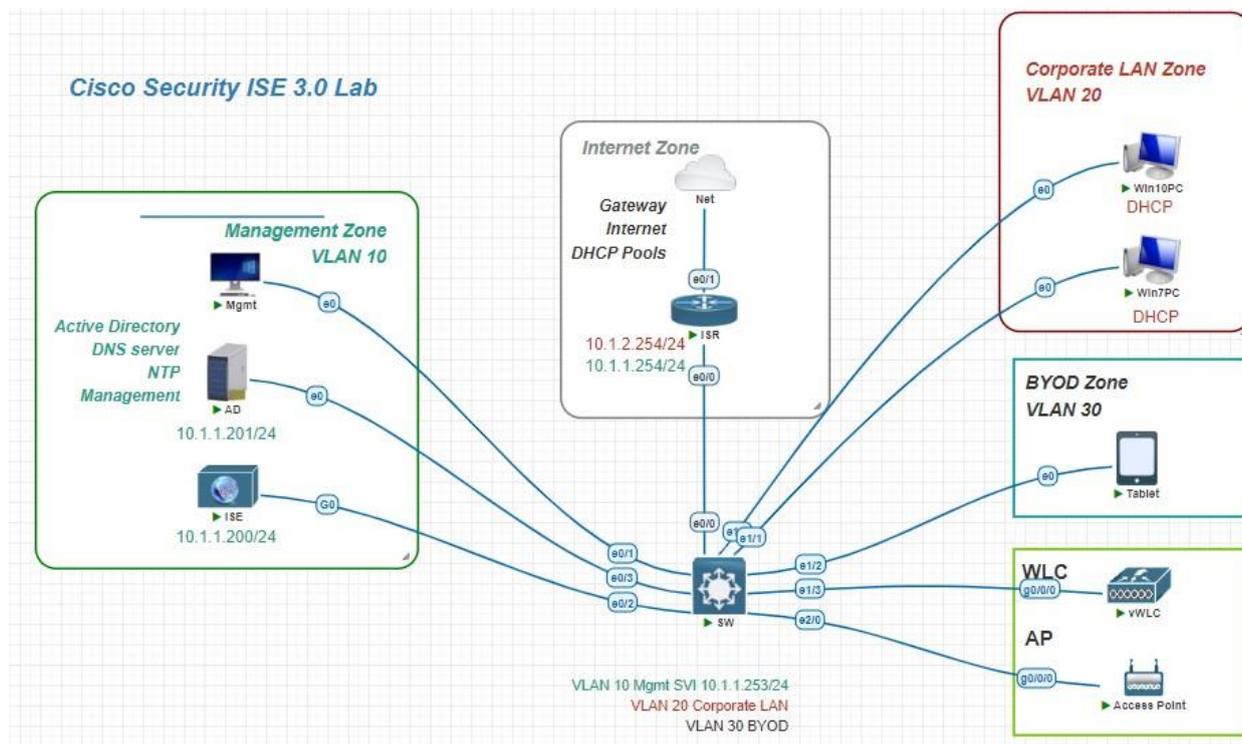


LAB - WIRELESS 802.1X WITH EAP-TLS AND PEAP

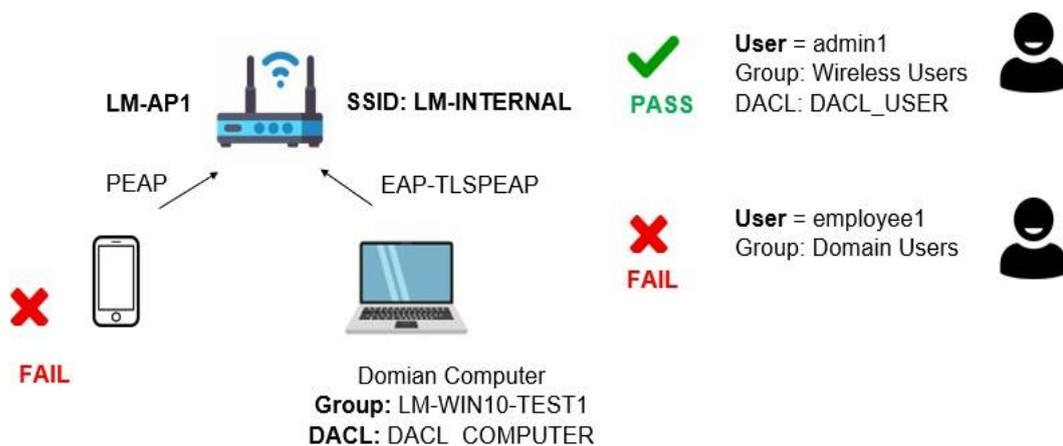
I. Sơ đồ:



II. Mục đích thực hiện:

Vì bảo mật Mạng cục bộ Wi-Fi (WLAN) là điều cần thiết và các loại xác thực EAP cung cấp một phương tiện tốt hơn có khả năng bảo mật kết nối WLAN, Một số loại xác thực EAP được triển khai phổ biến nhất bao gồm, EAP-TLS, PEAP.

- **EAP-TLS** thường được sử dụng cho mạng không dây. Certificate được cài trên cả authentication server và supplicant. Chính vì yêu cầu này mà cả client và server có một cặp key được ký bởi CA server. EAP-TLS được sử dụng tương tự như mã hóa SSL. EAP-TLS thiết lập một đường hầm mã hóa để certificate của user được gửi vào trong đó.
- **PEAP** (Protected EAP) đầu tiên bên server sử dụng certificate để tạo ra một đường hầm mã hóa. Sau đó quá trình chứng thực được diễn ra trong đường hầm đó bằng cách sử dụng (MS-CHAPv2) hoặc Generic Token Card (GTC)



Ta sẽ tạo SSID: LM-INTERNAL cho phép user admin1 group Wireless Users truy cập vào mạng wifi. Trong trường này ta ví dụ Phòng tài chính chỉ cho phép dùng laptop không được dùng điện thoại. Trên ISE ta sẽ bỏ tick xác thực PEAP để điện thoại không thể truy cập vào.

III. Thực hiện:

- Khâu chuẩn bị:
 - ✓ Cisco ISE
 - ✓ vWLC
 - ✓ Win Server cài DC
 - ✓ Chuẩn bị máy PC cài win 7 hoặc win 10

- ✓ Ta thực hiện cấu hình WLC:
 - ✓ Ta vào Wireless / General
 - ✓ Admin Status: Enable
 - ✓ AP Mode: FlexConnect

All APs > Details for APf40f.1b19.fb60

General		Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
General				Versions			
AP Name	APf40f.1b19.fb60	Primary Software Version	8.3.150.0				
Location	default location	Backup Software Version	0.0.0.0				
AP MAC Address	f4:0f:1b:19:fb:60	Predownload Status	None				
Base Radio MAC	38:1c:1a:9b:3d:b0	Predownload Version	None				
Admin Status	Enable	Predownload Next Retry Time	NA				
AP Mode	FlexConnect	Predownload Retry Count	NA				
AP Sub Mode	None	Boot Version	12.4.23.0				
Operational Status	REG	IOS Version	15.3(3)JD17\$				
Port Number	1	Mini IOS Version	0.0.0.0				
Venue Group	Unspecified	IP Config					
Venue Type	Unspecified	CAPWAP Preferred Mode	Ipv4 (Global Config)				
Add New Venue		DHCP Ipv4 Address	10.215.29.224				
Language		Static IP (Ipv4/Ipv6)	<input type="checkbox"/>				

- ✓ Tab High Availability:
- ✓ Primary Controller vWLC
- ✓ Management IP Address (Ipv4/Ipv6): 10.1.1.100

All APs > Details for APf40f.1b19.fb60

General		Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
	Name	Management IP Address(Ipv4/Ipv6)					
Primary Controller	vWLC	10.1.1.100					
Secondary Controller							
Tertiary Controller							
AP Failover Priority	Low						

- ✓ Trong Tab WLANS/ General
- ✓ Profile Name: LM-INTERNAL
- ✓ SSID: LM-INTERNAL
- ✓ Status: tick enable
- ✓ Interface/ InterfaceGroup(G): lm-user1
- ✓ Broadcast SSID: tick enable

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > New

Type: WLAN

Profile Name: LM-INTERNAL

SSID: LM-INTERNAL

ID: 3

- ✓ Trong tab Security/ Layer 2
- ✓ Layer 2 Security: WPA + WPA2
- ✓ WPA2 Policy: tick vào enable
- ✓ 802.1x: tick vào enable

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs > Edit 'LM-INTERNAL'

General **Security** QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: WPA+WPA2

MAC Filtering:

Fast Transition

Fast Transition: Adaptive

Over the DS:

Reassociation Timeout: 20 Seconds

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy:

WPA2 Policy:

WPA2 Encryption: AES TKIP CCMP256 GCMP128 GCMP256

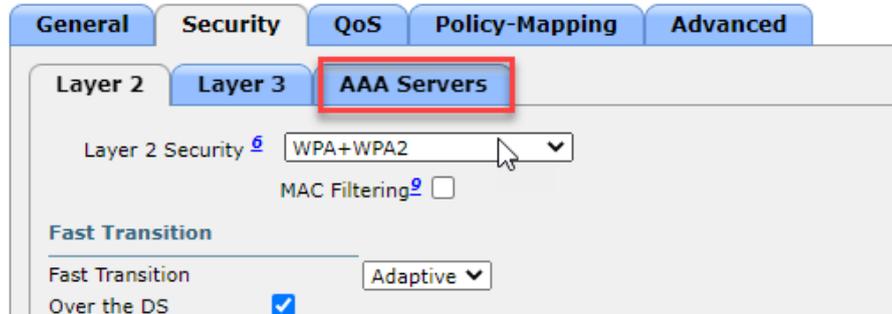
OSEN Policy:

Authentication Key Management

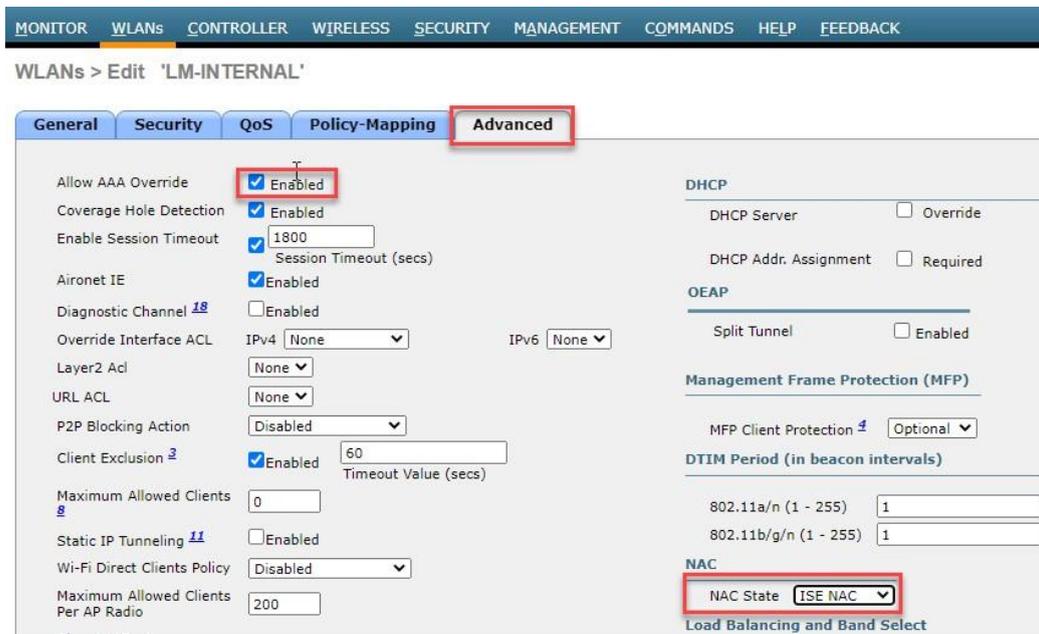
802.1X: Enable

- Tiếp tục ta chọn qua phần AAA Server
 - +Authentication Server, bật enabled
 - +Accounting Server, bỏ chọn

