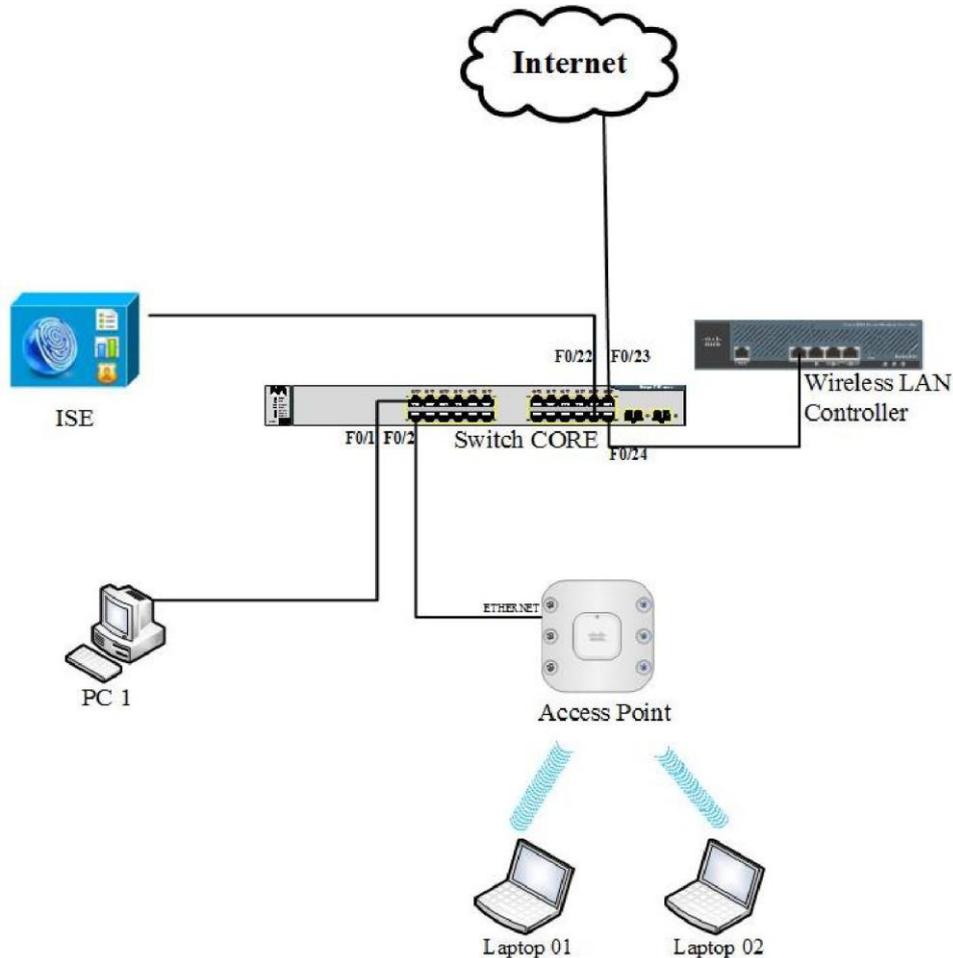


## LAB : CẤU HÌNH WIFI GUEST VỚI CISCO ISE

### 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 đều 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

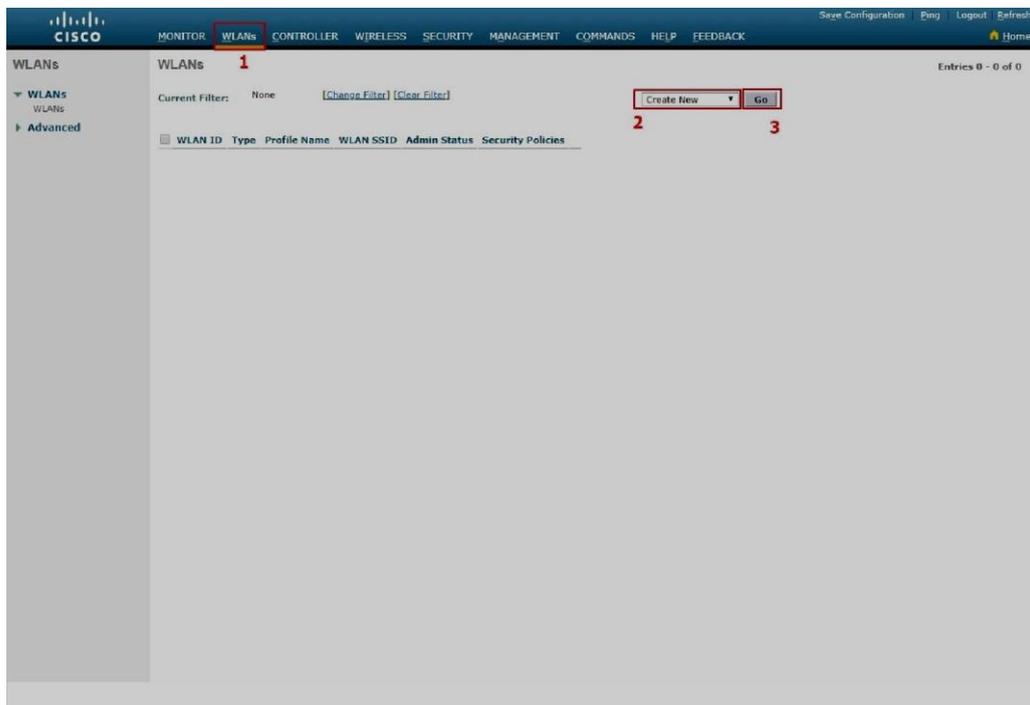
3. Cấu hình kết nối WLC với Cisco ISE

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

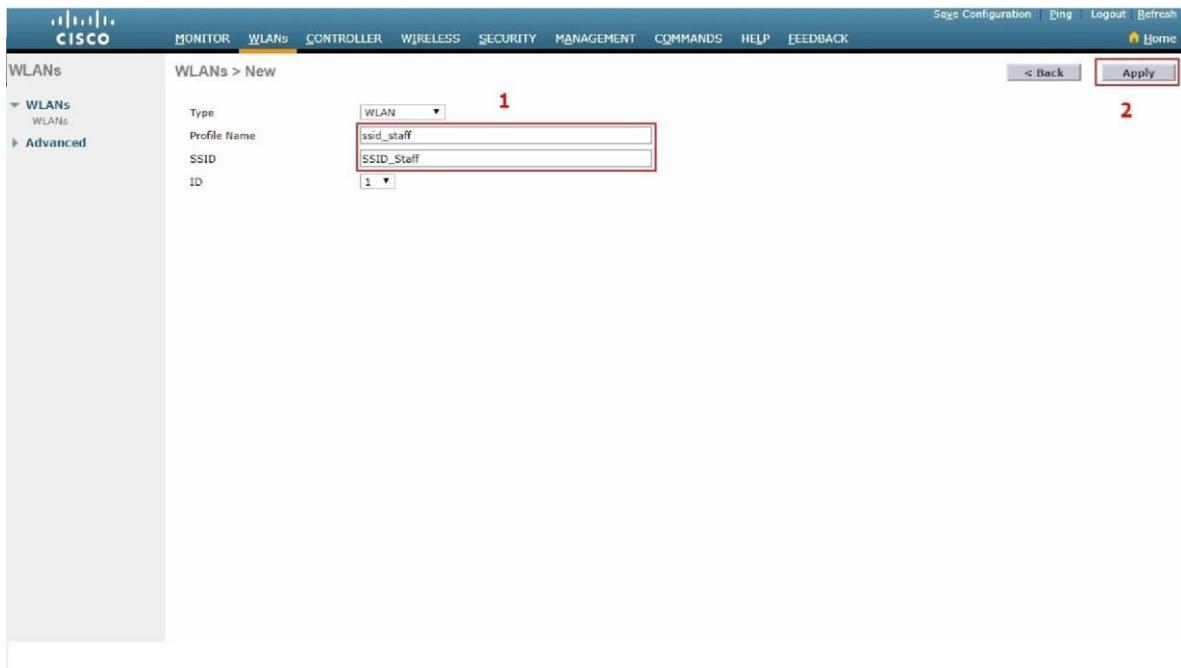
Truy cập vào WLC → Vào menu WLANs → Chọn Create New. Click Go

Đặt Profile name và SSID:

Profile Name: ssid\_staff

SSID: SSID\_Staff

Click Apply



The screenshot shows the Cisco WLC configuration interface for creating a new WLAN. The page title is "WLANs > New". The configuration form includes the following fields:

- Type: WLAN (indicated by a red '1')
- Profile Name: ssid\_staff
- SSID: SSID\_Staff
- ID: 1

The "Apply" button is highlighted with a red box and the number "2".

Trong tab General:

Tick chọn Status: Enabled

Interface/Interface Group (G): vlan\_10

WLANs > Edit 'ssid\_staff'

General Security QoS Policy-Mapping Advanced

Profile Name: ssid\_staff  
 Type: WLAN  
 SSID: SSID\_Staff  
 Status: **1**  Enabled

Security Policies: [WPA2][Auth(802.1X)]  
 (Modifications done under security tab will appear after applying the changes.)

Radio Policy: **2** All  
 Interface/Interface Group(s): wlan\_10  
 Multicast Vlan Feature:  Enabled  
 Broadcast SSID:  Enabled  
 NAS-ID: none

Foot Notes:  
 1 Web Policy cannot be used in combination with IPsec  
 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs  
