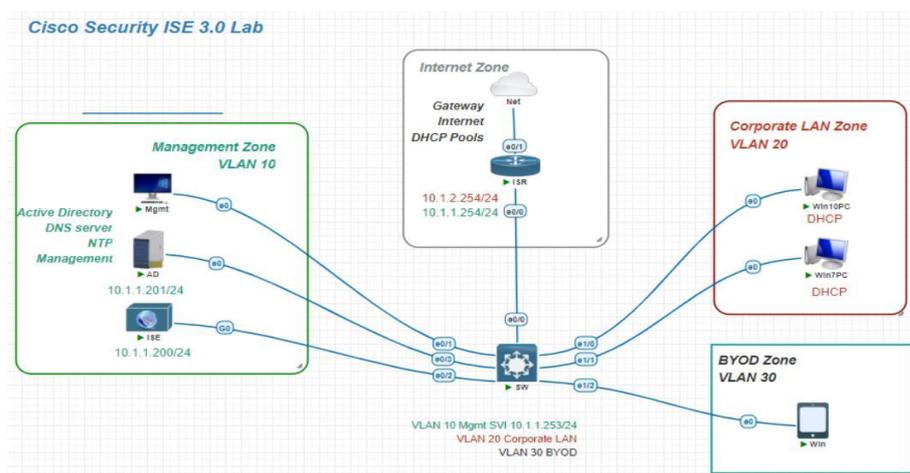


LAB : XÁC THỰC WIRED VỚI 802.1X VÀ MAB

I. Sơ đồ:



II. Mục đích thực hiện:

Tiến hành xác thực và phân quyền cho user khi truy cập vào thiết bị thông qua ISE, các bạn sẽ xác thực theo hai phương thức là Dot1x và MAB

+ **Dot1x** : 802.1x là một chứng thực chuẩn IEEE, được sử dụng cho mạng có dây lẫn không dây. Là phương pháp đóng mở dựa trên điều kiện mà server AAA xác thực. Các thiết bị muốn đi vào mạng có dây được gọi là supplicant.

+ **MAB** (MAC Authentication Bypass): là một cơ chế xác thực dựa trên địa chỉ MAC cho phép các máy khách trong mạng tích hợp với Identity Based Networking Services (IBNS) và Network Admission Control (NAC) bằng cách sử dụng địa chỉ MAC của máy khách. Tính năng MAC Authentication Bypass được áp dụng cho các môi trường mạng có cấu hình máy khách cuối không nằm dưới sự kiểm soát của quản trị viên, nghĩa là các yêu cầu IEEE 802.1X không được hỗ trợ trên các mạng này.

III. Thực hiện:

1. Cấu hình Switch AAA với Radius:

✓ Trên cmd switch:

```
aaa new-model
dot1x system-auth-control

radius server ISE
address ipv4 10.1.1.200 auth-port 1812 acct-port 1813
key evel

radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 30 tries 3
radius-server timeout 2

aaa group server radius ISE-GROUP
server name ISE
ip radius source-interface Vlan10

aaa authentication dot1x default group ISE-GROUP
aaa authorization network default group ISE-GROUP
aaa accounting update periodic 5
aaa accounting dot1x default start-stop group ISE-GROUP

aaa server radius dynamic-author
client 10.1.1.200 server-key evel

snmp-server community evel RO
snmp-server enable traps snmp linkdown linkup
```

2. Thêm switch vào ISE:

2.1 Tạo Device Type Group:

- ✓ Chuyển đến ISE Management



- ✓ Click Tab Administration/Network Resources/Network Devices



- ✓ Click vào tab “Network Device Groups”

- ✓ Click “+ Add”



- ✓ Name: LAN Switches
- ✓ Parent Group: All Device Types
- ✓ Click Save

Edit Group

Name*
LAN Switches

Description

Group Hierarchy
Device Type > All Device Types > LAN Switches

2.2 Tạo Location Group

✓ Click “+ Add”



✓ Name: **My LAN**

✓ Parent Group: **All Locations**

✓ Click Save

Edit Group

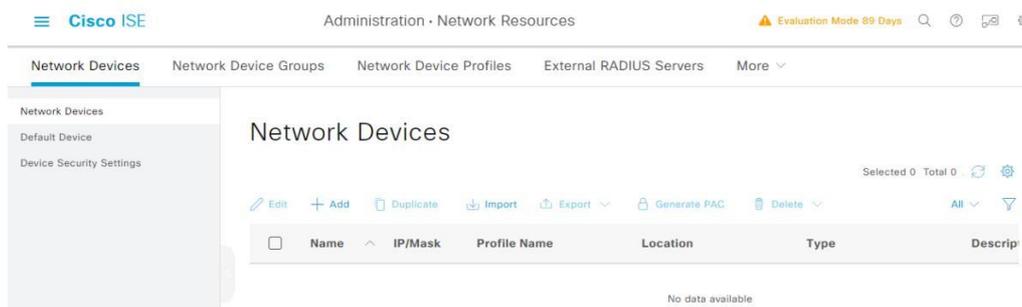
Name*
My LAN

Description

Group Hierarchy
Location > All Locations > My LAN

2.3 Thêm switch vào ISE radius

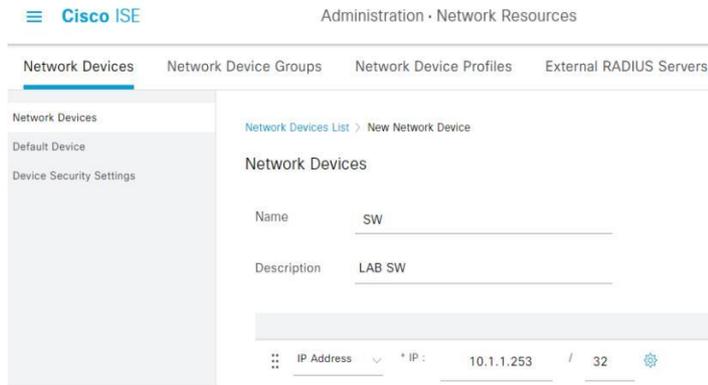
- ✓ Click vào tab “Network Devices”
- ✓ Click “+ Add”



- ✓ Name: SW
- ✓ Description: LAB SW
- ✓ IP Address: 10.1.1.253
- ✓ Model Name: IOL
- ✓ Version: 15.2
- ✓ Location: My LAN
- ✓ Device Type: LAN Switches

✓ Select Radius checkbox

✓ Shared Secret: **eve1**



Device Profile	Cisco	▼ ⓘ
Model Name	IOL	▼
Software Version	15.2	▼
Network Device Group		
Location	My LAN	▼
IPSEC	Is IPSEC Device	▼
Device Type	LAN Switches	▼

∨ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**Shared Secret eve1 [Hide](#) Use Second Shared Secret ⓘ✓ **Bật SNMP**✓ **SNMP Version: 2c**✓ **SNMP RO Community: eve1** ∨ SNMP SettingsSNMP Version 2c ∨SNMP RO Community eve1 [Hide](#)✓ **Click Submit**

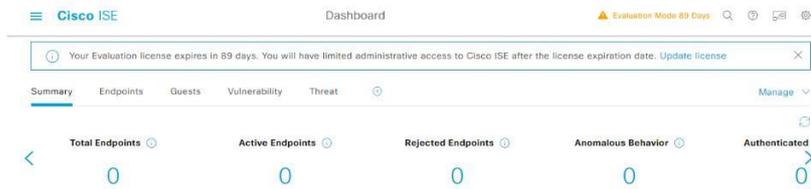
The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · Network Resources', and 'Evaluation Mode 89 Days'. The main menu has 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', and 'More'. The left sidebar shows 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices' and shows a table with one device entry:

Name	IP/Mask	Profile Name	Location	Type
SW	10.1.1.253/32	Cisco ⓘ	My LAN	LAN Switches

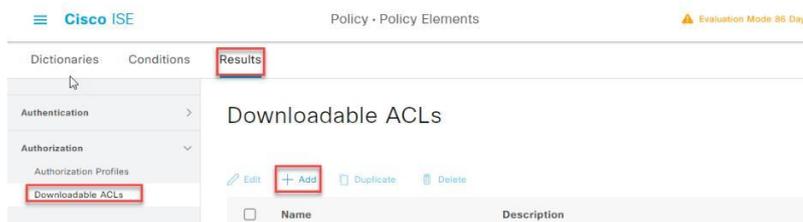
3. Tạo authorization Profiles và DACLs:

