

Authentification basée sur les attributs ISE et LDAP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurer LDAP](#)

[Configuration du commutateur](#)

[Configuration ISE](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer Cisco Identity Services Engine (ISE) et utiliser les attributs d'objets LDAP (Lightweight Directory Access Protocol) pour authentifier et autoriser dynamiquement les périphériques.

Note: Ce document est valide pour les configurations qui utilisent LDAP comme source d'identité externe pour l'authentification et l'autorisation ISE.

Contribué par Emmanuel Cano et Mauricio Ramos Ingénieur des services professionnels Cisco.

Édité par Neri Cruz ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les sujets suivants :

- Connaissance de base des ensembles de politiques ISE, des politiques d'authentification et d'autorisation
- Protocole MAB (Mac Authentication Bypass)
- Connaissances de base du protocole Radius
- Connaissances de base du serveur Windows

Components Used

Les informations de ce document sont basées sur les versions logicielles et matérielles suivantes :

- Cisco ISE, correctif 11 de la version 2.4
- Microsoft Windows Server, version 2012 R2 x64
- Commutateur Cisco Catalyst 3650-24PD, version 03.07.05.E (15.2(3)E5)
- Ordinateur Microsoft Windows 7

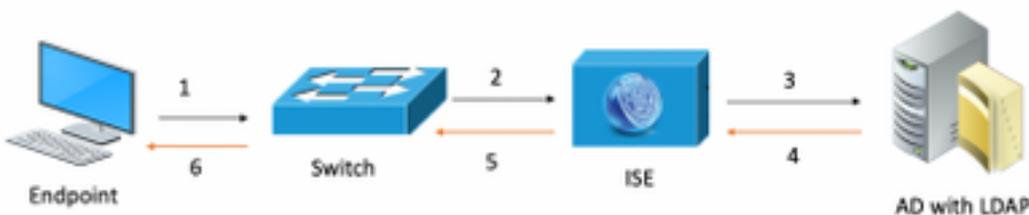
Note: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Cette section décrit comment configurer les périphériques réseau, l'intégration entre ISE et LDAP, et enfin configurer les attributs LDAP à utiliser dans la stratégie d'autorisation ISE.

Diagramme du réseau

Cette image illustre la topologie de réseau utilisée :



Voici le flux de trafic, comme illustré dans le schéma de réseau :

1. L'utilisateur connecte son ordinateur portable au port de commutation désigné.
2. Le commutateur envoie une requête d'accès Radius à l'ISE pour cet utilisateur
3. Lorsque l'ISE reçoit les informations, il interroge le serveur LDAP pour le fichier utilisateur spécifique, qui contient les attributs à utiliser dans les conditions de la stratégie d'autorisation.
4. Une fois que l'ISE a reçu les attributs (port de commutateur, nom de commutateur et adresse MAC de périphérie), il compare les informations fournies par le commutateur.
5. Si les informations d'attributs fournies par le commutateur sont identiques à celles fournies par LDAP, l'ISE envoie un ACCEPT RADIUS avec les autorisations configurées sur le profil d'autorisation.

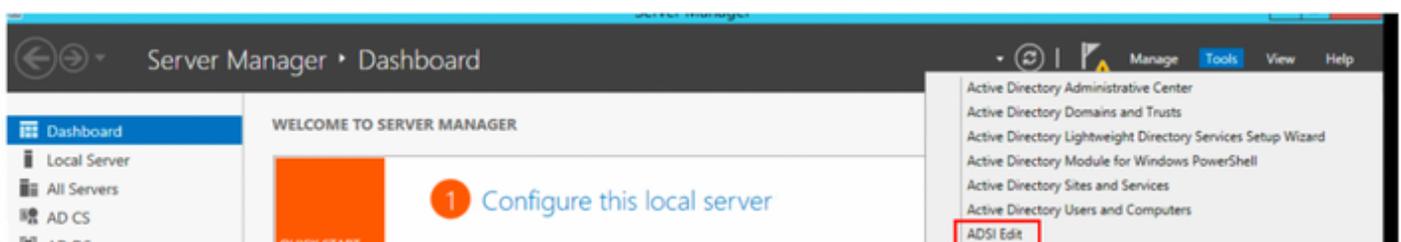
Configurations

Utilisez cette section afin de configurer LDAP, le commutateur et l'ISE.

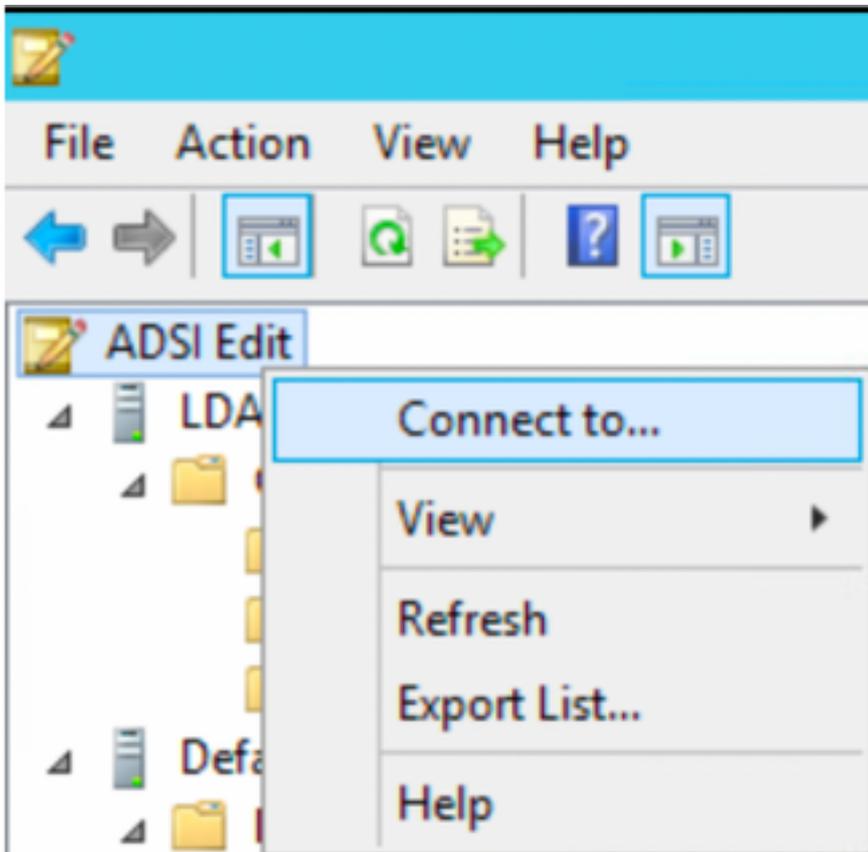
Configuration LDAP

Procédez comme suit pour configurer le serveur LDAP :

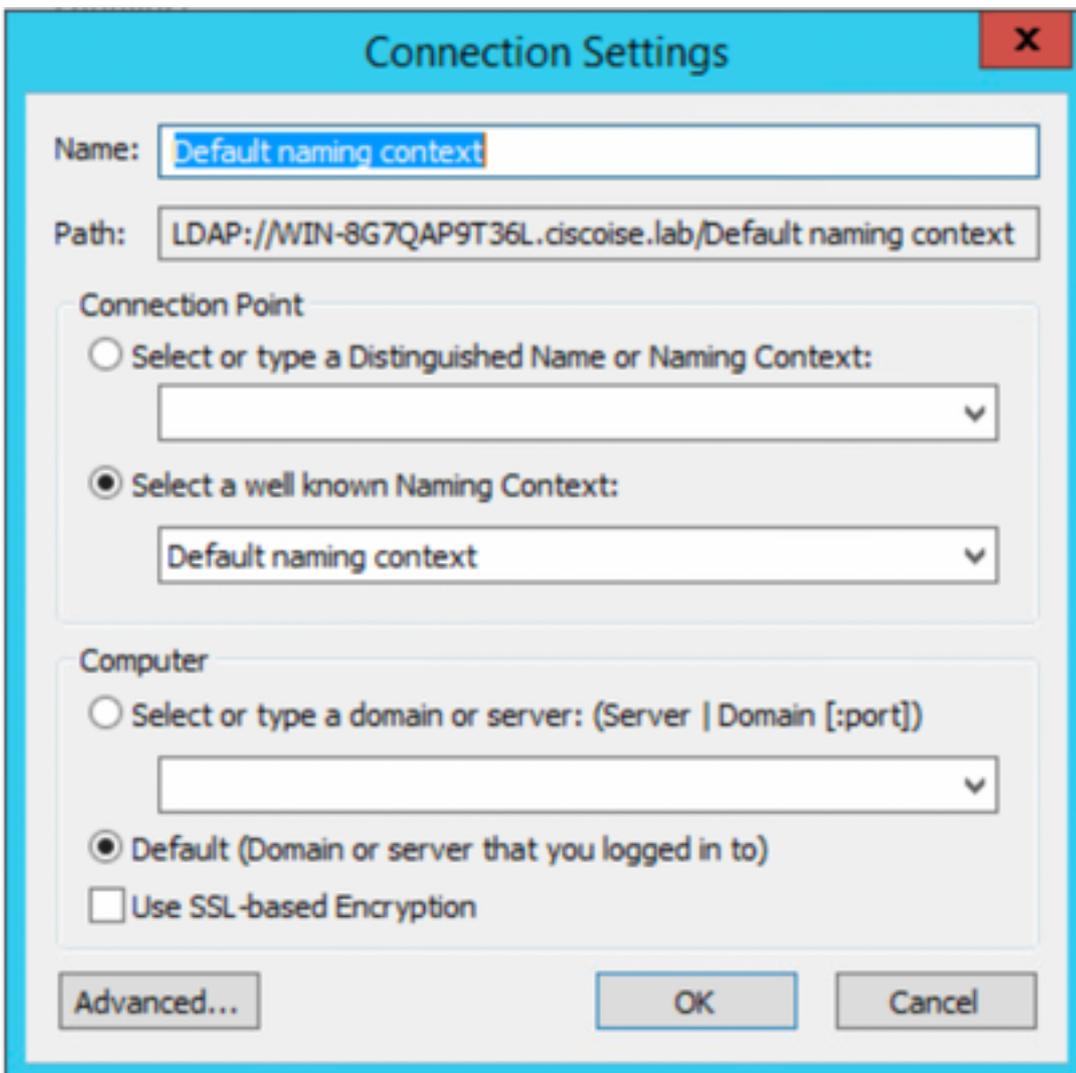
1. Accédez à **Gestionnaire de serveur > Tableau de bord > Outils > Modifier ADSI**



