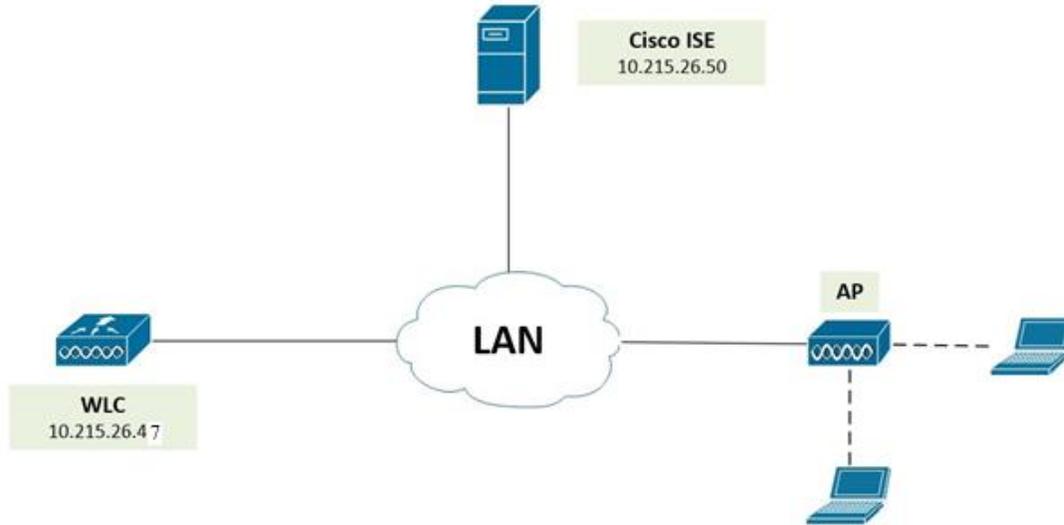


Lab – Cấu hình WIFI Guest sử dụng Hotspot Portal trên Cisco ISE (Wireless setup in ISE)

1. Sơ đồ



2. Thực hiện:

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. A 'License Warning' banner is visible. Below the navigation bar, there are several metrics cards: 'Total Endpoints' (14), 'Active Endpoints' (3), 'Authenticated Guests' (1), and 'BYOD Endpoints' (0). The 'AUTHENTICATIONS' section shows a donut chart with 'inter...oints: [80%]' and 'guest users: [20%]'. The 'NETWORK DEVICES' section shows a table with columns 'Device Name', 'Type', and 'Location', and a donut chart with segments for 'wcl09: [7.14%]', 'nad_1...26.48: [14.29%]', 'nad_1...26.45: [14.29%]', and 'nad_1...26.47: [64.29%]'. A red box labeled '1' highlights the 'Wireless Setup (BETA)' link in the top right corner, and another red box labeled '2' highlights the 'Wireless Setup (BETA)' link in the middle right area.

