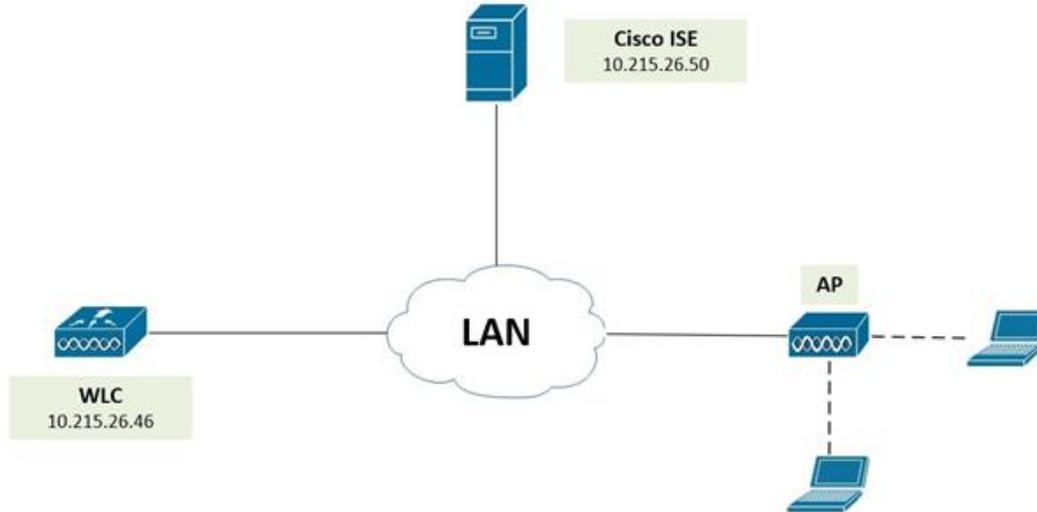


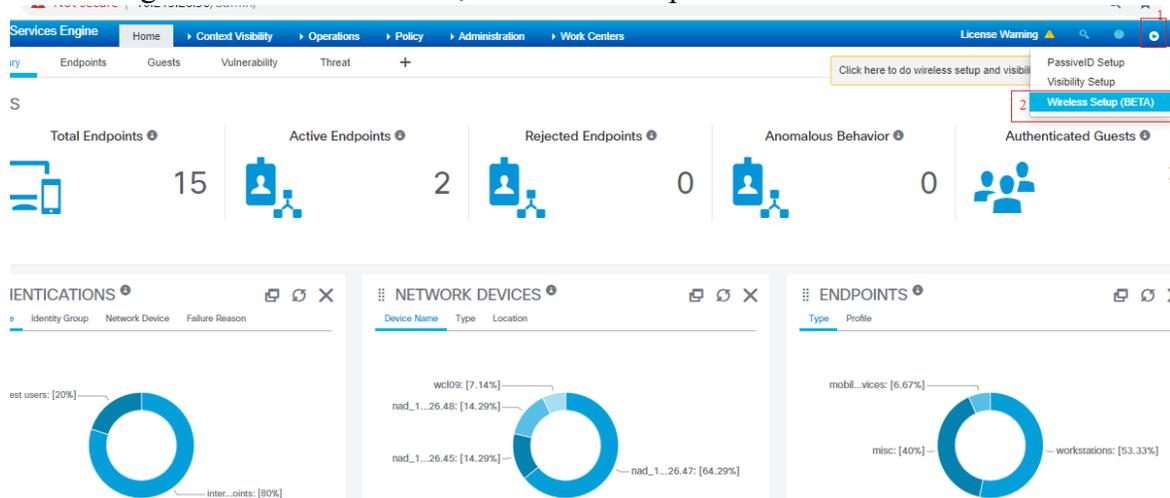
# Lab – Cấu hình Guest portal Self-Register bằng Wizard trên Cisco ISE

## 1. Sơ đồ



## 2. Cấu hình Guest Self-Register bằng Wizard trên Cisco ISE:

- Login vào Cisco ISE -> Chọn Wireless Setup



- Cửa sổ hiện thị ra -> chọn Guest Access -> Chọn SETUP Self-Register



What can we help you set up today?

ISE Wireless Setup is beta software - do not use in production networks.

Please choose a feature.

#### Guest Access

Allow guests to access your wireless network.

1



#### Secure Access

Allow access to your wireless network using 802.1X secure authentication.

