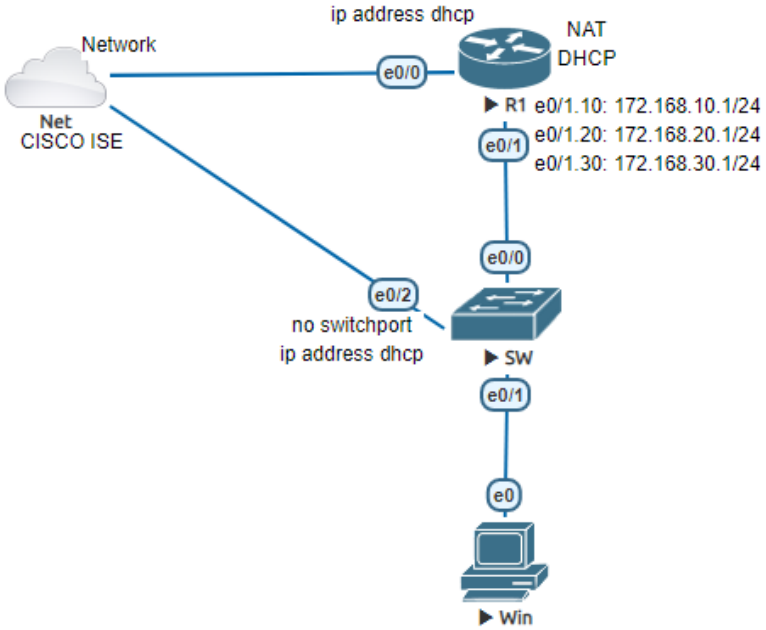
Lab – Cấu hình Dynamic Assign VLAN và 802.1X với Cisco ISE

Sơ đồ:



Mô tả:

- Sơ đồ Lab gồm 1 router, 1 switch layer 2, 1 Cisco ISE được dựng trong đám mây đóng vai trò là server RADIUS và 1 PC được đấu nối như hình. Bài Lab này có thể dựng trên lab ảo hoá sử dụng các IOL Router L3-ADVENTERPRISEK9-M-15.4-2T, IOL Switch i86bi_linux_l2-advipservicesk9, qemu win-7-x86-IPCC
- Trên sơ đồ này, học viên sẽ thực tập cấu hình xác thực 802.1x và dynamic assign vlan cho PC đảm bảo PC được xác thực và phân quyền dựa vào các vlan khác nhau trên mô hình.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị và đặt địa chỉ IP (trừ PC) cũng như các hostname của các thiết bị được chỉ ra mô hình.
2. Trên switch cấu hình trunk trên interface e0/0, cấu hình tạo ra thêm các vlan 10, 20 và 30 đặt tên lần lượt là: IT, SALE, ACCOUNTING
3. Học viên tiến hành xin IP từ đám mây Net trên cổng e0/0 của router bằng câu lệnh ip address dhcp, cấu hình NAT Overload đảm bảo mọi địa chỉ có thể đi internet. Cấu hình DHCP để cấp ip cho các vlan 10, 20 và 30 và cấu hình router-on-stick trên router để các lớp mạng có thể ping thấy nhau.
1. Cấu hình xin ip từ dhcp cho switch để giao tiếp với cisco ISE, xác thực 802.1x trên switch và Cisco ISE đảm bảo các PC trong các vlan 10, 20 và 30 có thể vào mạng được.
2. Cấu hình dynamic assign vlan trên Cisco ISE để PC vào được các vlan 10, 20, 30.

Thực hiện:

Bước 1: Kết nối và cấu hình cơ bản:
Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

Bước 2: Cấu hình trunk và vlan trên switch:
Học viên thực hiện cấu hình trên switch theo yêu cầu đặt ra.

Bước 3: Cấu hình NAT, dhcp và router-on-a-stick trên router:
Học viên thực hiện cấu hình trên router theo yêu cầu đã đặt ra.

Bước 4: Cấu hình xác thực 802.1x:
Cấu hình:

- Cisco ISE trong đám mây đã được dựng sẵn. Cấu hình IP trên cổng của Switch để có thể giao tiếp với Cisco ISE

```
SW(config)#interface e0/2
SW(config-if)#no switchport
SW(config)-if)#ip address dhcp
SW(config-if)#no shutdown
SW(config-if)#do 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            172.168.1.10    YES DHCP   up                    up
Ethernet0/3            unassigned      YES unset  up                    up
```

- Cấu hình bật xác thực 802.1x trên switch:

```
SW(config)#aaa new-model
SW(config)#aaa authentication dot1x default group radius
SW(config)#aaa authorization network default group radius
SW(config)#dot1x system-auth-control
SW(config)#exit
```

- Cấu hình thông tin radius server trên switch:

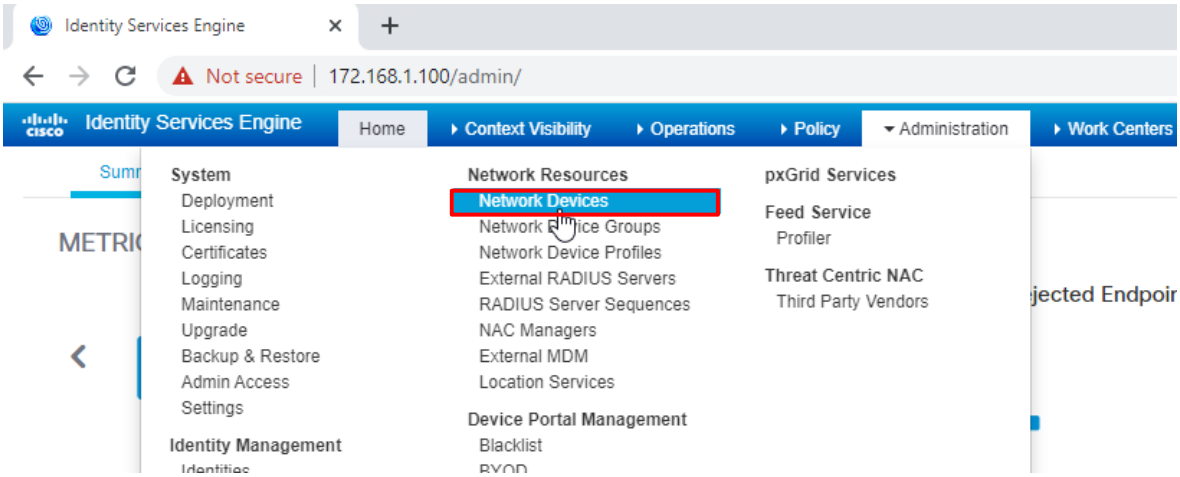
```
SW(config)#radius server Cisco_ISE
SW(config-radius-server)#address ipv4 172.168.1.100
SW(config-radius-server)#key VnPro123
SW(config-radius-server)#exit
```

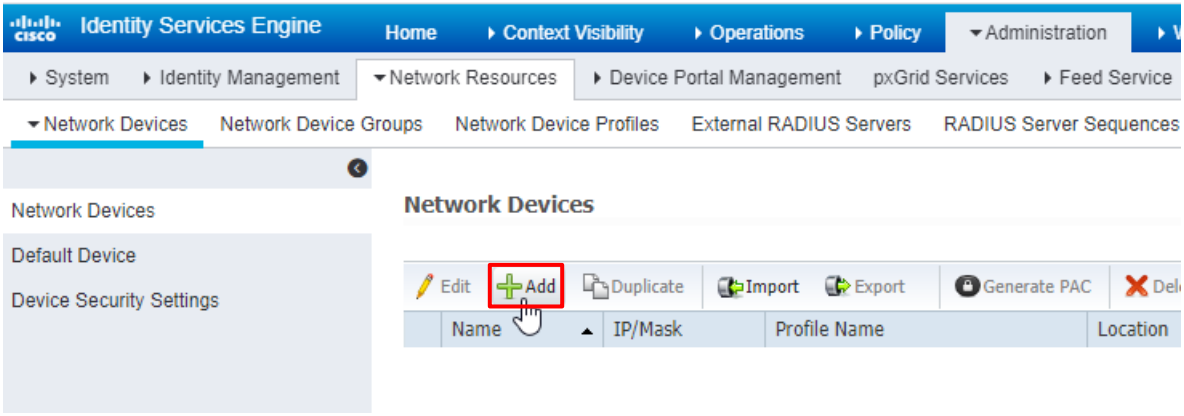
- Cấu hình bật 802.1x trên interface e0/1:

```
SW1(config)#interface e0/1
```

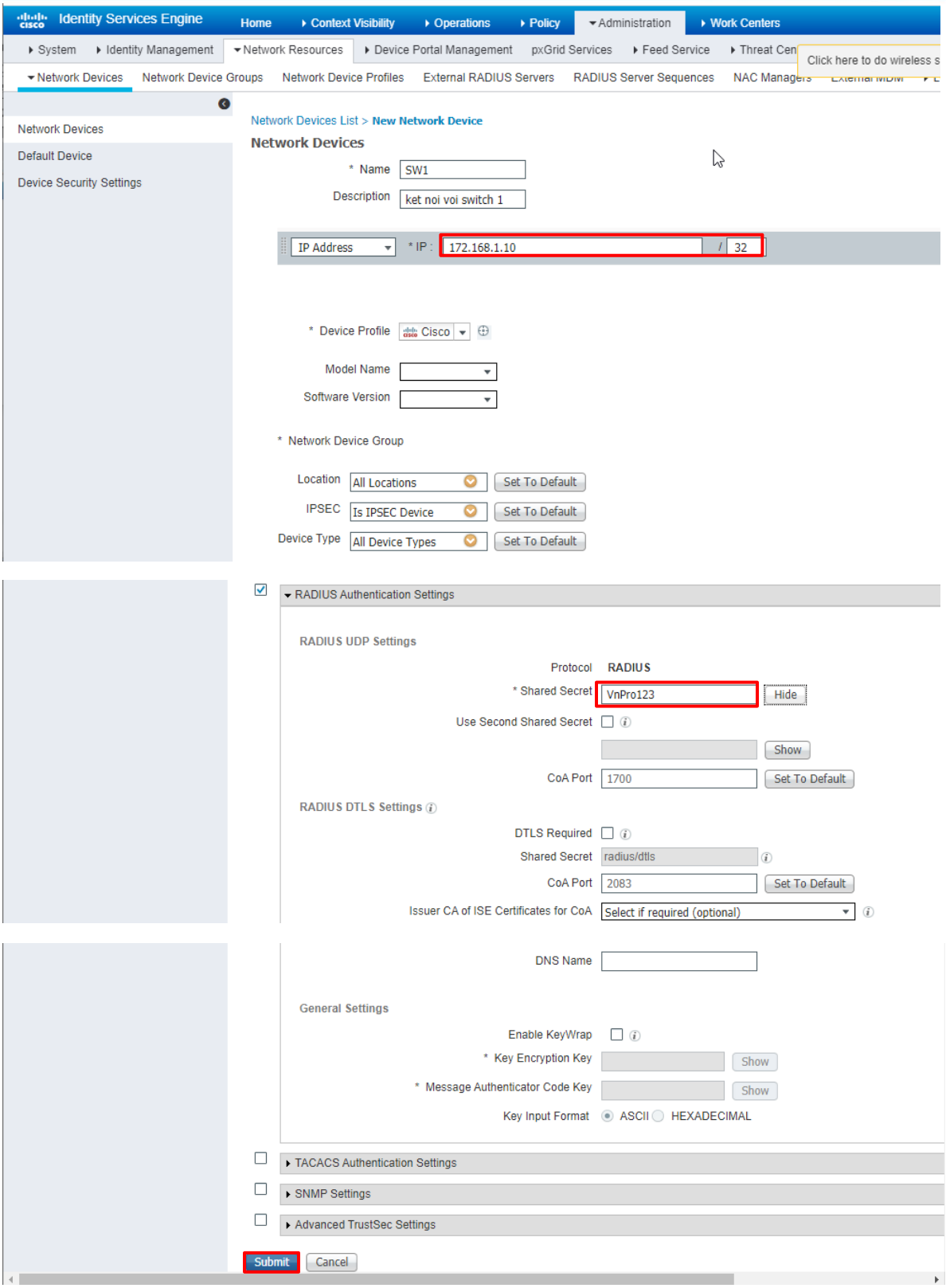
```
SW1(config-if)#switchport mode access
SW1(config-if)#authentication port-control auto
SW1(config-if)#dot1x pae authenticator
SW1(config-if)#spanning-tree portfast
SW1(config-if)#exit
```

- Truy cập vào Cisco ISE, trường hợp này Cisco ISE có địa chỉ 172.168.1.100 sau đó cấu hình network devices để có thể trao đổi với switch: Vào Administration->Network Devices->Add:

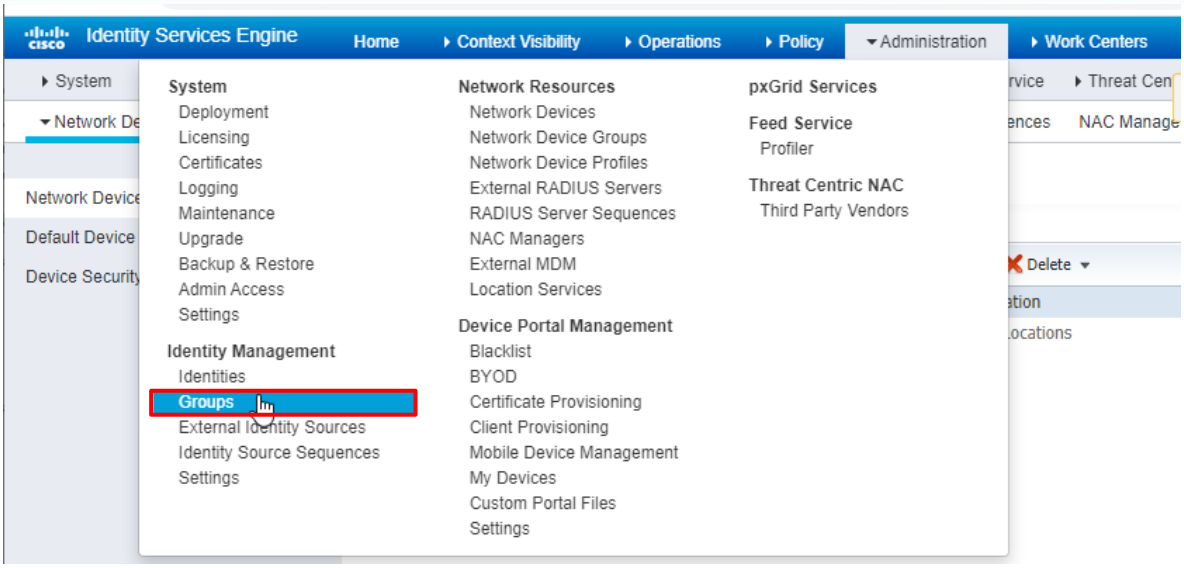


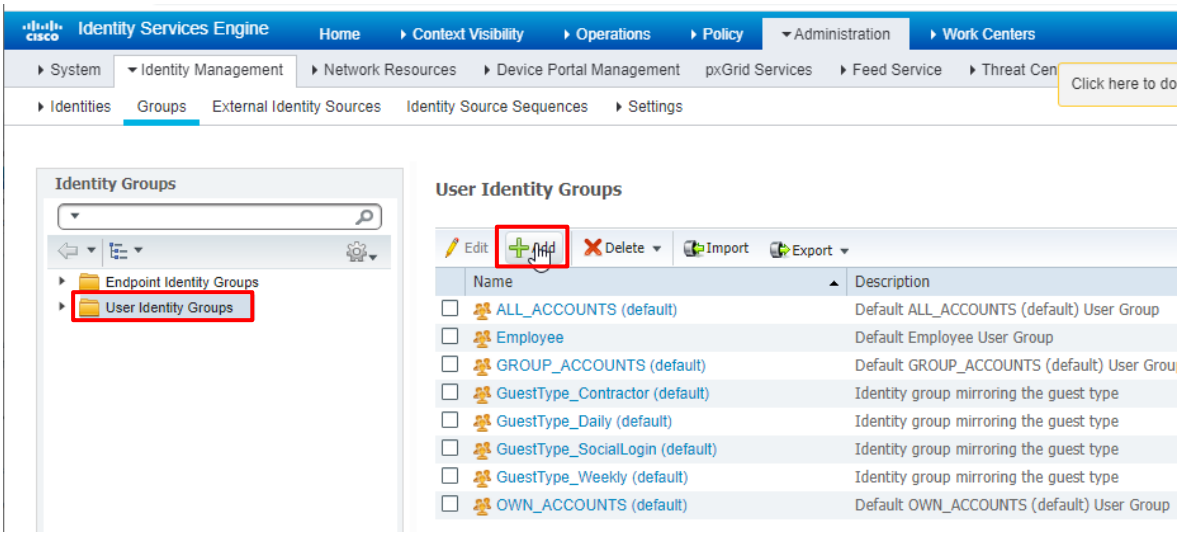


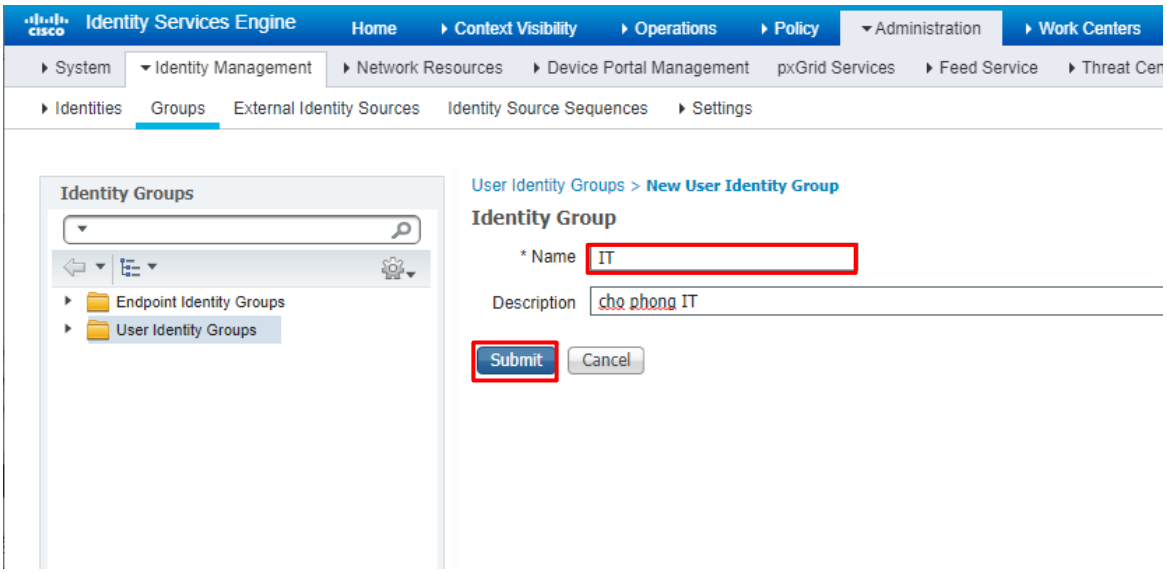
- Cấu hình các thông số như hình rồi nhấn submit:



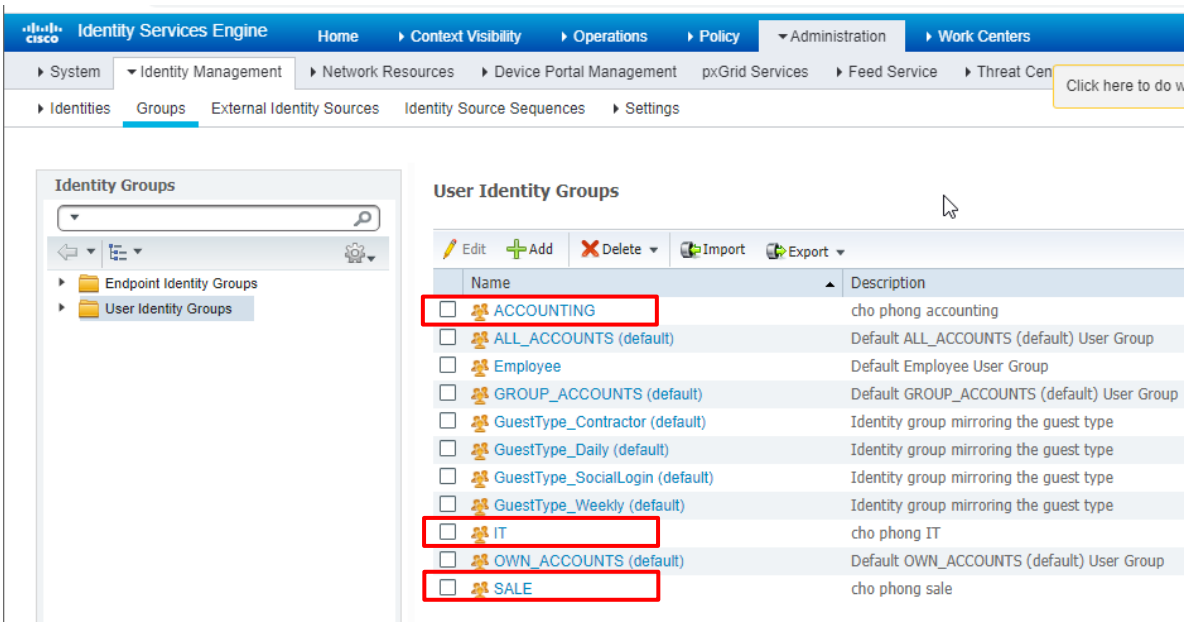
- Cấu hình tạo ra các group IT, SALE và ACCOUNTING trên Cisco ISE: Administration->Groups->User Identity Groups->Add:


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Backup & Restore
Admin Access
Settings
Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
Device Portal Management
Blacklist
BYOD
Certificate Provisioning
Client Provisioning
Mobile Device Management
My Devices
Custom Portal Files
Settings
pxGrid Services
Feed Service
Profiler
Threat Centric NAC
Third Party Vendors

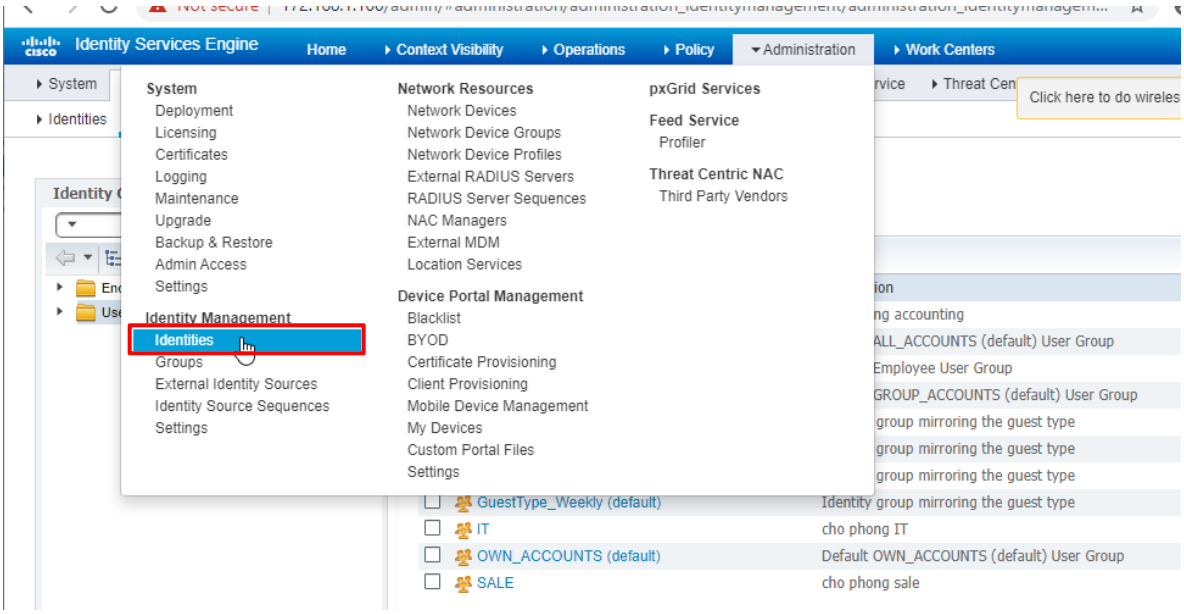

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups
Edit
Add
Delete
Import
Export
Name
Description
ALL_ACCOUNTS (default)
Default ALL_ACCOUNTS (default) User Group
Employee
Default Employee User Group
GROUP_ACCOUNTS (default)
GuestType_Contractor (default)
Identity group mirroring the guest type
GuestType_Daily (default)
GuestType_SocialLogin (default)
GuestType_Weekly (default)
OWN_ACCOUNTS (default)
Default OWN_ACCOUNTS (default) User Group

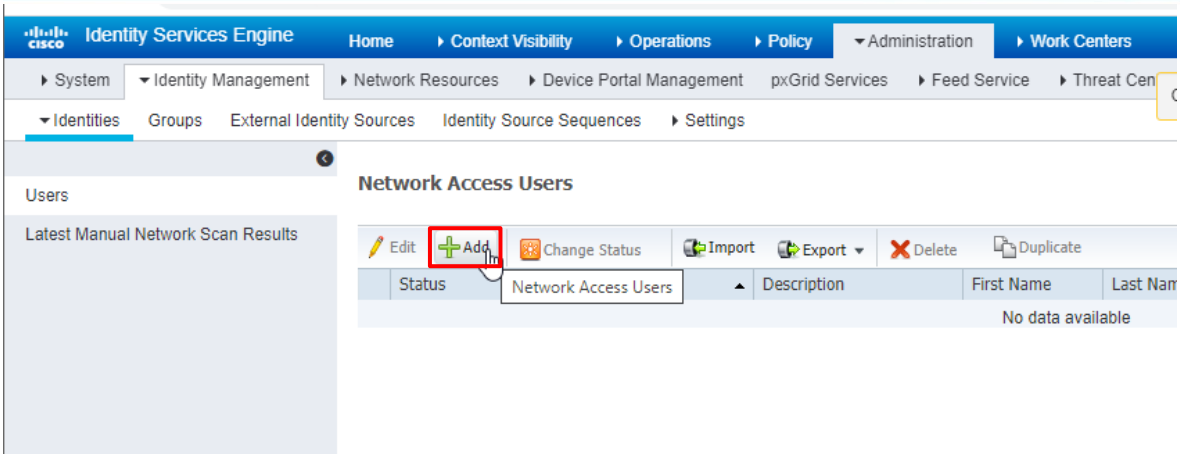

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > New User Identity Group
Identity Group
* Name
IT
Description
cho phong IT
Submit
Cancel

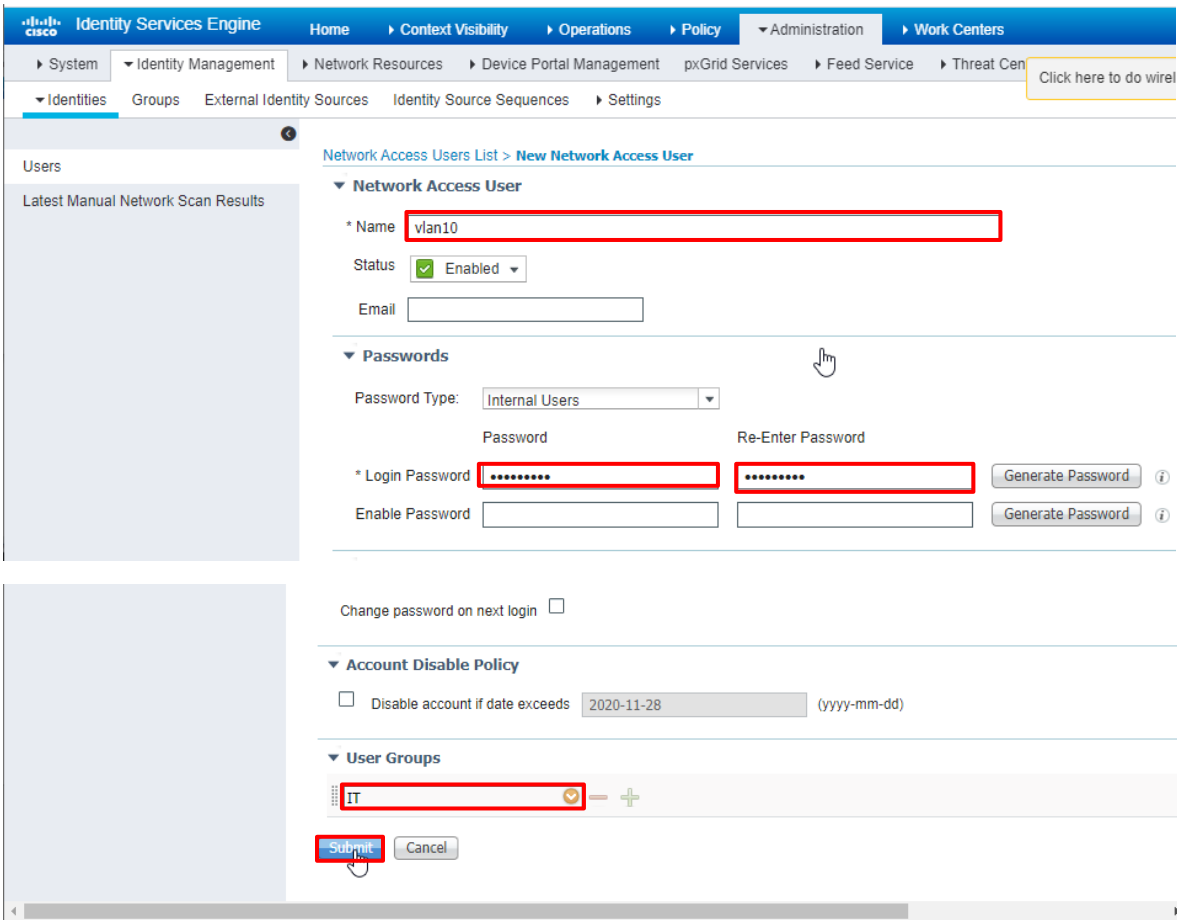
Làm tương tự cho group SALE và ACCOUNTING:



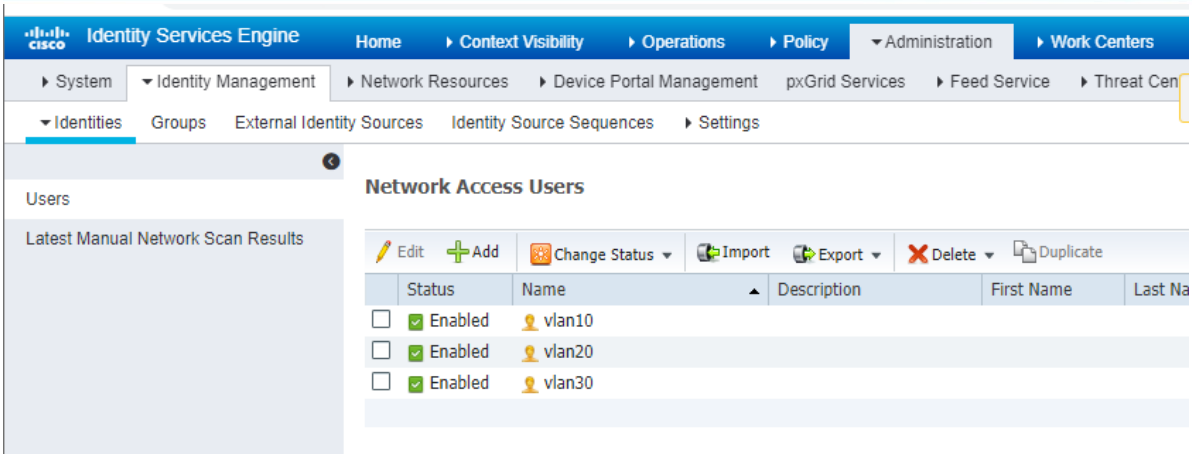
Tạo các user cho các group, đối với group IT tạo username vlan10 pass VnPro@123, group SALE username vlan20 pass VnPro@123 và group ACCOUNTING username vlan30 pass VnPro@123 bằng cách vào Administration->Identities->Users->Add:



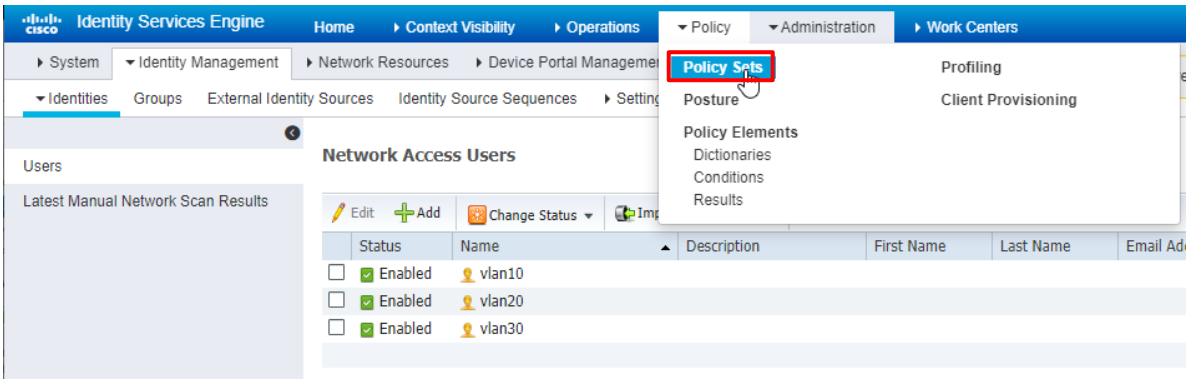




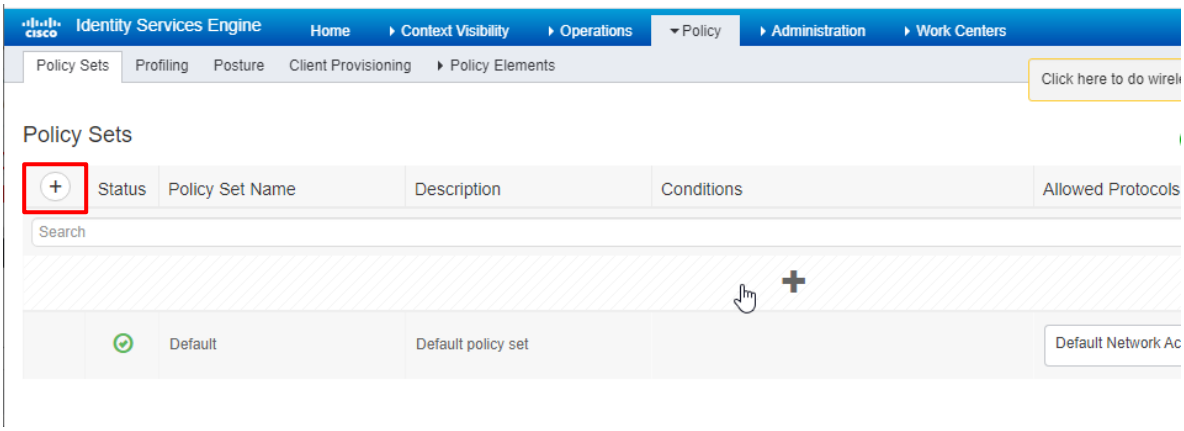
Làm tương tự cho user vlan20 và 30.



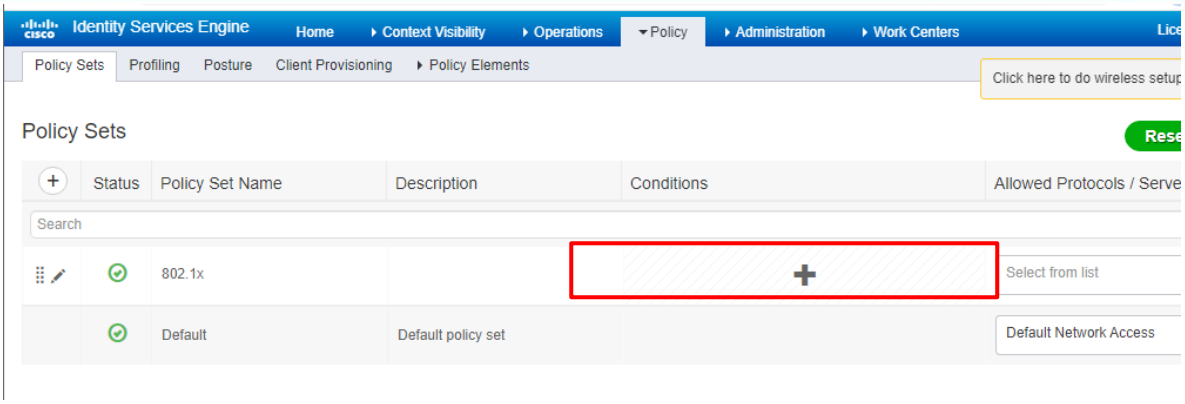
Tạo policy để xác thực Policy->Policy Sets:

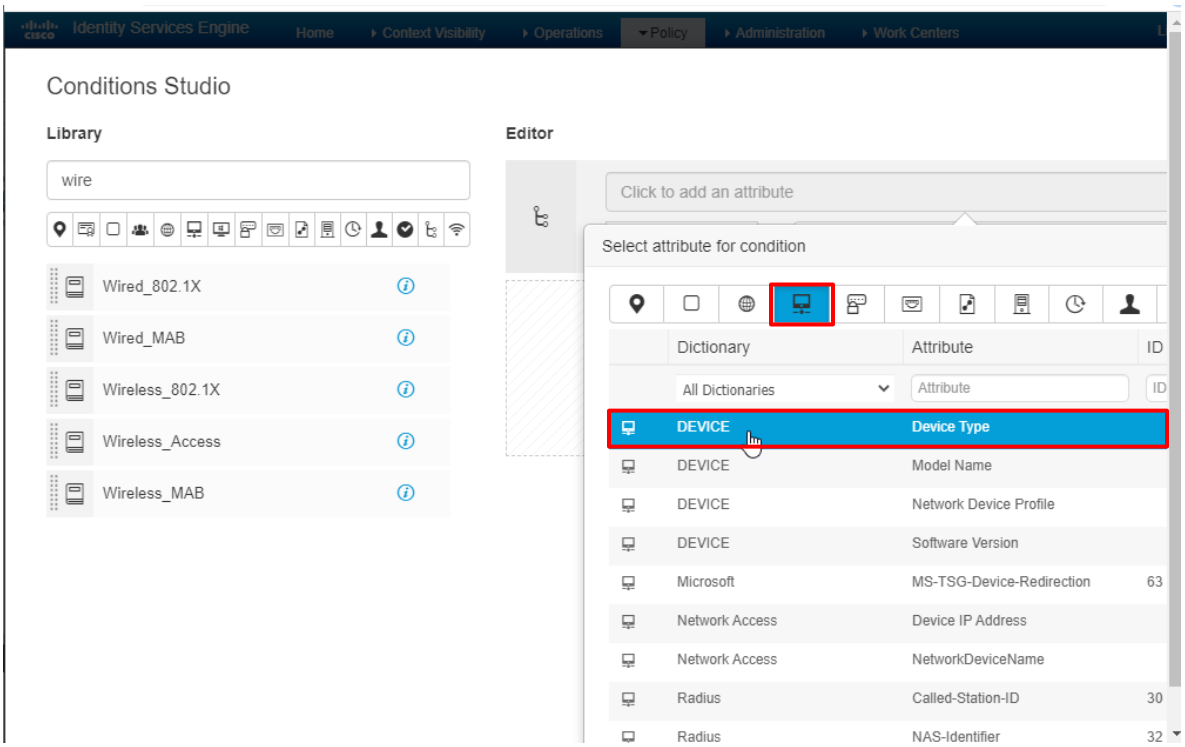


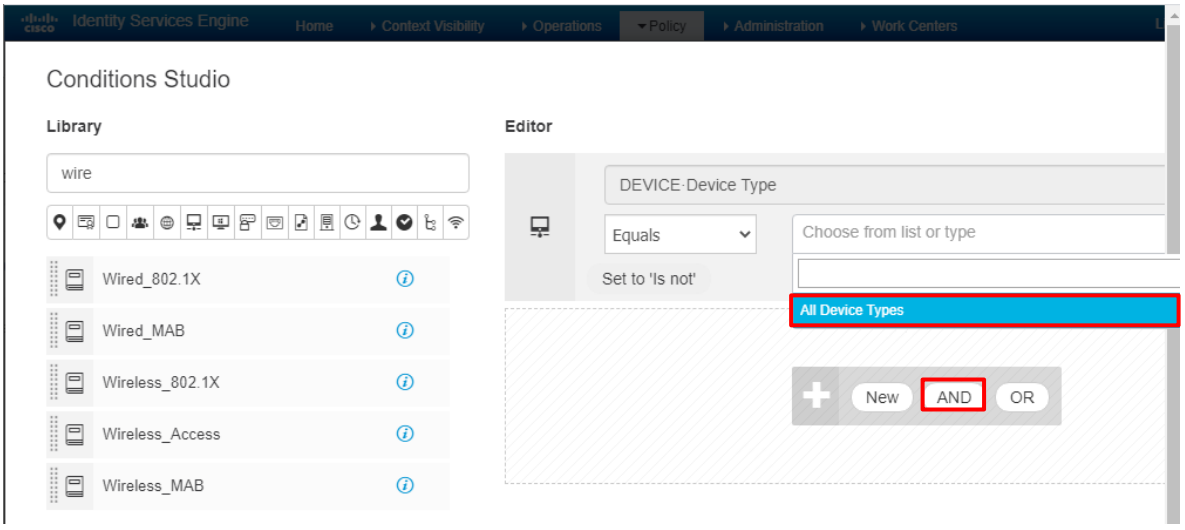
Bấm nút + để tạo ra 1 Policy mới đặt tên là 802.1x

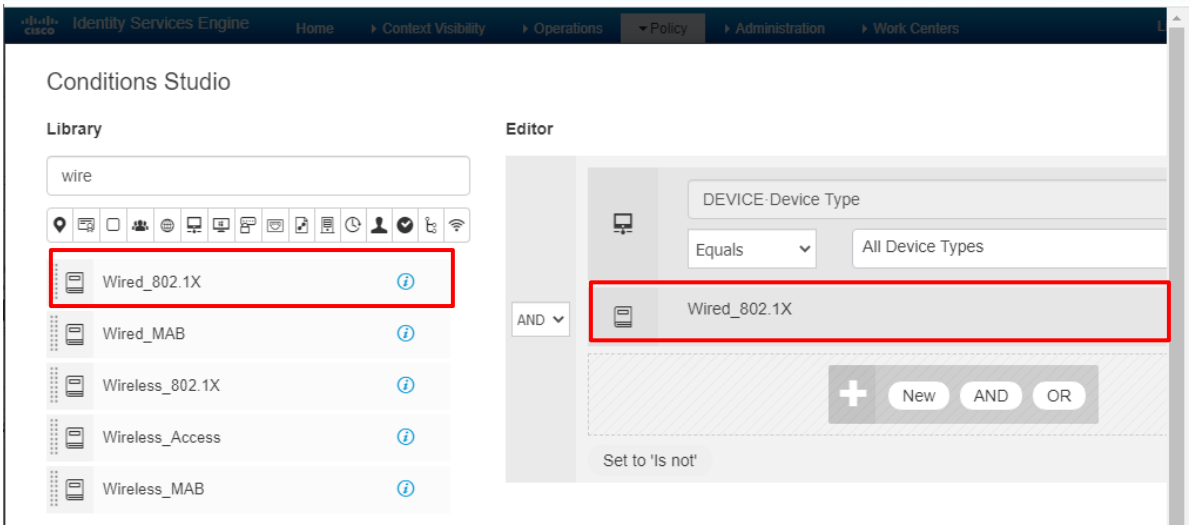


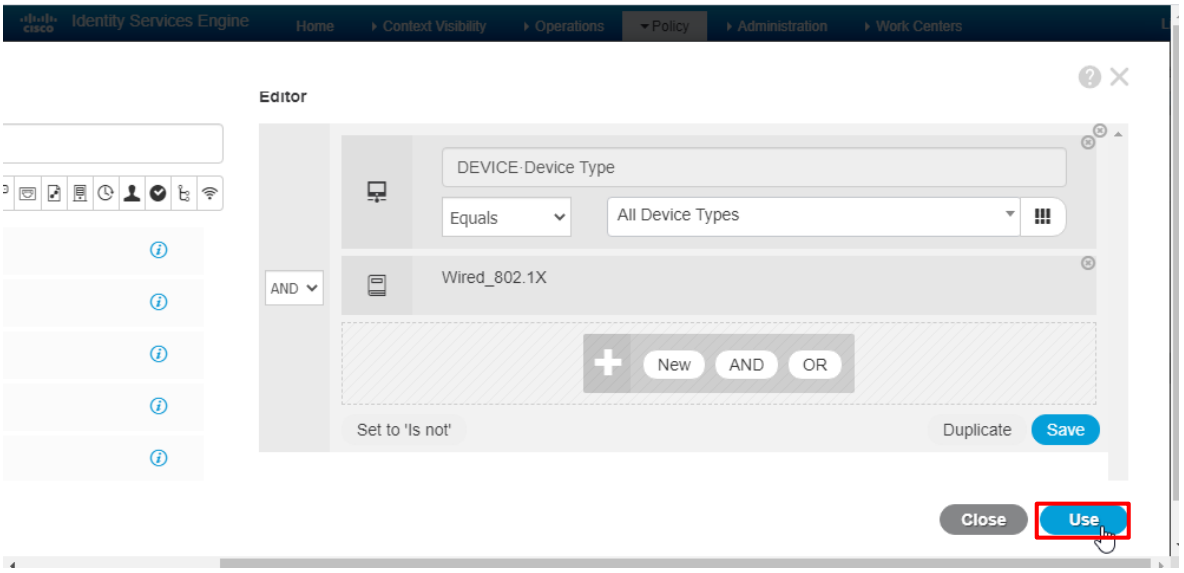
Sau đó bấm + chỗ Conditions của Policy để đặt các điều kiện của Policy


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Policy Sets
Profiling
Posture
Client Provisioning
Policy Elements
Click here to do wireless setup
Policy Sets
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Serve
Search
802.1x
Select from list
Default
Default policy set
Default Network Access