 2(b) When Flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS  
 2(c) When Flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode  
 3 When client exclusion is enabled, a Timeout Value of zero means Infinity (will require administrative override to reset excluded clients)  
 4 Client MFP is not active unless WPA2 is configured  
 5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled  
 6 WMM and open or AES security should be enabled to support higher 11n rates  
 8 Value zero implies there is no restriction on maximum clients allowed.  
 9 MAC Filtering is not supported with FlexConnect Local authentication  
 10 MAC Filtering should be enabled.  
 11 Guest tunneling, Local switching, DHCP Required should be disabled.  
 12 Max-associated-clients feature and Central Assoc feature are not supported with FlexConnect Local Authentication.  
 13 VLAN based central switching is not supported with FlexConnect Local Authentication.  
 14 Enabling gtk-randomize will prevent clients from decrypting broadcast and multicast packets.  
 15 Fast Transition is supported with WPA2 and open security policy.  
 16 Override Bandwidth Contracts parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.  
 18 When Diagnostic Channel is enabled, P2P Blocking Action will be assigned to Drop Action

Trong Security → Layer 2:

Layer 2 Security: WPA + WPA2

WPA + WPA2 Parameters: tích chọn WPA2 Policy-AES

Authentication Key Management: tích chọn PSK

WLANs > Edit 'ssid\_staff'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security # WPA+WPA2 **1**  
 MAC Filtering

