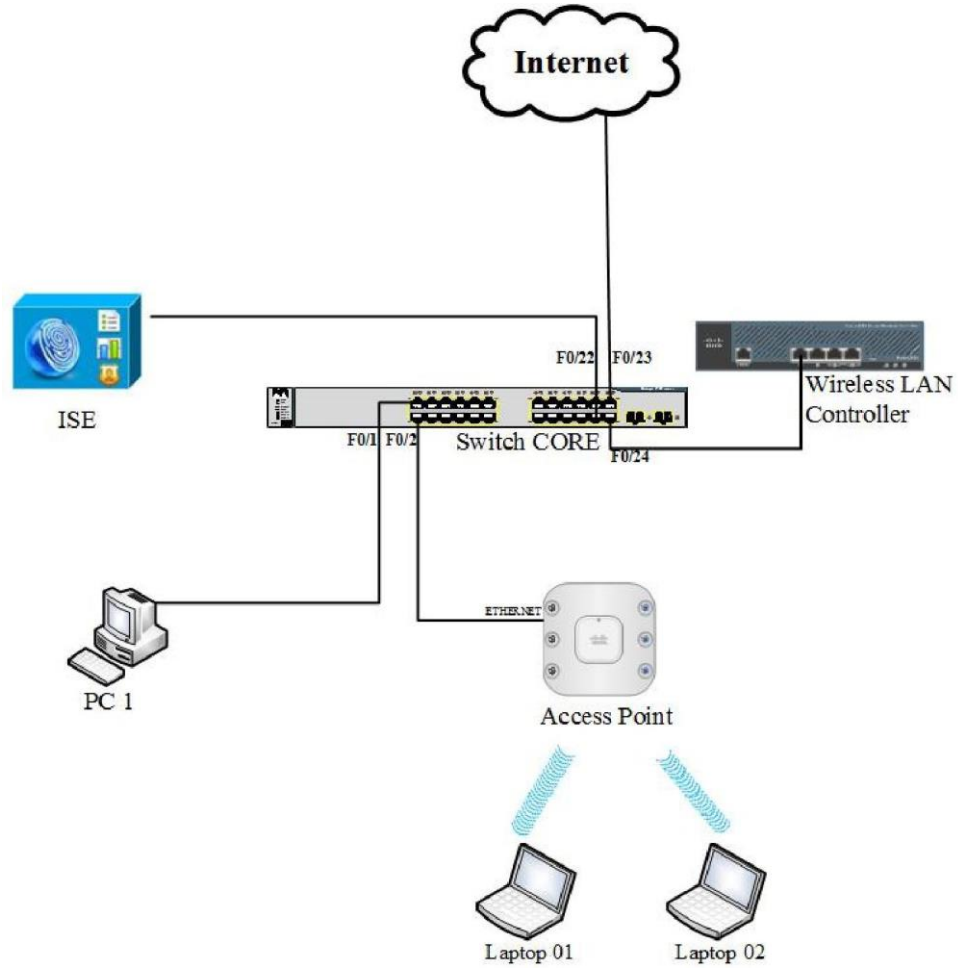
LAB : XÁC THỰC RADIUS 802.1x VỚI CISCO ISE

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 đề 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

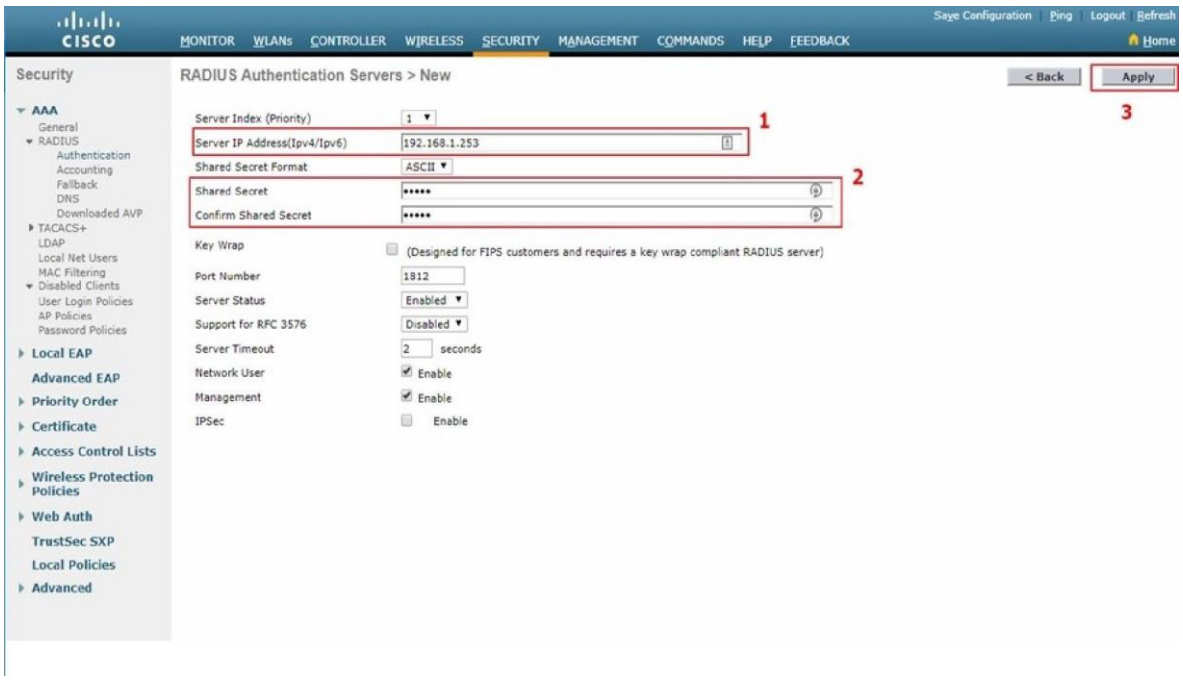
Vào menu SECURITY → AAA → RADIUS → Authentication

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

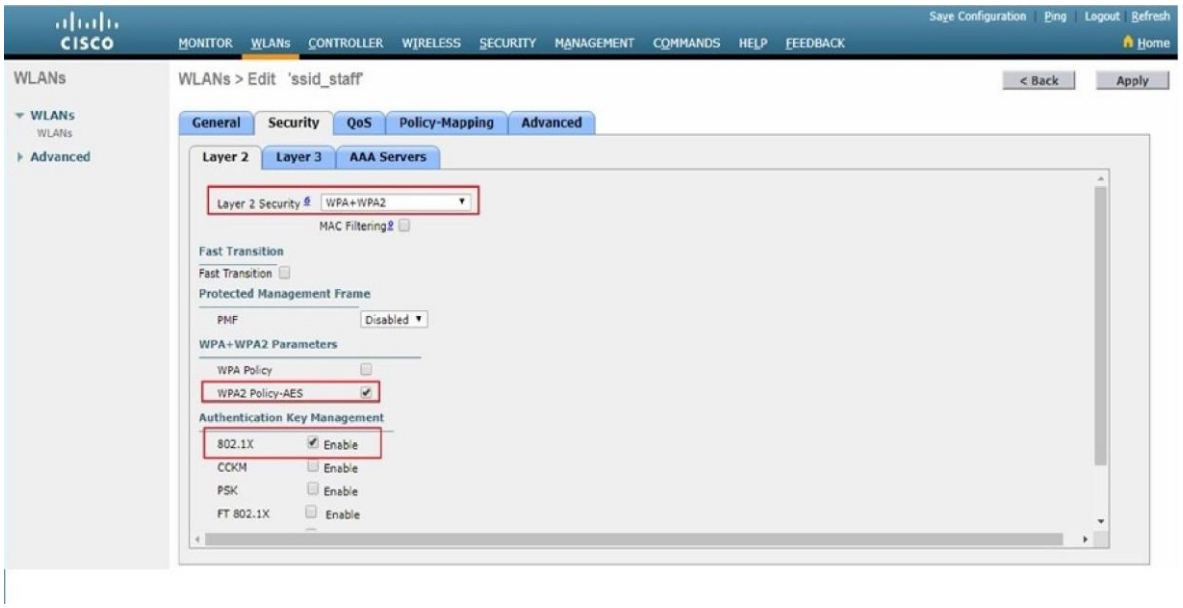
SSID: SSID_Staff

Click Apply

Trong tab General:

Tick chọn Status: Enabled

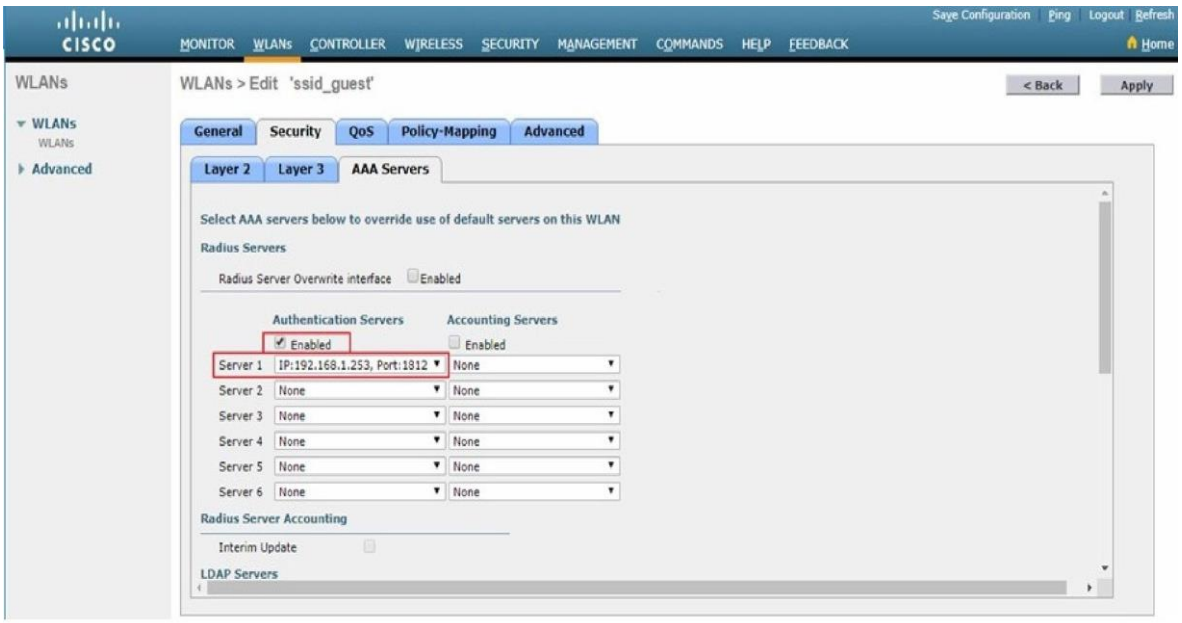
Interface/Interface Group (G): management



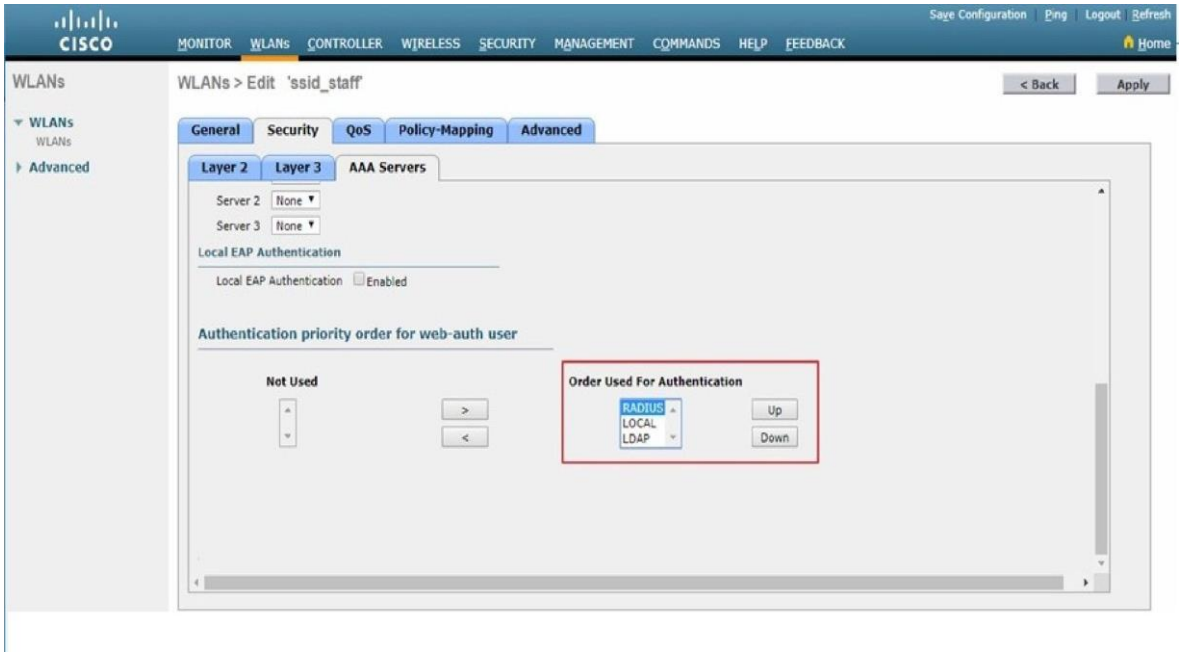
Trong tab Security → AAA Servers:

Tick chọn Enabled ở mục Authentication Servers

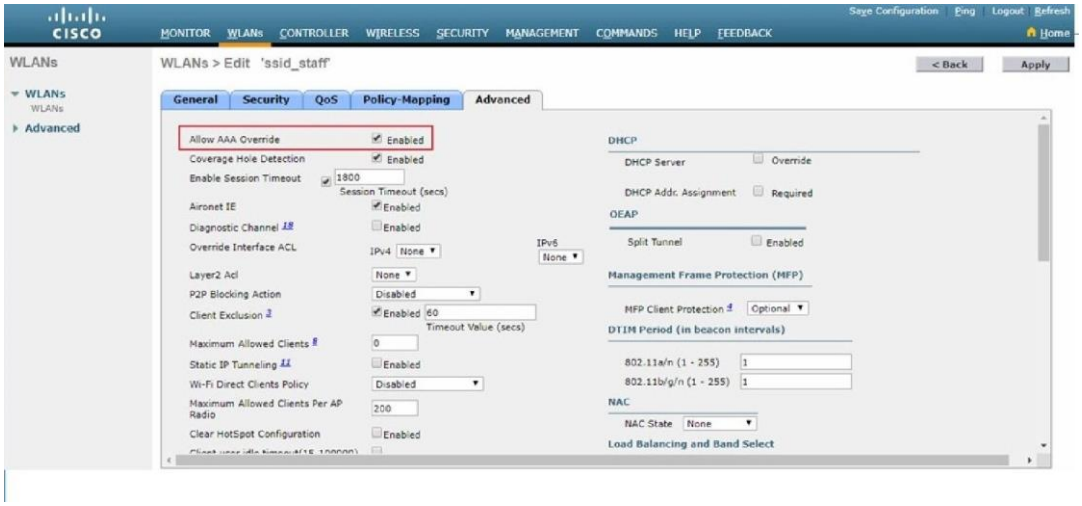
Chọn Server 1 là server mà chúng ta vừa thêm ở bước 2



