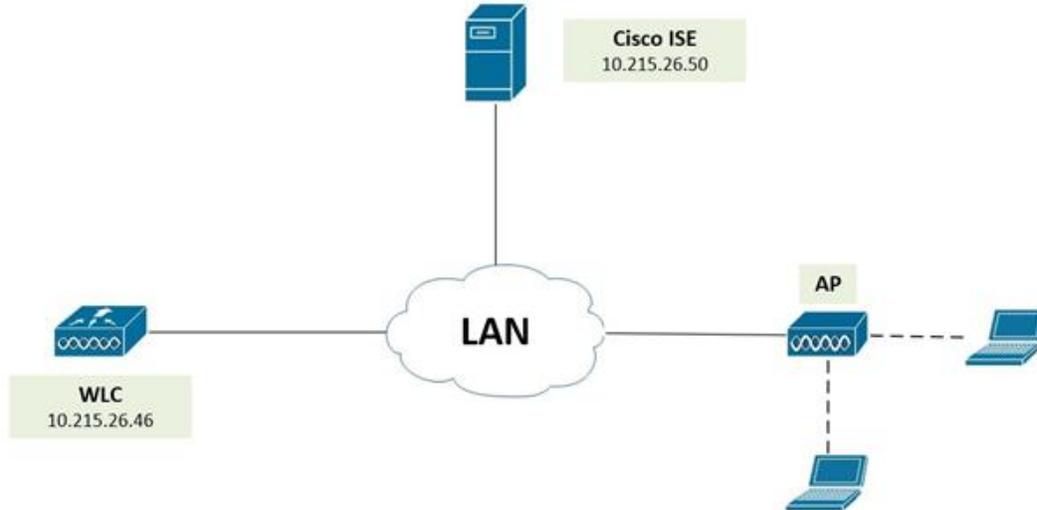


Lab – Wireless Guest Self-Register (Cấu hình Manual trên WLC và Cisco ISE)

1. Sơ đồ



2. Cấu hình trên WLC

- Đầu tiên ta phải cấu hình để AP Join vào WLC hay chưa, vào mục Wireless để kiểm tra

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	PoE Status	Speed Eth0
3602-1928	192.168.3.230	AIR-CAP3602I-N-K9	d4:8c:b5:93:1e:52	0 d, 00 h 05 m 35 s	Enabled	REG	PoE/Full Power	100 Mbps

- Ta cấu hình khai báo Radius Server (Cisco ISE) với WLC như sau: vào mục Security -> AAA-> Radius -> Authentication -> New

- Ta khai báo các tham số của Authentication bao gồm các thông tin sau như sau:

- Địa chỉ IP của Radius Server
- Shared Secret: lưu ý thông tin Shared secret phải giống nhau giữa WLC và Radius Server, điền lại thông tin shared secret 1 lần nữa tại mục Confirm
- Enable Support CoA
- Enable Network User

Chọn Apply để lưu cấu hình Authentication Server.

- Tại mục Security này, ta phải tạo ra 1 ACL để có thể Redirect traffic xác thực của Guest đến được Cisco ISE, ta tạo như sau: Tại tab Security -> Access Control List -> Chọn FlexConnect ACLs -> Chọn New

- Ta tiến hành đặt tên cho ACL này và chọn Apply để lưu lại

Security > Access Control Lists > New

Access Control List Name: **1**

2

- Sau khi Apply, ta sẽ có 1 ACL được tạo ra như bên dưới

Security > FlexConnect Access Control Lists

Acl Name:

- Tuy nhiên ACL này vẫn chưa có bất kì hành động nào, ta sẽ tiếp hành tạo hành động cho ACL này bằng cách click vào ACL vừa tạo và tiến hành tạo rule cho ACL này như sau: click vào Add New Rule và tạo hành động giống như hình bên dưới

Security > Access Control Lists > Edit

General

Access List Name: redirect-guest

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
-----	--------	----------------	---------------------	----------	-------------	-----------	------