Fast Transition  
 Fast Transition

Protected Management Frame  
 PMF Disabled

WPA+WPA2 Parameters

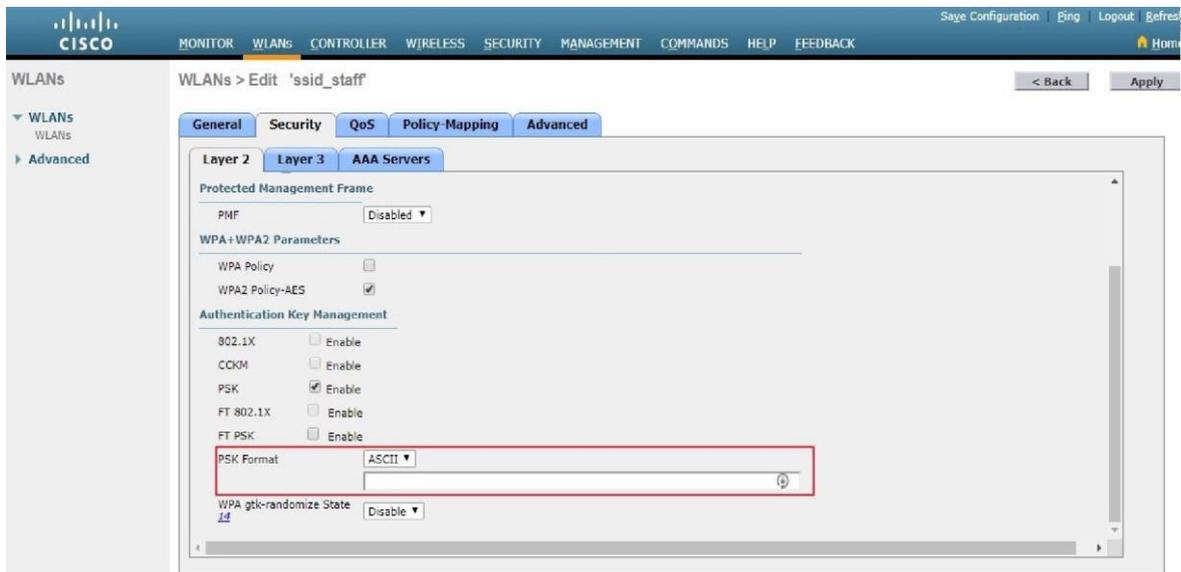
WPA Policy   
 WPA2 Policy-AES  **2**

Authentication Key Management

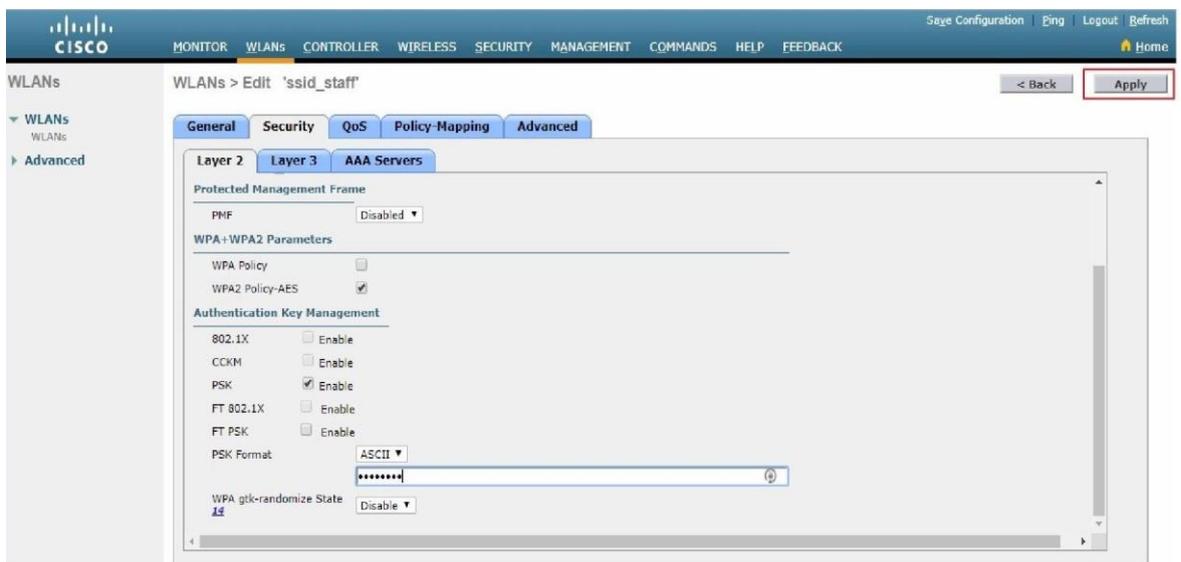
802.1X  Enable  
 CCKM  Enable  
 PSK  Enable **3**  
 FT 802.1X  Enable

Foot Notes:  
 1 Web Policy cannot be used in combination with IPsec  
 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs  
 2(b) When Flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS  
 2(c) When Flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode  
 3 When client exclusion is enabled, a Timeout Value of zero means Infinity (will require administrative override to reset excluded clients)  
 4 Client MFP is not active unless WPA2 is configured  
 5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled  
 6 WMM and open or AES security should be enabled to support higher 11n rates  
 8 Value zero implies there is no restriction on maximum clients allowed.  
 9 MAC Filtering is not supported with FlexConnect Local authentication  
 10 MAC Filtering should be enabled.  
 11 Guest tunneling, Local switching, DHCP Required should be disabled.  
 12 Max-associated-clients feature and Central Assoc feature are not supported with FlexConnect Local Authentication.  
 13 VLAN based central switching is not supported with FlexConnect Local Authentication.  
 14 Enabling gtk-randomize will prevent clients from decrypting broadcast and multicast packets.  
 15 Fast Transition is supported with WPA2 and open security policy.  
 16 Override Bandwidth Contracts parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.  
 18 When Diagnostic Channel is enabled, P2P Blocking Action will be assigned to Drop Action

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

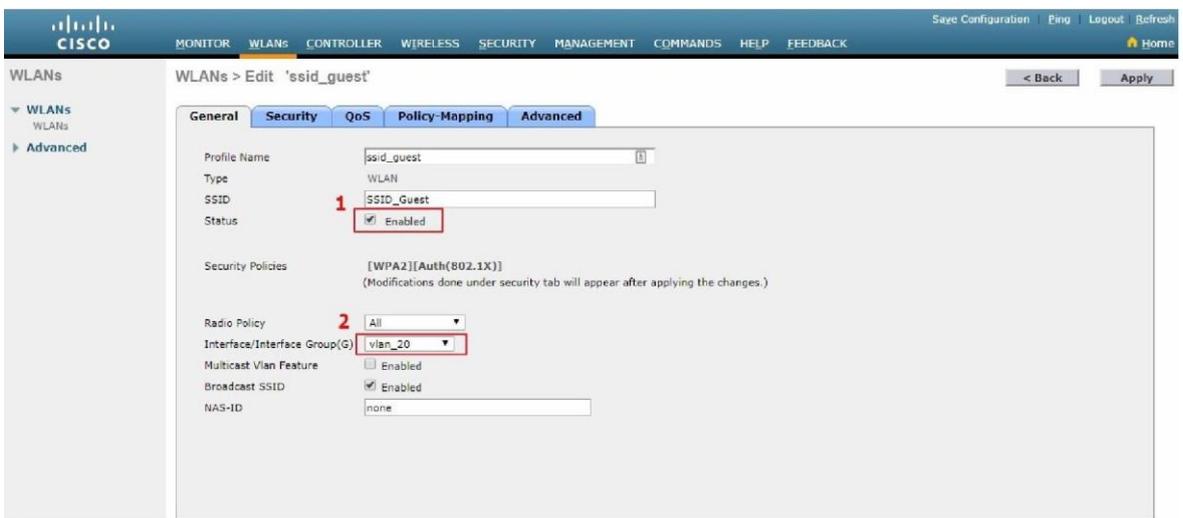
Click Apply



Trong tab General:

Tick chọn Status: Enabled

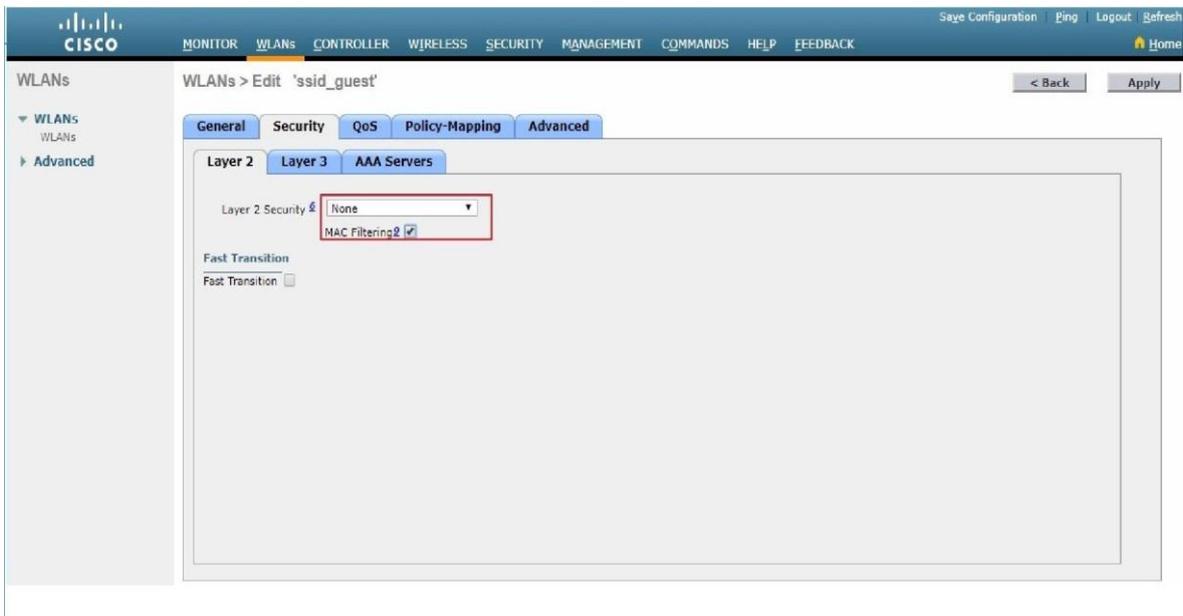
Interface/Interface Group (G): vlan\_20



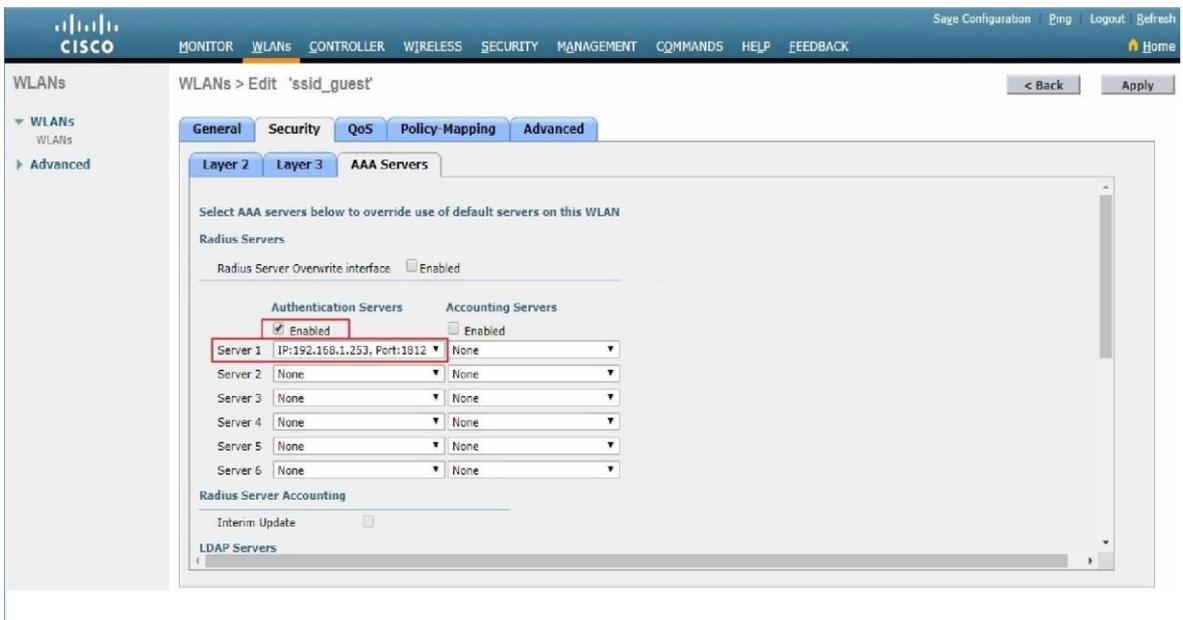
Trong Security → Layer 2:

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

The screenshot shows the Cisco WLAN configuration interface for the 'ssid\_staff' WLAN. The 'Advanced' tab is selected, and the 'AAA Servers' section is visible. Under 'Order Used For Authentication', a dropdown menu is highlighted with a red box, showing 'RADIUS' as the selected option. Other options in the dropdown are 'LOCAL' and 'LDAP'. The 'Local EAP Authentication' section is also visible, with 'Local EAP Authentication' checked as 'Enabled'. Below the configuration area, there are 'Foot Notes' providing additional information about various features and their compatibility.