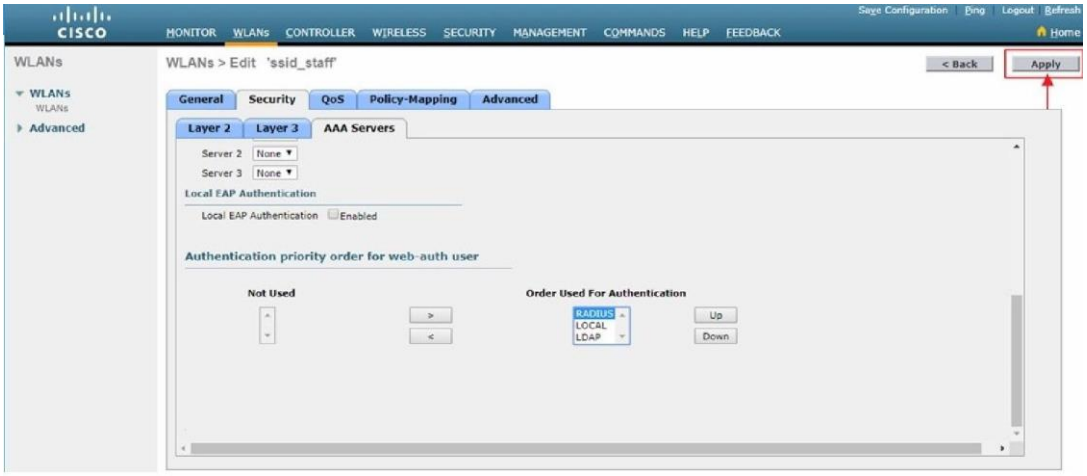
Kéo xuống, trong phần Order Used for Authentication, click chọn RADIUS và click UP để phương thức xác thực RADIUS nằm đầu tiên



Vào tab Advanced, tích chọn Allow AAA Override



Click Apply

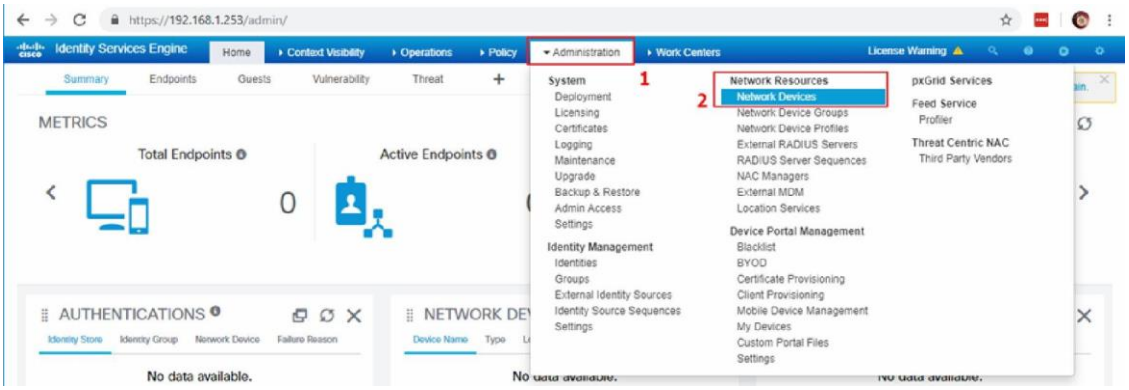


Yêu cầu 4: Cấu hình Cisco ISE

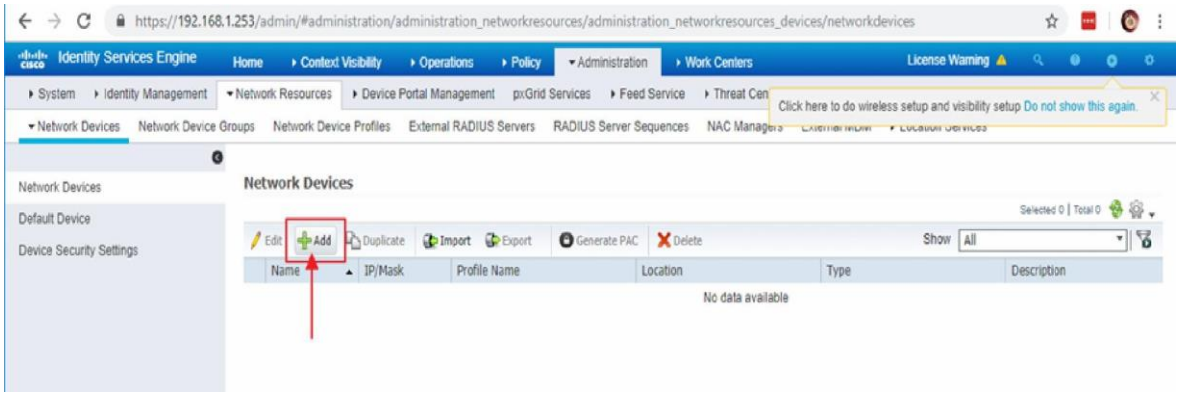
4.1. Thêm WLC vào Cisco ISE

Truy cập vào Cisco ISE

Vào menu Administration → Network Resources → Network Devices

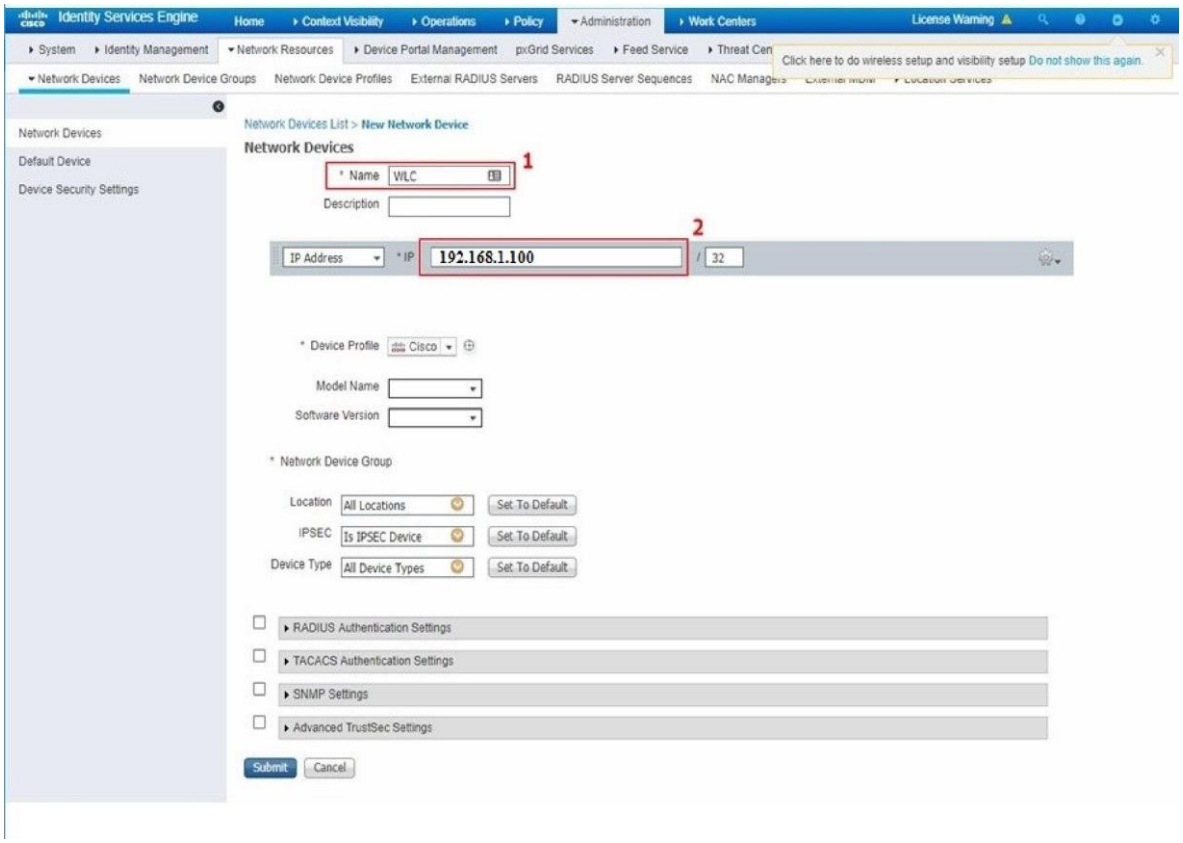


Click Add



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

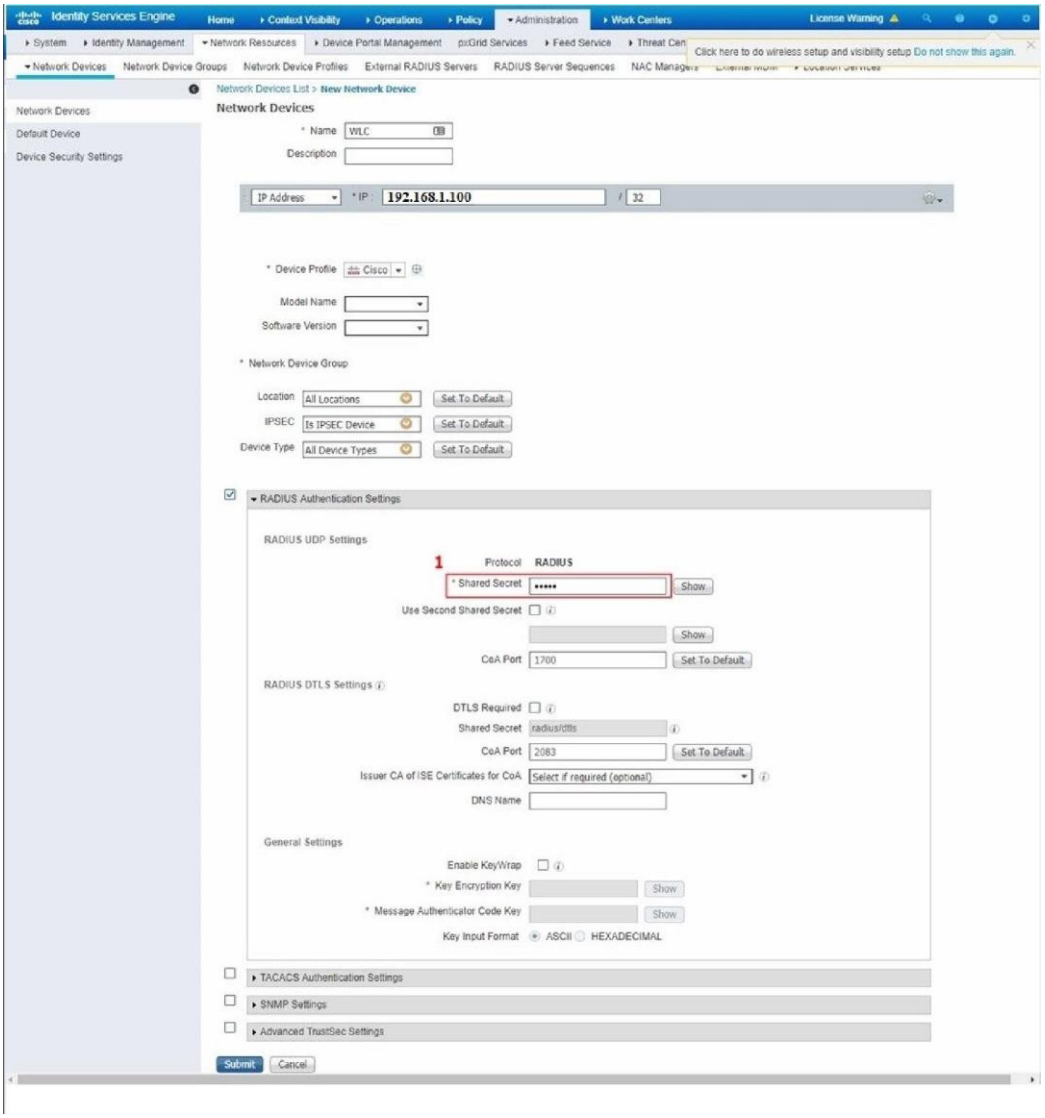
Nhập IP thiết bị



Tích chọn vào mục RADIUS

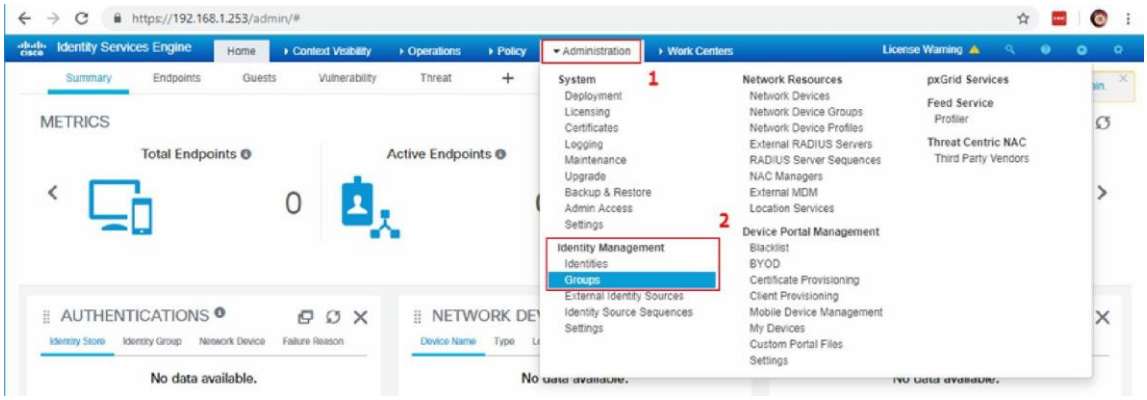
Nhập shared secret (giống với shared secret đã đặt ở bước 2, bài lab này chọn shared secret là vnpro)

