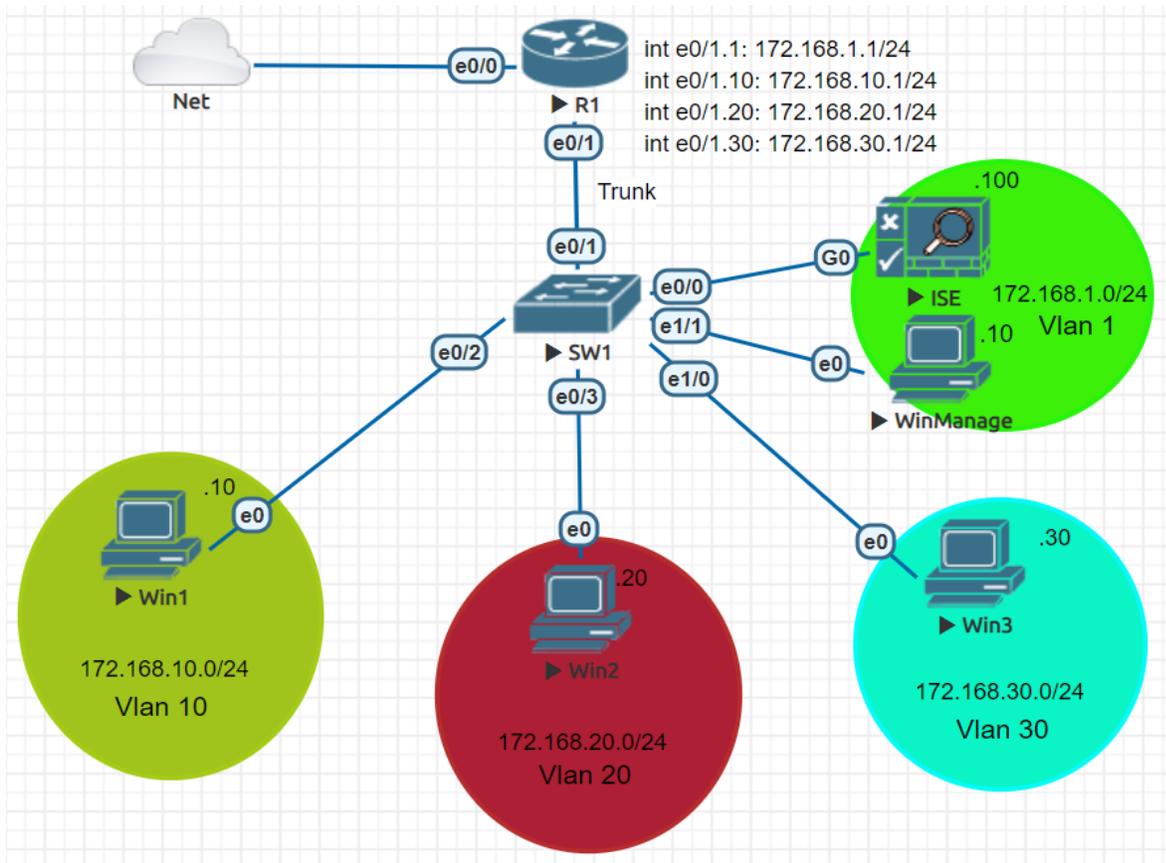


LAB – Cấu hình Dynamic Assign VLAN và 802.1X với Cisco ISE

Sơ đồ:



Mô tả:

- Sơ đồ Lab gồm 1 router, 1 switch layer 2, 1 Cisco ISE đóng vai trò là server RADIUS và 4 PC được đấu nối như hình.
- Trên sơ đồ này, học viên sẽ thực tập cấu hình xác thực 802.1x và dynamic assign vlan cho các PC đảm bảo các PC được xác thực và phân quyền dựa vào các vùng vlan trên mô hình.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị và đặt địa chỉ IP (trừ các PC trong vlan 10, 20 và 30) cũng như các hostname của các thiết bị được chỉ ra mô hình.
2. Trên switch cấu hình trunk trên interface e0/1, cấu hình tạo ra thêm các vlan 10, 20 và 30 đặt tên lần lượt là: IT, SALE, ACCOUNTING. Sau đó cấu hình ip cho vlan 1 là 172.168.1.10/24.
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 1, 10, 20 và 30 điều chỉnh sao cho dhcp cấp địa chỉ như trong

hình cho các PC và cấu hình router-on-stick trên router để các lớp mạng có thể ping thấy nhau.

4. Cấu hình các thông tin cho cisco ise như ip và gateway, cấu hình ip cho PC trong vlan 1. Bắt đầu cấu hình 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.
5. Cấu hình dynamic assign vlan trên Cisco ISE để các PC vào được các vlan như trong mô hình.

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-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:

- Cấu hình đặt ip và gateway cho cisco ise:

```
CiscoISE/admin(config)# interface gigabitEthernet 0
CiscoISE/admin(config-GigabitEthernet)#ip address 172.168.1.100 255.255.255.0
CiscoISE/admin(config-GigabitEthernet)# exit
CiscoISE/admin(config)# ip default-gateway 172.168.1.1
```

- Cấu hình bật xác thực 802.1x trên switch:

```
SW1(config)#aaa new-model
SW1(config)#aaa authentication dot1x default group radius
SW1(config)#aaa authorization network default group radius
SW1(config)#dot1x system-auth-control
SW1(config)#exit
```

- Cấu hình thông tin radius server trên switch:

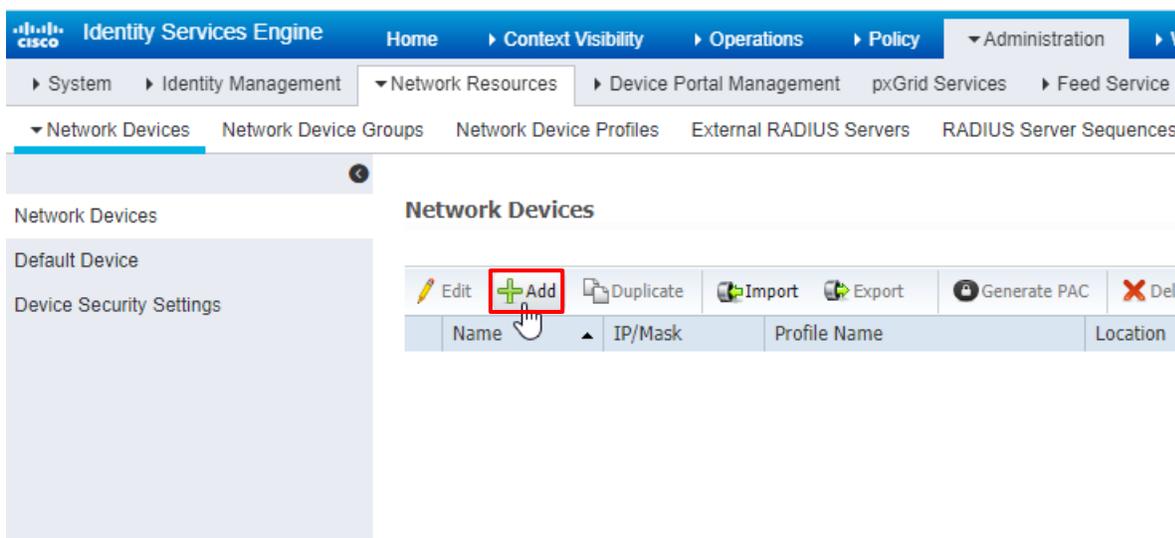
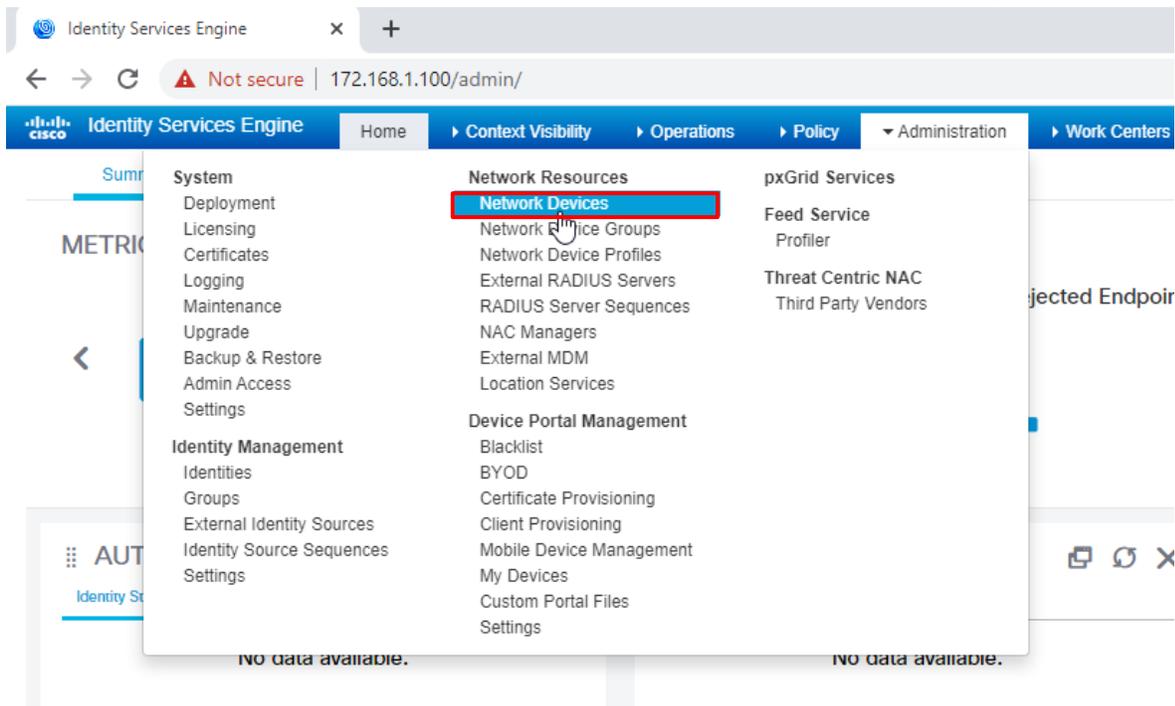
```
SW1(config)#radius server Cisco_ISE
SW1(config-radius-server)#address ipv4 172.168.1.100
SW1(config-radius-server)#key VnPro123
SW1(config-radius-server)#exit
```

