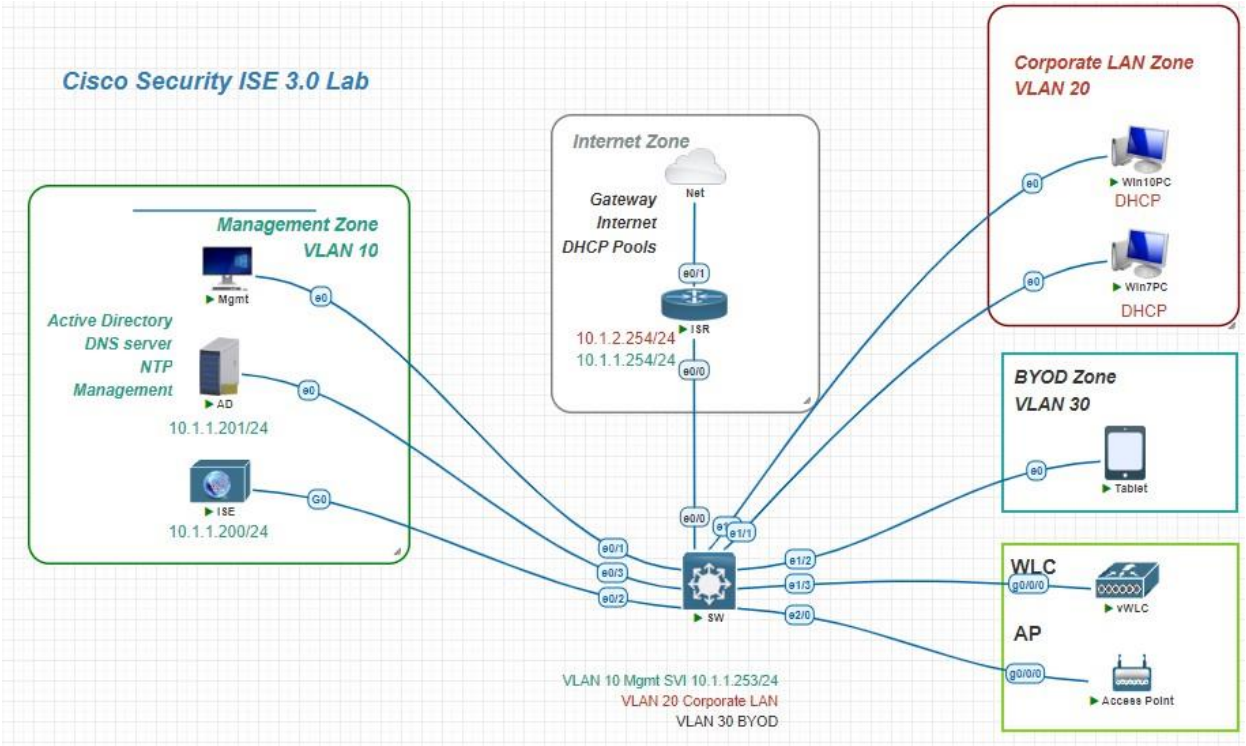
LAB - WIRELESS 802.1X WITH EAP-TLS AND PEAP

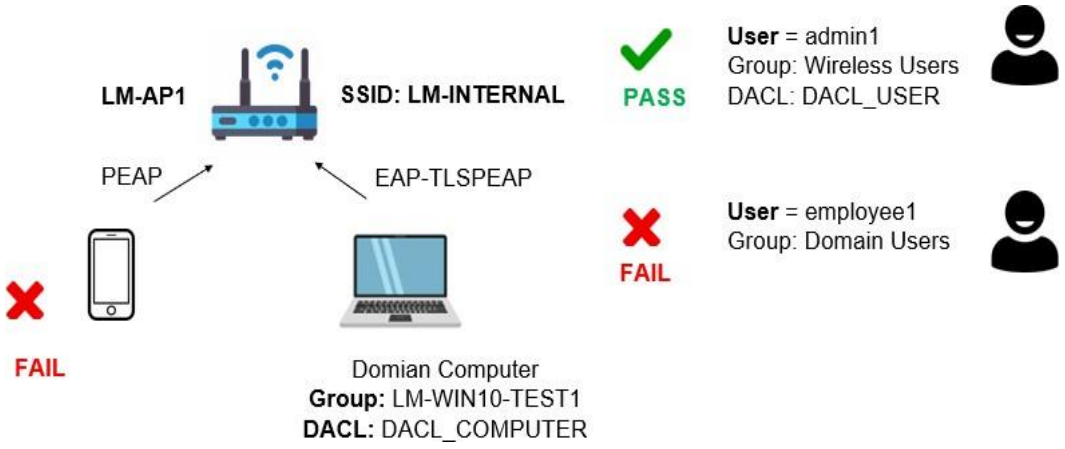
I. Sơ đồ:



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)

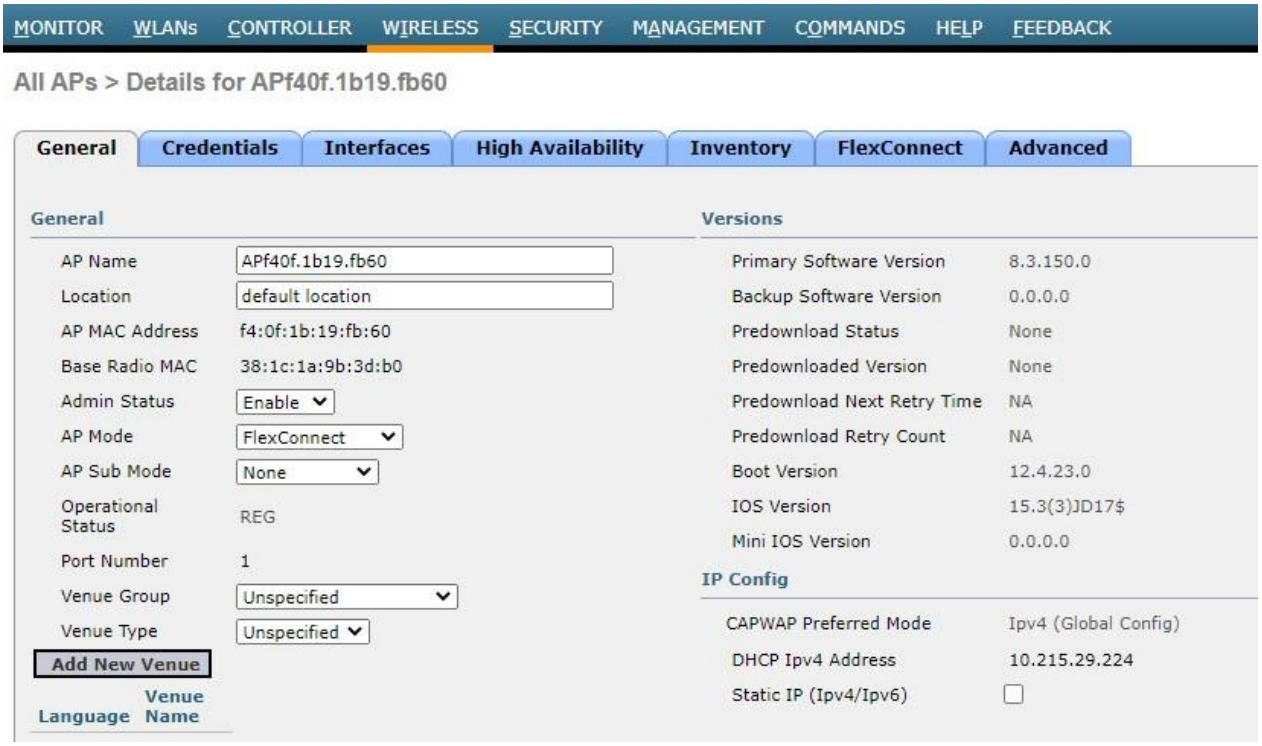


Ta sẽ tạo SSID: LM-INTERNAL cho phép user admin1 group Wireless Users truy cập vào mạng wifi. Trong trường này ta ví dụ Phòng tài chính chỉ cho phép dùng laptop không được dùng điện thoại. Trên ISE ta sẽ bỏ tick xác thực PEAP để điện thoại không thể truy cập vào.

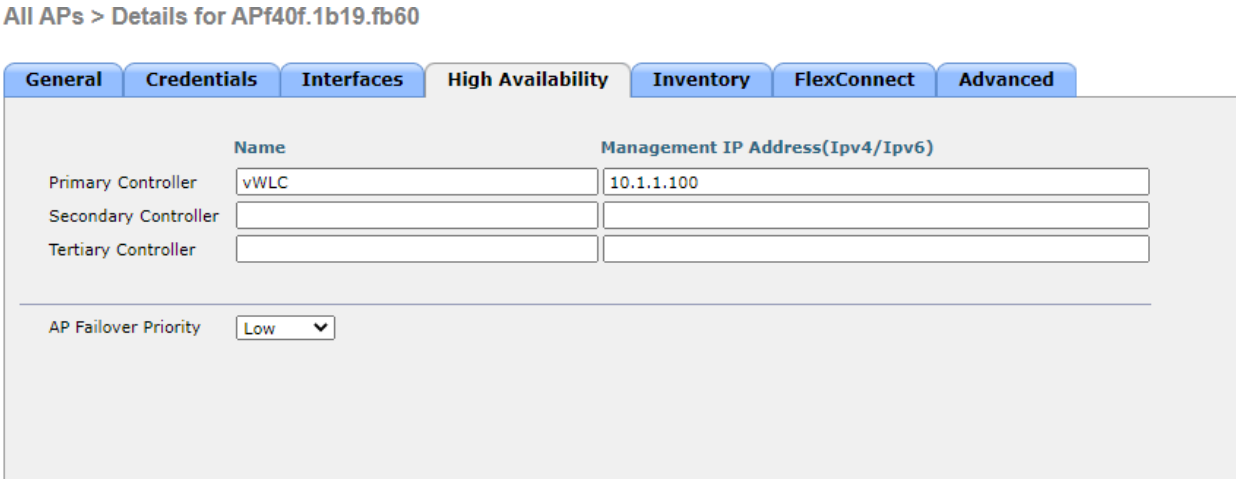
III. Thực hiện:

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

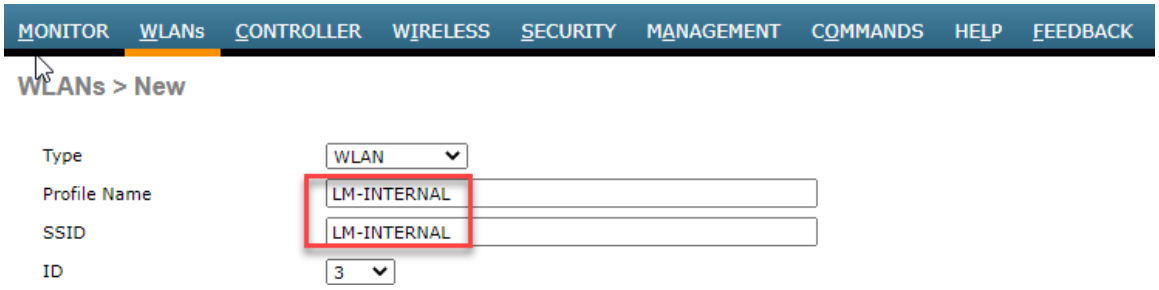
  - ✓ Ta thực hiện cấu hình WLC:
  - ✓ Ta vào Wireless / General
  - ✓ Admin Status: Enable
  - ✓ AP Mode: FlexConnect



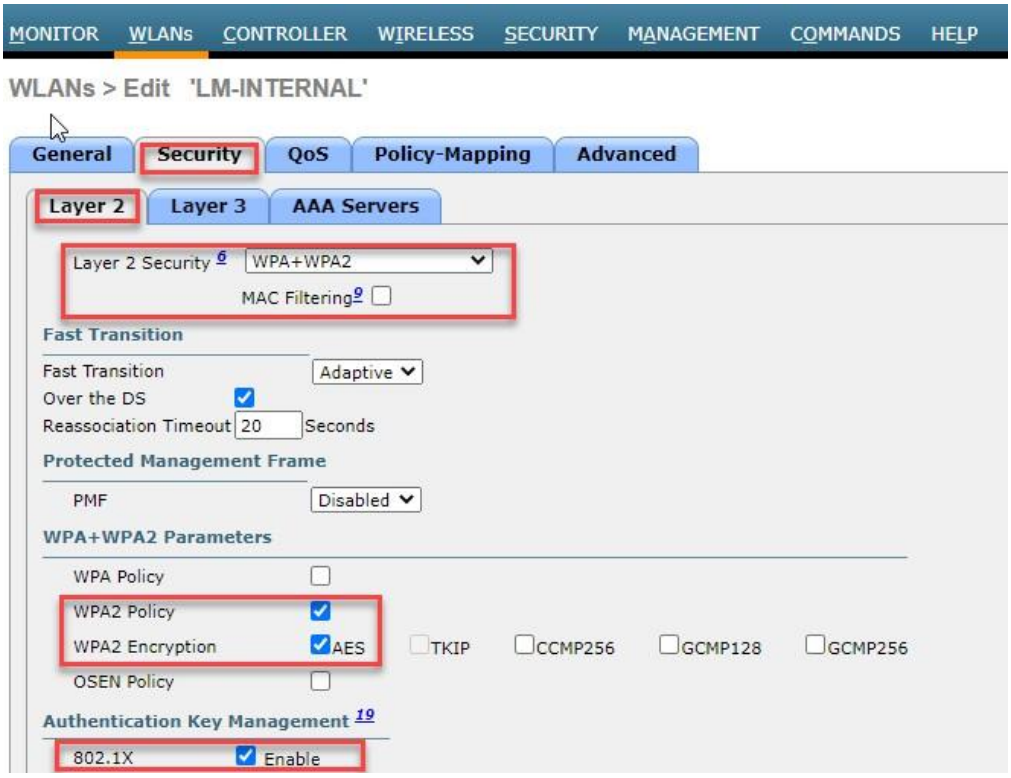
- ✓ Tab High Availability:
- ✓ Primary Controller vWLC
- ✓ Manegement IP Address (Ipv4/Ipv6): 10.1.1.100



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



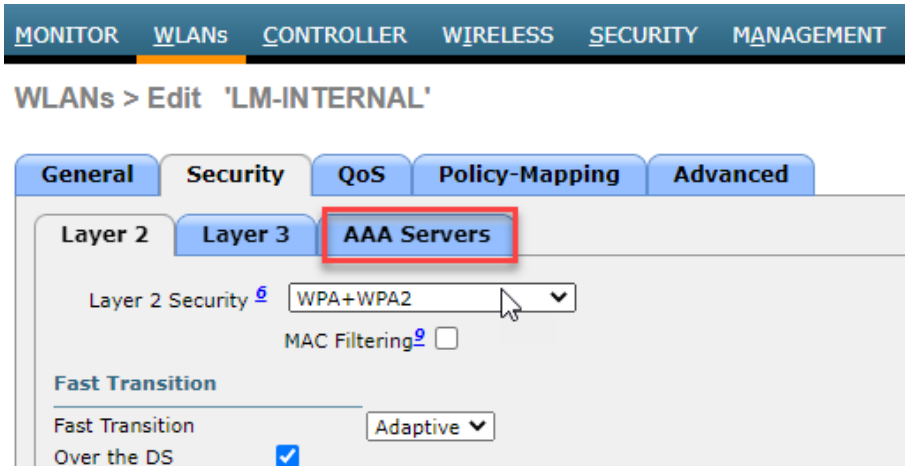
- ✓ Trong tab Security/ Layer 2
- ✓ Layer 2 Security: WPA + WPA2
- ✓ WPA2 Policy: tick vào enable
- ✓ 802.1x: tick vào enable



