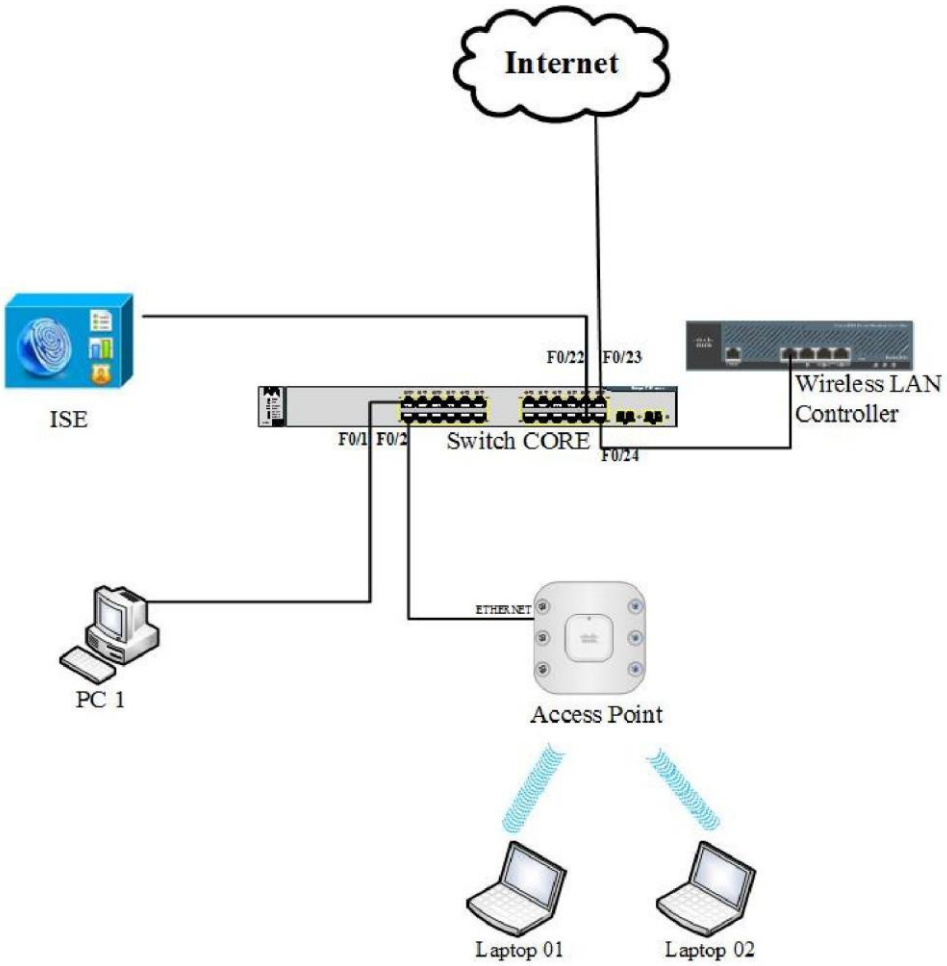
LAB : CẤU HÌNH WIFI GUEST VỚI CISCO ISE

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 thiết bị, Network 192.168.1.0/24

+ VLAN 10: VLAN cho SSID Staff, Network 10.0.10.0/24

+ VLAN 20: VLAN cho SSID Guest, Network 10.0.20.0/24

- 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 thuộc VLAN 1 và có thể được quản lý tập trung trên WLC

