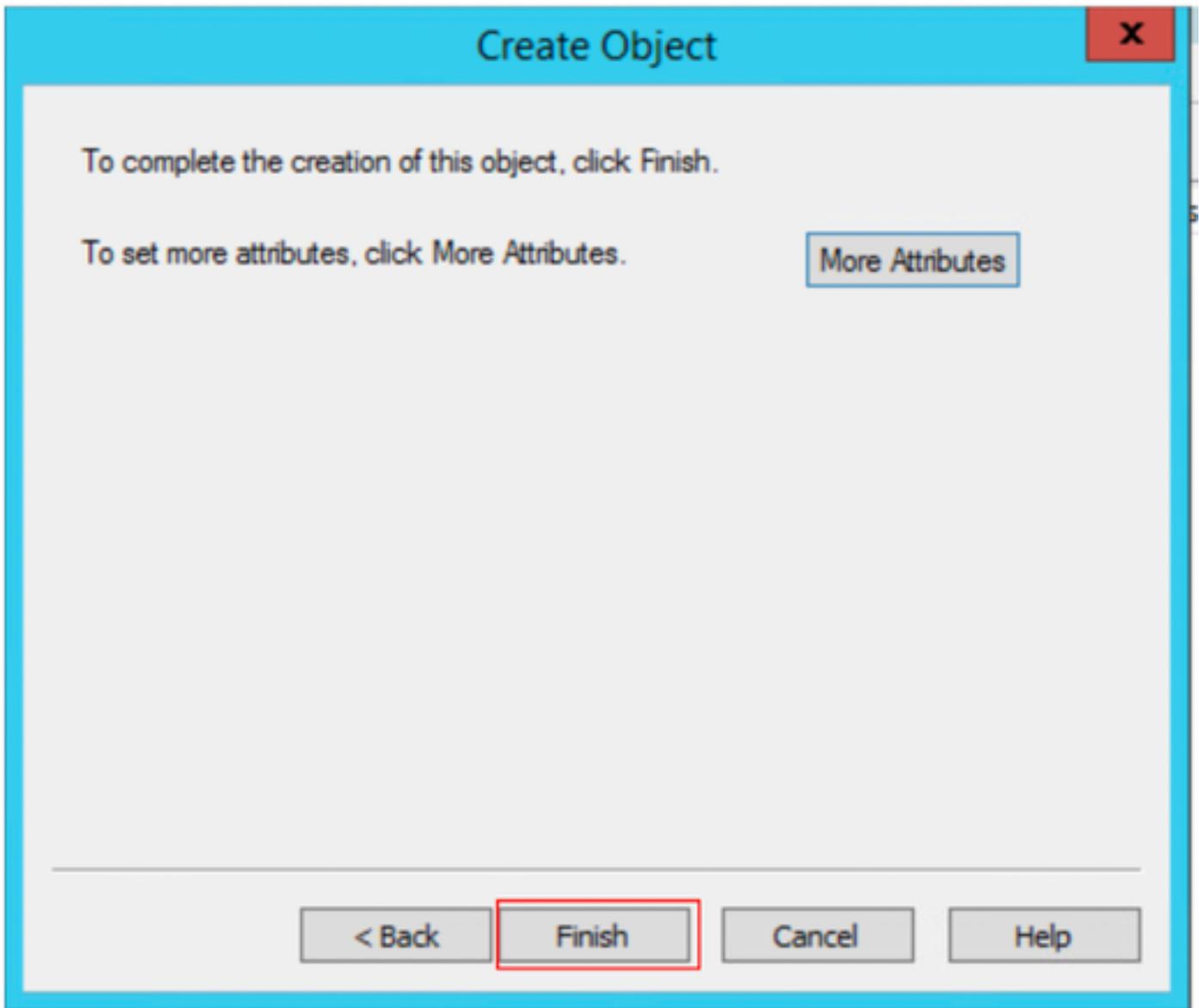
Value(s): 6C:B2:AE:3A:68:6C

Add Remove

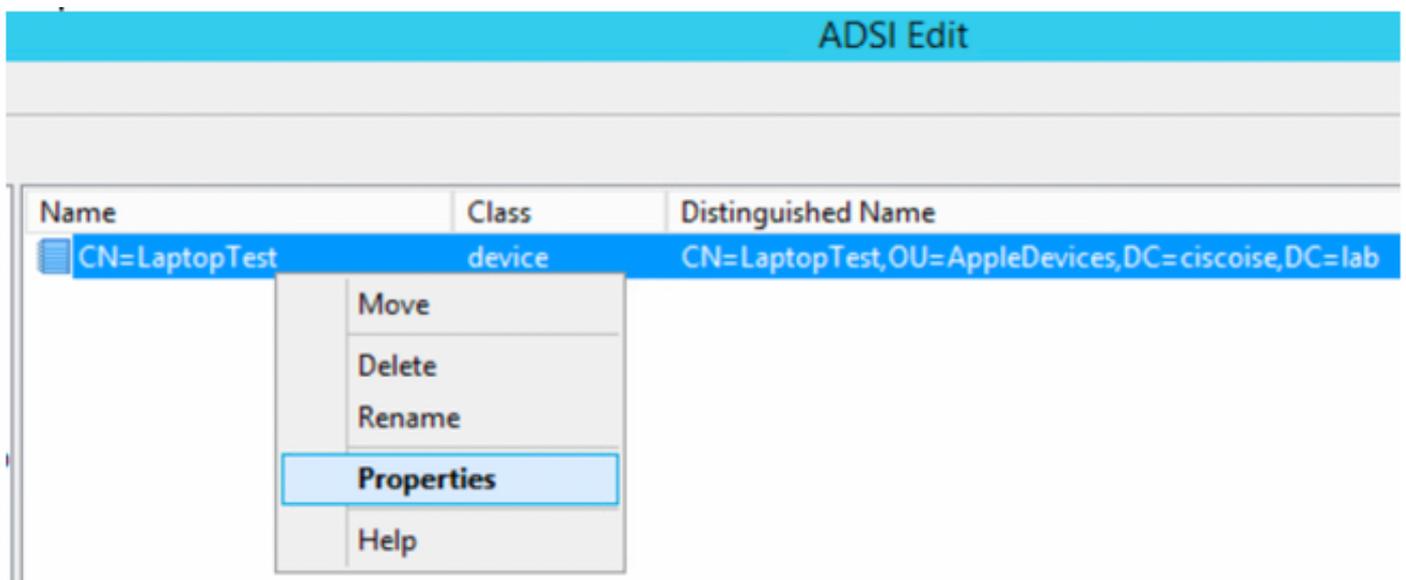
