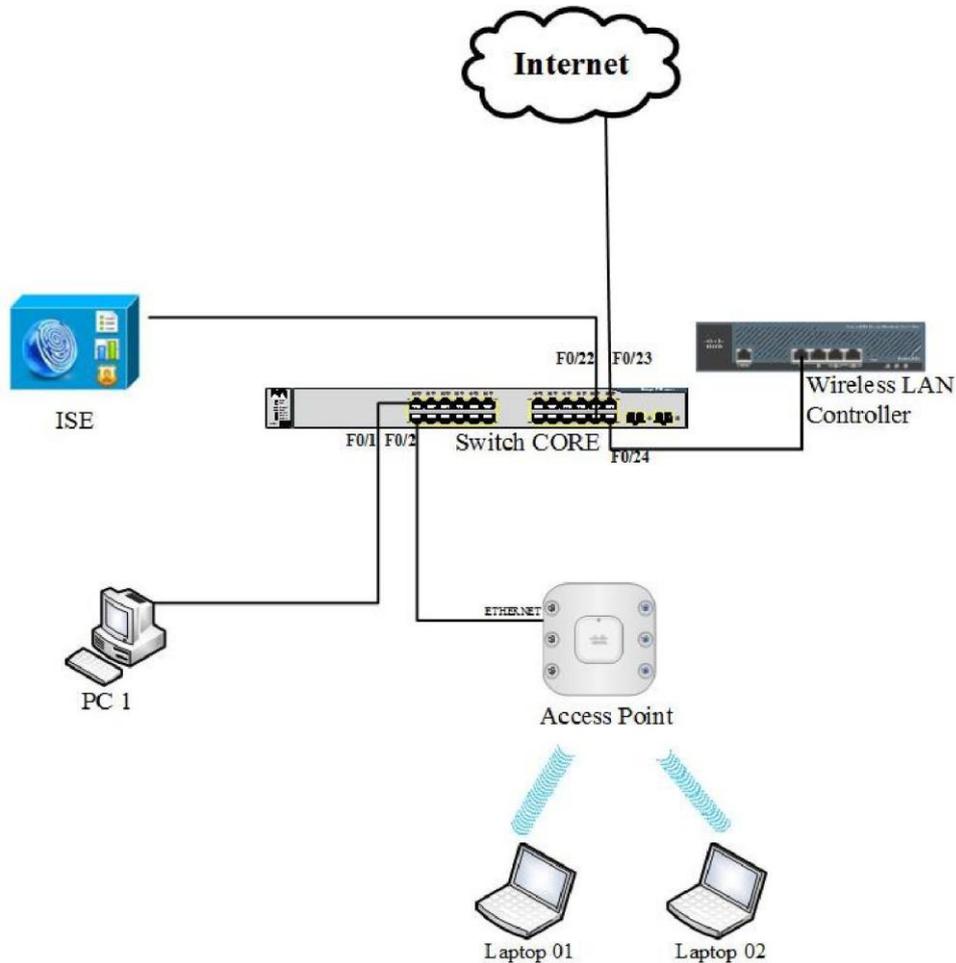


LAB : XÁC THỰC RADIUS 802.1x VỚI CISCO ISE

I. Sơ đồ



II. Mô tả

Bài lab gồm một PC, một Access Point, một Switch, một WLC và một Server Cisco ISE

Đặt IP theo sơ đồ sau:

Tên thiết bị	Địa chỉ IP
ISE	192.168.1.253/24
WLC	192.168.1.100/24
AP	192.168.1.1/24
PC	192.168.1.2/24
F0/23	DHCP
Interface VLAN 1	192.168.1.10/24

Interface kết nối với Internet là interface layer 3, Interface kết nối với WLC và Access Point là trunk

III. Yêu cầu

1. Cấu hình trên switch core

- Tạo các VLAN sau trên Switch Core:

+ VLAN 1: VLAN quản lý, IP 192.168.1.0/24

+ VLAN 10: VLAN cho user thuộc nhóm Staff trong SSID Staff, IP 10.0.10.0/24

+ VLAN 30: VLAN cho user thuộc nhóm VIP trong SSID Staff, IP 10.0.30.0/24

- Đặt IP cho các interface VLAN để Switch core làm default gateway cho tất cả VLAN, cấu hình để Switch core làm DHCP Server cấp IP cho tất cả VLAN, cấu hình định tuyến để tất cả VLAN đều có thể truy cập Internet

2. Cấu hình các tham số cơ bản cho WLC và cấu hình để Access Point nhận IP quản lý thuộc VLAN 1, và có thể được quản lý tập trung trên WLC

3. Cấu SSID Staff xác thực kiểu 802.1x, database lấy từ Cisco ISE

4. Cấu hình Cisco ISE:

- Tạo hai user group: staff và VIP

- Nếu user xác thực bằng tài khoản trong group Staff → cấp IP thuộc VLAN 10

- Nếu user xác thực bằng tài khoản trong group VIP → cấp IP thuộc VLAN 30

IV. Cấu hình

Yêu cầu 1, 2: Cấu hình trên switch core, WLC và AP:

Tham khảo bài Lab 3: Cấu hình Cisco WLC 2504

Lưu ý: Tạo đủ 3 Interface cho 3 VLAN 1, 10 và 30

Yêu cầu 3: Cấu hình SSID Staff xác thực kiểu 802.1x

3.1. Kết nối WLC với Radius

Vào menu SECURITY → AAA → RADIUS → Authentication

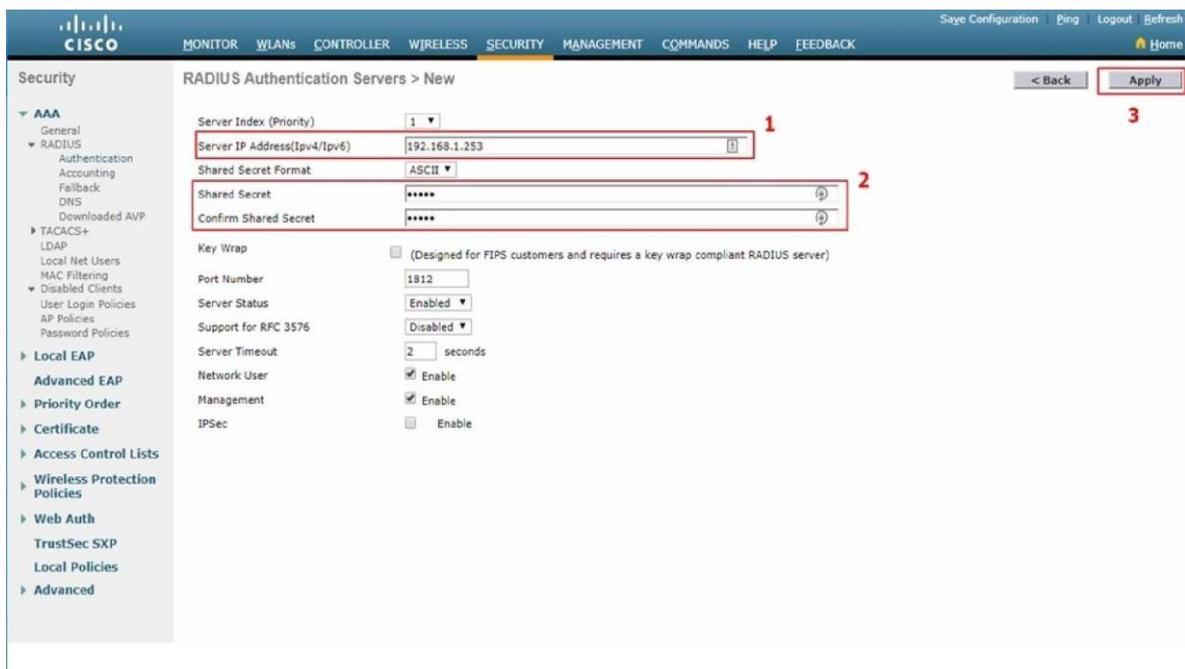
Click New để thêm RADIUS Authentication Server (trong bài lab này, RADIUS Authentication Server chính là Cisco ISE).



Nhập địa chỉ IP của Cisco ISE (192.168.1.253)

Đặt và confirm shared secret. Secret này phải giống nhau trên Cisco WLC và Cisco ISE (bài lab này chọn secret là vnpro)

Click Apply



3.2. Tạo SSID xác thực bằng 802.1x

Truy cập vào WLC

Vào menu WLANs → Chọn Create New. Click Go



Đặt Profile name và SSID:

Profile Name: ssid_staff

SSID: SSID_Staff

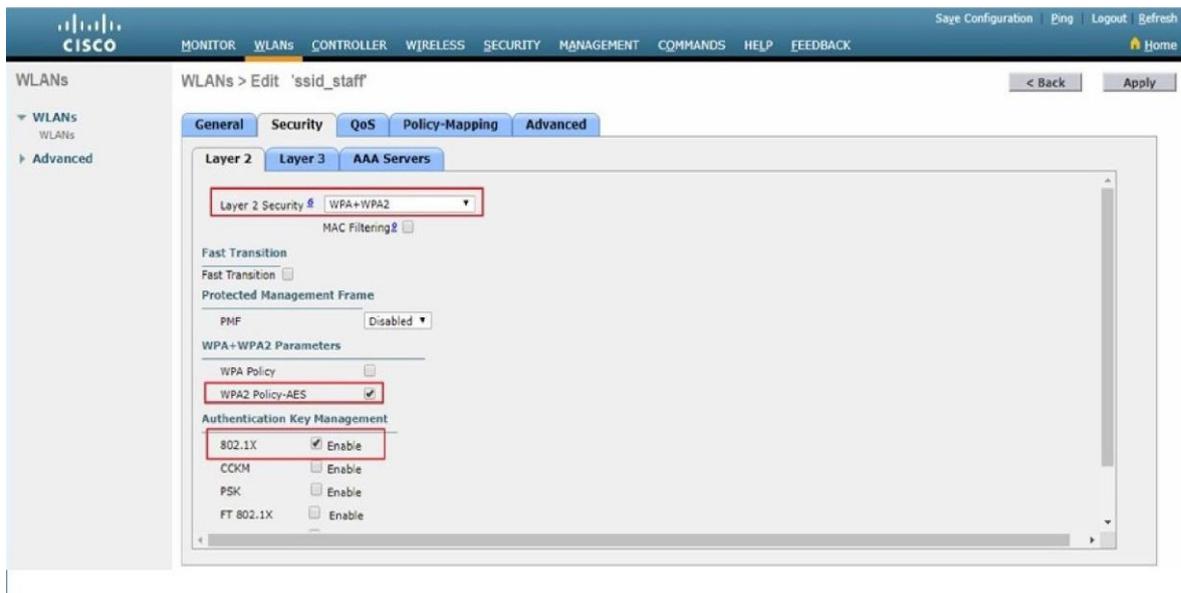
Click Apply



Trong tab General:

Tick chọn Status: Enabled

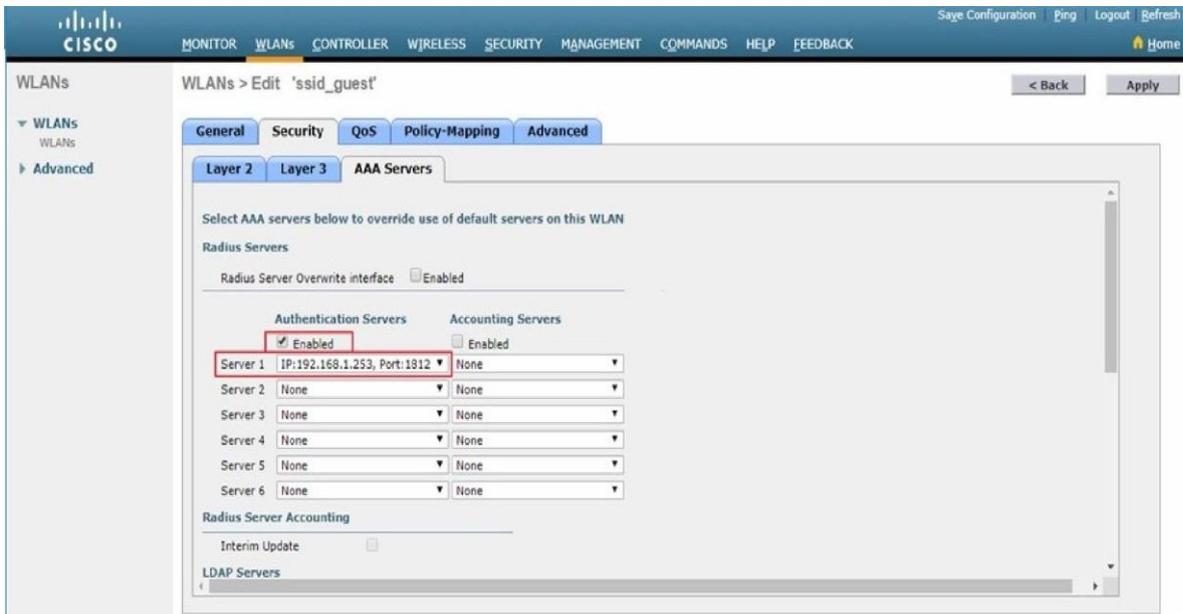
Interface/Interface Group (G): management