3.1 Tạo 3 DACL

- ✓ Chuyển hướng đến ISE Management

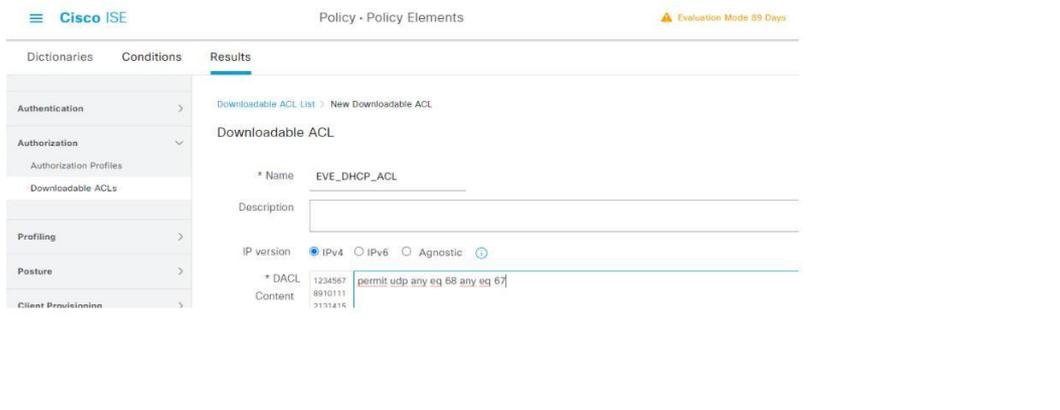


- ✓ Click Tab Policy/Policy Elements/Results
- ✓ Chuyển hướng đến Authorization/Downloadable ACLs
- ✓ Click “+ Add”



- ✓ Chuyển hướng đến Authorization/Downloadable ACLs
 - ✓ Click “+ Add”
 - ✓ Name: **EVE_DHCP_ACL**
 - ✓ IP Version: IPv4
 - ✓ Thêm ACL line
- ```
permit udp any eq 68 any eq 67
```
- ✓ Check DACL Syntax, must be Valid

✓ Click Save.



The screenshot shows the Cisco ISE interface for configuring a Downloadable ACL. The configuration includes:

- Name: EVE\_DHCP\_ACL
- Description: (empty field)
- IP version: IPv4 (selected)
- ACL Content:
 

| * DACL  | 1234567 | Content                        |
|---------|---------|--------------------------------|
| 8910111 |         | permit udp any eq 68 any eq 67 |
| 9151415 |         |                                |

✓ Click “+ Add”

✓ Name: **PERMIT\_AD\_ONLY**

✓ IP Version: IPv4

✓ Add ACL lines

```
permit udp any eq 68 any eq 67
permit udp any any eq 53
permit ip any host 10.1.1.201
```

✓ Check DACL Syntax, must be Valid

✓ Click Save.

✓ Click “+ Add”

✓ Name: **WIRED\_PERMIT\_ALL**

✓ IP Version: IPv4

✓ Add ACL line

```
permit ip any any
```

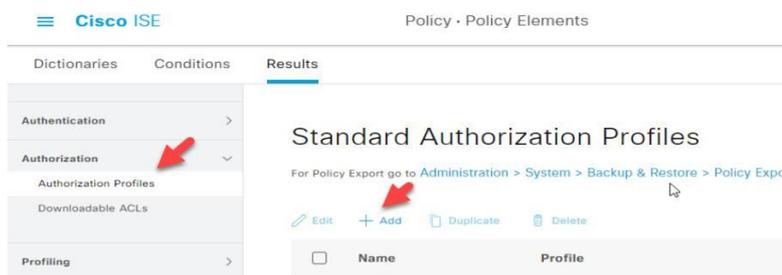
✓ Check DACL Syntax

✓ Click Save.

### 3.2 Tạo 3 Authorization Profiles:

✓ Chuyển hướng đến Authorization/Authorization Profiles

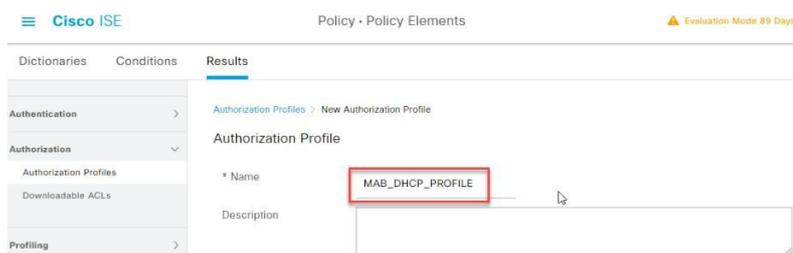
✓ Click “+ Add”



✓ Name: **MAB\_DHCP\_PROFILE**

✓ Bật DACL

✓ Chọn DACL: **EVE\_DHCP\_ACL**





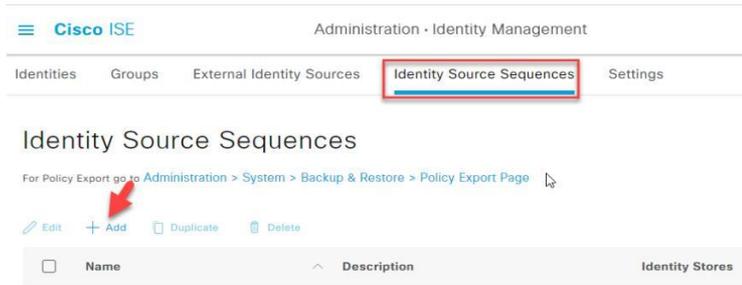
- ✓ Click “+ Add”
- ✓ Name: **WIRED\_AD\_ONLY\_PROFILE**
- ✓ Bật DACL
- ✓ Chọn DACL: **PERMIT\_AD\_ONLY**
- ✓ Click “+ Add”
- ✓ Name: **WIRED\_PERMIT\_ALL\_PROFILE**
- ✓ Bật DACL
- ✓ Chọn DACL đã chọn: **WIRED\_PERMIT\_ALL**

### 3.3 Tạo Source Identity sequence

- ✓ Chuyển hướng đến ISE Management



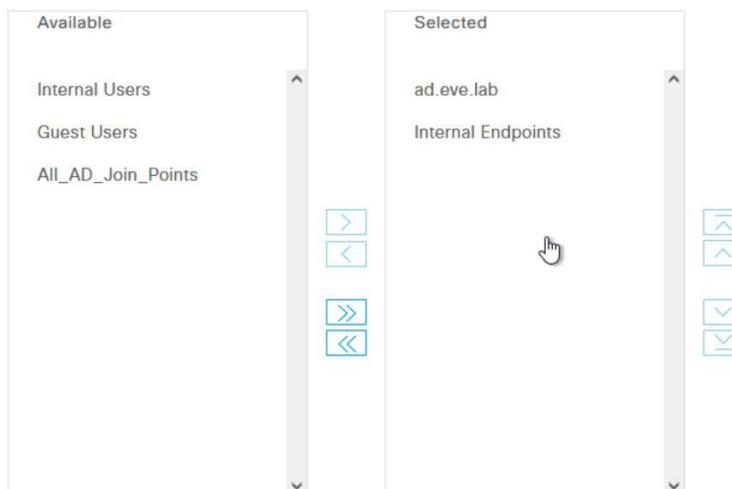
- ✓ Click Tab Administration/Identity Management/Groups
- ✓ Click Tab: Identity Source Sequences
- ✓ Click “+ Add”



The screenshot shows the Cisco ISE Administration interface for Identity Management. The 'Identity Source Sequences' tab is selected and highlighted with a red box. Below the navigation bar, there are options to 'Edit', '+ Add', 'Duplicate', and 'Delete'. A red arrow points to the '+ Add' button. Below these options is a table with columns for 'Name', 'Description', and 'Identity Stores'.