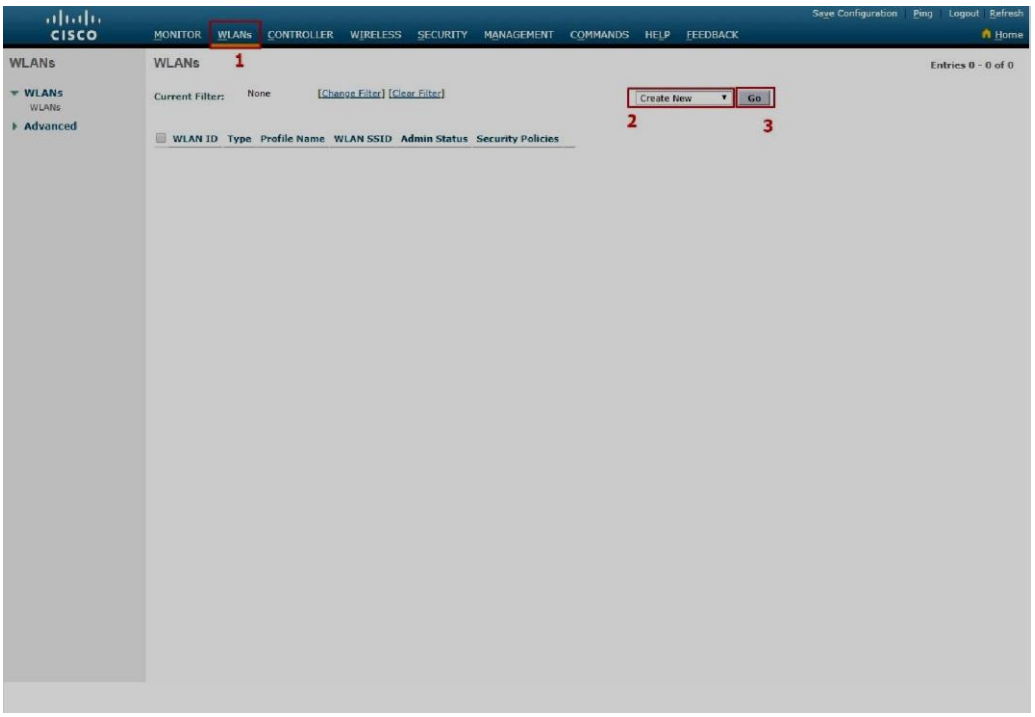
3. Cấu hình kết nối WLC với Cisco ISE

4. Cấu hình SSID Staff xác thực kiểu WPA2, cấp IP thuộc VLAN 10

5. Cấu SSID Guest, xác thực qua Web Portal trên Cisco ISE, cấp IP thuộc VLAN 20

IV. Cấu hình

Yêu cầu 1, 2: tham khảo bài LAB 3: Cấu hình Cisco WLC 2504



Lưu ý: Tạo đủ 3 Interface cho 3 VLAN 1, 10 và 20

Yêu cầu 3: Cấu hình kết nối Cisco WLC với Cisco ISE

Tham khảo bài LAB 6: Xác thực radius 802.1x với Cisco ISE

Yêu cầu 4: Tạo SSID xác thực bằng WPA2

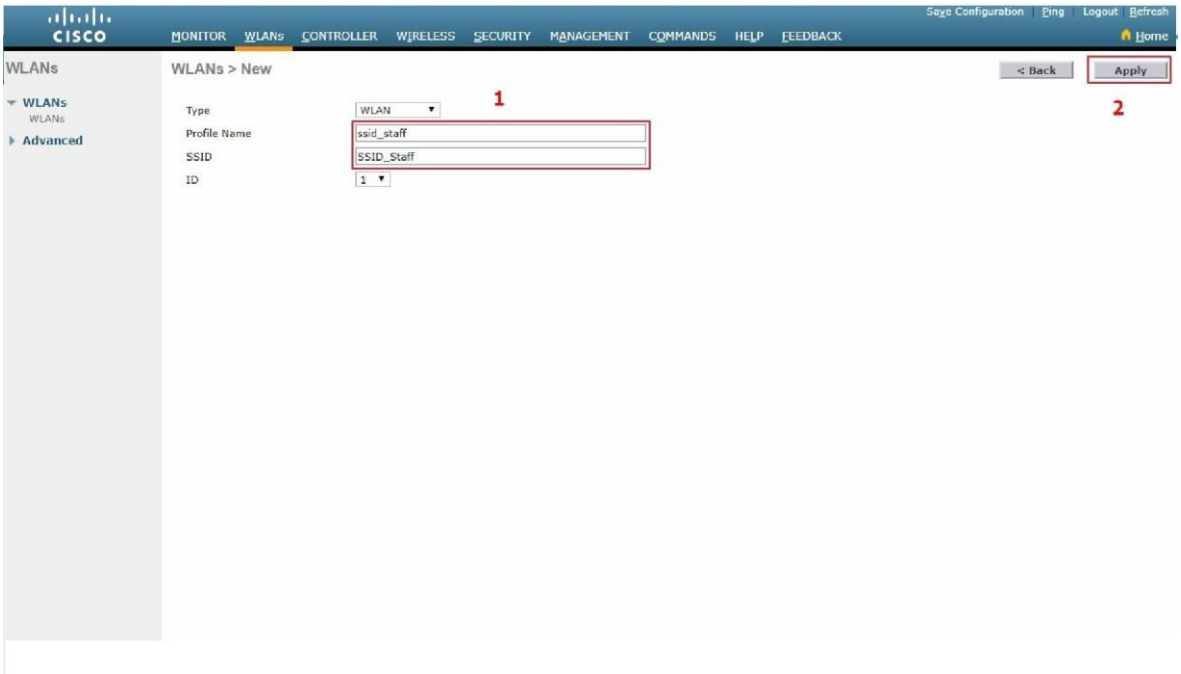
Truy cập vào WLC → Vào menu WLANs → Chọn Create New. Click Go

Đặt Profile name và SSID:

Profile Name: ssid_staff

SSID: SSID_Staff

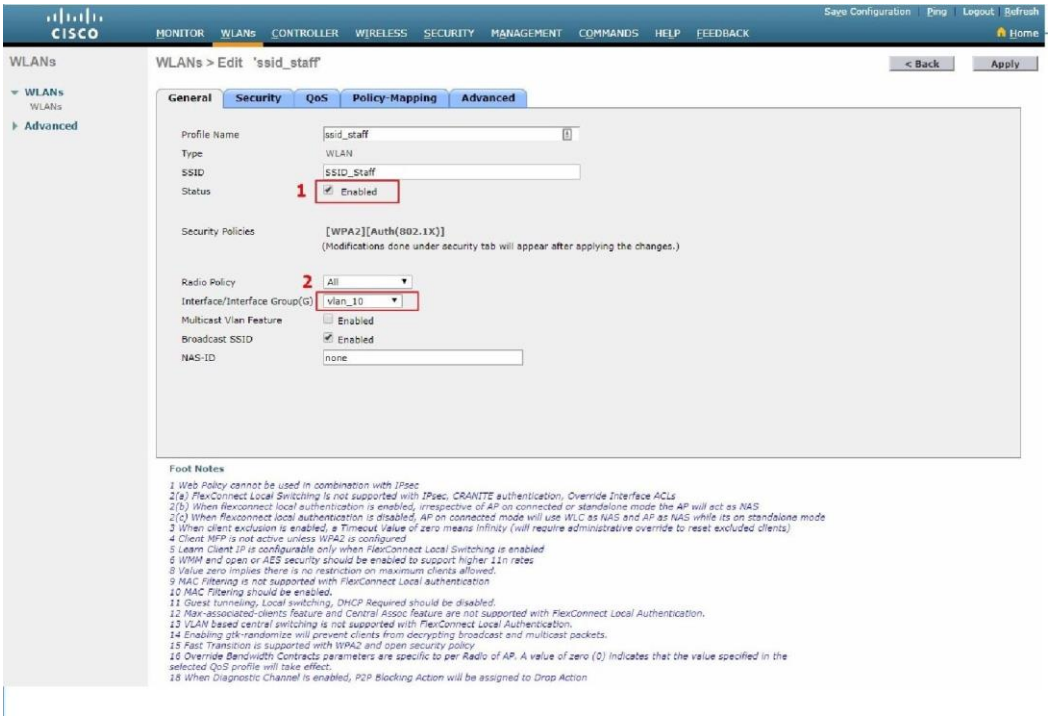
Click Apply



Trong tab General:

Tick chọn Status: Enabled

Interface/Interface Group (G): vlan_10

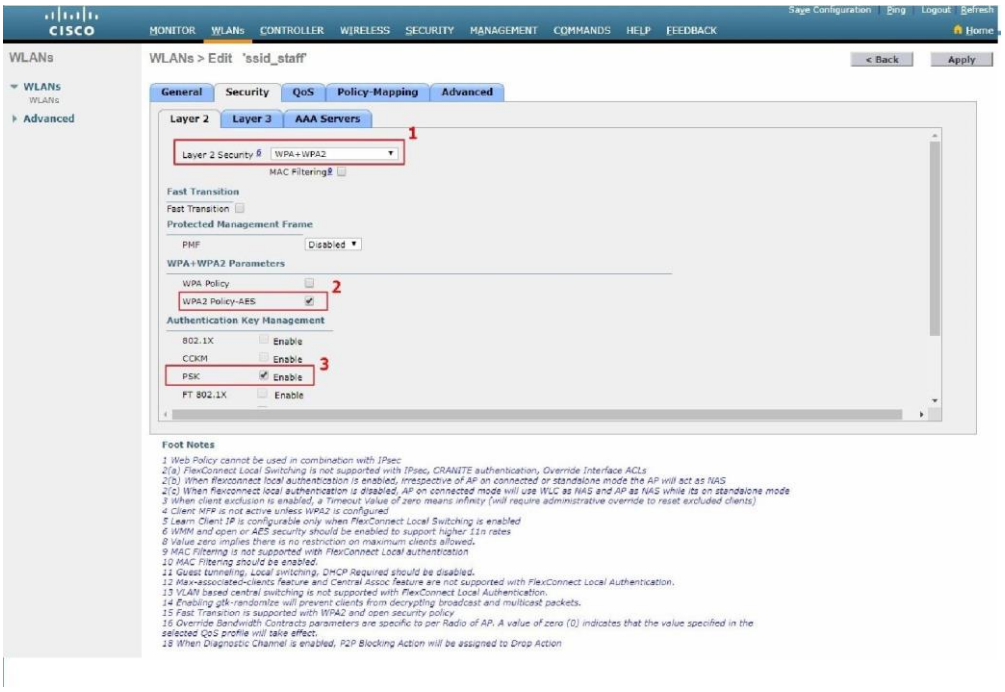


Trong Security → Layer 2:

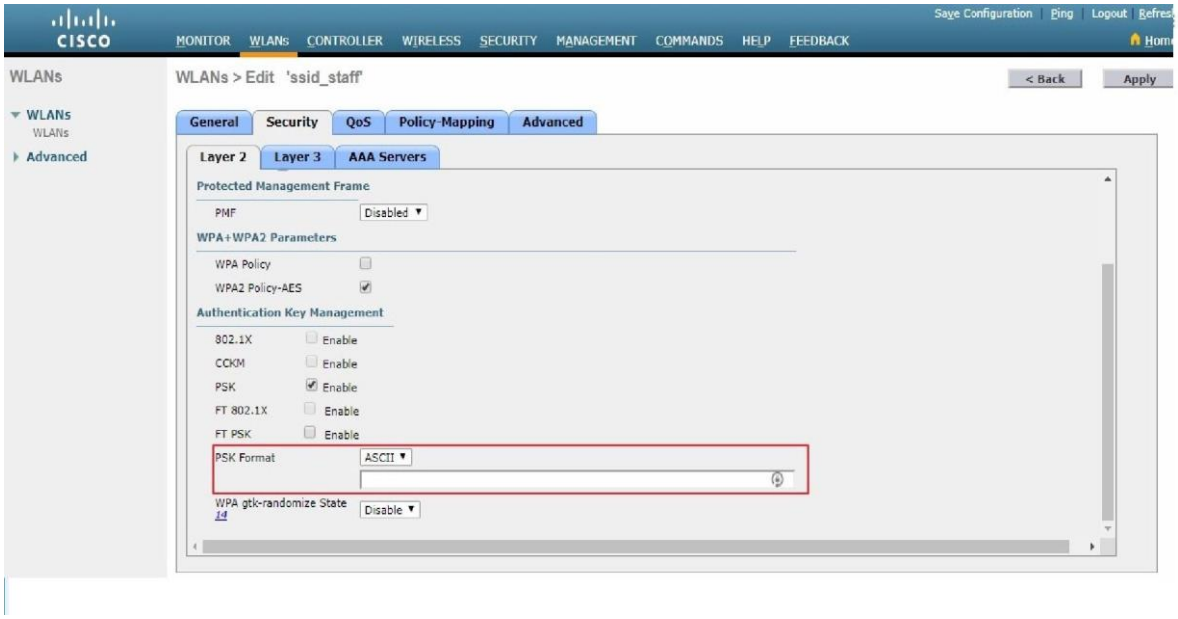
Layer 2 Security: WPA + WPA2

WPA + WPA2 Parameters: tích chọn WPA2 Policy-AES

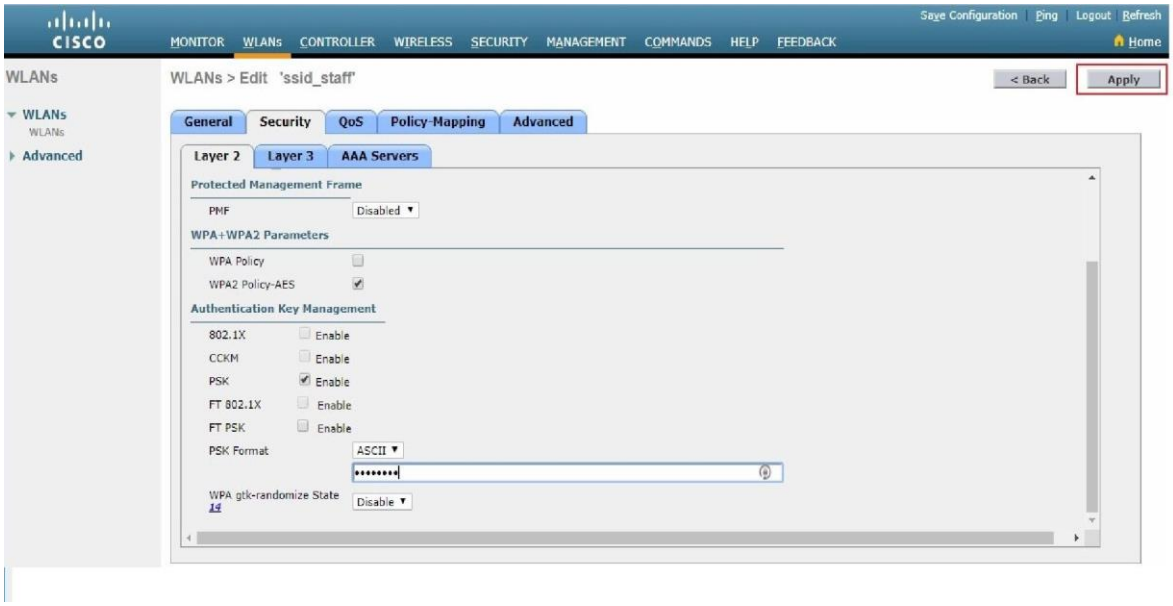
Authentication Key Management: tích chọn PSK



Kéo xuống, chọn PSK Format là ASCII và đặt mật khẩu: (bài lab này đặt mật khẩu là vnpro123)



Click Apply



Yêu cầu 5: Cấu hình SSID Guest, xác thực qua Web Portal trên Cisco ISE

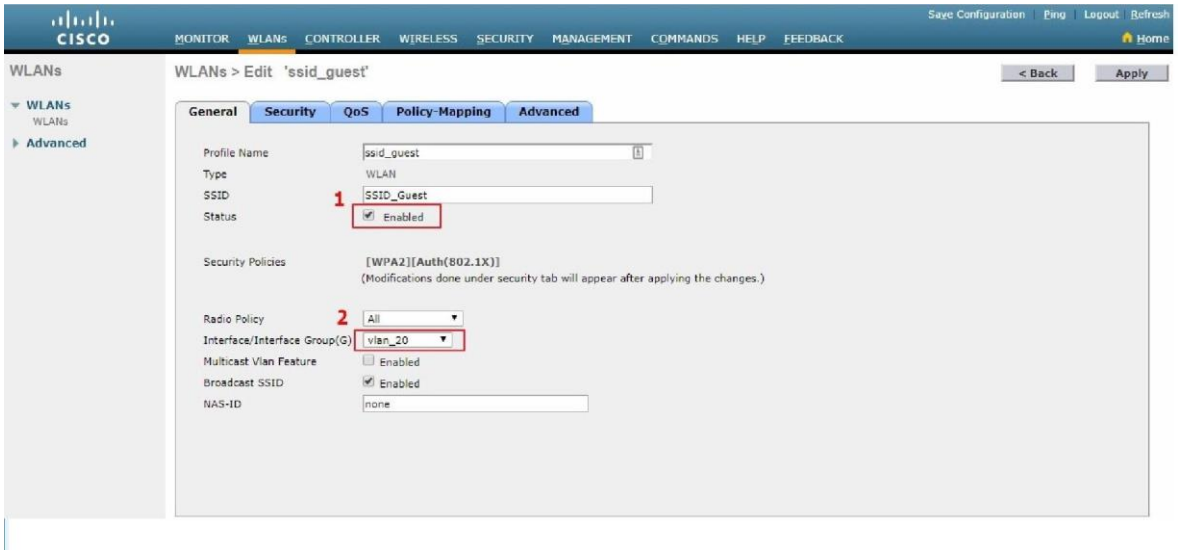
5.1. Tạo SSID

Truy cập vào WLC

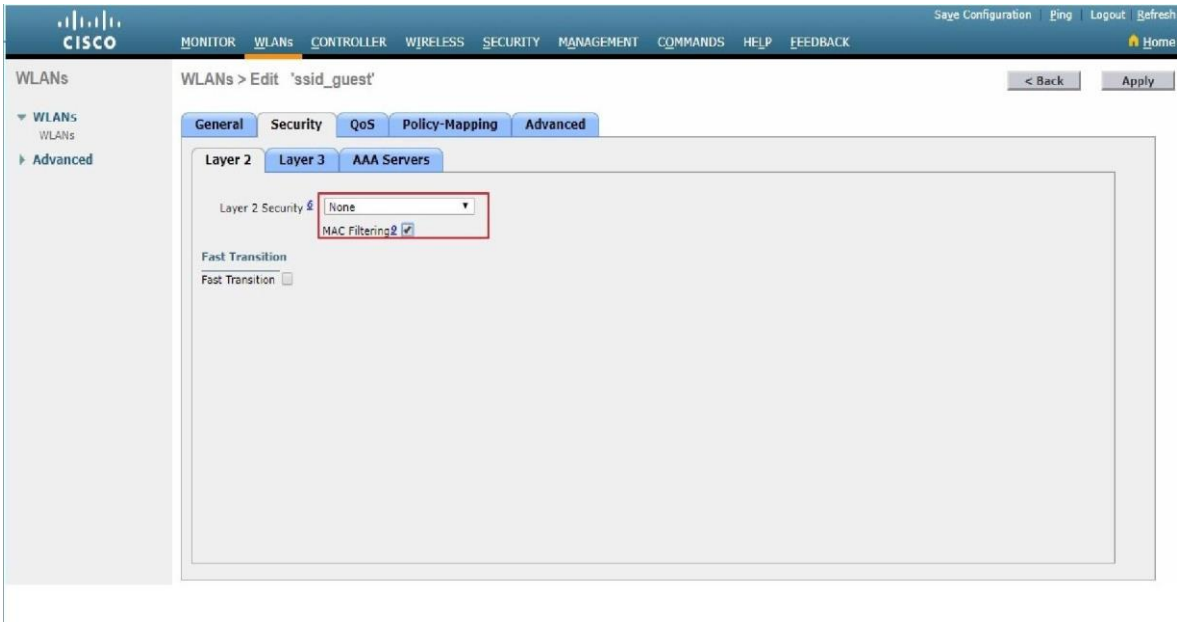
Vào menu WLANs → Chọn Create New. Click Go