Sau đó click Submit

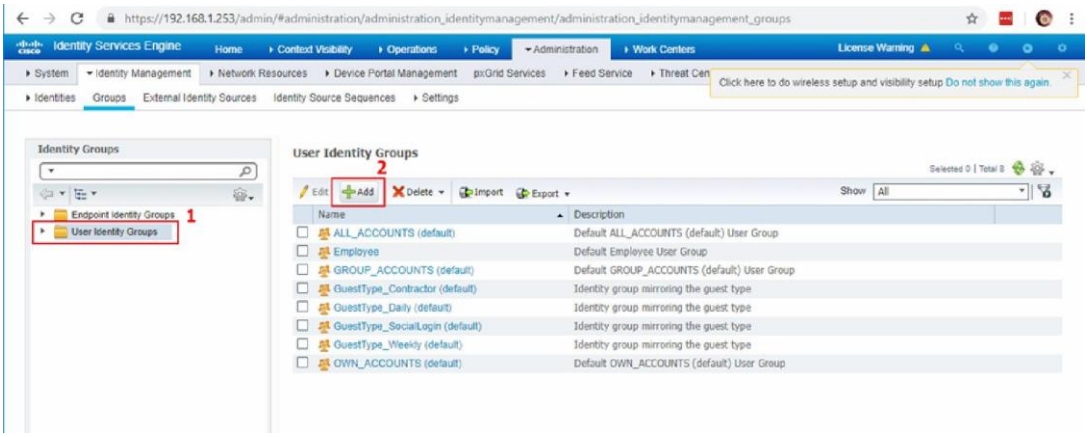


4.2. Tạo group

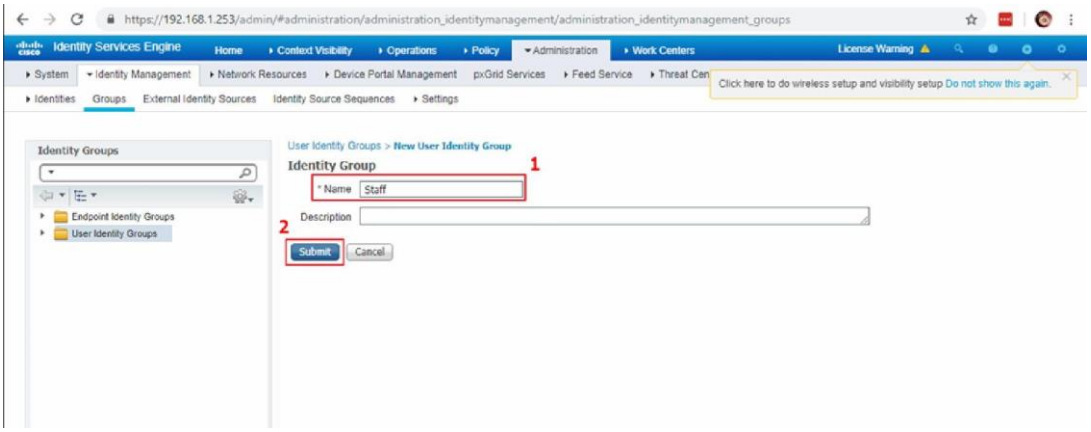
Vào menu Administration → Identity Management → Groups



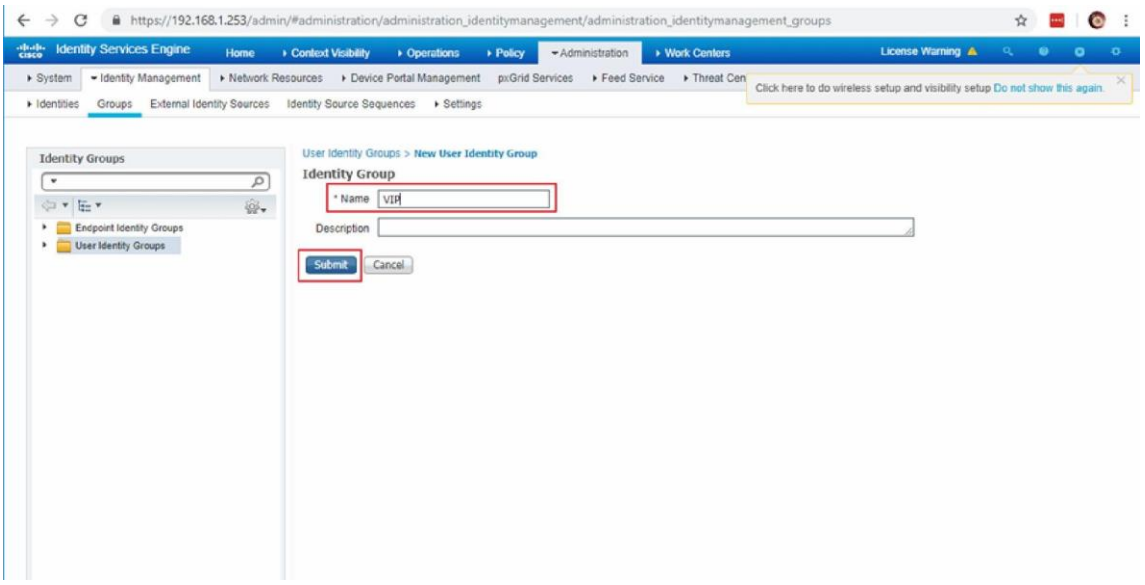
Click vào mục User Identity Group, sau đó click Add



Đặt tên group là Staff và click Submit

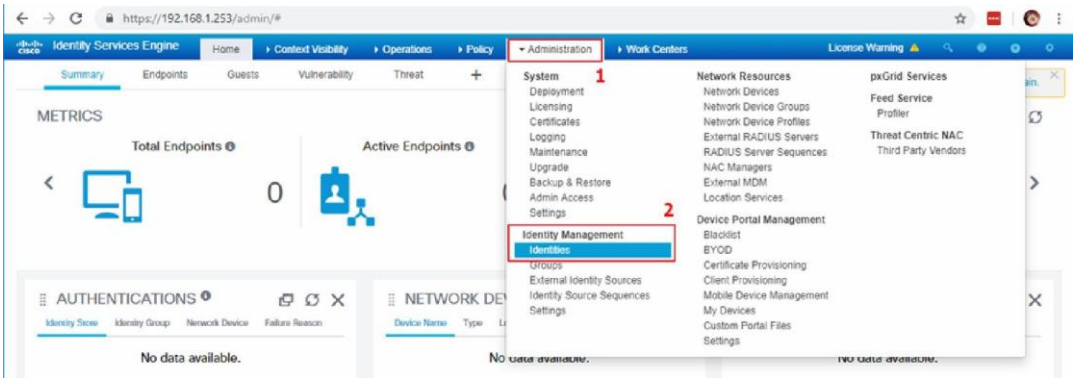


Thực hiện tương tự cho group VIP

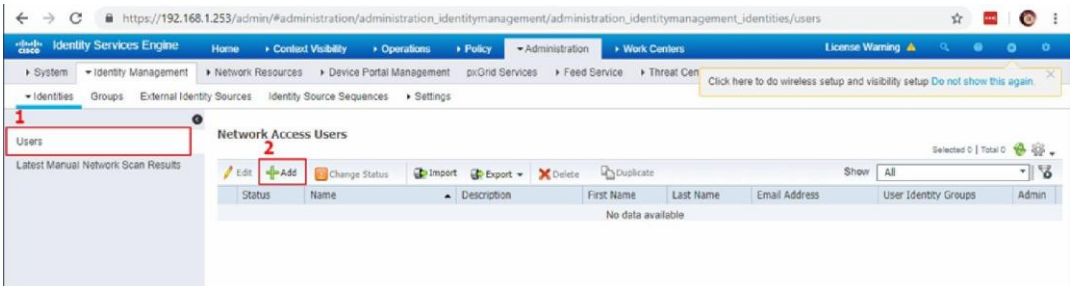


4.3. Tạo user

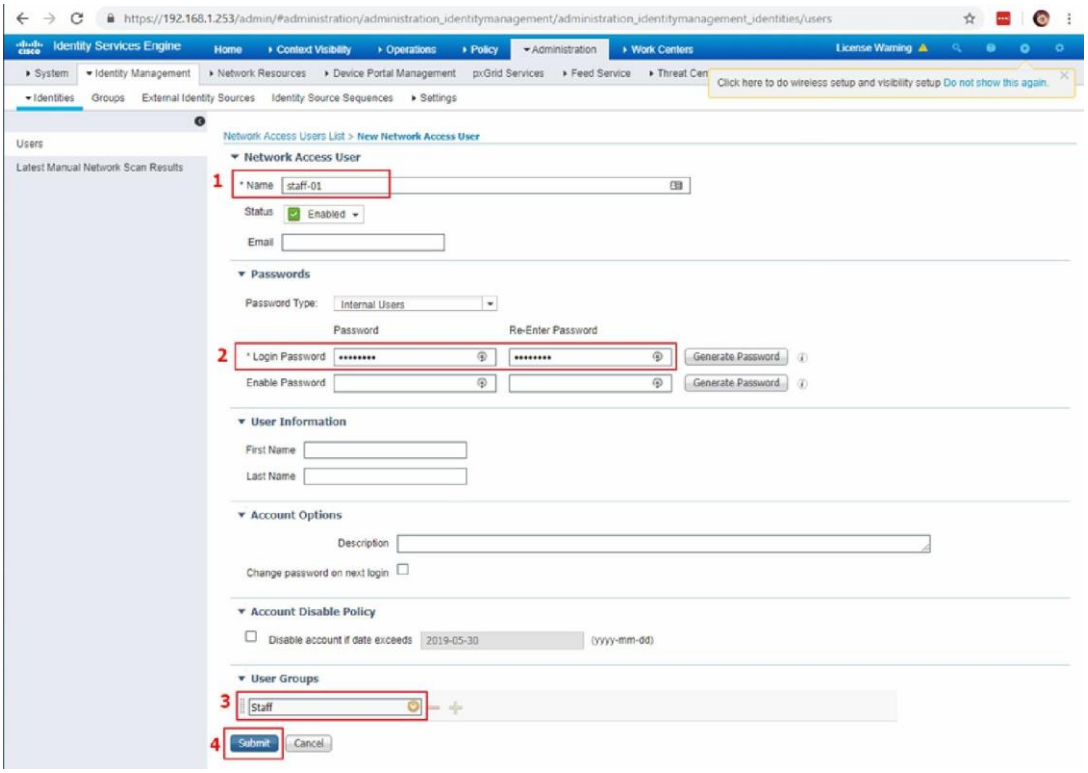
Vào menu Administration → Identity Management → Identities



Click chọn Users, sau đó click Add



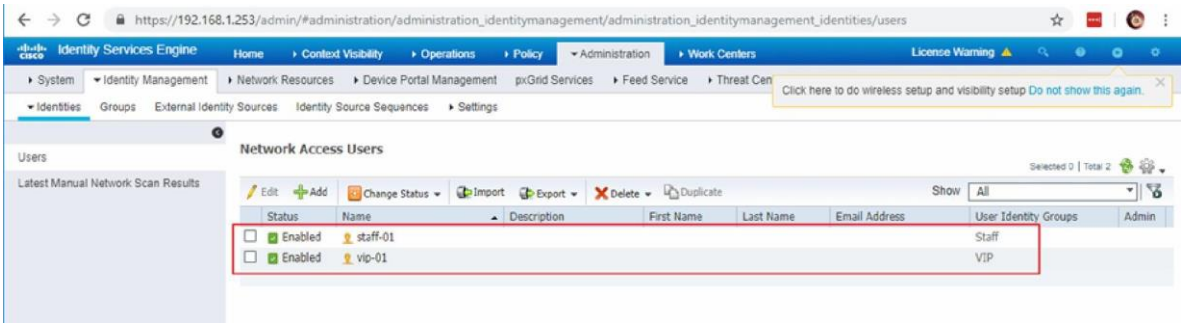
Nhập: Username, Password và confirm password, chọn User Groups, click Submit



Tạo 2 user:

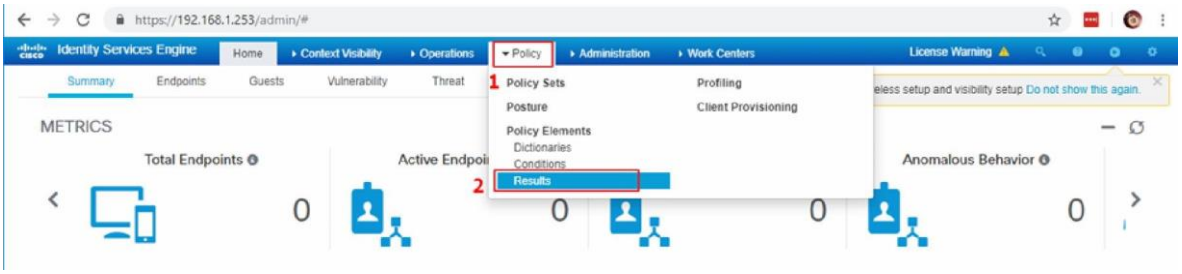
User staff-01, password Qwe@#123, thuộc nhóm Staff

