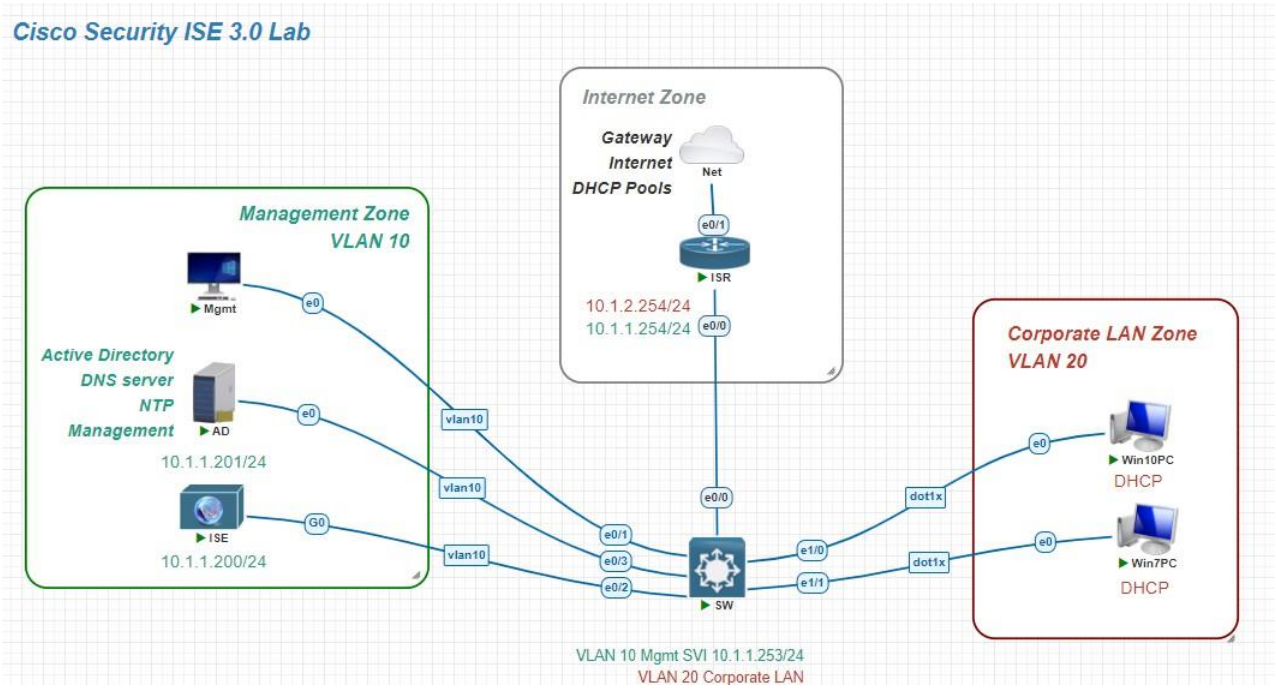
LAB - TÍCH HỢP CISCO ISE VỚI ACTIVE DIRECTORY

I. Sơ đồ:



II. Mục đích thực hiện:

Nếu ISE của bạn chưa được tích hợp với Active Directory (AD), bạn nên xem xét sử dụng thông tin đăng nhập AD để xác thực với ISE thay vì thông tin lưu trữ cục bộ trên ISE. Không chỉ có thông tin đăng nhập AD thuận tiện hơn khi sử dụng, nó còn dễ dàng theo dõi hoạt động của người dùng hơn trong ISE khi họ đang sử dụng thông tin đăng nhập của riêng họ so với thông tin được lưu trữ cục bộ.

Điều tuyệt vời ở ISE là giống như hầu hết các thiết bị kết nối mạng (điển hình là PC hay laptop), nó sẽ quay trở lại thông tin đăng nhập cục bộ khi AD fail nên nguy cơ tự khóa bạn khỏi ISE là rất nhỏ. (tức là khi join vào AD, ISE vẫn sẽ giữ thông tin đăng nhập cục bộ (local) của bạn trước đó).

Một điều thú vị khác về tích hợp AD là bạn có thể sử dụng các nhóm bảo mật AD cho việc Kiểm soát truy cập dựa trên vai trò (RBAC) trên ISE. Khi bạn đã thiết lập các role trong ISE và tạo các nhóm AD, nó cũng đơn giản như việc thêm người dùng

AD vào nhóm bảo mật khi họ gia nhập và loại bỏ chúng khỏi nhóm AD khi họ nghỉ hưu hoặc thay đổi vị trí.

III. Thực hiện:

3.1 Cấu hình ban đầu:

Thực hiện cấu hình IP cho PC, Router, thực hiện NAT sao cho PC có thể ping thấy ISE Server.

SW:

```
configure terminal
hostname SW
aaa new-model
vtp mode transparent
spanning-tree mode pvst
spanning-tree extend system-id
vlan 10
name mgmt
exit
vlan 20
name Corp_user_vlan20
exit
vlan 30
name BOYD
```

```
exit
interface Ethernet0/0
no shutdown
switchport trunk encapsulation dot1q
switchport mode trunk
exit
interface Ethernet0/1
no shutdown
description mgmt node
switchport access vlan 10
switchport mode access
exit

interface Ethernet0/2
no shutdown
description ise node
switchport access vlan 10
switchport mode access
exit
```

```
interface Ethernet0/3
no shutdown
description AD node
switchport access vlan 10
switchport mode access
exit

interface Ethernet1/0
no shutdown
description win10 node
switchport access vlan 20
switchport mode access
exit

interface Ethernet1/1
no shutdown
description win10 node
switchport access vlan 20
switchport mode access
exit
```

```
interface Ethernet1/2
no shutdown
description Tablet
switchport access vlan 30
switchport mode access
exit

interface Vlan10
no shutdown
ip address 10.1.1.253 255.255.255.0
exit
```

