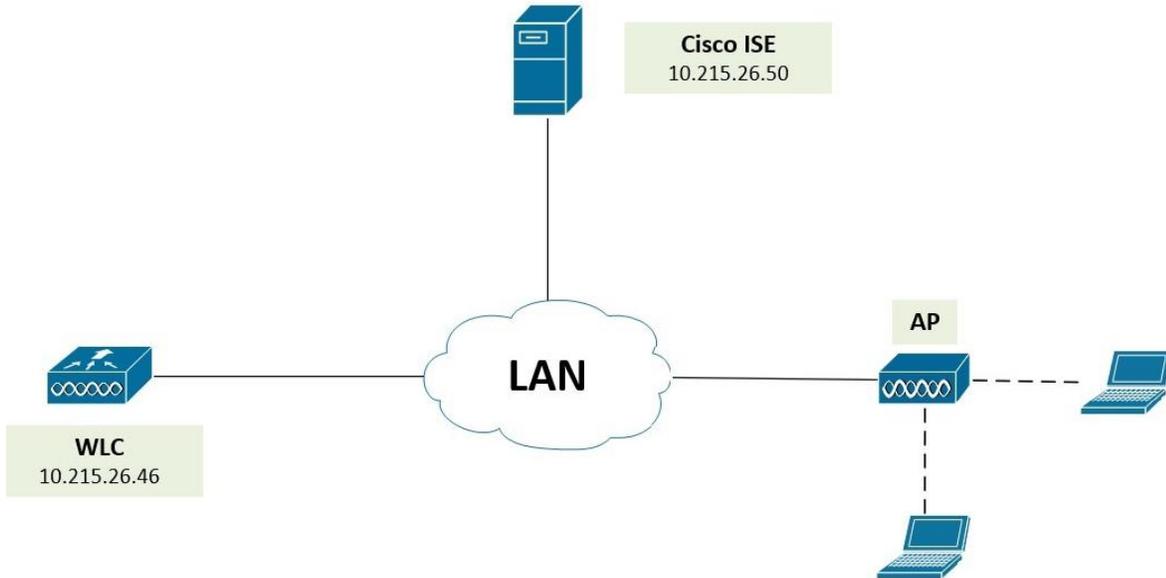


Lab – Wireless Guest Sponsored (Cấu hình Manual trên WLC và Cisco ISE)

1. Sơ đồ



2. Cấu hình trên WLC

- Đầu tiên ta phải cấu hình để AP Join vào WLC, 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

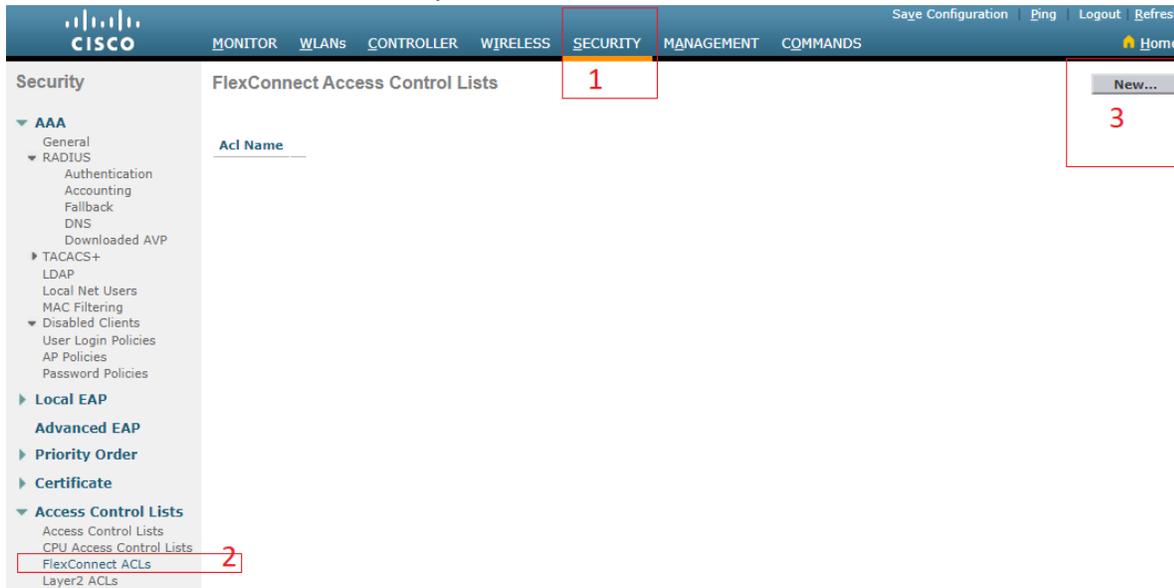
- Ta cấu hình khai báo Radius Server (Cisco ISE) với WLC như sau: vào mục Security -> AAA-> Radius -> Authentication -> New

