ISEおよびLDAP属性ベースの認証

内容

概要

このドキュメントでは、Cisco Identity Services Engine(ISE)を設定し、Lightweight Directory Access Protocol(LDAP)オブジェクト属性を使用してデバイスを動的に認証および許可する方法について説明します。

注：このドキュメントは、LDAP を ISE 認証および承認のための外部 ID ソースとして使用するセットアップに適用されます。

著者：シスコプロフェッショナルサービスエンジニア、Emmanuel CanoおよびMauricio Ramos

編集：Neri Cruz Cisco TACエンジニア

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISEポリシーセット、認証、および認可ポリシーに関する基礎知識
- Mac認証バイパス(MAB)
- Radiusプロトコルに関する基礎知識
- Windowsサーバに関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE、バージョン2.4パッチ11
- Microsoft Windows Serverバージョン2012 R2 x64
- CiscoスイッチCatalyst 3650-24PD、バージョン03.07.05.E(15.2(3)E5)
- Microsoft Windows 7マシン

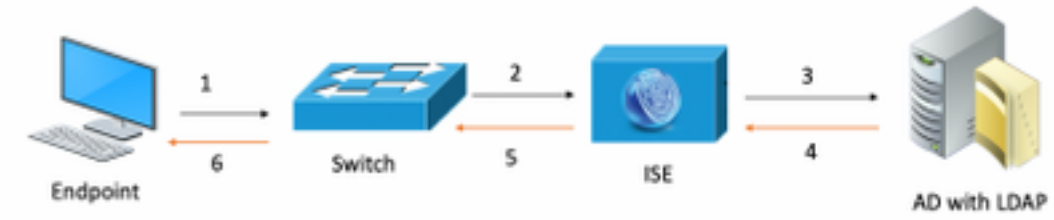
注：このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

コンフィギュレーション

このセクションでは、ネットワークデバイスの設定方法、ISEとLDAPの統合、および最終的にISE認可ポリシーで使用するLDAP属性の設定方法について説明します。

ネットワーク図

次の図に、使用するネットワーク トポロジを示します。



次のネットワーク図にトラフィック フローを示します。

1. ユーザは自分のpc/ラップトップを指定スイッチポートに接続します。
2. スイッチはそのユーザのRADIUS Access-RequestをISEに送信します
3. ISEが情報を受信すると、LDAPサーバに対して特定のユーザフィールドを照会します。これには、認可ポリシー条件で使用される属性が含まれます。
4. ISEが属性 (スイッチポート、スイッチ名、およびデバイスのMACアドレス) を受信すると、スイッチが提供する情報を比較します。
5. スイッチによって提供される属性情報がLDAPによって提供される属性情報と同じ場合、ISEはRADIUS Access-Acceptを、認可プロファイルに設定された権限とともに送信します。

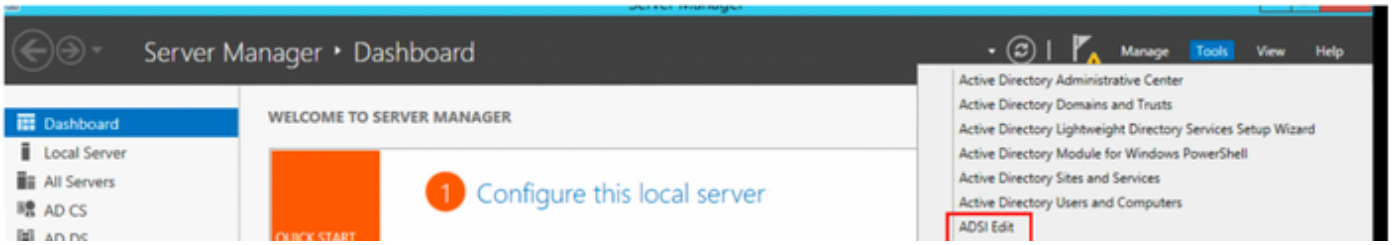
設定

このセクションでは、LDAP、スイッチ、およびISEを設定します。

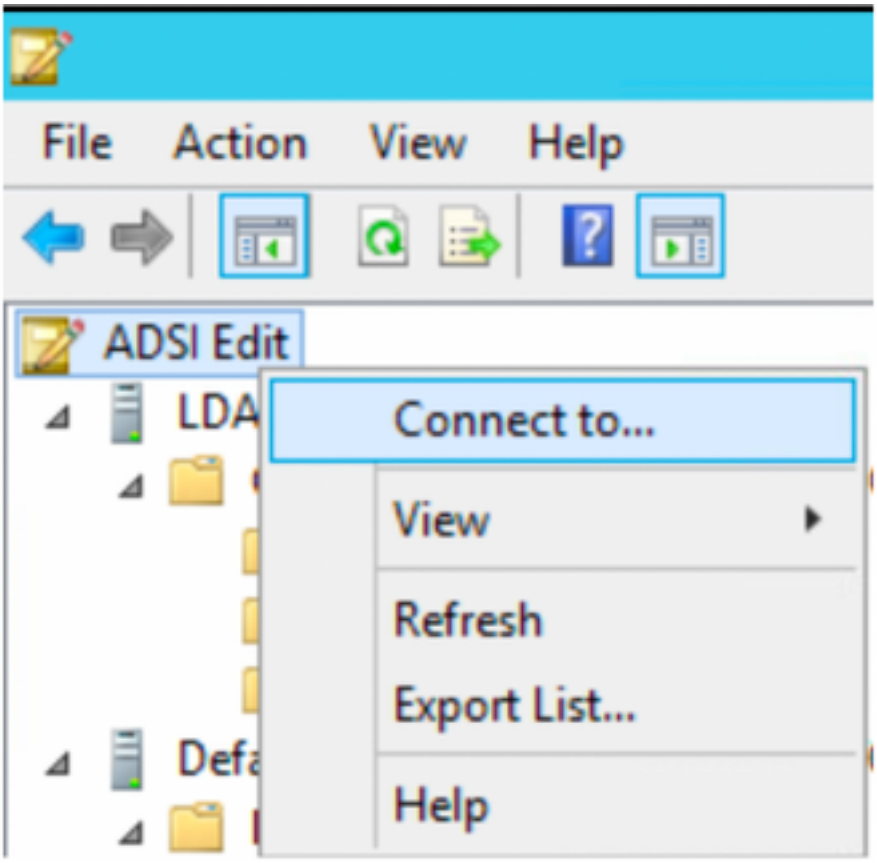
設定 [LDAP]

LDAPサーバを設定するには、次の手順を実行します。

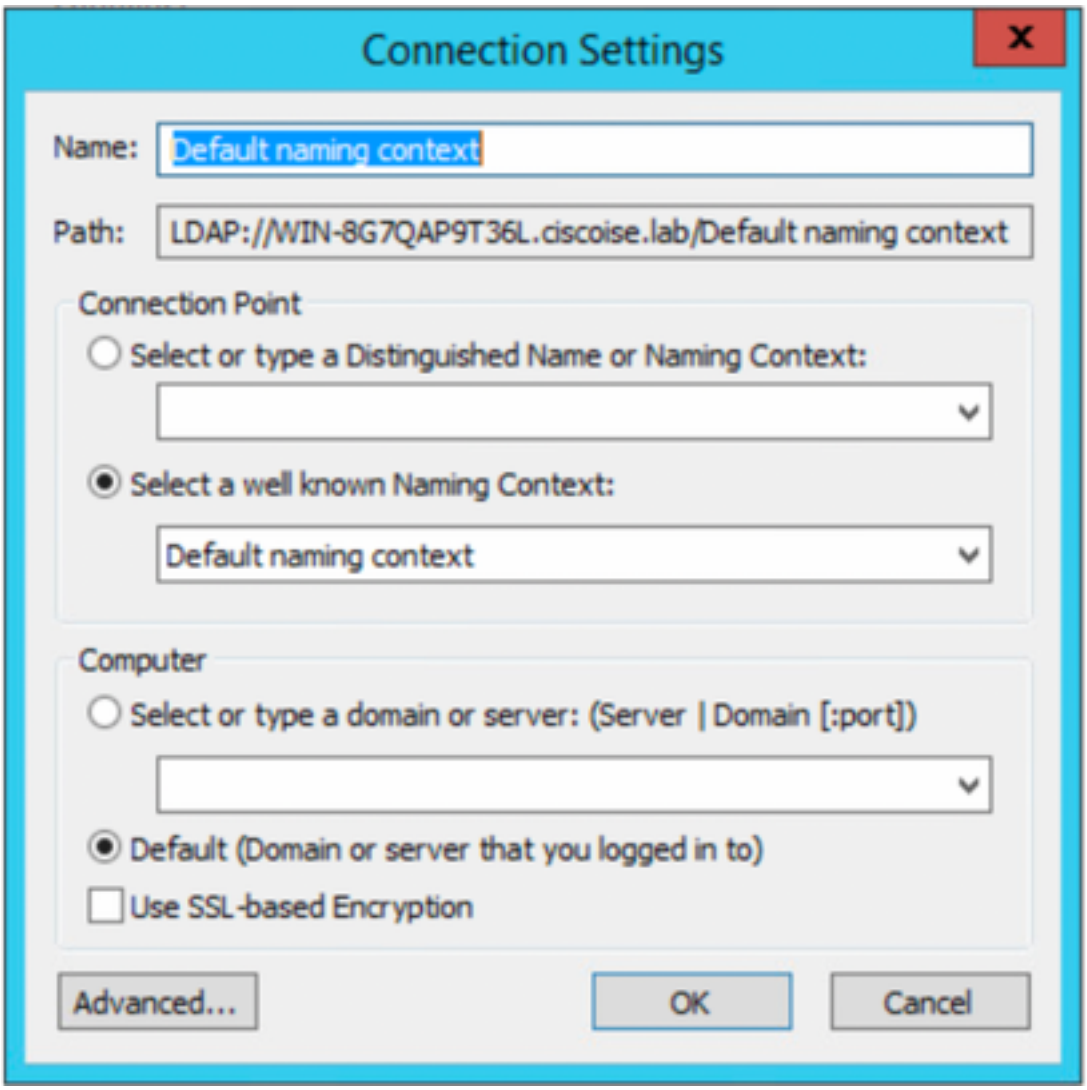
1. 「サーバー・マネージャ」>「ダッシュボード」>「ツール」>「ADSI編集」に移動します。