OK Cancel

12. Wählen Sie **OK**, um die Informationen zu speichern und mit der Geräteobjektconfiguration fortzufahren.

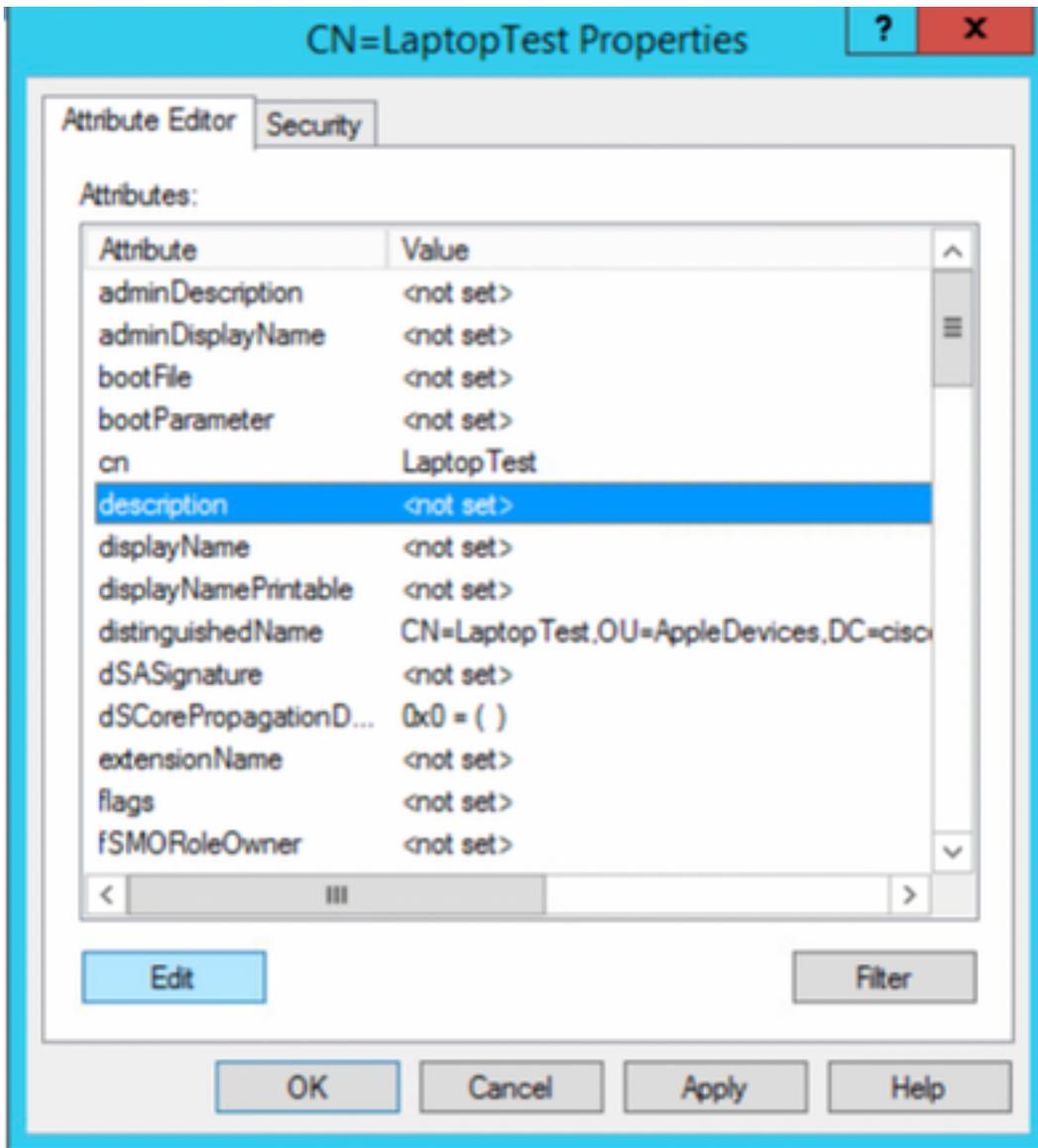
13. Wählen Sie **Fertig stellen**, um das neue Geräteobjekt zu erstellen.