SETUP

#### Bring Your Own Device (BYOD)

Allow access to your wireless network through personal devices.

SETUP

#### Self Registration

Guests register themselves to log onto this network.

SETUP

2

#### Hotspot

Guests are allowed access to this network without authentication.

SETUP

#### Sponsored

Sponsors register guests to provide network access.

SETUP

- Tiếp theo click chuột vào REGISTER để add thông tin WLC, điền thông tin của WLC bao gồm địa chỉ IP của WLC, username và Password dùng để đăng nhập WLC và cuối cùng là thông tin Shared Secret giữa WLC và Cisco ISE -> Chọn Register sau khi điền đầy đủ thông tin

1  
2  
3  
4

SETUP | SELF REGISTRATION

Wireless LAN Controller

Choose or register a Wireless LAN Controller.

REGISTER

WLC

WLC-01  
IP address: 10.215.26.40

Register a Wireless LAN Controller.

WLC IP ADDRESS  
10.215.26.46

USERNAME  
WLC-01

PASSWORD  
.....

SHARED SECRET  
.....

Register

- Chọn Commit để qua bước tiếp theo

1  
2  
3  
4

SETUP | SELF REGISTRATION

Wireless LAN Controller

Choose or register a Wireless LAN Controller. 3/10 WLCs created

REGISTER

WLC

WLC-08  
IP address: 10.215.26.47

WLC

WLC-01  
IP address: 10.215.26.46

WLC

WLC-01  
IP address: 10.215.26.40

Commit 2

- Tiếp theo, tạo thông tin SSID trên Cisco ISE bao gồm các thông tin sau:

- (1) Wireless Network Name (SSID): Tên của SSID
  - (2) Default WLC Interface (Vlan): SSID tương ứng với Interface WLAN nào trên WLC
  - (3) Account Access Duration: Thời gian Account tồn tại
  - (4) Post Login Redirect: chuyển hướng trang web sau khi xác thực thành công
- Sau khi tạo đầy đủ thông tin, chọn ADD để tạo SSID từ Cisco Ise áp cho WLC.

1 SETUP | SELF REGISTRATION

Wireless Network

1 Add a Wireless network.

2 WIRELESS NETWORK NAME (SSID)  
Self-Register-Test

3 DEFAULT WLC INTERFACE (VLAN)  
management

4 ACCOUNT ACCESS DURATION  
1 day

POST LOGIN REDIRECT  
Redirect to custom URL  
http://vnpro.vn

Add

- Chọn Commit để tiếp tục

1 SETUP | SELF REGISTRATION

Wireless Network

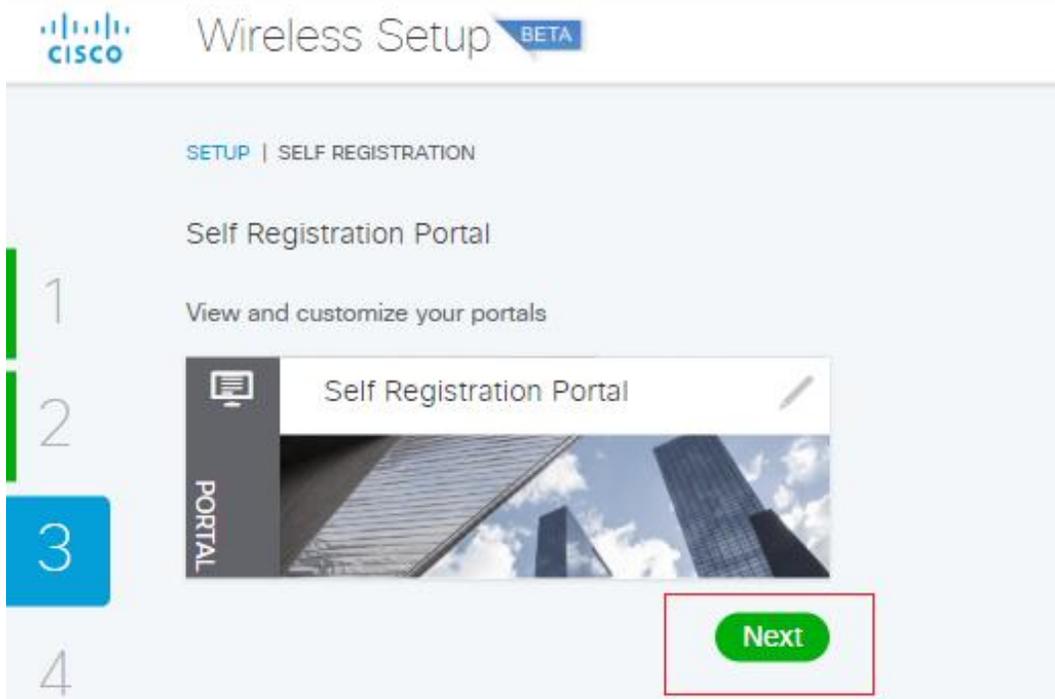
1 Choose or add a wireless network. The wireless network you select will remain disabled until the end of your setup where you can 'Go Live.' 1/10 WLANs created