Security > Access Control Lists > Edit

General

Access List Name: redirect-guest

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.215.26.49 / 255.255.255.255	Any	Any	Any	Any
2	Permit	10.215.26.49 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any

Lưu ý: địa chỉ IP trên ACL là địa chỉ IP của Cisco Ise

- Tiếp theo ta sẽ tạo SSID trên WLC: Chọn WLAN -> tại mục Create new chọn Go

WLANs

WLANs > Create New

WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies

- Điền thông tin Profilename và SSID (2 thông tin này không nhất thiết phải giống nhau) -> Chọn Apply để lưu lại cấu hình

WLANs > New

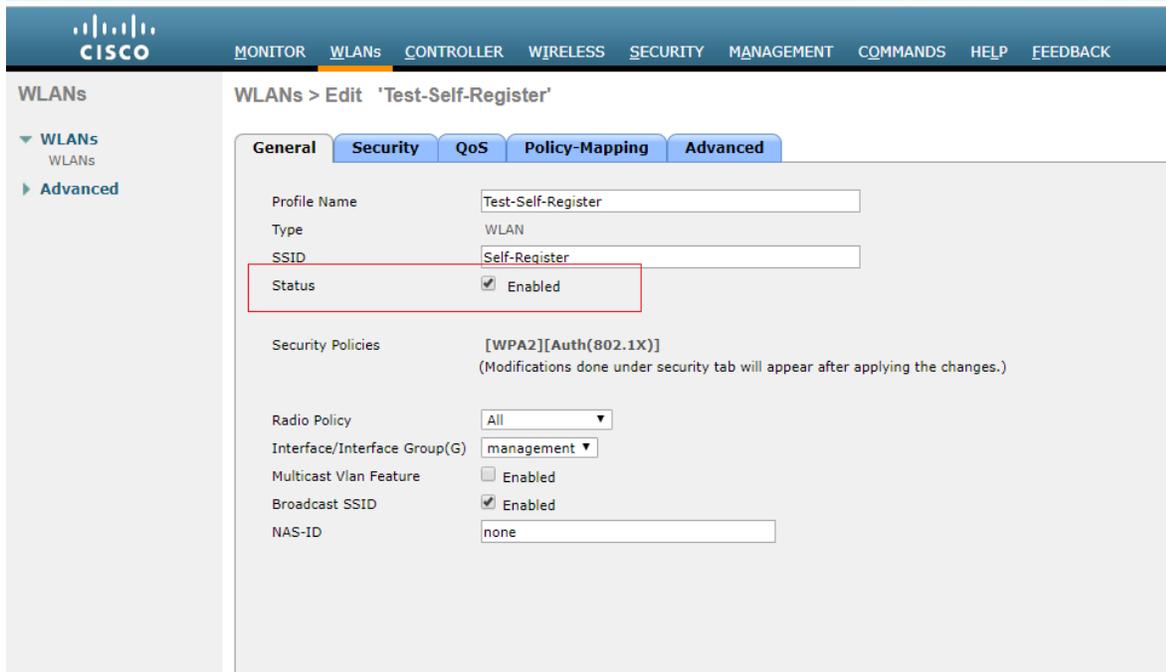