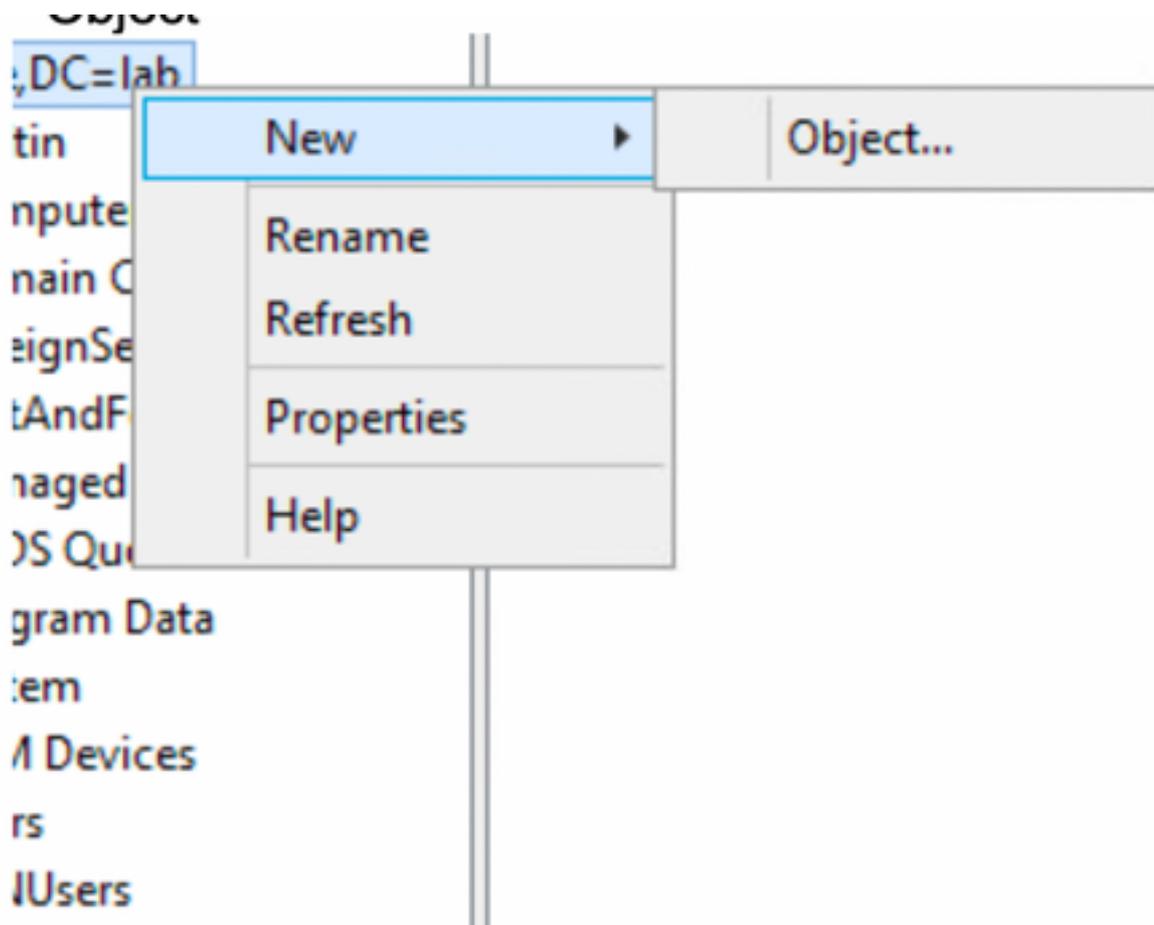
2. Cliquez avec le bouton droit de la souris sur l'icône de modification ADSI et sélectionnez **Se connecter à...**



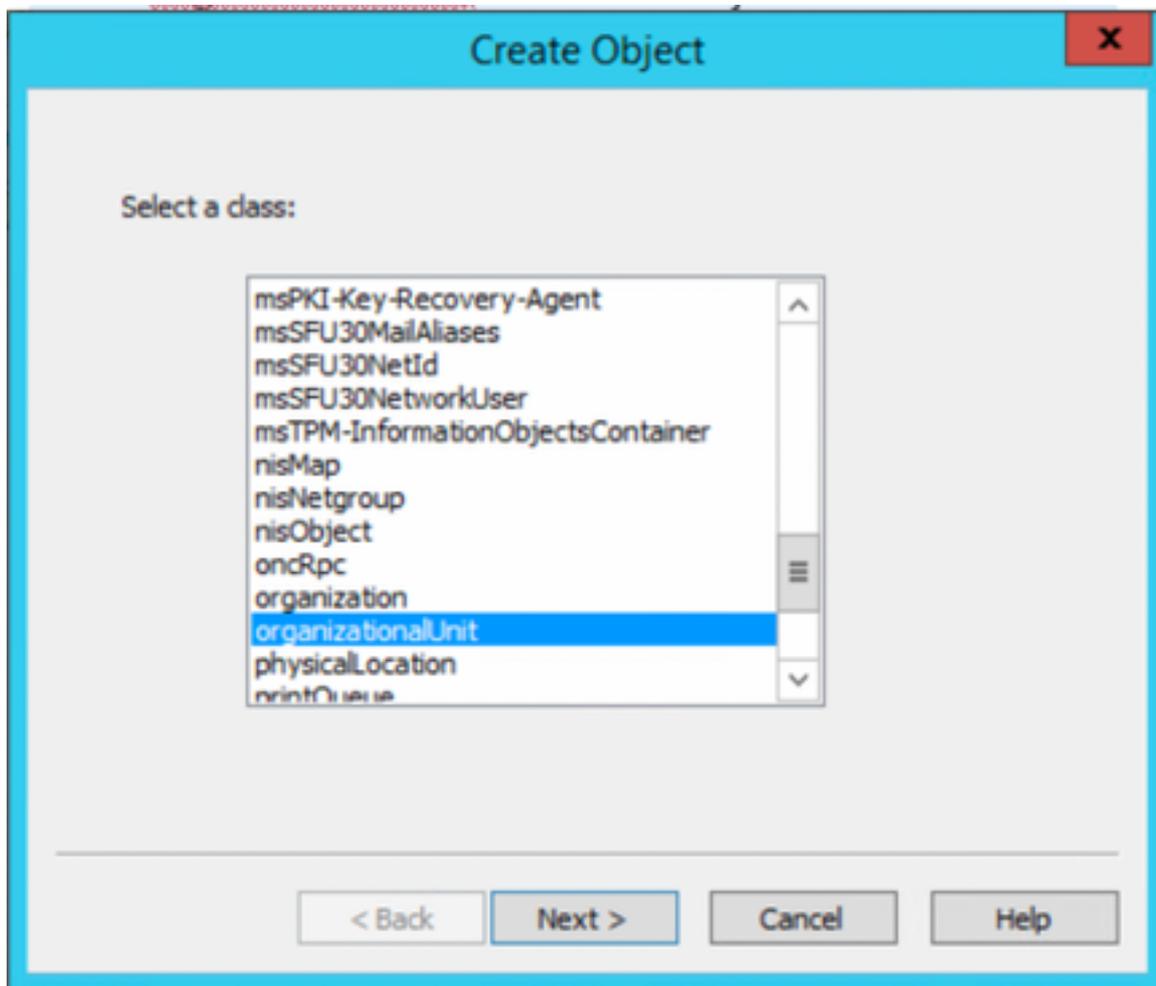
3. Sous Paramètres de connexion, définissez un nom et sélectionnez le bouton **OK** pour démarrer la connexion.