✓ Name: **EVE\_Sequence**

✓ Chọn Identity sources: **ad.eve.lab** và **Internal Endpoints**



The screenshot shows the Identity Source Selection interface. It consists of two columns: 'Available' and 'Selected'. The 'Available' column contains 'Internal Users', 'Guest Users', and 'All\_AD\_Join\_Points'. The 'Selected' column contains 'ad.eve.lab' and 'Internal Endpoints'. There are navigation buttons between the columns: '>' and '<' for moving items between columns, and '>>' and '<<' for moving all items. On the right side of the 'Selected' column, there are up and down arrow buttons for reordering items.

✓ Click: Save

## 4. Tạo Policy Set

### 4.1 Tạo dot1x và MAB Policy

- ✓ Chuyển hướng đến ISE Management



- ✓ Click Tab Policy/Policy Sets

- ✓ Click “+ Add”

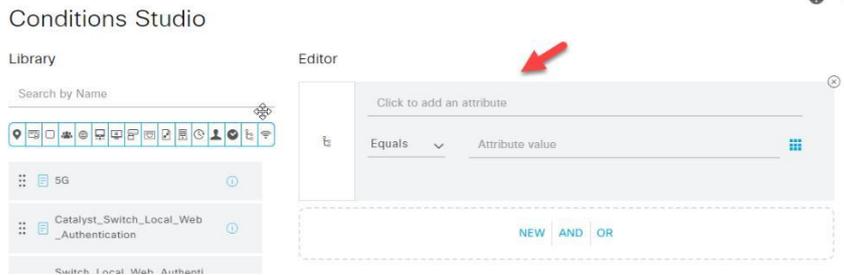


- ✓ Name: **EVE-POLICY**

- ✓ Click “+” for New conditions



- ✓ Trong điều kiện Studio “Click to add an attribute”

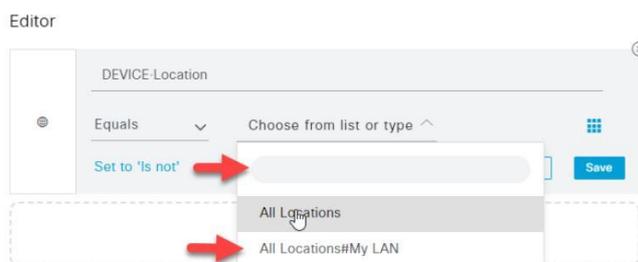


✓ Trong trường Editor “Click Tab Location”

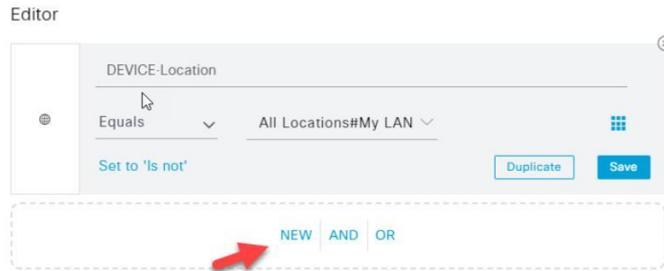
✓ Chọn Attribute **DEVICE:Location**



✓ Chọn equals từ danh sách list: **All Locations/My LAN**



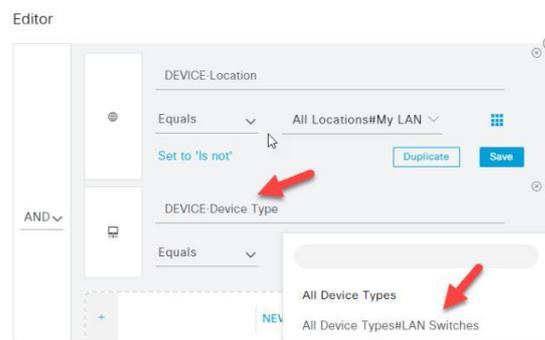
✓ Click **New** to add another attribute



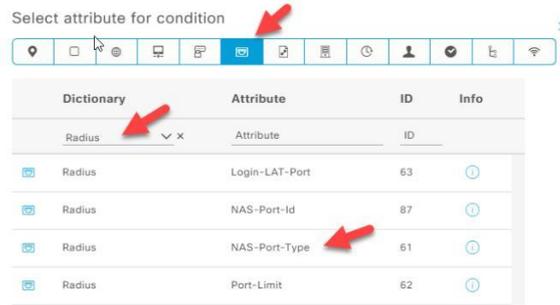
- ✓ Trong trường Editor “Click Tab Network Device”



- ✓ Chọn Attribute DEVICE: **Device Type**
- ✓ Chọn equals từ list: **All Device Types/LAN Switches**

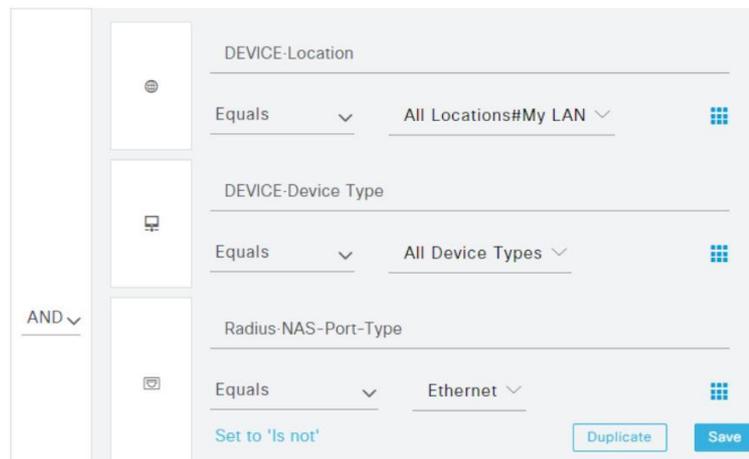


- ✓ Click **New** to add another attribute
- ✓ Trong trường Editor “Click Tab Port”
- ✓ Dưới Dictionary chọn: **Radius**
- ✓ Chọn **Radius/NAT-Port-Type**



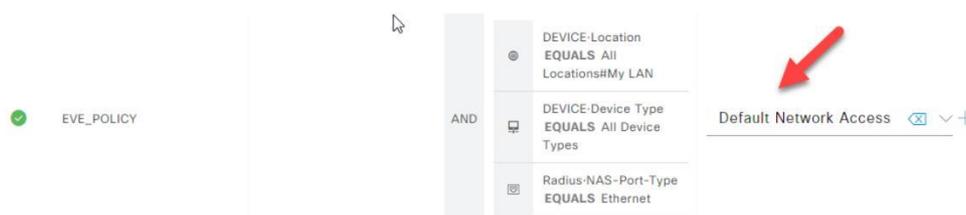
✓ Chọn Equal: Ethernet

Editor



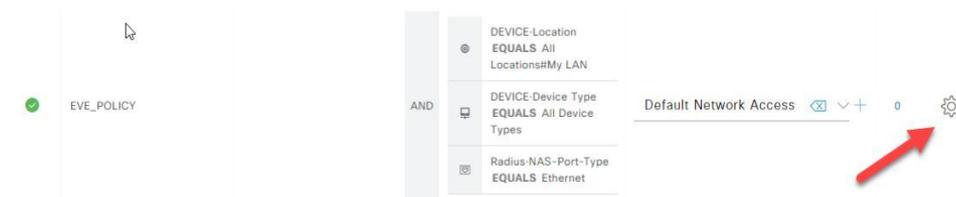
✓ Click Use

✓ Chọn Default Network Access for allowed Protocols



## 4.2 Tạo Authentication Policy

- ✓ Click vào View Policy “>”



- ✓ Mở rộng Authentications Policy
- ✓ Tại mục Default rules select Use: EVE\_Sequence



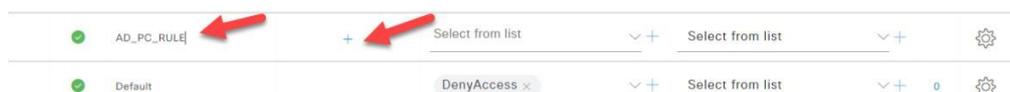
## 4.3 Tạo Corporate PC Authorization Policy

- ✓ Chuyển hướng đến Authorization Policy
- ✓ Mở rộng Authorization Policy
- ✓ Click “+” To add New rule



