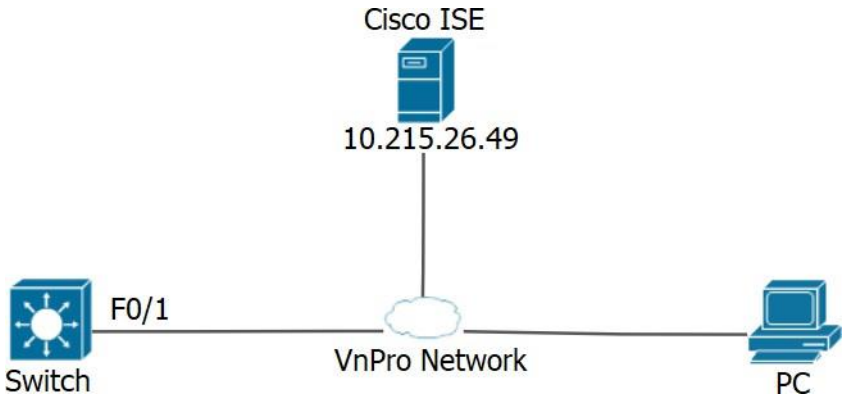
LAB - XÁC THỰC VÀ PHÂN QUYỀN LOGIN BẰNG TACACS+

I. Sơ đồ:



Ta có bảng thông tin như sau:

Tên thiết bị	Interface	IP/Netmask	Gateway
Cisco ISE	NIC	10.215.26.49	-
Switch	F0/1	DHCP	-
PC	NIC	DHCP	-

II. Yêu cầu:

1. Cấu hình ban đầu

- Thực hiện cấu hình IP cho PC, Switch sao cho switch và PC có thể ping thấy ISE server.

2. Cấu hình TACACS+:

- Tiến hành xác thực và phân quyền privilege cho các user truy cập telnet đến Switch như sau (việc xác thực/phân quyền phải do Cisco ISE kiểm soát):
  - Username: *guest*, password *VnPro@123*, privilege 7
  - Username: *adminvnpro*, password *VnPro@123*, privilege 15
- Cấu hình xác thực local với privilege cho các user như trên để khi hoạt động xác thực với Cisco ISE không thành công, chuyển sang phương thức xác thực/phân quyền local.

III. Thực hiện:

Cấu hình cho Switch

```
Switch(config)#no cdp run
Switch(config)# int f0/1
Switch(config-if)#no switchport
Switch(config-if)# ip address dhcp
Switch(config-if)# no shutdown
```

Cấu hình telnet:

```
Switch(config)# line vty 0 4
Switch(config-line)#transport input telnet
```

Kết nối PC với VnPro Network. Tiến hành ping để kiểm tra kết nối tới ISE Server:

```
C:\Users\hoang>ping 10.215.26.49

Pinging 10.215.26.49 with 32 bytes of data:
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
Reply from 10.215.26.49: bytes=32 time=1ms TTL=61
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
```

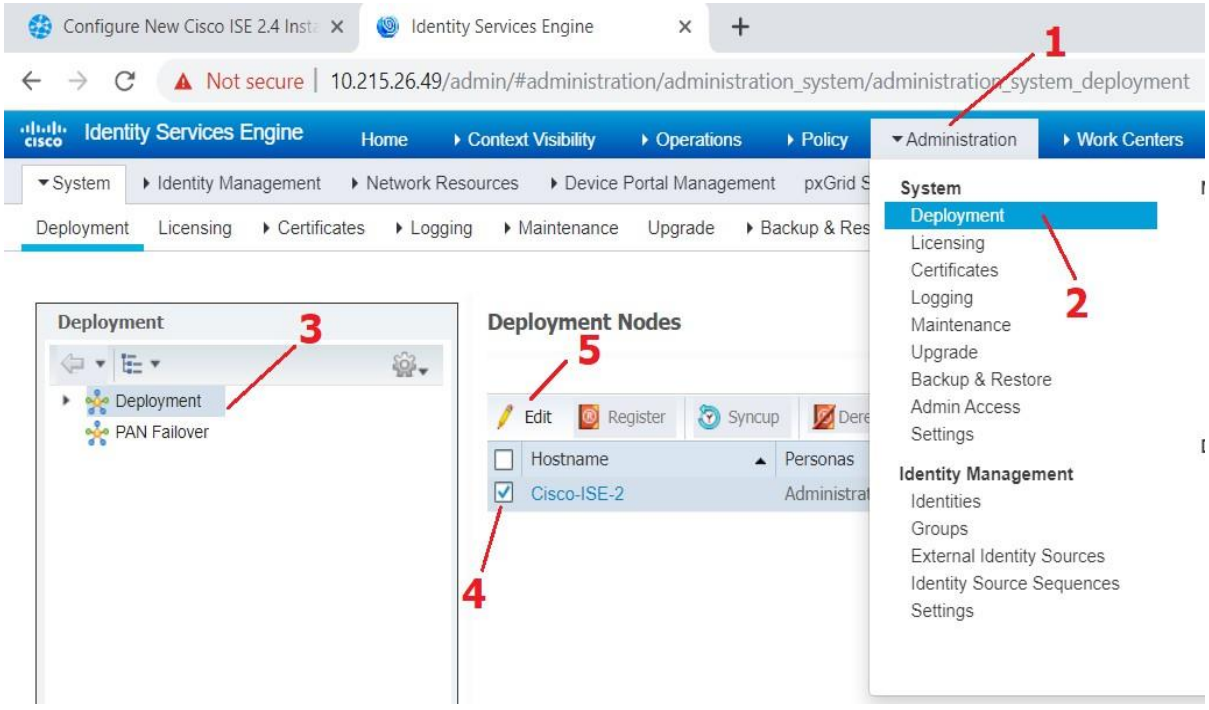
Bật tính năng TACACS+ trên ISE:

Đầu tiên, ta mở trình duyệt và truy cập vào IP 10.215.26.49 (IP của ISE Server). Đăng nhập bằng username và password:

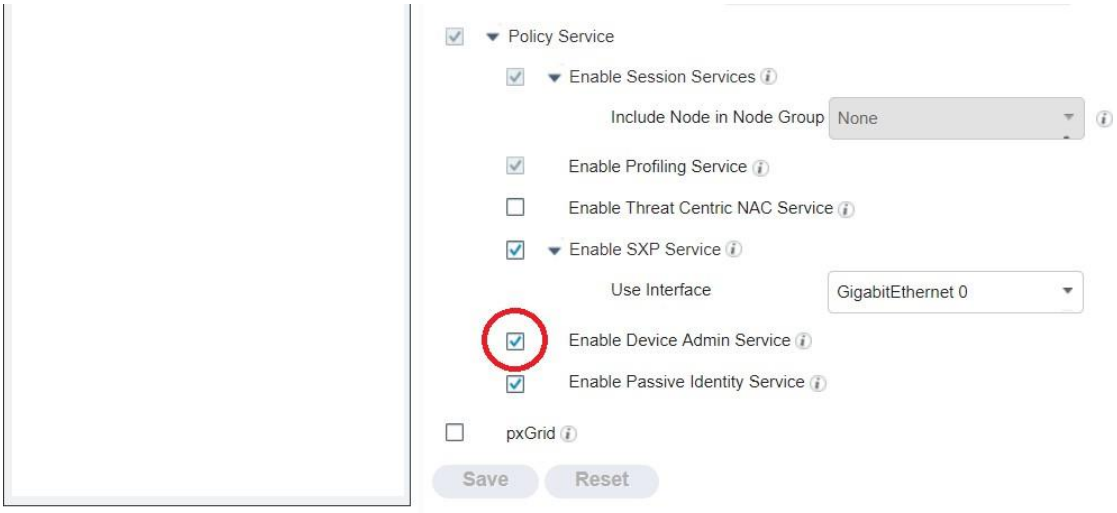
Username: admin

Password: VnPro@123

✓ Vào **Administration → Deployment →** Tích chọn hostname của Cisco ISE → **Edit**:



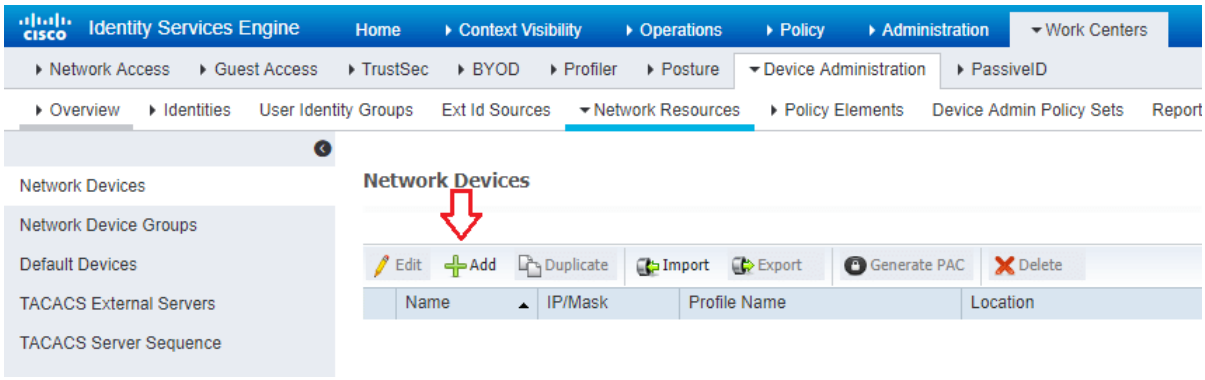
✓ Ở phần Policy Service, chọn **Enable Device Admin Service** và Save lại:

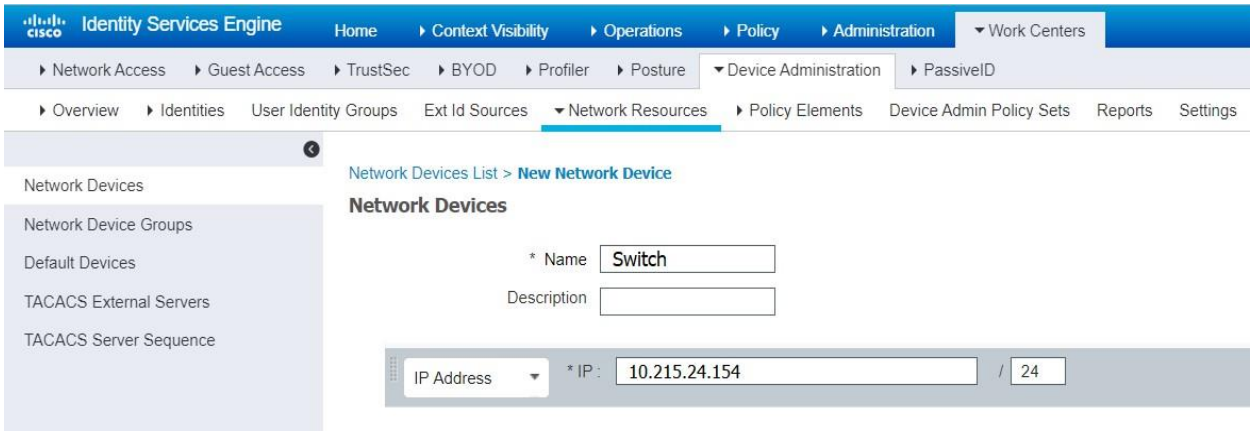


Thêm Switch vào ISE:

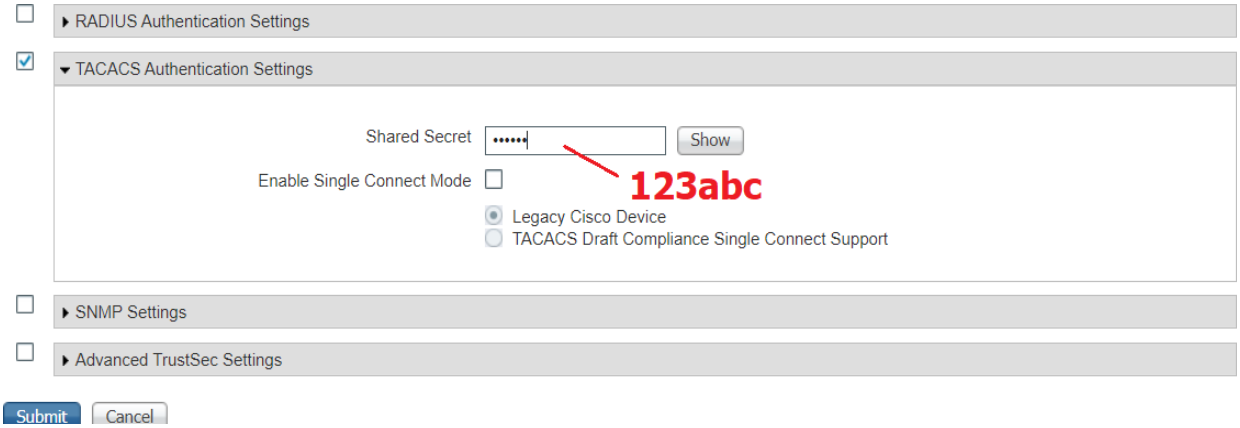
✓ Vào **Work Centers → Device Administration → Network Resources → Network Devices → Add:**

✓ Nhập tên, và IP của Switch mà ta nhận được từ DHCP do VnPro Network cấp:





✓ Ở phần **TACACS Authentication** Settings ta chỉ định chuỗi "**Shared Secret**" để Switch và ISE giao tiếp với nhau.

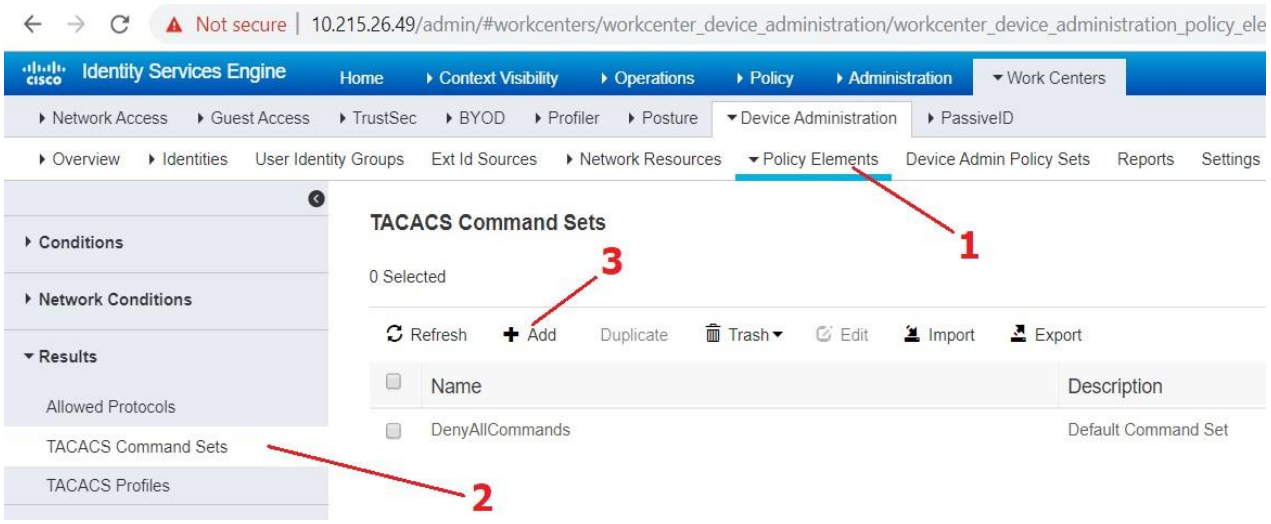


✓ Sau đó bấm submit.

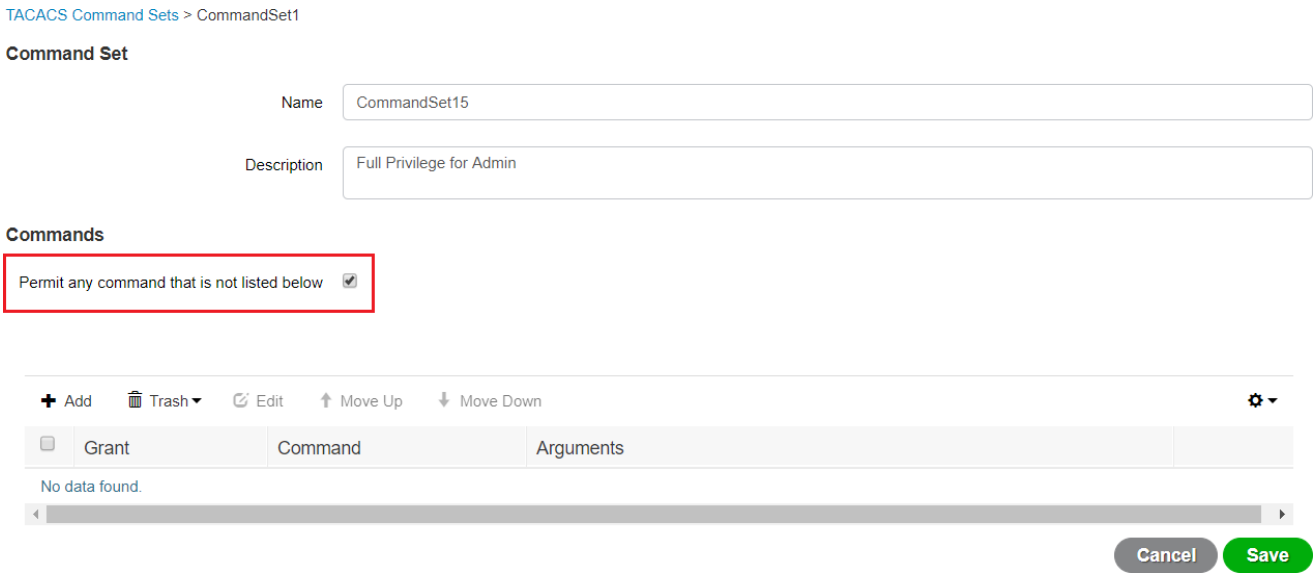
✓ **<u>Cấu hình xác thực/phân quyền bằng TACACS+:</u>**