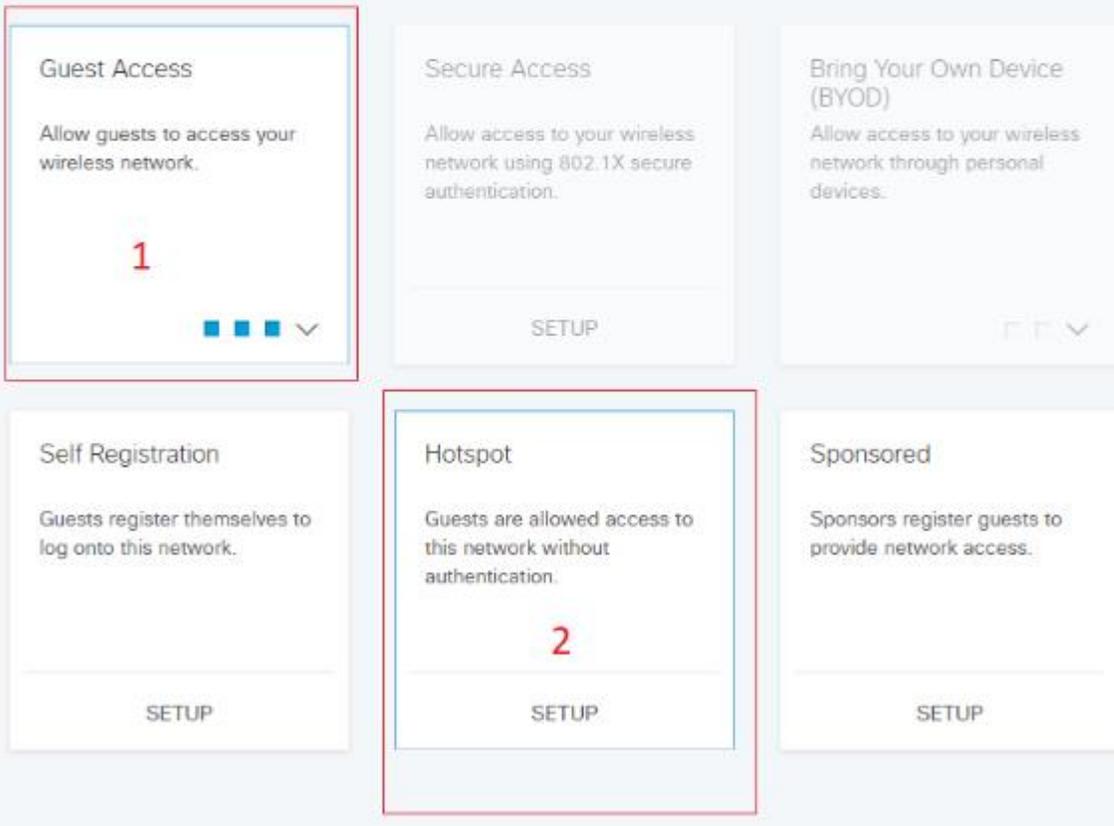
- Chọn Guest Access -> Hotspot



What can we help you set up today?

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

Please choose a feature:



The screenshot displays the Cisco ISE Wireless Setup interface. It features six selectable options, each with a description and a 'SETUP' button. The 'Guest Access' option is highlighted with a red box and a red number '1'. The 'Hotspot' option is also highlighted with a red box and a red number '2'. The other options are 'Secure Access', 'Bring Your Own Device (BYOD)', 'Self Registration', and 'Sponsored'.

- Tiếp theo click chuột vào REGISTER để add thông tin WLC, điền thông tin của WLC vào mục 2 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



Wireless Setup BETA

SETUP | HOTSPOT

Wireless LAN Controller

1

Register a Wireless LAN Controller.

WLC IP ADDRESS

2

10.215.26.47

USERNAME

3

WLC-08

PASSWORD

4

●●●●●●●●

SHARED SECRET

●●●●●●●●

Register

- Click Commit để tiếp tục



Wireless Setup BETA

SETUP | HOTSPOT

Wireless LAN Controller

1

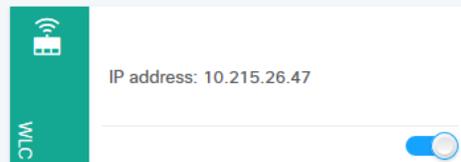
Choose or register a Wireless LAN Controller.