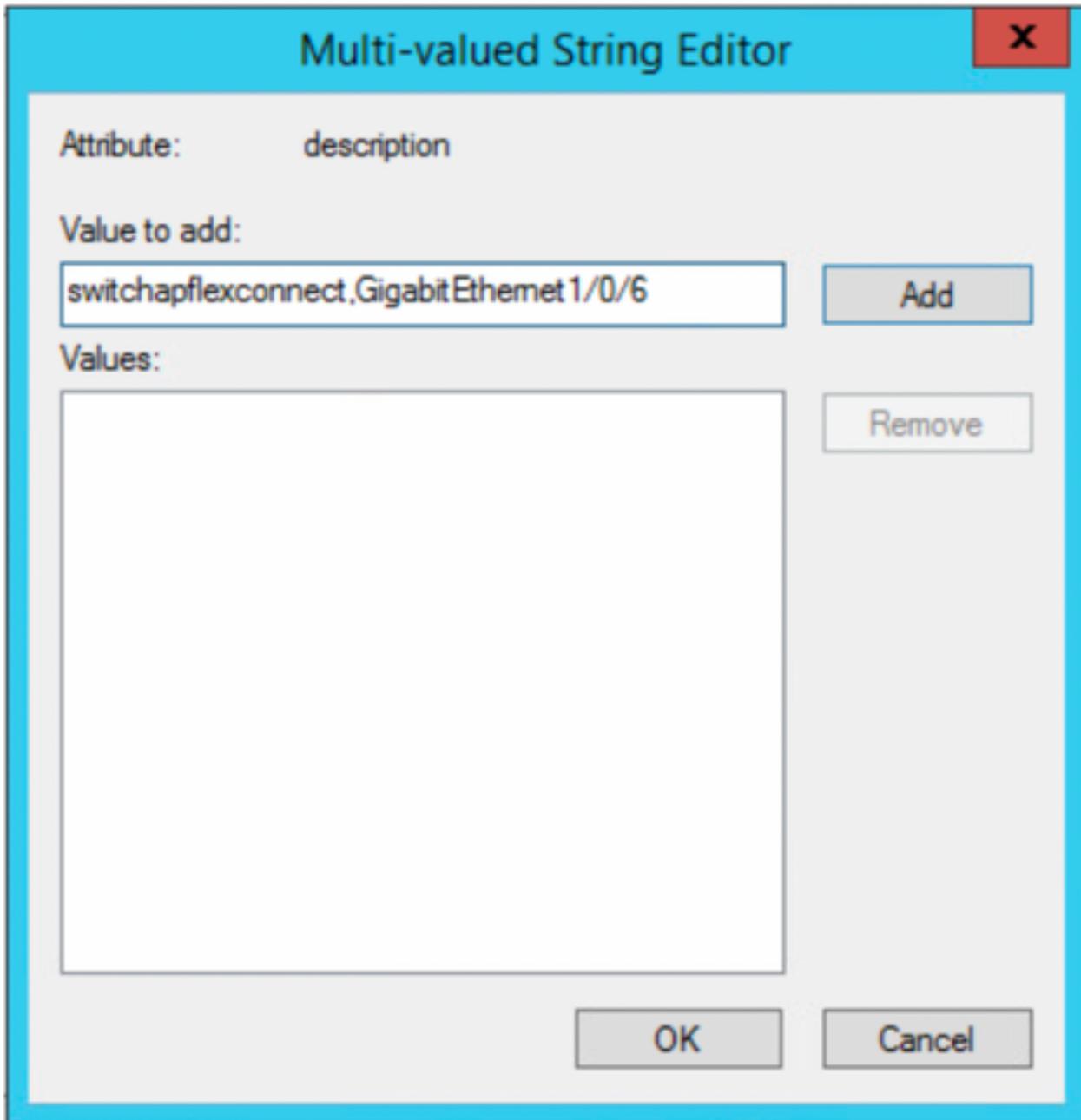
14. Klicken Sie mit der rechten Maustaste auf das Geräteobjekt, und wählen Sie **Eigenschaften** aus.



15. Wählen Sie die **Beschreibung der** Option aus, und wählen Sie **Bearbeiten** aus, um den Switch-Namen und den Switch-Port festzulegen, an den das Gerät angeschlossen werden soll.



16. Definieren Sie den Switch-Namen und den Switch-Port. Trennen Sie jeden Wert durch ein Komma. Wählen Sie **Hinzufügen** und dann **OK**, um die Informationen zu speichern.



- Switchapflexconnect ist der Switch-Name.
- GigabitEthernet1/0/6 ist der Switch-Port, an den das Endgerät angeschlossen ist.

**Hinweis:** Sie können Skripts verwenden, um einem bestimmten Feld Attribute hinzuzufügen. In diesem Beispiel definieren wir die Werte jedoch manuell

**Hinweis:** Beim AD-Attribut wird die Groß-/Kleinschreibung beachtet, wenn bei der LDAP-Abfrage alle MAC-Adressen in Kleinbuchstaben von ISE in Großbuchstaben konvertiert werden. Um dieses Verhalten zu vermeiden, deaktivieren Sie die Process Host Lookup-Suche unter zulässigen Protokollen. Einzelheiten hierzu finden Sie unter: [https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin\\_guide/b\\_ISE\\_admin\\_3\\_0.pdf](https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf)

## Switch-Konfiguration

Im Folgenden wird die Konfiguration für die 802.1x-Kommunikation zwischen der ISE und dem Switch beschrieben.

```
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 !

```

**Hinweis: Möglicherweise müssen die globale Konfiguration und die Schnittstellenkonfiguration in Ihrer Umgebung angepasst werden.**

## ISE-Konfiguration

Im Folgenden wird die Konfiguration der ISE beschrieben, um die Attribute vom LDAP-Server abzurufen und die ISE-Richtlinien zu konfigurieren.

1. Gehen Sie auf der ISE zu **Administration->Identity Management->External Identity Sources**, wählen Sie den **LDAP**-Ordner aus, und klicken Sie auf **Hinzufügen**, um eine neue Verbindung mit LDAP zu erstellen.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation pane on the left is expanded to 'External Identity Sources', with 'LDAP' selected. The main content area displays 'LDAP Identity Sources' with buttons for 'Edit', 'Add', 'Duplicate', and 'Delete'. The 'Add' button is highlighted with a red box. Below these buttons is a table with columns for 'Name' and 'Description'.

