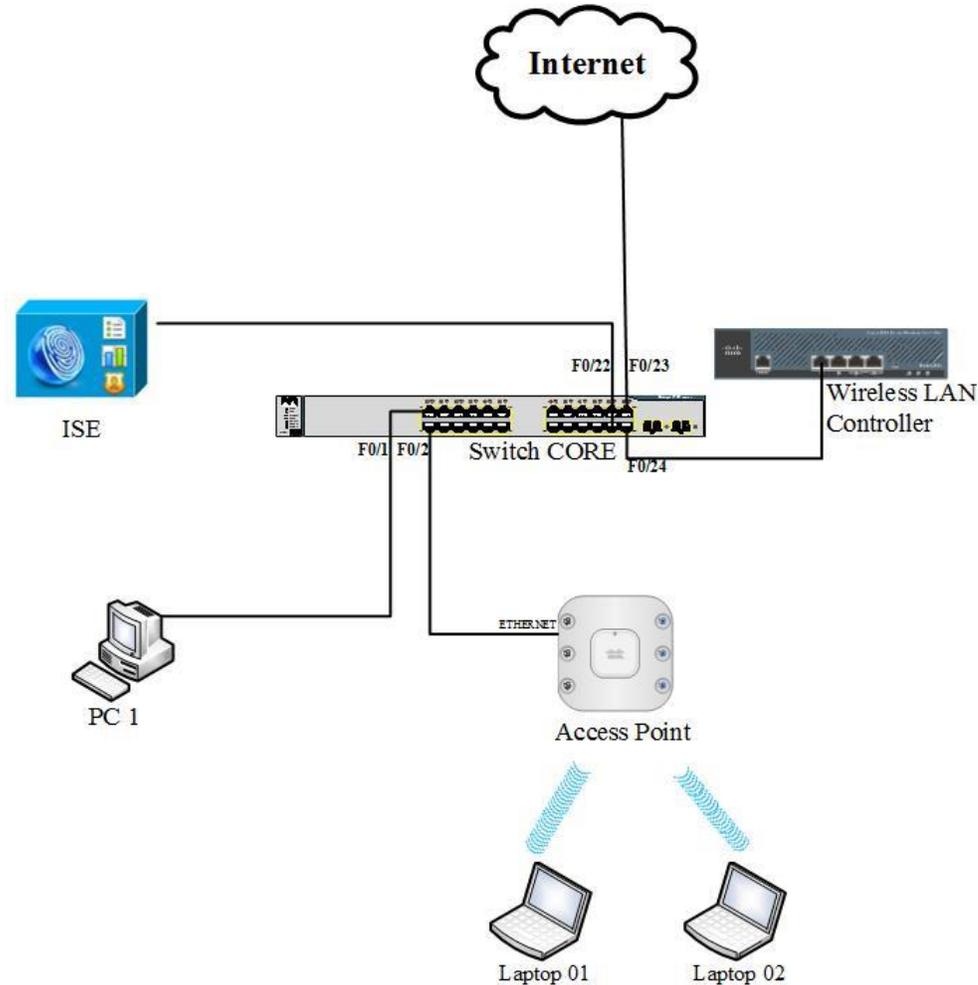


Lab – Xác thực Wireless 802.1x sử dụng Cisco ISE

I. Sơ đồ



II. Thực hiện:

1. Cấu hình trên vWLC:

- Cấu hình WLC trở đến Radius server trên Cisco ISE, mục Security -> RADIUS-> Authentication chọn NEW để khởi tạo



- Điền thông tin địa chỉ IP của Cisco ISE và điền Shared Secret (Lưu ý: Shared Secret phải giống nhau trên Cisco ISE và WLC)

Security

RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address(Ipv4/Ipv6) 10.215.26.50 1

Shared Secret Format ASCII

Shared Secret ***** 2

Confirm Shared Secret ***** 2

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for CoA Disabled

Server Timeout 2 seconds

Network User Enable

Management Enable

Management Retransmit Timeout 2 seconds

Tunnel Proxy Enable

IPSec Enable

- Tạo SSID như sau:

WLANs

WLANs 2

Advanced

WLANs

Current Filter: None [Change Filter] [Clear Filter]

Create New Go 3

| WLAN ID | Type | Profile Name | WLAN SSID | Admin Status | Security Policies |
|---------|------|--------------|-----------|--------------|-------------------|
|---------|------|--------------|-----------|--------------|-------------------|

WLANs > New

Type WLAN

Profile Name Test_ISE 1

SSID Wireless-ISE 2

ID 1

< Back Apply 3

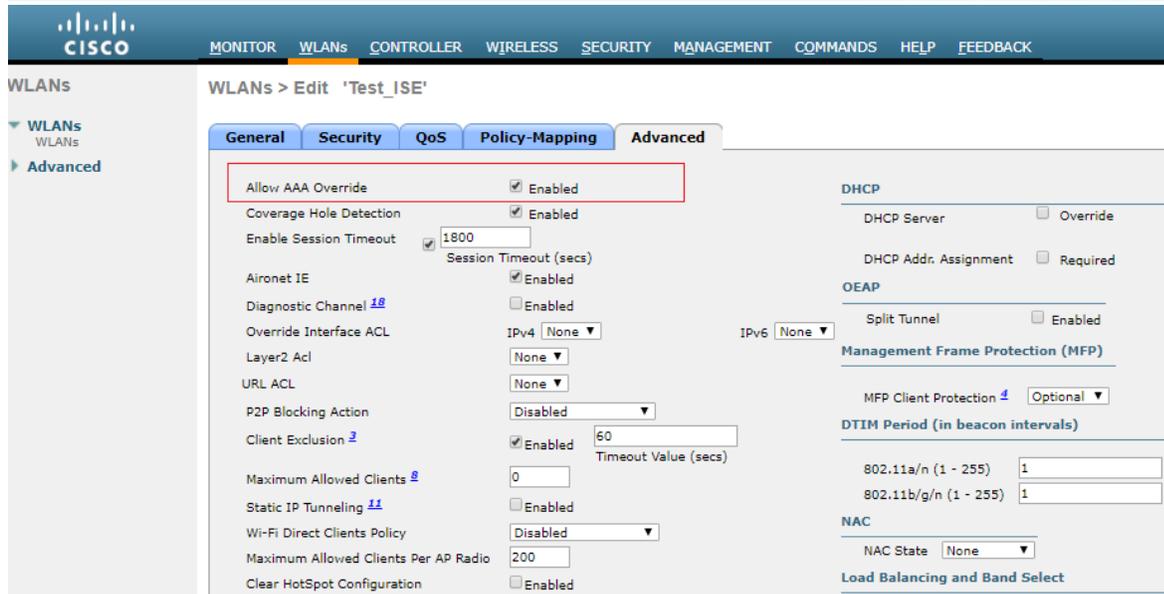
- Tiếp tục qua tab Security, tại mục Layer 2 chọn phương thức xác thực WPA + WPA2, tại mục Authentication key chọn 802.1x

The screenshot shows the Cisco WLAN configuration interface for 'Test_ISE'. The 'Security' tab is active, and the 'Layer 2' sub-tab is selected. A red box labeled '1' highlights the 'Layer 2 Security' dropdown menu set to 'WPA+WPA2'. Below it, 'MAC Filtering' is disabled. The 'Fast Transition' section has 'Fast Transition Over the DS' checked and 'Reassociation Timeout' set to 20 seconds. The 'Protected Management Frame' section has 'PMF' set to 'Disabled'. The 'WPA+WPA2 Parameters' section has a red box labeled '2' around the 'WPA2 Policy' (checked), 'WPA2 Encryption' (checked, with 'AES' selected), and 'OSEN Policy' (unchecked). The 'Authentication Key Management' section has a red box labeled '3' around the '802.1X' checkbox, which is checked and labeled 'Enable'.