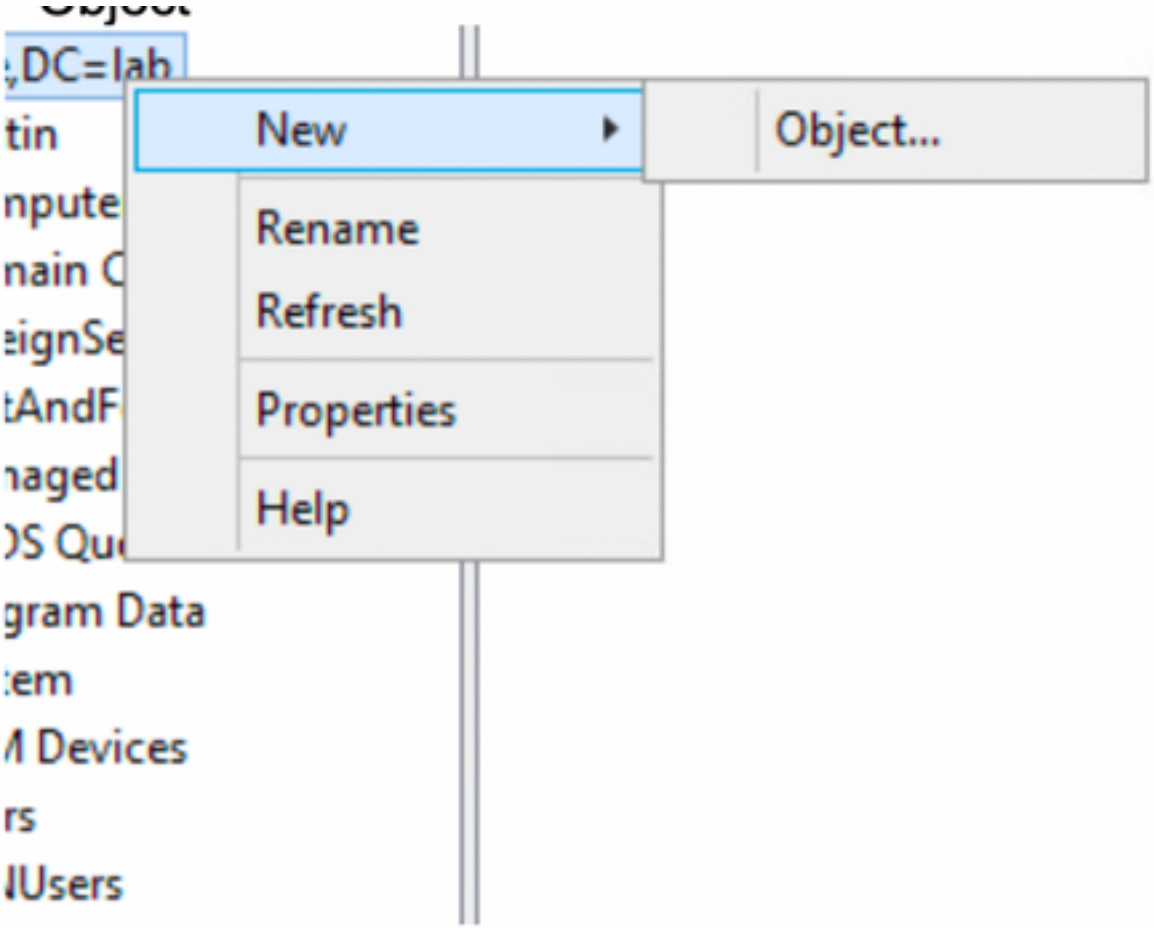
2. ADSI Editアイコンを右クリックし、**Connect to...を選択します。**



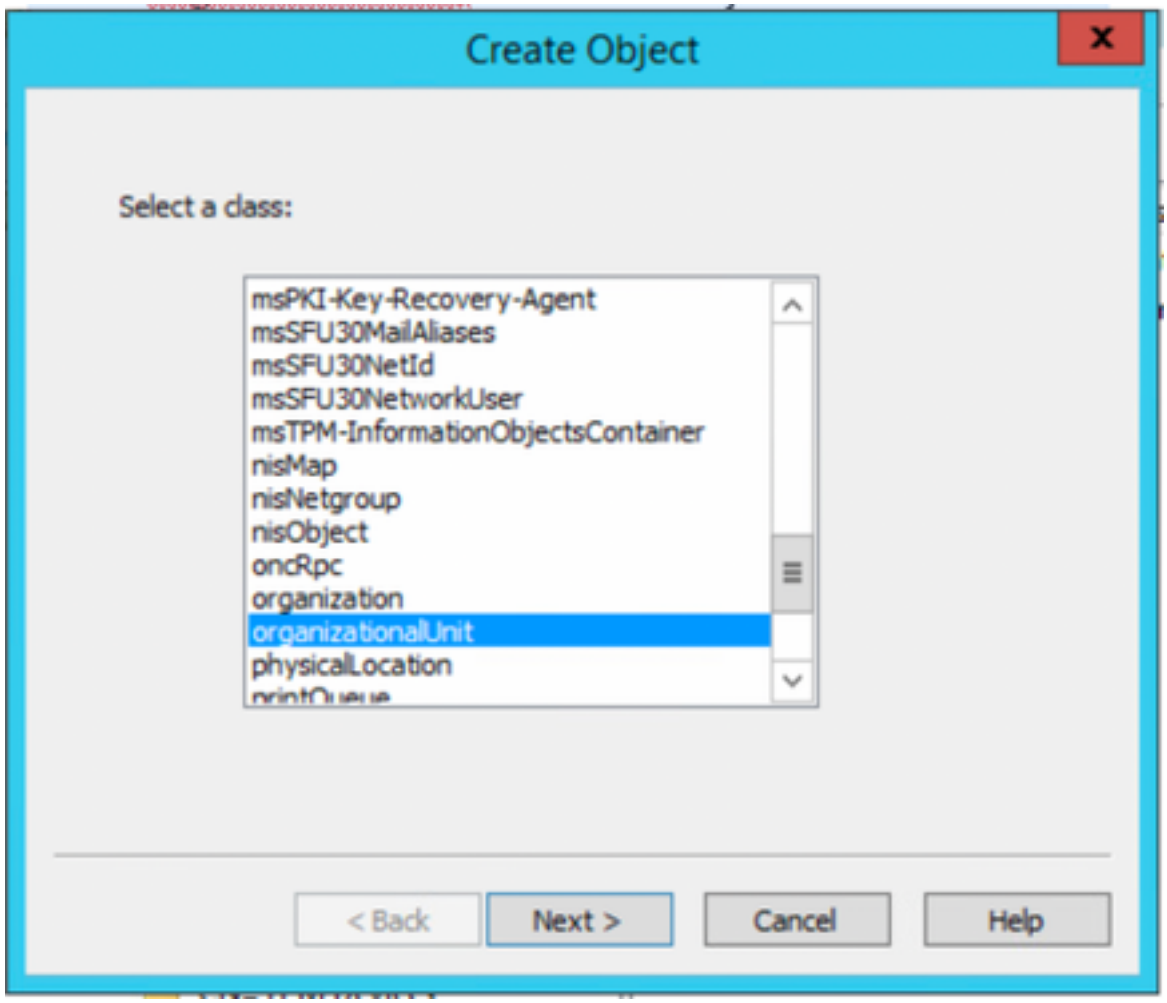
3.接続の設定で名前を定義し、「**OK**」ボタン**を選択**して接続を開始します。



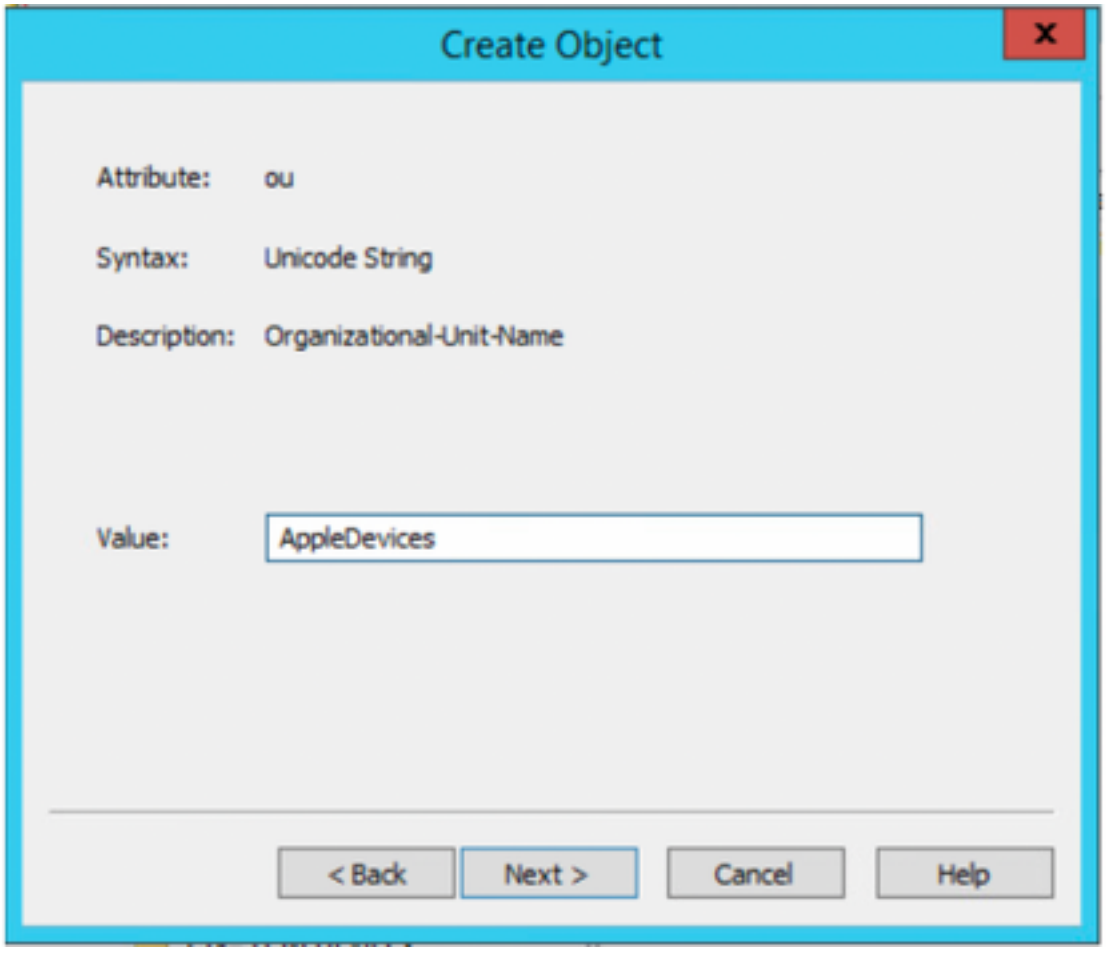
4.同じ[ADSI Edit]メニューでDC接続(DC=ciscodemo、DC=lab)を右クリックし、[**New**]を選択し、オプション[**Object**]を選択します



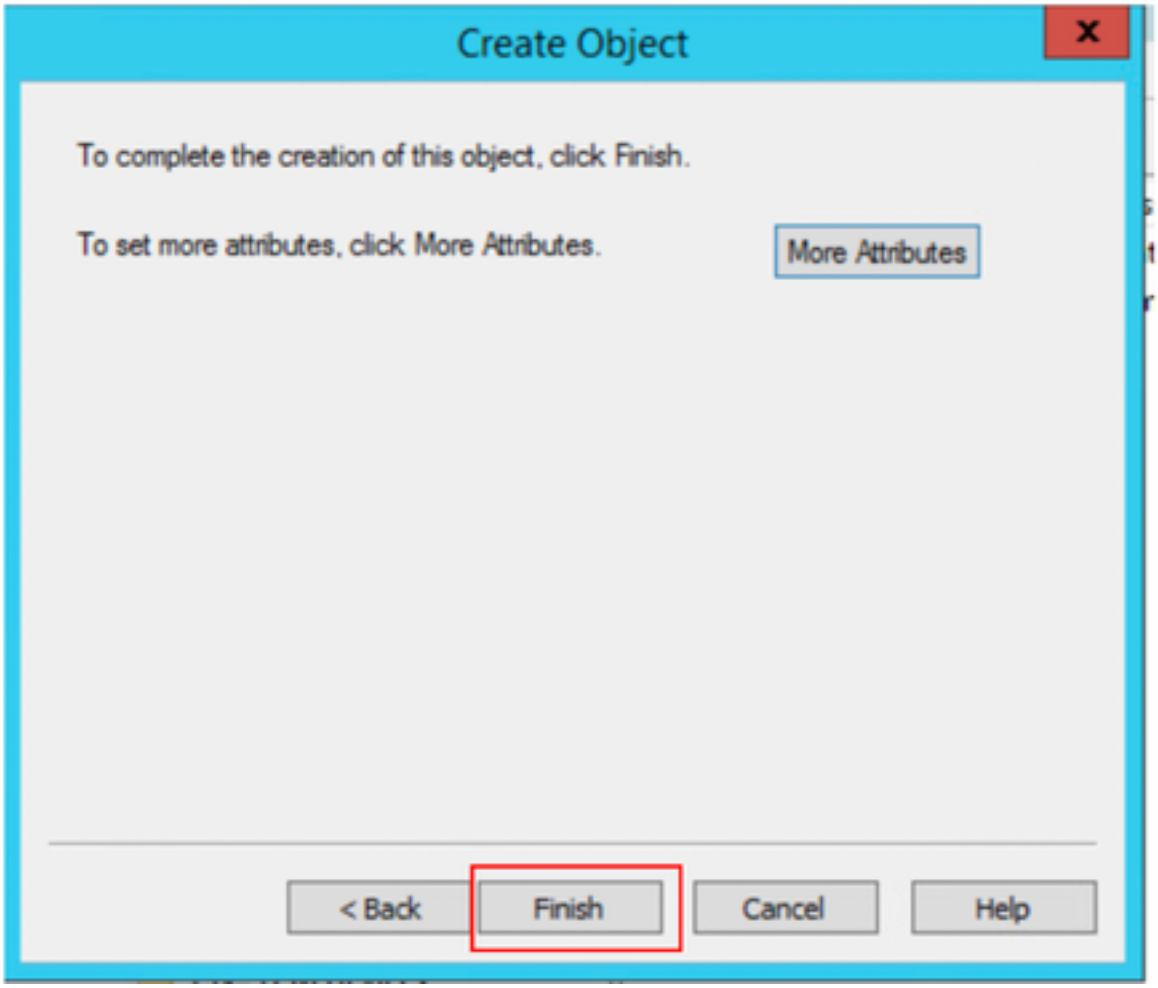
5.新しいオブジェクトとし**て[OrganizationalUnit]**オプションを選択し、[次へ]を選択**します。**