✓ Name: AD\_PC\_RULE

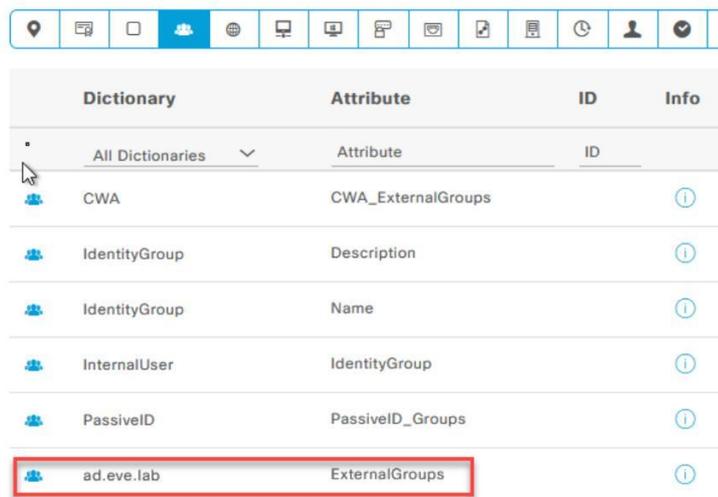
✓ Click “+” For new Condition



✓ Chọn Tab: Identity Group

✓ Chọn: ad.eve.lab/ExternalGroups

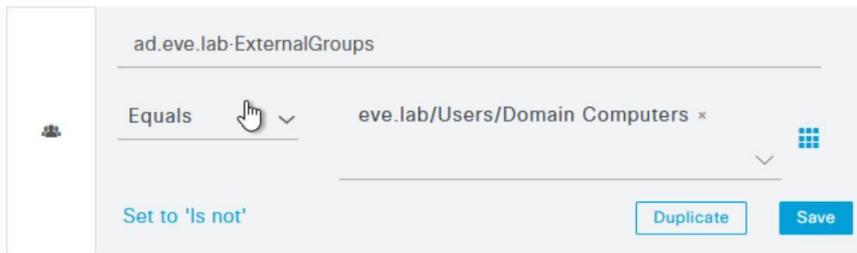
Select attribute for condition



✓ Chọn Equal: eve.lab/Users/Domain Computers

✓ Click: Use

### Editor



- ✓ Chọn Profiles: WIRED\_AD\_ONLY
- ✓ Chọn Security Group: Employees



## 4.4 Tạo Corporate User Authorization Policy

- ✓ Chuyển hướng đến AD\_PC\_RULE/Actions/Insert new rule below

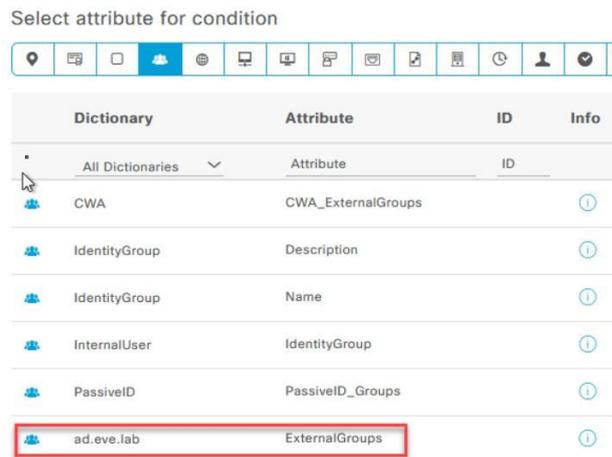


- ✓ Name: AD\_USER\_ACCESS
- ✓ Click “+” to add New conditions



- ✓ Chọn Tab: Identity Group

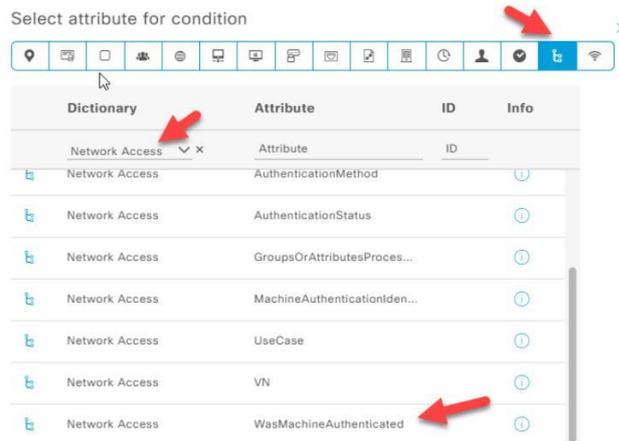
- ✓ Attribute: ad.eve.lab/ExternalGroups
- ✓ Equals: eve.lab/Users/Domain Users
- ✓ Click Use



- ✓ Click New for another condition in this rule



- ✓ Chọn Tab: Unclassified
- ✓ Chọn Dictionary: Network Access
- ✓ Chọn Attribute: WasMachineAuthenticated
- ✓ Equals: True
- ✓ Click Use



- ✓ Chọn Profiles: WIRED\_PERMIT\_ALL\_PROFILE
- ✓ Chọn Security Group: Employees



#### 4.5 Tạo MAB Authorization Policy (Android)

- ✓ Chuyển hướng đến AD\_USER\_ACCESS Actions/Insert New Rule below

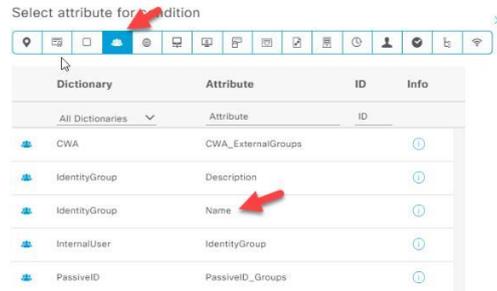


- ✓ Name: MAB\_RULE
- ✓ Click “+” to add New conditions

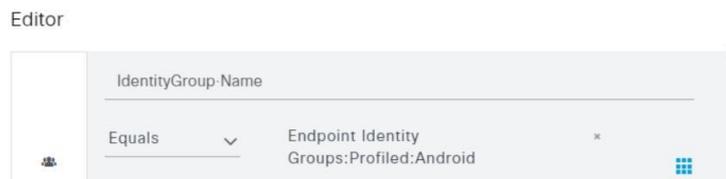


✓ Chọn Tab Identity Group

✓ Attribute: Name



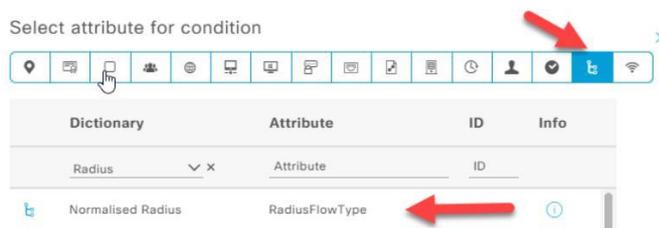
✓ Equals: Endpoint Identity Groups: Profiled: Android