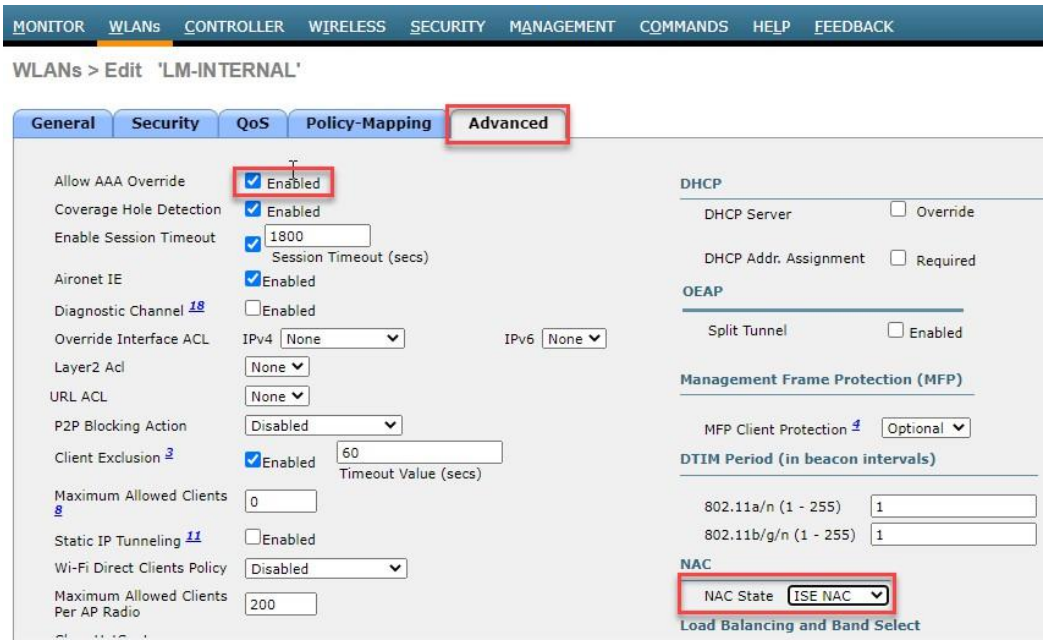
- Tiếp tục ta chọn qua phần AAA Server

+Authentication Server, bật enabled

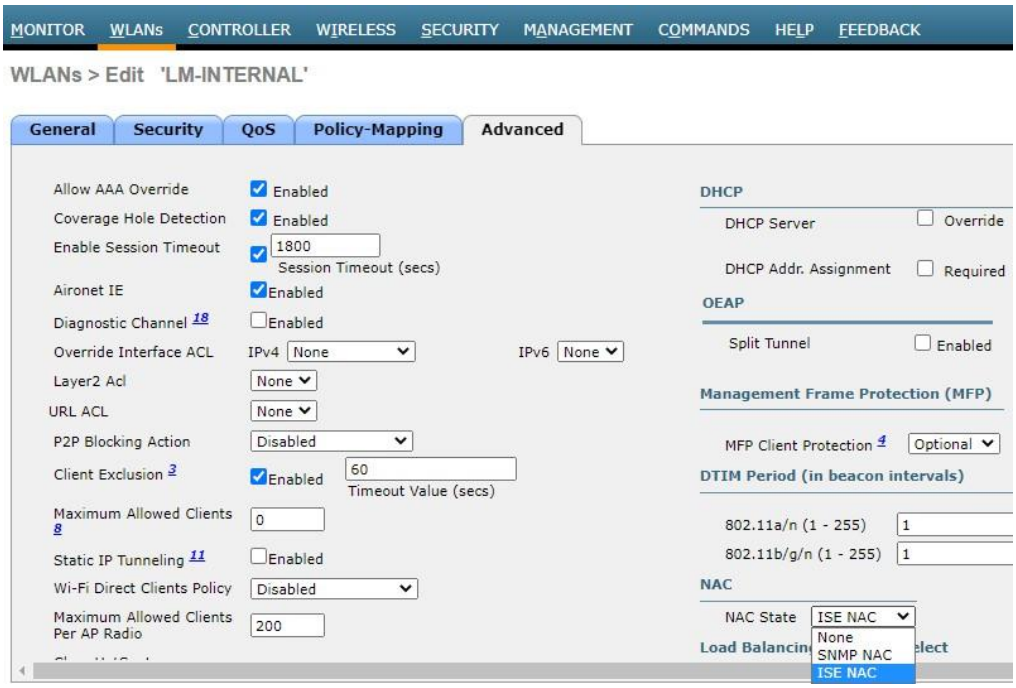
+Accounting Server, bỏ chọn



- tiếp tục ta chọn qua phần WLAN/ Advanced



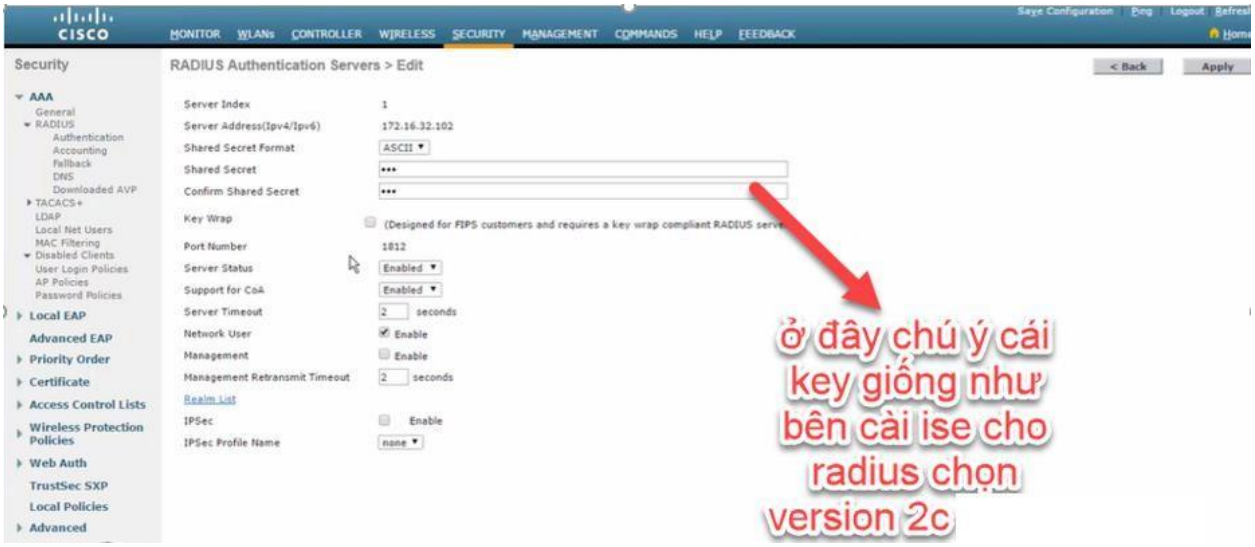
- ✓ Chuyển qua tab Advanced /
- ✓ Mục NAC State : Chọn ISE NAC



Chọn Tab Security / RADIUS Authentication Servers:

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

✓ Cài đặt Shared Secret



✓ Tại Tab Management

✓ Add New

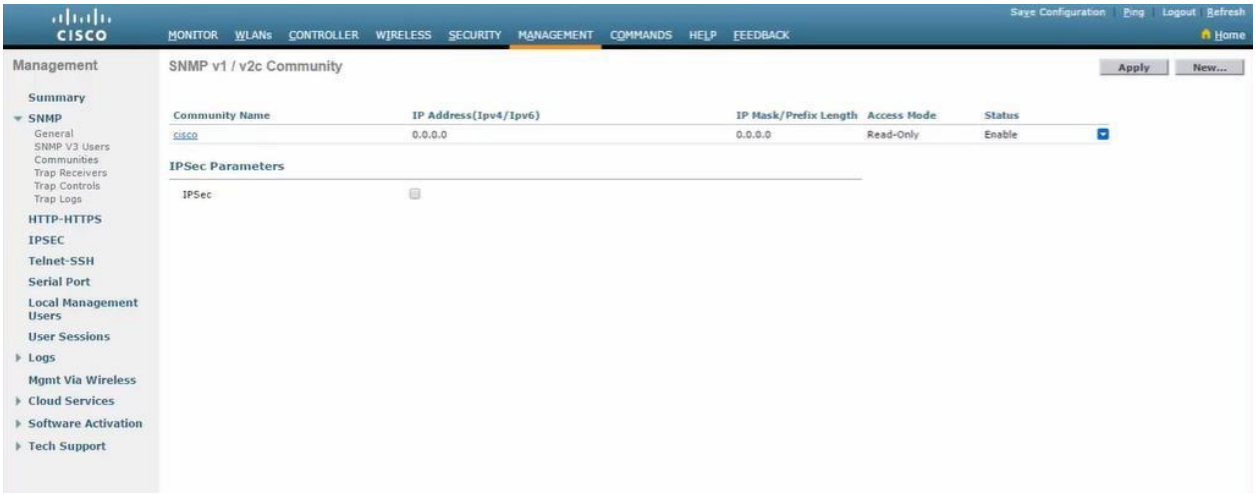
✓ Community Name: cisco

✓ IP Address (Ipv4/Ipv6): 0.0.0.0

✓ IP Mask/Prefix length: 0.0.0.0

✓ Access Node: Read-Only

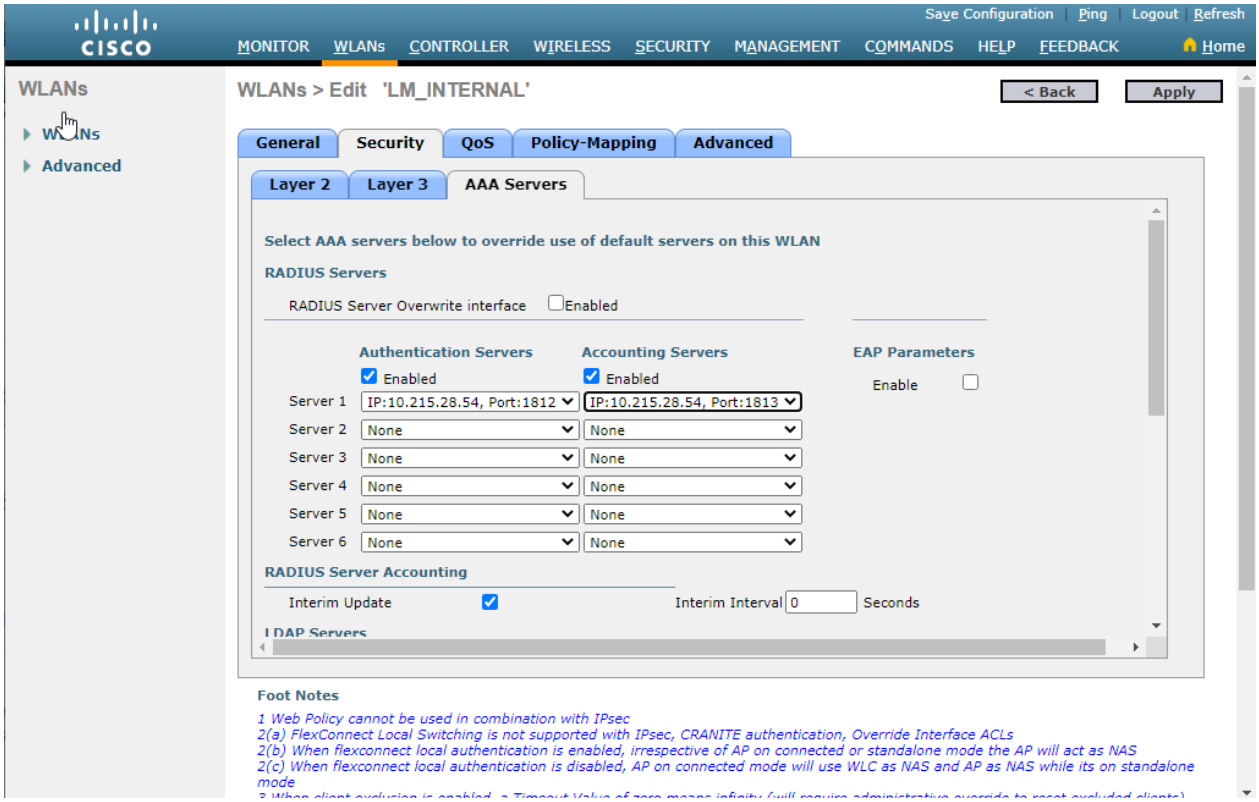
✓ Status: Enable



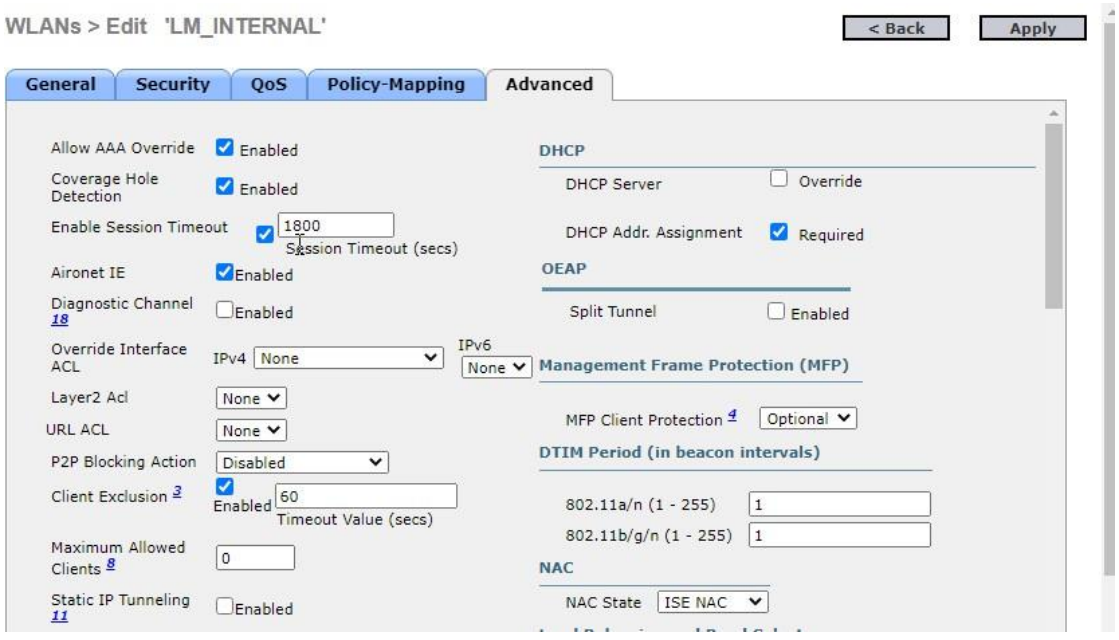
✓ Tại Tab WLAN / Security / AAA Servers

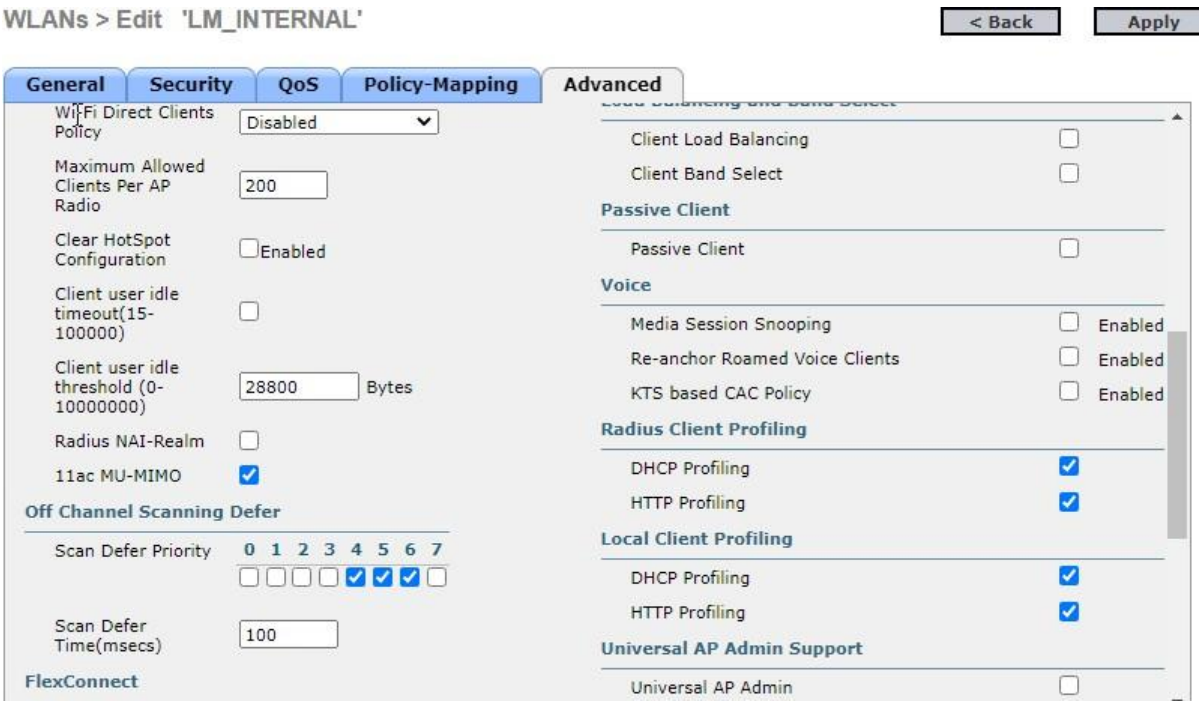
✓ Mục Authentication Server: IP 10.1.1.200 Port 1812

✓ Mục Accounting Server: IP 10.1.1.200 Port 1813

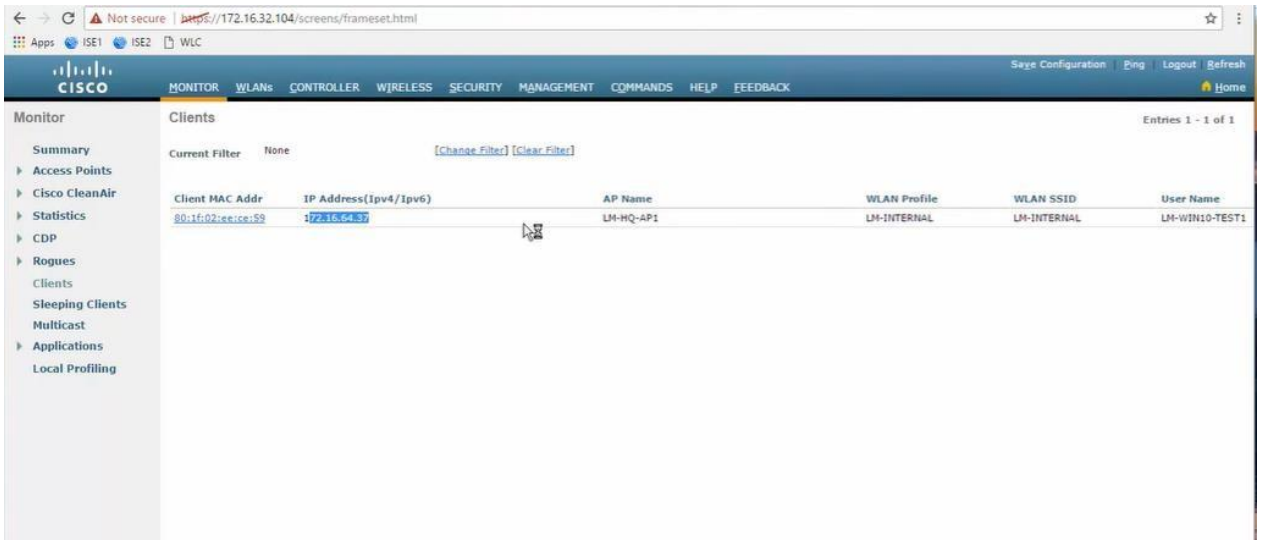


✓ Tại Tab Advance: các bạn sẽ tick đầy đủ như hình sau





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



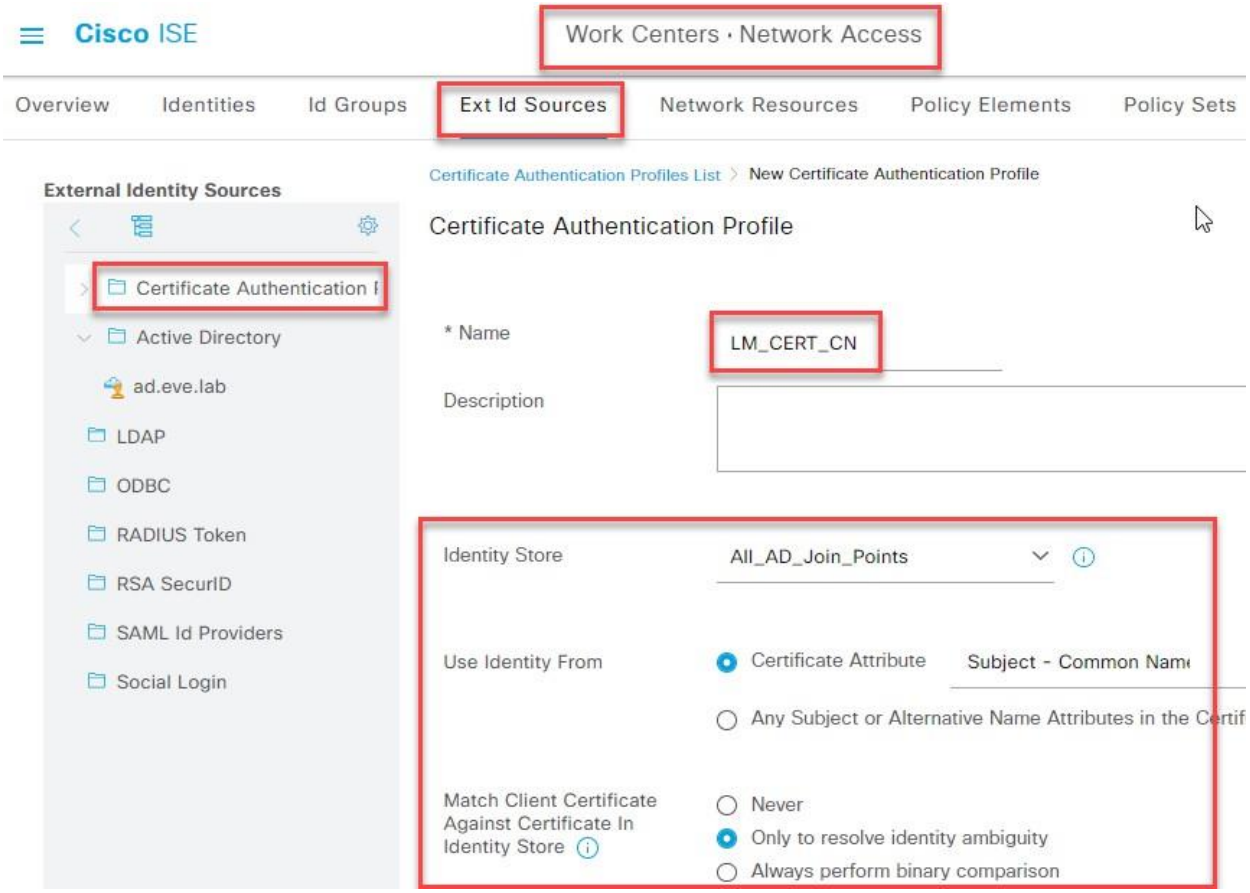
✓ Quay lại Cisco ISE

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

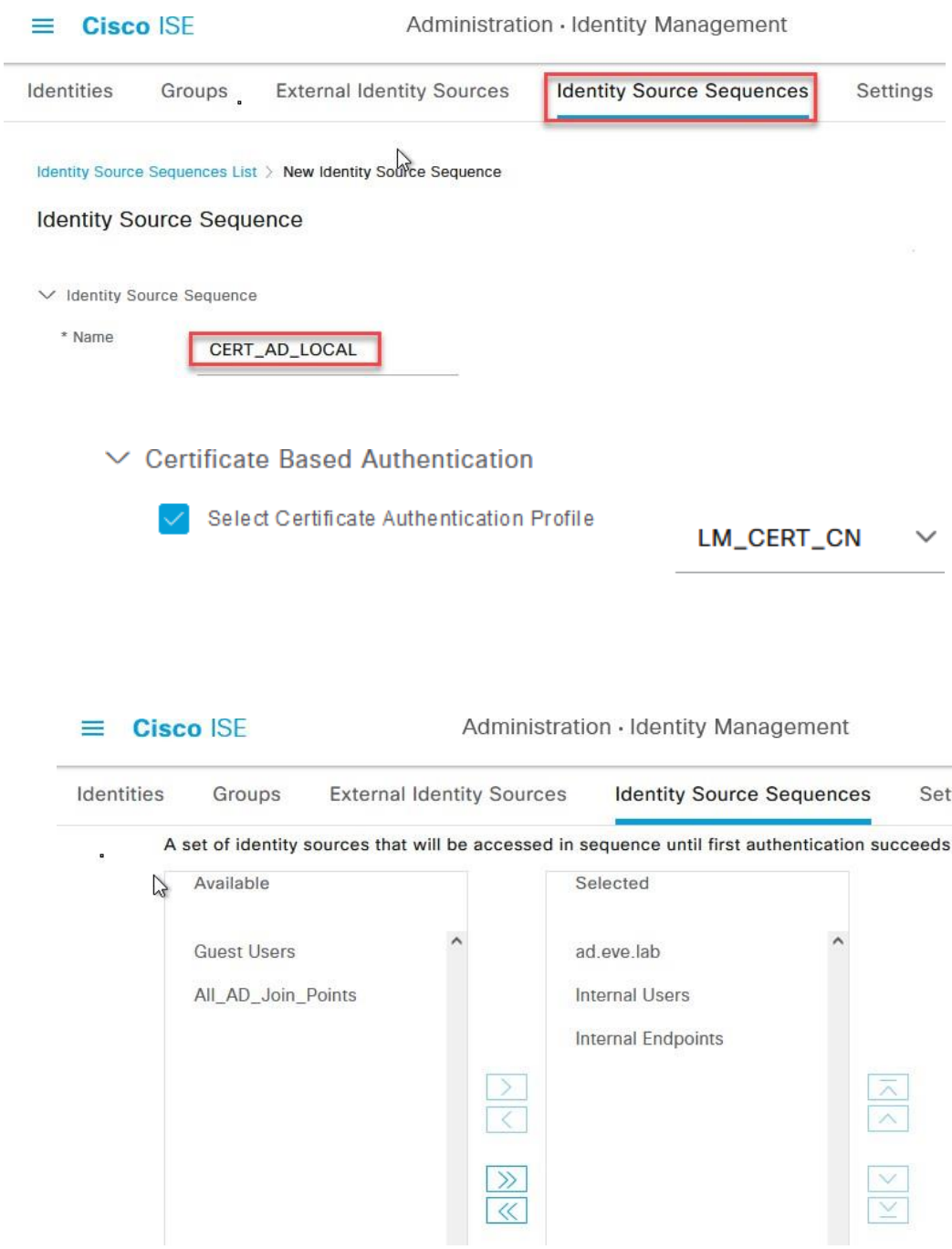
✓ Ta tạo một Certificate Authentication Profile

✓ Name: LM_CERT_ON

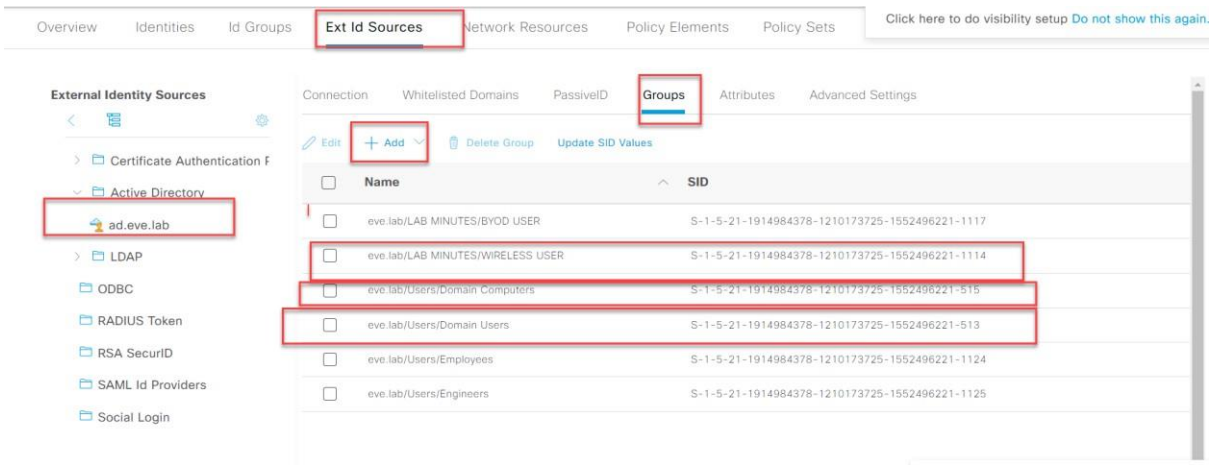
- ✓ Identity Store:All_AD_Join_Points
- ✓ User Identity From: Certificate Attribute: Subject-Common
- ✓ Match Client Certificate Against: tick vào Only to resolve ambiguity



- ✓ 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)