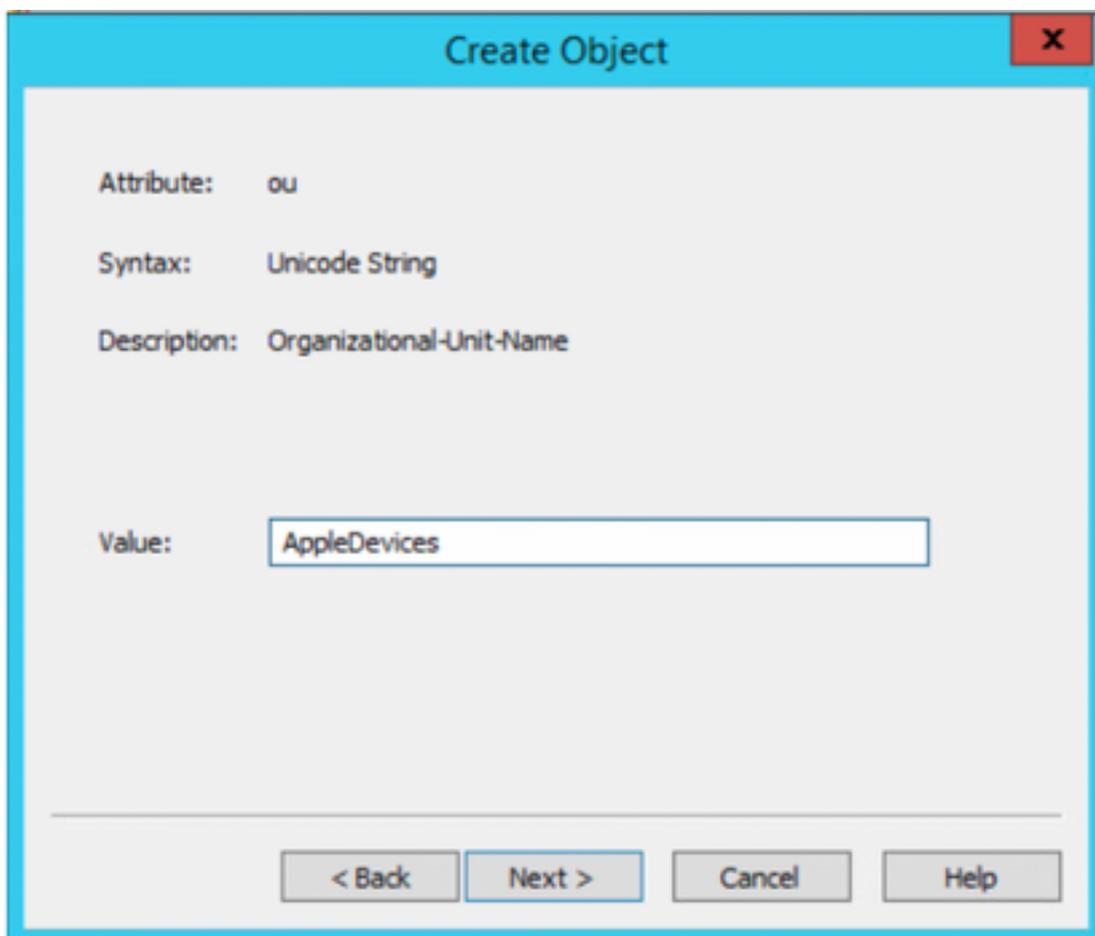
4. Dans le même menu ADSI Edit, cliquez avec le bouton droit de la souris dans la connexion DC (DC=ciscodemo, DC=lab), sélectionnez **Nouveau**, puis sélectionnez l'option **Objet**



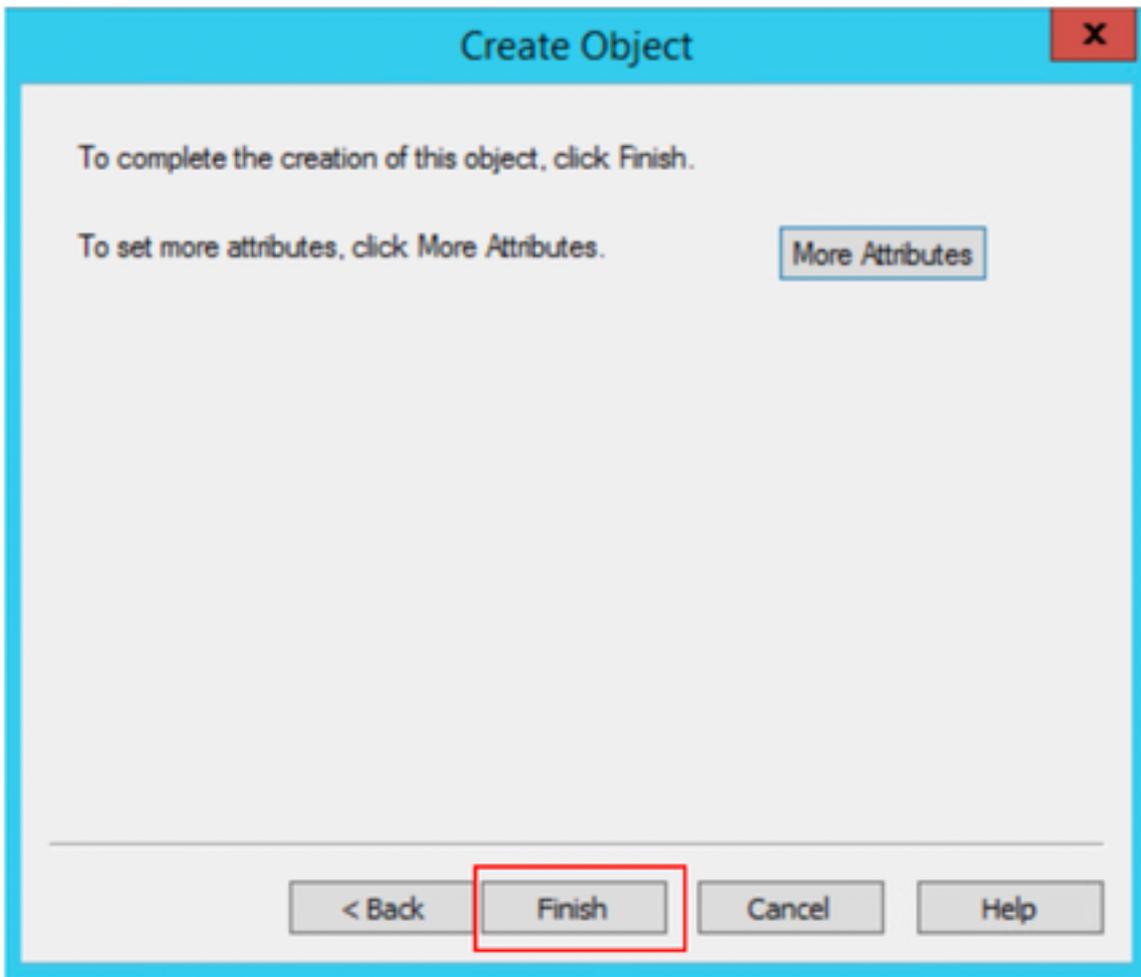
5. Sélectionnez l'option **Unité d'organisation** comme nouvel objet et sélectionnez **Suivant**.



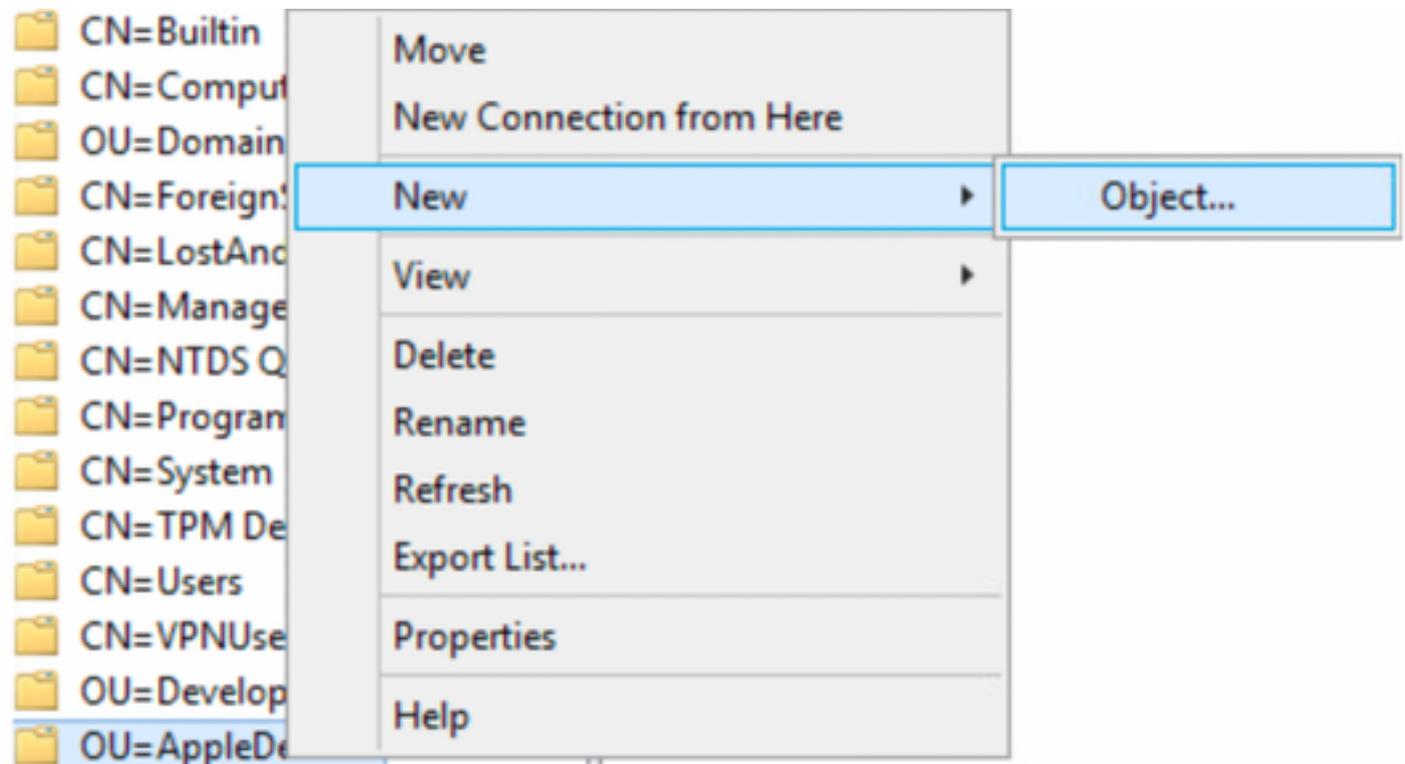
6. Définissez un nom pour la nouvelle unité d'organisation et sélectionnez **Suivant**