1/10 WLCs created

2



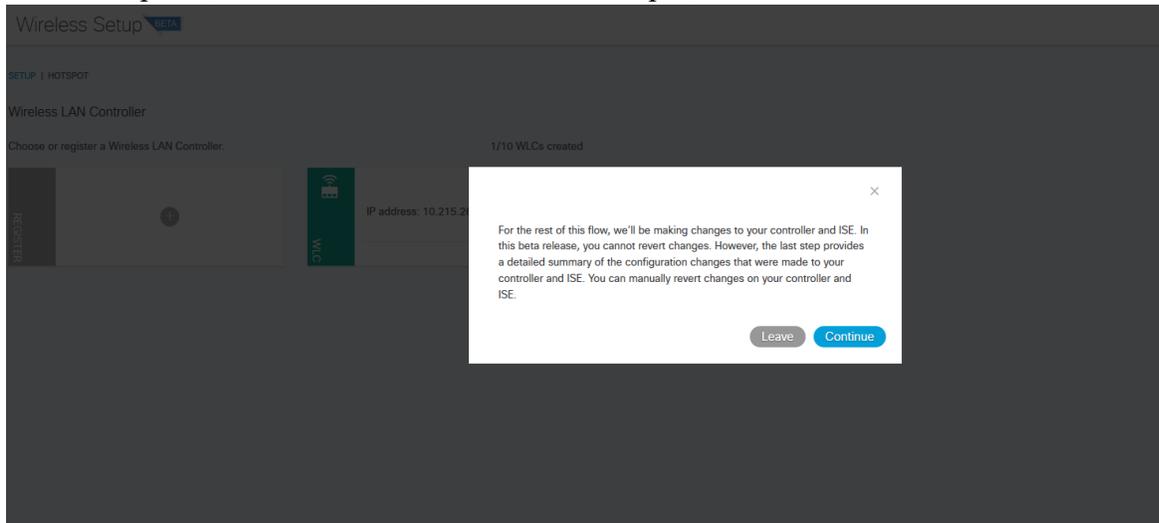
3



4

Commit

- Hộp thoại mới mở ra, chọn Continue để tiếp tục



- Tiếp theo khởi tạo SSID trên WLC bằng hotspot trên Cisco ISE bằng cách điền các thông tin bên dưới, bao gồm các thông tin sau:
 - (1) Wireless Network Name (SSID): Tên của SSID
 - (2) Default WLC Interface (VLAN): SSID này sử dụng Interface nào trên WLC
 - (3) Post Login Redirect: có 3 tùy chọn sau:
 - a. Redirect to success page: chuyển trang đến trang thông báo thành công
 - b. Redirect to original URL: chuyển đến URL chính
 - c. Redirect to custom URL: chuyển đến trang của khách hàng

Chọn ADD để hoàn tất và qua bước tiếp theo



Wireless Setup BETA

SETUP | HOTSPOT

Wireless Network

1

Add a Wireless network.

2

WIRELESS NETWORK NAME (SSID)

Hotspot-Test

3

DEFAULT WLC INTERFACE (VLAN)