Đặt Profile name và SSID:
Profile Name: ssid_guest
SSID: SSID_Guest
Click Apply

Trong tab General:
Tick chọn Status: Enabled
Interface/Interface Group (G): vlan_20



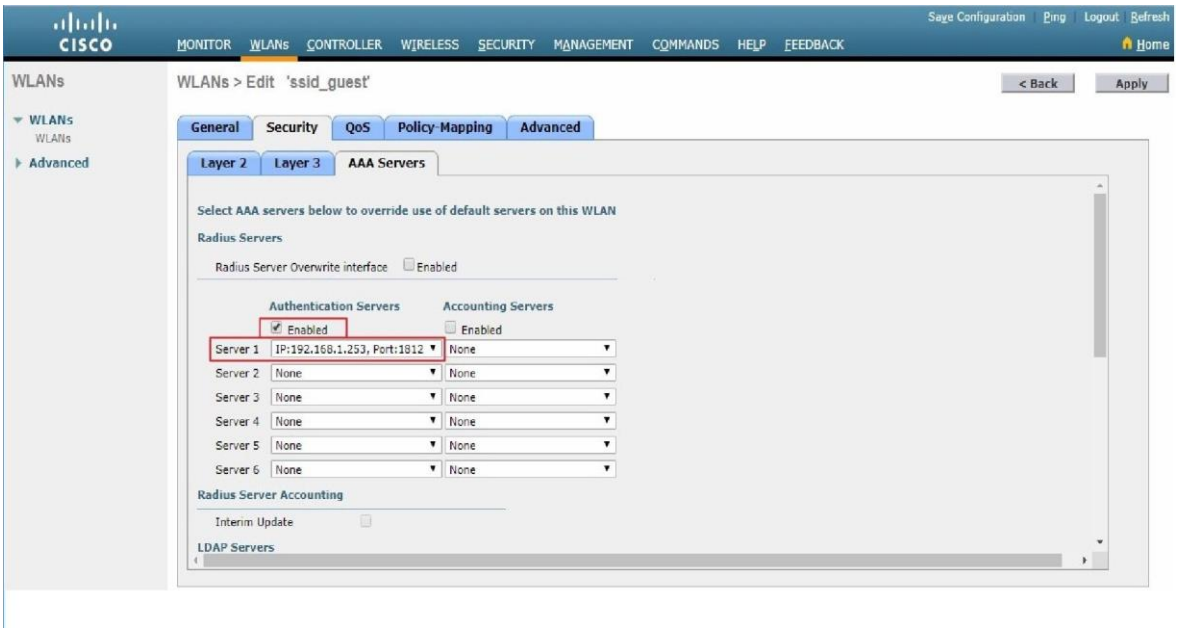
Trong Security → Layer 2:
Layer 2 Security: None
Tích chọn Mac Filtering



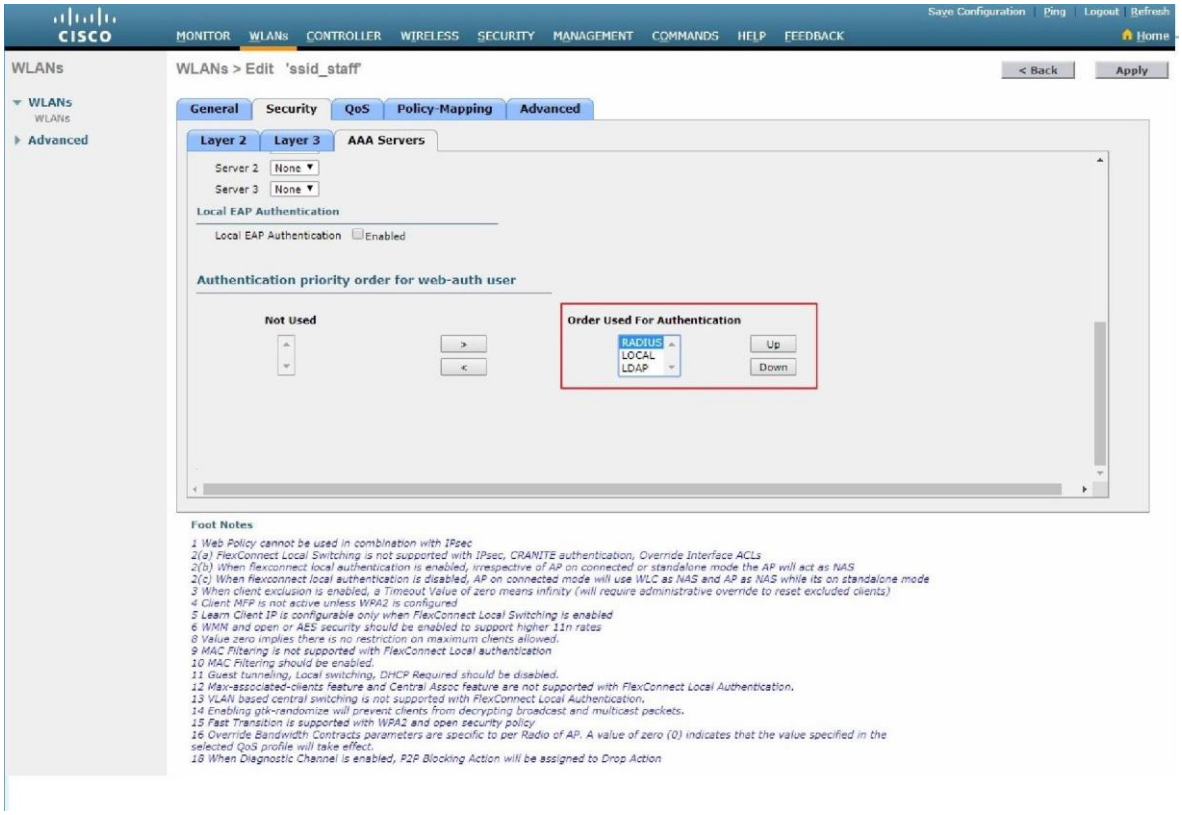
Trong tab Security → AAA Servers:

Tích chọn Enabled ở Authentication Servers

Chọn Server 1 là Cisco ISE đã thêm ở bước 2



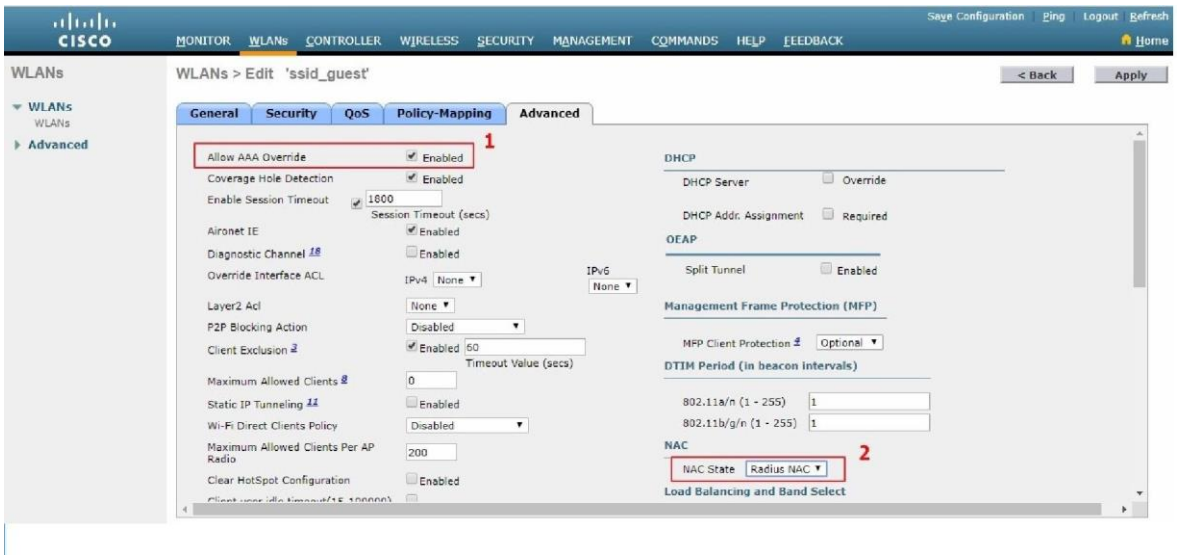
Kéo xuống, trong phần Order Used for Authentication, click chọn RADIUS và click UP để phương thức xác thực RADIUS nằm đầu tiên