✓ Vào **Work Center → Device Admin Policy Sets**:

✓ Chọn **Policy Elements → Result → TACACS Command Sets → Add**:

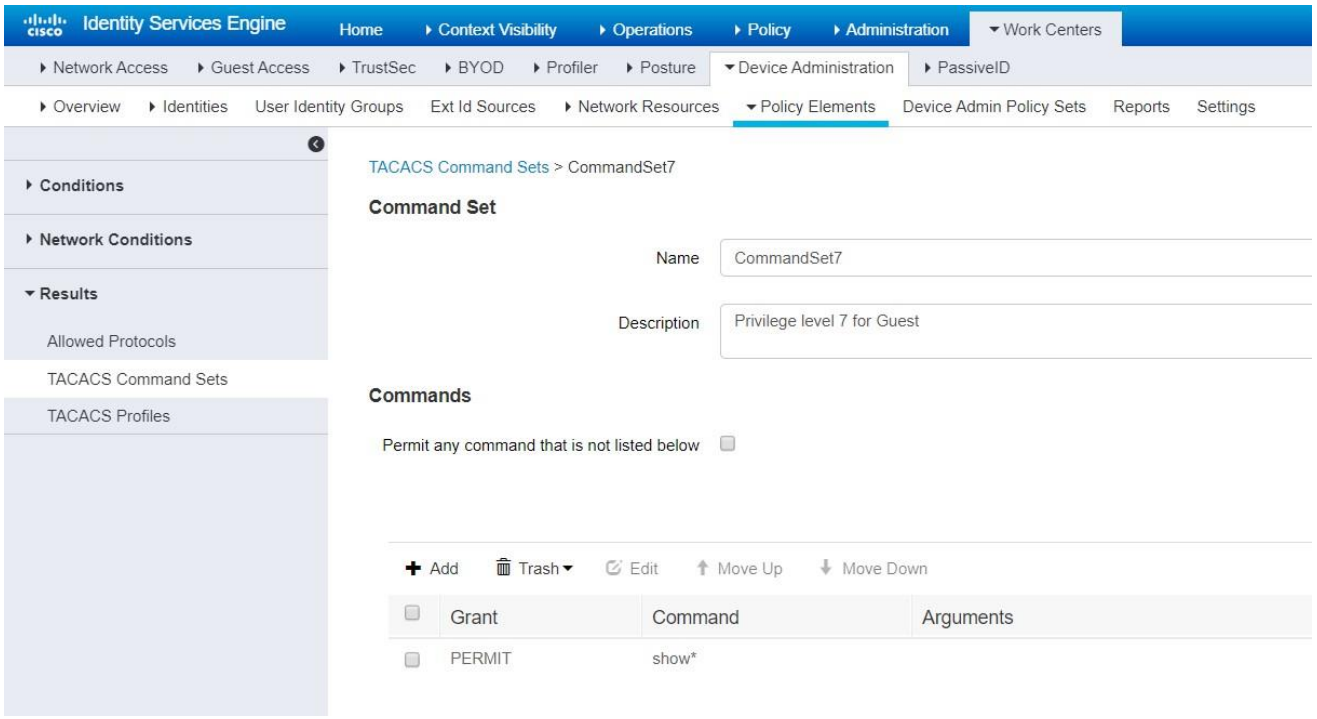


✓ Tạo command set cho user ***adminvnpro*** có thể dùng đầy đủ các lệnh khi telnet:



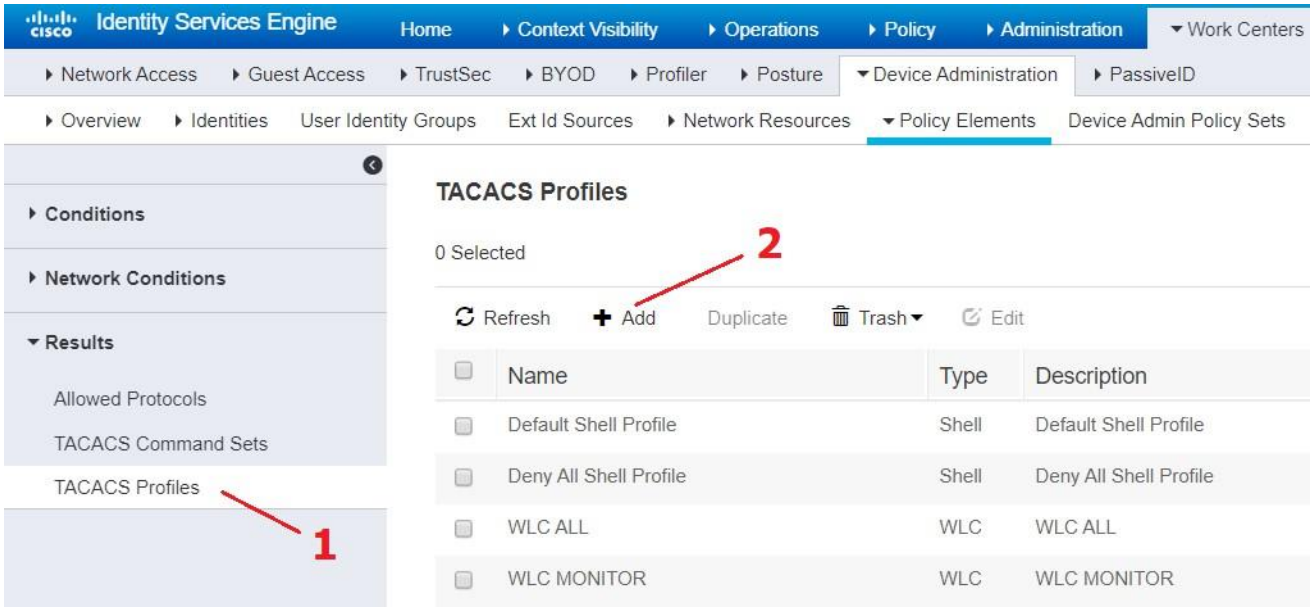
✓ Tích chọn "**Permit any command that is not listed below**" và bấm Save.