ISR:

```
configure terminal
hostname ISR

ip dhcp pool lan
network 10.1.1.0 255.255.255.0
default-router 10.1.1.254
dns-server 10.1.1.254 8.8.8.8
```

```
domain-name test.lab
exit


ip dhcp pool VLAN20
network 10.1.2.0 255.255.255.0
default-router 10.1.2.254
domain-name eve.lab
dns-server 10.1.1.201
exit


ip dhcp pool VLAN30
network 10.1.3.0 255.255.255.0
default-router 10.1.3.254
domain-name eve.lab
dns-server 10.1.1.201
exit
ip dhcp excluded-address 10.1.1.1 10.1.1.9
ip name-server 8.8.8.8
ip name-server 1.1.1.1
interface Ethernet0/0.10
```

```
no shutdown
encapsulation dot1Q 10
ip address 10.1.1.254 255.255.255.0
ip nat inside
ip virtual-reassembly in
exit

interface Ethernet0/0.20
no shutdown
encapsulation dot1Q 20
ip address 10.1.2.254 255.255.255.0
ip nat inside
ip virtual-reassembly in
exit

interface Ethernet0/0.30
no shutdown
encapsulation dot1Q 30
ip address 10.1.3.254 255.255.255.0
ip nat inside
```

```
ip virtual-reassembly in

exit

interface Ethernet0/1

no shutdown

ip address dhcp

ip nat outside

ip virtual-reassembly in

duplex auto



ip nat inside source list nat interface Ethernet0/1 overload

ip access-list standard nat

permit 10.1.1.0 0.0.0.255

permit 10.1.2.0 0.0.0.255

permit 10.1.3.0 0.0.0.255
```

3.2 Cấu hình Active Directory:

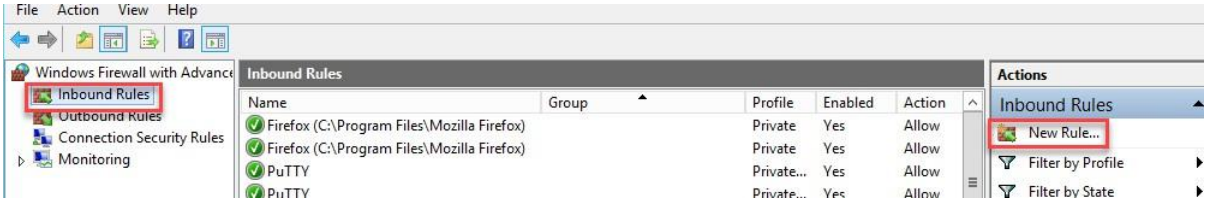
1. Cấu hình ip tĩnh cho winserver:

- ✓ IP Address: 10.1.1.201
- ✓ Mark: 255.255.255.0
- ✓ Gateway: 10.1.1.254
- ✓ DNS Server : 10.1.1.201