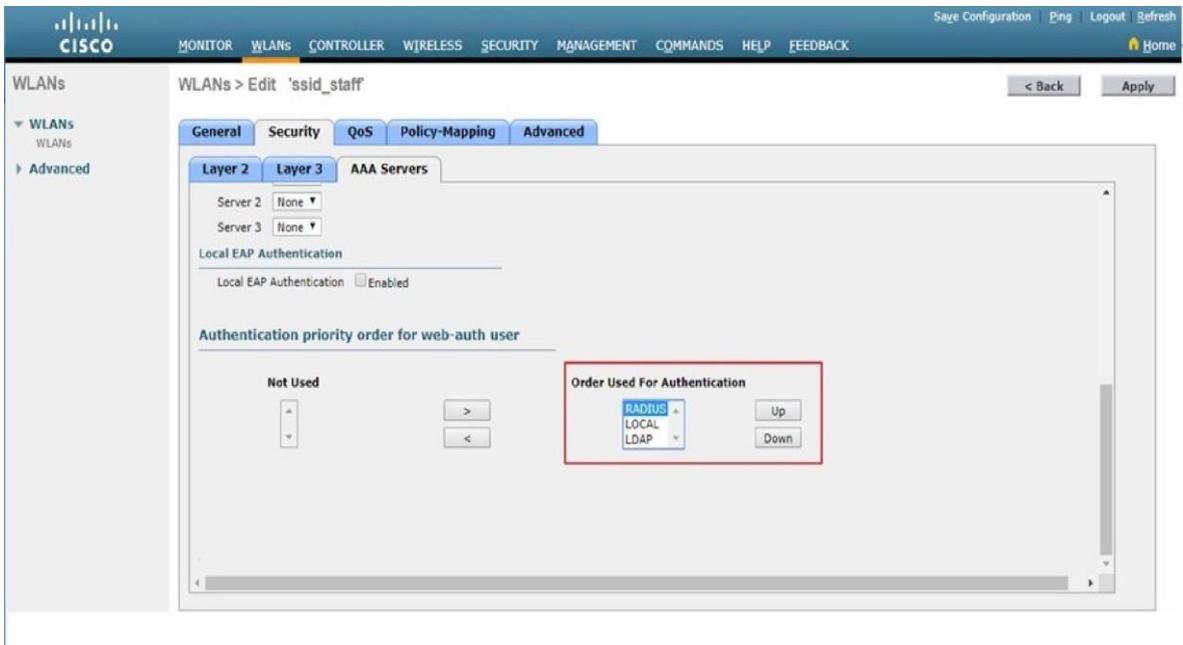
Trong tab Security → AAA Servers:

Tick chọn Enabled ở mục Authentication Servers

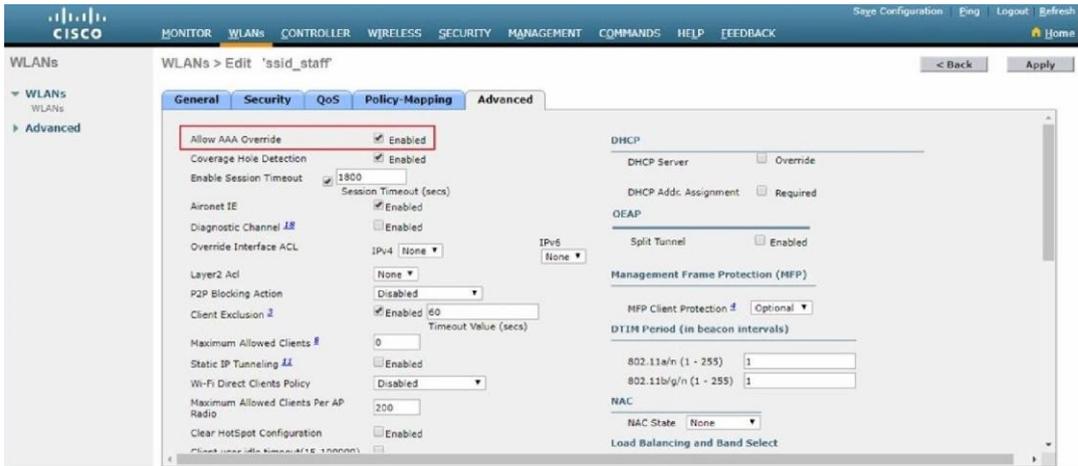
Chọn Server 1 là server mà chúng ta vừa thêm ở bước 2



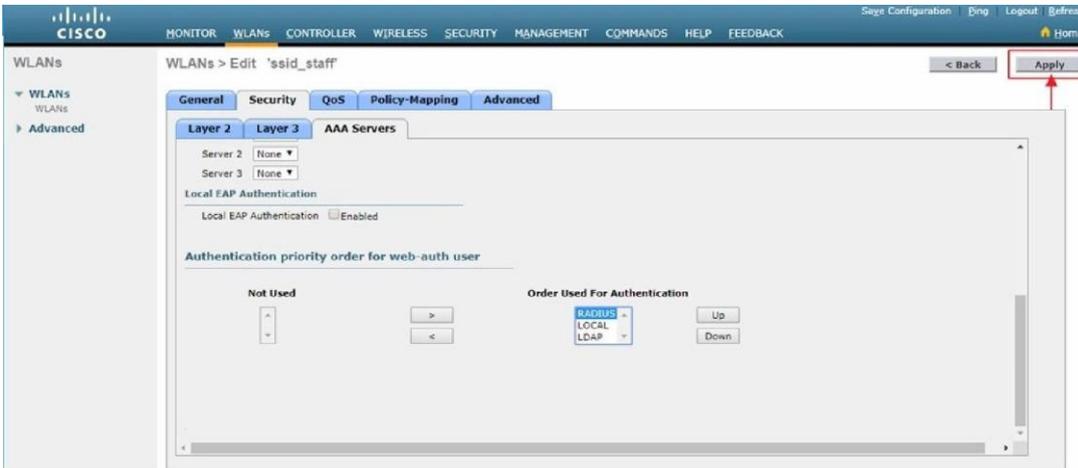
Kéo xuống, trong phần Order Used for Authentication, click chọn RADIUS và click UP để phương thức xác thực RADIUS nằm đầu tiên



Vào tab Advanced, tích chọn Allow AAA Override



Click Apply

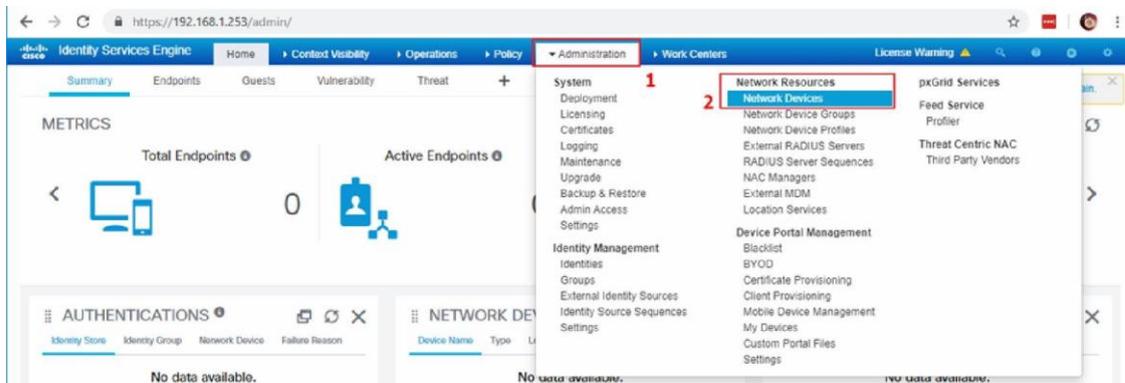


Yêu cầu 4: Cấu hình Cisco ISE

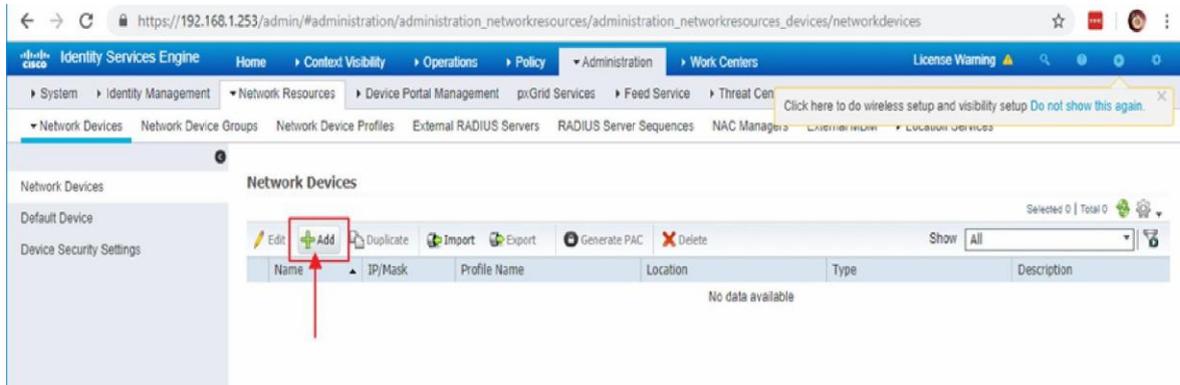
4.1. Thêm WLC vào Cisco ISE

Truy cập vào Cisco ISE

Vào menu Administration → Network Resources → Network Devices

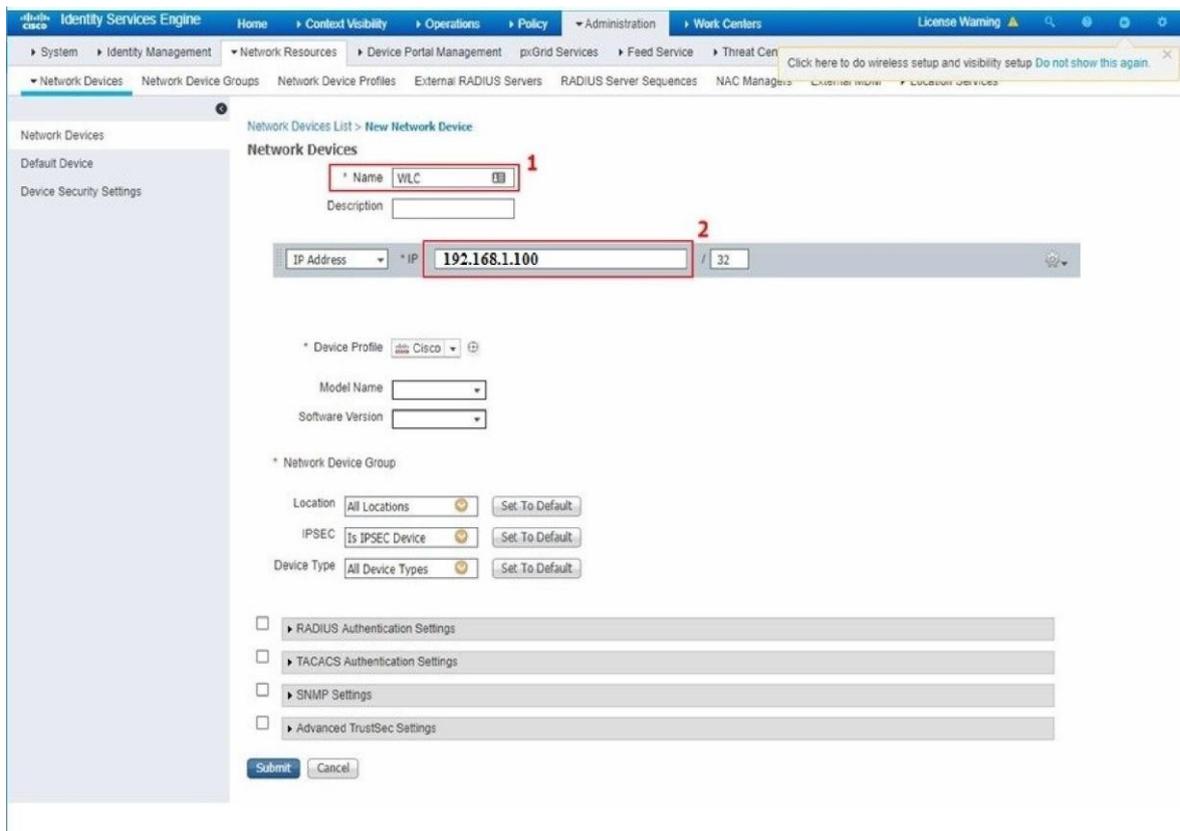


Click Add



Đặt tên cho thiết bị (có thể đặt tùy ý)