- ✓ 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

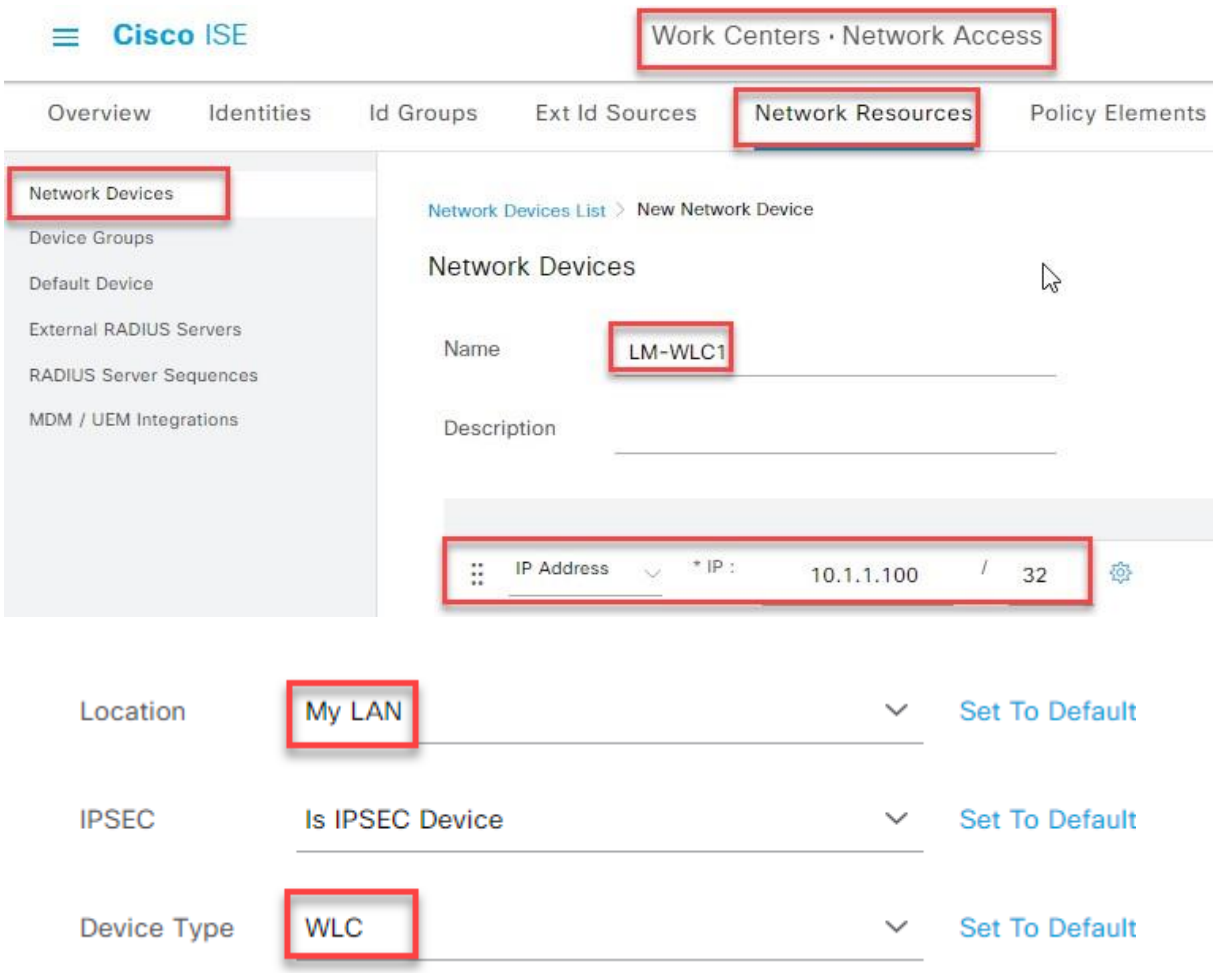
✓ Network Devices

✓ Name: LM-WLC1

✓ IP Address: 10.1.1.100/23

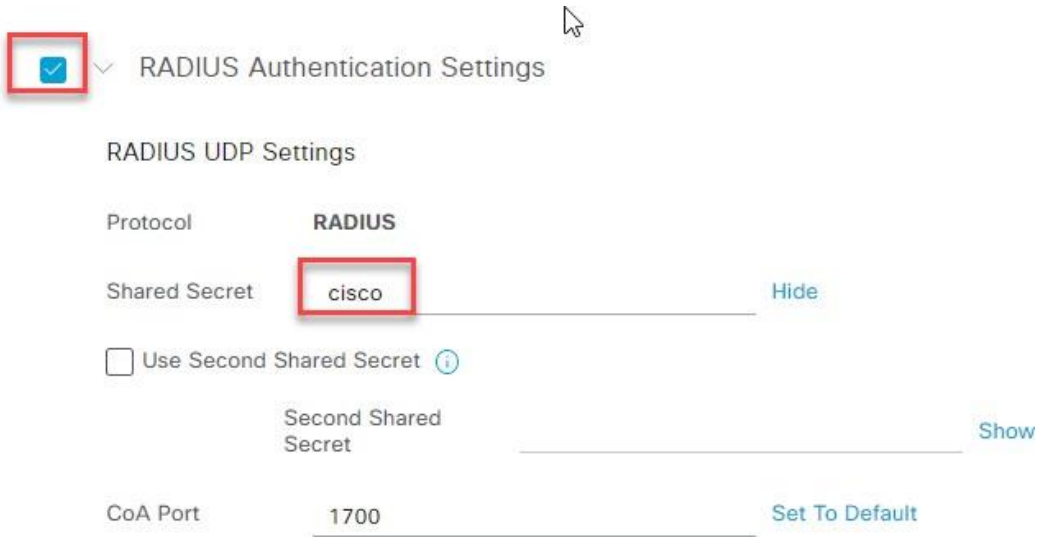
✓ Location: MY_LAN

✓ Device Type: WLC



✓ Tick vào RADIUS Authentication Settings:

✓ Shared Secret: cisco

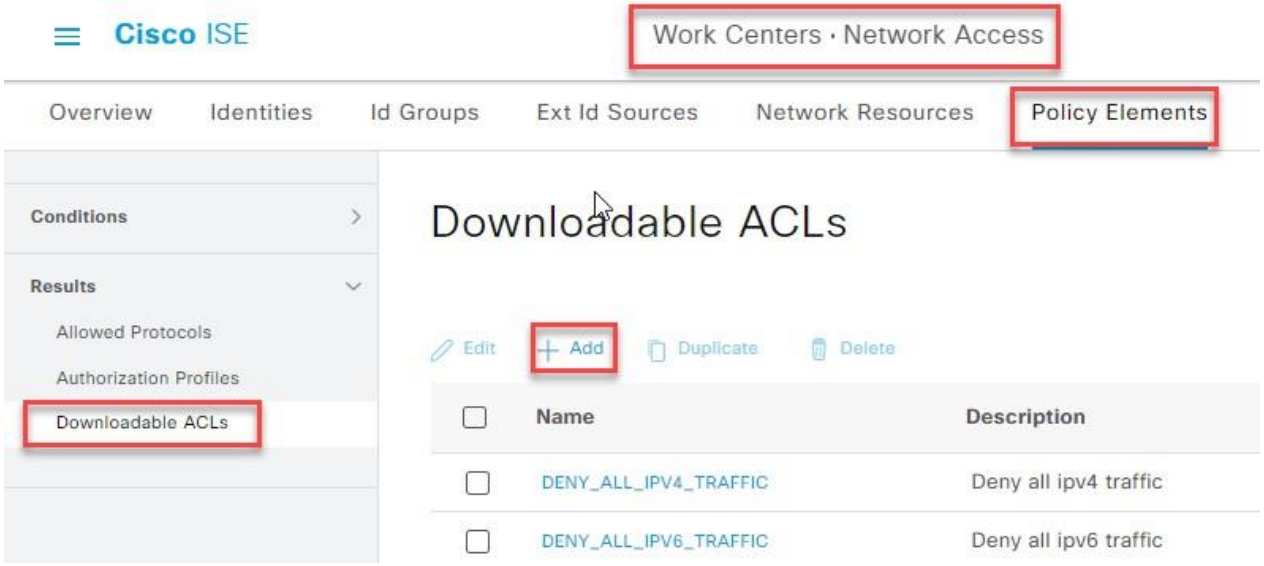


✓ Tick vào SNMP Settings:

✓ SNMP Version: 2c

✓ SNMP RO Community: cisco

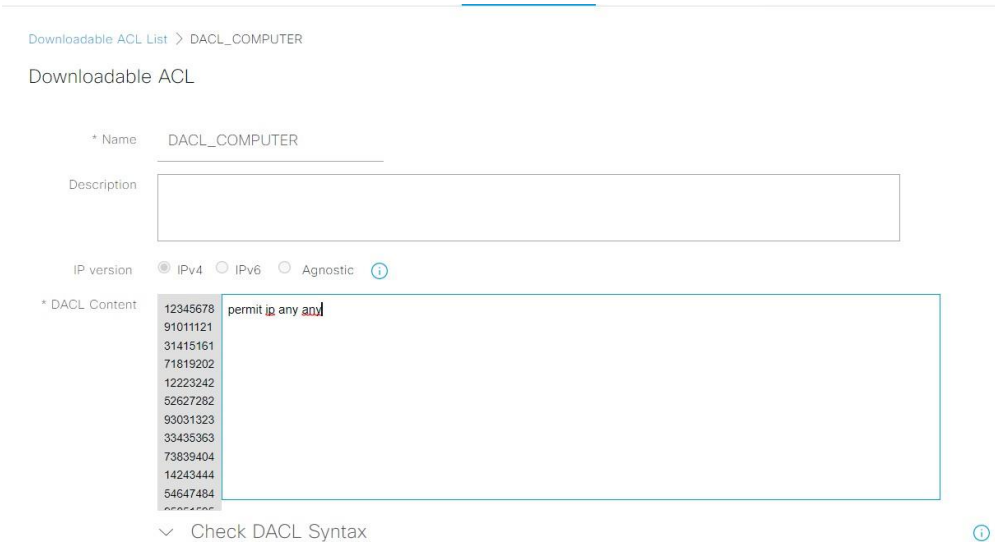
✓ Ta vào Mục Work Center / Network Access / Policy Elements / Results / Downloadable ACLs / + Add



✓ Ta tạo một DACL:

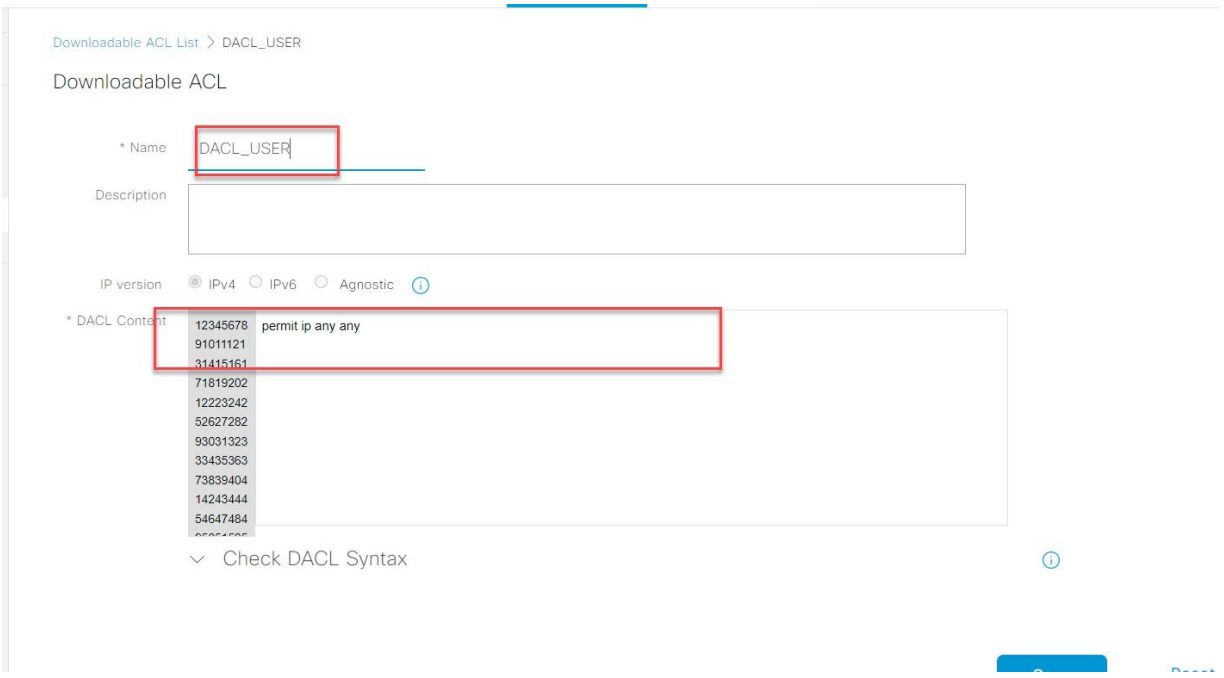
✓ Name: DACL_COMPUTER

✓ DACL Content: permit ip any any

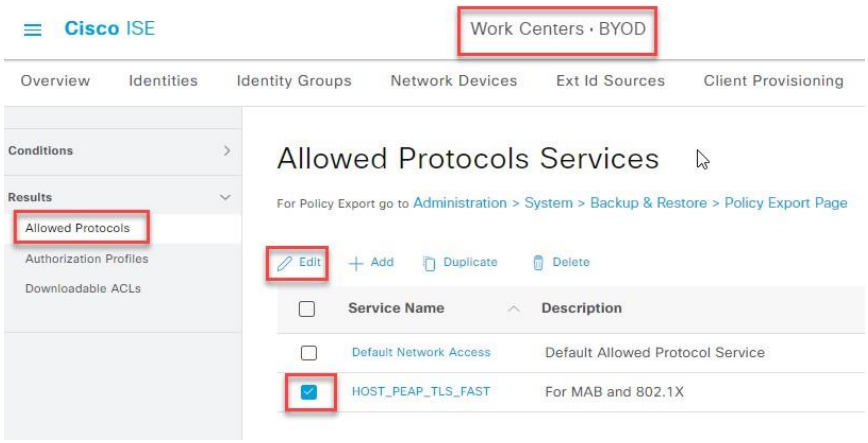


✓ Name: DACL_USER

✓ DACL Content: permit ip any any



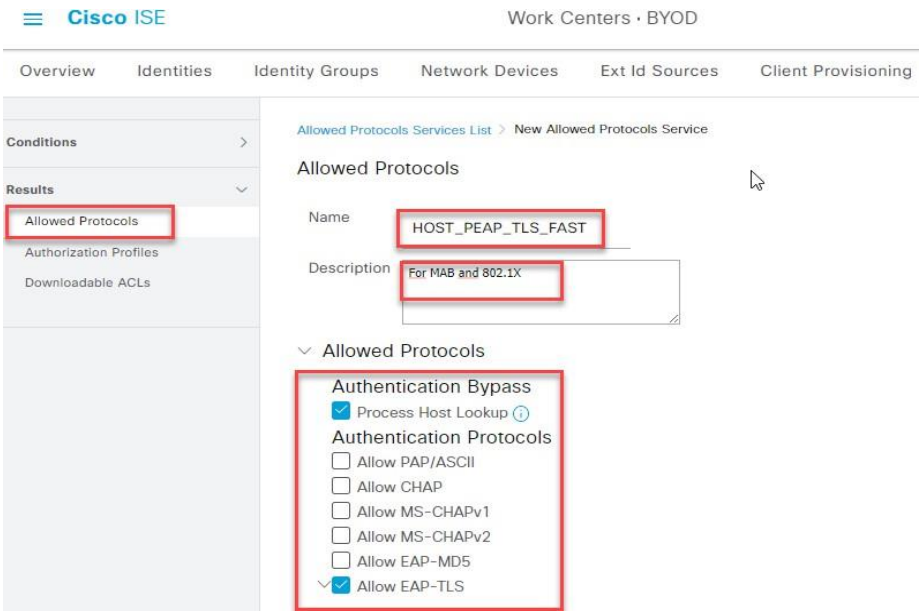
✓ Ta vào Mục Work Center / Network Access / Policy Elements / Allowed Protocols/ lick vào HOST_PEAD_TLS_FAST/ edit