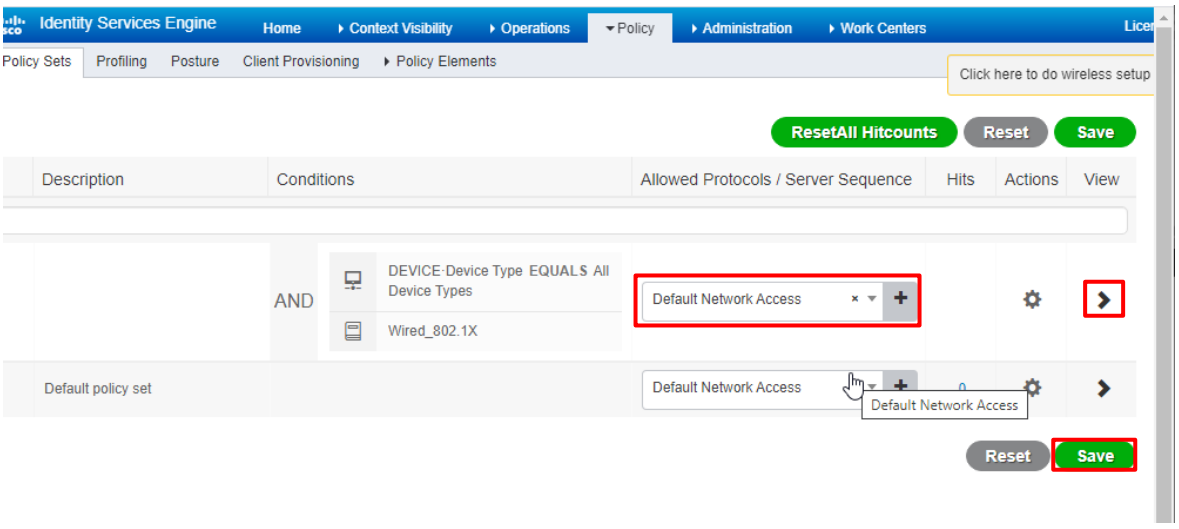

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Conditions Studio
Library
wire
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access
Wireless_MAB
Editor
Click to add an attribute
Select attribute for condition
Dictionary
Attribute
ID
All Dictionaries
Attribute
DEVICE
Device Type
DEVICE
Model Name
DEVICE
Network Device Profile
DEVICE
Software Version
Microsoft
MS-TSG-Device-Redirection
63
Network Access
Device IP Address
Network Access
NetworkDeviceName
Radius
Called-Station-ID
30
Radius
NAS-Identifier
32


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Conditions Studio
Library
wire
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access
Wireless_MAB
Editor
DEVICE·Device Type
Equals
Choose from list or type
Set to 'Is not'
All Device Types
New
AND
OR

