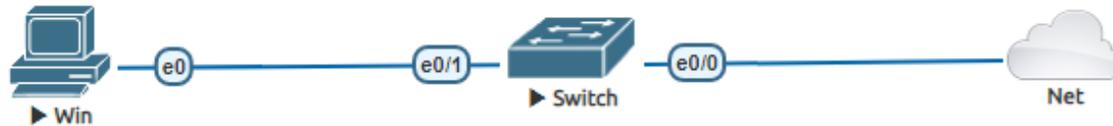


Lab – Cấu hình xác thực 802.1X với wired LAN



Mô tả:

Bài lab này có thể được thực hiện trên LAB giả lập sử dụng các IOL Switch i86bi_linux_12-advipservicesk9, qemu win-7-x86-IPCC

Switch kết nối với đám mây net, trong đám mây sẽ là hệ thống mạng, có Cisco ISE, DHCP Server cấp IP cho thiết bị

Trong bài Lab này học viên thực hiện cấu hình xác thực 802.1x trên Switch sử dụng Cisco ISE

1. Cấu hình trên Switch

```
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#interface Ethernet 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
Switch(config-if)#exit
Switch(config)#interface vlan 1
Switch(config-if)#ip address dhcp
Switch(config-if)#no shutdown
```

```
Switch#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	unset	up	up
Ethernet0/1	unassigned	YES	unset	up	up
Ethernet0/2	unassigned	YES	unset	up	up
Ethernet0/3	unassigned	YES	unset	up	up
Vlan1	192.168.3.149	YES	DHCP	up	up

- Khai báo Radius Server

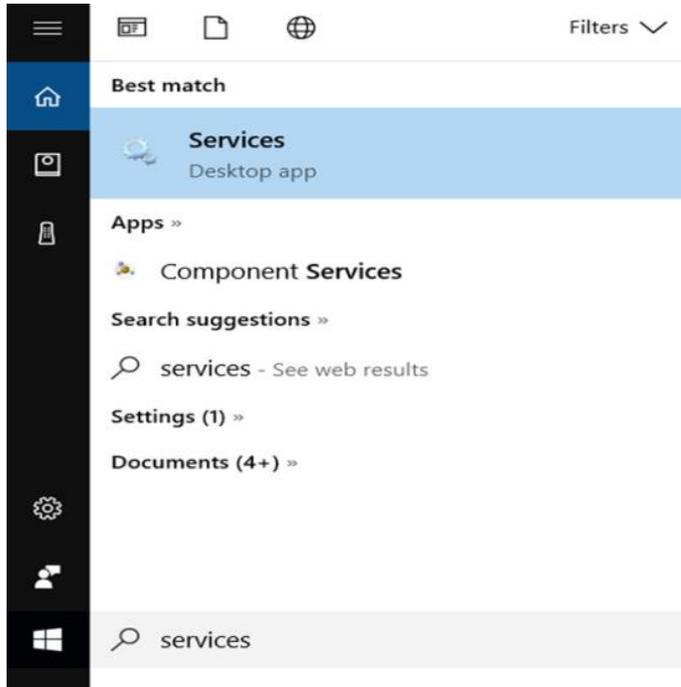
```
Switch(config)#radius-server host 10.215.26.50
```

```
Switch(config)#radius-server key VnPro123