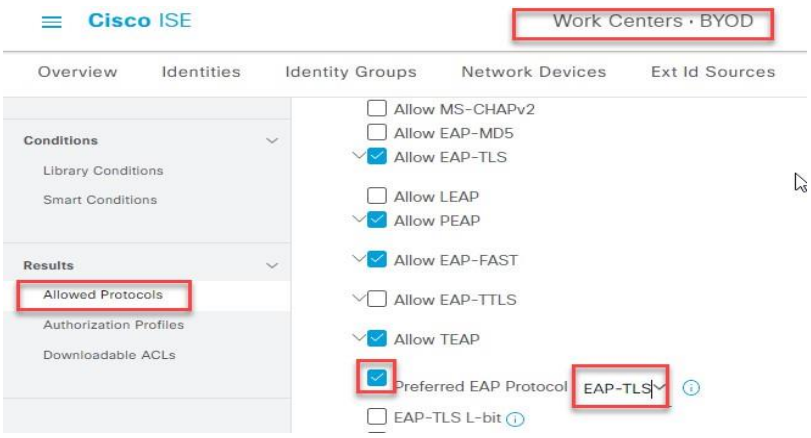
✓ Tại phần edit của HOST_PEAP_TLS_FAST

✓ Description: For MAB and 802.1X

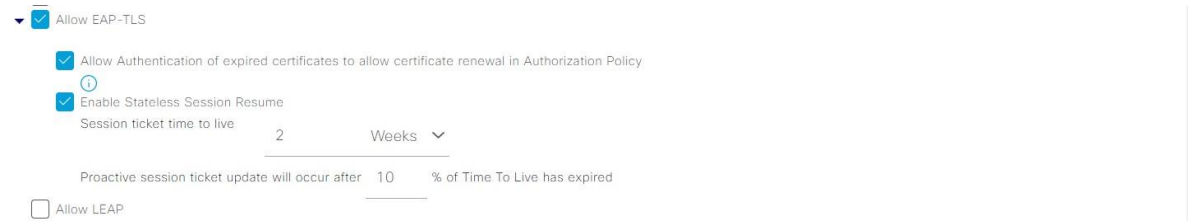
✓ Các bạn sẽ tick đầy đủ như hình.



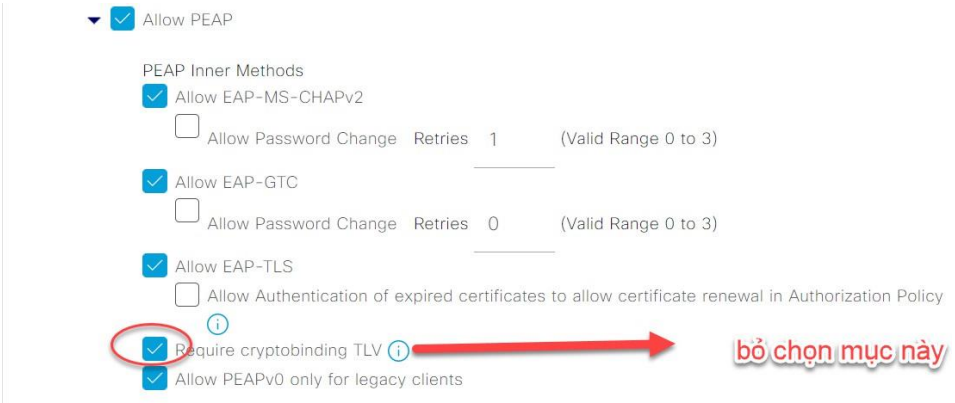
✓ Tại mục Preferred EAP Protocol: EAP-TLS



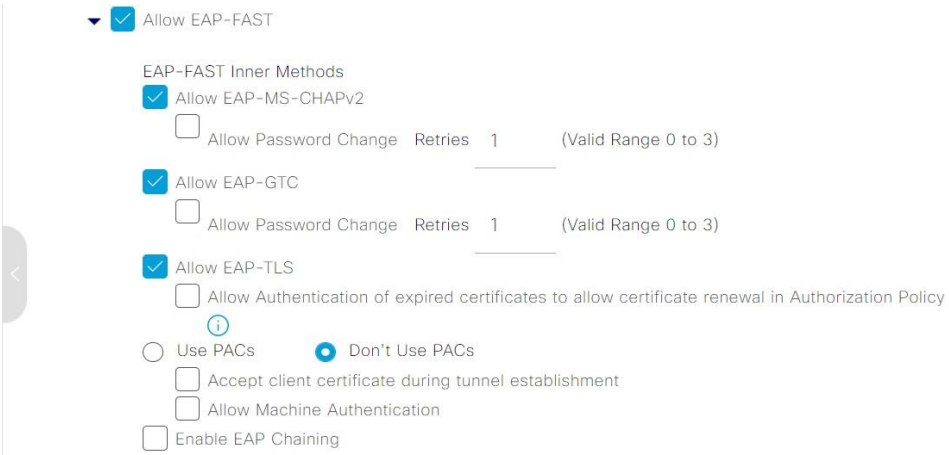
- ✓ Tick vào tab Allow EAP-TLS
- ✓ Tick vào Allow Authentication of expired certificates
- ✓ Tick vào Enable Stateless Session Resume
- ✓ Session ticket time to live: 2 Weeks
- ✓ Proactive session ticket update: 10%

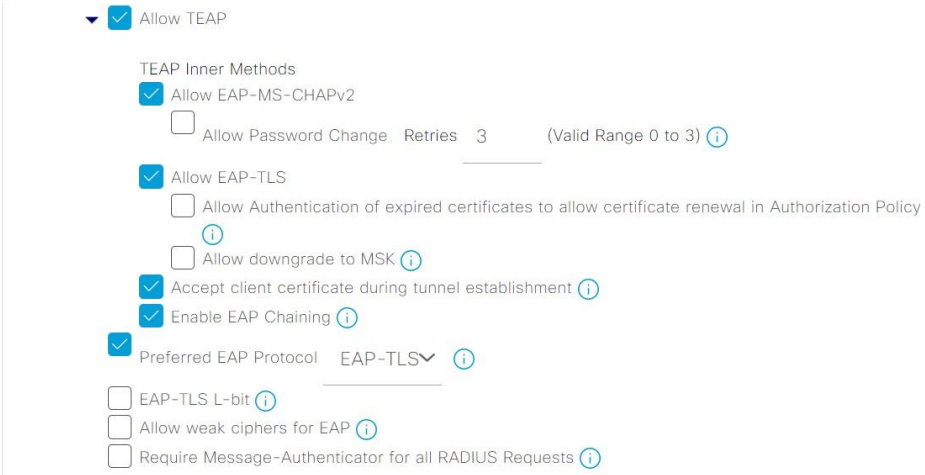


- ✓ Tab Allow PEAP
- ✓ Bỏ chọn mục Require cryptobinding TLV

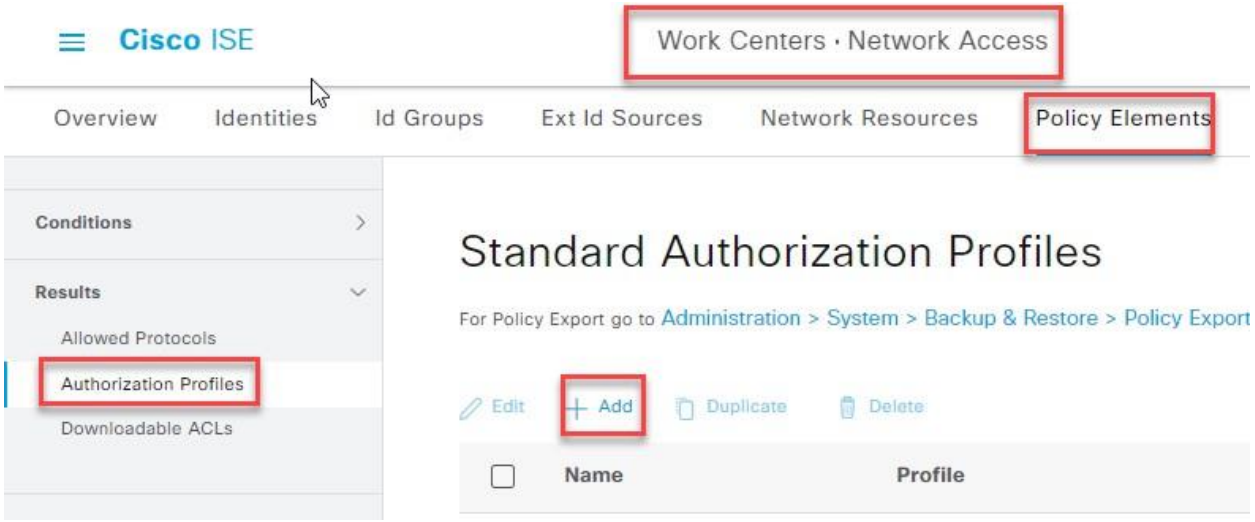


- ✓ Tick vào Allow EAP-FAST
- ✓ Ta sẽ tick đầy đủ vào


Allow EAP-FAST
EAP-FAST Inner Methods
Allow EAP-MS-CHAPv2
Allow Password Change Retries 1 (Valid Range 0 to 3)
Allow EAP-GTC
Allow Password Change Retries 1 (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

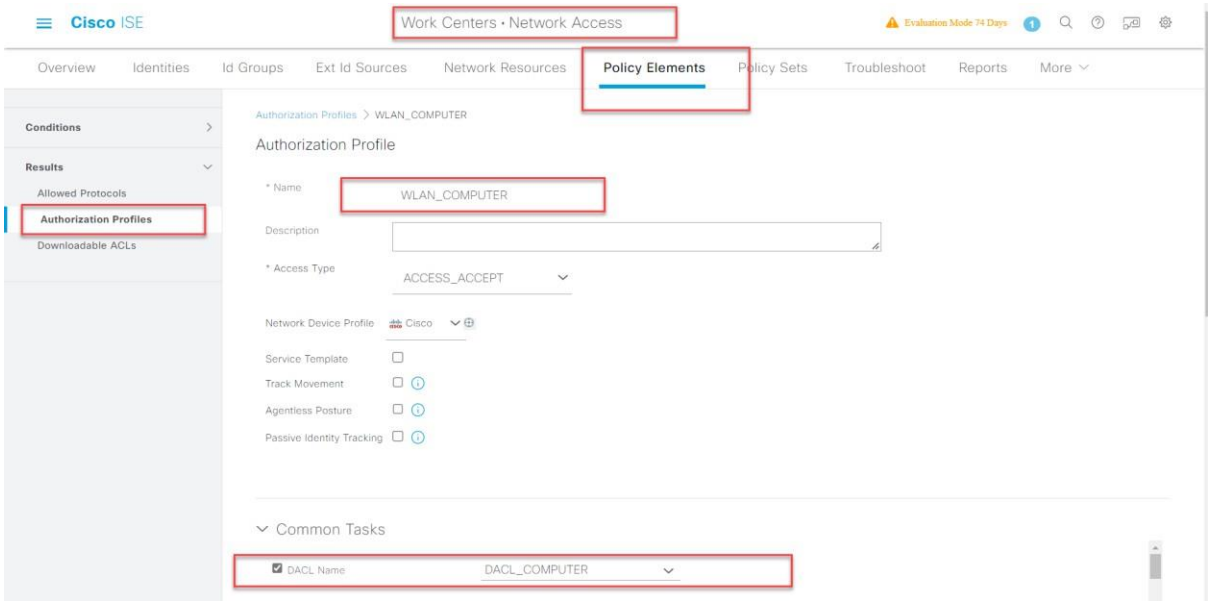

Allow TEAP
TEAP Inner Methods
Allow EAP-MS-CHAPv2
Allow Password Change Retries 3 (Valid Range 0 to 3)
Allow EAP-TLS
Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
Allow downgrade to MSK
Accept client certificate during tunnel establishment
Enable EAP Chaining
Preferred EAP Protocol EAP-TLS
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