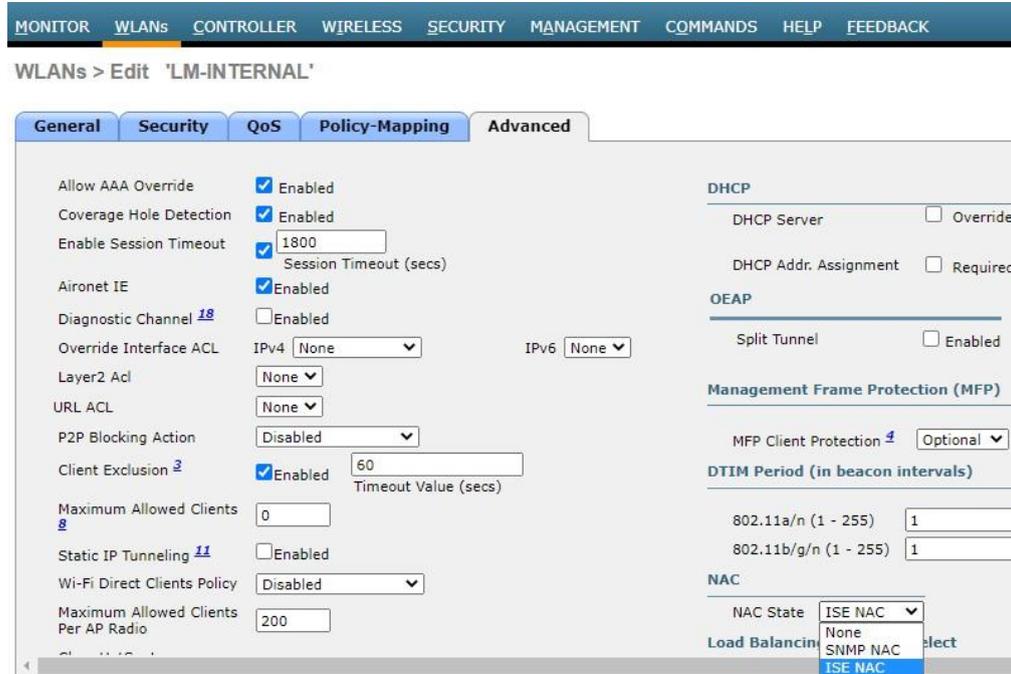
WLANs > Edit 'LM-INTERNAL'



- tiếp tục ta chọn qua phần WLAN/ Advanced

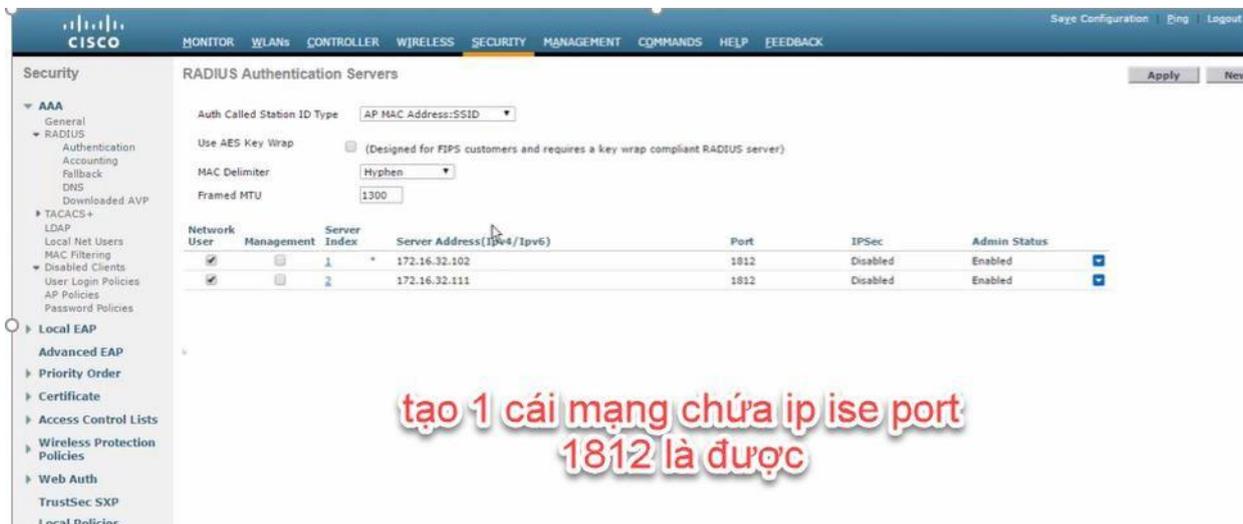


- ✓ Chuyển qua tab Advanced /
- ✓ Mục NAC State : Chọn ISE NAC

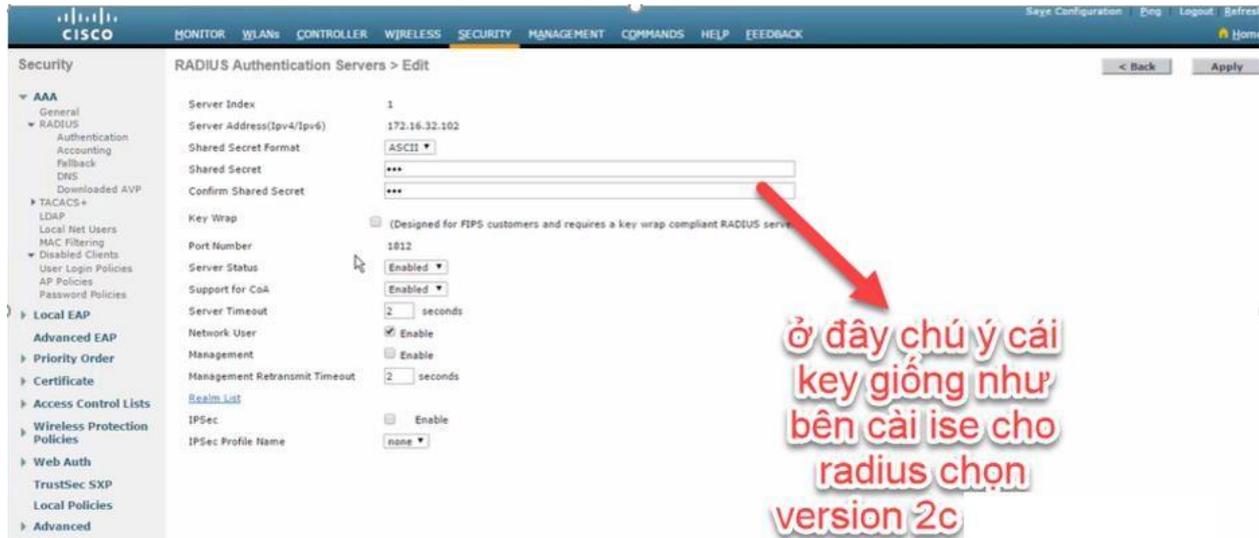


Chọn Tab Security / RADIUS Authentication Servers:

- ✓ Server address: 10.1.1.102
- ✓ Port: 1812
- ✓ Admin Status: Enable



✓ Cài đặt Shared Secret



The screenshot shows the 'RADIUS Authentication Servers > Edit' configuration page. The 'Shared Secret' field is highlighted with a red arrow and a text box containing the following text:

ở đây chú ý cái key giống như bên cài ise cho radius chọn version 2c

- ✓ Tại Tab Management
- ✓ Add New
- ✓ Community Name: cisco
- ✓ IP Address (Ipv4/Ipv6): 0.0.0.0
- ✓ IP Mask/Prefix length: 0.0.0.0
- ✓ Access Node: Read-Only
- ✓ Status: Enable



The screenshot shows the 'Management > SNMP v1 / v2c Community' configuration page. The table below shows the configuration for the 'cisco' community:

Community Name	IP Address(Ipv4/Ipv6)	IP Mask/Prefix Length	Access Mode	Status
cisco	0.0.0.0	0.0.0.0	Read-Only	Enable

- ✓ Tại Tab WLAN / Security / AAA Servers
- ✓ Mục Authentication Server: IP 10.1.1.200 Port 1812
- ✓ Mục Accounting Server: IP 10.1.1.200 Port 1813

WLANs > Edit 'LM_INTERNAL'

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 Override interface Enabled

Authentication Servers Enabled Accounting Servers Enabled EAP Parameters Enable

Server 1 IP:10.215.28.54, Port:1812 IP:10.215.28.54, Port:1813

Server 2 None None

Server 3 None None

Server 4 None None

Server 5 None None

Server 6 None None

RADIUS Server Accounting

Interim Update Interim Interval 0 Seconds

IDAP Servers

Foot Notes

1 Web Policy cannot be used in combination with IPsec
 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)

✓ Tại Tab Advance: các bạn sẽ tick đầy đủ như hình sau

WLANs > Edit 'LM_INTERNAL'

General Security QoS Policy-Mapping Advanced

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800 Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Disabled

Client Exclusion Enabled 60 Timeout Value (secs)

Maximum Allowed Clients 0

Static IP Tunneling Enabled

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

OEAP

Split Tunnel Enabled

Management Frame Protection (MFP)

MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

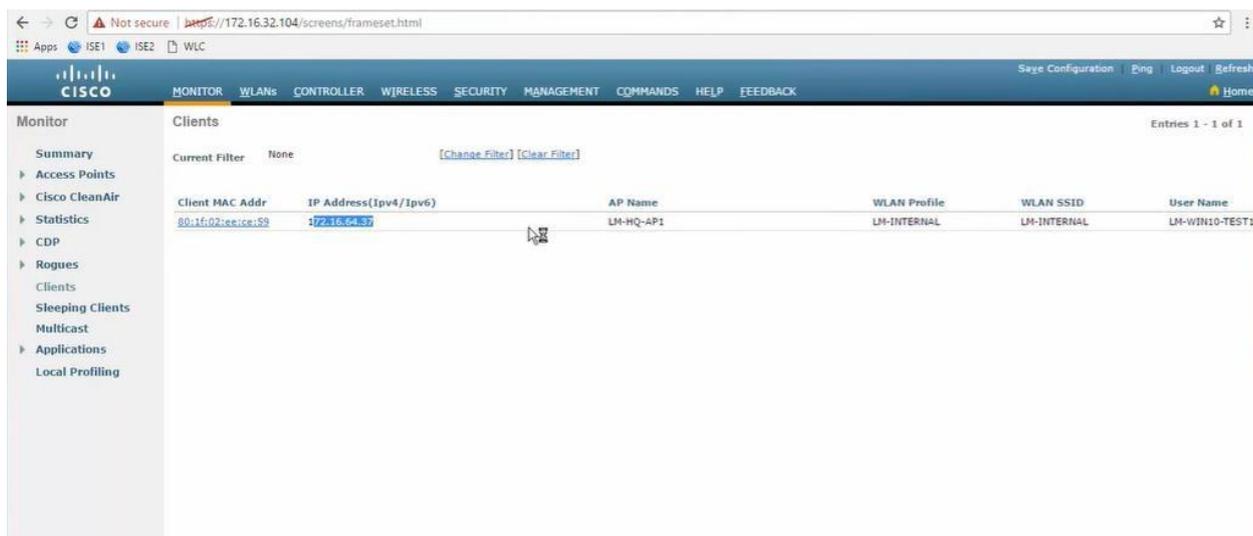
802.11b/g/n (1 - 255) 1

NAC

NAC State ISE NAC

General	Security	QoS	Policy-Mapping	Advanced
WiFi Direct Clients Policy	Disabled			
Maximum Allowed Clients Per AP Radio	200			
Clear HotSpot Configuration	<input type="checkbox"/> Enabled			
Client user idle timeout(15-100000)	<input type="checkbox"/>			
Client user idle threshold (0-10000000)	28800 Bytes			
Radius NAI-Realm	<input type="checkbox"/>			
11ac MU-MIMO	<input checked="" type="checkbox"/>			
Off Channel Scanning Defer				
Scan Defer Priority	0 1 2 3 4 5 6 7			
	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>			
Scan Defer Time(msecs)	100			
FlexConnect				
Local Client Load Balancing and Band Select				
Client Load Balancing <input type="checkbox"/>				
Client Band Select <input type="checkbox"/>				
Passive Client				
Passive Client <input type="checkbox"/>				
Voice				
Media Session Snooping <input type="checkbox"/> Enabled				
Re-anchor Roamed Voice Clients <input type="checkbox"/> Enabled				
KTS based CAC Policy <input type="checkbox"/> Enabled				
Radius Client Profiling				
DHCP Profiling <input checked="" type="checkbox"/>				
HTTP Profiling <input checked="" type="checkbox"/>				
Local Client Profiling				
DHCP Profiling <input checked="" type="checkbox"/>				
HTTP Profiling <input checked="" type="checkbox"/>				
Universal AP Admin Support				
Universal AP Admin <input type="checkbox"/>				

✓ Tại Tab MONITOR: ta sẽ quan sát được MAC của thiết bị Client đã join



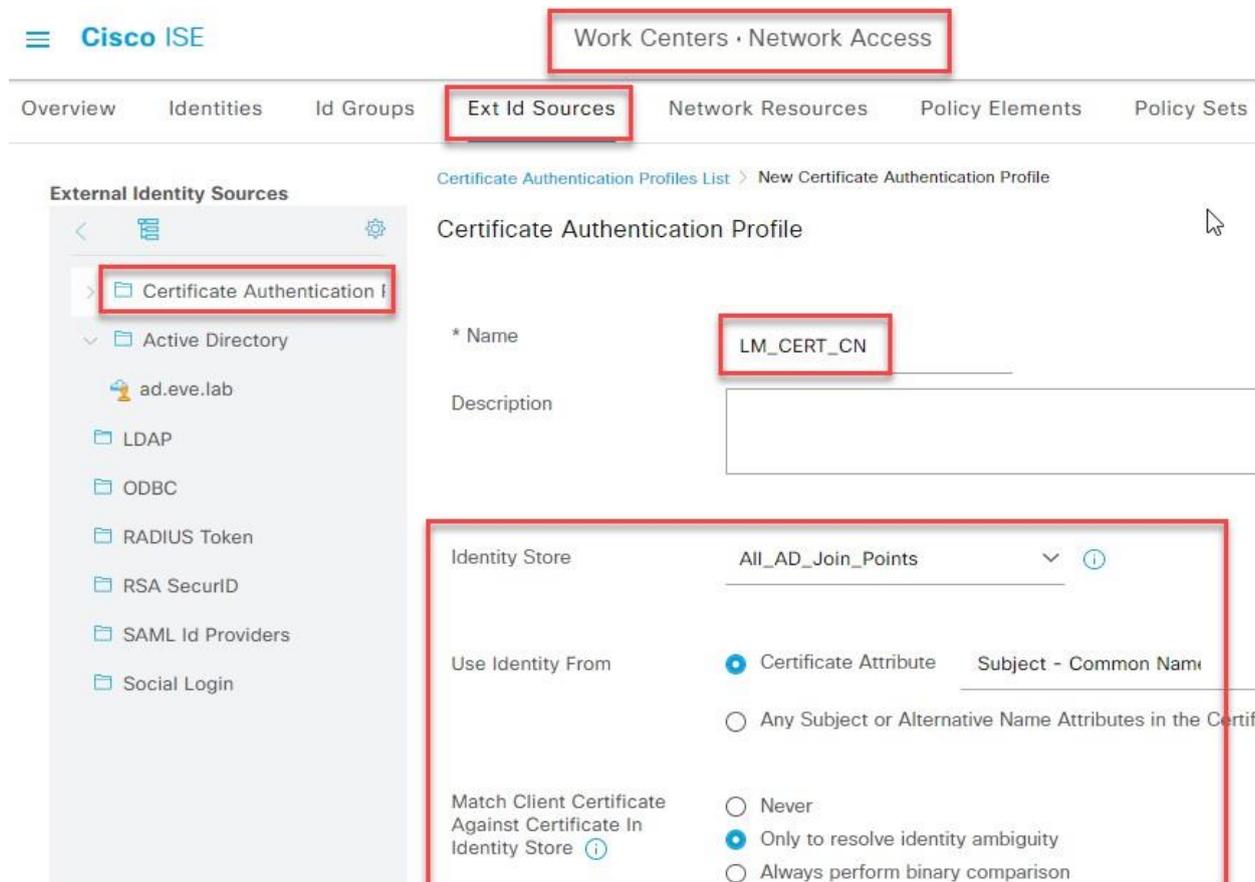
✓ Quay lại Cisco ISE

✓ Ta vào Mục Work Center / Network Access / Ext id Sources / Certificate Authentication

✓ Ta tạo một Certificate Authentication Profile

✓ Name: LM_CERT_ON

- ✓ Identity Store: All_AD_Join_Points
- ✓ User Identity From: Certificate Attribute: Subject-Common
- ✓ Match Client Certificate Against: tick vào Only to resolve ambiguity



- ✓ Ta vào Mục Work Center / Network Access / Identities / Identity Source Sequences
- ✓ Name: CERT_AD_LOCAL
- ✓ Certificate Based Authentication: tick vào Select Certificate Authentication Profile: LM_CERT_CN
- ✓ Authentication Search List: add các identity source (ad.eve.lab; Internal Uses; Internal Endpoints)

[Identity Source Sequences List](#) > [New Identity Source Sequence](#)

Identity Source Sequence

Identity Source Sequence

* Name

Certificate Based Authentication

Select Certificate Authentication Profile

☰ Cisco ISE Administration · Identity Management

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

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Guest Users	ad.eve.lab
All_AD_Join_Points	Internal Users
	Internal Endpoints

Navigation buttons: > < >> << (Available to Selected) and < > << >> (Selected to Available)

- ✓ Ta vào Mục Work Center / Network Access / Ext Id Sources / Active Directory / ad.eve.lab / +Add
- ✓ eve.lab/WIRELESS USER
- ✓ eve.lab/Domain Computer
- ✓ eve.lab/Domain Users

✓ Ta vào Mục Work Center / Network Access / Network Resources / Network Devices/ + Add

- ✓ Network Devices
- ✓ Name: LM-WLC1
- ✓ IP Address: 10.1.1.100/23
- ✓ Location: MY_LAN
- ✓ Device Type: WLC

Cisco ISE Work Centers · Network Access

Overview Identities Id Groups Ext Id Sources **Network Resources** Policy Elements

Network Devices

Network Devices List > New Network Device

Network Devices

Name **LM-WLC1**

Description

IP Address * IP : 10.1.1.100 / 32

Location **My LAN** Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type **WLC** Set To Default

✓ Tick vào RADIUS Authentication Settings:

✓ Shared Secret: cisco

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret **cisco** Hide

Use Second Shared Secret ⓘ

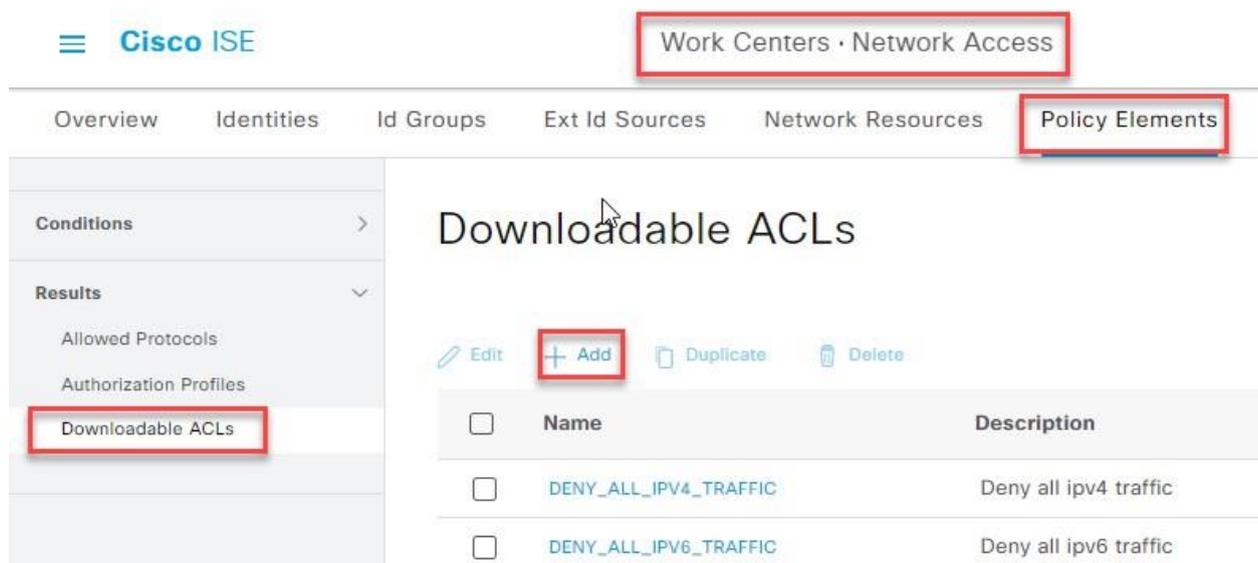
Second Shared Secret Show

CoA Port 1700 Set To Default

- ✓ Tick vào SNMP Settings:
- ✓ SNMP Version: 2c
- ✓ SNMP RO Community: cisco



- ✓ Ta vào Mục Work Center / Network Access / Policy Elements / Results / Downloadable ACLs / + Add



Name	Description
DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic

- ✓ Ta tạo một DACL:
- ✓ Name: DACL_COMPUTER
- ✓ DACL Content: permit ip any any

Downloadable ACL List > DACL_COMPUTER

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

12345678	permit ip any any
91011121	
31415161	
71819202	
12223242	
52627282	
93031323	
33435363	
73839404	
14243444	
54647484	
99999999	