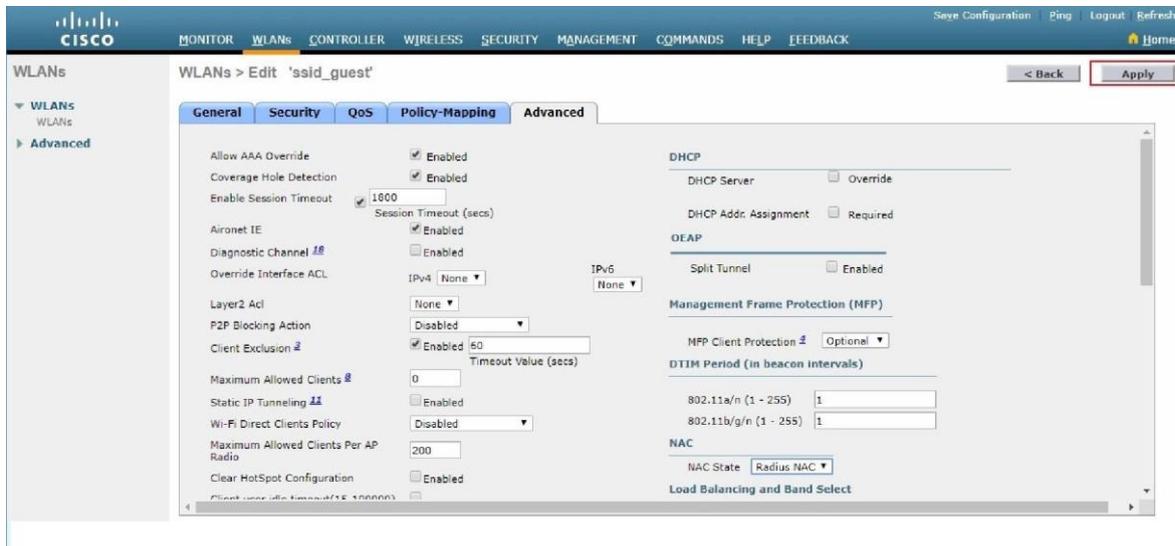
**Foot Notes:**

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRAMITE authentication, Override Interface ACLs
- 2(b) When Flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When Flexconnect local authentication is disabled, AP on connected mode will use MLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 8 Value zero implies there is no restriction on maximum clients allowed.
- 9 MAC Filtering is not supported with FlexConnect Local authentication
- 10 MAC Filtering should be enabled.
- 11 Guest tunneling, Local switching, DHCP Required should be disabled.
- 12 Max-associated-clients feature and Central Assoc feature are not supported with FlexConnect Local Authentication.
- 13 VLAN based central switching is not supported with FlexConnect Local Authentication.
- 14 Enabling gtk-randsize will prevent clients from decrypting broadcast and multicast packets.
- 15 Fast Transition is supported with WPA2 and open security policy.
- 16 Override Bandwidth Contracts parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.
- 18 When Diagnostic Channel is enabled, P2P Blocking Action will be assigned to Drop Action

Trong tab Advanced:  
 Tích chọn Allow AAA Override  
 NAC State là RADIUS NAC

The screenshot shows the Cisco WLAN configuration interface for the 'ssid\_guest' WLAN. The 'Advanced' tab is selected, and the 'Policy-Mapping' section is visible. In the 'Policy-Mapping' section, the 'Allow AAA Override' checkbox is checked and highlighted with a red box and the number '1'. In the 'NAC' section, the 'NAC State' dropdown menu is set to 'Radius NAC' and highlighted with a red box and the number '2'. Other settings in the 'Policy-Mapping' section include 'Coverage Hole Detection' (checked), 'Enable Session Timeout' (checked, 1800), 'Aironet IE' (checked), 'Diagnostic Channel' (checked), 'Override Interface ACL' (IPv4: None, IPv6: None), 'Layer2 Acl' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (checked, 60), 'Maximum Allowed Clients' (0), 'Static IP Tunneling' (checked), 'Wi-Fi Direct Clients Policy' (Disabled), 'Maximum Allowed Clients Per AP Radio' (200), 'Clear HotSpot Configuration' (checked), and 'Client over the time' (checked).