2. Definieren Sie auf der Registerkarte **Allgemein** einen Namen und wählen Sie die MAC-Adresse als Attribut für den Betreffnamen aus.

## LDAP Identity Source

General Connection Directory Organization Groups Attributes Advanced Settings

\* Name

Description

▼ Schema

\* Subject Objectclass  \* Group Objectclass

\* Subject Name Attribute  \* Group Map Attribute

\* Group Name Attribute  Certificate Attribute

Subject Objects Contain Reference To Groups

Group Objects Contain Reference To Subjects

Subjects In Groups Are Stored In Member Attribute As

User Info Attributes

First Name  Department

Last Name  Organizational Unit

Job Title  Locality

Email  State or Province

Telephone  Country

Street Address

3. Konfigurieren Sie auf der **Registerkarte Verbindung** die IP-Adresse, die Admin-DN und das Kennwort des LDAP-Servers, um eine erfolgreiche Verbindung herzustellen.

## LDAP Identity Source

General Connection Directory Organization Groups Attributes Advanced Settings

Primary Server Secondary Server

Enable Secondary Server

\* Hostname/IP  (i) Hostname/IP

\* Port  Port

Specify server for each ISE node

Access  Anonymous Access  Authenticated Access

Admin DN  Admin DN

Password  Password

Secure Authentication  Enable Secure Authentication  Enable Server Identity Check

LDAP Server Root CA  (i) LDAP Server Root CA  (i)

Issuer CA of ISE Certificates  (i) Issuer CA of ISE Certificates  (i)

Save Reset

**Hinweis:** Der verwendete Standard-Port ist Port 389.

4. Wählen Sie auf der Registerkarte **Attribute** die MACAddress-Attribute und die Beschreibungsattribute aus. Diese Attribute werden in der Autorisierungsrichtlinie verwendet.

LDAP Identity Source

General Connection Directory Organization Groups **Attributes** Advanced Settings

Edit + Add - Delete Attribute

<input type="checkbox"/>	Name	Type	Default	Internal Name
<input type="checkbox"/>	description	STRING		description
<input type="checkbox"/>	distinguishedName	STRING		distinguishedName
<input type="checkbox"/>	macAddress	STRING		macAddress

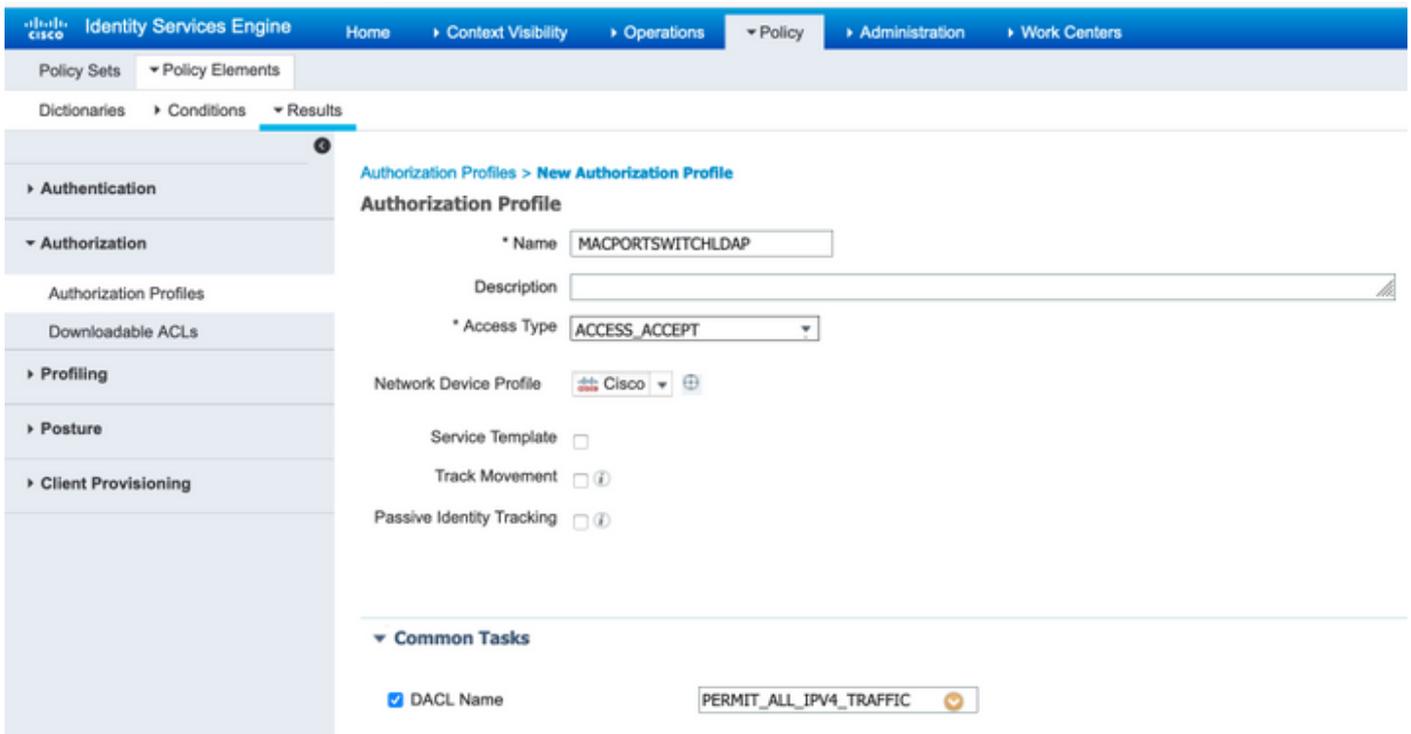
5. Um ein erlaubtes Protokoll zu erstellen, gehen Sie zu **Richtlinien->Richtlinienelemente->Ergebnisse->Authentifizierung->Zulässige Protokolle**. Definieren und Auswählen von Process Host Lookup und Zulassen von PAP/ASCII als einzigen zulässigen Protokollen Wählen Sie abschließend **Speichern**