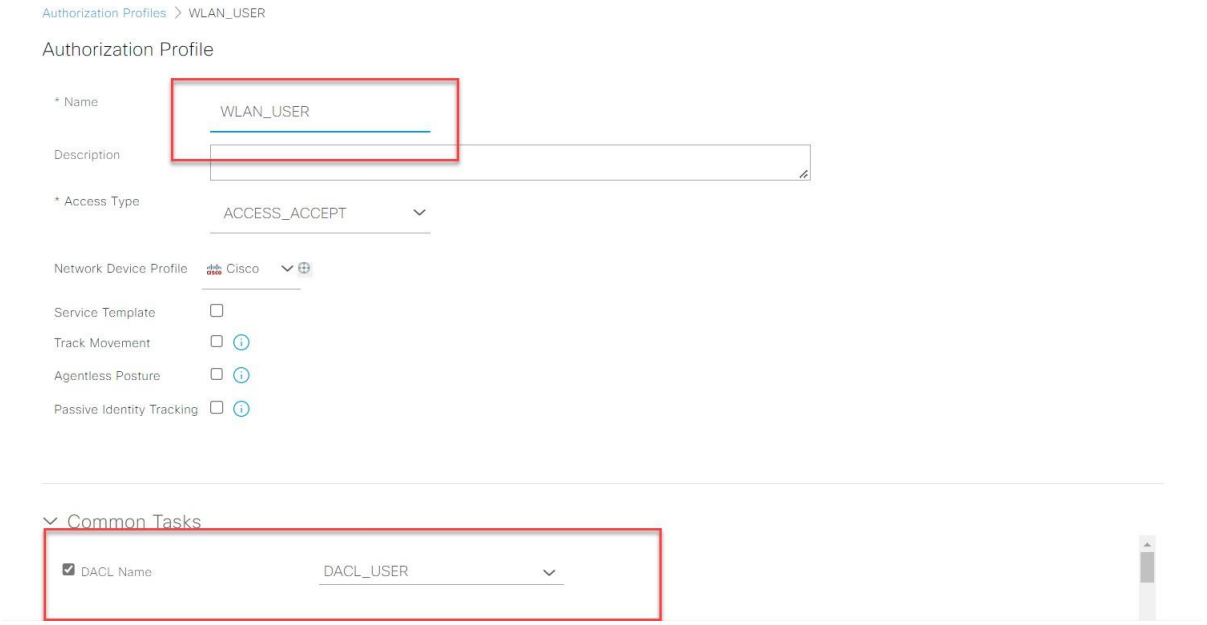
✓ Name: WLAN_COMPUTER

✓ DACL Name: DACL_COMPUTER



✓ Name: wlan_user

✓ DACL Name: DACL_USER



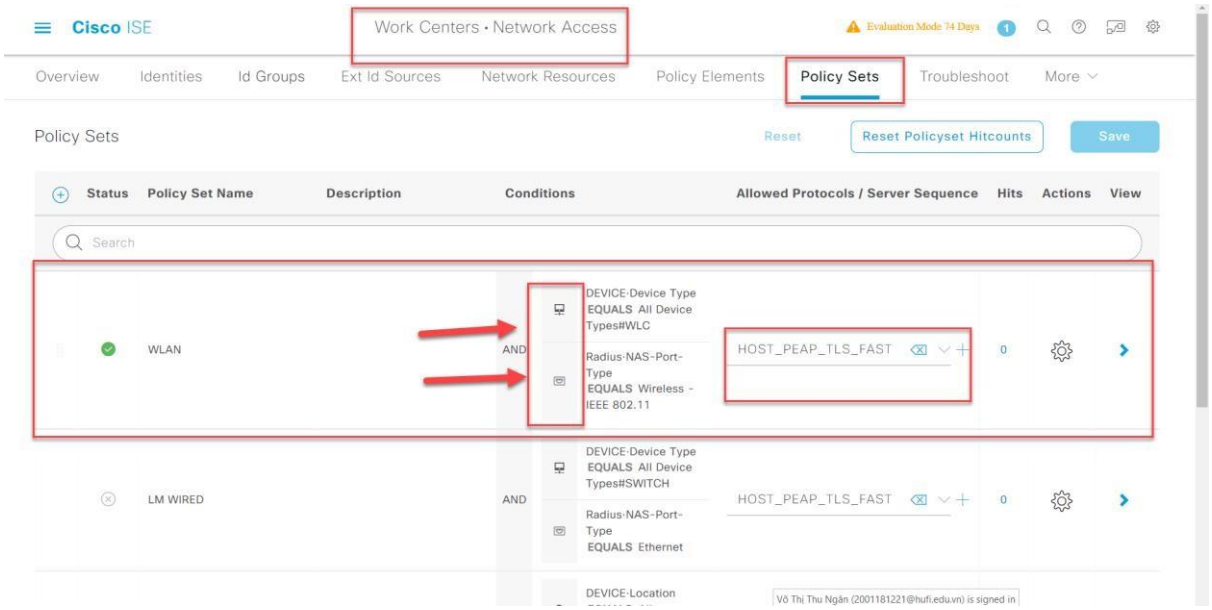
✓ Ta vào Mục Work Center / Network Access / Policy Sets

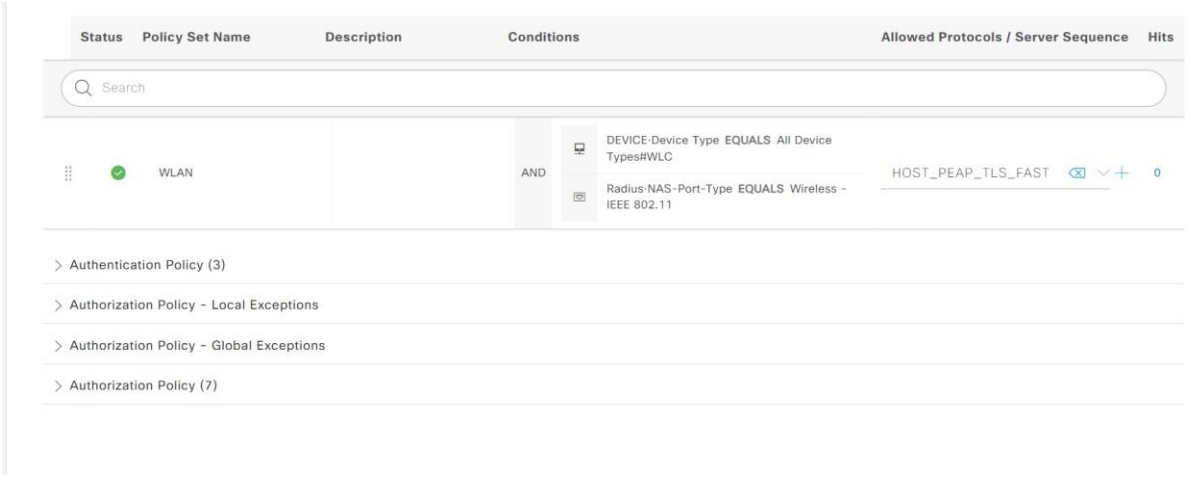
✓ Tao tạo một Policy mới:

✓ Name: WLAN

✓ Conditions:

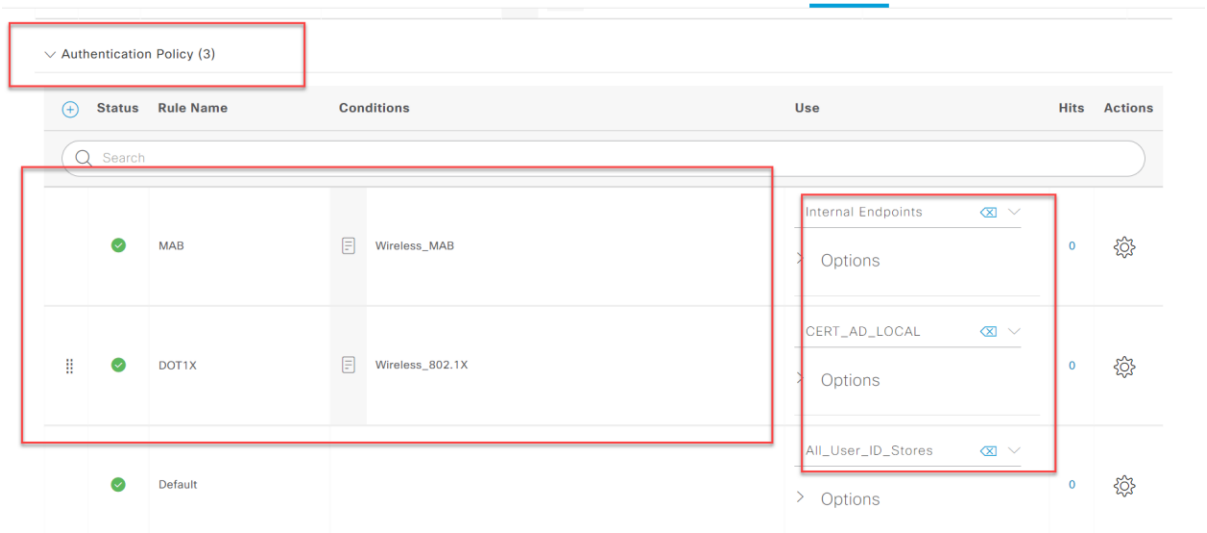
- DEVICE:Device Type EQUALS All Device Types#WLC
- Radius-NAS-Port-Type EQUALS IEEE 802.11
- Allowed Protocols / Server Sequence: HOST_PEAP_TLS_FAST





✓ Tab Authentication Policy:

✓ Ta add policy MAB và DOT1X như hình



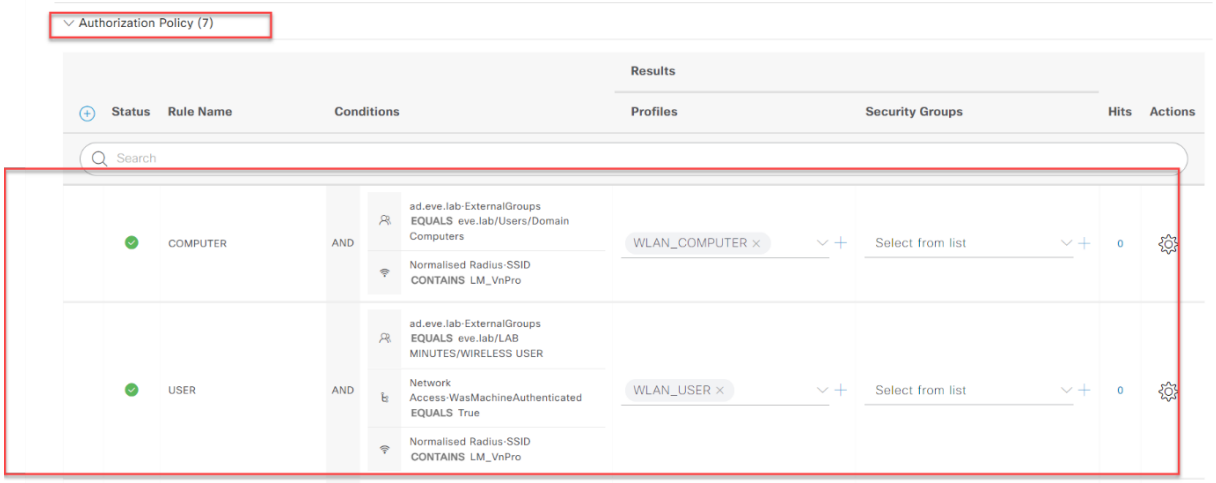
✓ Tab Authorization Policy

✓ 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



✓ Tại Domain Controller ta tạo

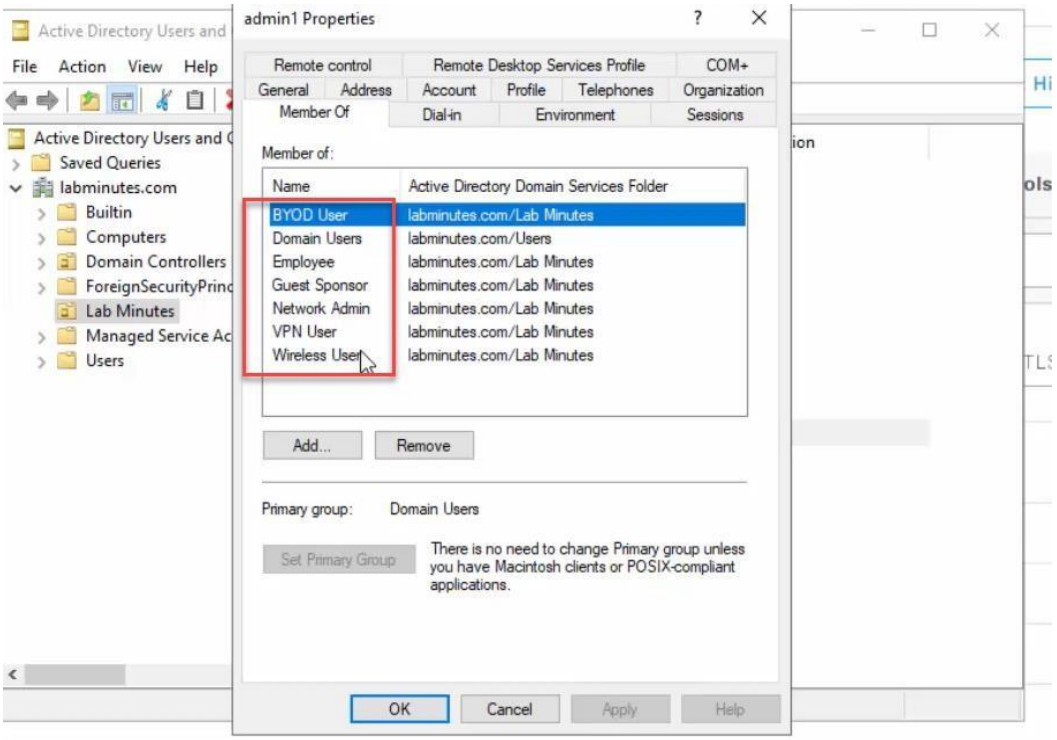
+ admin1

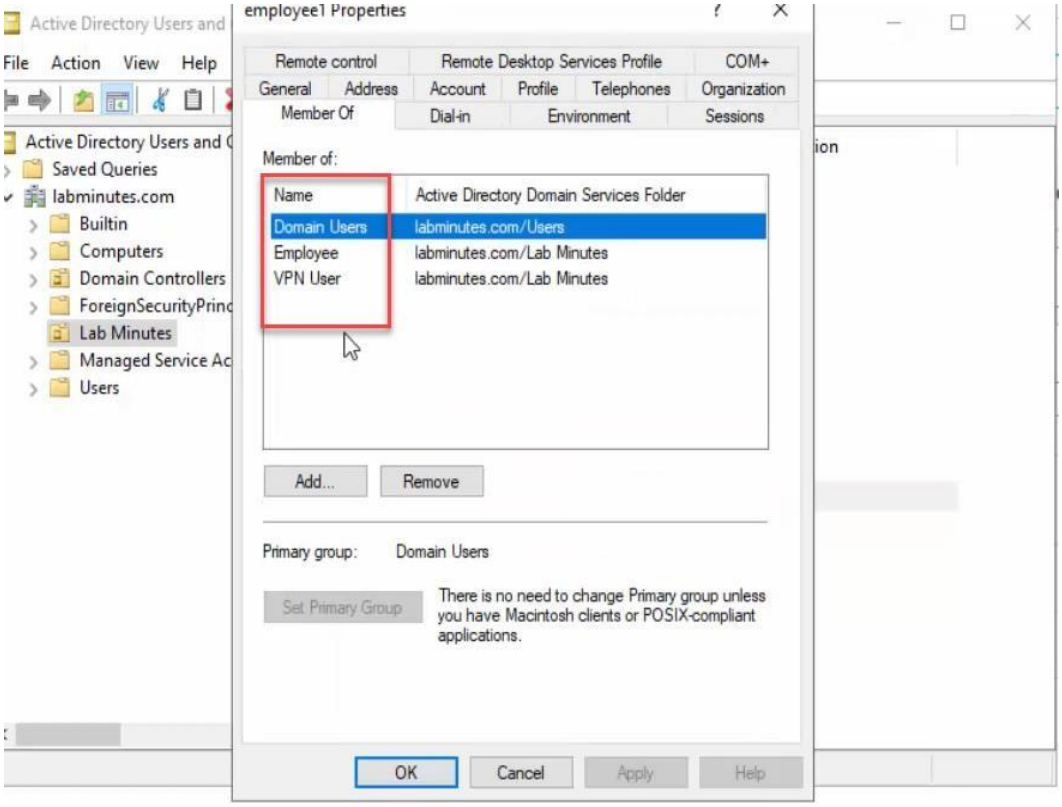
+ employee1

✓ Các group Wireless USER, NHANVIEN

✓ Add admin1 vào USER DC

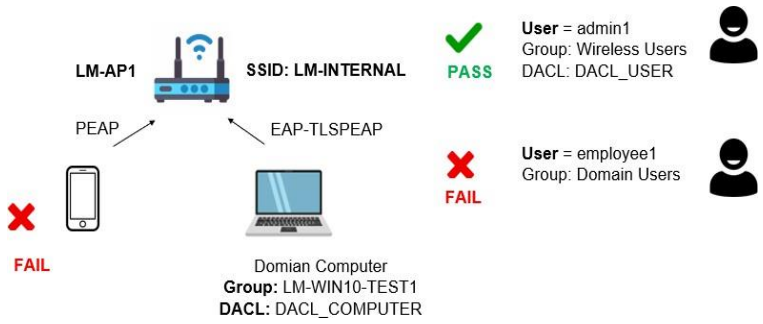
✓ Add employee1 vào USER DC



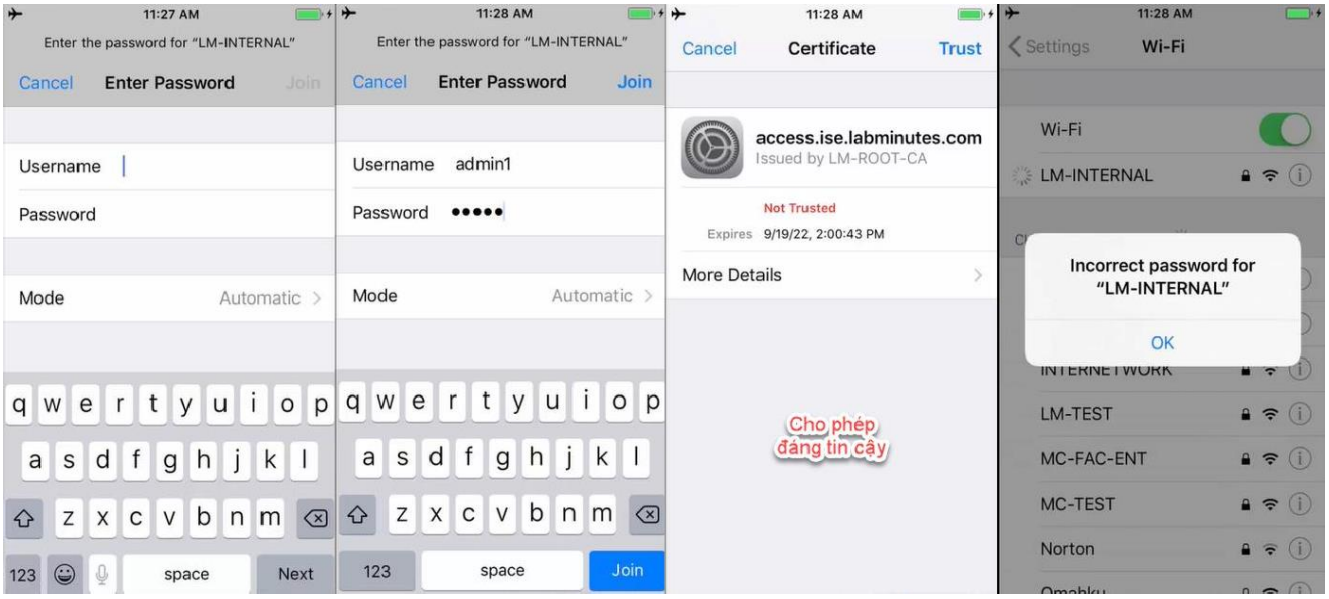


✓ Tiến hành đăng nhập vào DC coi các user đã tạo có thành công không, do bảng winserver2016, dễ gặp lỗi khi tạo user, nếu tạo user thành công đăng nhập rồi ta hả add vào các group.

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

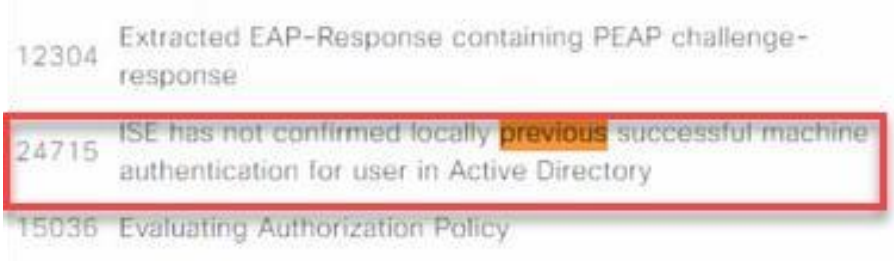


Ta sẽ tiếp hành truy cập wifi trên iphone (user: admin1)



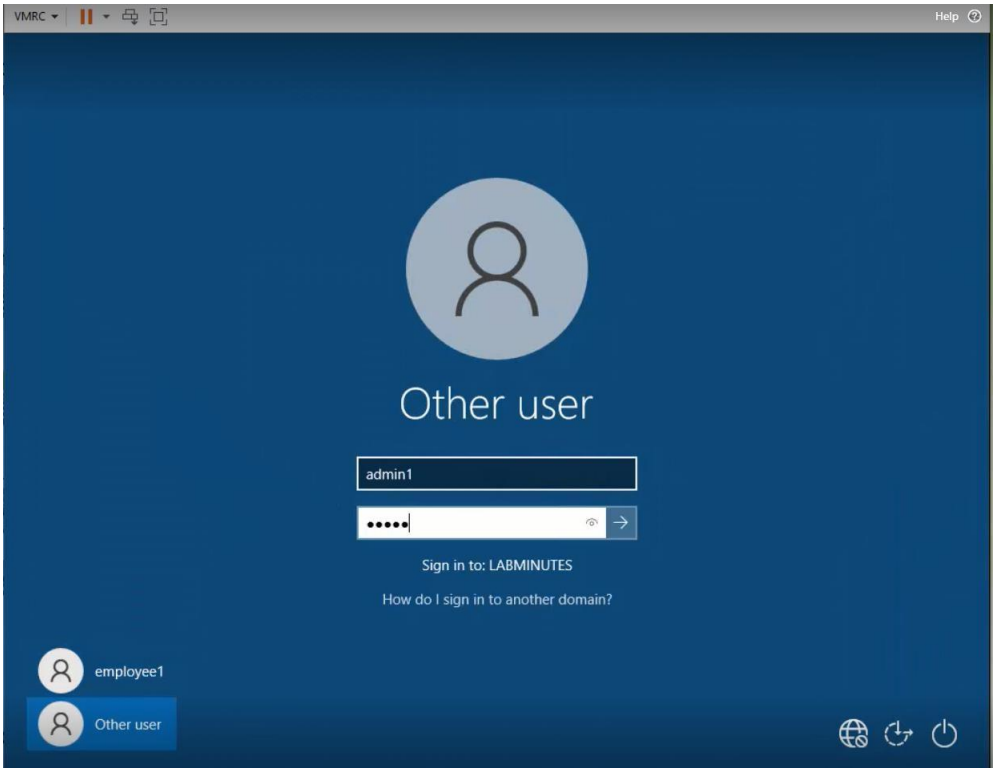
✓ Vào mục Operation/ RADIUS/ Live logs

✓ Khi này ta sẽ thấy xác thực **fail**

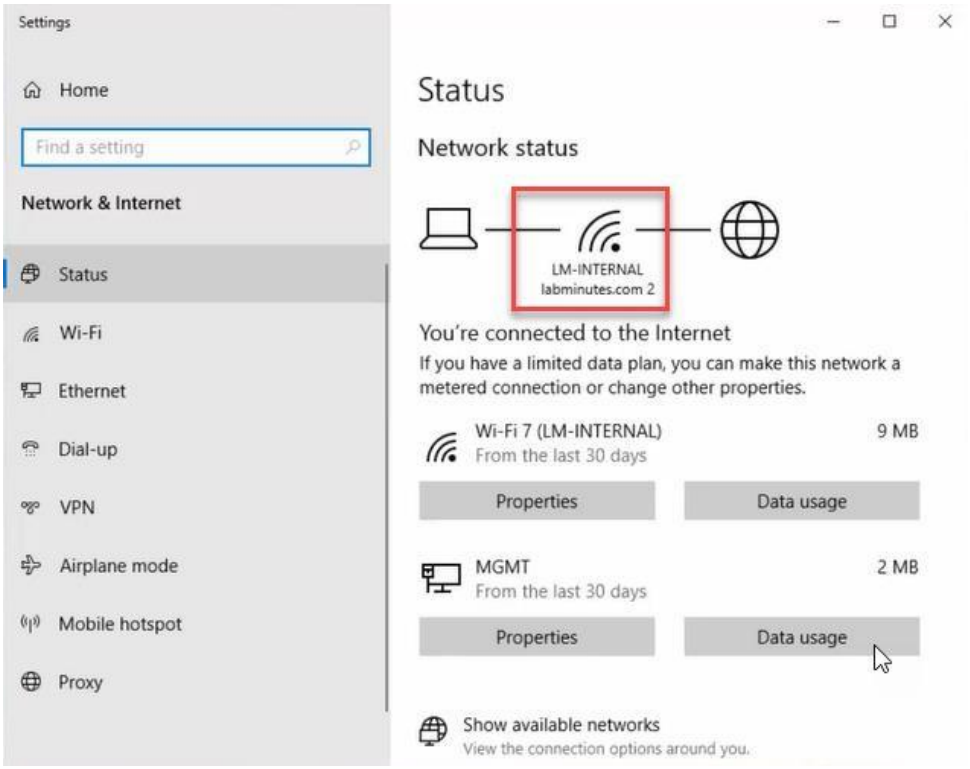


✓ Thử kết quả kết nối qua laptop

✓ Truy cập vào user: admin1

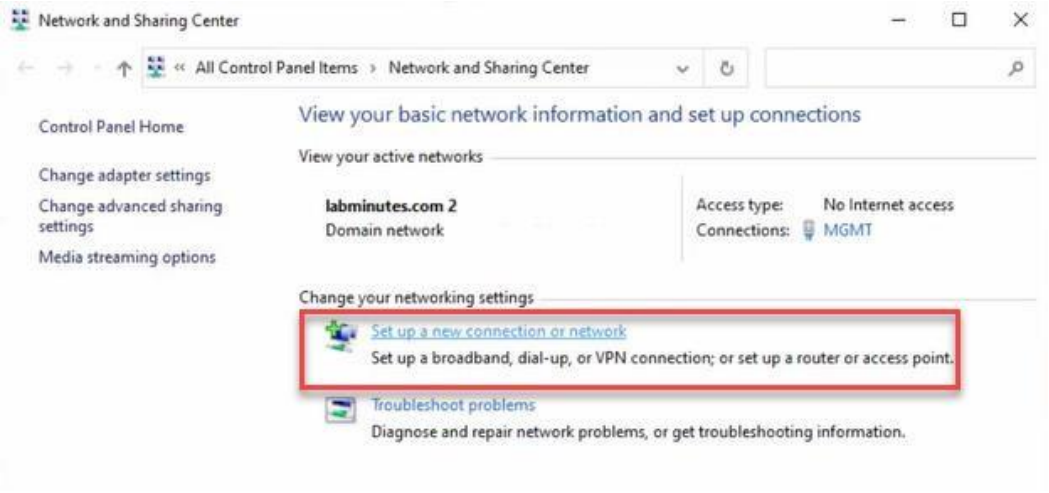


✓ Vào phần setting / Network Status/ kết nối wifi LM-INTERNAL



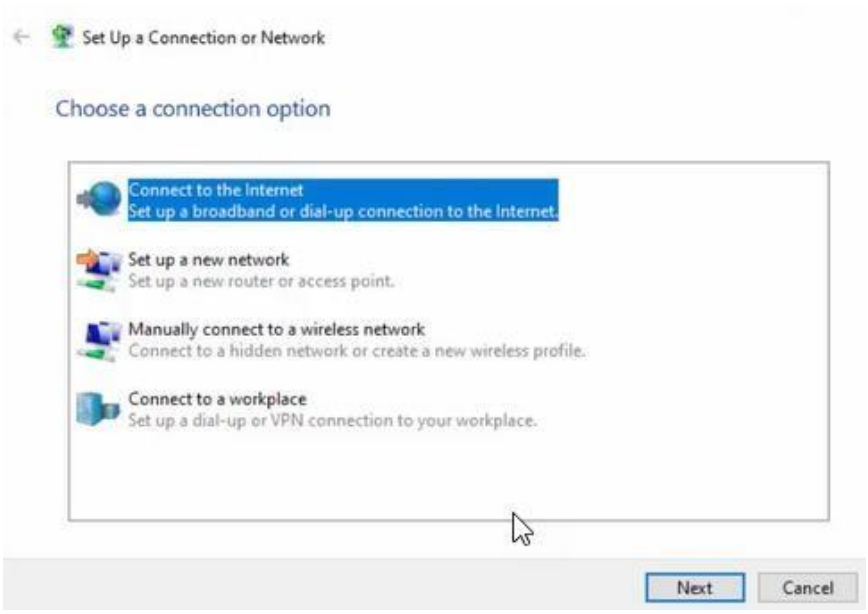
✓ Chuyển hướng sang Network and Sharing Center"

✓ Lick vào Set up a new connection or network

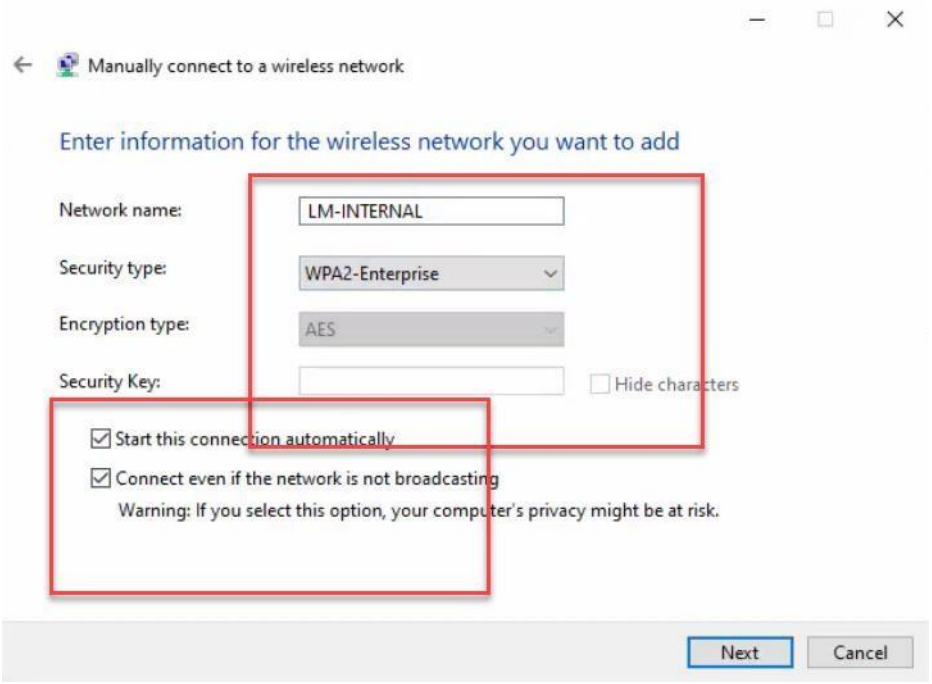


✓ Trong mục Set Up A Connection or Network

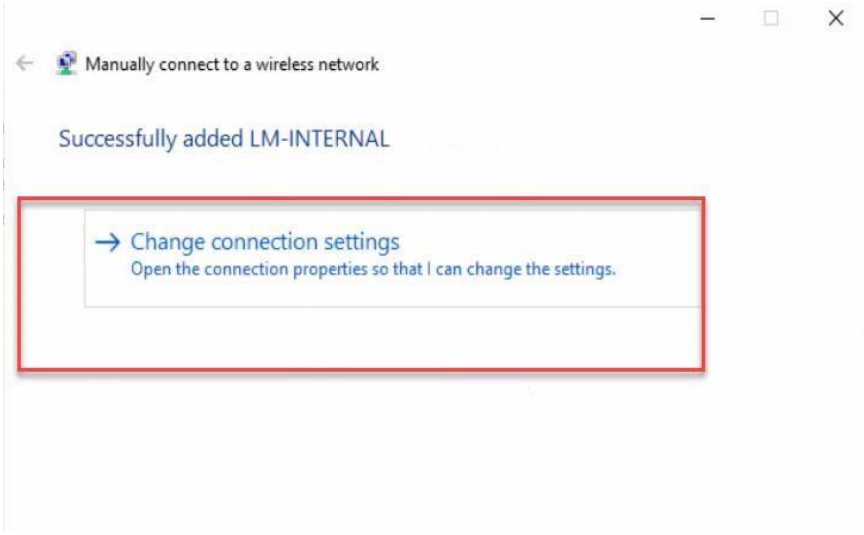
✓ Chọn Manually connect to a wireless network