✓ Ta cũng tạo thêm command set cho user ***guest*** có privilege là 7, khi user này telnet vào Switch chỉ dùng được lệnh các lệnh *show*:

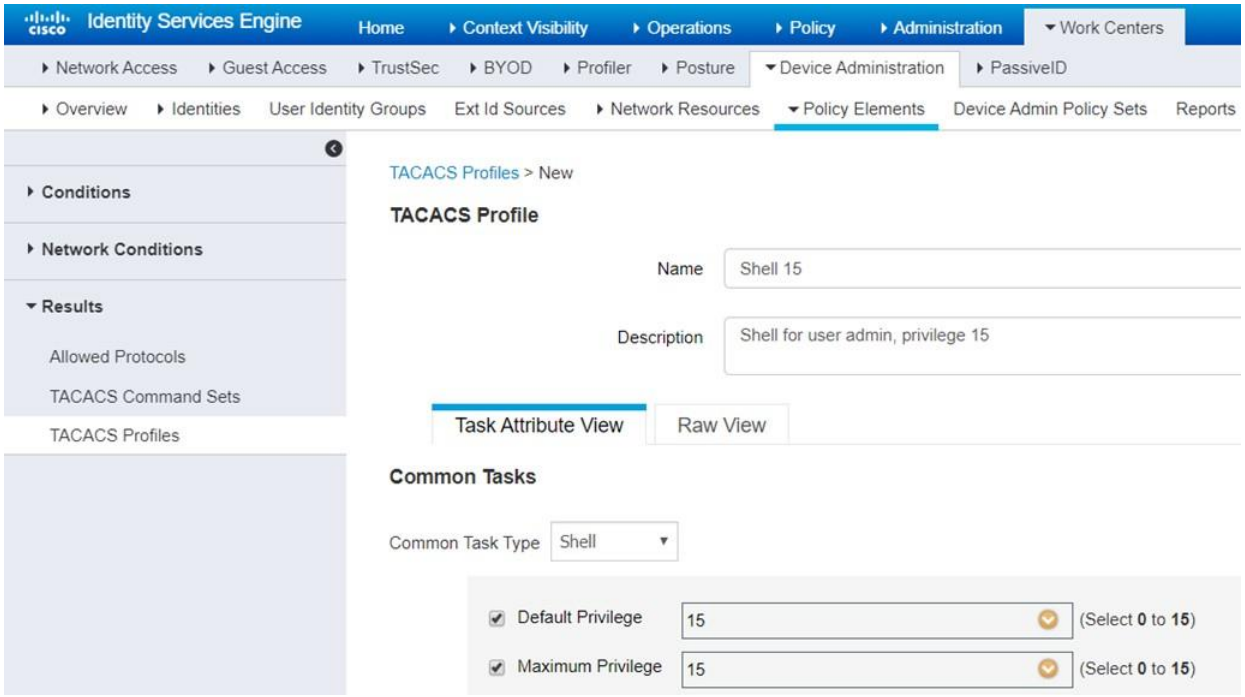


✓ Sau đó bấm **Submit**.

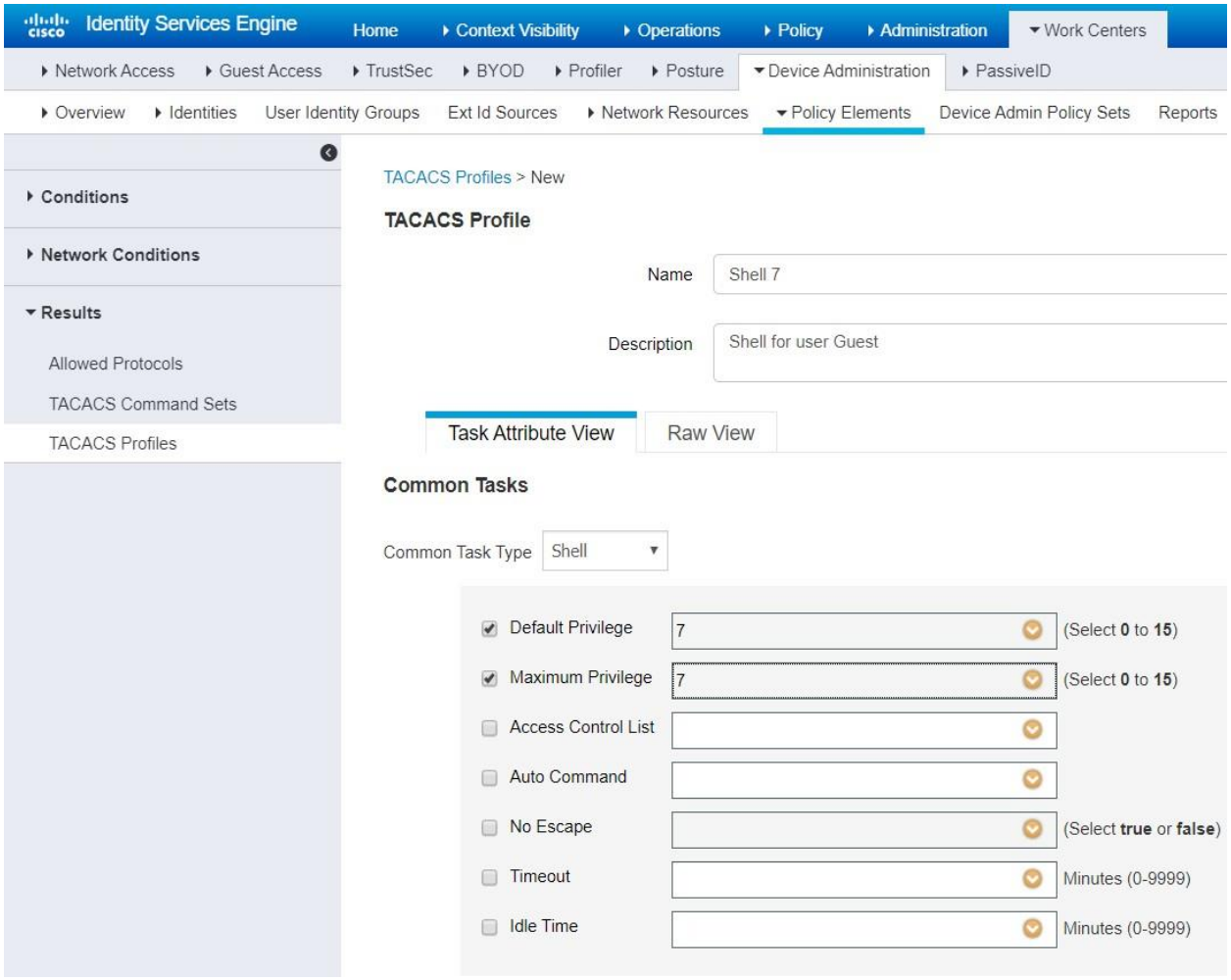
✓ Tiếp theo, ta vào **TACACS Profiles → Add**:



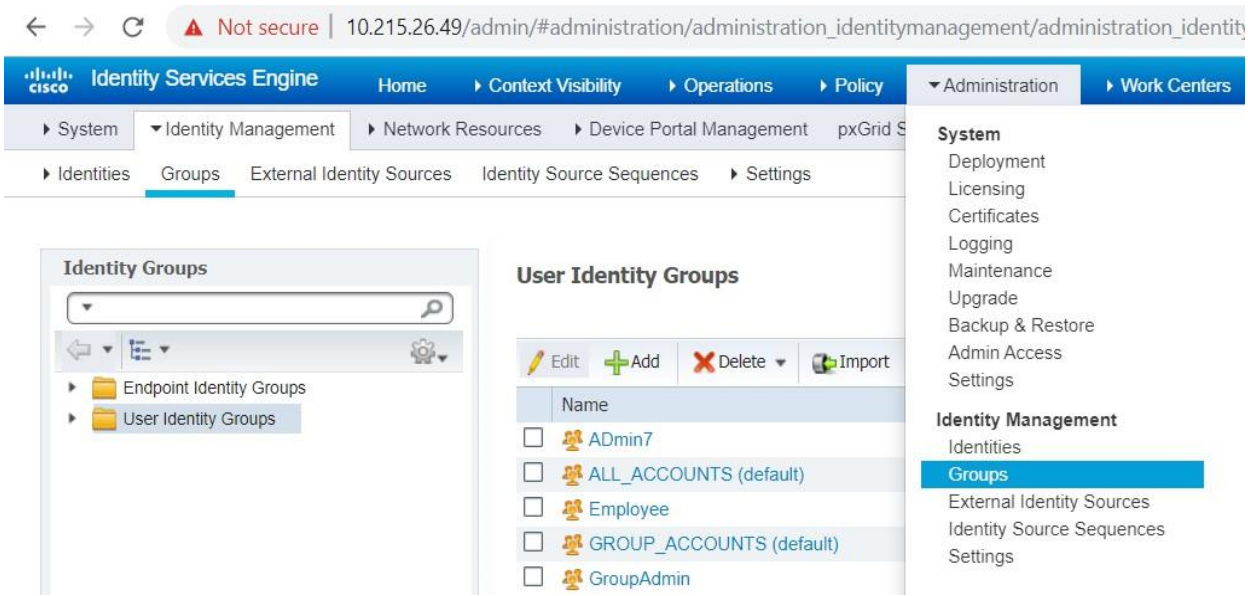
✓ Tạo profile cho ***adminvnpro*** với privilege 15:



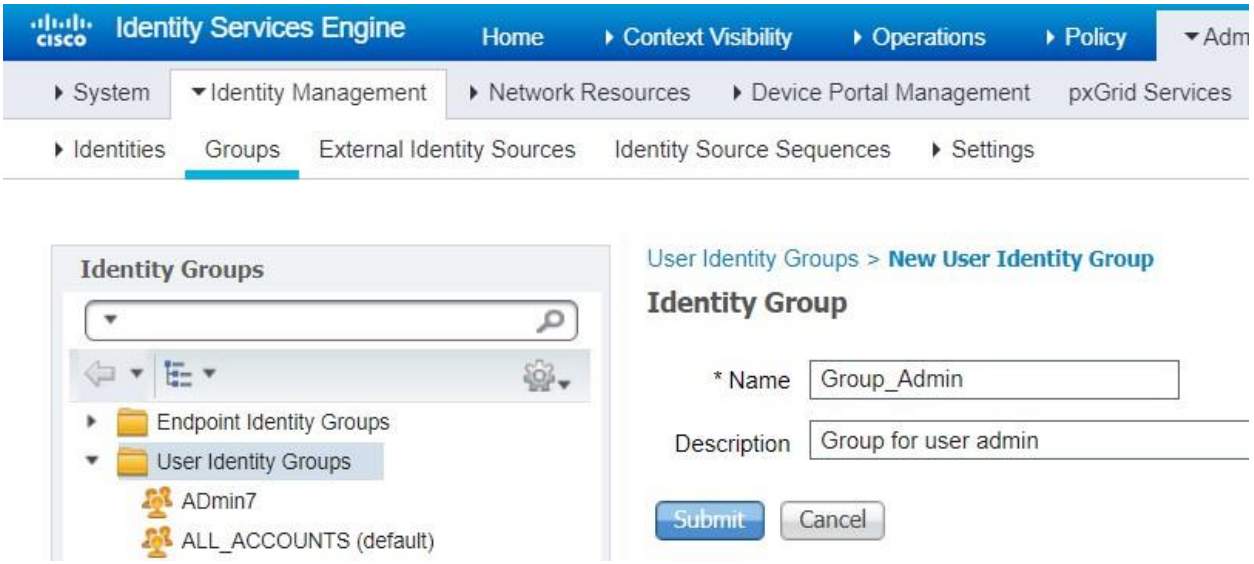
✓ Profile cho ***guest*** với privilege 7:

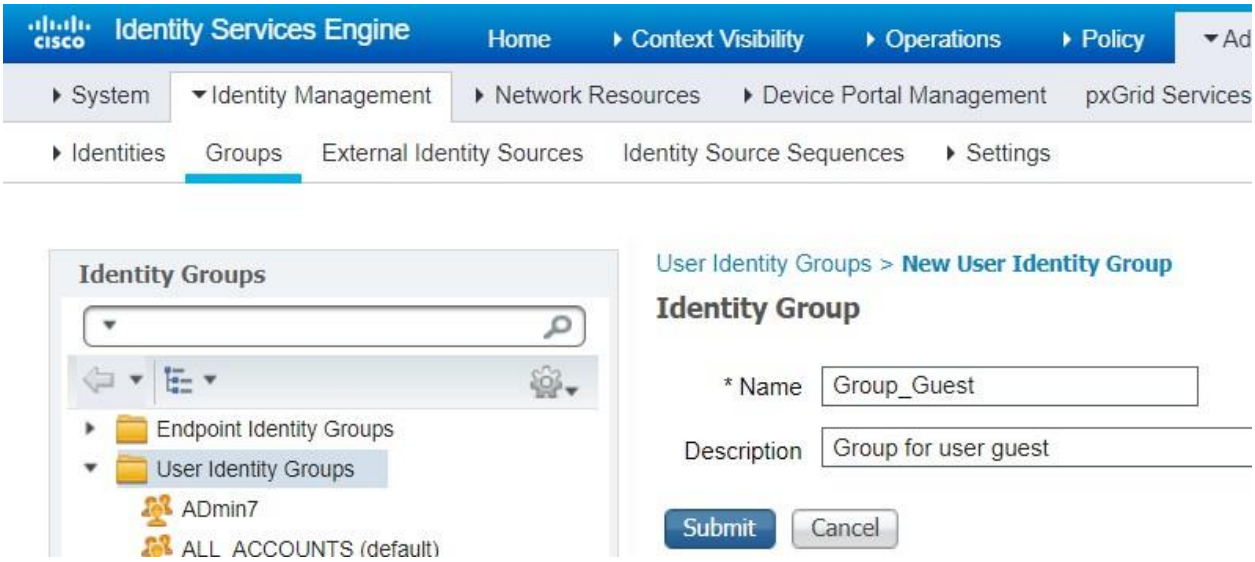


✓ Vào **Administration → Groups → User Identify Groups → Add**:

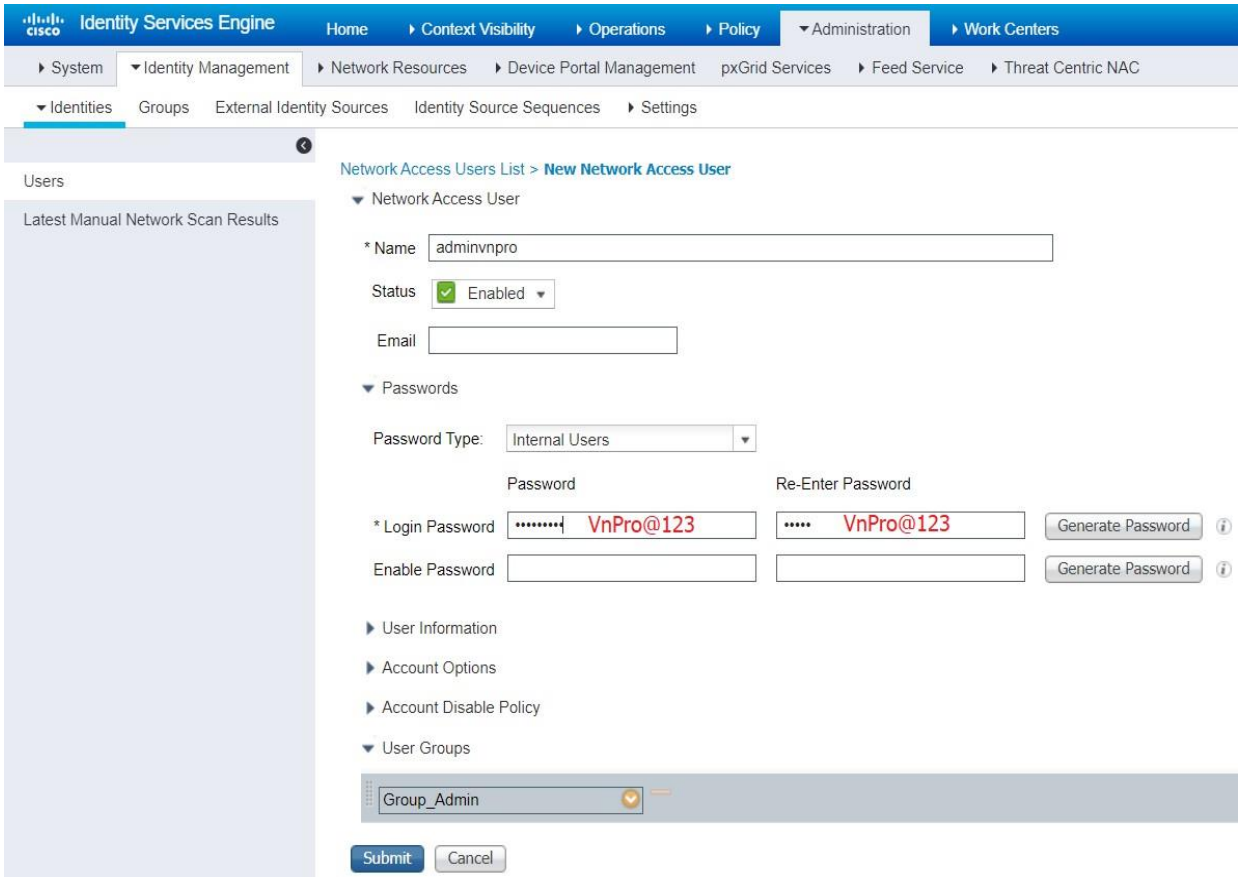


✓ Tạo 2 group cho user ***adminvnpro*** và user ***guest*****:**





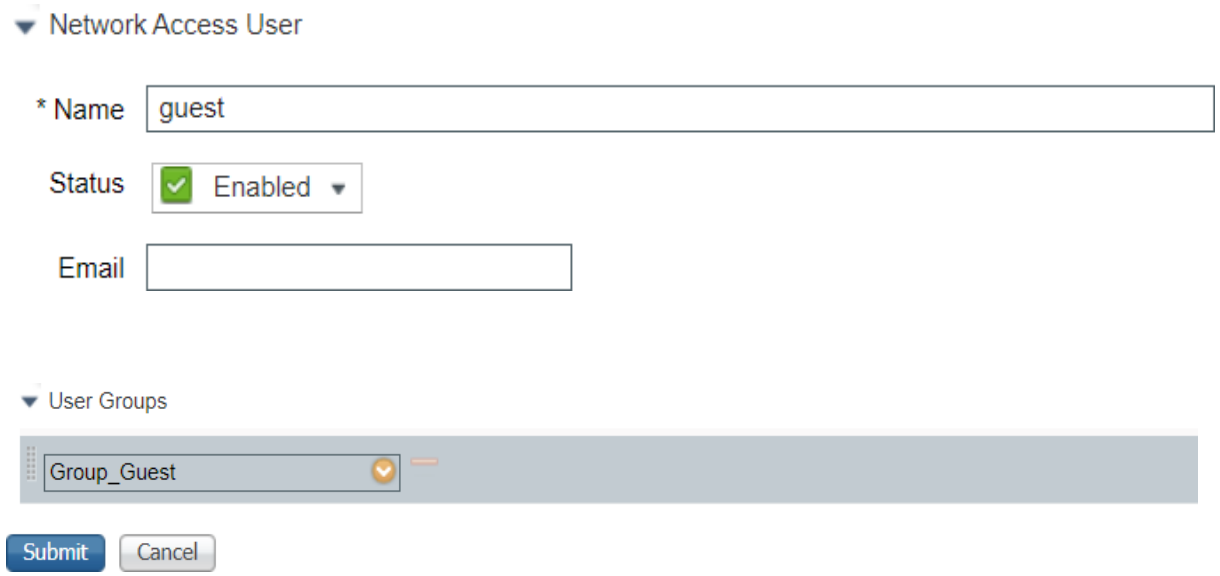
✓ Vào **Identities → Add →** Tạo user ***adminvnpro***:



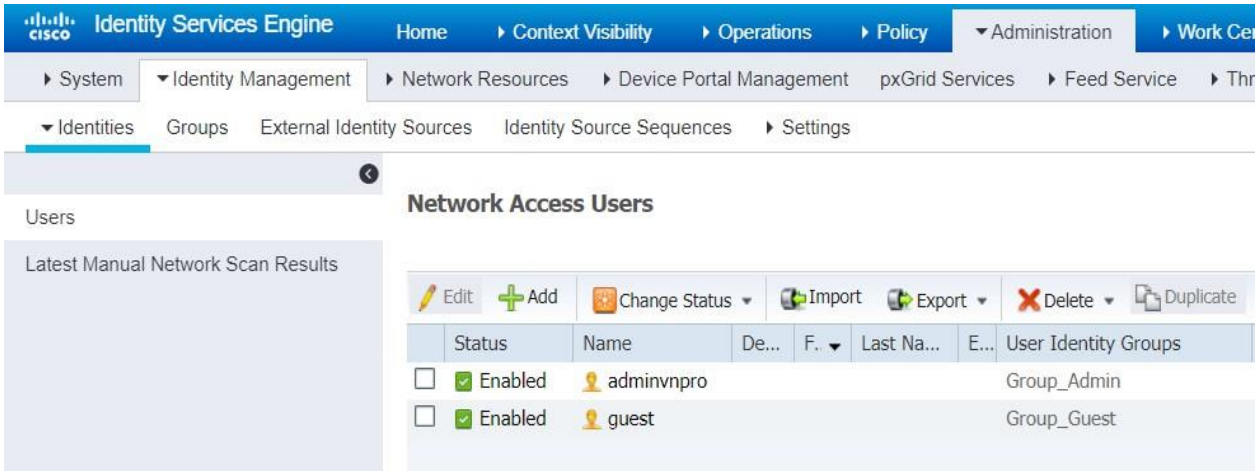
Trong đó:

- **Password Type:** Internal Users
- **User Group:** Group_Admin

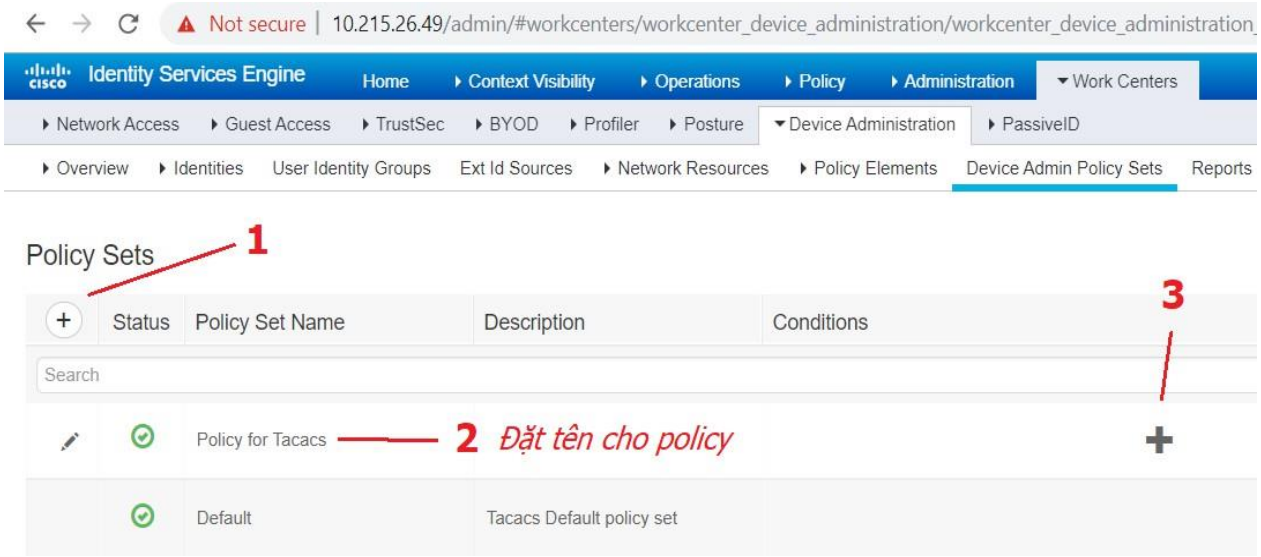
Tương tự, ta cũng tạo thêm user ***guest*** với **User Groups** là Group_Guest:



✓ Kết quả:

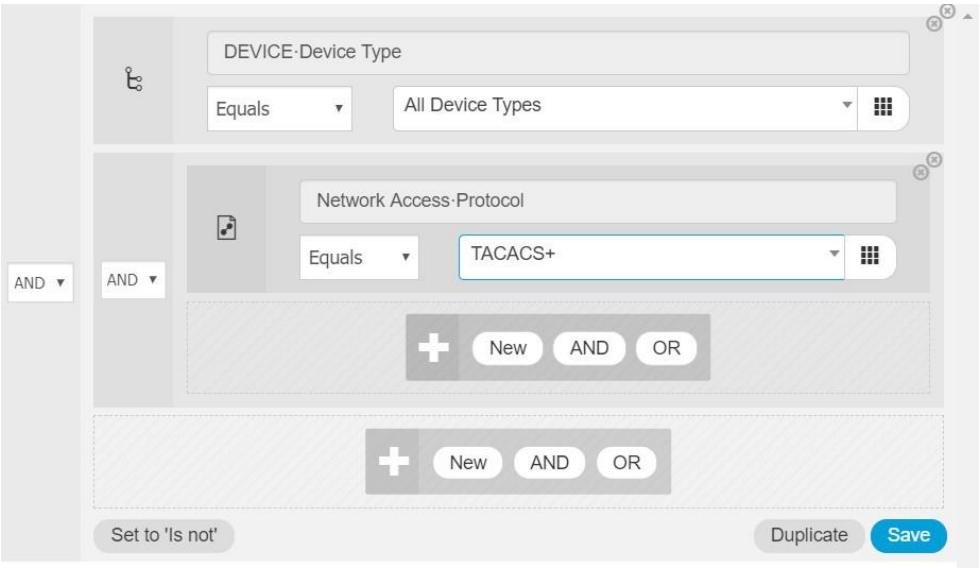


✓ Tiếp theo, ta vào **Work Center → Device Admin Policy Sets → bấm (+):**

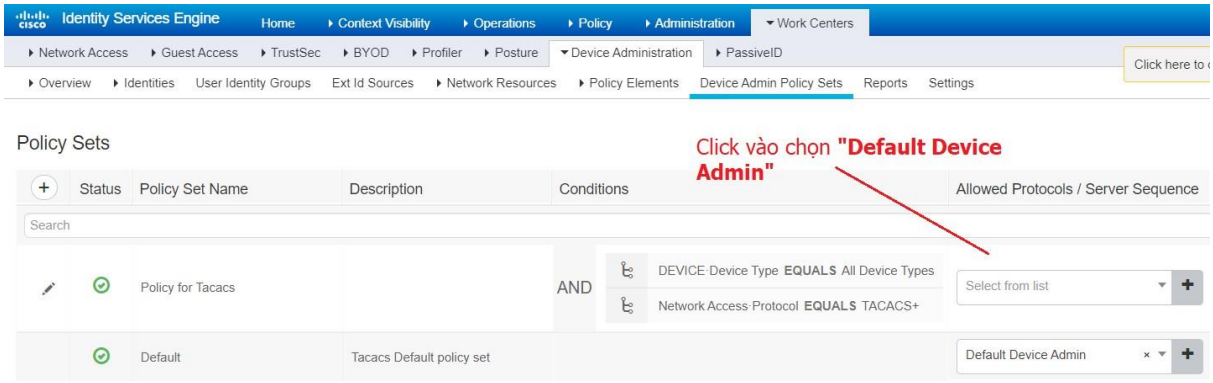


✓ Tạo policy như sau:

✓ Sau khi click **"AND"** ta chọn **"New"** và thiết lập như sau:

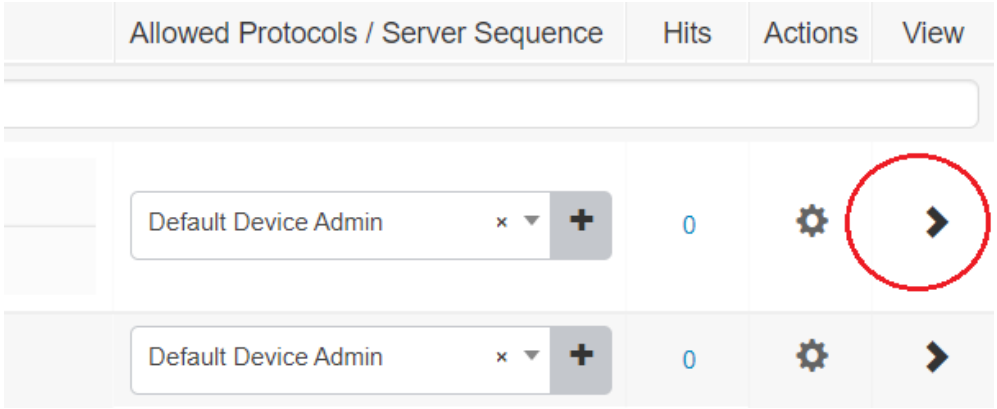


✓ Sau đó bấm **"Use"**, ta được kết quả:

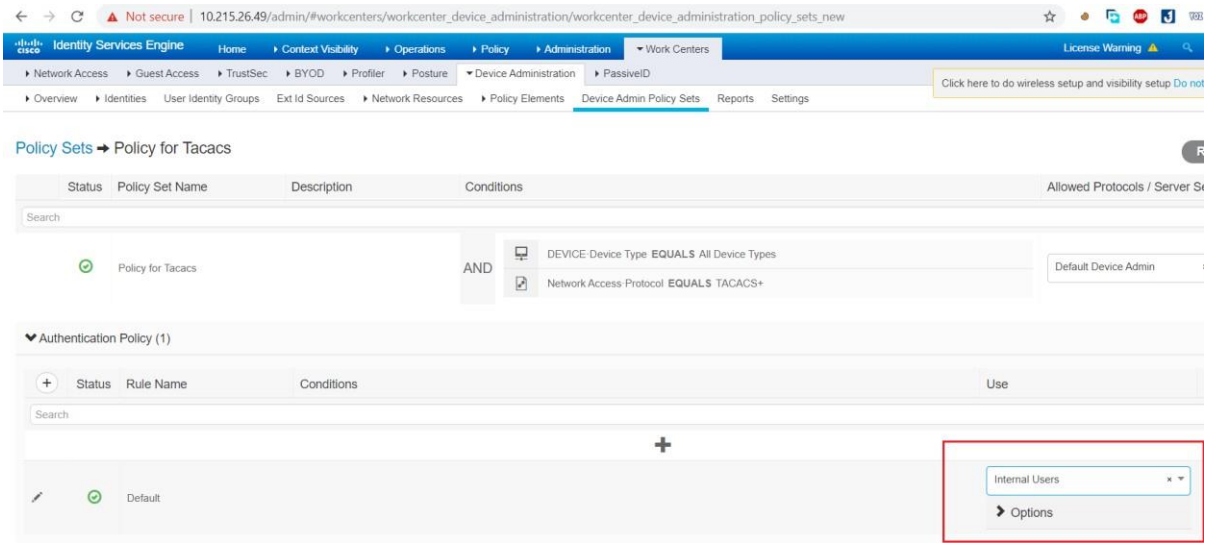


✓ Sau đó save lại.

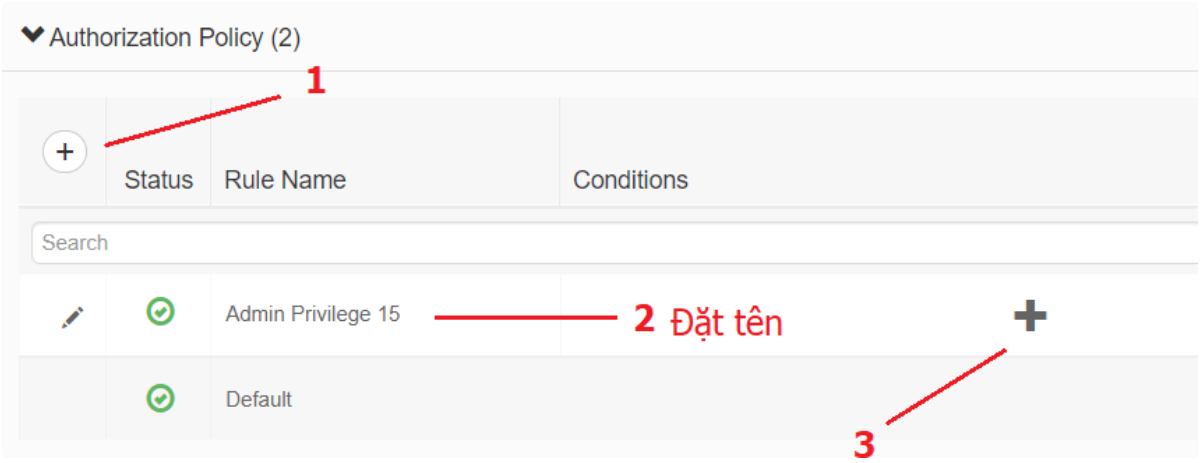
✓ Sau đó, ta click vào mũi tên qua phải của policy vừa mới tạo:



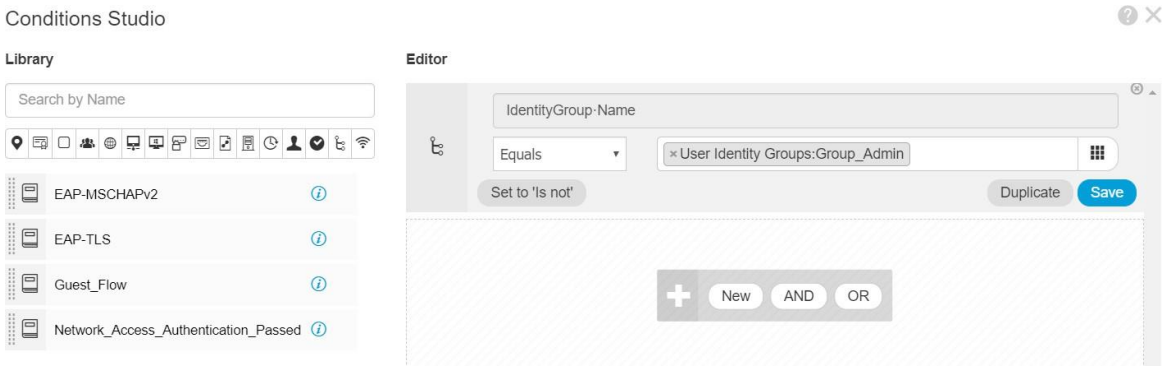
✓ Ở phần **"Authentication Policy"** ta chọn Use: **Internal Users**:



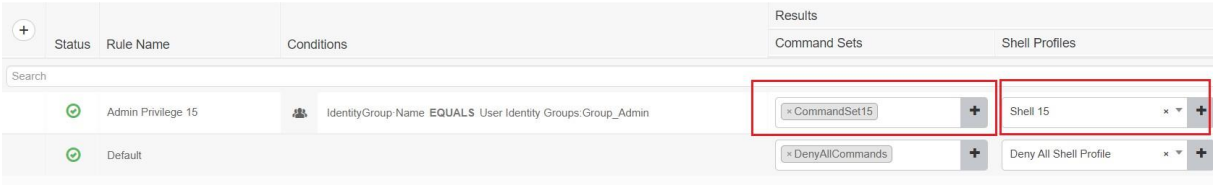
✓ Tiếp theo, ta cấu hình phần **Authorization Policy:**



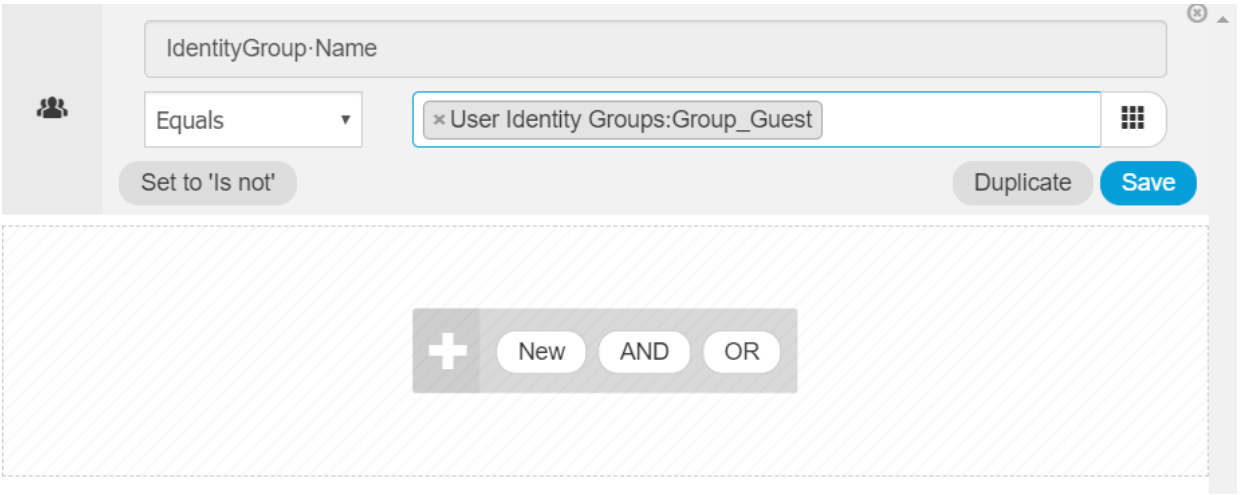
✓ Cấu hình conditions như sau:

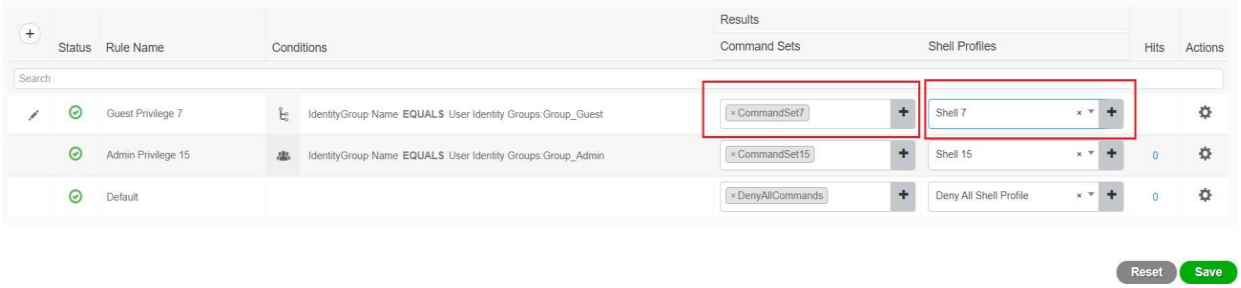


✓ Sau đó bấm **"Use"** để quay lại mục **Authorization Policy**, ở mục bên phải, ta chọn command set là "**CommandSet15**" và shell profile là "**Shell 15**".



✓ Tương tự vậy, ta cũng tạo **Authorization Policy** cho account ***guest***:





✓ Sau đó ta save lại.

Chỉ định TACACS+ Server cho Switch:

```
Switch(config)#aaa new-model
Switch(config)#tacacs server ISE
Switch(config)#address ipv4 10.215.27.205
Switch(config)#key cisco123
```

Cấu hình Switch xác thực với ISE bằng giao thức TACACS+:

Trên Switch, ta dùng các lệnh sau:

```
Switch(config)# aaa new-model
Switch(config)# aaa group server tacacs+ ISESRV
Switch(config-sg-tacacs+)# server 10.215.26.49
Switch(config-sg-tacacs+)# exit

Switch(config)#aaa authentication login VTY group ISESRV local
Switch(config)#aaa authorization exec VTY group ISESRV local if-authenticated

Switch(config)#aaa accounting exec default start-stop group ISESRV

Switch(config)#aaa accounting commands 1 default start-stop group ISESRV

Switch(config)#aaa accounting commands 15 default start-stop group ISESRV

Switch(config)#aaa accounting network default start-stop group ISESRV
```

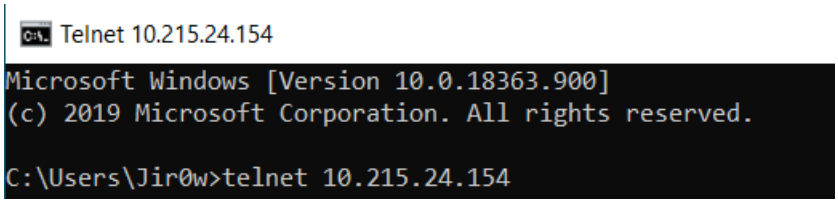
```
Switch(config)#aaa accounting connection default start-stop group ISESRV

Switch(config)#aaa accounting system default start-stop group ISESRV
```

Cấu hình telnet cho Switch:

```
Switch(config)#line vty 0 4
Switch(config-line)#login authentication VTY
Switch(config-line)#authorization exec VTY
Switch(config-line)#exit
```

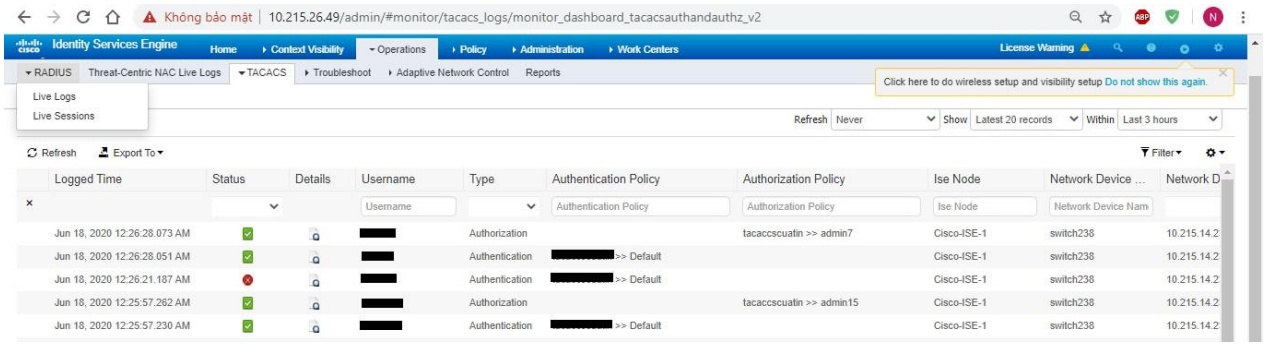
✓ Ta dùng PC **telnet** vào Switch thông qua **IP mà VnPro network cấp** với username là ***adminvnpro*** password là ***VnPro@123*:**



✓ Kết quả: Telet thành công:

✓ Gõ "?" để kiểm tra các lệnh user này có thể sử dụng, ta thấy user adminvnpro có thể dùng tất cả các lệnh:

✓ Ta kiểm tra **Tacacs+ log** trên cisco ise: **Operation->Tacacs->Live logs** được như sau:



✓ *Dấu tick màu xanh cho thấy đã pass xác thực nếu màu đỏ là chưa hoàn tất lab*

✓ Hoàn tất bài lab.