Type: WLAN

Profile Name: Test-Self-Register

SSID: Self-Register

ID: 1

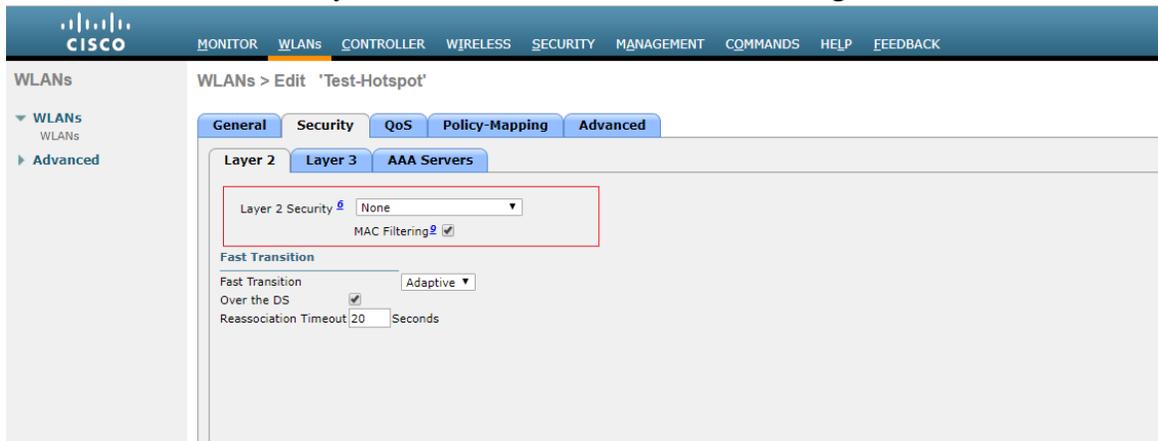
- Tại tab General -> Enable Status SSID để cho phép SSID này hoạt động



The screenshot shows the Cisco WLAN configuration interface for a profile named 'Test-Self-Register'. The 'Security' tab is selected. The configuration includes:

- Profile Name: Test-Self-Register
- Type: WLAN
- SSID: Self-Register
- Status: Enabled
- Security Policies: [WPA2][Auth(802.1X)] (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

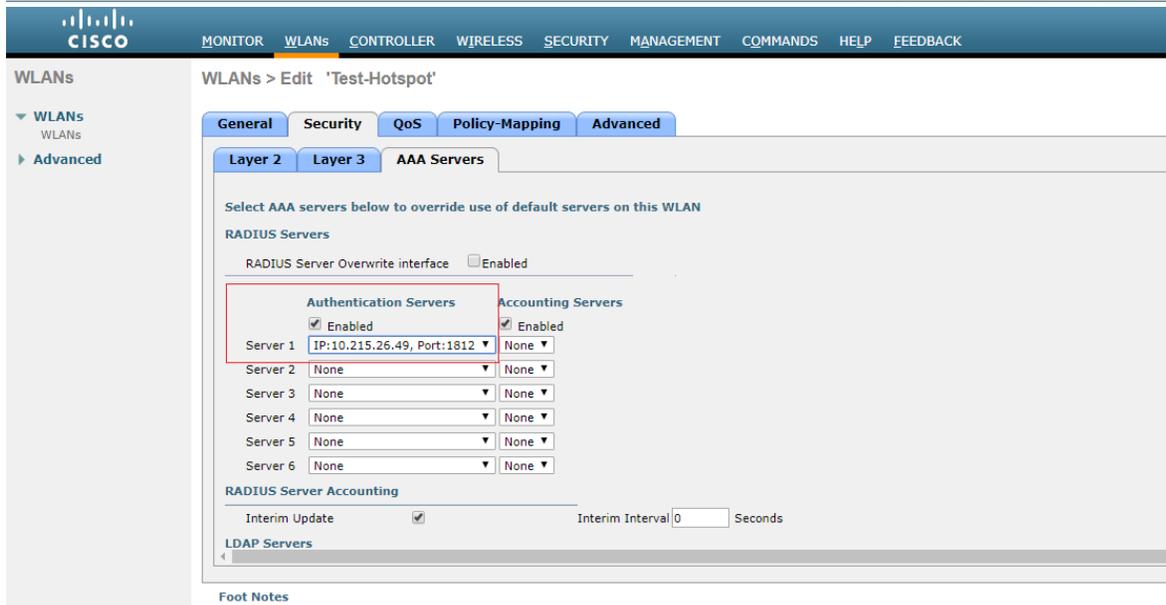
- Qua tab Security,
 - o Tại mục layer 2 chọn None và check Mac Filtering



