

Autenticazione basata sugli attributi ISE e LDAP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configura LDAP](#)

[Configurazione degli switch](#)

[Configurazione di ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare Cisco Identity Services Engine (ISE) e utilizzare gli attributi degli oggetti LDAP (Lightweight Directory Access Protocol) per autenticare e autorizzare i dispositivi in modo dinamico.

Nota: Questo documento è valido per le configurazioni che usano LDAP come origine identità esterna per l'autenticazione e l'autorizzazione ISE.

Contributo di Emmanuel Cano e Mauricio Ramos Cisco Professional Services Engineer.

A cura di Neri Cruz Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei set di policy, dell'autenticazione e delle policy di autorizzazione ISE
- Mac Authentication Bypass (MAB)
- Conoscenze base del protocollo Radius
- Conoscenze base di Windows Server

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE, versione 2.4 patch 11
- Microsoft Windows Server, versione 2012 R2 x64
- Cisco Switch Catalyst 3650-24PD, versione 03.07.05.E (15.2(3)E5)
- computer con Microsoft Windows 7

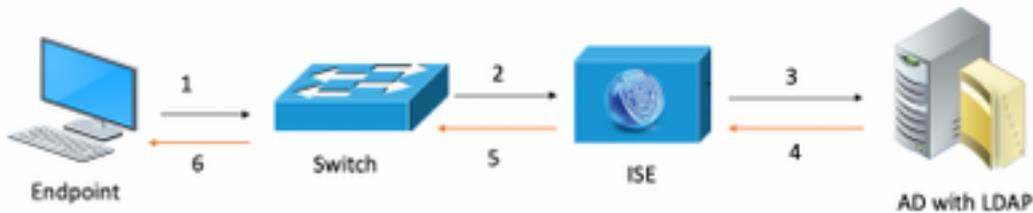
Nota: Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione viene descritto come configurare i dispositivi di rete, l'integrazione tra ISE e LDAP e infine come configurare gli attributi LDAP da utilizzare nella policy di autorizzazione ISE.

Esempio di rete

Nell'immagine è illustrata la topologia di rete utilizzata:



Di seguito è riportato il flusso del traffico, come mostrato nello schema della rete:

1. L'utente collega il PC/notebook alla porta dello switch designata.
2. Lo switch invia una richiesta di accesso Radius per l'utente all'ISE
3. Quando l'ISE riceve le informazioni, interroga il server LDAP per il campo utente specifico, che contiene gli attributi da utilizzare nelle condizioni del criterio di autorizzazione.
4. Una volta ricevuti gli attributi (porta dello switch, nome dello switch e indirizzo MAC del dispositivo), ISE confronta le informazioni fornite dallo switch.
5. Se le informazioni sugli attributi fornite dallo switch sono le stesse di quelle fornite da LDAP, ISE invierà un messaggio di autorizzazione RADIUS con le autorizzazioni configurate nel profilo di autorizzazione.

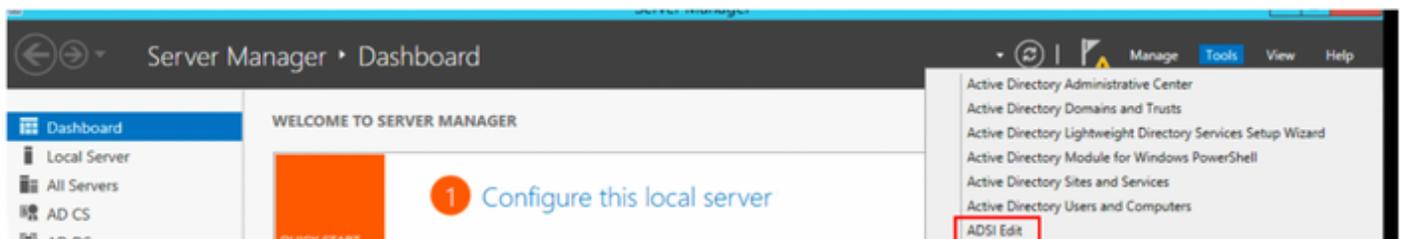
Configurazioni

Utilizzare questa sezione per configurare il protocollo LDAP, lo switch e l'ISE.

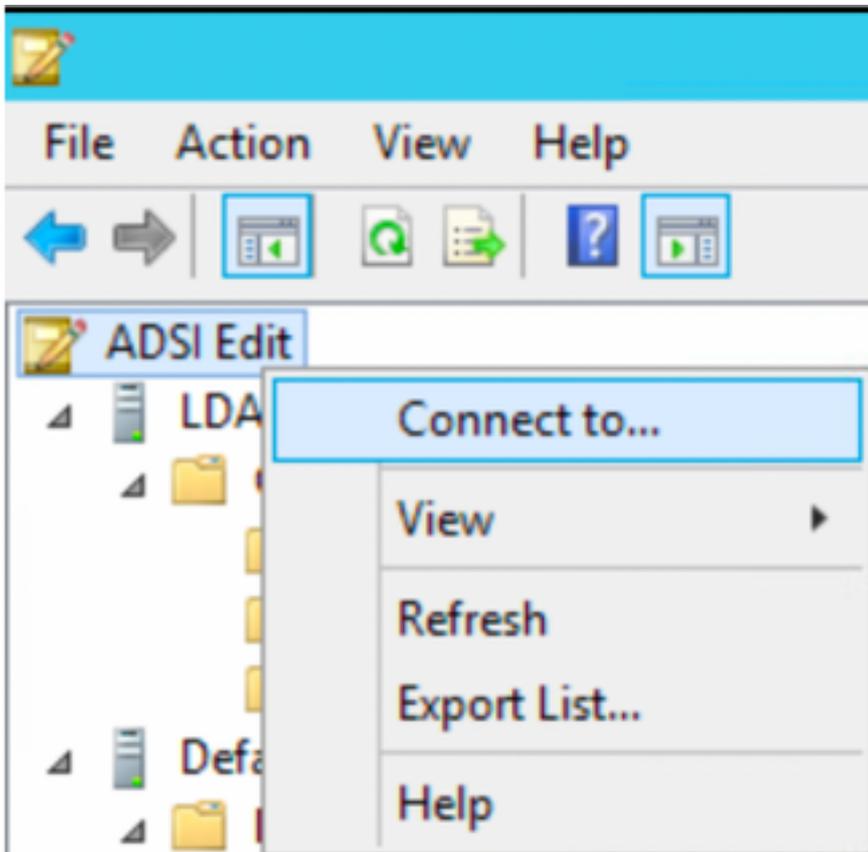
Configurazione LDAP

Per configurare il server LDAP, effettuare le seguenti operazioni:

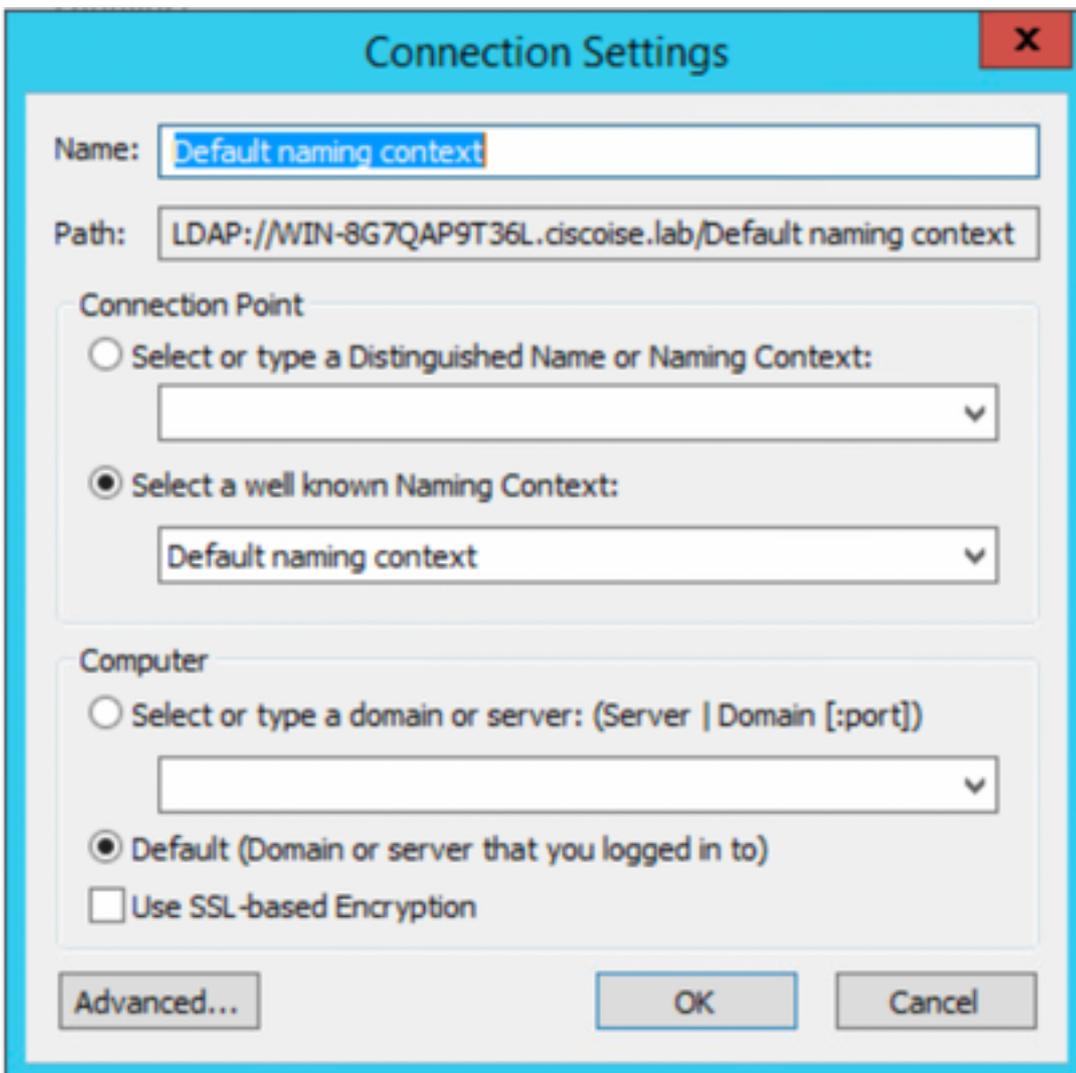
1. Passare a **Server Manager > Dashboard > Strumenti > Modifica ADSI**