- Cấu hình bật 802.1x trên interface e0/2, e0/3 và e1/0:

```
SW1(config)#interface range e0/2-3, e1/0
SW1(config-if-range)#switchport mode access
```

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

- Mở PC Manage vào web và gõ địa chỉ Cisco ISE 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:

Identity Services Engine Administration Work Centers

Network Resources Device Portal Management pxGrid Services Feed Service Threat Center

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

Network Devices List > New Network Device

Network Devices

* Name: SW1
Description: ket noi voi switch 1

IP Address * IP: 172.168.1.10 / 32

* Device Profile: Cisco
Model Name
Software Version

* Network Device Group

Location: All Locations Set To Default
IPSEC: Is IPSEC Device Set To Default
Device Type: All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS
* Shared Secret: VnPro123 Hide
Use Second 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

TACACS Authentication Settings
 SNMP Settings
 Advanced TrustSec Settings

Submit Cancel

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

The screenshot shows the 'Administration' menu in the Identity Services Engine. The 'Groups' option under 'Identity Management' is highlighted with a red box. Other menu items include System, Network Resources, Device Portal Management, and various services like pxGrid and Threat Centric NAC.

The screenshot shows the 'Identity Groups' page. The 'User Identity Groups' section is active, and the 'Add' button is highlighted with a red box. A table lists existing user identity groups with columns for Name and Description.

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

The screenshot shows the 'New User Identity Group' form. The 'Name' field is filled with 'IT' and the 'Description' field is filled with 'cho phong IT'. The 'Submit' button is highlighted with a red box.

User Identity Groups > New User Identity Group

Identity Group

* Name

Description

Làm tương tự cho group SALE và ACCOUNTING:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, and Work Centers. The 'Identities' section is expanded to show 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'User Identity Groups' table is displayed with the following entries:

Name	Description
<input type="checkbox"/> ACCOUNTING	cho phong accounting
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> IT	cho phong IT
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
<input type="checkbox"/> SALE	cho phong sale

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:

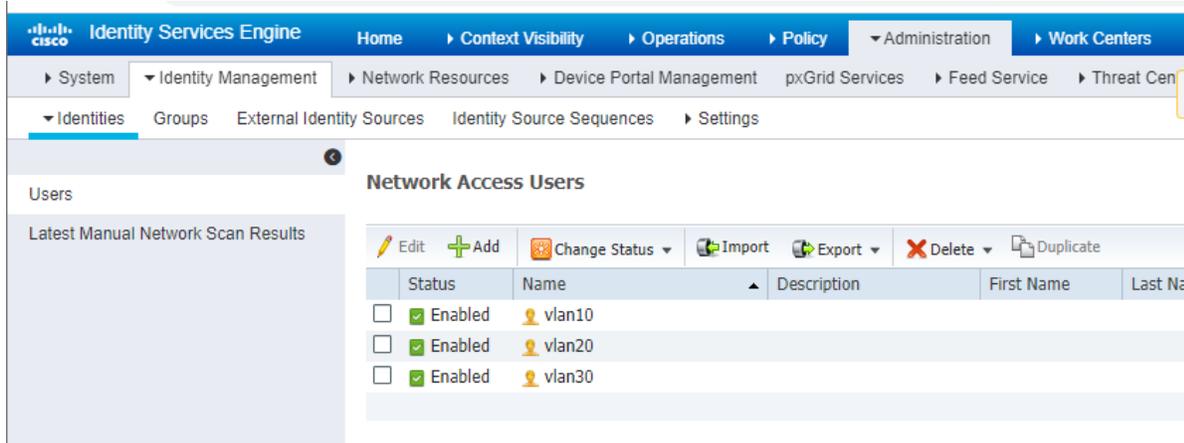
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console with the navigation menu expanded. The 'Identities' option is highlighted with a red box. The menu items are:

- 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

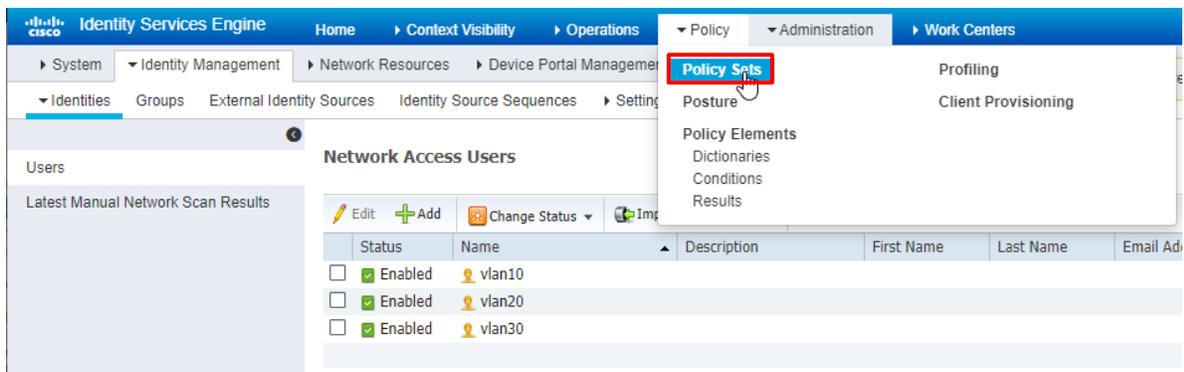
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Center'. The main content area is titled 'Network Access Users' and contains a table with columns for 'Status', 'Network Access Users', 'Description', 'First Name', and 'Last Name'. The table is currently empty, displaying 'No data available'. Above the table, there are several action buttons: 'Edit', 'Add' (highlighted with a red box), 'Change Status', 'Import', 'Export', 'Delete', and 'Duplicate'.

The screenshot shows the 'New Network Access User' form in the Cisco Identity Services Engine. The form is titled 'Network Access Users List > New Network Access User'. It contains several sections: 'Network Access User' with fields for '* Name' (filled with 'vlan10'), 'Status' (set to 'Enabled'), and 'Email'. The 'Passwords' section includes 'Password Type' (set to 'Internal Users'), 'Login Password' (filled with asterisks), 'Re-Enter Password' (filled with asterisks), and 'Enable Password' (empty). There are 'Generate Password' buttons with information icons. A checkbox for 'Change password on next login' is present. The 'Account Disable Policy' section has a checkbox for 'Disable account if date exceeds' with a date field set to '2020-11-28'. The 'User Groups' section shows a dropdown menu with 'IT' selected. At the bottom, there are 'Submit' and 'Cancel' buttons.