- (1) Địa chỉ IP của Radius Server
- (2) 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
- (3) Enable Support CoA
- (4) Enable Network User

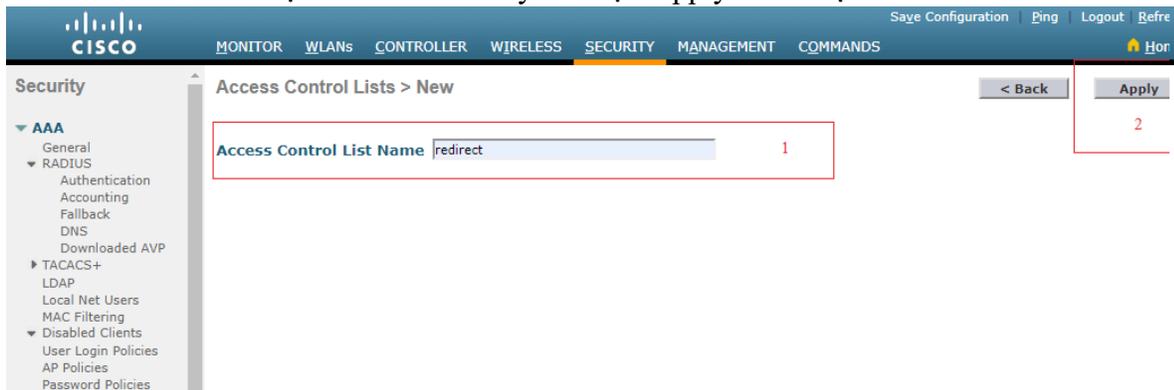
Chọn Apply để lưu cấu hình Authentication Server.

- Ta tiếp tục khai báo thông tin Accounting bao gồm các thông tin sau như sau: Tại RADIUS -> Click Accounting -> New

- 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



- 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

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

< Back Add New Rule

Security > Access Control Lists > Edit

General

Access List Name: redirect

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.215.26.50 / 255.255.255.255	Any	Any	Any	Any
2	Permit	10.215.26.50 / 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	Any	DNS	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any