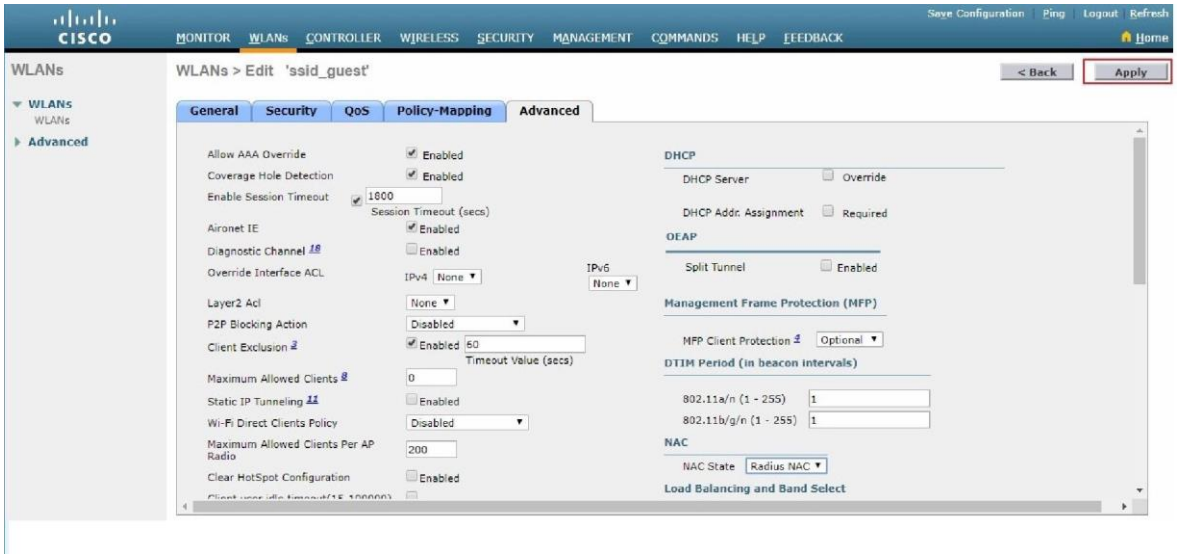
Trong tab Advanced:

Tích chọn Allow AAA Override

NAC State là RADIUS NAC



Click Apply

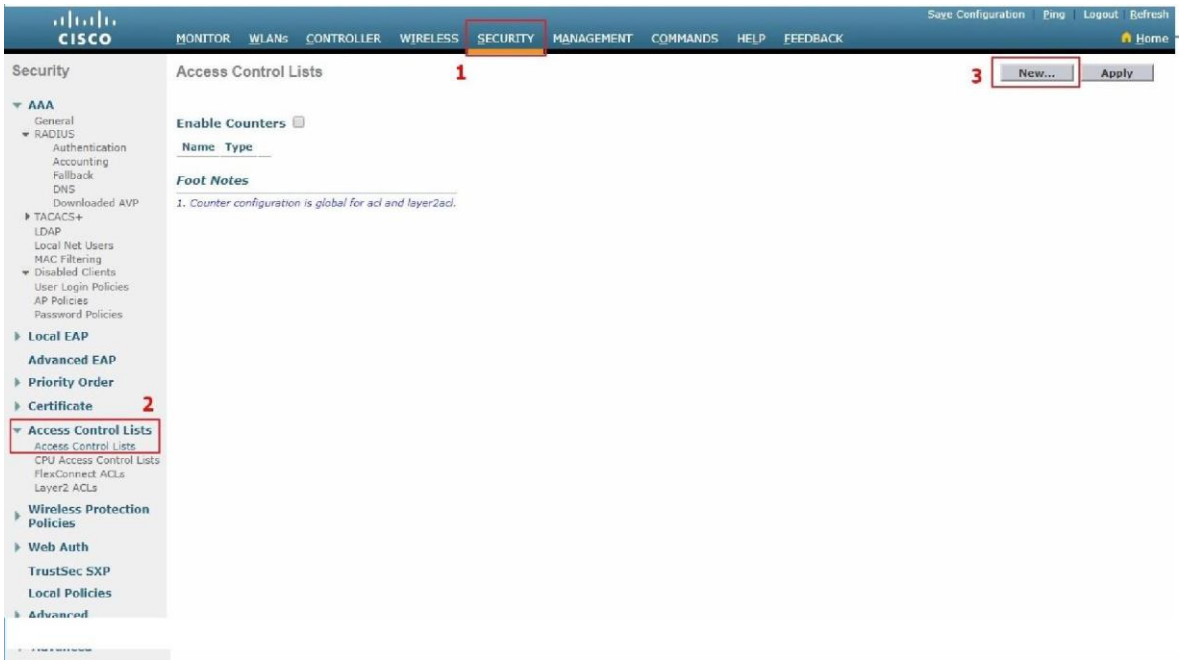


5.2. Cấu hình Access List để redirect người dùng

Khi người dùng chưa xác thực xong, AP sẽ chặn không cho dữ liệu người dùng đi qua, trong đó có dữ liệu trao đổi giữa người dùng và ISE để hiển thị trang chào. Do đó, phải viết ACL permit những dữ liệu này.

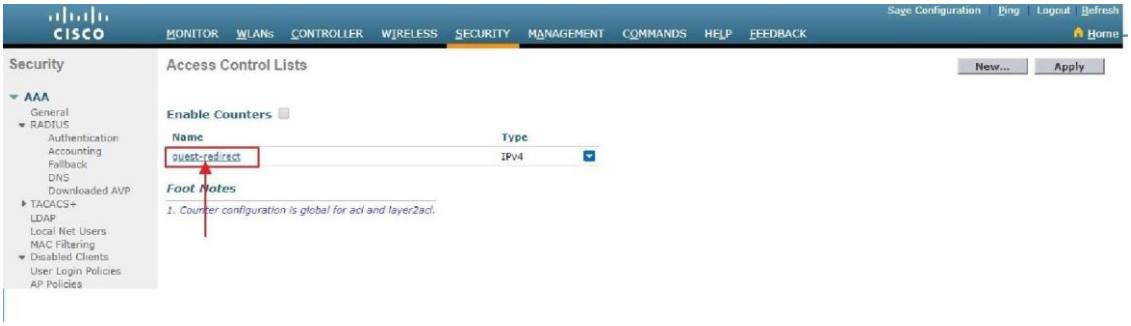
Trên WLC, vào tab SECURITY → Access Control Lists → Access Control Lists