management

4

POST LOGIN REDIRECT

Redirect to custom URL

http://vnpro.vn

Account Access Duration: 30 days

Add

- Chọn Commit để tiếp tục



Wireless Setup BETA

SETUP | HOTSPOT

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

3

4

ADD

+

WLAN

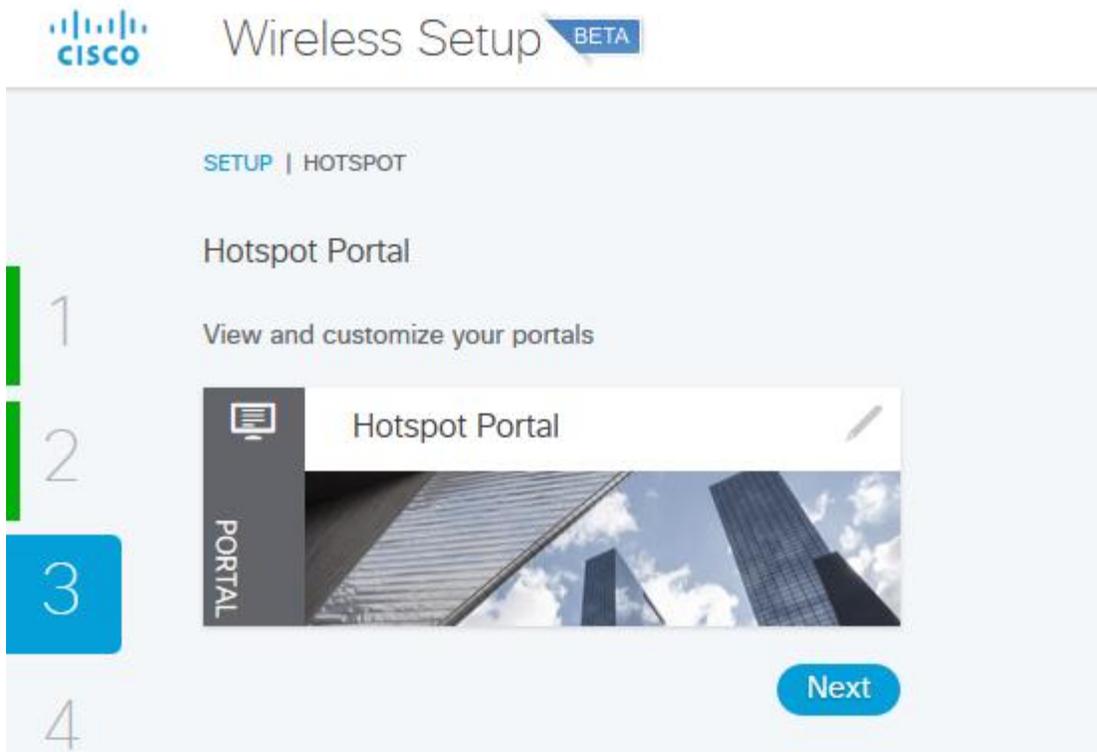
Hotspot-Test

Account Access Duration: 30 days

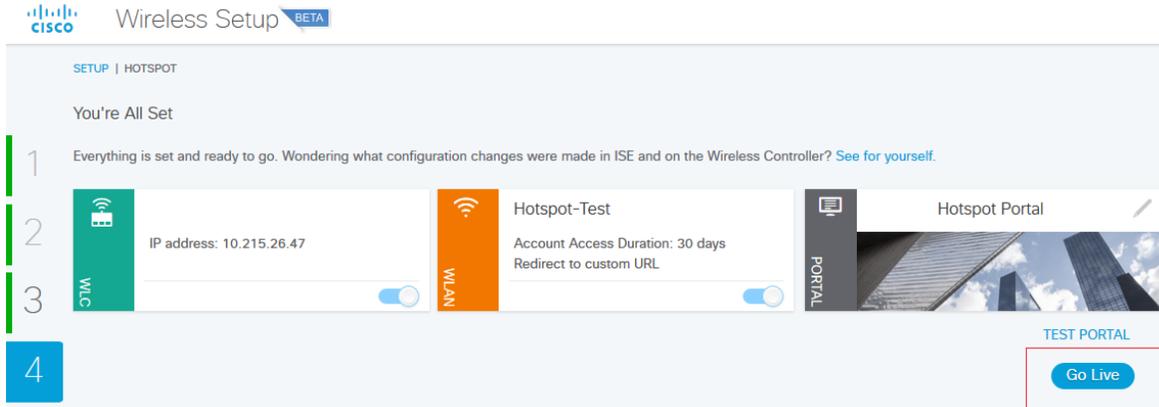
Redirect to custom URL

Commit

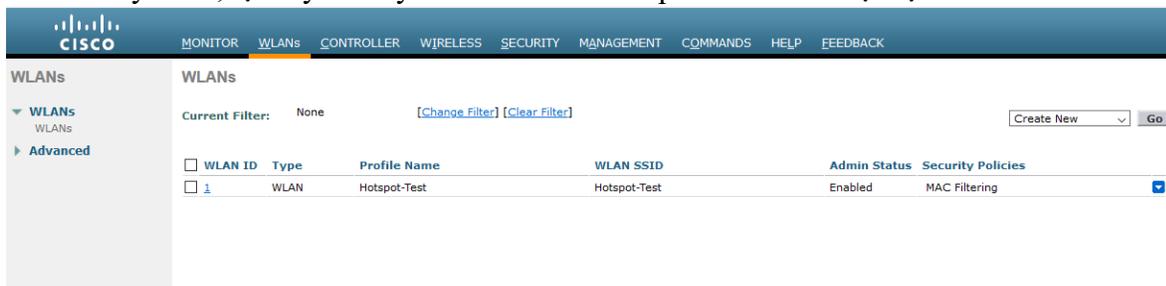
- Chọn Next để tiếp tục



- Chọn Go Alive để hoàn tất, có thể xem trước trang portal bằng cách click vào Test Portal



- Sau khi hoàn tất cấu hình, đăng nhập vào WLC để kiểm tra thông tin SSID đã được tạo hay chưa, tại đây ta thấy 1 SSID tên là Hotspot-Test đã được tạo trên WLC



- SSID đã được kích hoạt phát sóng

The screenshot shows the Cisco WLAN configuration interface for 'Hotspot-Test'. The 'General' tab is selected. The configuration includes: Profile Name: Hotspot-Test; Type: WLAN; SSID: Hotspot-Test; Status: Enabled; Security Policies: MAC Filtering (with a note that changes in the Security tab will appear after applying); Radio Policy: All; Interface/Interface Group(G): management; Multicast Vlan Feature: Enabled; Broadcast SSID: Enabled; NAS-ID: none.

- Chuyển qua tab Security: tại Layer 2 ta thấy phương thức bảo mật là None và check Mac-Filtering, Layer 3 None và đã có thông tin AAA serves

The screenshot shows the Cisco WLAN configuration interface for 'Hotspot-Test' in the Security tab, specifically the Layer 2 configuration. The configuration includes: Layer 2 Security: None; MAC Filtering: ; Fast Transition: Adaptive; Over the DS: ; Reassociation Timeout: 20 Seconds.

The screenshot shows the Cisco WLAN configuration interface for 'Hotspot-Test' in the Security tab, specifically the Layer 3 configuration. The configuration includes: Layer 3 Security: None.

The screenshot shows the 'AAA Servers' configuration page for the 'Hotspot-Test' WLAN. The 'Authentication Servers' and 'Accounting Servers' sections are highlighted with a red box. Both sections have 'Server 1' configured with IP: 10.215.26.50 and Port: 1812, and are checked as 'Enabled'. Other servers (Server 2-6) are set to 'None'. The 'RADIUS Server Accounting' section has 'Interim Update' checked and 'Interim Interval' set to 0 seconds.