2. Tạo firewall NTP inbound rule

✓ *Control Panel/Windows Defender Firewall/Advanced settings*

✓ *Inbound Rules/New rule*



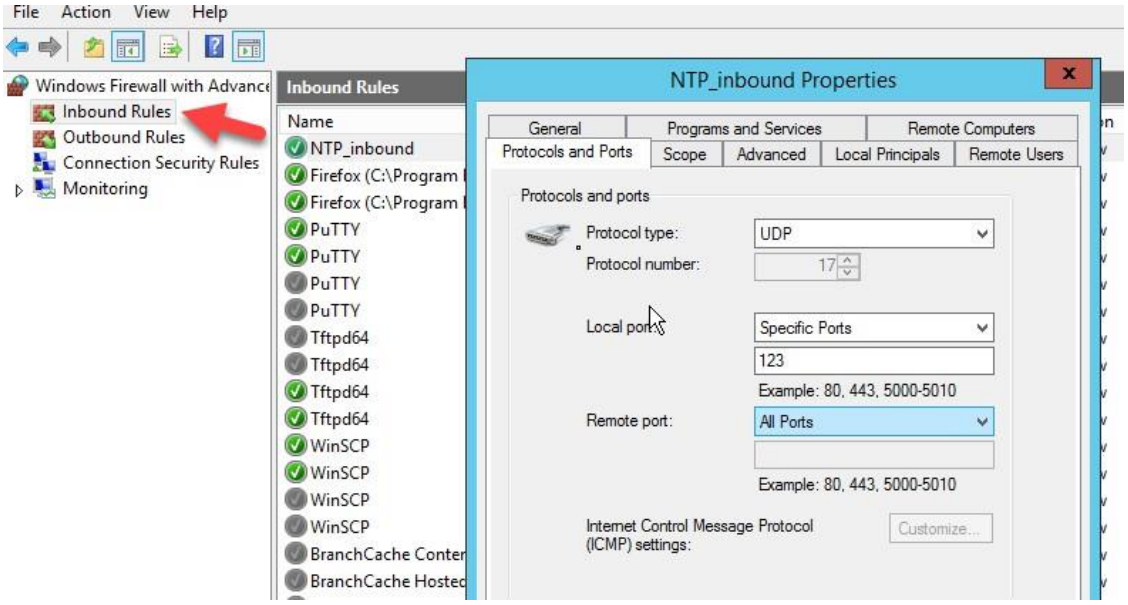
✓ Rule type: Port > Next

✓ Protocol and Ports: UDP 123 > Next

✓ Action: Allow the Connection > Next

✓ Profile: check all, domain, private, public > Next

✓ Name: NTP_inbound

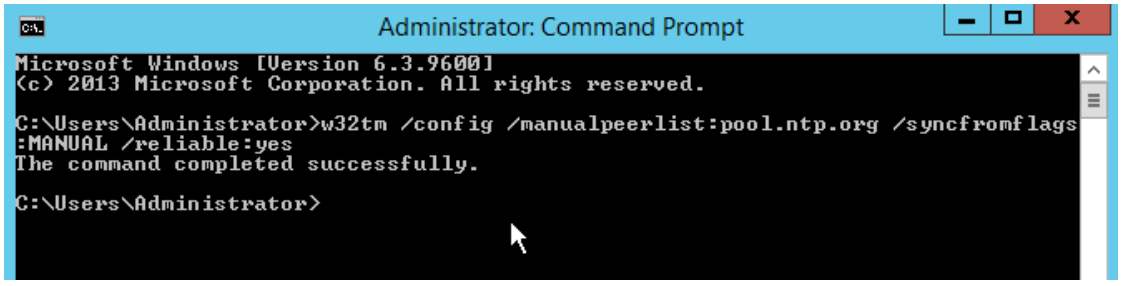


3. Cấu hình external NTP server:

✓ Mở windows CMD

✓ Gõ

w32tm /config /manualpeerlist:pool.ntp.org /syncfromflags:MANUAL /reliable:yes



4. Chỉnh sửa Registry files:

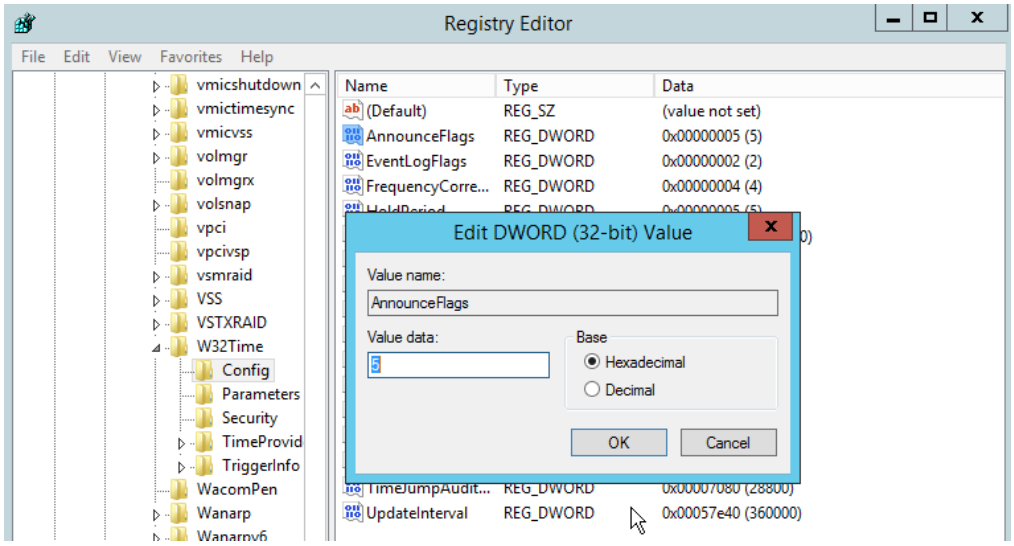
✓ Chọn Start > Run, type **regedit**, và sau đó chọn OK

✓ Chuyển hướng đến registry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags

✓ Chuột phải **Announce Flags**, và sau đó chọn **Modify**

✓ Thay đổi type Value thành 5 và click OK.

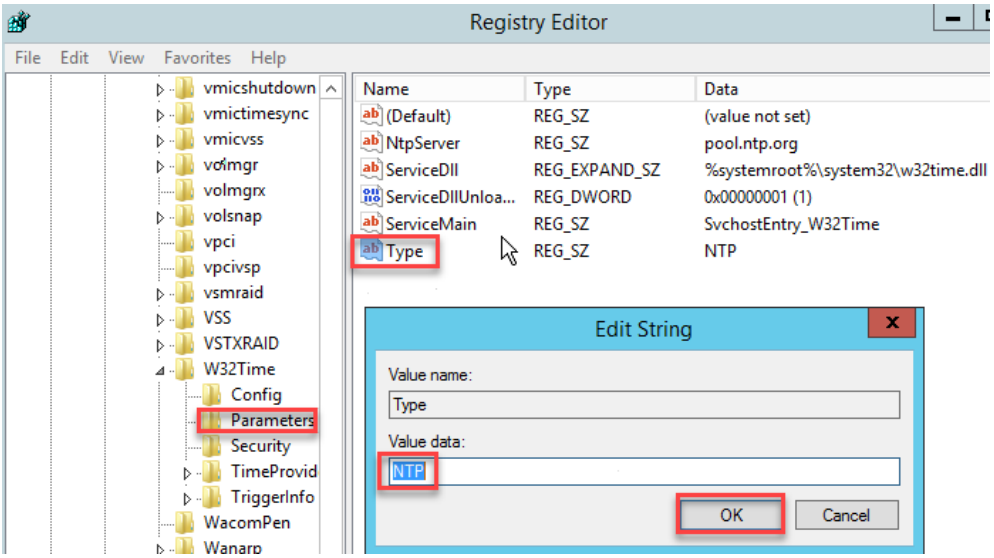


✓ Chuyển hướng đến registry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type

✓ Chuột phải **Type**, và sau đó chọn **Modify**

✓ Thay đổi Value như NTP và click OK.

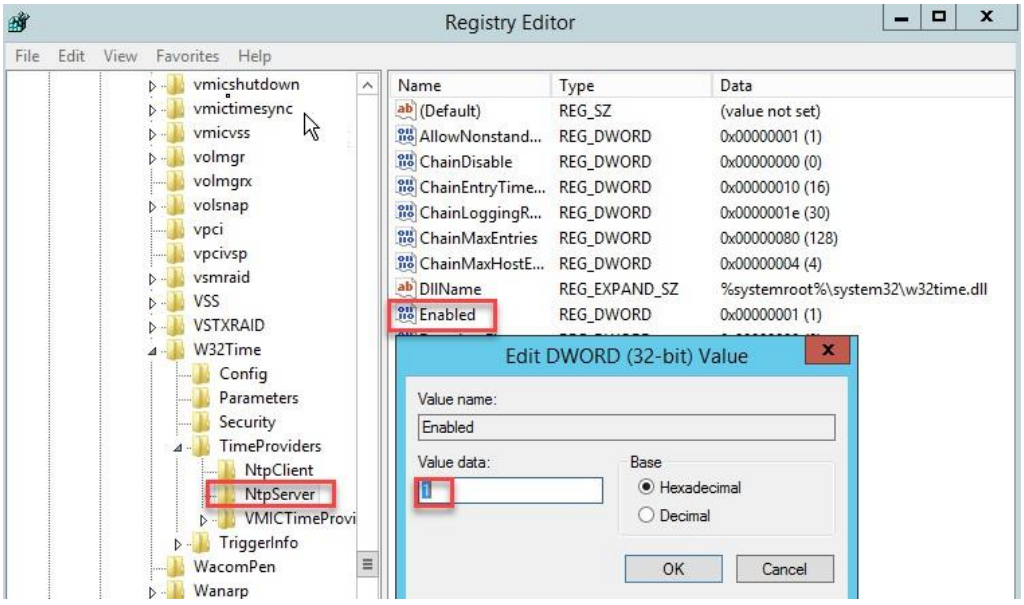


✓ Bật NTP server. Mở Location

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpSer ver

✓ Chuột phải **Enabled**, và sau đó chọn **Modify**

✓ Trong trường DWORD Value, chọn type 1



5. Restart NTP service

- ✓ Mở windows CMD
- ✓ Nhập:

