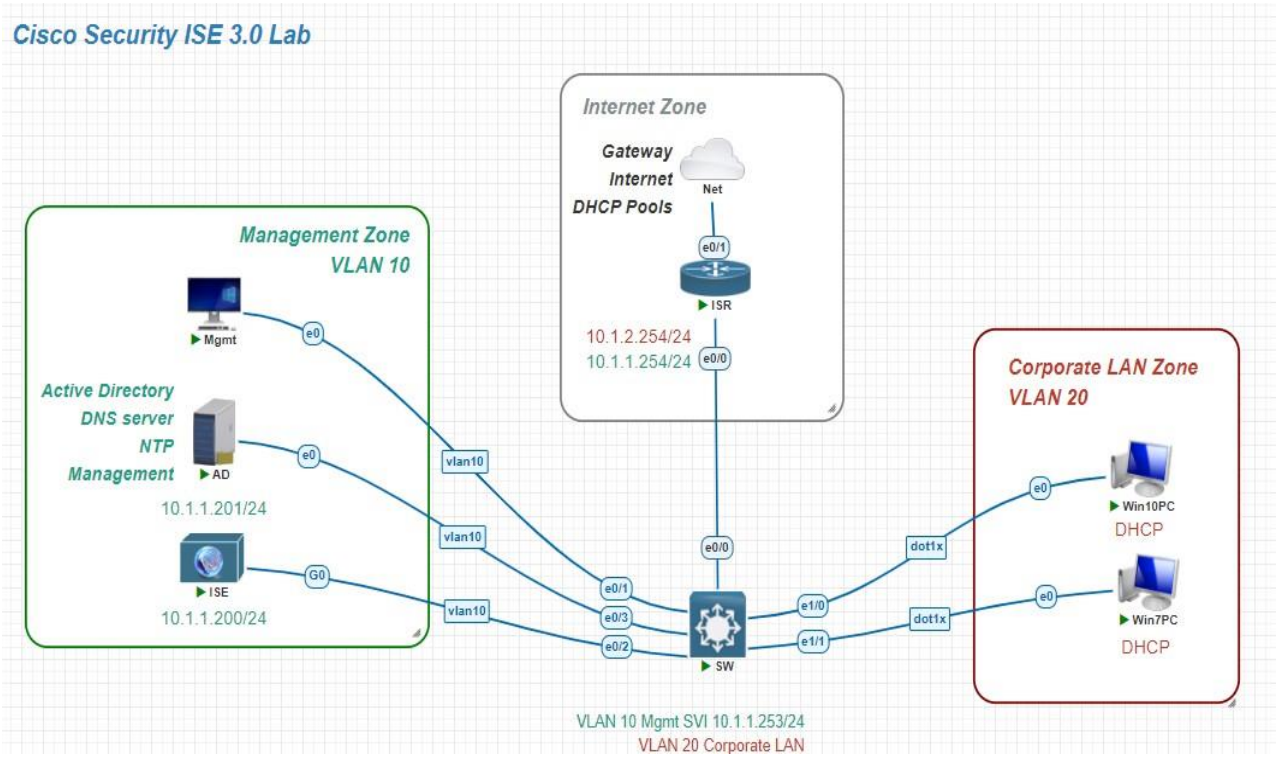
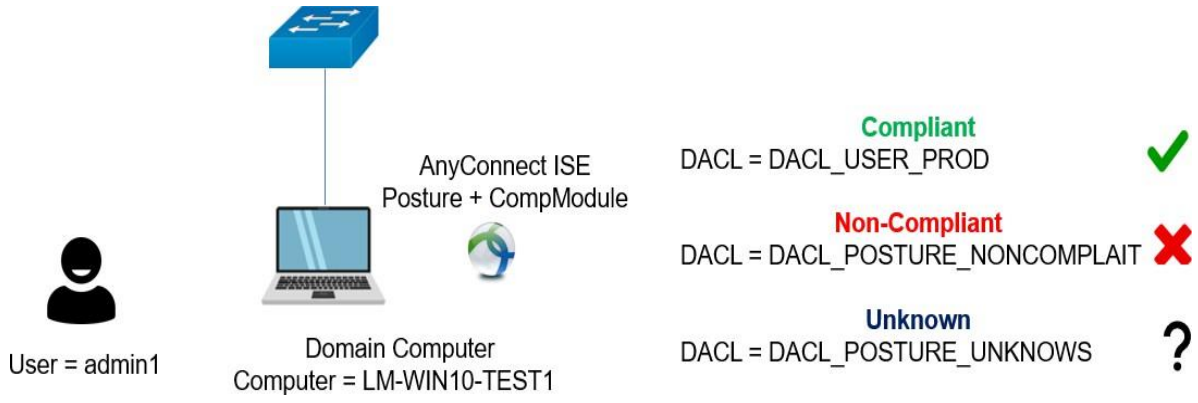
LAB - POSTURE

I. Sơ đồ:



II. Mục đích thực hiện:



Trong trường hợp này, Ta giả sử đang có một thiết bị muốn truy cập vào hệ thống mạng của công ty. Đầu tiên, ISE sẽ chặn tất cả lưu lượng không phải WEB cho đến khi ISE nhận được, Thiết bị đó sẽ redirect đến ISE Provisioning Portal và dowload anyconnect về, và anyconnect sẽ quét các product trong Thiết bị xem có đáp ứng yêu cầu của ISE hay khống và tiến hành cho phép truy cập hệ thống.

Qui trình tạo ra Posture :

1 Posture Conditions => **2** Posture Remediations => **3** Posture Requirement => **4** Posture Policy => **5** Client Provision => **6** Posture Policy

Posture Conditions là tập hợp các quy tắc trong **chính sách bảo mật** nhằm xác định một điểm cuối tuân thủ. Một số mục này bao gồm cài đặt tường lửa, phần mềm chống virus, chống phần mềm độc hại, các bản sửa lỗi, mã hóa ổ đĩa và hơn thế nữa.

Sau khi các **Posture Conditions** được xác định, các biện pháp **Posture Remediation** (nếu cần) có thể được định cấu hình. **Posture Remediation** là phương pháp **AnyConnect** sẽ xử lý các điểm cuối không tuân thủ. Một số biện pháp khắc phục có thể được giải quyết tự động thông qua AnyConnect trong khi các biện pháp khác có thể được người dùng cuối giải quyết theo cách thủ công.

Posture Requirement là các bước hành động tức thì được **AnyConnect** thực hiện khi một điểm cuối không tuân thủ. Một điểm cuối được coi là tuân thủ nếu nó thỏa mãn tất cả các điều kiện về tư thế.

Sau khi được định cấu hình, các **Posture Requirement** sau đó có thể được tham chiếu bởi **Posture Policy** để thực thi tuân thủ. **Client Provision** là chính sách được sử dụng để xác định phiên bản **AnyConnect** được sử dụng cũng như mô-đun tuân thủ sẽ được cài đặt trên điểm cuối trong quá trình cung cấp. Mô-đun tuân thủ là một thư viện mà tác nhân tư thế sử dụng để xác định xem điểm cuối có tuân thủ các điều kiện tư thế xác định hay không. Cuối cùng.

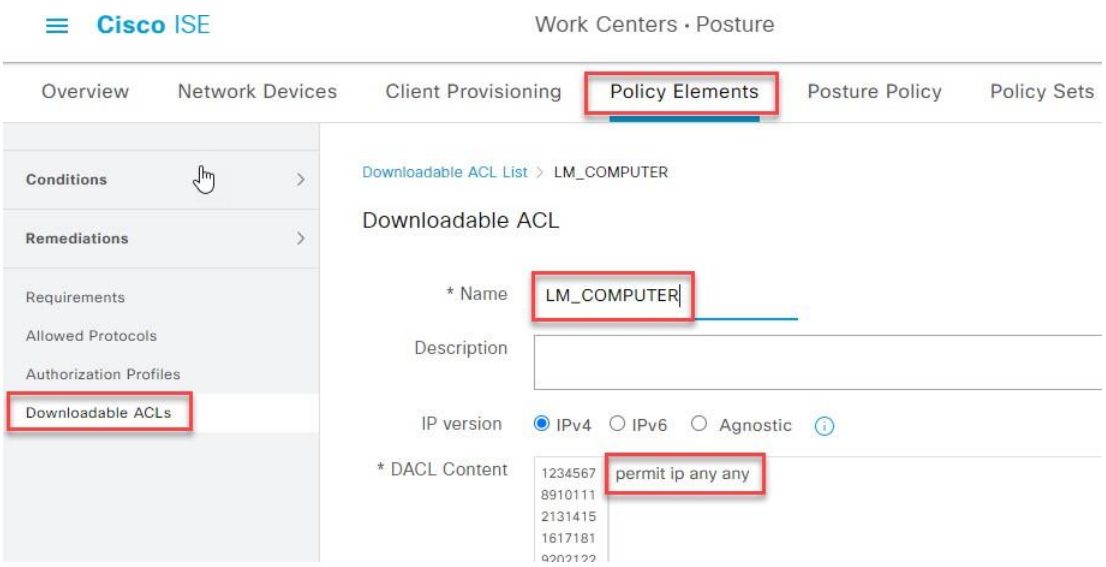
Cuối cùng, **Policy access** sẽ cho **Posture Policy** của chúng tôi và xác định dạng chính sách nào mà điểm cuối sẽ phải tuân theo nếu nó tuân thủ, không tuân thủ hoặc yêu cầu cung cấp AnyConnect.

III. Thực hiện:

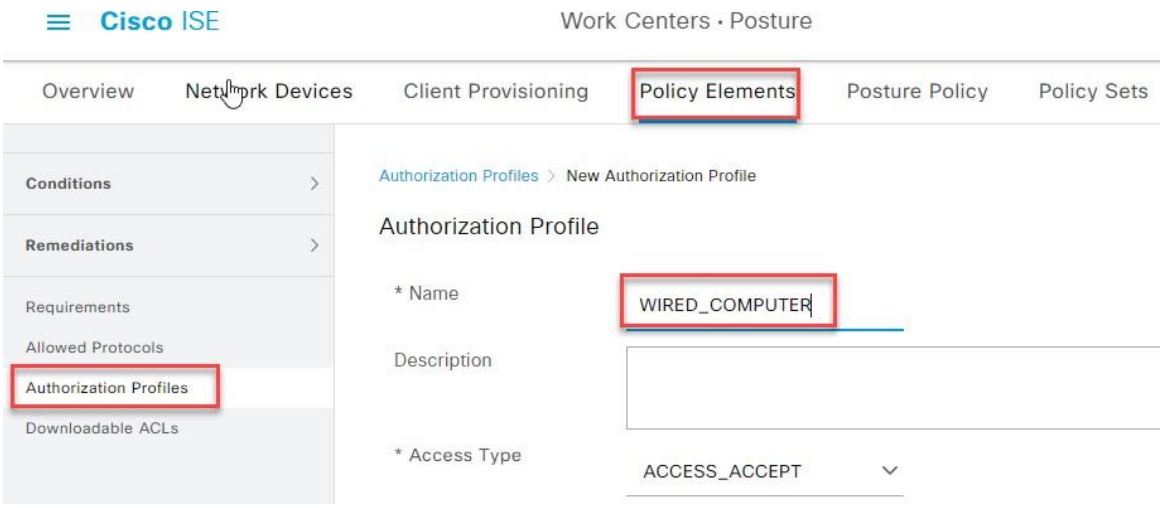
1. Cấu hình Download ACL:

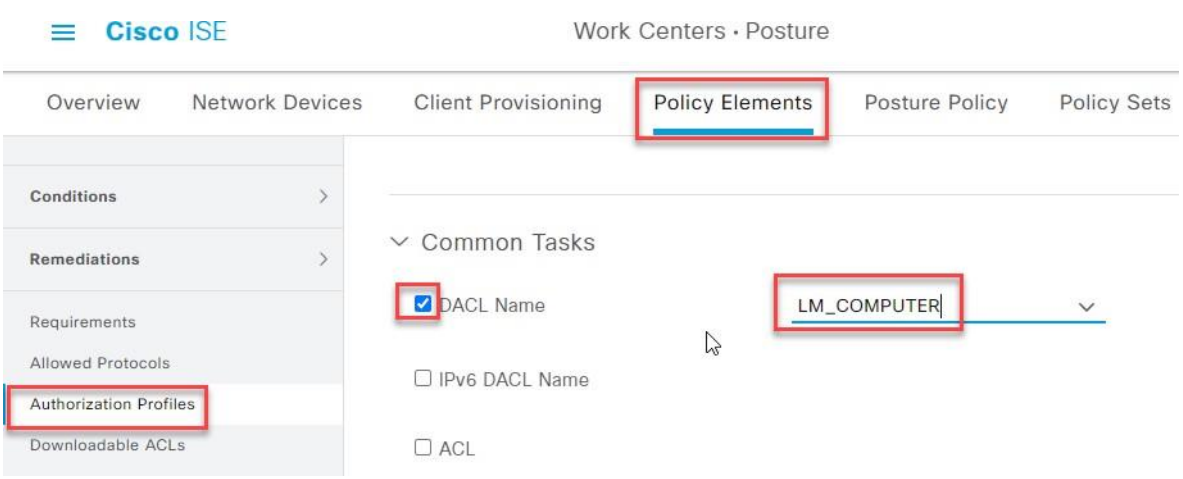
✓ Name: LM_COMPUTER

✓ DACL: permit ip any any



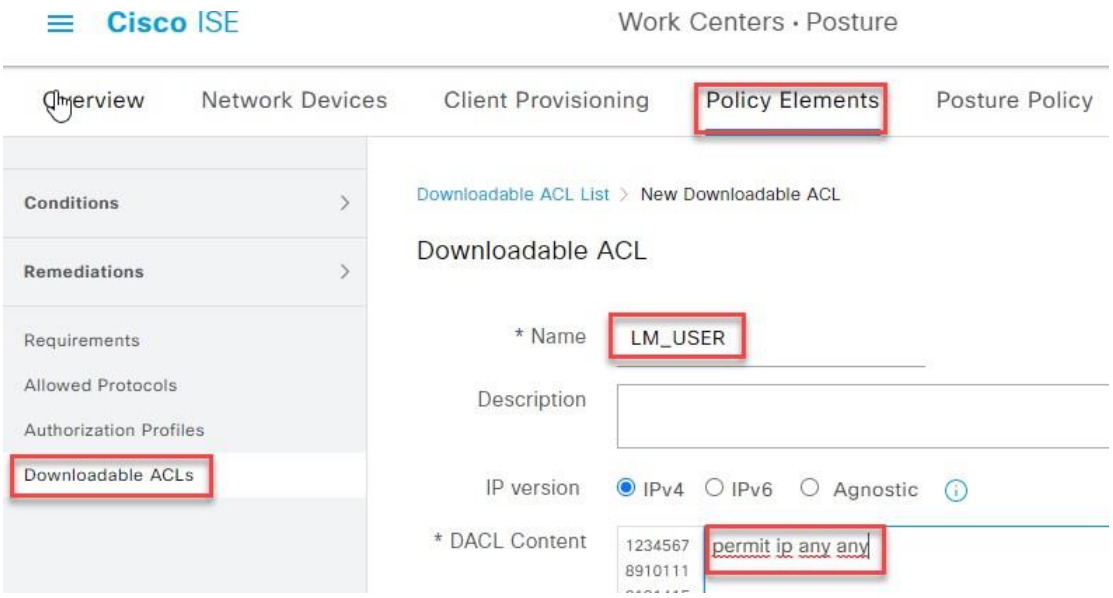
2. Cấu hình Authorization Profiles:

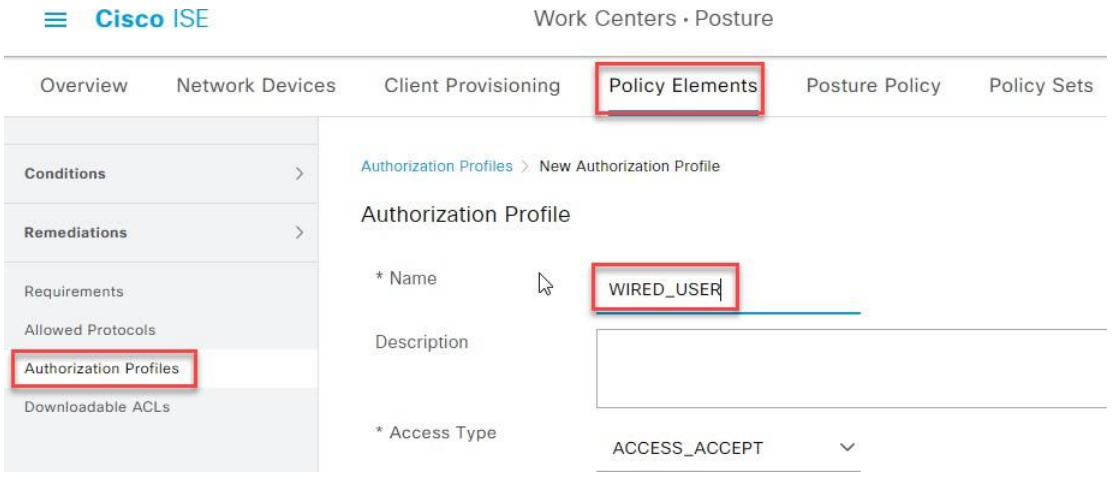


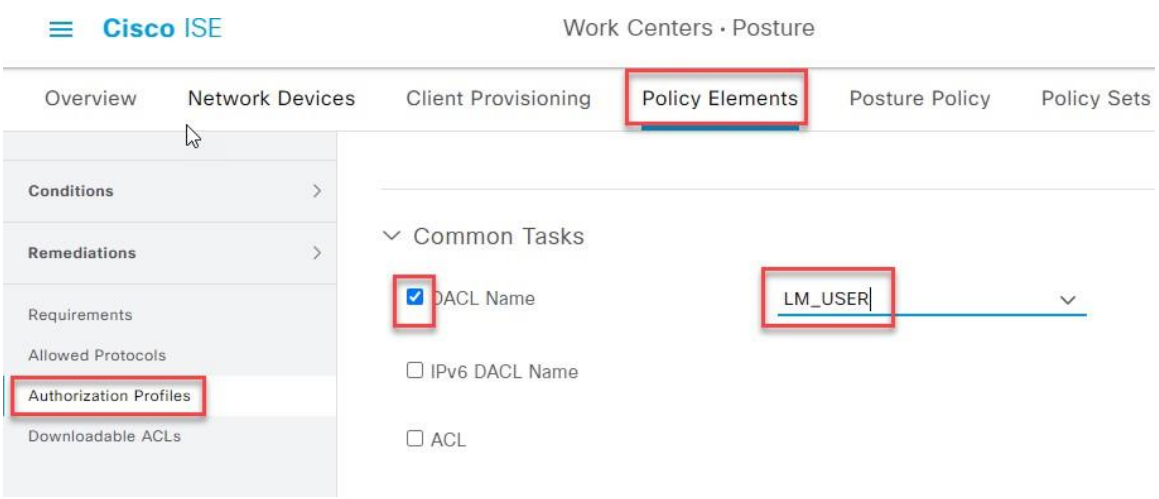


✓ Name: LM_USER

✓ DACL: permit ip any any



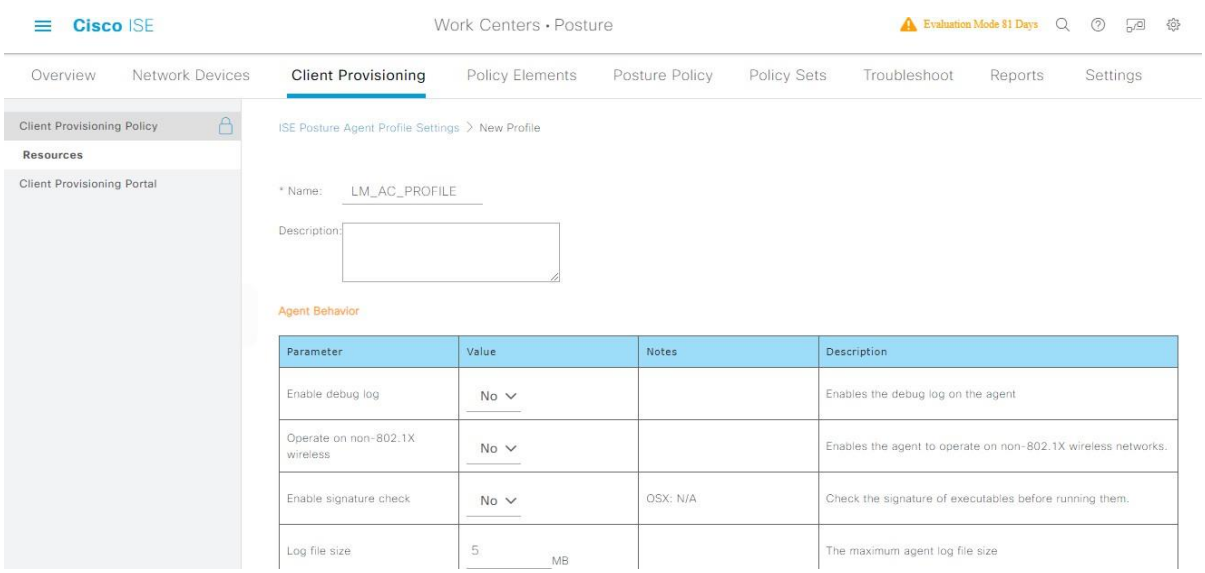


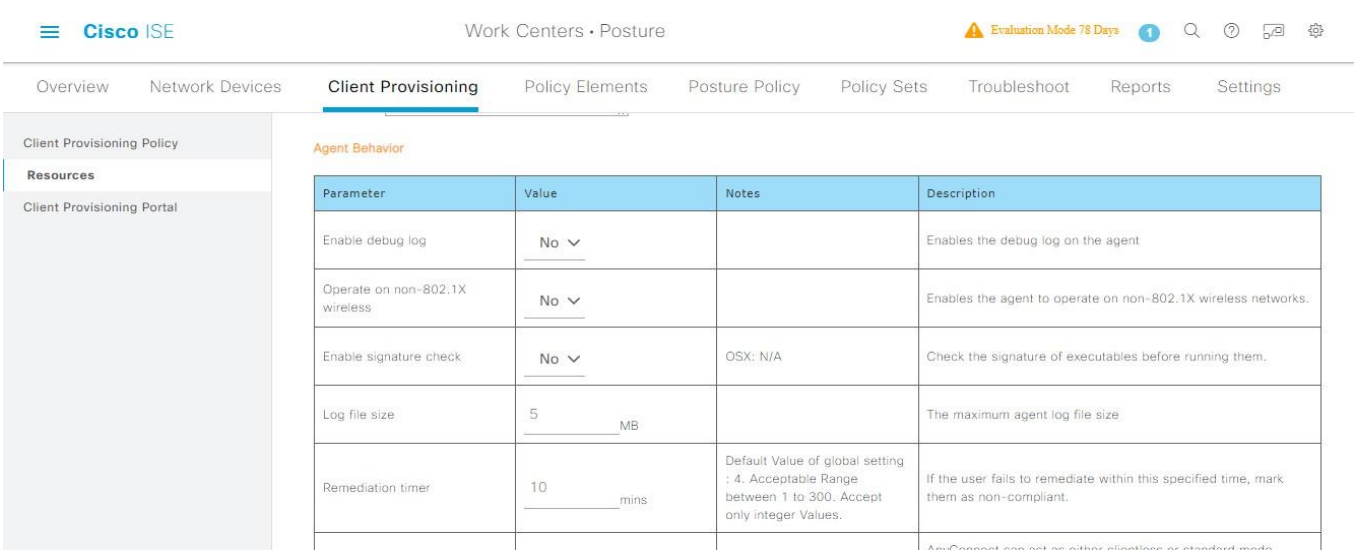


3. Cấu hình Client Provisioning:

3.1 Tạo AnyConnect Posture Profile:

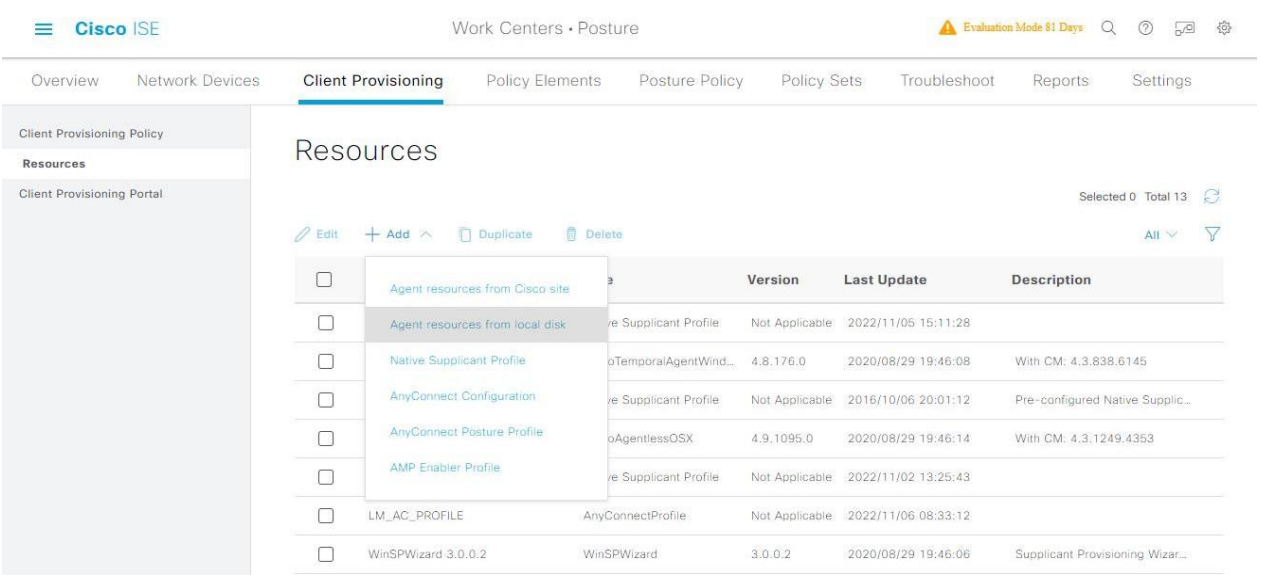
- ✓ Vào Resource → +Add → Anyconnect Posture Profile
- ✓ Name: LM_AC_PROFILE
- ✓ Remediation timer: 10
- ✓ Server name rule: *.eve.lab