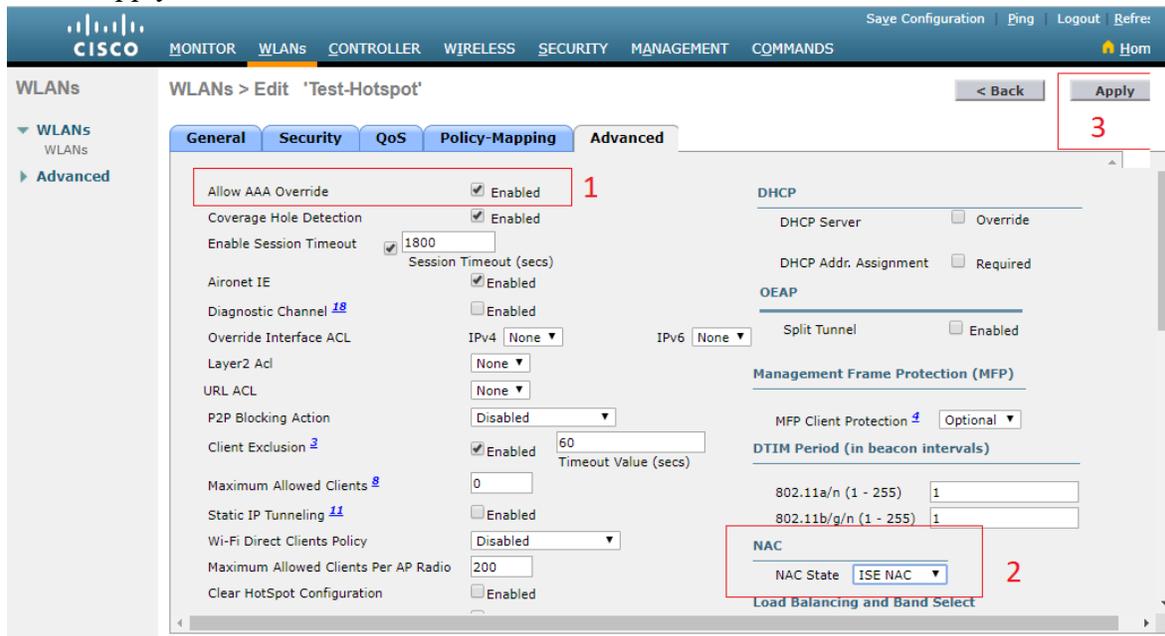
The screenshot shows the Cisco WLAN configuration interface for a profile named 'Test-Hotspot'. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The configuration includes:

- Layer 2 Security: None
- MAC Filtering:
- Fast Transition: Adaptive
- Fast Transition Over the DS:
- Reassociation Timeout: 20 Seconds

- o Tại mục layer 3 chọn None, qua mục AAA server chọn đến địa chỉ Authentication Server mà chúng ta đã cấu hình lúc này



- Qua tab Advanced -> Check Allow AAA override, tìm đến mục NAC -> chọn ISE NAC -> Apply để lưu cấu hình



- Tiếp tục cấu hình để AP có thể Redirect user khi kết nối đến SSID thì chúng ta cần cấu hình như sau: qua tab Wireless -> chọn AP đang kết nối -> qua tab Flexconnect -> Click vào External WebAuthentication ACLs

The screenshot shows the Cisco ISE configuration interface for AP1928. The 'WIRELESS' tab is selected. Under the 'FlexConnect' sub-tab, the 'External WebAuthentication ACLs' link is highlighted with a red box. Other visible elements include the 'WLAN Support' checkbox, 'Inheritance Level' set to 'Group-Specific', and 'FlexConnect Group Name' set to 'default-flex-group'.