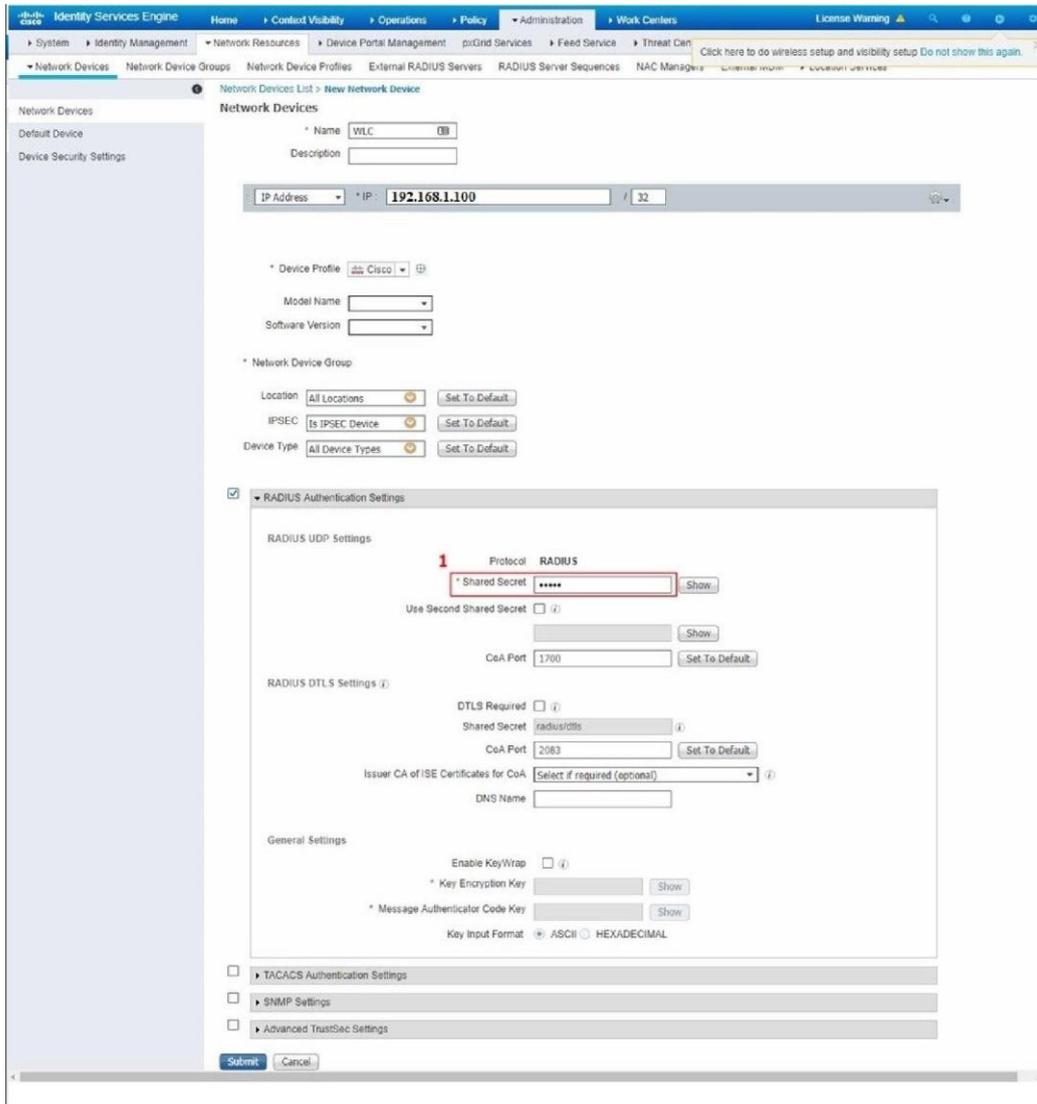
Nhập IP thiết bị



Tích chọn vào mục RADIUS

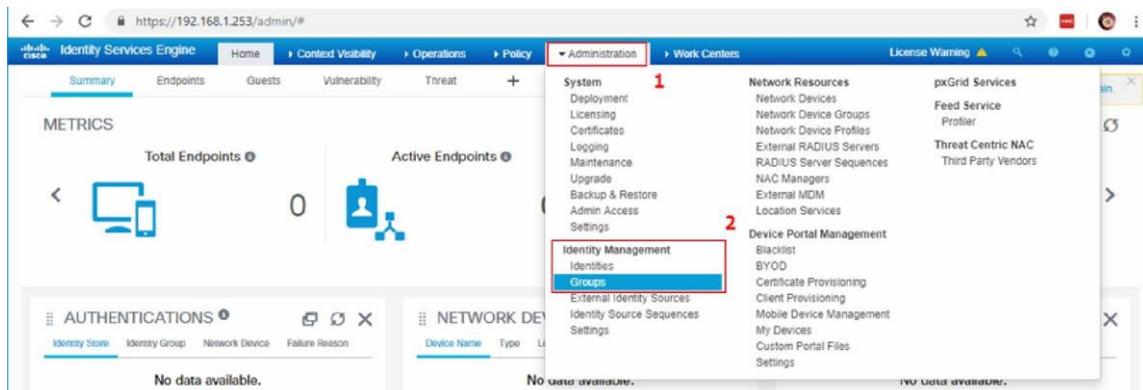
Nhập shared secret (giống với shared secret đã đặt ở bước 2, bài lab này chọn shared secret là vnpro)

Sau đó click Submit

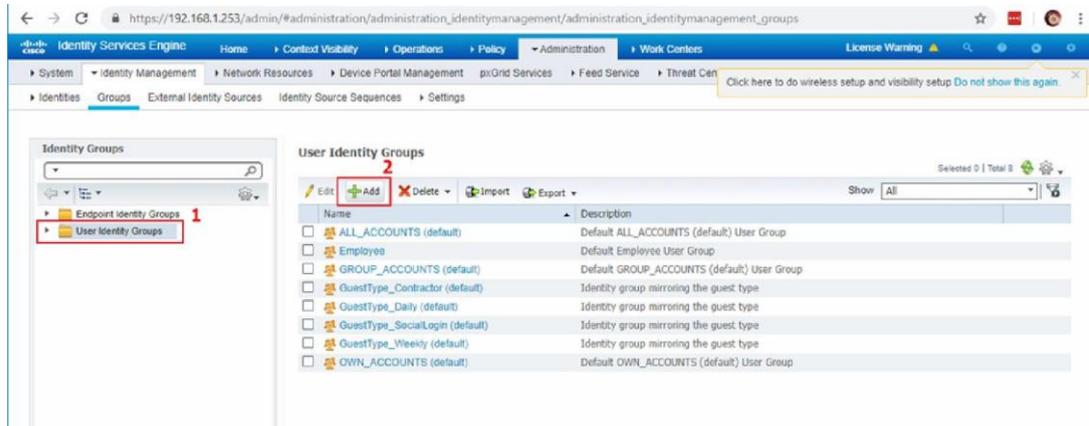


4.2. Tạo group

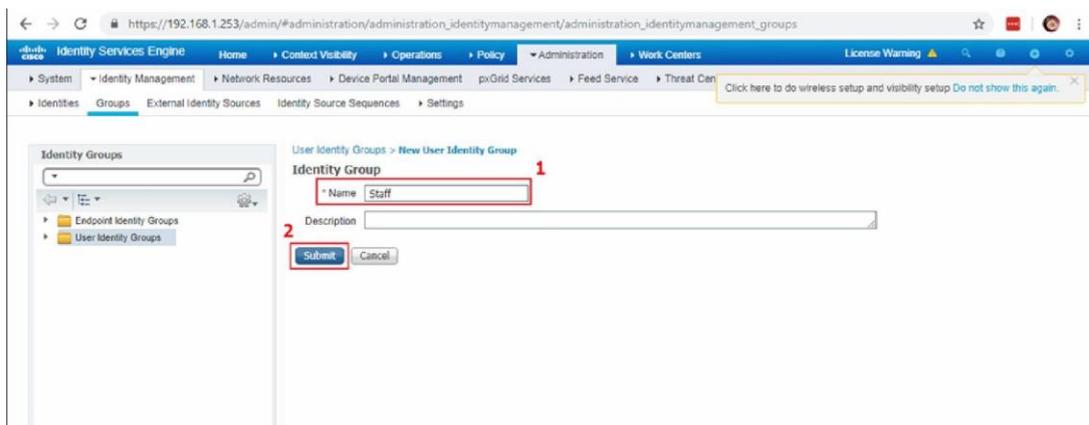
Vào menu Administration → Identity Management → Groups



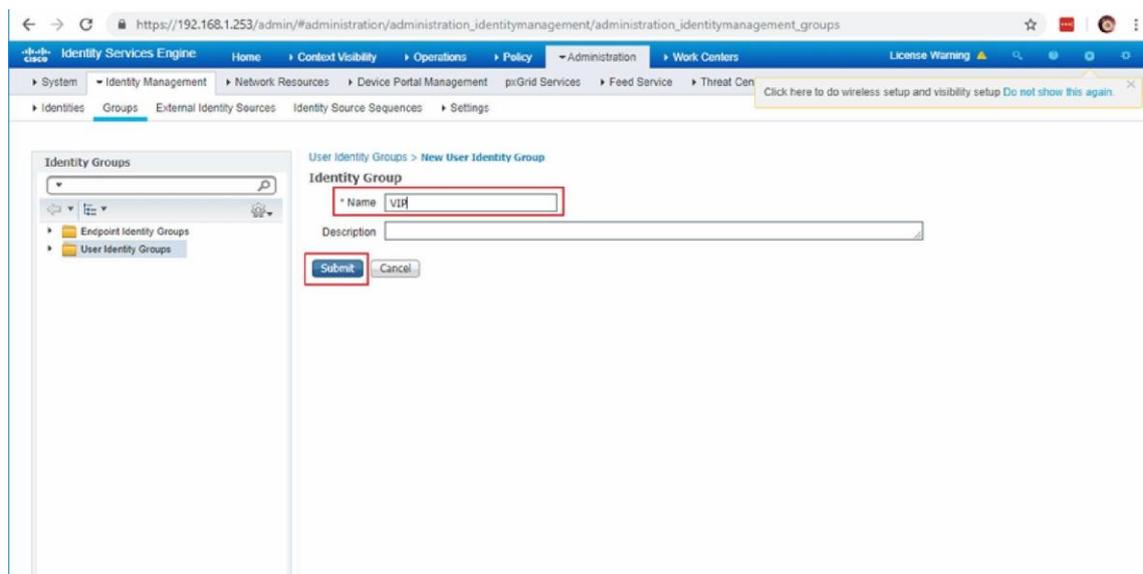
Click vào mục User Identity Group, sau đó click Add