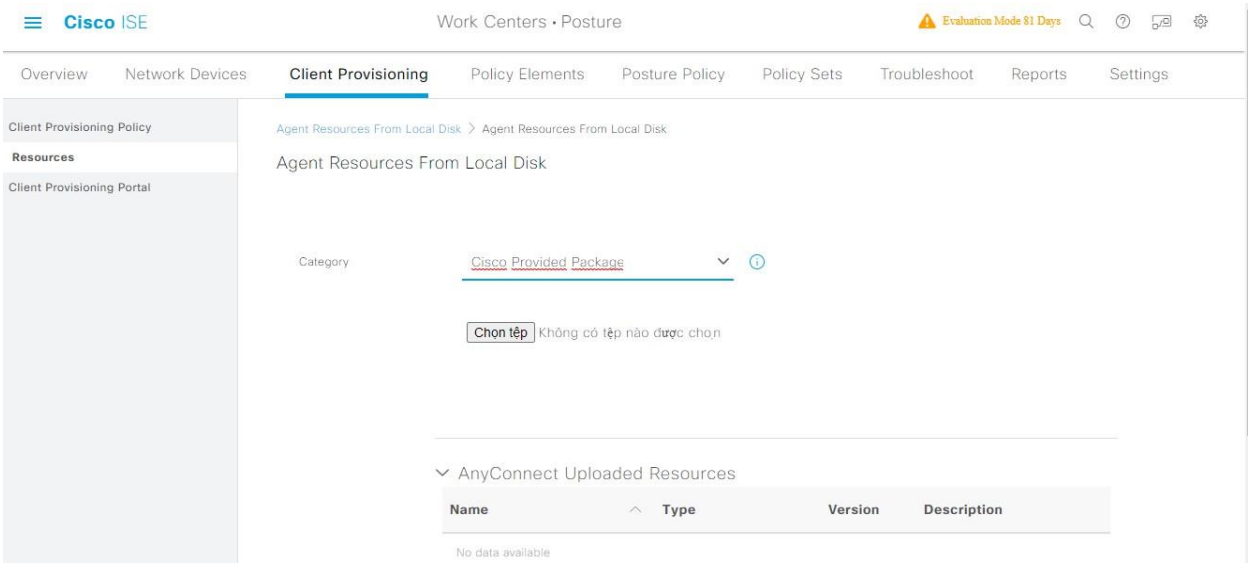


3.2 Tạo AnyConnect Configuration:

✓ Đầu tiên ta vào Resource , ta chọn +Add, chuyển đến mục Agent resource from local disk

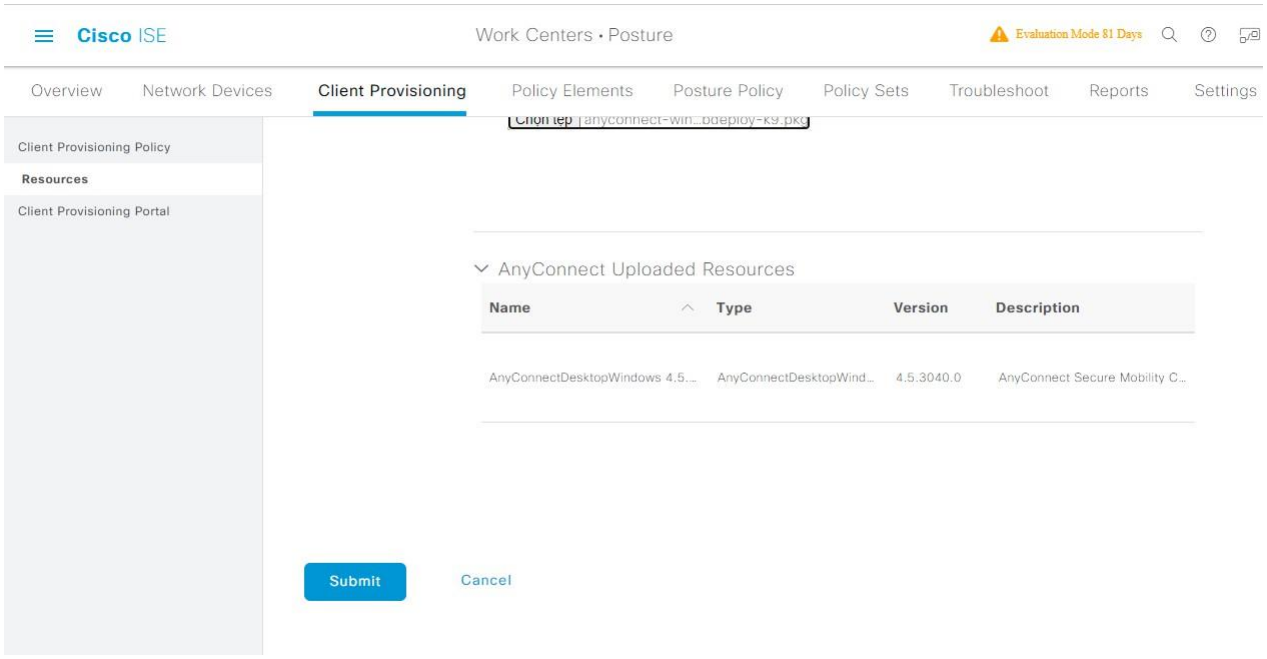


✓ Trong mục Category: chọn mục Cisco Provided Package

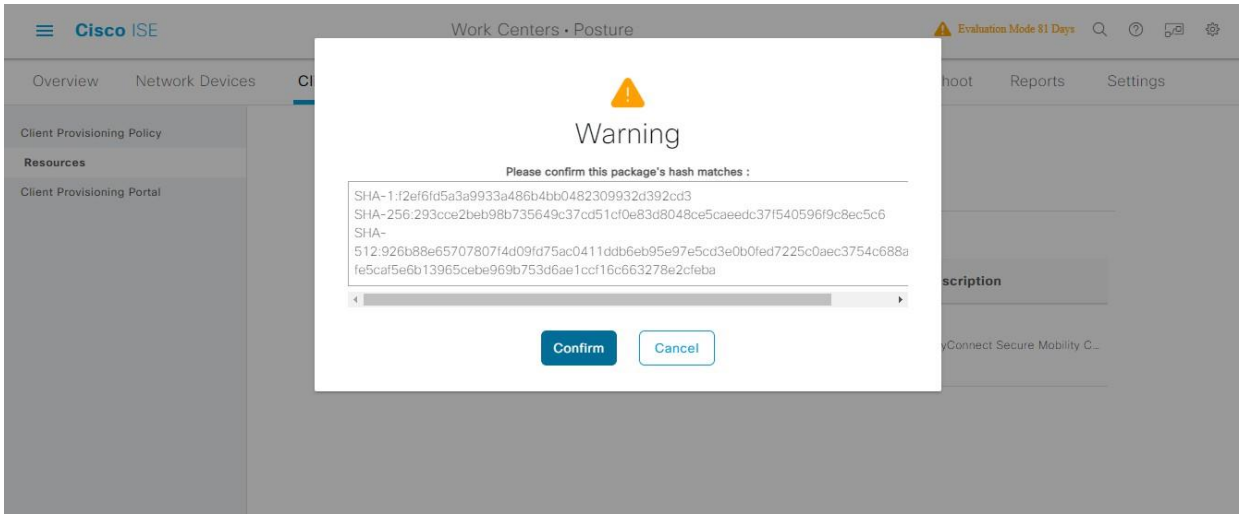


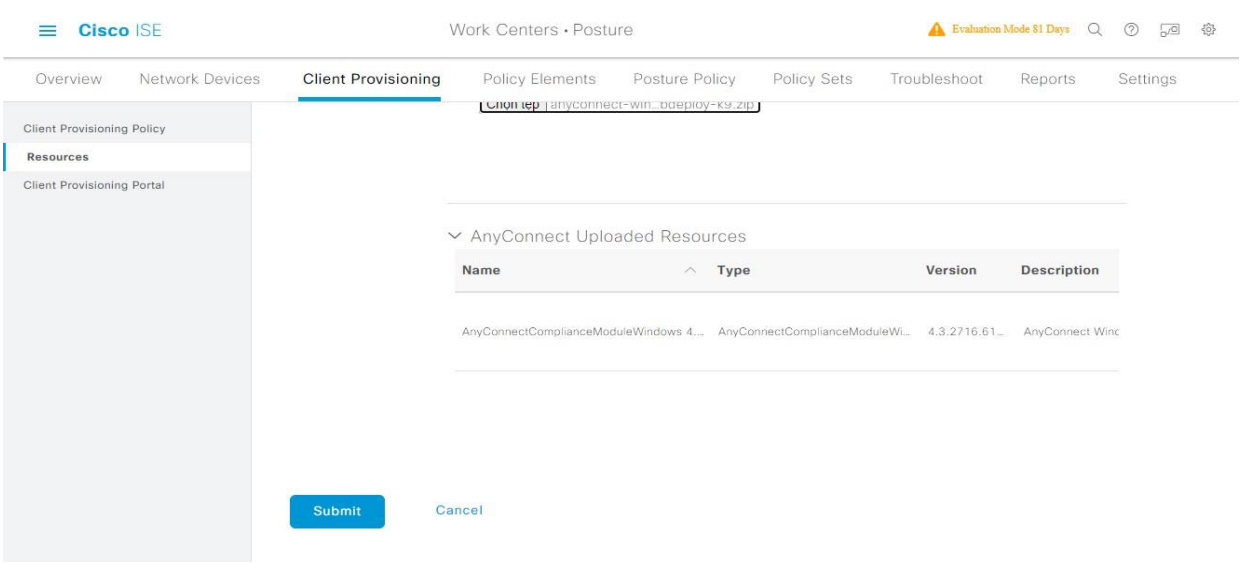
✓ Chọn 2 file **AnyConnectDesktopWindows4.5** , **AnyConnectCompliantModule** và lần lượt import vào

✓ Lưu ý: File Anyconnect Desktop và Compliant sẽ có sẵn trên các PC, chỉ cần chọn và import vào là được. 2 file này được dùng cho các user tải về khi họ truy cập vào hệ thống.

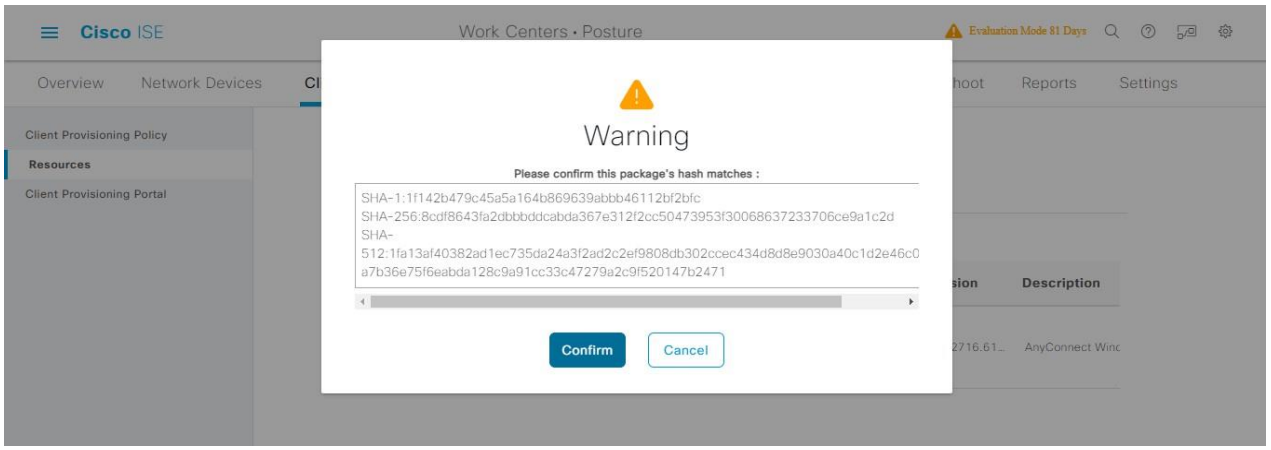


✓ Ta chọn Confirm

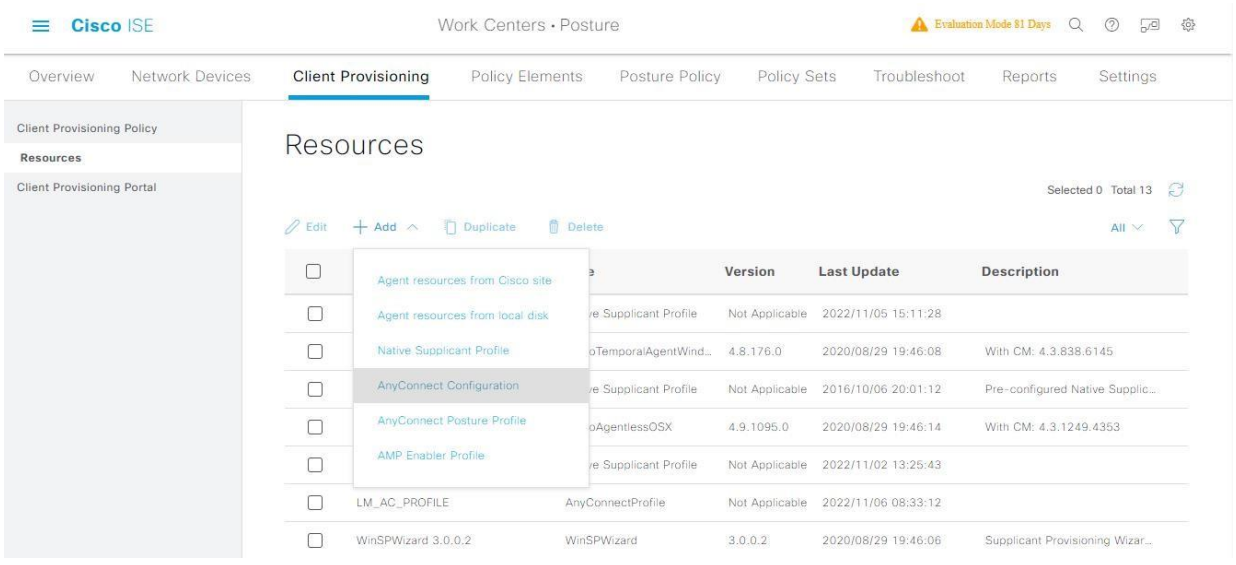




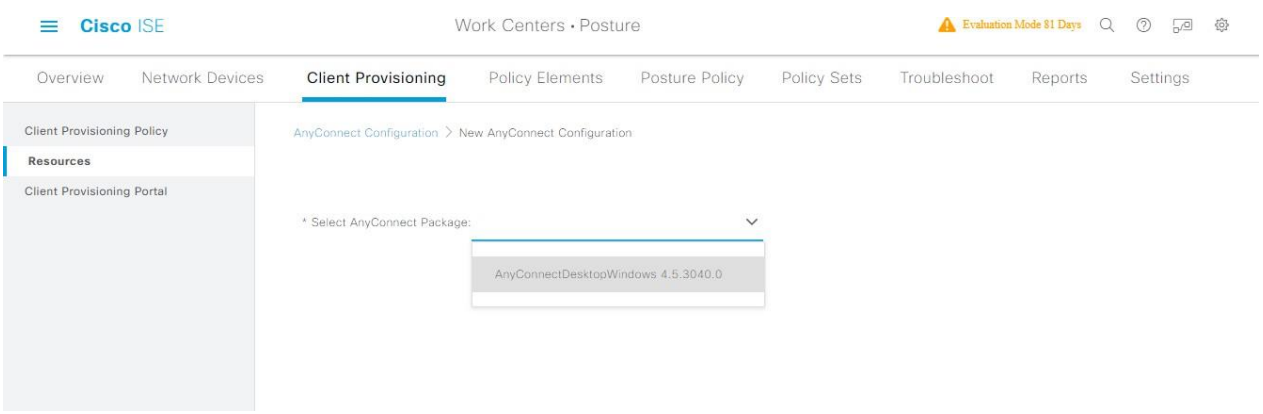
✓ Ta tiếp tục chọn Confirm



✓ Trên tab Client Provisioning, chọn mục AnyConnect Configuration.



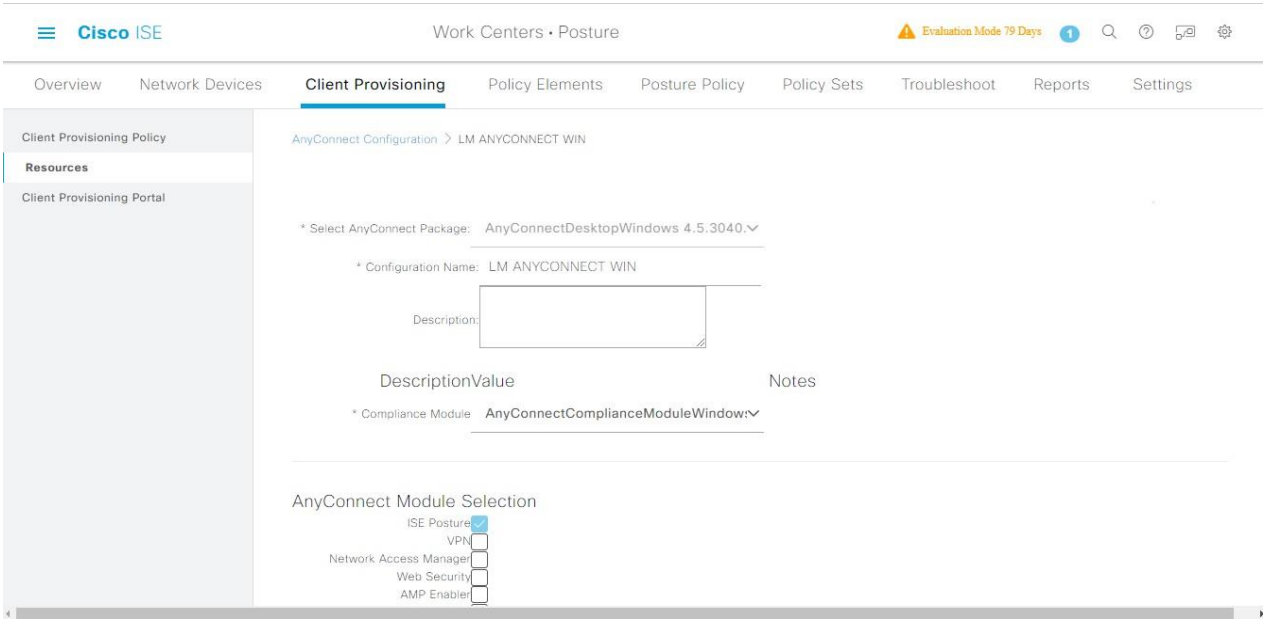
✓ Mục Select AnyConnect Package: chọn AnyconnectWindow 4.5 3040.0



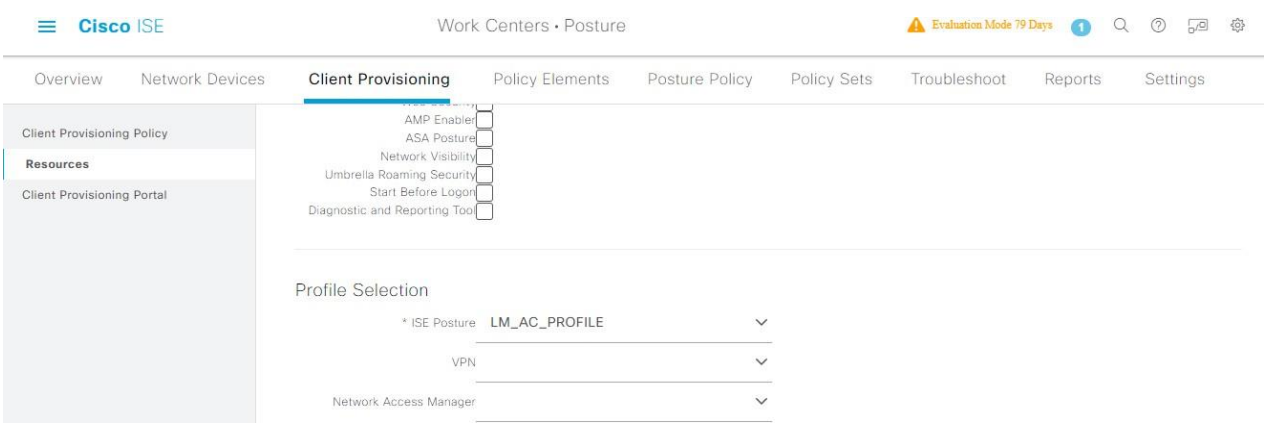
✓ Mục Configuration Name: LM ANYCONNECT WIN