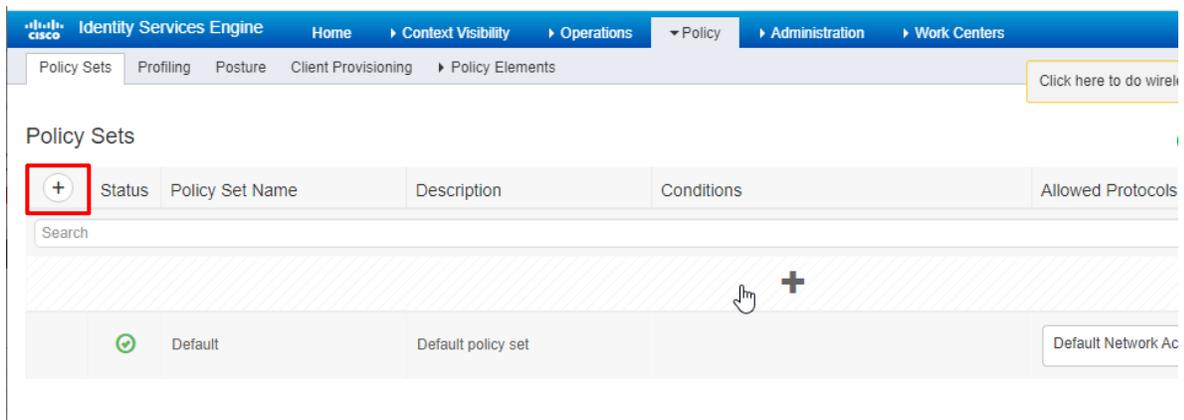
Làm tương tự cho user vlan20 và 30.



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
	✔	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	ID
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

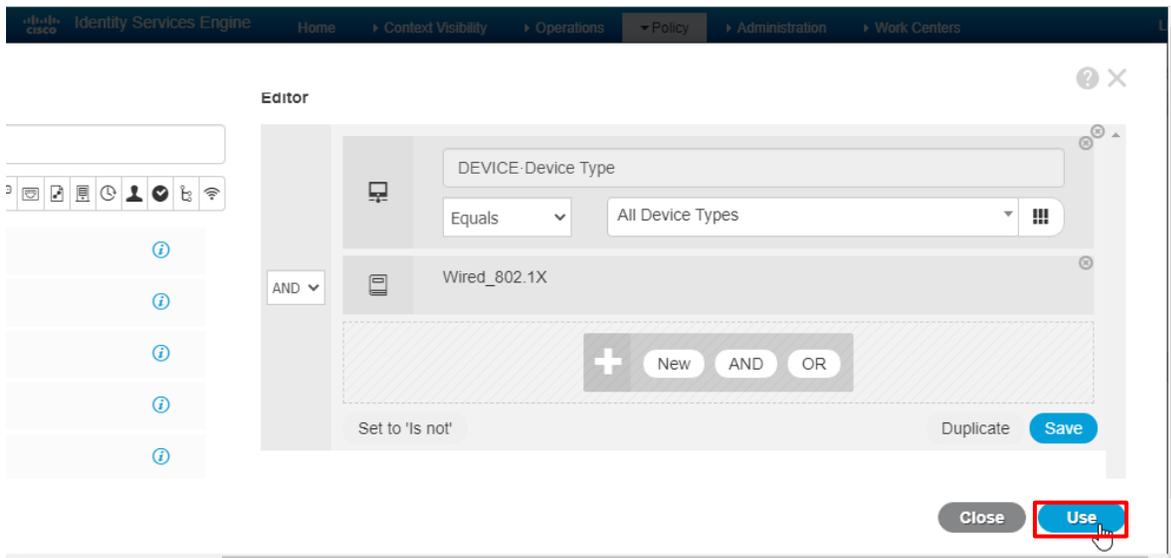
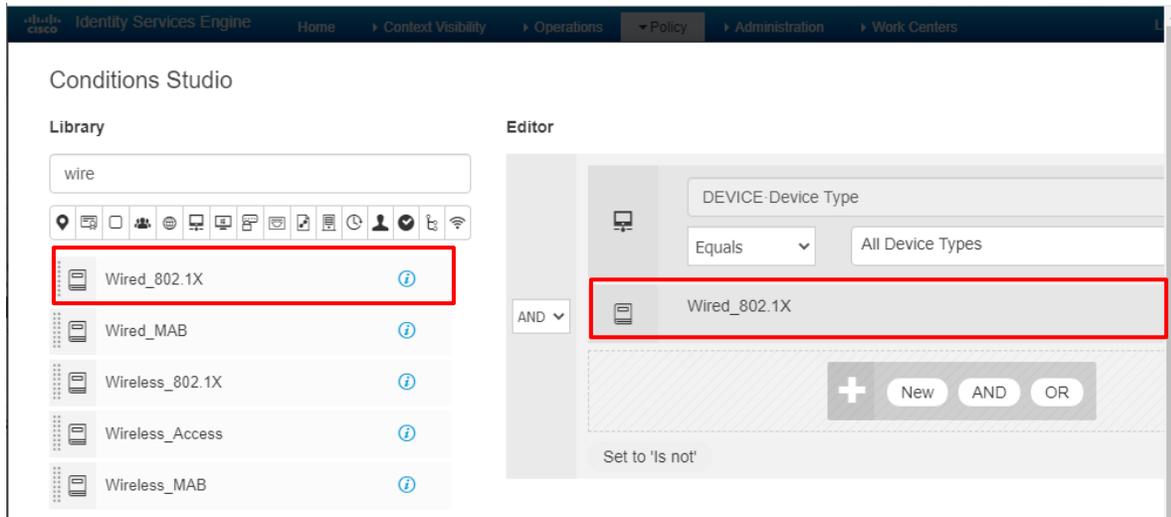
Equals

Set to 'Is not'

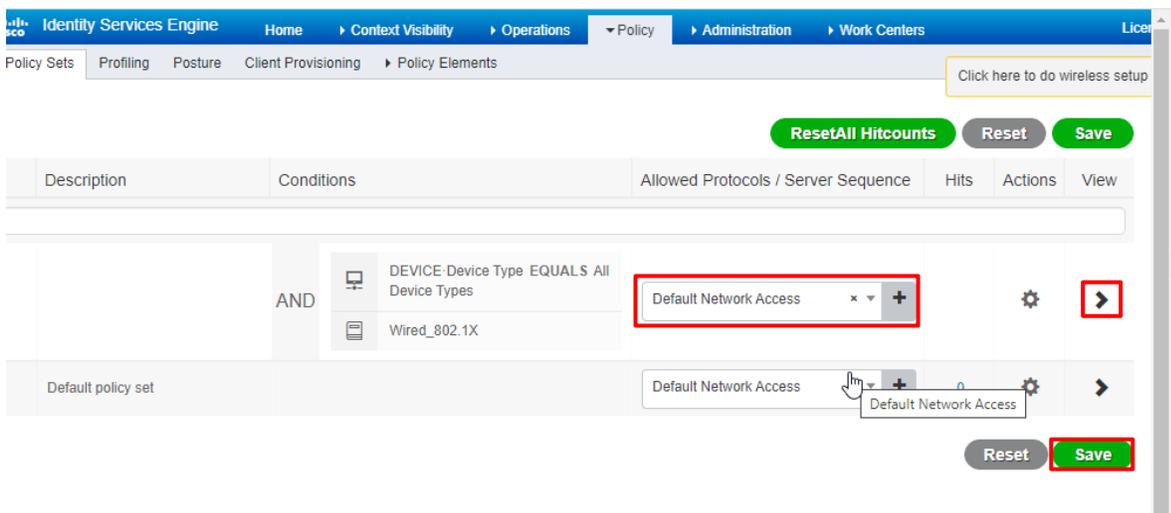
Choose from list or type

All Device Types

+ New AND OR



Sau đó chỉnh sửa Policy vừa tạo



Chỗ Authentication Policy

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. A button labeled "Click here to do wireless setu" is visible. The page title is "Policy Sets → 802.1x". A table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, and Allow. A search bar is present. Below the table, a red box highlights the "Authentication Policy (1)" section. This section contains a table with columns for Status, Rule Name, Conditions, and Use. A red box highlights the first row of this table, which has a status of "On" and a rule name of "Default". Below this table are sections for "Authorization Policy - Local Exceptions" and "Authorization Policy - Global Exceptions".