net stop w32time && net start w32time

6. Verify NTP

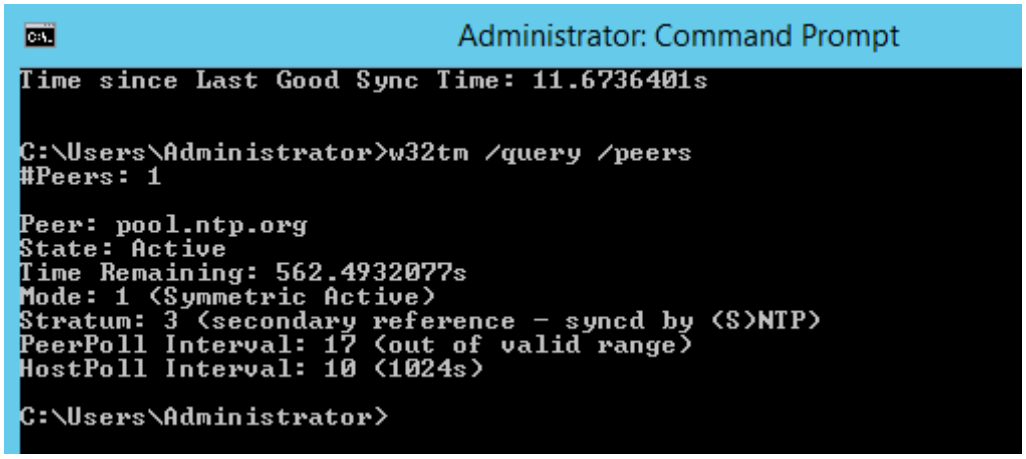
- ✓ Mở windows CMD
- ✓ Enter:

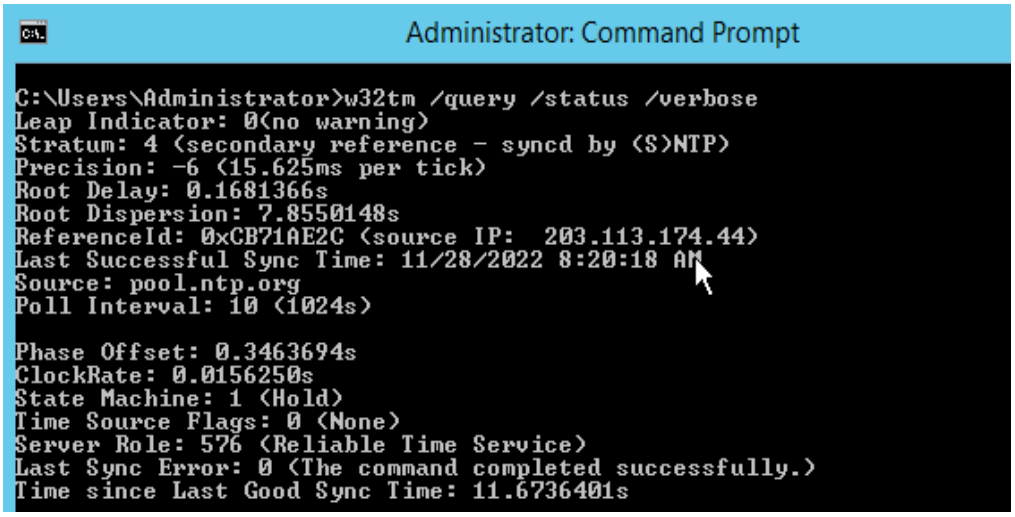
w32tm /query /status /verbose

→ Hiển thị trạng thái đồng bộ hóa cuối cùng hoặc bất kỳ lỗi nào.

w32tm /query /peers

→ Hiển thị NTP.





7. Cấu hình Windows server name:

✓ Mở Server manager

✓ Click Local Server

✓ Click Computer Name

✓ Click Change

✓ Chọn Name: ad

✓ Click OK

✓ Click Close và restart Server

8. Cấu Windows server Active Directory:

1. Cài đặt Active Directory Server role

✓ Mở Server manager

✓ Click Add roles và features

✓ Click 3 lần Next

✓ Chọn Active Directory Domain Services, và click Add features

✓ Click 3 lần Next, và Install

✓ Sau khi cài đặt hoàn tất, Click close

2. Chuyển hướng đến Server manager, (biểu tượng lá cờ vàng)

✓ Click on *Promote this server to a domain controller*

✓ Chọn "Add new forest"

✓ Để domain name "eve.lab"

✓ Click Next

✓ Type 2 times DSRM password (example: Test123)

✓ Click Next 5 times

✓ Click Install

✓ Sau khi server đã rebooted và nếu required, thay administrator

9. Cấu DNS Server:

✓ Chuyển hướng đến Server manager, Tools/DNS

Tạo Reverse Lookup Zones

- ✓ Chuột phải Reverse lookup Zones/New Zone, Next
- ✓ Rời Primary Zone and click Next
- ✓ Rời To all DNS servers
- ✓ domain: eve.lab, click Next
- ✓ IPv4 Reverse Lookup Zone, Next
- ✓ Network ID: 10.1.1, Next, Next
- ✓ Cho phép both non-secure và secure dynamic updates, Next
- ✓ Kết thúc

Tạo new A record for ISE

- ✓ Chuyển hướng đến forward lookup zone eve.lab
- ✓ Tạo New host (A or AAAA)
- ✓ Name: ise
- ✓ IP Address: 10.1.1.200
- ✓ Bật Create associated pointer (PTR) record
- ✓ Add Host

7. Cấu hình AD Corporate users:

Chuyển hướng đến Server manager, Tools/Active Directory Users and Computers

- ✓ Chuột phải trên Users directory/New/user
- ✓ First Name: Jenny
- ✓ Last name: Doe

- ✓ Username: jennydoe
- ✓ Click Next
- ✓ Password (2 lần): Silver2021
- ✓ Bỏ tick User must change password at next login
- ✓ Tick vào: User cannot change password and Password never expires
- ✓ Click Next và Finish

Chuyển hướng đến Server manager, Tools/Active Directory Users and Computers

- ✓ Chuột phải trên Users directory/New/user
- ✓ First Name: John
- ✓ Last name: Doe
- ✓ Username: johndoe
- ✓ Click Next
- ✓ Password (2 times): Gold2021
- ✓ Bỏ tick User must change password at next login
- ✓ Tick: User cannot change password and Password never expires
- ✓ Click Next và Finish