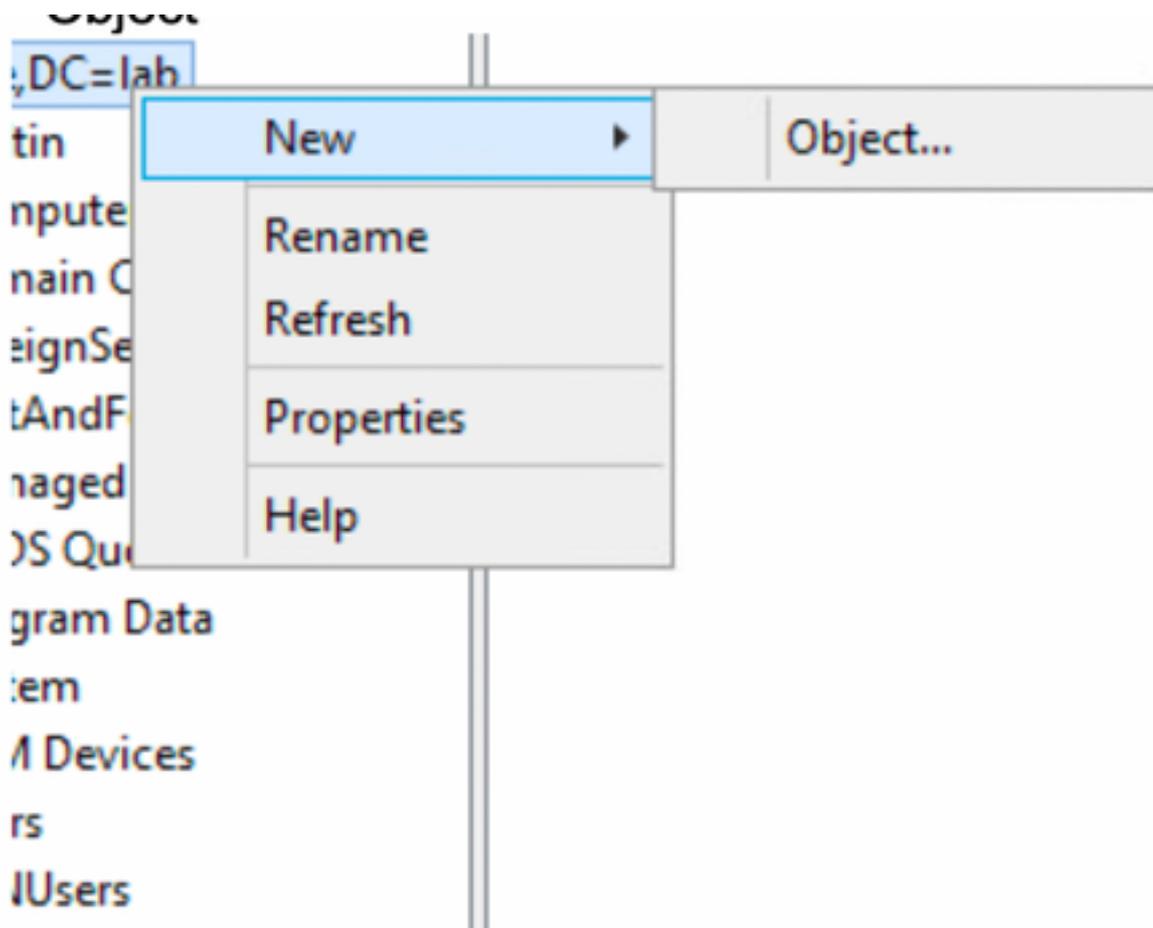
2. Fare clic con il pulsante destro del mouse sull'icona Modifica ADSI e selezionare **Connetti a...**



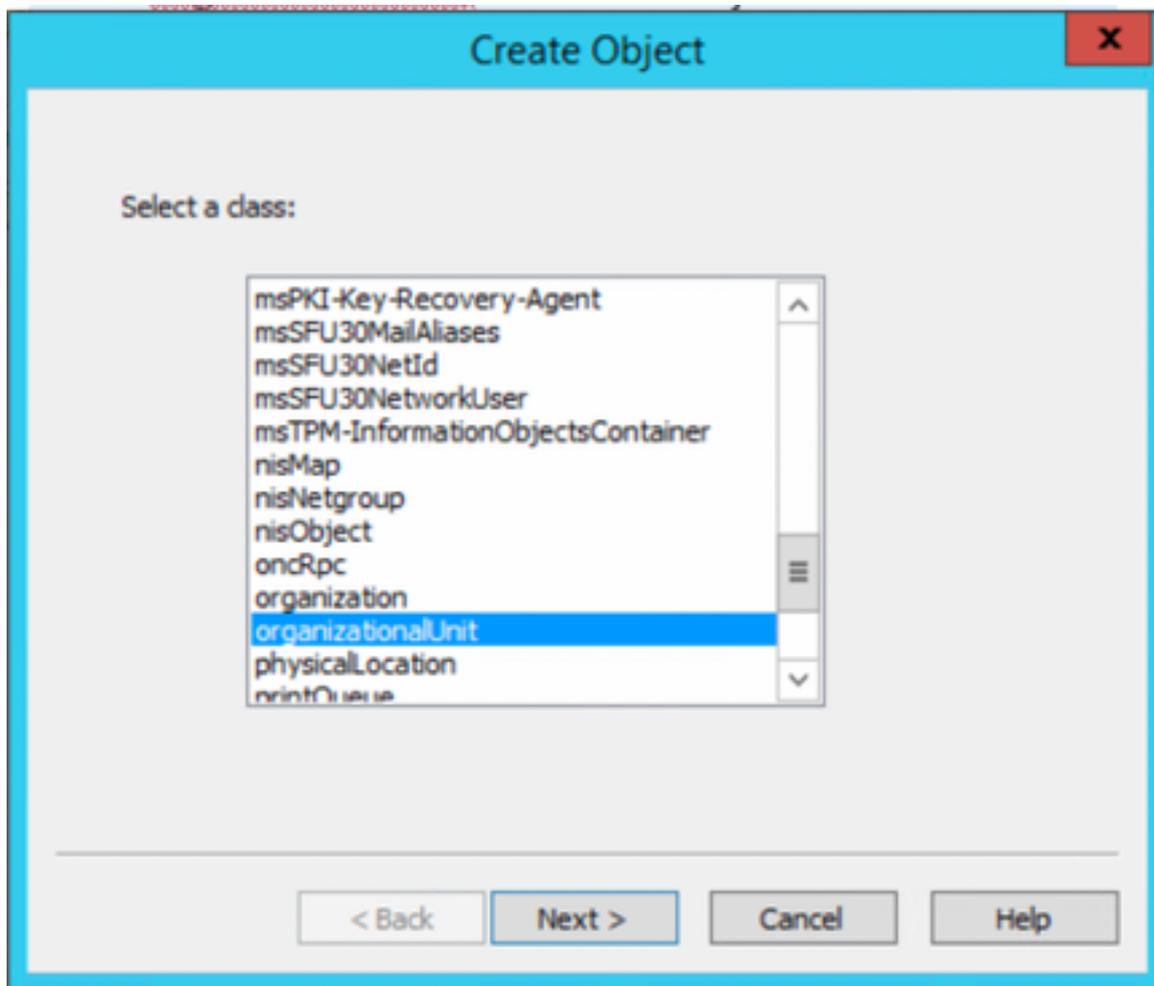
3. In Impostazioni connessione definire un nome e selezionare il pulsante **OK** per avviare la connessione.