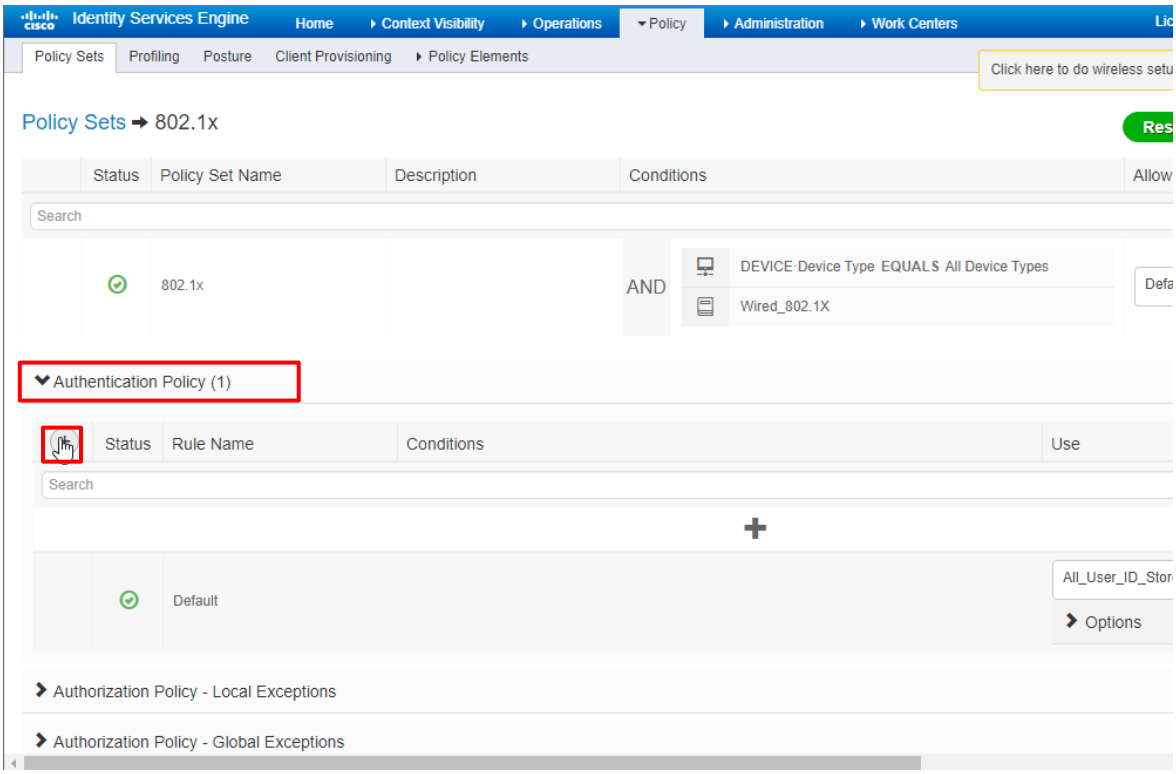


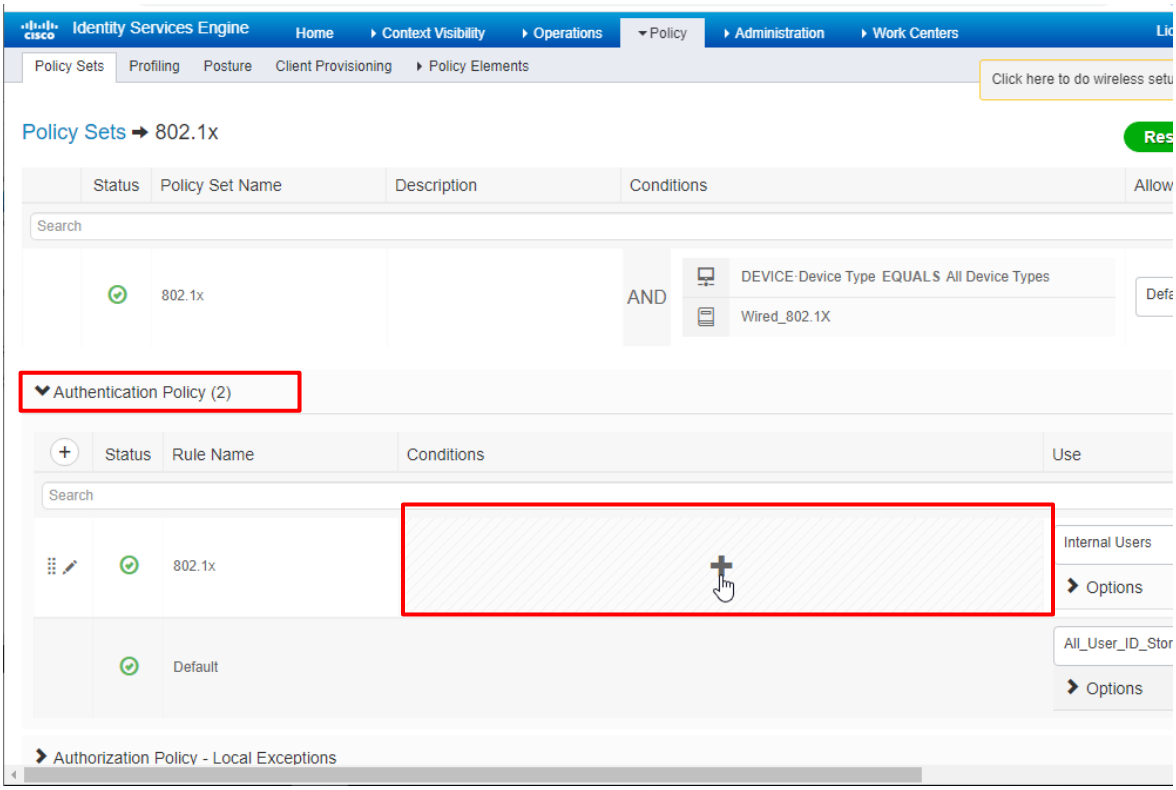


Sau đó chỉnh sửa Policy vừa tạo

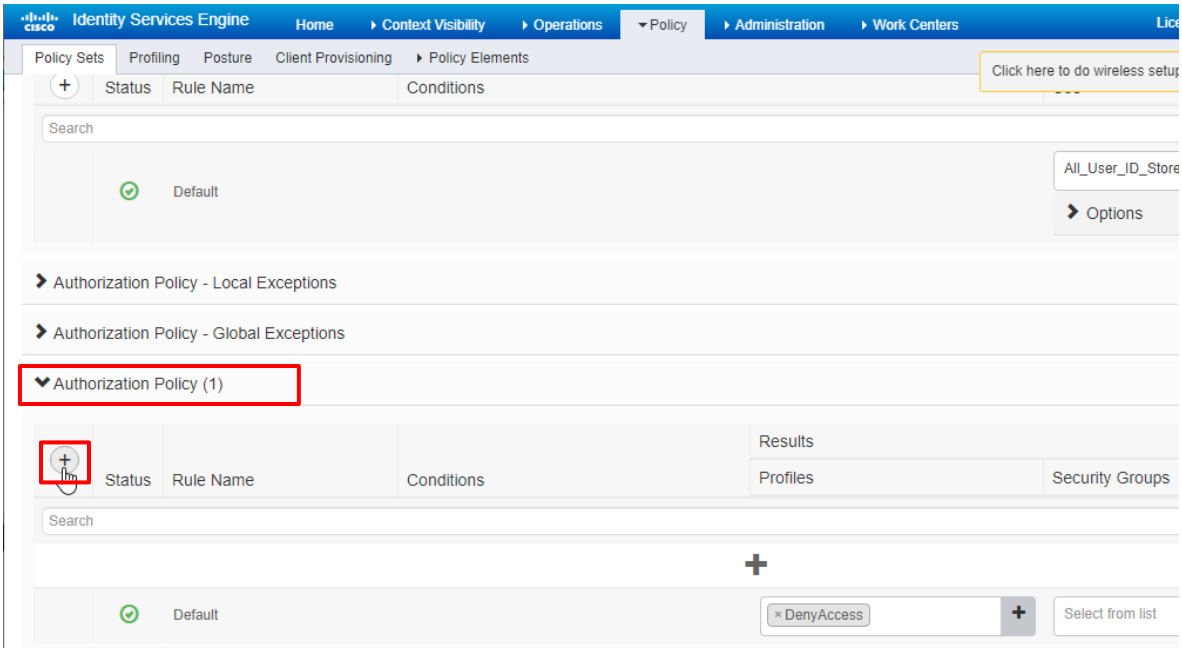


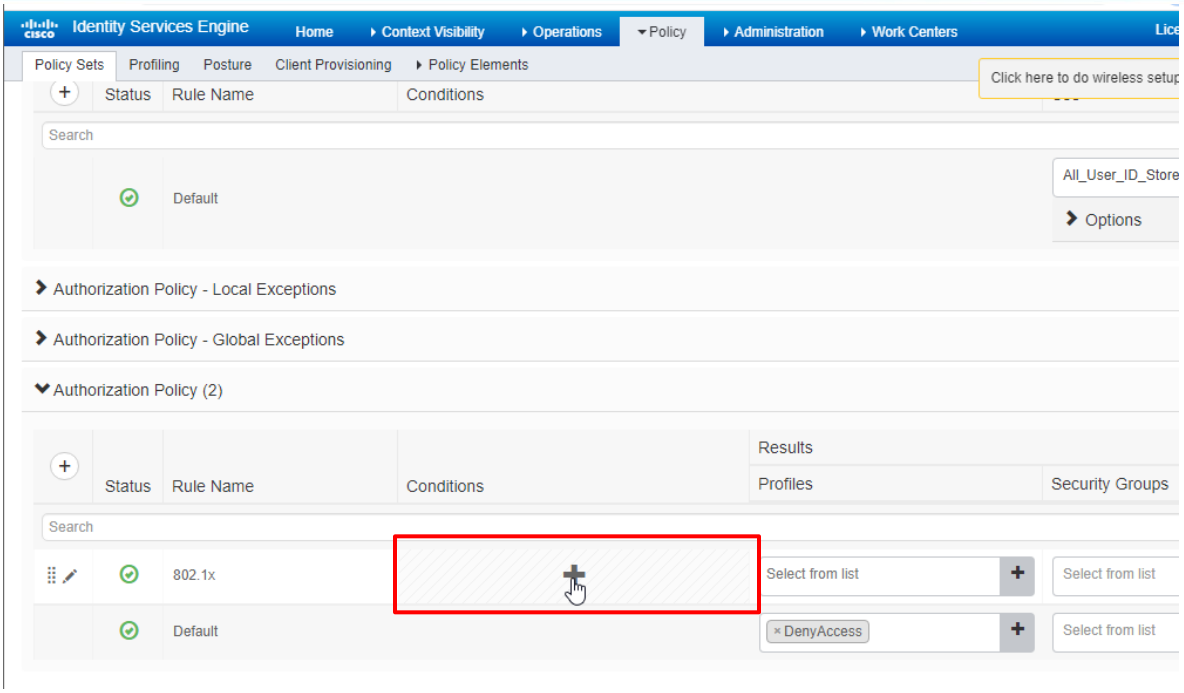
Chổ Authentication Policy

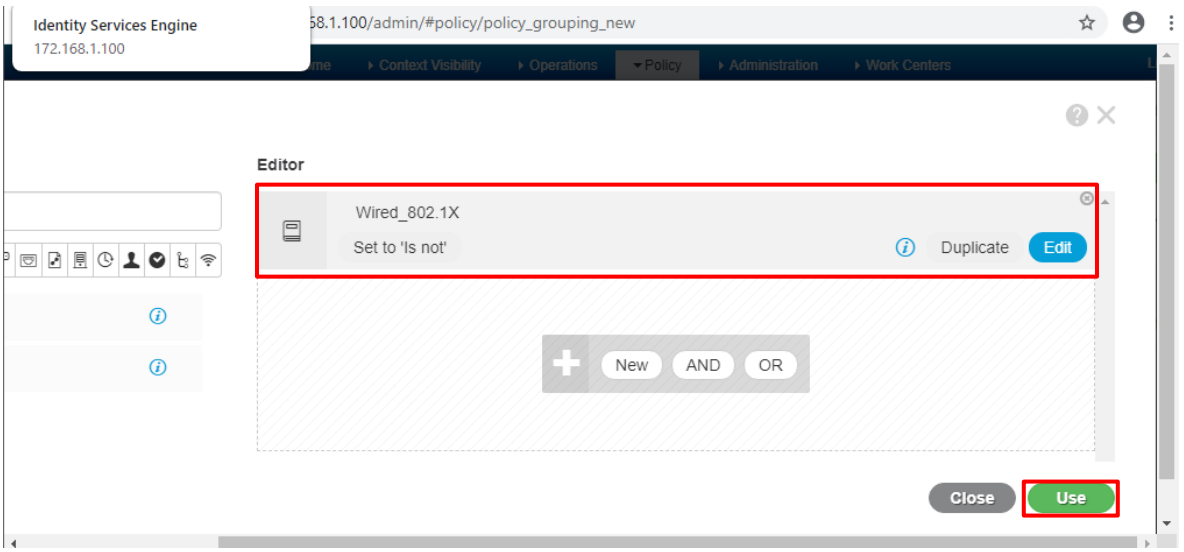


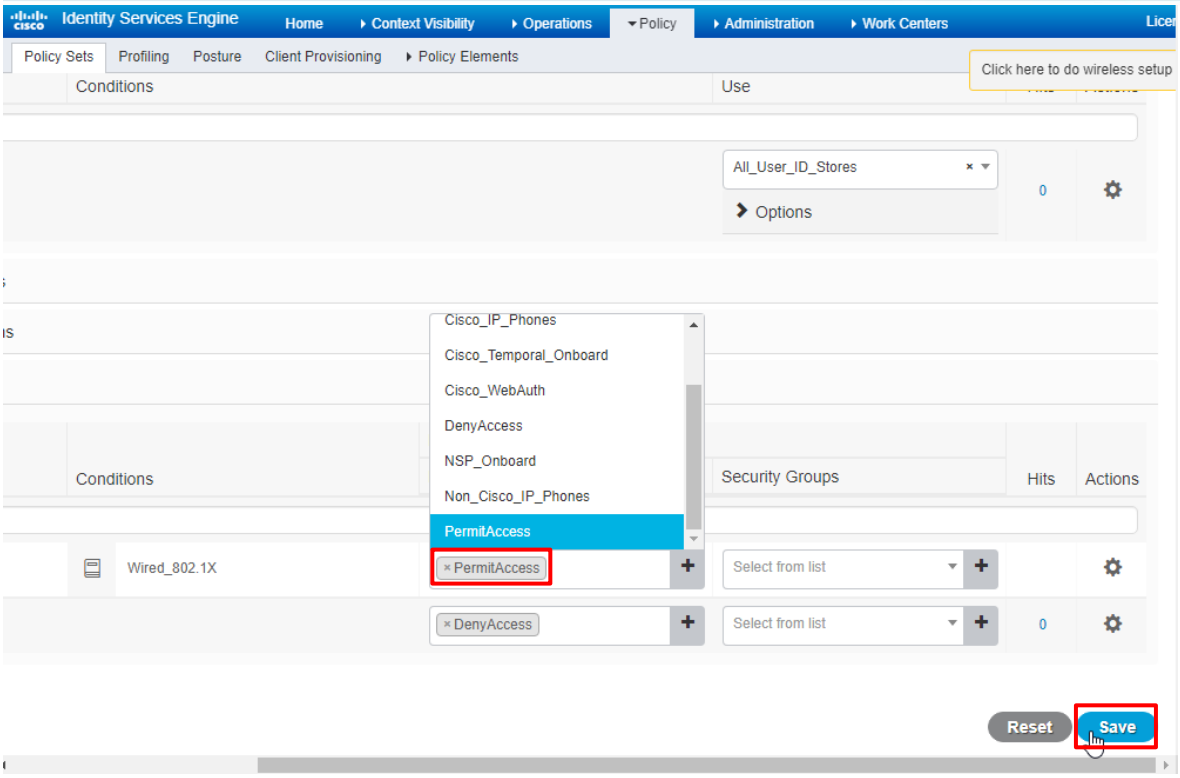


Chỗ Authorization Policy




Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Policy Sets
Profiling
Posture
Client Provisioning
Policy Elements
Click here to do wireless setup
Status
Rule Name
Conditions
Search
Default
All_User_ID_Store
Options
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (2)
Results
Profiles
Security Groups
802.1x
Select from list
DenyAccess


Identity Services Engine
172.168.1.100
58.1.100/admin/#policy/policy_grouping_new
Context Visibility
Operations
Policy
Administration
Work Centers
Editor
Wired_802.1X
Set to 'Is not'
Duplicate
Edit
New
AND
OR
Close
Use



Kiểm tra:

Kiểm tra cấu hình 802.1x trên switch:

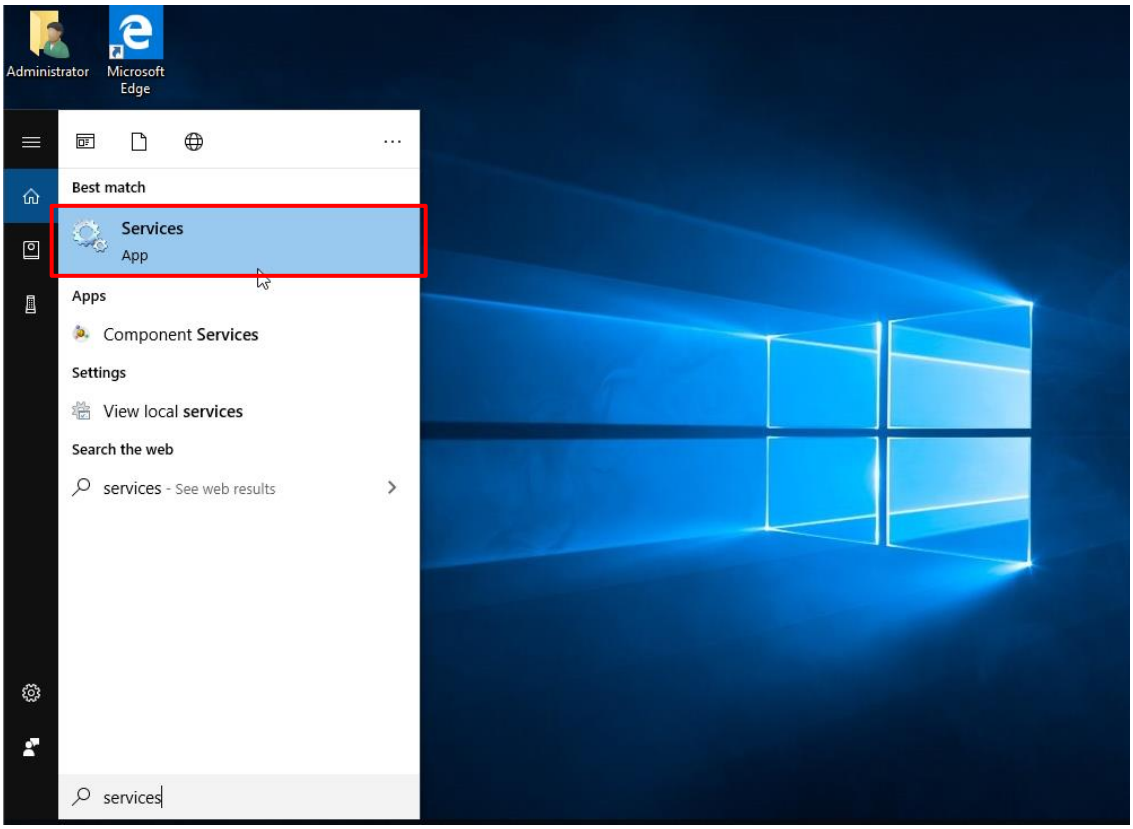
```
SW1#show dot1x all
Sysauthcontrol                  Enabled
Dot1x Protocol Version                3

Dot1x Info for Ethernet0/1
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

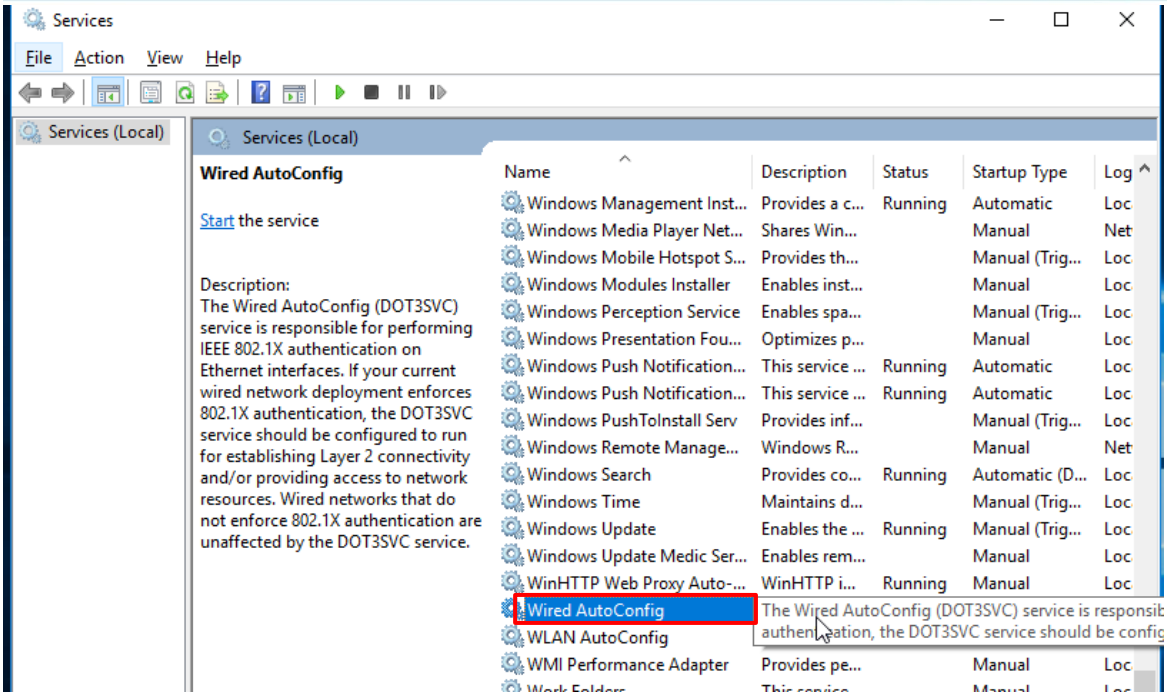
Kiểm tra server radius đã cấu hình trên switch:

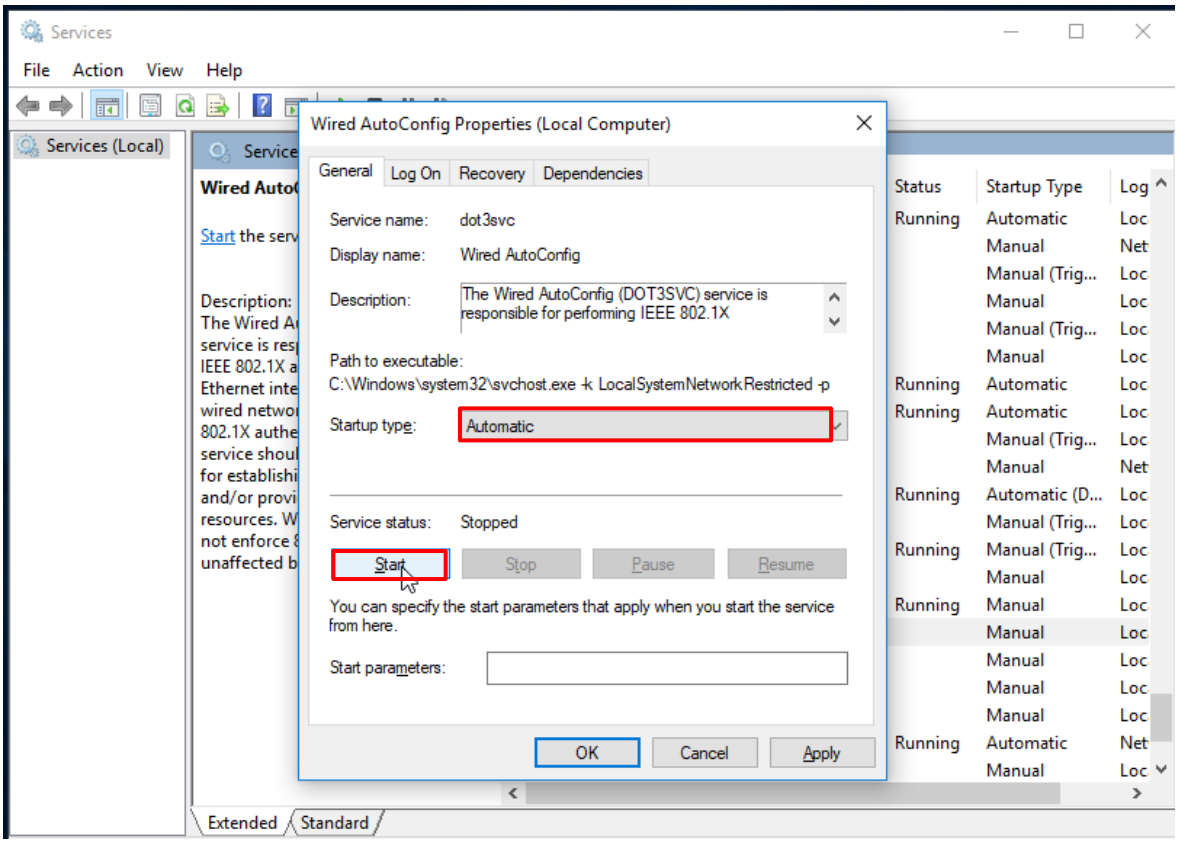
```
SW1#show radius server-group all
```

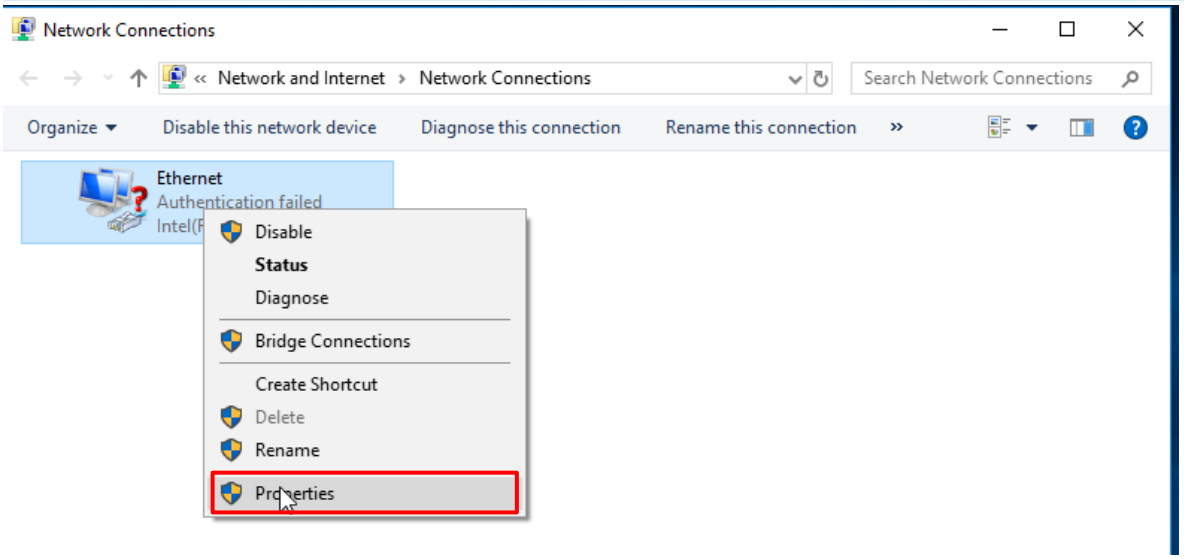
```
Server group radius
    Sharecount = 1   sg_unconfigured = FALSE
    Type = standard   Memlocks = 1
    Server(172.168.1.100:1645,1646) Transactions:
    Authen: 16   Author: 0        Acct: 0
    Server_auto_test_enabled: FALSE
     Keywrap enabled: FALSE
```

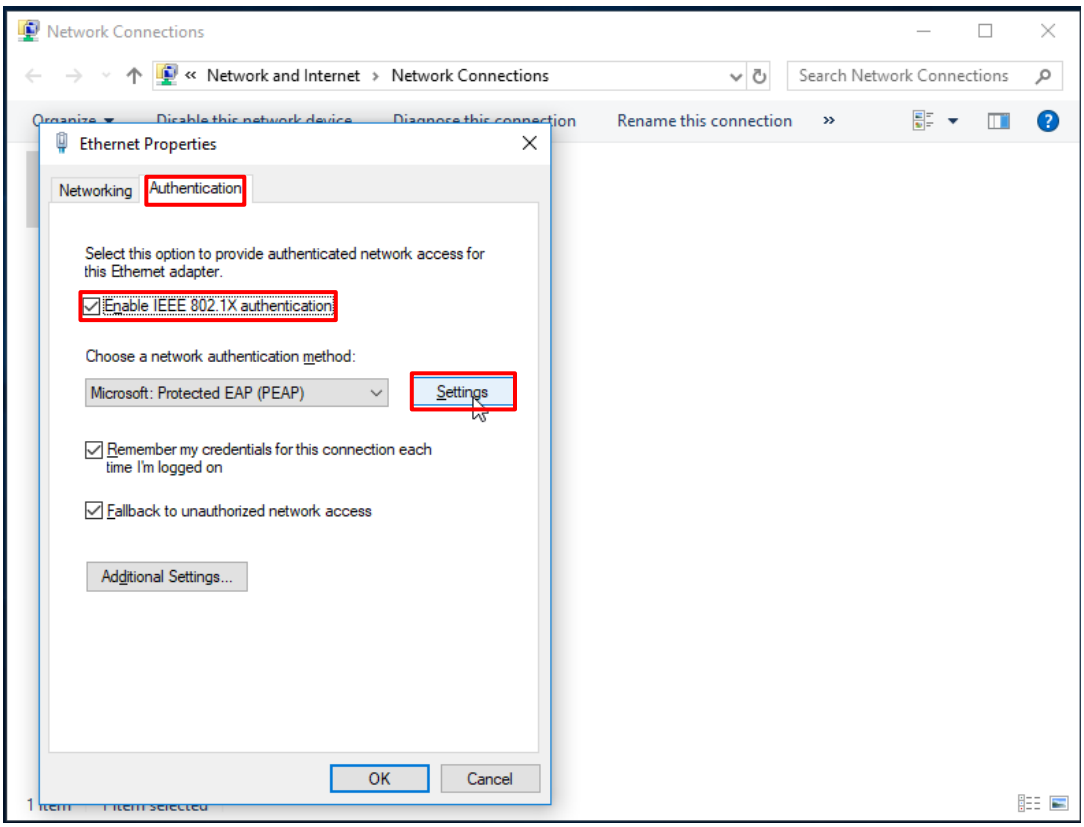
Kiểm tra cấu xác thực trên PC win1:

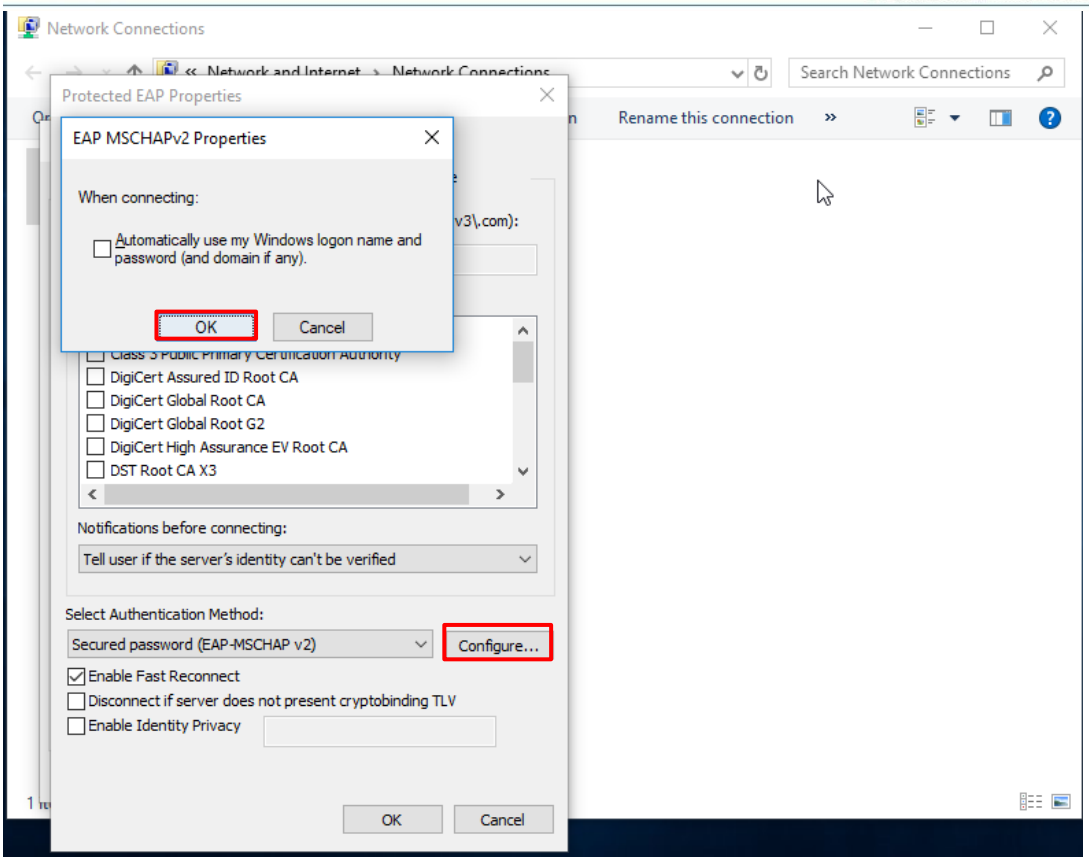


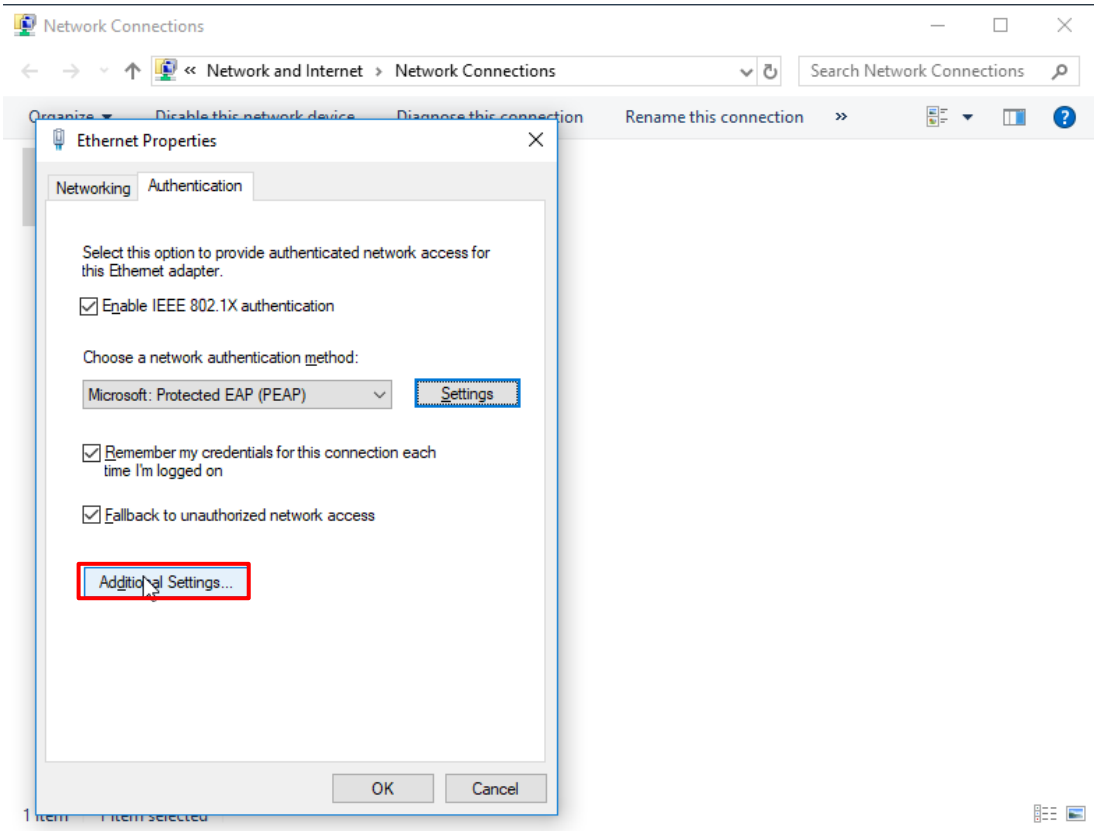

Services
File Action View Help
Services (Local)
Wired AutoConfig
Start the service
Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.
Name
Description
Status
Startup Type
Log
Windows Management Inst... Provides a c... Running Automatic Loc
Windows Media Player Net... Shares Win... Manual Net
Windows Mobile Hotspot S... Provides th... Manual (Trig... Loc
Windows Modules Installer Enables inst... Manual Loc
Windows Perception Service Enables spa... Manual (Trig... Loc
Windows Presentation Fou... Optimizes p... Manual Loc
Windows Push Notification... This service ... Running Automatic Loc
Windows Push Notification... This service ... Running Automatic Loc
Windows PushToInstall Serv Provides inf... Manual (Trig... Loc
Windows Remote Manage... Windows R... Manual Net
Windows Search Provides co... Running Automatic (D... Loc
Windows Time Maintains d... Manual (Trig... Loc
Windows Update Enables the ... Running Manual (Trig... Loc
Windows Update Medic Ser... Enables rem... Manual Loc
WinHTTP Web Proxy Auto-... WinHTTP i... Running Manual Loc
Wired AutoConfig
WLAN AutoConfig
WMI Performance Adapter Provides pe... Manual Loc