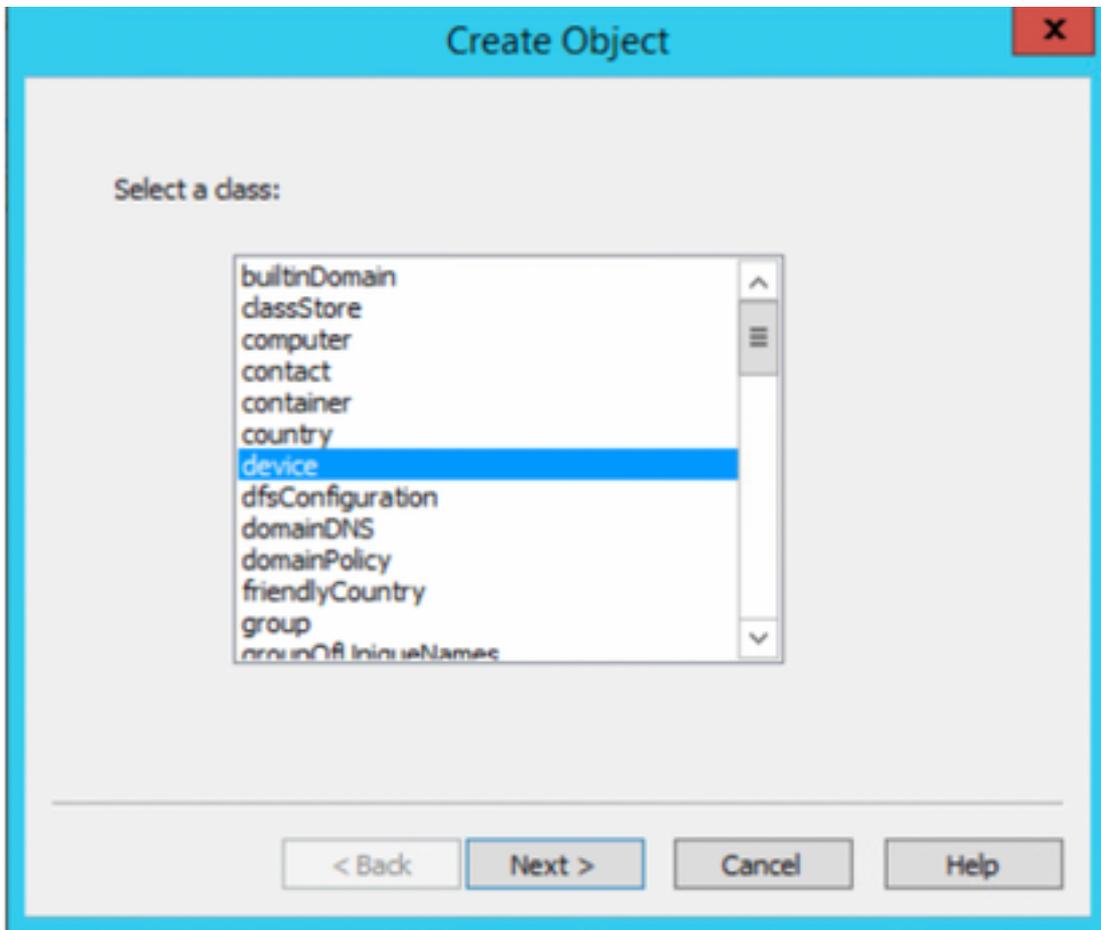
7. Sélectionnez **Terminer** afin de créer la nouvelle unité d'organisation



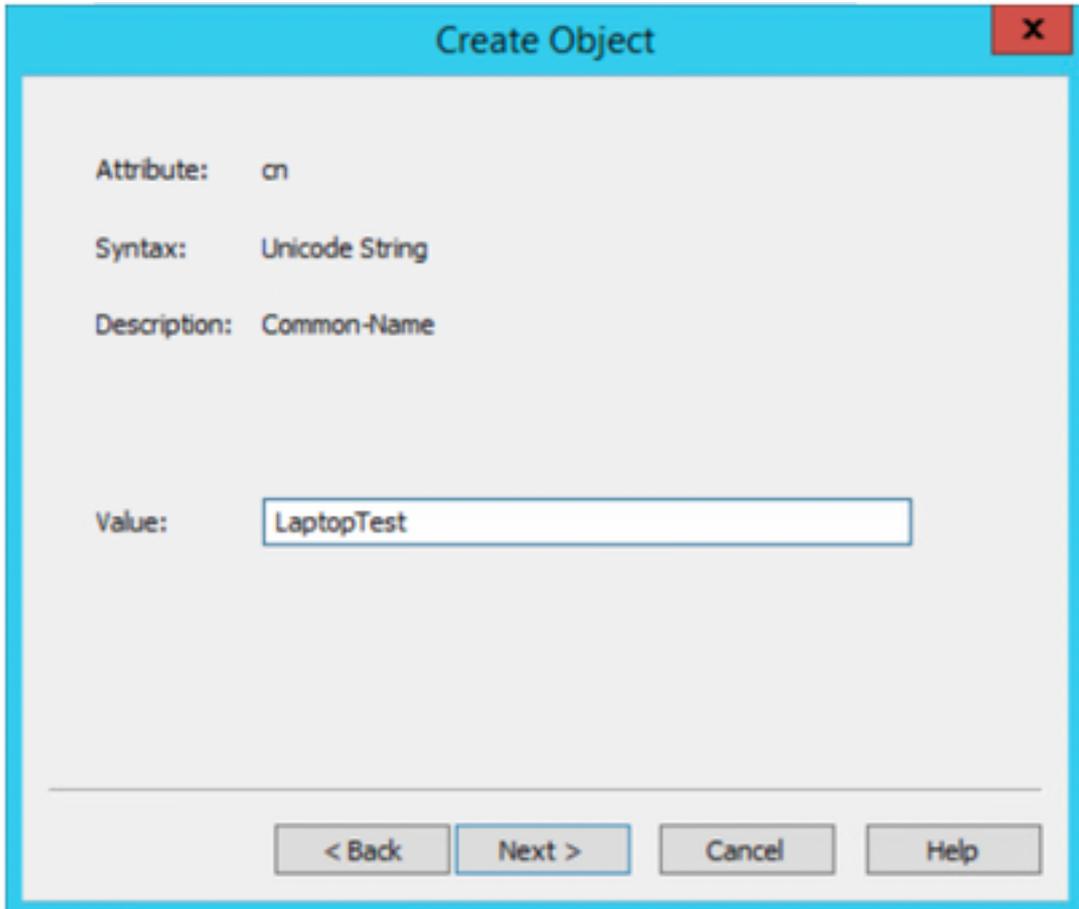
8. Cliquez avec le bouton droit sur l'unité d'organisation qui vient d'être créée et sélectionnez **Nouveau > Objet**



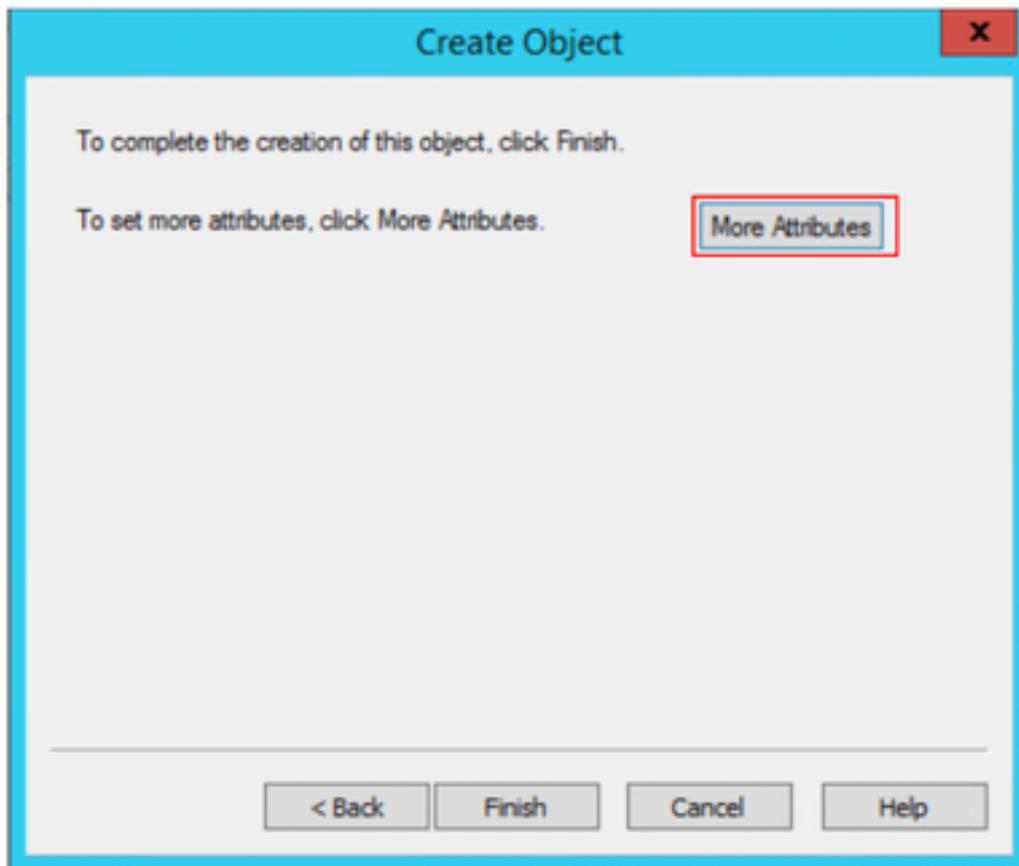
9. Sélectionnez le **périphérique** en tant que classe d'objet et sélectionnez **suivant**



10. Définissez un nom dans le champ Valeur et sélectionnez **Suivant**



11. Sélectionnez l'option **Autres attributs**



11. Dans le menu déroulant, **sélectionnez une propriété à afficher**, sélectionnez l'option **macAddress**, puis définissez l'adresse MAC du point de terminaison qui sera authentifiée sous le champ **Modifier l'attribut** et sélectionnez **Ajouter** un bouton pour enregistrer l'adresse MAC du périphérique.