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

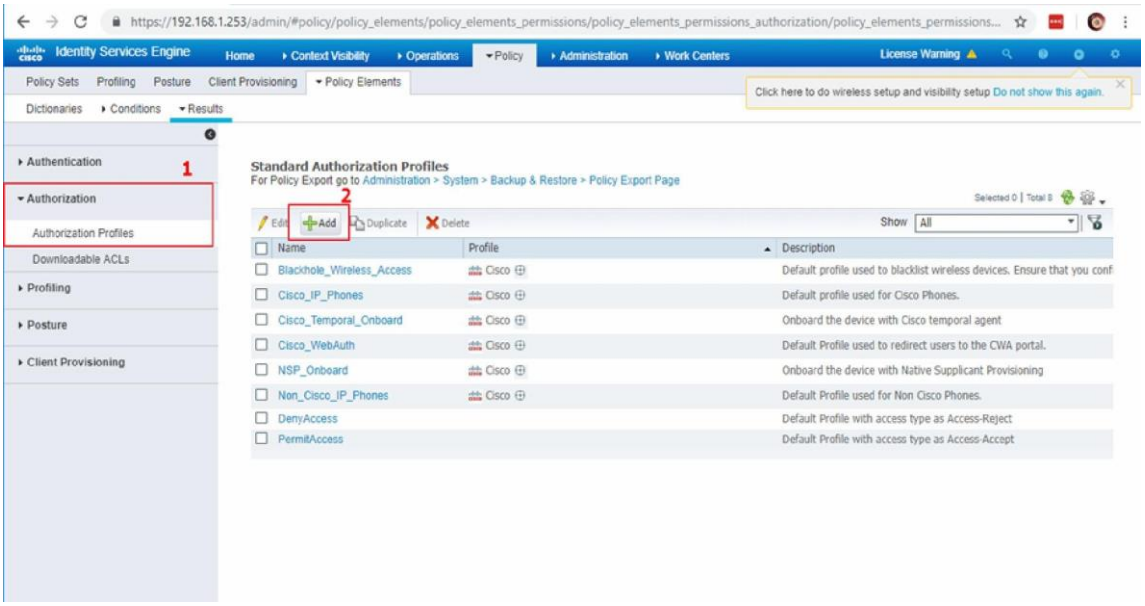


4.4. Tạo Result

Vào menu Policy > Results



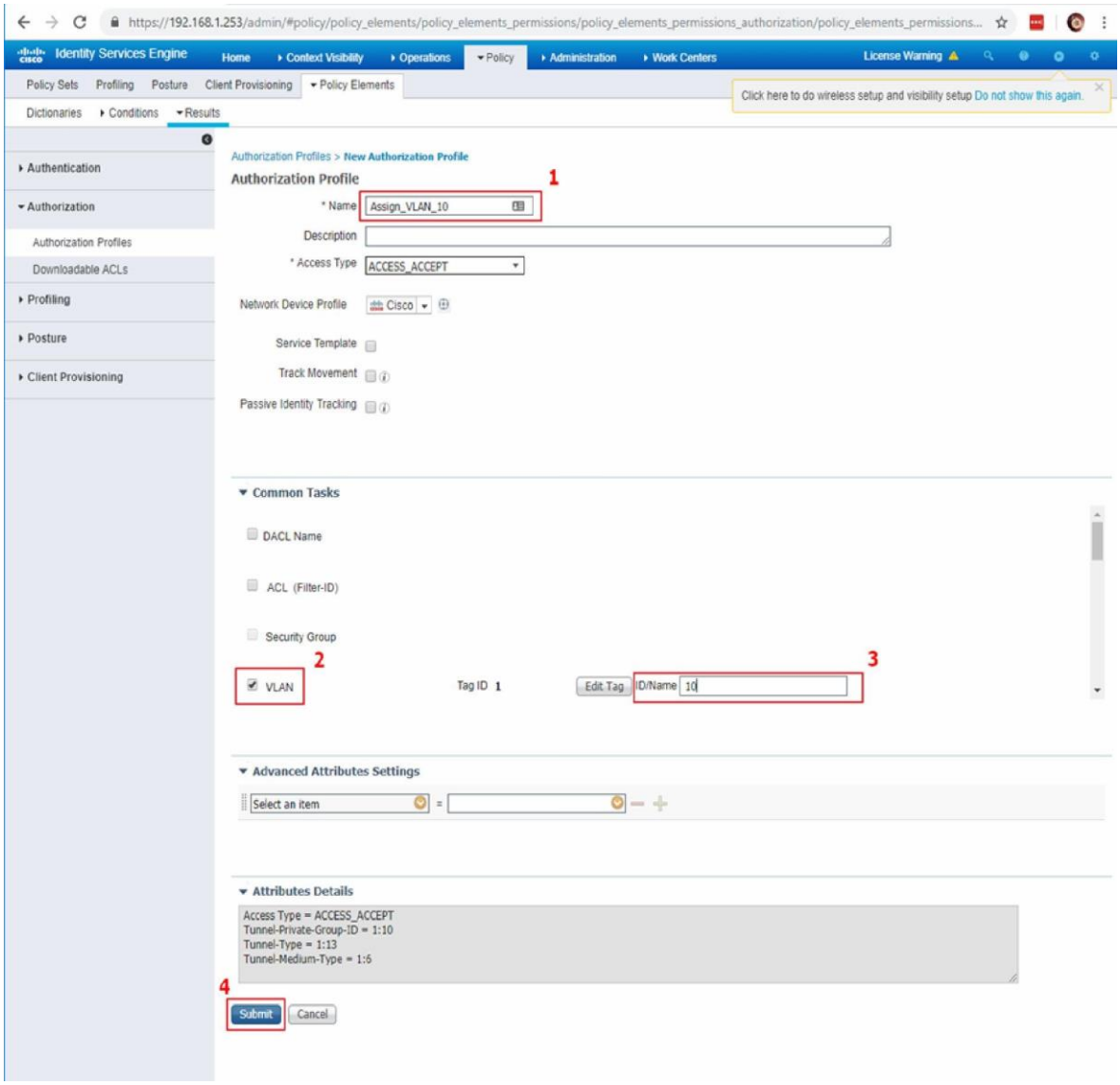
Vào mục Authorization → Authorization Profiles. Click Add



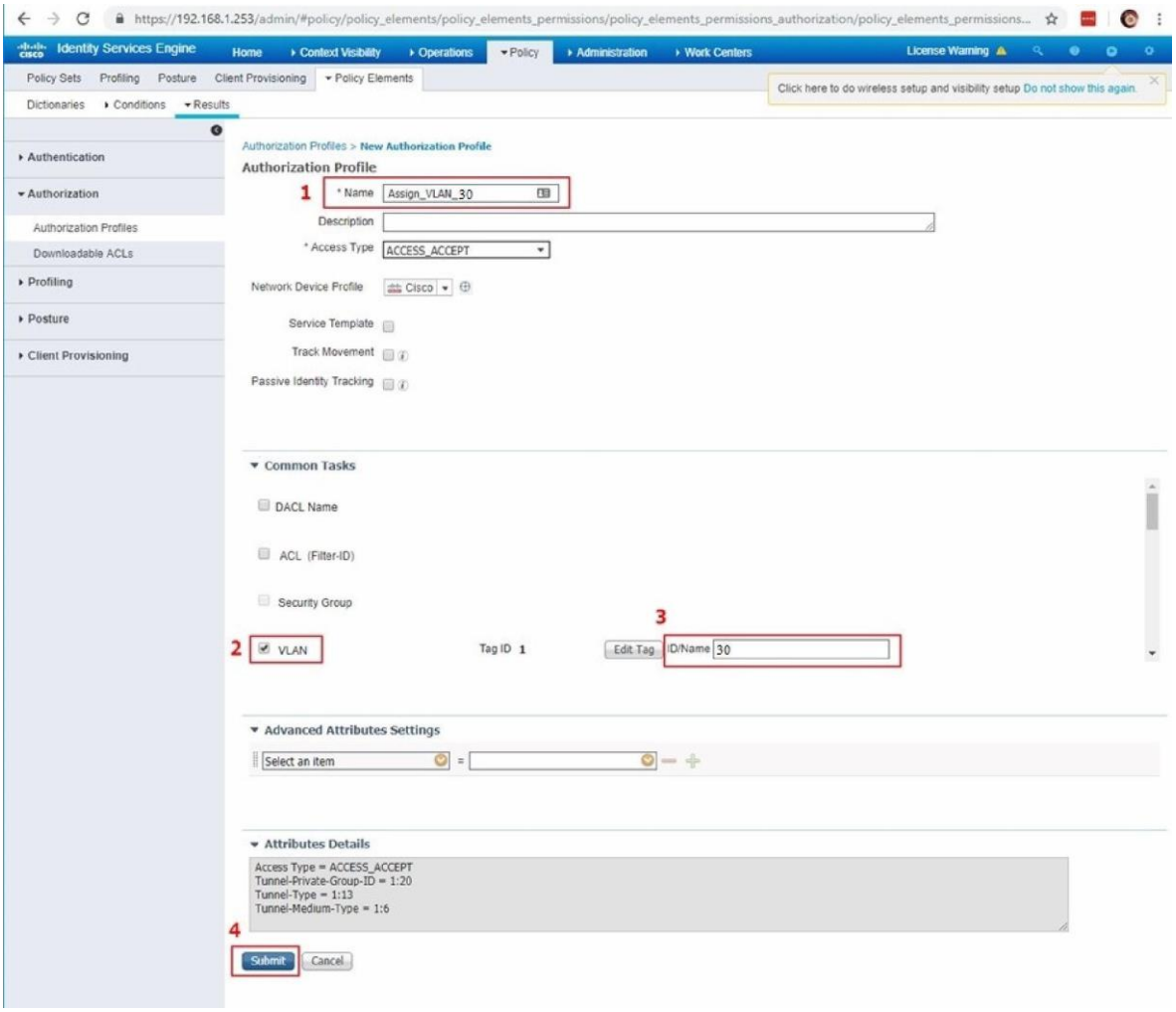
Đặt tên cho Profile: Assign_VLAN_10

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

Sau đó click Submit



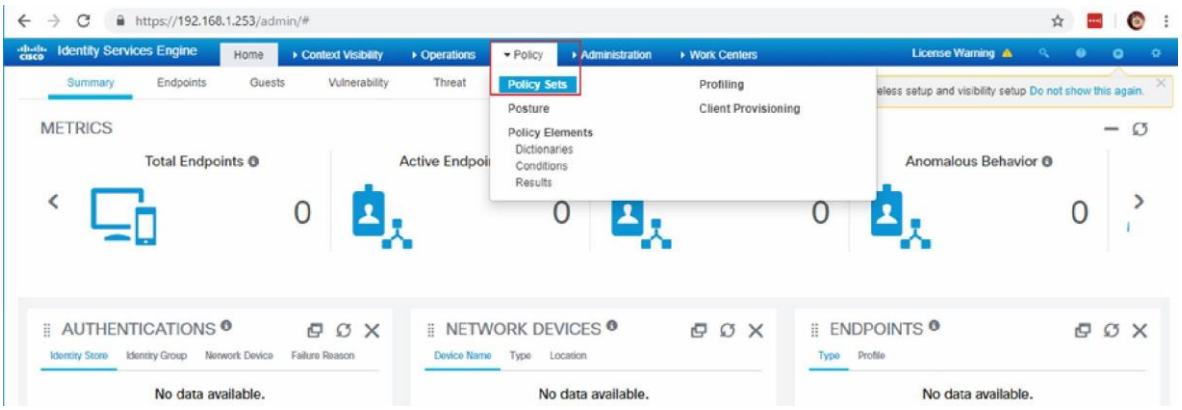
Thực hiện tương tự để tạo profile Assign_VLAN_30



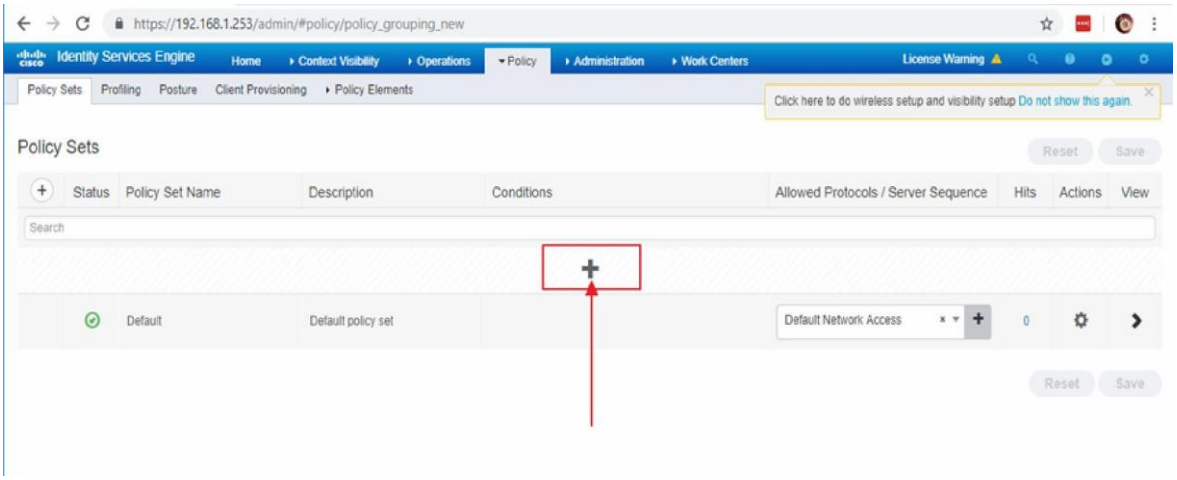
4.5. Cấu hình Policy

Tạo Policy

Vào menu Policy → Policy Set

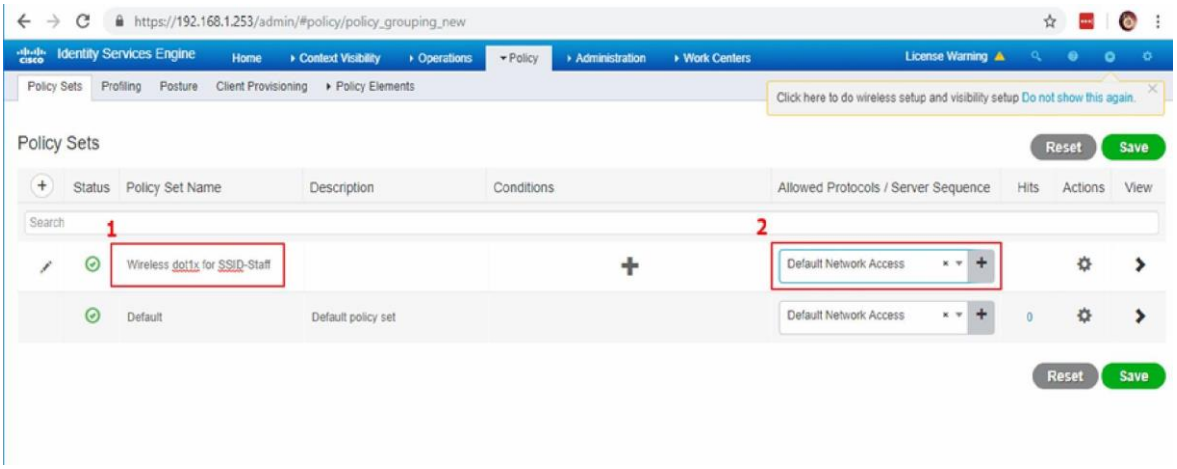


Click Add (icon +)

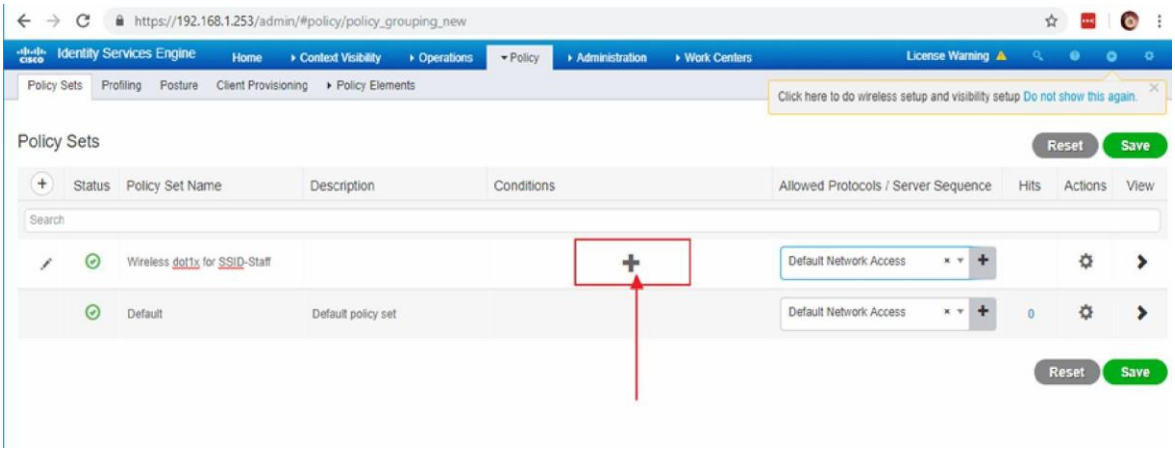


Đặt tên cho policy: Wireless dot1x for SSID-Staff

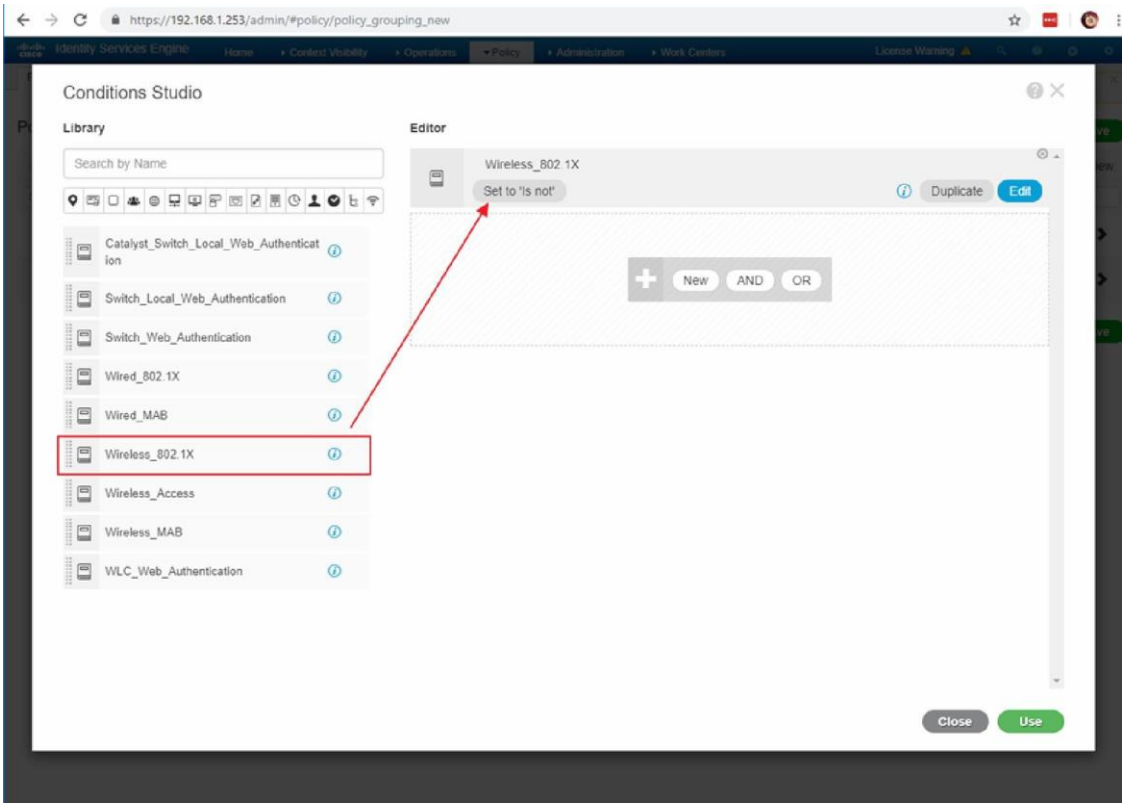
Chọn Allowed Protocols là Default Network Access