Click New

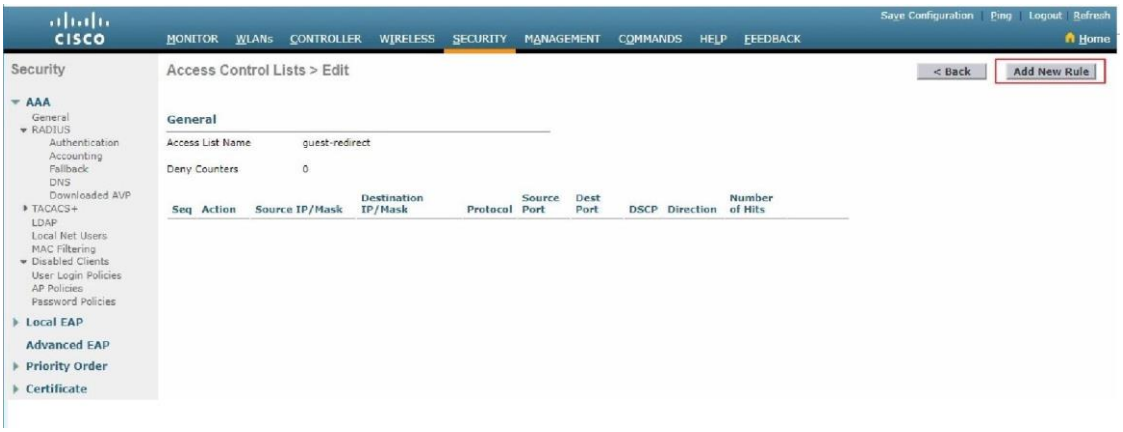


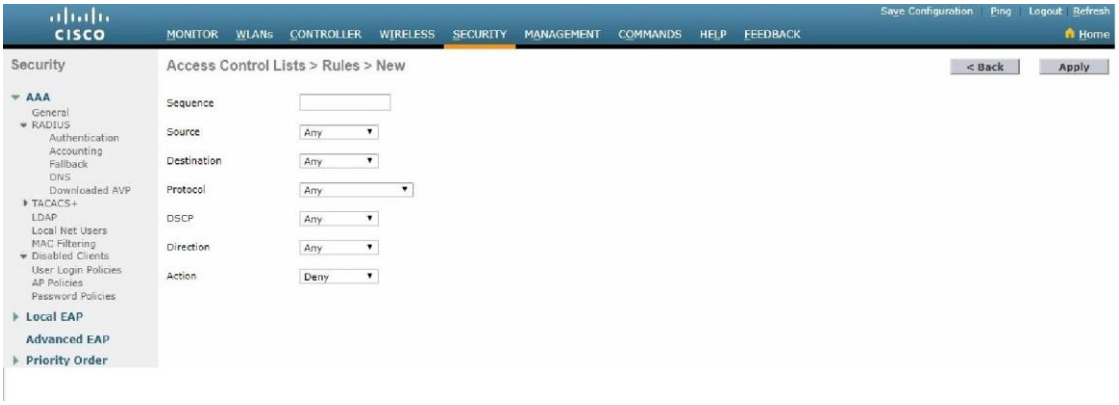
Đặt tên cho ACL (bài lab này đặt tên cho ACL là guest-redirect) sau đó click Apply

Click vào tên của ACL vừa tạo để chỉnh sửa



Để thêm rule cho ACL, click vào Add New Rule. Sau đó nhập các tham số và click Apply

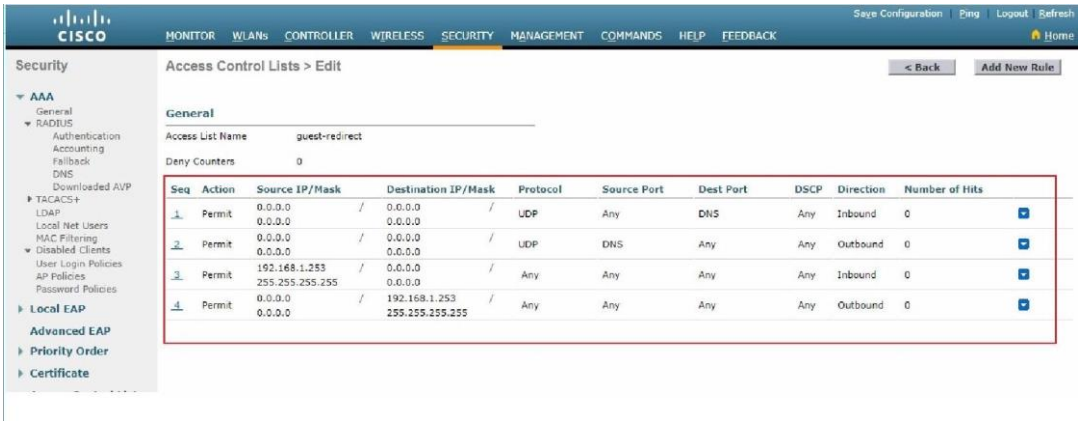




5.3. Tạo các rule

Cho phép DNS đi vào/ra access point

Cho phép traffic từ/đến ISE



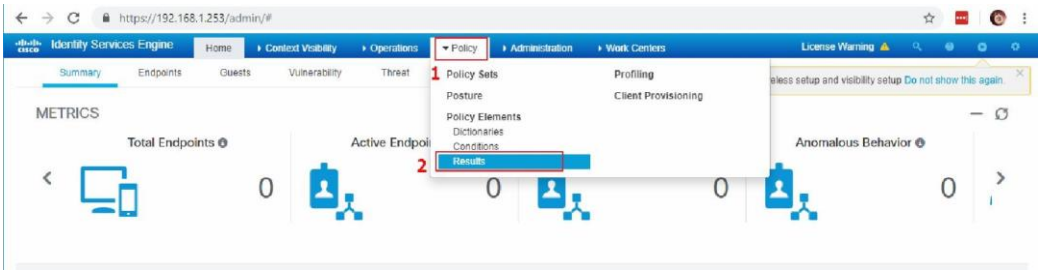
5.4. Cấu hình Cisco ISE

Thêm WLC vào Cisco ISE

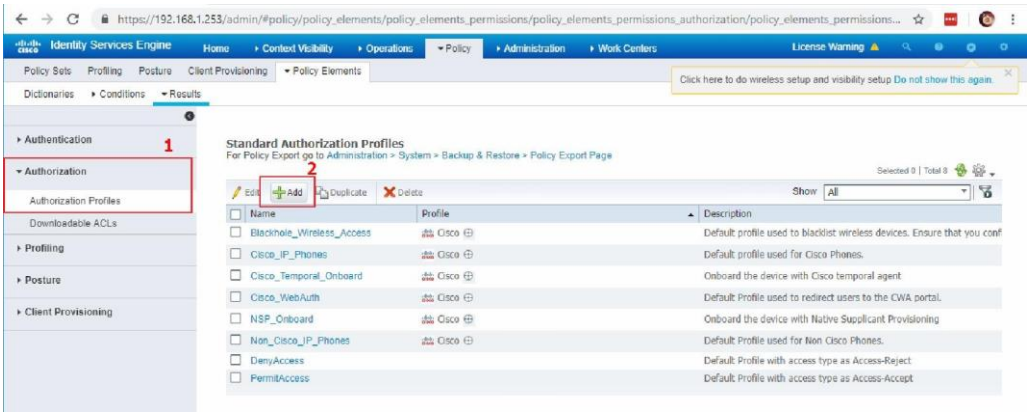
Tham khảo bài Lab 6:Xác thực radius 802.1x với Cisco ISE