- Tại mục Policy -> click Add ACL mà chúng ta đã tạo lúc này -> chọn Apply để lưu lại cấu hình

The screenshot shows the 'External WebAuth ACL Mappings' configuration page for AP1928. The 'Add' button under the 'WebAuth ACL' dropdown is highlighted with a red box. The page also shows a table for 'WLAN ACL Mapping' and a 'Policies' section with another 'Add' button highlighted.

- Bây giờ chúng ta sẽ tiến hành cấu hình Portal trên Cisco ISE để Guest xác thực khi kết nối vào SSID là Self-Register, chúng ta có thể sử dụng Portal default trên Cisco ISE hoặc ta có thể tạo mới 1 Portal khác trên Cisco ISE (ở đây mình sẽ sử dụng Portal default trên Cisco ISE)
- Đầu tiên đăng nhập vào Cisco ISE và Add thiết bị WLC vào Cisco ISE -> chọn Administration -> Chọn Network devices, sau khi cửa sổ hiện ra chọn ADD để tiến hành Add WLC vào Cisco ISE bao gồm Tên WLC (1), địa chỉ IP của WLC (2), sau đó click vào Radius Authentication Setting -> điền thông tin Shared Secret vào (lưu ý Shared Secret phải giống với WLC) -> chọn Submit để lưu cấu hình

- Tiếp theo, ta sẽ tạo Result cho việc Authentication trên Cisco ISE, ta làm như sau: Chọn Policy -> Result -> chọn Authentication Profiles -> Add

- Một cửa sổ mới hiện ra ta điền các thông tin cho Authentication như bên dưới, đầu tiên là Tên của profile này và Action Types là Access_Accept, tại mục Common Tasks -> tìm đến Web Redirection (CWA, MDM, NSP, CPP) -> chọn Centralized Web Auth -> tại ô ACL ta điền tên ACL mà chúng ta đã tạo ở WLC vào -> tại mục Value chọn Self-

Registered Guest Portal (default), tại mục này ta điền thông tin địa chỉ IP của Cisco ISE vào mục Static IP/ Host name/FQDN, sau đó chọn Submit để lưu cấu hình

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: Self-Register

Description: [Empty]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: [Empty]

Track Movement: [Empty]

Passive Identity Tracking: [Empty]

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth: [Empty] ACL: redirect-guest Value: Self-Registered Guest Portal

 Display Certificates Renewal Message

 Static IP/Host name/FQDN: 10.215.26.49

- Tiếp theo ta sẽ tạo Policy cho việc truy cập vào SSID Self-Register như sau: Chọn Policy -> Policy Set -> chọn biểu tượng Setting và click vào Insert new row above.

Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	🟢	Dot1x_Radius		Wired_802.1X	Default Network Access	120	⚙️	➡
	🟢	Default	Default policy set		Default Network Access	0	⚙️	➡

Insert new row above

- Ta có thể sửa tên cho Policy vừa tạo, ở đây mình đặt là Test-Self-Register-> Tại mục Condition chọn kiểu xác thực là Wireless_MAB, tại mục Allowed Protocol/ Server Sequence chọn Default Network Access -> chọn Save để lưu cấu hình sau đó chọn biểu tượng mũi tên > để tiếp tục cấu hình cho Policy này

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Dot1x_Radius		Wired_802.1X	Default Network Access	120	⚙️	➔
✓	Test-Self-Register		Wireless_MAB	Default Network Access		⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

- Tại mục Authentication Policy, tại mục USE chọn Internal Endpoint, tại mục option -> If User not found chọn Continue

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Endpoints	0	⚙️

Options:

- If Auth fail: REJECT
- If User not found: CONTINUE
- If Process fail: DROP

- Tiếp tục kéo xuống mục Authorization Policy, Click vào biểu tượng Setting -> Chọn Insert new row above để tạo ra cách thức xác thực cho SSID Self-Register
- Cấu hình như hình bên dưới, sau khi tạo xong các Row chọn Save để lưu lại cấu hình

The screenshot shows the 'Policy Elements' configuration page in Identity Services Engine. The 'Authorization Policy (3)' section is expanded, showing three rules:

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
Active	Guest-Access	AND Wireless_MAB Guest_Flow Radius Called-Station-ID ENDS_WITH Self-Register	PermiAccess	Select from list		
Active	Guest-Redirect	AND Wireless_MAB Radius Called-Station-ID ENDS_WITH Self-Register	Self-Register	Select from list		
Active	Default		DenyAccess	Select from list	0	

The 'Save' button is highlighted with a red box.