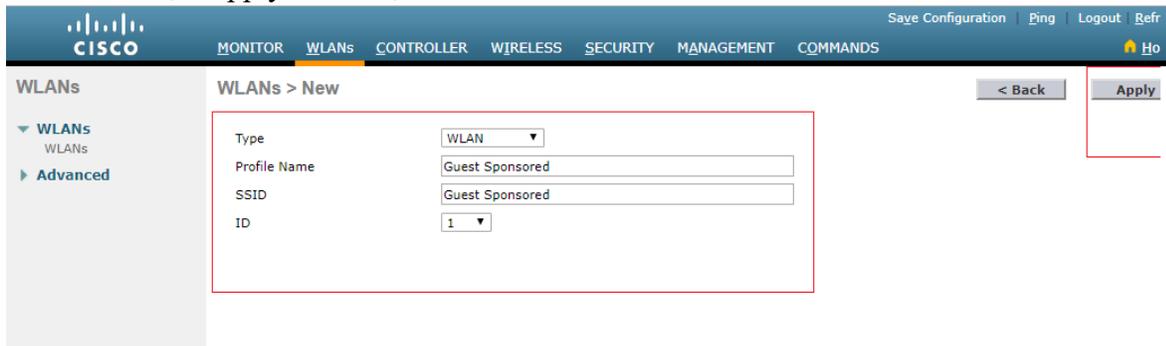
< Back Add New Rule

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

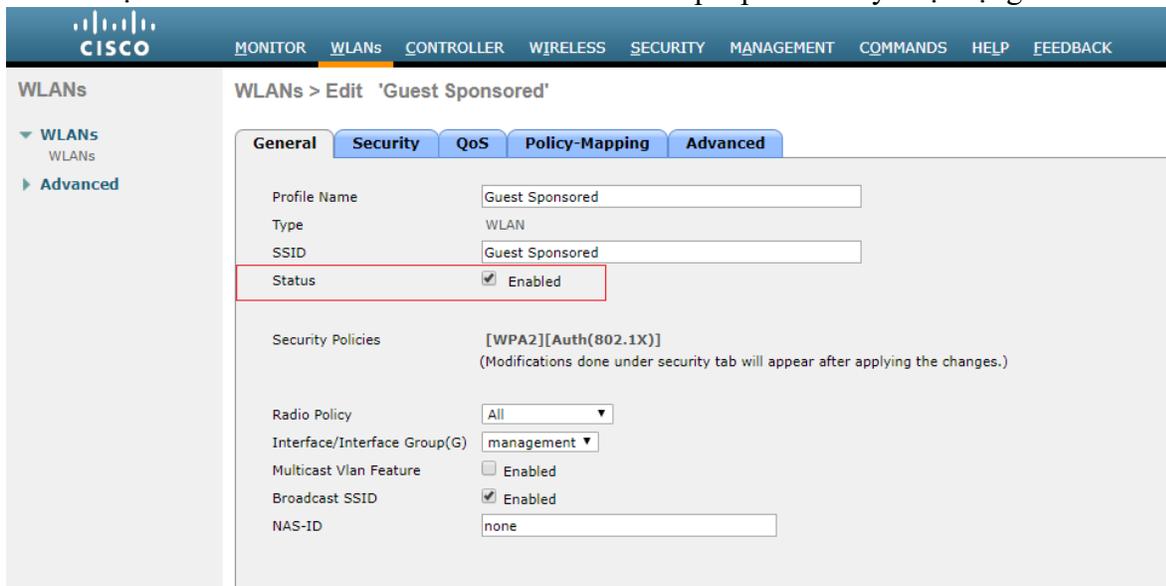
- Tiếp theo ta sẽ tạo SSID trên WLC: Chọn WLAN -> tại mục Create new chọn Go



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



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



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

WLANs > Edit 'Guest Sponsored'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security

MAC Filtering

Fast Transition

Fast Transition Adaptive

Over the DS

Reassociation Timeout Seconds

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

WLANs > Edit 'Guest Sponsored'

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	<input type="checkbox"/> None	<input type="checkbox"/> None
Server 3	<input type="checkbox"/> None	<input type="checkbox"/> None
Server 4	<input type="checkbox"/> None	<input type="checkbox"/> None
Server 5	<input type="checkbox"/> None	<input type="checkbox"/> None
Server 6	<input type="checkbox"/> None	<input type="checkbox"/> None

RADIUS Server Accounting

Interim Update Interim Interval Seconds

LDAP Servers

- 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

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

The screenshot shows the Cisco ISE configuration interface for AP1928 External WebAuth ACL Mappings. The left sidebar contains navigation options like Access Points, Radios, Advanced, Mesh, ATF, RF Profiles, FlexConnect Groups, OEAP ACLs, and Network Lists. The main content area is titled 'All APs > AP1928 > External WebAuth ACL Mappings' and includes a 'Back' button and an 'Apply' button. The configuration details include:

- AP Name: AP1928
- Base Radio MAC: 0c:d9:96:b0:3a:30
- WLAN ACL Mapping section with a 'WLAN Id' field set to 0 and a 'WebAuth ACL' dropdown set to 'redirect', with an 'Add' button below.
- A table with columns 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL'.
- Policies section with a 'Policy ACL' dropdown set to 'redirect' and an 'Add' button below.
- Policy Access Control Lists section.

- Bây giờ chúng ta sẽ tiến hành cấu hình Portal trên Cisco ISE để Guest xác thực khi kết nối vào SSID là Guest Sponsored, 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

Network Devices List > New Network Device

Network Devices

* Name 1

Description

IP Address / 2

IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings 3

RADIUS UDP Settings

Protocol

* Shared Secret 4

CoA Port

RADIUS DTLS Settings

- Để xác thực Guest Sponsored ta cần phải tạo Account cho User Guest để đăng nhập khi sử dụng phương thức xác thực này, ta làm như sau: Tại menu Administration -> Identities

Engine Home > Context Visibility > Operations > Policy > Administration 1 > Work Centers License Warning

System
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Backup & Restore
Admin Access
Settings

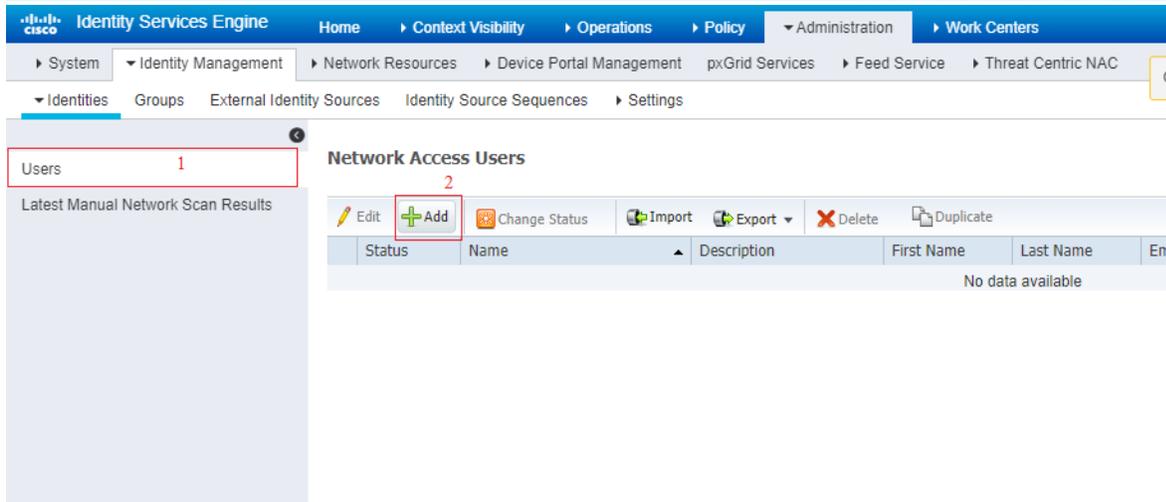
Identity Management 2
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings

Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Location Services

pxGrid Services
Feed Service
Profiler
Threat Centric NAC
Third Party Vendors

Device Portal Management
Blacklist
BYOD
Certificate Provisioning
Client Provisioning
Mobile Device Management
My Devices
Custom Portal Files
Settings

- Tại mục Users -> click Add để tạo mới User



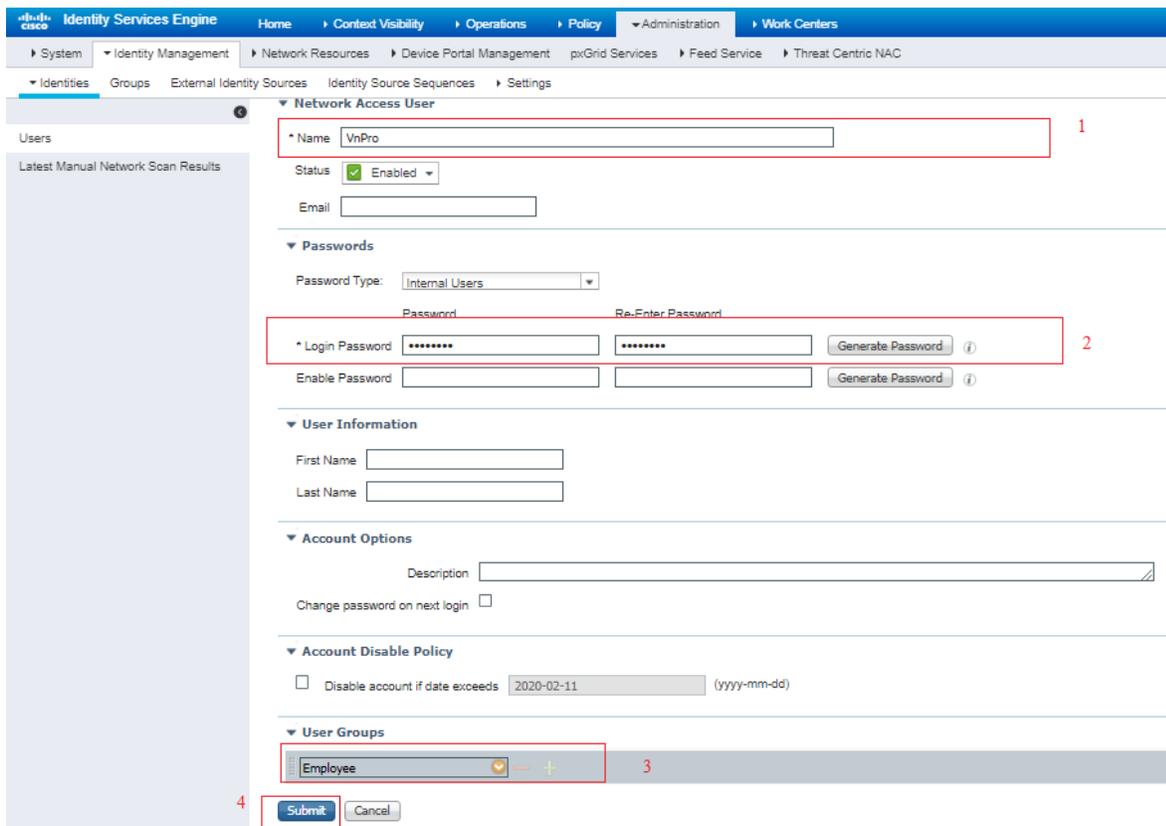
- Ta điền các thông tin sau:

(1) Tên đăng nhập

(2) Login Password: Password dùng để đăng nhập

(3) User Groups: Chọn Group Employee

Sau khi điền đầy đủ thông tin ta 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

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure th
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
PermitAccessInternet	Cisco	
Permit_dot1x_wireless	Cisco	
vlan10	Cisco	
vlan11	Cisco	
vlan5	Cisco	
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