2 ADD

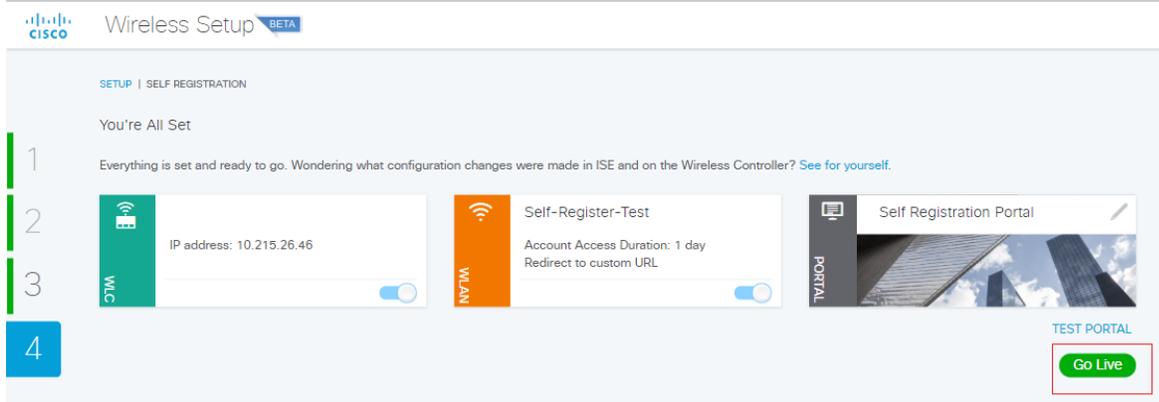
3 WLAN Self-Register-Test  
Account Access Duration: 1 day  
Redirect to custom URL

4 Commit

- Chọn Next để tiếp tục



- Chọn Go live để hoàn tất



- Kiểm tra thông tin trên WLC sau khi cấu hình trên Cisco ISE, ta thấy tại mục Wireless đã xuất hiện SSID với Name Self-Register-Test



- SSID đã được Enable và phương thức xác thực là Mac Filtering

WLANs > Edit 'Self-Register-Test'

General Security QoS Policy-Mapping Advanced

Profile Name: Self-Register-Test  
Type: WLAN  
SSID: Self-Register-Test  
Status:  Enabled

Security Policies: MAC Filtering  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All  
Interface/Interface Group(G): management  
Multicast Vlan Feature:  Enabled  
Broadcast SSID:  Enabled  
NAS-ID: none

WLANs > Edit 'Self-Register-Test'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: None  
MAC Filtering:

Fast Transition  
Fast Transition Over the DS:  Adaptive  
Reassociation Timeout: 20 Seconds

- Các thông tin Radius Server cũng đã được áp sẵn trên WLC

WLANs > Edit 'Self-Register-Test'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface:  Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.215.26.50, Port:1812	<input checked="" type="checkbox"/> Enabled IP:10.215.26.50, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

RADIUS Server Accounting  
Interim Update:  Interim Interval: 0 Seconds

LDAP Servers

- Ngoài ra trên WLC cũng có thêm một ACL được tạo ra tự động, ACL này dùng để chuyển hướng lưu lượng xác thực bằng Portal trên WLC được đẩy đến CISCO ISE

The screenshot shows the Cisco WLC interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'SECURITY' tab is active. On the left, the 'Security' menu is expanded to 'Access Control Lists', with 'FlexConnect ACLs' highlighted. The main content area shows 'FlexConnect Access Control Lists' with a table containing one entry: 'ACL\_WEBAUTH\_REDIRECT'.