Remarque : utilisez deux-points au lieu de points ou un trait d'union entre les octets d'adresse MAC.

cn=LaptopTest

Attributes

Path:

Class: device

Select which properties to view: Optional

Select a property to view: macAddress

Attribute Values

Syntax: IA5String

Edit Attribute:

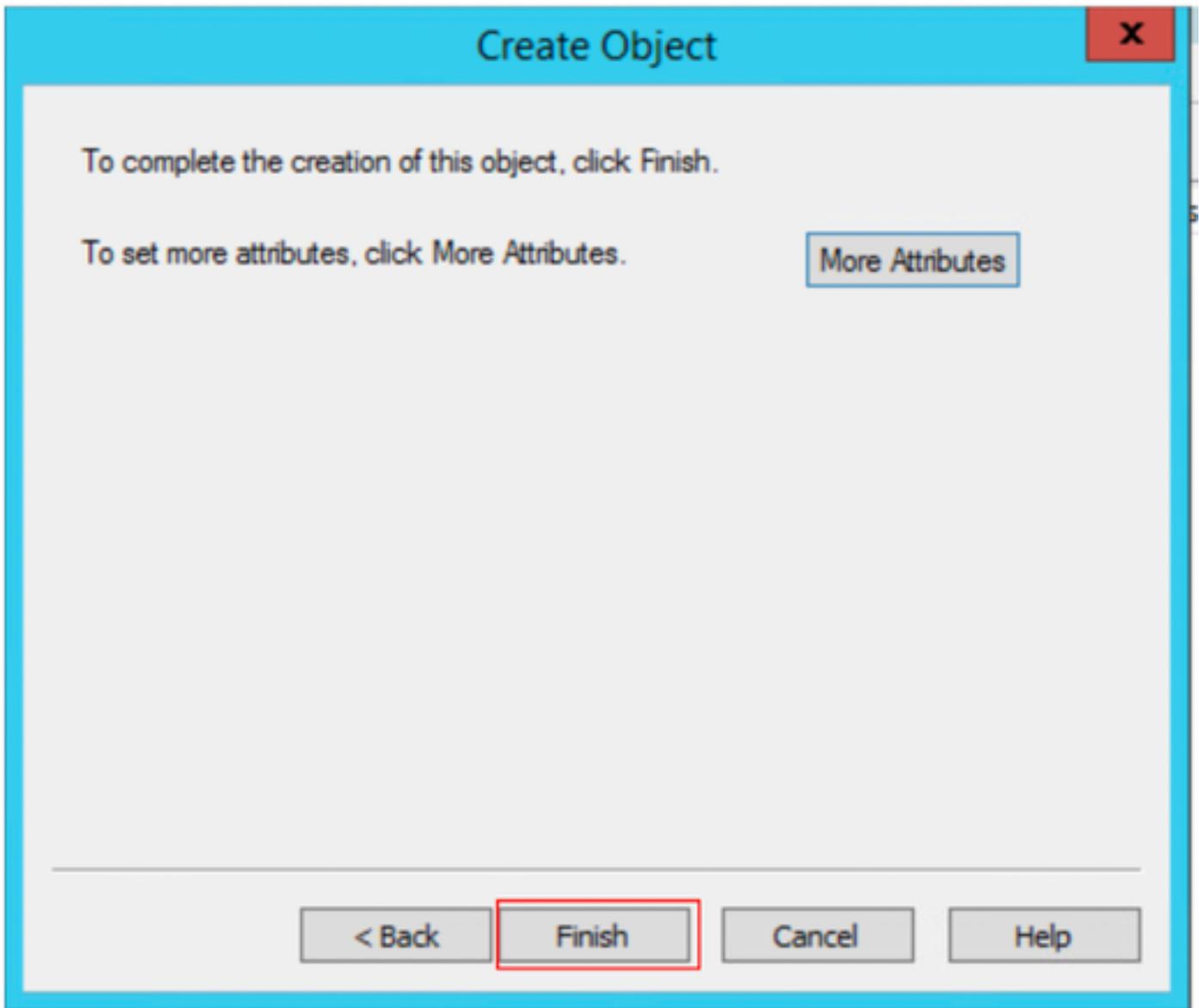
Value(s): 6C:B2:AE:3A:68:6C

Add Remove

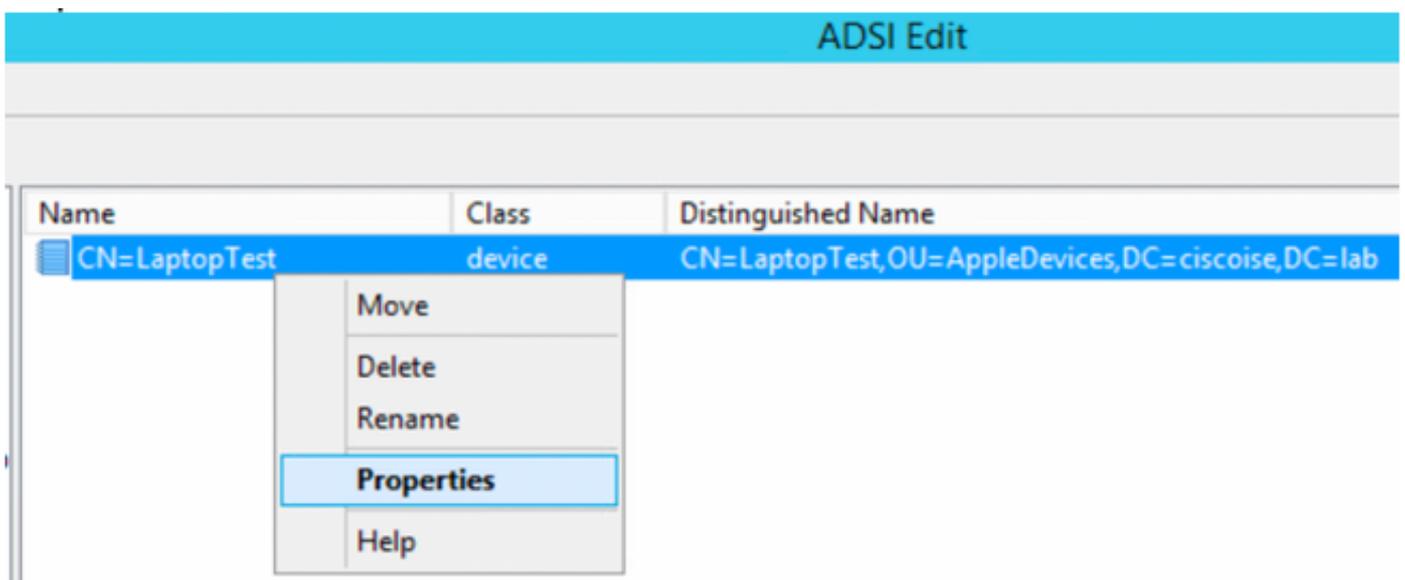
OK Cancel

12. Sélectionnez **OK** afin d'enregistrer les informations et continuer avec la configuration de l'objet du périphérique