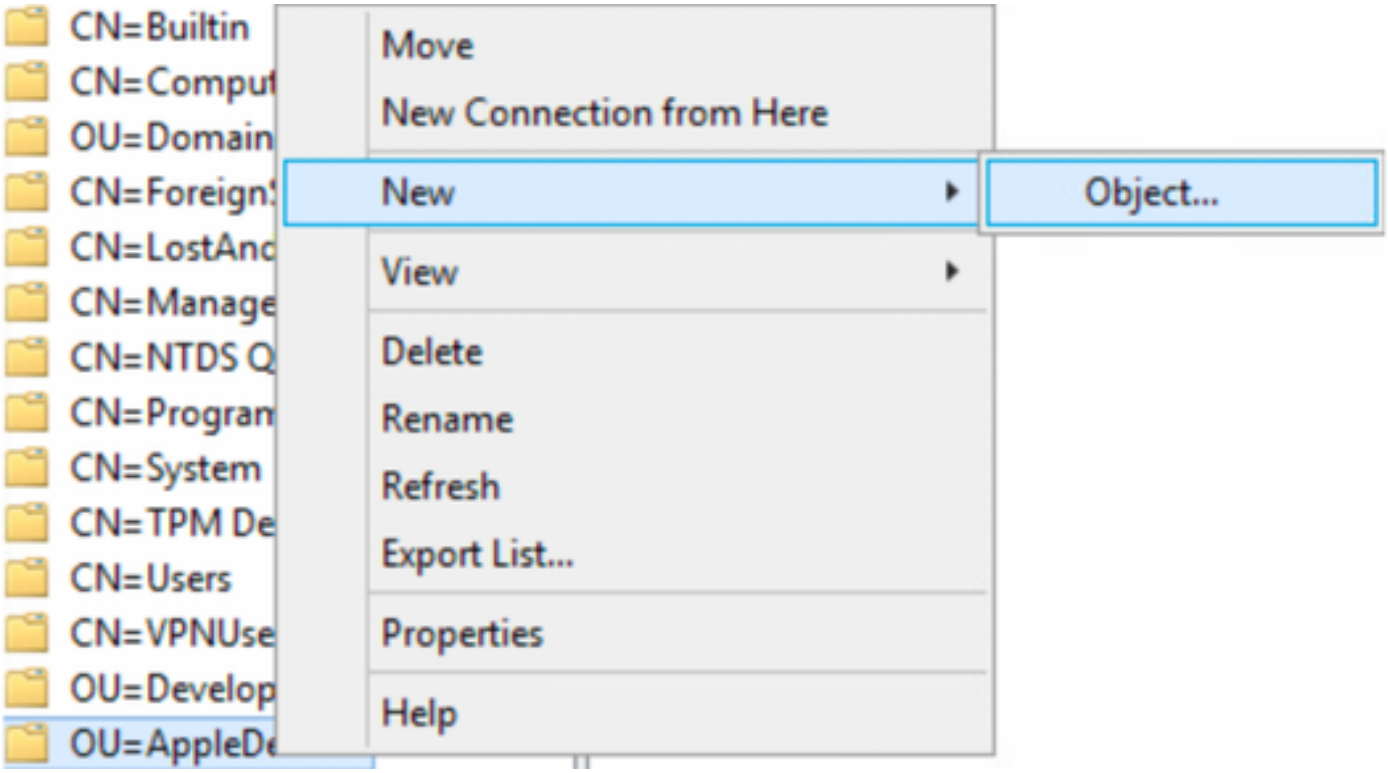
6.新しいOrganizationalUnitの名前を定義し、[**Next**]を選択します



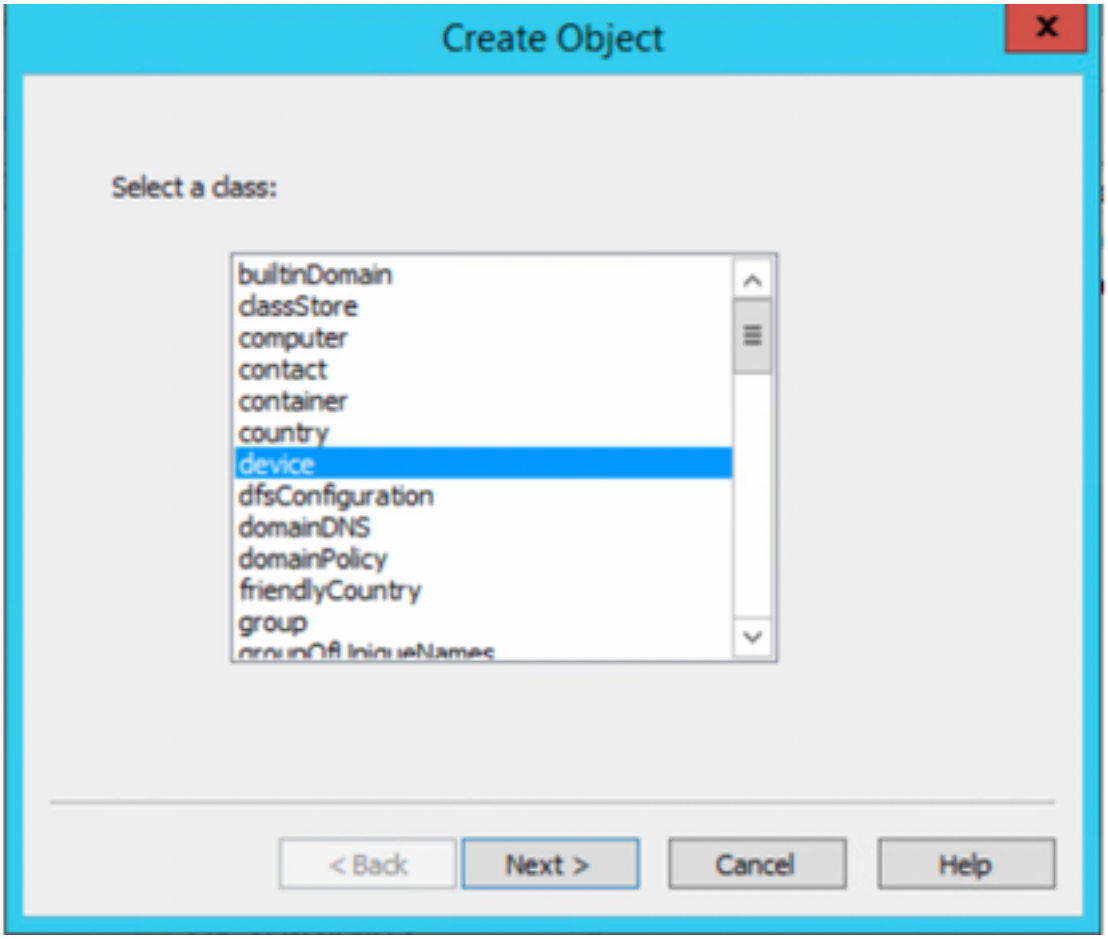
7.新しい組織ユニットを作成するには、[完了]を選択します



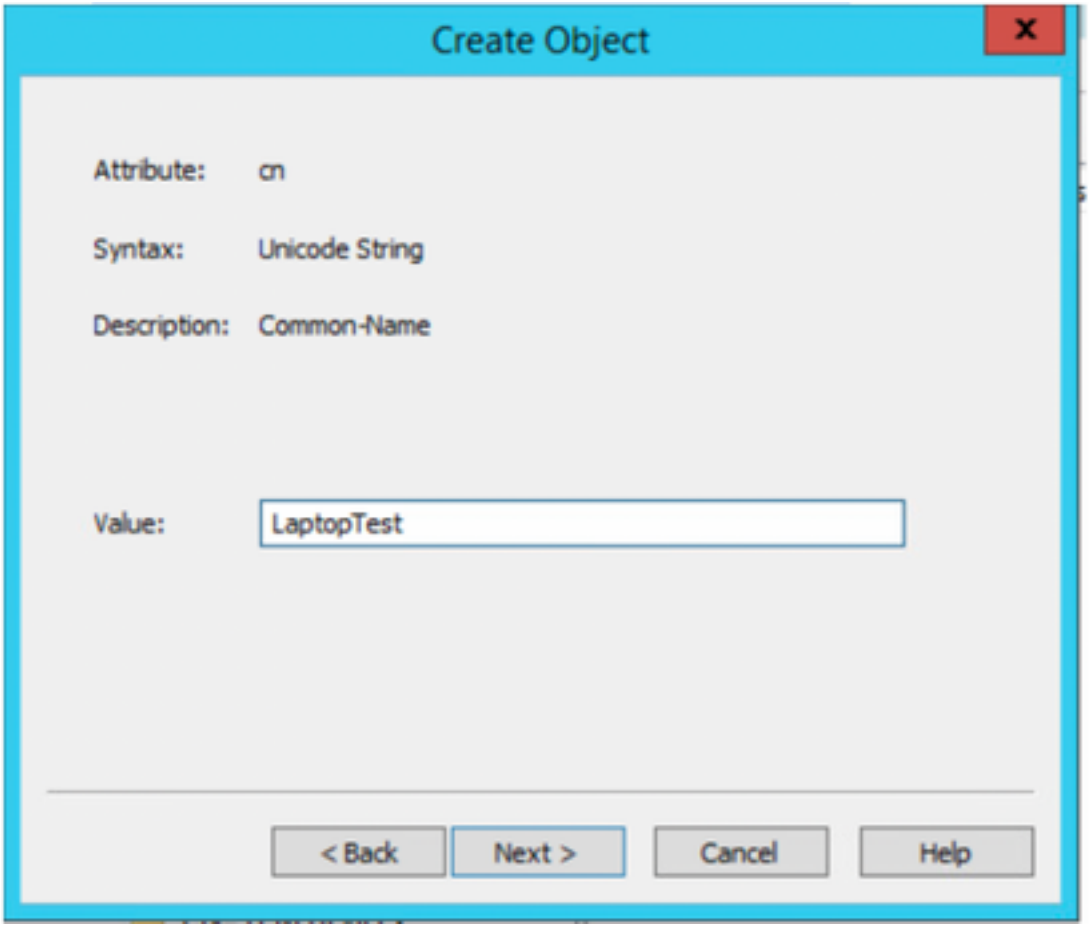
8.作成したOrganizationalUnitを右クリックし、[**New**] > [Object]を選択します