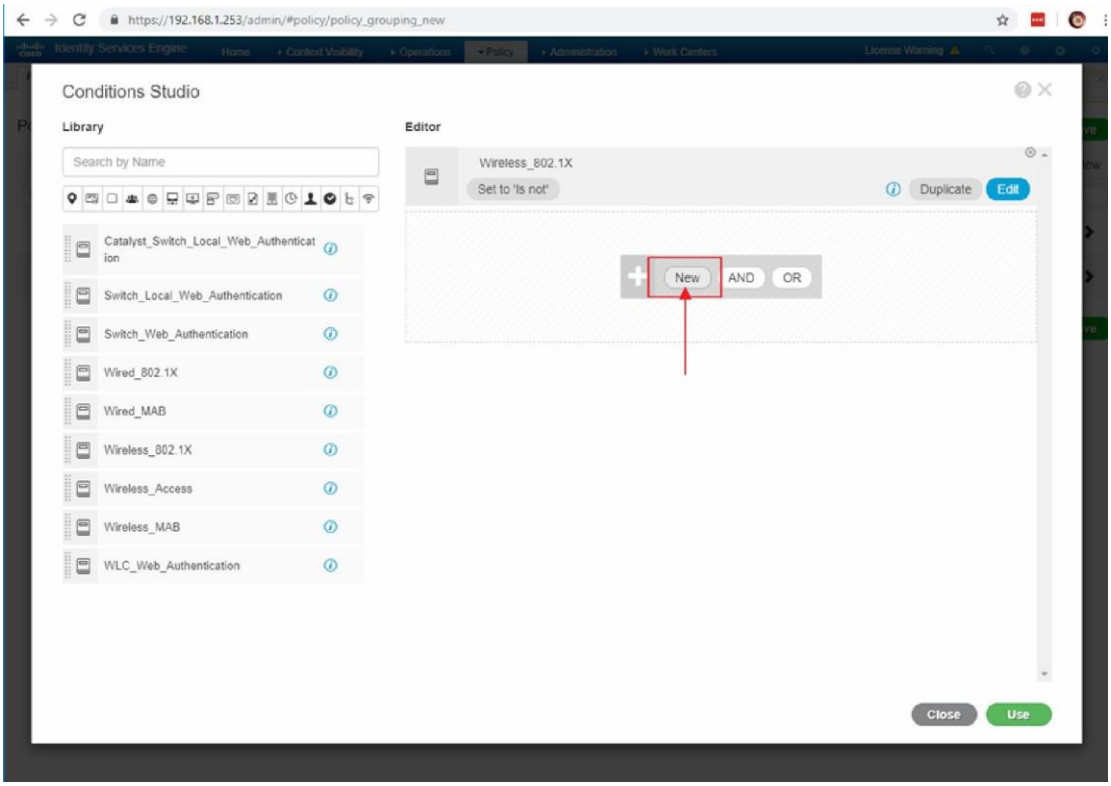
Click Add ở mục Condition



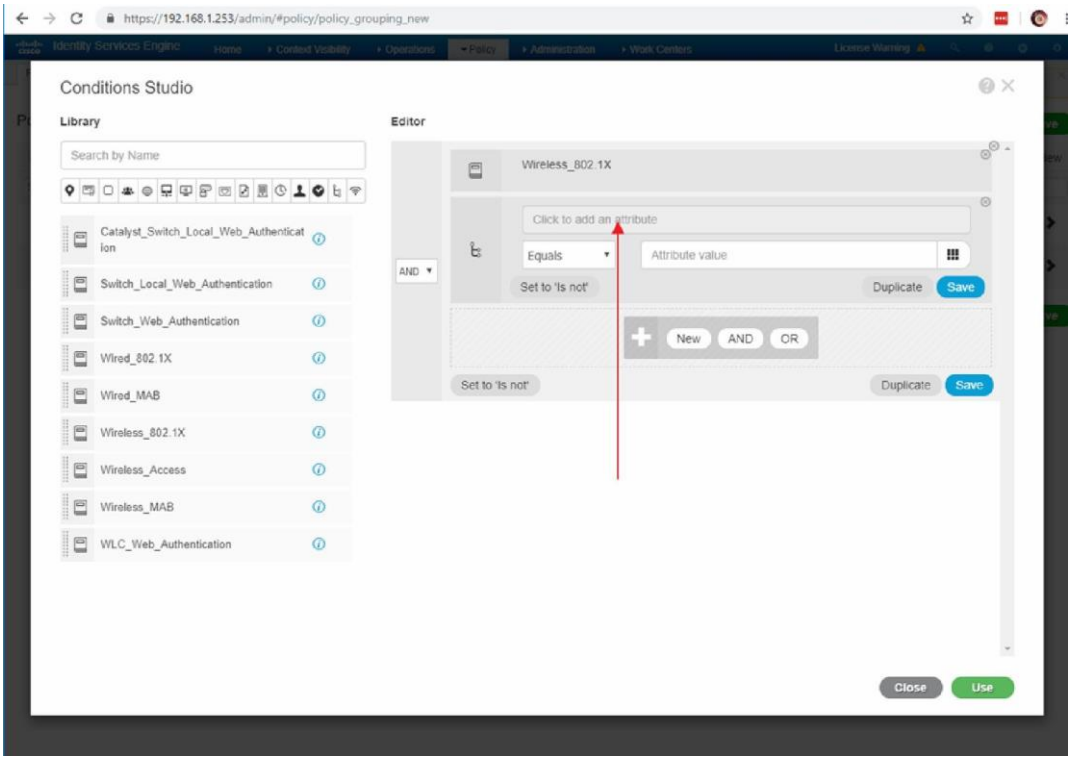
Kéo mục Wireless_802.1X ở cột Library và thả vào cột Editor


https://192.168.1.253/admin/#policy/policy_grouping_new
Conditions Studio
Library
Search by Name
Catalyst_Switch_Local_Web_Authentication
Switch_Local_Web_Authentication
Switch_Web_Authentication
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access
Wireless_MAB
WLC_Web_Authentication
Editor
Wireless_802.1X
Set to 'Is not'
Duplicate
Edit
New
AND
OR
Close
Use

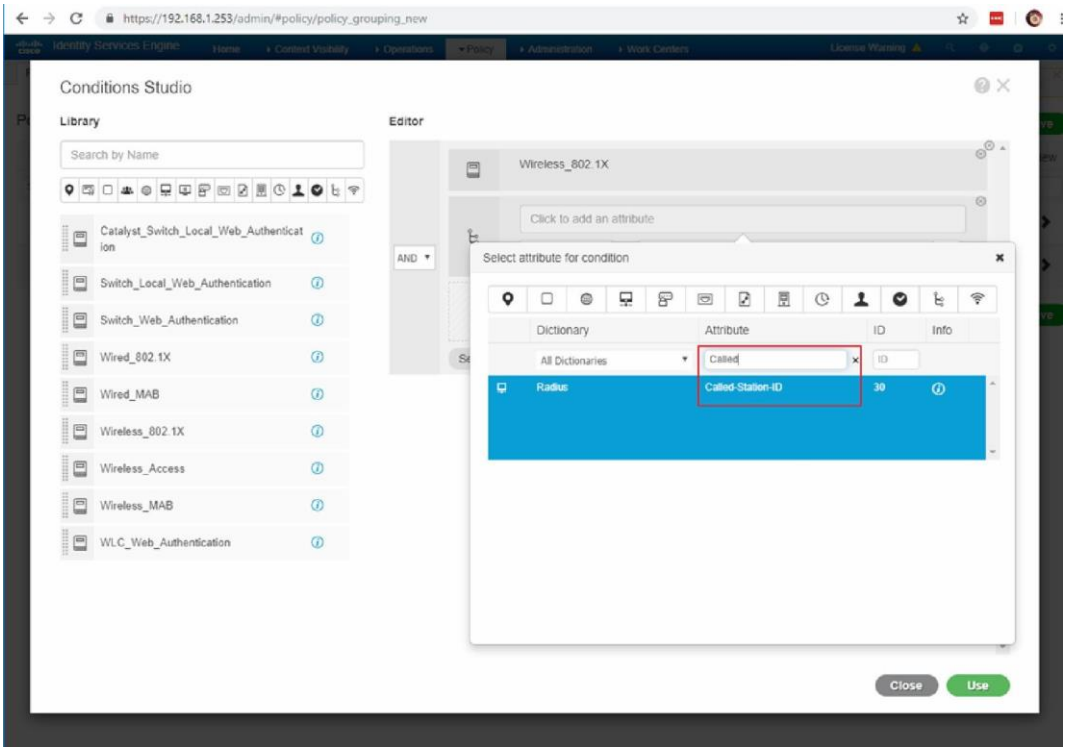
Click New


https://192.168.1.253/admin/#policy/policy_grouping_new
Conditions Studio
Library
Search by Name
Catalyst_Switch_Local_Web_Authentication
Switch_Local_Web_Authentication
Switch_Web_Authentication
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access
Wireless_MAB
WLC_Web_Authentication
Editor
Wireless_802.1X
Set to 'Is not'
Duplicate
Edit
New
AND
OR
Close
Use

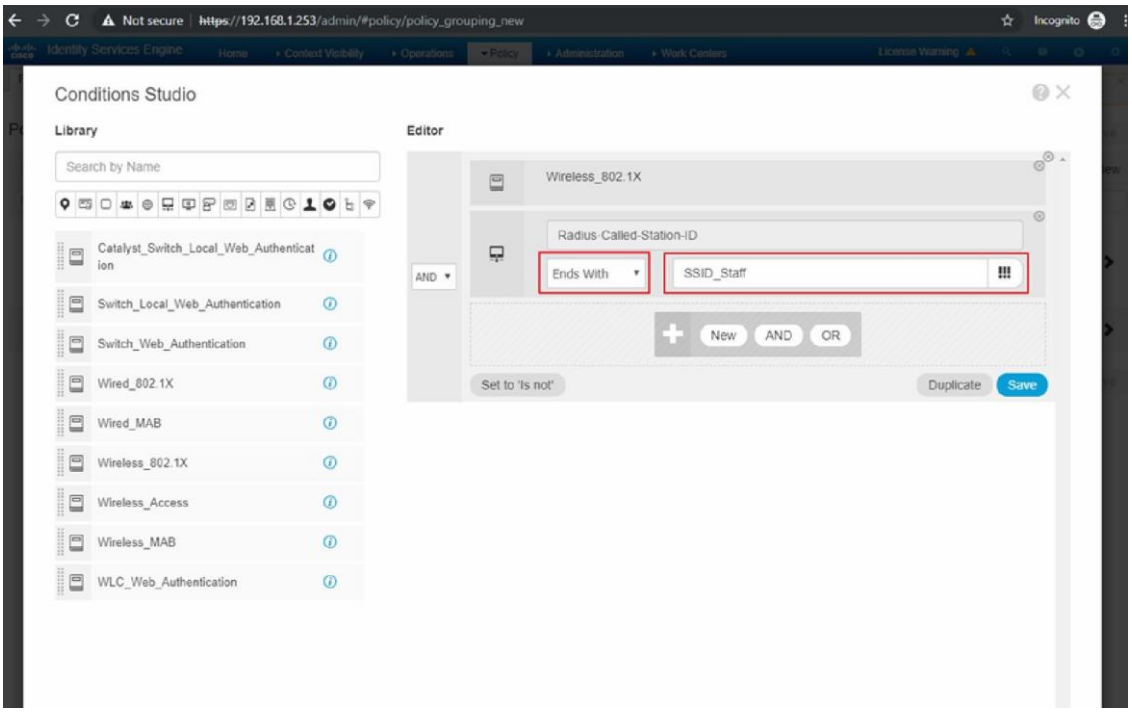
Click vào mục “Click to add an attribute”



