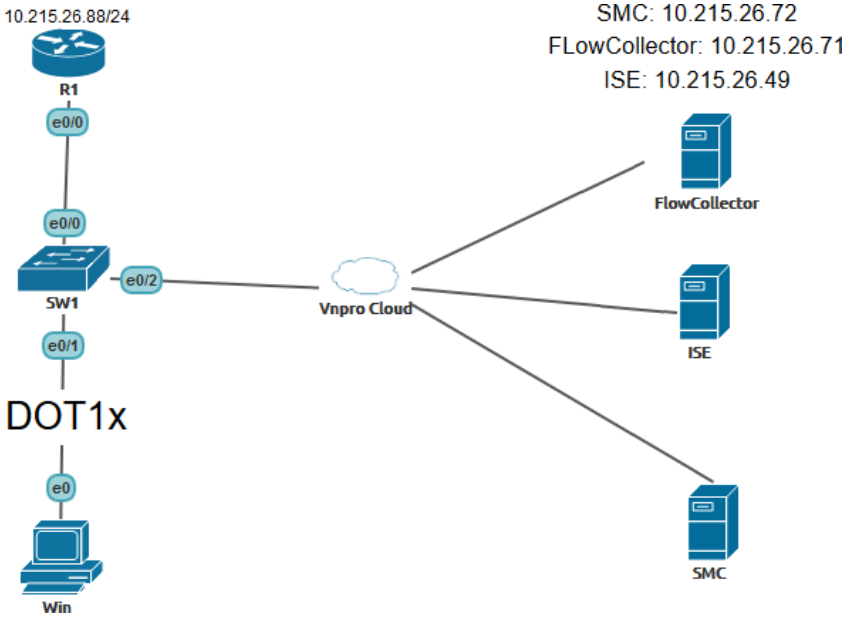
LAB - TÍCH HỢP STEALTHWATCH

I. SƠ ĐỒ:



II. MỤC ĐÍCH:

Trong bối cảnh an ninh mạng thì tầm quan trọng của visibility trong hệ thống mạng là rất lớn. Để đáp ứng nhu cầu của quản trị mạng thì Cisco đã mang đến cho các quản trị viên hay các giải pháp chuyên về bảo mật trong đó là Cisco ISE và Stealthwatch, hai thiết bị này có chức năng và thế mạnh khác nhau. Chính vì thế Cisco đã đưa ra giải pháp tích hợp hai thiết bị trên thông qua giao thức PxGrid

III. THỰC HIỆN:

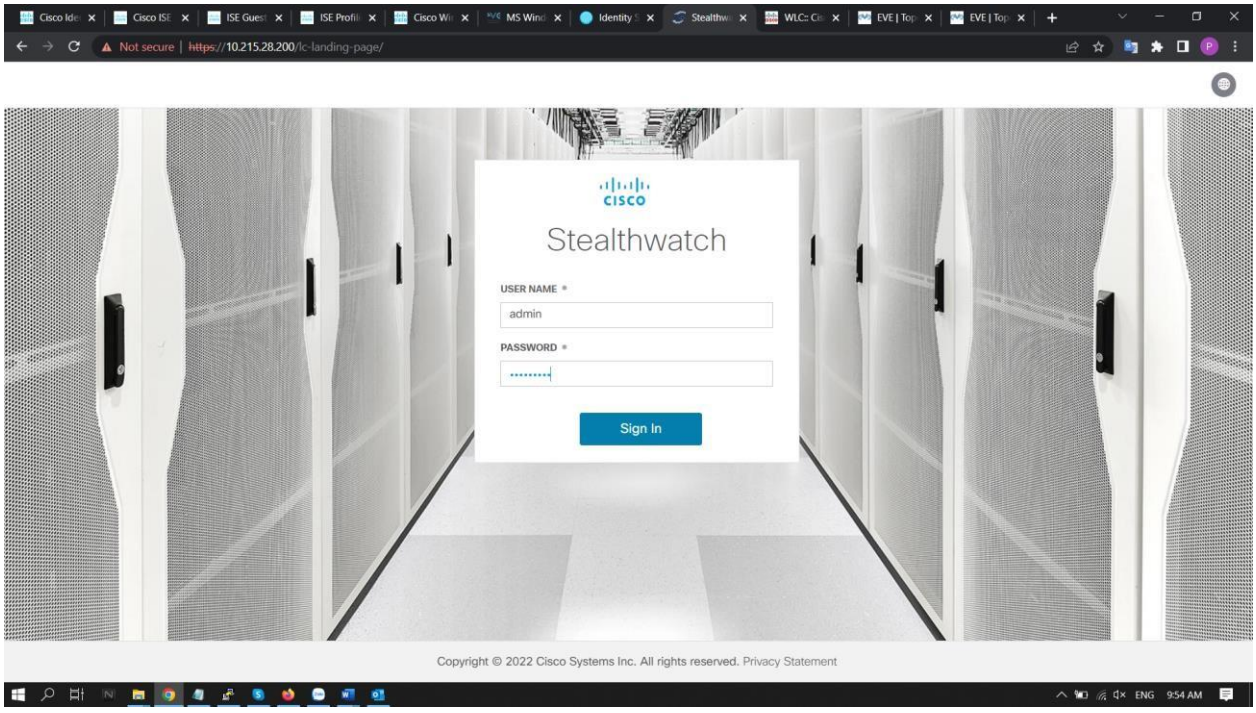
Phần 1: liên kết Stealth Watch và Cisco Ise qua giao thức PxGrid

Cấu hình:

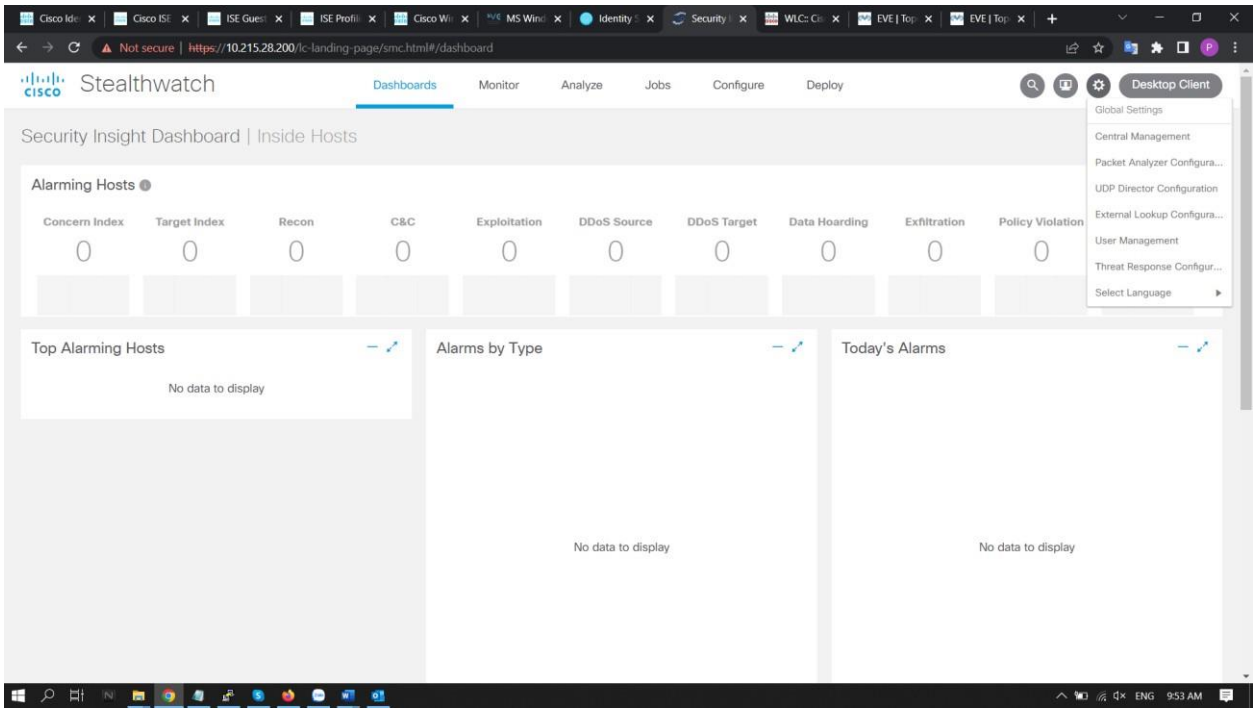
- ✓ Đầu tiên ở bước 1 chúng ta tiến hành vào Stealthwatch Management Console để tạo ra 1 CSR file (Cisco Cloud Services Router) có đuôi .csr để có thể dùng cho Cisco ISE ở bước 2 để Cisco ISE có thể tạo ra 1 Certificate phản hồi.

Bước 1:

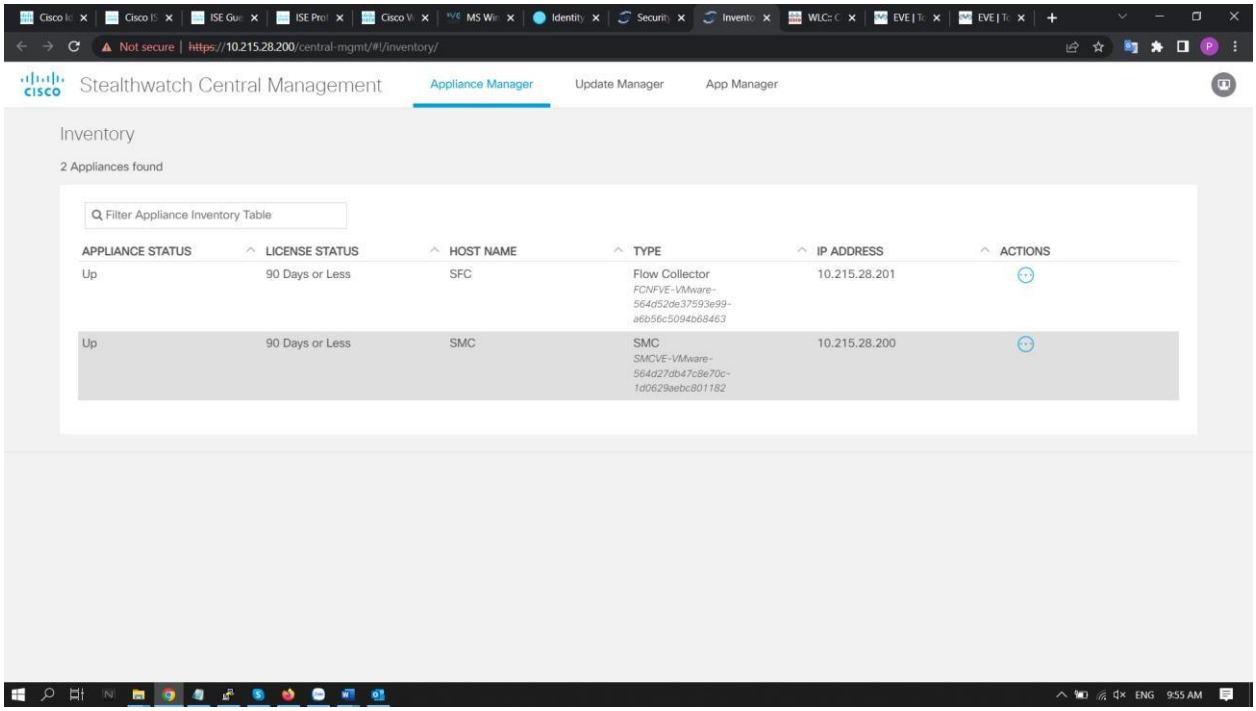
1.1 : Đăng nhập vào Stealthwatch Management Console.

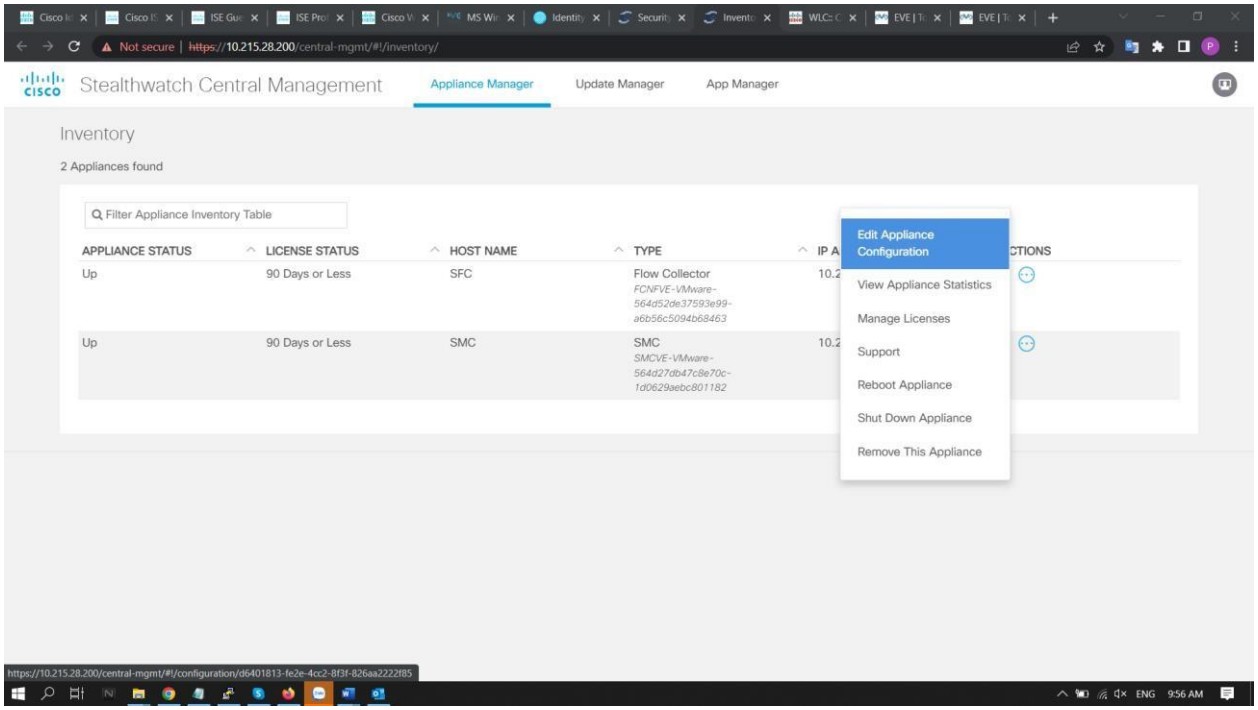


1.2 : Click vào biểu tượng Global Settings sau đó click Central Management.