Check DACL Syntax ⓘ

✓ Name: DACL_USER

✓ DACL Content: permit ip any any

Downloadable ACL List > DACL_USER

Downloadable ACL

* Name

Description

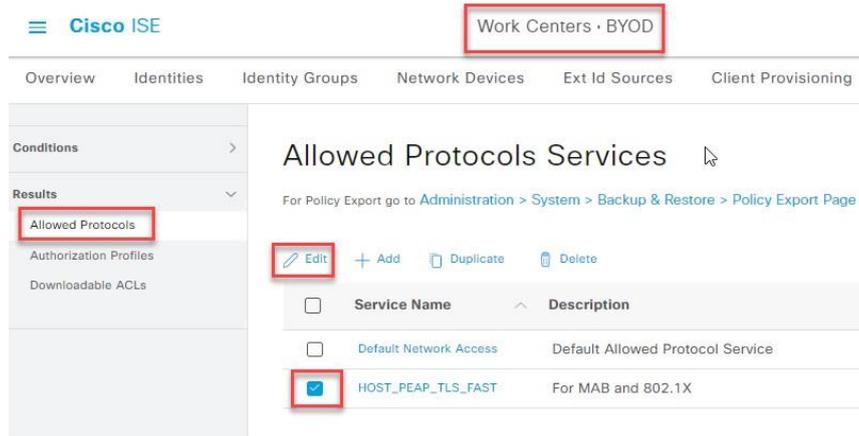
IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

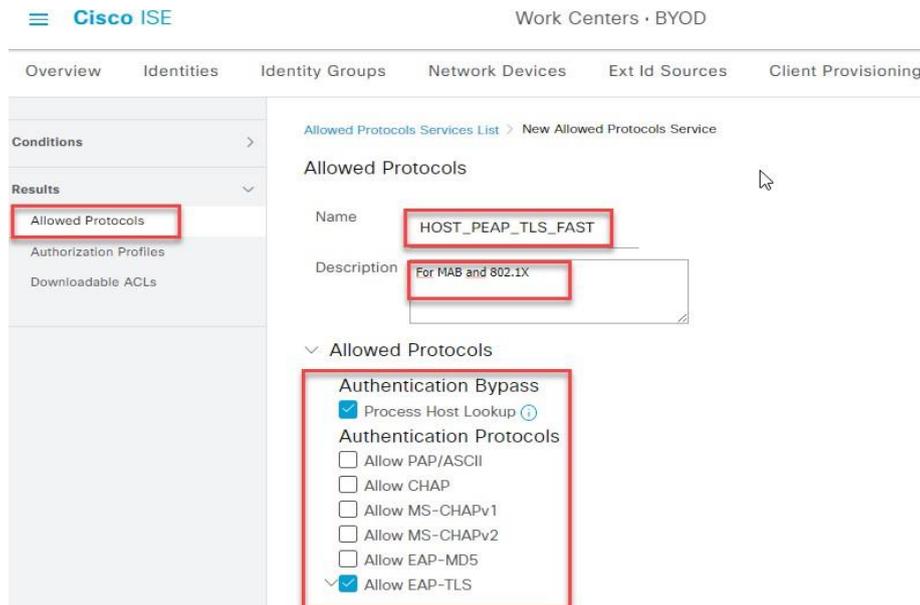
12345678	permit ip any any
91011121	
31415161	
71819202	
12223242	
52627282	
93031323	
33435363	
73839404	
14243444	
54647484	
99999999	

Check DACL Syntax ⓘ

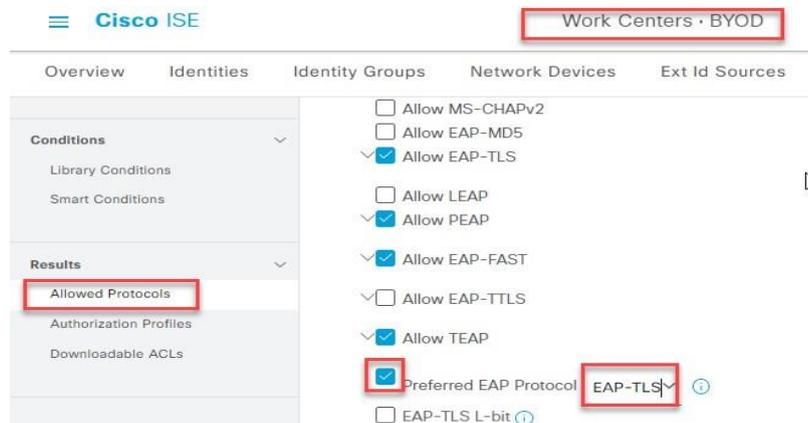
✓ Ta vào Mục Work Center / Network Access / Policy Elements / Allowed Protocols/ lick vào HOST_PEAAD_TLS_FAST/ edit



- ✓ Tại phần edit của HOST_PEAP_TLS_FAST
- ✓ Description: For MAB and 802.1X
- ✓ Các bạn sẽ tick đầy đủ như hình.



- ✓ Tại mục Preferred EAP Protocol: EAP-TLS



- ✓ Tick vào tab Allow EAP-TLS
- ✓ Tick vào Allow Authentication of expired certificates
- ✓ Tick vào Enable Stateless Session Resume
- ✓ Session ticket time to live: **2 Weeks**
- ✓ Proactive session ticket update: **10%**

▼ Allow EAP-TLS

- Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- Enable Stateless Session Resume
Session ticket time to live: Weeks
- Proactive session ticket update will occur after % of Time To Live has expired
- Allow LEAP

- ✓ Tab Allow PEAP
- ✓ Bỏ chọn mục Require cryptobinding TLV

▼ Allow PEAP

PEAP Inner Methods

- Allow EAP-MS-CHAPv2
 Allow Password Change Retries: (Valid Range 0 to 3)
- Allow EAP-GTC
 Allow Password Change Retries: (Valid Range 0 to 3)
- Allow EAP-TLS
 Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- Require cryptobinding TLV **bỏ chọn mục này**
- Allow PEAPv0 only for legacy clients

- ✓ Tick vào Allow EAP-FAST
- ✓ Ta sẽ tick đầy đủ vào

Allow EAP-FAST

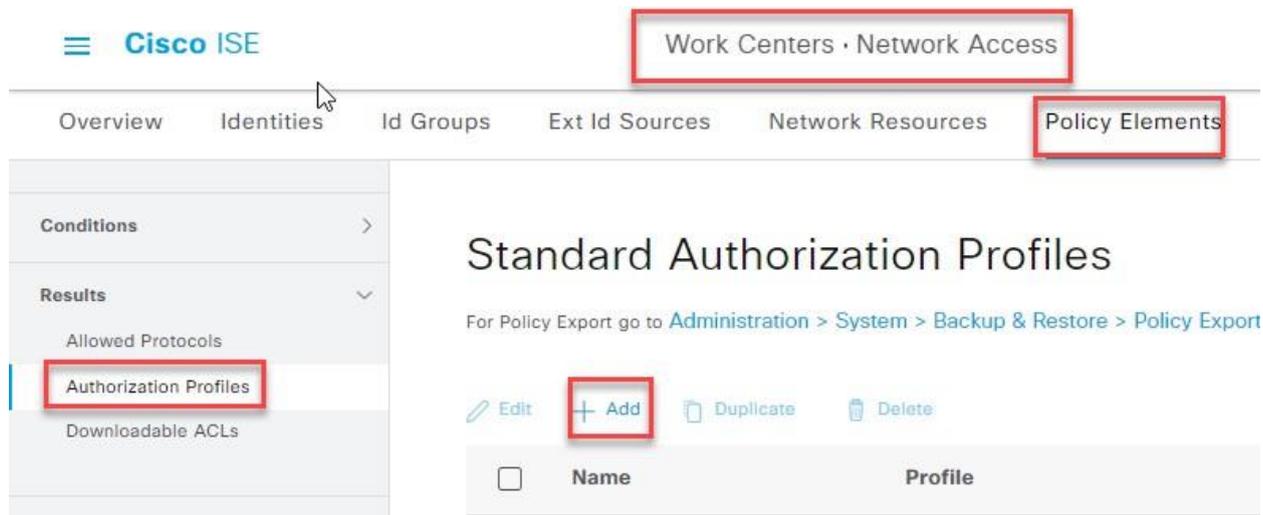
EAP-FAST Inner Methods

 Allow EAP-MS-CHAPv2 Allow Password Change Retries (Valid Range 0 to 3) Allow EAP-GTC Allow Password Change Retries (Valid Range 0 to 3) Allow EAP-TLS Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Use PACs Don't Use PACs Accept client certificate during tunnel establishment Allow Machine Authentication Enable EAP Chaining Allow TEAP

TEAP Inner Methods

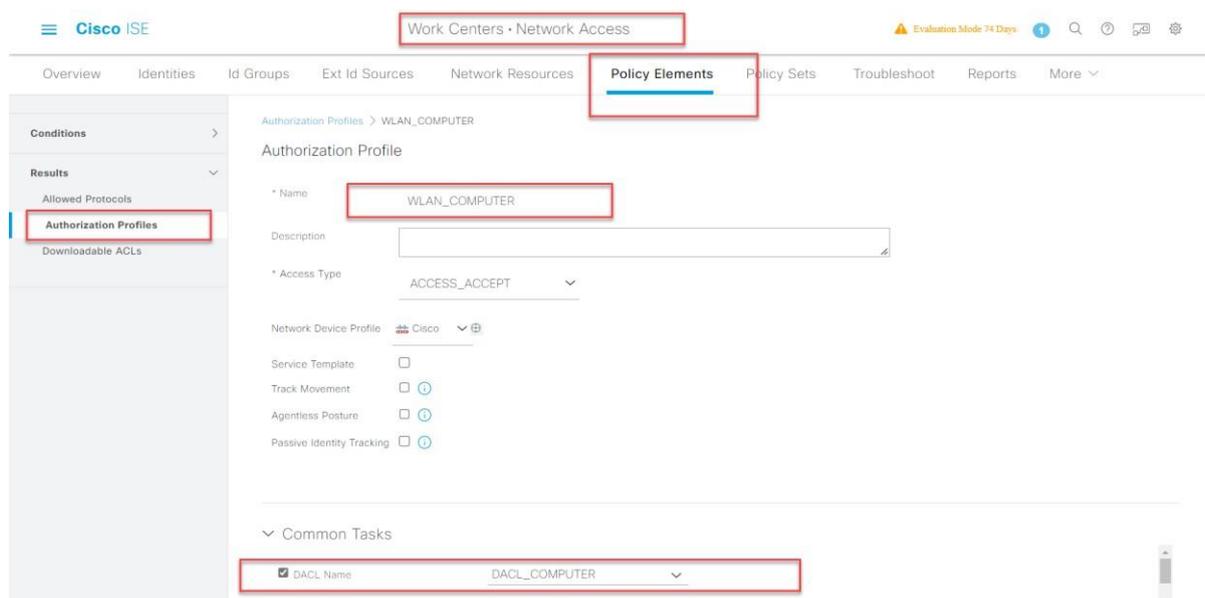
 Allow EAP-MS-CHAPv2 Allow Password Change Retries (Valid Range 0 to 3)  Allow EAP-TLS Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Allow downgrade to MSK  Accept client certificate during tunnel establishment  Enable EAP Chaining  Preferred EAP Protocol  EAP-TLS L-bit  Allow weak ciphers for EAP  Require Message-Authenticator for all RADIUS Requests 