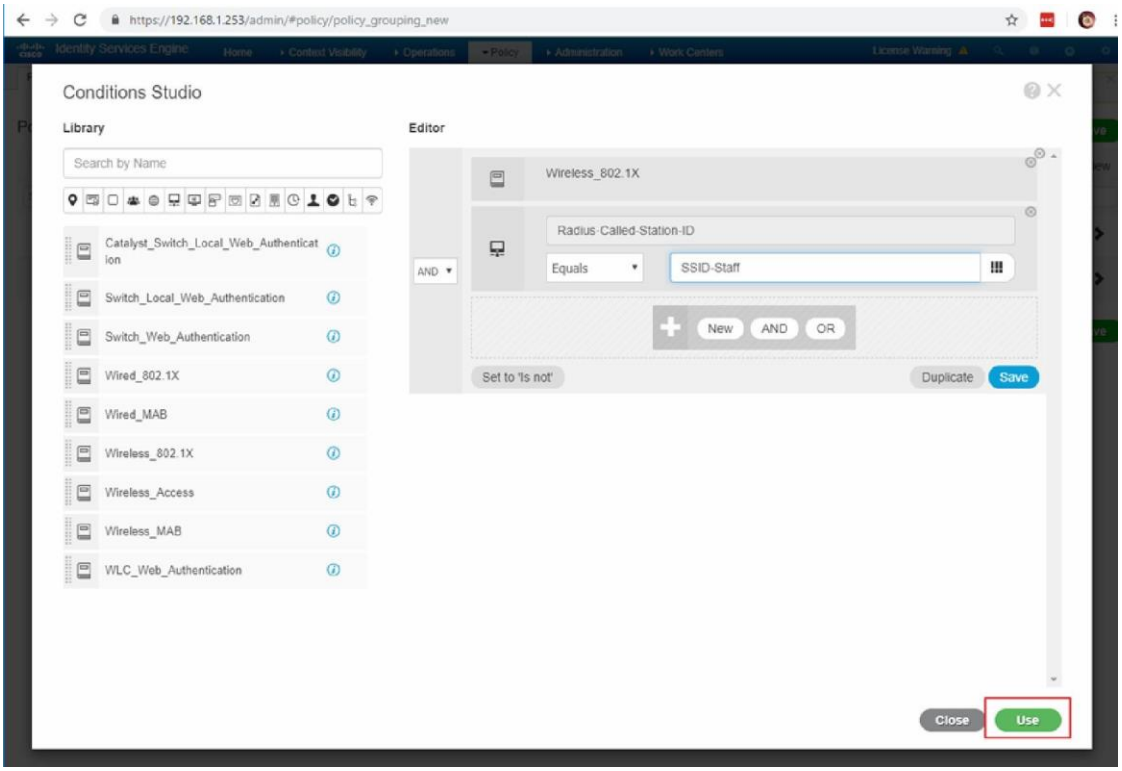
Chọn Attribute Called-Station-ID



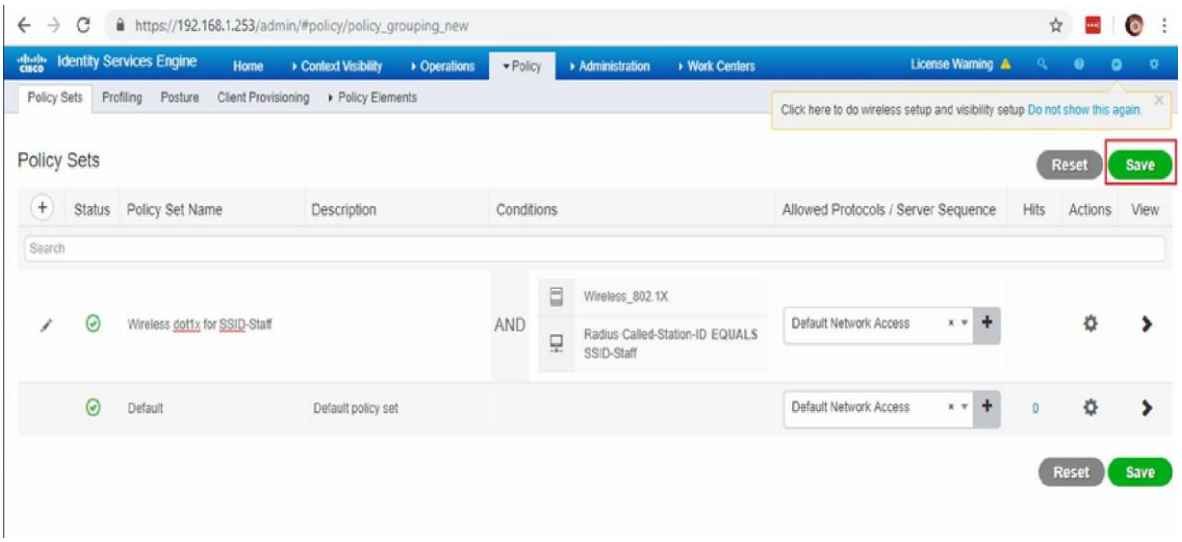
Chọn Value là ENDS_WITH SSID-Staff



Click Use

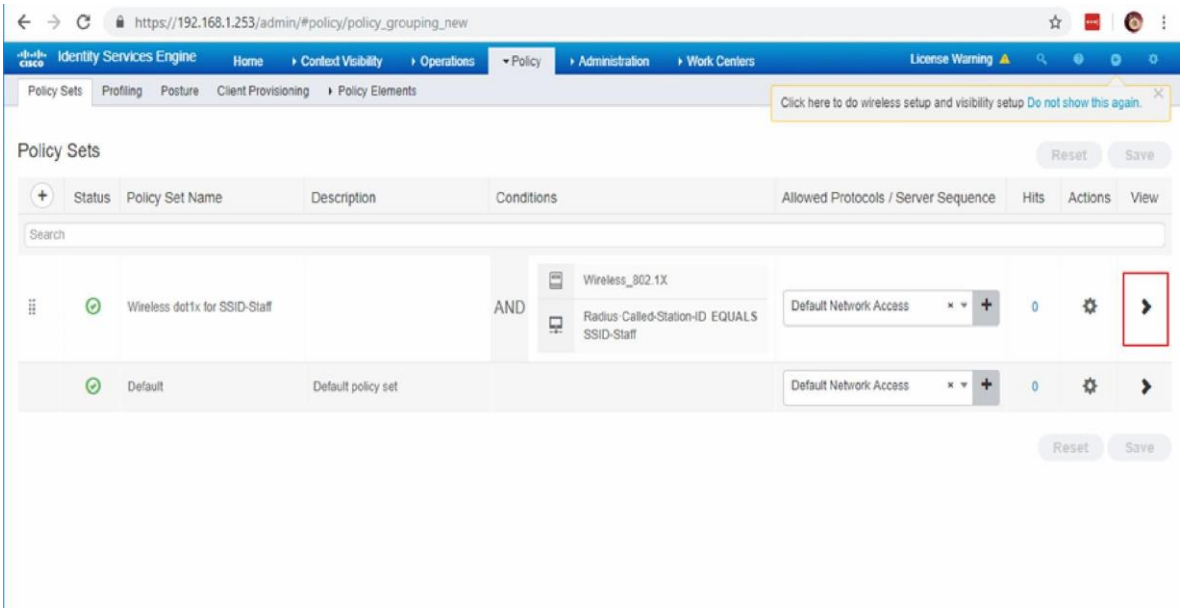


Click Save



4.6. Tạo Authentication Policy

Click vào icon “>” ở cuối Policy

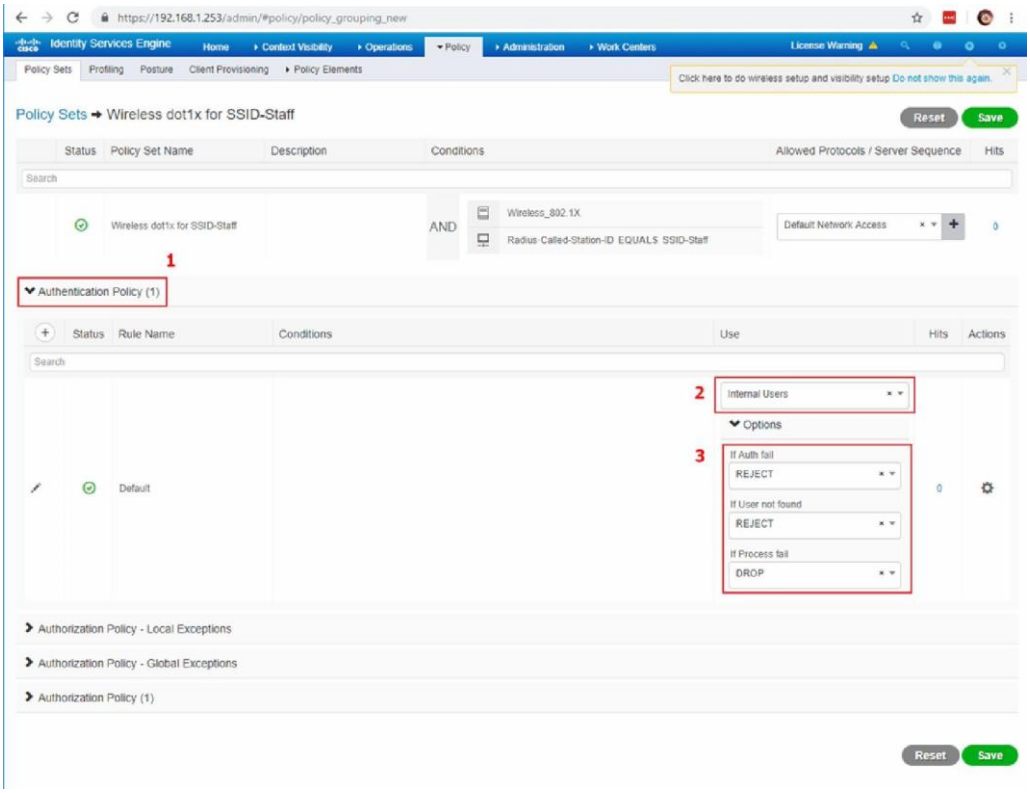


Trong phần Authenticaion Policy, chọn Internal Users. Trong phần Options:

If Auth fail: REJECT

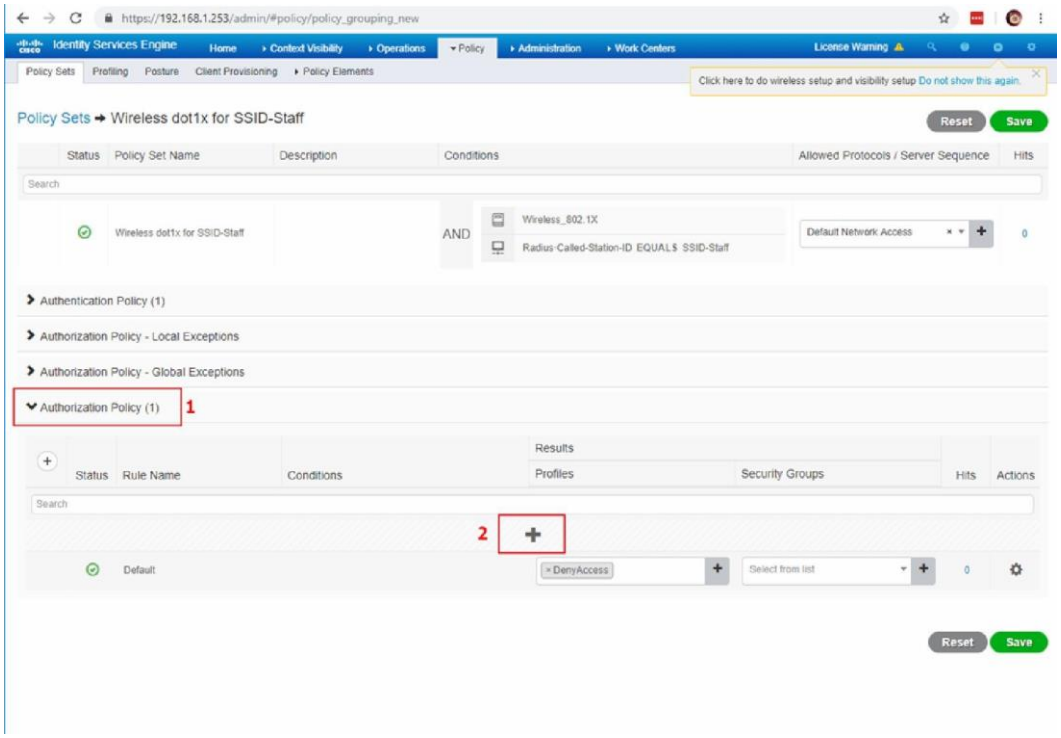
If User not fount: REJECT

If Process fail: DROP

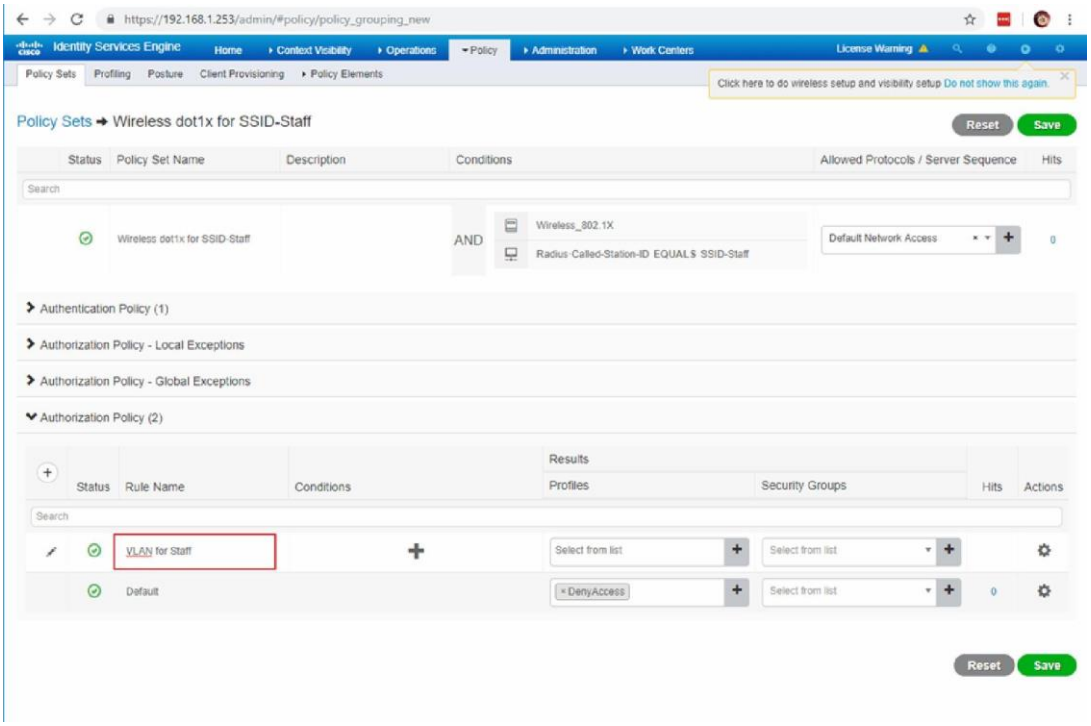


4.7. Tạo Authorization Policy cho User trong Group Staff và VIP

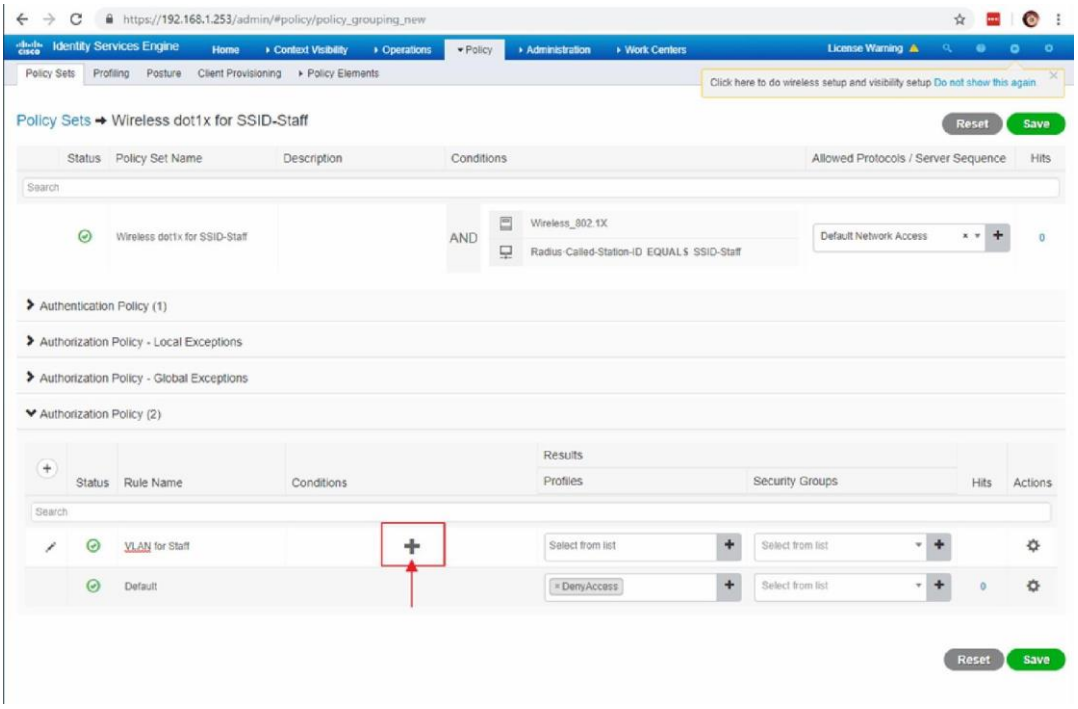
Trong phần Authorization Policy, click Add để thêm Rule