```

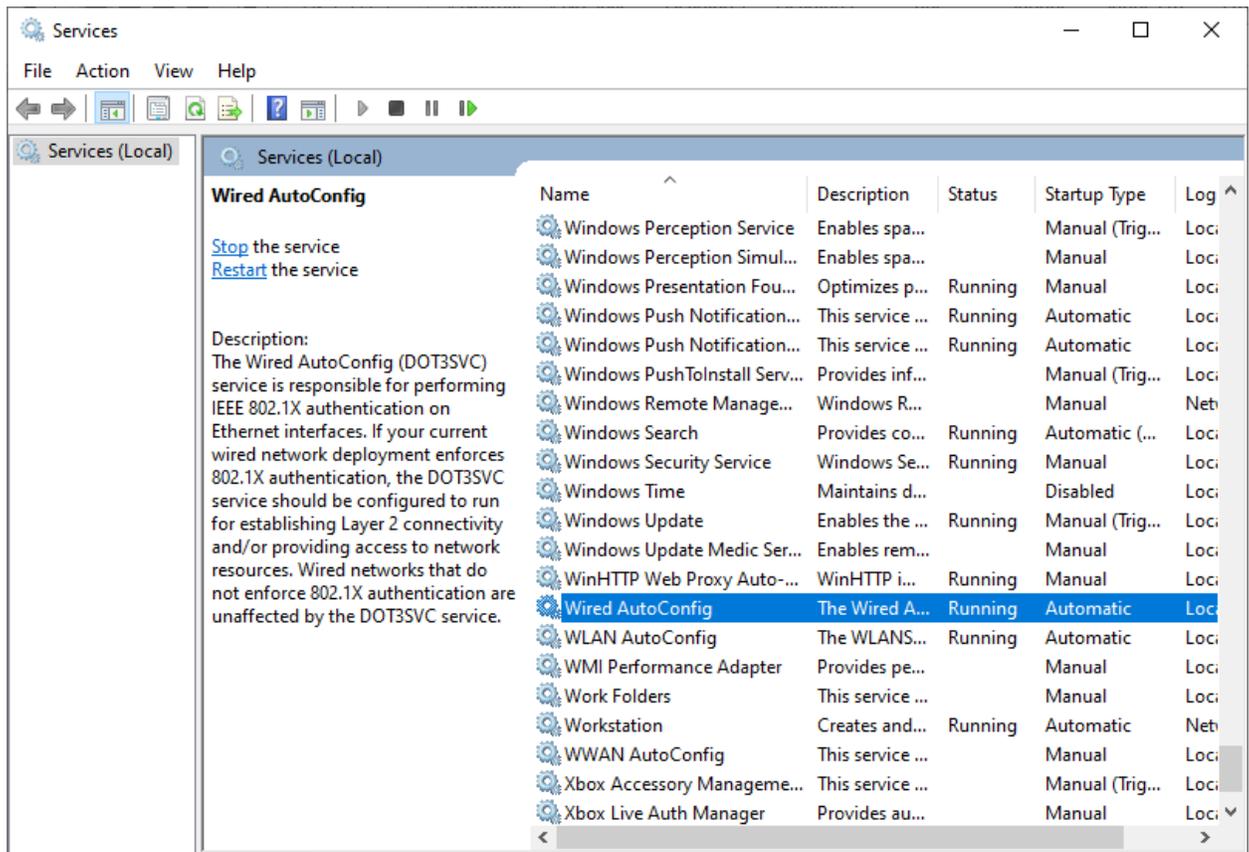
2. Cấu hình trên Windows 10

Cấu hình bật xác thực 802.1x trên Window 10 như sau:

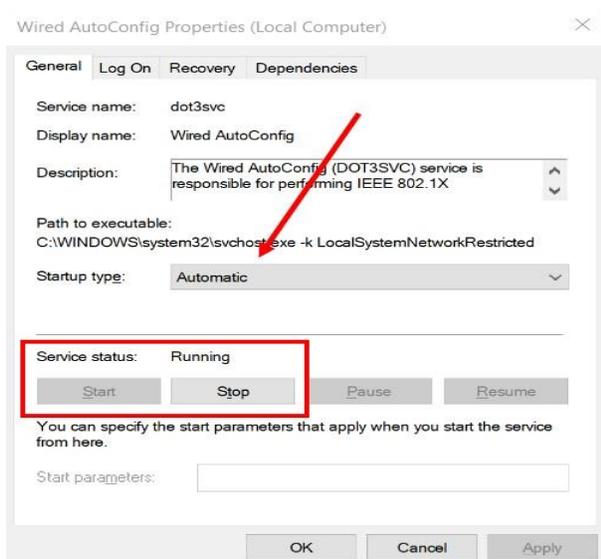
- Tìm Services



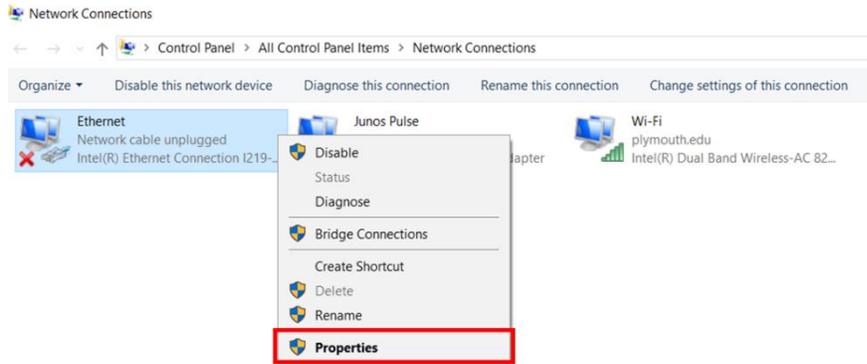
Tìm và double click vào **Wire AutoConfig**



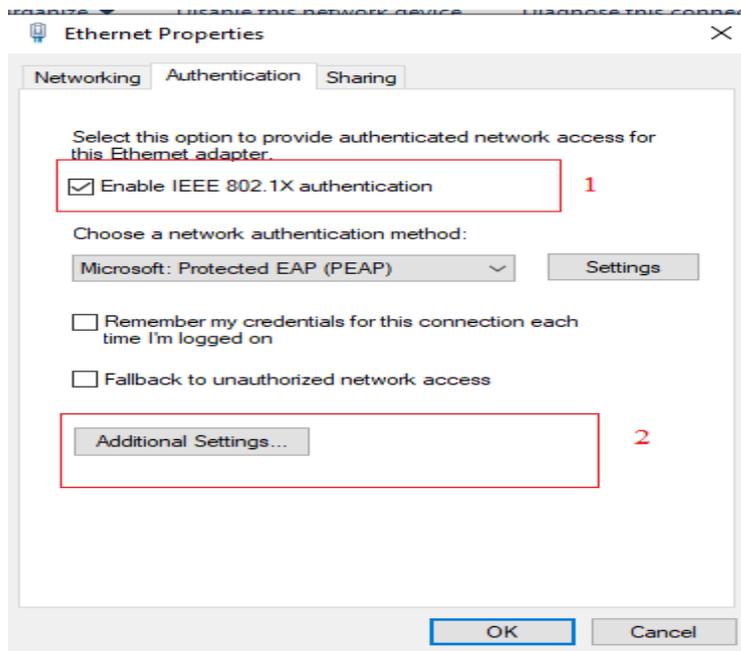
Start dịch vụ



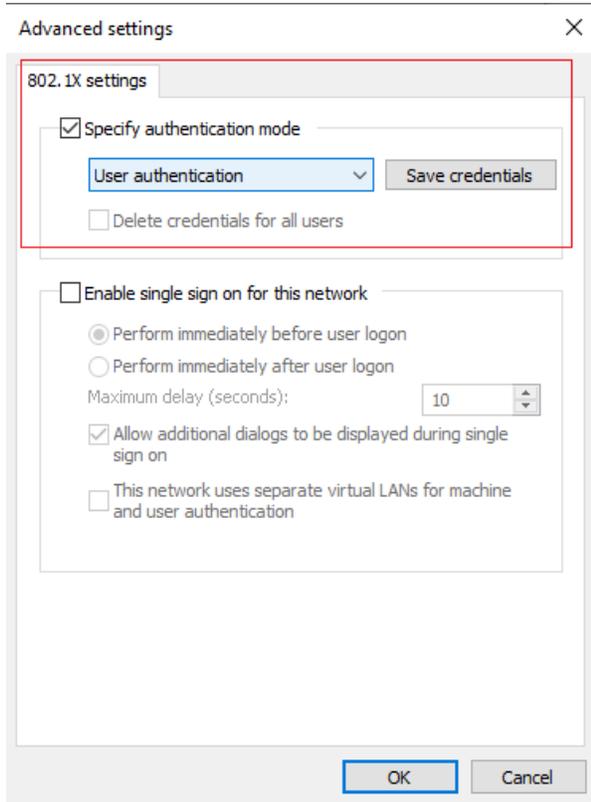
Tiếp theo, mở CMD gõ **netsh advbase reset** để vào **Network Connection**, click chuột phải vào Card Vào giao diện card mạng Ethernet -> chọn **Properties**



Qua tab Authentication, check **Enable IEEE 802.1X authentication**



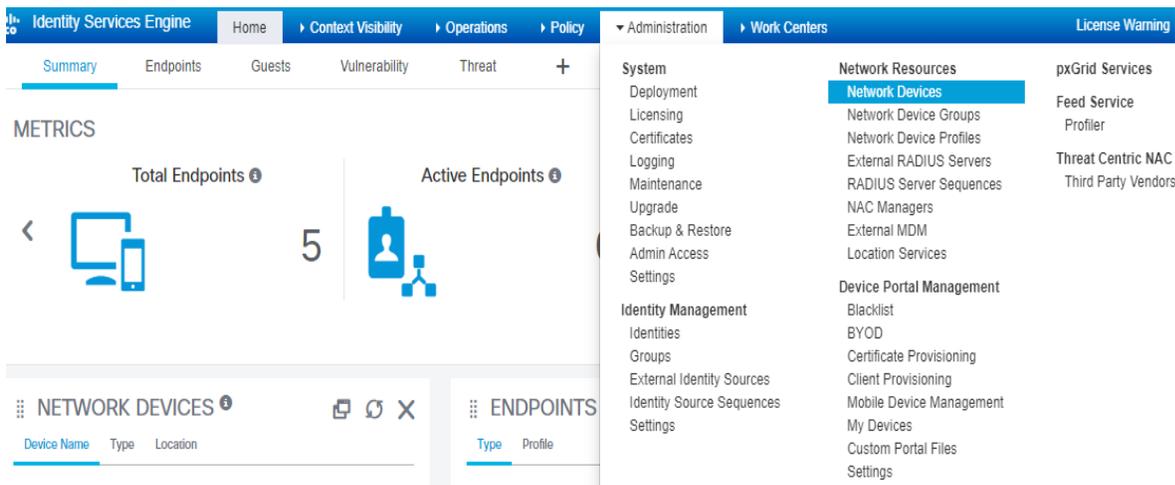
Tiếp tục chọn **Additional Setting** chọn xác thực bằng **user authentication** -> **ok** để lưu lại



3. Cấu hình Radius trên Cisco ISE

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

- Đầu tiên ở mục Administration -> Network Devices



Thực hiện ADD devices:

Network Devices

Name	IP/Mask	Profile Name	Location	Type	Description
Sw-Test	192.168.3.149...	Cisco	All Locations	All Device Types	