The screenshot shows the 'Allowed Protocols Services List > MAB\_MacAddress' configuration page. The 'Name' field is set to 'MAB\_MacAddress'. Under 'Allowed Protocols', the 'Authentication Bypass' section has 'Process Host Lookup' checked. The 'Authentication Protocols' section has 'Allow PAP/ASCII' checked.

6. Um ein Autorisierungsprofil zu erstellen, gehen Sie zu **Richtlinien->Richtlinienelemente->Ergebnisse->Autorisierung->Autorisierungsprofile**. Wählen Sie **Hinzufügen**, und definieren Sie die Berechtigungen, die dem Endpunkt zugewiesen werden.

The screenshot shows the 'Standard Authorization Profiles' configuration page. The 'Add' button is highlighted with a red box. Below the buttons is a table of existing profiles:

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco
<input type="checkbox"/>	Cisco_IP_Phones	Cisco
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco



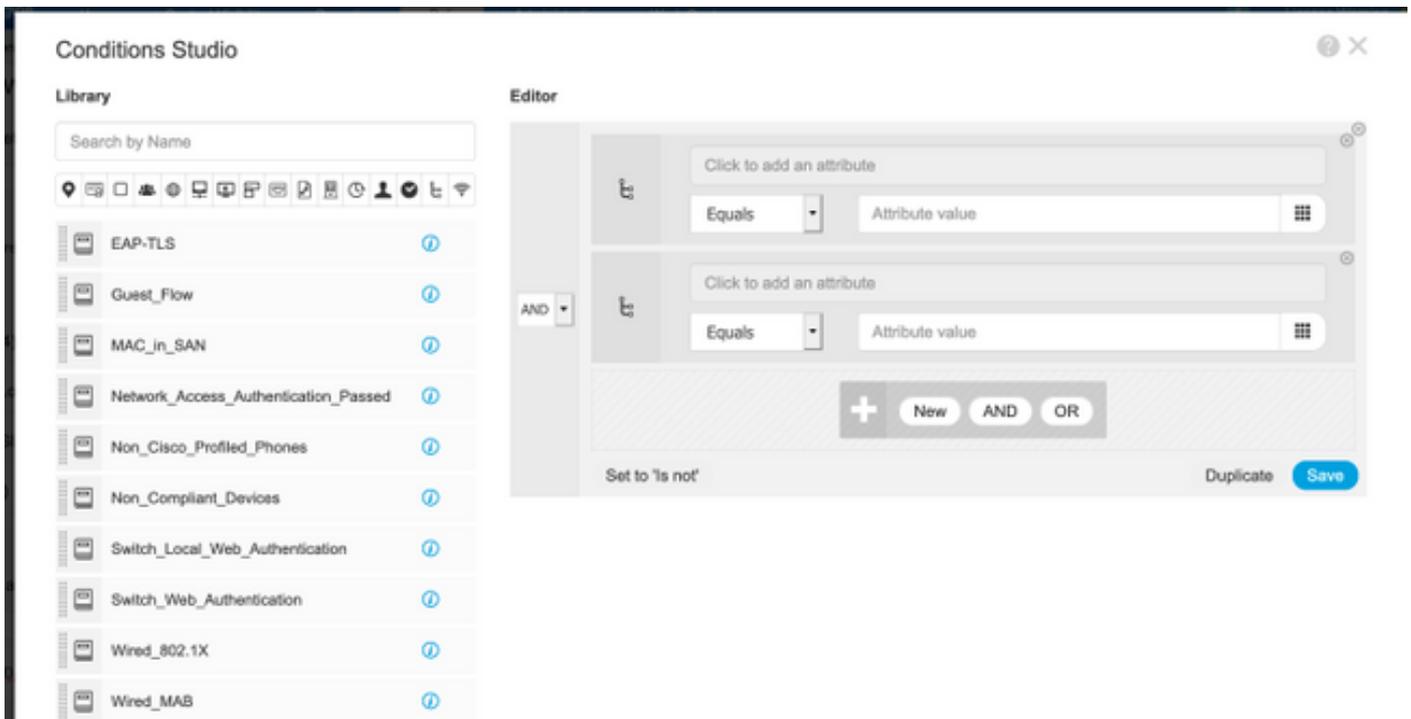
7. Gehen Sie zu Policy-> Policy Set, und erstellen Sie einen Richtlinienatz mit der vordefinierten Bedingung Wired\_MAB und dem in Schritt 5 erstellten Zugelassenen Protokoll.



8. Erstellen Sie unter dem neu erstellten Richtlinienatz eine Authentifizierungsrichtlinie mit der vordefinierten **Wired\_MAB** Library und der **LDAP**-Verbindung als externe Identitätsquellensequenz.



9. Definieren Sie unter **Autorisierungsrichtlinie** einen Namen, und erstellen Sie eine zusammengesetzte Bedingung mithilfe der LDAP-Attributbeschreibung, RADIUS NAS-Port-ID und NetworkDeviceName. Fügen Sie abschließend das in Schritt 6 erstellte Autorisierungsprofil hinzu.



Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	MAB_LDAP	AND kmap_mab-description CONTAINS Radius NAS-Port-Id kmap_mab-description CONTAINS Network Access NetworkDeviceName	MACPORTSWITCHLDAP	Select from list	0	⚙️
✓	Default		DenyAccess	Select from list	0	⚙️

Nachdem Sie die Konfiguration angewendet haben, sollten Sie ohne Benutzereingriff eine Verbindung zum Netzwerk herstellen können.

## Überprüfung

Wenn Sie mit dem designierten Switch-Port verbunden sind, können Sie **show authentication session interface GigabitEthernet X/X/X-Details** eingeben, um den Authentifizierungs- und Autorisierungsstatus des Geräts zu überprüfen.

```
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_Gil/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
```

Auf der ISE können Sie RADIUS Live Logs zur Bestätigung verwenden.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Server	Authorization Profiles
Jan 20, 2020 06:21:47.825 PM	✓		0	employee1@ciscodemo.lab	6C-B2-AE-3A-68-6C	Unknown		ise23-1	MACPORTSWITCHLDAP
Jan 20, 2020 06:21:47.801 PM	✓		0	employee1@ciscodemo.lab	6C-B2-AE-3A-68-6C	Unknown		ise23-1	MACPORTSWITCHLDAP

## Fehlerbehebung

Überprüfen Sie auf dem LDAP-Server, ob das erstellte Gerät über eine MAC-Adresse, einen korrekten Switch-Namen und einen konfigurierten Switch-Port verfügt

# CN=LaptopTest Properties



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	Laptop Test
nisMapName	<not set>
o	<not set>
objectCategory	CN=Device,CN=Schema,CN=Configuration,...

