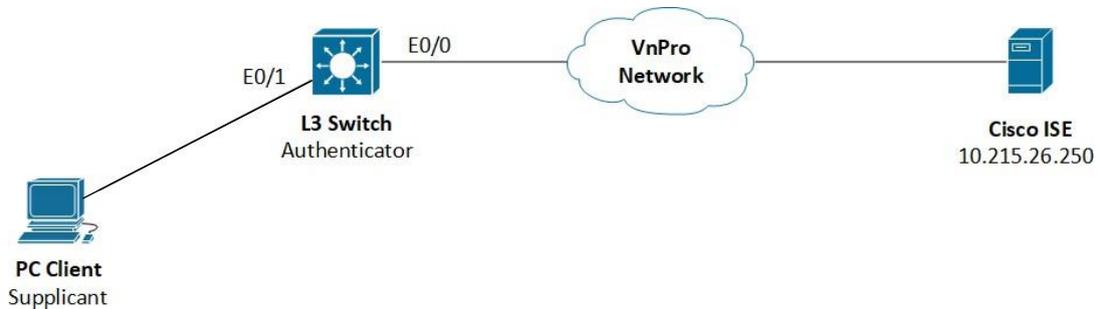


## LAB : CẤU HÌNH XÁC THỰC 802.1X VỚI WIRED LAN

### I. Sơ đồ



Hình 1: Sơ đồ bài Lab

### II. Yêu cầu

#### 2.1. Cấu hình trên Switch

Đối với các sw hoạt động Version 12.2 ta cấu hình như sau:

```
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
```

// cấu hình 802.1X trên cổng Switch

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#spanning-tree portfast
```

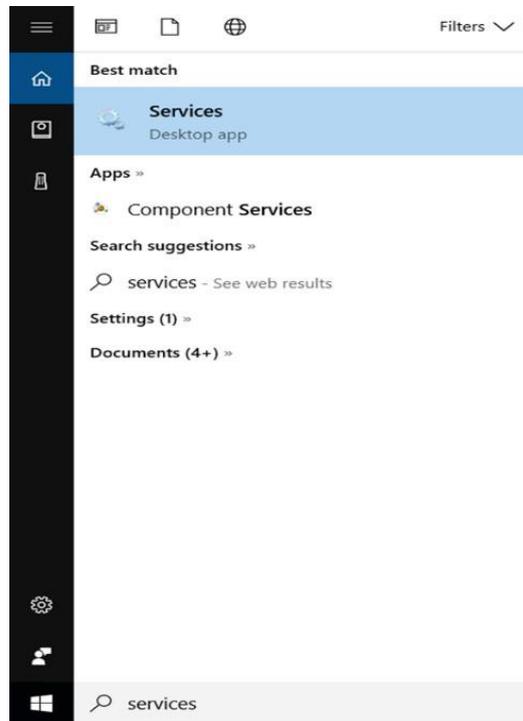
- Khai báo Radius Server

```
Switch(config)#radius-server host 10.215.26.50 // tạo shared key