✓ Compliance Module: AnyConnectCompliantModuleWindow

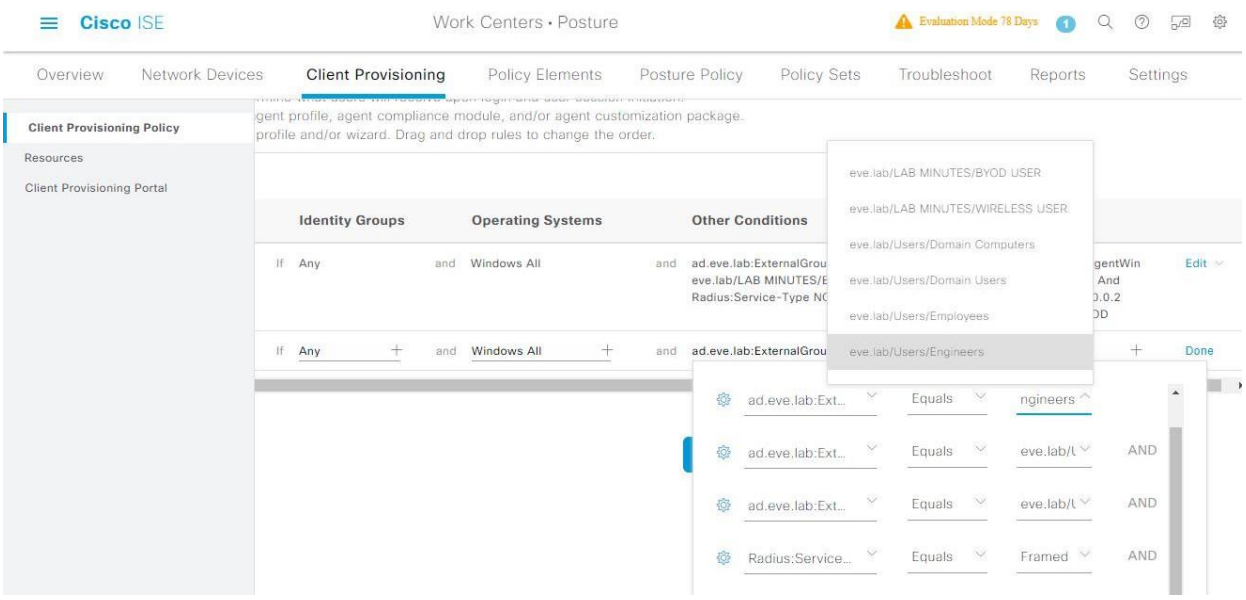
✓ Bỏ tick VPN

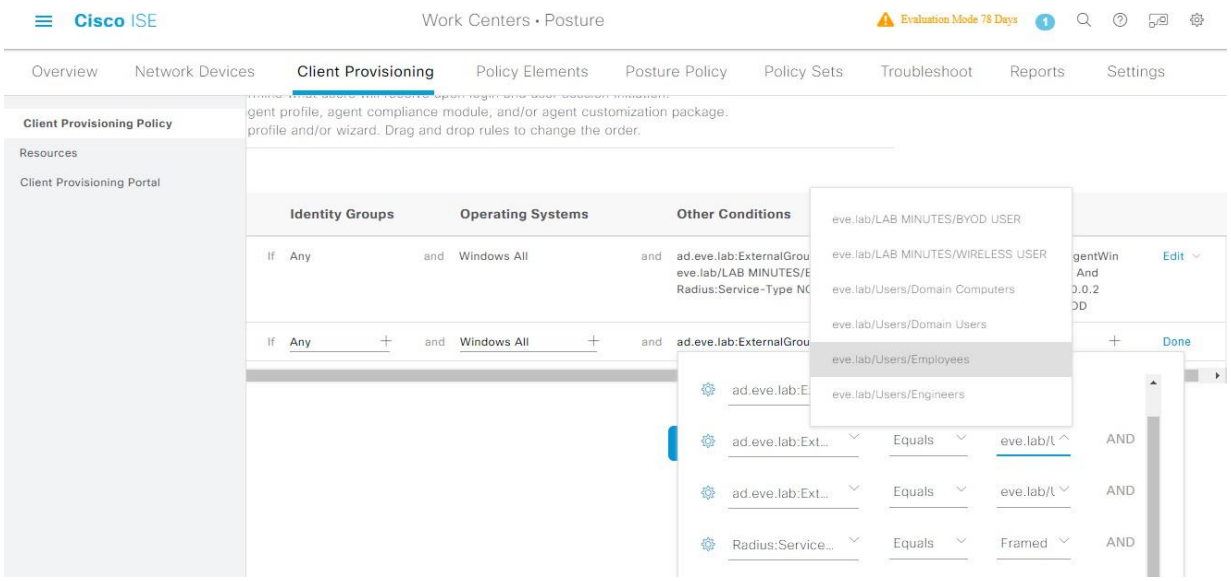


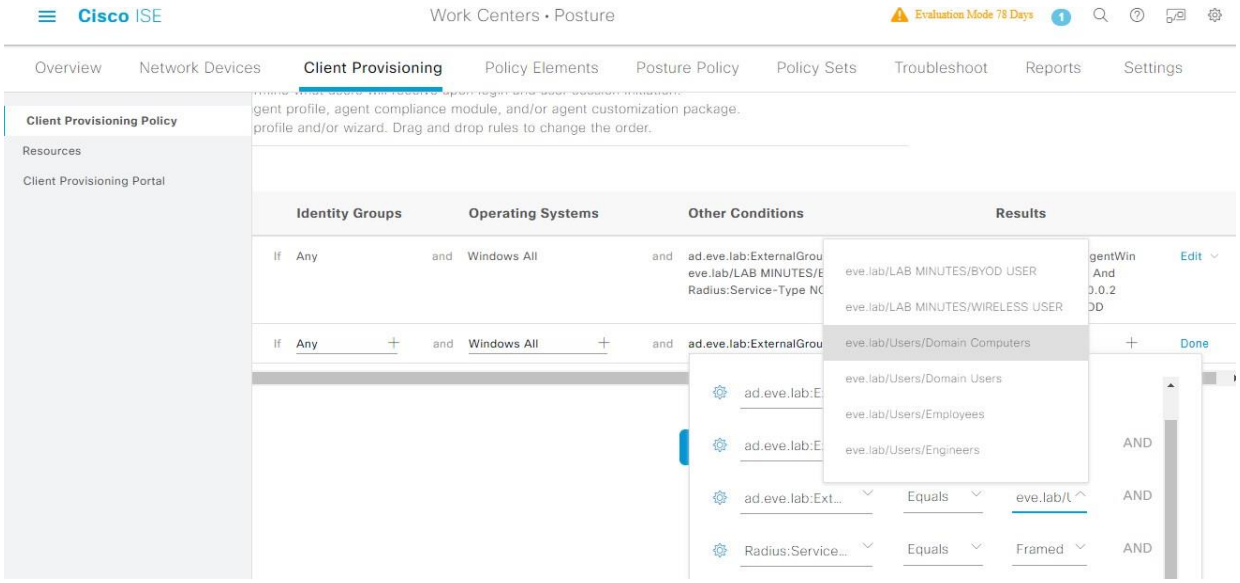
✓ ISE Posture: chọn LM_AC_PROFILE



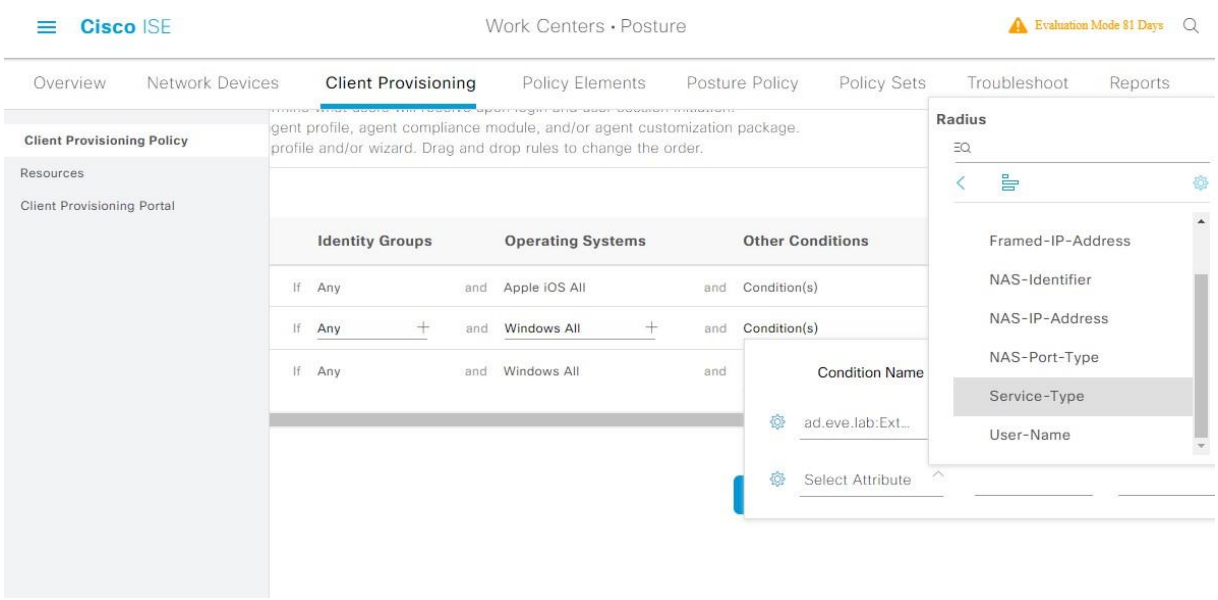
- ✓ Chuyển hướng đến Client Provisioning
- ✓ Chọn tab Client Provisioning Policy
- ✓ Chọn edit
- ✓ Insert new policy
- ✓ Identify Groups: Any
- ✓ Operating Systems: Windows All
- ✓ Other Conditions:
  - ad.eve.lab:ExternalGroup EQUALS eve.lab/Users/Domain Computers
  - Radius:Service-Type EQUALS Framed
- ✓ Results: LM ANYCONNECT WIN

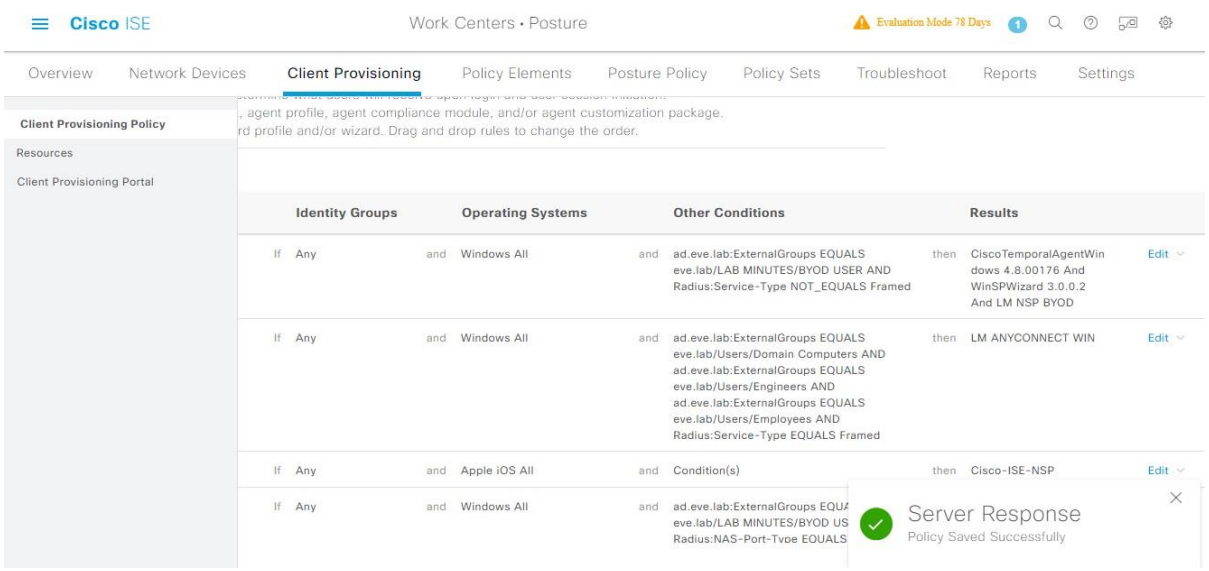


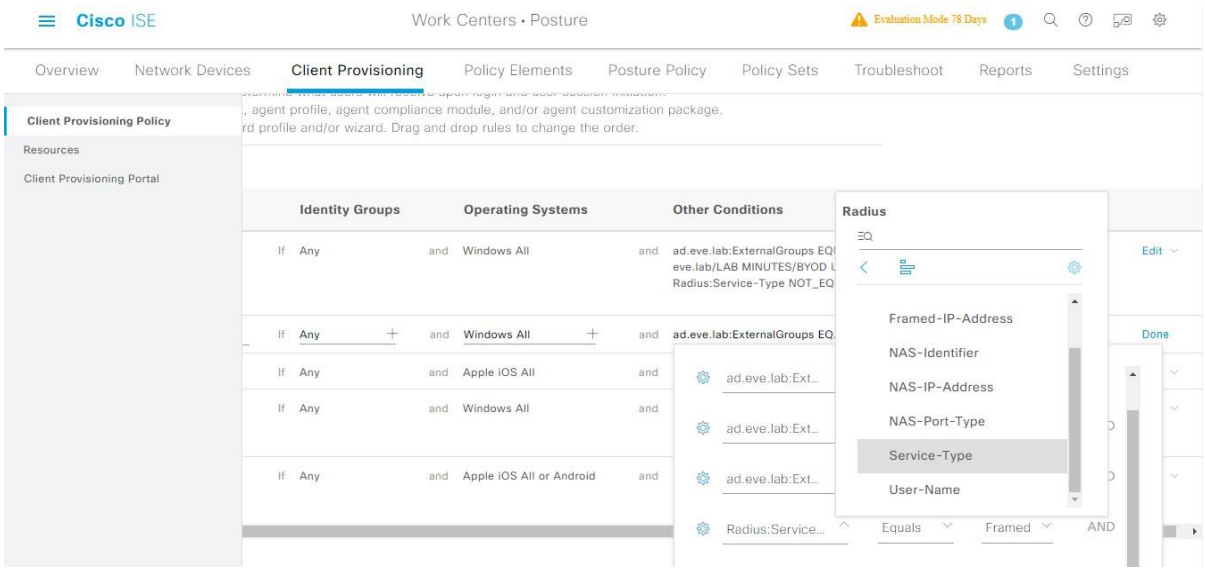


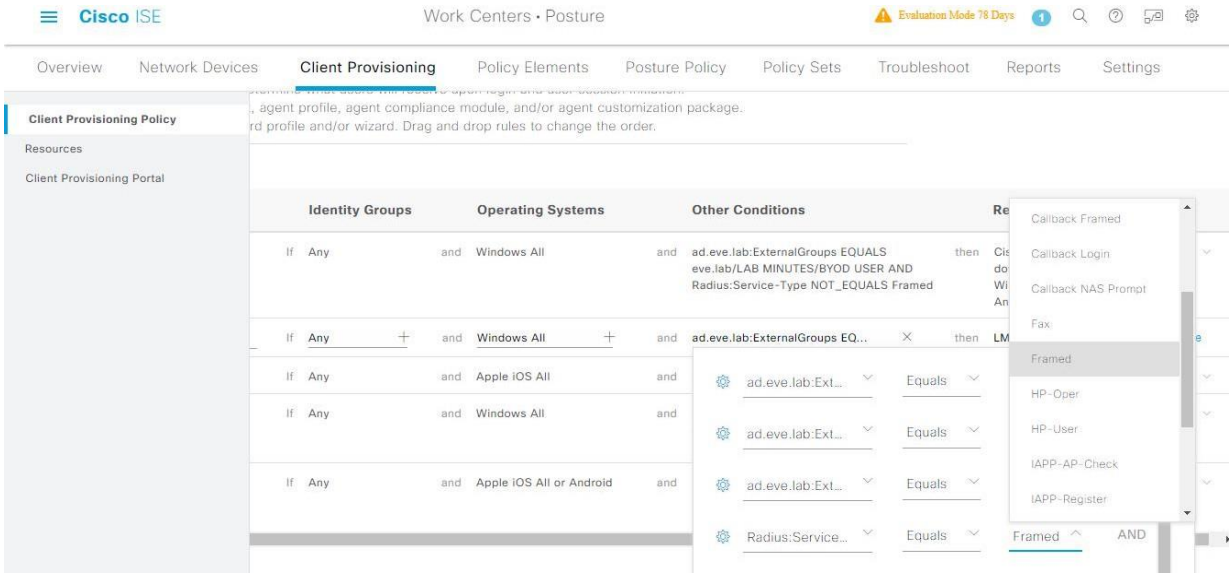


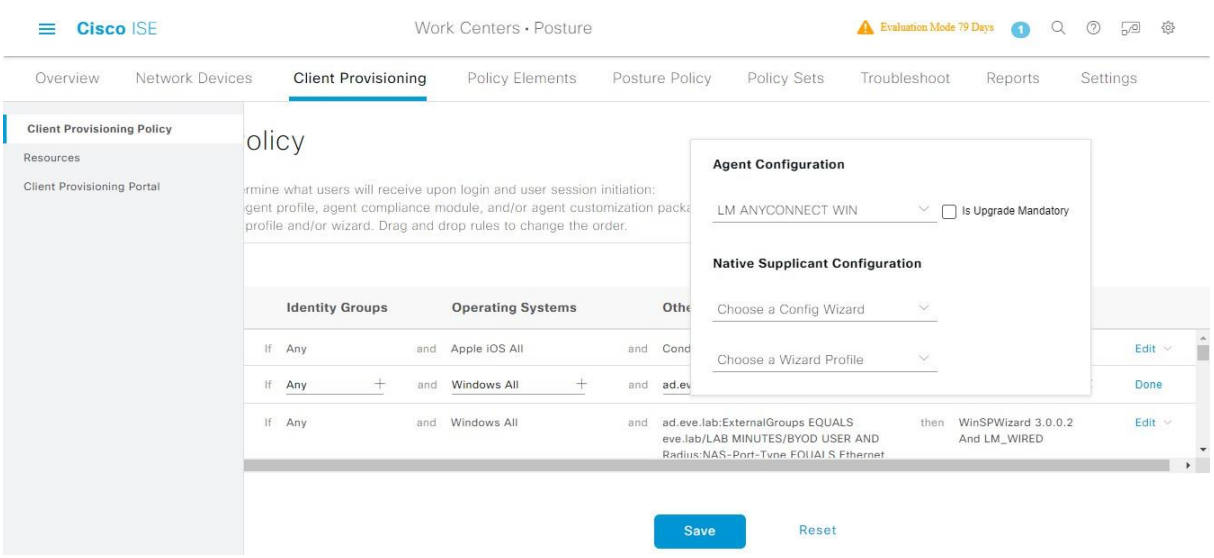
✓ Cấu hình Client Provisioning Policy:


Cisco ISE
Work Centers · Posture
Evaluation Mode 81 Days
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Client Provisioning Policy
Resources
Client Provisioning Portal
gent profile, agent compliance module, and/or agent customization package.
profile and/or wizard. Drag and drop rules to change the order.
Identity Groups
Operating Systems
Other Conditions
If Any and Apple iOS All and Condition(s)
If Any and Windows All and Condition(s)
If Any and Windows All and
Radius
Framed-IP-Address
NAS-Identifier
NAS-IP-Address
NAS-Port-Type
Service-Type
User-Name
Condition Name
ad.eve.lab:Ext...
Select Attribute


Cisco ISE
Work Centers · Posture
Evaluation Mode 78 Days
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Client Provisioning Policy
Resources
Client Provisioning Portal
, agent profile, agent compliance module, and/or agent customization package.
rd profile and/or wizard. Drag and drop rules to change the order.
Identity Groups
Operating Systems
Other Conditions
Results
If Any and Windows All and ad.eve.lab:ExternalGroups EQUALS eve.lab/LAB MINUTES/BYOD USER AND Radius:Service-Type NOT_EQUALS Framed then CiscoTemporalAgentWindows 4.8.00176 And WinSPWizard 3.0.0.2 And LM NSP BYOD Edit
If Any and Windows All and ad.eve.lab:ExternalGroups EQUALS eve.lab/Users/Domain Computers AND ad.eve.lab:ExternalGroups EQUALS eve.lab/Users/Engineers AND ad.eve.lab:ExternalGroups EQUALS eve.lab/Users/Employees AND Radius:Service-Type EQUALS Framed then LM ANYCONNECT WIN Edit
If Any and Apple iOS All and Condition(s) then Cisco-ISE-NSP Edit
If Any and Windows All and ad.eve.lab:ExternalGroups EQUA
eve.lab/LAB MINUTES/BYOD US
Radius:NAS-Port-Type EQUALS
Server Response
Policy Saved Successfully

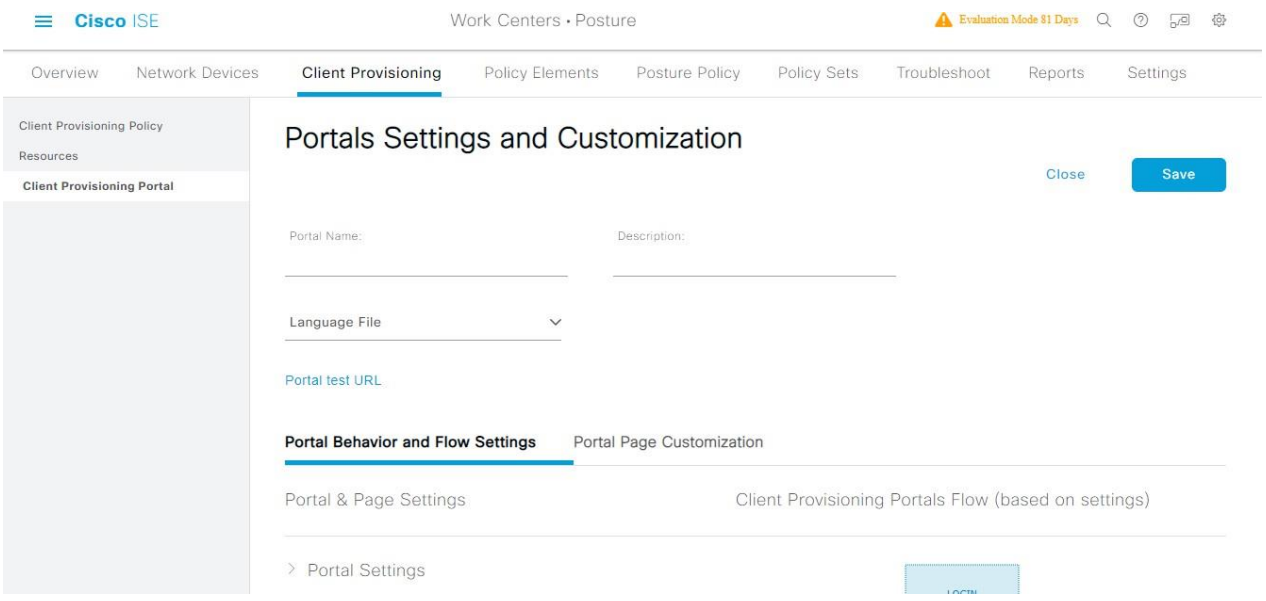

Cisco ISE
Work Centers · Posture
Evaluation Mode 78 Days
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Client Provisioning Policy
Resources
Client Provisioning Portal
Identity Groups
Operating Systems
Other Conditions
Radius
Framed-IP-Address
NAS-Identifier
NAS-IP-Address
NAS-Port-Type
Service-Type
User-Name
Edit
Done
Equals
Framed
AND


Cisco ISE
Work Centers · Posture
Evaluation Mode 78 Days
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Client Provisioning Policy
Resources
Client Provisioning Portal
Identity Groups
Operating Systems
Other Conditions
Callback Framed
Callback Login
Callback NAS Prompt
Fax
Framed
HP-Oper
HP-User
IAPP-AP-Check
IAPP-Register
Equals
Framed
AND

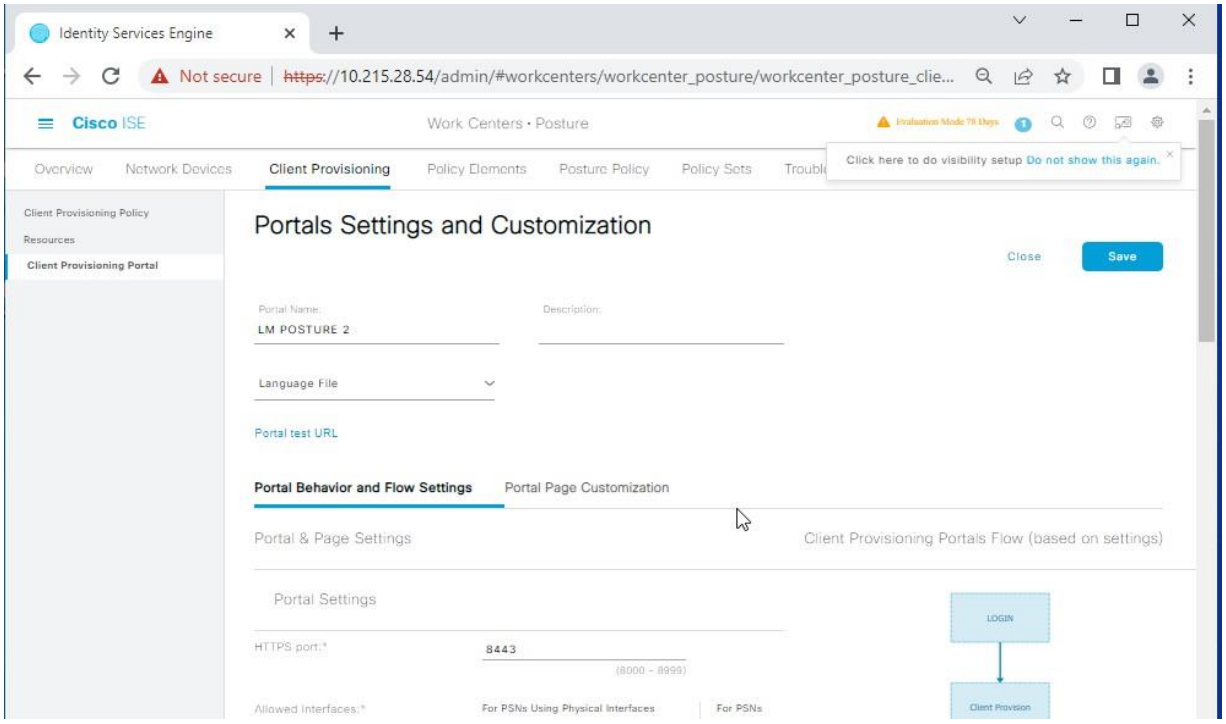


3.3 Cấu hình Portal Settings and Customization:

- ✓ Ta sẽ tạo giao diện Portal để các user đăng nhập và download Anyconnect về thiết bị của họ
- ✓ Vào Client Provisioning Portal
- ✓ Tạo Portal mới



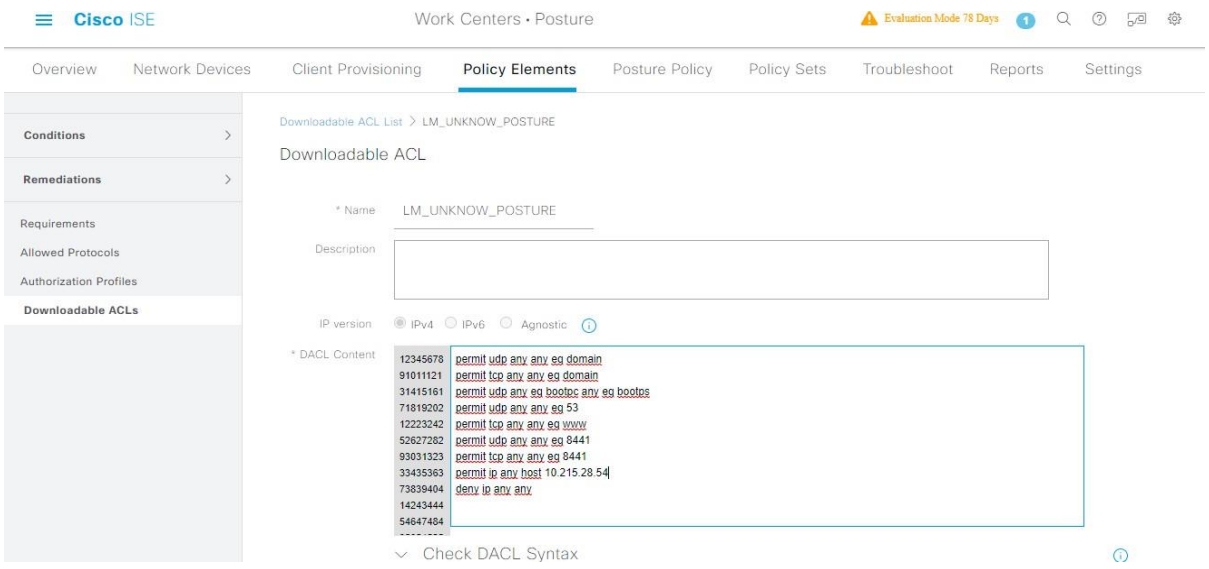
- ✓ Portal Name: LM POSTURE 2, sau đó Save



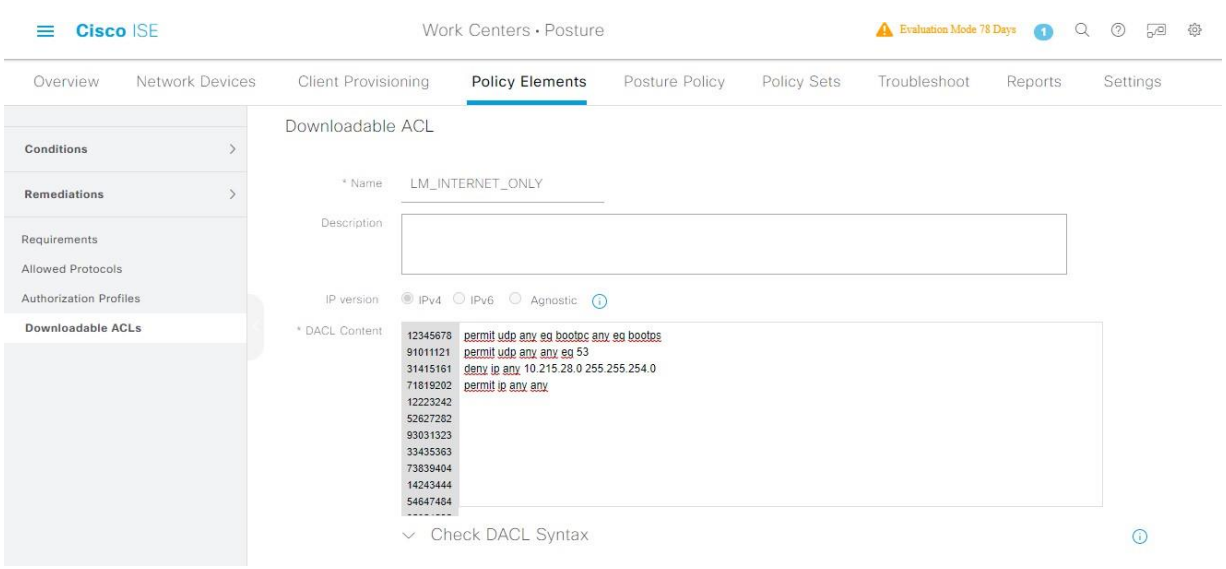
3.4 Cấu hình DACL:

✓ Name: LM_UNKNOW_POSTURE

✓ DACL Content:

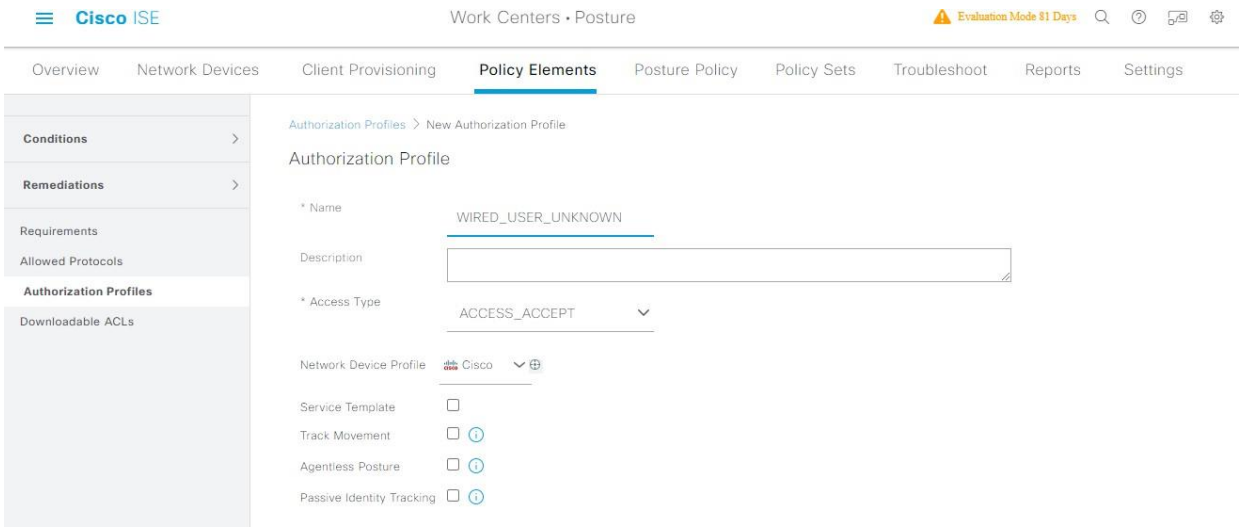


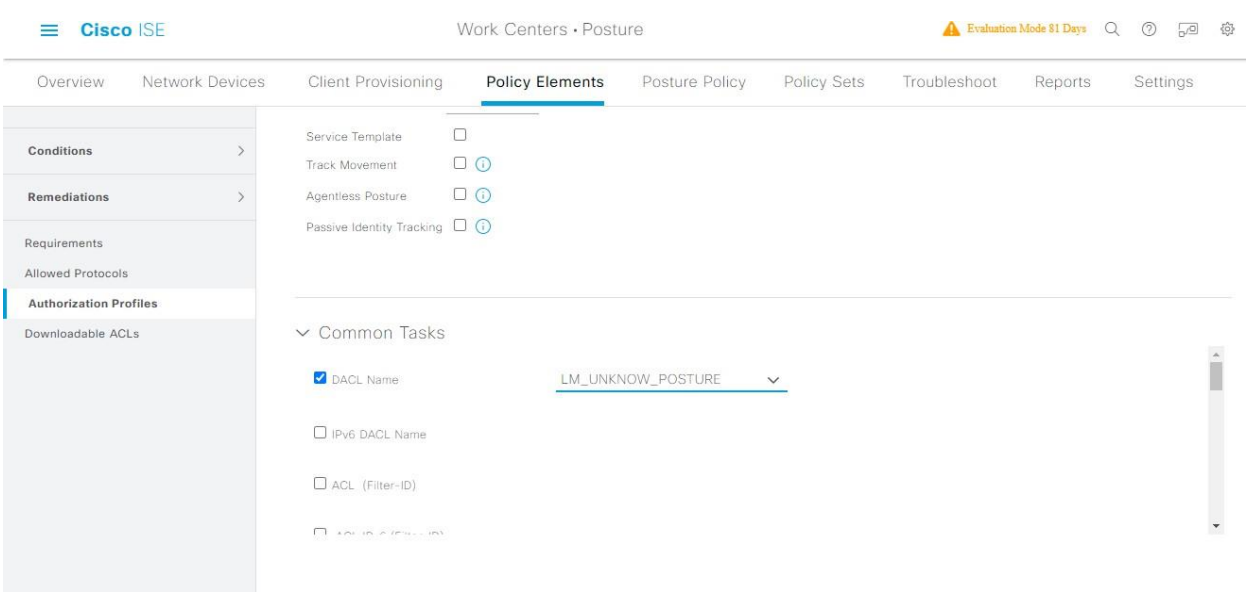
✓ Name: LM_INTERNET_ONLY



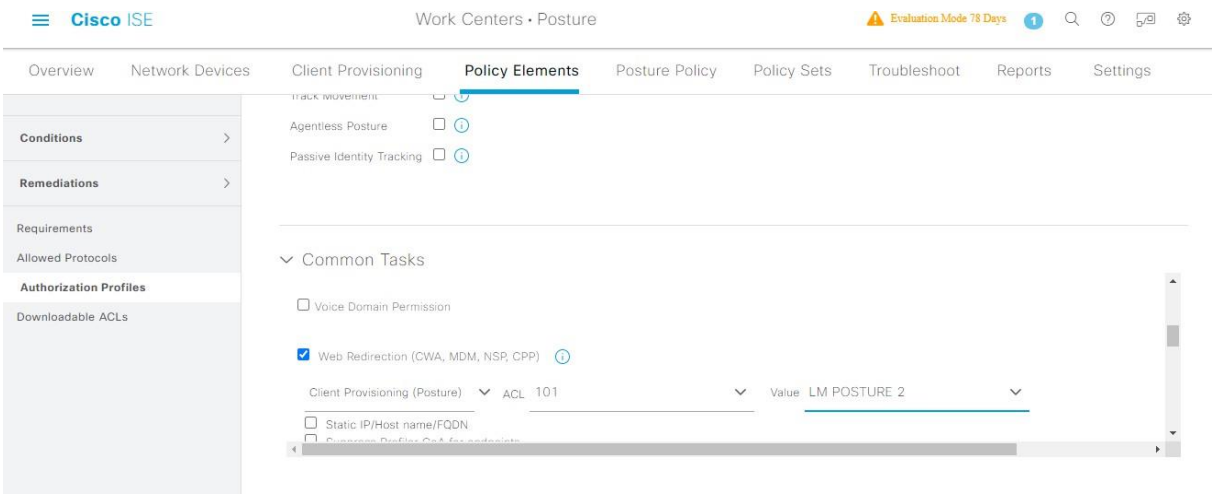
3.5 Cấu hình Authorization Profiles:

- ✓ Name: WIRED_USER_UNKNOW
- ✓ Common Task: LM_UNKNOW_POSTURE

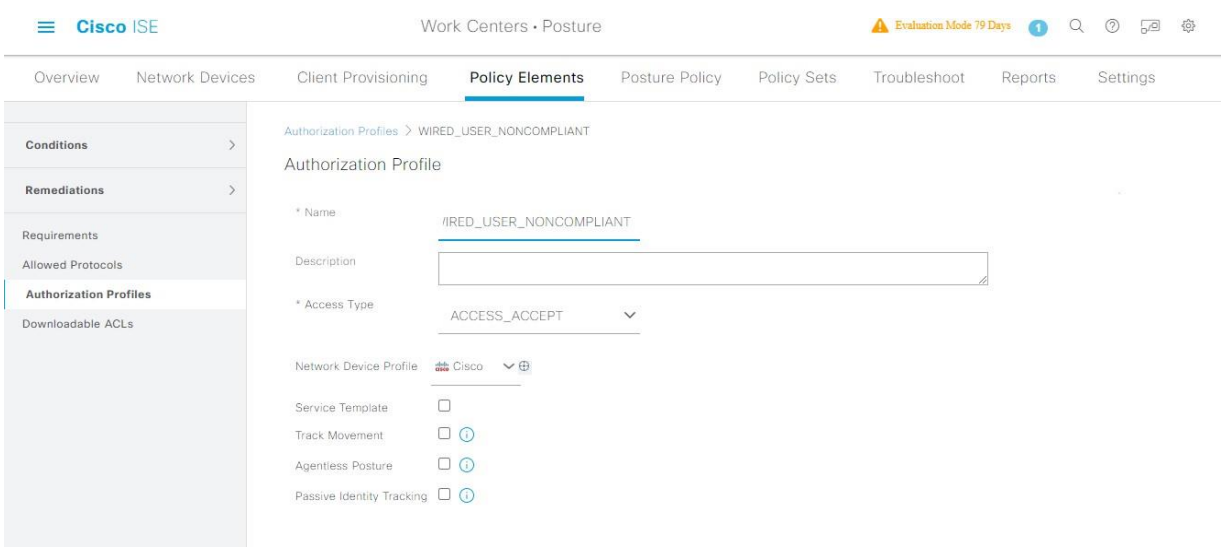




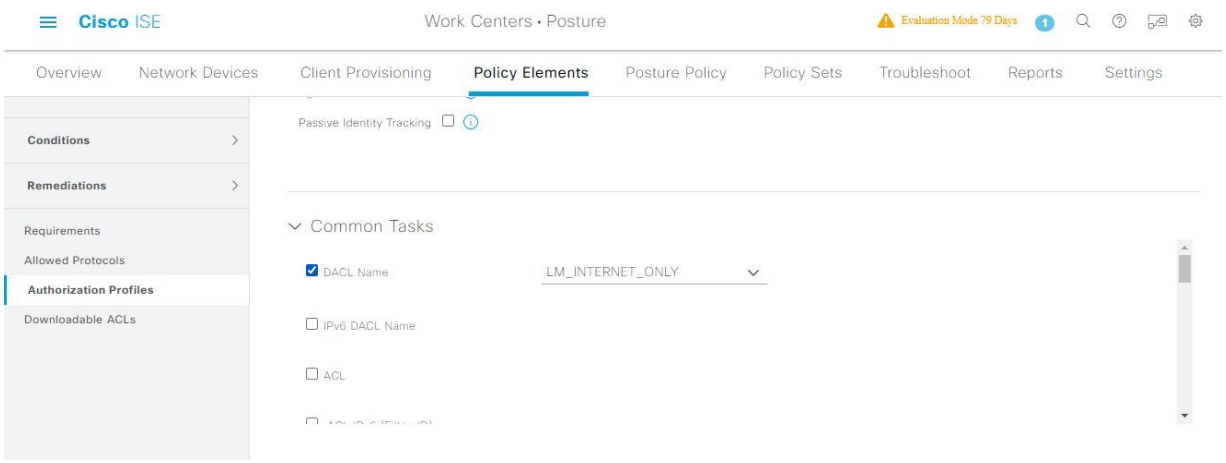
- ✓ Tại mục Web Redirection:
- ✓ Ta chọn mục: Client Provisioning (Posture)
- ✓ ACL : 101 (ACL này đã có trên switch 3k)
- ✓ Value: LM POSTURE 2



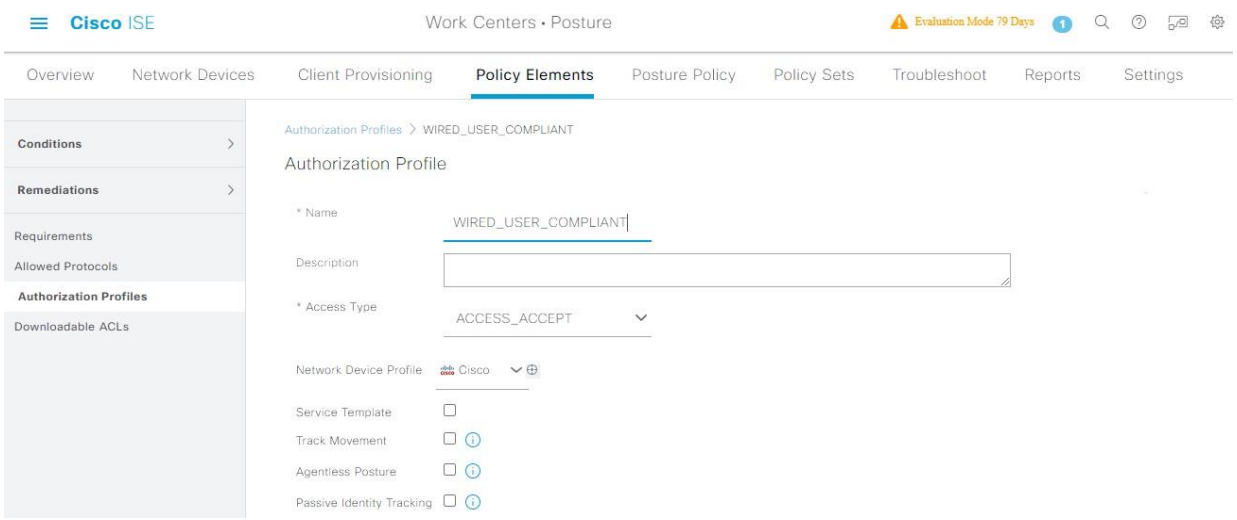
✓ Name: WIRED_USER_NONCOMPLIANT



✓ Authorization Profiles, mục DACL Name: LM_INTERNET_ONLY

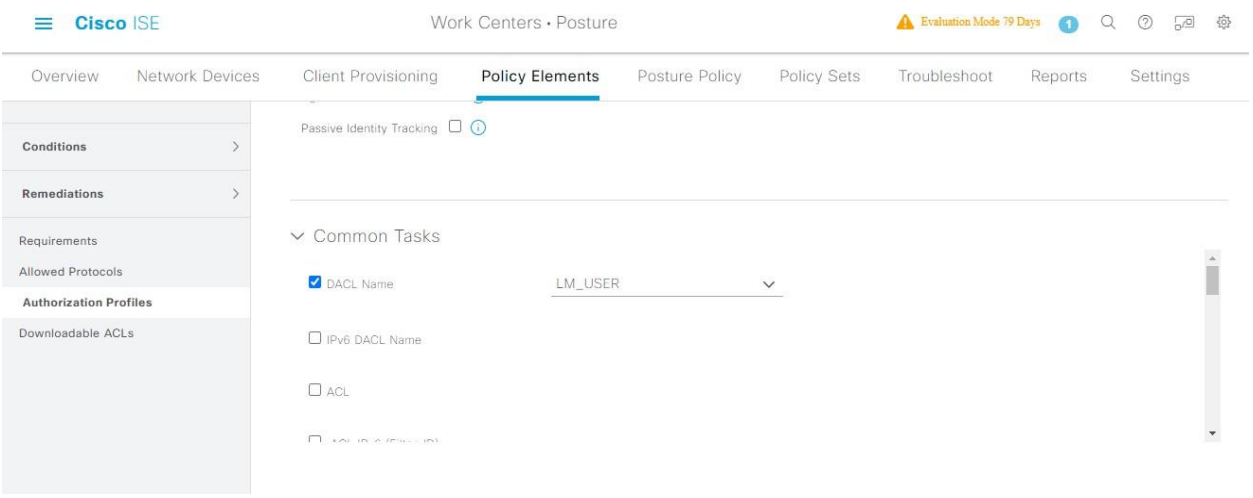


✓ Authorization Profiles: WIRED_USER_COMPLIANT



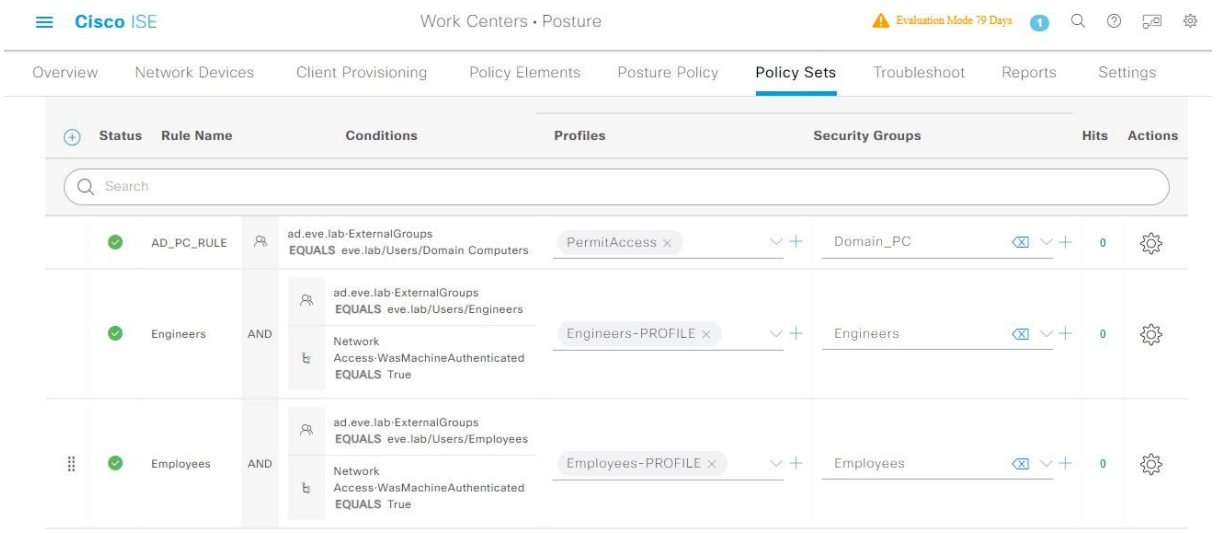
✓ Policy Elements:

✓ DACL Name: LM_USER

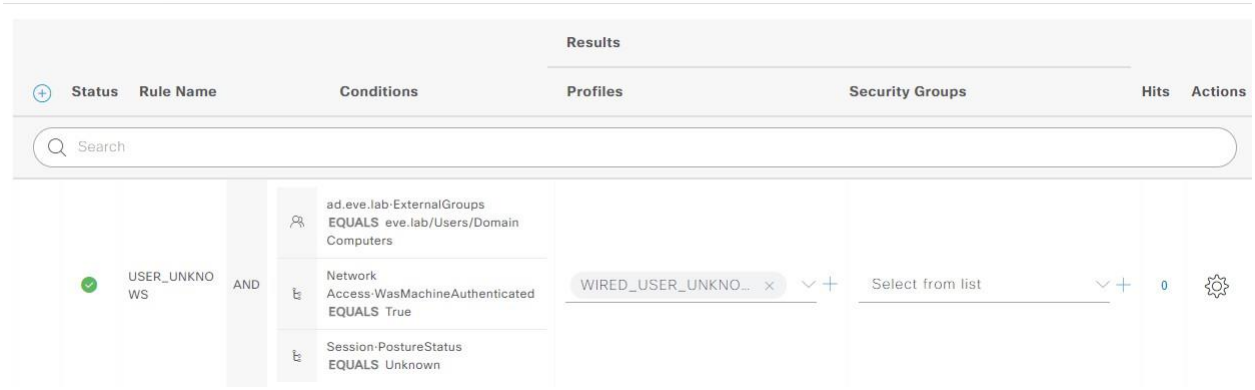


✓ Cấu hình Policy set:

✓ Dưới các mục authorization đã tạo, bấm vào biểu tượng bánh răng, insert policy below



✓ Name: USER UNKNOWN



Mục Condition chọn:

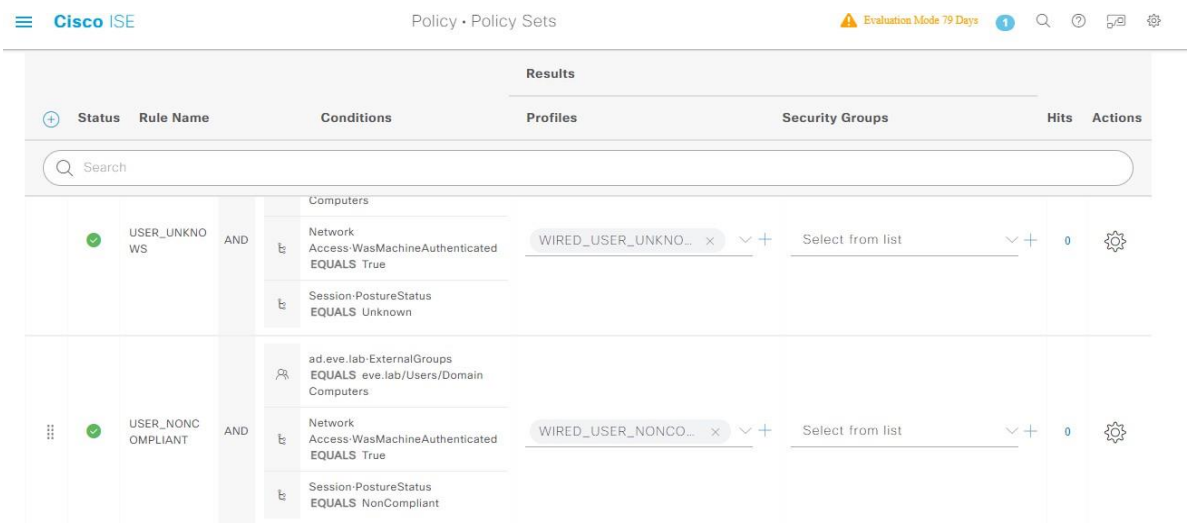
✓ ad.eve.lab-ExternalGroup EQUALS eve.lab/Users/Domain Computers

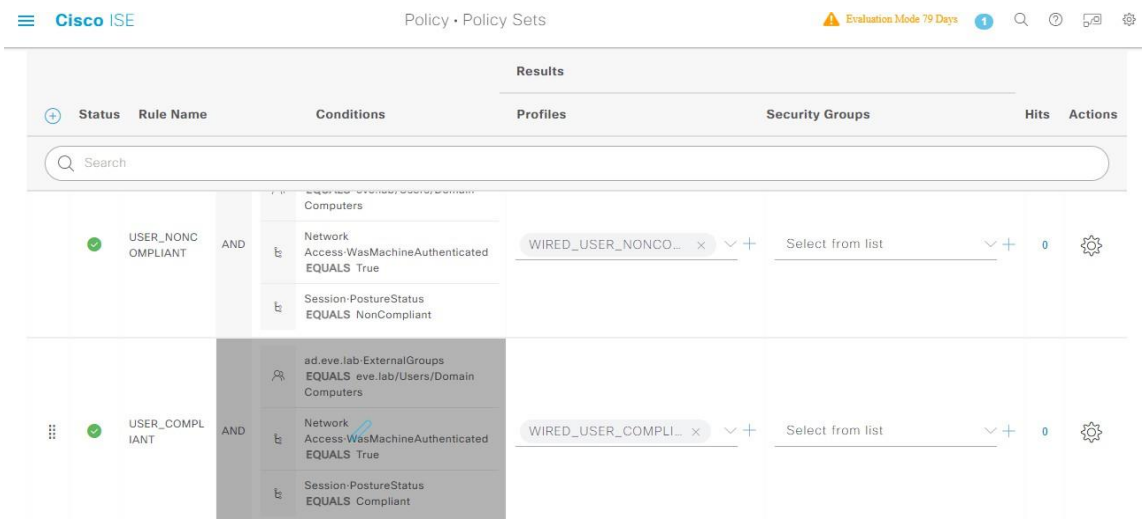
✓ Network Access-WasMachineAuthenticated EQUALS True

✓ Session-PostureStatus EQUALS Unknown

Mục Profiles:

✓ WIRED_USER_UNKNOWN

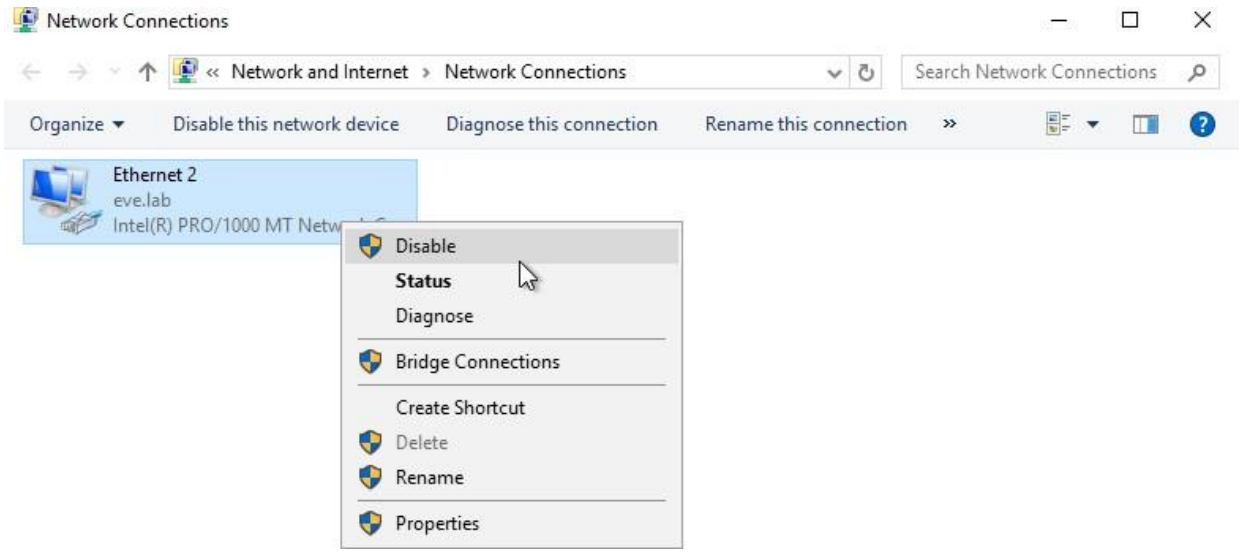


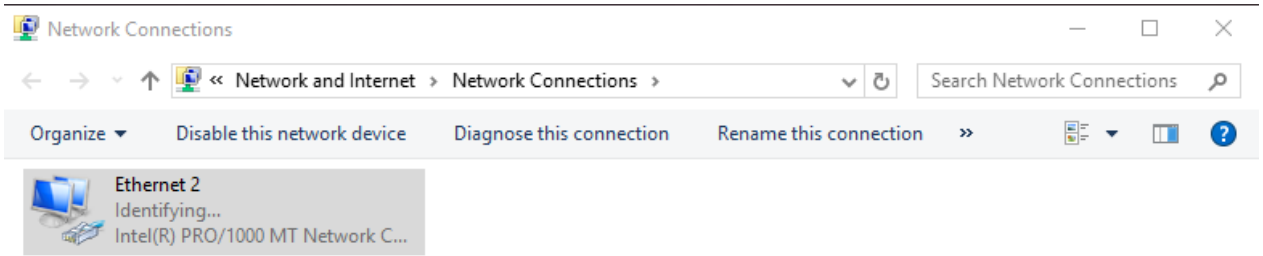


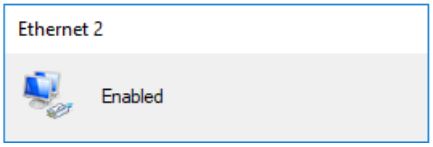
✓ Save.