- ✓ Network name: LM-INTERNAL
- ✓ Security type: WPA2-Enterprise
- ✓ Tick vào Start this connection automatically
- ✓ Tick vào Connect even if the network is net broadcasting
- ✓ Chọn next



✓ Lick vào Change added LM-INTERNAL

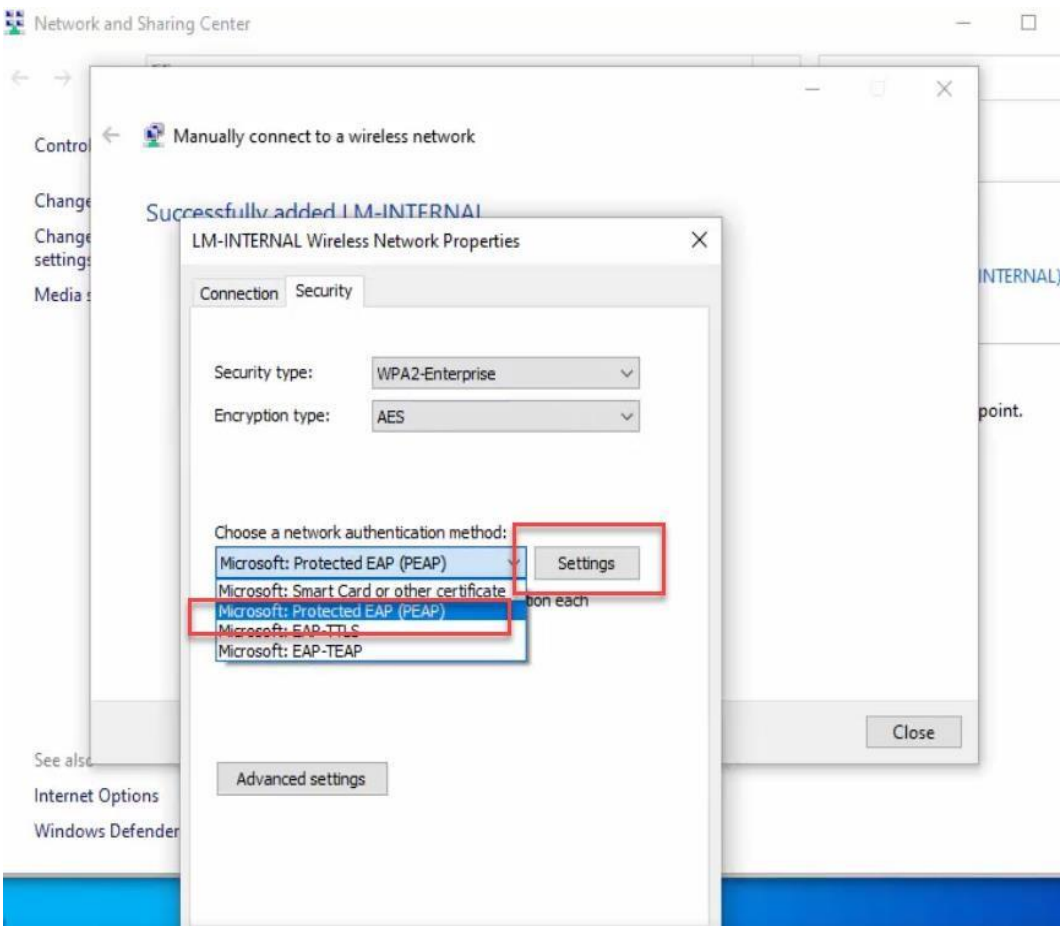


✓ Tại tab Security

✓ Mục Choose a network authentication method:

✓ Mircosoft: Protected EAP (PEAP)

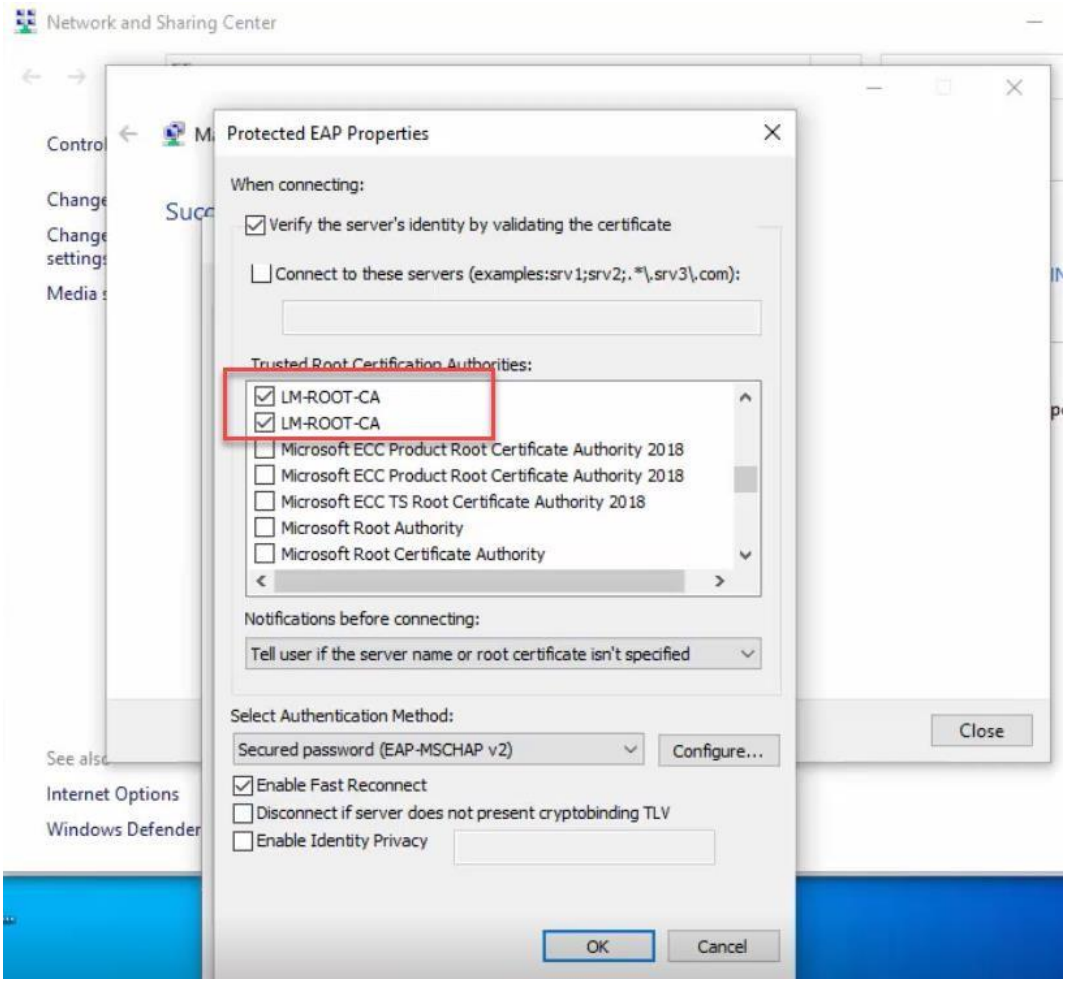
✓ Ta chọn tiếp Setting



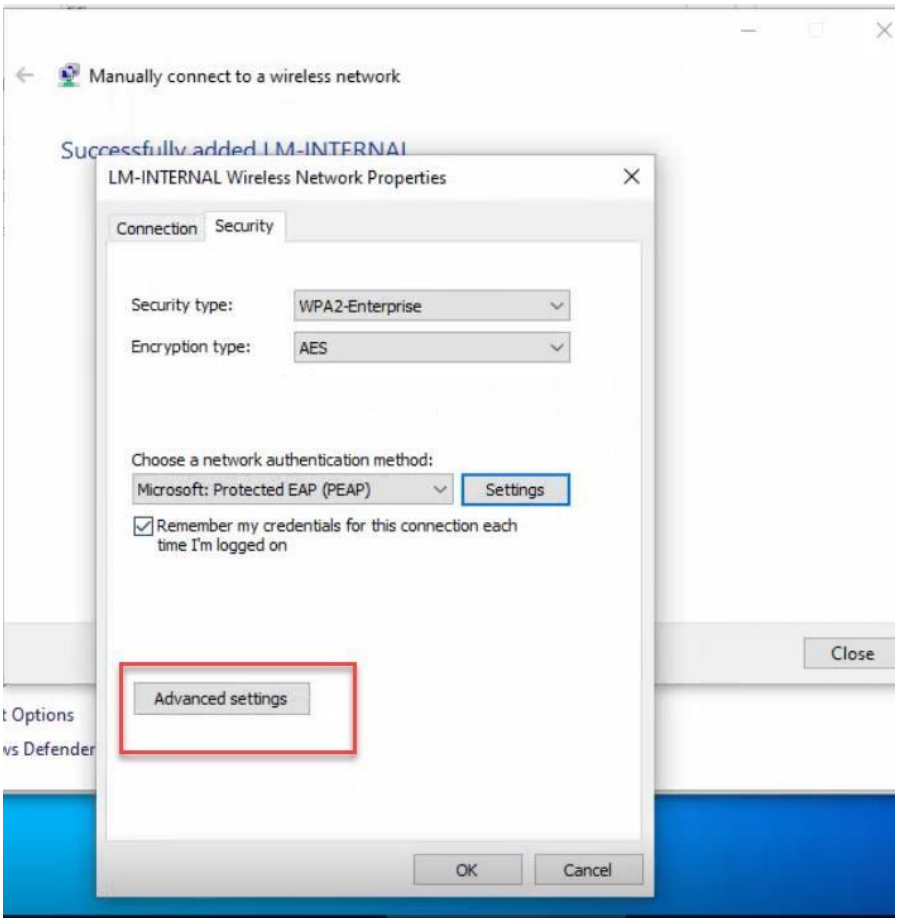
✓ Tại mục Setting:

✓ Trusted Root Certification Authorities:

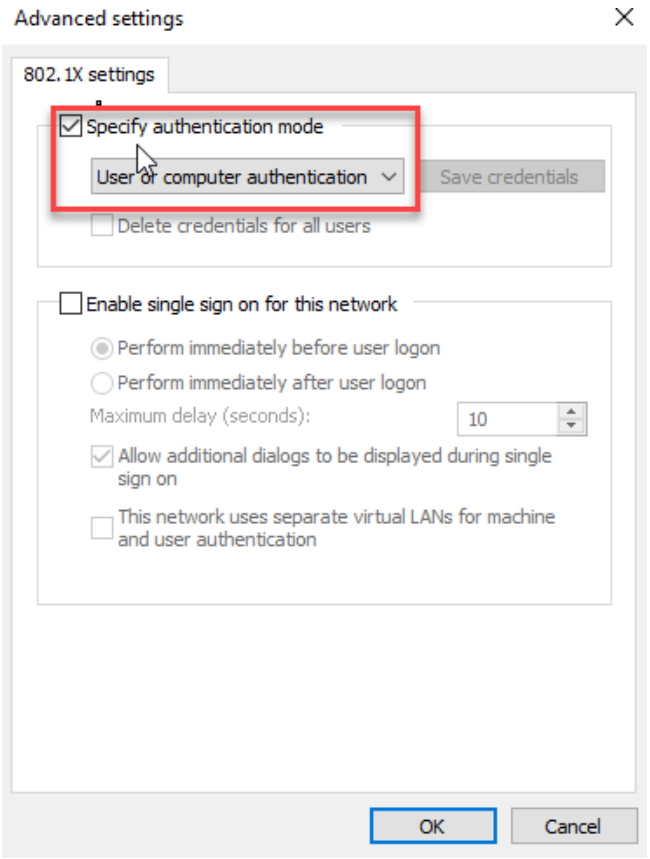
✓ Tick vào LM-ROOT-CA như hình:



✓ Lick vào Advanced settings:

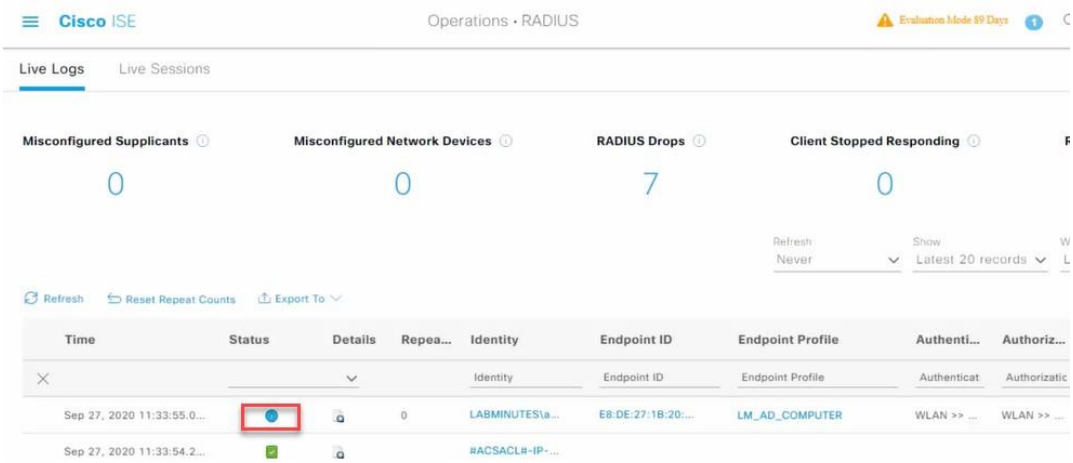


✓ Lick vào ô Specify authentication mode: User or computer authentication



✓ Truy cập vào ISE/ Operation / RADIUS

✓ Ta sẽ thấy xác thực thành công



✓ Ta xem lại thông tin device