- 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 Redirction (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 SponSored 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 Profile

Name: SponSored

Description: [Empty]

Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: [Unchecked]

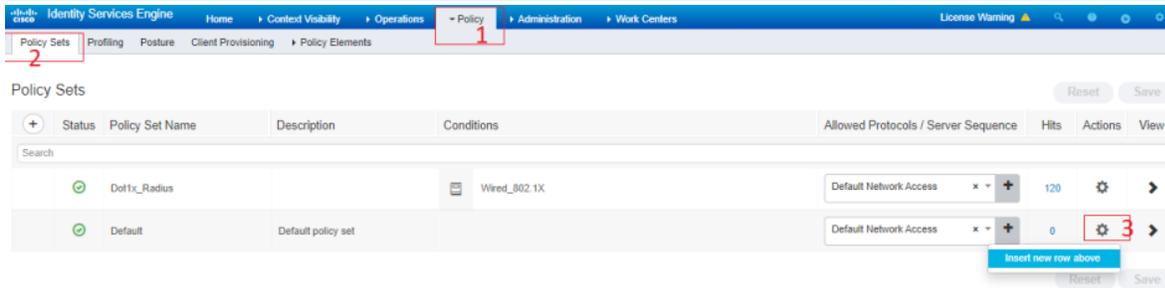
Track Movement: [Unchecked]

Passive Identity Tracking: [Unchecked]

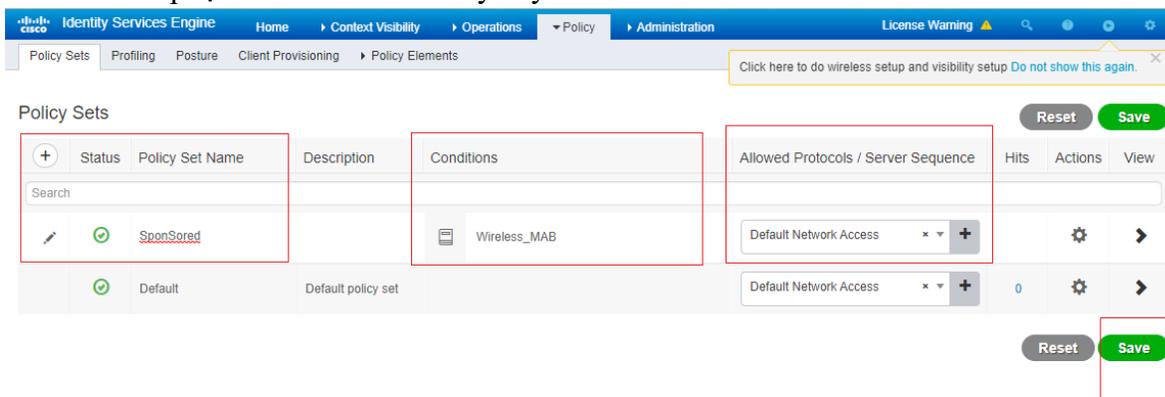
Common Tasks

- Web Redirection (CWA, MDM, NSP, CPP)
 - Centralized Web Auth
 - ACL: redirect
 - Value: SponSored Guest Portal (defau
- Display Certificates Renewal Message
- Static IP/Host name/FQDN: 10.215.26.50
- Suppress Profiler CoA for endpoints in Logical Profile

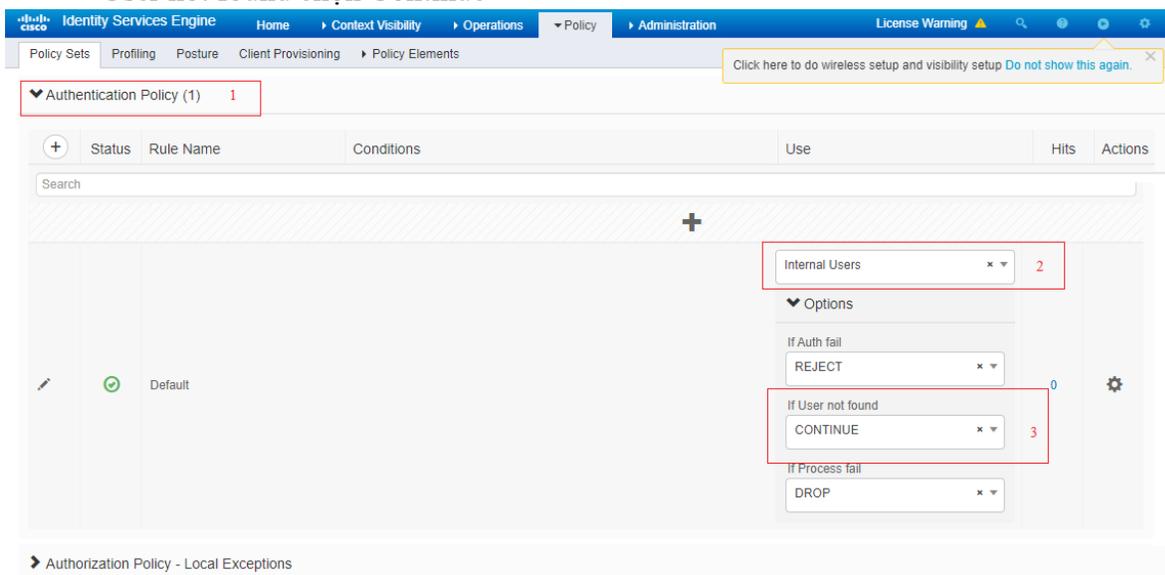
- Tiếp theo ta sẽ tạo Policy cho việc truy cập vào SSID Guest SponSored như sau: Chọn Policy -> Policy Set -> chọn biểu tượng Setting và click vào Insert new row above.