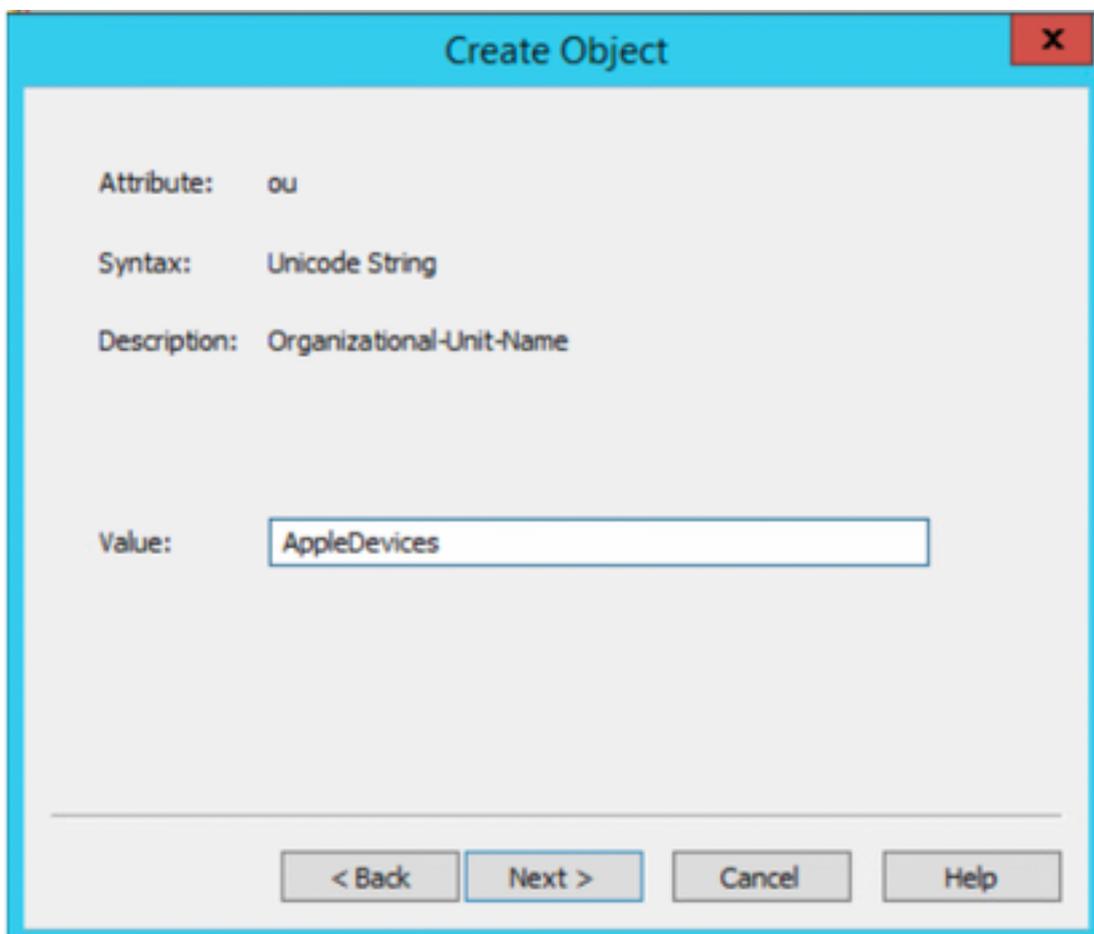
4. Nello stesso menu Modifica ADSI, fare clic con il pulsante destro del mouse su Connessione DC (DC=ciscodemo, DC=lab), selezionare **Nuovo**, quindi selezionare l'opzione **Oggetto**



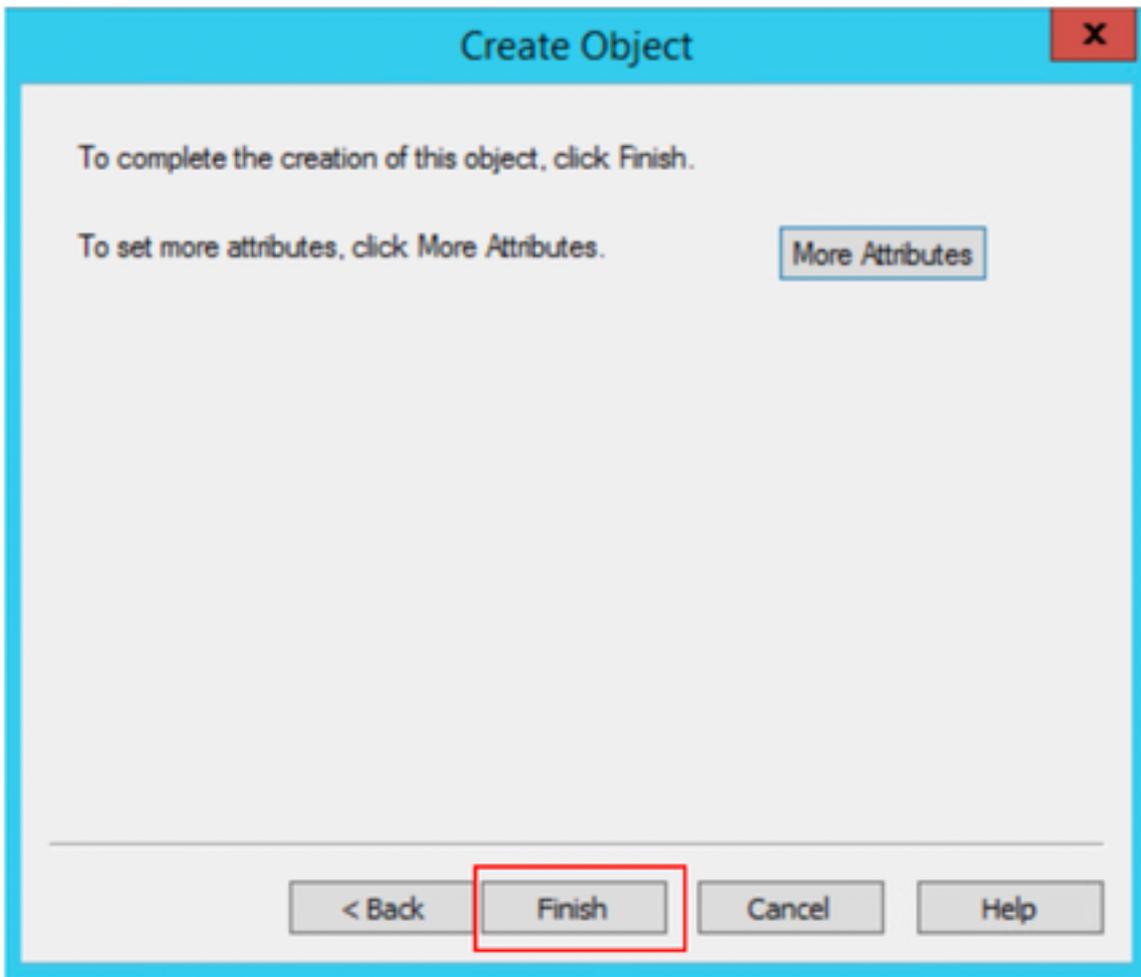
5. Selezionare l'opzione **OrganizationalUnit** come nuovo oggetto e selezionare **avanti**.



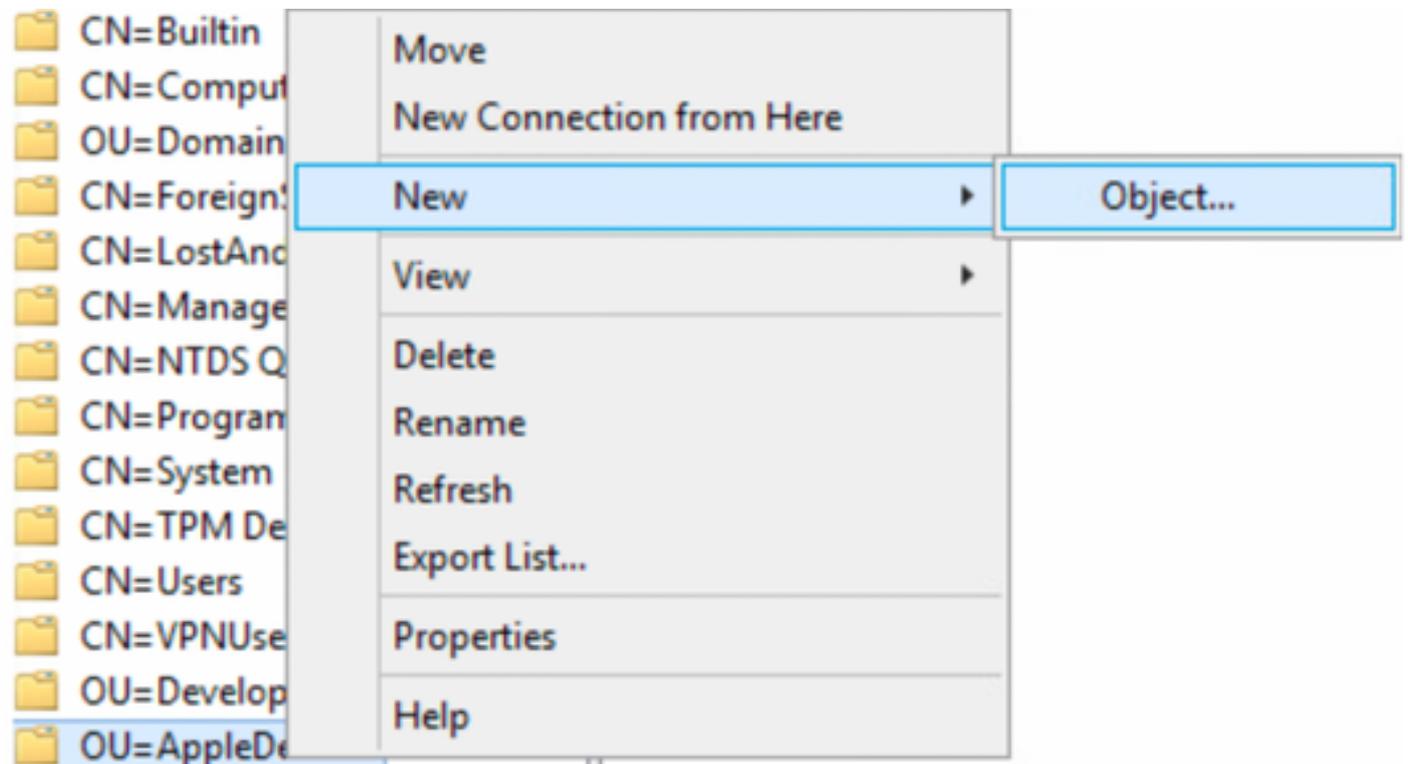
6. Definire un nome per la nuova unità organizzativa e selezionare **Avanti**