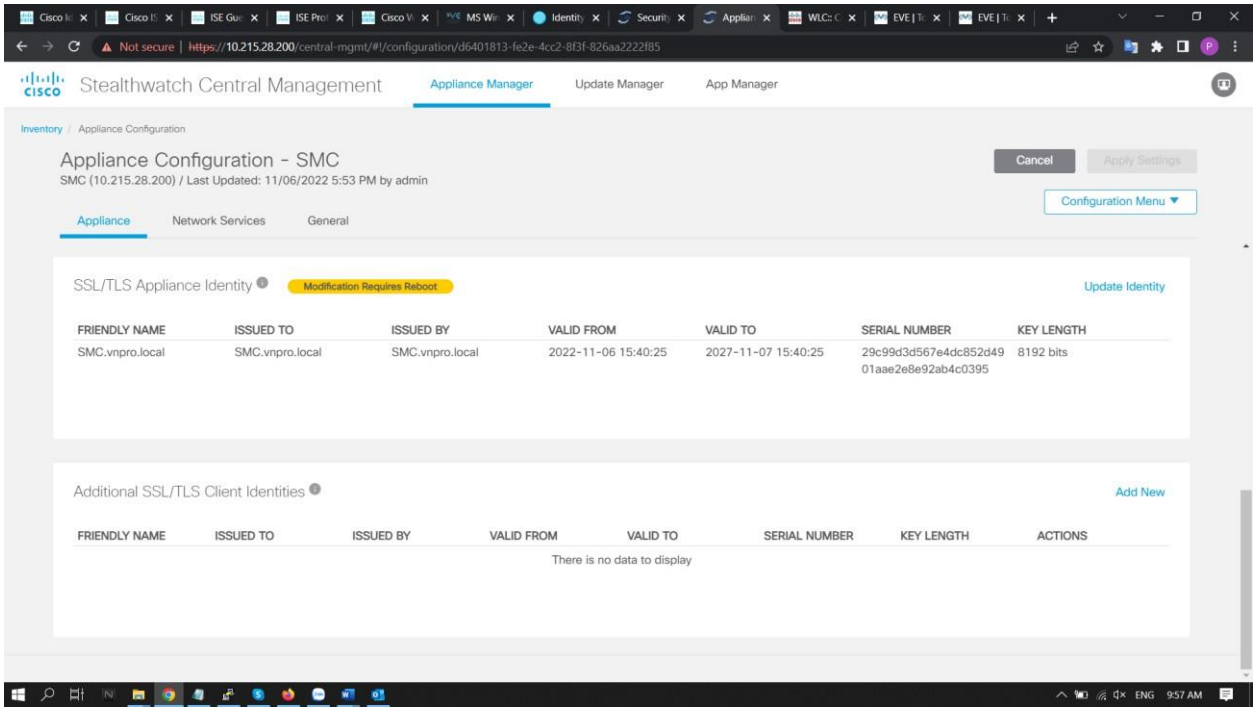
1.3 : Tại Appliance Manager inventory, click vào biểu tượng mở rộng của phía bên phải cùng của SMC (biểu tượng hình tròn màu xanh như hình bên dưới):



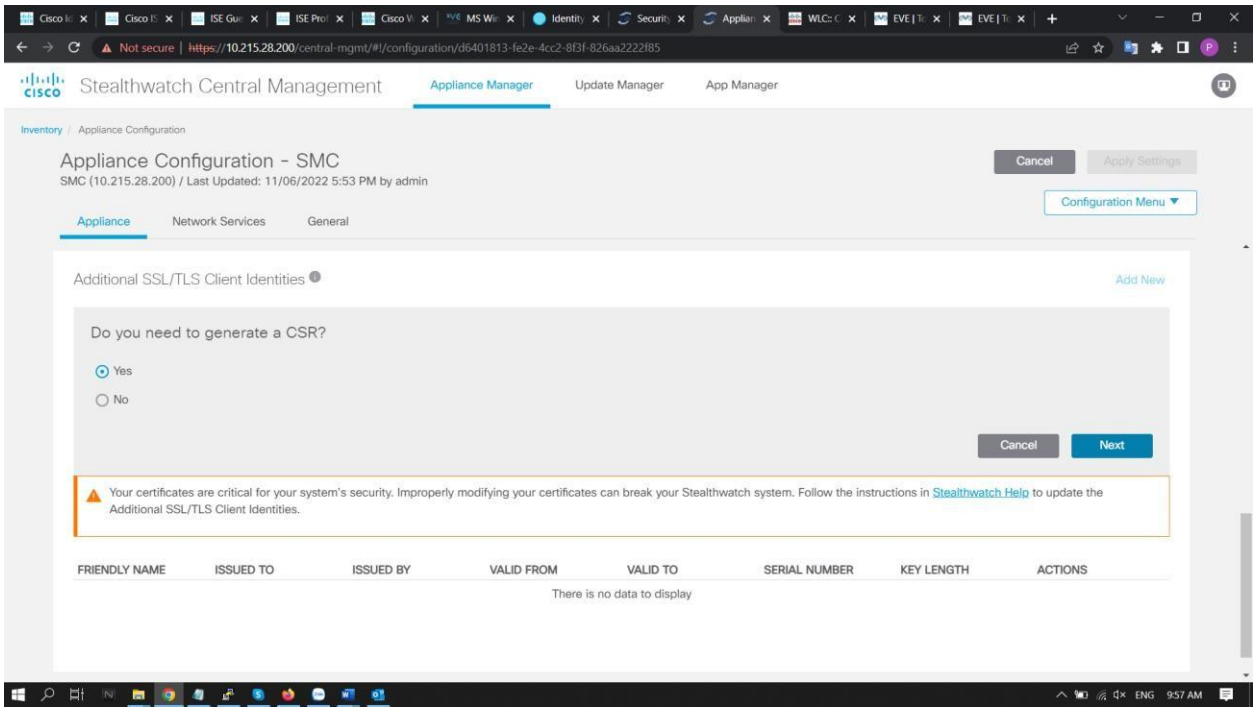


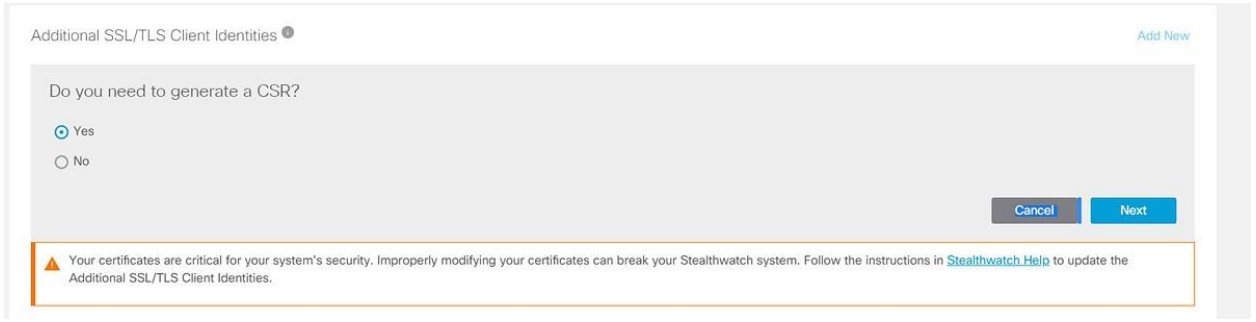
Up	90 Days or Less	StealthWatchManagamentConsole	SMC *SMCVE-VMware-564d31c5190bafab-207f5103327cb459*	10.215.26.72	

1.4 : Tiếp tục ta vào Additional SSL/TLS Client Identities ngay phía dưới của mục Appliance

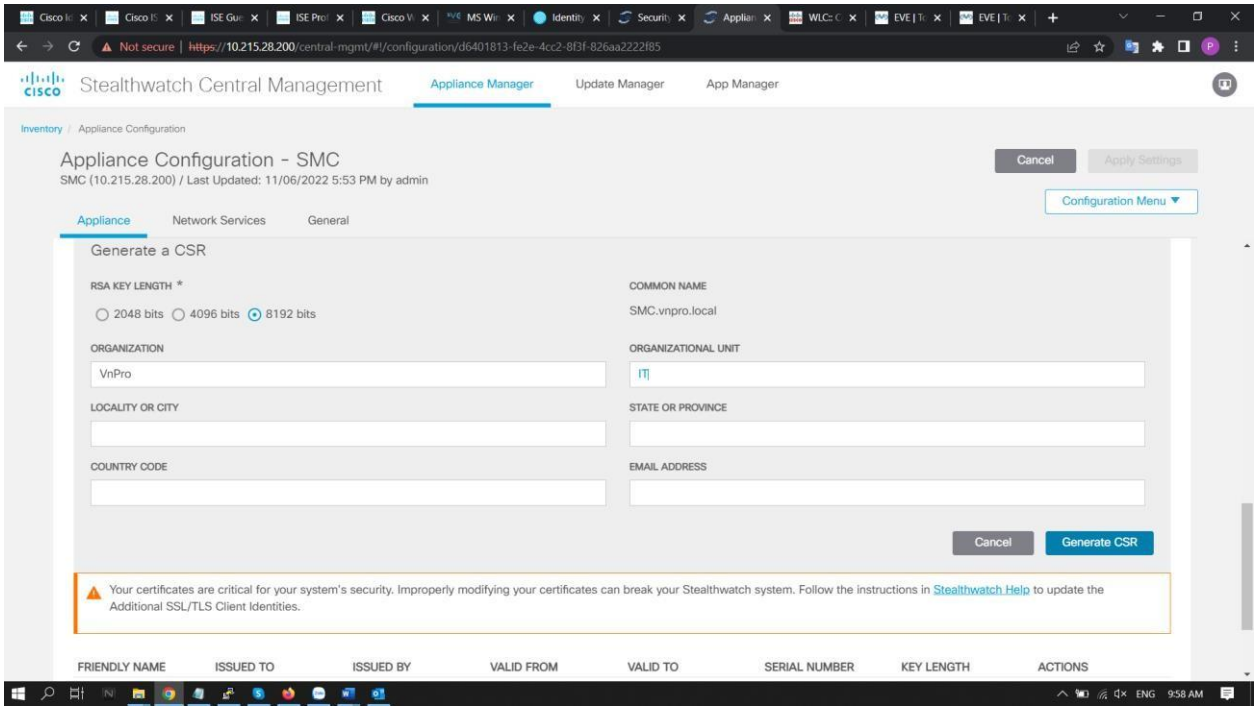


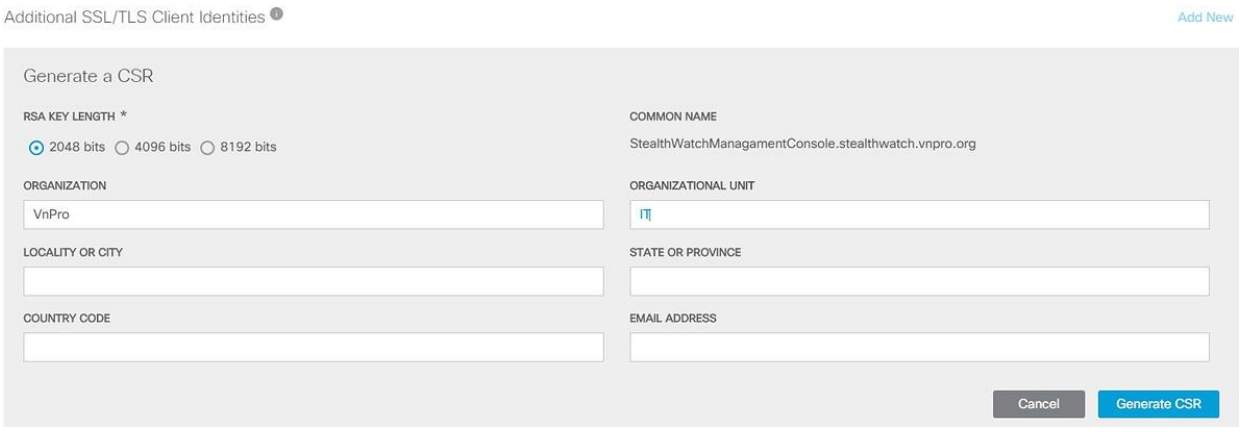
1.5 : Ta tiến hành click vào Add new, hộp thoại bên dưới sẽ hiện ra ta tiến hành click Next



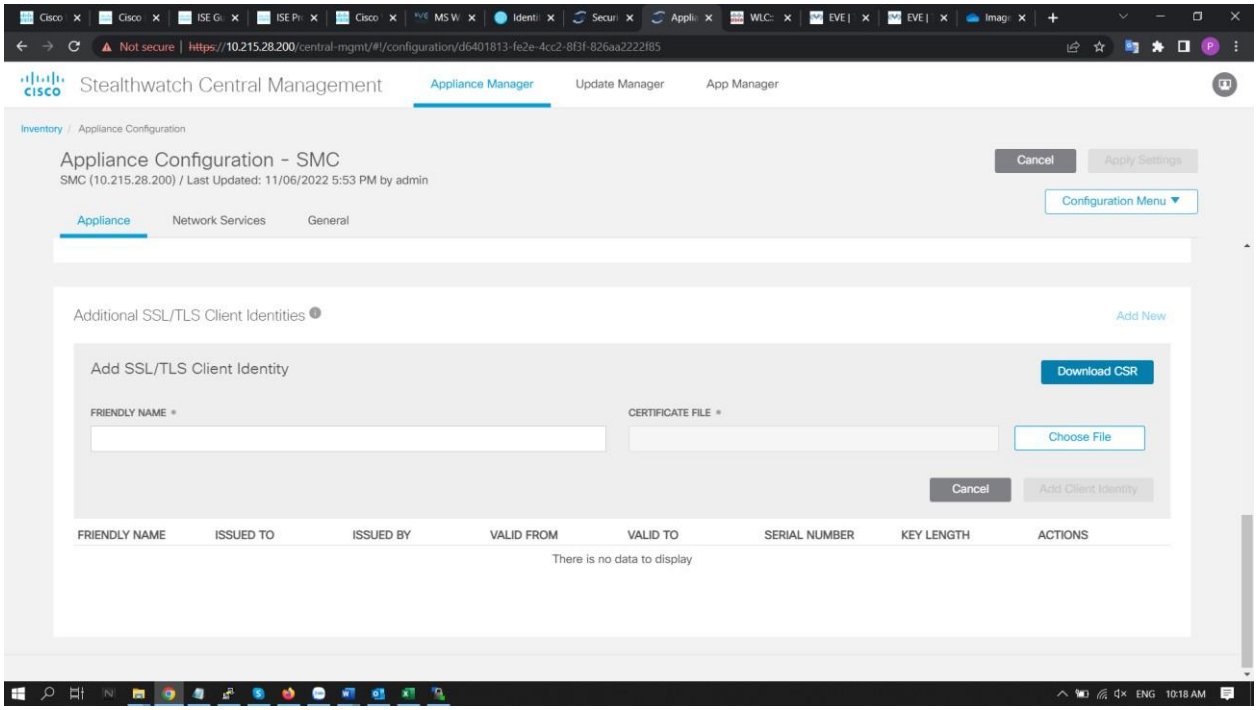


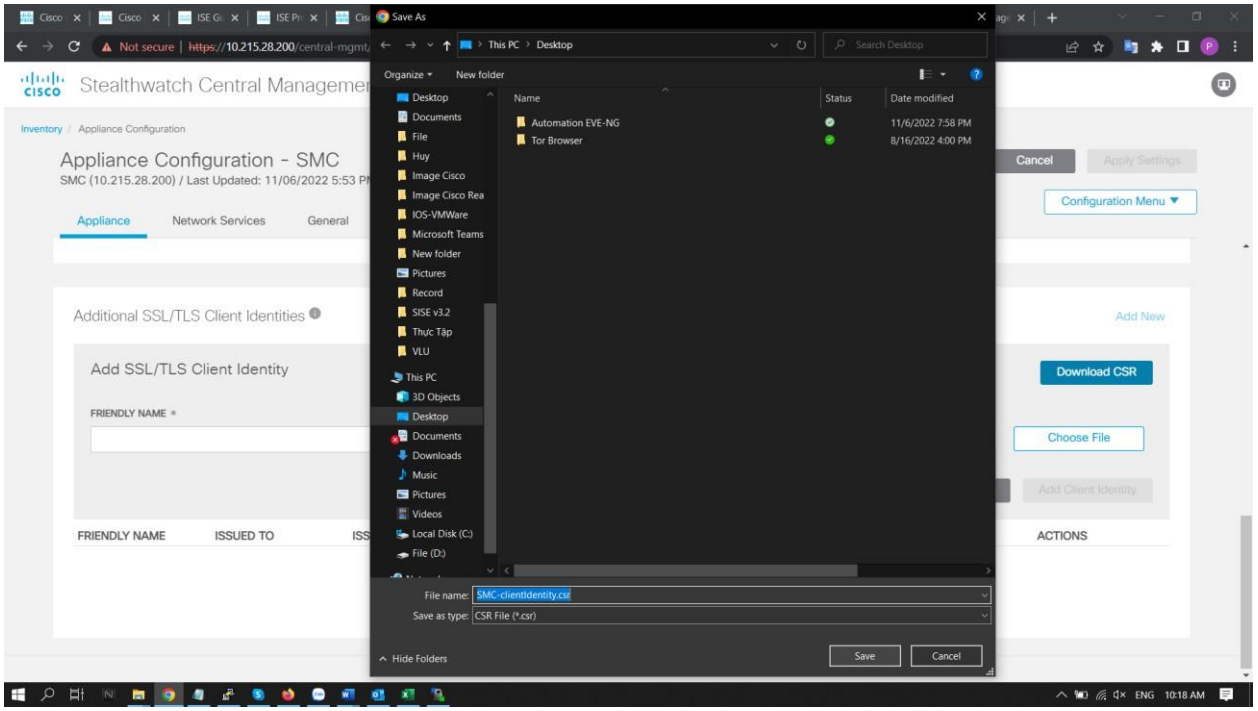
1.6 : Ta tiến hành Generate CSR theo mẫu ví dụ bên dưới, sau đó click Generate CSR:

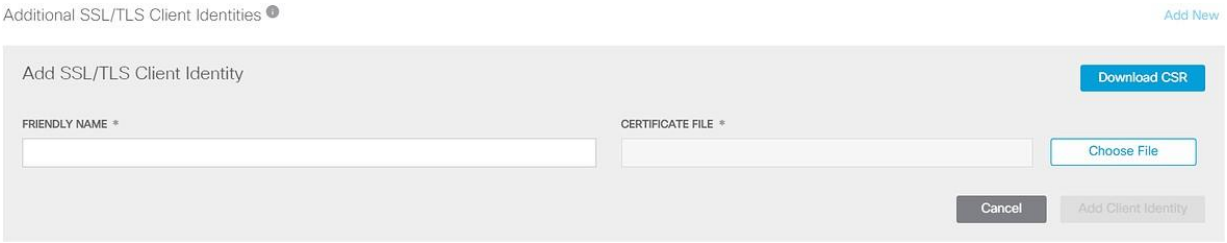




1.7: Tiếp theo tại Additional SSL/TLS Client Identities ta click vào biểu tượng Download CSR.