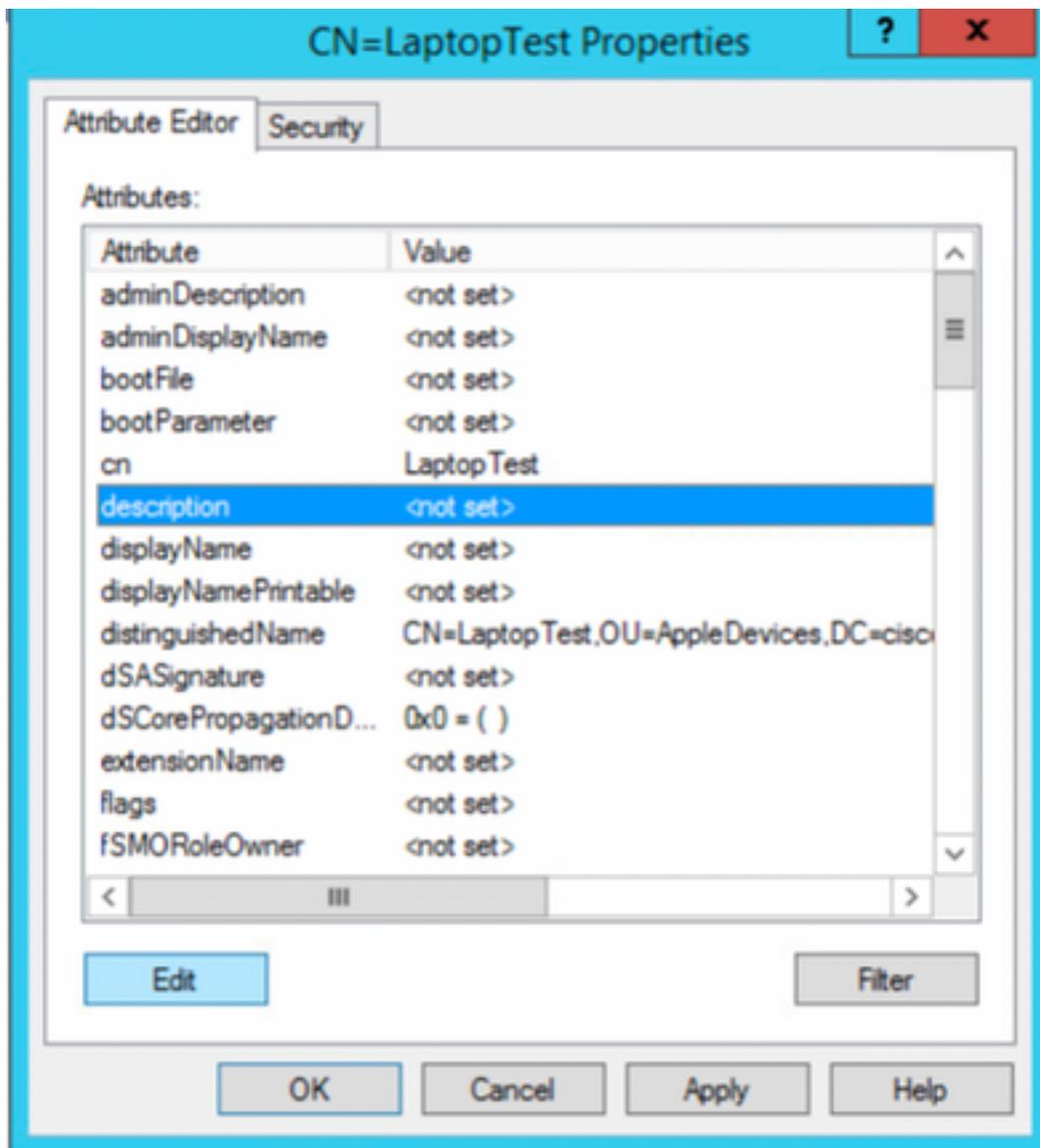
13. Sélectionnez **Terminer** afin de créer le nouvel objet de périphérique



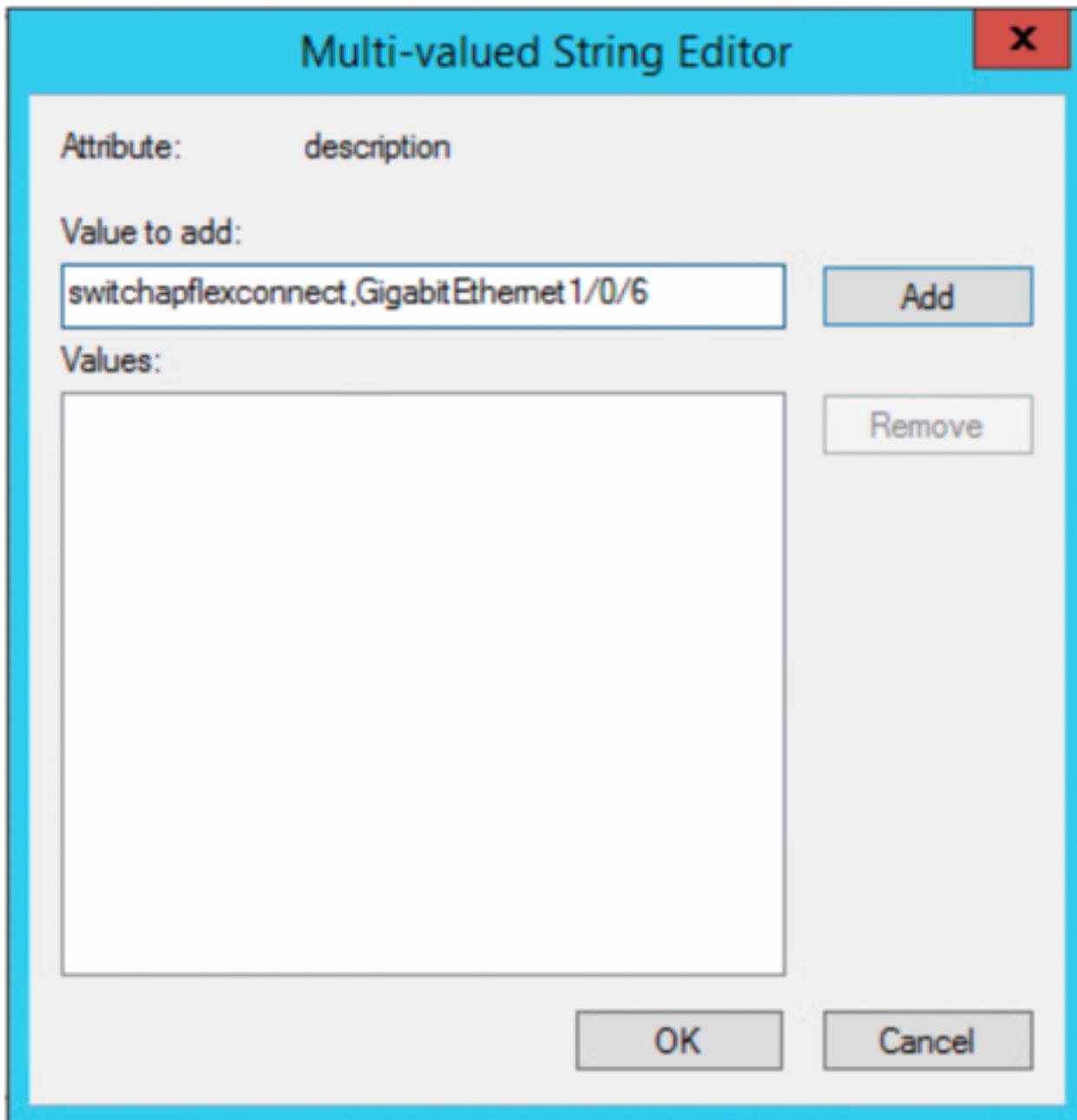
14. Cliquez avec le bouton droit sur l'objet du périphérique et sélectionnez l'option **Propriétés**



15. Sélectionnez **description** de l'option et **Modifier** afin de définir le nom du commutateur et le port de commutateur où le périphérique sera connecté.



16. Définissez le nom du commutateur et le port de commutateur. Veillez à utiliser une virgule pour séparer chaque valeur. Sélectionnez **Ajouter**, puis **OK** pour enregistrer les informations.



- Switchapflexconnect est le nom du commutateur.
- GigabitEthernet1/0/6 est le port de commutation auquel le point d'extrémité est connecté.

Note: Il est possible d'utiliser des scripts afin d'ajouter des attributs à un champ spécifique, cependant, pour cet exemple, nous définissons les valeurs manuellement

Note: L'attribut AD est sensible à la casse, si vous utilisez toutes les adresses Mac dans ISE en minuscules convertis en majuscules au cours de la requête LDAP. Afin d'éviter ce comportement, désactivez la recherche d'hôte de processus sous les protocoles autorisés. Vous trouverez des détails sur ce lien : https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

Configuration du commutateur

La section suivante décrit la configuration de la communication 802.1x entre ISE et le commutateur.

```
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
```

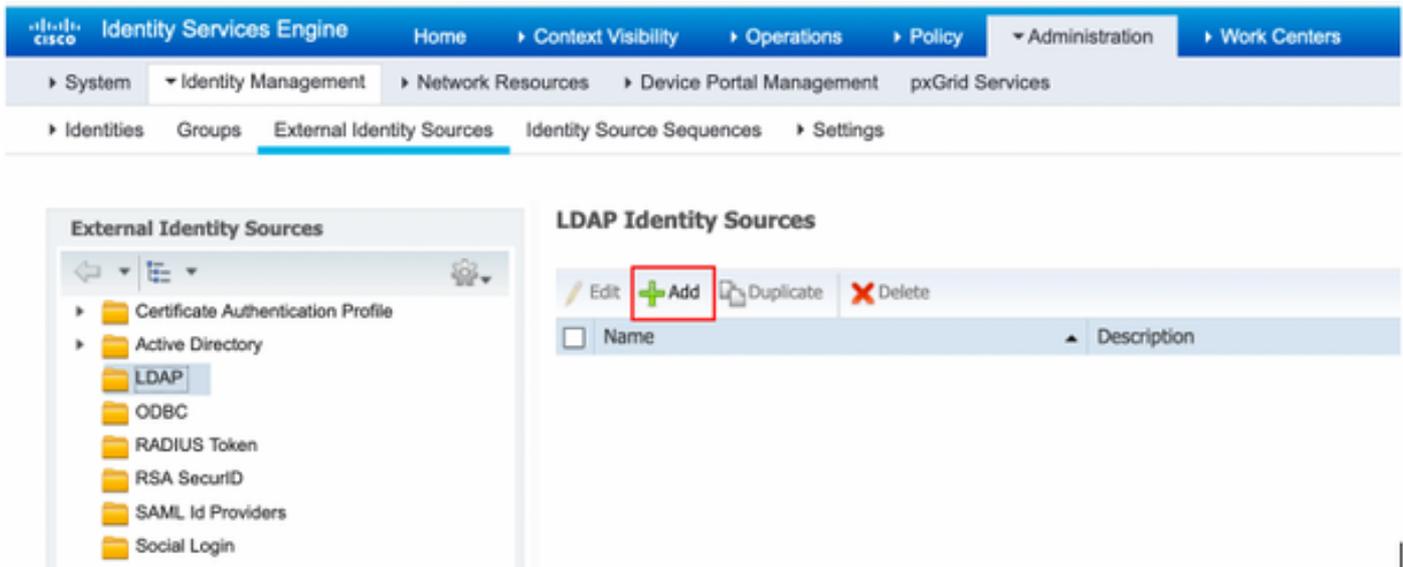
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access 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: Il se peut que la configuration globale et la configuration d'interface doivent être ajustées dans votre environnement

Configuration ISE

Les éléments suivants décrivent la configuration sur ISE pour obtenir les attributs du serveur LDAP et configurer les stratégies ISE.