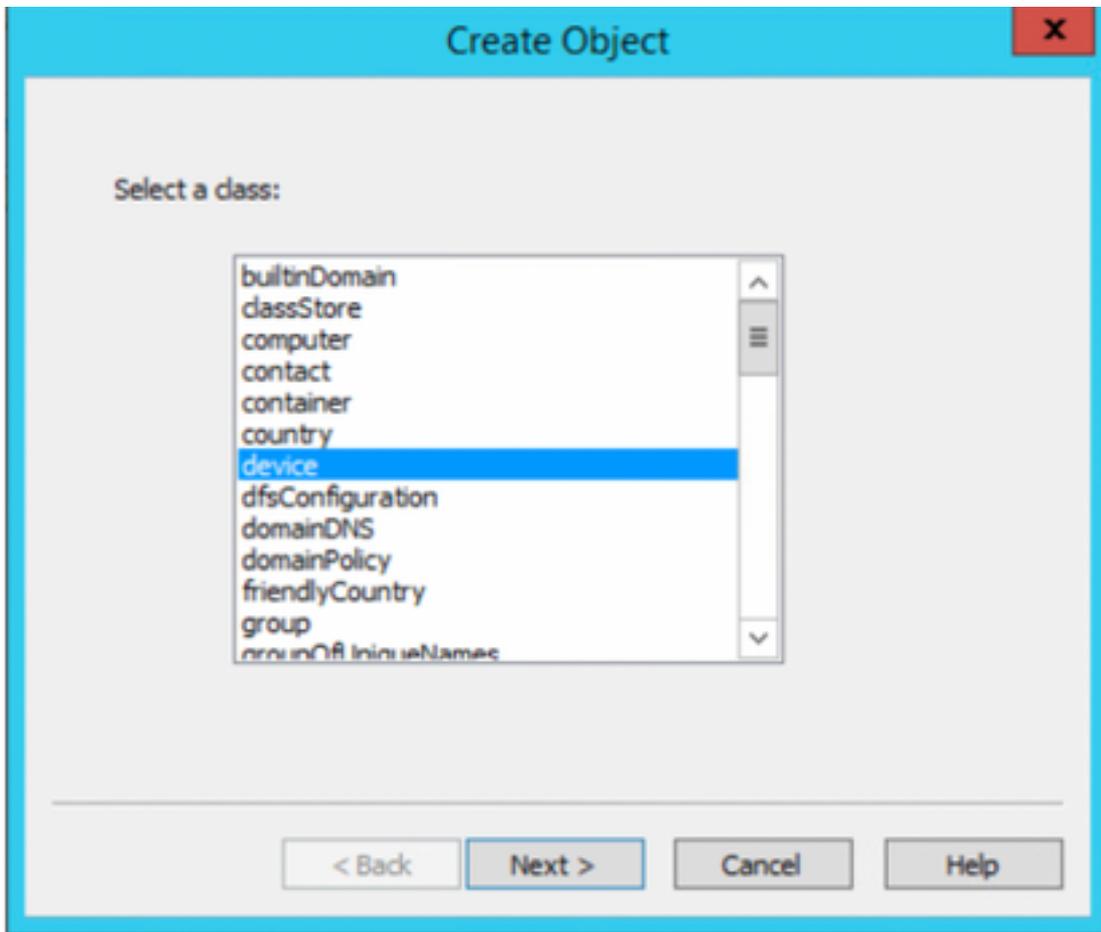
7. Selezionare **Fine** per creare la nuova unità organizzativa



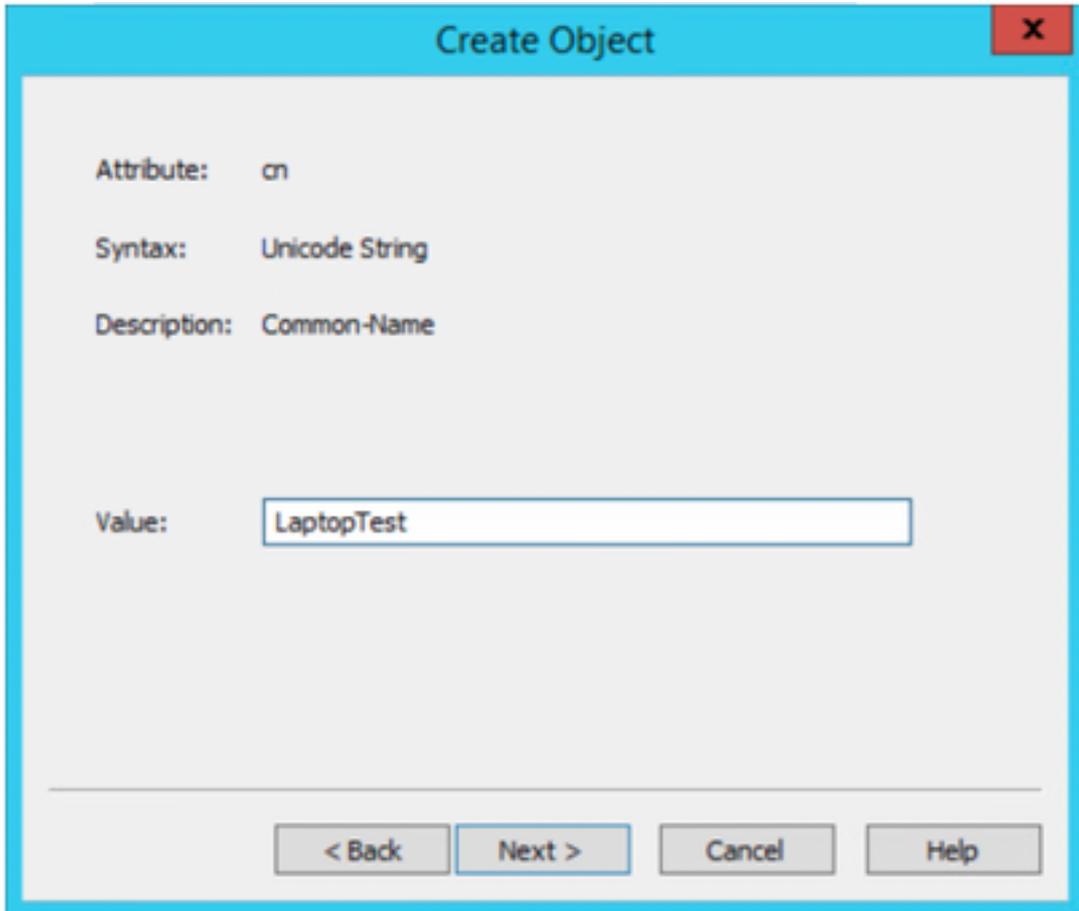
8. Fare clic con il pulsante destro del mouse sull'unità organizzativa appena creata e selezionare **Nuovo > Oggetto**



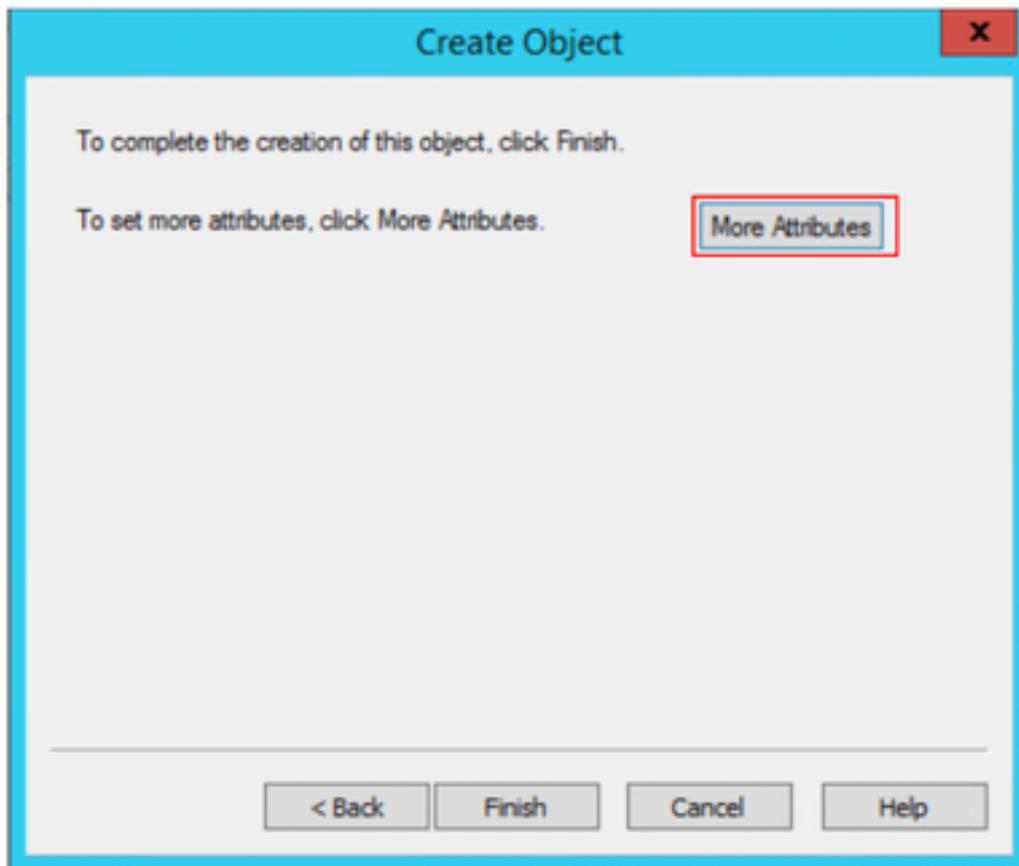
9. Selezionare **device** (dispositivo) come object class (classe oggetto), quindi selezionare **avanti**



10. Definire un nome nel campo Valore e selezionare **Successivo**



11. Selezionare l'opzione **Altri attributi**



11. Per il menu a discesa, **Selezionare una proprietà da visualizzare**, selezionare l'opzione **macAddress**, quindi definire l'indirizzo Mac dell'endpoint che verrà autenticato nel campo **Modifica attributo** e selezionare Pulsante **Aggiungi** per salvare l'indirizzo MAC del dispositivo.