The screenshot shows the 'Policy-Mapping' configuration page for the 'Hotspot-Test' WLAN. The 'Allow AAA Override' checkbox is checked and highlighted with a red box. Other settings include 'Coverage Hole Detection' (checked), 'Aironet IE' (checked), 'Diagnostic Channel' (unchecked), 'Override Interface ACL' (IPv4: None, IPv6: None), 'Layer2 Acl' (None), 'URL ACL' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (checked, 60s timeout), 'Maximum Allowed Clients' (0), 'Static IP Tunneling' (unchecked), and 'Wi-Fi Direct Clients Policy' (Disabled). On the right, 'DHCP Server' is unchecked, 'DHCP Addr. Assignment' is checked, 'OEAP Split Tunnel' is unchecked, 'MFP Client Protection' is set to 'Optional', and 'DTIM Period' is set to 1 for both 802.11a/n and 802.11b/g/n. The 'NAC State' is set to 'ISE NAC' and is highlighted with a red box.

Tất cả các thông tin bao gồm SSID, các phương thức bảo mật cũng như cấu hình đến Radius Server đề đã có thông tin trên WLC

- 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 with the 'SECURITY' tab selected. The left sidebar shows the navigation menu with 'FlexConnect ACLs' highlighted. The main content area is titled 'FlexConnect Access Control Lists' and contains a table with one entry: 'ACL_WEBAUTH_REDIRECT'.

- Ngoài những cấu hình đã được cài đặt sẵn trên WLC từ WLC, ta cá hình thêm trên WLC để Client có thể đăng nhập 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 with the 'WIRELESS' tab selected. The left sidebar shows the navigation menu with 'FlexConnect Groups' highlighted. The main content area is titled 'All APs > Details for 3602-1928' and contains the 'FlexConnect' configuration page. The 'PreAuthentication Access Control Lists' section is highlighted, showing 'External WebAuthentication ACLs' selected.

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

The screenshot shows the Cisco ISE configuration interface for 'External WebAuth ACL Mappings'. The left sidebar contains navigation options like 'Access Points', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', 'FlexConnect Groups', 'OEAP ACLs', 'Network Lists', and 'Media Stream'. The main content area shows configuration for AP Name '3602-1928' and Base Radio MAC '0c:d9:96:b0:3a:30'. Under 'WLAN ACL Mapping', the 'WebAuth ACL' is set to 'ACL_WEBAUTH_REDIRECT'. Below this, a table lists 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL'. Under 'Policies', the 'Policy ACL' is also set to 'ACL_WEBAUTH_REDIRECT'. Red boxes highlight the 'Apply' button at the top right, the 'Add' button under 'WebAuth ACL', and the 'Add' button under 'Policy ACL'.

- 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

The screenshot shows the Cisco ISE 'Policy Elements' configuration page. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is expanded, and 'Policy Elements' is selected. The left sidebar shows 'Authentication' and 'Authorization' sections, with 'Authorization Profiles' highlighted. The main content area is titled 'Standard Authorization Profiles' and lists several profiles: 'Blackhole_Wireless_Access', 'Cisco_IP_Phones', 'Cisco_Temporal_Onboard', 'Cisco_WebAuth', 'NSP_Onboard', 'Non_Cisco_IP_Phones', 'WS_Hotspot-Test_HotspotPortal_Profile', 'DenyAccess', and 'PermitAccess'. Red boxes highlight the 'Policy' menu item (1), the 'Policy Elements' dropdown (2), the 'Authorization Profiles' sidebar item (3), and the 'WS_Hotspot-Test_HotspotPortal_Profile' row (4).

Tiếp theo: ta giữ nguyên thông tin mặc định ban đầu, trong mục Common Tasks -> tìm đến mục Web Redirection (CWA, MDM, NSP, CPP) -> check vào ô Static IP/Host name/ FQDN và điền thông của Cisco Ise vào để Client mở được trang xác thực nằm trên Cisco ISE, các thông tin còn lại để nguyên theo mặc định -> chọn Save để lưu lại cấu hình

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > WS_Hotspot-Test_HotspotPortal_Profile

Authorization Profile

* Name: WS_Hotspot-Test_HotspotPorta

Description: Wireless Setup generated Authorization Profile for portal: WS_Hotspot-Test_HotspotPortal