✓ Sau khi có được 1 CSR file từ Stealthwatch ta tiến hành thực hiện bước tiếp

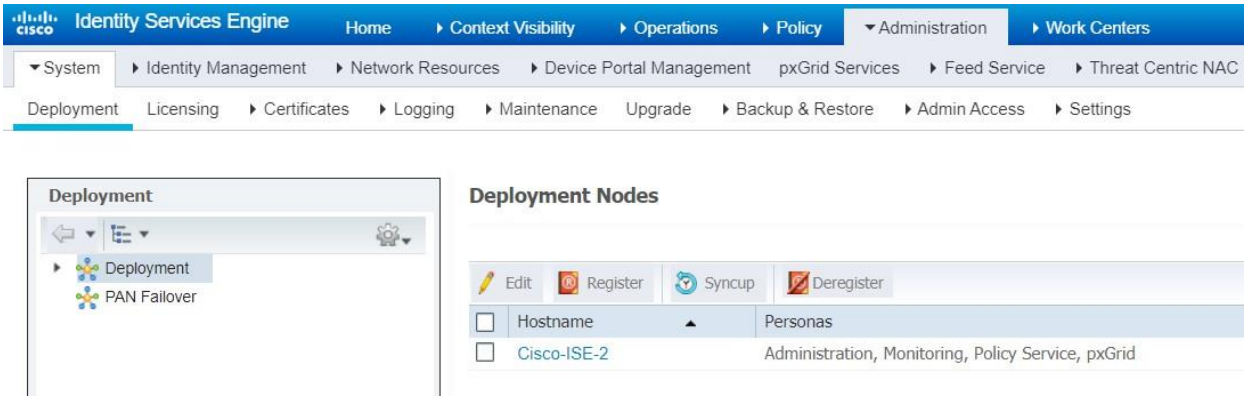
theo là đưa CSR file này vào Cisco ISE để Cisco ISE có thể tạo ra 1 chứng

chỉ (Certificate) phản hồi có đuôi .cer lại cho Stealthwatch với mật khẩu của chứng chỉ phản hồi này sẽ được thiết đặt trên Cisco ISE.

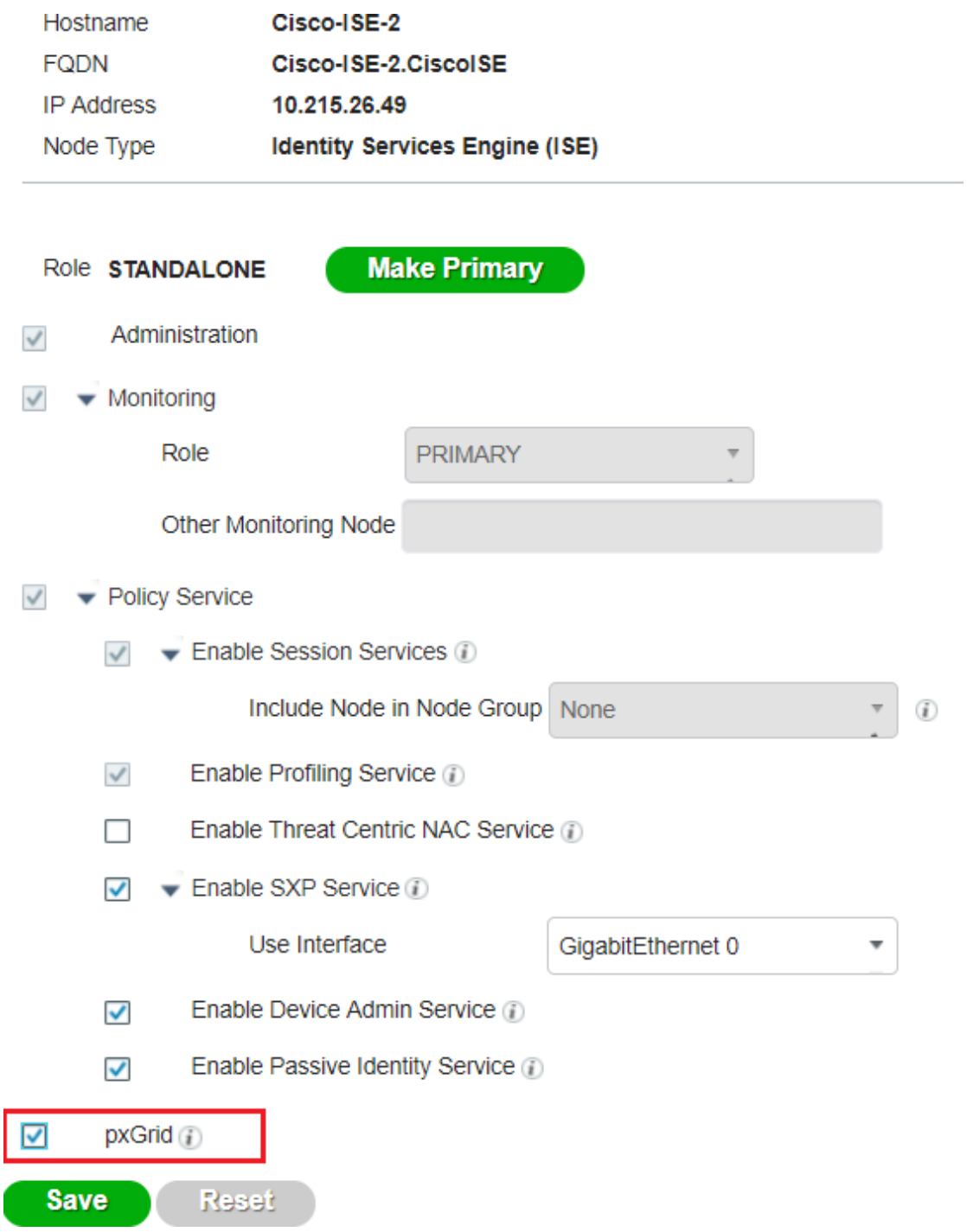
Bước 2:

2.1 : Ta đăng nhập vào Cisco ISE Management Interface.

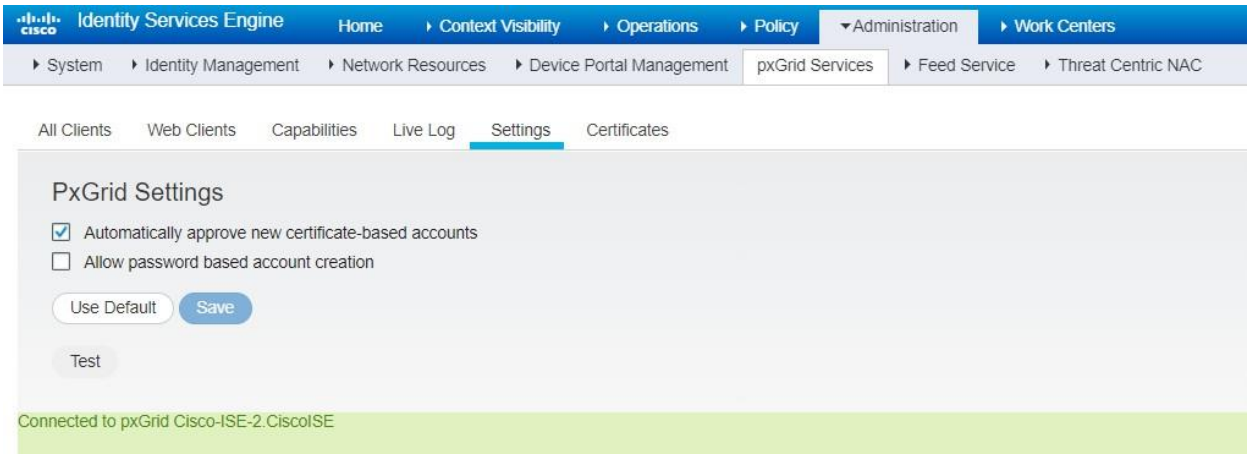
2.2 : Tiến hành vào Cisco ISE để bật PxGrid cho phép Stealthwatch giao tiếp với Cisco ISE thông qua giao thức này: ta vào Administration → System → Deployment.



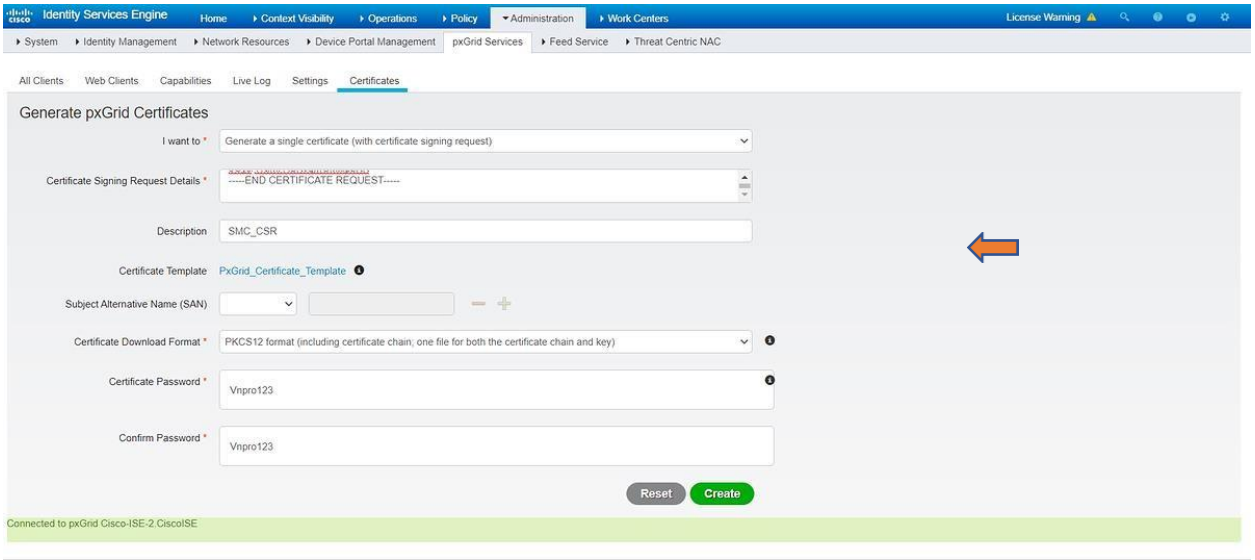
✓ Ta click vào Cisco-ISE-2 → tick vào box PxGrid và click Save.



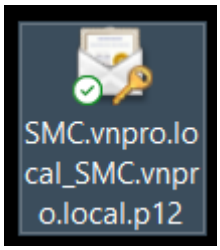
2.3 : Tiếp theo ta tiến hành vào Administration/ PxGrid Services/ Settings và tick vào box Automatically approve new certificate-based accounts/ Save.



2.4 : Sau đó tiến hành tạo Certificate: di chuyển đến Administration / PxGrid Services / Certificates.(Ta tiến hành điền vào mẫu như bên dưới sau đó click Create). Với thông tin trong mục Certificate Signing Request Details là nội dung của file .csr vừa download ở bước trên.



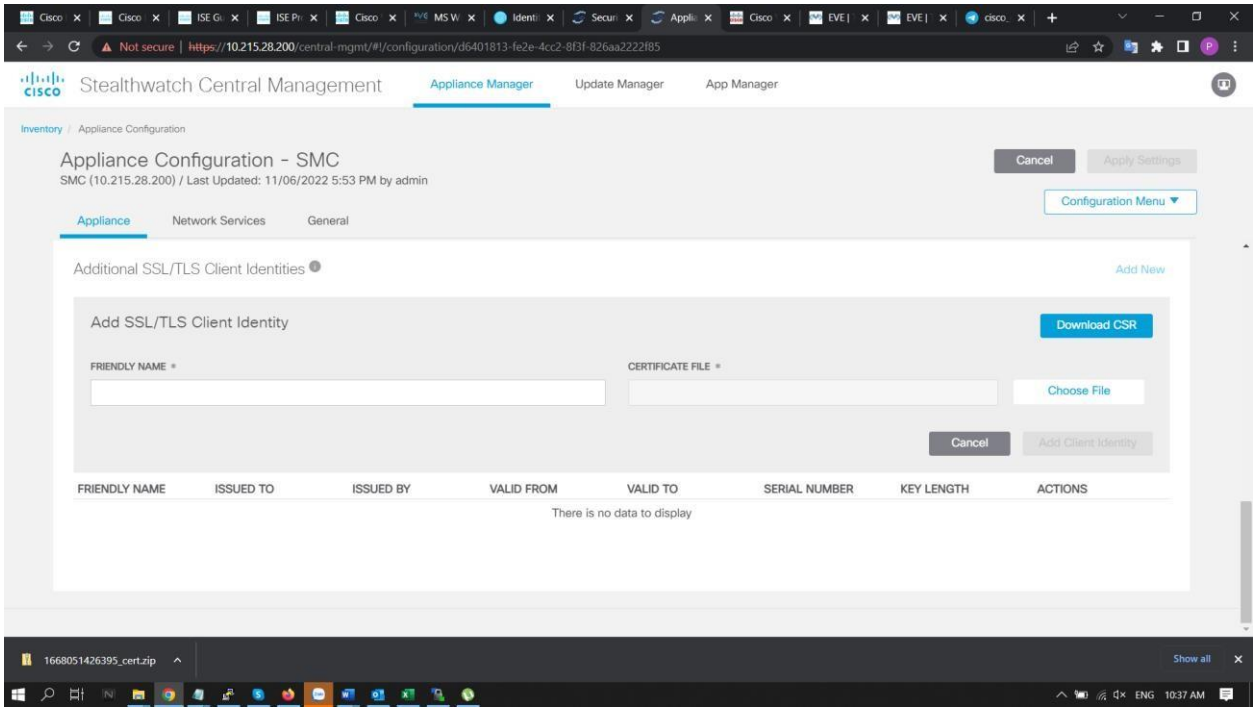
✓ Sau khi click Create ta lập tức được file dạng .zip, giải nén file .zip được 1 file dạng .p12