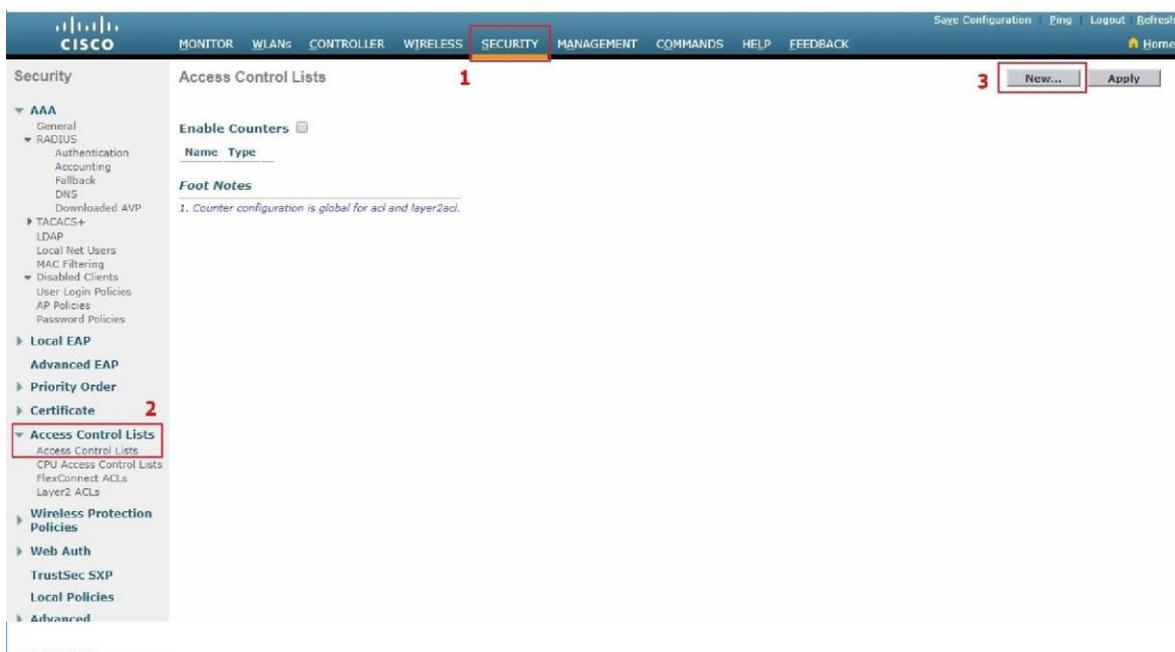
Click Apply



### 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



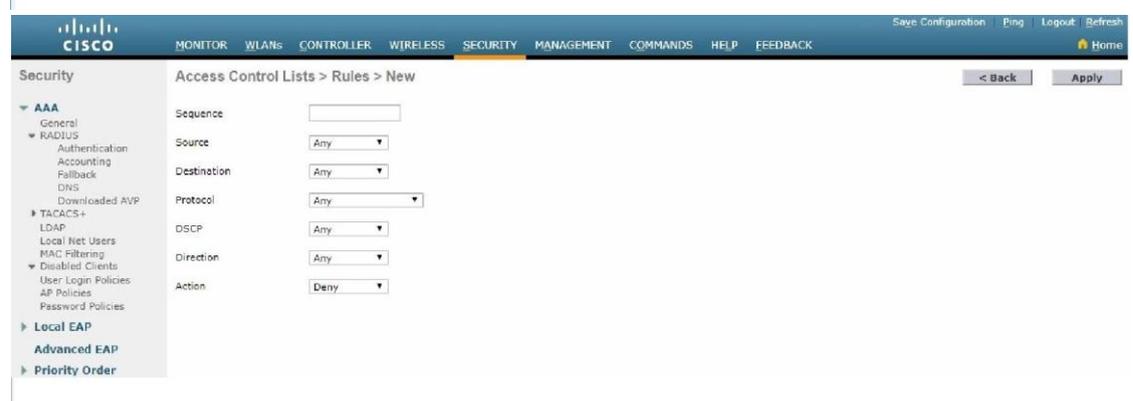
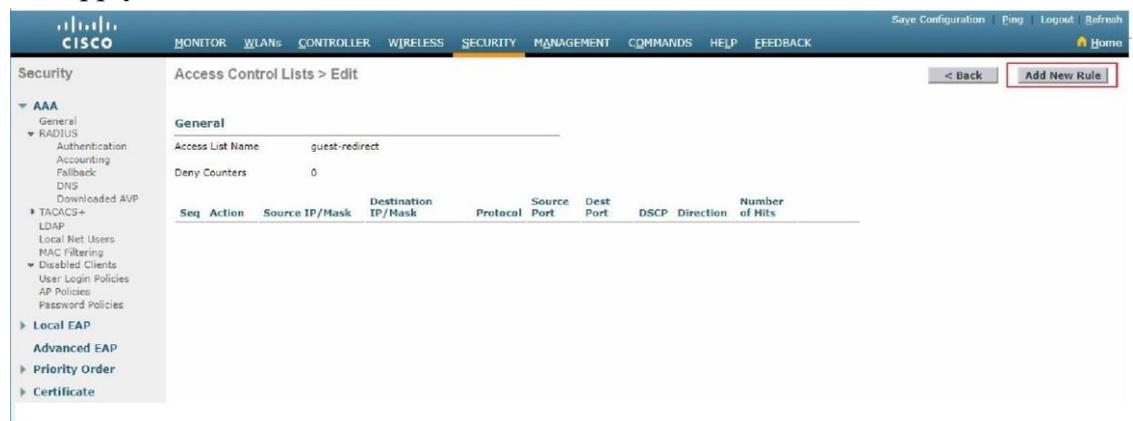
Đặt tên cho ACL (bài lab này đặt tên cho ACL là guest-redirect) sau đó click Apply



Click vào tên của ACL vừa tạo để chỉnh sửa



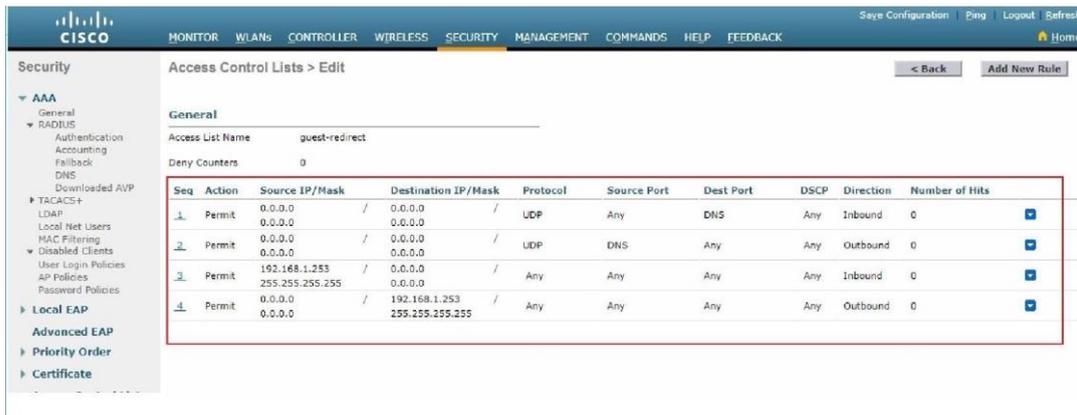
Để thêm rule cho ACL, click vào Add New Rule. Sau đó nhập các tham số và click Apply



### 5.3. Tạo các rule

Cho phép DNS đi vào/ra access point

Cho phép traffic từ/đến ISE



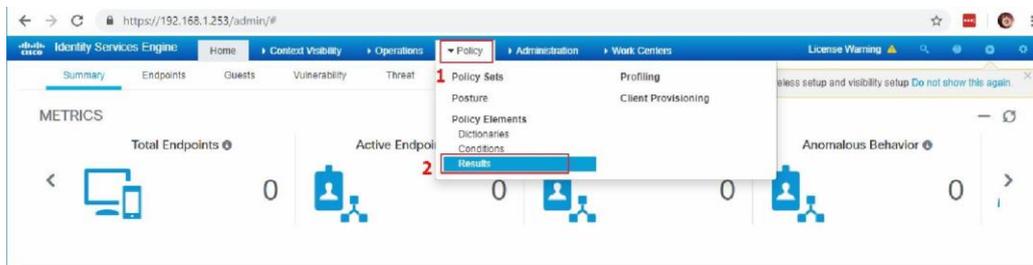
### 5.4. Cấu hình Cisco ISE

Thêm WLC vào Cisco ISE

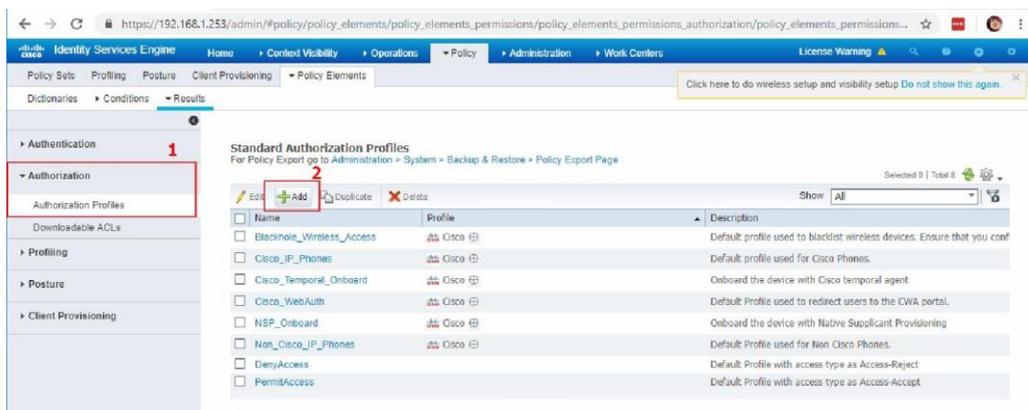
Tham khảo bài Lab 6: Xác thực radius 802.1x với Cisco ISE