- Ta có thể sửa tên cho Policy vừa tạo, ở đây mình đặt là Sponsored -> 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



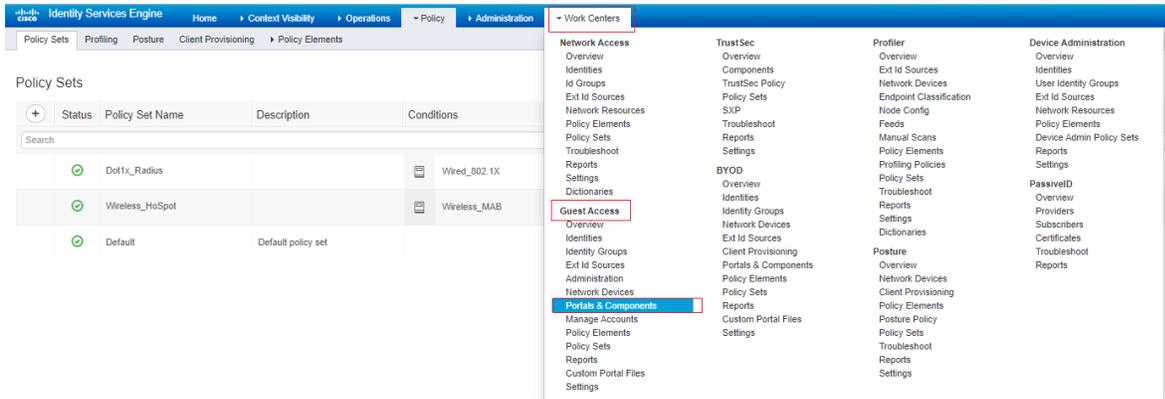
- Tại mục Authentication Policy, tại mục USE chọn Internal Users, tại mục option -> If User not found chọn Continue



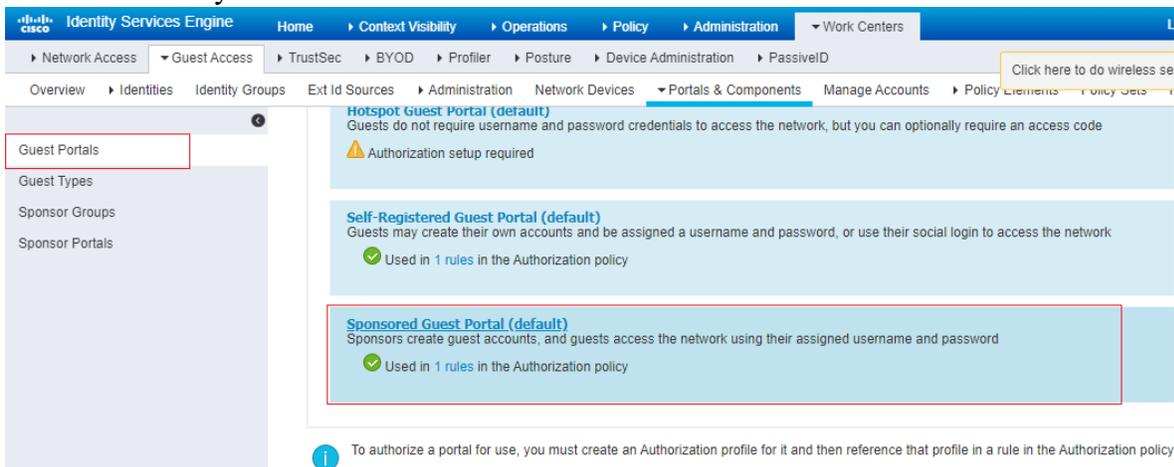
- Tiếp tục kéo xuống mục Authorization Policy, Click vào biểu tượng Setting -> Chọn Insert new row above để tạo ra cách thức xác thực cho SSID Guest Sponsored