This screenshot is similar to the one above, showing the same Cisco Identity Services Engine interface. The breadcrumb navigation and main menu are identical. The page title is "Policy Sets → 802.1x". The table listing policy sets is the same. A red box highlights the "Authentication Policy (2)" section. This section contains a table with columns for Status, Rule Name, Conditions, and Use. A red box highlights the first row of this table, which has a status of "On" and a rule name of "802.1x". A red box also highlights the "Conditions" column for this row, which is currently empty. Below this table are sections for "Authorization Policy - Local Exceptions" and "Authorization Policy - Global Exceptions".

The screenshot shows the Identity Services Engine (ISE) interface. The browser address bar displays '172.168.1.100' and the URL path '/admin/#policy/policy_grouping_new'. The navigation menu includes 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main area is titled 'Editor' and contains a policy rule named 'Wired_802.1X' with the condition 'Set to 'Is not''. The rule is highlighted with a red border. To the right of the rule are 'Duplicate' and 'Edit' buttons. Below the rule is a dashed box containing a '+ New AND OR' button. At the bottom right, there are 'Close' and 'Use' buttons, with 'Use' highlighted in green.

Chỗ Authorization Policy

The screenshot shows the 'Policy Sets' section of the Identity Services Engine interface. The navigation menu includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy Elements' sub-menu is active. A table lists policy sets with columns for '+', 'Status', 'Rule Name', and 'Conditions'. A 'Default' policy set is listed with a green checkmark. Below the table are sections for 'Authorization Policy - Local Exceptions' and 'Authorization Policy - Global Exceptions'. A red box highlights the 'Authorization Policy (1)' section. Below this, another table is visible with columns for '+', 'Status', 'Rule Name', 'Conditions', 'Results', 'Profiles', and 'Security Groups'. A red box highlights the '+' icon in the first column of this table. At the bottom, there is a '+ DenyAccess' button and a 'Select from list' button.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' section is active, showing a table of Policy Sets. A red box highlights a plus sign icon in the 'Conditions' column of the '802.1x' row. Below the table, there are sections for 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (2)'. The 'Authorization Policy (2)' section contains a table with columns for 'Status', 'Rule Name', 'Conditions', 'Results', 'Profiles', and 'Security Groups'. A red box highlights a plus sign icon in the 'Conditions' column of the '802.1x' row. To the right of the table, there are 'Select from list' buttons and a 'DenyAccess' button.

The screenshot shows the Cisco Identity Services Engine (ISE) Editor interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' section is active, showing the 'Editor' page. A red box highlights a plus sign icon in the 'Conditions' column of the '802.1x' row. Below the table, there are sections for 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (2)'. The 'Authorization Policy (2)' section contains a table with columns for 'Status', 'Rule Name', 'Conditions', 'Results', 'Profiles', and 'Security Groups'. A red box highlights a plus sign icon in the 'Conditions' column of the '802.1x' row. To the right of the table, there are 'Select from list' buttons and a 'DenyAccess' button.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The 'Policy Elements' page is active, showing a list of conditions. A dropdown menu is open for the 'Wired_802.1X' condition, with 'PermitAccess' selected and highlighted in blue. The 'DenyAccess' option is also visible and circled in red. The 'Save' button at the bottom right is circled in red.

Kiểm tra:

Kiểm tra cấu hình 802.1x trên switch:

```
SW1#show dot1x all

Sysauthcontrol          Enabled
Dot1x Protocol Version      3

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

```
Dot1x Info for Ethernet0/3
-----
```

```
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

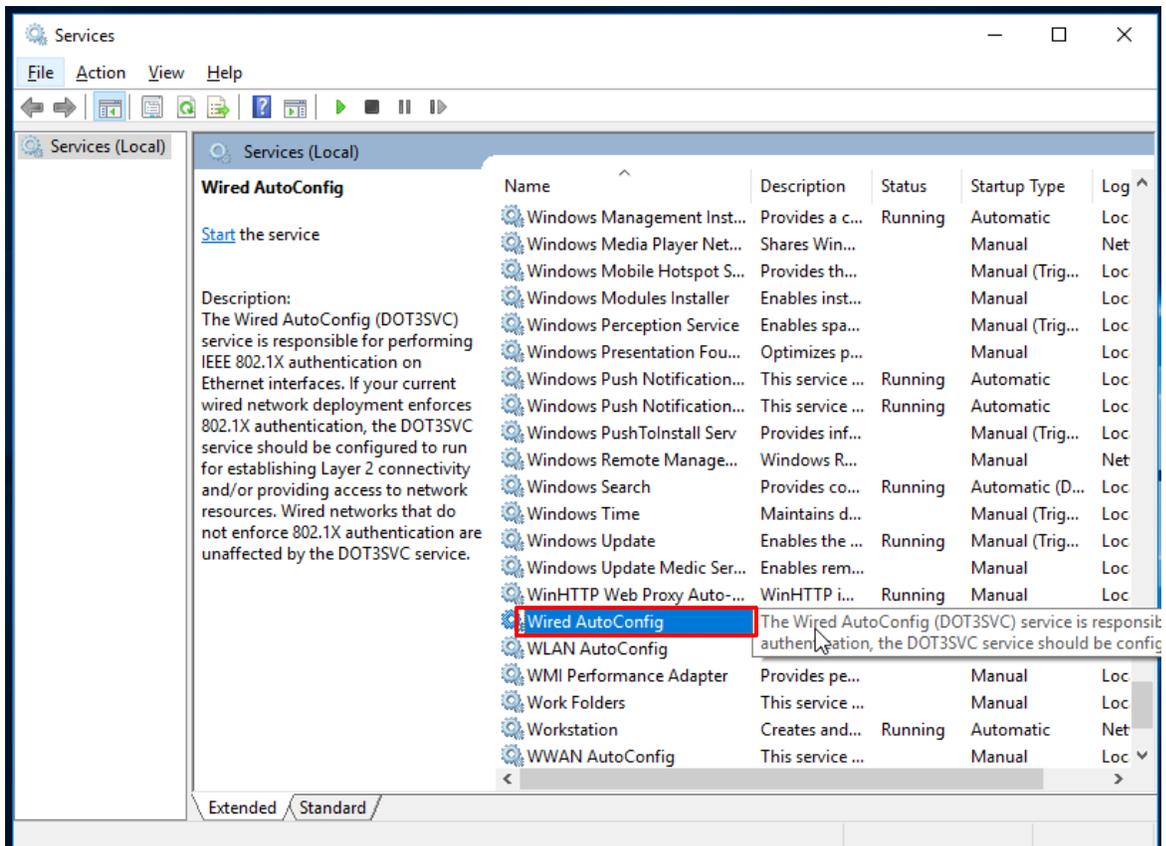
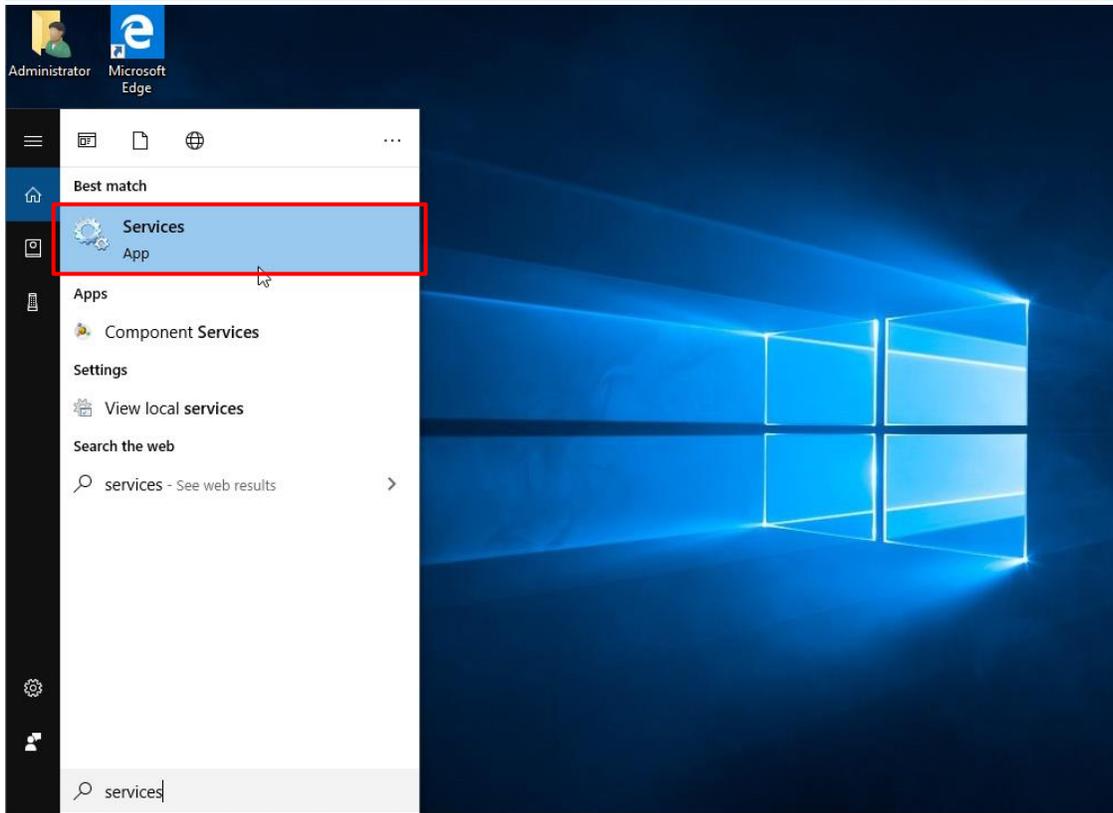
Dot1x Info for Ethernet1/0