5.5. Tạo Result

Vào menu Policy → Results



Vào mục Authorization → Authorization Profiles. Click Add



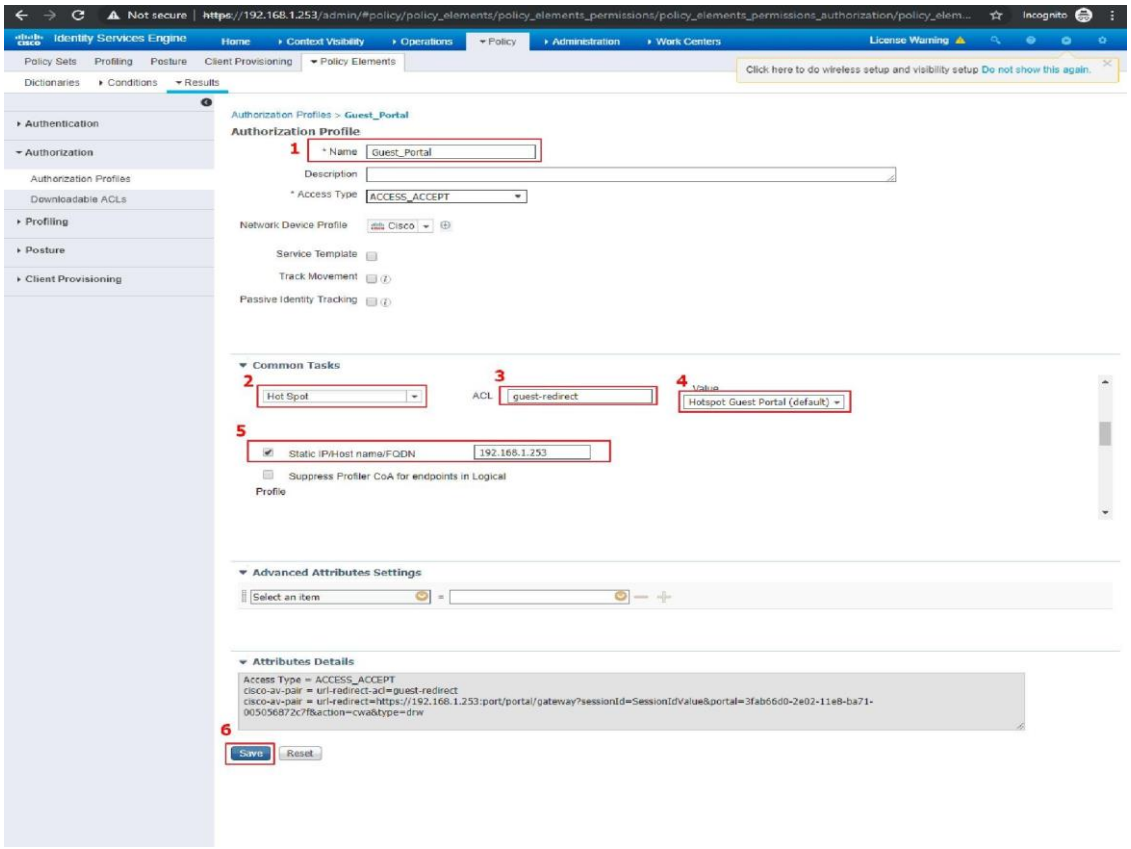
Đặt tên cho Profile: Guest_Portal

Trong phần Common Tasks, tích chọn Web Redirection

Chọn kịch bản là Hot Spot, ACL là tên ACL đã tạo ở bước 5, Value là Hot Spot Guest Portal (default)

Tích chọn Static IP/Hostname/FQDN và nhập IP của Cisco ISE vào

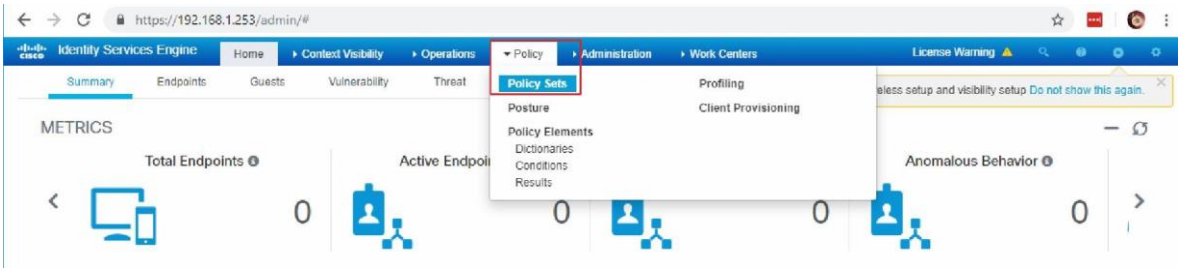
Click Submit



5.6. Cấu hình Policy

Tạo Policy

Vào menu Policy → Policy Set

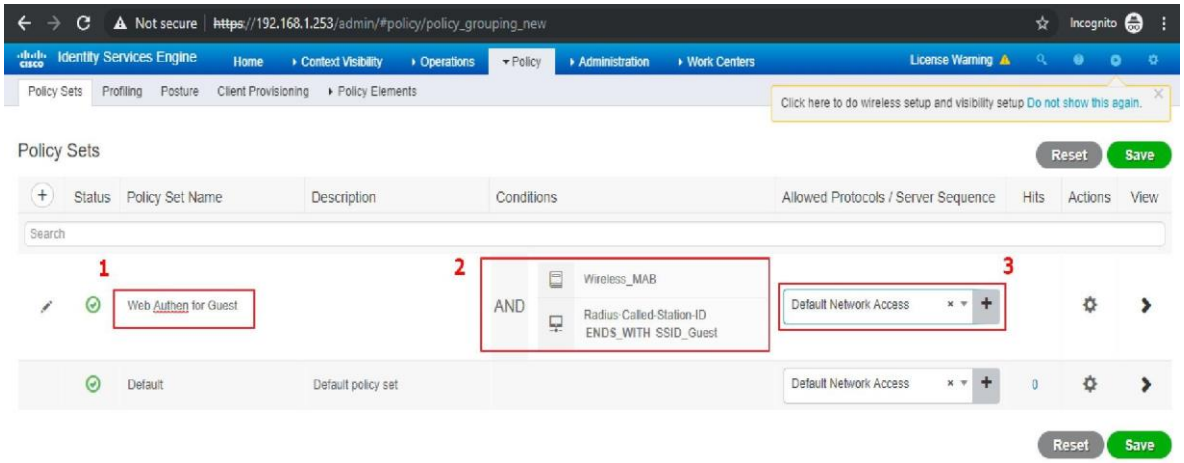


Tạo Policy như sau:

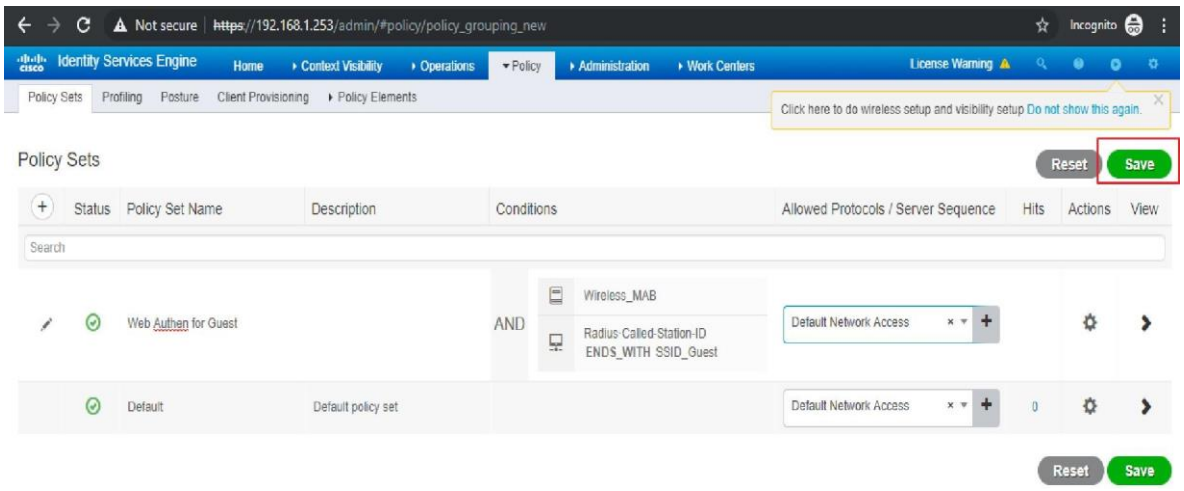
Tên: Web Authen for Guest

Conditions: Wireless_MAB AND Radius: Called-Station-ID ENDS_WITH SSID_Guest

Allowed Protocols: Default Network Access



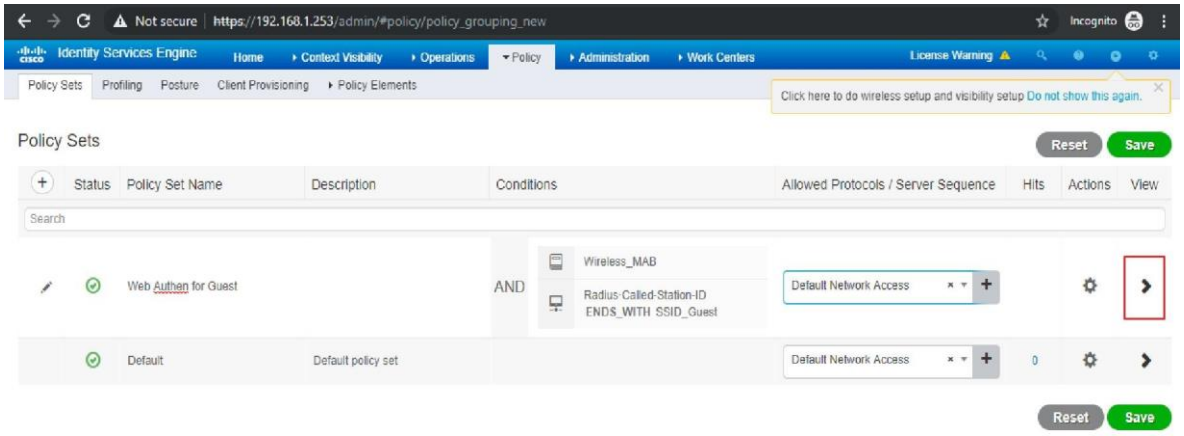
Click Save



Chi tiết cách tạo Policy, tham khảo bài Lab 6: Xác thực radius 802.1x với Cisco ISE

5.7. Tạo Authentication Policy

Click vào icon “>” ở cuối Policy

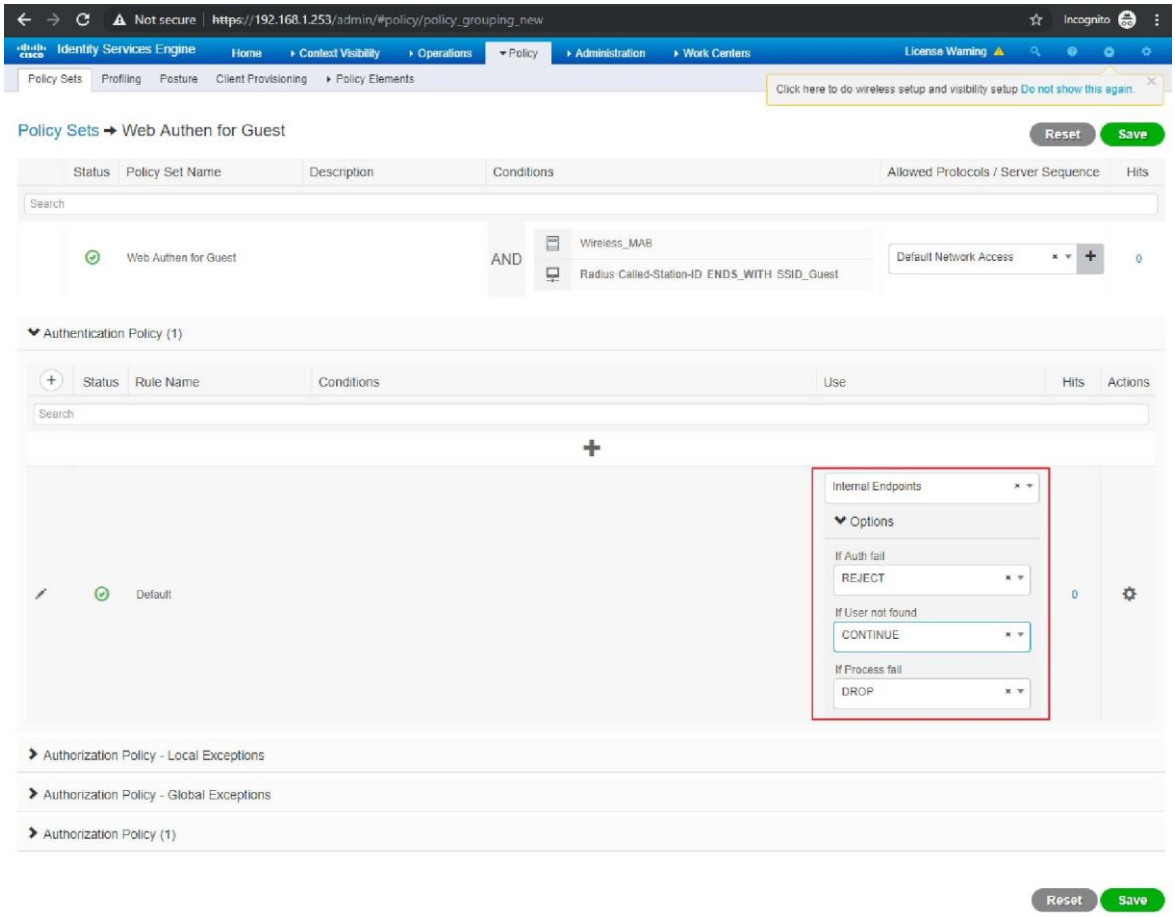


Trong phần Authenticaion Policy, chọn Internal Endpoints. Trong phần Options:

If Auth fail REJECT

If User not fount: CONTINUE

If Process fail: DROP



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

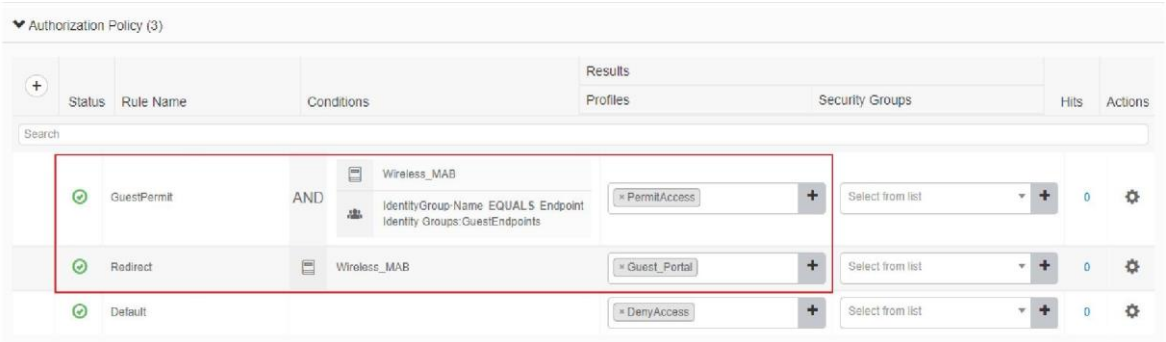
Trong phần Authorization Policy, tạo 2 Rule như sau:

Rule 1:

- Tên: Redirect
- Conditions: Wireless_MAB
- Results → Profiles: Guest_Portal (đã tạo ở bước 6.2)

Rule 2:

- Tên: GuestPermit
- Conditions: Wireless_MAB AND IdentityGroup: Name EQUALS Endpoint Identity Groups: GuestEndpoints
- Results → Profiles: PermitAccess



Click Save

V. Kiểm tra