8. Thêm User Groups vào Active directory:

1. Chuyển hướng đến Server manager, Tools/Active Directory Users and Computers

   ✓ Chuột phải vào Users directory/New/Group

   ✓ Name: Employees

   ✓ Click OK

   ✓ Chuột phải vào Users directory/New/Group

   ✓ Name: Engineers

   ✓ Click OK

9. Thêm users into created AD groups

1. Chuột phải vào user John Doe và chọn: Add to group

   ✓ Enter the object names to select: Engineers

   ✓ Click Check name

   ✓ Click OK

2. Chuột phải vào user Jenny Doe and select: Add to group

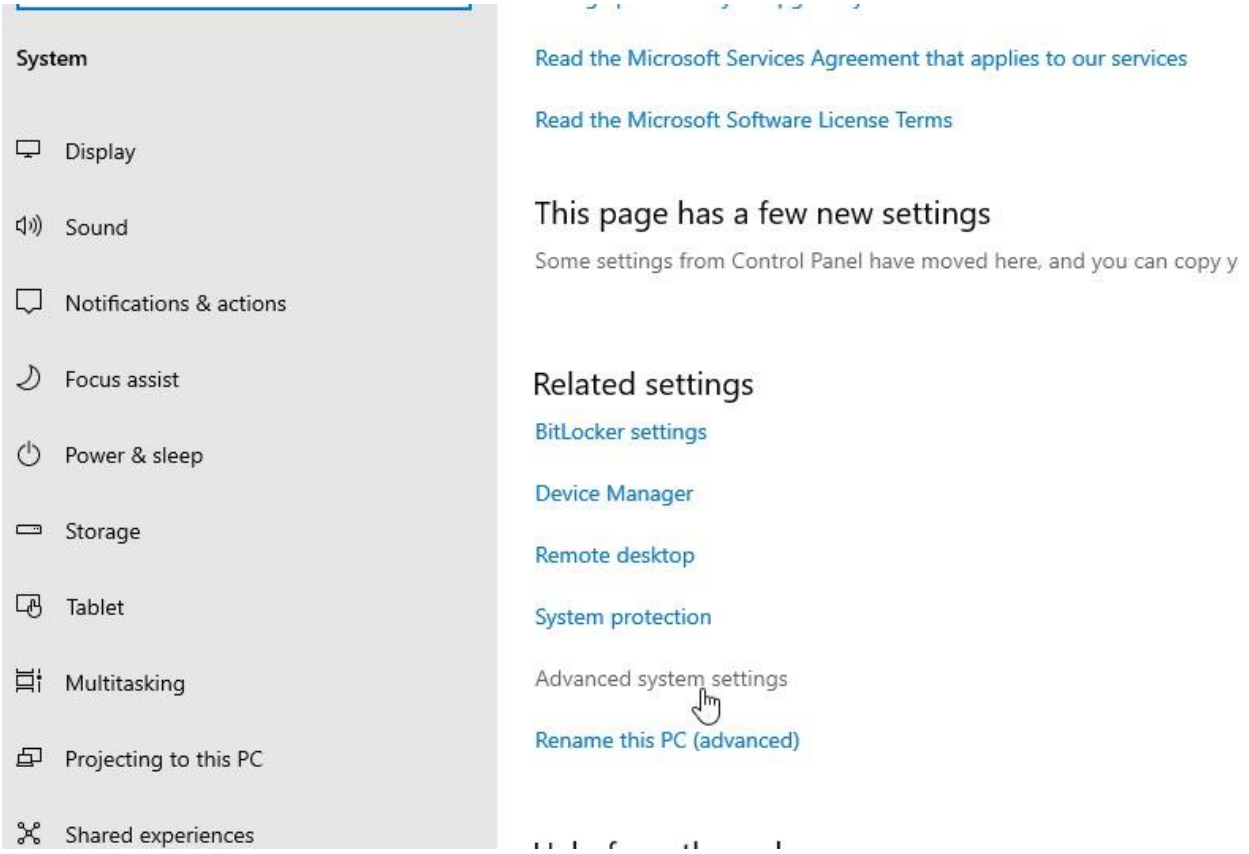
   ✓ Enter the object names to select: Employees