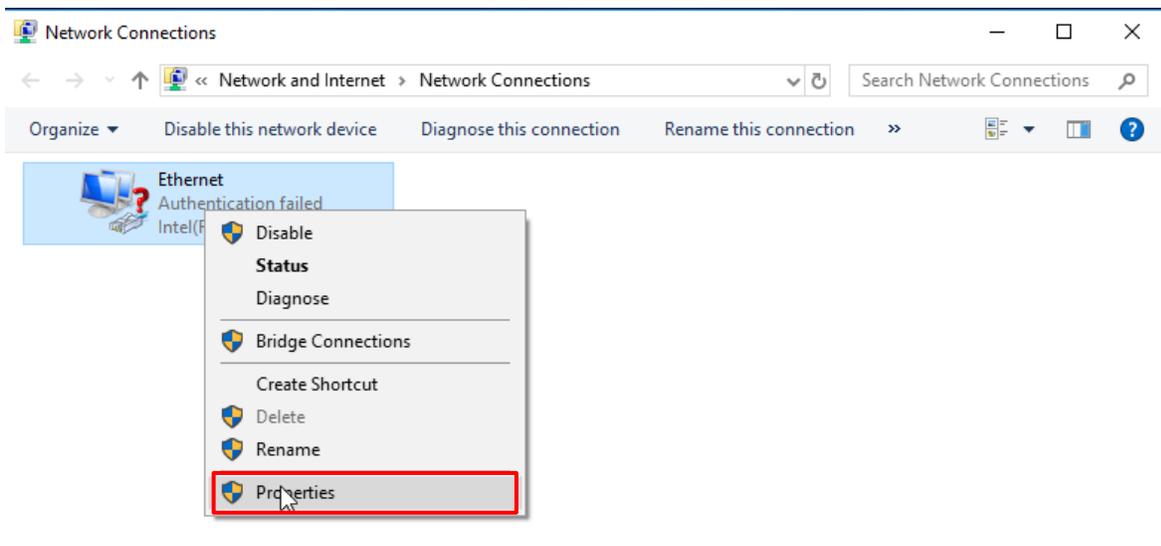
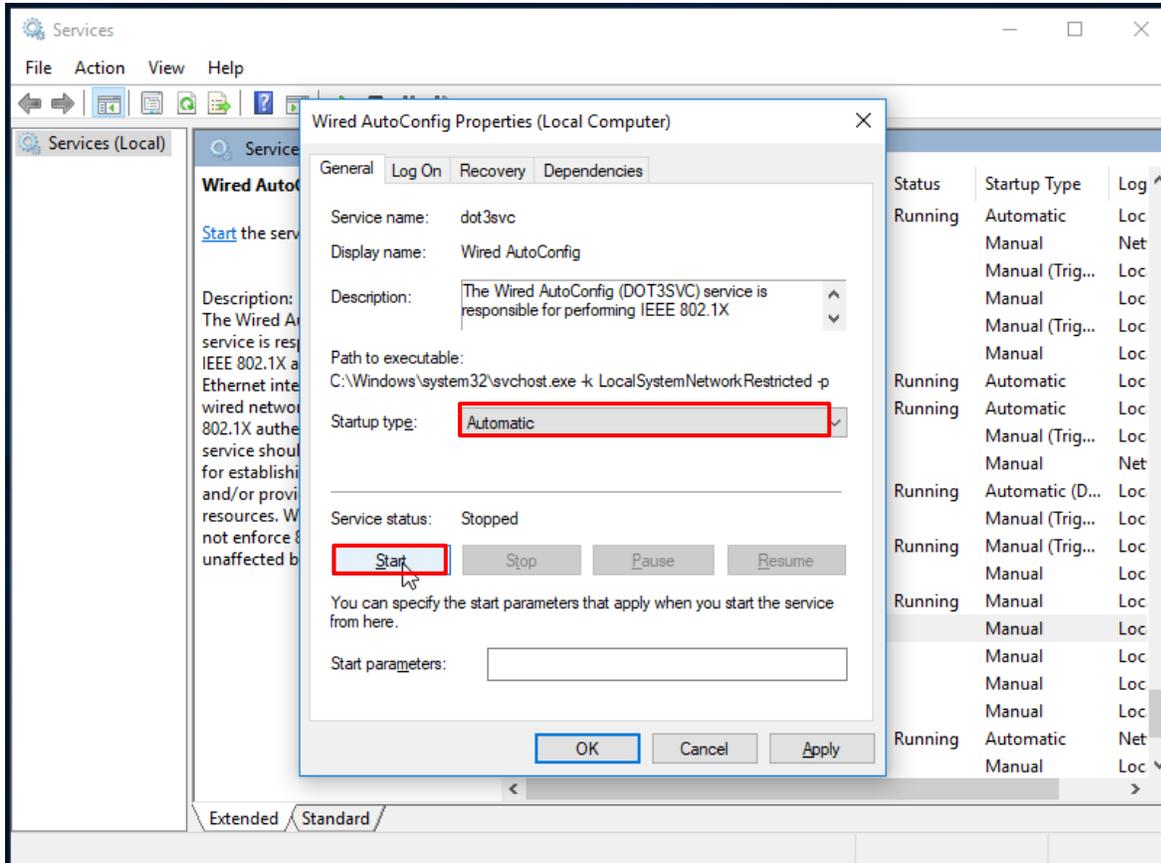
```
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

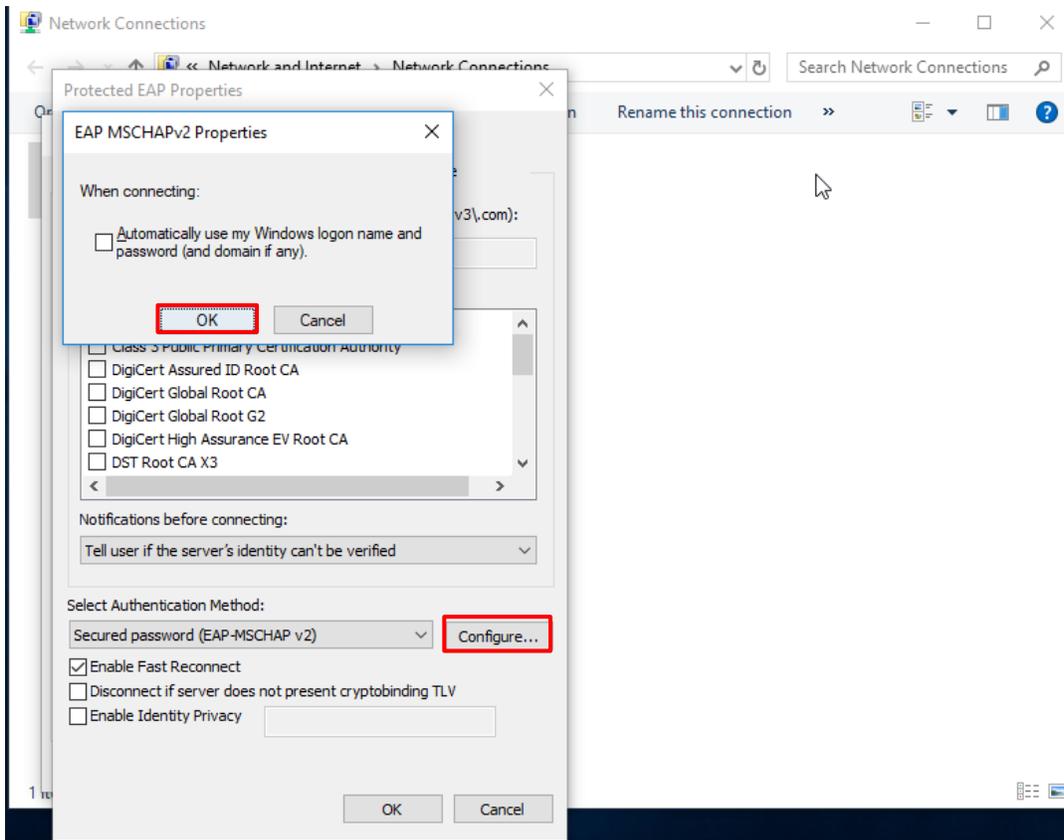
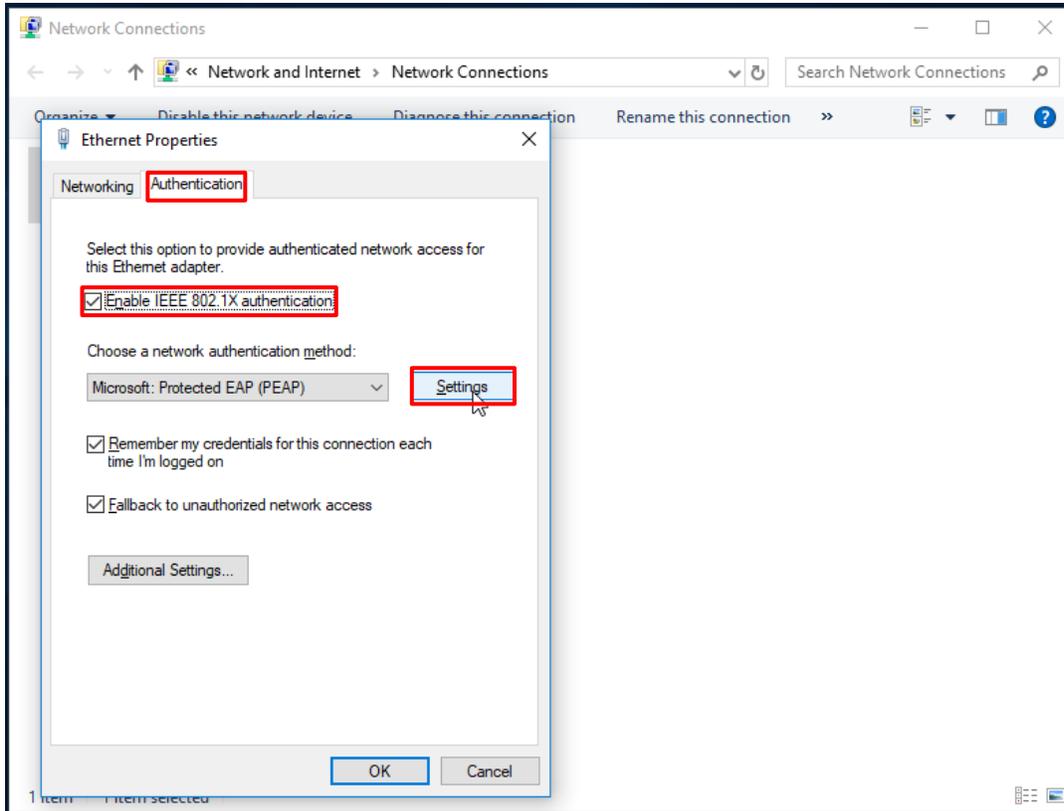
Kiểm tra server radius đã cấu hình trên switch:

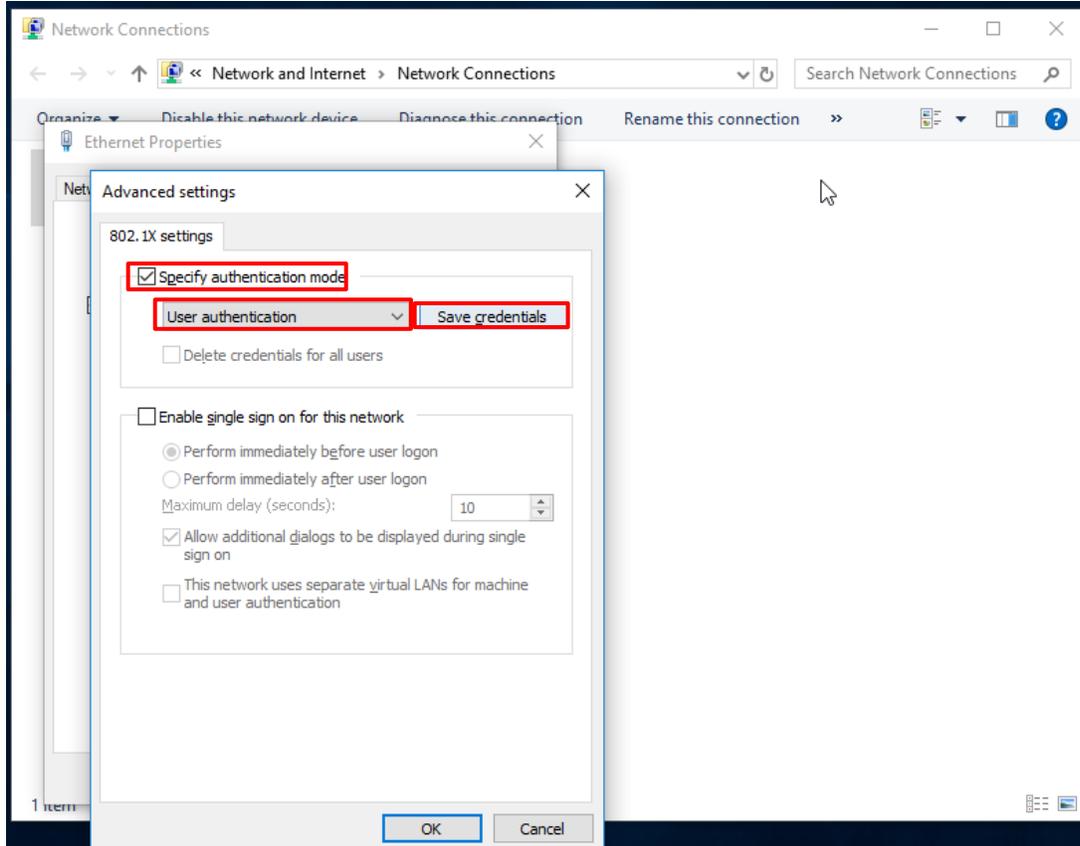
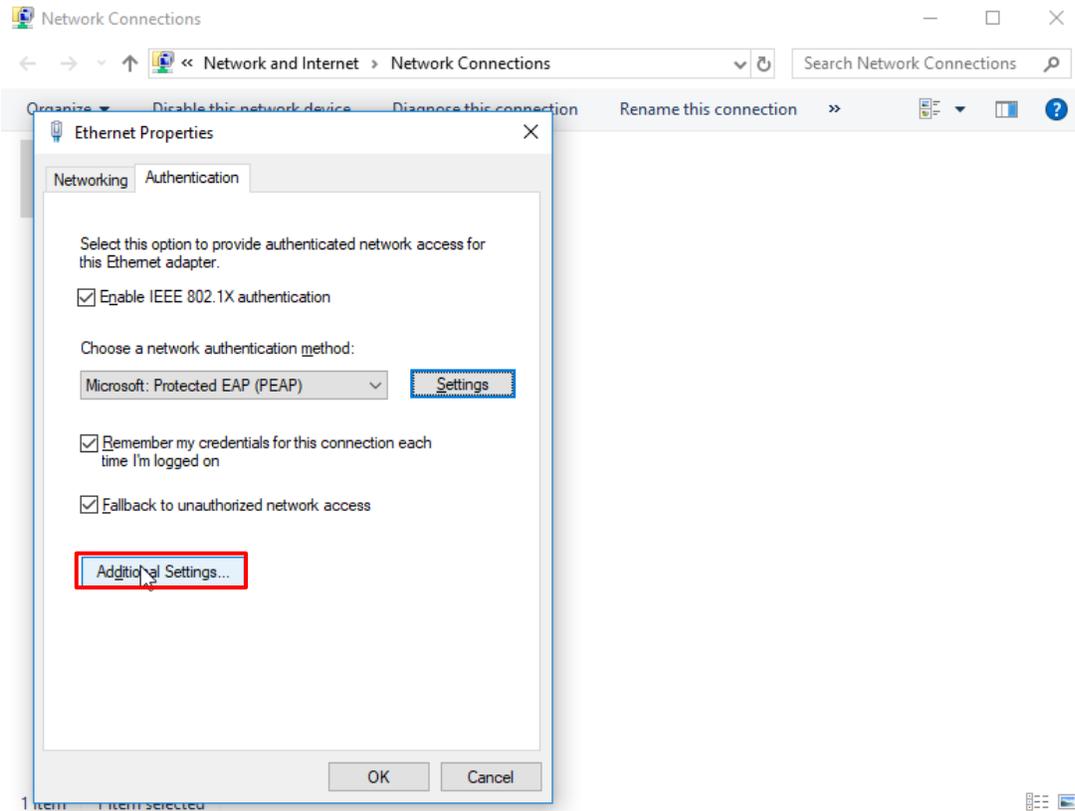
```
SW1#show radius server-group all
Server group radius
  Sharecount = 1  sg_unconfigured = FALSE
  Type = standard  Memlocks = 1
  Server(172.168.1.100:1645,1646) Transactions:
  Authen: 16  Author: 0      Acct: 0
  Server_auto_test_enabled: FALSE
  Keywrap enabled: FALSE
```

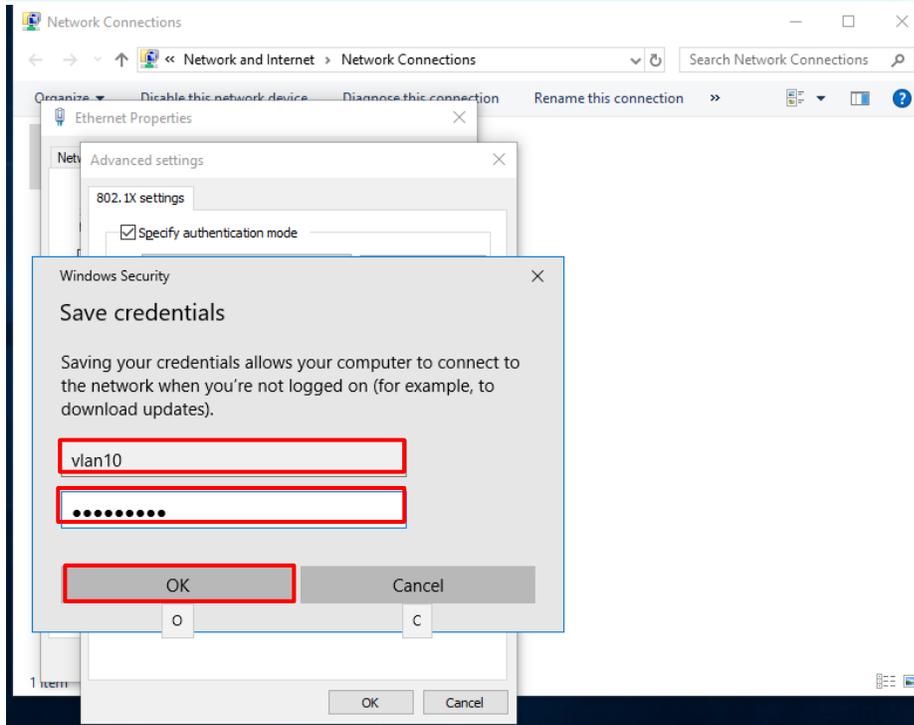
Kiểm tra cấu xác thực trên PC win1:











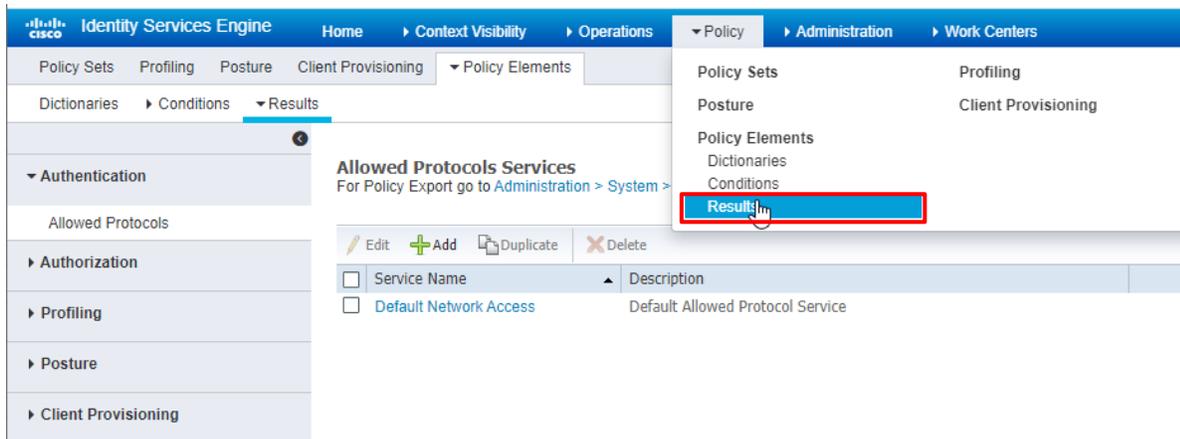
Bước 5: Cấu hình dynamic assign vlan: Cấu hình:

- 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:



Standard Authorization Profiles
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to bla
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Ci
<input type="checkbox"/> Cisco_Temporal_Onboard	Cisco	Onboard the device with i