Đặt tên group là Staff và click Submit

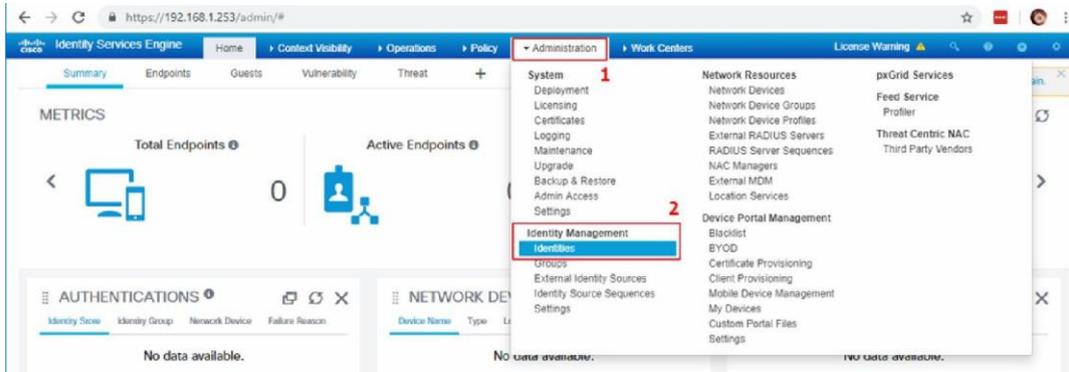


Thực hiện tương tự cho group VIP

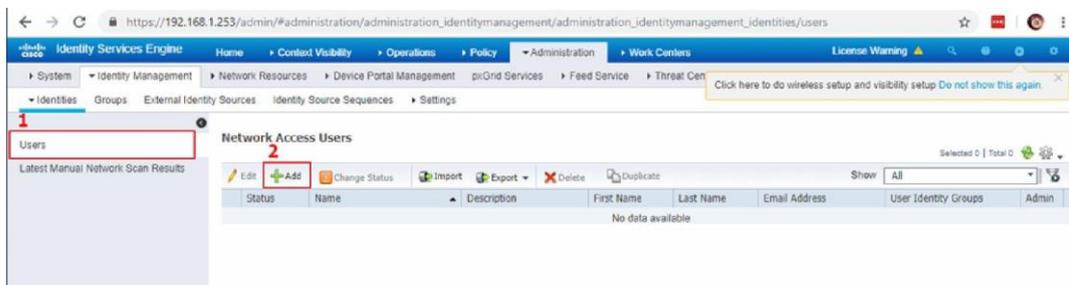


4.3. Tạo user

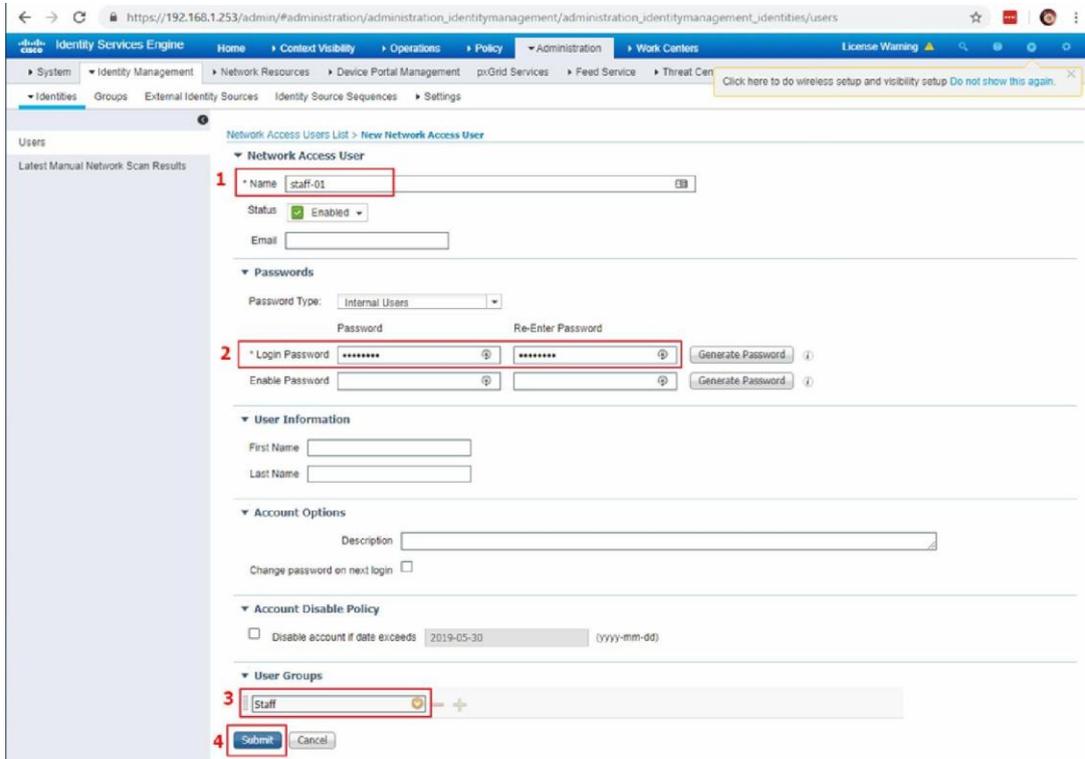
Vào menu Administration → Identity Management → Identities



Click chọn Users, sau đó click Add



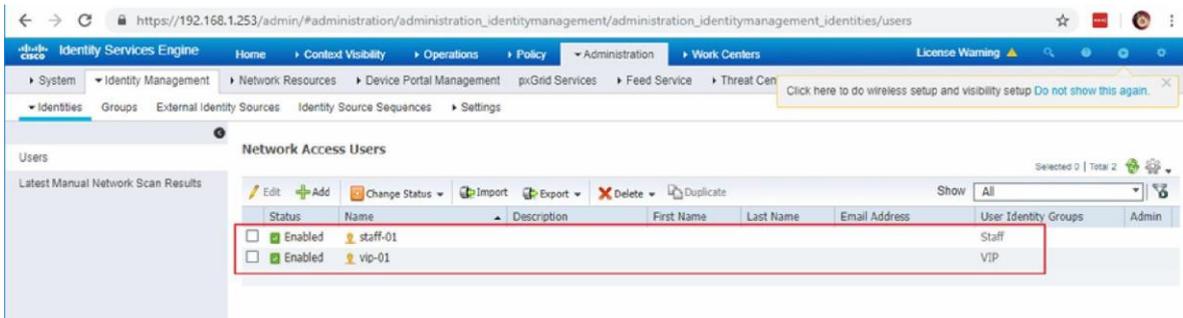
Nhập: Username, Password và confirm password, chọn User Groups, click Submit



Tạo 2 user:

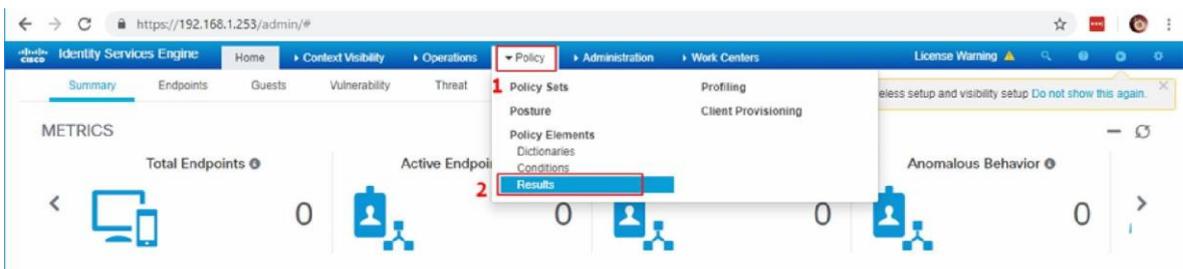
User staff-01, password Qwe@#123, thuộc nhóm Staff

User vip-01, password Vnpro@149, thuộc nhóm VIP

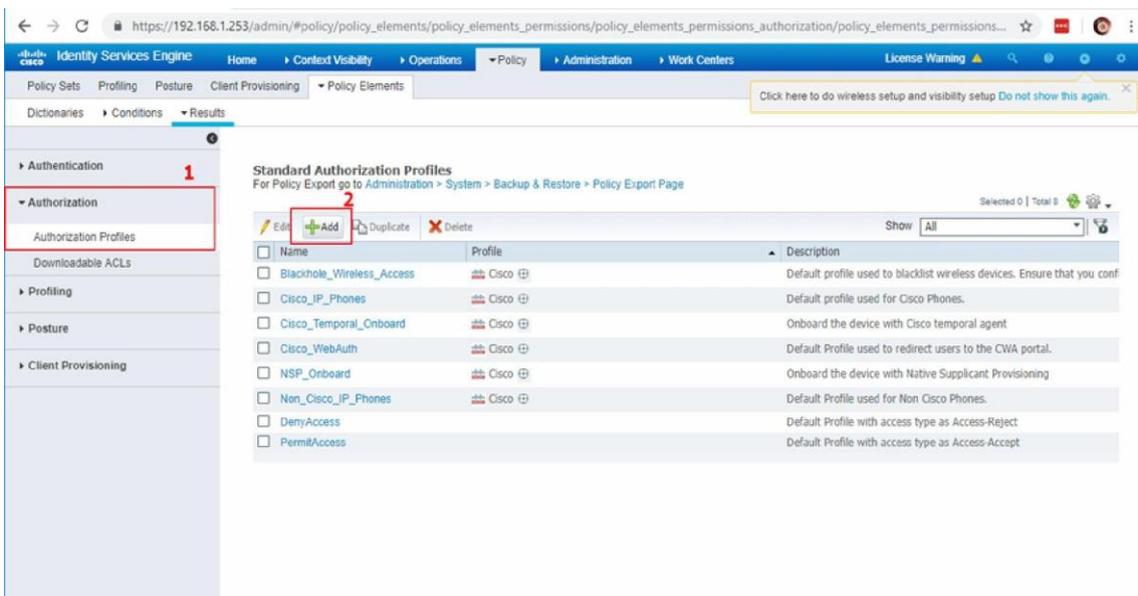


4.4. Tạo Result

Vào menu Policy > Results



Vào mục Authorization → Authorization Profiles. Click Add



Đặt tên cho Profile: Assign_VLAN_10

Trong phần Common Tasks, tích chọn VLAN và đặt ID là 10

Sau đó click Submit

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

Policy Sets Profiling Posture Client Provisioning Policy Elements

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

ACL (Filter-ID)

Security Group

VLAN Tag ID 1

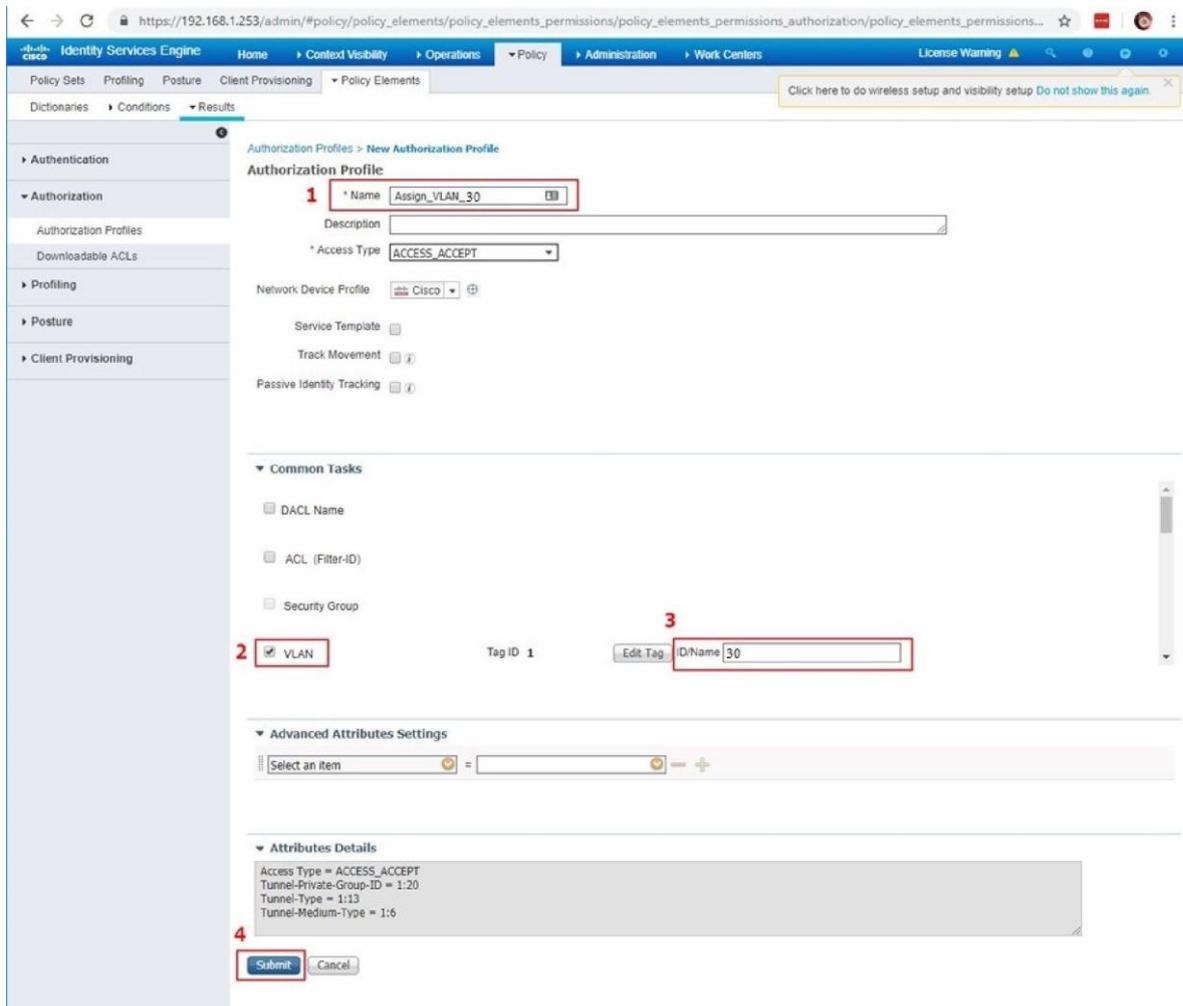
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:10
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:5