- Cấu hình như hình bên dưới, sau khi tạo xong các Row chọn Save để lưu lại cấu hình

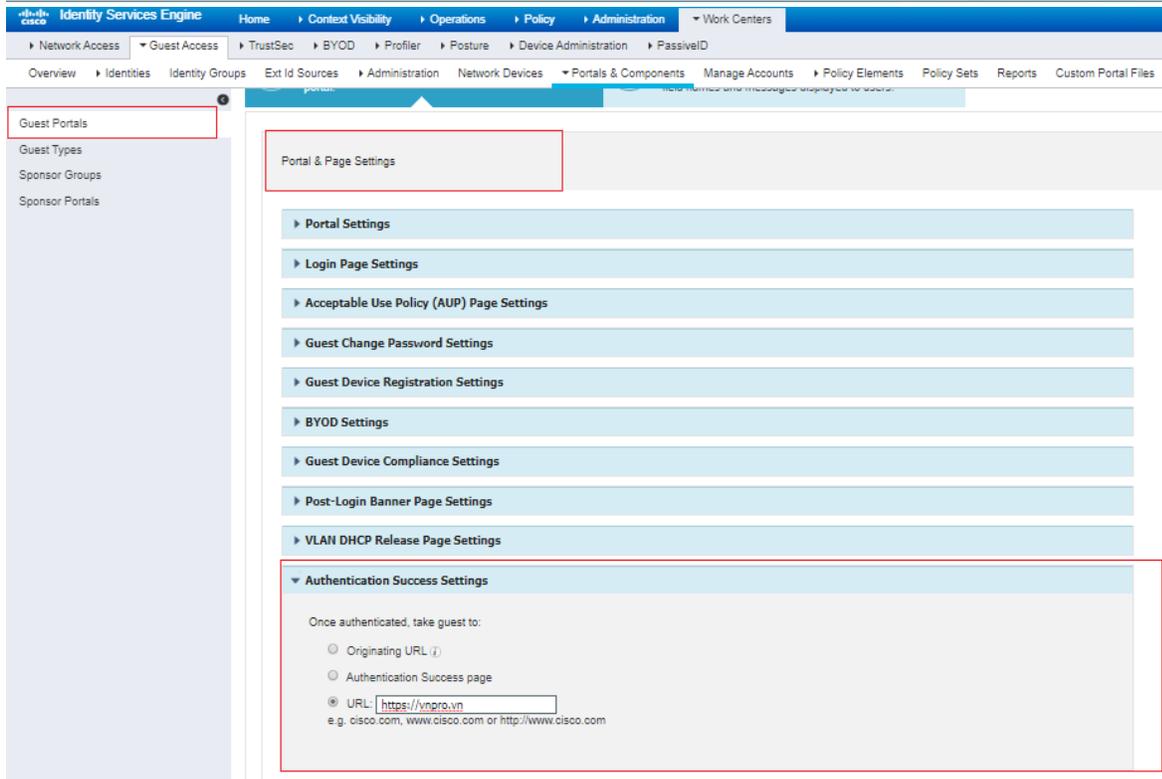
- Ta có thể cấu hình cho Portal SponSored này tự động Redirect đến Website của doanh nghiệp của mình như sau: vào mục Work Centers -> Guest Access -> Portals & Components



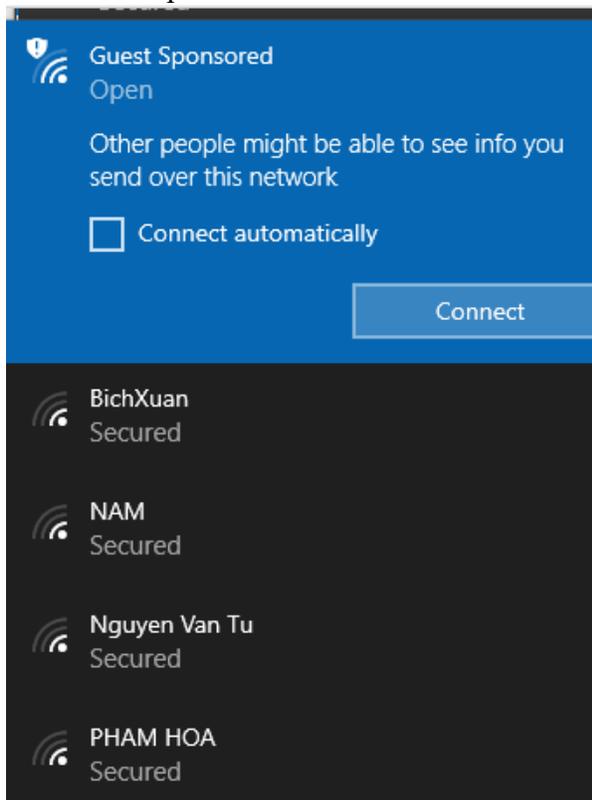
- Tại mục Guest Portal -> Click vào Sponsored Guest Portal (default) để cấu hình cho Portal này