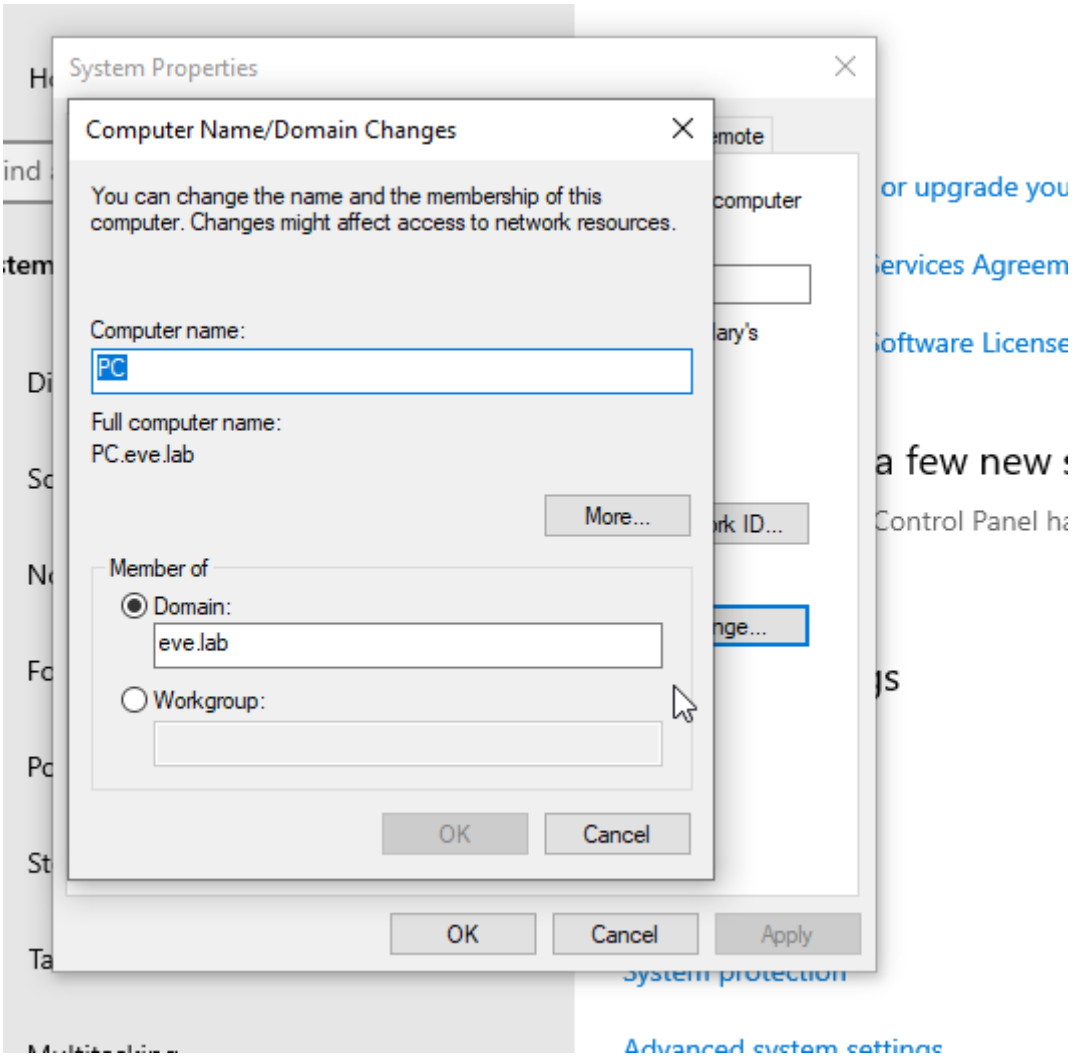
   ✓ Click Check name

   ✓ Click OK

3.3 THÊM PC VÀO DOMAIN:

- Đã cấu hình domain “eve.lab”, username: administrator password: Test123





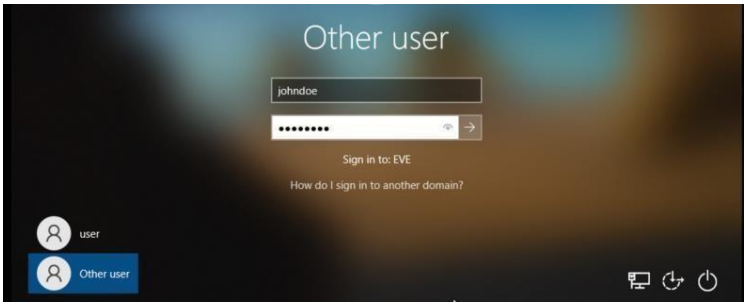
✓ Đợi boot lại pc

✓ Vào cmd xem lại ip

Ghi chú: PC windows phải được cấu hình để có IP thông qua DHCP. Switch và ISP router được cấu hình với nhóm VLANs và DHCP Pools thích hợp.

1. Windows 10 host

- ✓ Chuyển đến: Start/Settings/About
- ✓ Vào: Advanced System Settings, Click
- ✓ Click Tab: Computer Name
- ✓ Click: Change
- ✓ Type Computer Name: John-PC
- ✓ Chọn radio button: Domain
- ✓ Type domain: eve.lab
- ✓ Click OK
- ✓ Type your AD server administrator username and password
- ✓ (Ví dụ: administrator/Test123)
- ✓ Click OK
- ✓ Click Close và restart PC
- ✓ Chọn Other user và login: johndoe/Gold2021



2. Windows 7:

- ✓ Chuyển hướng đến: Start/Control Panel/System và Security/System/Advanced system settings
- ✓ Chọn Tab: Computer Name
- ✓ Chọn: Change
- ✓ Type Computer Name: Jenny-PC
- ✓ Chọn radio button: Domain
- ✓ Type domain: eve.lab
- ✓ Chọn OK
- ✓ Type your AD server administrator username and password (example: administrator/Test123)
- ✓ Chọn OK
- ✓ Chọn Close và restart PC
- ✓ Chọn Switch user/Other user
- ✓ Login với AD: jennydoe/Silver2021

3.4 Cài đặt ISE:

Type: setup

Hostname: ise

IP address: 10.1.1.200

Netmask: 255.255.255.0

Default gateway: 10.1.1.254

Default domain: eve.lab

Primary name server: 10.1.1.201

NTP Server: 10.1.1.201

User: admin

Password: Test123

```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
localhost login: setup
```