✓ Ta vào Mục Work Center / Network Access / Policy Elements /
Authorization Profiles/ + Add



✓ Name: WLAN_COMPUTER

✓ DACL Name: DACL_COMPUTER



✓ Name: wlan_user

✓ DACL Name: DACL_USER

Authorization Profiles > WLAN_USER

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

DACL Name

✓ Ta vào Mục Work Center / Network Access / Policy Sets

✓ Tạo tạo một Policy mới:

✓ Name: WLAN

✓ Conditions:

- DEVICE:Device Type EQUALS All Device Types#WLC
- Radius-NAS-Port-Type EQUALS IEEE 802.11
- Allowed Protocols / Server Sequence: HOST_PEAP_TLS_FAST

Work Centers · Network Access

Overview Identities Id Groups Ext Id Sources Network Resources Policy Elements **Policy Sets** Troubleshoot More

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	WLAN		AND DEVICE-Device Type EQUALS All Device Types#WLC RADIUS-NAS-Port-Type EQUALS Wireless - IEEE 802.11	HOST_PEAP_TLS_FAST	0	⚙️	➔
⊗	LM WIRED		AND DEVICE-Device Type EQUALS All Device Types#SWITCH RADIUS-NAS-Port-Type EQUALS Ethernet	HOST_PEAP_TLS_FAST	0	⚙️	➔

Vũ Thị Thu Ngân (2001181221@hufi.edu.vn) is signed in

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
+	WLAN		AND DEVICE-Device Type EQUALS All Device Types#WLC RADIUS-NAS-Port-Type EQUALS Wireless - IEEE 802.11	HOST_PEAP_TLS_FAST	0

- > Authentication Policy (3)
- > Authorization Policy - Local Exceptions
- > Authorization Policy - Global Exceptions
- > Authorization Policy (7)

✓ Tab Authentication Policy:

✓ Ta add policy MAB và DOT1X như hình

Authentication Policy (3)

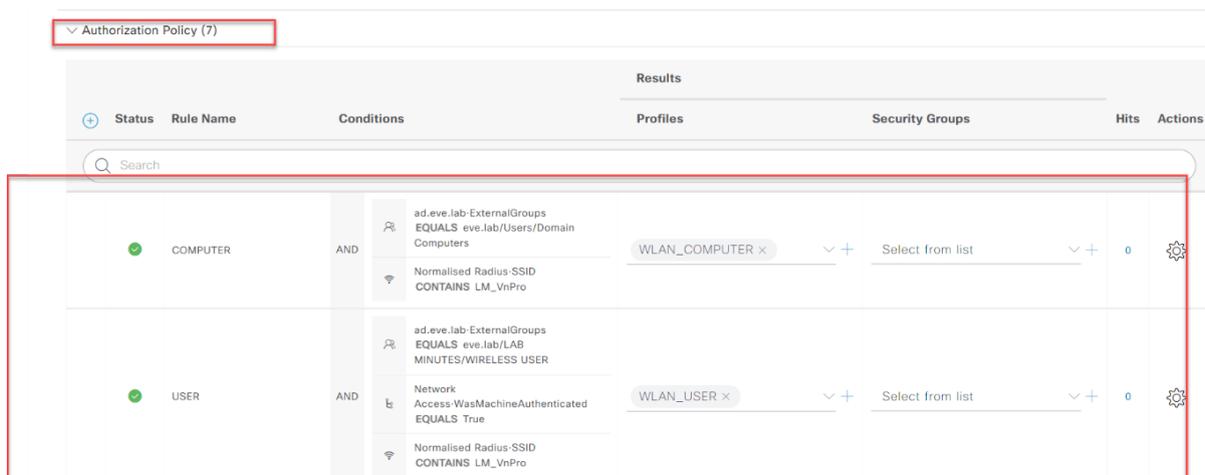
Status	Rule Name	Conditions	Use	Hits	Actions
+	MAB	Wireless_MAB	Internal Endpoints > Options	0	⚙️
⋮	DOT1X	Wireless_802.1X	CERT_AD_LOCAL > Options	0	⚙️
+	Default		All_User_ID_Stores > Options	0	⚙️

- ✓ Tab Authorization Policy
- ✓ Ta tạo 2 mục phân quyền: COMPUTER VÀ USER

✓ Rule name: COMPUTER

✓ Condition:

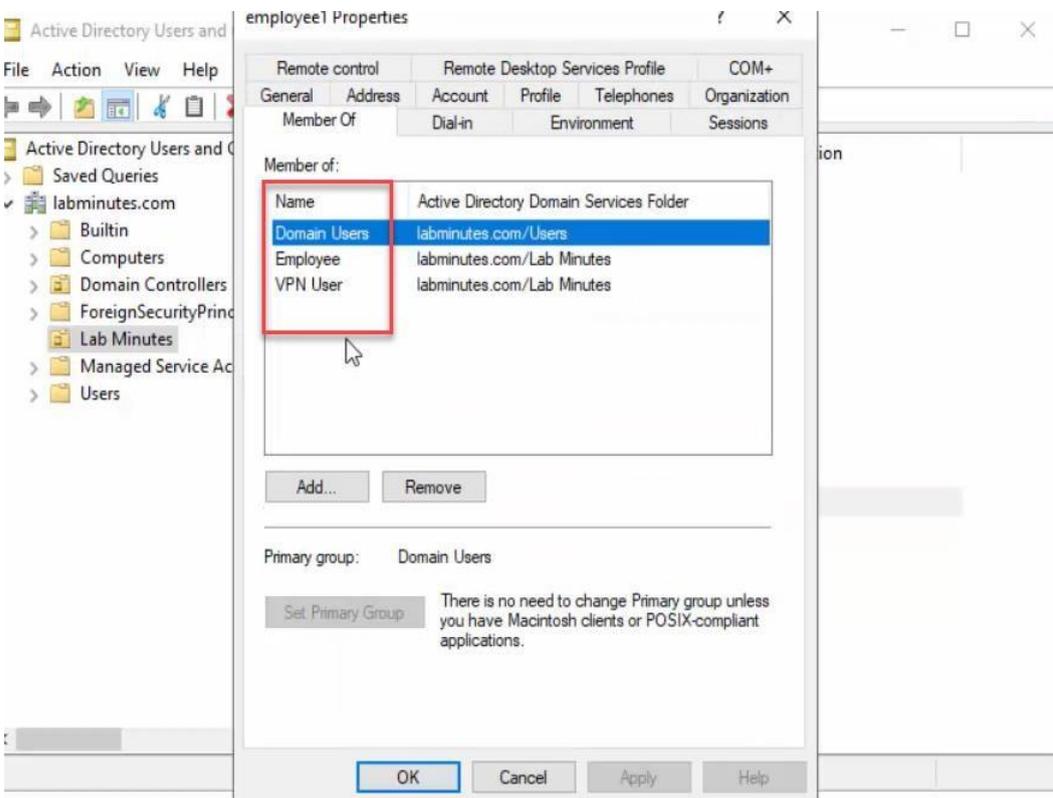
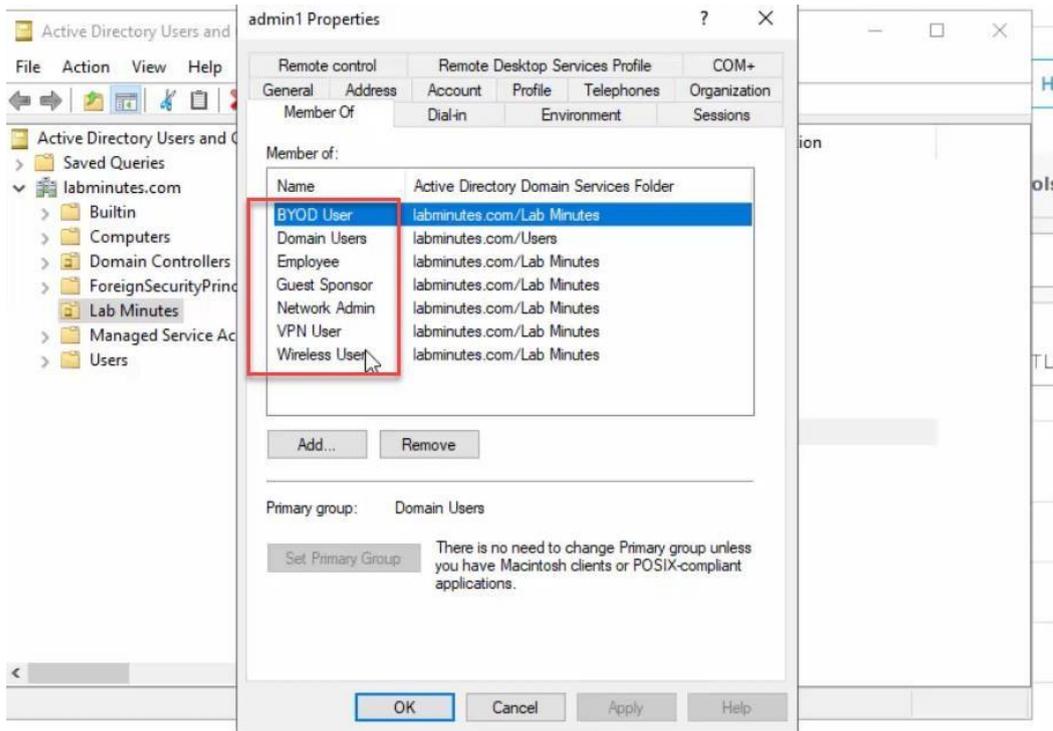
- ad.eve.lab ExternalGroups EQUALS eve.lab/Users/Domain Computers
- and Normalised Radius-SSID CONTAINS LM_VnPro



The screenshot shows a table of Authorization Policies. The table has columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. Two rules are listed:

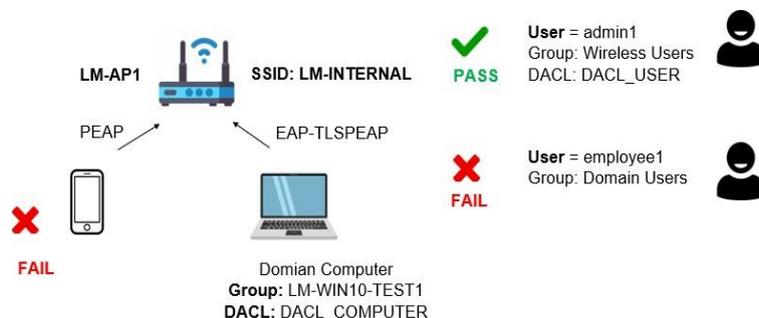
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	COMPUTER	ad.eve.lab-ExternalGroups EQUALS eve.lab/Users/Domain Computers AND Normalised Radius-SSID CONTAINS LM_VnPro	WLAN_COMPUTER x	Select from list	0	⚙️
✓	USER	ad.eve.lab-ExternalGroups EQUALS eve.lab/LAB MINUTES/WIRELESS USER AND Network Access-WasMachineAuthenticated EQUALS True AND Normalised Radius-SSID CONTAINS LM_VnPro	WLAN_USER x	Select from list	0	⚙️