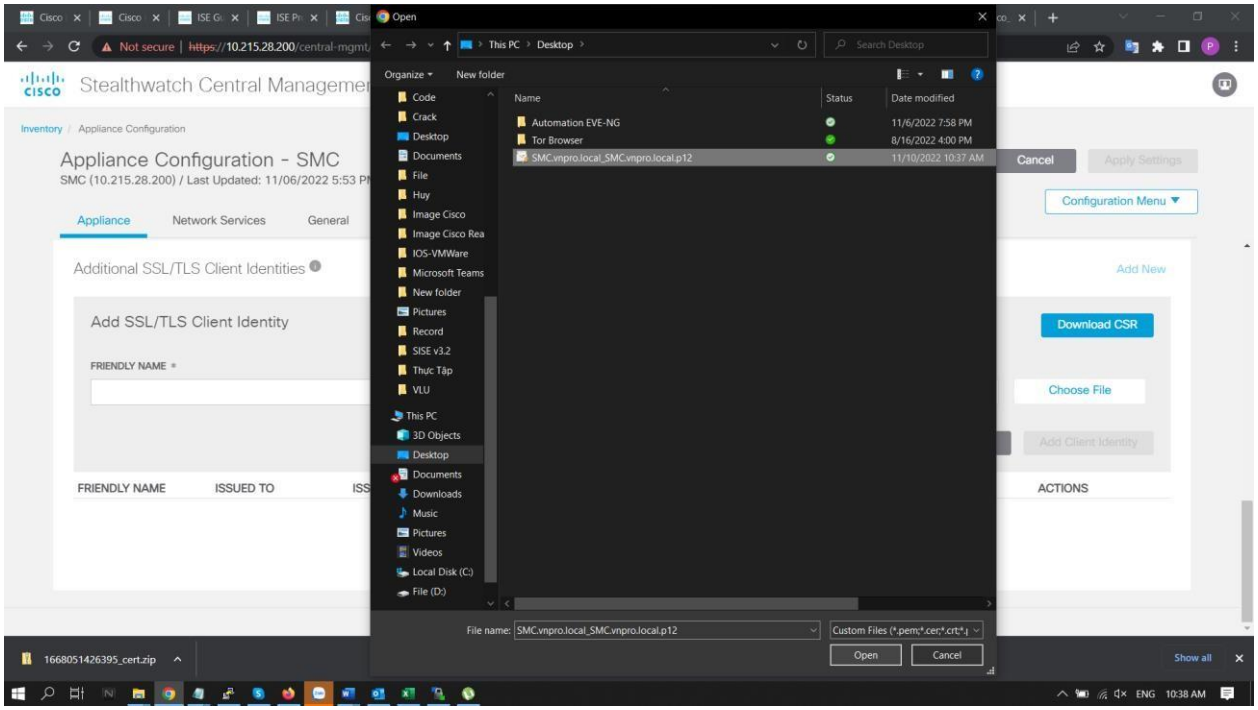


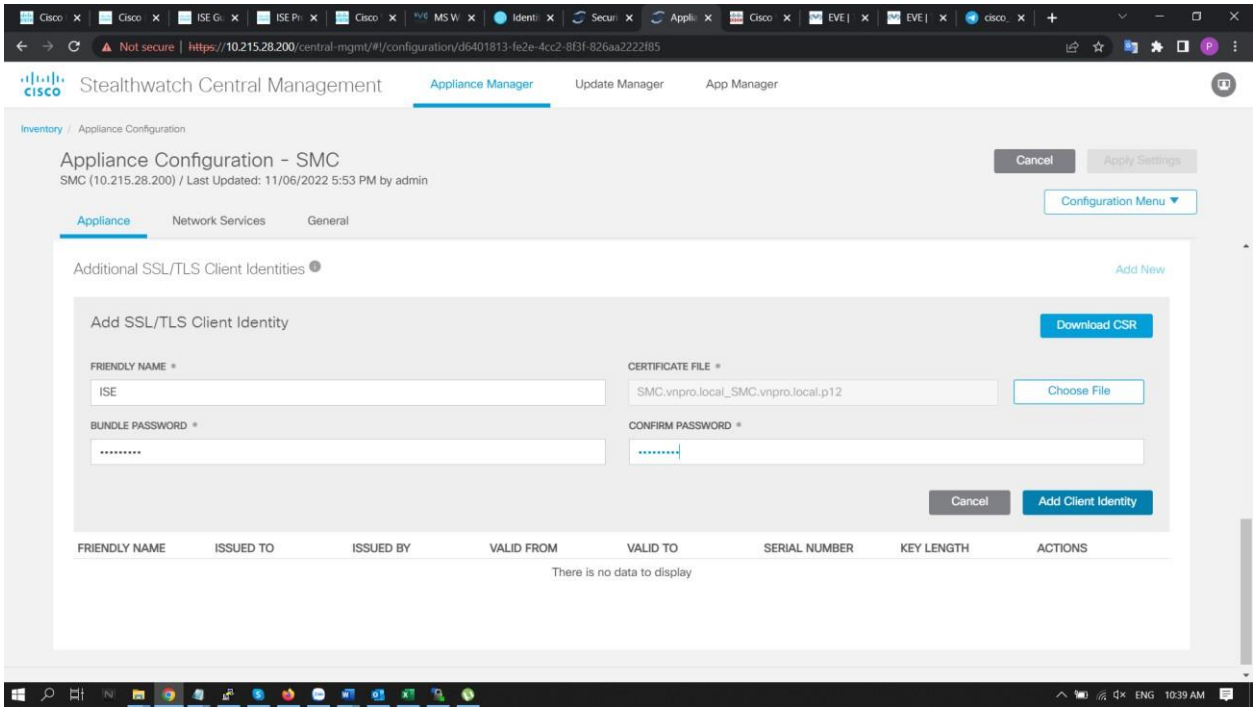
✓ Sau khi ta có được Certificate Request từ Cisco ISE thì lúc này ta tiến hành đưa file .p12 trên vào Stealthwatch để Stealthwatch có thể thêm Cisco ISE vào SSL/TLS Client Identities của mình

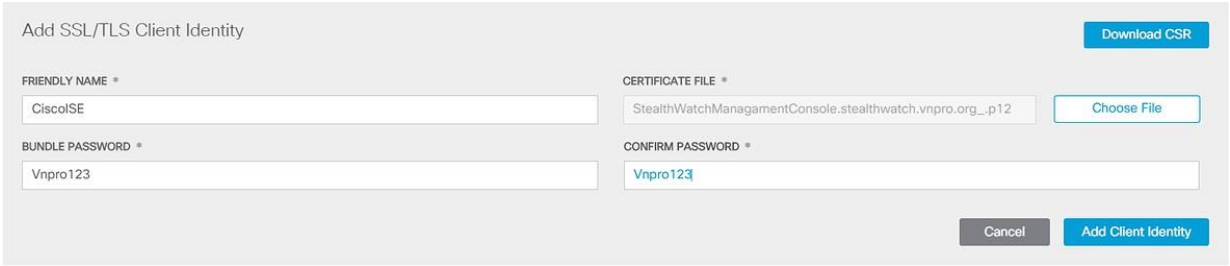
Bước 3:

3.1 : Quay trở lại màn hình của bước 1.7 ta tiến hành chọn Choose File, sau đó chọn đường dẫn đến file mà ta đã giải nén có đuôi .p12 đã giải nén ở bước 2.4 vào, sau đó tiến hành điền password mà ta đã nhập ở bước 2.4 và click Add Client Identity:

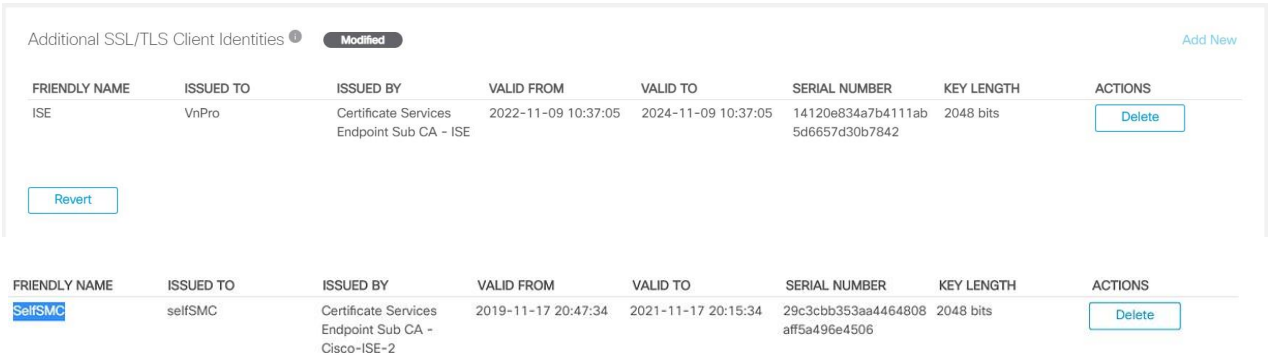



Stealthwatch Central Managemer
Appliance Configuration - SMC
SMC (10.215.28.200) / Last Updated: 11/06/2022 5:53 PM
Appliance
Network Services
General
Additional SSL/TLS Client Identities
Add SSL/TLS Client Identity
FRIENDLY NAME *
FRIENDLY NAME
ISSUED TO
ACTIONS
Cancel
Apply Settings
Configuration Menu
Add New
Download CSR
Choose File
Add Client Identity
Open
This PC > Desktop
Search Desktop
Organize
New folder
Name
Status
Date modified
Automation EVE-NG
11/6/2022 7:58 PM
Tor Browser
8/16/2022 4:00 PM
SMC.vnpro.local_SMC.vnpro.local.p12
11/10/2022 10:37 AM
File name: SMC.vnpro.local_SMC.vnpro.local.p12
Custom Files (*.pem;*.cer;*.crt;*.
Open
Cancel
1668051426395_cert.zip
Show all
ENG 10:38 AM


Not secure | https://10.215.28.200/central-mgmt/#!/configuration/d6401813-fe2e-4cc2-8f3f-826aa2222f85
Stealthwatch Central Management
Appliance Manager
Update Manager
App Manager
Inventory / Appliance Configuration
Appliance Configuration - SMC
SMC (10.215.28.200) / Last Updated: 11/06/2022 5:53 PM by admin
Cancel
Apply Settings
Configuration Menu
Appliance
Network Services
General
Additional SSL/TLS Client Identities
Add New
Add SSL/TLS Client Identity
Download CSR
FRIENDLY NAME *
ISE
CERTIFICATE FILE *
SMC.vnpro.local_SMC.vnpro.local.p12
Choose File
BUNDLE PASSWORD *
CONFIRM PASSWORD *
Cancel
Add Client Identity
FRIENDLY NAME
ISSUED TO
ISSUED BY
VALID FROM
VALID TO
SERIAL NUMBER
KEY LENGTH
ACTIONS
There is no data to display
ENG 10:39 AM


Add SSL/TLS Client Identity
Download CSR
FRIENDLY NAME *
CiscoISE
CERTIFICATE FILE *
StealthWatchManagamentConsole.stealthwatch.vnpro.org_.p12
Choose File
BUNDLE PASSWORD *
Vnpro123
CONFIRM PASSWORD *
Vnpro123
Cancel
Add Client Identity

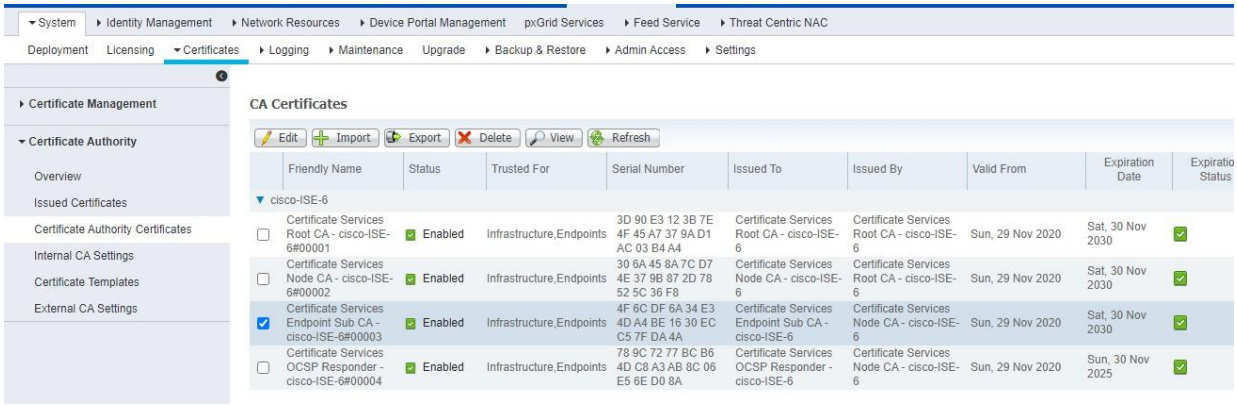
3.2 : Tiếp theo ta tiến hành click Apply Change và thu được kết quả như sau:



✓ Sau khi hoàn tất bước 3 lúc này ta vào lại Cisco ISE để có thể lấy Certificate có đuôi .pem, khi có file Cert từ Cisco ISE chúng ta có thể quay lại Trust Store của Stealthwatch và thêm Cisco ISE vào Trust Store của mình thông qua file .pem mà Cisco ISE đã cung cấp.

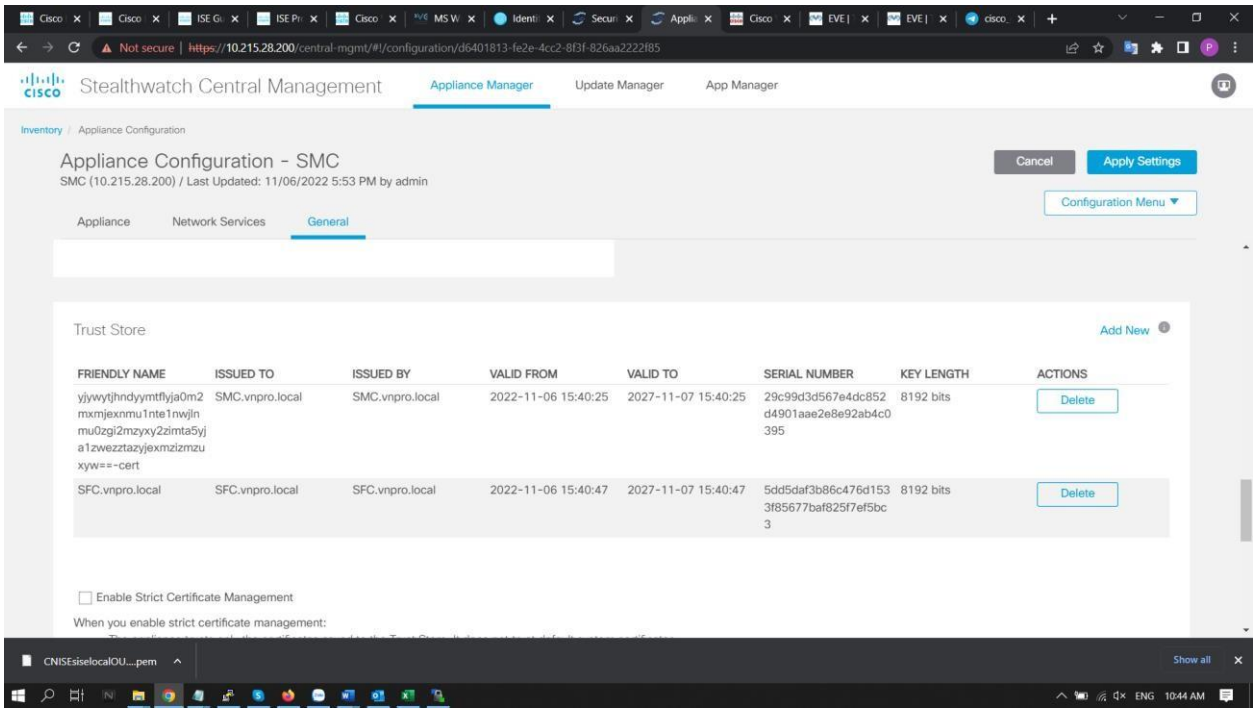
Bước 4:

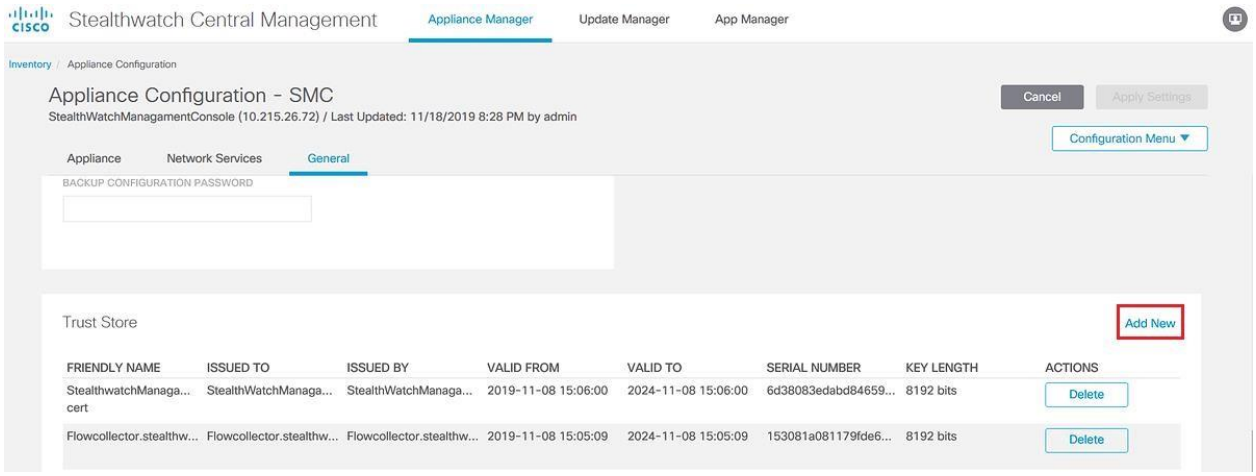
4.1 : Tại giao diện Cisco ISE, ta di chuyển vào Administration > System > Certificates, chọn tiếp tục Certificate Authority và click Certificates Authority Certificates. Tại đây ta chọn Certificate Services Endpoint Sub CA - cisco-ISE và Click Export.