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise
Enter IP address[]: 10.1.1.200
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.1.1.254
Do you want to configure IPv6 address? Y/N [N]:
Enter default DNS domain[]: eve.lab
Enter primary nameserver[]: 10.1.1.201
Add secondary nameserver? Y/N [N]:
Enter NTP server[time.nist.gov]: 10.1.1.201
Add another NTP server? Y/N [N]:
Enter system timezone[UTC]:
Enable SSH service? Y/N [N]: Y
Enter username[admin]: admin
Enter password:
Enter password again:
```

✓ Chờ ise cài đặt xong.

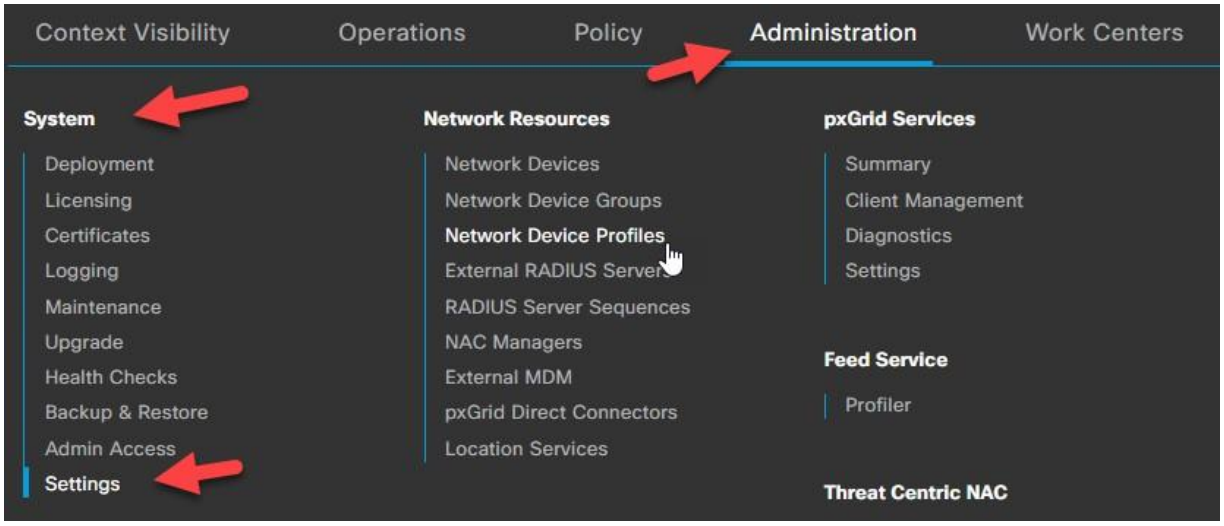
```
admin connected from 127.0.0.1 using console on ise
ise/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          10128
Database Server                        running          92 PROCESSES
Application Server                     running          37140
Profiler Database                      running          22370
ISE Indexing Engine                    running          38925
AD Connector                           running          40045
M&T Session Database                   running          33162
M&T Log Processor                      running          37370
Certificate Authority Service          running          39878
EST Service                            running          69586
SXP Engine Service                     running          162091
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
```

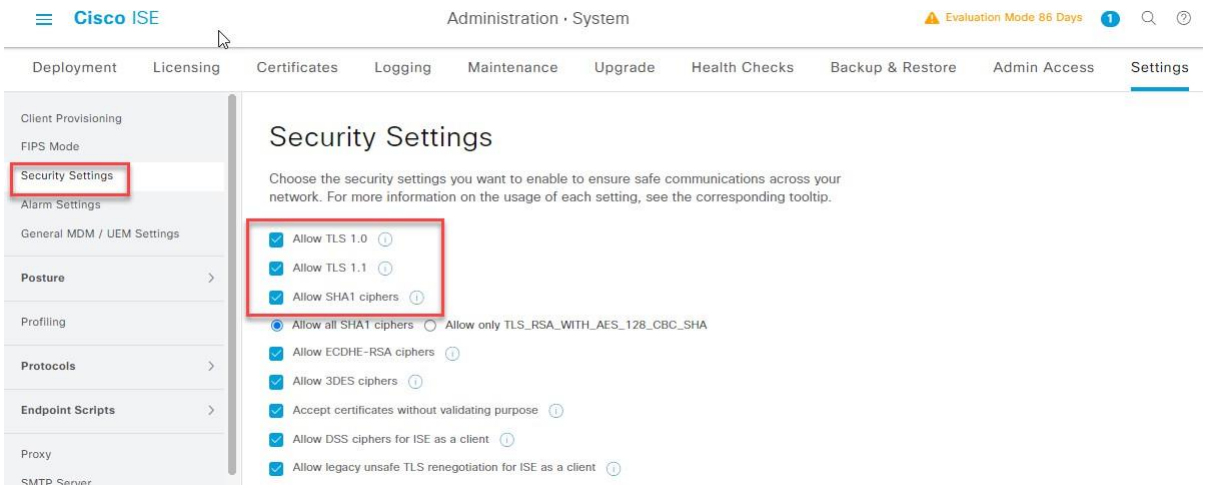
3.5 Cho phép SHA1 ciphers cho WIN7

- ✓ Mở PC Mgmnt và chuyển hướng đến Applications /Internet /Chromium Web Browser