3.6 Tiến hành test :

✓ Ta vào PC , disable và enable lại card mạng





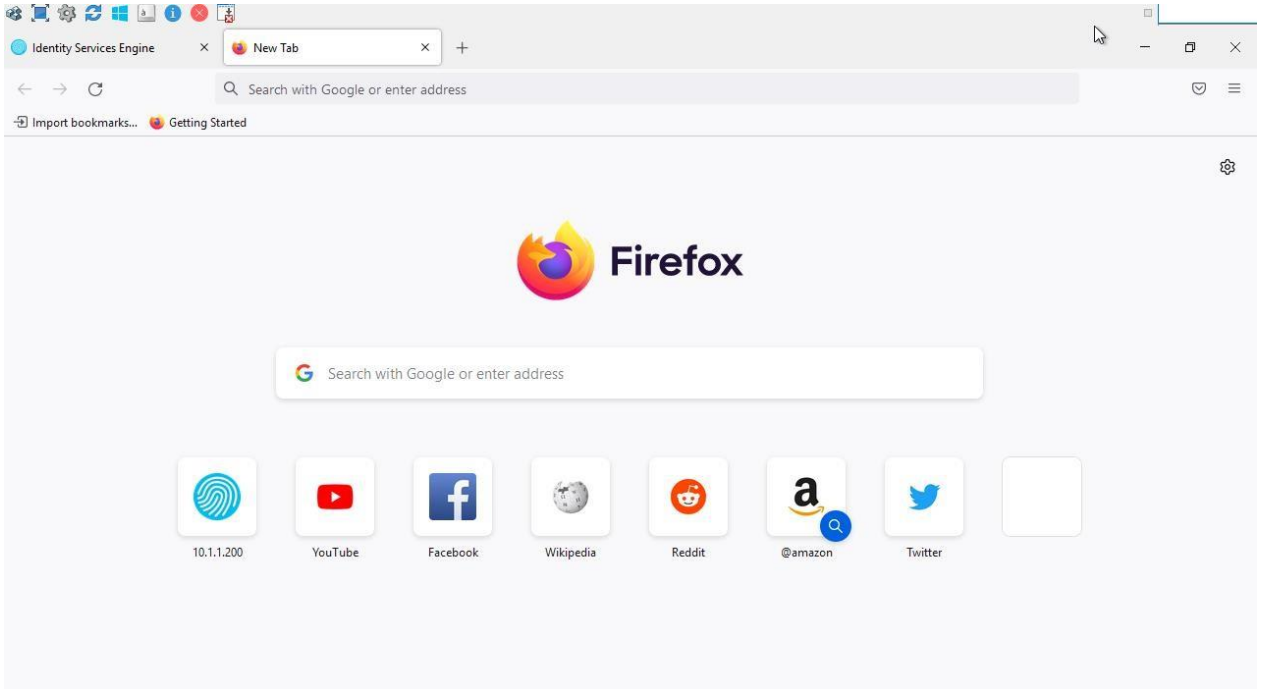


Kiểm tra lại trên SW3K:

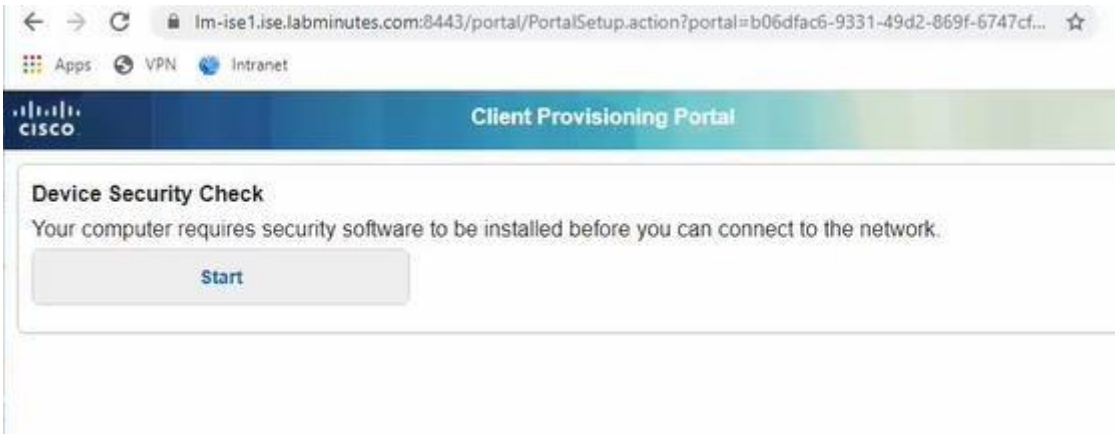
- ✓ show authentication sessions interface G0/1 details
- ✓ SW1#show authentication sessions interface G0/1 details

Xem mục Server Policy đã có DACL và Link URL Redirection web từ ISE

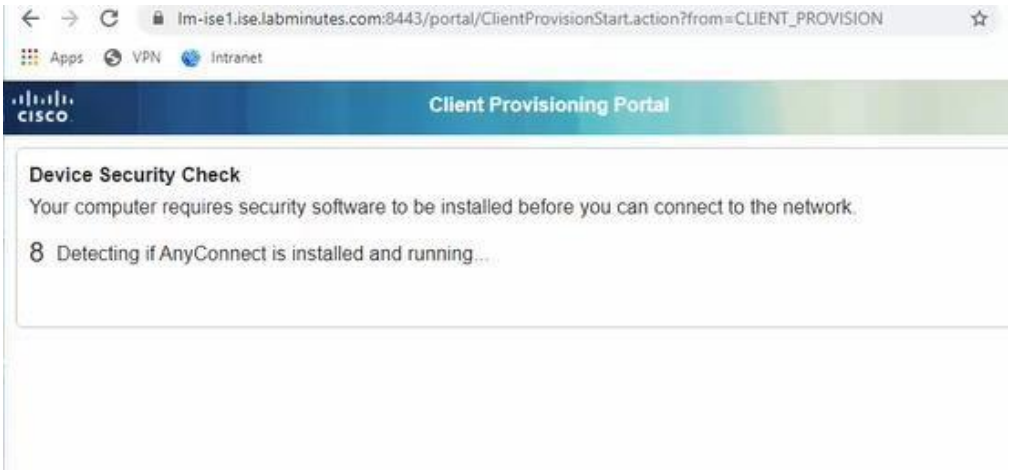
- ✓ Server Policies:
- ✓ Vlan Group:
  - ACS ACL: xACSACLx-IP-EVE_DHCP_ACL-5fe79837
  - URL WEB: ……
- ✓ SGT Value: 5
- ✓ Nếu đã có đủ điều trên, Trên PC, ta truy cập web bất kỳ để redirect sang portal :8443 của ISE



✓ Chọn Start để bắt đầu truy cập mạng

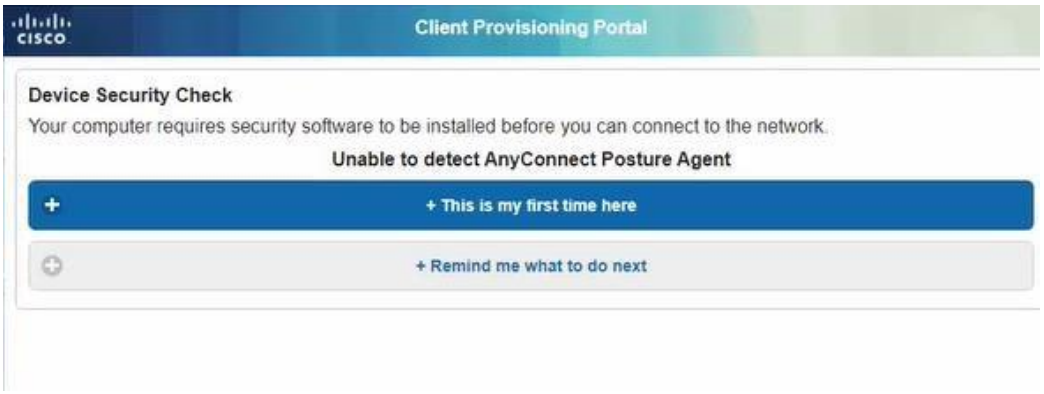


✓ Device Security Check: đợi vài giây để bắt đầu cài đặt và chạy



✓ Để Unable to detect AnyConnect Posture Agent

✓ Click vào " This is my first time here "



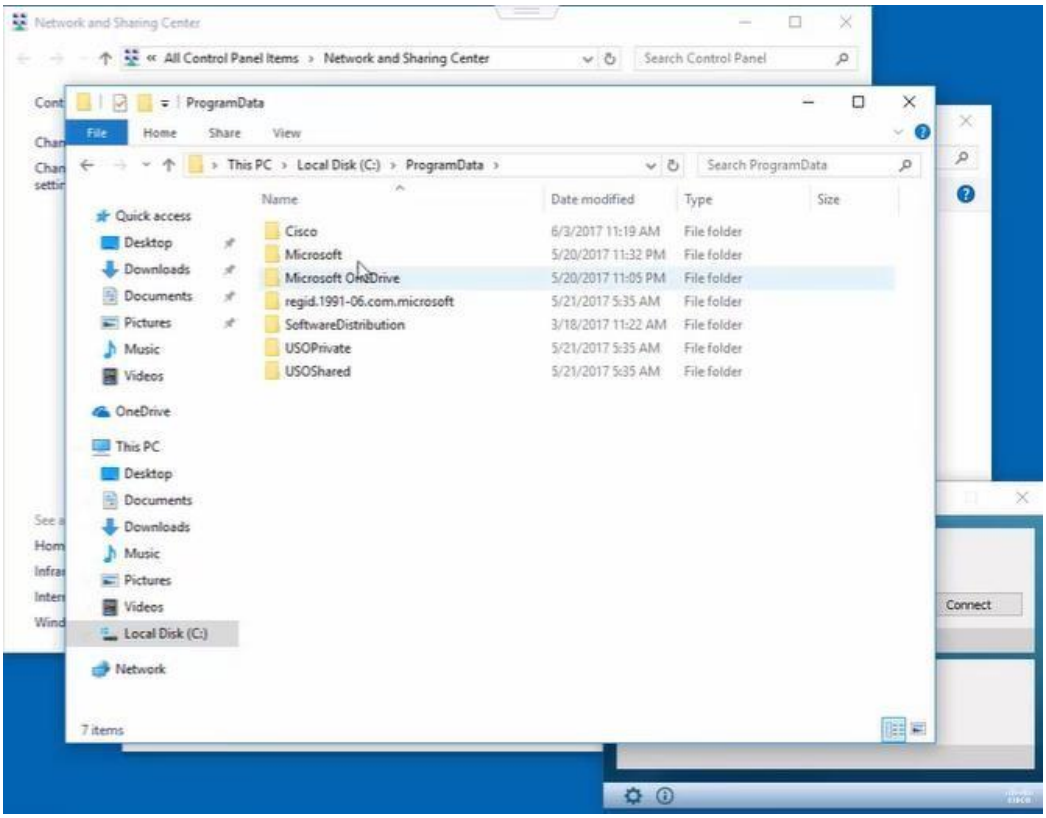
✓ Ta tiến hành Download AnyConnect về

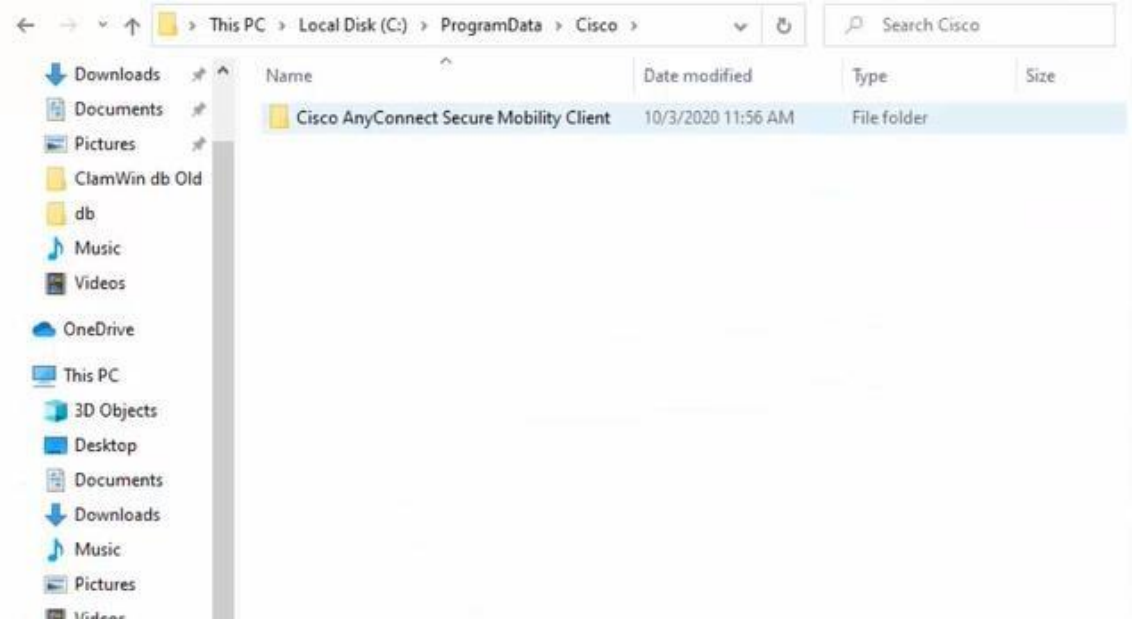
✓ Sau khi Download AnyConnect và Tiến hành truy cập mạng : Click vào Connect

✓ Quá trình Download và cài đặt đang diễn ra

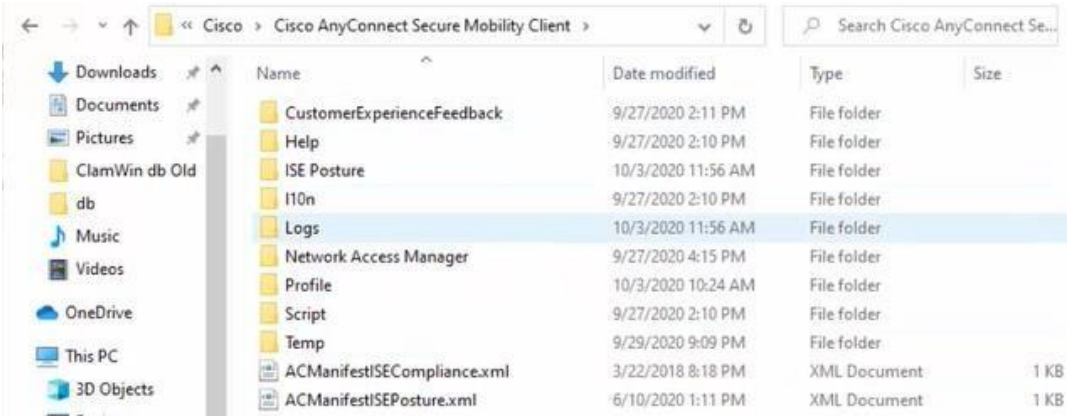
✓ Cài đặt thành công

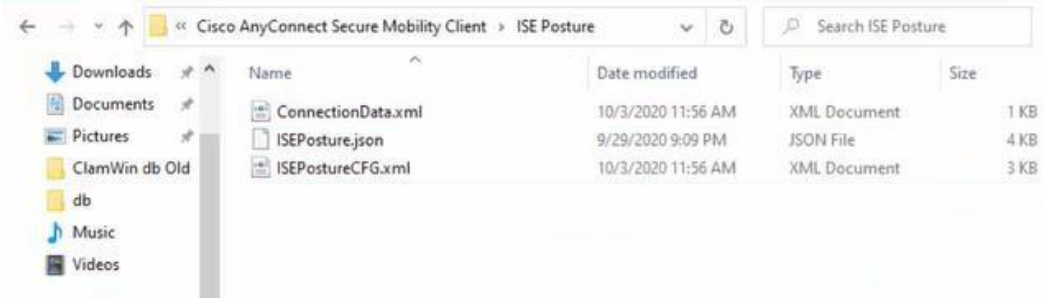
✓ Truy cập ổ C / ProgramData / Cisco / Cisco AnyConnect Secure Mobility Client





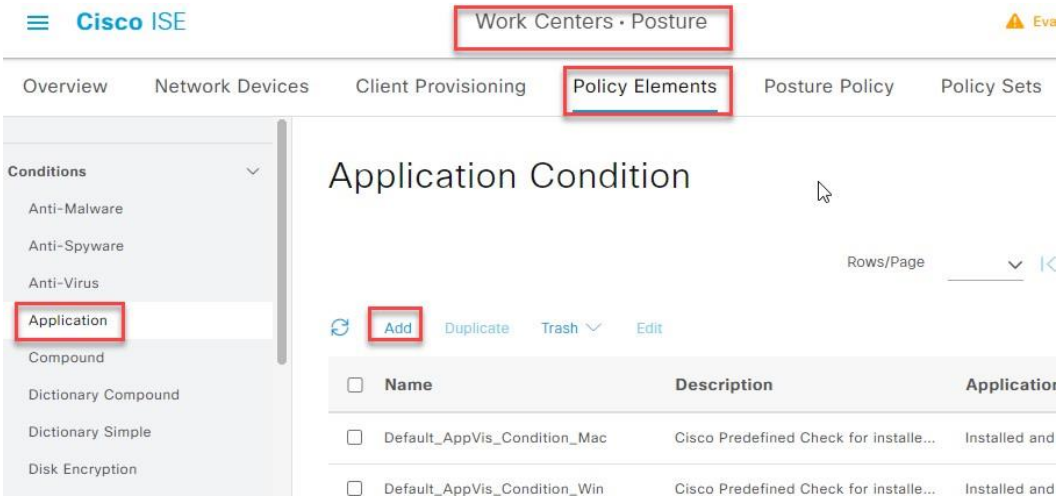
✓ Chọn tiếp Profile / ISE Posture / ISEPostureCFG.xml





✓ Cấu hình Posture Condition

✓ Work Center/ Posture / Policy Element / Application / +Add



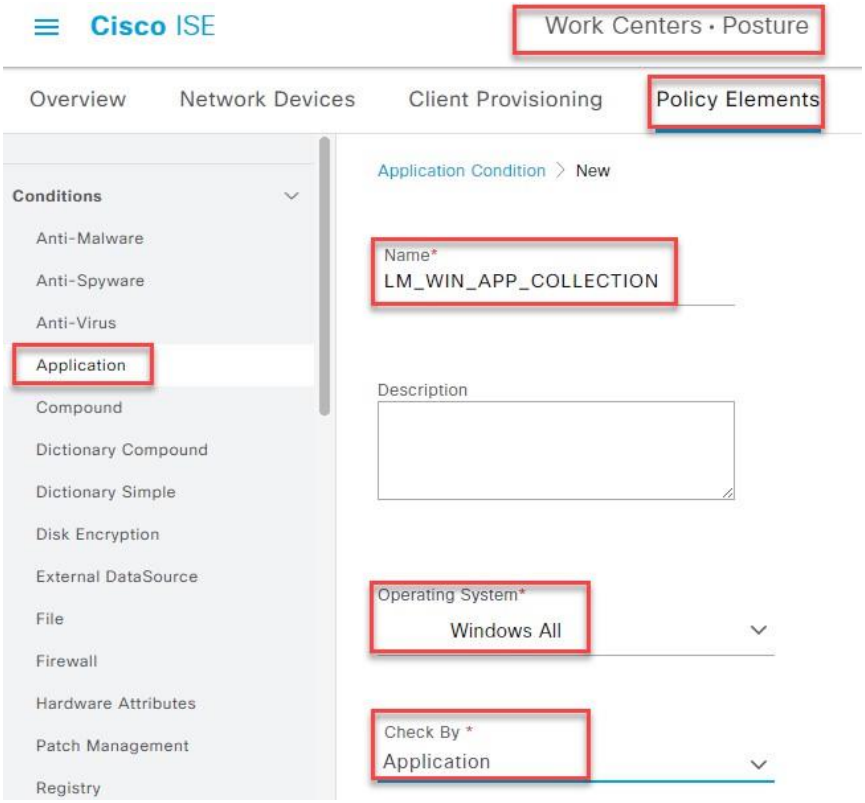
✓ Name: LM_WIN_APP_COLLECTION

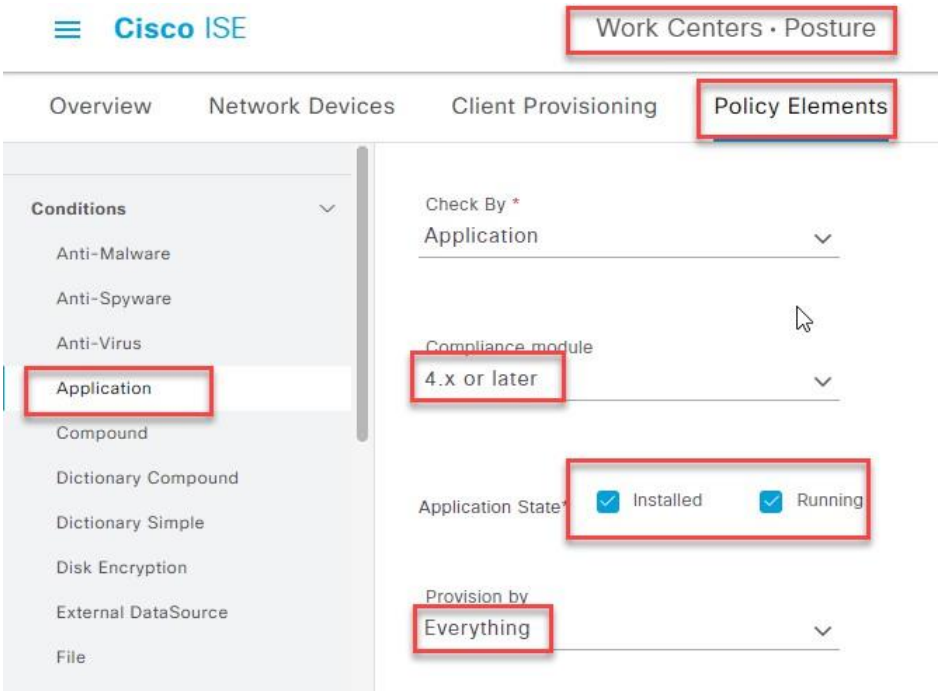
✓ Operating System: Windows All

✓ Check By: Application

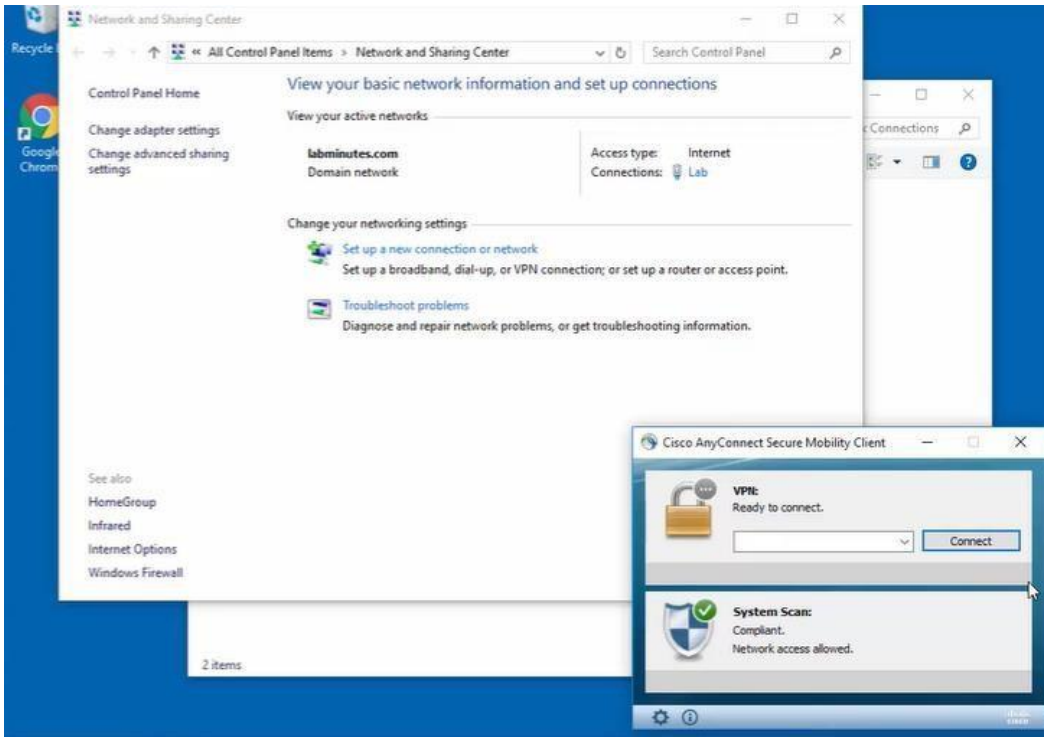
✓ Compliant Module: 4.x or later

✓ Provision by: Everything



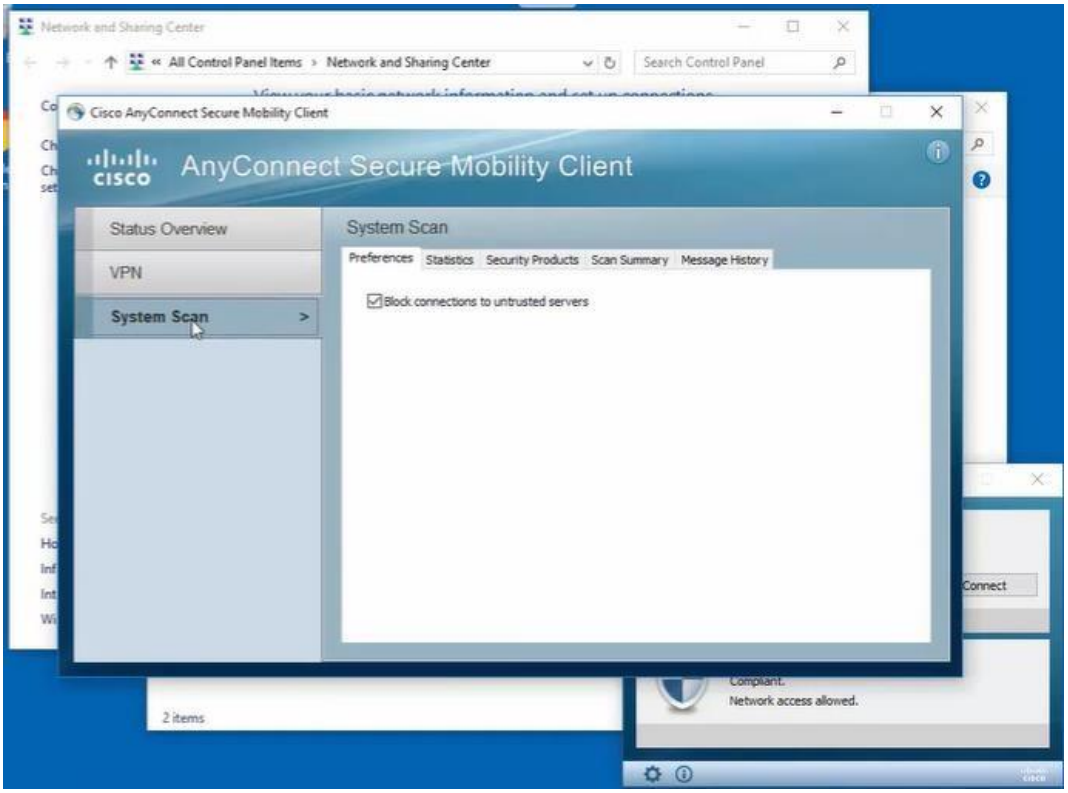


✓ System Scan: phần mềm anyconnect : Compliance

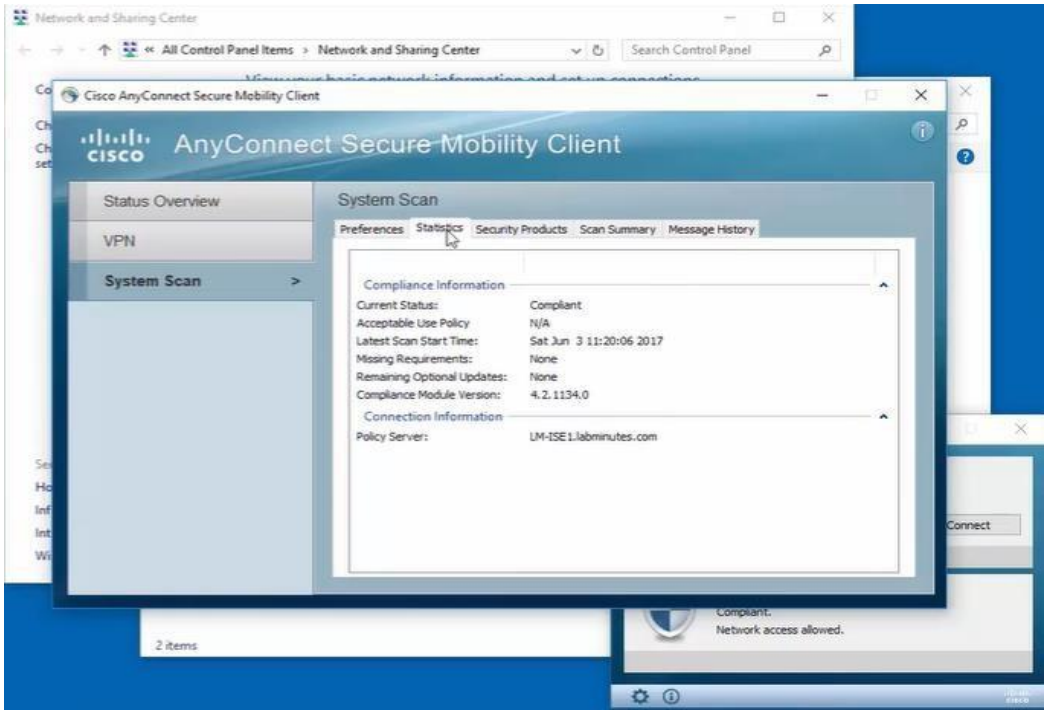


✓ Bật Setting Scan:

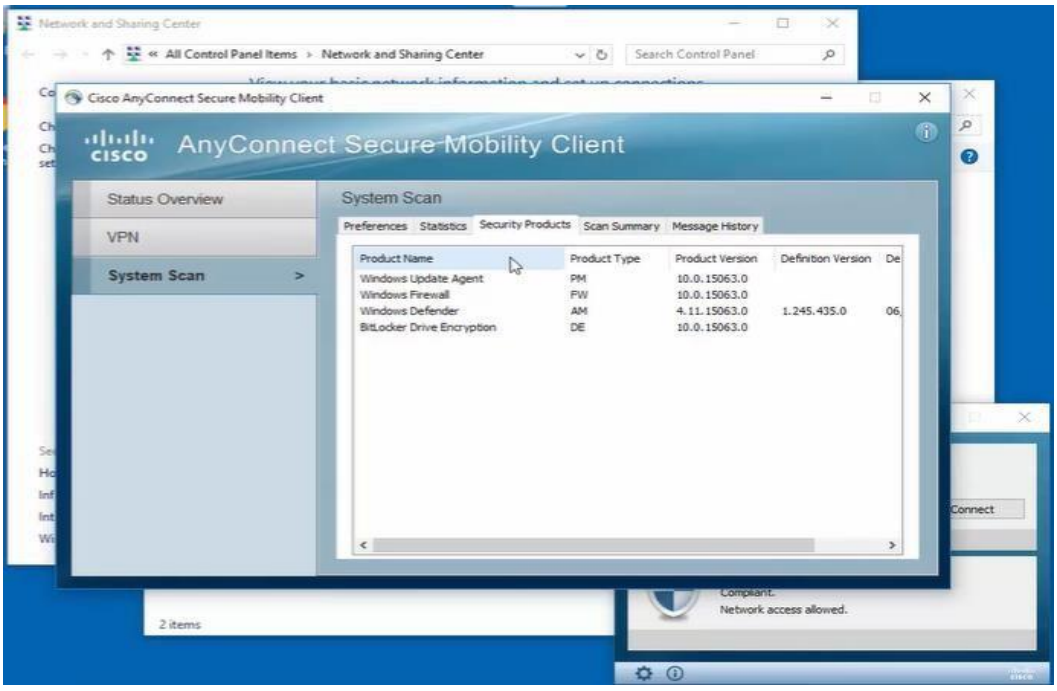
✓ System Scan: Click vào Connection to untrusted servers



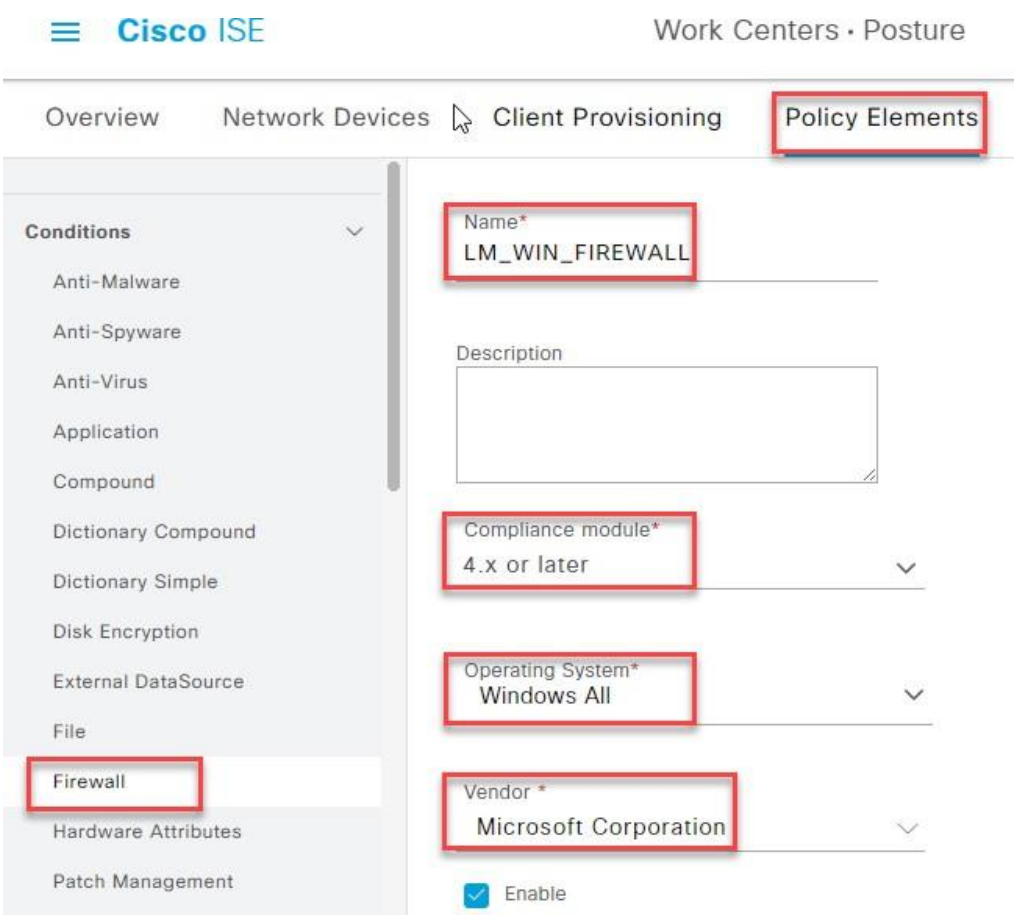
✓ System Scan: mở tab Statistics để xem thông tin Compliance

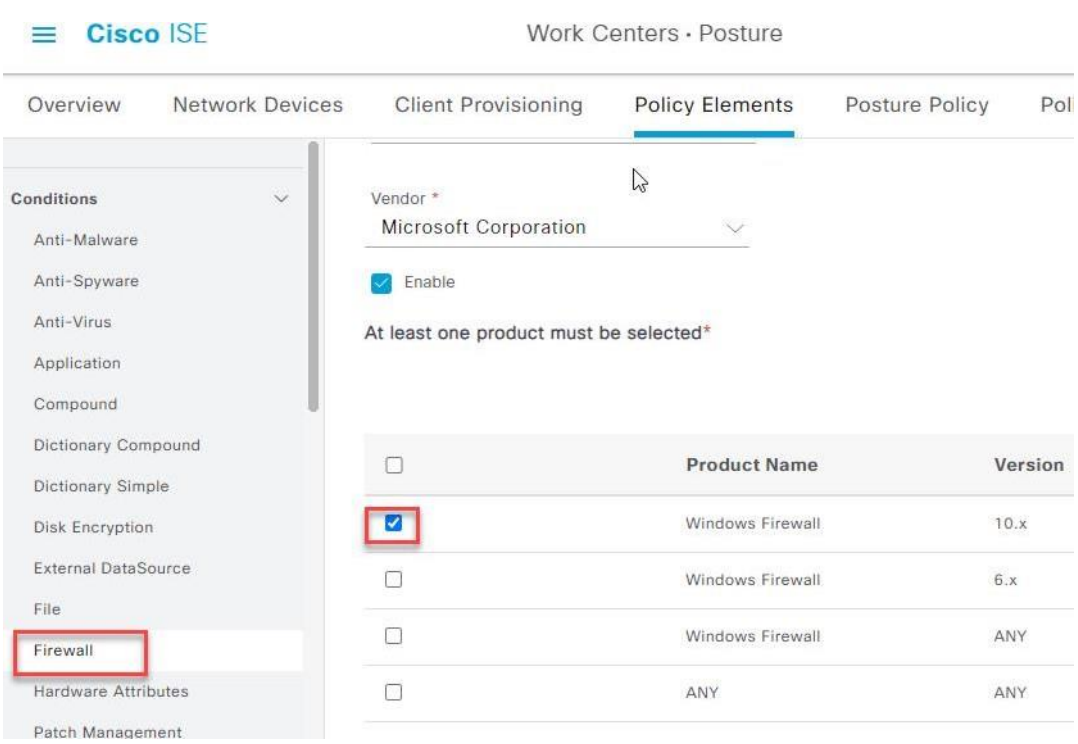


✓ System Scan: chọn tab Security Product , Product Name

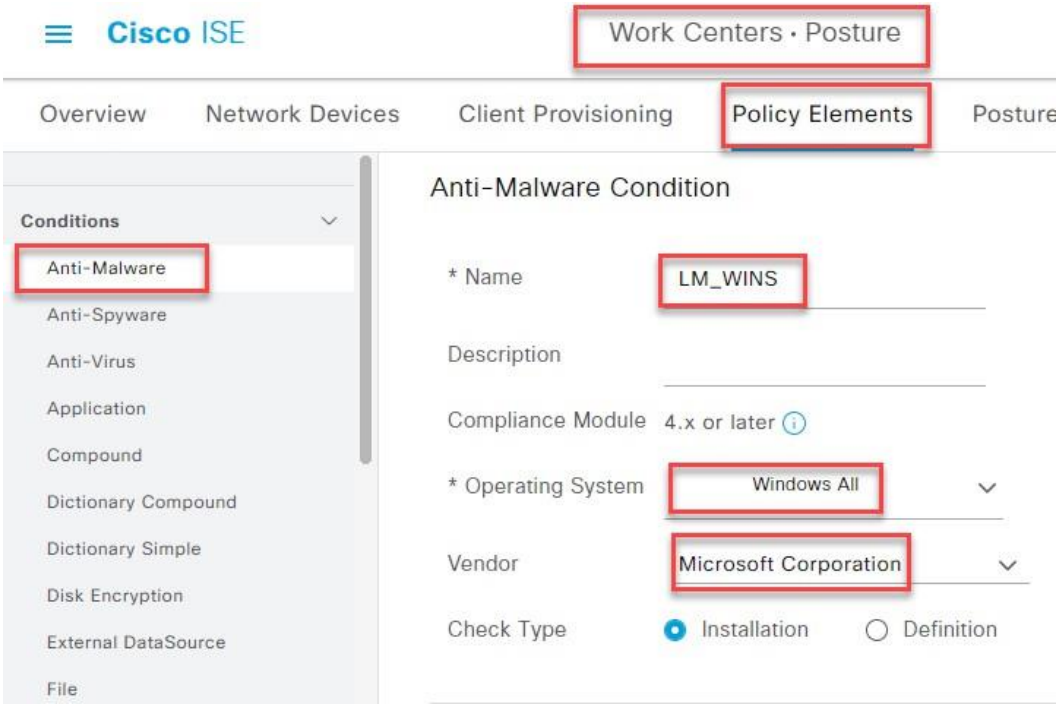


- ✓ Sau khi qua khỏi mode Unknown, ta tiếp tục cấu hình thêm phần Condition Posture
- ✓ Work Centers / Posture / Policy Elements / Firewall Condition
- ✓ Name: LM_WIN_FIREWALL
- ✓ Compliance module: 4.x or later
- ✓ Operating System: Windows All
- ✓ Vendor: Microsoft Corporation
- ✓ Tick vào mục Windows firewall và version 10.x



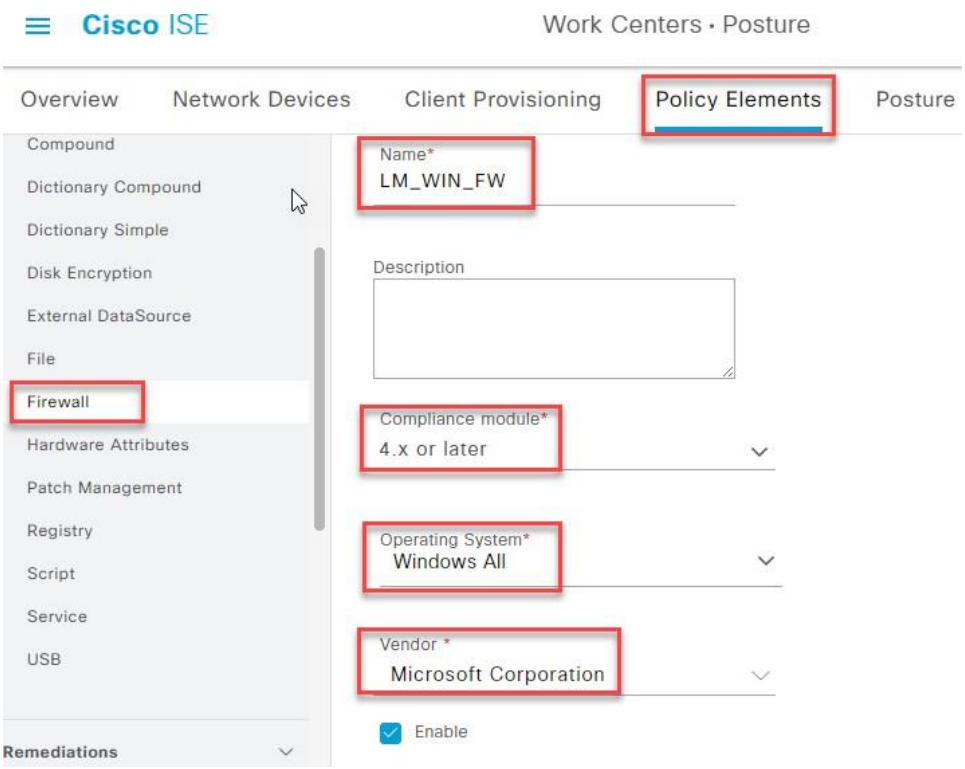


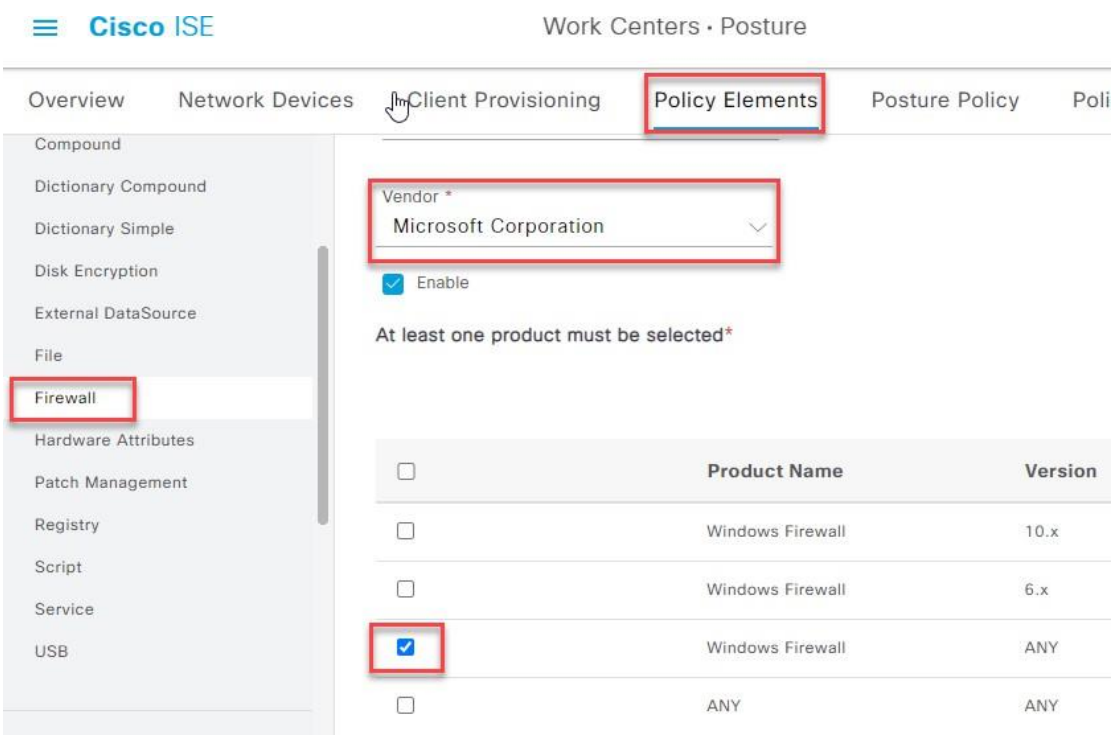
- ✓ Posture / Policy Elements / Anti-Malware
- ✓ Name: LM_WINS
- ✓ Operating System: Windows All
- ✓ Vendor: Microsoft Corporation
- ✓ Tab Product for Selected Vendor:
- ✓ Baseline Condition: Windows Defender 4.x



3.6 Cấu hình Posture Remediation:

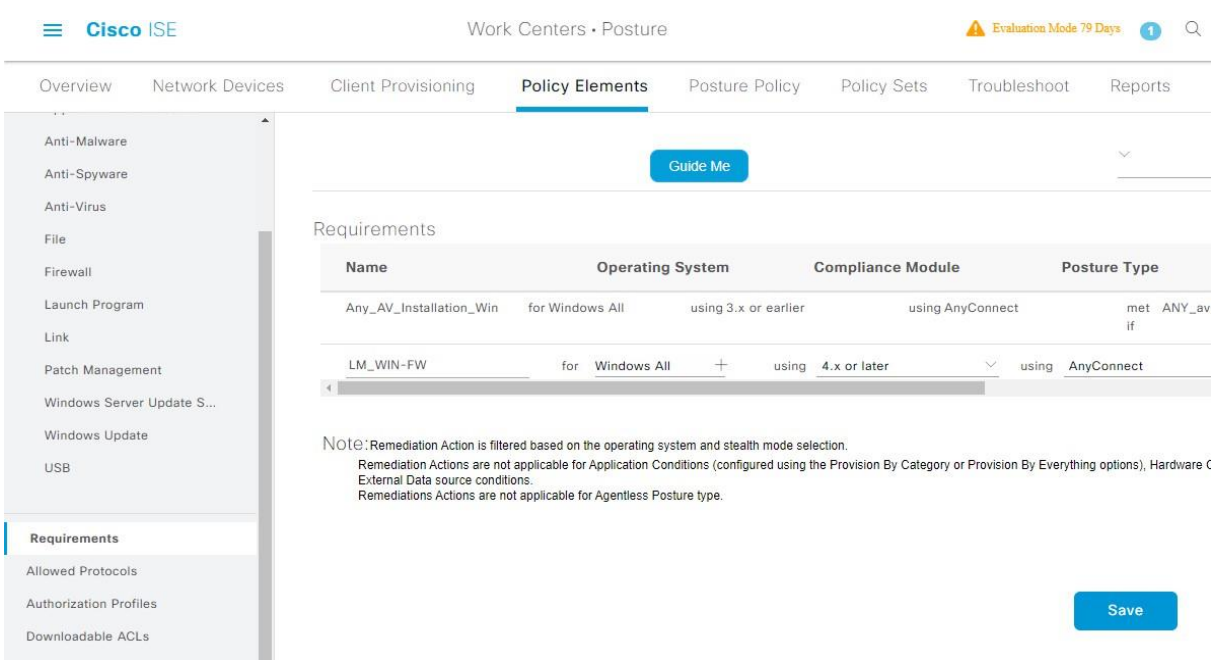
- ✓ Work Center / Posture / Firewall
- ✓ Name: LM_WIN_FW
- ✓ Operating System: Windows All
- ✓ Compliance module: 4.x or later
- ✓ Remediation Type: Manual
- ✓ Vendor name: Microsoft operation
- ✓ Window firewall + Any



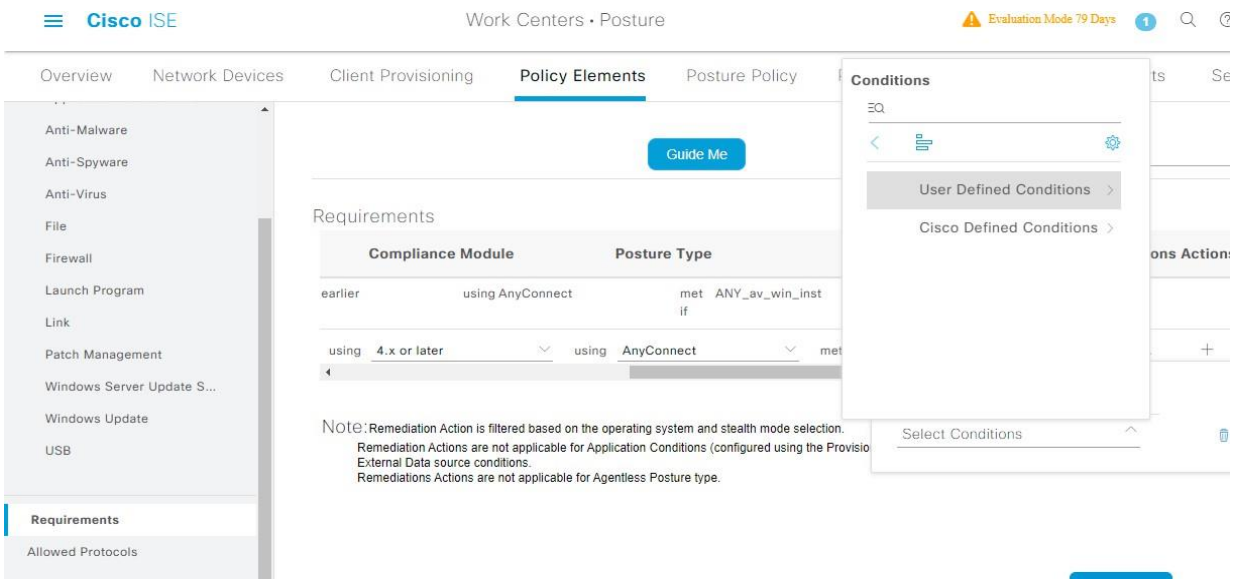


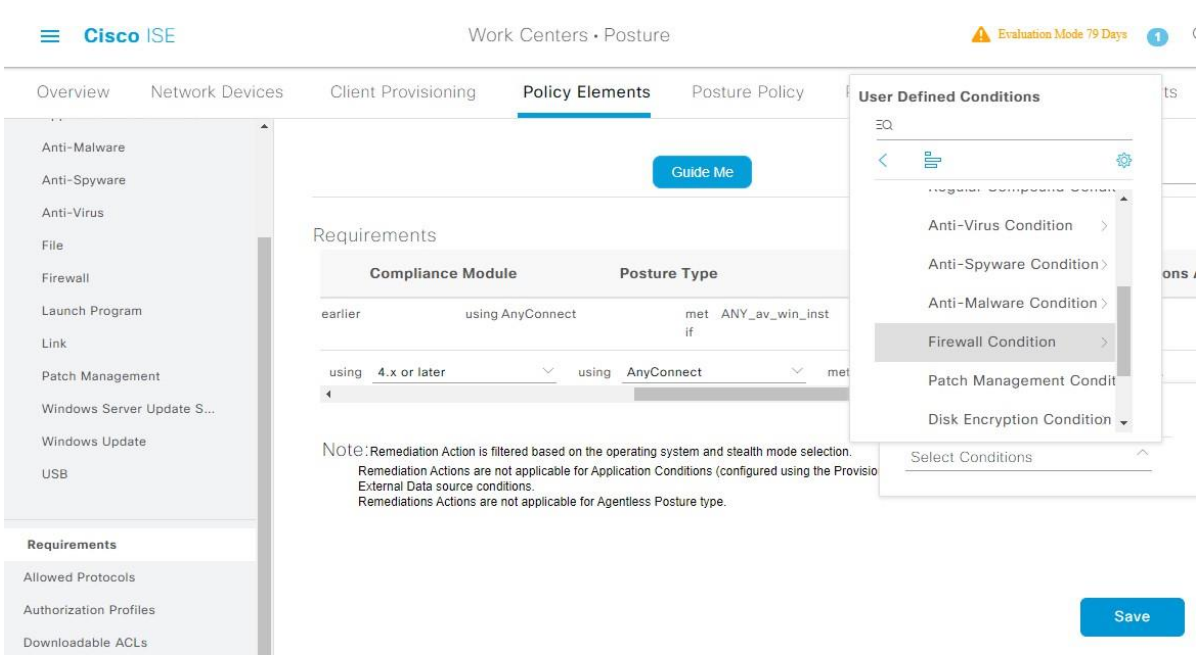
3.6Cấu hình Posture Requirement:

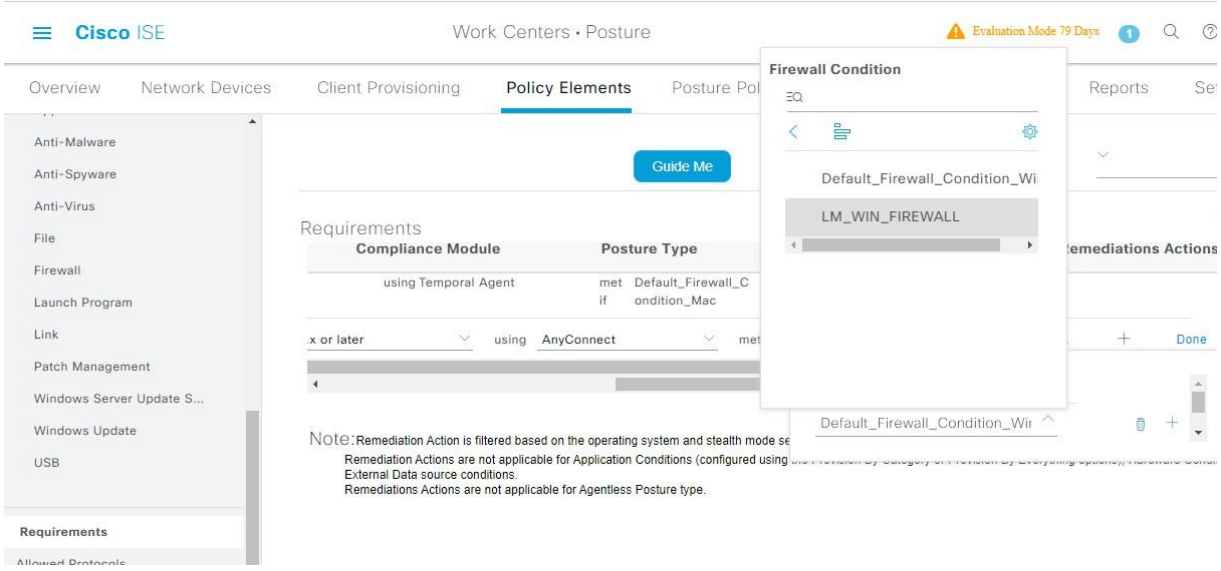
- ✓ Work Centers / Posture / Policy Element / Requirement
- ✓ Edit /new
- ✓ Name: LM_WIN_FW
- ✓ Operating System: Windows All
- ✓ Compliance module: 4.x or later



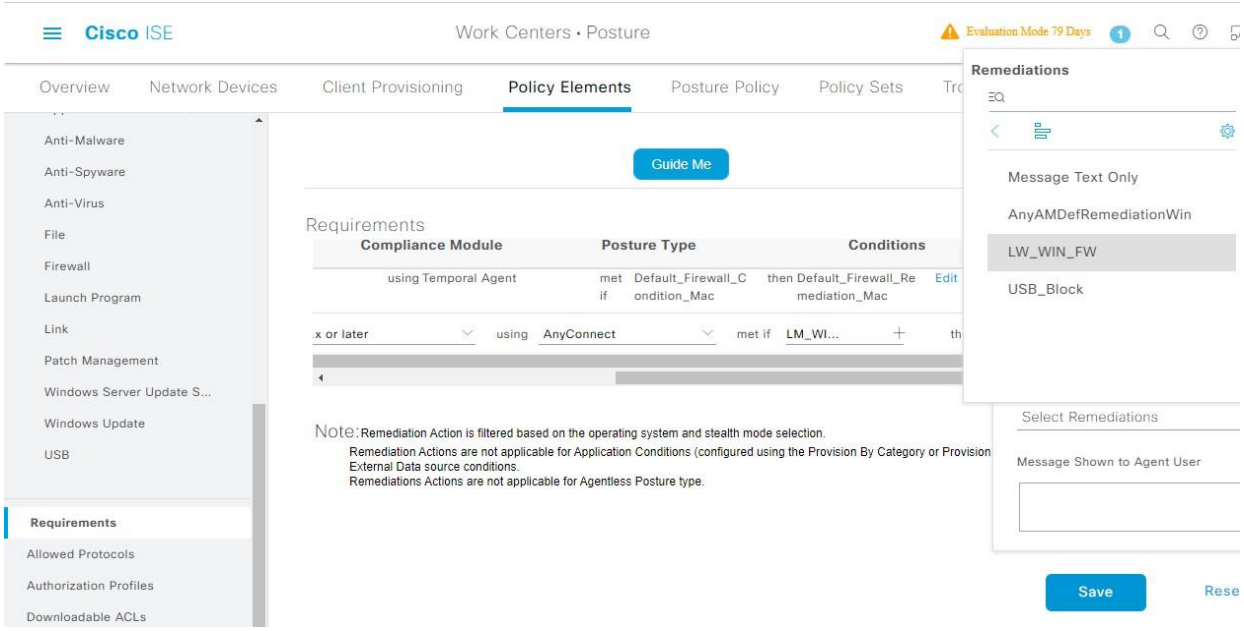
✓ Mục Conditions: Chọn User Defined Conditions / Firewall Condition / LM_WIN_FIREWALL



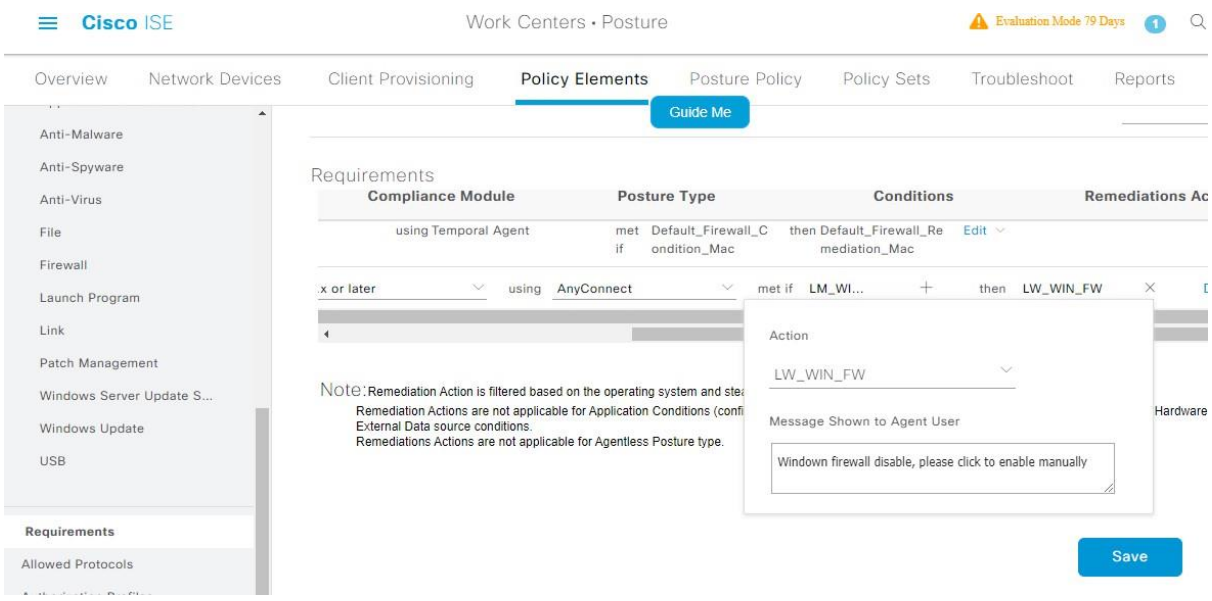

Cisco ISE
Work Centers · Posture
Evaluation Mode 79 Days
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Anti-Malware
Anti-Spyware
Anti-Virus
File
Firewall
Launch Program
Link
Patch Management
Windows Server Update S...
Windows Update
USB
Requirements
Allowed Protocols
Authorization Profiles
Downloadable ACLs
Guide Me
Requirements
Compliance Module
Posture Type
earlier
using AnyConnect
met if
ANY_av_win_inst
using
4.x or later
using
AnyConnect
Note: Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provisio
External Data source conditions.
Remediations Actions are not applicable for Agentless Posture type.
User Defined Conditions
Anti-Virus Condition
Anti-Spyware Condition
Anti-Malware Condition
Firewall Condition
Patch Management Condit
Disk Encryption Condition
Select Conditions
Save


Cisco ISE
Work Centers · Posture
Evaluation Mode 79 Days
Overview
Network Devices
Client Provisioning
Policy Elements
Reports
Anti-Malware
Anti-Spyware
Anti-Virus
File
Firewall
Launch Program
Link
Patch Management
Windows Server Update S...
Windows Update
USB
Requirements
Guide Me
Requirements
Compliance Module
Posture Type
using Temporal Agent
met if
Default_Firewall_Condition_Mac
x or later
using
AnyConnect
Done
Note: Remediation Action is filtered based on the operating system and stealth mode se
Remediation Actions are not applicable for Application Conditions (configured using
External Data source conditions.
Remediations Actions are not applicable for Agentless Posture type.
Firewall Condition
Default_Firewall_Condition_Wi
LM_WIN_FIREWALL
Default_Firewall_Condition_Wi

✓ Mục Remediation: LW_WIN_FW



✓ Mục Message Show to Agent User: “Window firewall disable, please click to enable manually”



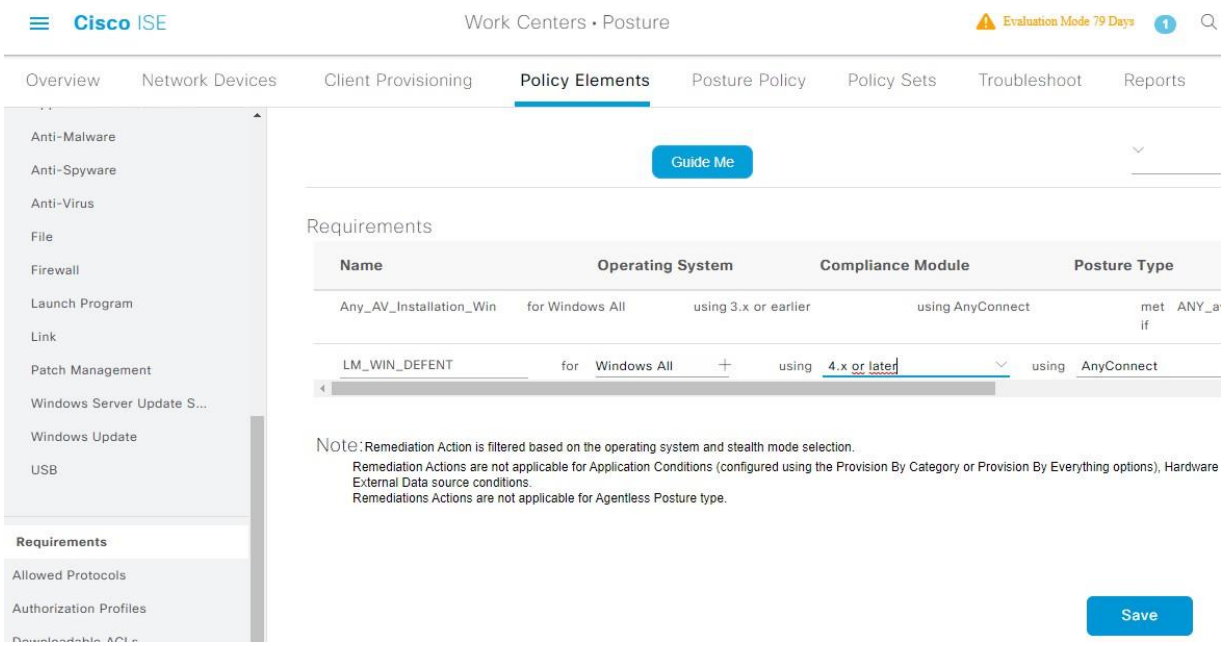
✓ Add +

✓ Name: LM_WIN_DEFENT

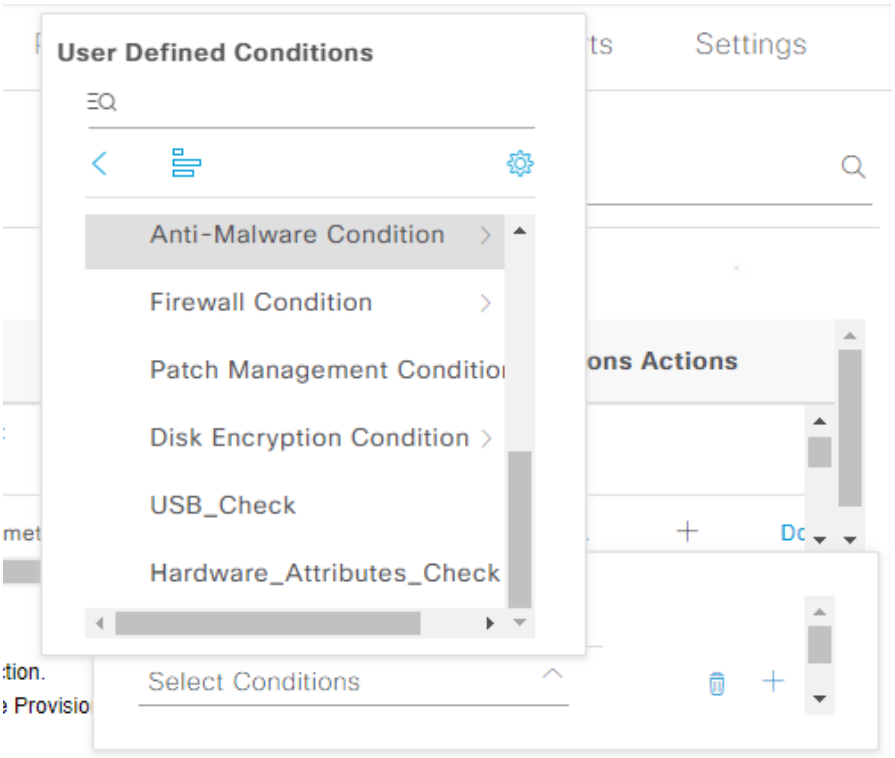
✓ Windows All: Windows All

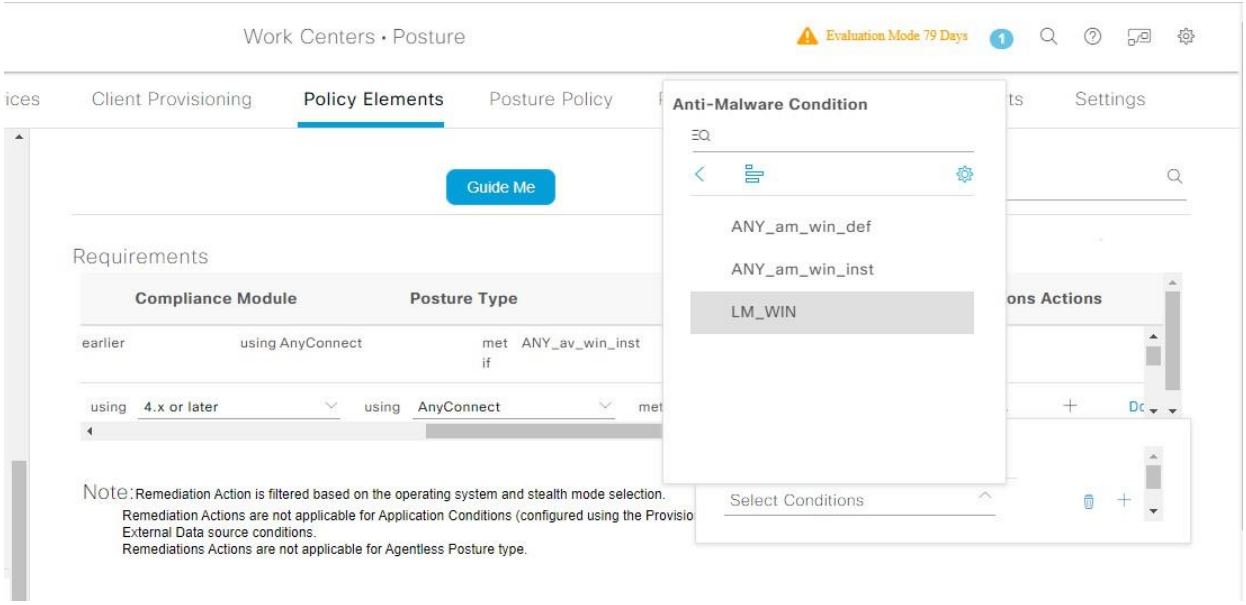
✓ Compliance Module : 4.x or later

✓ Posture Type: Anyconnect



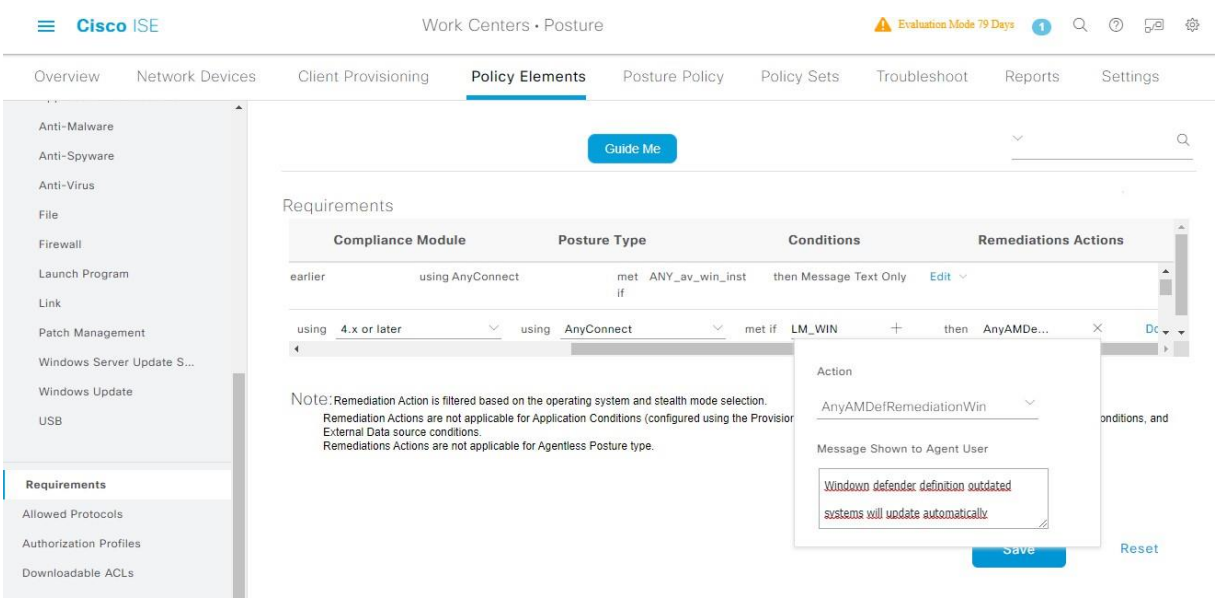
✓ User Defined Conditions / Anti-Malware Condition / LM_WIN



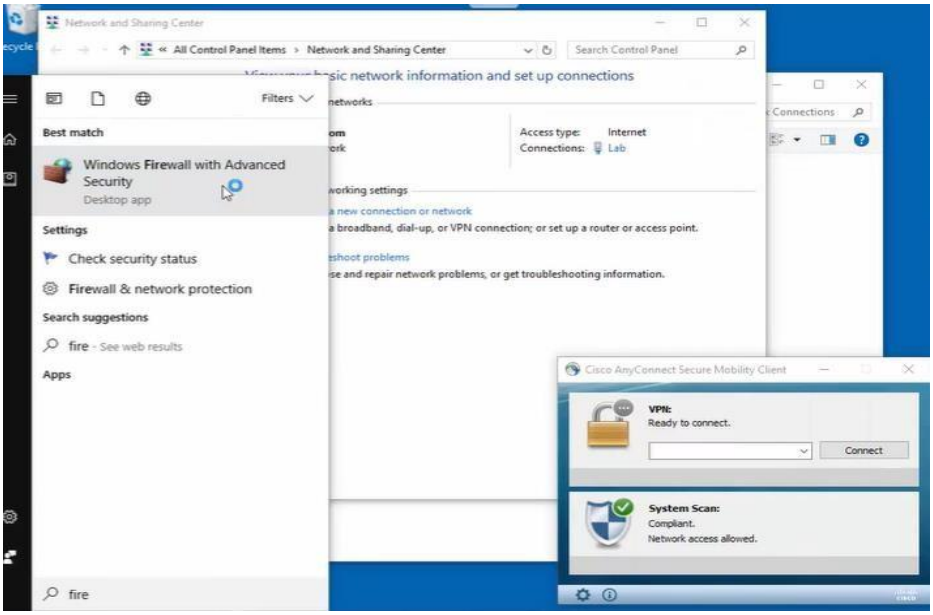


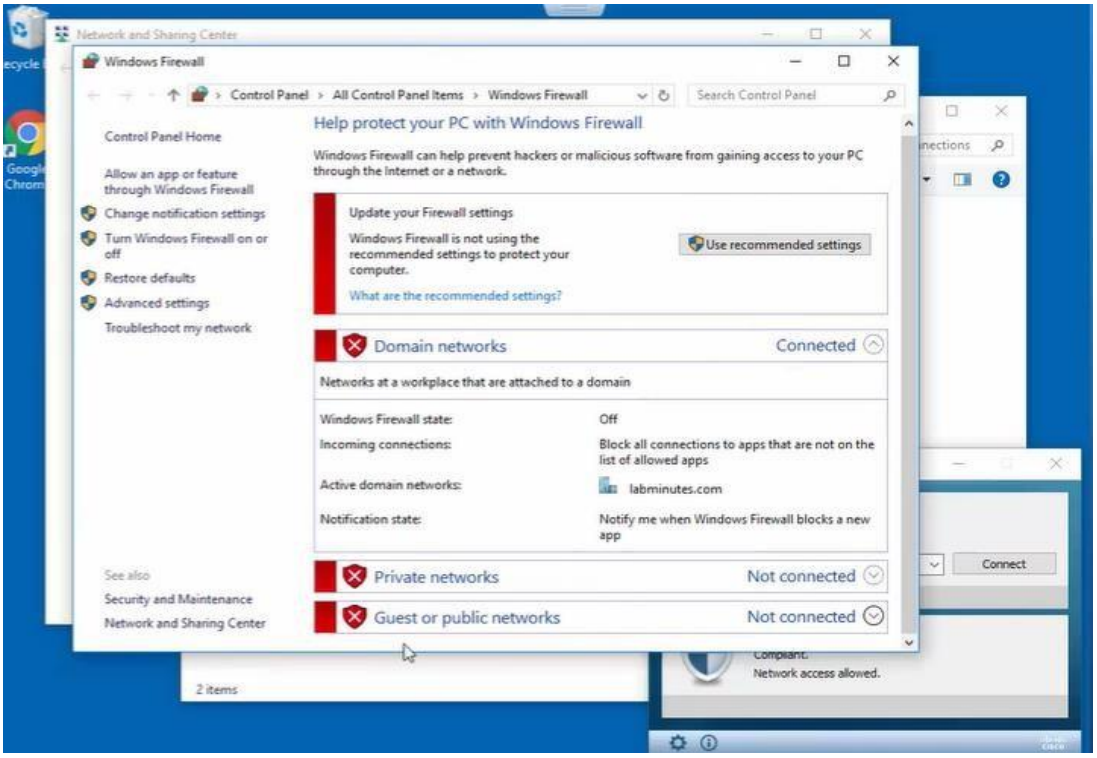
✓ Remediations Action: Chọn AnyAMDefRemediation /

✓ Message Show to Agent User: Win Windows defender definition outdated systems will update automatically