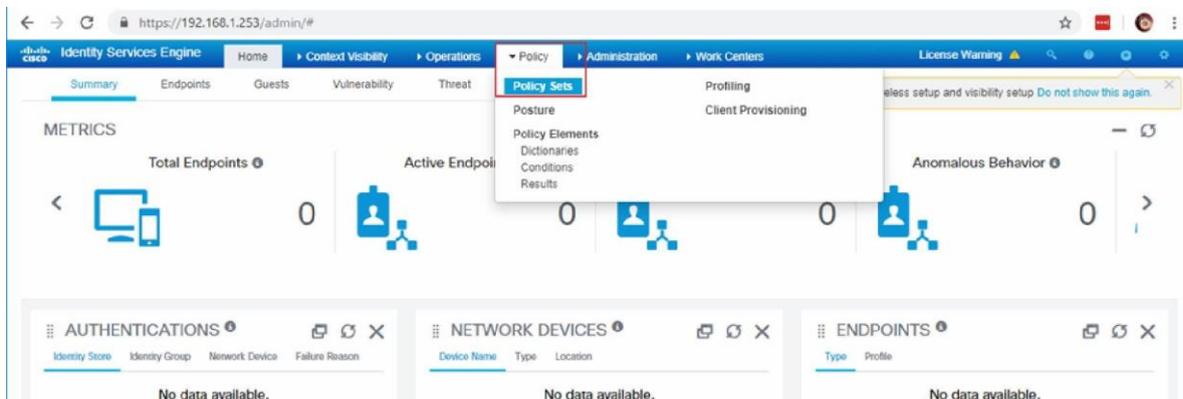
Thực hiện tương tự để tạo profile Assign_VLAN_30



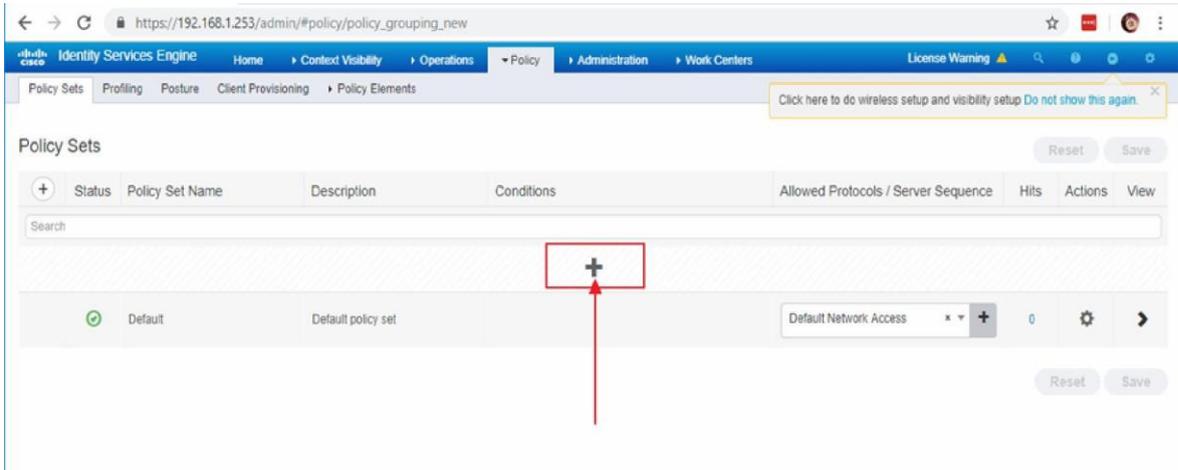
4.5. Cấu hình Policy

Tạo Policy

Vào menu Policy → Policy Set

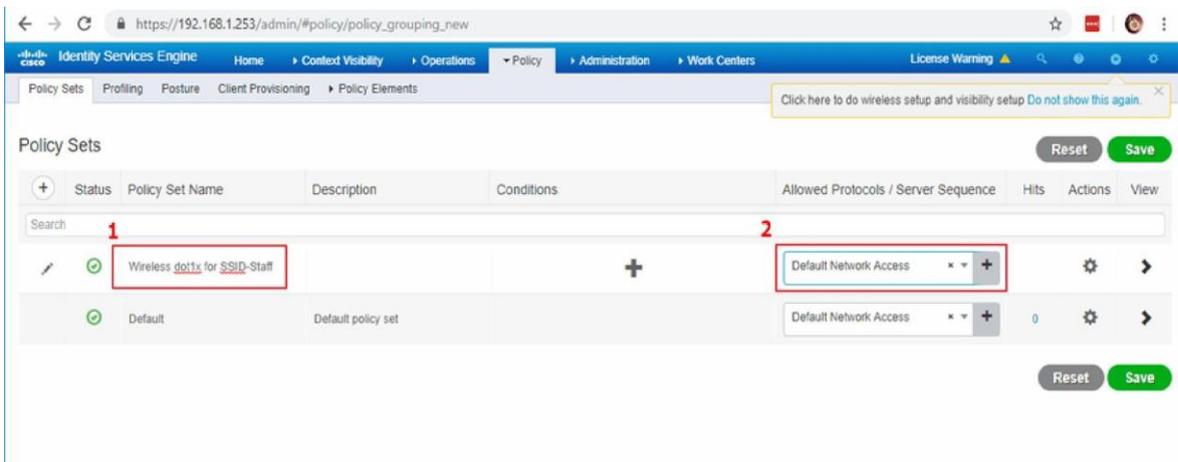


Click Add (icon +)

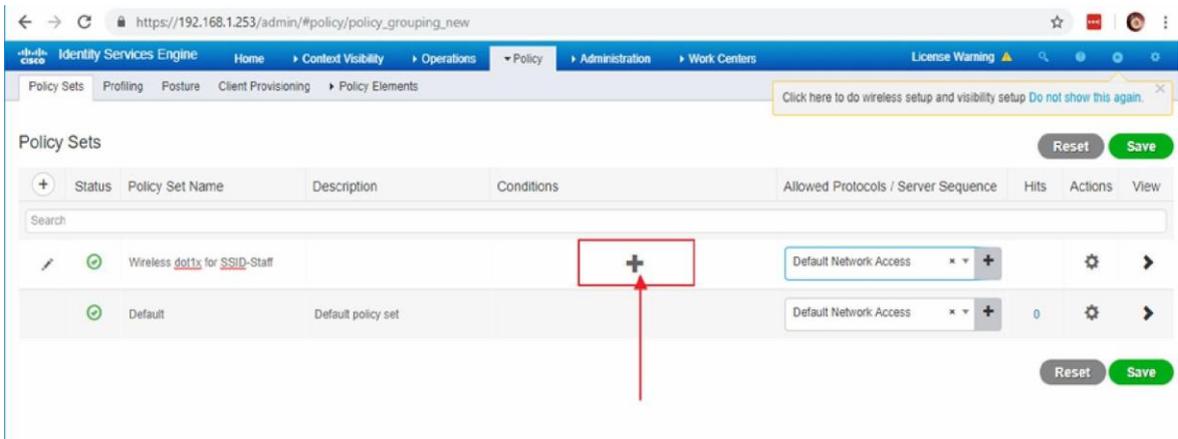


Đặt tên cho policy: Wireless dot1x for SSID-Staff

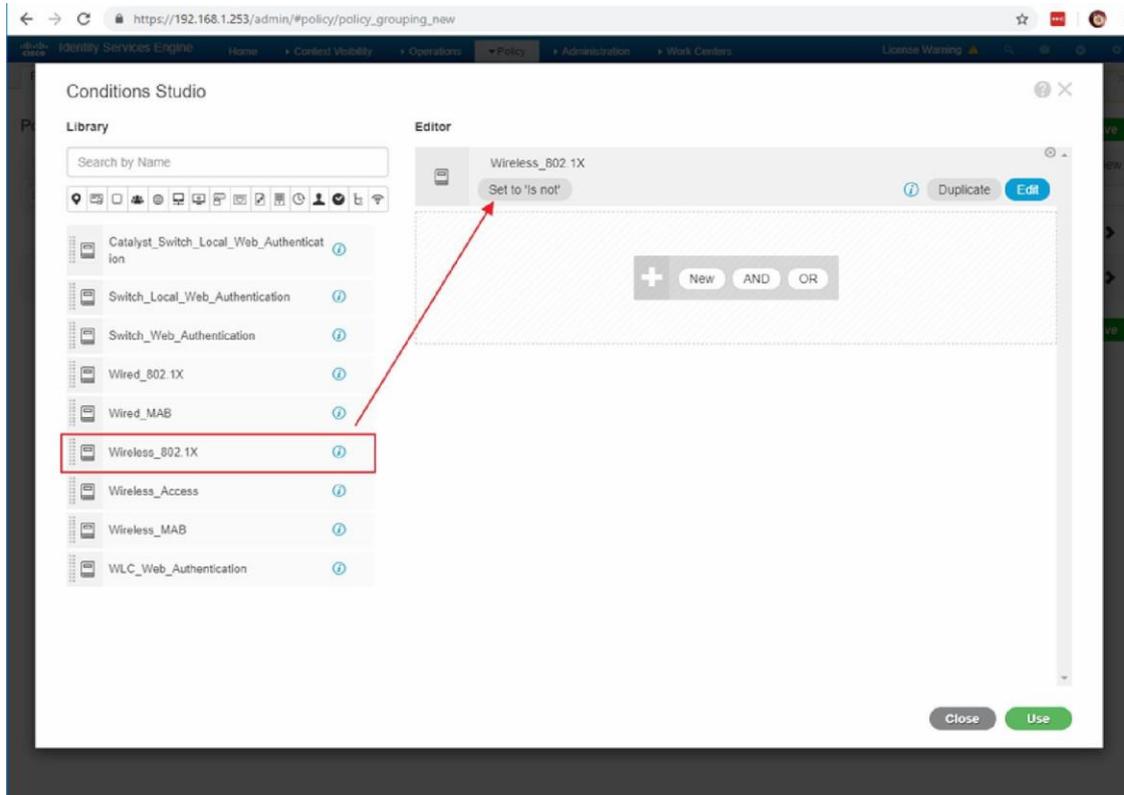
Chọn Allowed Protocols là Default Network Access