- ✓ Truy cập vào ISE thông qua https://ise.eve.lab
- ✓ username: admin và password: Test123
- ✓ Chuyển hướng đến ISE Management

- ✓ Click Tab Administration/System/Settings



✓ Chuyển hướng đến mục Security Settings và cho phép SHA1 Ciphers.



3.6 Thêm ISE vào DOMAIN:

Bật dịch vụ ISE SXP:

1. Mở Mgmnt PC và chuyển hướng đến Applications/Internet/Chromium Web Browser

✓ Truy cập ISE thông qua link https://ise.eve.lab

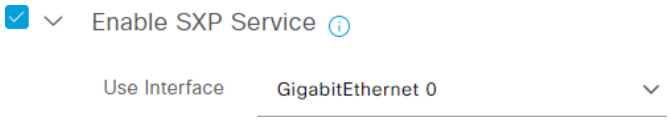
✓ Username: admin và password: Test123

✓ Chuyển hướng đến ISE Management

✓ Chọn Tab Administration/System/Deployment

✓ Chọn "ise"/Edit

✓ Chuyển hướng đến "Enable SXP Service"



✓ Chọn enable

✓ Bấm **Save**

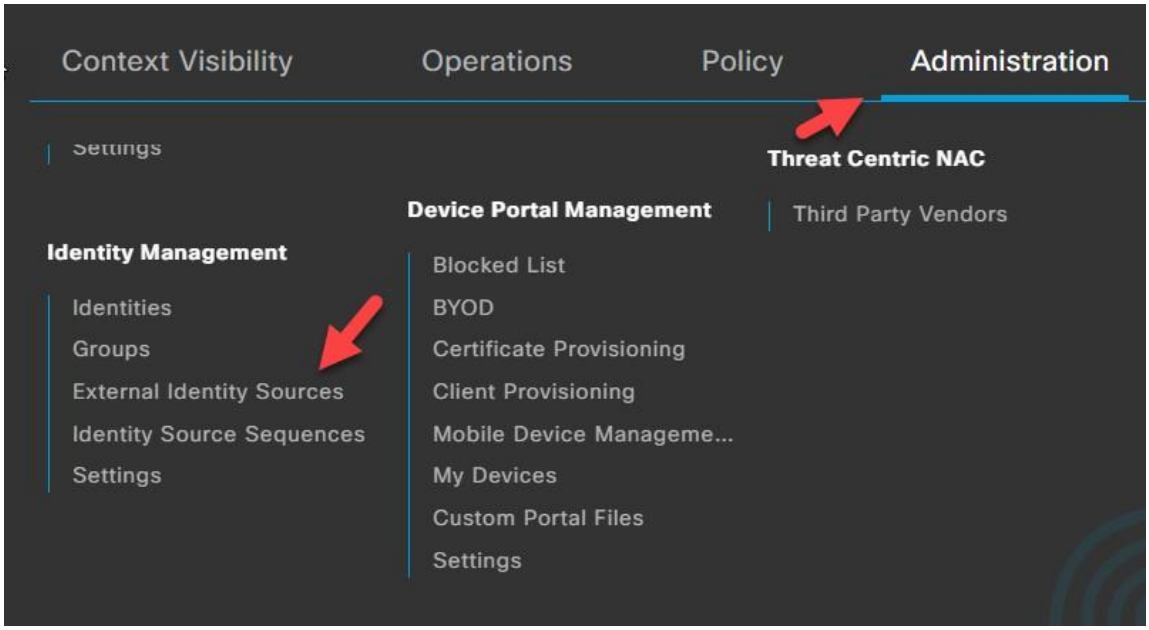
2. Mở Mgmnt PC và chuyển hướng đến Applications/Internet/Chromium Web Browser

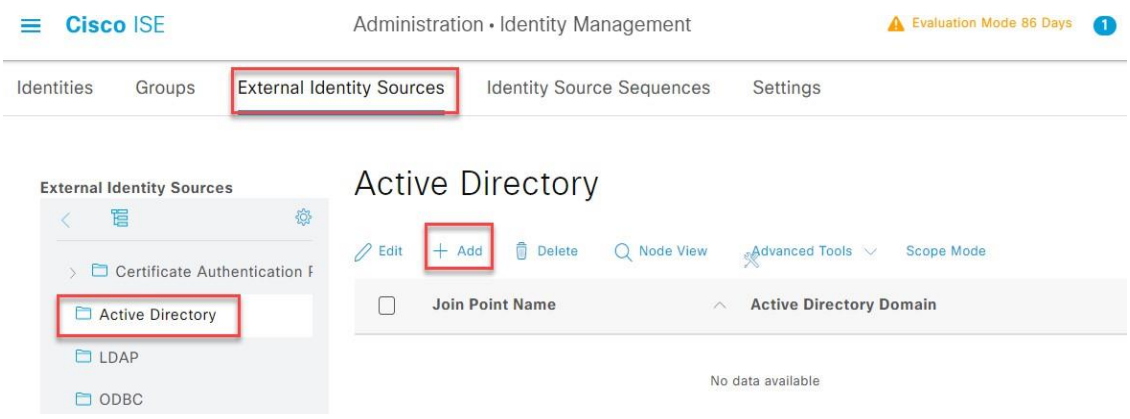
✓ Truy cập vào ISE thông qua link: https://ise.eve.lab

✓ username: admin và password: Test123

✓ Chuyển hướng đến ISE Management

✓ Chọn Tab Administration/Identity Management/External Identity Sources





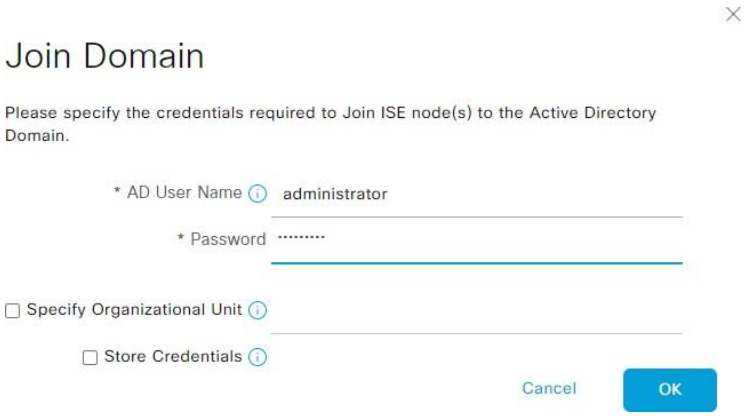
✓ Chọn Active Directory và "+ Add"

✓ Thêm point name: ad.eve.lab

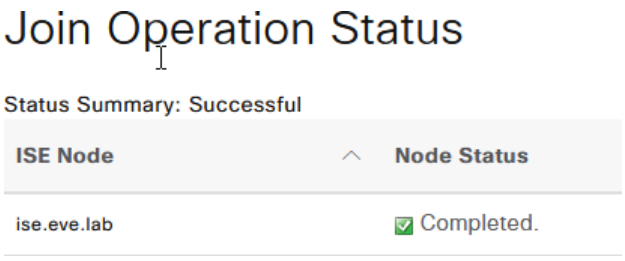
✓ Active Directory domain name: eve.lab

✓ Chọn Submit và Yes để Join

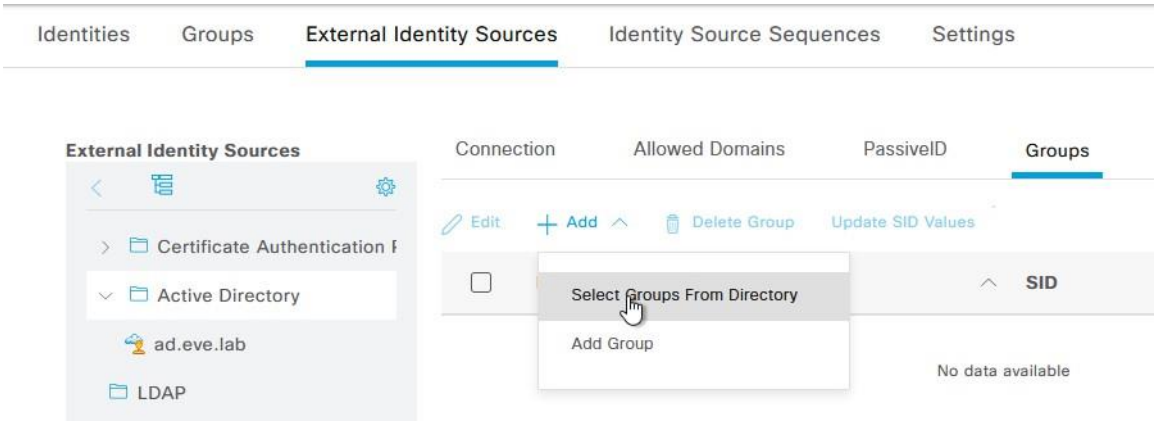
✓ User name: administrator, Password: Test123



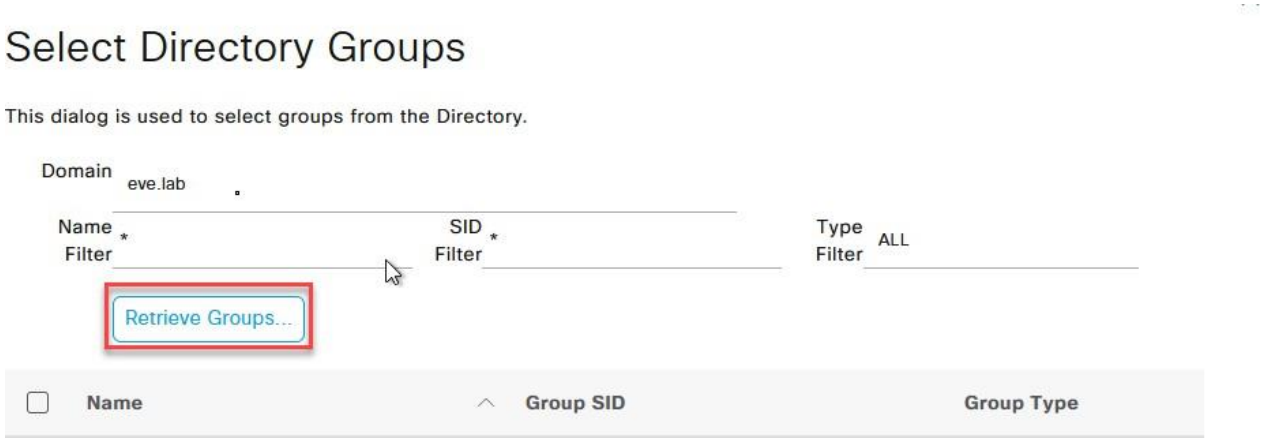
✓ Chọn OK, Status nên là completed



✓ Chọn Tab Groups/Select Groups From Directory



✓ Chọn **Retrieve Groups**



✓ Chọn Domain Computers, Engineers và Employees, Chọn OK

✓ Click **Save**