- Tiếp tục qua tab AAA Servers chọn IP của CISCO ISE, chọn Apply để lưu cấu hình

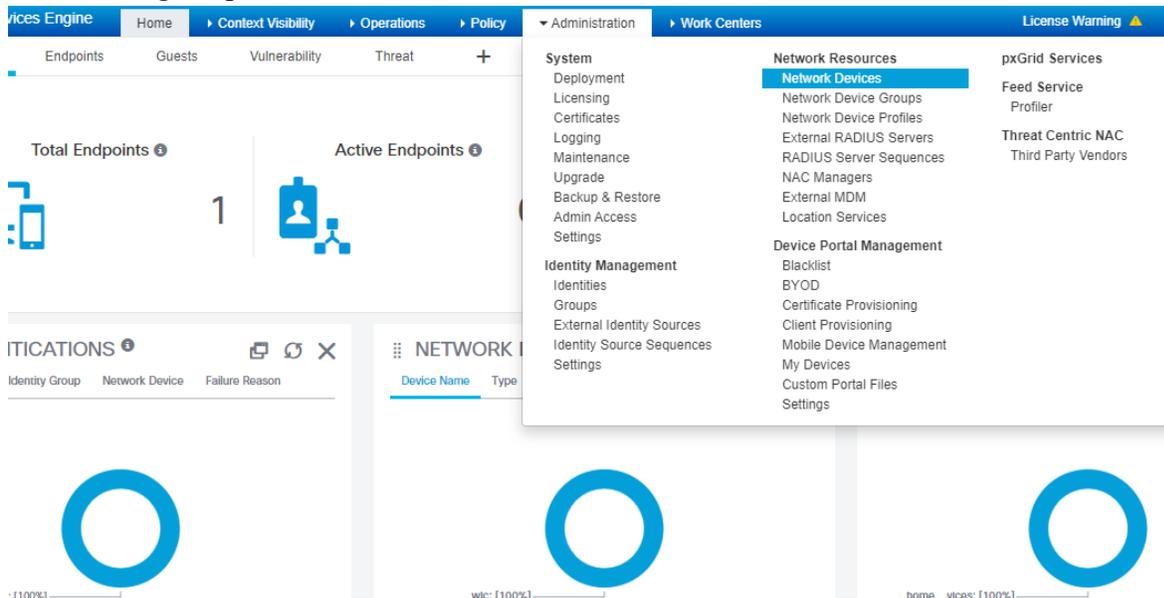
The screenshot shows the Cisco WLAN configuration interface for 'Test_ISE' with the 'AAA Servers' sub-tab selected. A red box highlights the 'Authentication Servers' section where 'Server 1' is set to 'IP:10.215.26.50, Port:1812'. The 'RADIUS Servers' section has 'RADIUS Server Overwrite interface' disabled. The 'Accounting Servers' section has 'Accounting Servers' checked and 'EAP Parameters' disabled. The 'RADIUS Server Accounting' section has 'Interim Update' checked and 'Interim Interval' set to 0 seconds.

- Qua tab Advanced chọn Allow AAA override



2. Cấu hình trên Cisco ISE:

- Đăng nhập vào Cisco ISE, Tại menu Administration -> Network Devices



- Chọn Add để add devices vào Cisco ISE

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar has 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices' and contains a toolbar with 'Edit', 'Add', 'Duplicate', 'Import', 'Export', 'Generate PAC', and 'Delete'. Below the toolbar is a table with columns for Name, IP/Mask, Profile Name, Location, and Type. The table is currently empty, showing 'No data available'. A red box highlights the 'Add' button in the toolbar.

- Ta điền tên của thiết bị và địa chỉ IP của thiết bị cần Add

The screenshot shows the 'New Network Device' form in the Cisco ISE interface. The form is titled 'Network Devices List > New Network Device'. It contains several input fields: 'Name' (filled with 'WLC'), 'Description', 'IP Address' (filled with '10.215.26.48 / 32'), 'Device Profile' (set to 'AlcatelWired'), 'Model Name', 'Software Version', 'Network Device Group', 'Location' (set to 'All Locations'), 'IPSEC' (set to 'Is IPSEC Device'), and 'Device Type' (set to 'All Device Types'). Each of these fields has a 'Set To Default' button next to it. A red box labeled '1' highlights the 'Name' field, and another red box labeled '2' highlights the 'IP Address' field. A note below the form states: 'IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected'.