✓ Click: New to add another condition

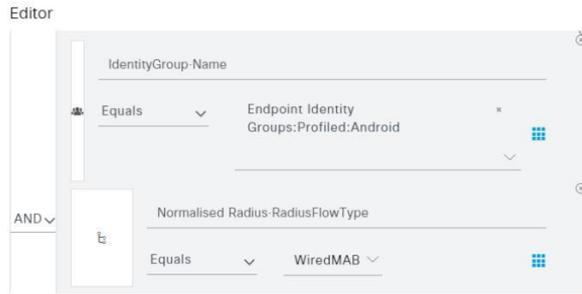
✓ Chọn Tab: Unclassified

✓ Chọn Condition: Normalized Radius/Radius FlowType



✓ Equals: WiredMAB

✓ Click Use



✓ Chọn Profiles: MAB\_DHCP\_PROFILE

✓ Chọn Security Groups: BOYD



#### 4.6 Lưu cấu hình Authorization Policy

✓ Click SAVE

## 4.7 Cấu hình lab switch ports

```
interface Ethernet1/0
description win10 node
switchport access vlan 20
switchport mode access

authentication host-mode multi-auth
authentication port-control auto
mab

dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast edge

spanning-tree bpdudfilter enable
spanning-tree bpduguard enable

interface Ethernet1/1
description win7 node
switchport access vlan 20
switchport mode access

authentication host-mode multi-auth
authentication port-control auto
mab

dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast edge

spanning-tree bpdudfilter enable
spanning-tree bpduguard enable

interface Ethernet1/2
description Tablet EVE Pro lab with Android
switchport access vlan 30

switchport mode access
authentication host-mode multi-auth
authentication open

authentication port-control auto
mab

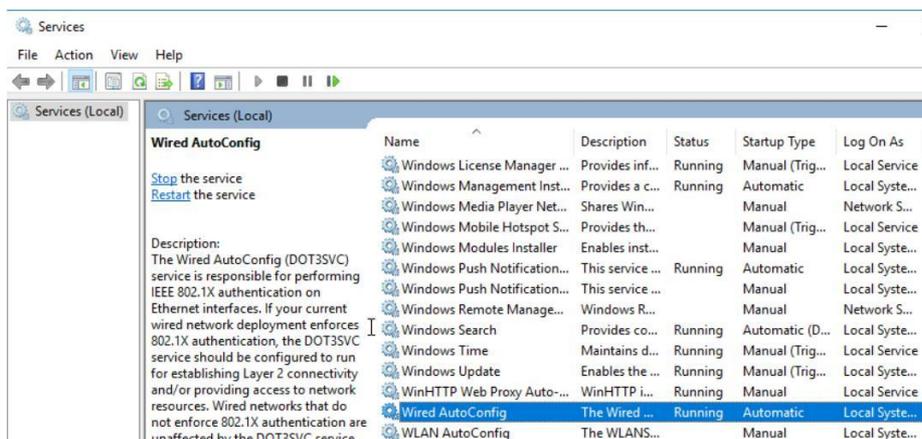
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast edge

spanning-tree bpdudfilter enable
spanning-tree bpduguard enable
```

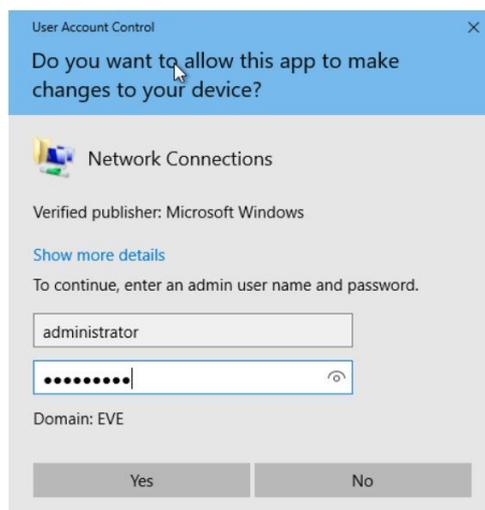
## 5. Windows 10 Dot1x Authentication

### 5.1 Cấu hình Windows 10 PC for Dot1x authentication

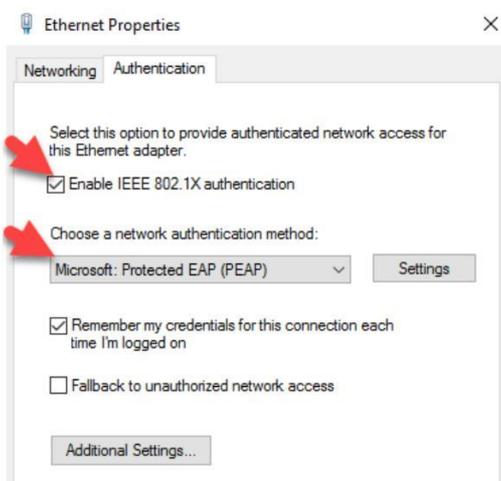
- ✓ Mở Windows 10
- ✓ Chuyển hướng đến Windows Control Panel, Administrative Tools/Services
- ✓ Chắc rằng Windows đã bật và chạy Wired Autoconfig Service
- ✓ Nếu nó chưa hoạt động, log off Windows và log in
- ✓ Login: eve\administrator, Password: Test123



- ✓ Chuyển hướng đến Start/Settings/Network & Internet
- ✓ Chuyển hướng đến Advanced Network Settings/Change Adapter Settings
- ✓ Chuột phải vào ethernet adapter và chọn Properties.
- ✓ Username: eve\administrator, Password: Test123



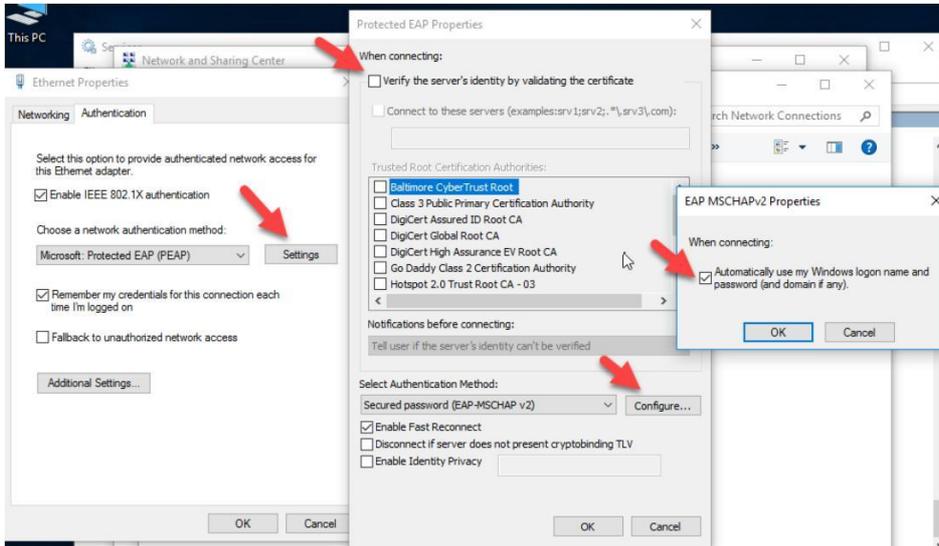
- ✓ Chọn Tab Authentication
- ✓ Bật IEEE 802.1X authentication



- ✓ Click Chọn network authentication method Settings
- ✓ Bỏ Tick Verify the Server's identity by validating the certificate
- ✓ Click trên Select Authentication Method: Configure

✓ Check: Khi kết nối, Automatically sử dụng Windows Logon name và password

✓ Click OK 2 lần



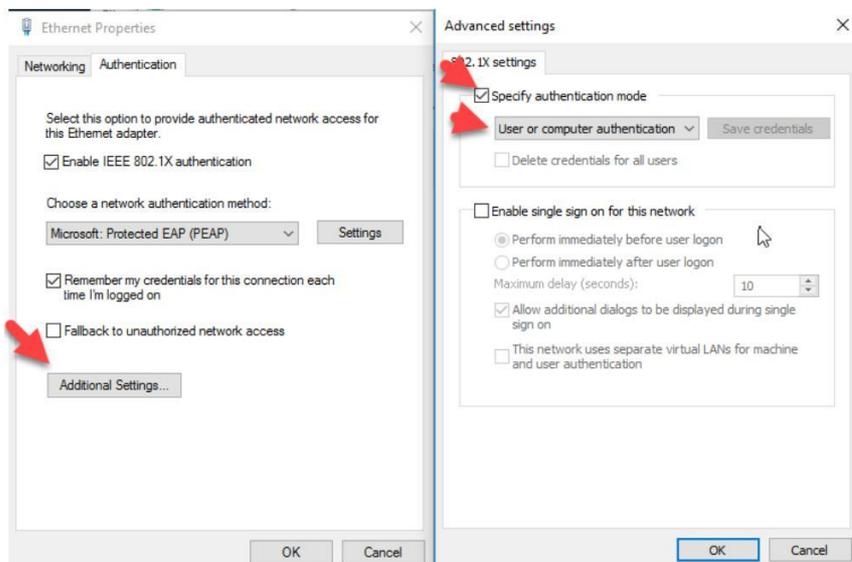
✓ Click Additional Settings

✓ Check Specify authentication mode

✓ Chọn User or Computer authentication

✓ Click OK 2 lần

## ✓ Reboot Windows 10



## ✓ Click OK 2 lần

## ✓ Reboot Windows 10

### 5.2 Windows 10 Verification

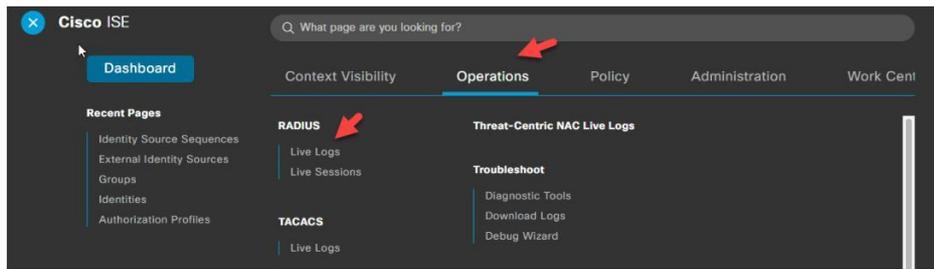
Note: sau khi reboot Windows 10 machine, không login vào, nhưng ta sẽ kiểm tra kết quả trên Switch:

## ✓ show access-lists

```
SW#sh access-lists
Extended IP access list xACSACLx-IP-PERMIT_AD_ONLY-5fdf2f06 (per-
user)

 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit ip any host 10.1.1.201
```

## ✓ Chuyển hướng đến ISE management/Operations/Live Logs



- ✓ Bạn sẽ thấy John-PC được xác thực nhưng chỉ được gán cho WIRED\_AD\_ONLY\_PROFILE

| Time                       | Status                               | Details | Repea... | Identity                         | Endpoint ID       | Endpoint... | Authenti... | Authoriz... | Authorization Profiles | IP Address | Re... |
|----------------------------|--------------------------------------|---------|----------|----------------------------------|-------------------|-------------|-------------|-------------|------------------------|------------|-------|
| Dec 26, 2020 11:20:29.5... | <span style="color: green;">●</span> |         | 0        | host\John-PC.exe lab             | 50-8A-00-05-00-00 | Windows1... | EVE-POLI... | EVE-POLI... | WIRED_AD_ONLY_PROFILE  | 10.1.2.2   | N     |
| Dec 26, 2020 11:20:29.2... | <span style="color: green;">●</span> |         |          | xACSACLx-IP-PERMIT_AD_ONLY-SM... |                   |             |             |             |                        |            | SV    |
| Dec 26, 2020 11:20:29.2... | <span style="color: green;">●</span> |         |          | host\John-PC.exe lab             | 50-8A-00-05-00-00 | Windows1... | EVE-POLI... | EVE-POLI... | WIRED_AD_ONLY_PROFILE  | 10.1.2.2   | SV    |

- ✓ Bây giờ ta login in Windows 10 john-PC, user: johndoe và password: Gold2021
- ✓ Chuyển hướng đến switch và show access-list, Bây giờ bạn sẽ thấy ACL được thay đổi thành permit ip any any

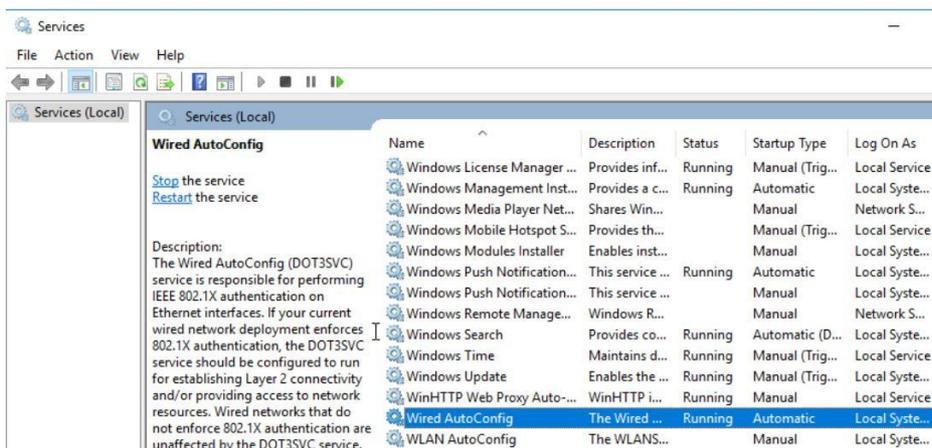
```
SW#sh access-lists
Extended IP access list xACSACLx-IP-WIRED_PERMIT_ALL-5fe06c43 (per-user)
1 permit ip any any
```

- ✓ Chuyển hướng đến ISE management/Operations/Live Logs again
- ✓ Bây giờ bạn sẽ thấy John Doe đã được xác thực nhưng chỉ được giao cho WIRED\_PERMIT\_ALL\_PROFILE

| Time                       | Status                               | Details | Repea... | Identity                           | Endpoint ID       | Endpoint... | Authent... | Authoriz... | Authorization Profiles   | IP Address |
|----------------------------|--------------------------------------|---------|----------|------------------------------------|-------------------|-------------|------------|-------------|--------------------------|------------|
| Dec 26, 2020 11:25:32.2... | <span style="color: green;">●</span> |         | 9        | EVE@ezone                          | 50-8A:00:05:00:00 | Windows1... | EVE-POL... | EVE-POL...  | WIRED_PERMIT_ALL_PROFILE | 10.1.2.2   |
| Dec 26, 2020 11:24:18.6... | <span style="color: green;">●</span> |         |          | BACKSLASH-P-WIRED_PERMIT_ALL-0Y... |                   |             |            |             |                          |            |
| Dec 26, 2020 11:24:19.6... | <span style="color: green;">●</span> |         |          | EVE@ezone                          | 50-8A:00:05:00:00 | Windows1... | EVE-POL... | EVE-POL...  | WIRED_PERMIT_ALL_PROFILE | 10.1.2.2   |

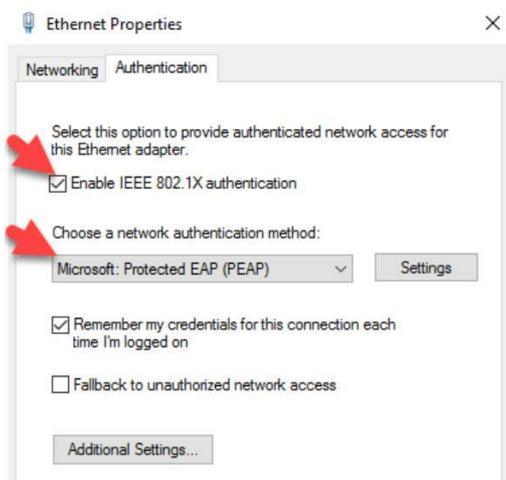
### 5.3 Xác thực Windows 7 Dot1x

- ✓ Khởi động lại Windows 7 và login vào: eve\administrator, password: Test123
- ✓ Mở Windows 7
- ✓ Chuyển hướng đến Windows Control Panel, Administrative Tools/Services
- ✓ Đảm bảo rằng Windows đã được bật và chạy Wired Autoconfig Service

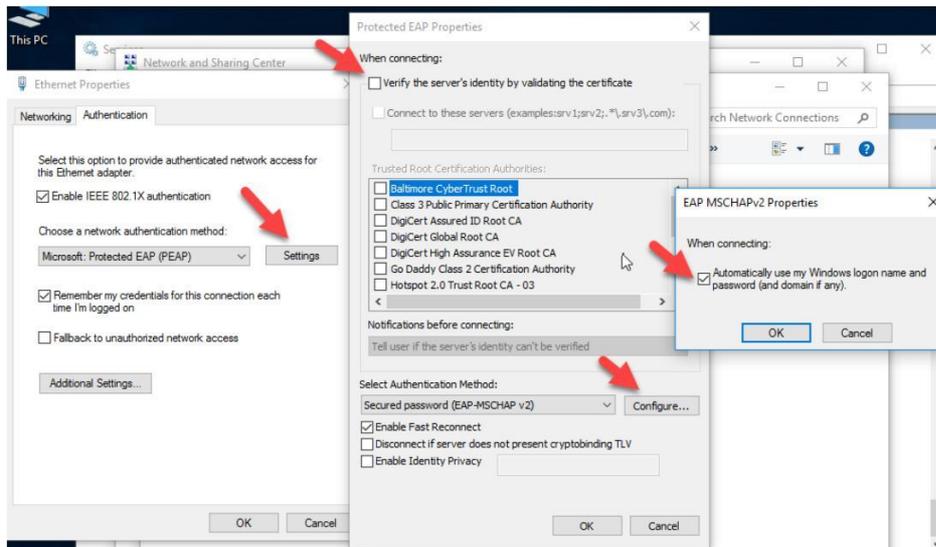


- ✓ Chuyển hướng đến Control panel/Network and Internet/Network and Sharing center
- ✓ Chuyển hướng đến Change Adapter Settings
- ✓ Chuột phải vào ethernet adapter và chọn Properties.
- ✓ Chọn Tab Authentication