- ✓ Tại Domain Controller ta tạo
 - + **admin1**
 - + **employee1**
- ✓ Các group Wireless USER, NHANVIEN
- ✓ Add **admin1** vào USER DC
- ✓ Add **employee1** vào USER DC

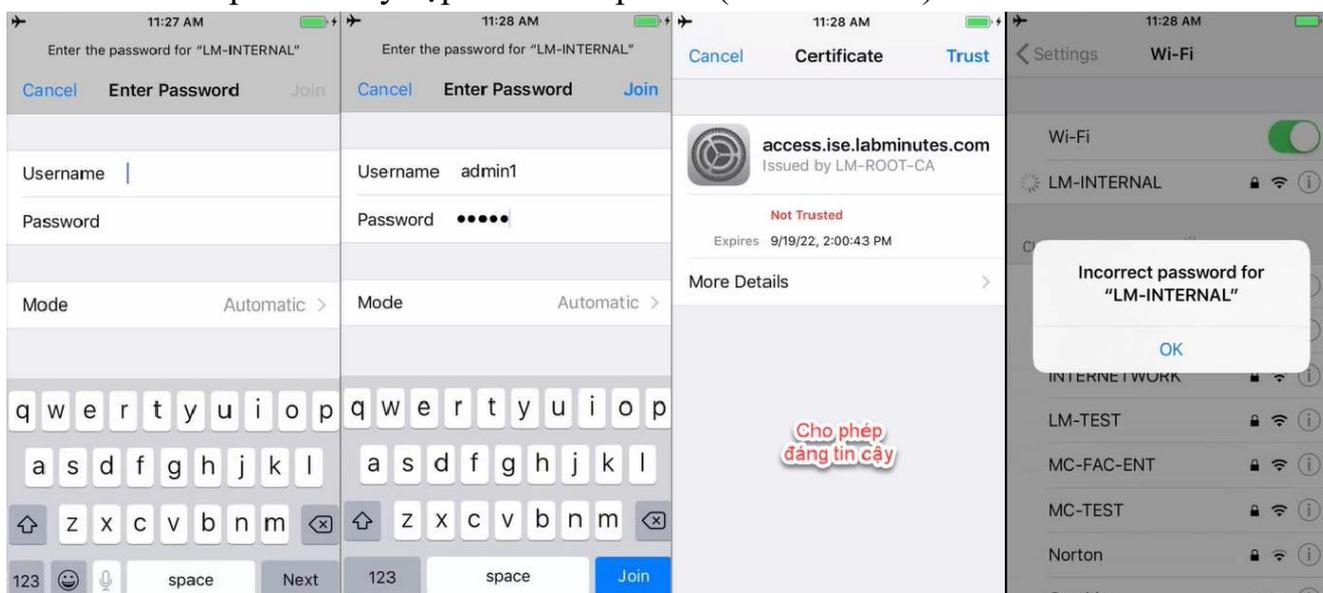


- ✓ Tiến hành đăng nhập vào DC coi các user đã tạo có thành công không, do bản winserver2016, dễ gặp lỗi khi tạo user, nếu tạo user thành công đăng nhập rồi ta hãy add vào các group.

Ta sẽ không cho phép các User thuộc Group: Wireless User truy cập:



Ta sẽ tiếp hành truy cập wifi trên iphone (user: admin1)



- ✓ Vào mục Operation/ RADIUS/ Live logs
- ✓ Khi này ta sẽ thấy xác thực **fail**

Cisco ISE Operations - RADIUS Evaluation Mode 89 Days

Live Logs Live Sessions

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authenti...	Authoriz...
X				Identity	Endpoint ID	Endpoint Profile	Authenticat	Authorizati
Sep 27, 2020 11:28:43.4...	●	🔒		admin1	4C:57:CA:56:EE:...		WLAN >> ...	WLAN

Overview

Event	5400 Authentication failed
Username	admin1
Endpoint Id	4C:57:CA:56:EE:B5
Endpoint Profile	Apple-Device
Authentication Policy	WLAN >> DOT1X
Authorization Policy	WLAN >> Default
Authorization Result	DenyAccess

Authentication Details

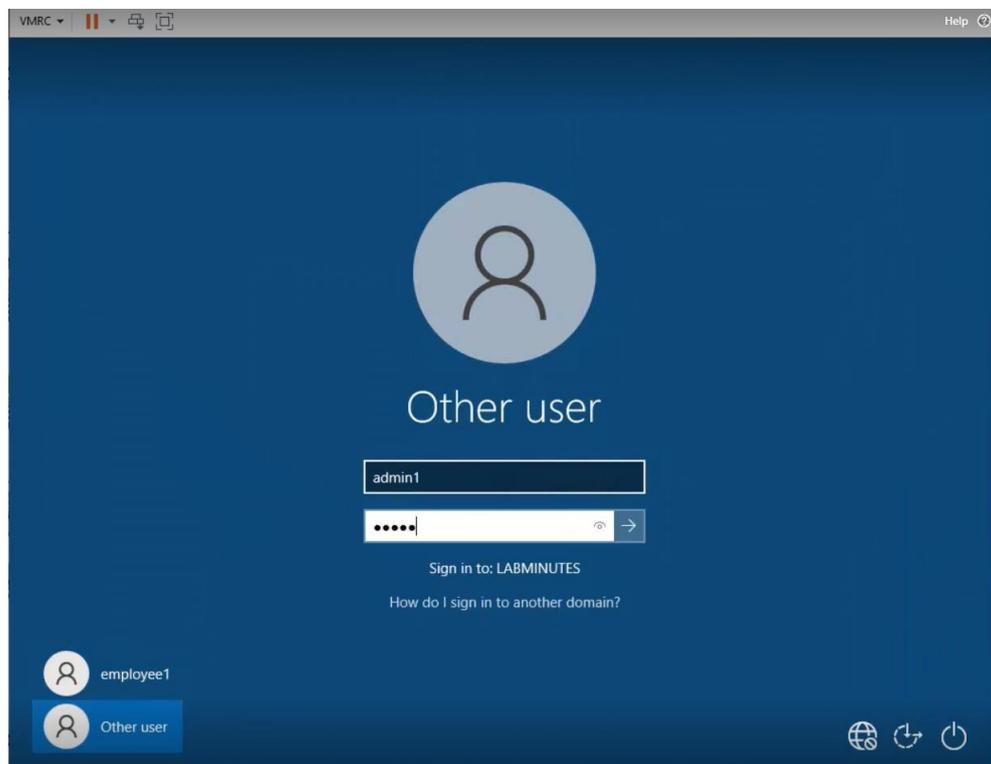
Source Timestamp	2020-09-27 11:30:03.69
Received Timestamp	2020-09-27 11:30:03.69
Policy Server	LM-ISE1
Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile

Authorization Profile with ACCESS_REJECT attribute was selected as result of the evaluation authorization rule. Check...

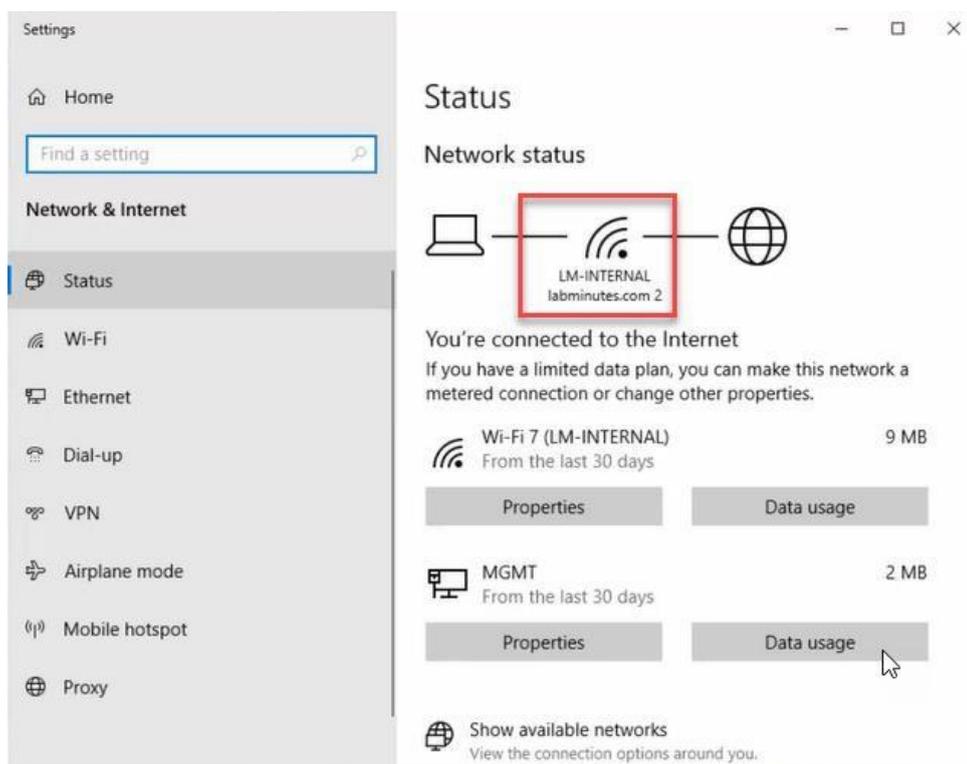
```

12304 Extracted EAP-Response containing PEAP challenge-response
24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036 Evaluating Authorization Policy
    
```

- ✓ Thử kết quả kết nối qua laptop
- ✓ Truy cập vào user: admin1

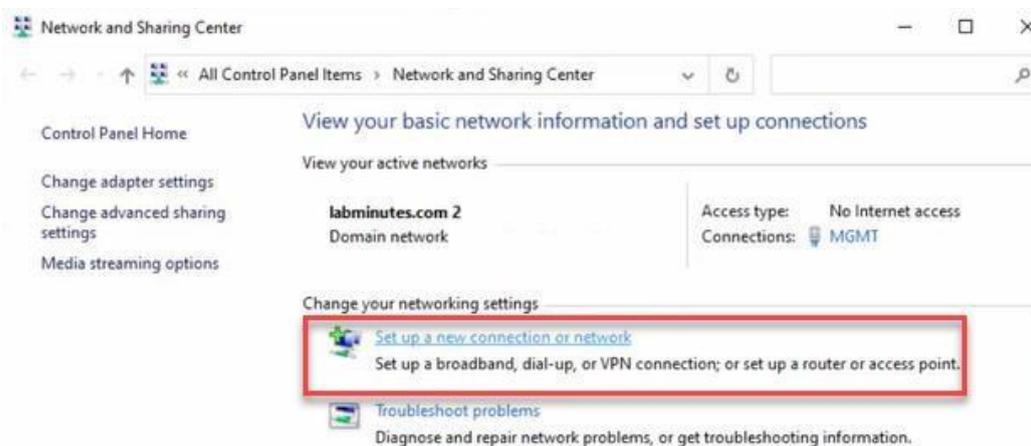


✓ Vào phần setting / Network Status/ kết nối wifi LM-INTERNAL



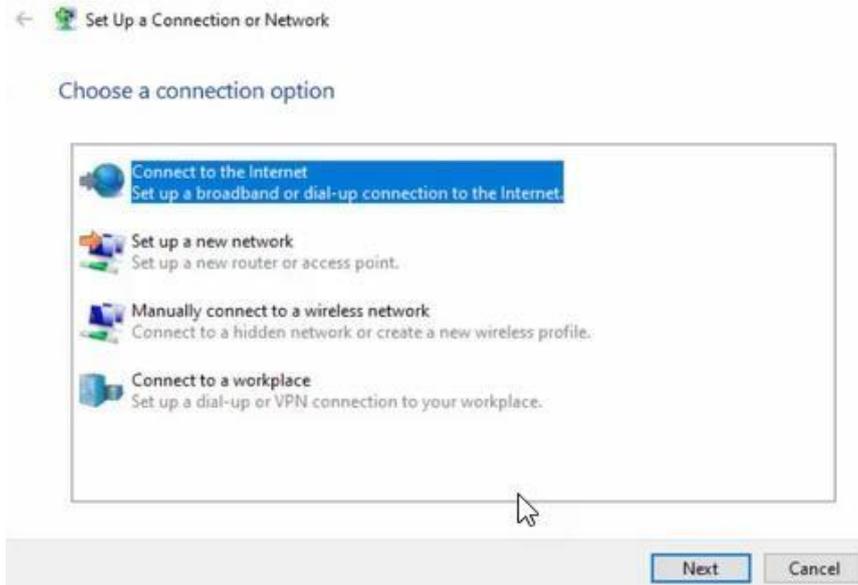
✓ Chuyển hướng sang Network and Sharing Center”