- Tiếp tục click vào RADIUS Authentication Settings, điền vào Shared Secret như đã điền ở WLC, chọn Submit để lưu cấu hình

Network Devices

Default Device

Device Security Settings

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: [masked] Show

CoA Port: [] Set To Default

RADIUS DTLS Settings

DTLS Required: DTLS Required

Shared Secret: radius/dtls

CoA Port: [] Set To Default

Issuer CA of ISE Certificates for CoA: Select if required (optional)

DNS Name: []

General Settings

- Tiếp tục, ta tạo Username và password để đăng nhập vào SSID, vào Administration -> Identities

Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade

Backup & Restore

Admin Access

Settings

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

Device Portal Management

Blacklist

BYOD

Certificate Provisioning

Client Provisioning

Mobile Device Management

My Devices

Custom Portal Files

Settings

pxGrid Services

Feed Service

Profiler

Threat Centric NAC

Third Party Vendors

- Chọn Add để tạo username và password

Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

| Status | Description | First Name | Last Name |
|-------------------|-------------|------------|-----------|
| No data available | | | |

- Điền thông tin username và password cần tạo, tại mục user group -> ALL_accounts -> chọn Submit để lưu cấu hình

- Tiếp tục ta tạo policy cho 802.1x, vào Policy -> Results

- Ta làm như sau:

Standard Authorization Profiles
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

| Name | Profile | Description |
|--|---------|--|
| <input type="checkbox"/> Blackhole_Wireless_Access | Cisco | Default profile used to blacklist wireless devices. Ensure |
| <input type="checkbox"/> Cisco_IP_Phones | Cisco | Default profile used for Cisco Phones. |
| <input type="checkbox"/> Cisco_Temporal_Onboard | Cisco | Onboard the device with Cisco temporal agent |
| <input type="checkbox"/> Cisco_WebAuth | Cisco | Default Profile used to redirect users to the CWA portal. |
| <input type="checkbox"/> NSP_Onboard | Cisco | Onboard the device with Native Supplciant Provisioning |
| <input type="checkbox"/> Non_Cisco_IP_Phones | Cisco | Default Profile used for Non Cisco Phones. |
| <input type="checkbox"/> Permit_dot1x | Cisco | |
| <input type="checkbox"/> Wireless-dot1x | Cisco | |
| <input type="checkbox"/> DenyAccess | | Default Profile with access type as Access-Reject |
| <input type="checkbox"/> PermitAccess | | Default Profile with access type as Access-Accept |

- Điền thông tin của Policy cần tạo, sau khi điền xong chọn Submit để lưu cấu hình

Authorization Profile

* Name: Permit-wireless-dot1x

Description: [Empty text area]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

DAACL Name

ACL (Filter-ID)

Security Group

VLAN Tag ID 1 Edit Tag ID/Name 3

Vlan chính là Vlan cho SSID đó

- Tiếp tục qua tab Policy Set để tạo Rule cho việc xác thực 802.1x, ta làm như sau: chọn Insert new role abow để tạo rule

Policy Sets

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|--------|-----------------|--------------------|------------|-------------------------------------|------|---------|------|
| ✔ | Default | Default policy set | | Default Network Access | 0 | 2 | |

- Ta có thể name của Rule để dễ dàng quản trị, tiếp theo ta chọn vào biểu tượng + để chọn phương thức xác thực wireless với 802.1x

Policy Sets

| Status | Policy Set Name | Description | Conditions |
|--------|-----------------|--------------------|------------|
| ✔ | Wireless_dot1x | | |
| ✔ | Default | Default policy set | |