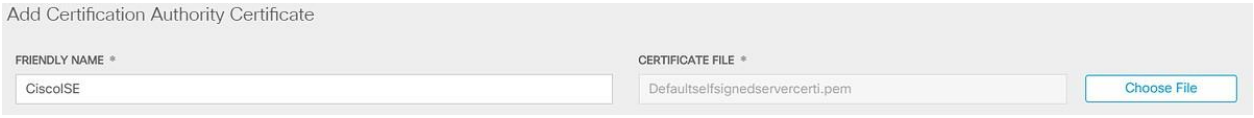
✓ Sau khi click Export ta được popup để tải về 1 file .pem (Lưu ý trình duyệt web cho phép bật popup để tải file)

4.2 : Tại Appliance Configuration – SMC ta chuyển sang tab General như hình bên dưới và click Add New tại mục Trust Store:

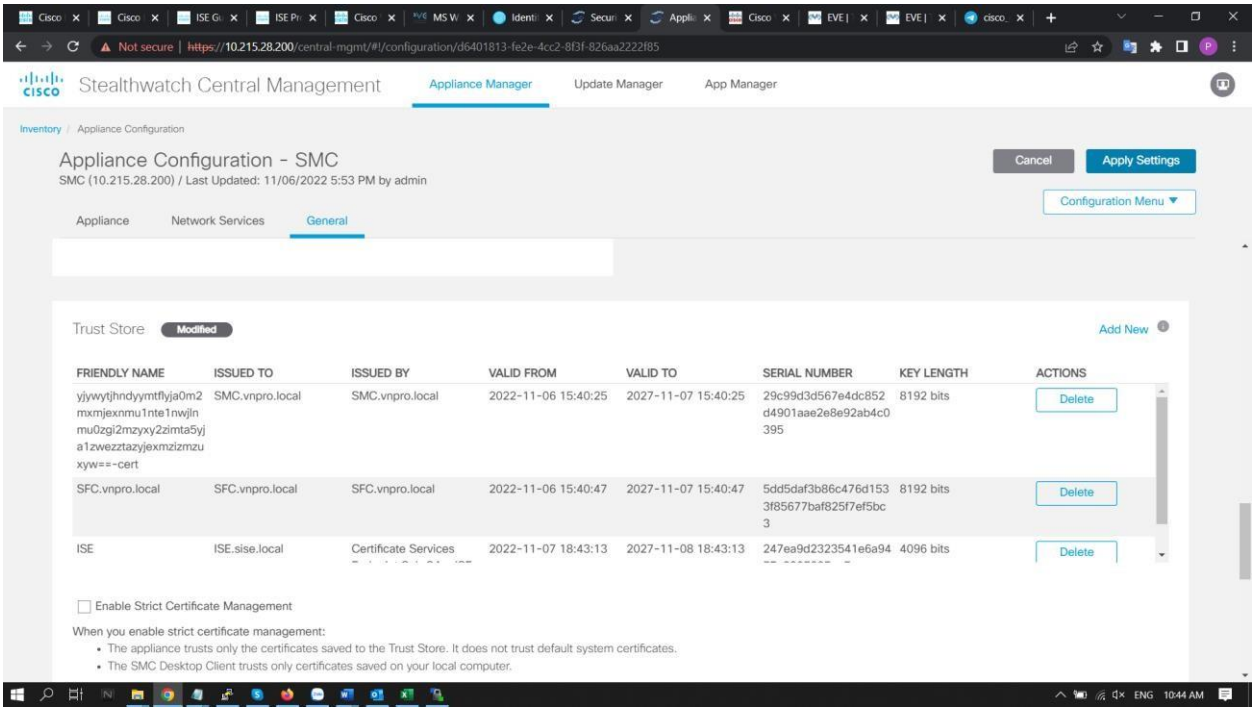


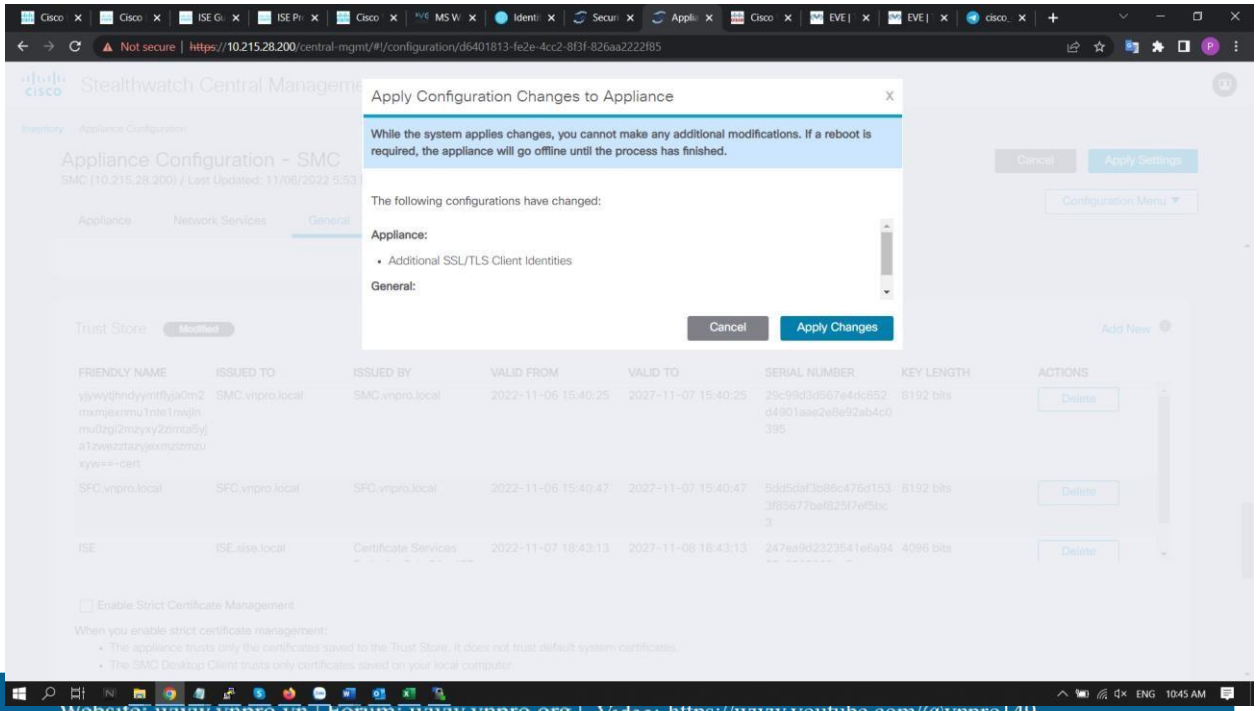


4.3 : Ta điền Friendly Name sau đó click Choose File để chọn file mà ta đã Export ở bước 4.1.

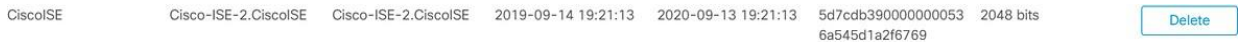


4.4 : Click Apply Changes, sau đó chờ quá trình thiết đặt cấu hình hoàn thành.





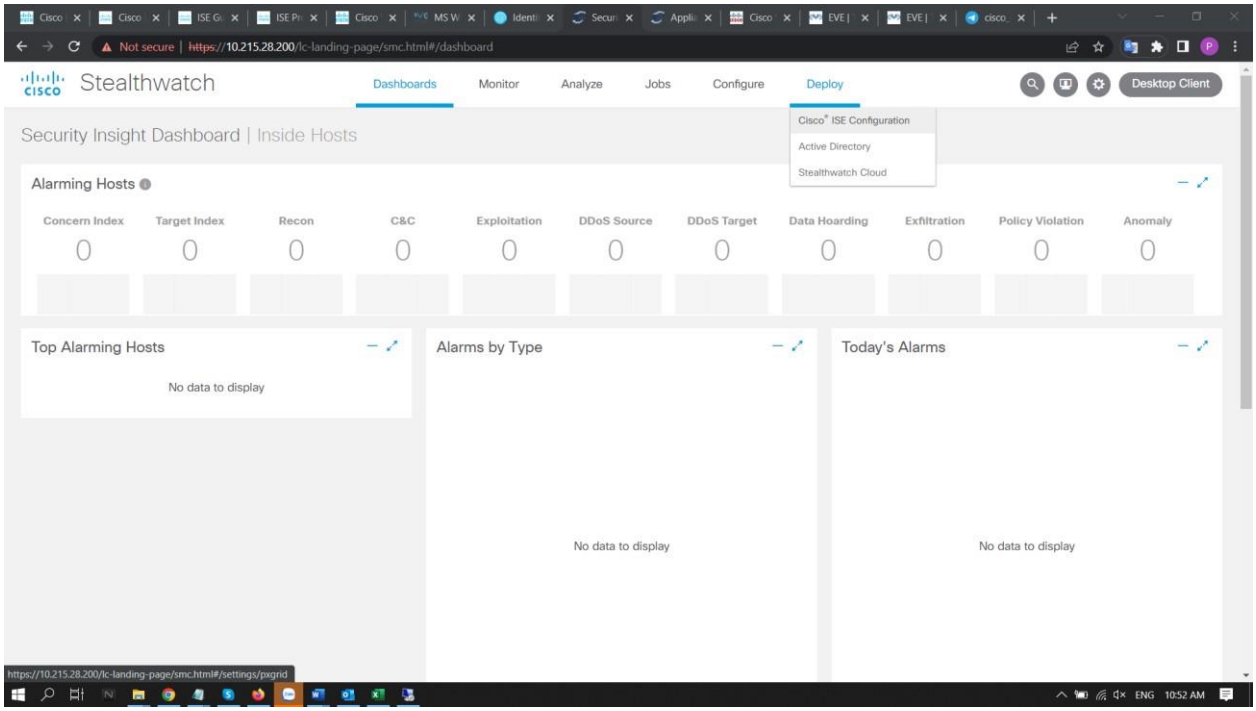
✓ Sau khi hoàn tất bước 4.4 thì tại tab General của Stealwatch Central Management ở mục Trust Store sẽ thấy Cisco ISE đã được thêm vào:

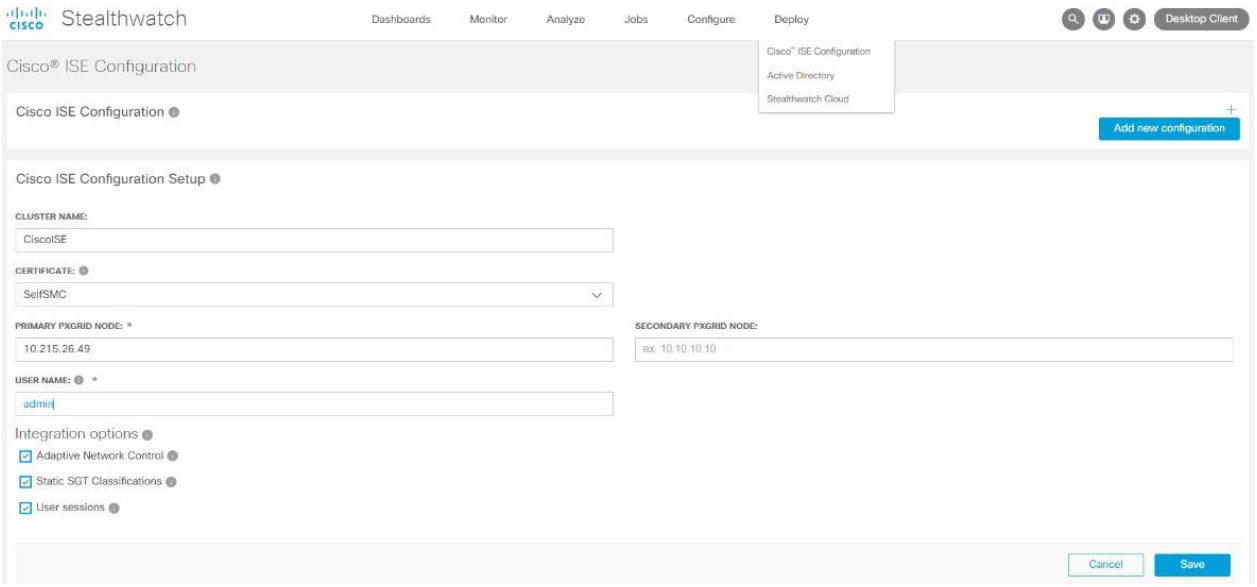


✓ Sau khi đã hoàn tất bước 4 chúng ta tiến hành Cisco ISE Configuration vào Stealthwatch SMC.

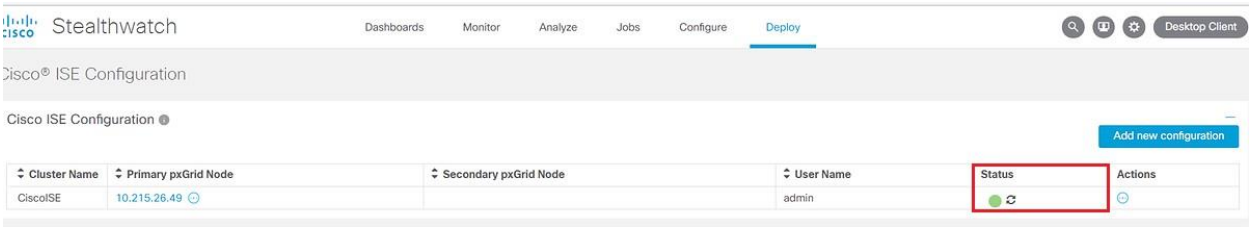
Bước 5:

5.1 : Ta quay trở lại giao diện của Stealthwatch Management Console: Chọn Deploy → Cisco ISE configuration → click Add new configuration, Ta điền thông tin name, chọn Certificate, điền IP của Cisco ISE, điền username và click Save.

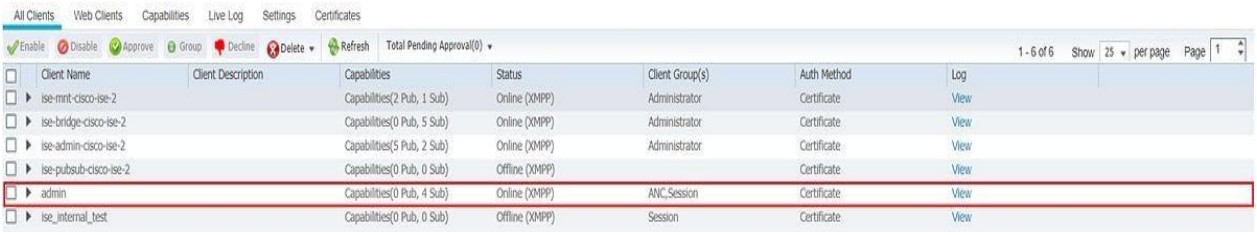




✓ Ta chờ quá trình thiết đặt hoàn tất. sau khi hoàn tất bước 5.1 trên SMC ta vào Deploy → Cisco ISE Configuration sẽ thấy được trang thái tại tab Status thì Active như sau:



5.2 : Trên Cisco ISE ta vào Administration → PxGrid Services để kiểm tra xem Cisco ISE đã có thể giao tiếp với Stealthwatch qua giao thức PxGrid hay chưa.



✓ Ta đã thấy được Client name “admin” mà chúng ta đã tạo tại bước 5.1 trên stealthwatch SMC.

✓ Sau khi hoàn thành bước 5.2 thì chúng ta đã có thể thấy được rằng lúc này cả Cisco ISE và Stealthwatch đều có thể thấy nhau thông qua giao thức PxGrid.

Tiếp theo, chúng ta sẽ tiến hành thực nghiệm quá trình trao đổi thông tin về người dùng giữa Cisco ISE và Stealthwatch thông qua cấu hình **Wired Dot1x** và **Flexible NetFlow.**

Bước 1: Thực hiện cấu hình Dot1x trên switch để thực hiện xác thực giữa switch-client (máy tính Windows) và xác thực Radius giữa switch-Cisco ISE.