                                                trên Switch
Switch(config)#radius-server key VnPro123
```

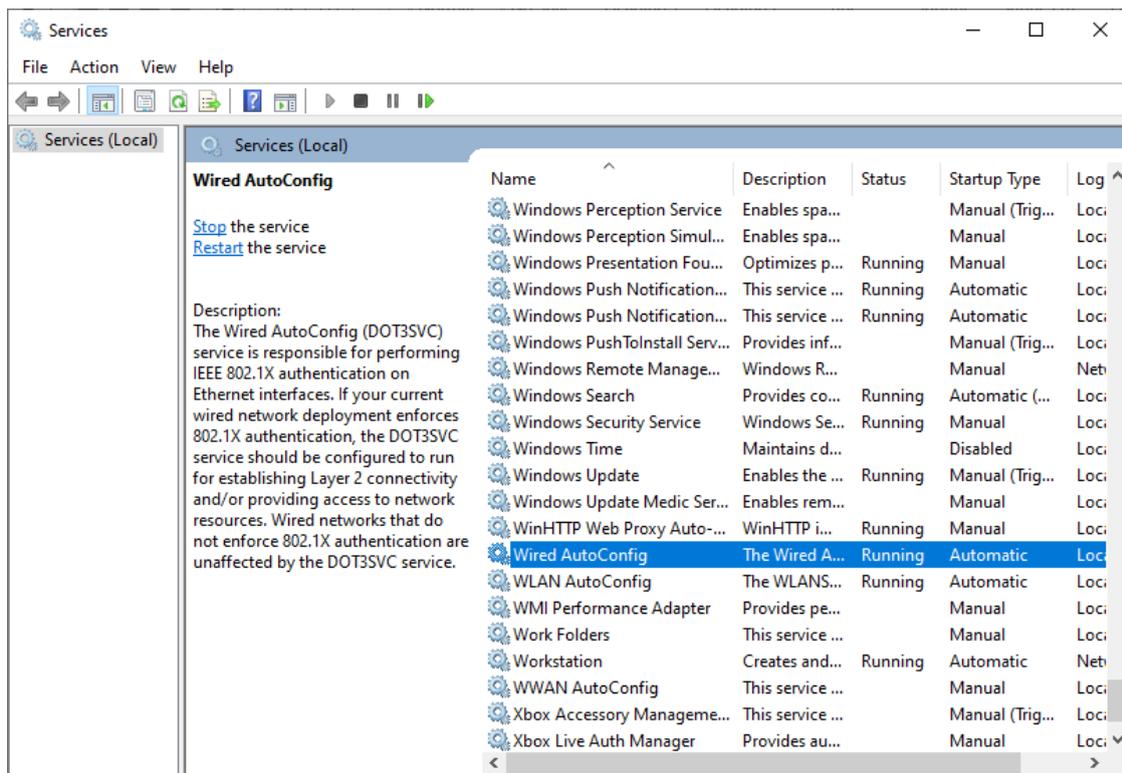
*Trên Windows 10*

Cấu hình bật xác thực 802.1x trên Window 10 như sa

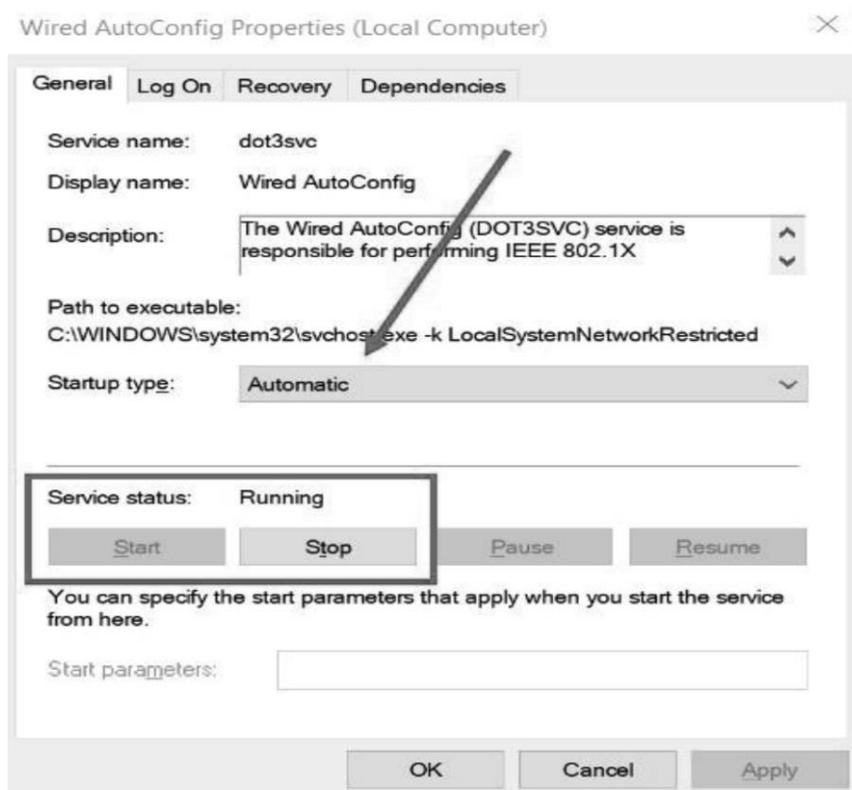
Tim Services:



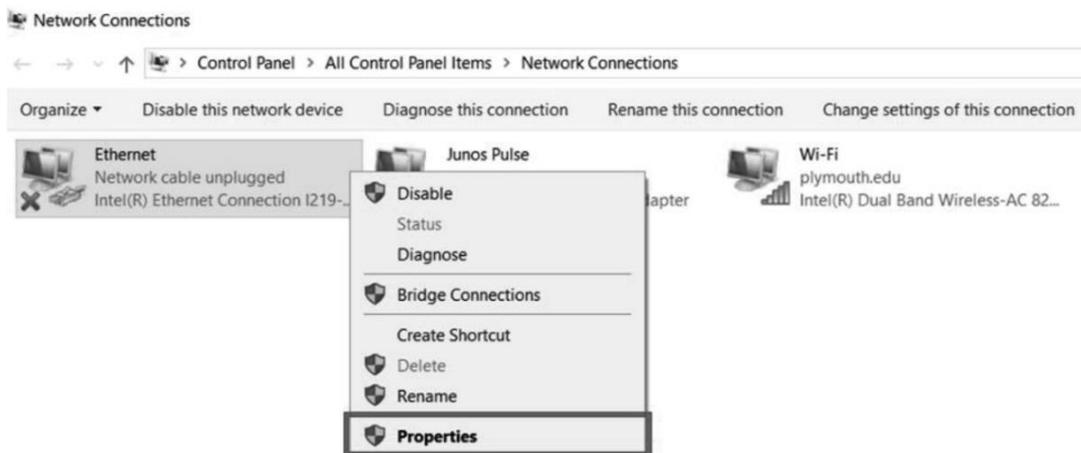
Tim và double click vào Wired AutoConfig:



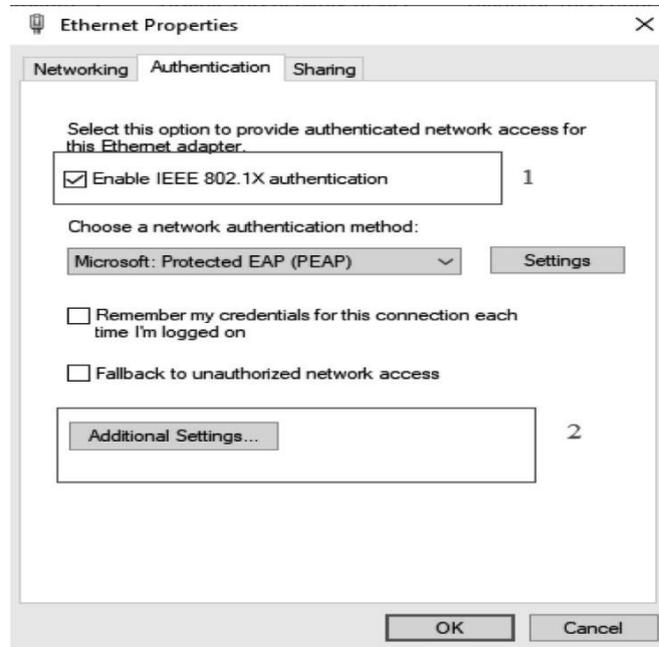
- Khởi động dịch vụ



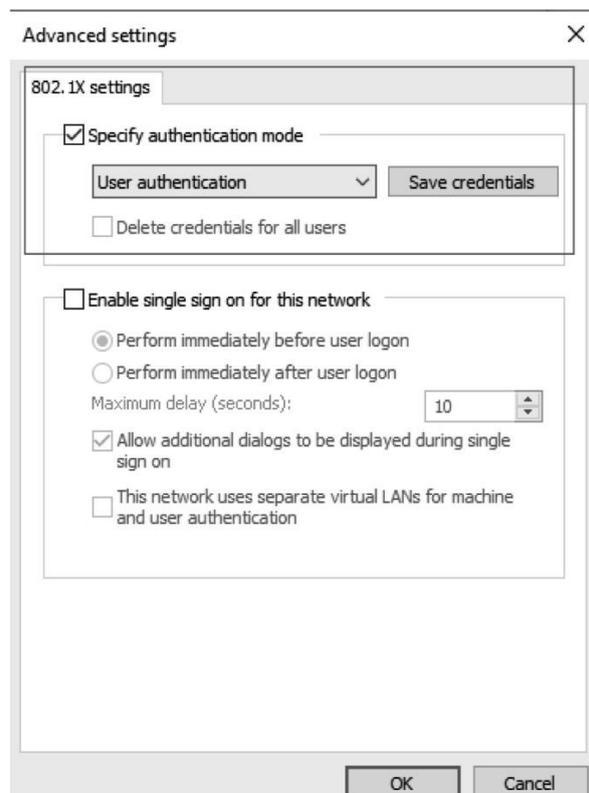