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Hot Spot ACL: ACL_WEBAUTH_REDIRECT Value: WS_Hotspot-Test_HotspotPc

Display Certificates Renewal Message

Static IP/Host name/FQDN: 10.215.26.50

Suppress Profiler CoA for endpoints in Logical Profile

- Ta tìm đến mục Portal để kiểm tra thông tin trang Portal đã tạo ra sẽ sử dụng Policy nào: Chọn Work Center -> Portals & Components -> Guest Portals, tìm đến Portal có tên khớp với SSID vừa tạo lúc nãy -> Click vào 1 rule để kiểm tra xem Portal này được sử dụng ở rule nào (mặc định là Rule Default Policy)

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components Manage Account

Guest Portals

Guest Types

Sponsor Groups

Sponsor Portals

Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest :

Create Edit Duplicate Delete

Self-Registered Guest Portal (default)
Guests may create their own accounts and be assigned a username and password, or use their s
⚠ Authorization setup required

Sponsored Guest Portal (default)
Sponsors create guest accounts, and guests access the network using their assigned username
⚠ Authorization setup required

WS_Hotspot-Test_HotspotPortal
Wireless Setup hotspot Portal
✔ Used in 1 rules in the Authorization policy

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

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	Default	Default policy set		Default Network Access	203	⚙️	➔

- Tiếp theo ta cần cấu hình lại Policy này như sau: Chọn Internal Endpoint -> check vào option -> tại mục If User npt found -> chọn Continue -> Click Save để lưu cấu hình

Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Default	Default policy set		Default Network Access	203

▼ Authentication Policy (1)

+	Status	Rule Name	Conditions	Use	Hits	Actions
✎	✔	Default		Internal Endpoints Options If Auth fail: REJECT If User not found: CONTINUE If Process fail: DROP	17	⚙️

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

- Kiểm tra SSID như sau:

Click vào biểu tượng wifi, chọn SSID để kết nối là Hotspot-Test -> Connect

- Webbrowser hiển thị ra, ta chọn detail -> go on to the webpage để tiếp tục truy cập vào trang Portal



This site is not secure

This might mean that someone's trying to trick you or steal any information that you send to the server. You should close this site immediately.

[Go to your Start page](#)

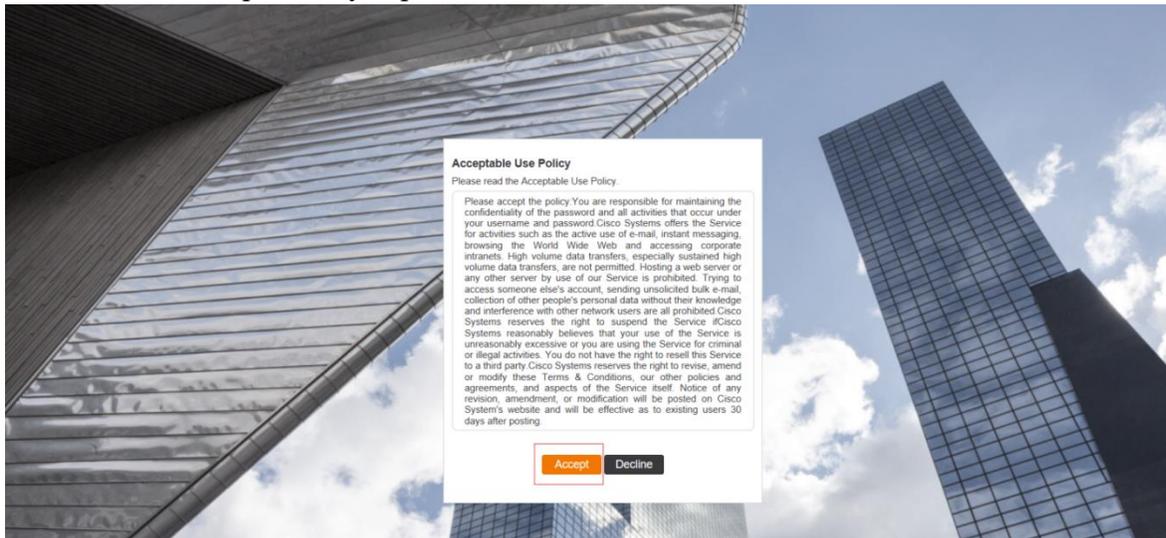
Details

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

[Go on to the webpage](#) (Not recommended)

- Click Accept để truy cập



Sau khi Accept truy cập, Browser sẽ Redirect đến trang Web mà chúng ta cấu hình trỏ đến



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