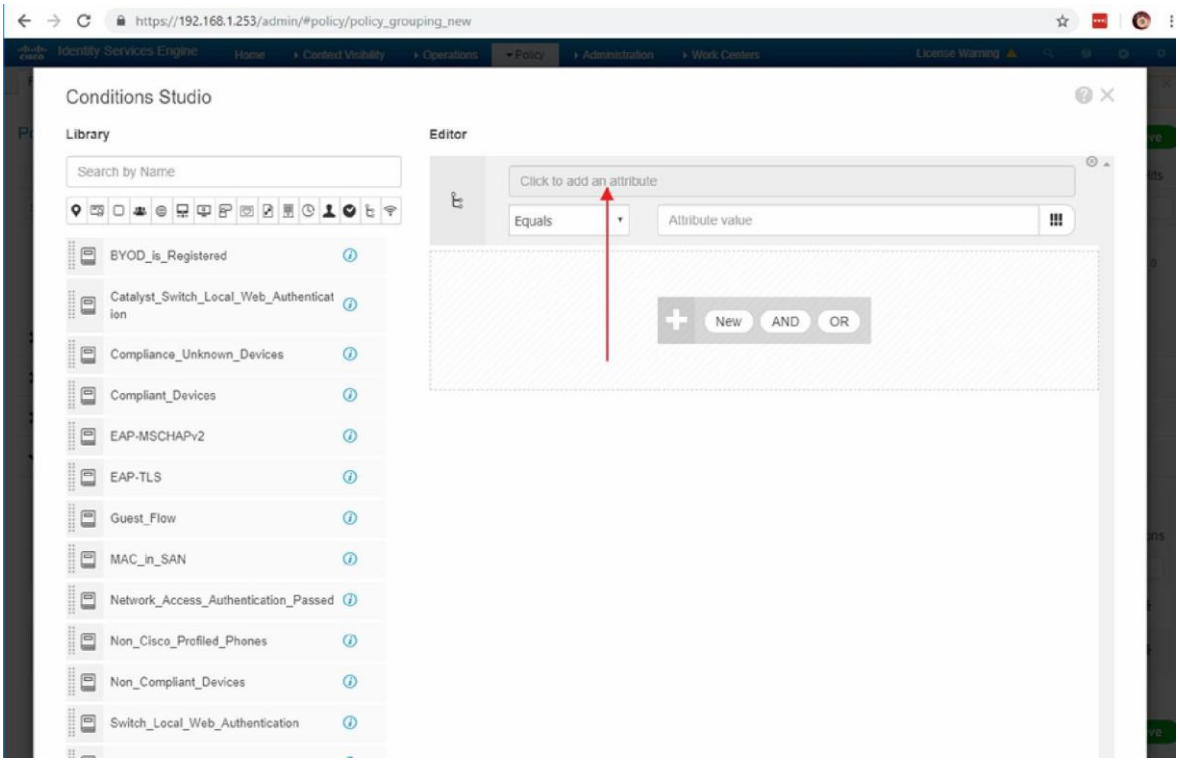
Đặt tên Rule là VLAN for Staff



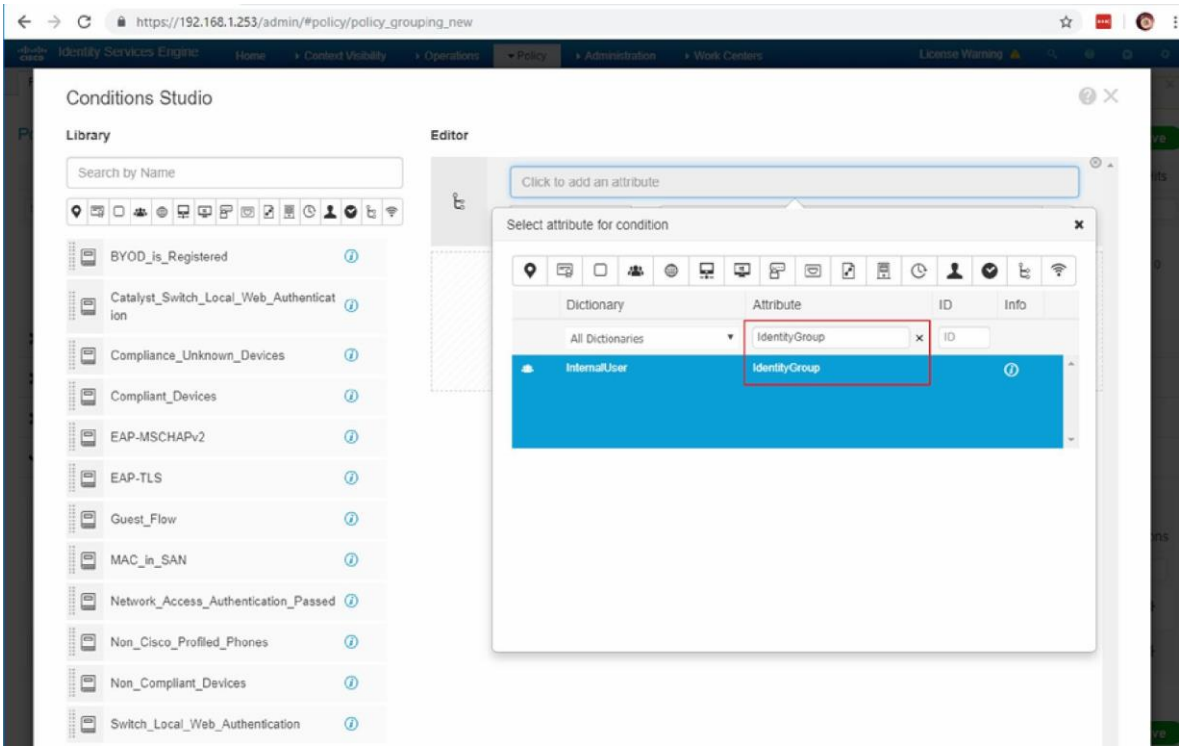
Ở phần Conditions, click Add



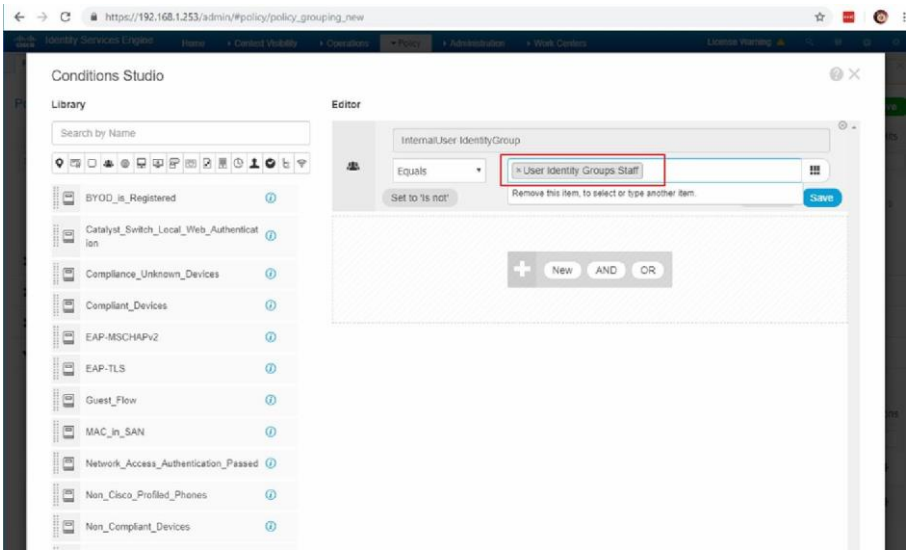
Click vào mục "click to add an attribute"



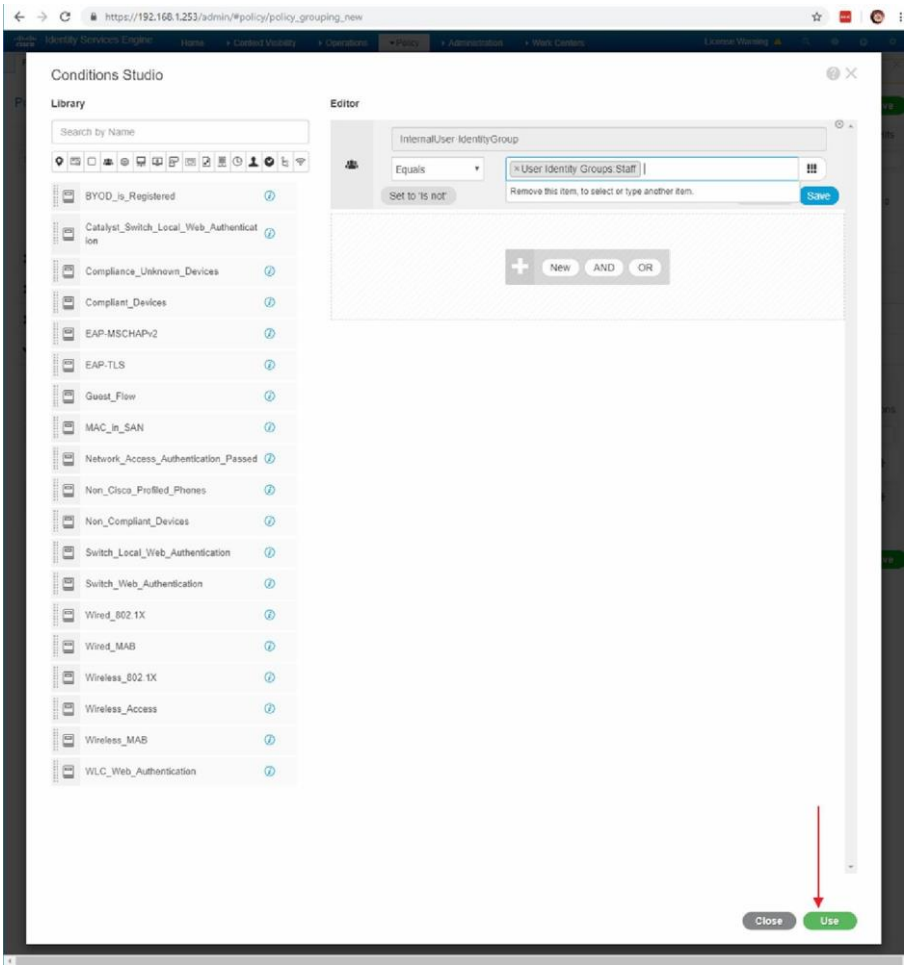
Chọn Attribute IdentityGroup



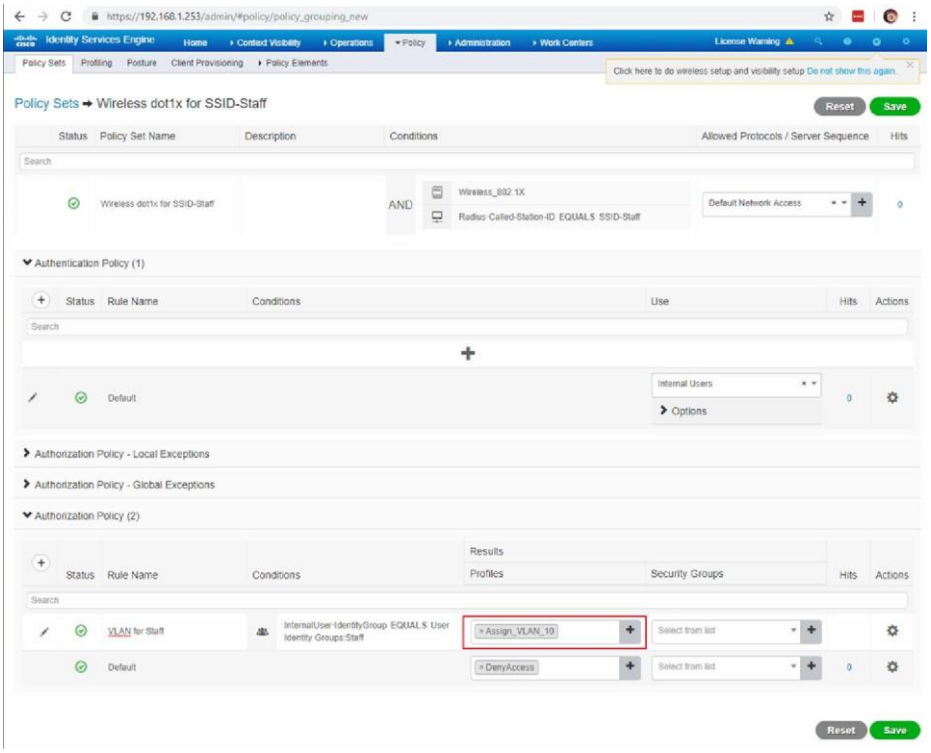
Ở phần value, chọn User Identity Groups: Staff