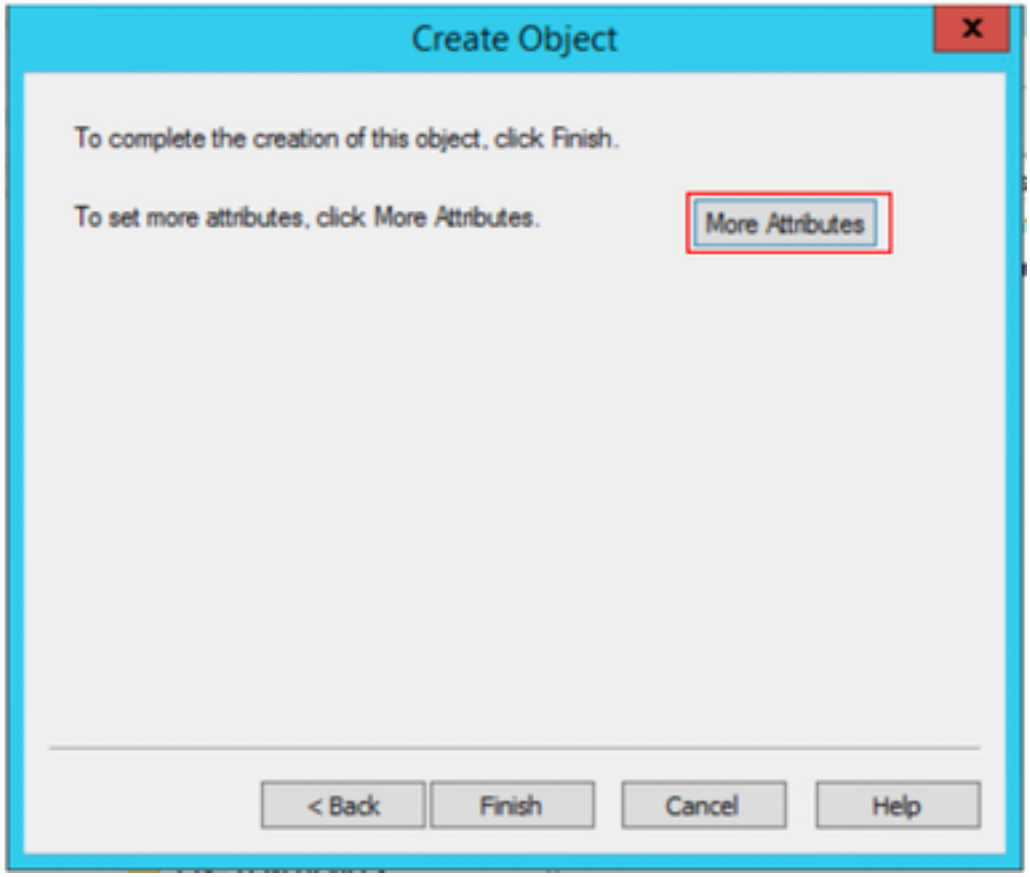
9.オブジェクトクラスとしてデバイスを選択し、 次



10.「値」フィールドで名前を定義し、「次へ」を選択**します**

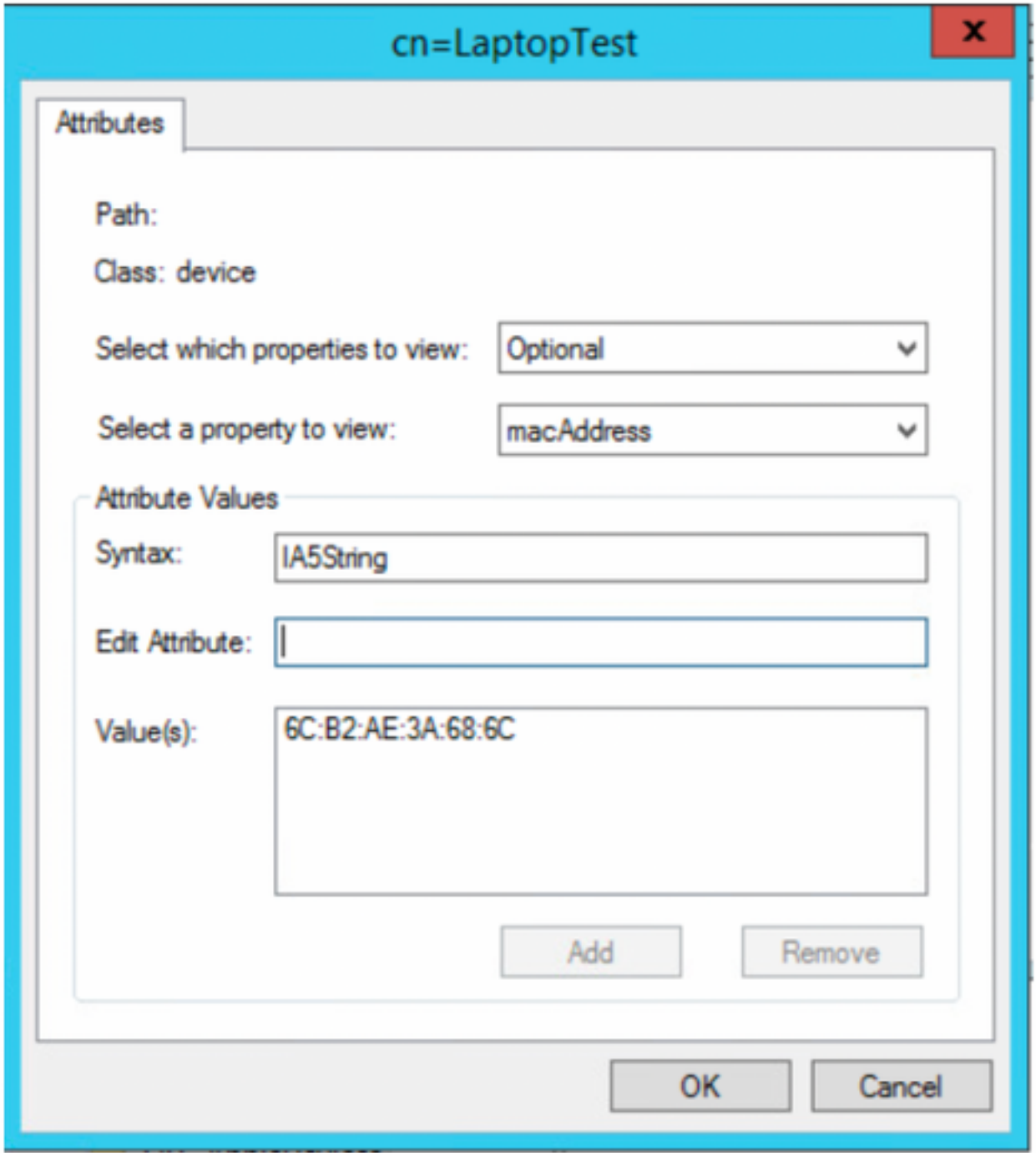


11.「その他の属性」オプションを**選択します**



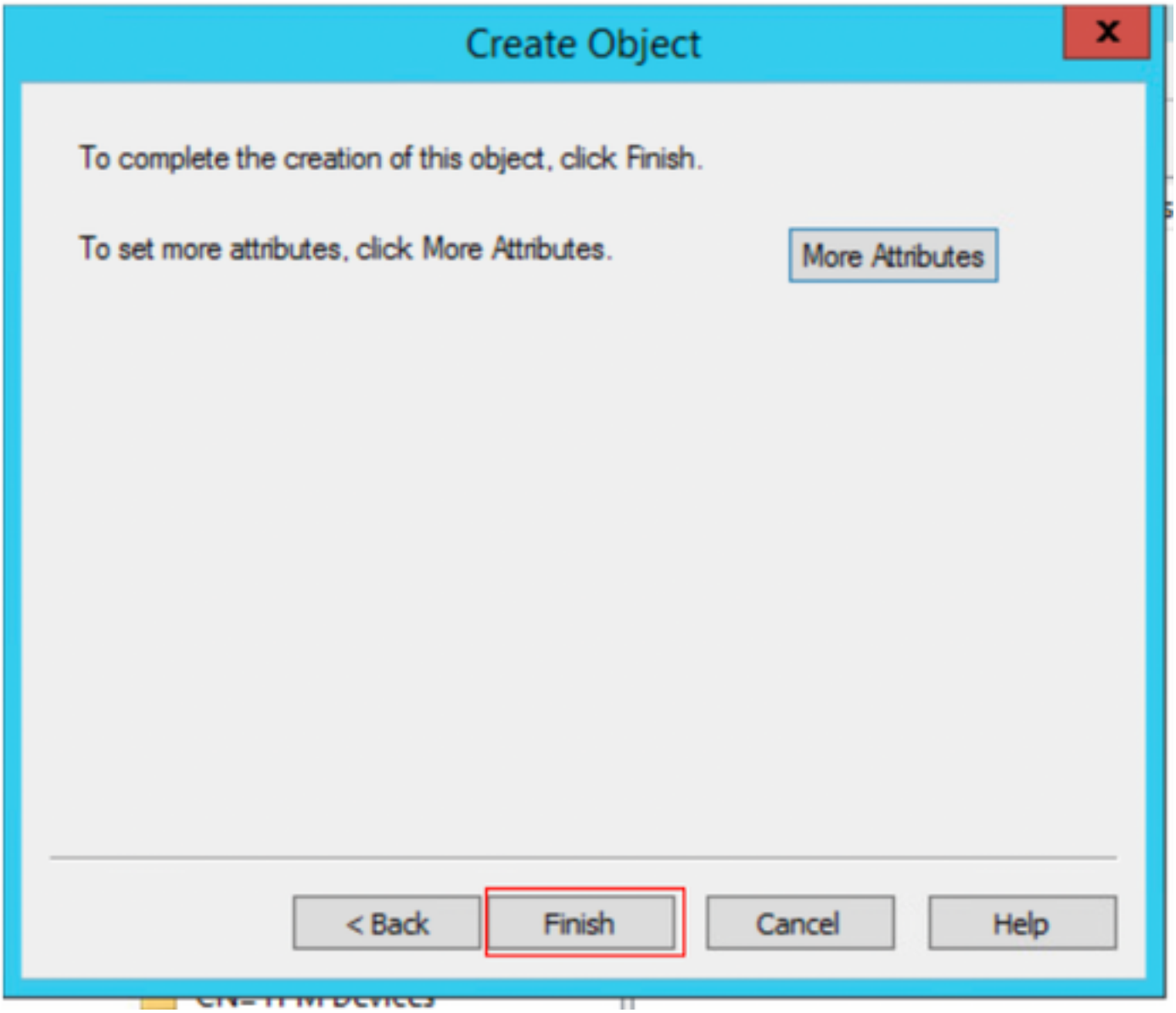
11.ドロップダウンメニューで、表示するプロパティを選択し**て、macAddressオプションを選択**し、次に**Edit属性フィールドで認証されるエンドポイントMacアドレスを定義し**て、 **[Add]**ボタンをクリックして、デバイスのMACアドレスを保存します。