The Wired AutoConfig (DOT3SVC) service is responsib
authentication, the DOT3SVC service should be config

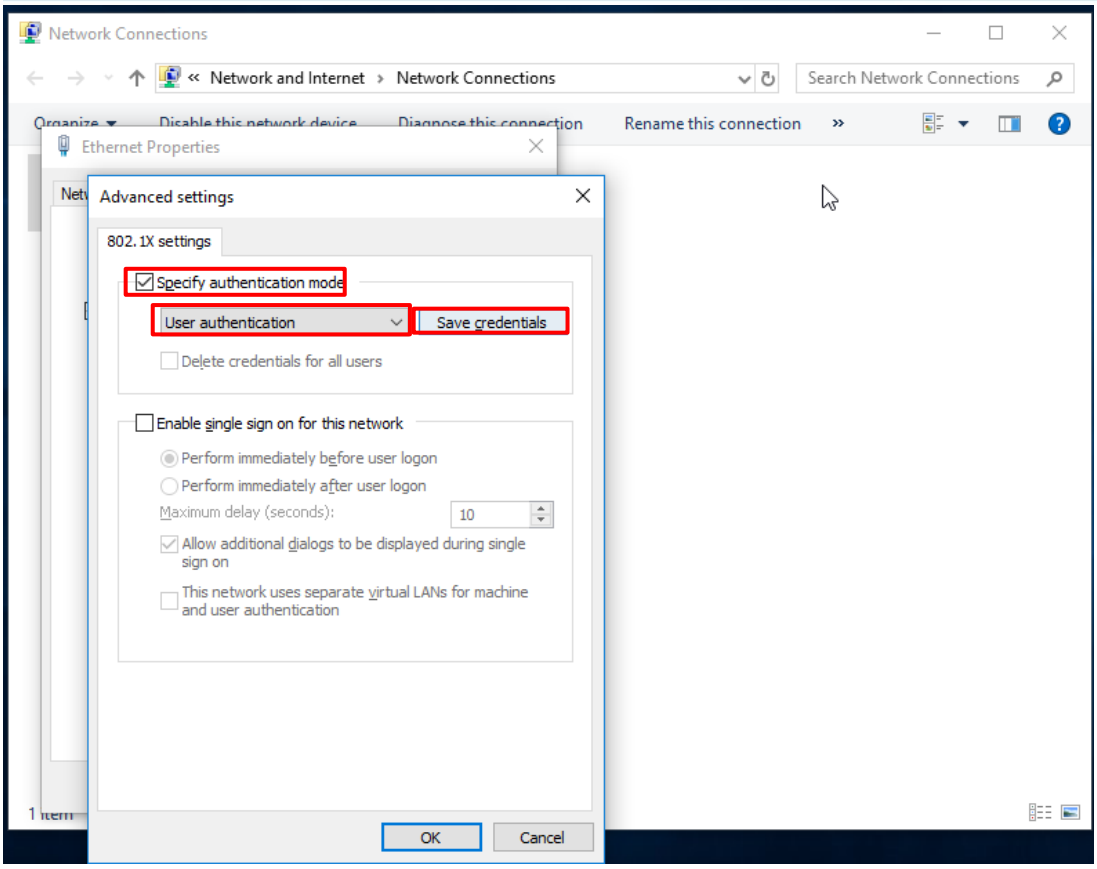

Services
File Action View Help
Services (Local)
Wired AutoConfig Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name: dot3svc
Display name: Wired AutoConfig
Description: The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X
Path to executable:
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Startup type: Automatic
Service status: Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
Extended
Standard

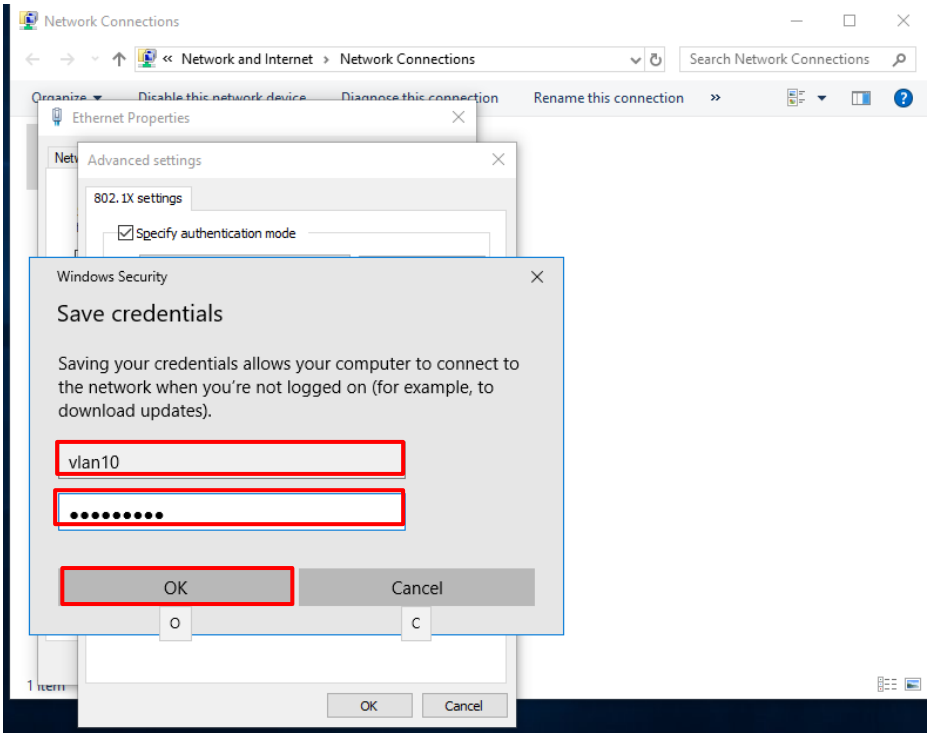

Network Connections
Network and Internet › Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Ethernet
Authentication failed
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties


Network Connections
Network and Internet › Network Connections
Search Network Connections
Rename this connection
Ethernet Properties
Networking
Authentication
Select this option to provide authenticated network access for this Ethernet adapter.
Enable IEEE 802.1X authentication
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Fallback to unauthorized network access
Additional Settings...
OK
Cancel


Network Connections
Search Network Connections
Rename this connection
Protected EAP Properties
EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert Global Root G2
DigiCert High Assurance EV Root CA
DST Root CA X3
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel


Network Connections
Network and Internet › Network Connections
Search Network Connections
Rename this connection
Ethernet Properties
Networking
Authentication
Select this option to provide authenticated network access for this Ethernet adapter.
Enable IEEE 802.1X authentication
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Fallback to unauthorized network access
Additional Settings...
OK
Cancel





Bước 1: Cấu hình dynamic assign vlan:

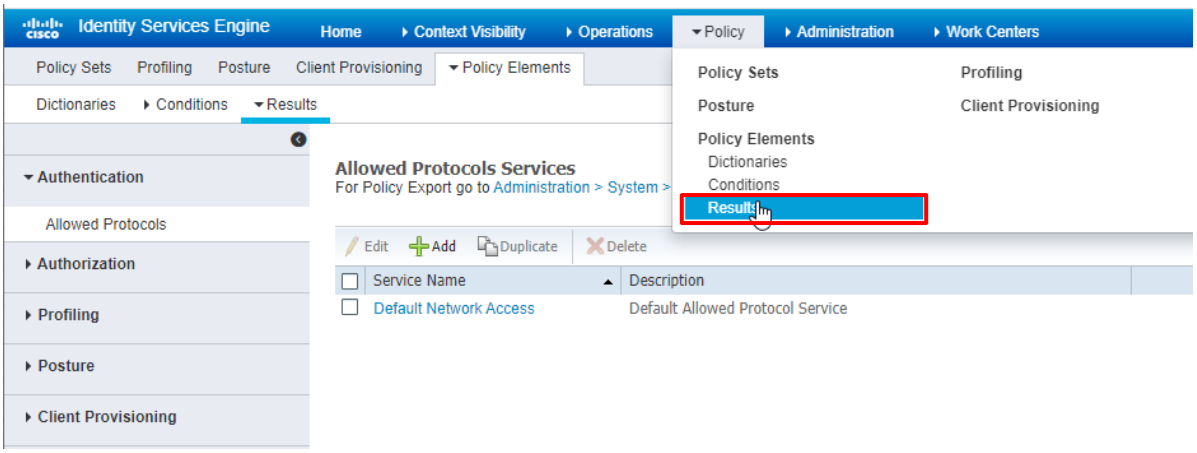
Cấu hình:

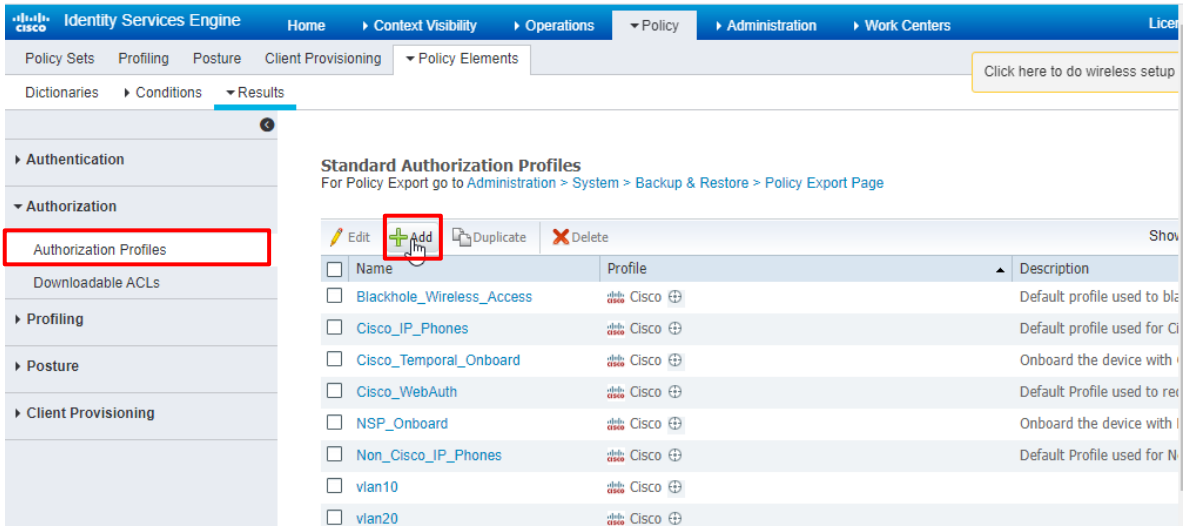
- Cấu hình trên switch:

```
SW1(config)#aaa server radius dynamic-author
SW1(config-locsvr-da-radius)#client 172.168.1.100
SW1(config-locsvr-da-radius)#server-key VnPro123
SW1(config-locsvr-da-radius)#exit
```

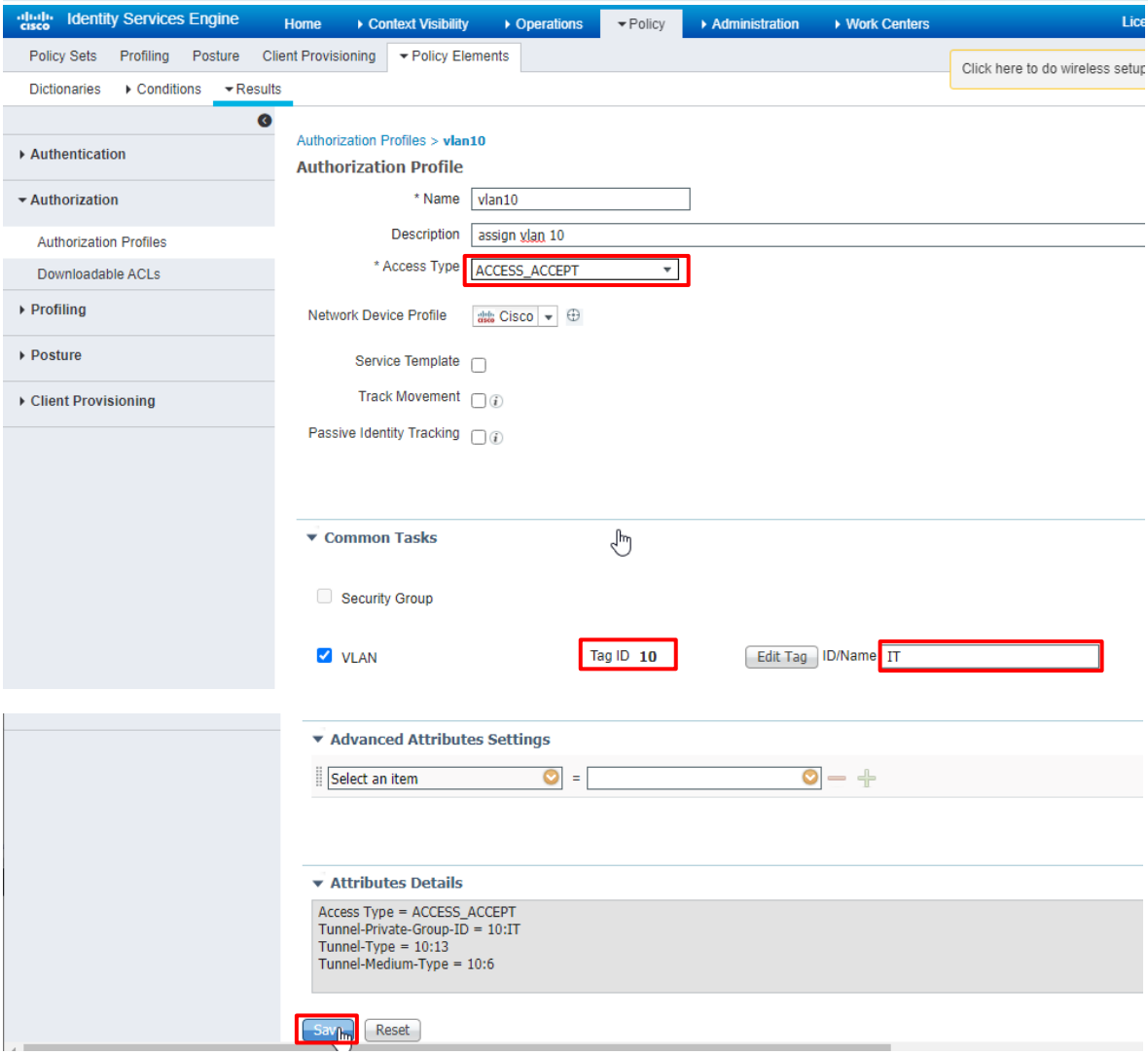
- Cấu hình trên Cisco ISE

Vào Policy->Results->Authorization->Authorization Profiles->Add:



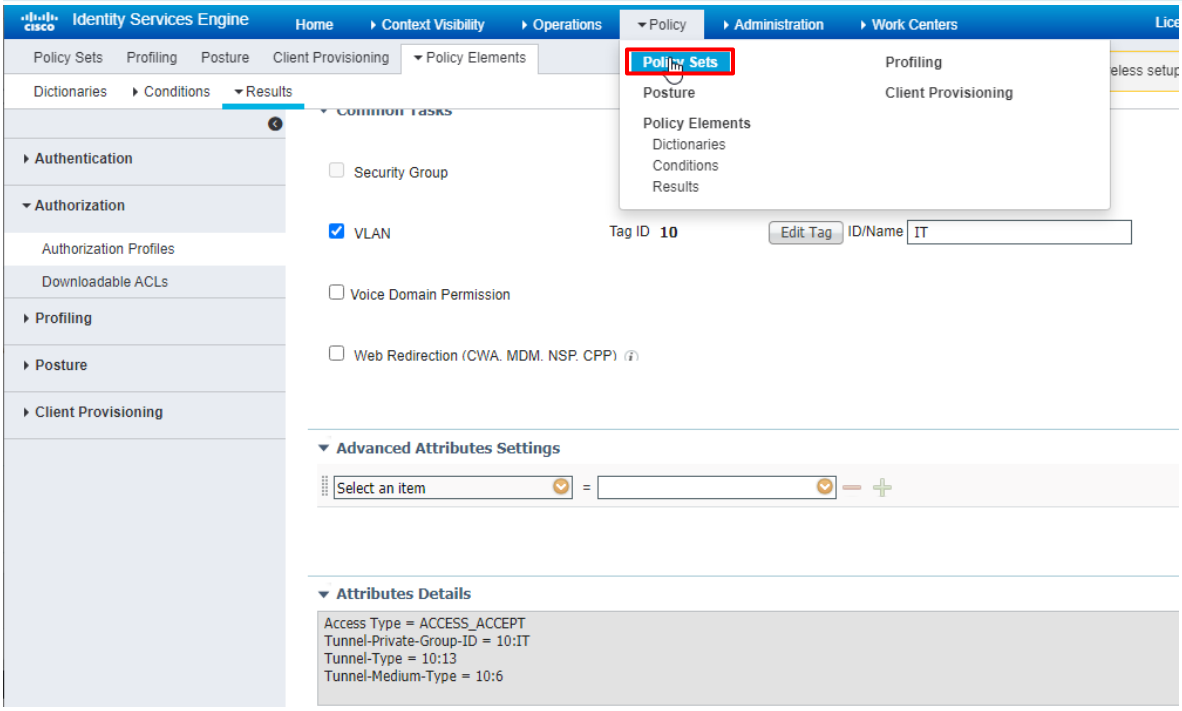


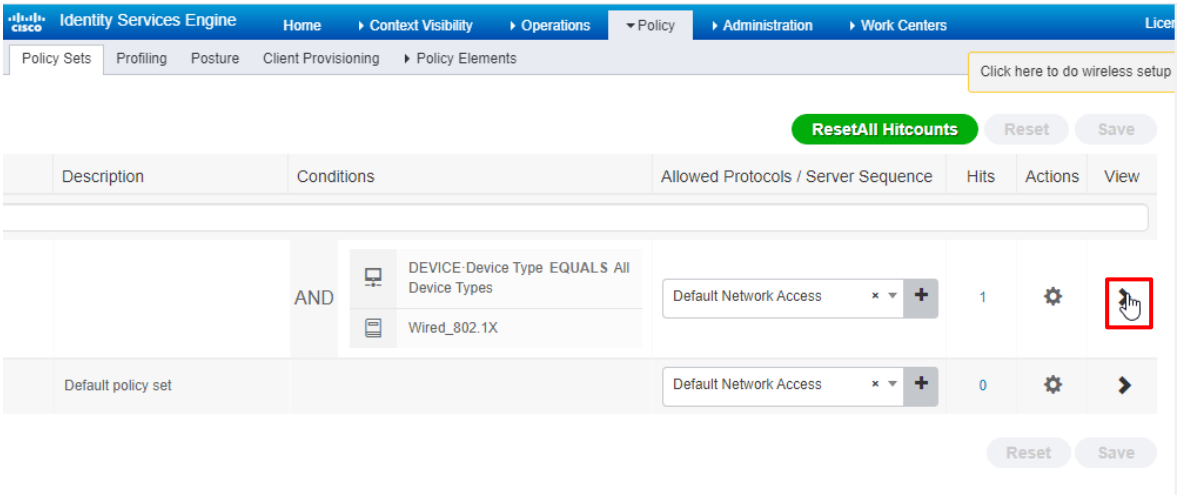
Xem thông tin id và name trên switch bằng lệnh show vlan brief:

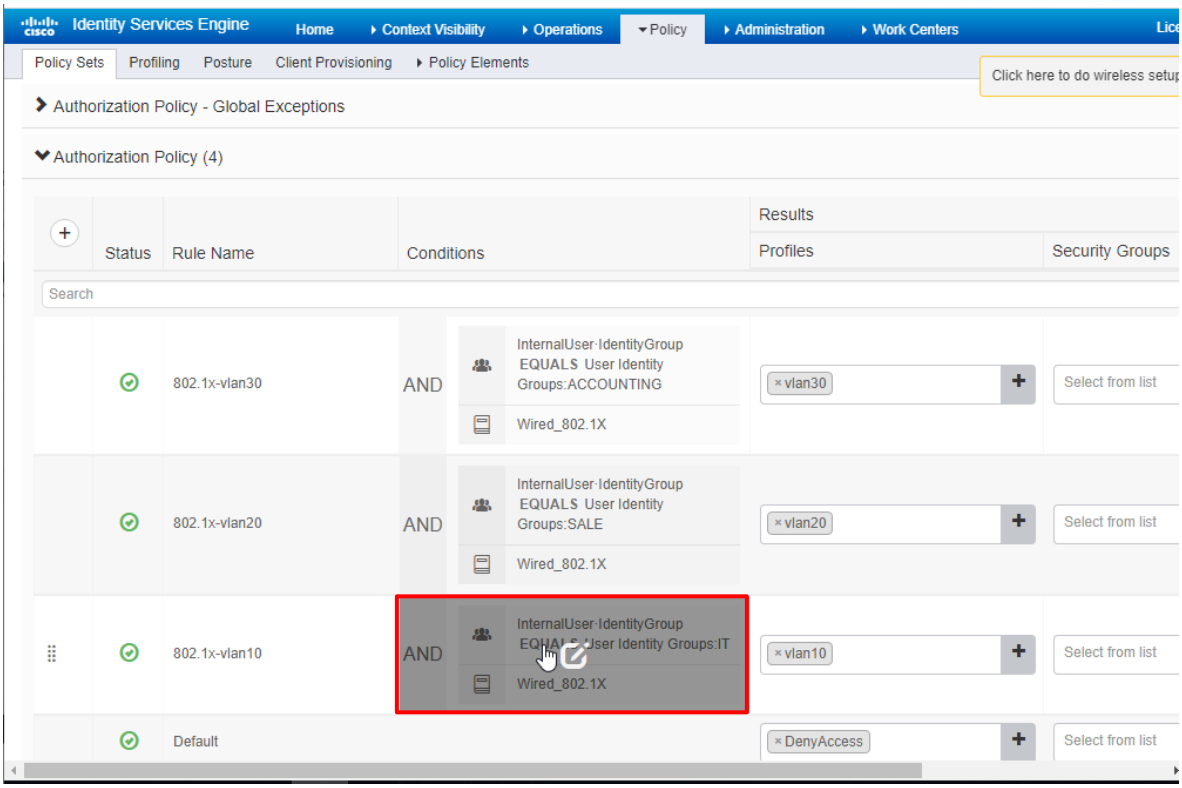


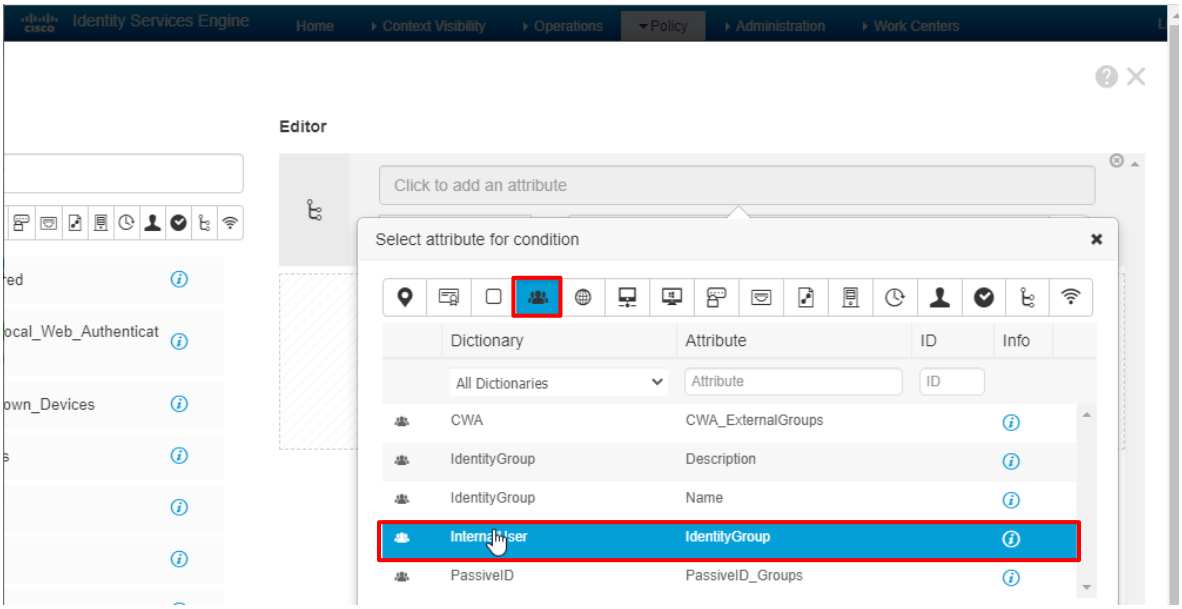
Tạo profile tương tự cho vlan 20 và 30.

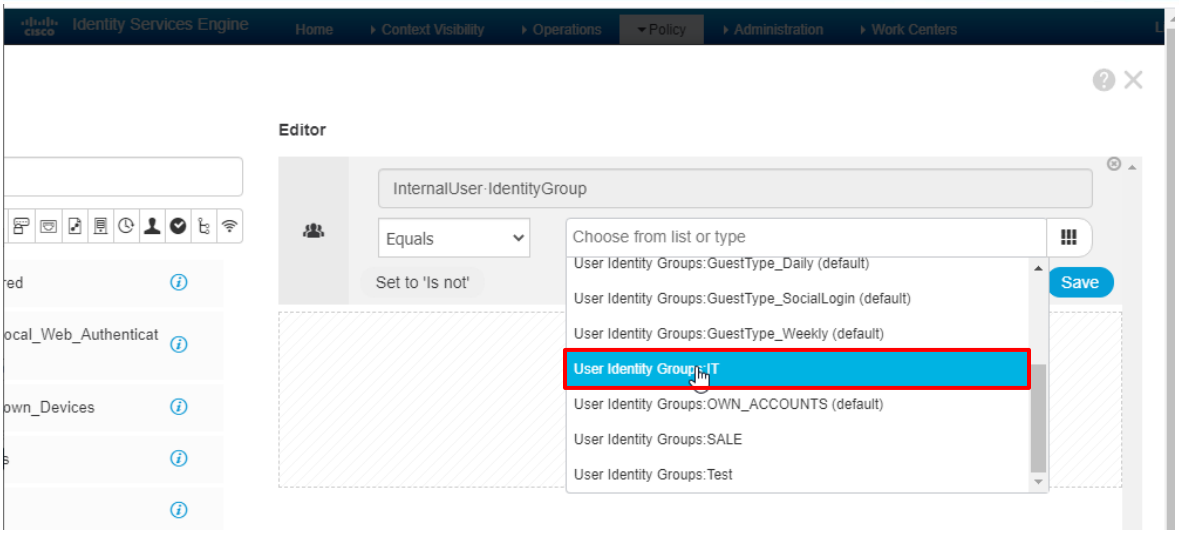
- Chỉnh lại policy:

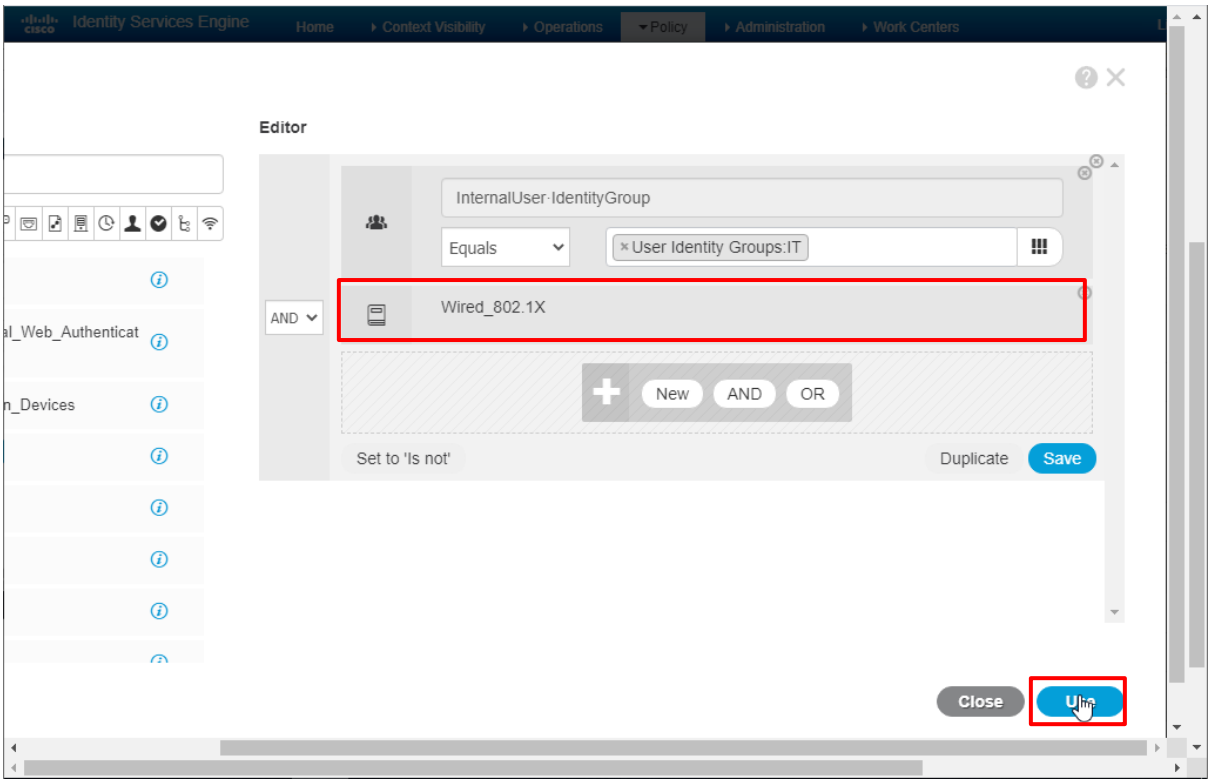

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Policy Sets
Profiling
Posture
Client Provisioning
Policy Elements
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Security Group
VLAN
Tag ID 10
Edit Tag
ID/Name IT
Voice Domain Permission
Web Redirection (CWA, MDM, NSP, CPP)
Advanced Attributes Settings
Select an item
Attributes Details
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 10:IT
Tunnel-Type = 10:13
Tunnel-Medium-Type = 10:6

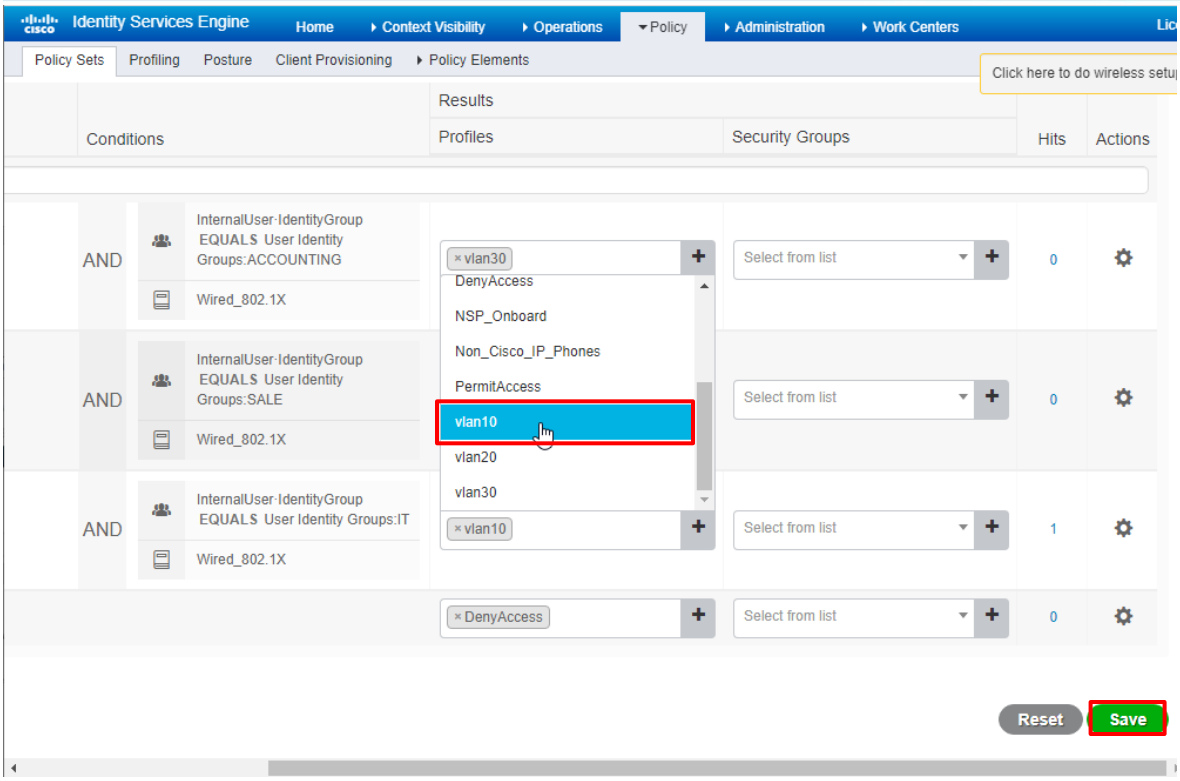

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Policy Sets
Profiling
Posture
Client Provisioning
Policy Elements
Click here to do wireless setup
ResetAll Hitcounts
Reset
Save
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
AND
DEVICE:Device Type EQUALS All Device Types
Wired_802.1X
Default Network Access
1
Default policy set
Default Network Access
0
Reset
Save


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Policy Sets
Profiling
Posture
Client Provisioning
Policy Elements
Click here to do wireless setup
Authorization Policy - Global Exceptions
Authorization Policy (4)
Status
Rule Name
Conditions
Results
Profiles
Security Groups
Search
802.1x-vlan30
AND
InternalUser·IdentityGroup EQUALS User Identity Groups:ACCOUNTING
Wired_802.1X
vlan30
Select from list
802.1x-vlan20
AND
InternalUser·IdentityGroup EQUALS User Identity Groups:SALE
Wired_802.1X
vlan20
Select from list
802.1x-vlan10
AND
InternalUser·IdentityGroup EQUALS User Identity Groups:IT
Wired_802.1X
vlan10
Select from list
Default
DenyAccess
Select from list


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Editor
Click to add an attribute
Select attribute for condition
Dictionary
Attribute
ID
Info
All Dictionaries
Attribute
ID
CWA
CWA_ExternalGroups
IdentityGroup
Description
IdentityGroup
Name
InternalUser
IdentityGroup
PassiveID
PassiveID_Groups


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Editor
InternalUser·IdentityGroup
Equals
Choose from list or type
Set to 'Is not'
Save
User Identity Groups:GuestType_Daily (default)
User Identity Groups:GuestType_SocialLogin (default)
User Identity Groups:GuestType_Weekly (default)
User Identity Groups:IT
User Identity Groups:OWN_ACCOUNTS (default)
User Identity Groups:SALE
User Identity Groups:Test

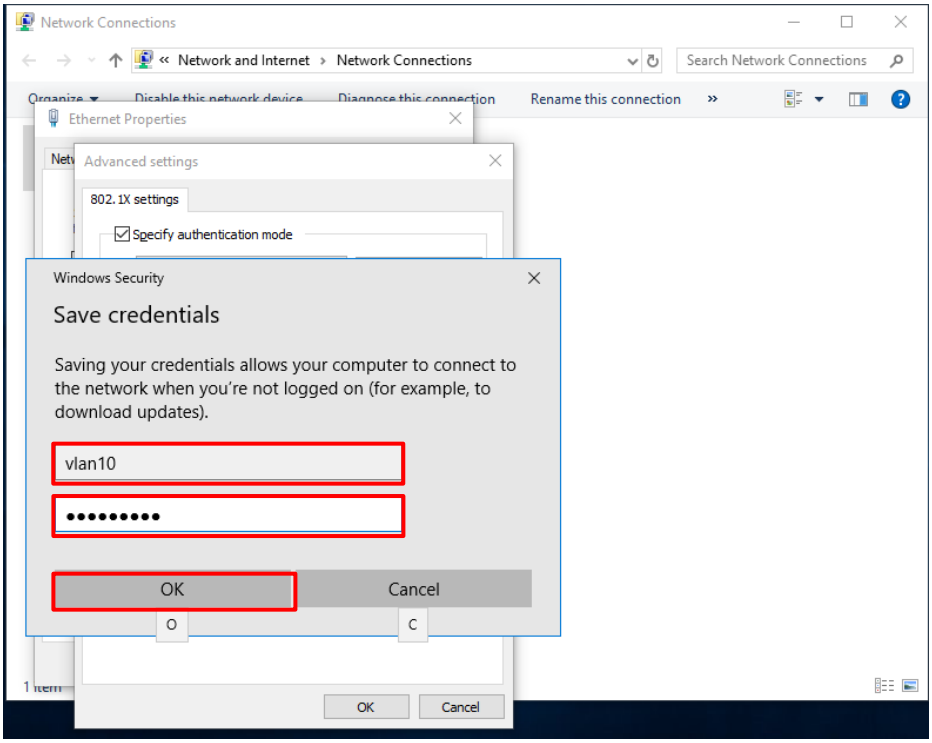

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Editor
InternalUser·IdentityGroup
Equals
User Identity Groups:IT
AND
Wired_802.1X
New
AND
OR
Set to 'Is not'
Duplicate
Save
Close



Làm tương tự cho group SALE và ACCOUNTNG.

Kiểm tra:

Nhập mật khẩu trên win1 và kiểm tra trên switch vlan có thay đổi sang vlan 10 không.



```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Et0/3
10   IT                               active    Et0/1
20   SALE                             active
30   ACCOUNTING                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```