- ✓ Đầu tiên trên các cổng của switch cấu hình đưa về mode access và đặt ip cho interface vlan 1

```
SW1(config)#int range g0/0-2
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#exit
```

```
SW1(config)#int vlan 1
SW1(config-if)#ip add 10.215.26.85 255.255.255.0
SW1(config-if)#no shut
```

```
SW1#show ip int bri
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
```

Vlan1 10.215.26.85 YES manual up up

```
SW1#show vlan bri

VLAN Name                        Status    Ports
---- ----------------------------------------------------------------
1    default                     active    Et0/0, Et0/1, Et0/2, Et0/3
1002 fddi-default                act/unsup
1003 token-ring-default          act/unsup
1004 fddinet-default             act/unsup
1005 trnet-default               act/unsup
```

```
SW1(config)#aaa new-model
SW1(config)#aaa authentication dot1x default group radius
SW1(config)#dot1x system-auth-control
SW1(config)#int g0/1
SW1(config-if)#dot1x port-control auto
SW1(config-if)#dot1x pae authenticator
SW1(config-if)# authentication host-mode multi-auth
SW1(config)#radius-server host 10.215.26.49
SW1(config)#radius-server key Vnpro123
```

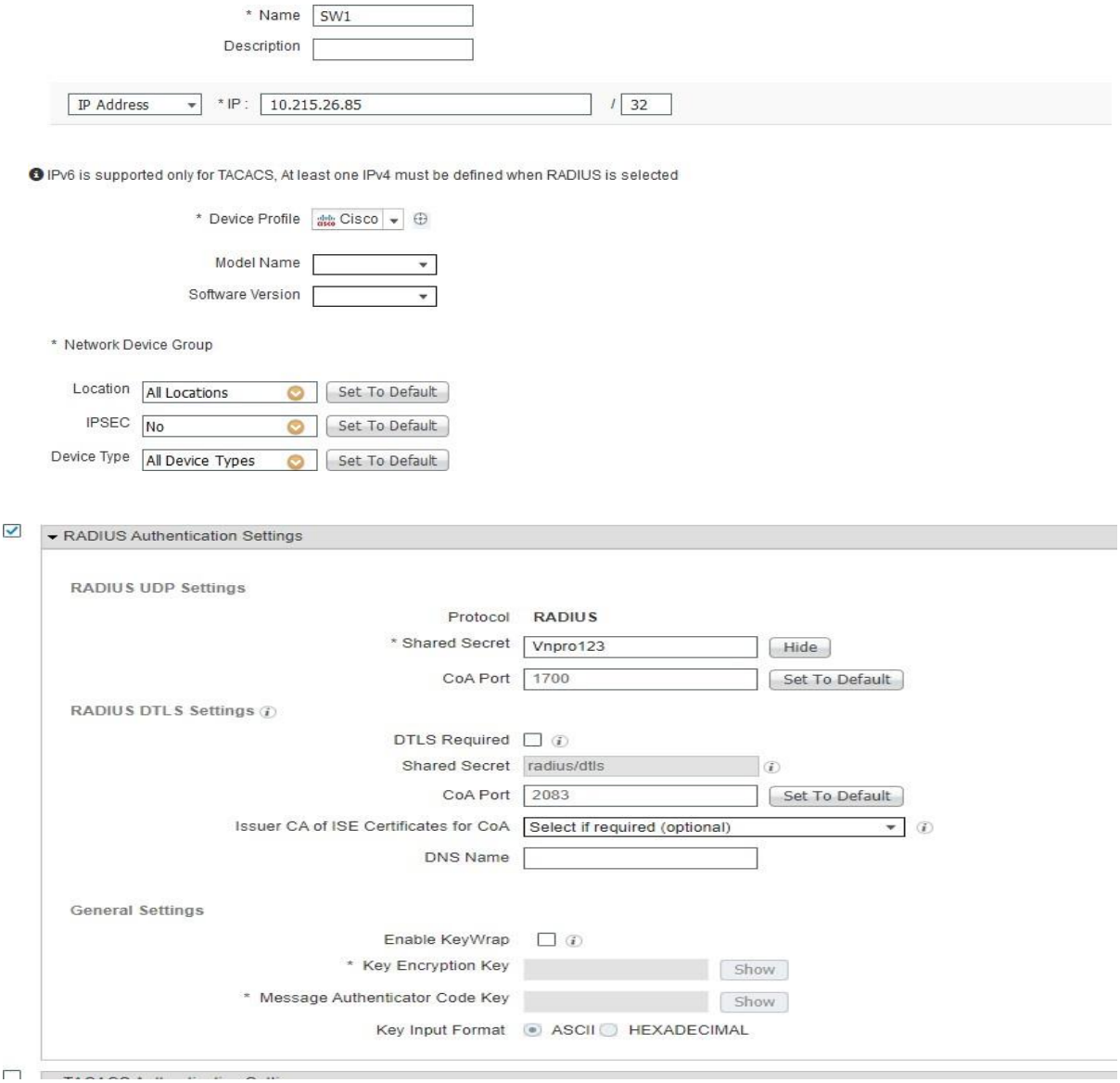
Cấu hình địa chỉ ip cho cổng e0/0 của R1 và trỏ default route về đám mây của

Vnpro.

```
R1(config)#int g0/0
R1(config-if)# ip address 10.215.26.88 255.255.255.0
R1(config)# ip route 0.0.0.0 0.0.0.0 10.215.26.1
```

- ✓ Tiếp theo, chúng ta tiếp tục thực hiện tạo policy và chỉ định Switch cho cisco ISE chứng thực.
- ✓ Chúng ta tiến hình thực hiện cấu hình cisco theo dãy hình bên dưới.

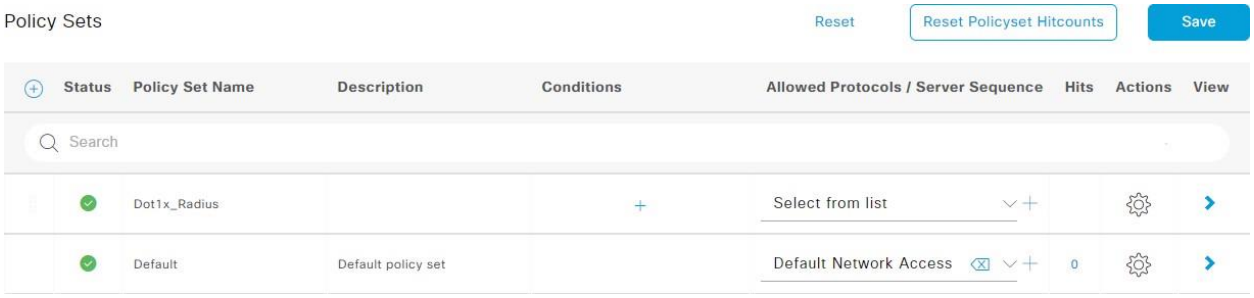
- ✓ Chuyển hướng đến Administration / Network Resources / Network Devices
- ✓ Name: SW1
- ✓ IP: 10.215.26.85/32
- ✓ Click vào RADIUS: và điền share secret

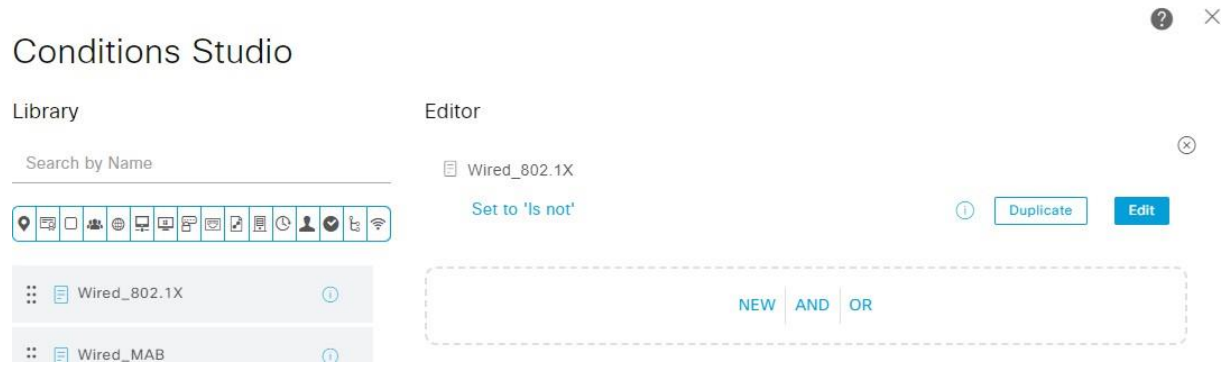


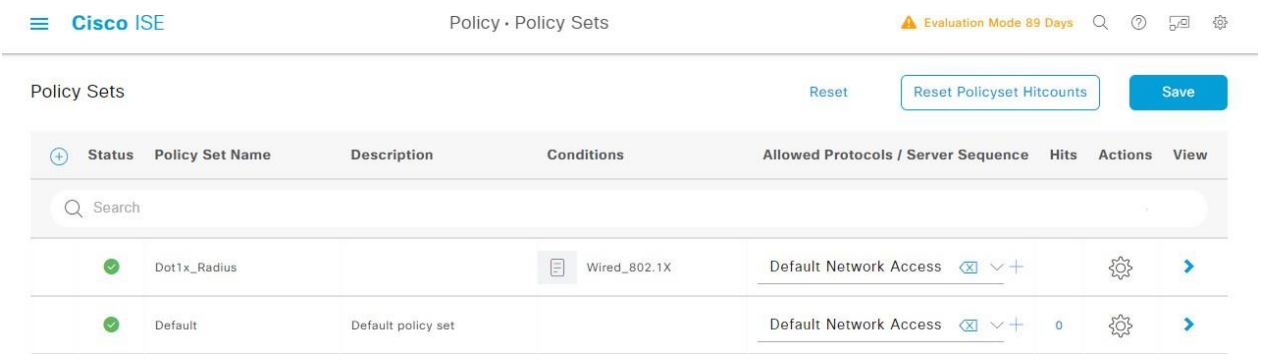
✓ Tiếp tục chúng ta set policy dot1x và radius trên cisco ISE.Vào tab **Policy → Policy Sets**.

✓ Nếu chưa tạo Policy cho wired dot1x thì click vào vòng khoanh đỏ → điền **policy name** → Trong mục **condition** bấm vào dấu + hoặc **dấu cây bút** → kéo thả như ảnh dưới đây.

✓ Tạo một policy mới: Dot1x_Radius

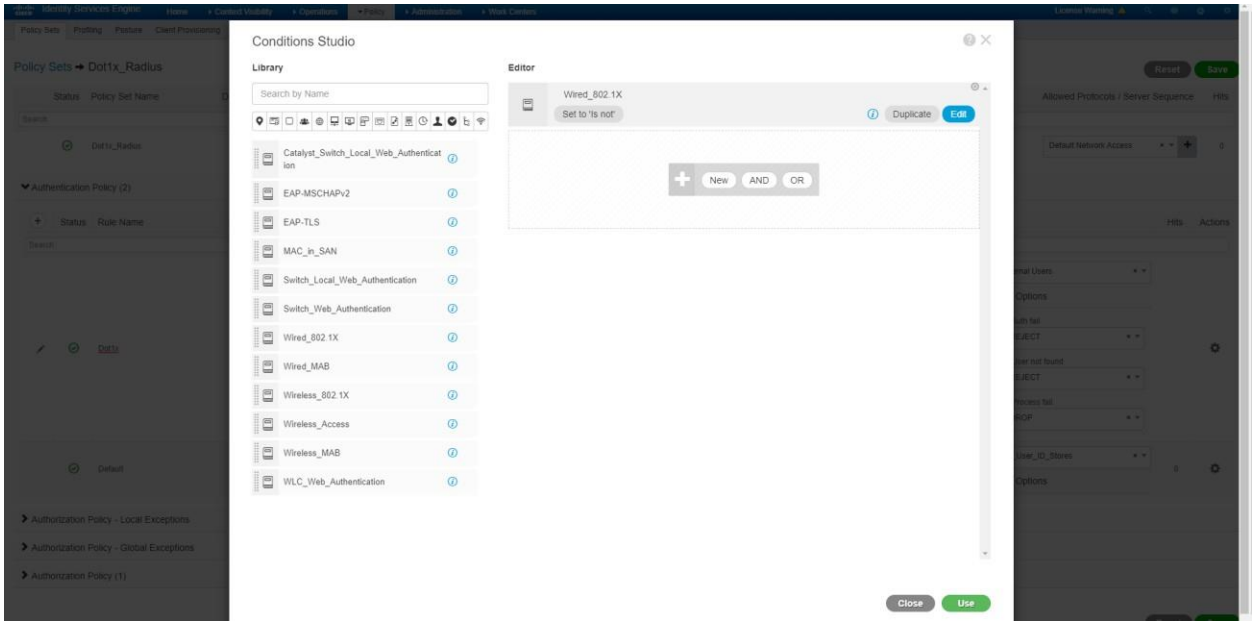




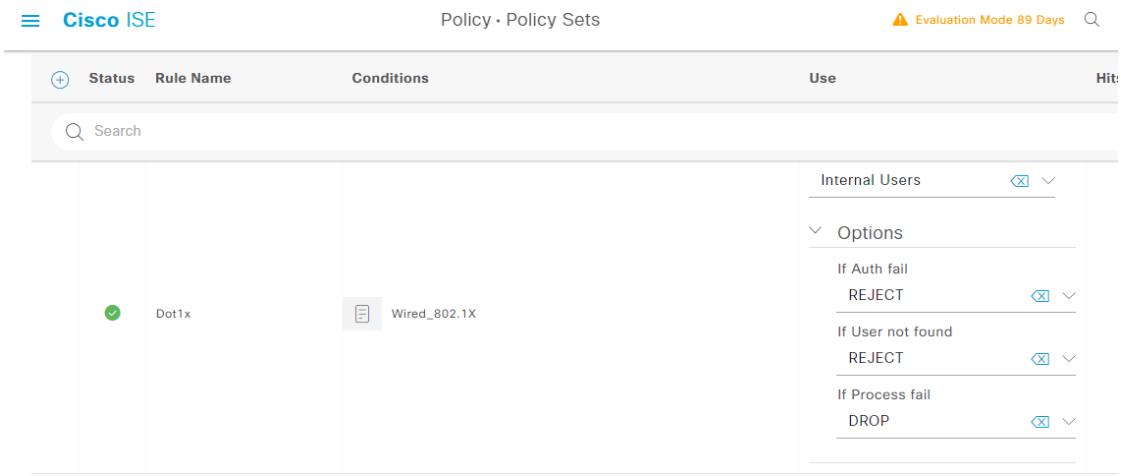


✓ Chọn Use, sau đó bấm vào mũi tên ở cuối hàng.

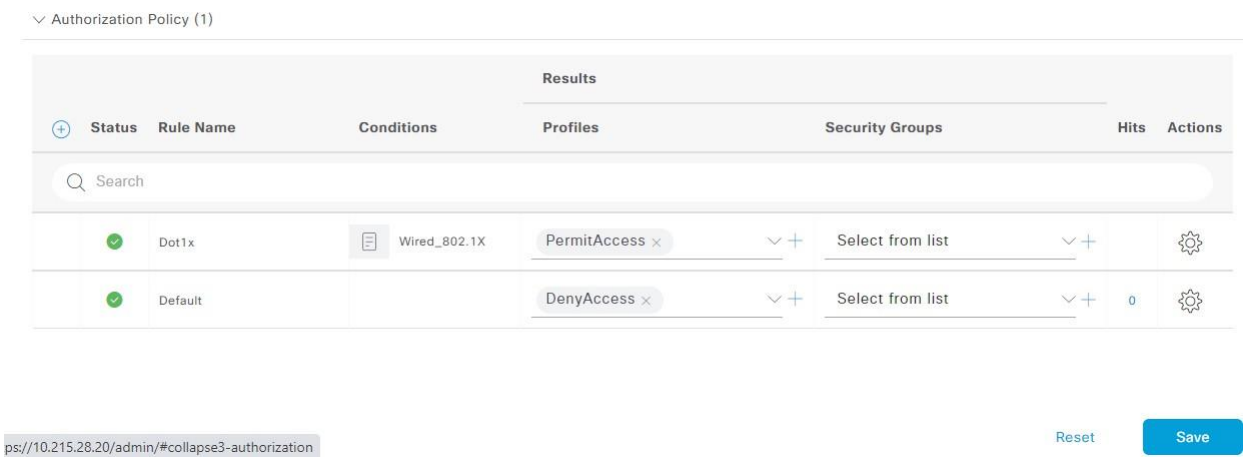
Trong mục **Authentication Policy** → Tick chọn dấu **"+"** để add policy → Trong mục **Condition** kéo thả mục **wired_802.1X** từ bên trái qua bên phải như ảnh dưới đây → Chọn **Use**.



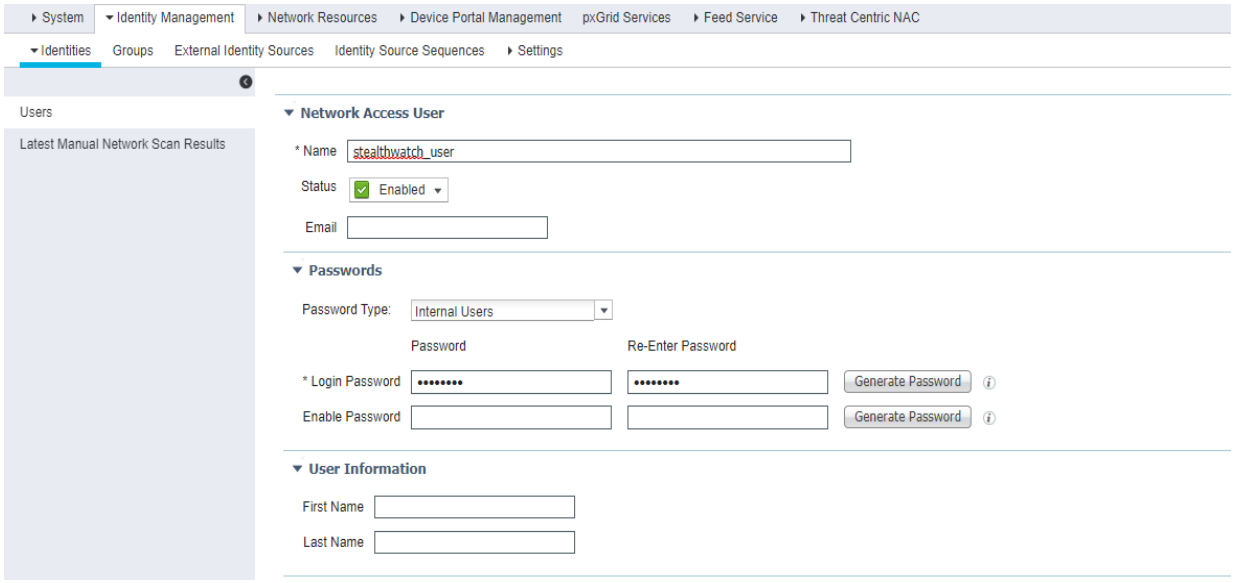
- ✓ Chúng ta có thể điều chỉnh các option để hiệu chỉnh cho việc xác thực, chẳng hạn nếu xác thực fail thì sẽ REJECT.