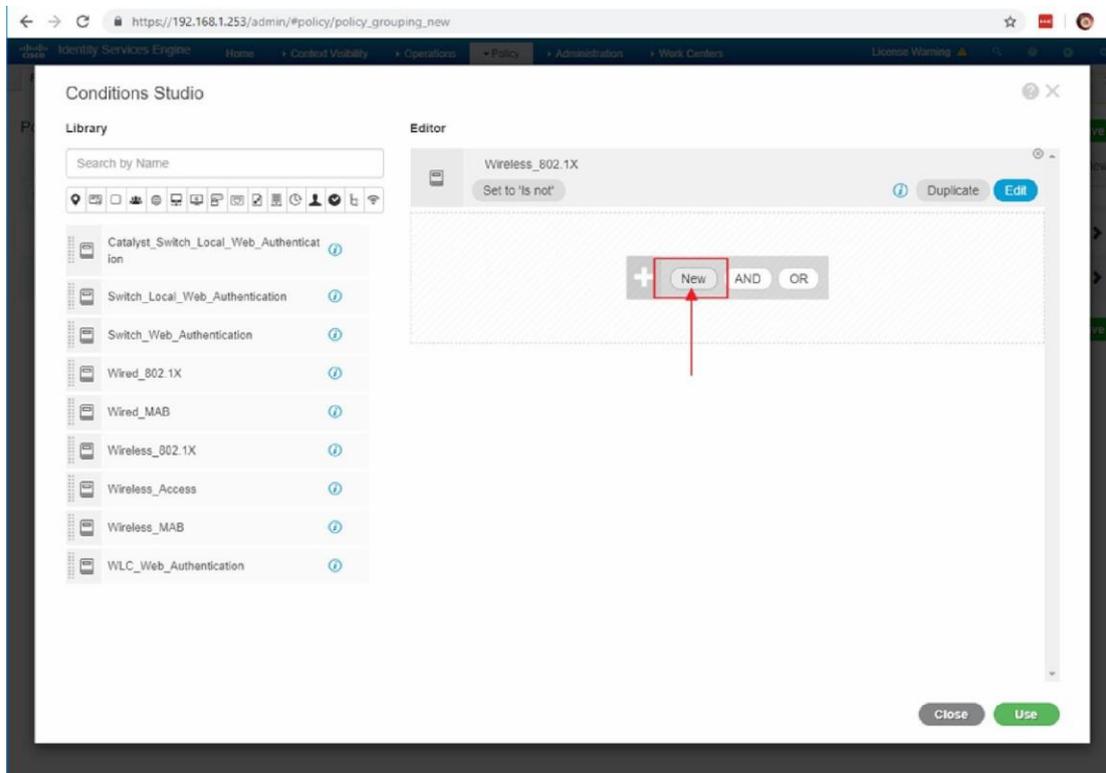
Click Add ở mục Condition



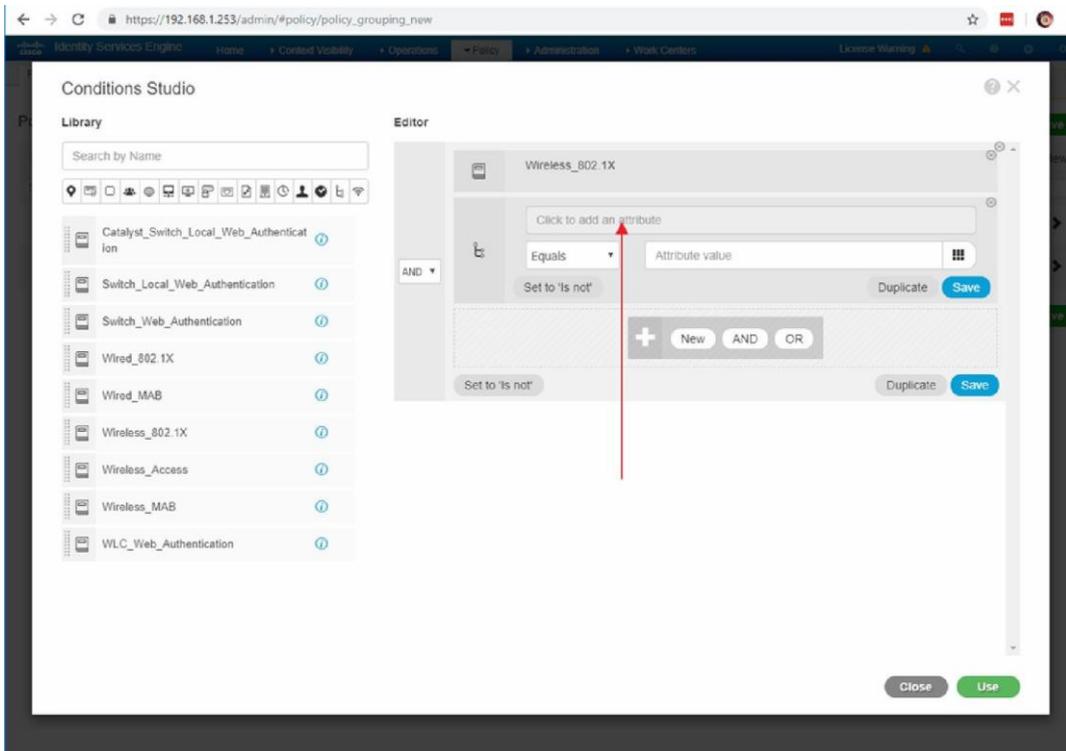
Kéo mục Wireless_802.1X ở cột Library và thả vào cột Editor



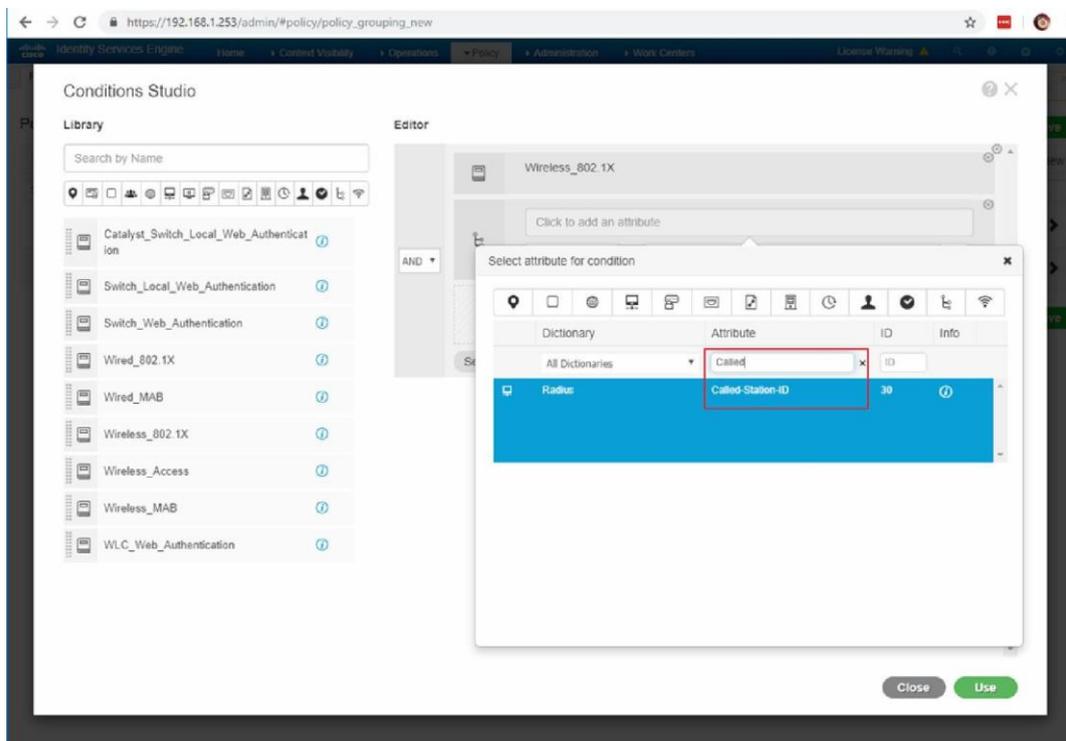
Click New



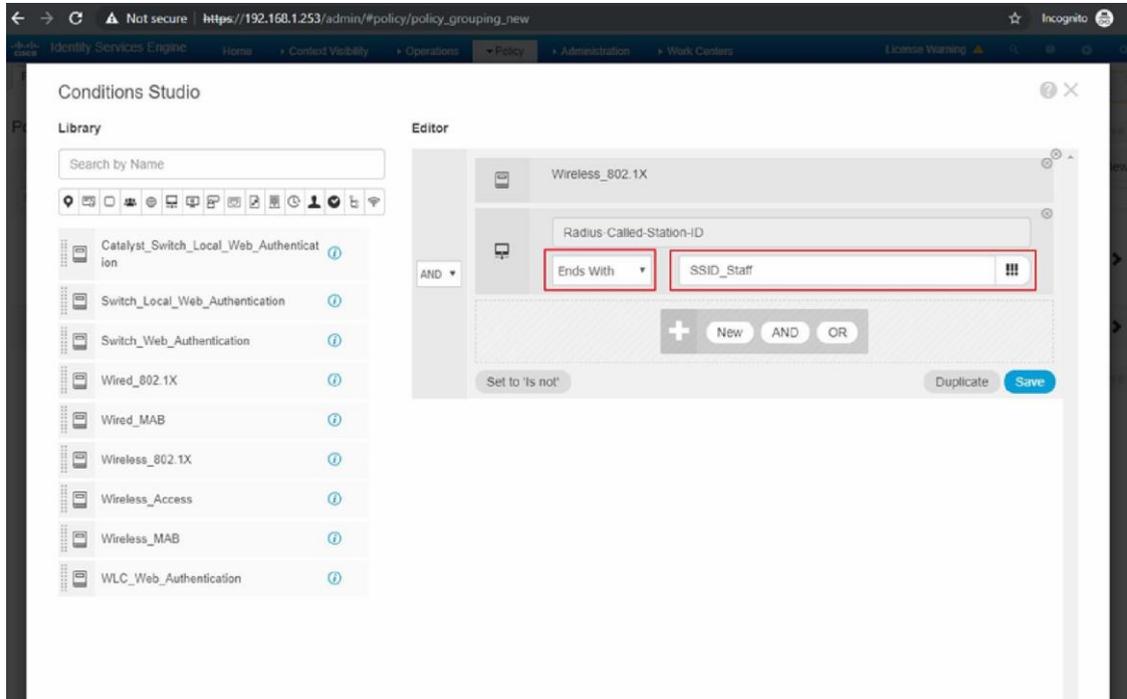
Click vào mục “Click to add an attribute”