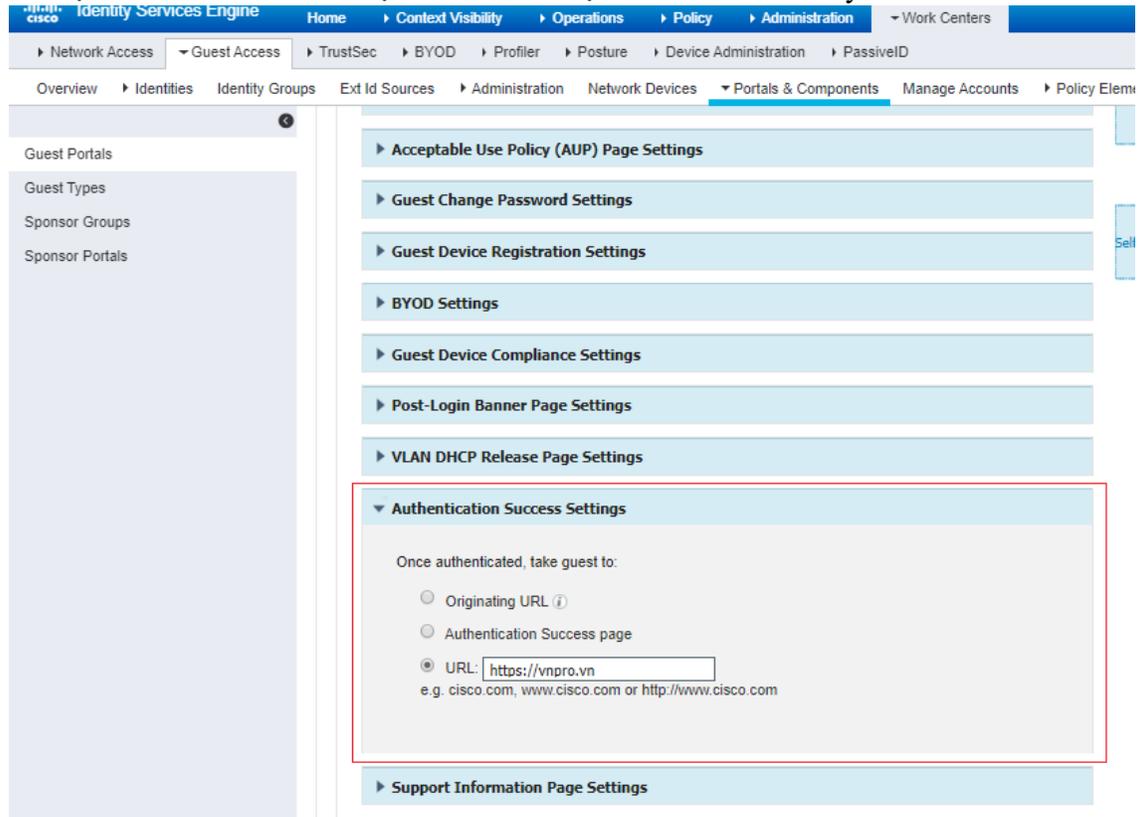
- Ta có thể cấu hình cho Portal Self-Register này tự động Redirect đến Website của doanh nghiệp của mình như sau: vào mục Work Centers -> Guest Access -> Portals & Components

The screenshot shows the 'Work Centers' menu in Identity Services Engine. The 'Guest Access' and 'Portals & Components' options are highlighted with red boxes.