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to re
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with I
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for N
<input type="checkbox"/> vlan10	Cisco	
<input type="checkbox"/> vlan20	Cisco	

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

Authorization Profile

* Name:
Description:
* Access Type:
Network Device Profile:
Service Template:
Track Movement:
Passive Identity Tracking:

Common Tasks

Security Group
 VLAN Tag ID: ID/Name:

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

Tạo profile tương tự cho vlan 20 và 30.

- **Chỉnh lại policy:**

The screenshot shows the Cisco ISE Policy Sets configuration page. The 'Policy Sets' menu item is highlighted in red. The configuration shows 'VLAN' checked under 'Common Tasks' with 'Tag ID' set to 10 and 'ID/Name' set to 'IT'. Below, 'Advanced Attributes Settings' and 'Attributes Details' are visible.

The screenshot shows the Cisco ISE Policy Elements configuration page. The 'Policy Elements' menu item is highlighted. A table shows policy elements with conditions and actions. A red box highlights the 'View' icon for the first policy element.

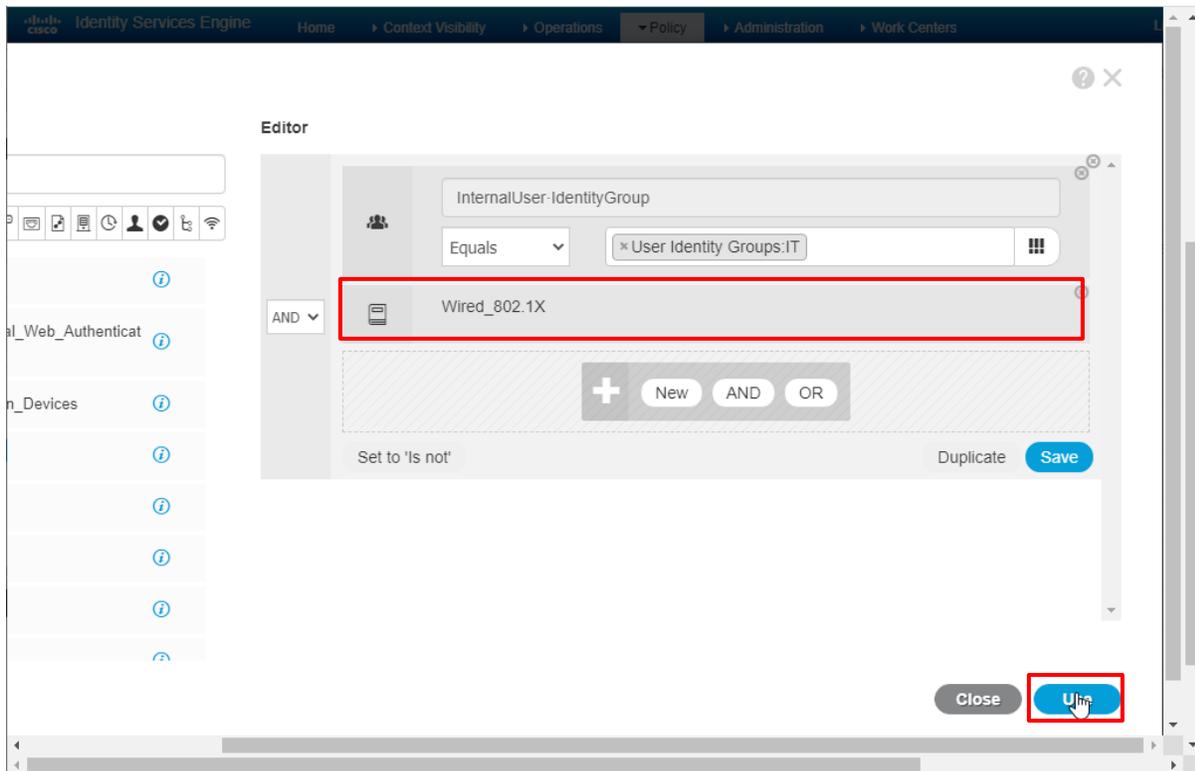
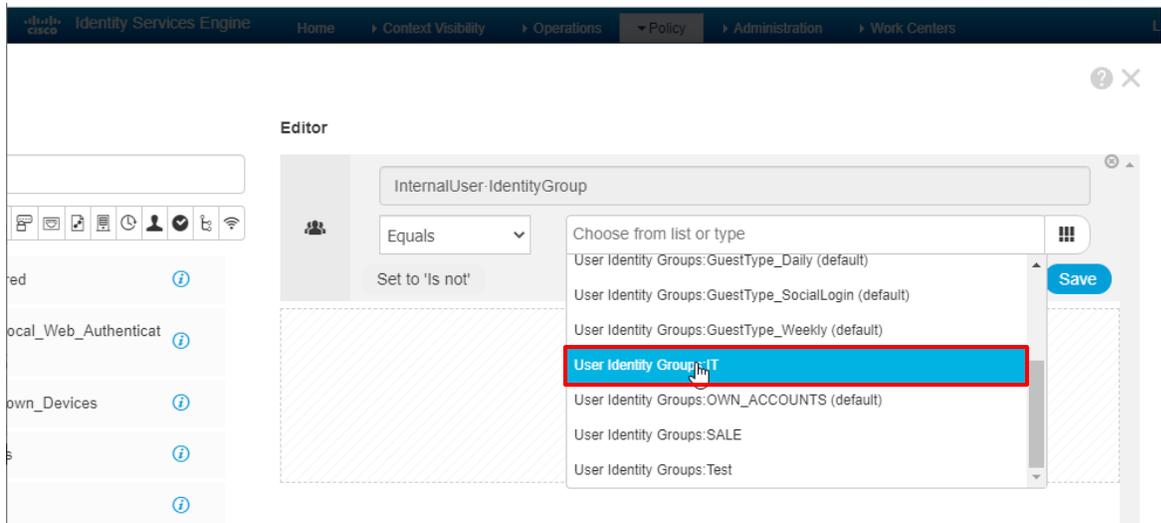
Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	AND DEVICE-Device Type EQUALS All Device Types Wired_802.1X	Default Network Access	1	⚙️	
Default policy set		Default Network Access	0	⚙️	➔

The screenshot shows the Cisco Identity Services Engine (ISE) Policy configuration page. The navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area is titled "Authorization Policy - Global Exceptions" and shows a list of four policies. The third policy, "802.1x-vlan10", is highlighted with a red box. The table below shows the details of these policies.

Status	Rule Name	Conditions	Results
✔	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

The screenshot shows the Cisco Identity Services Engine (ISE) Editor interface. A dialog box titled "Select attribute for condition" is open, displaying a list of attributes. The "InternalUser" attribute is highlighted with a red box. The dialog box includes a search bar and a list of attributes with their respective dictionaries and IDs.