Nota: tra gli ottetti dell'indirizzo MAC è possibile utilizzare due punti anziché punti o trattini.

cn=LaptopTest X

Attributes

Path:

Class: device

Select which properties to view: Optional ▾

Select a property to view: macAddress ▾

Attribute Values

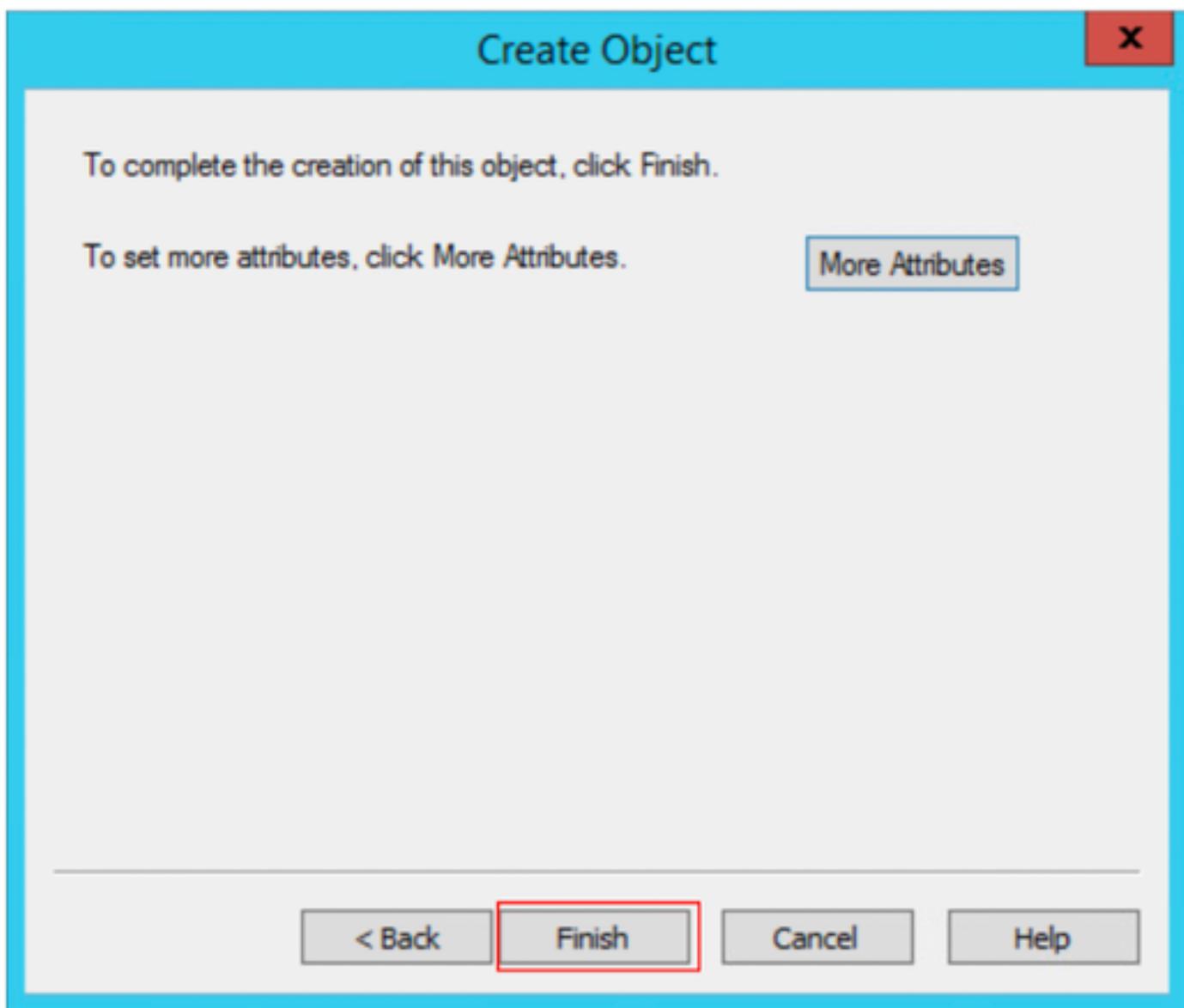
Syntax: IA5String

Edit Attribute: |

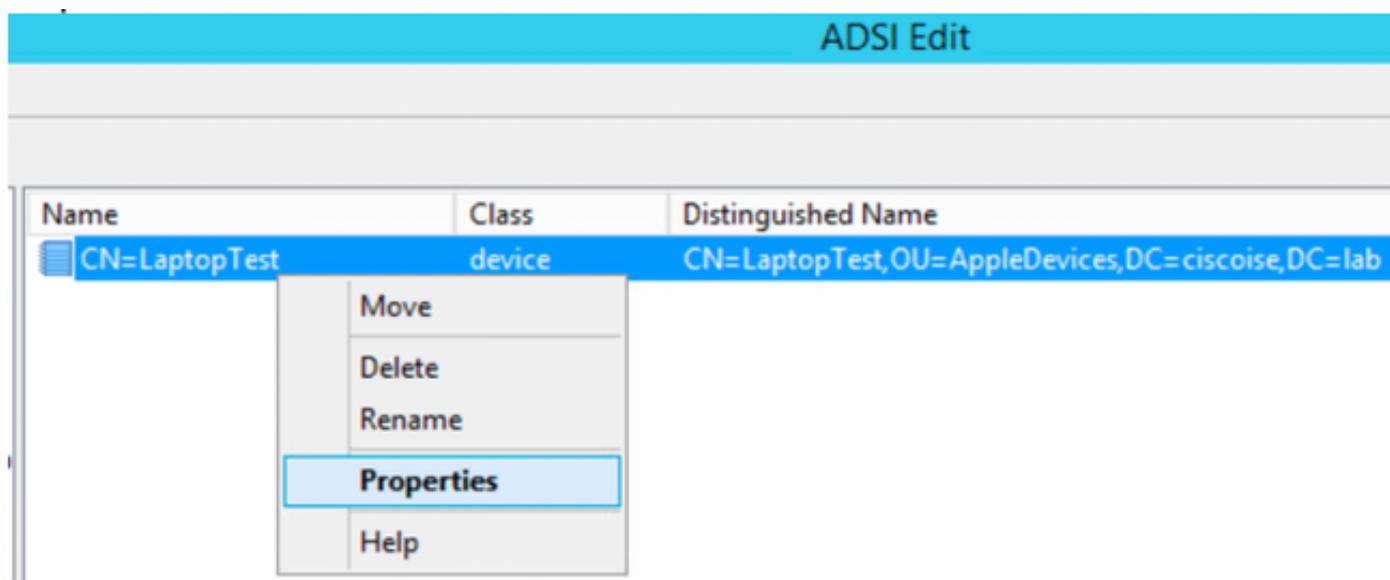
Value(s): 6C:B2:AE:3A:68:6C

12. Selezionare **OK** per salvare le informazioni e continuare con la configurazione dell'oggetto dispositivo

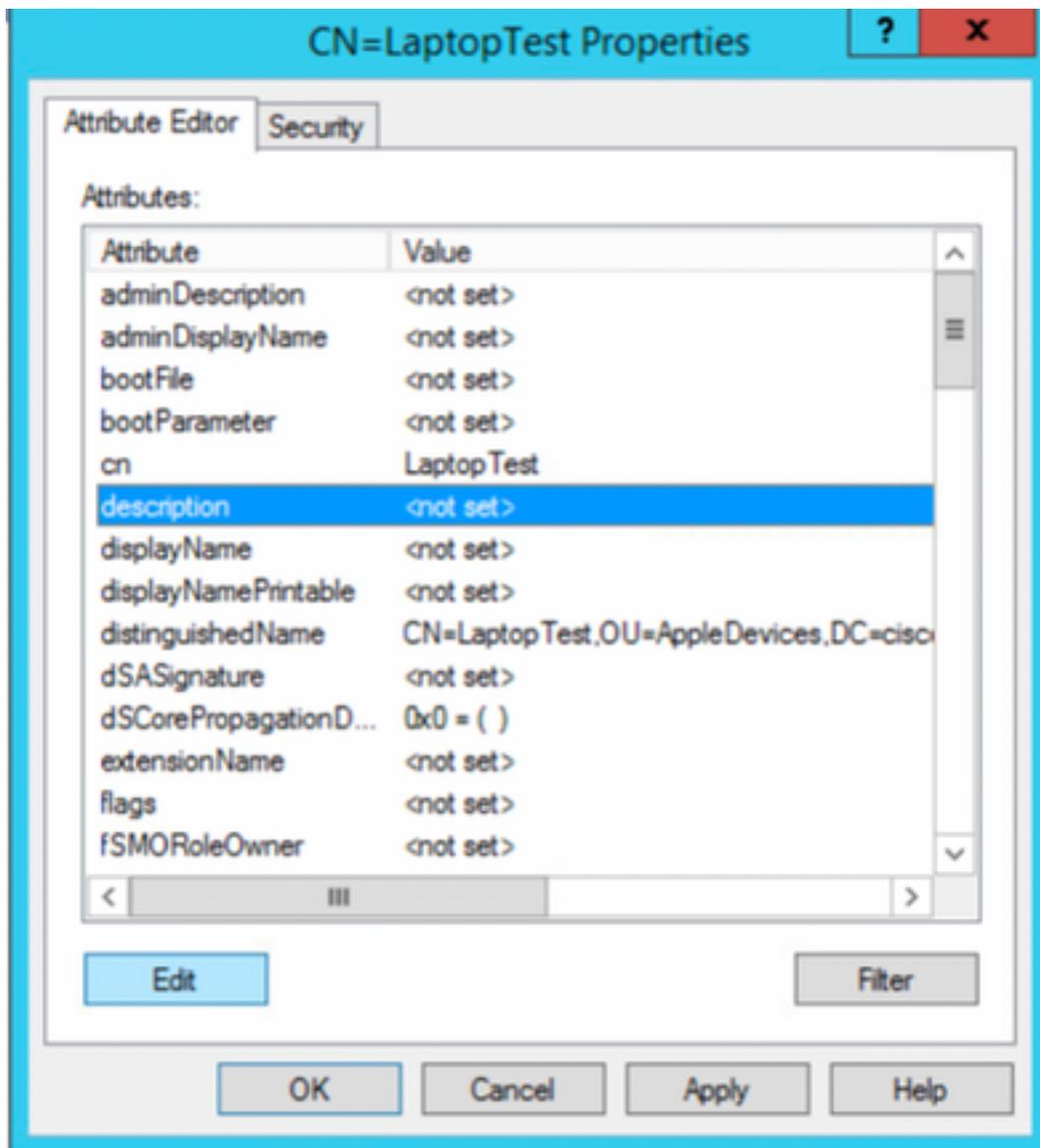
13. Selezionare **Finish** (Fine) per creare il nuovo oggetto dispositivo



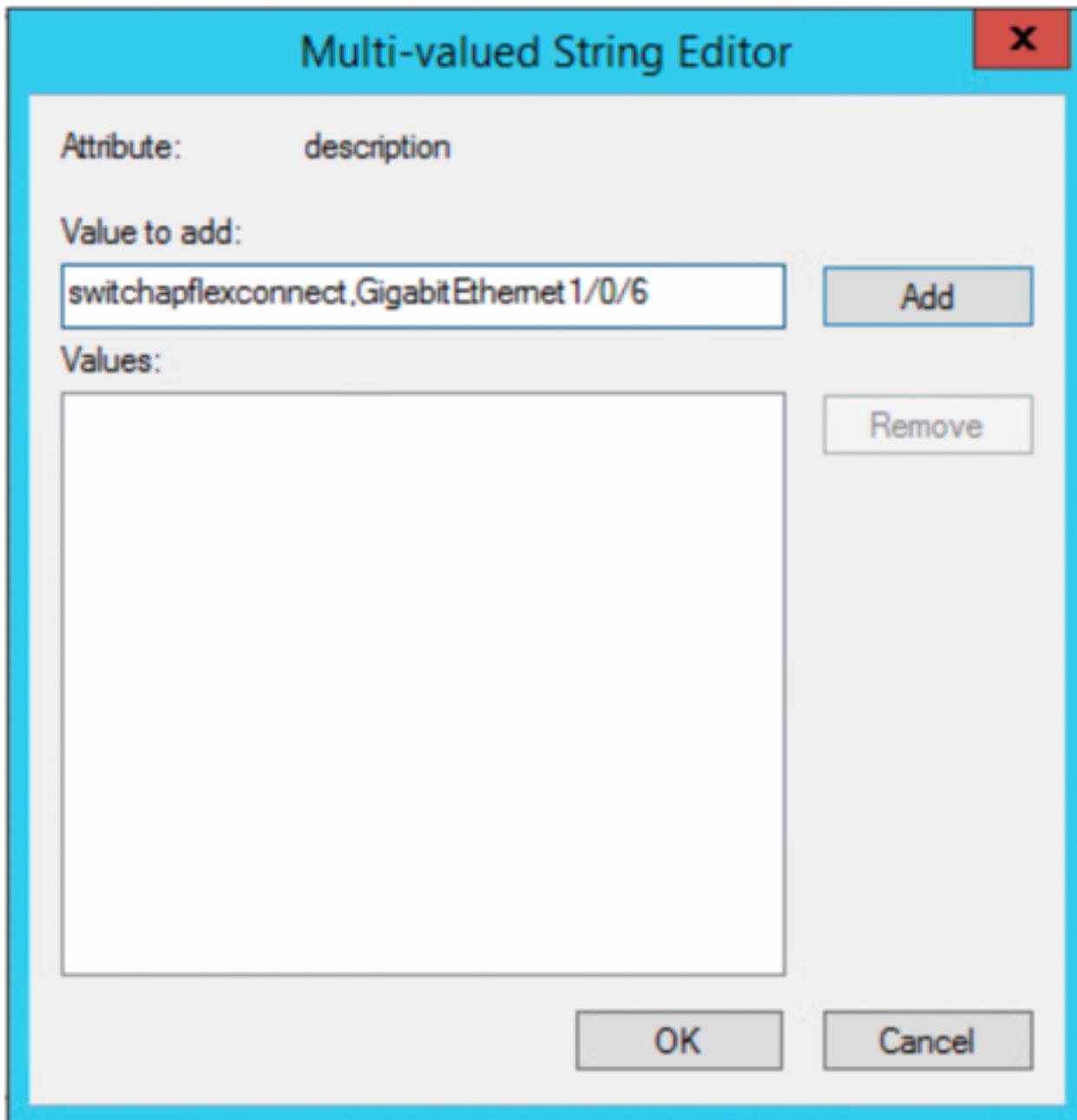
14. Fare clic con il pulsante destro del mouse sull'oggetto dispositivo e selezionare l'opzione **Properties**



15. Selezionare l'opzione **description** (Descrizione) e selezionare **Edit** (Modifica) per definire il nome dello switch e la porta dello switch a cui verrà connesso il dispositivo.



16. Definire il nome dello switch e la porta dello switch. Utilizzare una virgola per separare ciascun valore. Selezionare **Aggiungi**, quindi **OK** per salvare le informazioni.



- Switchapflexconnect è il nome dello switch.
- Gigabit Ethernet1/0/6 è la porta dello switch a cui è connesso l'endpoint.

Nota: È possibile utilizzare gli script per aggiungere attributi a un campo specifico. Tuttavia, in questo esempio i valori vengono definiti manualmente

Nota: L'attributo AD fa distinzione tra maiuscole e minuscole, se si utilizzano tutti gli indirizzi Mac in lettere minuscole, ISE viene convertito in lettere maiuscole durante la query LDAP. Per evitare questo comportamento, disabilitare Ricerca host processi nei protocolli consentiti. Ulteriori informazioni sono disponibili al seguente link: https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