- Tại mục Guest Portal -> Click vào Self-Register Guest Portal (default) để cấu hình cho Portal này

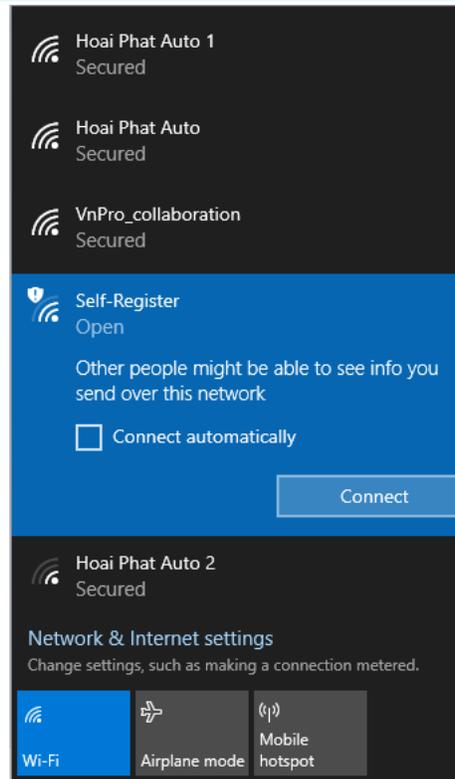
- Đầu tiên ta phải chắc chắn rằng Guest có thể đăng nhập thành công vào mạng sau khi tự đăng ký tài khoản, đảm bảo đã check vào *Allow guest to log in directly from the Self-Registration Success page*

- Tìm đến mục Authentication Success Settings và làm như hình bên dưới để Redirect tới một Website nào đó -> chọn Save để lưu lại cấu hình Portal này