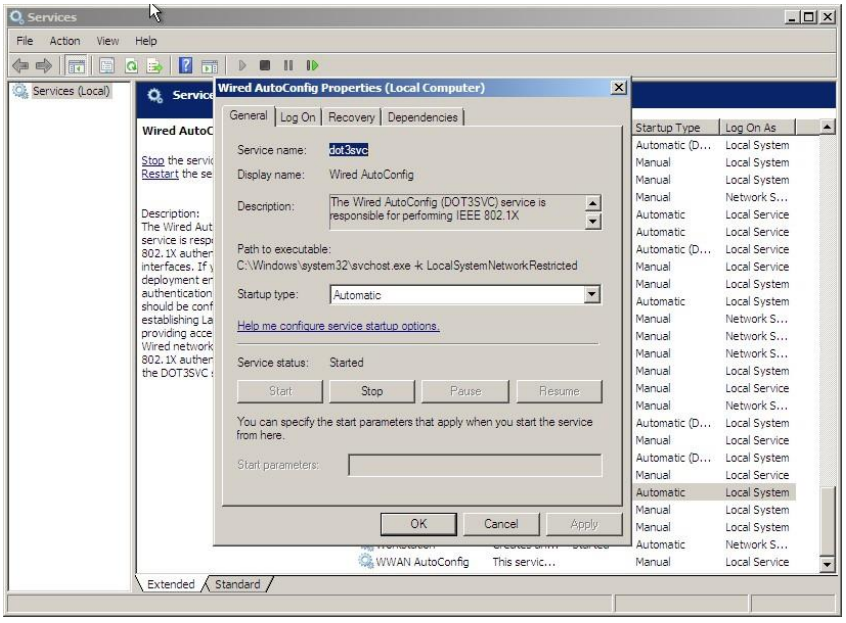
- ✓ Chúng ta tiếp tục set policy Authorization.Thực hiện như ảnh dưới đây.



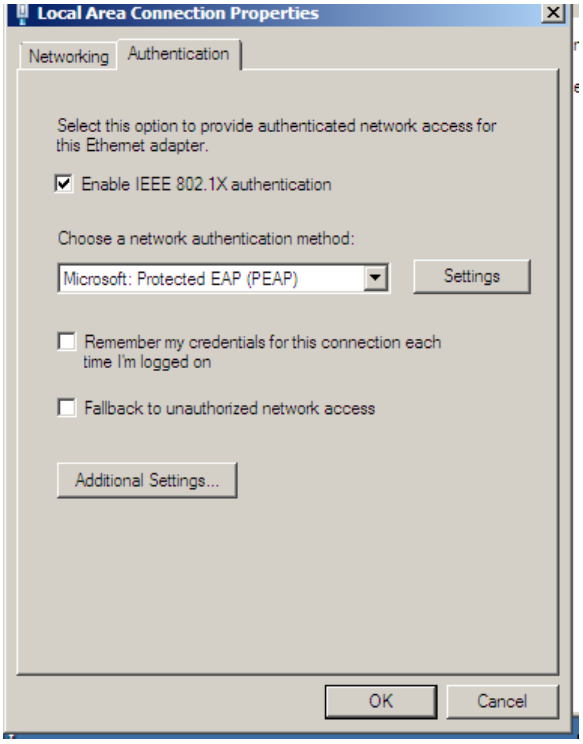
Như vậy chúng ta đã set xong policy. Bây giờ chúng ta tiến hành tạo user trên cisco ISE → **Chọn tab Administration → Identity Management → Identities**. Chúng ta tiến hành tạo user như 2 ảnh dưới đây.



- ✓ Như vậy chúng ta đã tạo được user và set policy cho wired dot1x trên Cisco ISE.
- ✓ Trên PC chúng ta tiến hành điều chỉnh card mạng cho việc xác thực dot1x. Đầu tiên, ta bấm tổ hợp phím Windows+R → services.msc → Tìm services Wired Autoconfig → Chuột phải chọn **Properties** → Trong tab **General** chọn các chỉ mục như ảnh dưới đây.

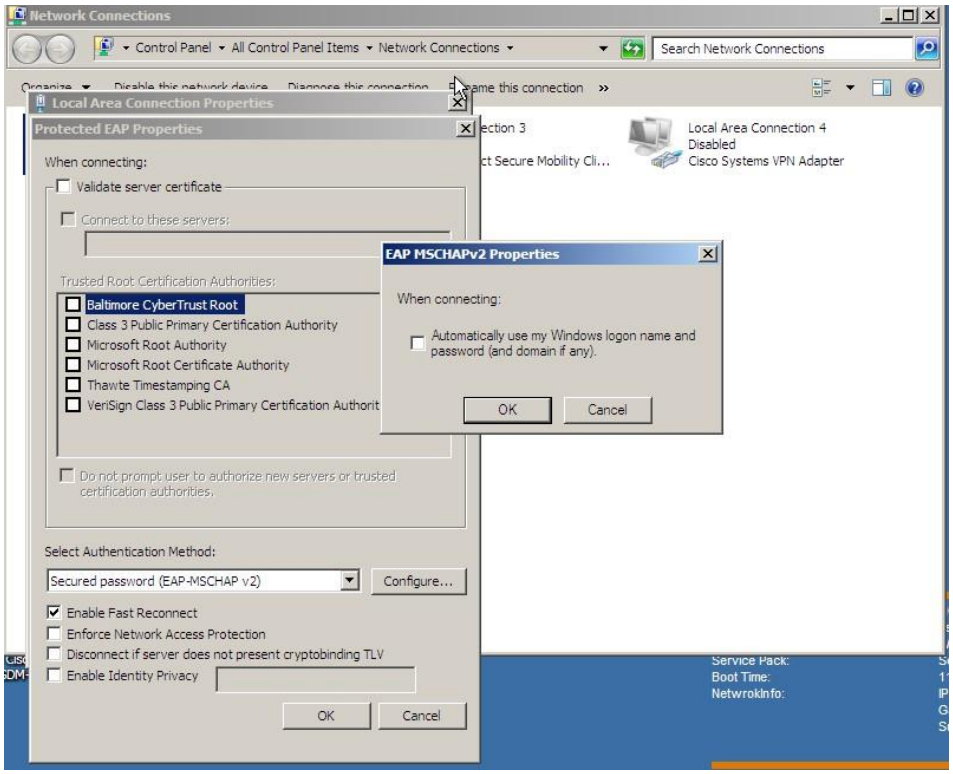


✓ Chuyển sang điều chỉnh card mạng, Chuột phải vào card mạng đang chạy → Properties → Trong tab Authentication tick chọn như ảnh dưới đây.

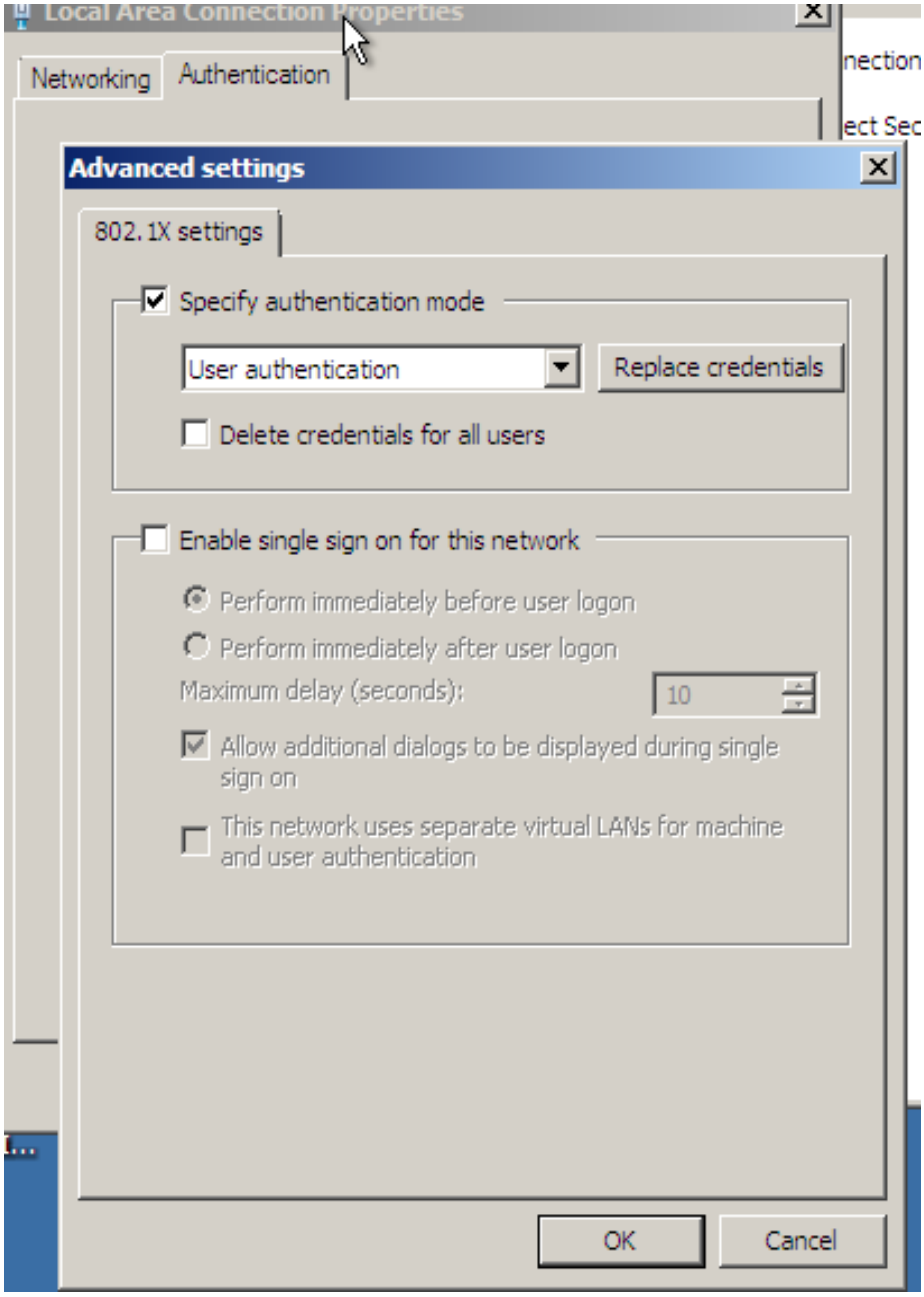


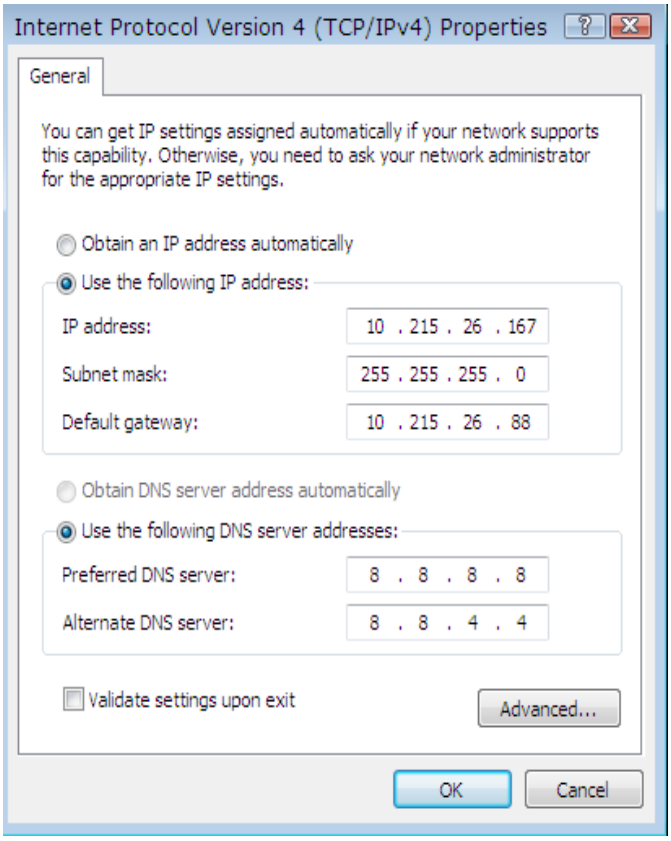
✓ Trong tab Choose a network authentication method Chọn Settings → Bỏ tick Validate server certificate (trong môi trường lab, chúng ta không cần windows xác thực chứng chỉ của Cisco ISE) → Trong mục Select Authentication Method Chọn Configure… → Bỏ tick Automatically use my Windows logon

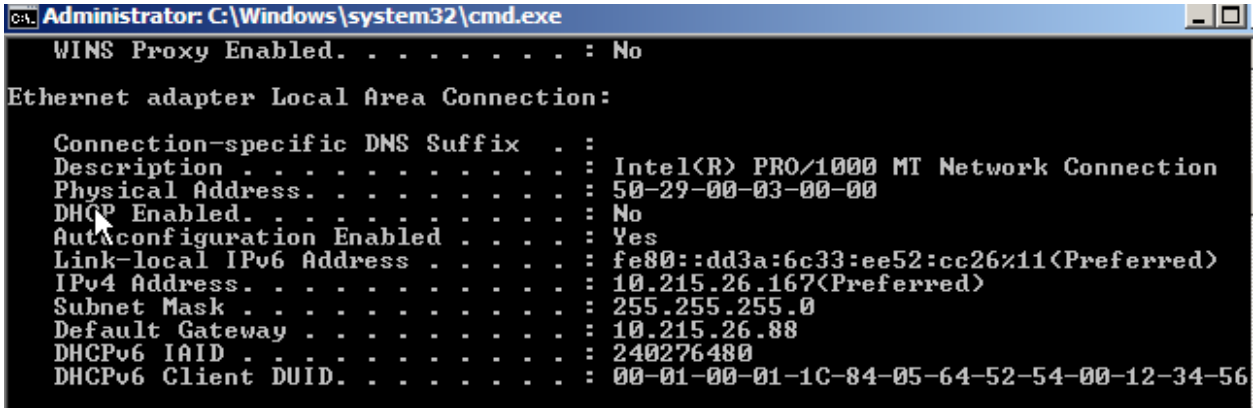
name and password (do chúng ta không dùng domain nên không cần dùng đến mục này) → Chọn Ok → Tiếp tục Ok để quay lại tab Authentication.



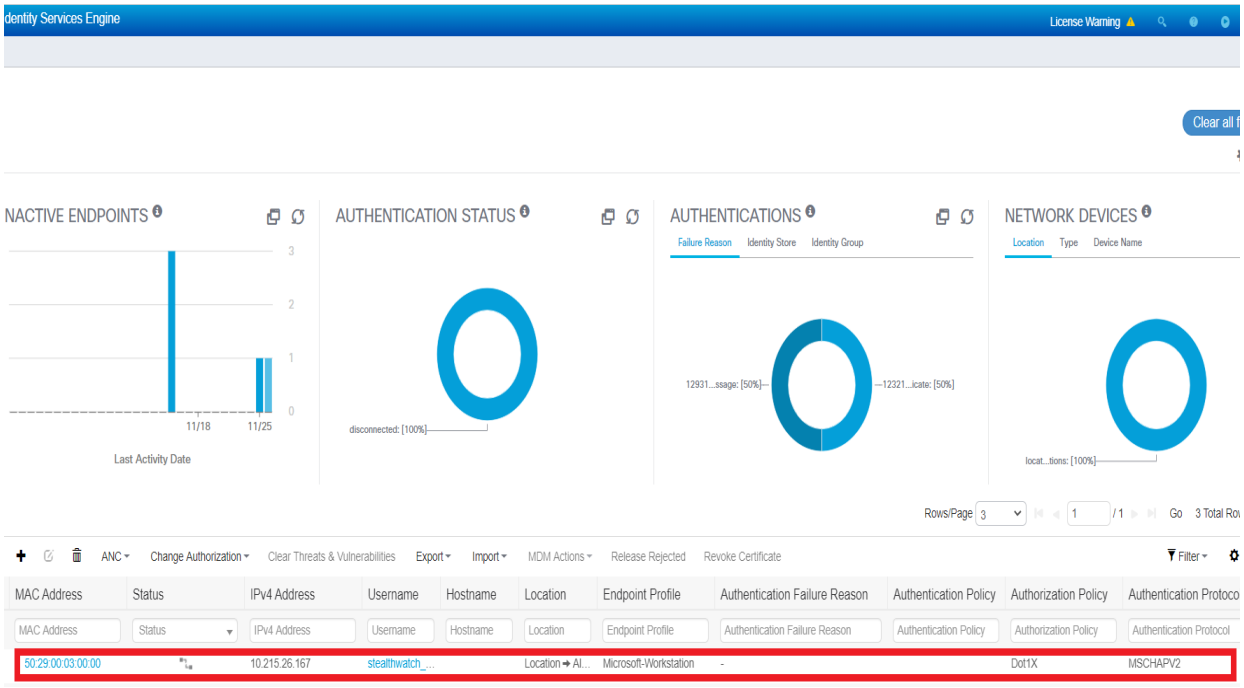
✓ Ta tiếp tục chọn Additional Settings… → Tick chọn Specify authentication mode → Chọn user authentication → Chọn Save/Replace credentials để nhập username/password đã tạo trên cisco ISE.