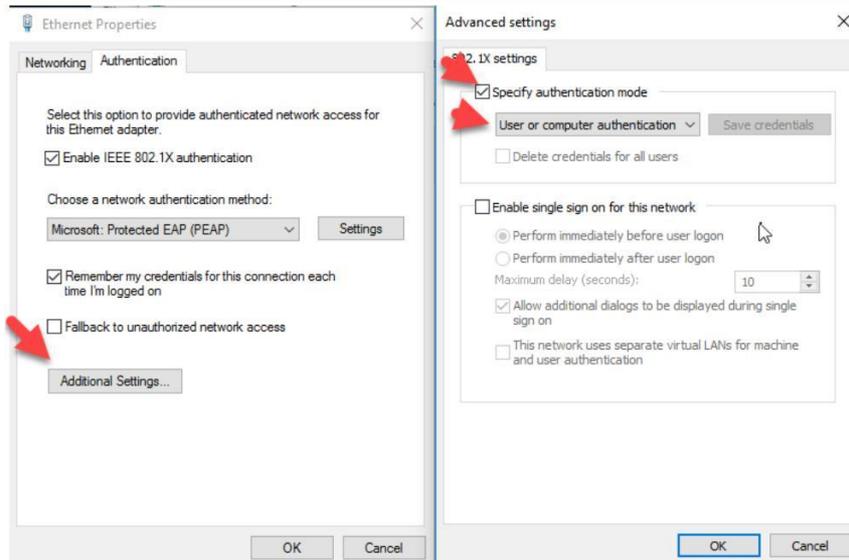
✓ Check Enable IEEE 802.1X authentication



- ✓ Click vào network authentication method Settings
- ✓ Bỏ tick Verify the Server's identity by validating the certificate
- ✓ Click vào Select Authentication Method: Configure
- ✓ Check: When connecting, Automatically use my Windows Logon name and password and domain if any
- ✓ Click OK 2 lần



- ✓ Click Additional Settings
- ✓ Check vào Specify authentication mode
- ✓ Chọn User or Computer authentication
- ✓ Click OK 2 lần



- ✓ Click OK 2 lần
- ✓ Khởi động lại Windows 7

## 5.4 Windows 7 Verification

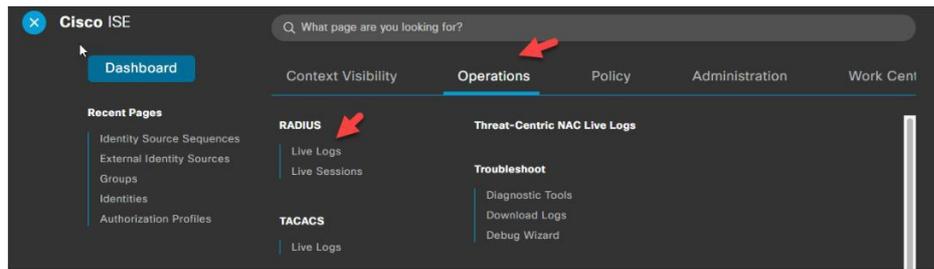
Lưu ý: Sau khi reboot Windows 7, không đăng nhập vào, các bạn sẽ kiểm tra kết quả trên Switch trước:

- ✓ Gõ: show access-lists

Bạn nên nhận thấy rằng DACL PERMIT\_AD\_ONLY đang được sử dụng. Có nghĩa là Windows 10 đã nhận được địa chỉ IP, và có thể giao tiếp với AD server

```
SW#sh access-lists
Extended IP access list xACSACLx-IP-PERMIT_AD_ONLY-5fdf2f06 (per- user)
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit ip any host 10.1.1.201
```

✓ Chuyển hướng đến ISE management/Operations/Live Logs



✓ Bạn sẽ thấy Jenny-PC được xác thực nhưng chỉ gán cho ACL:  
WIRED\_AD\_ONLY\_PROFILE

| Time                       | Status                               | Details | Repea... | Identity              | Endpoint ID       | Endpoint Profile      | Authent...  | Authoriz... | Authorization Profiles | IP Addr... |
|----------------------------|--------------------------------------|---------|----------|-----------------------|-------------------|-----------------------|-------------|-------------|------------------------|------------|
| Dec 26, 2020 11:52:38.2... | <span style="color: blue;">●</span>  |         | 1        | host/Jenny-PC eve lab | 50-0A-00-07-00-00 | Microsoft-Workstation | EVE-POLL... | EVE-POLL... | WIRED_AD_ONLY_PROFILE  | 10.1.2.1   |
| Dec 26, 2020 11:52:38.1... | <span style="color: green;">●</span> |         |          | host/Jenny-PC eve lab | 50-0A-00-07-00-00 | Microsoft-Workstation | EVE-POLL... | EVE-POLL... | WIRED_AD_ONLY_PROFILE  | 10.1.2.1   |

✓ Bây giờ login Windows 7 Jenny-PC , user: jennydoe and password: Silver2021

✓ Chuyển hướng đến switch và `show access-list`, Bây giờ bạn sẽ thấy ACL được thay permit all

```
SW#sh access-lists
Extended IP access list xACSACLx-IP-WIRED_PERMIT_ALL-5fe06c43 (per-user)
 1 permit ip any any
```

✓ Chuyển hướng đến ISE management/Operations/Live Logs again

✓ Bây giờ bạn sẽ thấy rằng John Doe đã được xác thực nhưng chỉ gán cho WIRED\_PERMIT\_ALL\_PROFILE

| Time                       | Status                               | Details | Repea... | Identity     | Endpoint ID       | Endpoint...  | Authenti... | Authoriz... | Authorization Profiles   | IP Address | Network D |
|----------------------------|--------------------------------------|---------|----------|--------------|-------------------|--------------|-------------|-------------|--------------------------|------------|-----------|
| Dec 26, 2020 11:56:20.6... | <span style="color: green;">●</span> |         | 0        | EVEjennyb... | 50:0A:00:07:00:00 | Microsoft... | EVE-POLL... | EVE-POLL... | WIRED_PERMIT_ALL_PROFILE | 10.1.2.1   | SW        |
| Dec 26, 2020 11:56:20.6... | <span style="color: green;">●</span> |         | 0        | EVEjennyb... | 50:0A:00:07:00:00 | Microsoft... | EVE-POLL... | EVE-POLL... | WIRED_PERMIT_ALL_PROFILE | 10.1.2.1   | SW        |

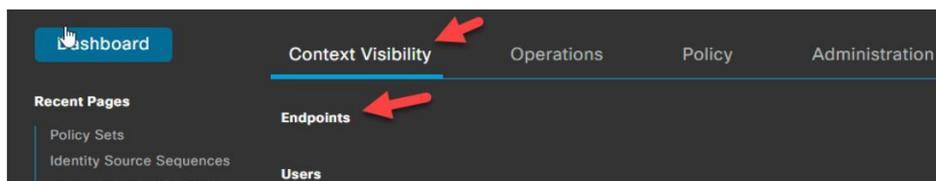
## 5.6 Xác thực máy tính bằng Android

### 5.6.1 Cấu hình Android Device MAB authentication (EVE PRO Lab với Android)

- ✓ Khởi động lại thiết bị Android

| Time                       | Status                             | Details     | Repea... | Identity | Endpoint ID       | Endpoint Pr       | Authentic | Authorizat  | Authorization Profiles | IP Address | Network De... | Device I  |           |
|----------------------------|------------------------------------|-------------|----------|----------|-------------------|-------------------|-----------|-------------|------------------------|------------|---------------|-----------|-----------|
| Dec 27, 2020 12:02:45.2... | <span style="color: red;">●</span> | Auth Failed | x        |          | 50:0A:00:08:00:00 | 50:0A:00:08:00:00 | Unknown   |             | DenyAccess             | 10.1.3.1   | SW            | Ethernet1 |           |
| Dec 27, 2020 12:01:14.8... | <span style="color: red;">●</span> |             |          |          | 50:0A:00:08:00:00 | 50:0A:00:08:00:00 | Unknown   | EVE-POLL... | EVE-POLL...            | DenyAccess | 10.1.3.1      | SW        | Ethernet1 |