1. Sur ISE, accédez à **Administration->Gestion des identités->Sources d'identité externes** et sélectionnez le dossier **LDAP** et cliquez sur **Ajouter** afin de créer une nouvelle connexion avec LDAP



The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid Services'. Under 'Identity Management', the 'External Identity Sources' option is selected. The main content area is divided into two panels. The left panel, titled 'External Identity Sources', shows a tree view with folders for 'Certificate Authentication Profile', 'Active Directory', 'LDAP' (highlighted), 'ODBC', 'RADIUS Token', 'RSA SecurID', 'SAML Id Providers', and 'Social Login'. The right panel, titled 'LDAP Identity Sources', contains a toolbar with 'Edit', 'Add' (highlighted in a red box), 'Duplicate', and 'Delete' buttons. Below the toolbar is a table with columns for 'Name' and 'Description'.

2. Sous l'onglet **Général**, définissez un nom et sélectionnez l'adresse MAC comme attribut Nom du sujet

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. Sous l'onglet **Connexion**, configurez l'adresse IP, le nom de domaine d'administration et le mot de passe du serveur LDAP pour obtenir une connexion réussie.

LDAP Identity Source

General Connection Directory Organization Groups Attributes Advanced Settings

Primary Server **Secondary Server**

Enable Secondary Server

* Hostname/IP ⓘ

* Port

Specify server for each ISE node

Access Anonymous Access

Authenticated Access

Admin DN

Password

Secure Authentication Enable Secure Authentication

Enable Server Identity Check

LDAP Server Root CA ⓘ

Issuer CA of ISE Certificates ⓘ

Hostname/IP

Port

Access Anonymous Access

Authenticated Access

Admin DN

Password

Secure Authentication Enable Secure Authentication

Enable Server Identity Check

LDAP Server Root CA ⓘ

Issuer CA of ISE Certificates ⓘ

Save Reset

Note: Le port 389 est le port par défaut utilisé.

4. Sous l'onglet **Attributs**, sélectionnez les attributs macAddress et description. Ces attributs seront utilisés dans la stratégie d'autorisation

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. Pour créer un protocole autorisé, accédez à **Policy->Policy Elements->Results->Authentication->Allowed Protocols**. Définissez et sélectionnez Process Host Lookup et Allow PAP/ASCII comme les seuls protocoles autorisés. Enfin, sélectionnez **Enregistrer**

Identity Services Engine Home Context Visibility Operations Policy Administration

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services List > MAB_MacAddress

Allowed Protocols

Name: MAB_MacAddress

Description:

Allowed Protocols

Authentication Bypass

Process Host Lookup

Authentication Protocols

Allow PAP/ASCII

6. Pour créer un profil d'autorisation, accédez à **Policy->Policy Elements->Results->Authorization->Authorization Profiles**. Sélectionnez **Ajouter** et définissez les autorisations qui seront attribuées au point de terminaison.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Policy Elements

Dictionaries Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

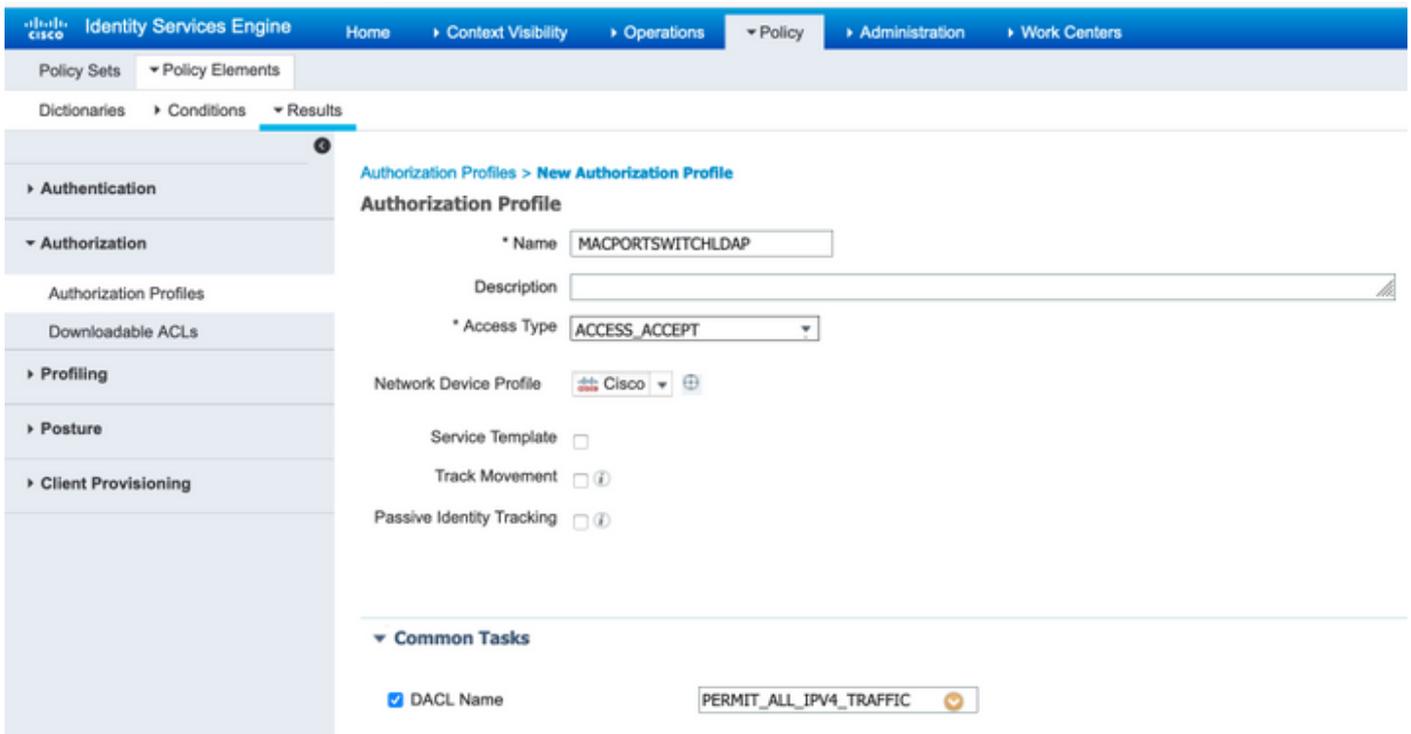
Posture

Standard Authorization Profiles

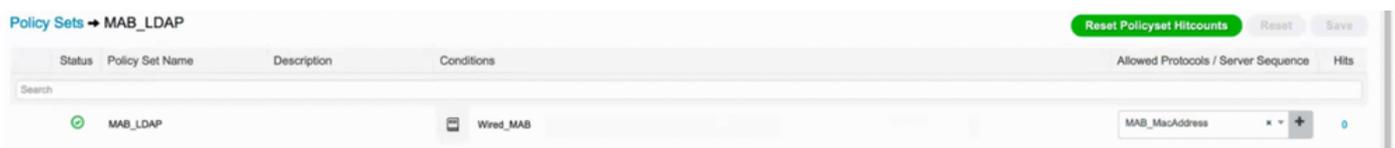
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit **Add** Duplicate Delete

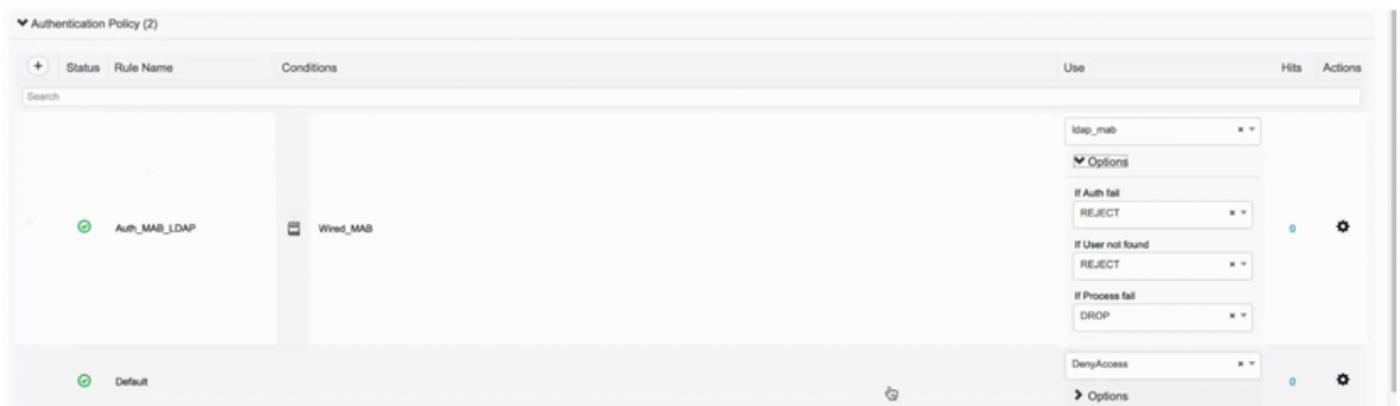
<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco
<input type="checkbox"/>	Cisco_IP_Phones	Cisco
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco



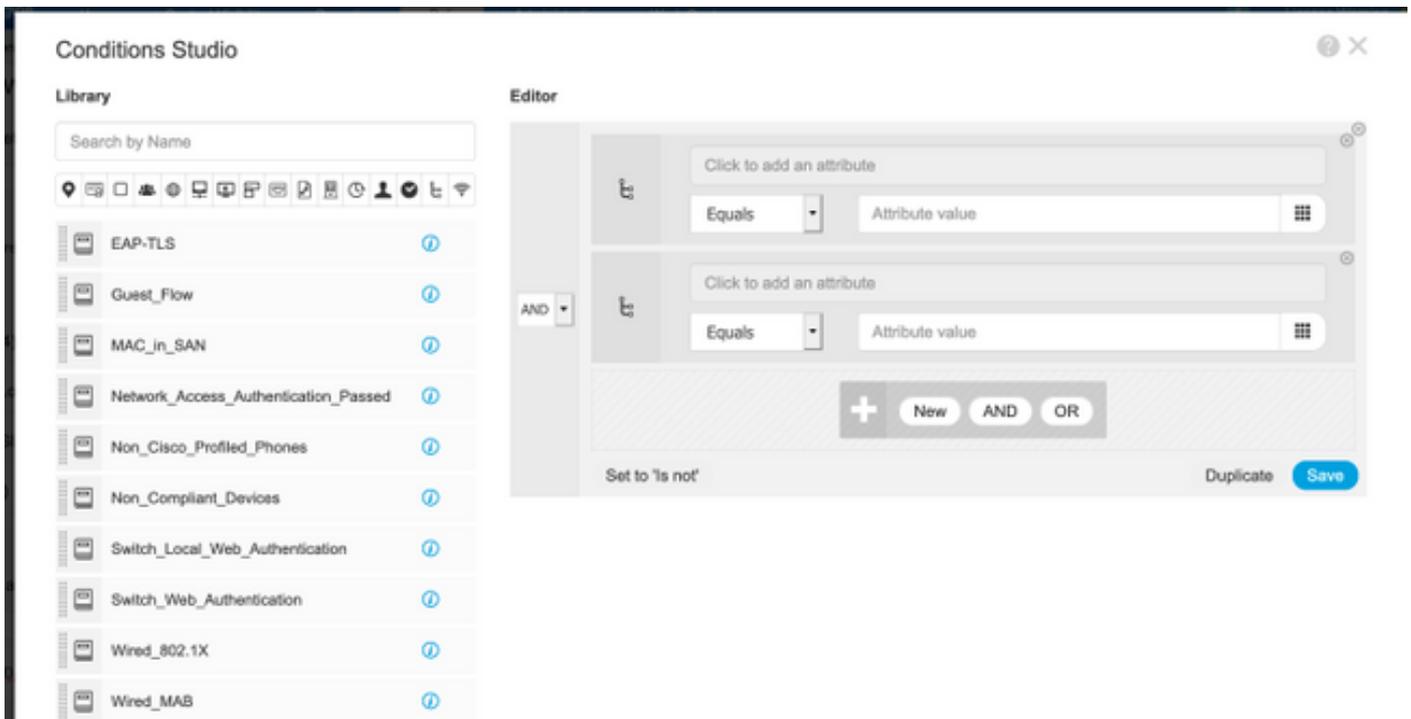
7. Accédez à Policy-> Policy Set et créez un jeu de stratégies à l'aide de la condition prédéfinie Wired_MAB et du protocole autorisé créé à l'étape 5.



8. Sous le nouveau jeu de stratégies créé, créez une stratégie d'authentification à l'aide de la séquence de source d'identité externe de la bibliothèque **Wired_MAB** prédéfinie et de la connexion **LDAP**



9. Sous **Stratégie d'autorisation**, définissez un nom et créez une condition composée à l'aide de la description de l'attribut LDAP, de l'ID de port NAS Radius et de NetworkDeviceName. Enfin, ajoutez le profil d'autorisation créé à l'étape 6.



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

Après avoir appliqué la configuration, vous devez pouvoir vous connecter au réseau sans intervention de l'utilisateur.

Vérification

Une fois connecté au port de commutateur désigné, vous pouvez taper **show authentication session interface GigabitEthernet X/X/X** pour valider l'état d'authentification et d'autorisation du périphérique.

```
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
```

Sur ISE, vous pouvez utiliser Radius Live Logs pour confirmer.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Server	Authorization Profiles
Jan 20, 2020 09:21:47.825 PM	✓		0	employee1@ciscodemo.lab	6C-B2-AE-3A-68-6C	Unknown	Authentication Policy	ise23-1	MACPORTSWITCHLDAP
Jan 20, 2020 09:21:47.801 PM	✓		0	employee1@ciscodemo.lab	6C-B2-AE-3A-68-6C	Unknown		ise23-1	MACPORTSWITCHLDAP

Dépannage

Sur le serveur LDAP, vérifiez que l'adresse MAC, le nom de commutateur approprié et le port de commutateur du périphérique créé sont configurés.

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

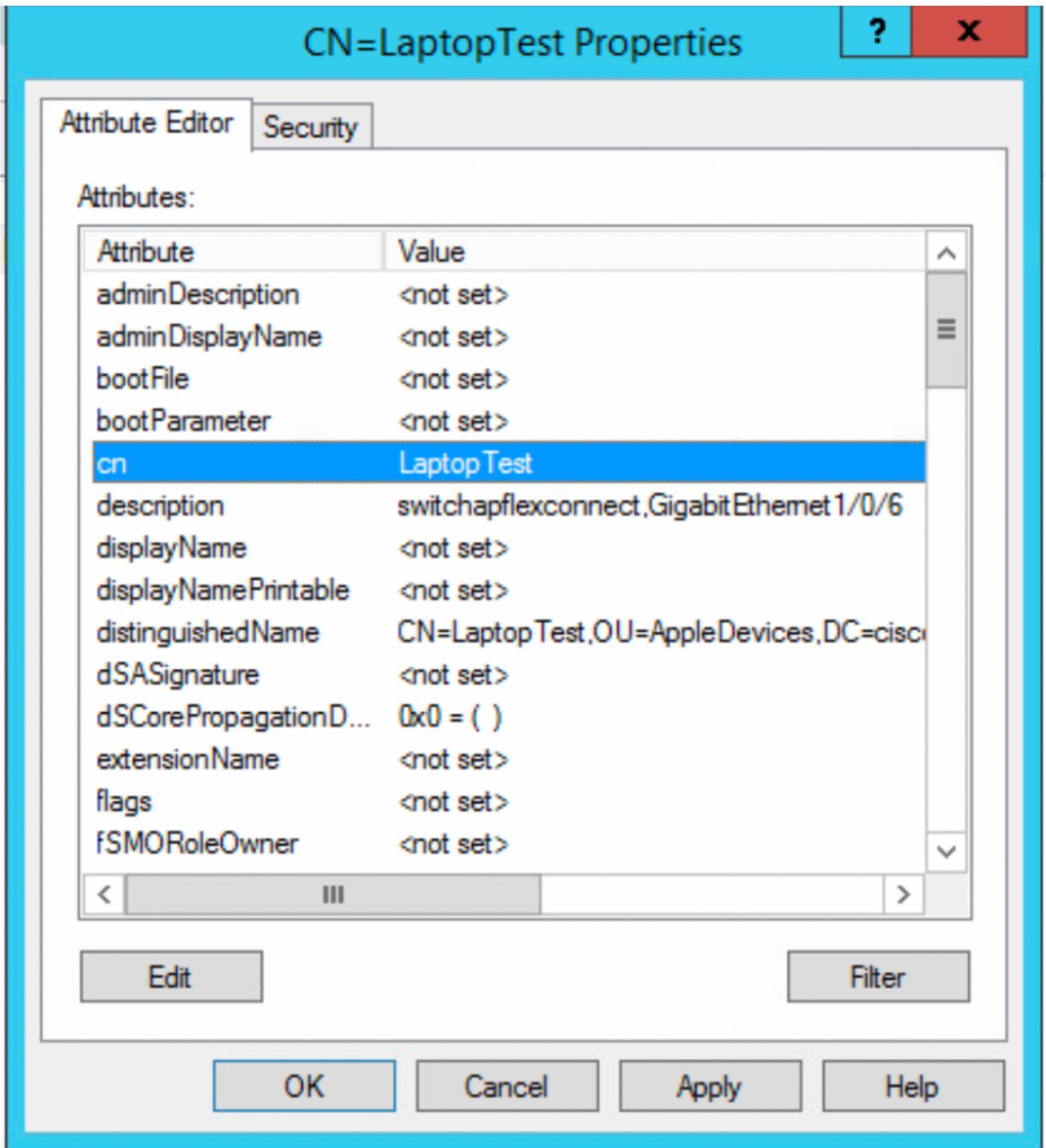
Filter

OK

Cancel

Apply

Help



Sur ISE, vous pouvez prendre une capture de paquets (Accédez à **Opérations->Dépannage->Outil de diagnostic->Dumps TCP**) afin de valider que les valeurs sont envoyées de LDAP à ISE