✓ Lick vào Set up a new connection or network

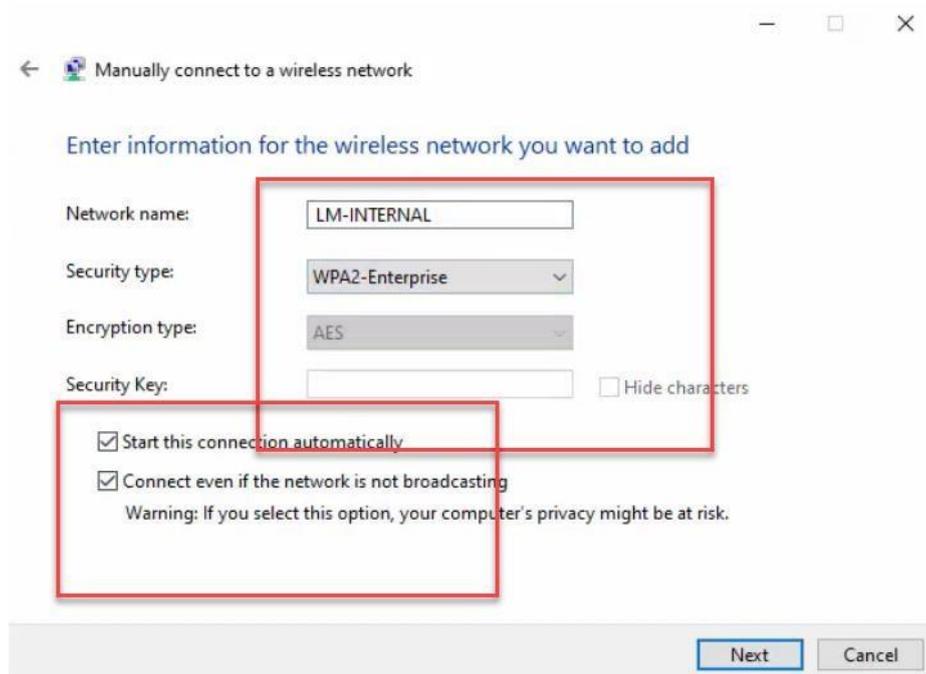


✓ Trong mục Set Up A Connection or Network

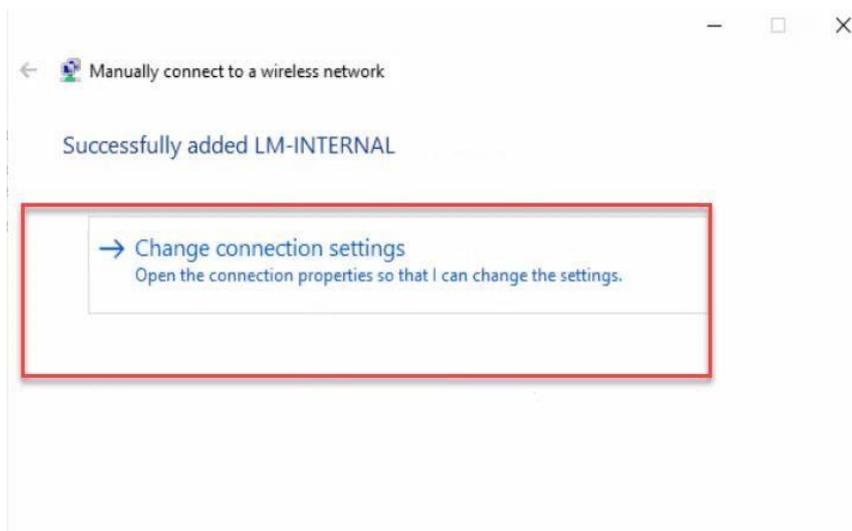
✓ Chọn Manually connect to a wireless network



- ✓ Network name: LM-INTERNAL
- ✓ Security type: WPA2-Enterprise
- ✓ Tick vào Start this connection automatically
- ✓ Tick vào Connect even if the network is not broadcasting
- ✓ Chọn next



✓ Lick vào Change added LM-INTERNAL

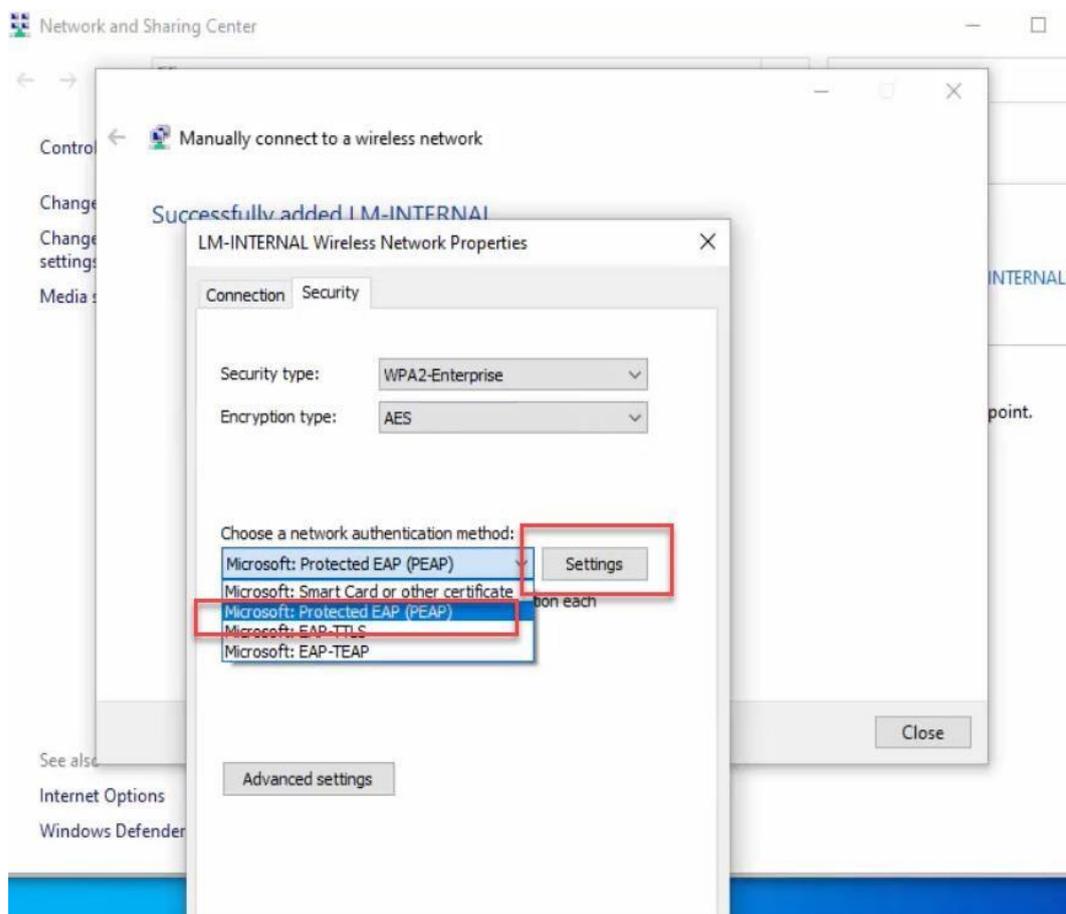


✓ Tại tab Security

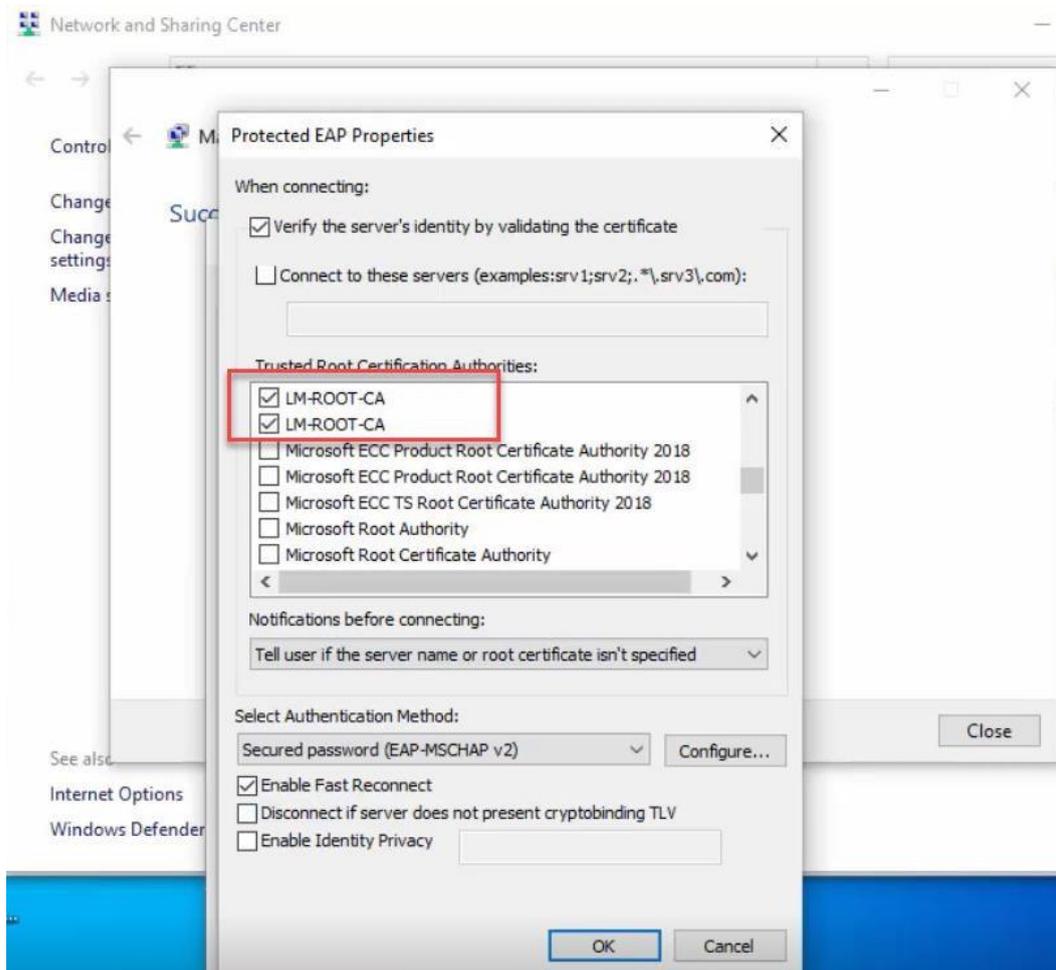
✓ Mục Choose a network authentication method:

✓ Microsoft: Protected EAP (PEAP)

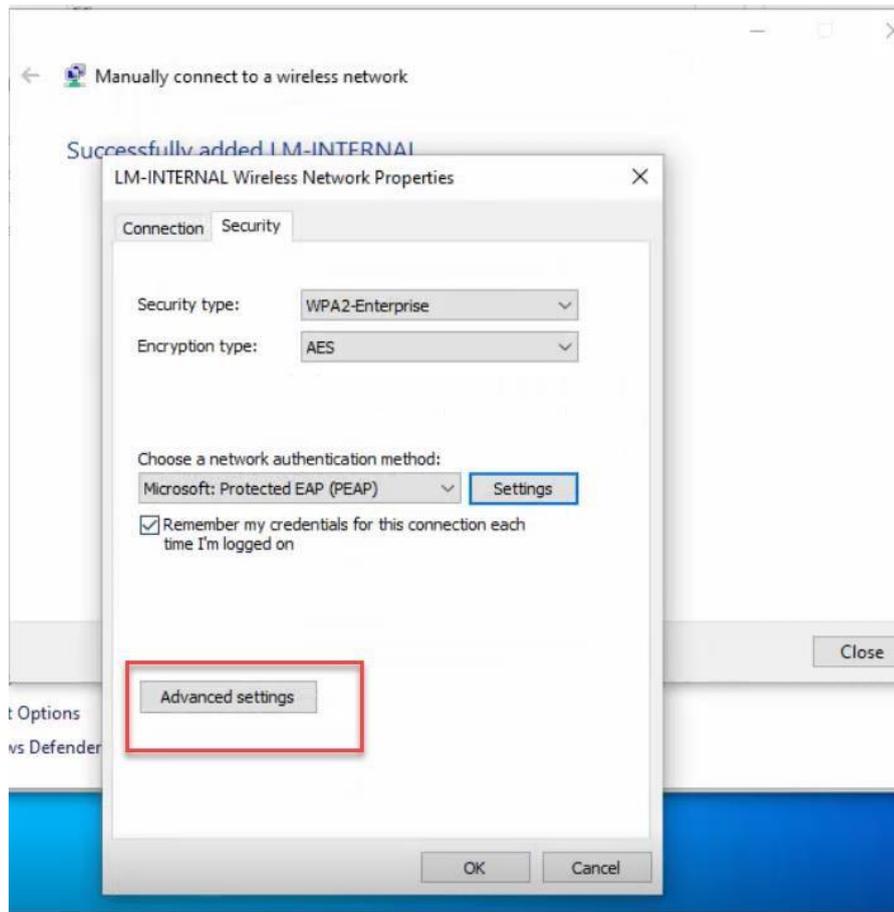
✓ Ta chọn tiếp Setting



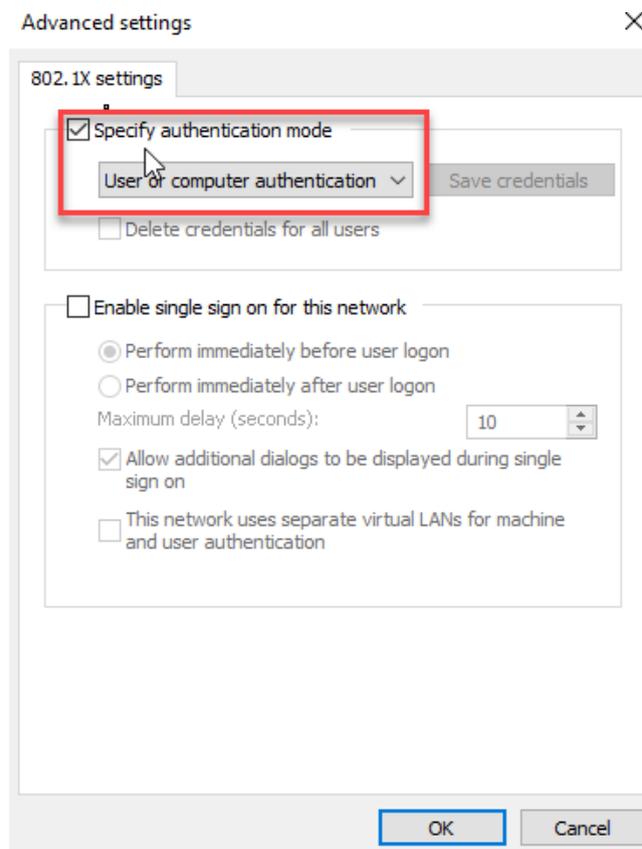
- ✓ Tại mục Setting:
- ✓ Trusted Root Certification Authorities:
- ✓ Tick vào LM-ROOT-CA như hình:



- ✓ Lick vào Advanced settings:

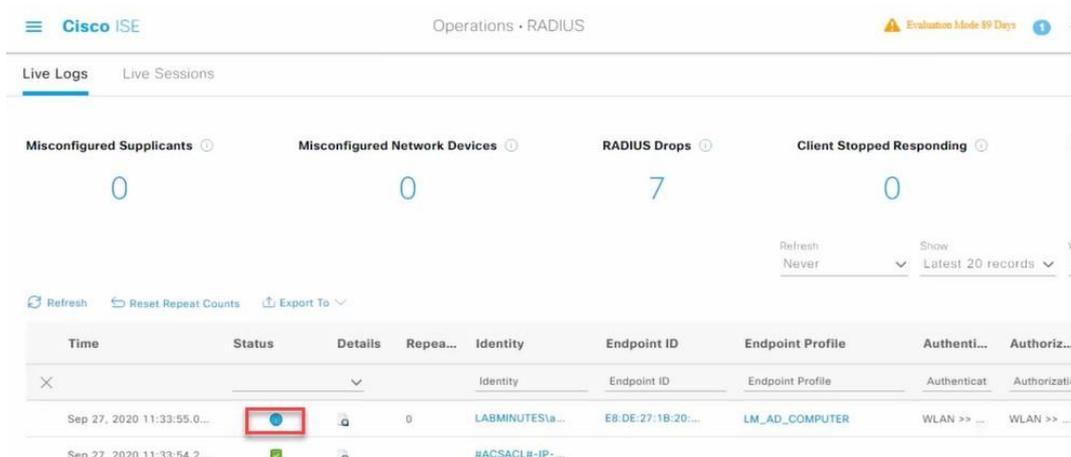


✓ Lick vào ô Specify authentication mode: User or computer authentication



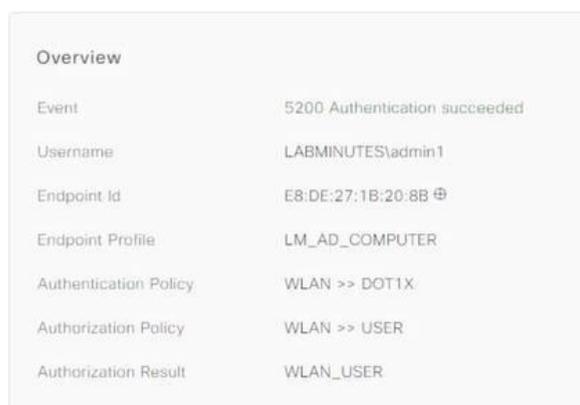
✓ Truy cập vào ISE/ Operation / RADIUS

✓ Ta sẽ thấy xác thực thành công



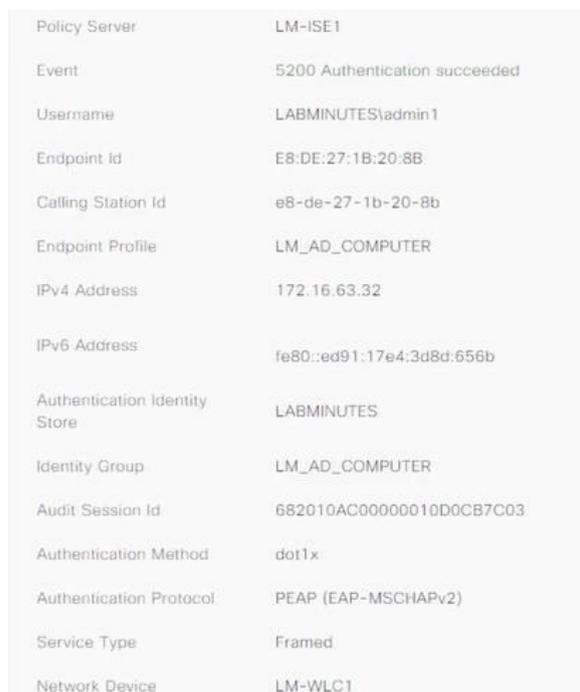
The screenshot shows the Cisco ISE Operations - RADIUS page. At the top, there are four summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (7), and Client Stopped Responding (0). Below these is a table of Live Logs. The table has columns for Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint Profile, Authenti..., and Authoriz... The first row in the table shows a successful authentication event on Sep 27, 2020 at 11:33:55.0... with a status of 'Success' (indicated by a green circle icon) and a red box highlighting the status icon. The identity is LABMINUTES\admin1 and the endpoint ID is E8-DE-27-1B-20-8B.

✓ Ta xem lại thông tin device



The screenshot shows the Overview section of a device's authentication details. It lists the following information:

- Event: 5200 Authentication succeeded
- Username: LABMINUTES\admin1
- Endpoint Id: E8:DE:27:1B:20:8B
- Endpoint Profile: LM_AD_COMPUTER
- Authentication Policy: WLAN >> DOT1X
- Authorization Policy: WLAN >> USER
- Authorization Result: WLAN_USER



The screenshot shows the Policy Server section of a device's authentication details. It lists the following information:

- Policy Server: LM-ISE1
- Event: 5200 Authentication succeeded
- Username: LABMINUTES\admin1
- Endpoint Id: E8:DE:27:1B:20:8B
- Calling Station Id: e8-de-27-1b-20-8b
- Endpoint Profile: LM_AD_COMPUTER
- IPv4 Address: 172.16.63.32
- IPv6 Address: fe80::ed91:17e4:3d8d:656b
- Authentication Identity Store: LABMINUTES
- Identity Group: LM_AD_COMPUTER
- Audit Session Id: 682010AC00000010D0CB7C03
- Authentication Method: dot1x
- Authentication Protocol: PEAP (EAP-MSCHAPv2)
- Service Type: Framed
- Network Device: LM-WLC1