注:MACアドレスオクテット間には、ドットやハイフンの代わりにニ重コロンを使用します。

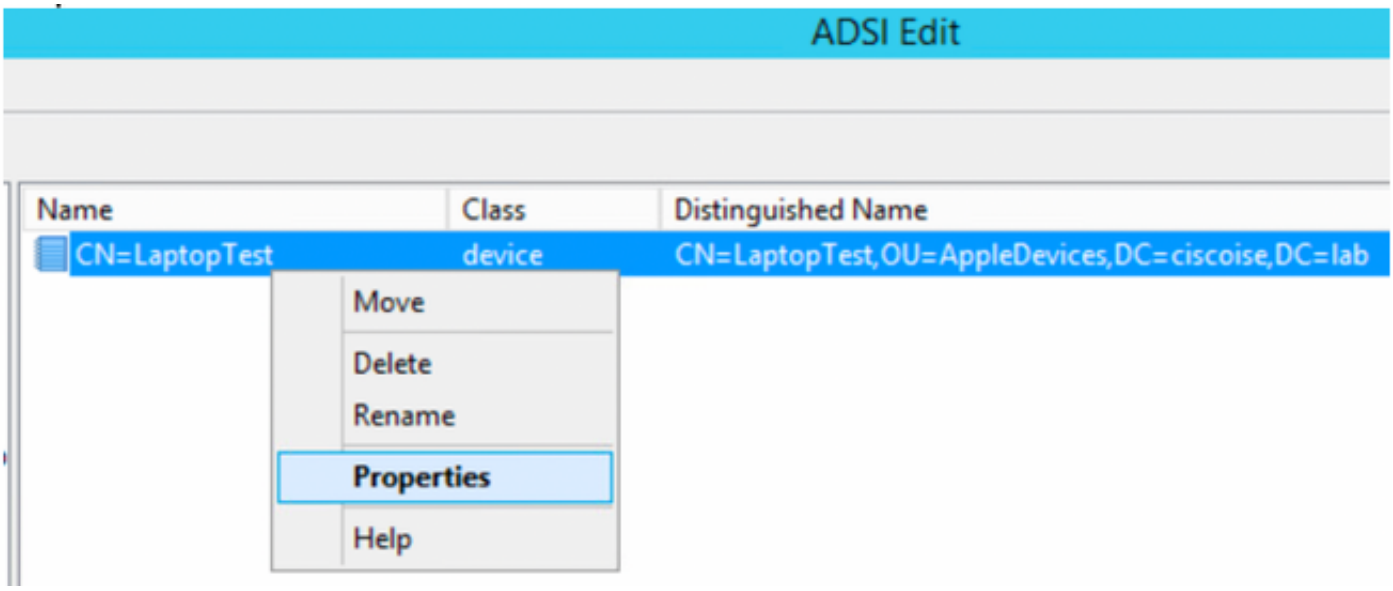


12. [**OK**]を選択して、情報を保存し、デバイスオブジェクトの設定を続行します

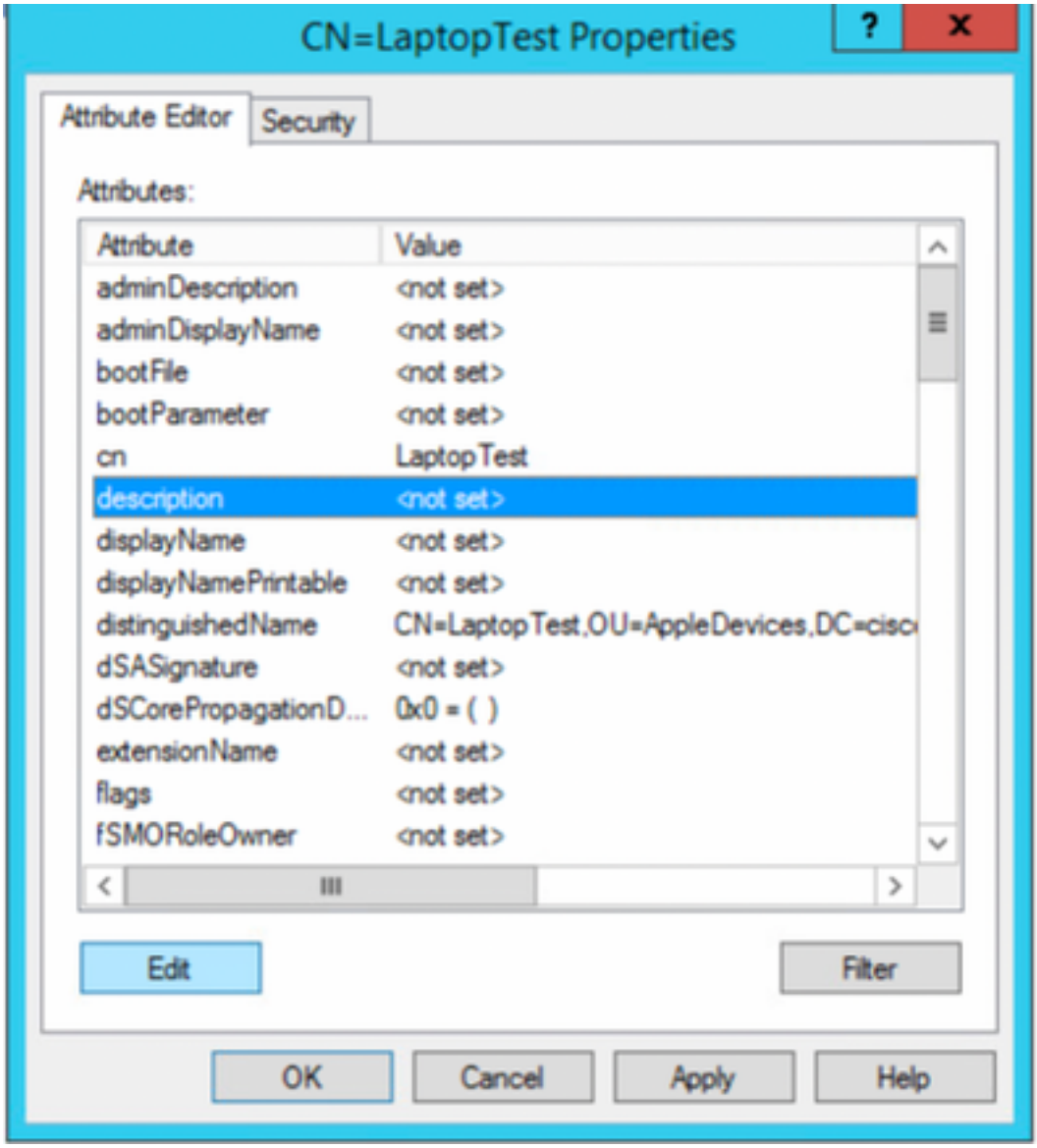
13.新しいデバイスオ**ブジェクト**を作成するには、[Finish]を選択します



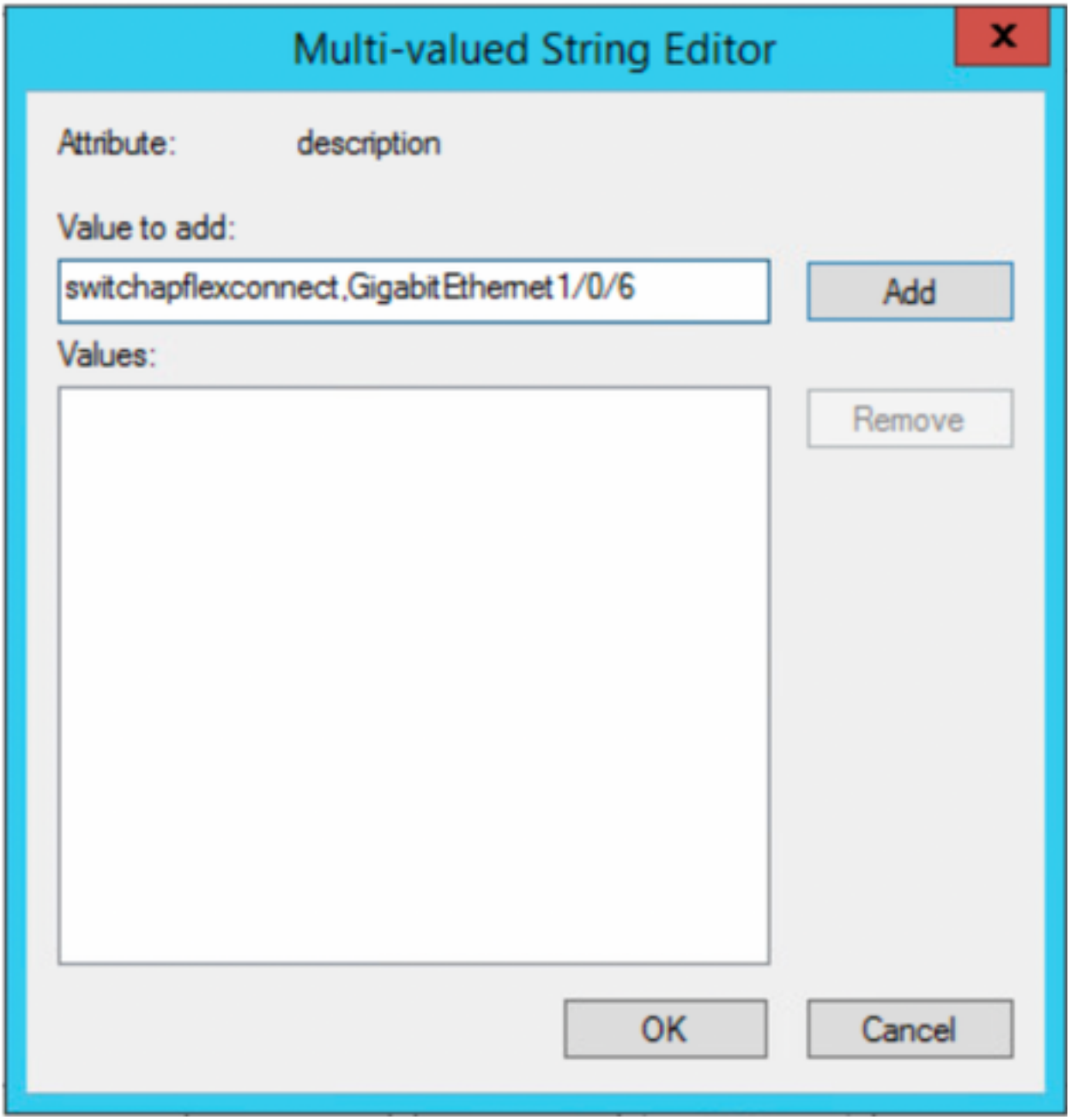
14.デバイスオブジェクトを右クリックし、[プロパティ]オプションを選択します



15.オプションの[description]を選択し、[Edit]を選択して、デバイスが接続されるスイッチ名とスイッチポートを定義します。



16.スイッチ名とスイッチポートを定義します。各値をカンマで区切ってください。[追**加]を**選択し、[**OK**]を選択して情報を保存します。



- **Switchflexconnectはスイッチ名です。**
- **GigabitEthernet1/0/6は、エンドポイントが接続されているスイッチポートです。**

注：スクリプトを使用して特定のフィールドに属性を追加することもできますが、この例では、値を手動で定義します

注：AD属性では大文字と小文字が区別されます。小文字のISEですべてのMacアドレスを使用すると、LDAPクエリ中に大文字に変換されます。この動作を回避するには、許可されたプロトコルでProcess Host Lookupを無効にします。詳細については、次のリンクを参照してください。
https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