Tiến hành khai báo thông tin như sau:

Network Devices List > Sw-Test

Đặt tên cho thiết bị

* 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:

Tiếp theo Click vào **Radius Authentication Setting** 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) - > Chọn Submit để lưu cấu hình

Network Devices

Default Device

Device Security Settings

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret [masked] Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings (i)

DTLS Required (i)

Shared Secret radius/dtls (i)

CoA Port 2083 Set To Default

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

DNS Name

General Settings

Enable KeyWrap (i)

* Key Encryption Key [masked] Show

* Message Authenticator Code Key [masked] Show

Key Input Format ASCII HEXADECIMAL

3.2 Tạo policy

Chọn Policy Sets

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers License

System Identity Management Network Resources Device Portal Management

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

Network Devices

Default Device

Device Security Settings

RADIUS DTLS Settings (i)

DTLS Required (i)

Shared Secret radius/dtls (i)

CoA Port 2083 Set To Default

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

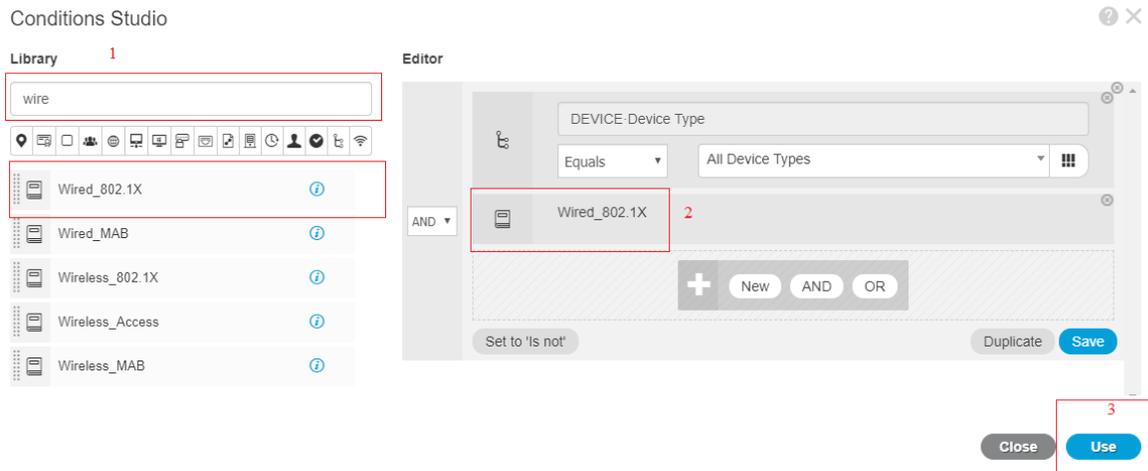
DNS Name

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

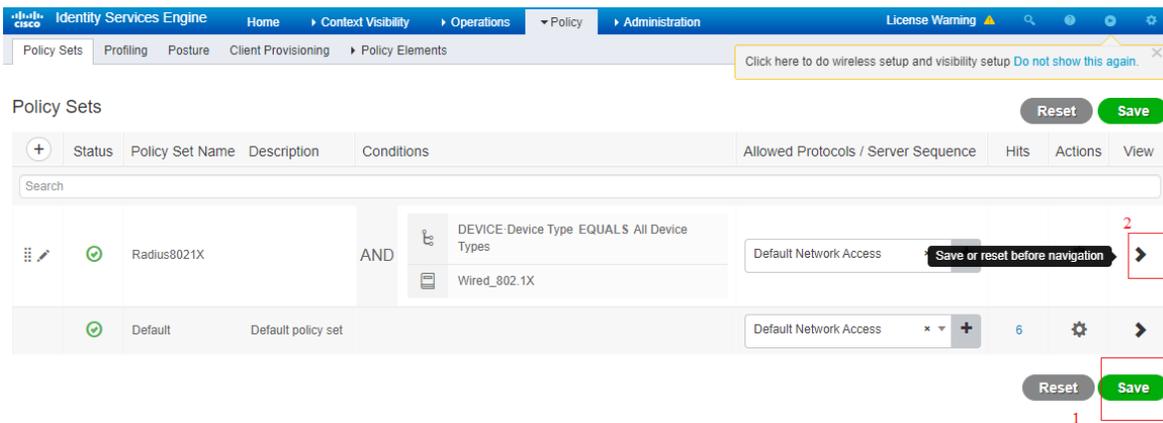
Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	Radius8021X		DEVICE Device Type EQUALS All Device Types	Default Network Access +	9		
	Default	Default policy set		Default Network Access +	6		

Tại mục Library tìm wire_802.1X và kéo vào mục editor-> Use



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



Tại mục Authentication Policy và Authorization Policy, ta làm như sau:

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. A 'License Warning' notification is present in the top right. The main content area is divided into two sections:

- Authentication Policy (2):** A table with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. Two rules are listed: 'dot1x' (status: green checkmark) with condition 'Wired_802.1X' and 'Internal Users' as the use, and 'Default' with condition 'All_User_ID_Stores' and 'All_User_ID_Stores' as the use. Both have 0 hits and an 'Options' link.
- Authorization Policy (2):** A table with columns for Status, Rule Name, Conditions, Results (Profiles), Security Groups, Hits, and Actions. Two rules are listed: 'dot1x' (status: green checkmark) with condition 'Wired_802.1X', 'PermitAccess' profile, and 'Select from list' security group, and 'Default' (status: green checkmark) with 'DenyAccess' profile and 'Select from list' security group. Both have 0 hits and an 'Options' link.

Sau khi cấu hình sau tiến hành lưu lại: chọn Save

3.3 Tạo username và Password trên Radius Server để xác thực trong mạng có dây Tại mục Administrator chọn Identities

The screenshot shows the Cisco ISE Administration console with the 'Administration' menu expanded. The 'Identities' option is highlighted in blue. The left navigation pane shows 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (4)'. The main content area shows a table with columns for Status, Rule Name, and Conditions. One rule is visible: 'Do1x' (status: green checkmark) with condition 'Wired_802.1X'.