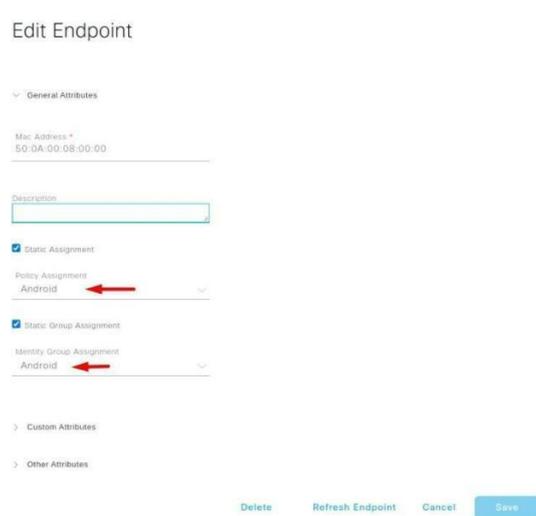
- ✓ Chuyển hướng đến ISE management/Operations/Live Logs Bạn sẽ nhận thấy rằng xác thực không thành công
- ✓ Chuyển hướng đến ISE management/Context Visibility/Endpoints



- ✓ Chọn thiết bị Android đang xác thực không thành công, và click vào edit

| MAC Address       | Status                               | IP Address | Username     | Hostname     | Location              | Endpoint Profile                 | Authentication Failure Re... | Authentication P... | Authorization P... | Authentication Protocol |
|-------------------|--------------------------------------|------------|--------------|--------------|-----------------------|----------------------------------|------------------------------|---------------------|--------------------|-------------------------|
| 50:0A:00:09:00:00 | <span style="color: green;">●</span> | 10.1.2.2   | EVEjennyb... | john-PC-a... | My LAN                | Windows10-Works...               | -                            | Default             | AD_USER_ACCESS     | MSCHAPV2                |
| 50:0A:00:09:00:00 | <span style="color: green;">●</span> | 10.1.201   |              | art.evee.lab |                       | Unknown                          |                              |                     |                    |                         |
| 50:0A:00:07:00:00 | <span style="color: green;">●</span> | 10.1.21    | EVEjennyb... | My LAN       | Microsoft-Workstat... |                                  |                              | Default             | AD_USER_ACCESS     | MSCHAPV2                |
| 50:0A:00:08:00:00 | <span style="color: red;">●</span>   | 10.1.3.1   | 50505050...  | My LAN       | Unknown               | 10039 Rejected per authorizat... |                              | Default             | Default            | Local                   |
| AA:BB:CC:DD:EE:FF | <span style="color: green;">●</span> | 10.1.1.253 |              |              | Cisco-Device          |                                  |                              |                     |                    |                         |

- ✓ Description: Android
- ✓ Static assignment: Android
- ✓ Static group assignment: Android
- ✓ Click save



- ✓ Gõ show access-lists
- ✓ Bạn sẽ thấy EVE\_DHCP\_ACL đang được sử dụng. Nghĩa là thiết bị Android đã nhận được địa chỉ IP, và truy cập được mạng.

```
SW#sh access-lists
Extended IP access list xACSACLx-IP-EVE_DHCP_ACL-5fe79837
(per-user)
 1 permit udp any eq bootpc any eq bootps
```

- ✓ Chuyển hướng đến ISE management/Operations/Live Logs again
- ✓ Bây giờ bạn sẽ thấy thiết bị Android đã được xác thực và gán cho MAB\_DHCP\_PROFILE

| Time                       | Status | Details | Repea... | Identity     | Endpoint ID    | Endpoint... | Authenti... | Authoriz... | Authorization Profiles | IP Address | Network De... | Device   |
|----------------------------|--------|---------|----------|--------------|----------------|-------------|-------------|-------------|------------------------|------------|---------------|----------|
| Dec 27, 2020 01:22:45.8... | ●      | q       | 1        | 50a.00.00.00 | 50.0A.00.00.00 | Android     | EVE-POL...  | EVE-POL...  | MAB_SMB_PROFILE        | 10.1.2.1   | SW            | Ethernet |
| Dec 27, 2020 01:17:45.4... | ●      | q       |          | 50a.00.00.00 | 50.0A.00.00.00 | Android     | EVE-POL...  | EVE-POL...  | MAB_SMB_PROFILE        | 10.1.2.1   | SW            | Ethernet |

## Kiểm tra phiên xác thực cho mab và dot1x:

- ✓ Gỡ show access-lists
- ✓ Bạn sẽ chú ý rằng xác thực dot1x có thiết bị Windows và mab có thiết bị Android

```
SW#sh authentication sessions

Interface Identifier Method Domain Status Fg Session ID
Et1/2 500a.0008.0000 mab DATA Auth 0A0101FD0000001000292FE5
Et1/0 500a.0005.0000 dot1x DATA Auth 0A0101FD000000110034F2B6
Et1/1 500a.0007.0000 dot1x DATA Auth 0A0101FD0000001200354CBE
```

- ✓ Chuyển hướng đến ISE management/Operations/Live Logs again

| Time                       | Status | Details | Repea... | Identity     | Endpoint ID       | Endpoint...  | Authenti...        | Authorization Policy         | Authorization Profiles   | IP Address |
|----------------------------|--------|---------|----------|--------------|-------------------|--------------|--------------------|------------------------------|--------------------------|------------|
| Dec 27, 2020 01:25:28.4... | ●      | q       | 0        | EVE/janitor  | 50.0A.00.07.00.00 | Microsoft... | EVE-POLICY -> D... | EVE-POLICY -> AD_USER_ACCESS | WIRED_PERMIT_ALL_PROFILE | 10.1.2.1   |
| Dec 27, 2020 01:35:24.3... | ●      | q       | 0        | EVE/janitor  | 50.0A.00.05.00.00 | Windows1...  | EVE-POLICY -> D... | EVE-POLICY -> AD_USER_ACCESS | WIRED_PERMIT_ALL_PROFILE | 10.1.2.2   |
| Dec 27, 2020 01:32:44.4... | ●      | q       | 1        | 50a.00.00.00 | 50.0A.00.00.00    | Android      | EVE-POLICY -> D... | EVE-POLICY -> BOYD_MAB       | MAB_SMB_PROFILE          | 10.1.2.1   |

- ✓ Chuyển hướng đến ISE management/Context visibility/Endpoints

| MAC Address       | Status    | IP Address | Username          | Hostname           | Location | Endpoint Profile    | Authentication Failure Re... | Authentication ... | Authorization P... | Authentication Protocol |
|-------------------|-----------|------------|-------------------|--------------------|----------|---------------------|------------------------------|--------------------|--------------------|-------------------------|
| 50.0A.00.05.00.00 | Connected | 10.1.2.2   | EVE/janitor       | John-PC.ess.joh... | My LAN   | Windows10-Work...   | -                            | Default            | AD_USER_ACCESS     | MSCHAPV2                |
| 50.0A.00.07.00.00 | Connected | 10.1.2.1   | EVE/janitor       |                    | My LAN   | Microsoft-Workst... | -                            | Default            | AD_USER_ACCESS     | MSCHAPV2                |
| 50.0A.00.00.00.00 | Connected | 10.1.2.1   | 50-0A-00-00-00-00 |                    | My LAN   | Android             | -                            | Default            | BOYD_SMB           | Linkup                  |