スイッチの設定

ISE802.1x

```
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
```

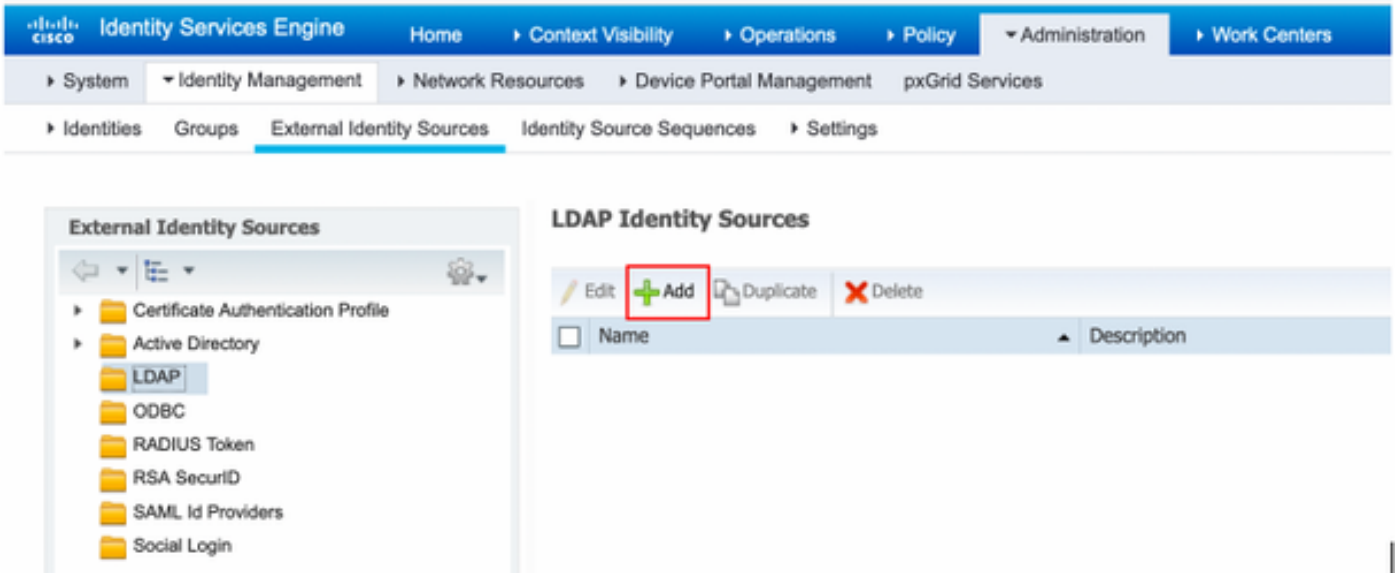
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access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

注：グローバルおよびインターフェイスの設定は、環境で調整する必要がある場合があります

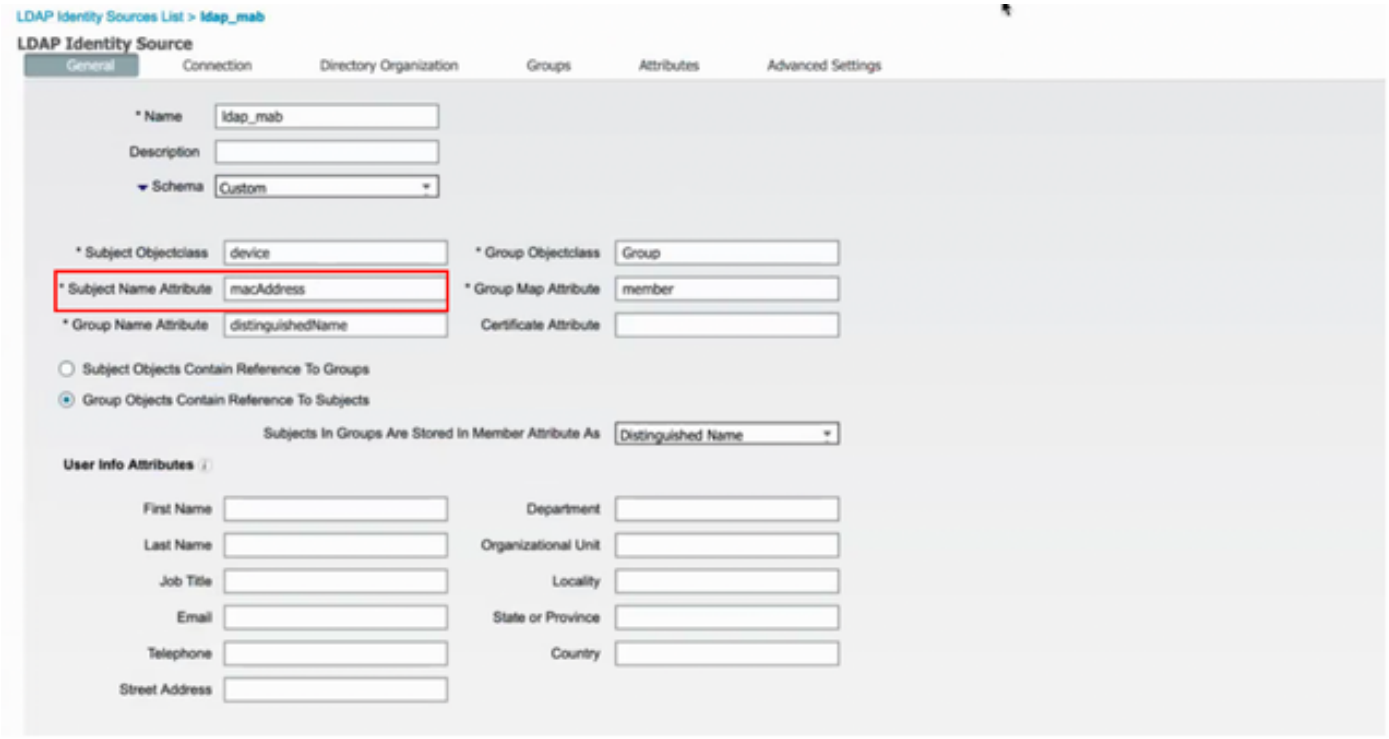
ISE の設定

次に、LDAPサーバから属性を取得し、ISEポリシーを設定するためのISEの設定について説明します。

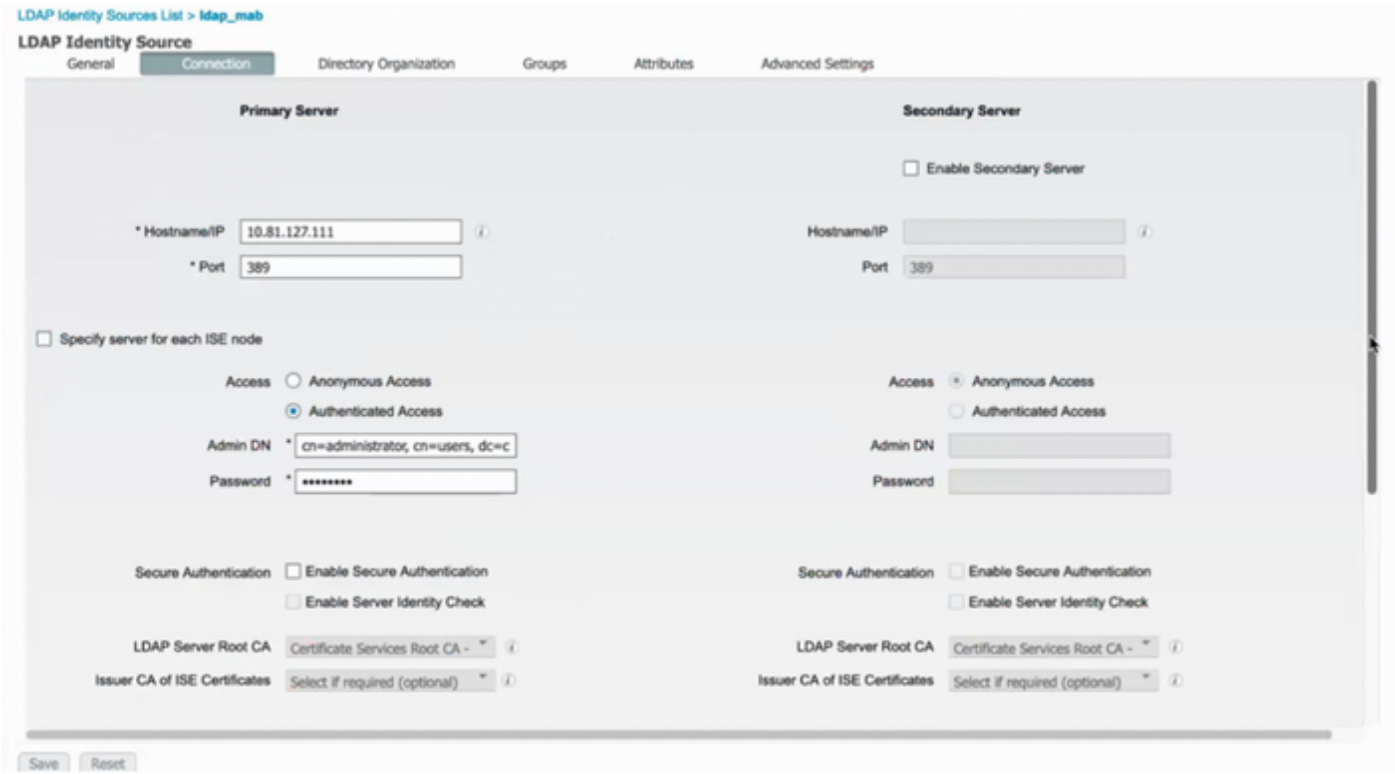
1. ISEで、**[Administration] > [Identity Management] > [External Identity Sources]に移動し、[LDAP]**フォルダを選択し、**[Add]**をクリックしてLDAPとの新しい接続を作成します