- Ngoài những cấu hình đã được cài đặt sẵn trên WLC từ WLC, ta cấu hình thêm trên WLC để Client có thể xác thực thành công: đầu tiên Click vào Wireless trên WLC -> Chọn AP đang Join vào WLC -> Chọn qua tab FlexConnect -> click vào External WebAuthentication ACLs

The screenshot shows the Cisco WLC interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WIRELESS' tab is active. On the left, the 'Wireless' menu is expanded to 'Access Points', with '802.11a/n/ac' highlighted. The main content area shows 'All APs > Details for AP1928'. The 'FlexConnect' tab is active, showing 'External WebAuthentication ACLs' selected.

- Tại mục Policy, Click Add ACL đã được tạo sẵn trên Controller -> chọn Save để lưu cấu hình

- Trên Cisco ISE, để Client có thể Redirect đến trang Portal trên Cisco ISE, ta phải chỉ ra địa chỉ IP của Portal để mở trang xác thực, ta làm như sau:

- Tiếp theo, tại mục Common Task, tìm đến mục Web Redirection (CWA, MDM, NSP, CPP) -> Static IP/Host name/ FQDN -> điền địa chỉ IP của Cisco Ise vào -> Chọn Submit để lưu lại cấu hình

- Tiếp theo ta kiểm tra xem Portal vừa tạo sẽ được áp vào Policy nào thì ta làm như sau: Chọn Work Center -> Portals & Components -> Guest Portals, tìm đến Portal có tên khớp với SSID vừa tạo lúc này -> Click vào **1 rule** để kiểm tra xem Portal này được sử dụng ở rule nào (mặc định là Rule Default Policy)

- Qua mục Policy Set để kiểm tra Policy: click Policy -> tại Policy Default click vào biểu tượng mũi tên như hình bên dưới

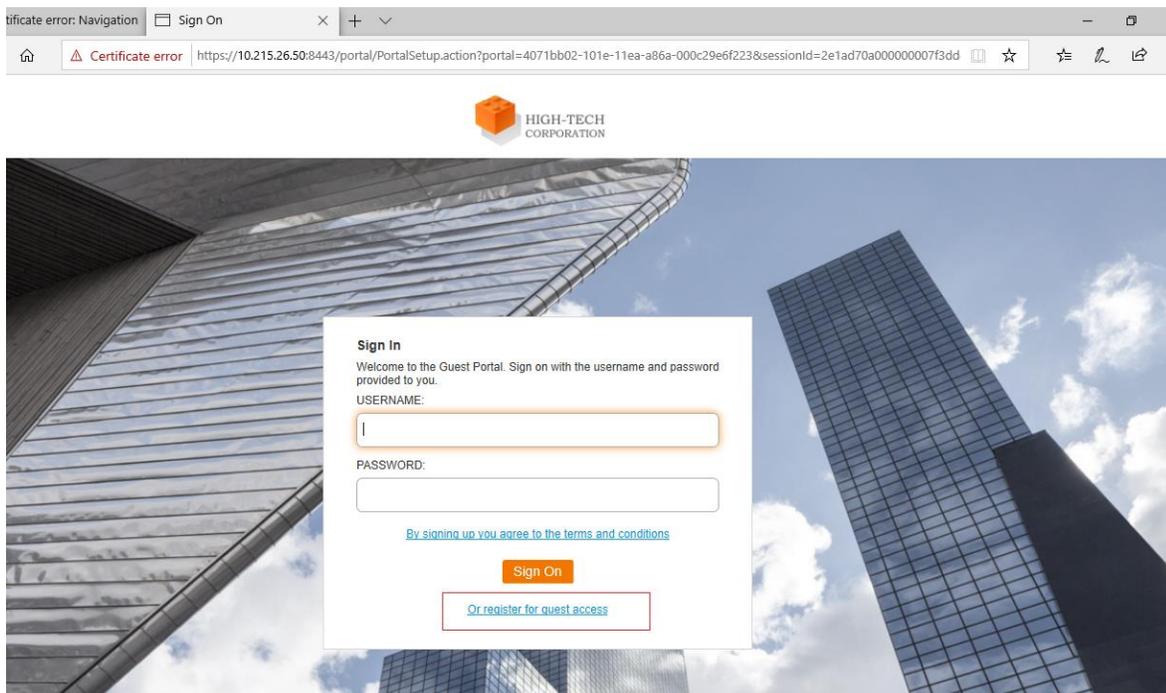
- Tiếp tục kiểm tra mục Authentication và Authorization trong Policy Default này
  - o Tại mục Authentication, ở mục USE chọn Internal Endpoint, tại mục option-> tại mục If User not found -> chọn Continue -> Click Save để lưu cấu hình