Configurazione degli switch

Di seguito viene descritta la configurazione della comunicazione 802.1x tra ISE e lo 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
```

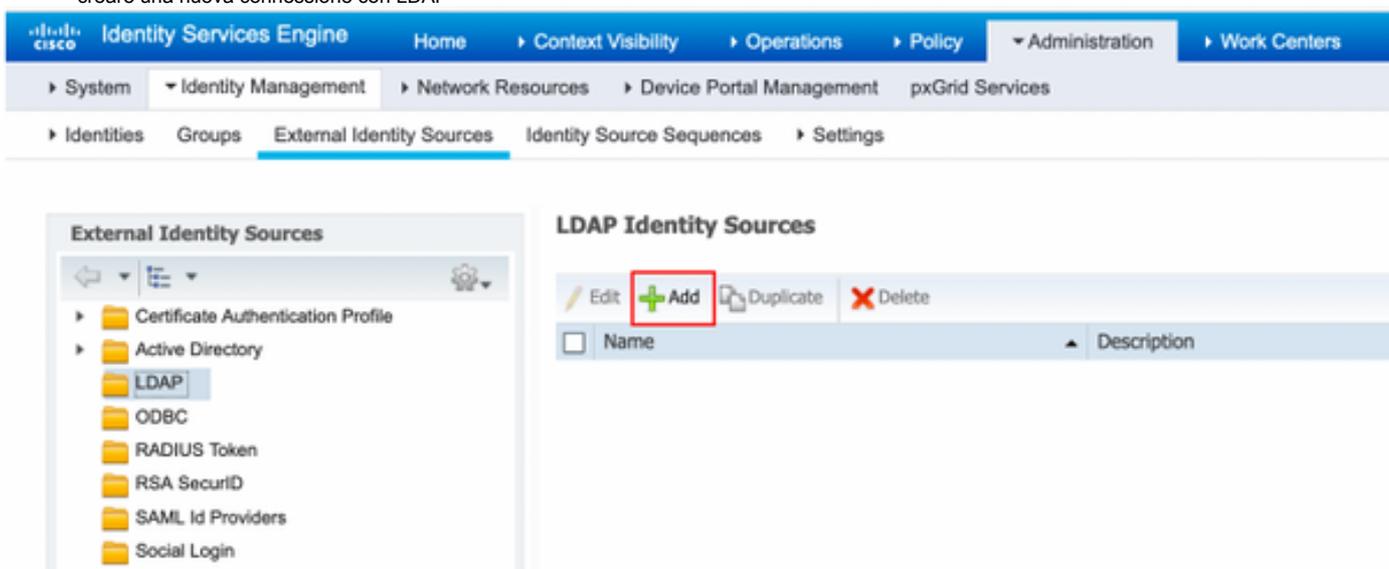
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access 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: Potrebbe essere necessario modificare la configurazione globale e dell'interfaccia nell'ambiente in uso

Configurazione di ISE

Di seguito viene descritta la configurazione di ISE per ottenere gli attributi dal server LDAP e configurare le policy ISE.

1. Ad ISE, andare in **Amministrazione->Gestione delle identità->Origini delle identità esterne** e selezionare la cartella **LDAP** e fare clic su **Aggiungi** per creare una nuova connessione con 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 panes. The left pane, 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 pane, 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. In **Generale**, definire un nome e selezionare l'indirizzo mac come Attributo nome soggetto

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. In **Connessione** configurare l'indirizzo IP, il DN di amministrazione e la password del server LDAP per ottenere una connessione riuscita.

LDAP Identity Source

General Connection Directory Organization Groups Attributes Advanced Settings

Primary Server Secondary Server

Enable Secondary Server

* Hostname/IP ⓘ

* Port

Hostname/IP ⓘ

Port

Specify server for each ISE node

Access Anonymous Access

Authenticated Access

Admin DN ⓘ

Password

Admin DN ⓘ

Password

Secure Authentication Enable Secure Authentication

Enable Server Identity Check

Secure Authentication Enable Secure Authentication

Enable Server Identity Check

LDAP Server Root CA ⓘ

Issuer CA of ISE Certificates ⓘ

LDAP Server Root CA ⓘ

Issuer CA of ISE Certificates ⓘ

Save Reset

Nota: La porta 389 è la porta predefinita utilizzata.

4. In **Attributi** scheda selezionare gli attributi macAddress e description, questi attributi verranno utilizzati nel criterio di autorizzazione

LDAP Identity Source

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

Edit **+** Add **X** 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. Per creare un protocollo consentito, passare a **Criterio->Elementi della policy->Risultati->Autenticazione->Protocolli consentiti**. Definire e selezionare Process Host Lookup e Allow PAP/ASCII come gli unici protocolli consentiti. Infine, selezionare **Salva**

Allowed Protocols Services List > MAB_MacAddress

Allowed Protocols

Name:

Description:

Allowed Protocols

Authentication Bypass

Process Host Lookup

Authentication Protocols

Allow PAP/ASCII

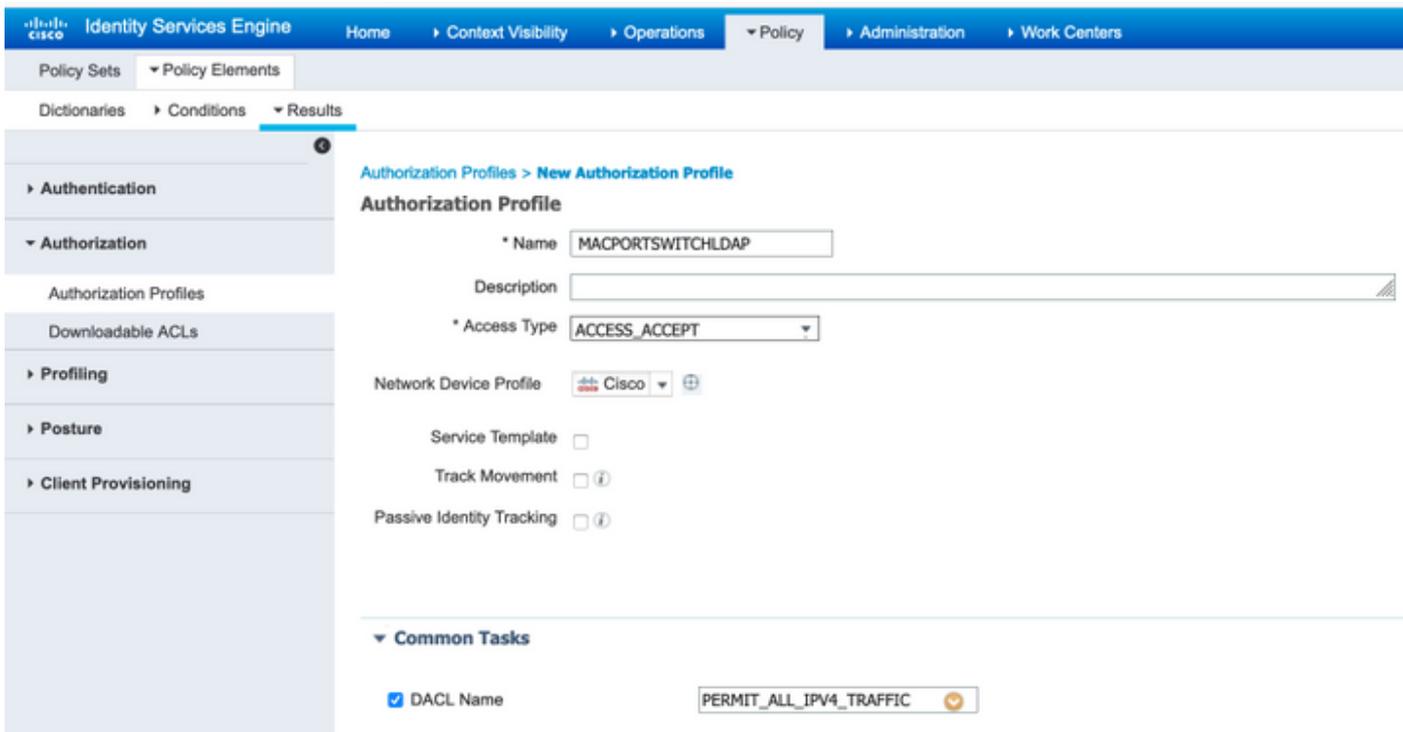
6. Per creare un profilo di autorizzazione, passare a **Criteri->Elementi criteri->Risultati->Autorizzazione->Profili di autorizzazione**. Selezionare **Aggiungi** e definire le autorizzazioni da assegnare all'endpoint.

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit **+** Add Duplicate **X** Delete

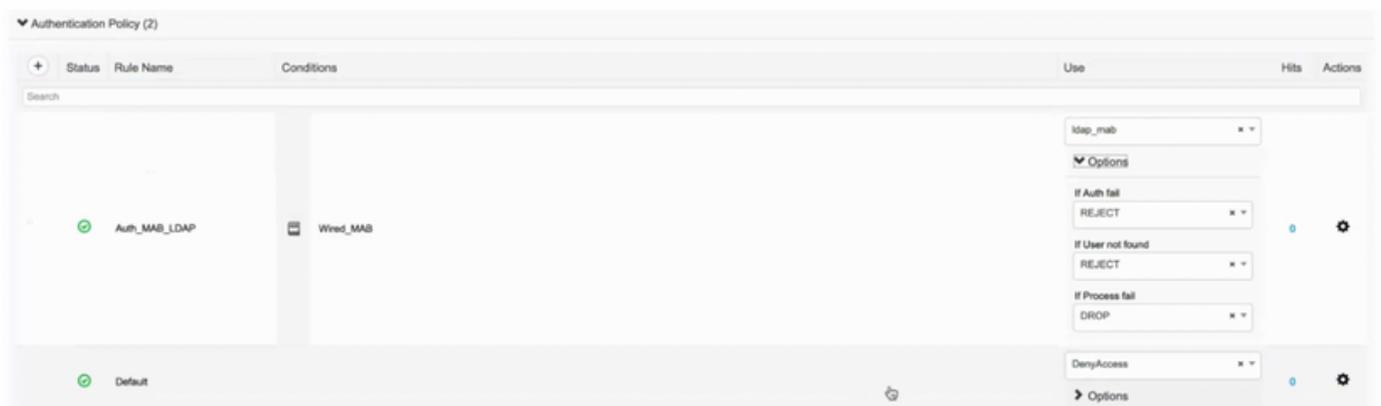
<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco
<input type="checkbox"/>	Cisco_IP_Phones	Cisco
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco



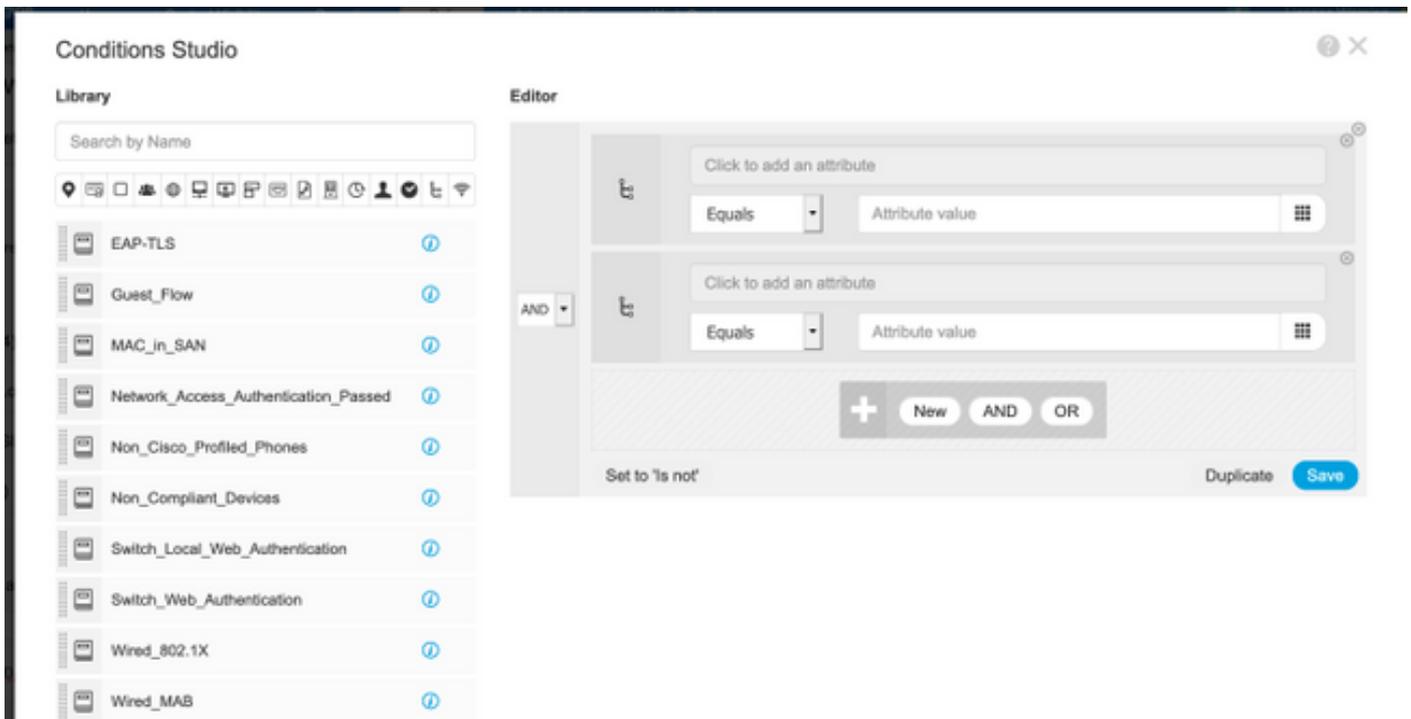
7. Andare a Policy-> Policy Set e creare un set di criteri usando la condizione predefinita Wired_MAB e il protocollo consentito creato nel passaggio 5.



8. Sotto il nuovo set di criteri creato creare un criterio di autenticazione utilizzando la libreria **Wired_MAB** predefinita e la connessione **LDAP** come sequenza di origine dell'identità esterna



9. In **Criteri di autorizzazione** definire un nome e creare una condizione composta utilizzando la descrizione dell'attributo LDAP, Radius NAS-Port-Id e NetworkDeviceName. Infine, aggiungere il profilo di autorizzazione creato nel passaggio 6.



Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
✓	MAB_LDAP	AND	<ul style="list-style-type: none"> 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	⚙️

Dopo aver applicato la configurazione, è possibile connettersi alla rete senza l'intervento dell'utente.

Verifica

Una volta connessi alla porta dello switch designata, è possibile digitare **show authentication session interface Gigabit Ethernet X/X/X details** per convalidare lo stato di autenticazione e autorizzazione 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_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
ISE consente di usare Radius Live Logs per la conferma.
```