2. [General] タブで名前を定義し、サブジェクト名属性としてMACアドレスを選択します

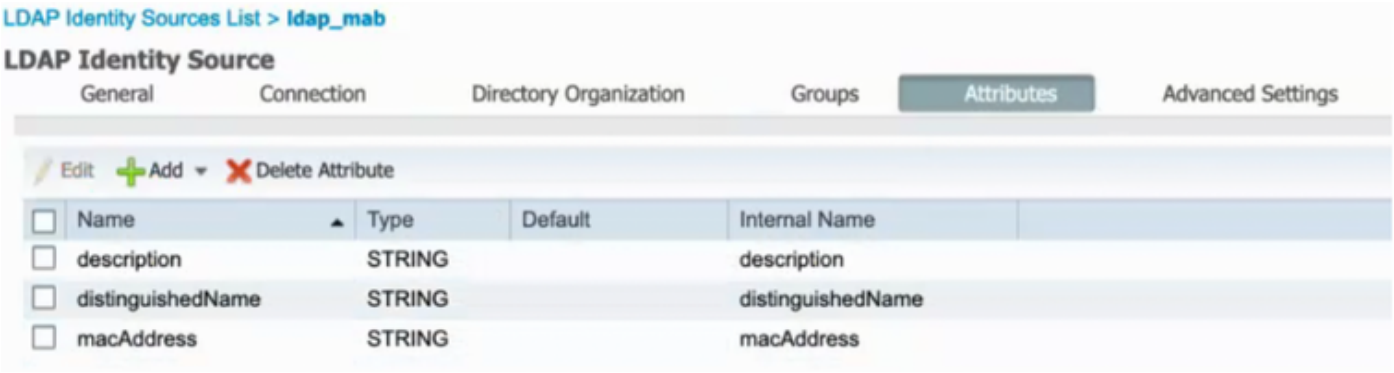


3. [Connection] タブで、LDAPサーバからのIPアドレス、管理DN、およびパスワードを設定し、正常な接続を確立します。

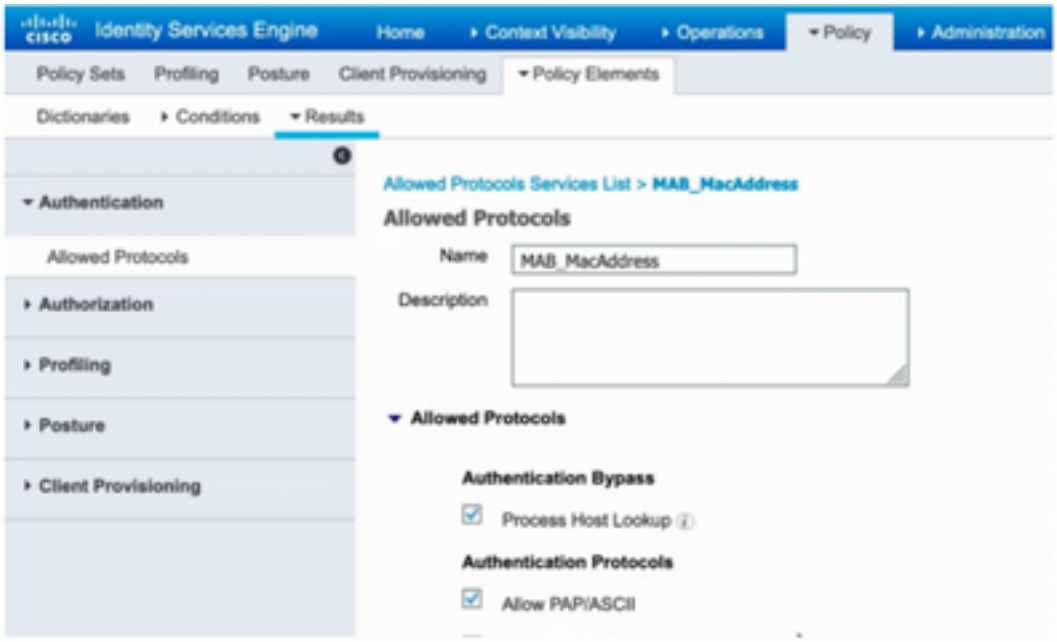


注：ポート389はデフォルトで使用されるポートです。

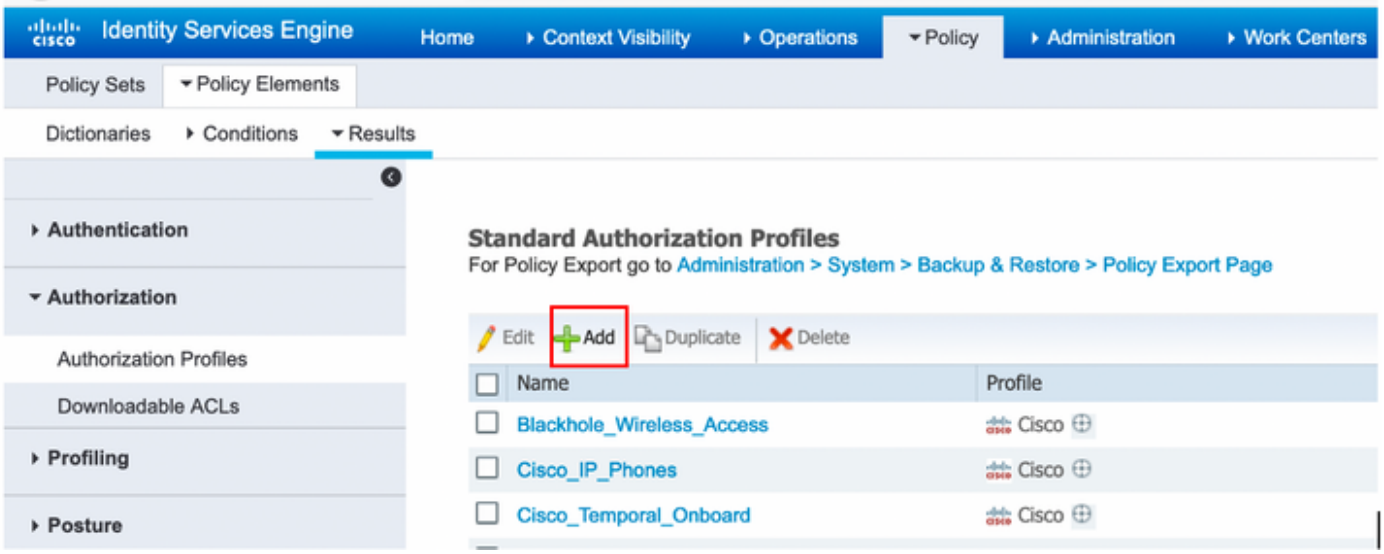
4. [Attributes] タブでmacAddress属性とdescription属性を選択すると、これらの属性が認可ポリシーで使用されます

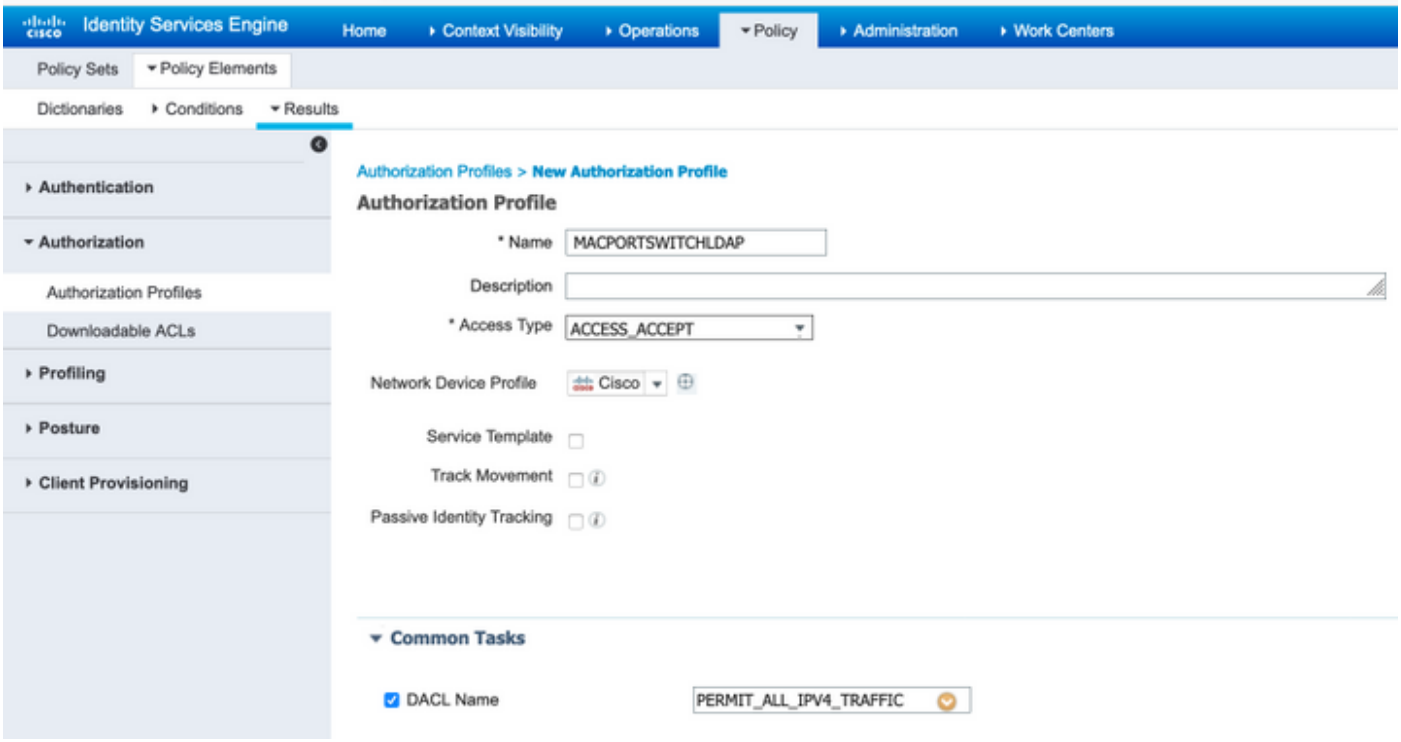


5.許可されたプロトコルを作成するには、**[Policy] -> [Policy Elements] -> [Results] -> [Authentication] -> [Allowed Protocols]に移動します。**許可される唯一のプロトコルとして、[Process Host Lookup]と[Allow PAP/ASCII]を定義して選択します。最後に[保存]を選択**します**

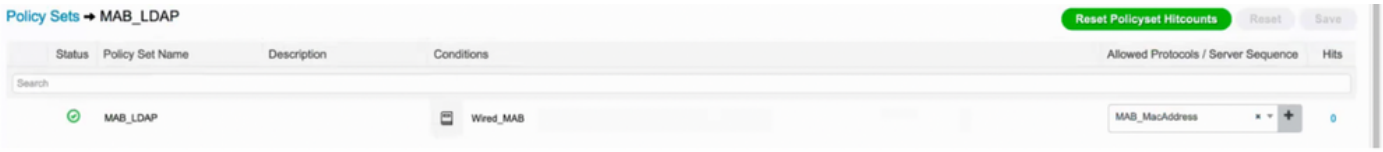


6.認可プロファイルを作成するには、**[Policy] -> [Policy Elements] -> [Results] -> [Authorization] -> [Authorization Profiles]に移動します。**[Add]を選択し、エンドポイントに割り当てる権限を定義します。