- Tiếp theo, tại mục Authorization Policy, ta thấy có 2 policy được tạo sẵn như hình bên dưới

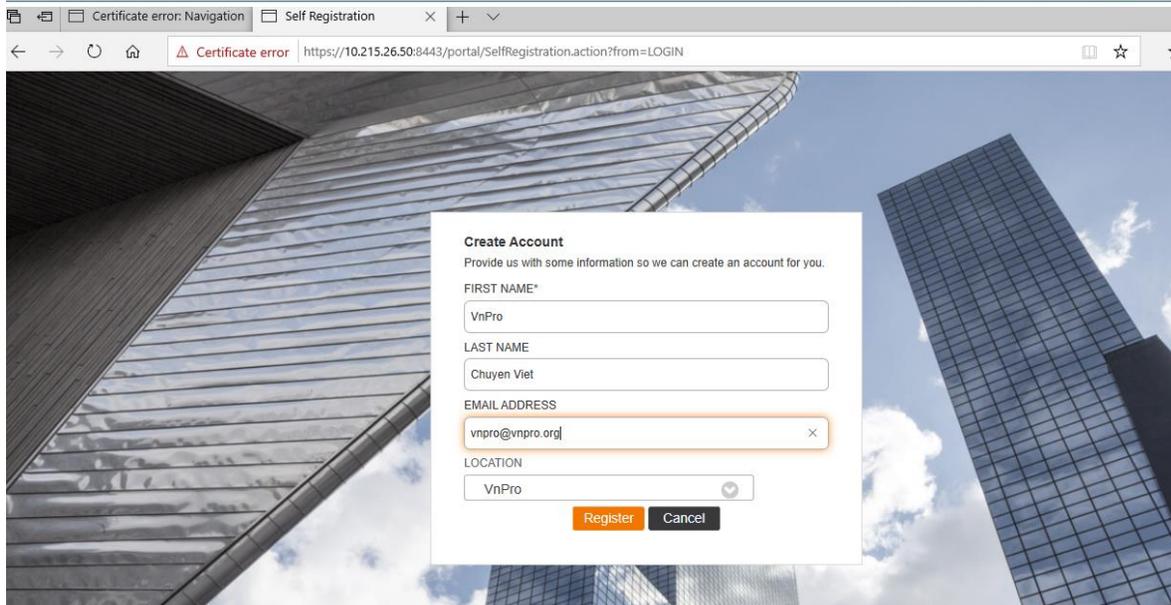
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✔	WS_Self-Register-Test_SelfRegistrationPortal_GuestAccessPolicy	Wireless_MAB Guest_Flow Radius-Called-Station-ID ENDS_WITH :Self-Register-Test	× PermiAccess	Guests	0	⚙
✔	WS_Self-Register-Test_SelfRegistrationPortal_RedirectPolicy	Wireless_MAB Radius-Called-Station-ID ENDS_WITH :Self-Register-Test	× WS_Self-Register-Test_SelfRegist	Select from list	0	⚙
✔	WS_Van Minh Pro_HotspotPortal_GuestAccessPolicy	InternalUser IdentityGroup EQUALS Endpoint Identity Groups:GuestEndpoints Radius-Called-Station-ID ENDS_WITH :Van Minh Pro	× PermiAccess	Guests	0	⚙

- Kiểm tra user kết nối vào SSID như sau:  
Click vào biểu tượng wifi, chọn SSID để kết nối là Self-Register-Test -> Connect