Chọn ADD để tạo User

The screenshot shows the Cisco ISE administration interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > License Warning. The main navigation includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. A yellow box highlights a link: "Click here to do wireless setup and visibility". The left sidebar shows "Users" and "Latest Manual Network Scan Results". The main content area is titled "Network Access Users" and contains a table with columns: Status, Network Access Users, Description, First Name, Last Name, Email Address, and User Identity Group. The table lists three users: adminvnpro (Group_Admin), guest (Group_Guest), and Loi. Above the table are action buttons: Edit, Add (highlighted with a red box), Change Status, Import, Export, Delete, and Duplicate.

Điền thông tin username và Password

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

The screenshot shows the configuration form for a Network Access User. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > License Warning. The main navigation is the same as in the previous screenshot. The left sidebar shows "Users" and "Latest Manual Network Scan Results". The main content area is titled "Network Access Users List > UVK". Under "Network Access User", there is a form with the following fields:

- * Name: UVK
- Status: Enabled (checked)
- Email: (empty)

 Under "Passwords", there is a form with the following fields:

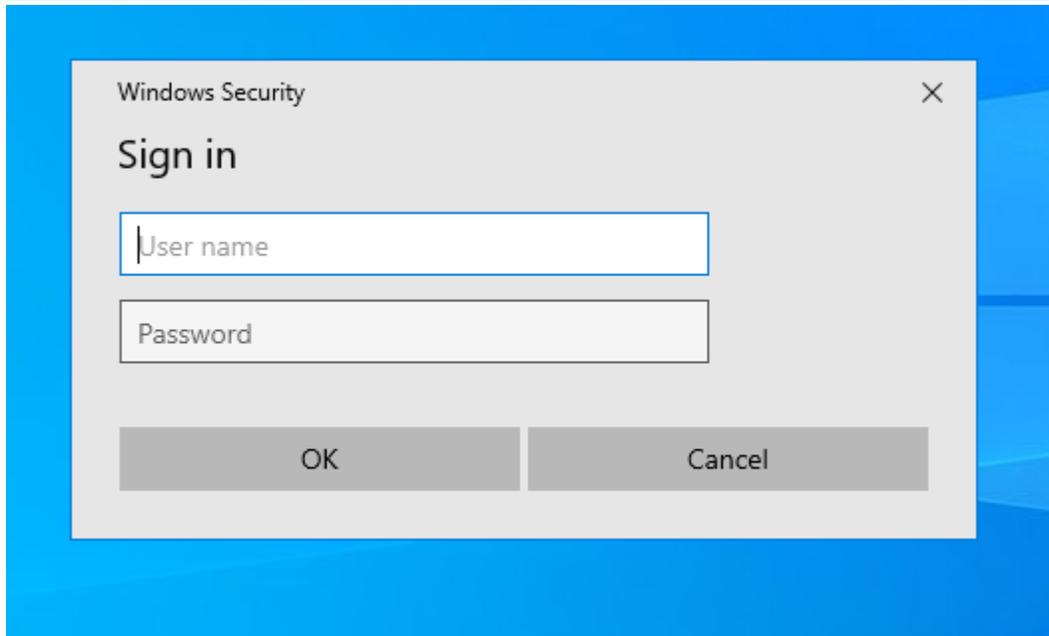
- Password Type: Internal Users
- Password: (empty)
- Re-Enter Password: (empty)
- * Login Password: (masked with dots) and (masked with dots) with a "Generate Password" button.
- Enable Password: (empty) and (empty) with a "Generate Password" button.

Sau khi xong chọn Submit để lưu cấu hình

4. Kiểm tra

Tiến hành kết nối PC vào cổng E0/1 của Switch đã cấu hình xác thực Dot1X

Cửa sổ yêu cầu xác thực để sử dụng mạng xuất hiện, tiến hành nhập Username và Password khai báo trên Radius server để đăng nhập vào mạng



Sau khi nhập đúng Username và Password trên Radius Server, ta có truy cập được mạng



CÔNG TY TNHH TƯ VẤN VÀ DỊCH VỤ CHUYÊN VIỆT
TRUNG TÂM TIN HỌC VNPRO

ĐC: 276 - 278 Ung Văn Khiêm, P. Thanh Mỹ Tây, Tp. Hồ Chí Minh
ĐT: (028) 35124257 | **Hotline:** 0933427079 **Email:** vnpro@vnpro.org