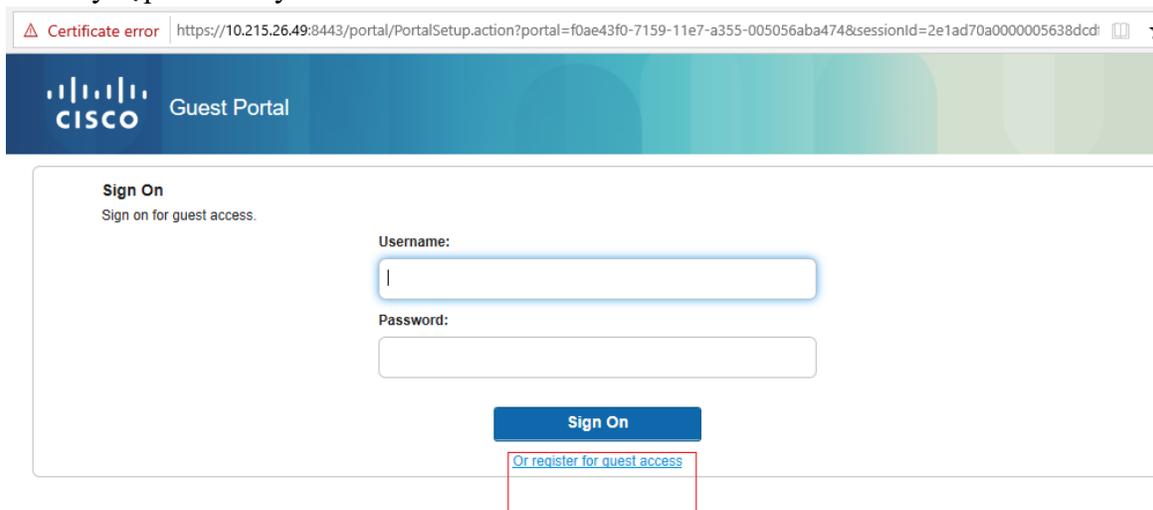


The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The left sidebar contains navigation options: Guest Portals, Guest Types, Sponsor Groups, and Sponsor Portals. The main content area is titled 'Portals & Components' and lists several settings categories: Acceptable Use Policy (AUP) Page Settings, Guest Change Password Settings, Guest Device Registration Settings, BYOD Settings, Guest Device Compliance Settings, Post-Login Banner Page Settings, and VLAN DHCP Release Page Settings. The 'Authentication Success Settings' category is expanded, showing the configuration for 'Once authenticated, take guest to:'. Three radio button options are visible: 'Originating URL (i)', 'Authentication Success page', and 'URL:'. The 'URL:' option is selected, and a text input field contains the value 'https://vnpro.vn'. Below the input field, a note reads 'e.g. cisco.com, www.cisco.com or http://www.cisco.com'. A 'Support Information Page Settings' category is also visible at the bottom.

- Kiểm tra SSID như sau, mở card mạng Wireless -> chọn SSID cần kết nối là Self-Register -> Connect để kết nối



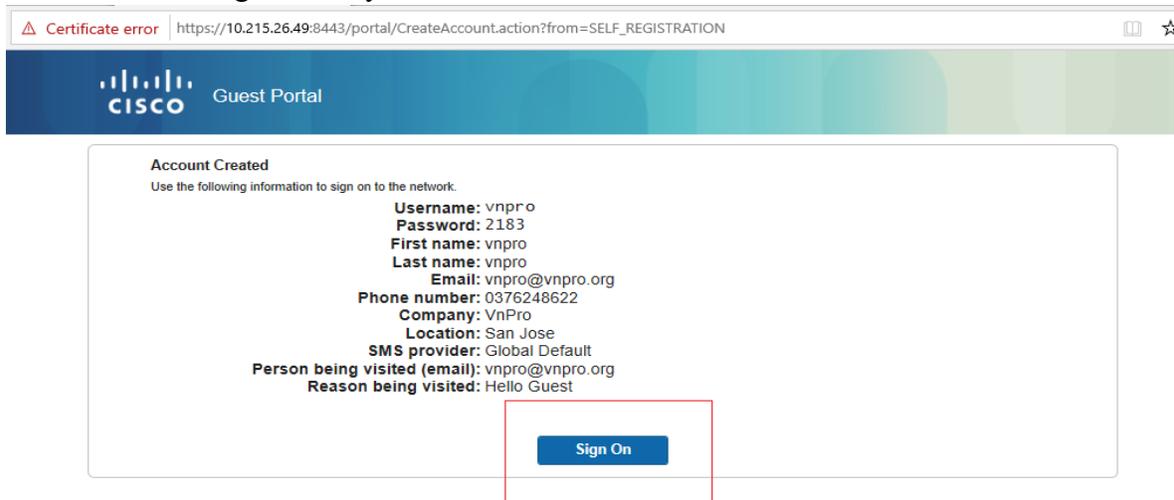
- Sau khi connect vào SSID này, Web browser sẽ truy cập đến Cisco để mở trang Portal trên Cisco ISE, người dùng ctrang Or register for guest access để có thể đăng kí tài khoản truy cập SSID này



- Tiếp theo người dùng sẽ tự điền tất cả các thông tin yêu cầu nhập bên dưới vào và chọn Register để sử dụng SSID này



- Sau khi Click Register, Portal sẽ thông báo rằng user đã đăng kí thành công, click Sign On để sử dụng SSID này



- Click Accept

Acceptable Use Policy × + ▾

error | https://10.215.26.49:8443/portal/SelfRegistrationSuccess.action?from=SELF_REGISTRATION_SUCCESS

 Guest Portal

Acceptable Use Policy
Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

- Click Continue

error | https://10.215.26.49:8443/portal/AupSubmit.action?from=AUP

 Guest Portal

Welcome Message
Click **Continue** to connect to the network.
You're very close to gaining network access.

- Web browser sẽ redirect đến Website mà chúng ta đã cấu hình lúc này