Local Area Connection Properties
Networking
Authentication
nection
ect Sec
Advanced settings
802.1X settings
Specify authentication mode
User authentication
Replace credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel





✓ Trên cisco ISE chúng ta có thể thấy PC đã xác thực thành công và truy cập được vào mạng.



Bước 2: Cấu hình Flexible netflow trên switch và router.

Trên R1:

Flow Record định nghĩa các thông tin Netflow, chẳng hạn như những packet trong flow. Nếu chúng ta muốn thiết lập 1 Flow Record tùy chỉnh, thì chúng ta sẽ sử dụng tổ hợp lệnh match và collect để chỉ định các thông tin cần gửi đi trong gói NetFlow PDU. “Match” sử dụng cho định nghĩa các flow chính(key flow), “Match” quyết định tính duy nhất của flow. “Collect” chỉ chỉ định những thông tin thêm-phụ trợ bao gồm việc cung cấp những chi tiết đến Stealthwatch FlowCollector để report và phân tích.

Những thông tin trong tổ hợp lệnh flow record bên dưới:

Tos : type of service.

TTL: time to live

Source port và destination port của gói TCP hoặc application chạy trên nền tcp.

Interface vào/ra (input/output).

Ngoài ra còn có thể cấu hình thêm những thông số quan trọng như *ipv4 source address*,*ipv4 destination address*….

```
R1(config)# flow record FLOW-RECORD
R1(config-flow-record)#description stealthwatch_router
R1(config-flow-record)# match ipv4 tos
R1(config-flow-record)# match ipv4 ttl
R1(config-flow-record)# match ipv4 protocol
R1(config-flow-record)# match transport tcp source-port
R1(config-flow-record)# match transport tcp destination-port
R1(config-flow-record)# match interface input
R1(config-flow-record)# match interface output
R1(config-flow-record)# collect transport tcp flags
R1(config-flow-record)# collect counter bytes long
R1(config-flow-record)# collect counter packets long
```

```
R1(config)# flow exporter FLOW-EXPORTER
/Trong destination cần trỏ về stealthwatch FlowCollector/
R1(config-flow-exporter)# destination 10.215.26.71
/source trong exporter chúng ta sẽ chọn cổng cần gửi thông tin về stealthwatch, đó là cổng e0/0 trên R1/
R1(config-flow-exporter)# source Ethernet0/0
/Stealthwatch sử dụng port 2055 để nhận flow/
```

```
R1(config-flow-exporter)# transport udp 2055
```

Flow monitor dùng để liên kết các flow exporter và record hay các cấu trúc khác của flexible netflow lại với nhau. Ngoài ra trong flow monitor, cấu hình *cache timeout* được khuyên dùng vì mặc định stealthwatch chỉ định thời gian này là 30 giây. Trong cấu hình này thời gian được tính bằng giây.

```
R1(config)# flow monitor FLOW-MON
R1(config-flow-monitor)# exporter FLOW-EXPORTER
R1(config-flow-monitor)# cache timeout inactive 60
R1(config-flow-monitor)# cache timeout active 15
R1(config-flow-monitor)# record FLOW-RECORD
```

- ✓ Sau đó chúng ta cần cho phép các cấu hình netflow trên từng cổng mà chúng ta cần phân tích flow.

```
R1(config)# interface g0/0
R1(config-if)#ip flow monitor FLOW-MON input
R1(config-if)# ip flow monitor FLOW-MON output
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
R1(config)#ip flow-export destination 10.215.26.71 2055
```

✓ Trên Switch 1: Chúng ta thực hiện tương tự trên router.

```
SW1 (config)# flow record FLOW-RECORD
SW1 (config-flow-record)#description stealthwatch
SW1 (config-flow-record)# match ipv4 tos
SW1 (config-flow-record)# match ipv4 ttl
SW1 (config-flow-record)# match ipv4 protocol
SW1 (config-flow-record)# match transport source-port
SW1 (config-flow-record)# match transport destination-port
SW1 (config-flow-record)# match interface input
SW1 (config-flow-record)# match interface output
SW1 (config-flow-record)# collect transport tcp flags
SW1 (config-flow-record)# collect counter bytes long
SW1 (config-flow-record)# collect counter packets long
```

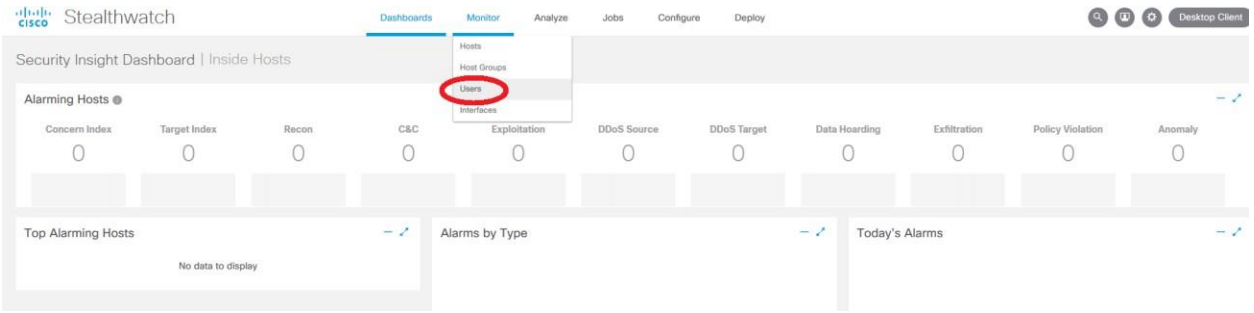
```
SW1 (config)# flow exporter FLOW-EXPORTER
//Destination sẽ trỏ về stealthwatch FlowCollector.
SW1 (config-flow-exporter)# destination 10.215.26.71
SW1 (config-flow-exporter)# transport udp 2055
```

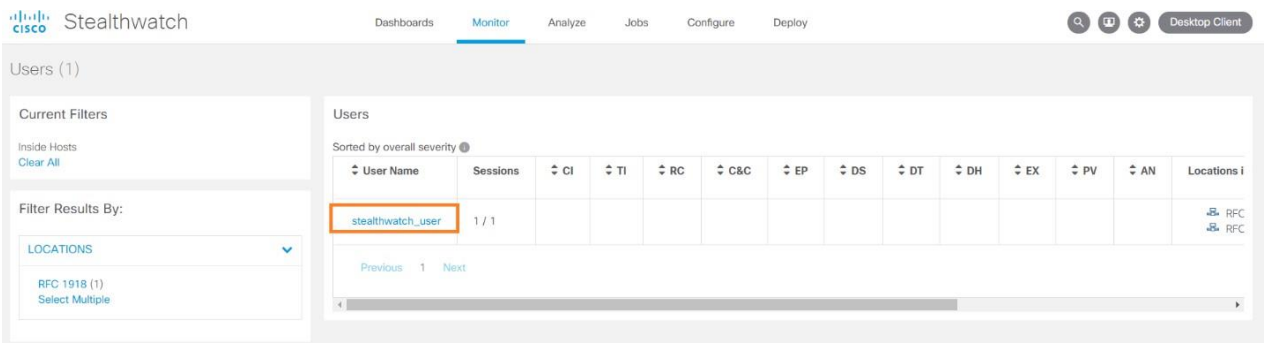
```
SW1 (config)# flow monitor FLOW-MON
SW1 (config-flow-monitor)# exporter FLOW-EXPORTER
SW1 (config-flow-monitor)# cache timeout inactive 15
```

```
SW1 (config-flow-monitor)# cache timeout inactive 15

SW1 (config)#ip flow-exporter destination 10.215.26.71 2055
```

```
SW1(config)#interface g0/0-2

SW1(config-if-range)# ip flow ingress

SW1(config-if-range)#  ip flow egress

SW1(config-if-range)# ip flow monitor FLOW-MON input

SW1(config-if-range)# ip flow monitor FLOW-MON output
```

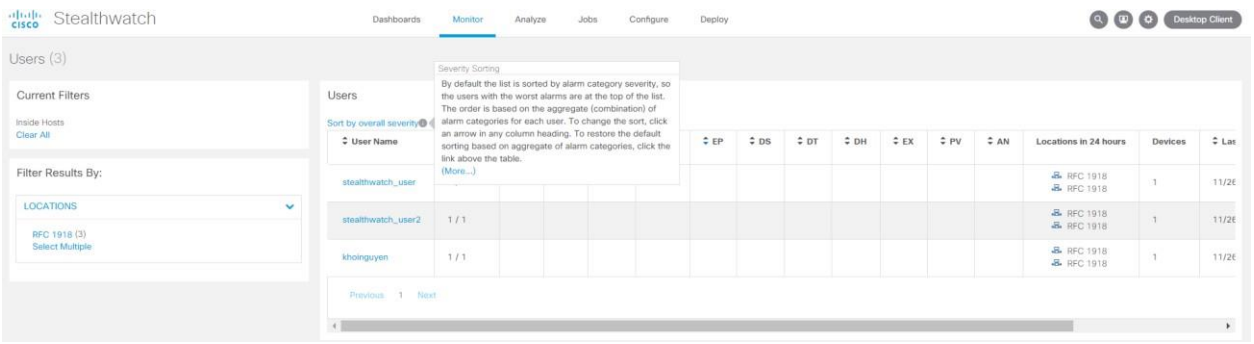
✓ Trên Stealth Watch-SMC:

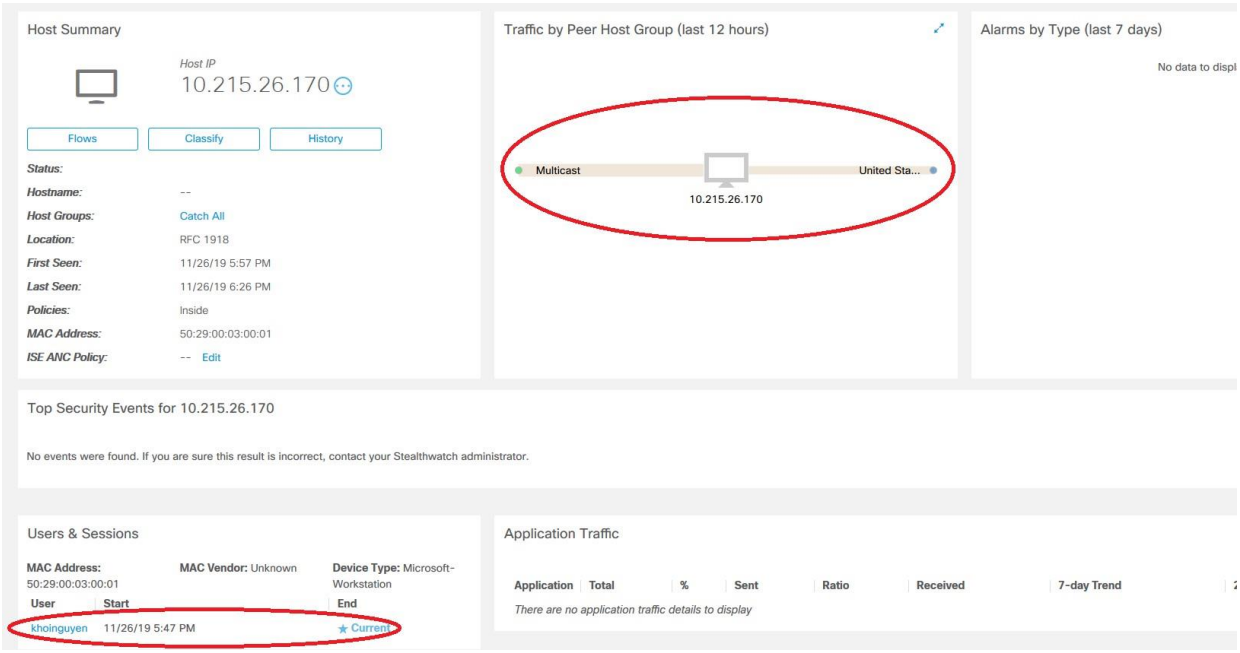




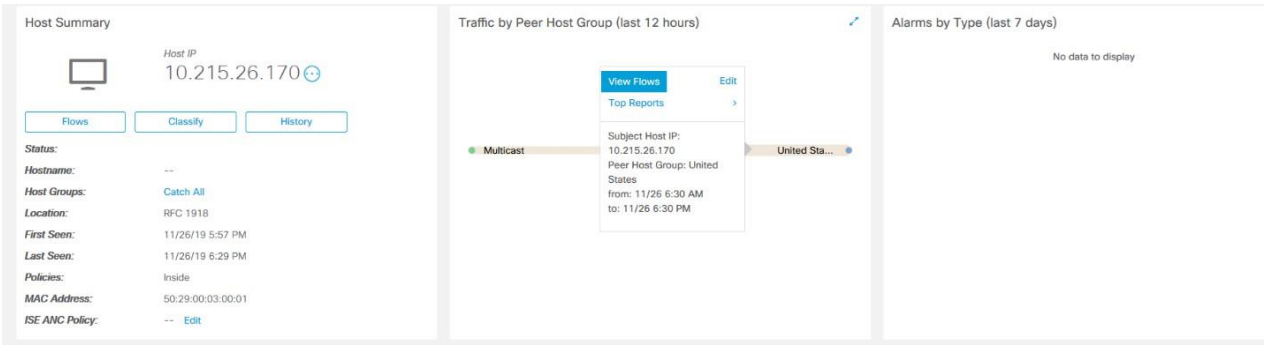
✓ Thử đổi địa chỉ MAC hoặc dùng PC khác để login vào user khác ở card mạng và đi traffic bất kỳ.

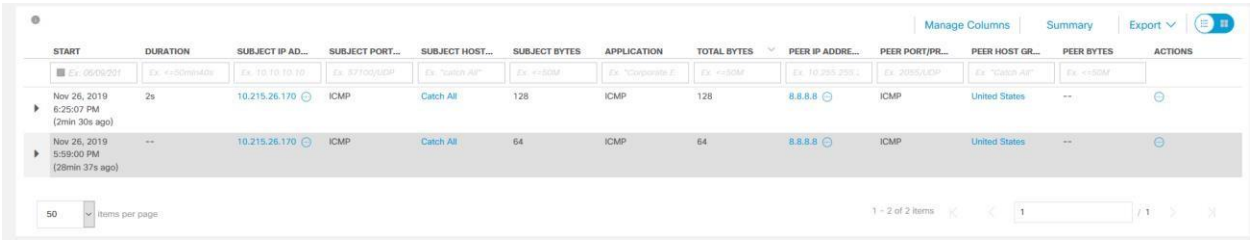
✓ Có thể thấy trong hình dưới đây, stealthwatch đã bắt được 3 user đã login vào mạng với username người dùng được gửi từ cisco ISE.

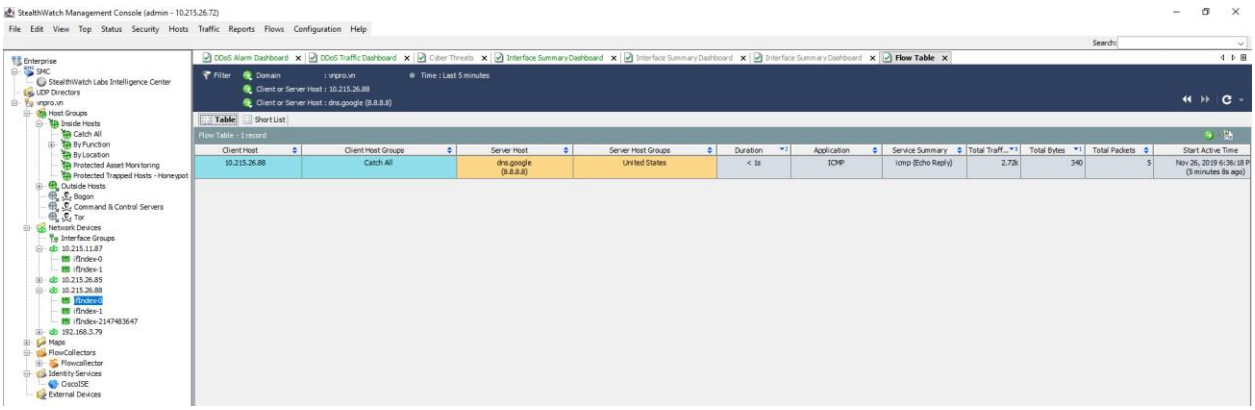




✓ Chuột phải vào đường flow từ 10.215.26.172 đi US chọn **View Flows**, chúng ta có thể quan sát flows đi được từ client trên mà cụ thể là gói icmp đi đến 8.8.8.8







✓ Ngoài ra chúng ta còn có thể quan sát được những dữ liệu application khác hay các transport udp/tcp.