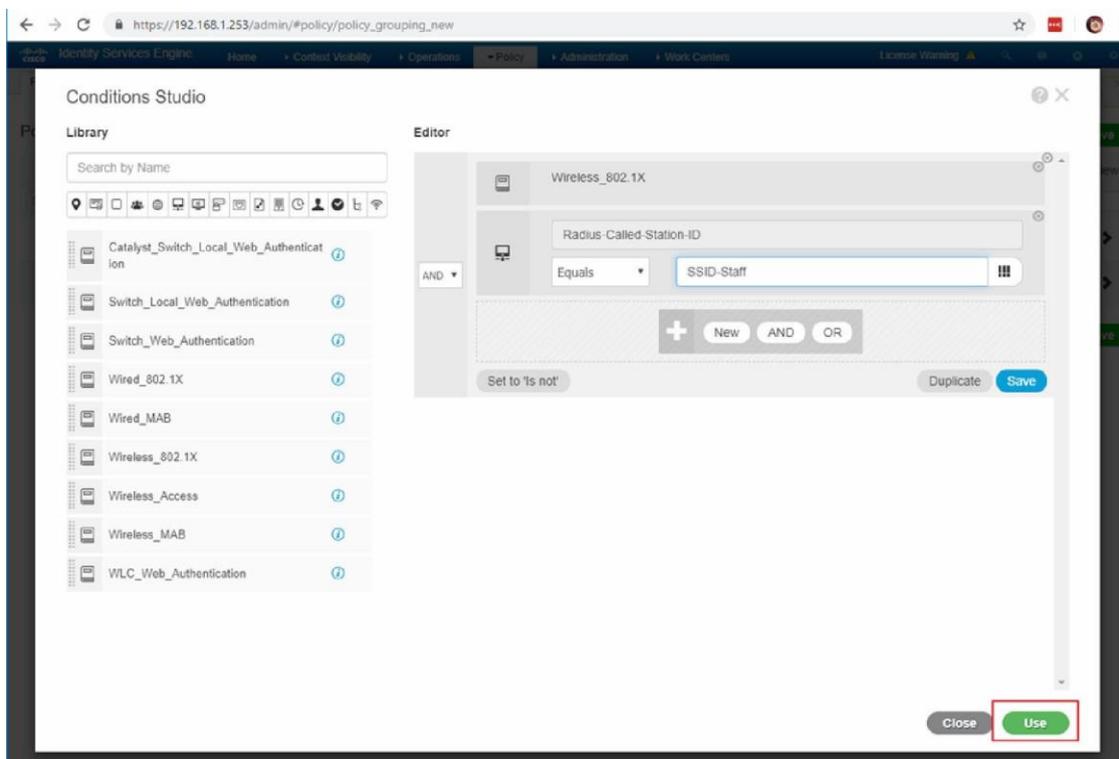
Chọn Attribute Called-Station-ID



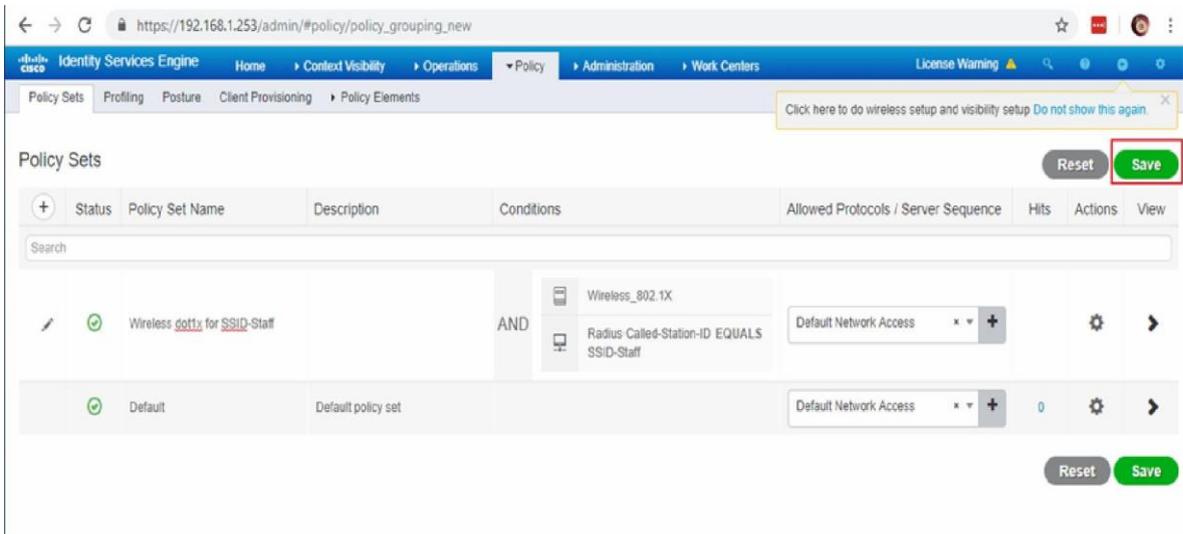
Chọn Value là ENDS_ WITH SSID-Staff



Click Use

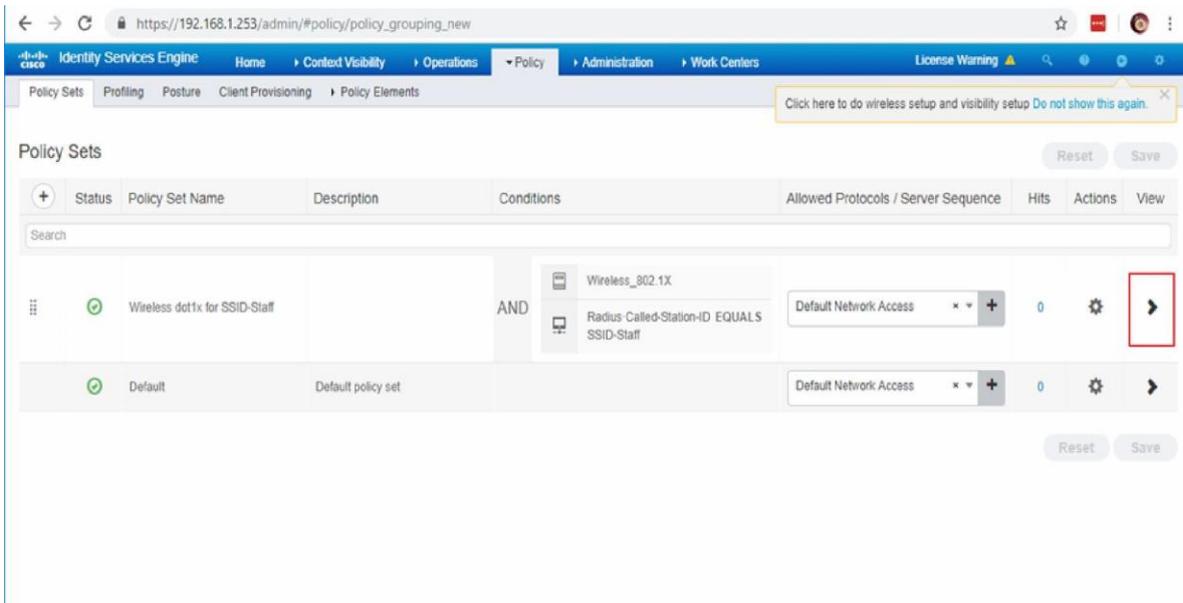


Click Save



4.6. Tạo Authentication Policy

Click vào icon “>” ở cuối Policy



Trong phần Authenticaion Policy, chọn Internal Users. Trong phần Options:

If Auth fail: REJECT

If User not fount: REJECT

If Process fail: DROP

The screenshot shows the 'Policy Sets' configuration page for 'Wireless dot1x for SSID-Staff'. The main configuration area shows conditions: 'Wireless_802.1X' AND 'Radius-Called-Station-ID EQUALS SSID-Staff'. Below this, the 'Authentication Policy (1)' section is expanded, showing a table with one rule named 'Default'. The 'Options' for this rule are: 'Internal Users', 'If Auth fail: REJECT', 'If User not found: REJECT', and 'If Process fail: DROP'. Red boxes and numbers 1, 2, and 3 highlight the 'Authentication Policy (1)' header, the 'Internal Users' dropdown, and the options list respectively.

4.7. Tạo Authorization Policy cho User trong Group Staff và VIP

Trong phần Authorization Policy, click Add để thêm Rule

The screenshot shows the 'Policy Sets' configuration page for 'Wireless dot1x for SSID-Staff'. The main configuration area shows conditions: 'Wireless_802.1X' AND 'Radius-Called-Station-ID EQUALS SSID-Staff'. Below this, the 'Authorization Policy (1)' section is expanded, showing a table with one rule named 'Default'. The 'Results' for this rule are: 'DenyAccess' and 'Select from list'. A red box and number 1 highlight the 'Authorization Policy (1)' header, and another red box and number 2 highlight the '+' button to add a new rule.

Đặt tên Rule là VLAN for Staff

Policy Sets → Wireless dot1x for SSID-Staff

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wireless dot1x for SSID-Staff		AND Wireless_802.1X Radius-Called-Station-ID EQUALS SSID-Staff	Default Network Access	0

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
✔	VLAN for Staff	+		Select from list	Select from list		
✔	Default			DenyAccess	Select from list	0	

Ở phần Conditions, click Add

Policy Sets → Wireless dot1x for SSID-Staff

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wireless dot1x for SSID-Staff		AND Wireless_802.1X Radius-Called-Station-ID EQUALS SSID-Staff	Default Network Access	0

Authentication Policy (1)

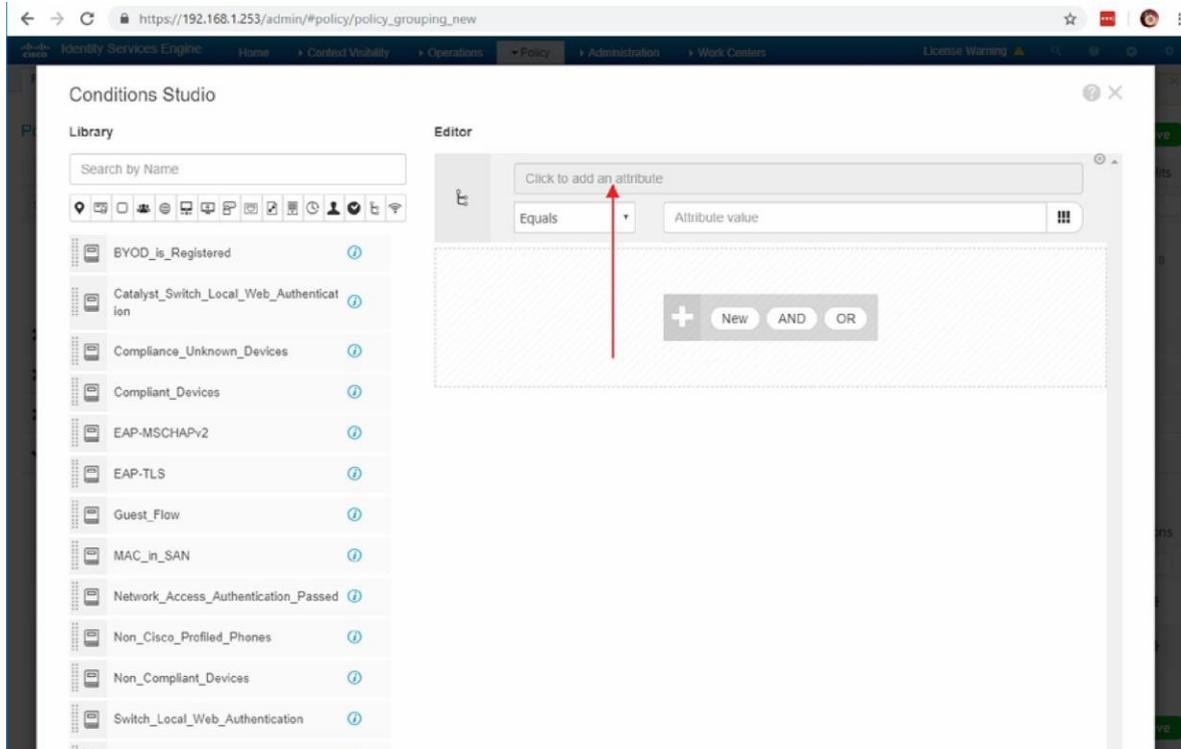
Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

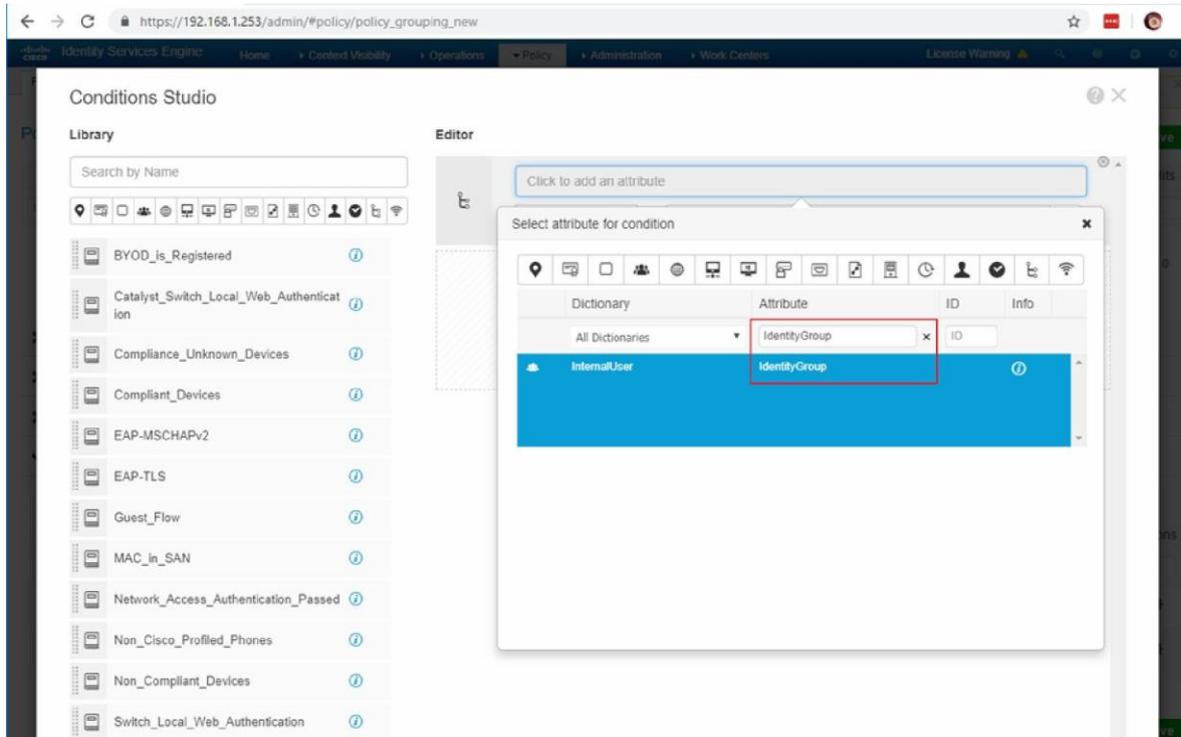
Authorization Policy (2)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
✔	VLAN for Staff	+		Select from list	Select from list		
✔	Default			DenyAccess	Select from list	0	

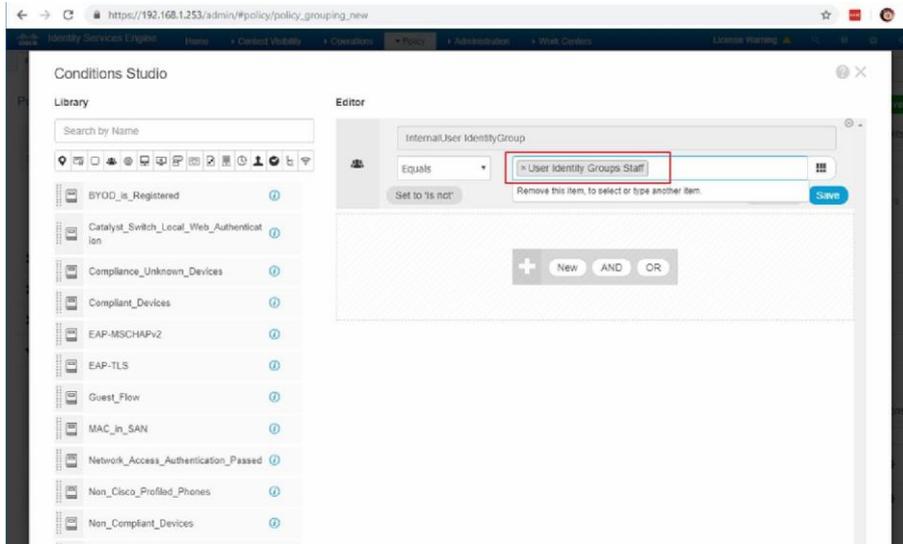
Click vào mục “click to add an attribute”