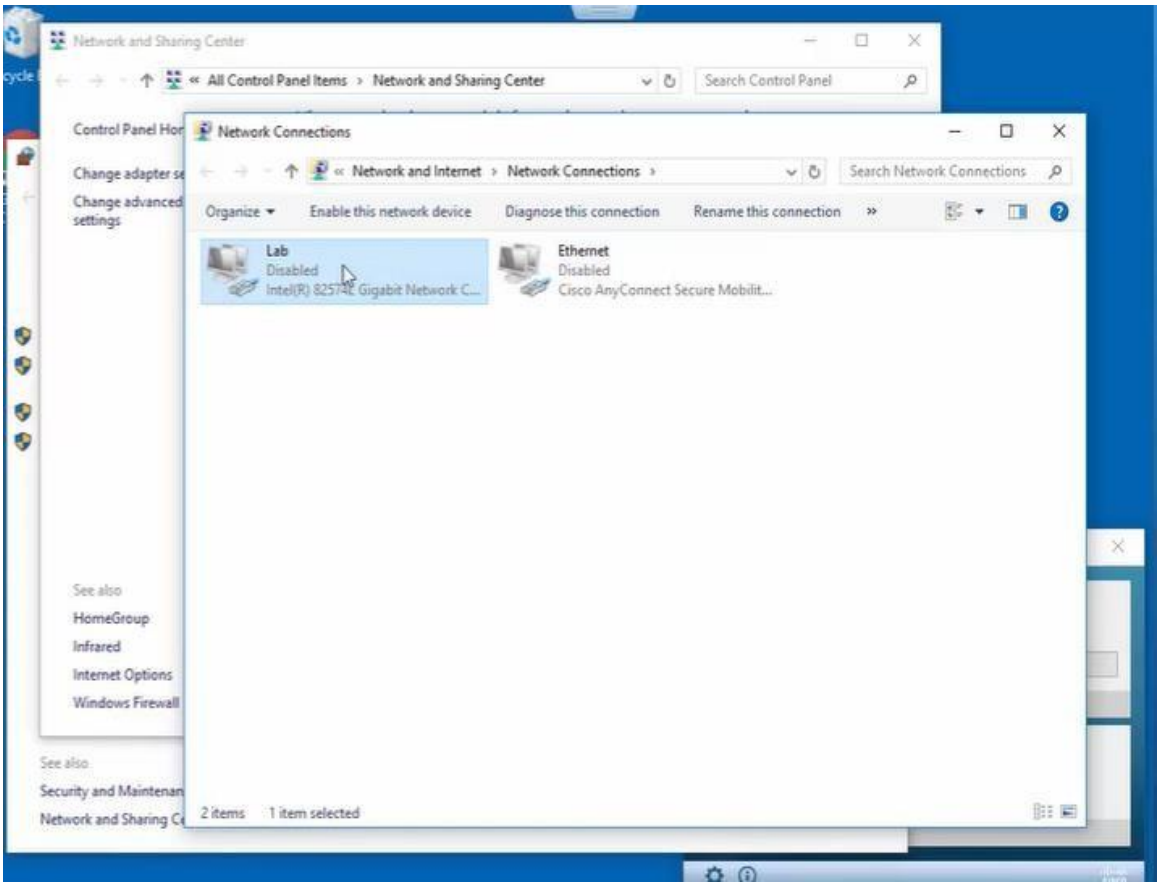


- ✓ Chuyển hướng đến Windows: mở Windows Firewall with Advanced Security
- ✓ Tắt firewall để đáp ứng điều kiện Non Compliant của Anyconnect Complaint

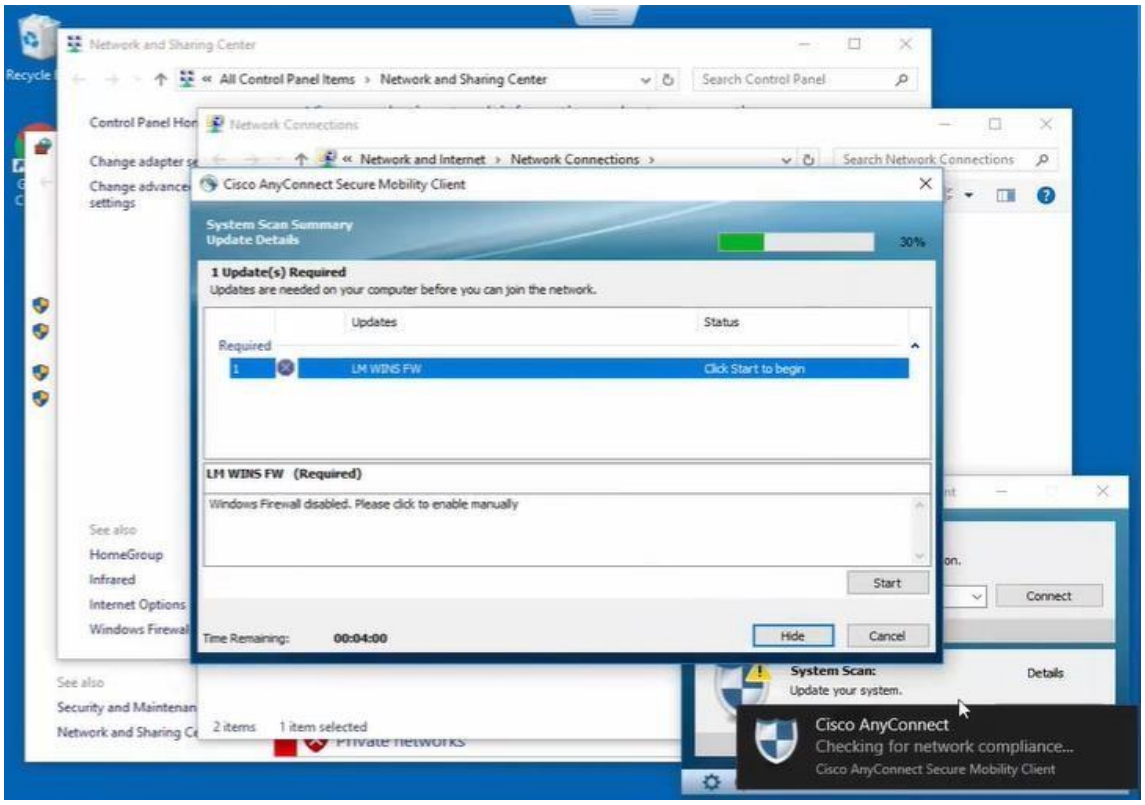




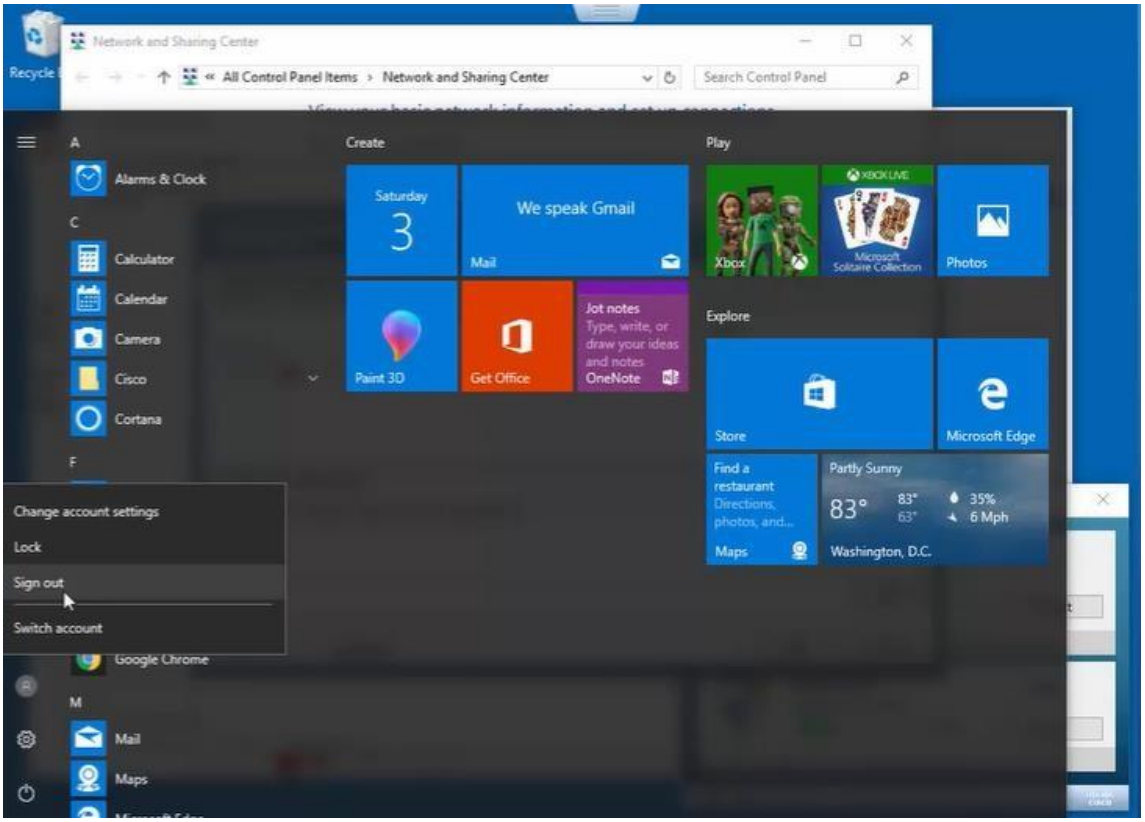
✓ Tắt mở lại card mạng:

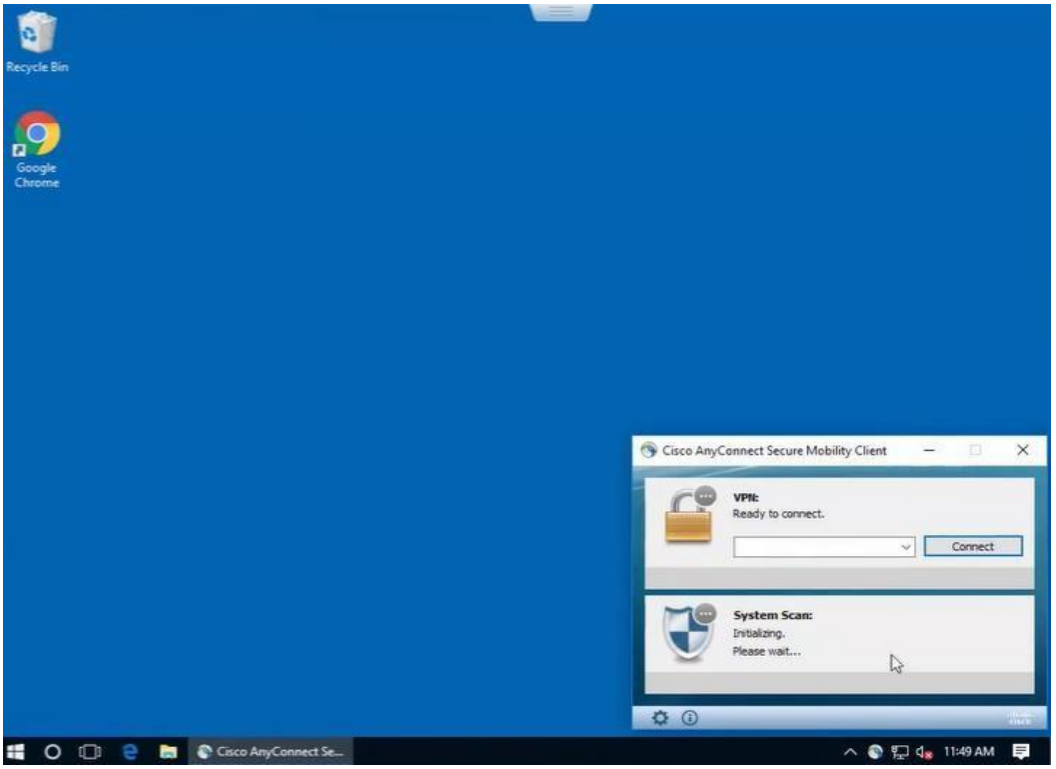


✓ Lick vào Systems scan: Cisco AnyConnect Secure Mobility Client: LM WINS FW



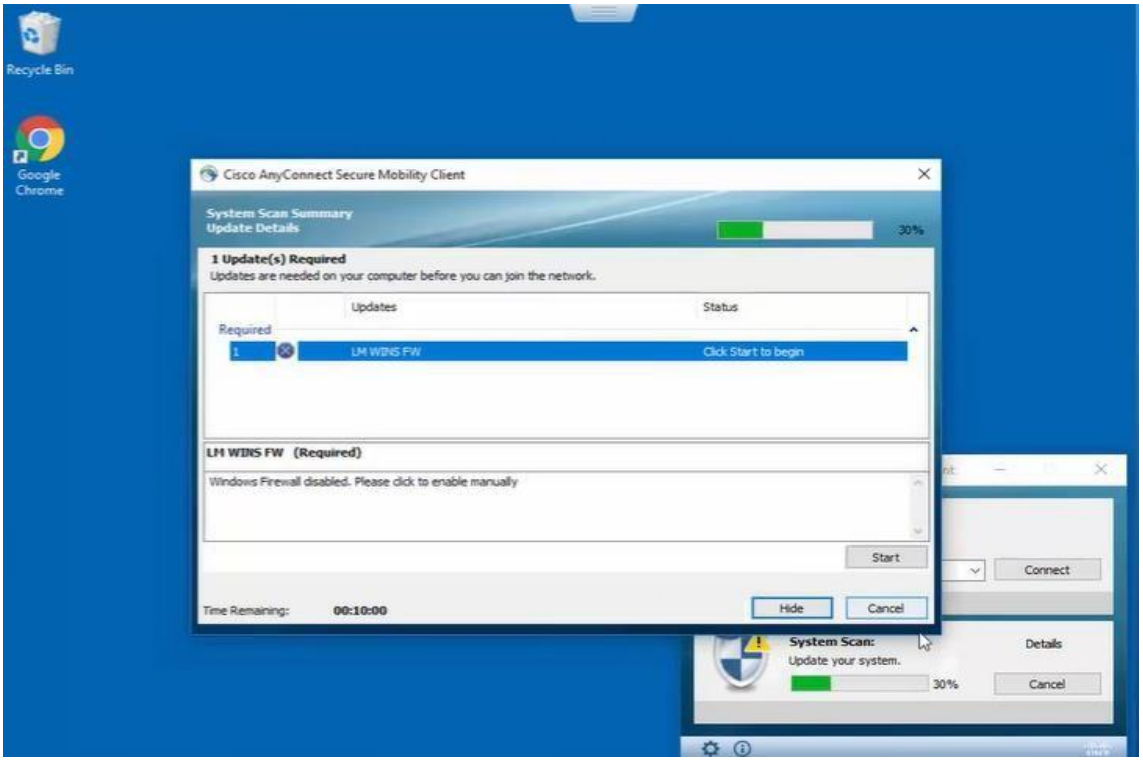
✓ Log out

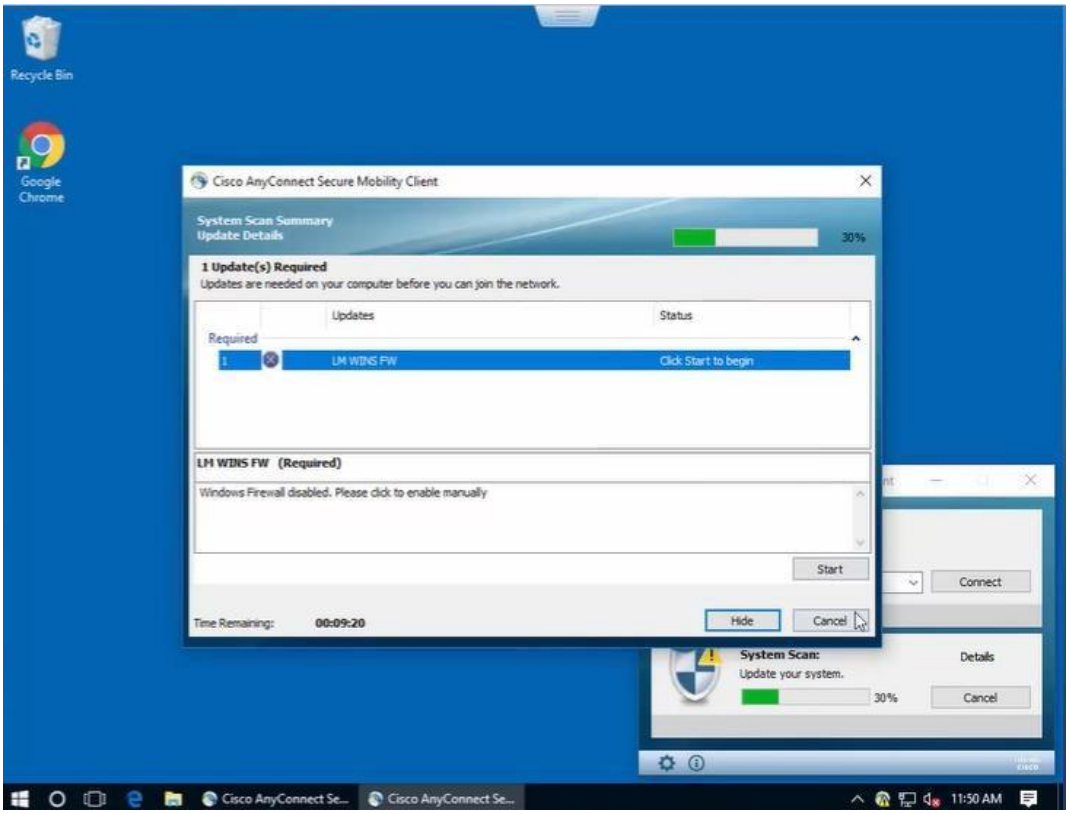


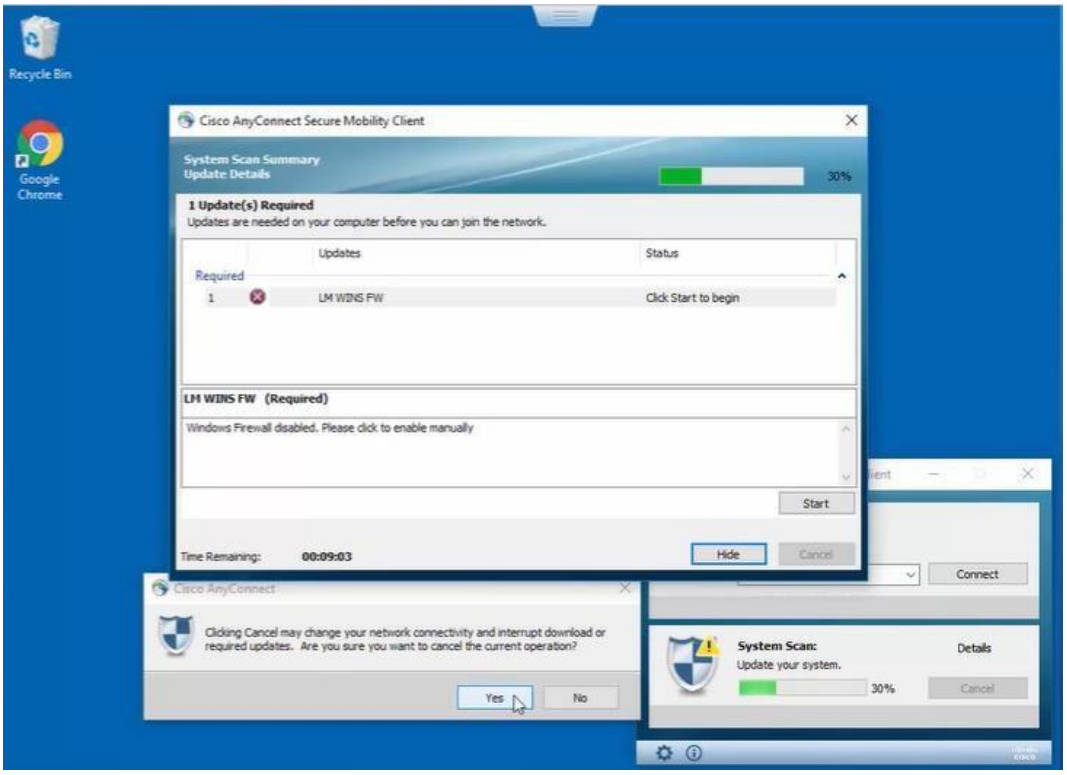


✓ Chú ý dòng LM WIN FW (Required)

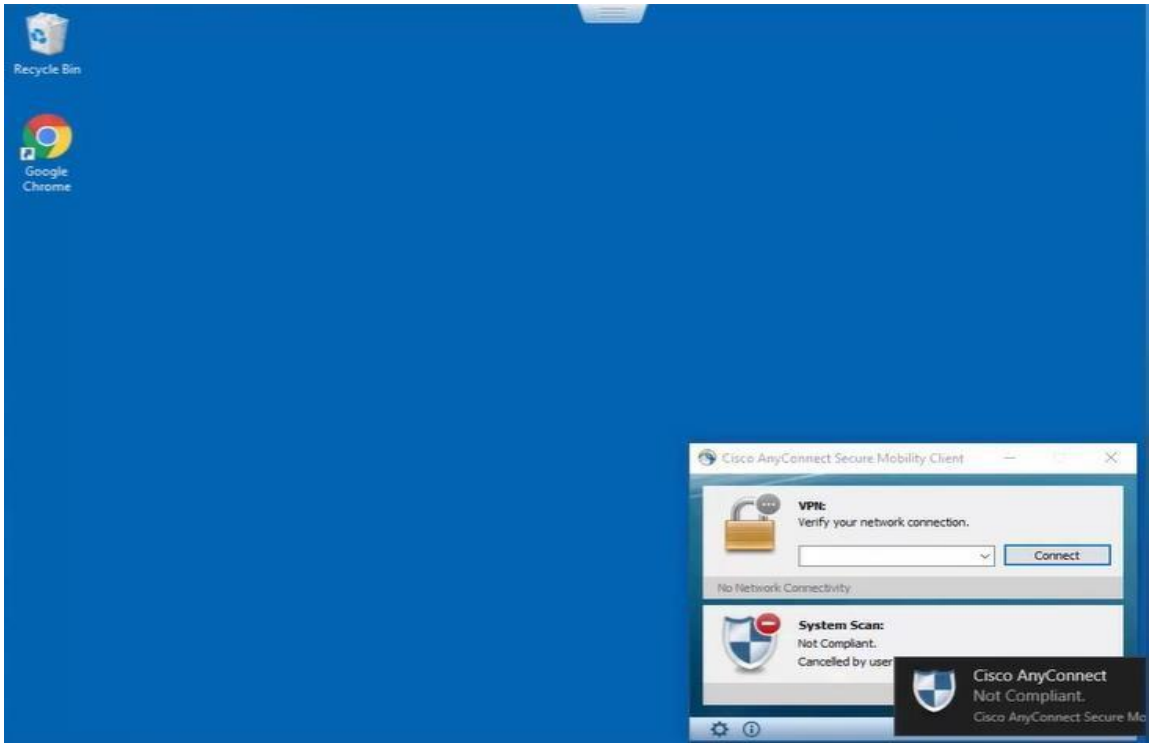
✓ Windows Firewall disabled. Please click to enable manually



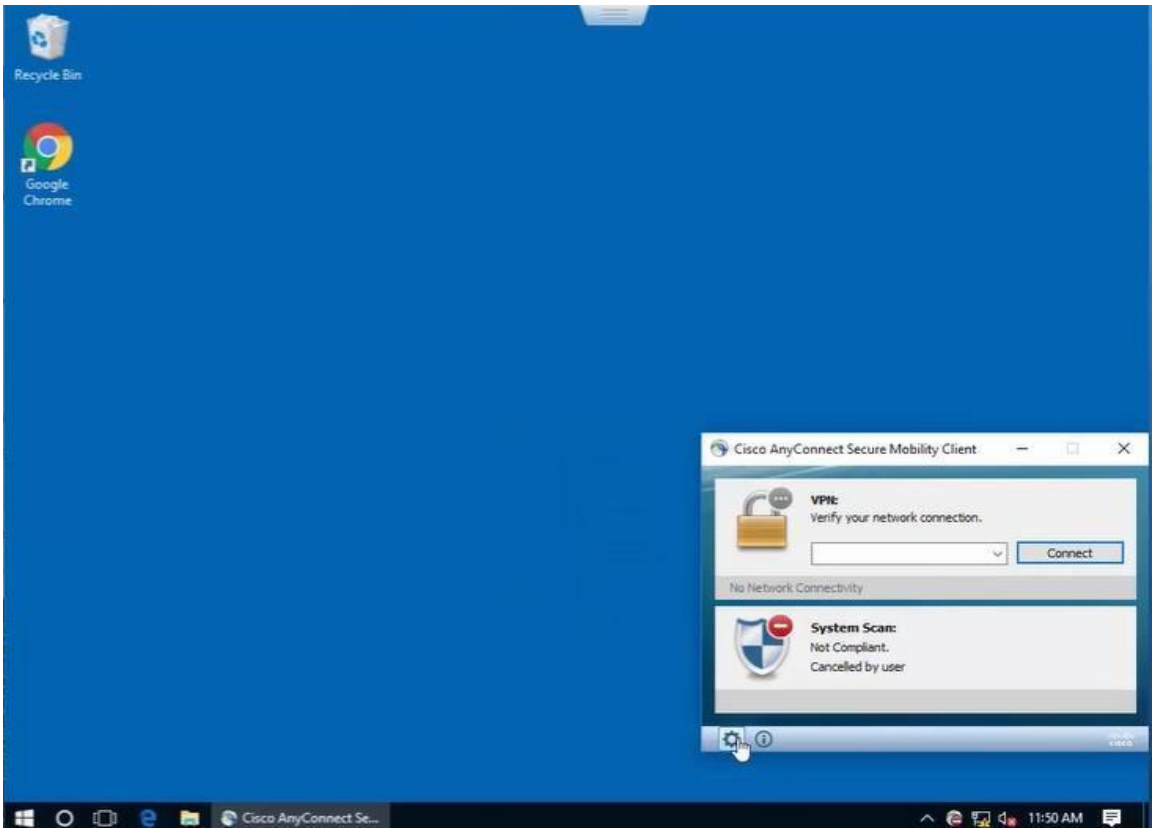

Recycle Bin
Google Chrome
Cisco AnyConnect Secure Mobility Client
System Scan Summary
Update Details
30%
1 Update(s) Required
Updates are needed on your computer before you can join the network.
Updates
Status
Required
1
LM WINS FW
Click Start to begin
LM WINS FW (Required)
Windows Firewall disabled. Please click to enable manually
Start
Time Remaining:
00:09:20
Hide
Cancel
Connect
System Scan:
Update your system.
Details
30%
Cancel
Cisco AnyConnect Se...
Cisco AnyConnect Se...
11:50 AM


Recycle Bin
Google Chrome
Cisco AnyConnect Secure Mobility Client
System Scan Summary
Update Details
30%
1 Update(s) Required
Updates are needed on your computer before you can join the network.
Updates
Status
Required
1
LM WINS FW
Click Start to begin
LM WINS FW (Required)
Windows Firewall disabled. Please click to enable manually
Start
Time Remaining:
00:09:03
Hide
Cancel
Cisco AnyConnect
Clicking Cancel may change your network connectivity and interrupt download or required updates. Are you sure you want to cancel the current operation?
Yes
No
Connect
System Scan:
Update your system.
Details
30%
Cancel

✓ Hệ thống System Scan: chuyển sang trạng thái Not Complain



✓ Click vào biểu tượng bánh răng để setting



Mục System Scan: chuyển đến tab Scan Summary:

✓ LM WIN FW (Not Requireds)

✓ LM WIN DEFENDER DEF (Requireds)