Edit

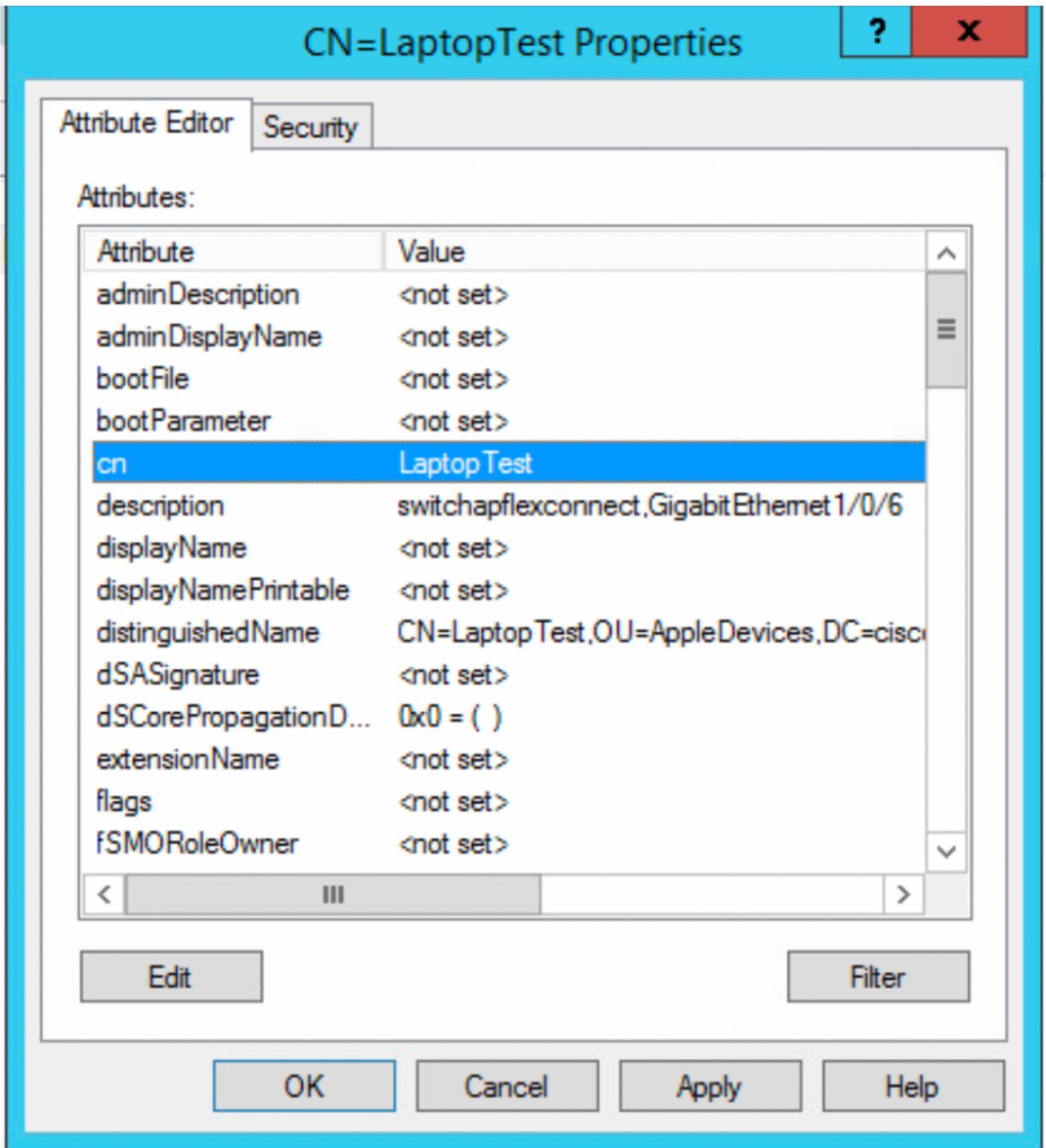
Filter

OK

Cancel

Apply

Help



Auf der ISE können Sie eine Paketerfassung (**Operations->Troubleshoot->Diagnostic Tool->TCP Dumps**) durchführen, um zu überprüfen, ob die Werte von LDAP an die ISE gesendet werden.