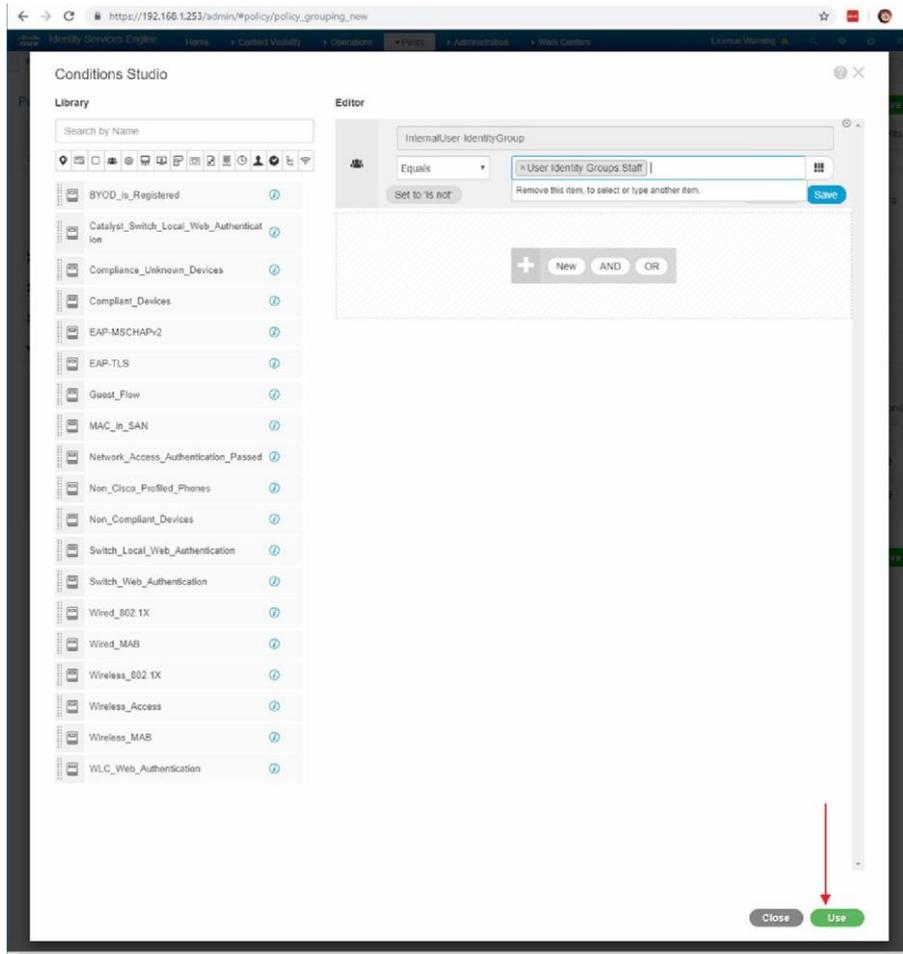
Chọn Attribute IdentityGroup



Ở phần value, chọn User Identity Groups: Staff



Click Use



Trong phần Results → Profiles, chọn profile Assign_VLAN_10 đã tạo ở bước 4.4.

Policy Sets → Wireless dot1x for SSID-Staff

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wireless dot1x for SSID-Staff		AND Wireless_802.1X Radius Called-Station-ID EQUALS SSID-Staff	Default Network Access	0

▼ Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		Internal Users	0	Options

► Authorization Policy - Local Exceptions

► Authorization Policy - Global Exceptions

▼ Authorization Policy (2)

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✔	VLAN for Staff	InternalUser IdentityGroup EQUALS User Identity Groups Staff	Assign_VLAN_10	Select from list	0	Options
✔	Default		DenyAccess	Select from list	0	Options

Reset Save

Click Save

Policy Sets → Wireless dot1x for SSID-Staff

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wireless dot1x for SSID-Staff		AND Wireless_802.1X Radius Called-Station-ID EQUALS SSID-Staff	Default Network Access	0

▼ Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		Internal Users	0	Options

► Authorization Policy - Local Exceptions

► Authorization Policy - Global Exceptions

▼ Authorization Policy (2)

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✔	VLAN for Staff	InternalUser IdentityGroup EQUALS User Identity Groups Staff	Assign_VLAN_10	Select from list	0	Options
✔	Default		DenyAccess	Select from list	0	Options

Reset Save

Click Add để tạo thêm Rule

The screenshot shows the 'Policy Sets' configuration page for 'Wireless dot1x for SSID-Staff'. The main configuration area shows a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. Below this, there are sections for 'Authentication Policy (1)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (2)'. In the 'Authorization Policy (2)' section, a table lists existing rules. A red box highlights the '+' icon in the first column of this table, with a red arrow pointing to it.

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
+							
✓	VLAN for Staff	InternalUser IdentityGroup EQUALS User Identity Groups Staff	Assign_VLAN_10	+	Select from list	+	0
✓	Default		DenyAccess	+	Select from list	+	0

Tạo rule thứ hai với tên VLAN for VIP. Trong đó:

Conditions dùng IdentityGroup EQUALS User Identity Groups: VIP

Results → Profiles: Assign_VLAN_30

The screenshot shows the same 'Policy Sets' configuration page, but now with three rules listed in the 'Authorization Policy (3)' section. The first rule, 'VLAN for VIP', is highlighted with a red box. Its configuration is: Status: ✓, Rule Name: VLAN for VIP, Conditions: InternalUser IdentityGroup EQUALS User Identity Groups:VIP, Results: Assign_VLAN_30, Profiles: +, Security Groups: Select from list, Hits: +, Actions: ⚙️.

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
+							
✓	VLAN for VIP	InternalUser IdentityGroup EQUALS User Identity Groups:VIP	Assign_VLAN_30	+	Select from list	+	⚙️
✓	VLAN for Staff	InternalUser IdentityGroup EQUALS User Identity Groups:Staff	Assign_VLAN_10	+	Select from list	+	⚙️
✓	Default		DenyAccess	+	Select from list	+	⚙️

Click Save

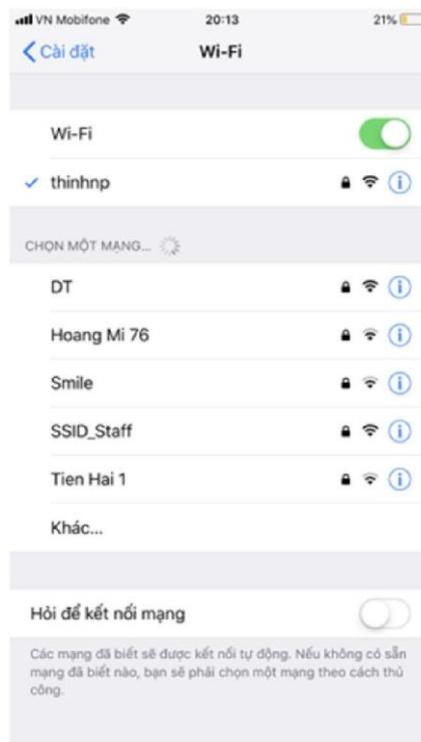
The screenshot shows the ISE configuration interface. At the top, there's a navigation bar with 'Policy Sets' selected. Below it, the policy set 'Wireless dot1x for SSID-Staff' is configured with conditions: 'Wireless_802.1X' AND 'Radius-Called-Station-ID EQUALS SSID-Staff'. The 'Save' button is highlighted with a red box.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wireless dot1x for SSID-Staff		Wireless_802.1X AND Radius-Called-Station-ID EQUALS SSID-Staff	Default Network Access	0

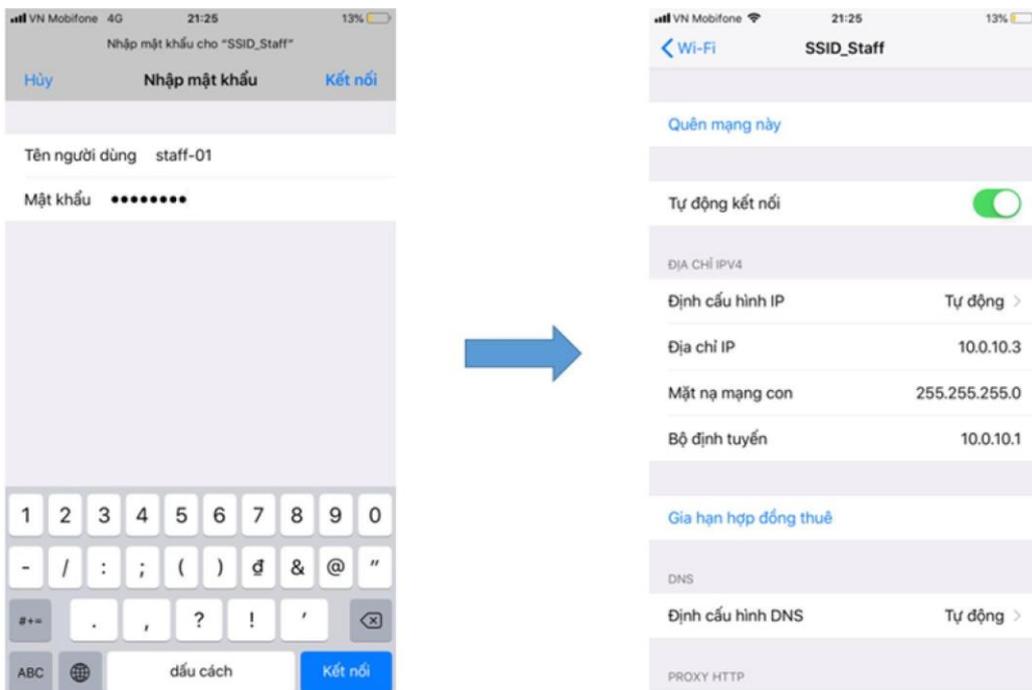
+	Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
✎	✔	VLAN for VIP	InternalUser-IdentityGroup EQUALS User Identity Groups:VIP	= Assign_VLAN_10	Select from list			⚙️
	✔	VLAN for Staff	InternalUser-IdentityGroup EQUALS User Identity Groups:Staff	= Assign_VLAN_10	Select from list		0	⚙️
	✔	Default		= DenyAccess	Select from list		0	⚙️

V. Kiểm tra

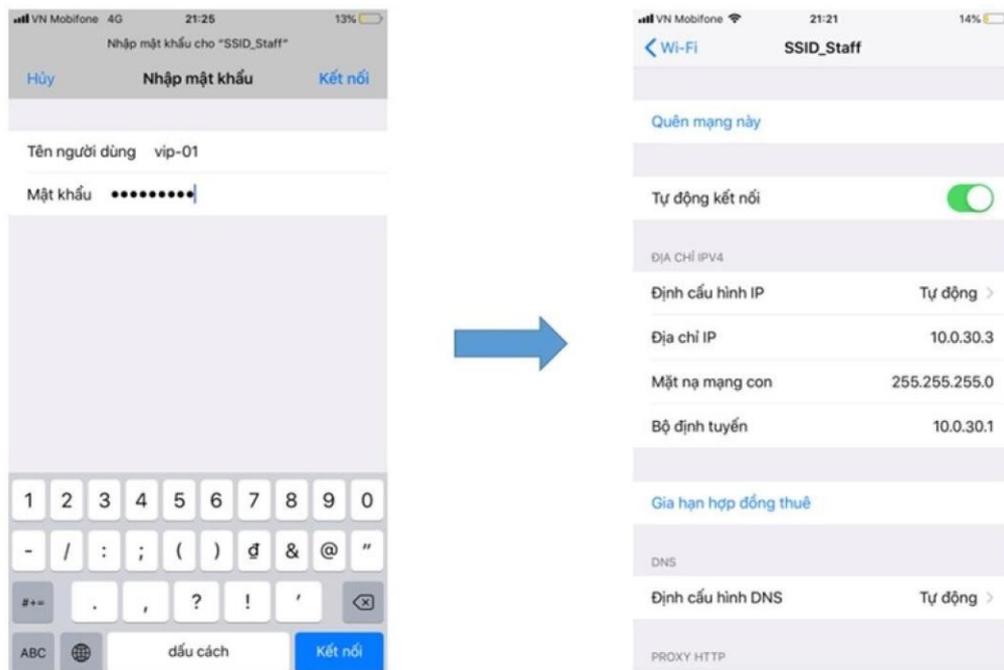
Sau khi cấu hình, AP đã có thể phát SSID_Staff



Kết nối vào với user staff-01, người dùng sẽ nhận được IP trong VLAN 10



Kết nối vào với user vip-01, người dùng sẽ nhận được IP trong VLAN 30



Lưu ý: nếu gặp thông báo về Chứng chỉ, click Tin Cây