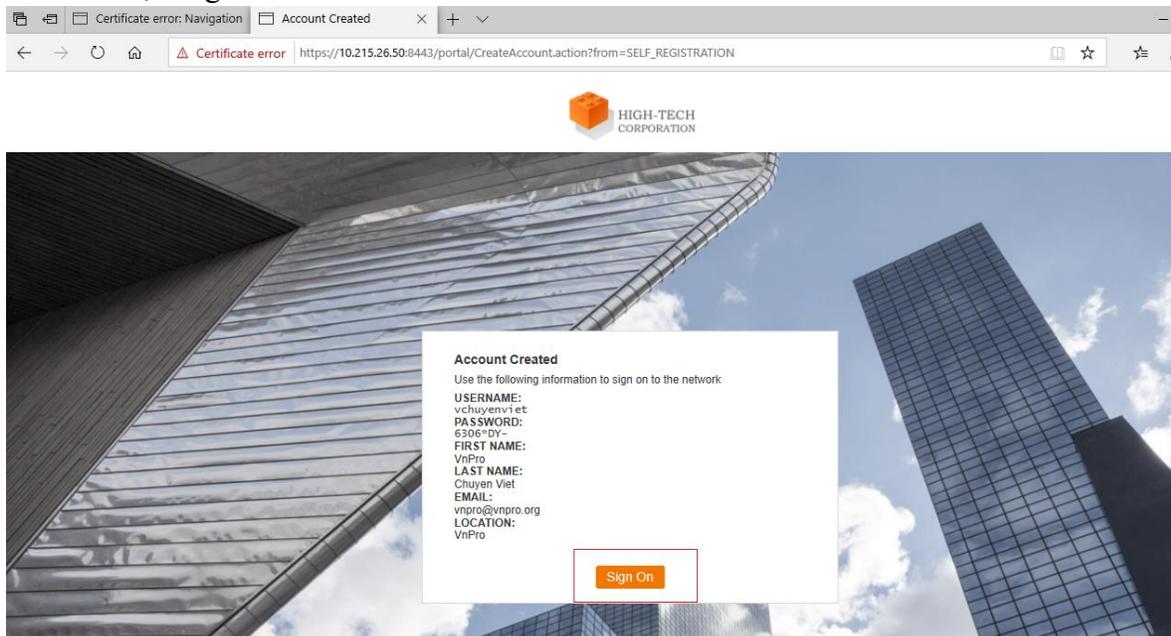
Cửa sổ Sign On hiển thị ra, chọn Or register for guest access để có thể tự tạo account để login vào mạng



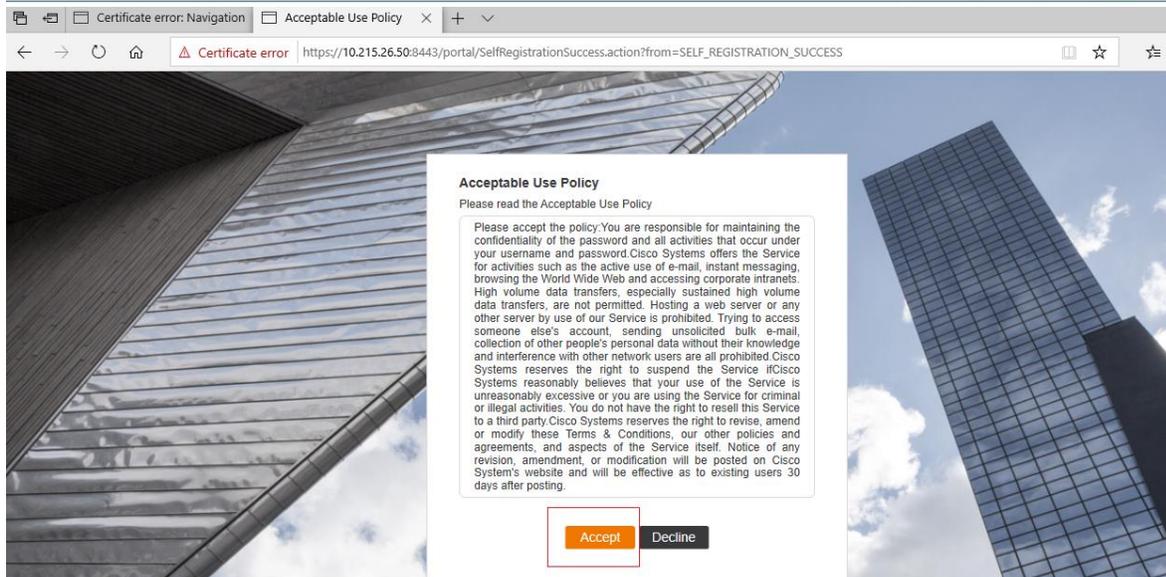
- Tiếp tục, điền đầy đủ các thông tin yêu cầu nhập bên dưới -> Chọn Register để truy cập mạng Wifi



## - Chọn Sign On



- Click Accept để đồng ý các điều khoản sử dụng



- Sau khi chấp nhận các điều khoản, Portal sẽ Redirect tới Website mà chúng ta đã cấu hình chuyển hướng sau khi xác thực thành công