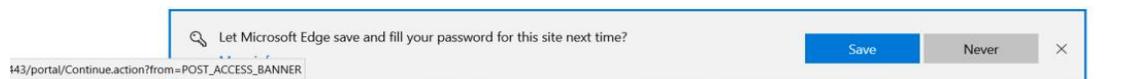
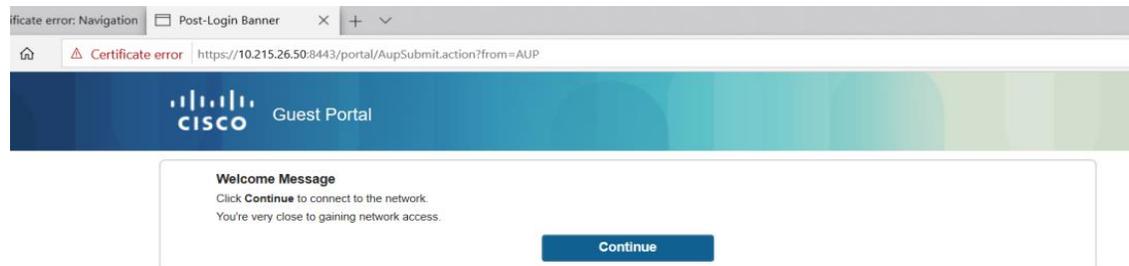
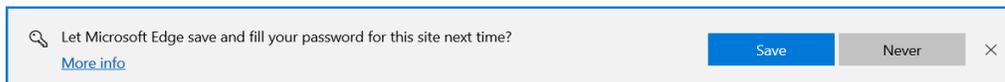
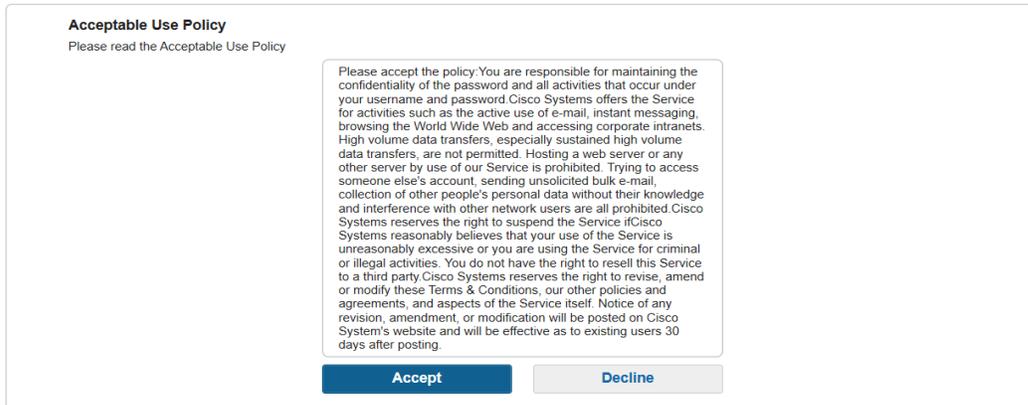
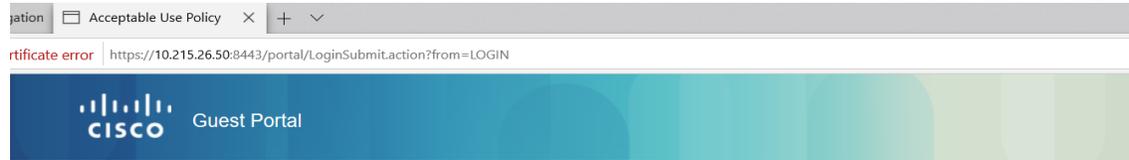


- Tìm đến mục Authentication Success Settings và làm như hình bên dưới để Redirect tới một Website nào đó -> chọn Save để lưu lại cấu hình Portal này



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





- Sau khi Click Continue, Web browser sẽ redirect đến Website mà chúng ta đã cấu hình lúc này



CÔNG TY TNHH TƯ VẤN VÀ DỊCH VỤ CHUYÊN VIỆT
TRUNG TÂM TIN HỌC VNPRO

ĐC: 276 - 278 Ung Văn Khiêm, P. Thanh Mỹ Tây, Tp. Hồ Chí Minh
ĐT: (028) 35124257 | Hotline: 0933427079 Email: vnpro@vnpro.org