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
CWA	CWA_ExternalGroups		?
IdentityGroup	Description		?
IdentityGroup	Name		?
InternalUser	IdentityGroup		?
PassiveID	PassiveID_Groups		?



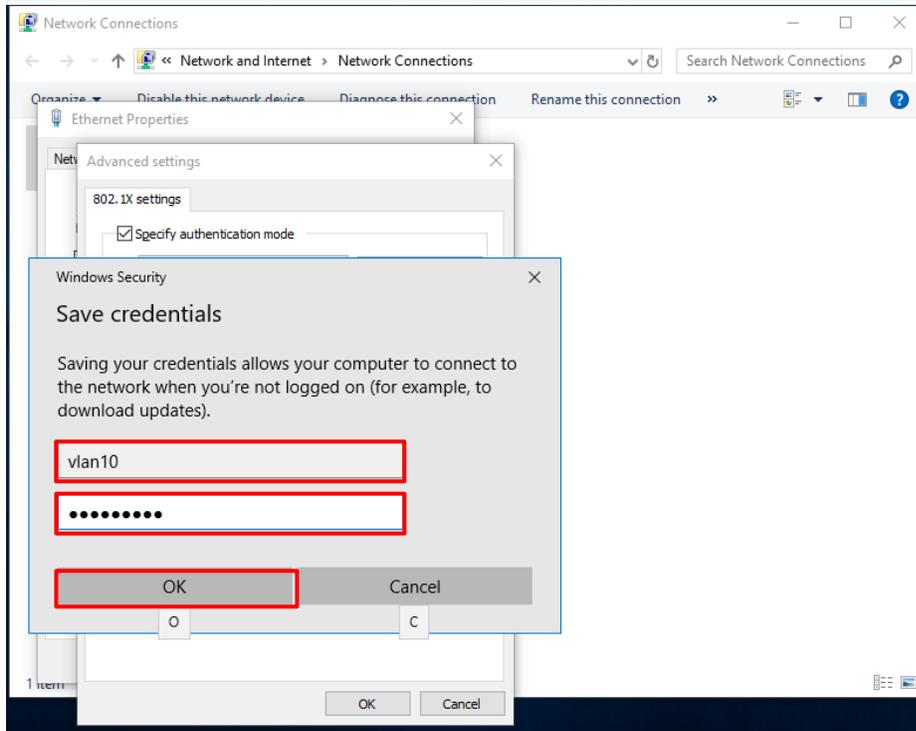
Conditions	Profiles	Security Groups	Hits	Actions
AND InternalUser-IdentityGroup EQUALS User Identity Groups:ACCOUNTING Wired_802.1X	vian30 DenyAccess NSP_Onboard Non_Cisco_IP_Phones PermitAccess vian10 vian20 vian30	Select from list	0	⚙️
AND InternalUser-IdentityGroup EQUALS User Identity Groups:SALE Wired_802.1X	vian10	Select from list	0	⚙️
AND InternalUser-IdentityGroup EQUALS User Identity Groups:IT Wired_802.1X	vian10	Select from list	1	⚙️
	DenyAccess	Select from list	0	⚙️

Reset Save

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	Et0/0, Et0/3, Et1/0, Et1/1 Et1/2, Et1/3
10	IT	active	Et0/2
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	



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