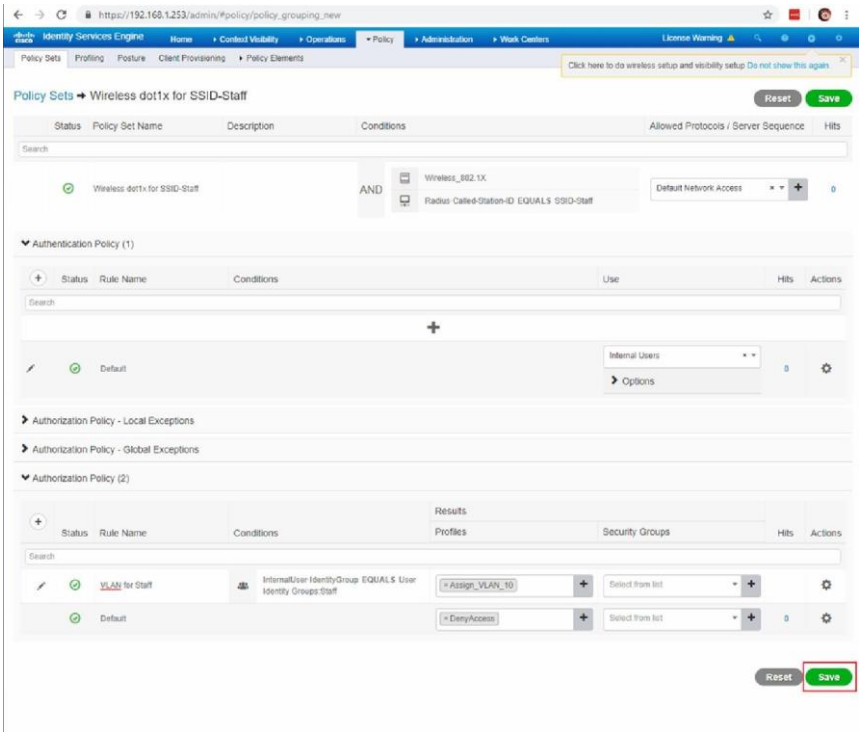
Click Use



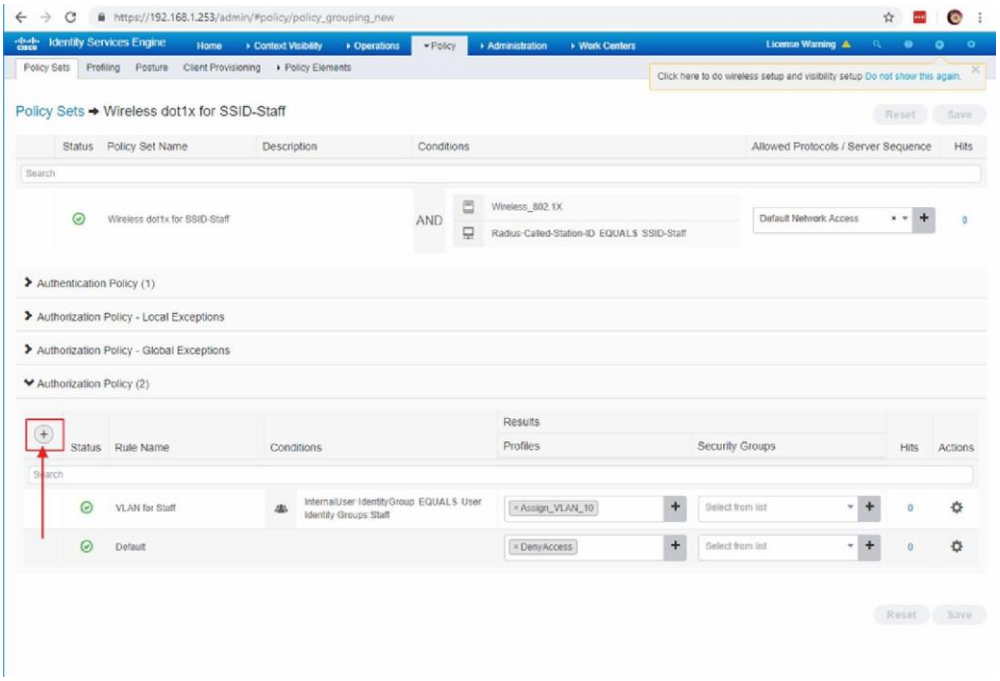
Trong phần Results → Profiles, chọn profile Assign_VLAN_10 đã tạo ở bước 4.4.



Click Save



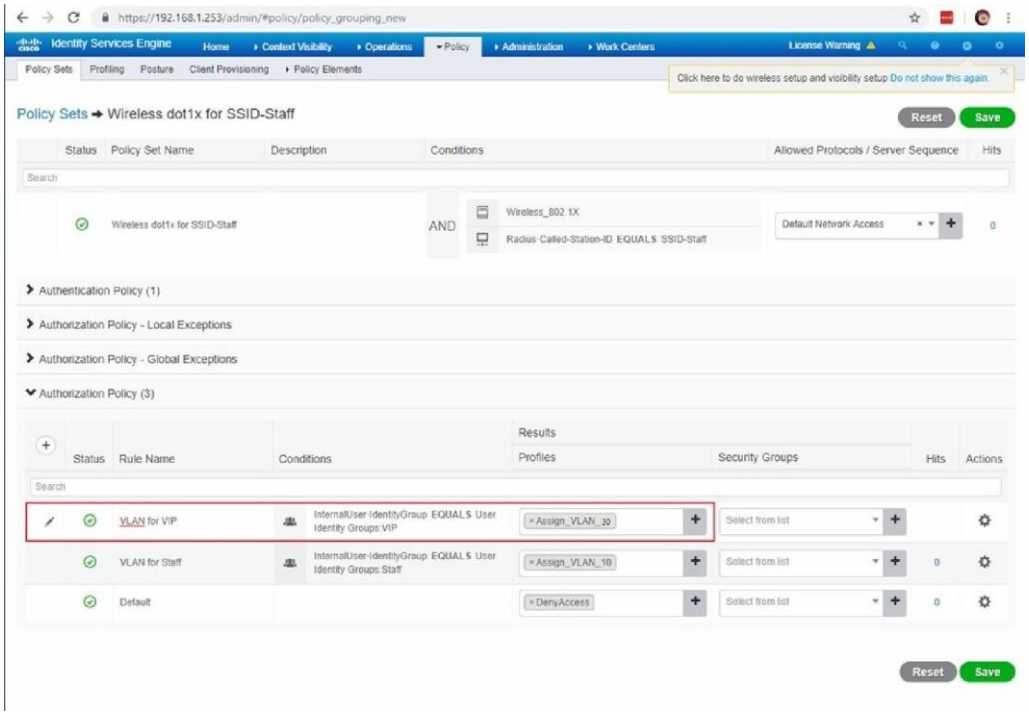
Click Add để tạo thêm Rule



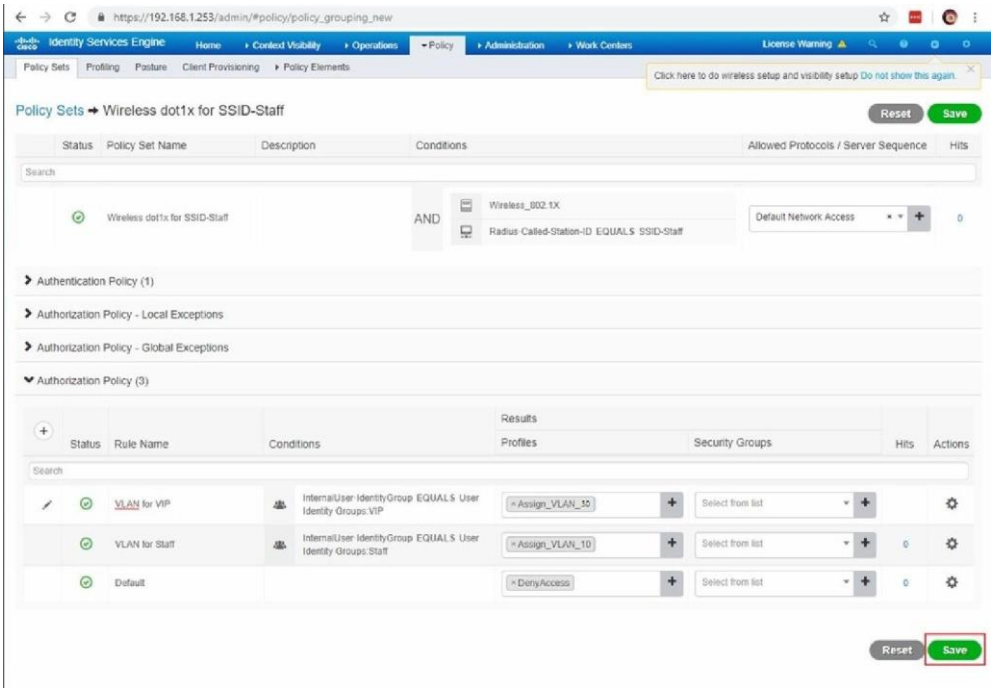
Tạo rule thứ hai với tên VLAN for VIP. Trong đó:

Conditions dùng IdentityGroup EQUALS User Identity Groups: VIP

Results → Profiles: Assign_VLAN_30

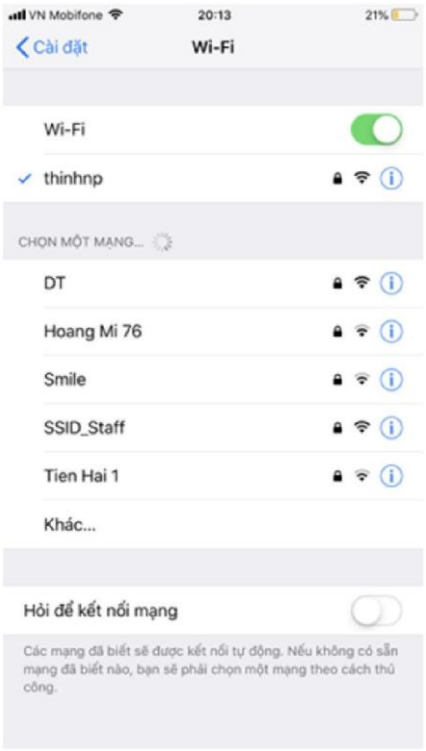


Click Save

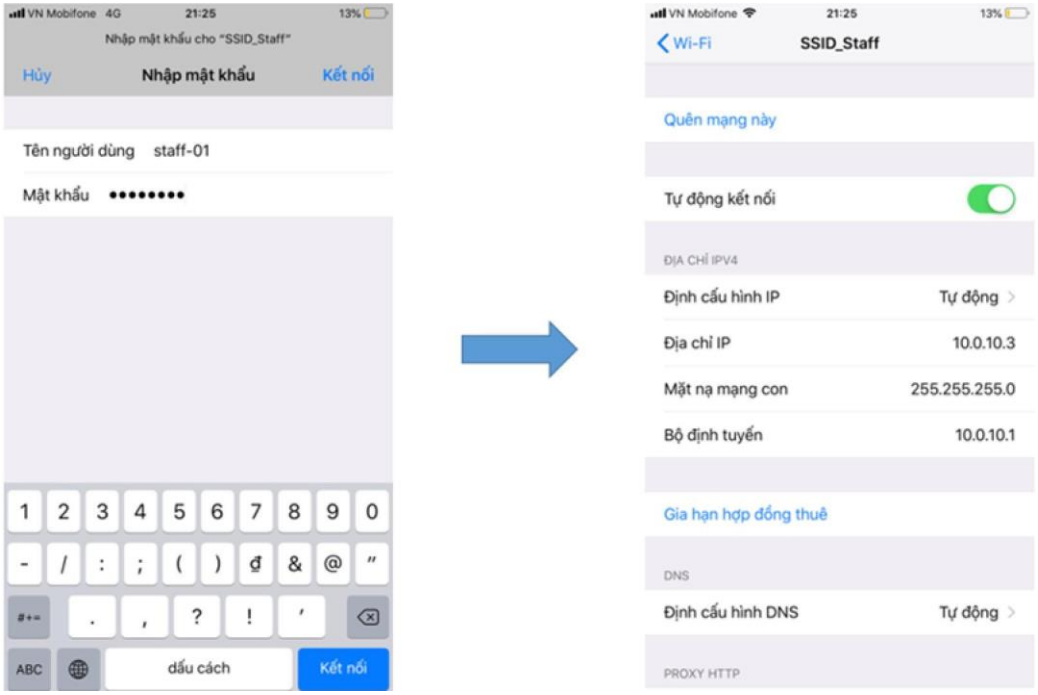


V. Kiểm tra

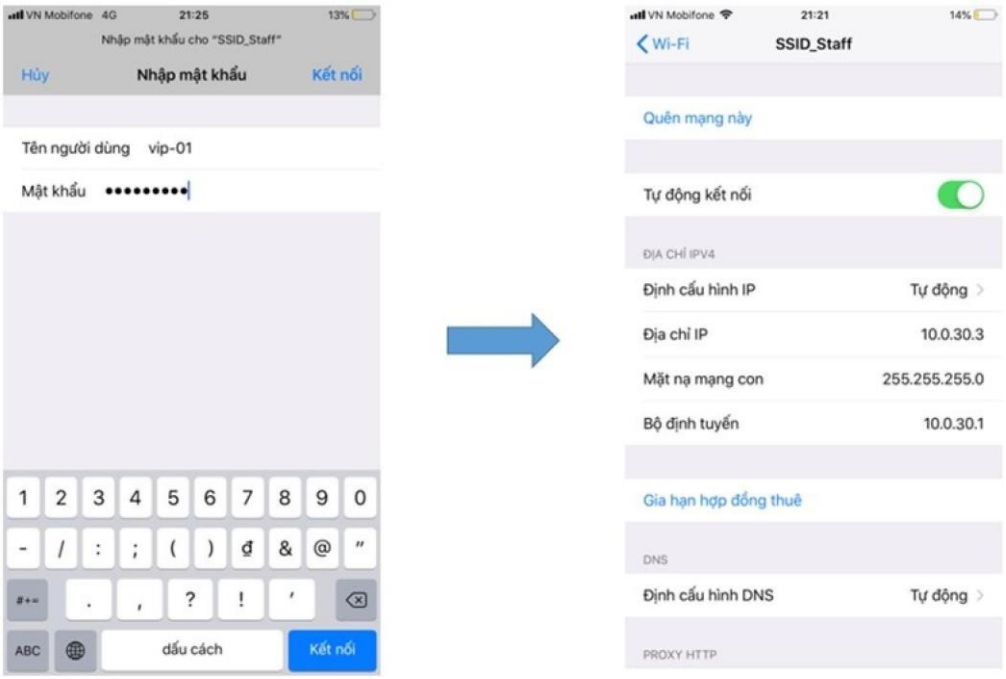
Sau khi cấu hình, AP đã có thể phát SSID_Staff



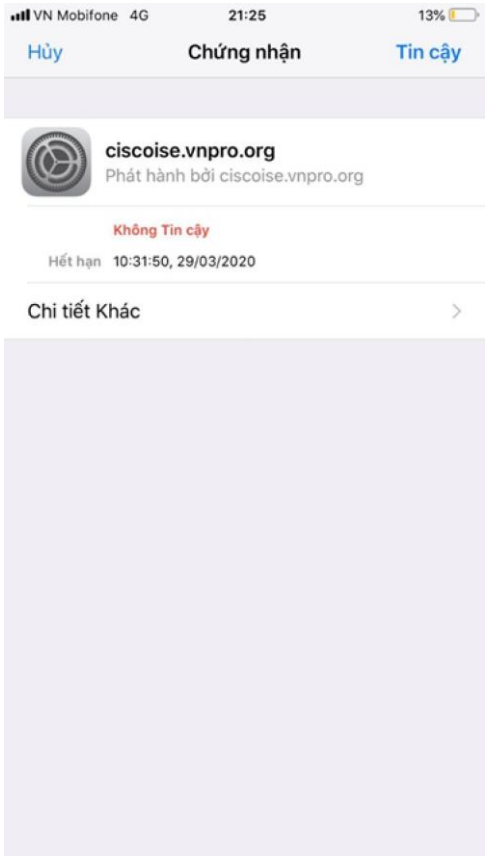
Kết nối vào với user staff-01, người dùng sẽ nhận được IP trong VLAN 10



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 Cậy


VN Mobifone 4G
21:25
13%
Hủy
Chứng nhận
Tin cậy
ciscoise.vnpro.org
Phát hành bởi ciscoise.vnpro.org
Không Tin cậy
Hết hạn 10:31:50, 29/03/2020
Chi tiết Khác