### 5.5. Tạo Result

Vào menu Policy → Results



Vào mục Authorization → Authorization Profiles. Click Add

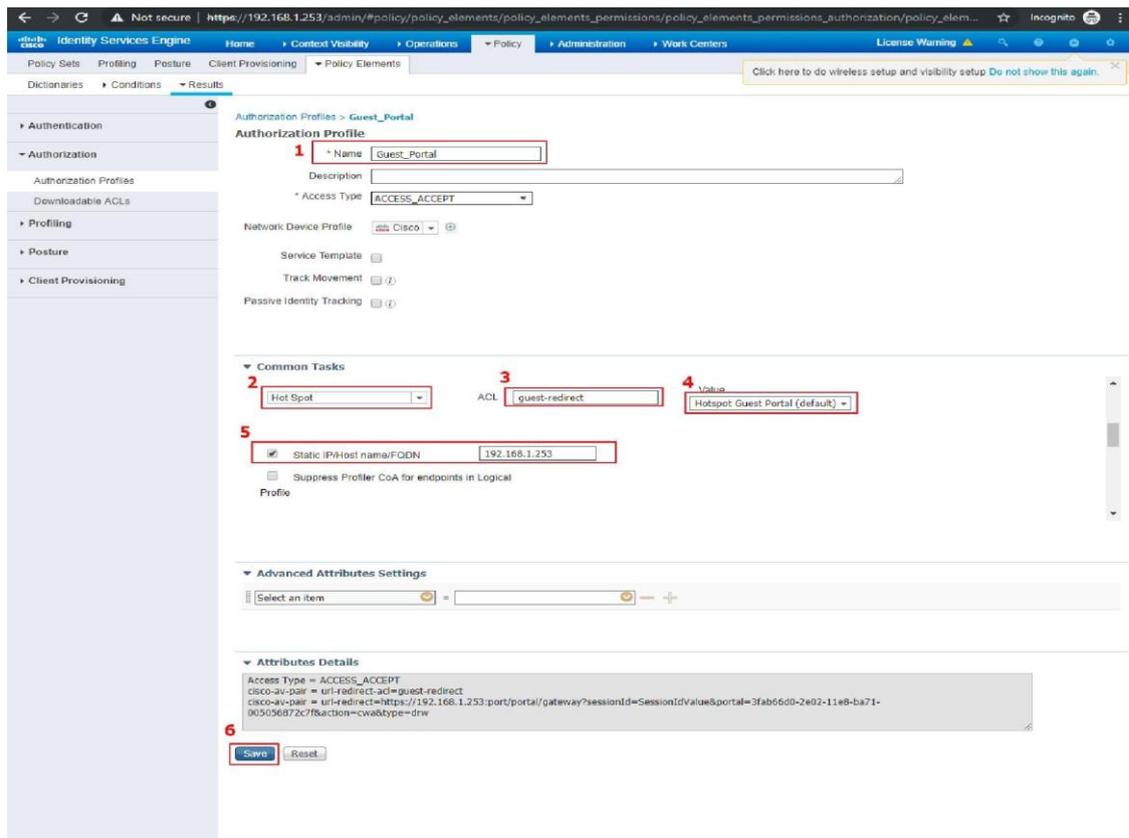


Đặt tên cho Profile: Guest\_Portal

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)

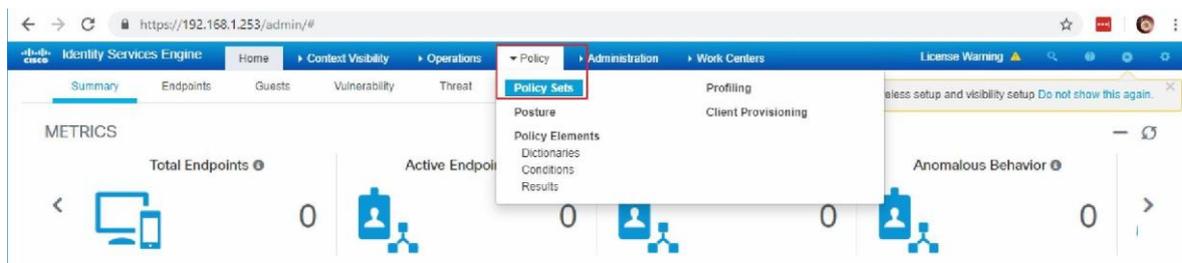
Tích chọn Static IP/Hostname/FQDN và nhập IP của Cisco ISE vào  
Click Submit



## 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

The screenshot shows the Cisco ISE Policy Sets configuration page. The table below represents the data visible in the interface:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Web Authen for Guest		Wireless_MAB AND Radius: Called-Station-ID ENDS_WITH SSID_Guest	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