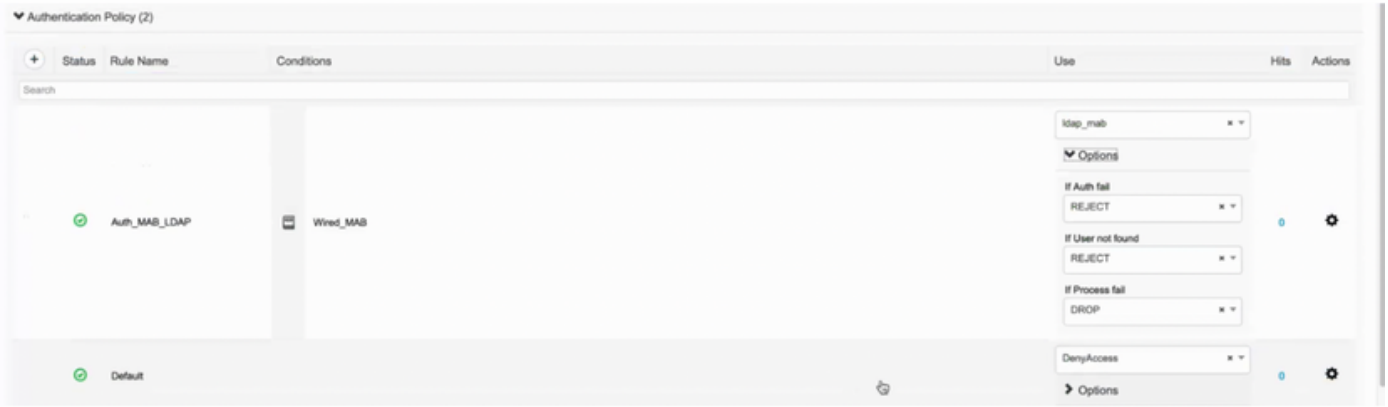




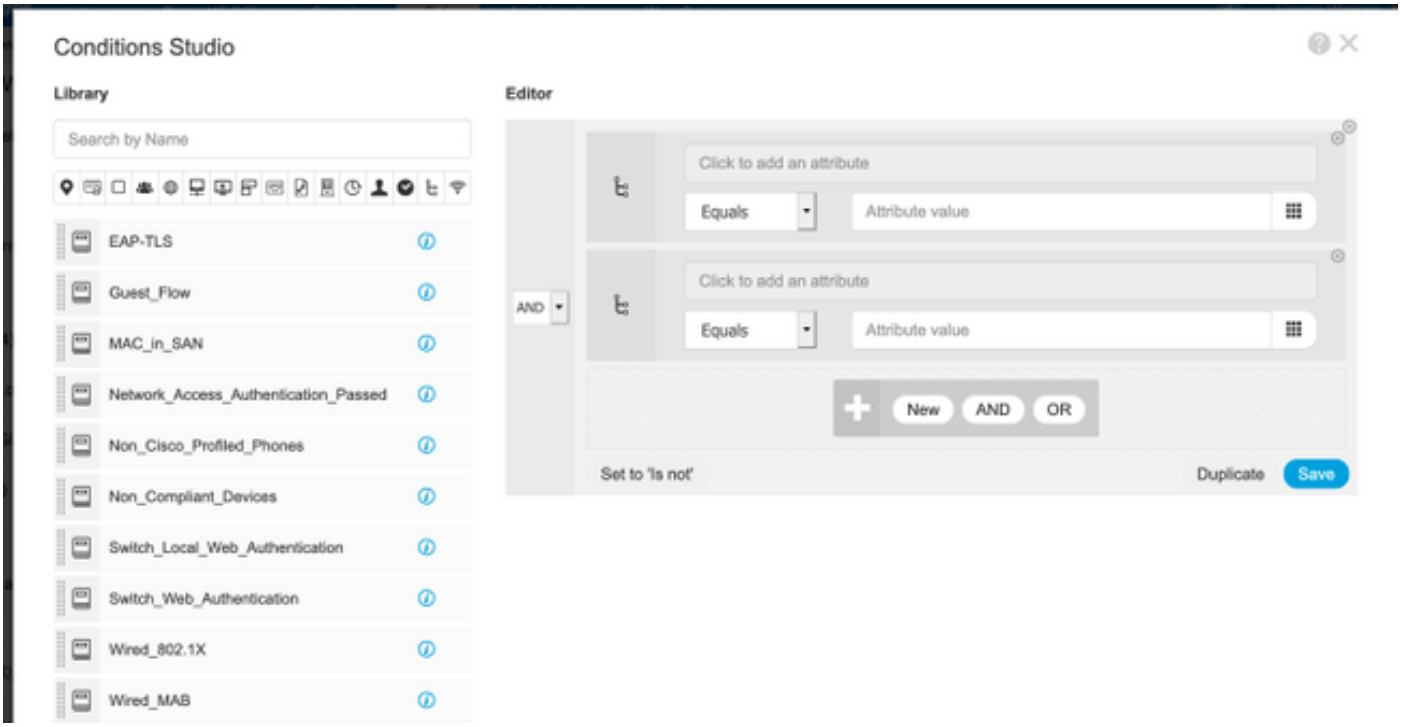
7. [Policy] -> [Policy Set] に移動し、事前に定義された条件Wired_MABと手順5で作成した許可プロトコルを使用してポリシーセットを作成します。

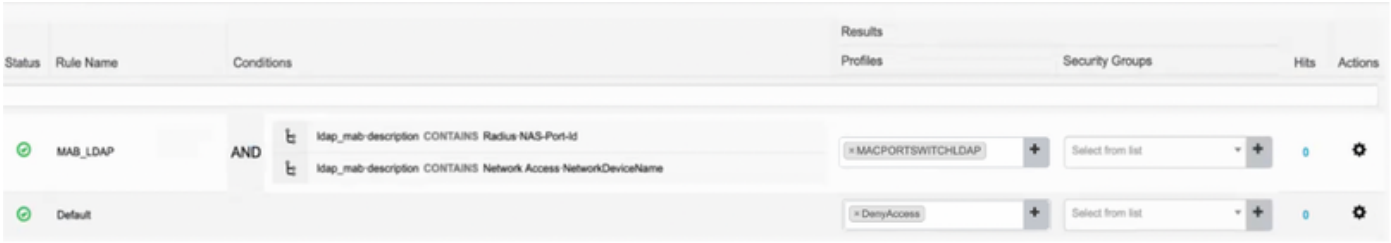


8.新しいポリシーセットで作成された認証ポリシーは、定義済みの**Wired_MAB** Libraryと**LDAP**接続を外部アイデンティティソースシーケンスとして使用します



9. [Authorization Policy] で、LDAP属性の説明、Radius NAS-Port-Id、およびNetworkDeviceNameを使用して名前を定義し、複合条件を作成します。最後に、手順6で作成した認可プロファイルを追加します。





構成を適用した後、ユーザーの介入なしにネットワークに接続できるようになります。

確認

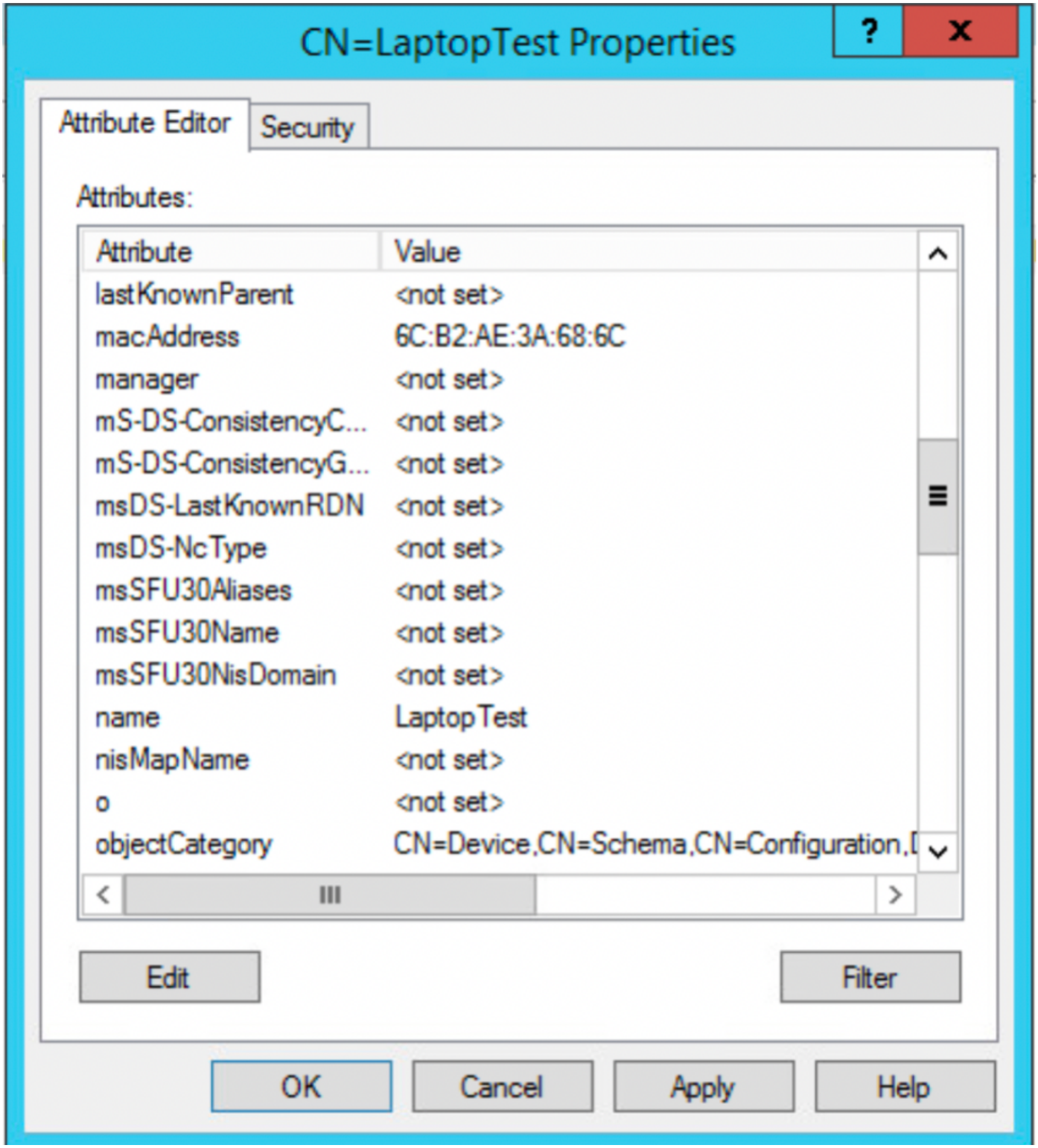
指定スイッチポートに接続したら、**show authentication session interface GigabitEthernet X/X/X detailsを入力して、デバイスの認証および許可ステータスを確認できます**。

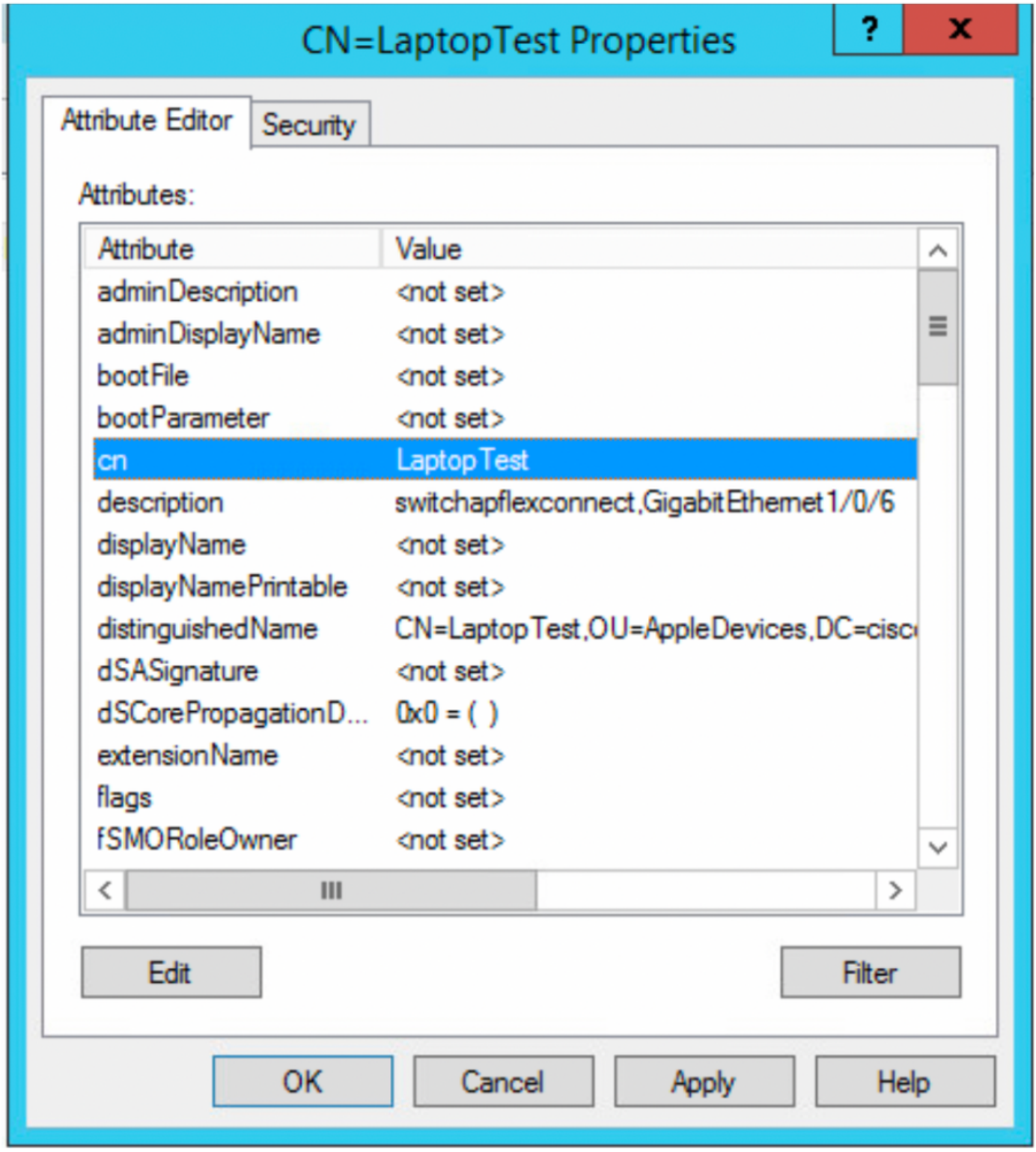
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID:
0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-
B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir:
both Session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

ISEでは、RADIUSライブログを使用して確認できます。

トラブルシュート

LDAPサーバで、作成したデバイスにMacアドレス、適切なスイッチ名、およびスイッチポートが設定されていることを確認します


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



ISEでパケットキャプチャ(**Operations->Troubleshoot->Diagnostic Tool->TCP Dumps**)を実行し、LDAPからISEに送信される値を検証できます