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		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

Risoluzione dei problemi

Sul server LDAP, verificare che l'indirizzo Mac, il nome dello switch e la porta dello switch del dispositivo creato siano stati configurati correttamente

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

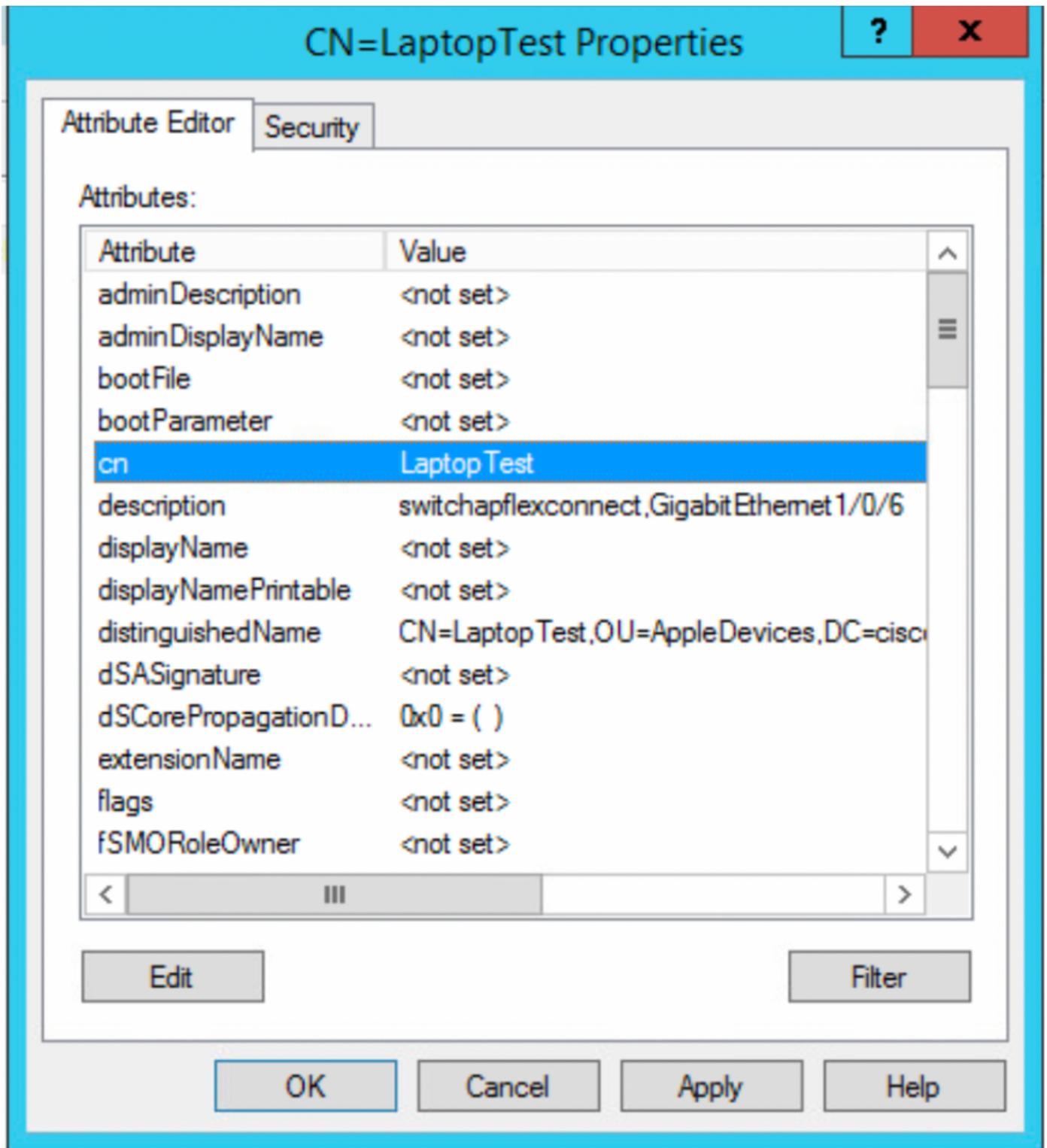
Filter

OK

Cancel

Apply

Help



Ad ISE, è possibile acquisire un pacchetto (andare a **Operazioni->Risoluzione dei problemi->Strumento diagnostico->Dump TCP**) per verificare che i valori vengano inviati da LDAP ad ISE

```

27 124.208890 18.85.127.189 18.85.127.111 LDAP 231 searchRequest(2) "(&(&appflexconnect,GigabitEthernet1/0/6)) who/subject=
28 124.208927 18.85.127.111 18.85.127.189 LDAP 232 searchResultEntry(2) "(&(&appflexconnect,GigabitEthernet1/0/6)) | searchResultEntry(2) success
29 124.325271 18.85.127.189 18.85.127.111 LDAP 233 searchRequest(3) "(&(&appflexconnect,GigabitEthernet1/0/6)) who/subject=
30 124.325283 18.85.127.111 18.85.127.189 LDAP 232 searchResultEntry(3) "(&(&appflexconnect,GigabitEthernet1/0/6)) | searchResultEntry(3) success
31 124.325373 18.85.127.189 18.85.127.111 LDAP 233 searchRequest(4) "(&(&appflexconnect,GigabitEthernet1/0/6)) who/subject=
32 124.325384 18.85.127.111 18.85.127.189 LDAP 36 searchResultEntry(4) success (2 results)
33 124.489445 18.85.127.189 18.85.127.111 LDAP 389 searchRequest(5) "(&(&appflexconnect,GigabitEthernet1/0/6)) who/subject=
34 124.489456 18.85.127.111 18.85.127.189 LDAP 389 searchResultEntry(5) success (2 results)
-----
* attributes: 3 items
  * PartOfAttributeList: 1 item description
    Type: description
    Value: 3 item
    AttributeList: switchflexconnect,GigabitEthernet1/0/6
  * PartOfAttributeList: 1 item distinguishedName
    Type: distinguishedName
    Value: 3 item
    AttributeList: CN=LaptopTest,OU=AppleDevices,DC=cisco
  * PartOfAttributeList: 1 item ipAddress
    Type: ipAddress
    Value: 3 item
    AttributeList: 18.82.42.34-18.82

```