- Kéo mục Wireless_802.1x từ mục Library vào mục editor -> chọn Use

Conditions Studio

Library

- Wireless_802.1X
- Wireless_MAB
- Wireless_802.1X
- Wireless_Access
- Wireless_MAB

Editor

Wireless_802.1X

Use

- Tại mục Allowed Protocols / Server Sequence chọn Default Network Access và chọn Save để lưu lại

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. A notification banner at the top right says "Click here to do wireless setup and visibility setup Do not show this again." The "Policy Sets" table is displayed with the following data:

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|--------|-----------------|--------------------|-----------------|-------------------------------------|------|---------|------|
| ✔ | Wireless-dot1x | | Wireless_802.1X | Default Network Access | 0 | ⚙️ | ➔ |
| ✔ | Default | Default policy set | | Default Network Access | 0 | ⚙️ | ➔ |

Red boxes highlight the "Allowed Protocols / Server Sequence" column for the "Wireless-dot1x" policy set (labeled "1") and the "Save" button at the bottom right (labeled "2").

- Tiếp tục chọn mũi biểu tượng mũi tên để tiếp tục cấu hình, tại mục Authentication Policy, chọn biểu tượng + để tạo rule như sau:

The screenshot shows the Cisco ISE Administration console with the breadcrumb navigation: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The "Policy Sets" table is filtered to show "Wireless-dot1x". Below the table, the "Authentication Policy (1)" section is expanded, showing a table with the following data:

| Status | Rule Name | Conditions |
|--------|-----------|------------|
| ✔ | Default | |

A red box highlights the "+" button in the "Conditions" column of the "Default" rule. Below the table, there are three expandable sections: "Authorization Policy - Local Exceptions", "Authorization Policy - Global Exceptions", and "Authorization Policy (1)".

Policy Sets → Wireless-dot1x

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|--------|-----------------|-------------|-----------------|-------------------------------------|------|
| ✔ | Wireless-dot1x | | Wireless_802.1X | Default Network Access | 0 |

▼ Authentication Policy (2)

| + | Status | Rule Name | Conditions | Use | Hits | Actions |
|---|--------|----------------|-----------------|---|------|---------|
| ✎ | ✔ | Wireless_dot1x | Wireless_802.1X | Internal Users Options: Internal Users | | ⚙️ |
| | ✔ | Default | | All_User_ID_Stores Options | 0 | ⚙️ |

- Tiếp tục cấu hình tại mục Authorization Policy, ta tiếp tục tạo rule cho mục này, tại tab Results Profile ta chọn vào Results ta đã tạo lúc này -> Chọn Save để lưu lại cấu hình

Policy Sets → Profiling → Posture → Client Provisioning → Policy Elements

Click here to do wireless setup and visibility setup Do not show this again.

| + | Status | Rule Name | Conditions | Use | Hits | Actions |
|---|--------|----------------|-----------------|-------------------------------|------|---------|
| ✎ | ✔ | Wireless_dot1x | Wireless_802.1X | Internal Users Options | | ⚙️ |
| | ✔ | Default | | All_User_ID_Stores Options | 0 | ⚙️ |

► Authorization Policy - Local Exceptions

► Authorization Policy - Global Exceptions

▼ Authorization Policy (2)

| + | Status | Rule Name | Conditions | Use | Security Groups | Hits | Actions |
|---|--------|----------------|-----------------|------------------|------------------|------|---------|
| ✎ | ✔ | Wireless-Dot1x | Wireless_802.1X | Select from list | Select from list | | ⚙️ |
| | ✔ | Default | | DenyAccess | Select from list | 0 | ⚙️ |

Reset Save

III. Kiểm tra

Sử dụng Laptop để kết nối vào SSID vừa tạo, điền thông tin username và password đã tạo trên Cisco ISE để có thể đăng nhập vào SSID này.

Sau khi thiết bị kết nối ta có thể kiểm tra trên Cisco ISE đã xác thực thành công hay chưa ta làm như sau: vào mục Operation -> Radius -> Live logs để xem user xác thực được hay chưa.