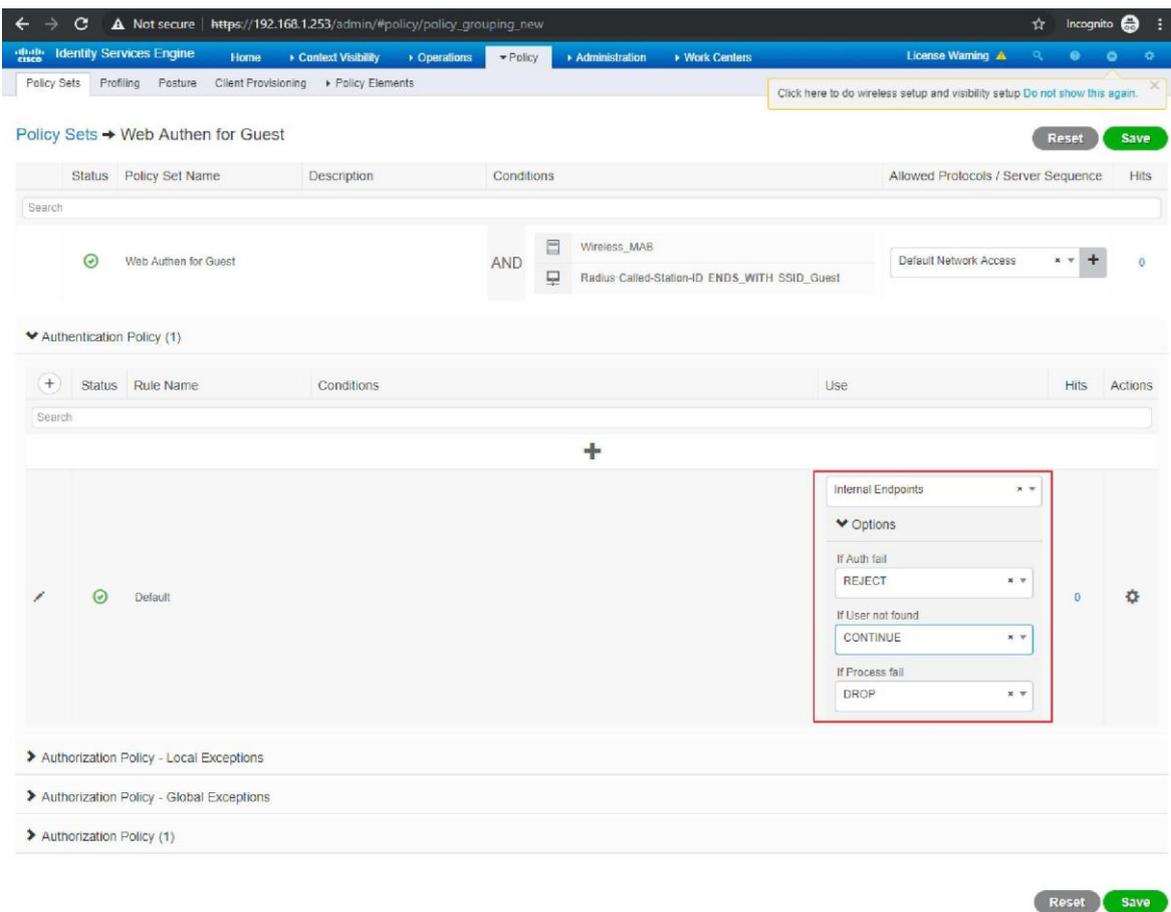
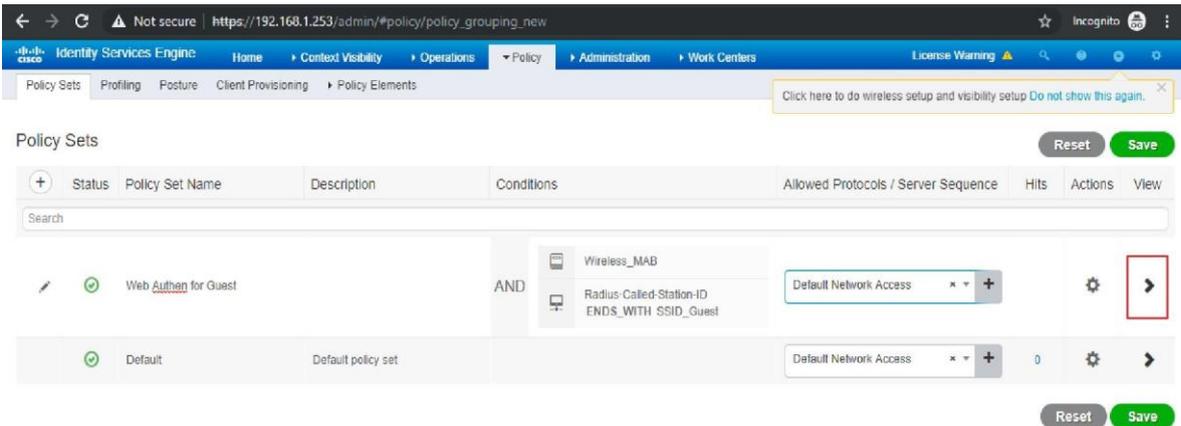
Click Save

The screenshot shows the same Cisco ISE Policy Sets configuration page as above, but with the 'Save' button in the top right corner highlighted by a red box.

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



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

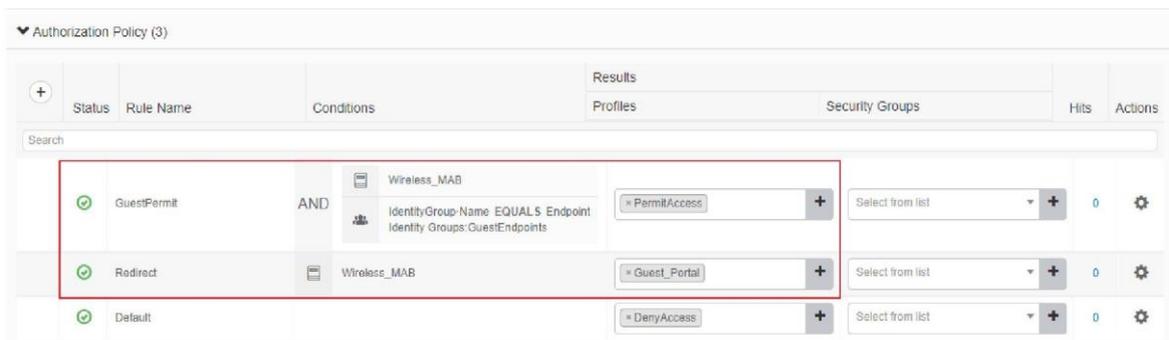
Trong phần Authorization Policy, tạo 2 Rule như sau:

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



▼ Authorization Policy (3)							
+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
		Search					
✓	GuestPermit	AND	Wireless_MAB IdentityGroup-Name EQUALS Endpoint Identity Groups: GuestEndpoints	PermitAccess	Select from list	0	⚙️
✓	Redirect		Wireless_MAB	Guest_Portal	Select from list	0	⚙️
✓	Default			DenyAccess	Select from list	0	⚙️

Click Save

## V. Kiểm tra