Tiếp theo, mở CMD gõ `nca.cpl` để vào Network Connections, click chuột phải vào Card mạng Ethernet → chọn Properties:



Tại tab Authentication, tích Enable IEEE 802.1X authentication (1):



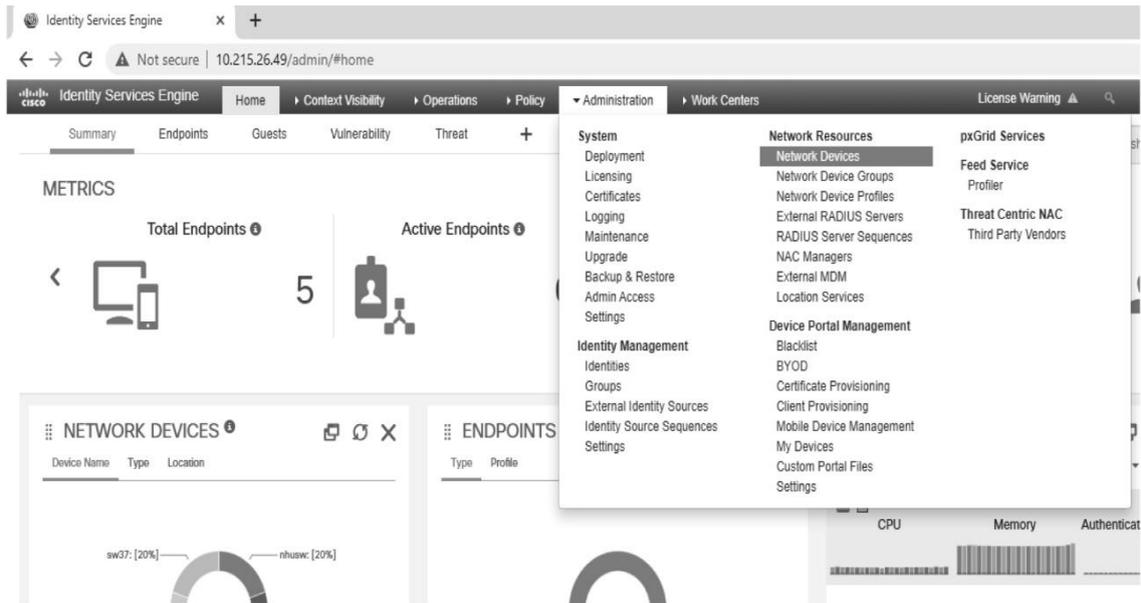
Tiếp tục chọn Additional Settings (2) chọn xác thực bằng user authentication và chọn ok để lưu lại:



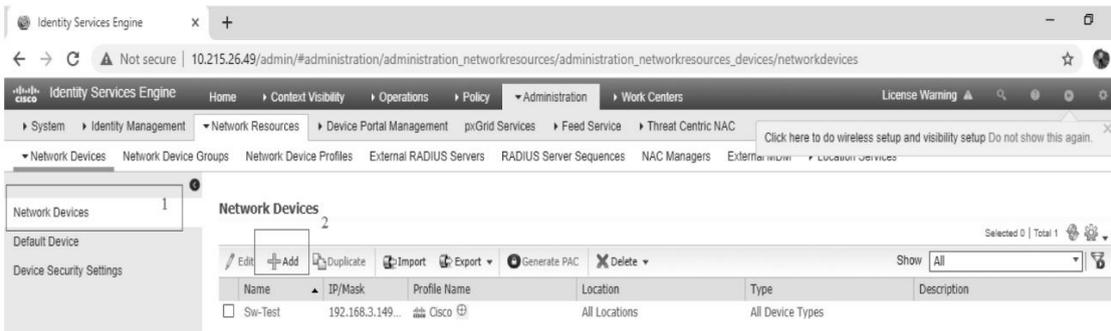
## Cấu hình Radius trên Cisco ISE

- Khai báo thiết bị để kết nối với Radius Server như sau:

Đầu tiên ở mục Administration chọn Network Devices:



Thực hiện thêm vào thiết bị. Các thiết bị được thêm vào là radius client:



Tiến hành khai báo thông tin như sau:

Identity Services Engine

10.215.26.49/admin/#administration/administration\_networkresources/administration\_networkresources\_devices/networkdevices

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External RADIUS Servers Location Services

Network Devices List > Sw-Test Đặt tên cho thiết bị

Network Devices

\* Name Sw-Test

Description

IP Address \* IP: 192.168.3.149 / 32 Khai báo địa chỉ IP của thiết bị

IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected

\* Device Profile Cisco

Model Name

Software Version

\* Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

Tiếp theo chọn Radius Authentication Settings để cấu hình Radius Server, tiếp theo khai báo Shared Secret cho Radius Server (Lưu ý share key phải giống nhau trên Switch và Radius) sau đó chọn Submit để lưu cấu hình:

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External RADIUS Servers Location Services

Network Devices

Default Device

Device Security Settings

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

\* Shared Secret \*\*\*\*\* Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/dtls

CoA Port 2083 Set To Default

Issuer CA of ISE Certificates for CoA Select if required (optional)

DNS Name

General Settings

Enable KeyWrap

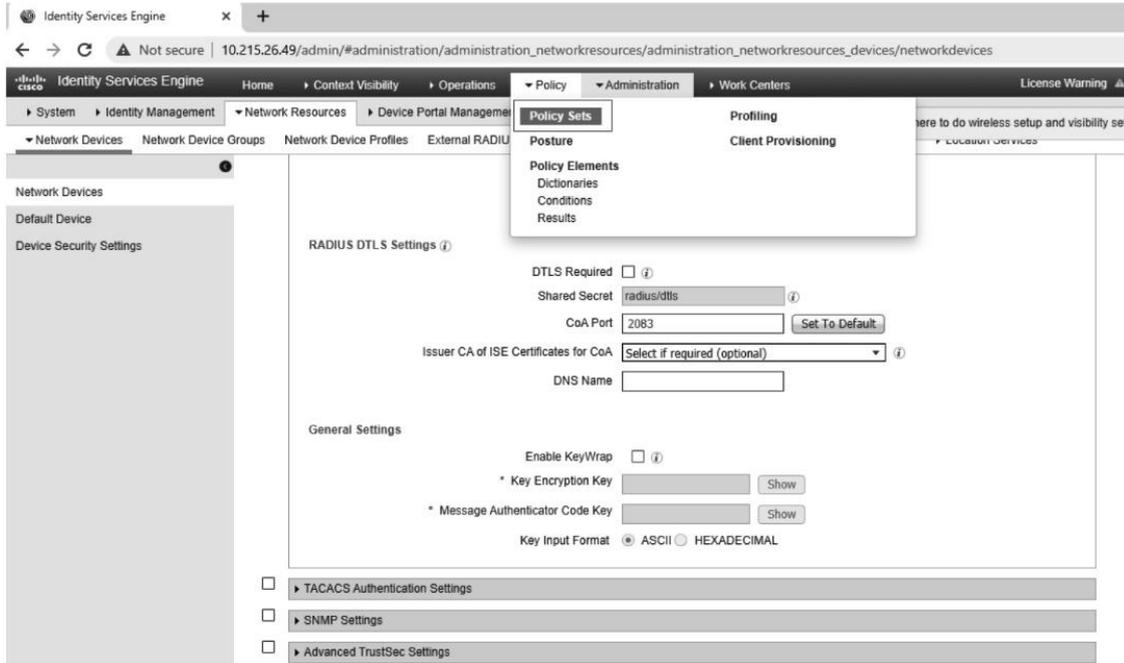
\* Key Encryption Key Show

\* Message Authenticator Code Key Show

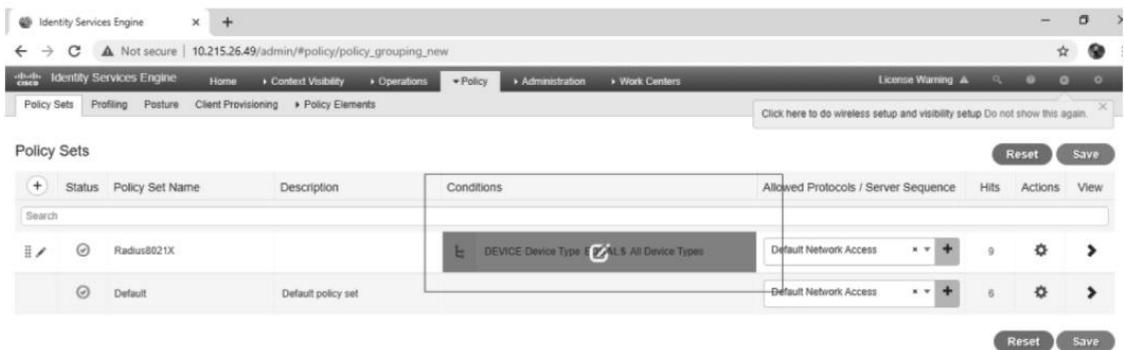
Key Input Format ASCII HEXADECIMAL

- Tạo policy:

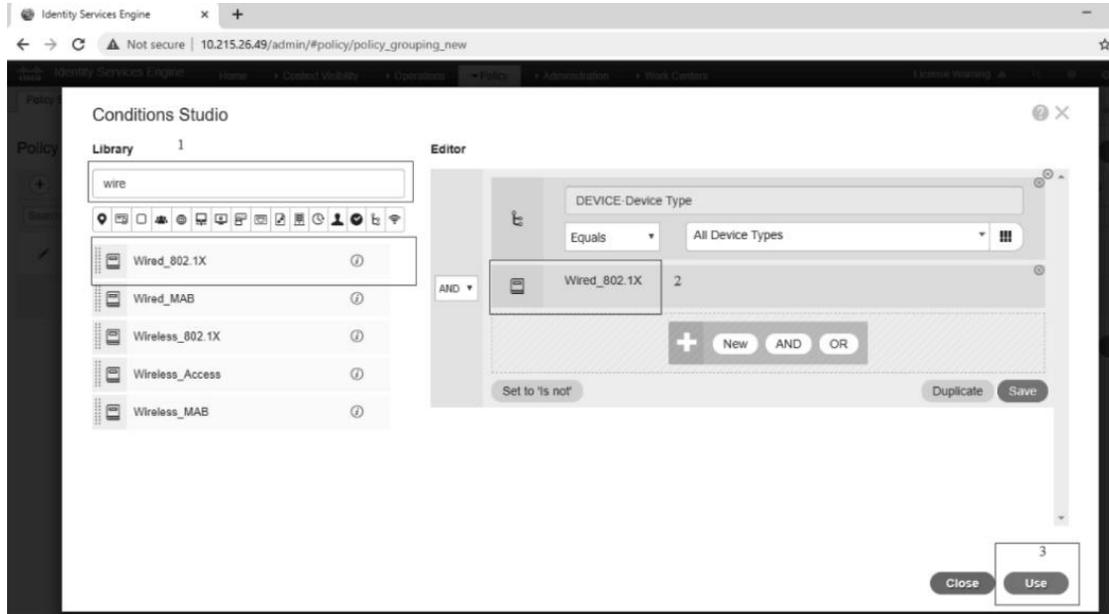
Chọn Policy Sets:



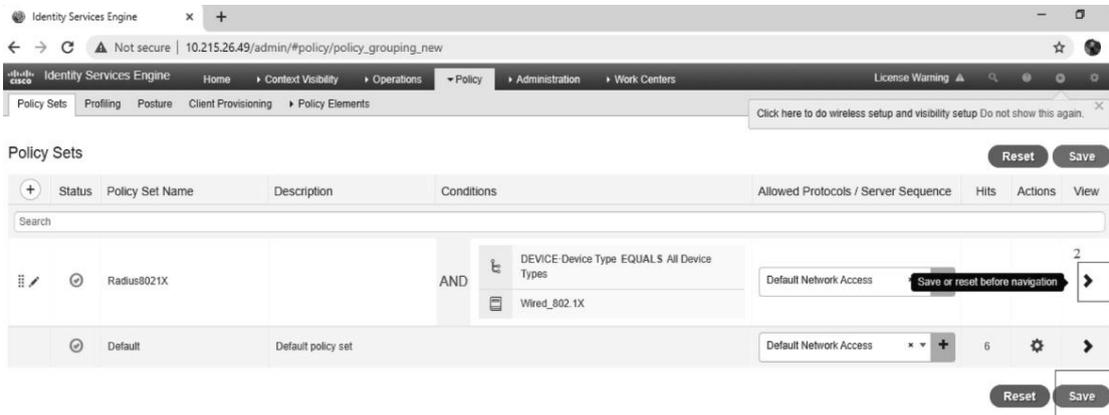
Click vào biểu tượng cây bút để cấu hình xác thực mạng có dây với 802.1x:



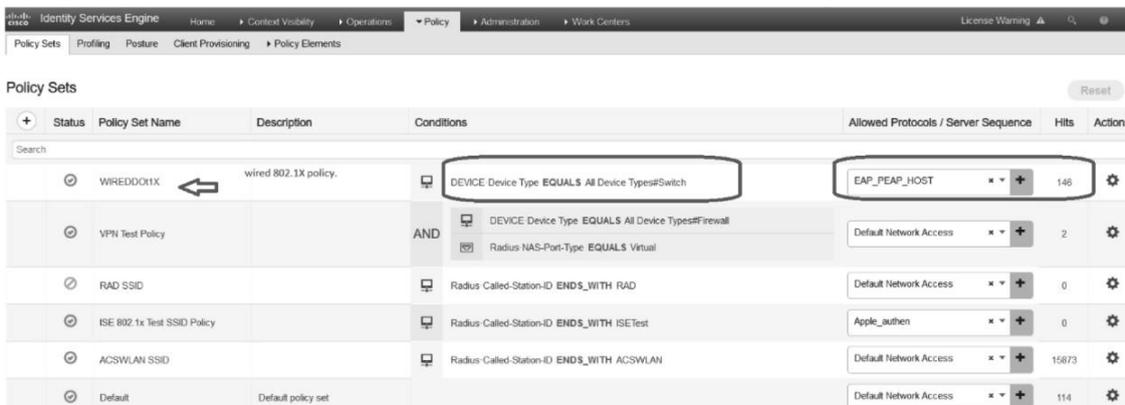
Tại mục Library tìm wired\_802.1X và kéo vào mục editor bấm Use:



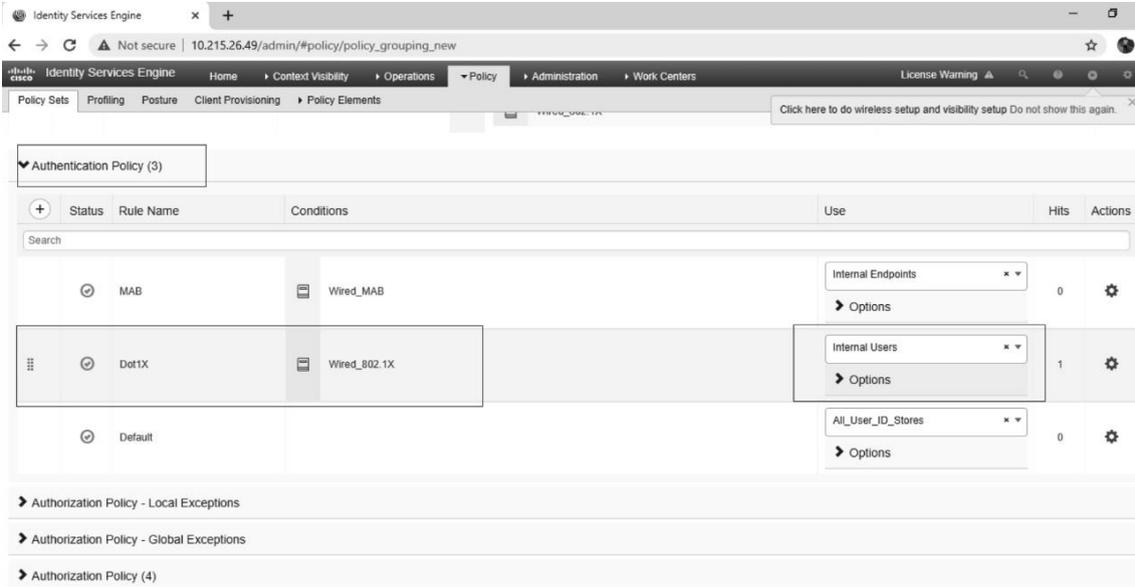
Sau khi xong tiến hành lưu lại và tiếp tục cấu hình cho Policy này như sau:



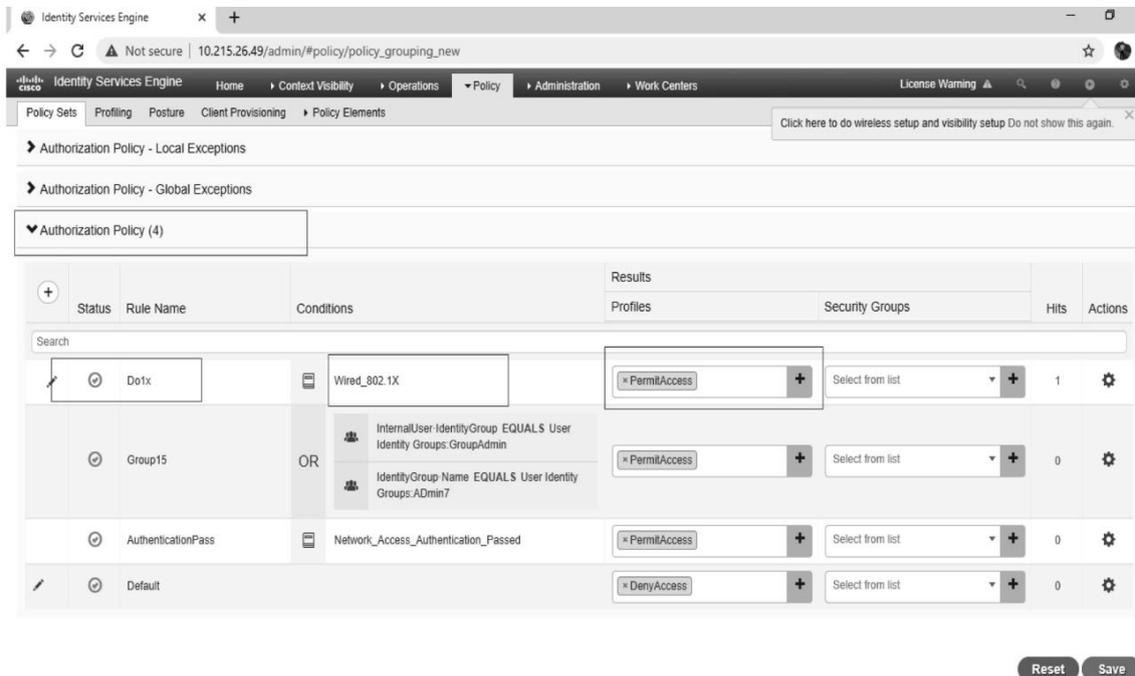
Điều kiện để chính sách được kích hoạt là thiết bị này thuộc về kiểu switch:



Tại mục authentication policy, ta làm như sau:



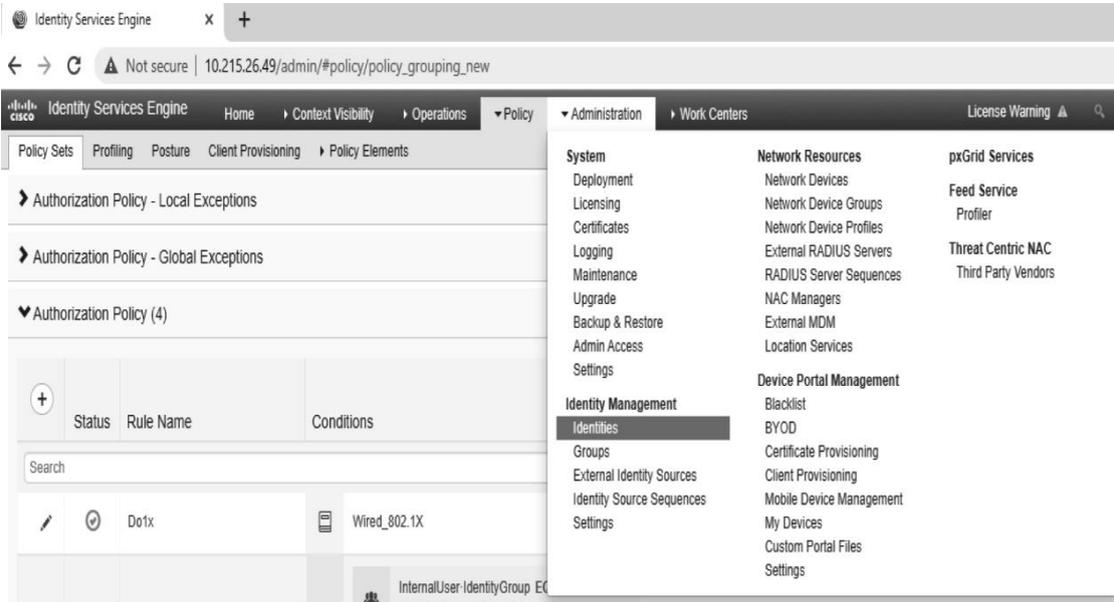
Tiếp tục tạo Policy như sau, đây là nơi đưa ra các authorization (thẩm quyền) cho người dùng sau quá trình xác thực:



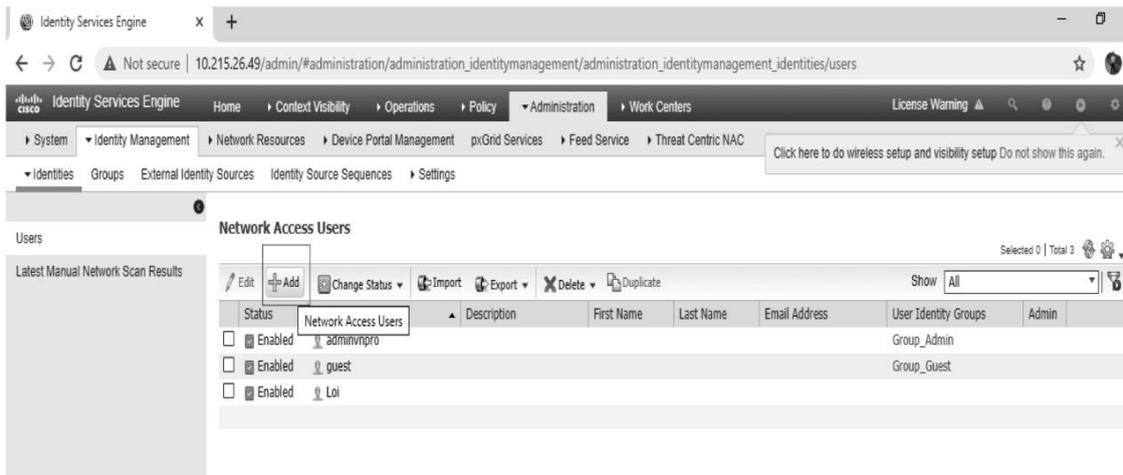
Chọn Save để lưu lại chính sách sau khi thay đổi xong.

- Tạo username và password trên Radius Server để xác thực trong mạng có dây:

Tại mục Administrator chọn Identities:



Chọn ADD để tạo User:



Điền thông tin username và Password:

*Lưu ý:* Password phải đủ mạnh: bao gồm các kí tự chữ hoa, chữ thường và kí tự đặc biệt.